Capítulo 4

Desafios de Segurança e Confiabilidade na Comunicação para Smart Grids

Yona Lopes, Tiago Bornia, Vitor Farias, Natalia C. Fernandes, Débora C. Muchaluat-Saade

Laboratório MídiaCom – Universidade Federal Fluminense (UFF) – Niterói, RJ – Brasil

Abstract

Smart grids will deeply change the way energy is delivered, from generation to consumers. In this new model, the amount of devices controlled and monitored dramatically rises allowing a more automated, smart, and efficient system. To ensure these goals, a network of highly secure communications, reliable, and that provides low delays is necessary so the monitoring and control of the grid can be performed correctly. However, the same interconnected system that transforms the old grid in a smart grid also brings new challenges to this scenario, such as security and reliability. Thus, the central focus of this chapter is the discussion of these challenges. We will discuss the key concepts related to smart grid, focusing on vulnerabilities and attacks that such network may suffer. Solutions and recommendations on key security challenges will also be addressed.

Resumo

A rede elétrica inteligente traz propostas que mudam de forma profunda a maneira como a energia é provida desde a geração até os consumidores finais. No novo modelo, a quantidade de dispositivos controlados e monitorados aumenta demasiadamente compreendendo inclusive o consumidor final, permitindo um sistema mais automatizado, inteligente e eficaz. Para tanto, será necessária uma rede de comunicação altamente segura, confiável e com baixos retardos, de forma que o monitoramento e o controle da rede elétrica possam ser realizados. No entanto, o mesmo sistema interconectado que torna a rede elétrica mais inteligente também traz novos desafios para este cenário, como segurança e confiabilidade. Assim, o foco central deste capítulo é a discussão sobre esses desafios. Serão abordados os principais conceitos relacionados a smart grid, com foco nas vulnerabilidades e ataques que esse tipo de rede pode sofrer. As soluções e recomendações relativas aos principais desafios de segurança também serão abordadas.

4.1. Introdução

Uma rede elétrica inteligente, conhecida como *Smart Grid*, traz propostas inovadoras que mudam de forma profunda a maneira como a energia é provida desde a geração até os consumidores finais [Lopes et al. 2015a]. O sistema elétrico tradicional, de forma geral, contava com uma comunicação que compreendia apenas parte do sistema, como as subestações e seus centros de controle, além da comunicação entre as subestações e entre os centros de controle. No novo modelo, a quantidade de dispositivos controlados e monitorados aumenta demasiadamente compreendendo inclusive o consumidor final, permitindo um sistema mais automatizado, inteligente e eficaz. A comunicação precisará dar o suporte para a estabilização das demandas e para a tarifação, garantindo uma resposta a demanda adequada e o livre mercado para compra e venda de energia em tempo real por consumidores finais. Para tanto, será necessária uma rede de comunicação altamente segura, confiável e com baixos retardos, de forma que o monitoramento e o controle da rede elétrica possam ser realizados.

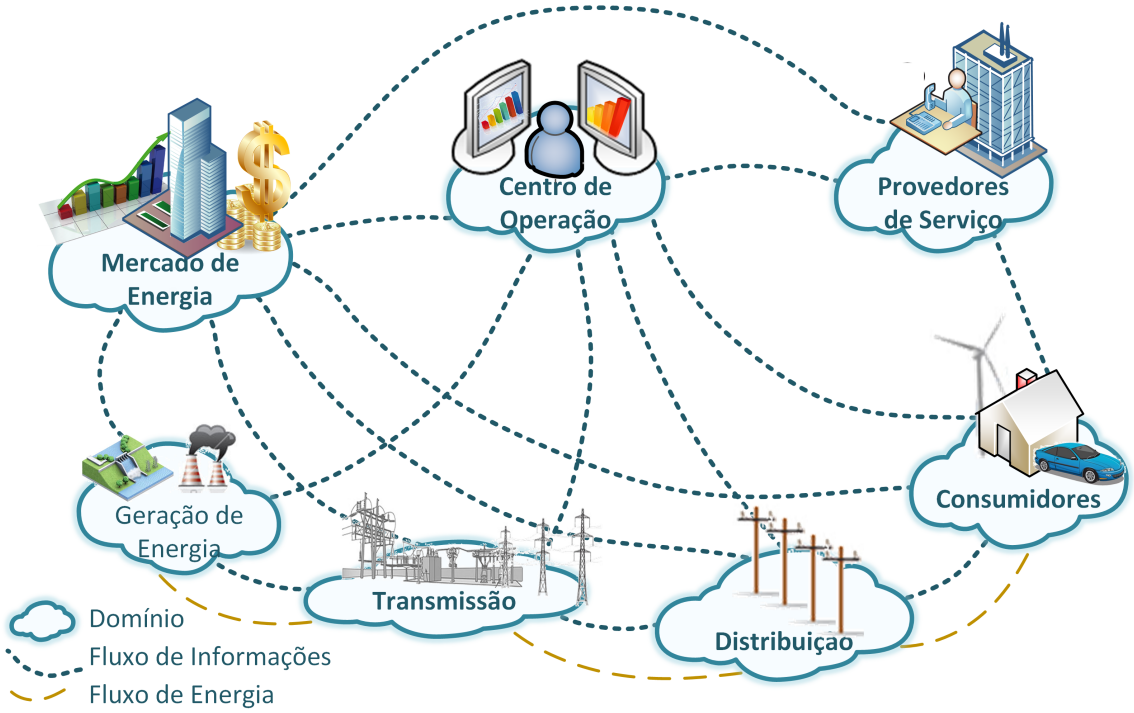


Figura 4.1. Atores das redes elétricas inteligentes e a comunicação entre eles, segundo o modelo proposto pelo NIST [NIST 2010, Lopes et al. 2015a].

De acordo com o modelo conceitual do NIST (*National Institute of Standards and Technology*) [NIST 2010], ilustrado na Figura 4.1, a rede elétrica inteligente é composta de sete domínios lógicos, com agentes e dispositivos inteligentes que devem ser interligados. Nesse novo cenário, os dispositivos finais da rede se tornam mais inteligentes e podem se comunicar diretamente com os centros de controle de dados. De fato, a implantação da rede elétrica inteligente começa com uma inserção em massa de medidores inteligentes. Além disso, o número de IEDs (*Intelligent Electronic Devices* – Dispositivos Eletrônicos Inteligentes) aumenta a fim de apoiar a Automação da Distribuição (*Distribution Automation* - DA). Em geral, a quantidade de dispositivos de automação, tais como

medidores inteligentes e IEDs, e a quantidade de dados coletados a partir desses dispositivos, aumentam significativamente. Dessa forma, a rede elétrica inteligente traz um enorme crescimento no volume de dados que deve ser gerenciado.

A fim de permitir uma implantação de sucesso das redes elétricas inteligentes, uma comunicação de rede robusta entre os dispositivos é necessária. Tal cenário envolve vários nós, enlaces, sistemas, protocolos e tecnologias para compor diferentes tipos de redes, formando uma arquitetura complexa e ampla. Este sistema interligado traz várias vantagens, tais como a visibilidade, a disponibilidade e o controle remoto que tornam possíveis várias novas operações para a concessionária, tornando o sistema mais inteligente. Além disso, novas aplicações de energia, tais como o planejamento de capacidade e o controle do horário de pico, irão melhorar o sistema. Também, novas aplicações facilitarão a implantação de novos serviços de energia, tais como sistemas para auditorias do uso de energia, programas de resposta à demanda e pontos de carregamento de veículos elétricos [Budka et al. 2014].

No entanto, o mesmo sistema interligado que permite a criação de diversas novas aplicações no provimento de energia elétrica também traz ameaças à segurança e faz com que todo o sistema fique vulnerável a ataques. No passado, as redes de comunicação para instalações elétricas ficavam restritas a áreas fechadas e seguras, como em subestações, que garantiam a segurança física da rede. Devido à integração com medidores inteligentes, nuvens, e outras fontes de informação, a segurança física para o acesso à rede não é mais uma opção, o que pode comprometer o controle do sistema elétrico.

Portanto, as redes elétricas inteligentes não podem avançar sem lidar com os problemas relacionados à segurança. Os ataques contra a rede de energia elétrica podem impactar diretamente a população e afetar as pessoas, o comércio, as empresas e qualquer um que não possa ficar sem energia elétrica. Qualquer possibilidade de evento que cause impacto na confidencialidade, na integridade e na disponibilidade dos domínios da rede elétrica inteligente é considerada uma ameaça.

Ataques que tentam ganhar vantagem em cima das vulnerabilidades encontradas em sistemas que trocam informações em uma rede são conhecidos como *data-centric threats* [Wei and Wang 2014]. Essas ameaças podem ser difíceis de detectar e podem resultar em danos críticos para a infraestrutura industrial. Um *worm* pode reprogramar uma instalação de controle industrial para degradar o equipamento e gerar logs de operação falsos, comprometendo a manutenção. Um atacante pode assumir o controle do sistema ou roubar informações confidenciais mesmo sem acesso físico à planta [Wei and Wang 2016]. Ataques contra instalações nucleares, como o primeiro worm descoberto em sistemas industriais como o Stuxnet [Falliere et al. 2011] e o ataque ao sistema elétrico ucraniano [Assante 2016], são uma demonstração do potencial destrutivo de ameaças cibernéticas.

Por exemplo, o SCADA (*Supervisory Control and Data Acquisition*), que é um sistema muito importante usado para supervisionar e controlar a operação do sistema elétrico, deve ser interligado com toda a estrutura de rede. Vulnerabilidades do sistema SCADA são geralmente correlacionadas ao uso de uma Interface Homem-Máquina (IHM) e os históricos de dados [Wilhoit 2013]. Históricos de dados são bancos de dados de *logs* que armazenam as tendências e informações históricas sobre os processos de um sistema de controle industrial. Se o atacante puder comprometer a IHM, ele terá acesso a áreas

seguras onde ele pode modificar o ajuste de dispositivos ou controlar equipamentos. Uma abertura ou fechamento indevido de um disjuntor pode causar uma interrupção no fornecimento de energia de forma desnecessária. Além disso, caso um circuito esteja em manutenção, um fechamento indevido de um disjuntor poderia ameaçar a vida humana. Da mesma forma, se um invasor puder acessar o histórico de dados, poderá ler o banco de dados centralizado com todas as informações de registro sobre o ambiente do sistema de controle industrial. Assim, o atacante terá informações sobre os sistemas de segurança, bem como uma lista de comandos usados em dispositivos como IEDs e Controladores Lógicos Programáveis (*Programmable Logic Controller* - PLC) e IEDs. Não só o SCADA é vulnerável a ataques, mas também medidores inteligentes e quaisquer IEDs. É importante notar que os medidores inteligentes estão nas residências dos clientes, que são potenciais atacantes. Estes poderiam alterar os dados de consumo, divulgar informações relacionadas à privacidade e usar medidores inteligentes como um ponto de entrada para grandes ataques. Portanto, interrupções e danos causados por ataques passivos ou ativos tornam-se uma ameaça real. As motivações para os ataques variam desde a redução de custos na conta de energia à promoção do terrorismo.

Este capítulo aborda as questões de segurança relacionadas às redes elétricas inteligentes, suas principais vulnerabilidades e ameaças. Assim, descrevem-se as principais falhas de arquitetura que tornam o sistema elétrico vulnerável a ataques para causar interrupções de energia, furto de energia e quebra de privacidade.

O restante do texto está organizado da seguinte forma. Inicialmente, uma breve descrição das redes elétricas inteligentes é feita na Seção 4.2. Em seguida, na Seção 4.3, os principais conceitos de segurança relacionados com as redes elétricas inteligentes são detalhados. Os ataques mais comuns relacionados a *smart grids*, considerando tanto ataques às subestações quanto ataques à Infrastrutura de Medição Avançada (AMI), são detalhados na Seção 4.3.2. As principais soluções atuais para criar um ambiente seguro para as comunicações de *smart grids* são apresentadas na Seção 4.4. Por fim, as últimas seções do capítulo apresentam as conclusões e direções futuras para pesquisas na área.

4.2. Redes Elétricas Inteligentes

Devido ao crescente aumento populacional e ao aumento do número de equipamentos em uso nas residências, a demanda por energia tem crescido cada vez mais nos últimos anos [Lopes et al. 2015a]. No entanto, para acompanhar esse crescimento, o setor precisa investir muito em infraestrutura. Um caminho, usado por muito tempo, foi o investimento no aumento da infraestrutura para geração de energia, com a construção de novas usinas geradoras para suprir essa demanda. Contudo, a regulamentação para as construções e demandas ambientais muitas vezes atrasam e/ou impedem esse tipo de construção. Essas caraterísticas resultam na necessidade de estudo e implementação de novos mecanismos e sistemas para suprir o aumento da demanda sem a construção de novas usinas geradoras. Assim, a modernização da infraestrutura existente e o desenvolvimento de novas propostas ganharam força nos últimos anos. Outro ponto importante é que o sistema elétrico já vinha passando pela necessidade de modernização, já que pouca inovação tinha sido feita nas últimas décadas. Consequentemente, os equipamentos utilizados e as tecnologias, algumas vezes, eram os mesmos de 40 anos atrás [Gungor et al. 2011]. Os medidores residenciais tradicionais, por exemplo, precisam de funcionários para realizar a leitura do

consumo e o corte/religamento de energia, o que gera um custo alto para a empresa concessionária. Desta necessidade inevitável de modernização do sistema elétrico, surgiram as redes elétricas inteligentes, ou *Smart Grids*, tornando imprescindível a implantação de um sistema de comunicação mais "inteligente" [Lopes et al. 2012].

Esta modernização vem causando uma grande revolução nas redes de energia elétrica, aumentando os ganhos em confiabilidade, eficiência energética, participação dos consumidores e geração de uma energia mais limpa [Patel et al. 2011]. Tal revolução está ocorrendo porque as redes elétricas inteligentes são baseadas em conceitos como a monitoração inteligente de todos os dispositivos do sistema e a transmissão dos fluxos de comunicação e de energia de forma bidirecional, cenário bastante distinto do tradicional. Dentre as novas propostas, destacam-se a geração de energia de forma distribuída, o amplo uso de fontes renováveis, o uso de carros elétricos, um intenso monitoramento da rede elétrica, o uso de medidores inteligentes, entre outros. Com as redes elétricas inteligentes, o consumidor passa a ser parte fundamental do funcionamento e controle da rede elétrica. Os consumidores, que no sistema tradicional apenas consomem energia, podem ter nesse novo modelo também o papel de produtor de energia elétrica. Além disso, os medidores inteligentes localizados nas residências passam a gerar uma quantidade enorme de informação que poderá ser usada para o gerenciamento e controle do sistema. Portanto, para que o desenvolvimento da rede elétrica inteligente seja possível, a inteligência e as tecnologias como as de supervisão, controle e proteção, antes existentes apenas em parte do sistema elétrico, se tornam imprescindíveis da geração até o consumidor final [Lopes et al. 2015a].

Um ponto importante é que esse novo sistema elétrico depende de uma sofisticada infraestrutura de redes de comunicação para dar suporte à comunicação entre os dispositivos inteligentes que monitoram e atuam na rede. Além disso, é necessário dar suporte às empresas de distribuição de energia e aos usuários, que podem consumir ou gerar energia [Budka et al. 2010]. Novas necessidades surgem, como o aumento da confiabilidade da rede, o aumento da eficiência operacional da rede, a melhora da qualidade para o consumidor e o aumento da variedade dos serviços providos. Porém, todas essas melhoras trazem diversos desafios para as redes de comunicação e um dos mais importantes, se não o mais importante deles, é o provimento de segurança. Conhecer as principais áreas chaves da rede elétrica inteligente ajuda a entender os problemas e desafios na área de segurança e suas possibilidades de solução.

4.2.1. Domínios das Redes Elétricas Inteligentes

O modelo conceitual das redes elétricas inteligentes foi proposto pelo NIST [NIST 2010] e é ilustrado na Figura 4.1 com fluxos bidirecionais de informação. O NIST divide o modelo em sete domínios que, juntos, representam a comunidade de redes inteligentes de interesse. Esses domínios são:

- Domínio de geração de energia: composto pelas tradicionais plantas de geração e pelo armazenamento de energia. Para que possa trocar informações sobre a energia gerada ou armazenada, o domínio de geração troca dados com o domínio da operação da rede elétrica e com o domínio do mercado de energia.

- Domínio dos consumidores: além da funcionalidade de consumo de energia, a geração de energia em pequena escala e o armazenamento de energia também se encontram nesse domínio. Para isso, o domínio dos consumidores se comunica com os domínios de operação da rede e de mercado de energia.

- Domínio de Distribuição e Domínio de Transmissão: os sistemas de transmissão e distribuição passam a ser muito mais ativos, trocando informação com a operação da rede elétrica, com consumidores e seus medidores inteligentes e com o mercado de energia.

- Domínio de provedores de serviços: se comunica com os consumidores para faturamento, operações de resposta à demanda e serviços de terceiros. Para obter informações de medições e controle da rede elétrica, se comunica também com o domínio de mercado e de operação da rede elétrica.

- Domínio do mercado de energia (atacado, varejo e comércio): é responsável pelo balanceamento de oferta e demanda de energia e, portanto, coleta e envia informações de oferta e demanda aos domínios de geração, provedores de serviços e operação da rede elétrica inteligente.

- Domínio da operação da rede elétrica: se comunica com todos os outros domínios a fim de coletar os dados para garantir o controle e a operação eficiente do sistema.

Esses domínios foram ilustrados na Figura 4.1 e se comunicam entre si conforme mostrado na figura.

Apesar de serem domínios separados, são intimamente relacionados. Uma aplicação de um domínio pode interferir na outra, pode necessitar de dados de outros domínios, pode se comunicar com outra aplicação, etc. Além disso, aplicações tradicionais deverão coexistir com as novas aplicações advindas das redes elétricas inteligentes (as áreas que darão origem a essas aplicações são descritas na Seção 4.2.2) e/ou evoluir para acompanharem as mudanças e novas aplicacões. Exemplos de aplicações tradicionais são a teleproteção e o SCADA também chamado de *software* supervisório. A teleproteção usa um sistema de comunicação entre duas subestações. Com isso, se um equipamento de proteção em uma subestação detecta uma falha em uma extremidade, a outra extremidade é notificada e ações de proteção são iniciadas a fim de isolar a falha. Já o sistema SCADA, que no passado era suportado por mainframes e sistemas fechados de fornecedores, atualmente, faz uso da rede de comunicação para interconectar todos os equipamentos das subestações que são supervisionados por ele. O SCADA é utilizado para supervisionar, controlar, otimizar e gerenciar os sistemas de geração e transmissão de energia elétrica. Já o SCADA de nova geração deve ser adaptado para um cenário com maior granularidade de supervisão e novas possibilidades. Dentre os benefícios trazidos pelos sistemas SCADA de nova geração, destacam-se a análise de consumo e demanda, a análise da carga dos consumidores, a verificação de falhas, o rearranjo da topologia, a análise da carga nos transformadores, a medição inteligente, entre outros [Lopes et al. 2012]. Com a evolução para as redes elétricas inteligentes, o SCADA incorporará novos elementos inteligentes, tais como: unidades de medição fasorial, relés inteligentes, novas fontes de

geração de energia com utilização de fontes renováveis, armazenamento de energia em veículos elétricos (EV), medidores inteligentes, etc [Giani et al. 2011].

Ao permitir geração de energia pelo consumidor, uma rede elétrica inteligente promove uma estreita relação entre compradores e vendedores, clientes e concessionárias. Um fluxo bidirecional de energia e comunicação bem como as capacidades *plug-and-play* são seu objetivo final e permitirão que várias tecnologias possam fornecer, entregar e utilizar os recursos de forma confiável, eficiente e segura.

4.2.2. Áreas chaves das Redes elétricas inteligentes

Como abordado anteriormente, as aplicações tradicionais, como a teleproteção e o SCADA, deverão coexistir com as novas aplicações advindas das redes elétricas inteligentes. Estas aplicações surgem de áreas chaves que permitem o desenvolvimento de novos sistemas. Dentre as áreas existentes estão a infraestrutura de medição avançada (AMI - *Advanced Metering Infrastructure*), a microgrid, a planta de energia virtual (VPP- *Virtual Power Plant*), o gerenciamento pelo lado da demanda (DSM - *Demand Side Management*) e a resposta à demanda (DR - *Demand Response*), detalhados a seguir [Lopes et al. 2012].

4.2.2.1. Infraestrutura de Medição Avançada

A AMI (*Advanced Metering Infrastructure*) é um sistema integrado composto por medidores inteligentes, infraestrutura de comunicação e sistemas de gerenciamento capazes de permitir comunicação bidirecional entre medidores e concessionária. A AMI visa permitir diversas facilidades para consumidores residenciais, comerciais e industriais. Sua infraestrutura será detalhada na Seção 4.3.3.1.

As concessionárias geralmente iniciam a implantação das redes elétricas inteligentes pela AMI. Isso se deve, principalmente, a necessidade de informações, monitoramento e comunicação bidirecional entre consumidores e concessionária. A AMI vai além da medição de energia periódica, gerando dados que são usados por outras aplicações ou domínios das redes elétricas inteligentes. Por exemplo, as medidas fornecidas pelos medidores inteligentes também são usados para dar suporte às aplicações de tarifas em tempo real (*Real Time Pricing* - RTP), tarifas horo-sazonais (*Time of Use* - TOU) e tarifa de picos críticos (*Critical Peak Pricing* - CPP), ferramentas usadas para tarifação e para resposta a demanda [Budka et al. 2010] [1]. Mecanismos de tarifação dinâmica, como o TOU e o CPP, contribuem para uma implementação da resposta a demanda eficiente, o que contribui para uma possível redução de custos. Além disso, o medidor pode fazer parte de um domínio de geração quando na casa do consumidor tiver uma geração local. Assim, as informações oriundas do gerador residencial, parte de uma rede de geração distribuída (GD), poderão ser trocadas através do uso do medidor inteligente e da AMI.

Com a AMI, torna-se possível a detecção de falhas na rede elétrica de distribuição e a detecção de furtos de energia. Além disso, quando a AMI está trafegando informações de alguma GD, torna-se parte do sistema de proteção e controle, tornando possível, por

[1] Resposta a Demanda, do inglês *Demand Response*, é a iniciativa de alterar temporariamente o consumo de energia em resposta às condições de fornecimento de energia ou aos eventos na rede [EPRI 2009].

exemplo, o isolamento de falhas nos sistemas elétricos. Outra vantagem é que a AMI permite que eletrodomésticos respondam a sinais de preço, aumentando ou diminuindo o consumo de acordo com as variações de mercado. Com a AMI, o religamento e o corte de energia podem ser feitos de forma remota, além de permitir o acompanhamento do consumo. Em resumo, a AMI permite às concessionárias de serviços públicos:

- obter uma leitura automática e remota (telemetria) e faturamento precisos;
- controlar remotamente o corte e religamento do fornecimento de energia;
- detectar interrupções na distribuição de energia;
- tarifar em tempo real e fazer a tarifação horo-sazonal (TOU);
- fornecer outras medições como água e gás;
- impedir a manipulação indevida de leituras e dados de faturamento;
- melhorar o serviço de suporte ao consumidor final através de comunicação em tempo real; e
- possibilitar a implementação do sistema de proteção e controle dos dispositivos sem a necessidade de implementação de nova infraestrutura.

A implementação da AMI, com informações em tempo real, contribui para maior retorno de investimento e custo operacional mais baixo, o que justifica o investimento em longo prazo. Outra aplicação de grande prioridade é a resposta à demanda, que usa os dados gerados em tempo real para tomar ações com relação à geração de energia. Nesse sentido, ter uma rede confiável, com informações disponíveis em tempo real, torna-se uma premissa básica para entrega de energia confiável para os usuários finais. A grande maioria das falhas no provimento de energia podem ser evitados ou contornados pelo monitoramento em tempo real, pelo diagnóstico e proteção da rede, que precisam ser confiáveis e seguros.

4.2.2.2. Microgrids

A *microgrid* é um novo paradigma que consiste na criação de pequenos sistemas elétricos localizados e compostos por geração, armazenamento e cargas com a ideia de ser autossuficiente. É um novo paradigma que pode combinar vários Recursos Energéticos Distribuídos (DER - *Distributed Energy Resources*) para formar um todo. As unidades de DER são as fontes geradoras de energia que podem ser compostas por unidades de geração distribuída e por unidades de armazenamento distribuído, incluindo veículos elétricos [Lopes et al. 2015a].

Assim, esse conceito inclui GD, armazenamento de energia, conexão entre GD e rede externa de energia, e mecanismos de controle [Pan et al. 2014]. Várias *microgrids* interligadas, de acordo com o conceito *plug and play*, podem criar uma rede macro, chamada de *macrogrid* [Lopes et al. 2012]. Com isso, o controle de uma *microgrid* deve considerar três camadas, sendo elas o fluxo de informação, o fluxo de tensão e a camada física (real), mostrada na Figura 4.2. Embora a *microgrid* opere principalmente ligada à rede de distribuição [Bayod-Rújula 2009], ela pode operar na forma de "ilha", onde a própria energia gerada pela geração distribuída supre a necessidade da demanda [Lopes et al. 2012]. Esse modo, também chamado de ilhamento, faz com que a *microgrid* funcione de forma autônoma, desligada da rede externa. Esse modo proporciona continuidade do fornecimento em caso de falhas na rede externa. Nesse caso, a *microgrid* pode ser ressincronizada com o macrossistema após a restauração da rede externa [Bayod-Rújula 2009]. Dessa forma, as *microgrids* podem melhorar a confiabilidade no fornecimento de energia, pois se baseiam na premissa de que a geração de energia, ou a maior parte dela, está próxima ao consumidor e restrita a uma área menor.

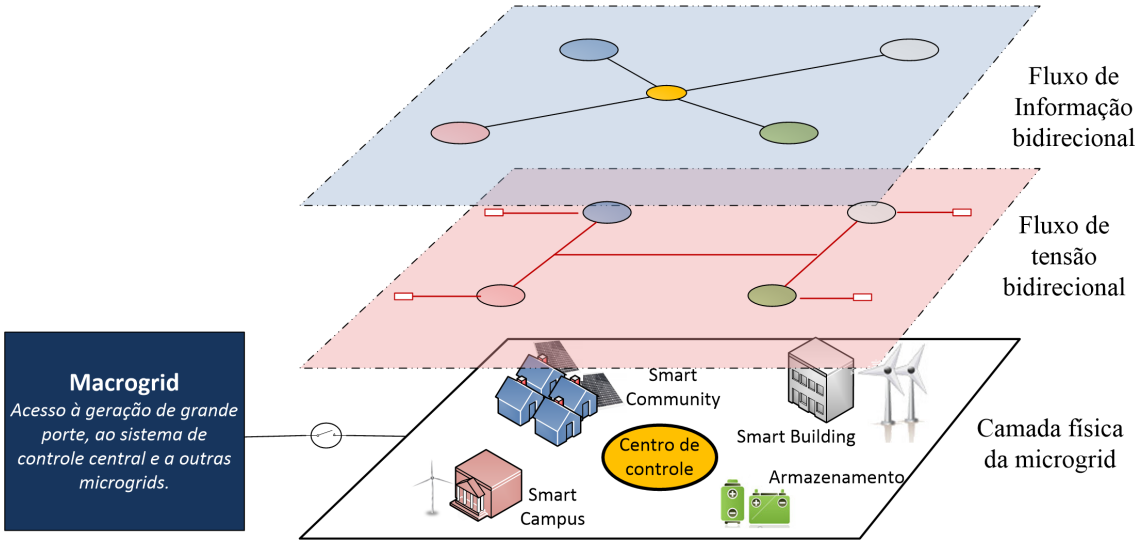


Figura 4.2. Exemplo de uma *microgrid*, onde a comunição e a distribuição elétrica coexistem, interligando as diversas fontes de geração distribuídas [Lopes et al. 2012].

Dentro do contexto de uma *microgrid*, as fontes de energia podem ser de geradores ou ainda de bancos de armazenamento de energia. Um tipo de banco de armazenamento que pode ser de grande utilidade no momento de uma falha do fornecimento são as baterias dos carros elétricos.

É desafiadora a necessidade de tornar o lado do consumidor mais inteligente, mais eficiente e rentável. Especialmente no futuro, a GD e as *microgrids* serão muito comuns com casas e prédios fazendo uso da energia renovável. Quando a capacidade das fontes geradoras exceder a própria demanda, o restante de energia deverá ser exportada para a *microgrid* e a *macrogrid*. Uma programação dinâmica e otimizada destes geradores distribuídos pode alimentar as demandas e reduzir o custo total, além de alcançar uma maior eficiência energética em escala.

Em uma *microgrid*, são usados controladores, que são dispositivos que são co-

nectados aos geradores e às cargas para controlar o funcionamento destes. As cargas são quaisquer dispositivos elétricos conectados à rede que necessitem de energia elétrica para funcionar, ou seja, os consumidores de energia. As cargas podem ter características bem diferentes, podendo ser usuários residenciais, comerciais ou industriais.

Ressalta-se que a *microgrid* tem seus próprios requisitos de controle entre geradores e consumidores de energia devido à sua escala limitada. Os métodos de controle utilizados dentro das *microgrids* podem ser centralizados, distribuídos ou hierárquicos ou métodos que combinam vários tipos. O mecanismo de controle deve permitir a adição e remoção flexível de geradores distribuídos em um estilo *"plug-and-play"*, sem perturbar o resto do sistema ou sem a necessidade de reconfigurar todo o sistema. O controle também pode atribuir diferentes prioridades às cargas, que podem ser priorizadas de acordo com a sua importância como mais ou menos críticas.

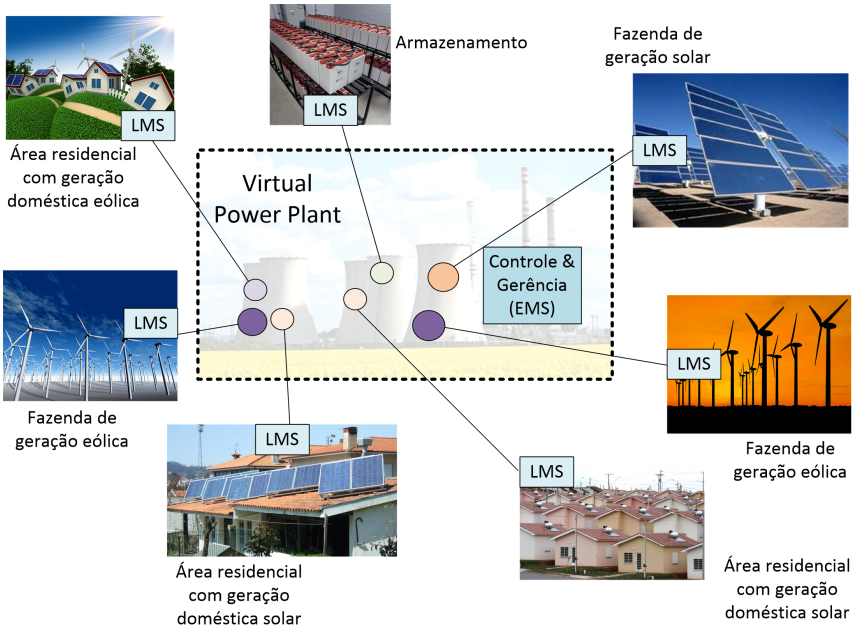
4.2.2.3. VPP (*Virtual Power Plant*)

Uma VPP, também conhecida como *Virtual Utility*, pode ser definida como um novo modelo de infraestrutura de energia que consiste na integração de diferentes tipos de GD controlados por um sistema de gerenciamento de energia (*Energy Management System* - EMS). A rede é composta por um controle centralizado de diferentes grupos de geração distribuída, chamados de *clusters*. Cada um destes *clusters* é controlado por uma estação de gerenciamento local (*Local Management Station* - LMS) e cada LMS tem informações sobre os requisitos de energia dos usuários conectados ao seu *cluster*, como eletricidade, nível de água no tanque, etc [Bayod-Rújula 2009]. Esse sistema é ilustrado na Figura 4.3.

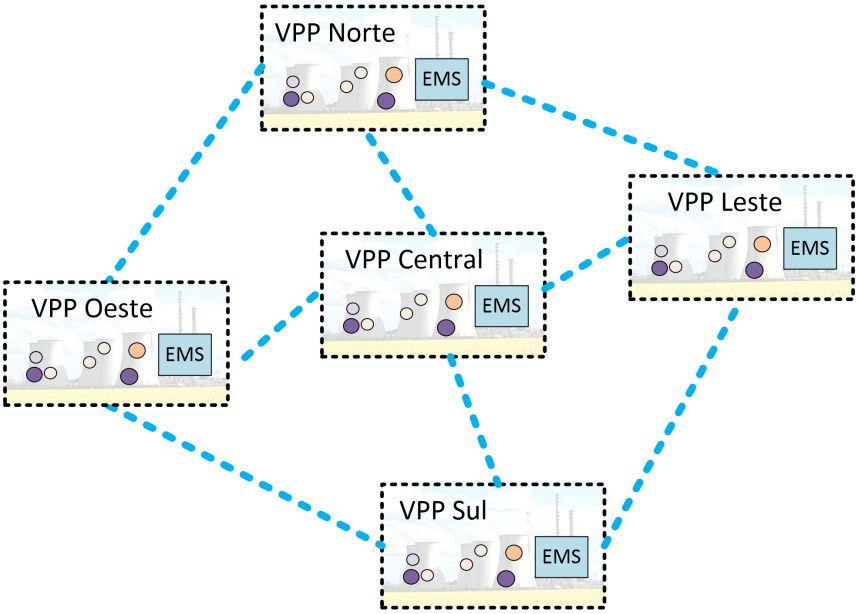
O EMS recebe as informações de cada LMS e define a entrada ou saída de energia de cada *cluster* na rede. Com a informação da EMS, o LMS configura o cluster para que ele entre em funcionamento ou fique em *standby*. Além disso, o EMS pode priorizar o uso de recursos de energia distribuídos (DER) ao invés do uso de combustíveis fósseis.

Os benefícios da VPP estão relacionados à otimização do rendimento de utilização de toda a rede, à alta confiabilidade da produção de energia, ao controle total da rede para atingir o principal objetivo da EMS, à alta velocidade necessária para acompanhar as mudanças rápidas na demanda do sistema e à alta integração dos DER [Bayod-Rújula 2009].

Para um operador de rede ou concessionária de energia, a compra de energia a partir de uma VPP é equivalente a compra a partir de uma planta convencional. O conceito de VPP não é por si só uma nova tecnologia, mas sim um método de organização de geração e armazenamento descentralizado de uma forma que maximiza o valor da energia gerada para a concessionária. A VPP usando GD, DER e armazenamento de energia tem potencial para substituir a planta convencional [Bayod-Rújula 2009].



(a) Modelo de VPP, com o controle local e central das várias fontes geradoras.



(b) Agregação de GD com resposta à demanda, através da gestão de diversas VPPs integradas.

Figura 4.3. Conceito de *Virtual Power Plant* (VPP) [Lopes et al. 2015a].

4.2.2.4. Gerenciamento pelo lado da demanda (DSM) e a resposta à demanda (DR)

Segundo o EPRI (*Electric Power Research Institute*), resposta à demanda (*Demand Response* - DR) é uma mudança temporária no consumo de energia em resposta às condições de fornecimento de energia ou aos eventos na rede [EPRI 2009]. A inclusão de novas fontes de energia e elementos de armazenamento combinados com a necessidade de re-

duzir os picos de carga impulsionaram a introdução de aplicações de resposta à demanda. Para isso, incentivos monetários podem ser usados de modo a evitar preços elevados de energia. Essas aplicações objetivam prover confiabilidade através de uma série de ações que visam reduzir a carga da rede no horário de pico, quando a concessionária está perto da sua capacidade máxima. Por exemplo, pode-se reduzir a quantidade de energia consumida pelos aparelhos durante o período de pico de potência, evitando inclusive apagões. Nesse cenário, o cliente passa a ter um papel ativo no fornecimento de energia elétrica. Esse sistema permite que consumidores transfiram o consumo de energia para momentos fora do horário de pico, tomando vantagem do preço da energia em tempo real, das informações da rede, controle da carga, etc [Bayod-Rújula 2009].

Conceitualmente, a resposta à demanda é equivalente ao aumento de geração no processo de equilíbrio do sistema. A solução de reduzir o uso de energia e utilizar a geração distribuída quando a oferta de energia é baixa tem ganhado cada vez mais aceitação no mercado. A DR e a DSM reduzem a carga e acrescentam a capacidade de geração em caso de emergência.

A DR, muitas vezes, usa a GD de forma que a energia passe a ser provida de um ponto mais próximo do consumo ou passe a receber energia de outras fontes conectadas à rede. Assim, em alguns casos, a DR pode não só reduzir o consumo global de energia, mas também mudar a origem da geração para uma GD. Ressalta-se que para que seja possível a implementação da DR, outro *driver* da rede elétrica inteligente precisa ser implementado: a automação da distribuição (DA). A DA é a ideia de se estender o monitoramento e controle da rede até a distribuição, de forma que dispositivos que antes não eram automatizados passem a ser. Atualmente, empresas de energia estão acostumadas com a gestão de um número limitado de pontos de monitoramento e controle, por exemplo, centenas de subestações. Novas tecnologias de comunicação devem ser introduzidas na distribuição a fim de conectar dezenas de milhares de *endpoints* encontrados na automação da distribuição.

4.2.2.5. As Áreas Chaves e o Desafio de Provimento de Segurança

A implementação das novas áreas advindas das redes elétricas inteligentes resulta no aumento do número de usuários com diferentes níveis de confiabilidade cooperando entre si e atuando no sistema, tornando o provimento de segurança uma questão crucial [Neuman and Tan 2011, Zhu et al. 2011]. Entre os mecanismos necessários para o provimento de segurança, destacam-se a autenticação das solicitações dos usuários, a autenticação de mensagens enviadas por aparelhos inteligentes, como mensagens de oferta de energia de fontes alternativas [Yan et al. 2011], e as métricas para avaliar a importância das informações trocadas entre usuários e fornecedores na rede [Chim et al. 2011]. A troca de mensagens tem impacto em todo o controle e gerência da rede, de forma que a autenticidade e a confiabilidade dos dados trocados devem ser sempre asseguradas pela infraestrutura da rede elétrica inteligente. A segurança na comunicação também diz respeito à confidencialidade dos dados da rede e dos usuários, tais como informações de endereço e de cartão de crédito [Lopes et al. 2015a].

Especialmente no modelo de *microgrid*, todas as casas podem fornecer e consu-

mir energia da *microgrid*, de tal forma que os fluxos energéticos podem fluir bidirecionalmente e ser dinamicamente reconfigurados. É importante que o sistema da *microgrid* funcione de forma distribuída, mas evitando que mensagens falsas sejam inseridas na rede com o fim de prejudicar a distribuição de energia ou a cobrança posterior ou, ainda, que informações sejam roubadas para ferir a privacidade dos usuários. Em particular, os roteadores das *microgrids* podem utilizar enlaces sem fio, os quais são mais susceptíveis a ataques do que redes cabeadas [Lopes et al. 2012]. Portanto, a segurança das *microgrids* e de seus roteadores deve contar com mecanismos de controle de acesso, gerência de chaves e certificados, detecção de intrusão e de mau comportamento, entre diversos outros [Zhu et al. 2011].

Para que os dados da GD e da AMI sejam trocados, os medidores inteligentes precisam estar conectados à rede, enviando e recebendo mensagens. Uma vez que segurança é uma preocupação, é natural supor que os medidores serão equipados com as técnicas de segurança padrão, tais como utilização de certificados digitais e criptografia [Lopes et al. 2012]. Contudo, já é sabido que o uso dessas técnicas não é suficiente para impedir que o sistema seja atacado [Cleveland 2008]. Vide a Internet, a qual está munida dessas e outras técnicas, mas ainda sofre com frequentes problemas de segurança, em especial os ataques de negação de serviço [Wang et al. 2011]. O volume de ataques está fortemente correlacionado com a quantidade de *hackers* espalhados pelo mundo. Muito embora muitos *hackers* ajam maliciosamente para obter vantagens, muitos são adolescentes querendo quebrar novas barreiras. No contexto das redes elétricas inteligentes, a preocupação é relativa à qual impacto que esses *hackers* teriam sobre a rede elétrica, uma vez que tiverem dentro de suas casas medidores inteligentes capazes de interferir ativamente no funcionamento do sistema. Os incentivos para criar ataques na rede vão desde conseguir mudar contas de luz até conseguir causar apagões em cidades inteiras [Rahman et al. 2012]. Dessa forma, a segurança na AMI interfere não apenas no gerenciamento doméstico da energia, mas também na segurança dos controles de automação das subestações em *grids* e *microgrids* [Lopes et al. 2012].

Outro fator chave para segurança é que as demandas para automação de sistemas de energia controlados por computador têm crescido enormemente devido a sua importância [Cheung et al. 2007]. Os IEDs, que participam da proteção, do controle e da automação do sistema elétrico, têm uma comunicação autônoma na rede e podem evitar que uma falha no sistema elétrico de potência seja propagada causando, por exemplo, um apagão. No entanto, caso tenham um mau funcionamento, devido a um ataque por exemplo, também podem causar uma falha. O sistema tem que ser seguro o suficiente para que o acesso desses dispositivos por terceiros mal intencionados não seja permitido. Por exemplo, um pequeno atraso na transmissão de dados para operar o equipamento de proteção pode resultar em falha na subestação [Cheung et al. 2007].

Muito tem se pesquisado na área de segurança para *smart grids*, mas, devido a sua importância e ampla gama de possibilidades de ataque, é uma das áreas com mais desafios e oportunidade de pesquisa.

4.3. Segurança da Informação em *Smart Grids*

A compreensão do impacto dos ataques sobre as comunicações da rede elétrica depende da compreensão do conceito de incidente cibernético. De acordo com FIPS (*Federal Information Processing Standards*), este conceito é definido da seguinte forma:

> "Uma ocorrência que ponha em risco real ou potencial, a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação dos processos que o sistema, armazena ou transmite ou que constitua uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança, ou políticas de uso aceitável."[PUB 2006]

Recentemente, a discussão sobre as ameaças de segurança cibernética contra as redes de energia elétrica aumentou e tornou-se uma questão fundamental para *smart grids*. A integração de modelos de informação com as redes de comunicação para sistemas de energia trouxe novos desafios de segurança relacionados com a autenticidade, confidencialidade, integridade e disponibilidade. A interconexão de dispositivos que são distribuídos em locais sem segurança física é uma das principais preocupações. Por exemplo, o uso de uma AMI configura uma ameaça especial, pois os usuários finais são capazes de introduzir diretamente informação no sistema. A invasão de medidores por usuários, vírus ou *hackers* executando ataques de negação de serviço poderia interromper o fornecimento de energia para uma cidade inteira.

Os ataques contra *smart grids* podem ser devastadores, pois incluem toda a rede de energia, compreendendo desde as subestações e redes de distribuição até as residências e instalações comerciais e industriais. As consequências dos ataques variam de falhas no serviço até danos físicos, no caso em que um atacante é capaz de perturbar o sistema de proteção, comprometendo a segurança em instalações elétricas. As soluções para essas ameaças ainda estão em discussão e podem incluir técnicas de segurança bem conhecidas já aplicadas na Internet e novos protocolos de segurança para comunicações em *smart grids*. Para proporcionar uma melhor compreensão desses ataques e suas medidas preventivas, os principais conceitos de segurança relacionados a este cenário serão discutidos: autenticação, autorização, responsabilização, privacidade, integridade, disponibilidade e proteção física.

- Autenticação

  A autenticação é a capacidade de verificar a identidade de uma entidade. Em redes inteligentes, todas as entidades no sistema devem ter uma identificação verificável. Isto significa que todas as partes envolvidas, como usuários, empresas, IEDs, sensores, dispositivos domésticos, medidores inteligentes, carros elétricos, etc., devem ser identificados de forma exclusiva no sistema de um modo seguro. Na Internet, isto pode ser conseguido pela utilização de uma infraestrutura de chave pública (PKI - *Public Key Infrastructure*) ou sistemas de identificação mais simples no caso de dispositivos menos sensíveis. Esta tecnologia poderia ser aplicada de um modo simples para as redes inteligentes. Por exemplo, os sistemas de supervisão e controle, tais como o SCADA, que têm uma função importante para automação de subestações e podem controlar os dispositivos de campo, devem ser identificados pelo

uso de uma certificação digital para evitar ataques *man-in-the-middle*. Isso implica a compra de um certificado publicamente verificável. Este tipo de investimento, no entanto, não é justificável para dispositivos dentro de uma rede doméstica. Neste caso, onde não espera-se que os dispositivos interajam com sistemas sensíveis, mas apenas forneçam informações e serviços úteis para o usuário, os dispositivos podem ser autenticados por certificados autoassinados ou esquemas de login/senha. Um bom sistema de autenticação é a base principal para fornecer todos os outros conceitos de segurança. A simples utilização de uma comunicação cifrada não fornece a segurança necessária, porque os usuários mal intencionados podem falsificar identidades e danificar o sistema. Assim, a capacidade de verificação da identidade da outra entidade é um fator chave para a implementação de um ambiente seguro.

- Autorização

  O conceito de autorização está intimamente relacionado com o conceito de autenticação. Ele representa a capacidade de verificar as políticas do sistema para conceder ou não o acesso de uma entidade autenticada para um sistema específico. Sistemas de autorização diferem na granularidade de políticas. Uma política muito simples seria a de conceder acesso a todos os usuários autenticados. Por exemplo, em uma rede doméstica, todos os dispositivos que foram registrados pelo usuário devem ser capazes de se conectar ao sistema de gestão da casa. No entanto, esta política não se encaixa em um acesso ao sistema de subestação, onde há usuários com diferentes níveis de prioridade, como visualização apenas ou autorização para alterar parâmetros. Além disso, os dispositivos podem ter autorização para interagir apenas com um conjunto pré-determinado de dispositivos, e assim por diante. Nestes casos, políticas relacionadas a atributos, papéis, tempo, etc., são necessárias.

- Responsabilização

  Outra questão importante para garantir a segurança em um sistema de comunicação é a capacidade de registrar eventos. Assim, sempre que um evento incomum acontece, o administrador do sistema deve ser capaz de rastrear quais eventos anteriores conduziram à situação. Isso é especialmente importante para realizar a auditoria e descobrir as causas de ataques, quando eles acontecem. Essa é a essência dos sistemas de responsabilização. Uma característica importante é que os logs do sistema devem ser armazenados e protegidos, a fim de evitar que um usuário subverta a informação registrada para encobrir a ação maliciosa.

- Privacidade

  Privacidade é outro requisito importante para *smart grids*. Nessas redes, diferentes tipos de informações sensíveis estão sendo transmitidas entre diferentes entidades. Isso inclui informações privadas sobre usuários, como os tipos de dispositivos que eles possuem em casa, os períodos em que eles estão em casa, os lugares onde eles foram com seus carros, e informações sobre as concessionarias elétricas, esse último com aspectos econômicos importantes. Um erro comum é associar privacidade apenas com o uso de cifras. Na verdade, a criptografia é a principal maneira de proporcionar privacidade, mas só quando a autenticidade dos pontos finais de comunicação já foi comprovada.

- Integridade

  A integridade é a capacidade de garantir que os dados fluam dos remetentes para os receptores sem quaisquer alterações no conteúdo. Ataques *man-in-the middle* são usados para espionar as informações, e também para alterar o conteúdo das mensagens entre sua origem e destino(s). As comunicações em *smart grid* devem garantir a integridade, pois a modificação de dados transmitidos de ou para sensores ou atuadores podem causar interrupções na rede elétrica ou danos severos. Além disso, a comunicação entre os usuários e os sistemas deve ser protegida, a fim de evitar a má utilização do sistema que pode causar prejuízos financeiros para os usuários e perturbações na rede elétrica.

- Disponibilidade

  A disponibilidade está relacionada com falhas e ataques de negação de serviço (*Denial of Service* – DoS). Em um ambiente não hostil, falhas na rede, falhas no *hardware* e/ou *software*, ou uma sobrecarga de usuários em um servidor podem causar indisponibilidade do serviço. Em ambientes hostis, *hackers* podem usar um pequeno número ou um número elevado de dispositivos, normalmente controlados remotamente, para interromper um serviço. Esses ataques são chamados de DoS e DoS distribuído (DDoS - *Distributed DoS*), respectivamente. Esses tipos de ataques geralmente causam indisponibilidade do serviço e consequentemente perdas financeiras. Uma das principais preocupações sobre DoS ou DDoS é que eles são geralmente difíceis de parar sem prejudicar os usuários legítimos. A principal razão é que o tráfego gerado pelo atacante é semelhante ao tráfego legítimo e, portanto, sistemas de *firewall* não podem bloquear apenas o tráfego atacante. *Hackers* são capazes de gerar este tipo de tráfego proveniente de fontes distribuídas através de *botnets*. *Botnets* são compostas de um conjunto de dispositivos comprometidos por um código malicioso que pode ser operado remotamente. Normalmente, um usuário com um dispositivo comprometido não sabe que é parte de uma *botnet*, porque *bots* são geralmente transparentes para o usuário e geram pequenas quantidades de tráfego em momentos muito específicos, desencadeados por um usuário remoto mal intencionado. Este tipo de ataque é um dos principais motivos de preocupação em redes elétricas inteligentes, porque o sistema de energia é composto por um grande número de dispositivos que geram dados para serviços específicos, como o SCADA. Se um *hacker* comprometer os medidores inteligentes, poderá usá-los para interromper um serviço de coleta de informações de energia ou ainda comprometer sistemas de proteção e controle de *microgrids*.

- Proteção Física

  Para efetuar ataques, um *hacker* precisa acessar dispositivos. Em redes de energia legadas, dispositivos de controle eram fisicamente protegidos. Com isso, os *hackers* teriam de invadir fisicamente uma instalação da concessionária, a fim de acessar um dispositivo e perturbar a rede de controle. Com o avanço das redes elétricas inteligentes, a rede de controle está interligada ao usuário final através de dispositivos como medidores inteligentes. Assim, ao invés de tentar comprometer um dispositivo de controle ou serviço através da rede, procurando por vulnerabilidades de *software*, o *hacker* pode invadir a rede adulterando um medidor inteligente que está

em sua casa, por exemplo. Quando um *hacker* tem acesso físico a um nó, torna-se muito fácil a alteração de códigos e o acesso aos dados armazenados no dispositivo, mudando seu comportamento. Uma vez que um *hacker* controla um nó de rede legítimo, ele torna-se um atacante interno. Isto significa que o atacante controla um nó que tem a confiança de todo o sistema. Assim, todas as mensagens injetadas serão consideradas como legítimas. Após infectar um nó, torna-se mais fácil comprometer outros nós legítimos através da rede, porque os sistemas de segurança são configurados para bloquear as ameaças externas e liberar a comunicação entre nós internos. Assim, a segurança física de dispositivos de comunicação é uma das principais preocupações para as redes de energia.

4.3.1. Segurança em Tecnologia da Informação x Segurança em Sistemas de Controle Industriais

Uma das principais razões para a ocorrência de falhas de segurança do sistema de energia é a diferença entre cenários de segurança na Tecnologia da Informação (TI) tradicional e sistemas de controle industrial (ICS - *Industrial Control Systems*). Normalmente, para o provisionamento de segurança no mundo da Internet, confidencialidade é uma das questões principais, pois os dados do usuário não podem ser divulgados. No ICS, mesmo que a confidencialidade seja importante para proteger os segredos industriais, não é a principal preocupação. Integridade e disponibilidade são, de fato, os requisitos essenciais para a execução correta do sistema de controle, mesmo na presença de atacantes internos ou externos. Uma falha de privacidade pode causar prejuízos, mas uma falha causada por uma mensagem falsa ou uma mensagem que não chega pode destruir equipamentos e/ou causar danos ainda mais graves.

Nos sistemas tradicionais de TI, a regra principal é manter o sistema atualizado. *Patches* para resolver as questões de segurança devem ser aplicados o mais rápido possível para parar possíveis ataques usando a vulnerabilidade exposta. Nenhum engenheiro ou analista de sistemas teria medo de atualizar o sistema. Esta é uma realidade diferente no ICS. Na verdade, os dispositivos têm geralmente *firmware* proprietário, que pode falhar após uma atualização. Normalmente, os fabricantes de dispositivos não assumem a responsabilidade no *patch* do dispositivo e engenheiros não se sentem confortáveis para atualizar o *firmware* e correr o risco de comprometer dispositivos muito caros. Por isso, é comum substituir equipamentos por outros mais seguros em vez de atualizar o *software* do dispositivo (Lüders, 2011). Outra diferença importante é que, em sistemas de TI tradicionais, os dispositivos são nativamente integrados com listas de *firewall*, de controle de acesso (*Access Control List* - ACL), e outros sistemas de segurança, o que não é uma realidade no ICS. Além disso, computadores conectados à Internet podem contar com protocolos de comunicação seguros para compartilhar informações sensíveis, enquanto os dispositivos em um ICS, em geral, são baseados em protocolos de comunicação muito simples e sem preocupação com segurança.

Outra preocupação em ambientes ICS é que existe o hábito dos operadores de utilizar logins e senhas padrão. Assim, quando um atacante tem acesso à rede, geralmente, é muito fácil de acessar e controlar dispositivos diferentes.

Além dessas vulnerabilidades, o cenário dos ICSs tem outra particularidade: rara-

mente ocorrem janelas de manutenção no ICS, pois os dispositivos não podem parar sem causar prejuízos à cadeia produtiva. Por exemplo, para executar a manutenção em um disjuntor, esse dispositivo deve ser desativado. Em *datacenters* tradicionais, a manutenção da máquina não interfere na prestação de serviços, pois o uso da virtualização permite copiar e mover máquinas virtuais sem a interrupção de serviço. Por isso, não só é mais fácil aplicar *patches* em sistemas de TI tradicionais, mas também é mais simples e menos dispendioso abrir uma janela de manutenção. Além disso, o ICS tem de trabalhar com um grande número de dispositivos legados, o que aumenta o desafio de fornecer um ambiente de comunicação segura.

Por fim, os dispositivos dos ICS são desenvolvidos para atender casos de uso e não para os casos de abuso [Lüders 2011]. Logo, os fabricantes de dispositivos se concentram em funcionalidades ao invés de se concentrarem em robustez da rede. Em sistemas de TI, o *hardware* geralmente é para uso geral e há muitos esforços para proporcionar ao software robustez contra ataques cibernéticos. No ICS, o hardware é muito específico e com desenvolvimento fechado. Assim, em geral, apenas o fabricante pode desenvolver novos softwares. Portanto, a comunidade não é capaz de produzir *patches* tão rapidamente como acontece no mundo de TI. Além disso, na área de TI, há uma cultura de rápida disseminação de ameaças na Internet, enquanto no ICS há uma falta de vontade/hábito de pesquisar e compartilhar incidentes. O principal motivo é que os engenheiros dos ICS normalmente tentam resolver falhas rapidamente por meio de reinicializações do sistema ou pela substituição de um dispositivo danificado, em vez de tentar descobrir a origem do problema. Por isso, muitas vezes os ataques cibernéticos nem mesmo são identificados como um incidente de segurança cibernética, porque os engenheiros ainda não são capazes de diferenciar entre um ataque cibernético e uma falha de *hardware*/*software* [Wilhoit 2013]. Outra razão para não compartilhar dados de incidentes é que as empresas não querem espalhar suas vulnerabilidades. Consequentemente, descobrir e resolver vulnerabilidades torna-se muito difícil.

4.3.2. Ataques em Redes de Comunicação para *Smart Grids*

Esta seção descreve os cenários de redes inteligentes em que os ataques ocorrem devido a falhas de segurança de comunicação em rede. Primeiramente, os ataques contra subestação e cenários de supervisão são discutidos. Em seguida, são apresentados ataques contra a AMI.

4.3.2.1. Ataques contra Subestações e Centros de Controle de Dados

Antes de discutir os ataques, é necessário entender por que uma subestação ou um Centro de controle de Dados (*Data and Control Center* - DCC) pode representar um cenário vulnerável. Isso ocorre devido à arquitetura de comunicação e protocolos usados nesses cenários.

Um dos principais elementos de uma subestação é o sistema SCADA (*Supervisory Control and Data Acquisition*). O SCADA é utilizado não só para subestações, mas também para tipos diferentes de ICS. A implantação do SCADA não evoluiu muito nos

últimos 30 anos em termos de segurança da informação, apesar de vários problemas de segurança terem sido documentados (Wilhoit, 2013). No contexto das redes elétricas inteligentes, esta evolução é de especial preocupação, uma vez que redes de comunicação estão evoluindo para interligar o sistema como um todo, o que implica mais ameaças da rede. O SCADA controla e monitora remotamente os equipamentos da subestação a partir do DCC da concessionária, utilizando Unidades Terminais Remotas (*Remote Terminal Unit* - RTUs) localizadas em subestações e interconectadas através de uma rede de comunicação até o DCC. Mais recentemente, os IEDs são usados para a mesma funcionalidade.

O monitoramento é realizado através da aquisição de dados, tais como valores de correntes e tensões, e a notificação do status dos dispositivos de campo, como disjuntores. O controle está relacionado com a realização de comandos em dispositivos da subestação, como abertura e fechamento de disjuntores. Para isso é necessária uma rede de comunicação que interligue o SCADA (estação mestre) até o RTU (*Remote Terminal Unit*) (escravo), tal como ilustrado na Figura 4.4, e o uso dos chamados protocolos SCADA. Note que o IED pode comunicar-se diretamente com o SCADA utilizando algum protocolo específico, de modo que os RTUs poderiam ser removidos. Soluções com um grande número de dispositivos conectados a RTUs também são utilizadas, apesar do fato de que o controle remoto pode ser realizado diretamente no IED, como ilustrado na Figura 4.4.

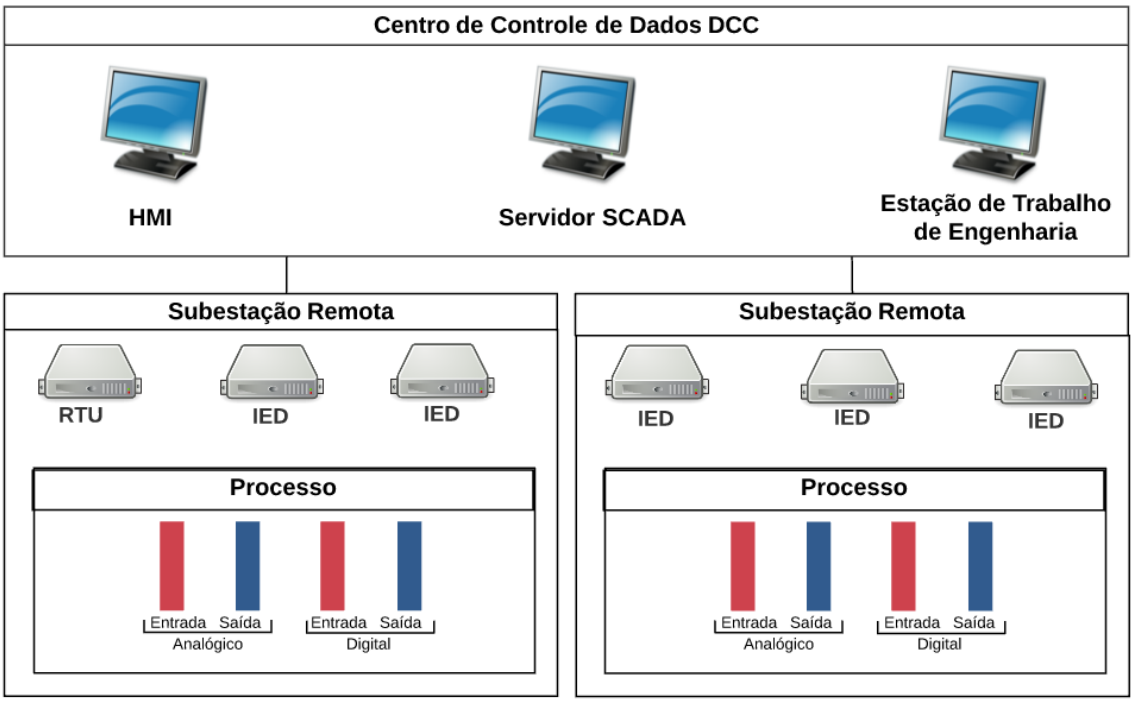


Figura 4.4. Esquema genérico de uma subestação.

A comunicação legada entre RTU e SCADA se dá por meio de protocolos SCADA e comunicação serial. Um dos protocolos SCADA mais antigos utilizados é MODBUS [Organization 2005], desenvolvido pela Modicon (atualmente Schneider) para sistemas de controle de processos industriais. O MODBUS, devido a necessidade de modernização, vem sendo atualizado desde 2005. No entanto, o DNP3 (*Distributed Network*

Protocol 3) [IEEE 2012] e o IEC 60870-5 [IEC 2007], ambos desenvolvidos na década de 90 e atualizados em 2012 e 2006 respectivamente, foram cada vez mais substituindo o protocolo MODBUS. Inicialmente, o DNP3 e o IEC 61870-5 foram criados para comunicação serial, como MODBUS. No entanto, em pouco tempo adquiriram versões para TCP/IP.

É importante enfatizar que a comunicação com esses protocolos acontece entre os RTUs/IEDs e o SCADA. Esta comunicação também é possível entre os IEDs e RTU. No entanto, nesse cenário o comando chega aos equipamentos através de cabos de controle conectados aos IEDs. Da mesma forma, as medidas de corrente e tensão, por exemplo, chegam ao IED através de fiação tradicional. Neste cenário, apenas a comunicação entre IED e SCADA é feita com comunicação e protocolos. Assim, um dispositivo de campo, tal como um disjuntor, recebe os comandos através de cabos de controle conectados aos IEDs (que podem ter recebido esse comando do SCADA).

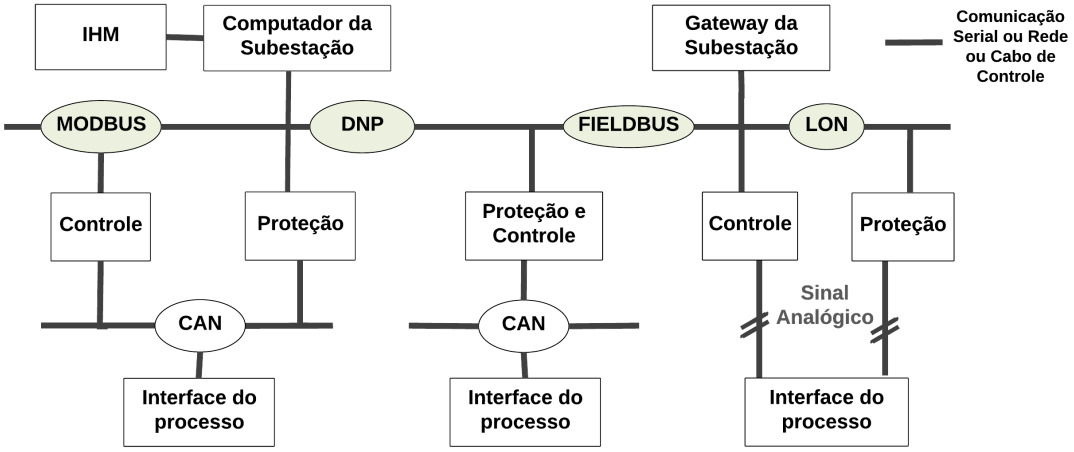
O DNP3, o IEC 60870-5, e os outros protocolos SCADA visam realizar o controle remoto e supervisão, mas não realizam funções de proteção elétrica. A filosofia de proteção, nesse cenário, é realizada sem o auxílio de protocolos e redes de comunicação. Por exemplo, depois de detectar uma condição anormal, o IED poderia iniciar um comando de proteção (trip) para abrir um disjuntor através de cabos de controle. Esse processo é feito automaticamente e de forma isolada, o mesmo IED que detectou o problema faz a tentativa de solução através de cabos de controle. Com isso, cada equipamento precisa estar diretamente conectado a um IED. Com a modernização das subestações, esses cabos de controle podem ser substituídos por uma rede de comunicação, como será discutido a seguir.

De fato, nos últimos anos, vários protocolos de automação de subestações que não são compatíveis uns com os outros foram propostos e implementados em subestações. A implantação de uma rede de subestação com diferentes protocolos trouxe muitos problemas para a automação de subestações, como dificuldade de manutenção, custos elevados, falta de interoperabilidade entre dispositivos de diferentes fabricantes, dentre outros. Para lidar com esses problemas, a norma IEC 61850 [IEC 2013] foi desenvolvida. Esta norma tem como objetivo garantir a interoperabilidade entre os dispositivos com o auxílio de uma modelagem própria e o uso de redes e sistemas de comunicação em subestações. Muitas concessionárias em todo o mundo já implantaram ou estão planejando implantar dispositivos de subestação baseados na norma IEC 61850 e redes de comunicação de acordo com esta norma [Budka et al. 2014]. A norma IEC 61850 define um modelo de objetos que representa formalmente as funções de proteção e controle, os equipamentos da subestação, a comunicação de dados e outros. Equipamentos de diferentes fornecedores podem ser instalados na mesma subestação desde que sejam implementados em uma rede de comunicação adequada e com os protocolos descritos na norma. Isso resulta em uma forte diferença entre a norma IEC 61850 e os protocolos SCADA tradicionais, tais como o DNP3 ou o IEC 60870-5, como ilustrado na Figura 4.5. A Figura 4.5(a) mostra o esquema de comunicação antes da implementação da norma IEC 61850, onde cada fornecedor usa um protocolo diferente para comunicar com o gateway da subestação e/ou com a IHM, seja a local ou a remota. Com isso, a implementação e a manutenção são mais caras além de mais difíceis e complexas. As equipes precisam de um conhecimento muito amplo para lidar com essa rede muito heterogênea. Além disso, protocolos como

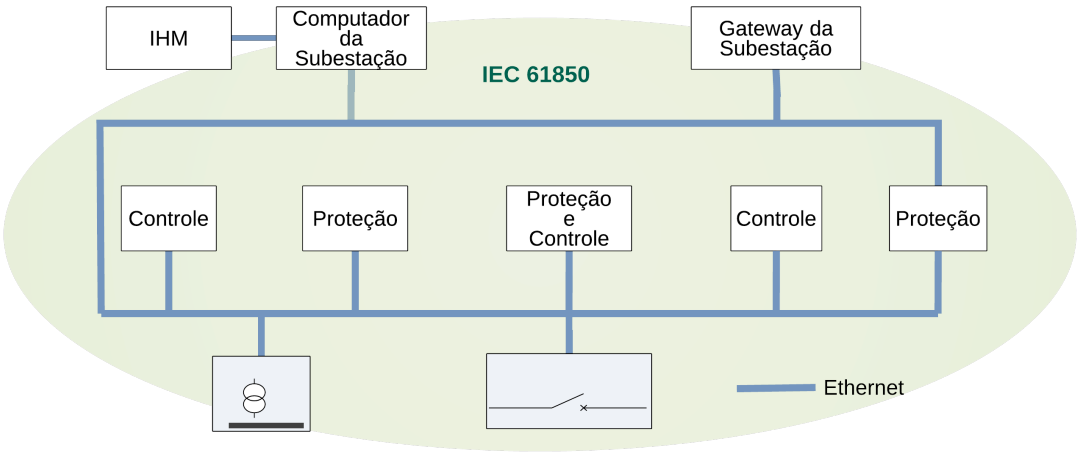
o DNP3 tem versões com comunicação serial (usando RS-232, RS-422 e/ou RS485) e rede ethernet, exigindo também o conhecimento de diversos padrões de camada física. Com a norma IEC 61850, como ilustrado na Figura 4.5(b), a comunicação é toda Ethernet de alta velocidade e padronizada com a modelagem IEC 61850. Nesse cenário, todos os equipamentos, independente de função ou de fornecedor, usam a mesma modelagem, facilitando a manutenção e configuração de toda rede. Além disso, com a norma IEC 61850, dispositivos de campo estão ligados por uma LAN Ethernet, substituindo os cabos de controle tradicionais. Portanto, os dispositivos de campo convencionais, como Transformadores de Corrente (TCs), Transformadores de Potencial (TPs), e disjuntores são substituídos por dispositivos modernos que se comunicam com os IEDs usando uma rede de comunicação e os protocolos padronizados na norma. A modelagem de dispositivos de automação é orientada a objeto e o modelo de comunicação utiliza três tipos de protocolos: GOOSE (*Generic Object Oriented Substation Event*), SV (*Sampled Values*) e MMS (*Manufacturing Message Specification*).

O MMS é um protocolo SCADA que é muito semelhante ao DNP3. Este protocolo utiliza um modelo cliente-servidor, onde os IEDs são servidores e o cliente é SCADA. O MMS usa as sete camadas do modelo OSI e seu atraso varia de 100 ms a 1000 ms. O protocolo GOOSE e o SV têm objetivos diferentes dos protocolos SCADA, e com isso um comportamento bastante diferente. Ambos são usados em esquemas de proteção e controle, e com isso têm restrições temporais muito mais rígidas, já que são usados em esquemas automáticos sem interação humana. Estes protocolos usam o modelo *publish-subscribe* (publicador-assinante) com um endereçamento MAC (*Media Access Control*) multicast. O SV também pode usar o modelo cliente-servidor e endereços unicast. Ambos têm limitações de tempo de até 3 ms e estão diretamente mapeados na camada de enlace, a fim de fornecer um tempo de resposta mais rápido. Essa restrição temporal rígida ocorre pois as mensagens GOOSE e SV são usadas em esquemas de proteção da rede elétrica. A mensagem SV é usada para enviar medidas de transformadores de instrumento e/ ou *Merging Units* e a mensagem GOOSE é usada para os esquemas de proteção e automatismos. Assim, o protocolo GOOSE e o SV permitem a comunicação entre os dispositivos da subestação e não envolvem o SCADA. Por exemplo, TCs e TPs podem enviar medições através de mensagens SV para os IEDs. Depois de detectar uma condição anormal analisando as mensagens SVs recebidas, o IED pode iniciar um comando para abrir um disjuntor (trip). No entanto, se este disjuntor falhar, o IED pode enviar uma mensagem GOOSE indicando que houve uma falha na abertura do seu disjuntor (*breaker failure*) para outros IEDs como um esforço para resolver o problema de outra forma e o mais rápido possível.

Muitas aplicações de energia em *smart grids* têm limitações de tempo rígidas em termos de disponibilidade de comunicação e atraso [IEC 2009]. Portanto, características específicas deste novo conceito de entrega de energia têm impulsionado vários projetos de pesquisa que visam a concepção de uma infraestrutura de comunicação adequada para atender a qualidade de serviço (QoS - *Quality of Service*) e a confiabilidade esperada para as redes elétricas inteligentes [Kounev et al. 2016]. Por exemplo, a norma IEC 61850 abordou o problema da inserção de recursos de energia distribuídos no sistema (DER - *Distributed Energy Resources*) [IEC 2009], recomendando o mesmo limite de tempo estabelecido para a proteção e controle em subestações.



(a) Esquema de comunicação de subestações legadas.



(b) Esquema de comunicação usando IEC61850

Figura 4.5. Comparação entre IEC61850 e outros esquemas de comunicação [Lopes et al. 2012].

A norma IEC 61850 recomenda atrasos de 3 ms a 100 ms para mensagens de proteção de acordo com o tipo de mensagem. Além disso, em 2010, o Departamento de Energia dos Estados Unidos analisou os requisitos de comunicação para funções das redes elétricas inteligentes (por exemplo, resposta à demanda e DER) e definiu valores da ordem de milissegundos para a proteção e controle de *smart grids* além de perfis de confiabilidade para cada serviço [DoE 2010]. Restrições temporais rígidas também foram descritas pela norma IEEE 1646 [1646 2004]. A norma IEEE 1646 firma requisitos de atraso para algumas operações de subestações em 4 ms e 5 ms, para frequências AC de 60 Hz e 50 Hz respectivamente.

Para as aplicações que requerem comunicação entre subestações, os requisitos de atraso são mais permissivos. Assim, a ativação de um esquema de proteção em uma

subestação deve ser iniciado em 8 ms após uma falha ser detectada numa subestação adjacente. Como consequência deste novo padrão de comunicação, a utilização de IEDs em subestações resultou em muitas vantagens tais como a comunicação de alta velocidade e custos reduzidos. No entanto, as melhorias deste sistema digital geram várias ameaças de segurança em subestações. Os ataques podem alterar os dados sendo enviados para esta rede, o que pode causar, por exemplo, uma abertura ou fechamento indevido de disjuntores, como discutido antes. No caso da abertura indevida, o sistema deixa de fornecer energia para as cargas sem que haja qualquer falha, causando uma interrupção desnecessária no fornecimento de energia para o consumidor. No caso de um fechamento indevido, mesmo em condição de falha o sistema é restabelecido, configurando um curto-circuito. Além disso, se o circuito estiver em manutenção, um fechamento indevido pode ameaçar a vida humana.

As próximas seções apresentam a descrição de ataques que podem causar grandes danos na subestação. Os ataques são subdivididos em dois tipos: o tipo um representa os ataques contra o SCADA; o tipo dois representa os ataques que podem ser executados após os ataques contra o SCADA, quando o atacante já está localmente na subestação.

4.3.2.2. Tipo 1: Ataques contra os sistemas de supervisão

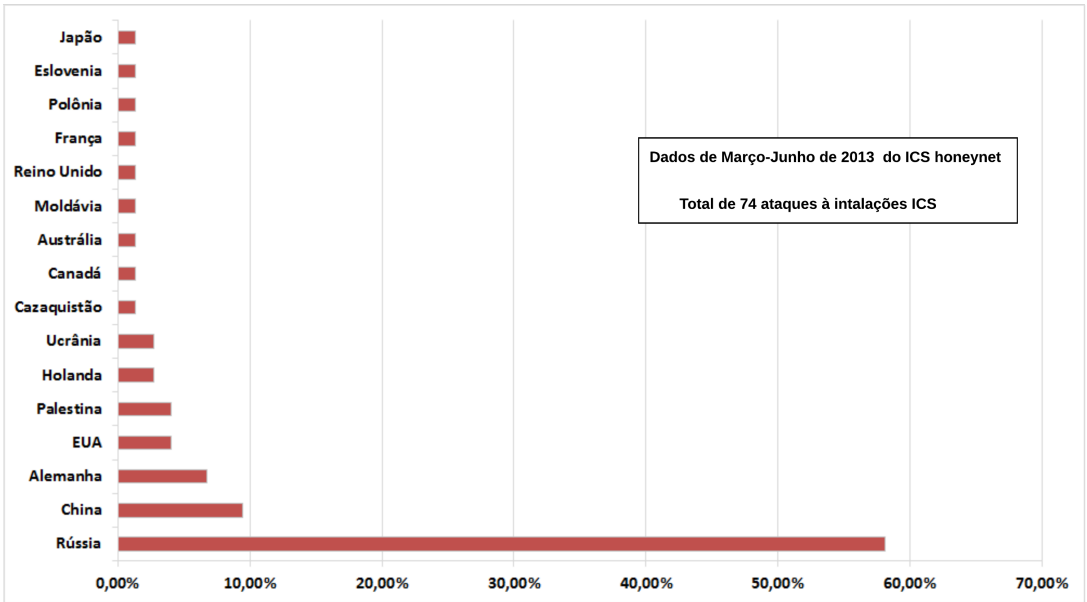


Figura 4.6. Origem dos ataques contra alvos ICS [Wilhoit 2013].

Os ataques contra os sistemas de supervisão acontecem em qualquer tipo de ICS. Um estudo recente espalhou uma série de *honeypots* em todo o mundo emulando um ICS operando com um SCADA e os protocolos de comunicação MODBUS e DNP3 controlando um sistema de bomba. Um *honeypot* é uma instalação que cria uma versão totalmente mimetizada de uma instalação real. A ideia é criar um ambiente atraente para os *hackers*,

a fim de estudar novas formas de ataques [Wilhoit 2013]. Esse estudo registrou 74 ataques específicos às instalações do ICS em um período de três meses. O número de tentativas de ataque foi ainda maior se considerarmos ataques automatizados genéricos como injeções SQL, atingindo 33.466 ataques. A Figura 4.6 mostra a distribuição da origem de ataques específicos a ICS.

Os ataques observados estavam relacionados a vulnerabilidades do SNMP (*Simple Network Management Protocol*), do servidor da IHM, da ausência de um sistema de autenticação adequado e de um VxWorks (*File Transfer Protocol* - FTP). Para melhor entender os ataques contra o SCADA, é preciso estudar a utilização do protocolo DNP3. Outros protocolos de comunicação, tais como MODBUS ou MMS no IEC 61850 sofrem ataques semelhantes, já que nenhum destes protocolos foi projetado considerando-se a existência de um ambiente de comunicação não-confiável. Assim, estes protocolos não empregam de forma nativa criptografia, autenticação e autorização.

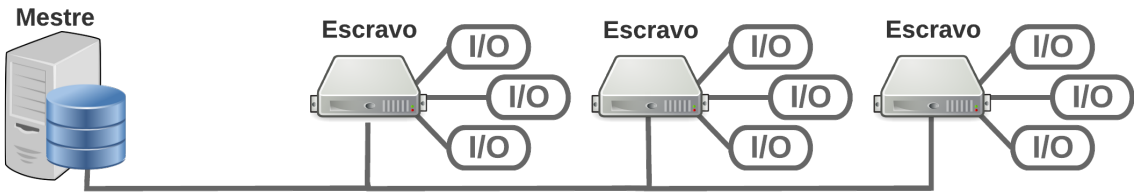
Em geral, os ataques contra os sistemas que usam o SCADA são divididos em três categorias: ataques que exploram especificações do protocolo de comunicação; ataques que exploram implementações do fabricante, como erros de configuração e falhas de código; e os ataques contra a infraestrutura subjacente, que têm como alvo a tecnologia da informação, os ativos de rede, e as políticas de segurança fracas do sistema [East et al. 2009]. Como os ataques aos protocolos SCADA são similares, nesse capítulo o DNP3 foi escolhido como enfoque.

O DNP3 permite três topologias possíveis entre o mestre e o dispositivo escravo (outstation) a ponto-a-ponto, a ponto-multiponto e a hierárquica, como mostrado na Figura 4.7. A comunicação entre o mestre e os dispositivos escravos é modelada de três maneiras diferentes: *unicast*, *broadcast*, e respostas não solicitadas. No modo unicast, o mestre envia uma solicitação e aguarda por uma resposta do escravo. Por exemplo, o mestre pode solicitar o estado do disjuntor ou executar um comando no disjuntor e o escravo responde com a leitura solicitada ou com o resultado da operação comandada, respectivamente. No *broadcast*, um pedido é encaminhado para todos os dispositivos escravos e não há resposta para o mestre. Na resposta não solicitada, dispositivos escravos enviam uma mensagem não solicitada para o mestre contendo atualizações periódicas, eventos ou alertas.

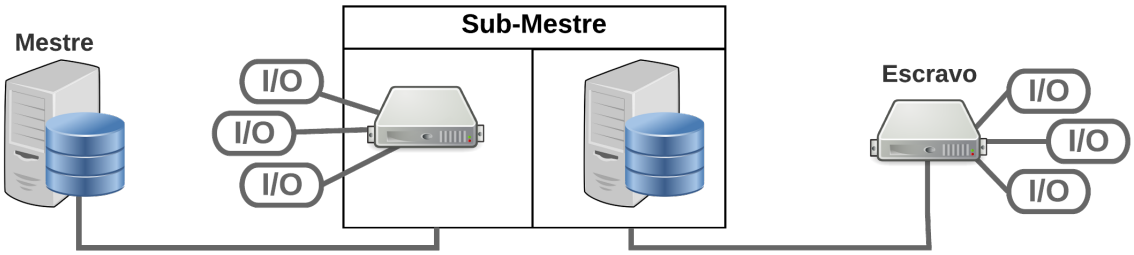
Ataques direcionados/provenientes do sistema de supervisão são baseados em interceptação de mensagens, injeção de mensagens falsas, e modificação de mensagens. Ataques contra redes trafegando o protocolo DNP3 podem ser classificados de acordo com a camada de arquitetura de rede onde ele ocorre. Seguem alguns exemplos de ataques contra o DNP3 [East et al. 2009]:

- Reconhecimento passivo de rede: O atacante com acesso adequado captura e analisa as mensagens que trafegam na rede para descobrir informações sobre a topologia de rede, os dispositivos em uso, as funcionalidades disponíveis, etc.
- Repetição de resposta *baseline* e *man-in-the-middle*: Nesses ataques, um invasor observa o tráfego de rede e injeta mensagens para o mestre passando-se por um dispositivo escravo e vice versa: para dispositivos escravos se passando pelo mestre. No caso do ataque *man-in-the-middle*, um dispositivo é colocado entre o mestre e

(a) Topologia ponto a ponto



(b) Topologia ponto-multiponto



(c) Topologia hierárquica

Figura 4.7. Topologias para DNP3 [East et al. 2009].

os escravos capturando e modificando o tráfego e personificando o outro. Os objetivos destes ataques são: espionar as informações que trafegam na rede, interromper o funcionamento do mestre e/ou dos escravos, modificar o comportamento do mestre e/ou dos escravos, e representar o mestre e/ou escravos para causar falhas no serviço.

- Modificação de campos da camada de enlace: Este ataque, que depende do estabelecimento de um ataque *man-in-the-middle*, tem muitas variações, de acordo com o campo de mensagem DNP3 que é modificado. O formato do quadro DNP3 é descrito na Figura 4.8. Por exemplo, o atacante poderia modificar o campo comprimento para interromper o processamento de mensagens; mudar o flag DFC para enviar um sinal falso de escravo ocupado para o mestre; ou mudar a mensagem para enviar o Código de Função 1, a fim de promover uma reinicialização desnecessária do escravo causando uma indisponibilidade temporária.

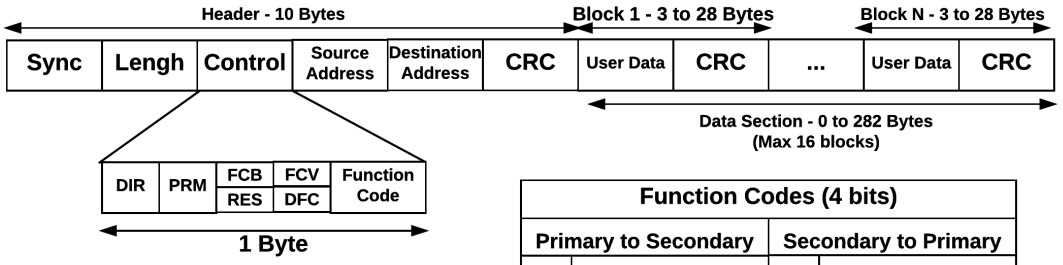
- Modificação de campos da pseudo camada de transporte: A chamada pseudo camada de transporte do DNP3 cuida da fragmentação dos pacotes. Este ataque é uma outra variação do *man-in-the-middle* para interromper o tratamento de mensagens fragmentadas. Neste caso, o atacante poderia mudar campos da mensagem de

transporte fazendo com que o destino descarte todos os fragmentos incompletos ou ainda causando erros de processamento ao juntar informações fragmentadas.

- Ataque de comandos em escravos: Nesta aplicação de ataque, o atacante usa um comando falso para gravar dados falsos em um escravo. Este ataque envia uma mensagem DNP3 com um *function code* (FC) que escreve objetos de dados falsos em um escravo, causando erros no dispositivo. Outra variação deste ataque é o uso de outros FCs para congelar e limpar os objetos de dados já existentes nos escravos, criando estados inconsistentes no sistema.

- Interceptação de arquivo de configuração: Esta aplicação de ataque visa a obtenção do arquivo de configuração de um escravo. Para fazer isso, o invasor envia uma mensagem indicando um arquivo de configuração corrompido enquanto representa a identidade do mestre. A estação escrava vítima, em seguida, reenvia o arquivo de configuração, que é interceptado pelo atacante.

- Negação de serviço com um único pacote: Neste ataque, o invasor envia pacotes de resposta especialmente montados que são capazes de travar o mestre. Este ataque explora ambos *firmware* e DNP3, visando interromper todo o sistema da subestação, uma vez que é capaz de parar o mestre. Como consequência, o centro de controle não pode mais monitorar e controlar a rede do SCADA. O ataque pode ser desencadeado por um pedido do mestre ou por qualquer outro evento escolhido pelo atacante, já que o DNP3 permite também que sejam enviadas respostas não solicitadas pelos escravos.



Function Codes (4 bits)

Primary to Secondary		Secondary to Primary	
Code	Description	Code	Description
0	Reset link	0	ACK
1	Reset user process	1	NACK
2	Test link	11	Response - link status
3	User data- require ack	14	Link down
4	User data - no ack	15	Link not used
9	Request link status		

Figura 4.8. Formato do quadro DNP3.

É importante notar que esses ataques são documentados e podem ser facilmente realizados utilizando ferramentas abertas [Rodofile et al. 2015]. A principal dificuldade

é obter o acesso à rede executando o sistema SCADA, que é pra ser uma rede segura. Os centro de controle de empresas, onde ficam os sistemas SCADA, costumam ter a rede complemente isolada da rede corporativa. Além disso, os dispositivos atacados estão fisicamente isolados dentro de subestações. Isso faz com que a preocupação com a segurança seja minimizada. Apesar disso, alguns ataques já foram relatados nesse tipo de rede mostrando que mesmo isoladas estão sujeitas a ataques [Wei and Wang 2014]. Com a implementação das redes elétrica inteligentes a proteção física deixa de existir fazendo com que as ameaças aumentem consideravelmente, o que requer uma redefinição de protocolos de comunicação para incluir segurança, considerando que a rede não está mais isolada em um ambiente de *smart grid*.

4.3.2.3. Tipo 2: Ataques contra a comunicação de dispositivos locais

Ataques contra os dispositivos locais da subestação dedicam-se ao uso indevido de um IED para perturbar o sistema elétrico. Detalhes específicos desses ataques dependem diretamente do protocolo de comunicação em uso. Para ilustrar, os protocolos da norma IEC 61850 serão usados como exemplo, já que além de um protocolo SCADA (MMS), a norma possui protocolos para realização de proteções na subestação (GOOSE e SV). Tanto o acesso remoto não autorizado quanto o acesso físico não autorizado podem resultar nos ataques descritos a seguir.

É importante perceber que há diferentes métodos para um invasor acessar um IED. A maneira mais simples é quando um atacante interno acessa o dispositivo e muda os parâmetros de configuração para danificar a rede. Outra possível ação de um invasor interno é conectar um dispositivo mal intencionado na rede, a fim de injetar um tráfego adulterado personificando os dispositivos desta rede. No entanto, também é possível ter acesso a um IED através de métodos externos, através de *exploits*, ou atacando um dispositivo que liga a subestação com o mundo exterior. Outra possibilidade é acessar um IED através do SCADA. Uma vez que o SCADA é comprometido, torna-se muito fácil o acesso aos IEDs, porque geralmente esses dispositivos são configurados com um login e senha padrão.

Uma das principais preocupações quando se analisa a comunicação dentro de uma subestação é que os requisitos de QoS de mensagens de proteção não são compatíveis com atrasos impostos pelos métodos de criptografia. Para proporcionar autenticidade e integridade, que são os requisitos mais básicos de segurança em sistemas de controle, é necessário que algum esquema de criptografia básico seja realizado. Um grande número de ataques tornam-se possíveis nesse cenário, já que não há nenhuma autenticação ou verificação de integridade nos protocolos de comunicação atuais, além de todas as outras vulnerabilidades do ICS descritas nas seções anteriores.

Esta seção concentra-se em ataques contra redes IEC 61850, a fim de ilustrar os impactos dos ataques realizados na comunicação entre IEDs e também entre todos os dispositivos locais. O protocolo GOOSE terá maior enfoque para exemplificar os ataques, pois permite a comunicação entre os IEDs. O foco principal do protocolo GOOSE é a transmissão de dados rápida e confiável entre dois ou mais IEDs. Mesmo assim, quando se utiliza GOOSE, uma subestação é propensa a diversos ataques, tais como:

- Ataque de negação de serviço: Este ataque é usado para impedir que usuários acessem recursos de rede. O atacante envia um grande número de mensagens para a máquina sob ataque usando uma ou mais máquinas já comprometidas. No cenário de subestação, este ataque visa parar um IED ou um concentrador local da subestação (no caso do uso de MMS). Além disso, o atacante provavelmente tem a intenção de retardar a entrega de mensagens críticas, como GOOSE e SV, entre as subestações e/ou desativar funções de monitoração e controle remoto, que usem MMS [Bayat et al. 2015]. Danos sérios podem ocorrer em subestações, uma vez que a comunicação é invadida e que o atacante impede a recepção de tráfego legítimo. Para executar este ataque, o atacante pode acessar o IED utilizando *exploits* de *firmware* ou contornando as medidas de segurança de rede. Uma vez que o atacante controla um IED, ele gera uma enorme quantidade de pacotes GOOSE para a rede da subestação. Como mensagens GOOSE são enviadas como se fossem em broadcast, todos os dispositivos da subestação começam a receber um grande número de mensagens GOOSE. Este ataque é também chamado de ataque de *flooding* [Li et al. 2015]. Duas consequências surgem: as mensagens legítimas podem não chegar ao destino em tempo por causa de filas de mensagens em *switches* de rede e em terminais; os IEDs podem parar de funcionar porque eles não são projetados para receber esse excesso de mensagens. Esta segunda consequência é mais fácil de observar se o atacante usa mensagens mal formadas [Khaitan et al. 2015, Lopes et al. 2015b, Noce et al. 2016].

- Falsificação de GOOSE (*spoofing*): Já que não há nenhuma autenticação ou verificação de integridade em mensagens GOOSE, os atacantes são capazes de enviar mensagens falsas na rede. Para injetar tráfego consistente, um atacante pode observar o tráfego de rede para descobrir dados como o número de status atual (stNum) de um fluxo de mensagens GOOSE. O parâmetro stNum funciona como um número de sequência. Assim, o atacante pode gerar mensagens GOOSE incrementando o stNum depois de inspecionar uma mensagem GOOSE inicial com o stNum verdadeiro. As mensagens GOOSE falsas são enviadas em *multicast* o mais rapidamente possível pelo atacante, com um número de stNum maior que o verdadeiro. Uma vez que o tráfego de ataque começa a ser processado pelo assinante, o tráfego legítimo com números de stNum mais baixos serão descartados [Kush et al. 2014]. Portanto, o atacante para o fluxo de informação legítimo, além de poder inserir qualquer tipo de informação falsa que possa afetar a rede de comunicação ou o sistema de potência.

- Personificação do dispositivo central: Neste ataque, o dispositivo atacante falsifica a identidade de um servidor do sistema de supervisão. É mais fácil de ser implantado se o atacante é capaz de conectar um computador à LAN da subestação. Um software de automação industrial que permita aos clientes implementar um SCADA pode ser usado para esse ataque, e, de fato, esses tipos de softwares estão facilmente disponíveis. Uma vez que o software estabeleça comunicação com um IED como mestre, qualquer comando pode ser executado prejudicando a subestação.

- Ataques contra Ethernet: O protocolo GOOSE especifica o uso de Ethernet para conectar dispositivos na LAN da subestação. Portanto, esta rede é propensa a todos

os ataques de camada 2 contra Ethernet, tais como ataques contra o ARP, ataques de inundação de MAC, ataques contra a *Spanning-Tree*, ataques de força bruta contra o *multicast*, ataques contra o VLAN *trunking*, ataques contra VLANs privadas, roubo de identidade, etc [Yoo and Shon 2015].

4.3.3. Ataques à Infrastrutura de Medição Avançada

À medida que a complexidade e o grau de automação nas plantas industriais e na infraestrutura das companhias de energia elétrica aumentaram, a necessidade de um sistema confiável e flexível que poderia permitir a coleta de medições em localizações geográficas afastadas ou lugares perigosos, levou a indústria a desenvolver uma infraestrutura de dispositivos com capacidades de processamento e de telecomunicações. Estes dispositivos são conhecidos como medidores inteligentes.

Infrastrutura de Medição Avançada (AMI) é um sistema de comando e controle que tem milhões de nós e atinge todos os consumidores e quase todos os sistemas da empresa. Com a utilização de medidores inteligentes, que coletam grandes quantidades de dados, e com a implantação do AMI, a necessidade de segurança na distribuição de energia torna-se evidente. Nesta seção, os tipos de ataques contra AMI serão apresentados e também as ameaças e as vulnerabilidades na rede de acesso.

4.3.3.1. Visão Geral da Infrastrutura de Medição Avançada

A implantação de uma comunicação bidirecional é o elemento chave de *smart grids*. Da mesma forma, a introdução de medidores inteligentes na rede de distribuição permite uma melhor compreensão da demanda e um melhor controle do consumo de energia e geração distribuída. A infraestrutura de medição avançada é uma parte essencial de um sistema de distribuição inteligente e refere-se à rede que conecta o operador de distribuição com o cliente. No final do operador, um sistema conhecido como sistema de gerenciamento de dados do medidor (*Meter Data and Management System* - MDMS) interliga medidores eletrônicos capazes de coletar informações precisas com base no tempo sobre o consumo de energia dos clientes.

Abordagens comuns para as redes de medidores são a ligação direta com o MDMS dentro do centro de dados e controle (*Data and Control Center* - DCC) ou através de um concentrador de medidores, como mostra a Figura 4.9. Esta rede local de medidores que se comunicam com um concentrador é conhecida como NAN (*Neighborhood Area Network*). Tecnologias popularmente usadas nessa comunicação são RF Mesh ou comunicação via rede elétrica nas frequências de banda estreita (*Power Line Communications over narrowband frequencies* - PLC-NB). PLC limita o número de medidores ligados a dispositivos nos enrolamentos secundários do transformador em que o concentrador é instalado. Assim, PLC é geralmente menos empregado do que uma alternativa de comunicação sem fio [Budka et al. 2014].

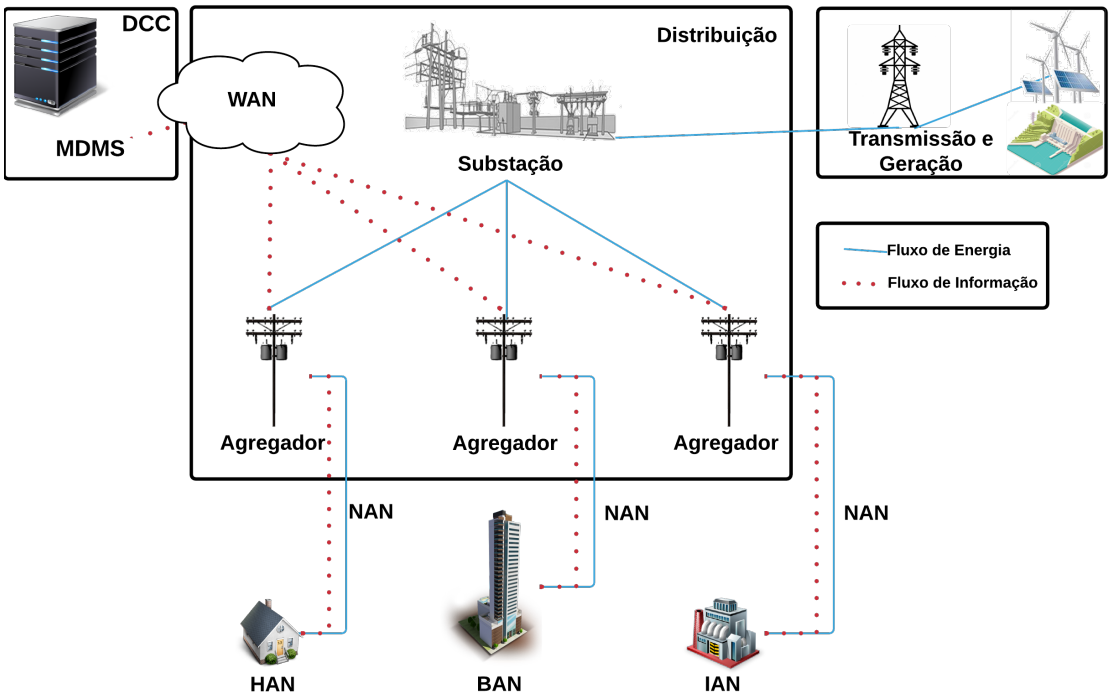


Figura 4.9. Estrutura AMI no contexto de *smart grid*.

Algumas das novas funcionalidades introduzidas com a implantação de medidores inteligentes, tais como informações de preços dinâmicos e a alta precisão e medição em tempo real do consumo de energia do consumidor, inserem uma série de vulnerabilidades que podem expor a privacidade do usuário. Essas vulnerabilidades são devidas à precisão da informação gerada por estes medidores. A assinatura elétrica de muitos aparelhos domésticos e atividade humana podem ser rastreadas por um invasor. Dados privados podem ser usados para roubo, sequestro e outras atividades criminosas. Informações sobre preços encorajam os consumidores a evitar o consumo de energia em horas de pico de demanda, e a controlar o seu consumo de energia de uma forma mais consciente, mas esses preços também podem ser manipulados para se controlar o mercado de energia. Ao confiar em tecnologias sem fio, uma NAN se torna vulnerável a sinal de interferência, espionagem, ataque de repetição, e ataques de injeção de dados. Estes são alguns exemplos da importância de investir em um sistema de comunicação seguro para a AMI que serão detalhados nas seções seguintes [Finster and Baumgart 2015].

Nas seções seguintes, este capítulo descreve ataques em estruturas cibernéticas internas da rede de distribuição. Os ataques contra a infraestrutura de medição avançada e à HAN (*Home Area Network*), tais como ataques contra a privacidade do usuário, os ataques contra o serviço de distribuição, bloqueio de sinalização e outro uso malicioso da rede de comunicação. De acordo com o relatório NIST sobre segurança cibernética para *smart grid*, como discutido antes, três principais objetivos para uma rede segura são: disponibilidade, integridade e confidencialidade [Group 2010]. No contexto de automação de distribuição e AMI, estes conceitos são aplicáveis como se segue:

- Disponibilidade: O acesso a funcionalidades do sistema deve estar pronto quando necessário. Se um ataque interrompe a comunicação entre uma casa inteligente e o centro da operação, ele compromete a disponibilidade do sistema.

- Integridade: A informação deve ser protegida contra a falsificação, alteração ou destruição. No contexto de NANs, um exemplo de perda de integridade é a modificação das informações de consumo de energia por um cliente malicioso que tenta negar sua responsabilidade financeira.

- Confidencialidade: O acesso à informação deve ser restrito a entidades autorizadas, a fim de proteger a privacidade e informações confidenciais. Esta é uma grande preocupação para os clientes, uma vez que um atacante pode adquirir uma grande quantidade de informações pessoais de um sistema preciso de monitoramento de energia.

4.3.3.2. Ataques contra a Disponibilidade de Serviço em Sistemas de Distribuição

Esta seção apresenta exemplos de ataques contra disponibilidade no sistema de distribuição e seus impactos. Ataques à disponibilidade tentam interromper a operação normal dos serviços e podem ser realizados em diferentes camadas de comunicação. Conforme os protocolos de comunicação para NANs forem escolhidos, outras vulnerabilidades podem surgir. Aqui vamos nos concentrar no bloqueio do canal, um ataque simples e genérico na camada física. O bloqueio consiste na transmissão de um sinal de interferência que diminui a relação sinal-ruído de um canal de comunicação sem fio.

A manutenção do equilíbrio entre a produção e consumo de energia é essencial para a estabilidade da rede. Com *smart grid*, a introdução de fontes de energia renováveis aumentou. Assim, a predição da energia produzida torna-se mais difícil, devido à natureza intermitente das fontes renováveis. Fontes de energia renováveis dependem de fatores ambientais que tornam a previsão de geração de energia mais complexa e menos precisa. Portanto, existe uma mudança de paradigma com a modernização de rede elétrica: na rede tradicional, a produção adapta-se à demanda, mas nas redes elétricas inteligentes, a demanda adapta-se à produção e faz com que o consumo de usuário seja mais eficiente. Os programas DSM (*Demand Side Management*) surgem como uma das soluções para ajustar o consumo do usuário à geração. DSM é uma ação ou decisão tomada pela empresa de energia para alterar ou modelar o padrão de consumo do usuário. O funcionamento correto da DSM depende de uma comunicação confiável entre a operadora e os consumidores. Dois exemplos de ataques de bloqueio de sinal contra programas DSM são discutidos a seguir, com diferentes motivações, que podem resultar em queda de energia.

No contexto de resposta à demanda em tempo real, um primeiro exemplo de ataque é o descrito a seguir. Nos programas em tempo real, o preço da energia é dinâmico ao longo do dia. O mercado usa a demanda de energia, o custo de geração de energia e as restrições das linhas de transmissão para calcular o preço que reflete a disponibilidade de recursos na rede. Em seguida, os usuários deste programa recebem mensagens do mercado a cada hora que custos de energia muda e ajustam seu consumo ao novo

preço. Li e Han descrevem uma possibilidade de manipulação do mercado por interferência do sinal de preço entre o mercado e os consumidores, como mostra a Figura 4.10 [Li and Han 2011]. Quando há baixa disponibilidade de energia, o mercado envia uma mensagem com um preço mais elevado para que os usuários reduzam o seu consumo e esperem por uma mensagem de preço mais baixo para aumentar ou normalizar o consumo. O atacante bloqueia o sinal de preço de uma área densamente povoada, enquanto os sistemas dos consumidores continuam trabalhando com o último preço recebido, e o atacante monitora o preço do mercado à espera de uma mudança significativa para parar a interceptação do sinal. Portanto, o atacante pode controlar as alterações de preços e usá-las para o lucro, por exemplo, se o sinal é bloqueado durante um preço mais elevado, quando o preço diminui, ele armazena energia, enquanto os outros usuários estão trabalhando com um preço mais elevado. Em seguida ele para o bloqueio, os usuários irão receber um preço mais baixo e vão aumentar o seu consumo, o preço tenderá a aumentar de novo e, neste momento, ele vende a energia armazenada. Como a operadora usa o preço para equilibrar a demanda e a oferta, se uma área densamente povoada não receber um aumento de preços e não reduzir o seu consumo, pode ocorrer um instabilidade na rede ou mesmo o apagão de uma grande área.

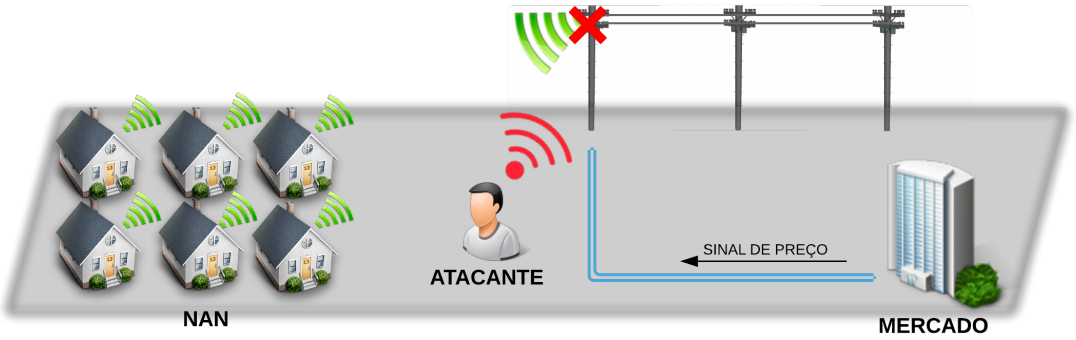


Figura 4.10. Bloqueio do sinal de preço para manipular o mercado de energia.

O segundo exemplo ocorre no controle direto de carga. DLC (*Direct load control*) é uma alternativa de programa DSM, em que o consumidor recebe incentivos ou descontos na conta de energia para permitir que a operadora tenha o controle direto de alguns aparelhos de sua casa. Em casos de emergência ou quando a demanda excede a oferta disponível, uma mensagem de comando é enviada para desligar algumas cargas e proteger a rede. Comandos de controle para reduzir o consumo de energia passam através da rede AMI, e semelhante aos programas de preços em tempo real, a operadora usa o DLC para equilibrar a demanda e a oferta, então, a intercepção de um comando de reduzir pode afetar a estabilidade da rede. Ataques contra esta comunicação podem danificar a rede. O impacto pode ser desde um simples desconforto dos usuários ou até mesmo a falta de energia em áreas críticas, comprometendo vidas humanas. Um usuário mal intencionado pode interromper esta comunicação e bloquear mensagens e assim enganar o programa, para que ele receba desconto na fatura por participar do programa sem desligar qualquer

carga. Após um caso de emergência, a operadora envia um comando para normalizar o consumo do usuário. Um adversário pode bloquear a chegada da mensagem impedindo a normalização de operação de um usuário específico. No pior dos casos, ataques terroristas podem bloquear o sinal em uma grande área, afetar a estabilidade da rede e causar falta de energia.

4.3.3.3. Ataques contra a Integridade dos Dados em Sistemas Distribuídos

Ataques que tentam manipular dados ao invés de bloquear serviços são tipicamente mais sofisticados do que um ataque de bloqueio. Além disso, as suas consequências são geralmente mais graves. Um atacante pode modificar dados para fraudar informações de consumo de energia em nome de um cliente. Outra possibilidade envolve a emissão de um comando de interrupção do serviço para um medidor, deixando uma residência sem energia. Além disso, o *firmware* do medidor é vulnerável a injeção de *malware* durante a atualização, ou um *firmware* modificado pode ser carregado comprometendo a sua capacidade de faturamento. Outra possibilidade é a de comprometer um grande número de dispositivos para corromper a visão global do sistema de detecção. Neste caso, um grande número de dispositivos seria capaz de injetar mensagens falsas na rede, que contém dados de medição falsa ou alarmes falsos. Uma falsa visão global do sistema poderia desencadear ações erradas através do sistema de supervisão de distribuição, causando falhas de energia.

A metodologia de ataque é muito semelhante aos ataques contra a Internet. Por exemplo, um invasor pode executar um *man-in-the-middle*, executar um ataque de repetição ou até mesmo criar um *botnet* de medidores inteligentes. No caso de um ataque *man-in-the-middle*, o usuário mal intencionado vai tentar personificar um medidor inteligente de confiança e/ou o DCC. O atacante vai se comunicar personificando os pares finais. Essa manobra permite a um atacante espionar dados, injetar falsos pacotes, reenviar os dados autênticos, e modificar a carga útil dos pacotes [Ur-Rehman et al. 2015]. Ataques de repetição são mais simples de executar, uma vez que eles são baseados em reenviar mensagens antigas, mas eles também são mais fáceis de evitar. Injetar novas mensagens falsas se passando por um medidor seria muito mais eficaz do que um ataque de repetição. Por exemplo, um usuário malicioso pode roubar as credenciais de um medidor inteligente fisicamente corrompendo o dispositivo. Em seguida, o usuário mal intencionado envia dados falsos usando as credenciais válidas de um computador. Normalmente dispositivos à prova de falsificação que evitem roubos de credenciais são caros e não se espera que os medidores inteligentes atendam este requisito. A última metodologia de ataque seria invadir um ou mais medidores através da rede de comunicação. Corrompendo muitos medidores, o *hacker* poderia criar um *botnet* de medidores. Em ambos os casos, é necessário encontrar e explorar vulnerabilidades não corrigidas do *firmware* do medidor. Como explicado anteriormente, o uso de assinaturas digitais para autenticação de *firmware* pode não ser suficiente para proteger um medidor inteligente [McDaniel and McLaughlin 2009]. A partir de experiências passadas, sabemos que falhas de segurança são inevitáveis, especialmente quando se lida com um sistema em que a pirataria pode ser tão facilmente monetizada. Assim, a segurança da rede de comunicação deve ser realizada com base em técnicas de segurança diferentes.

4.3.3.4. Ataques contra a Privacidade do Usuário em Sistemas de Distribuição

Tendo descrito possíveis ataques à disponibilidade de serviço e ataques contra a integridade do serviço que poderia ocorrer em sistemas de distribuição, agora serão descritos os problemas de segurança contra a privacidade do usuário. Na rede elétrica tradicional, funcionários da operadora coletam mensalmente as informações do medidor. Com os avanços promovidos pela AMI, os dados de medição tornaram-se mais detalhados e coletados em intervalos de tempo mais curtos [Siddiqui et al. 2012]. Embora os dados detalhados e granulares sejam importantes para permitir vários serviços de *smart grid*, eles criam grandes vulnerabilidades de privacidade. Os principais tipos de ataques contra a privacidade do usuário são a espionagem e a análise de tráfego. Ambos tiram proveito da comunicação sem fio da NAN para obter detalhes pessoais da vida do usuário. Espionagem é a escuta não autorizada de uma conversa privada, neste caso a interceptação de um canal de comunicação sem fio. Na análise de tráfego, o padrão de tráfego é monitorado com a intenção de inferir hábitos diários dos usuários.

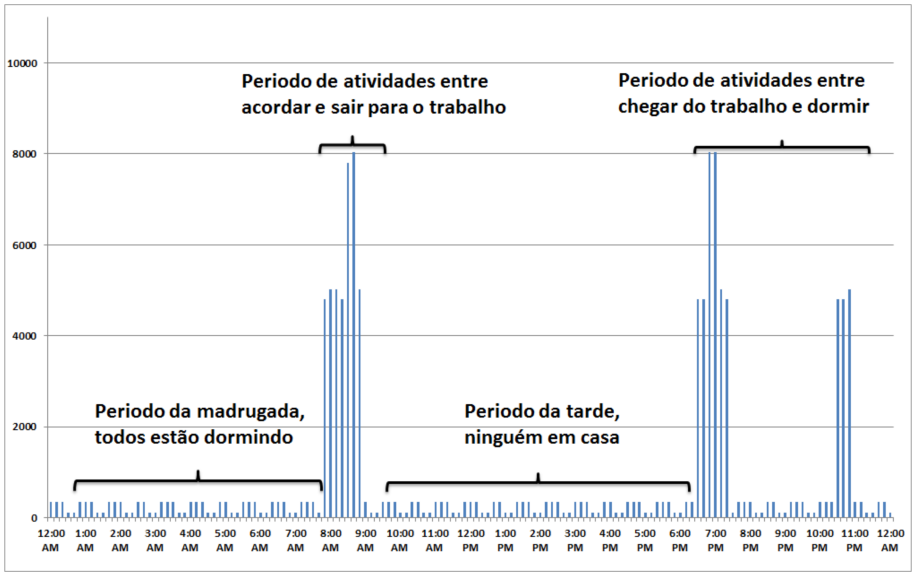


Figura 4.11. Exemplo de dados de medição do consumo de energia que poderiam ser usados para espionar a rotina do usuário [Molina-Markham et al. 2010].

A troca periódica de dados entre aparelhos inteligentes e o EMS (*Energy Management System*) permite ao usuário monitorar seu consumo em tempo real e controlar remotamente dispositivos domésticos. No entanto um adversário poderia escutar esta comunicação, adquirir o consumo do dispositivo e usar um algoritmo de criação de perfil de carga para identificar qual o dispositivo ligado. Cada dispositivo tem uma assinatura de carga, um comportamento elétrico único, que pode ser utilizado num processo de reconhecimento de dispositivos elétricos [Rahimi et al. 2011], e numa análise mais aprofundada, o intruso pode obter ainda conteúdos multimídia, como o canal de televisão a que o usuário está assistindo [Greveler et al. 2012]. A questão da privacidade é séria, não só por causa da exposição da vida pessoal do usuário, mas também pelo fato de que esta informação pode comprometer a própria segurança do usuário. Através de análise de tráfego, um perfil de consumo pode ser traçado e detalhes de rotina de um usuário podem

ser inferidos, a que horas ele acorda, que horas vai dormir, se está viajando, quais pessoas estão em casa em um hora específica, como mostrado na Figura 4.11. Esta informação pode ser usada para furto, roubo e até mesmo sequestro.

A detecção destes tipos de ataques torna-se difícil devido à sua natureza passiva. O adversário deseja roubar informações sem alteração de dados e sem modificar o funcionamento do sistema. Assim, a prevenção é mais importante do que a detecção.

4.4. Soluções e Recomendações

Depois de descrever os principais ataques à comunicação das redes elétricas inteligentes, as principais soluções para criar uma arquitetura de comunicação integrada, que forneça confiabilidade, privacidade e não repúdio serão abordadas.

4.4.1. Subestações e Criptografia na AMI

Como discutido anteriormente, a comunicação das redes elétricas inteligentes é vulnerável a diversos tipos de ataques. A comunicação de dados sem criptografia é uma das razões que aumentam a vulnerabilidade. A fim de entender melhor esse cenário e onde a criptografia pode ser usada, é necessário compreender que tipo de protocolos para subestações e *smart grid* são utilizados. Nesta seção, iremos classificá-los em três tipos. O primeiro tipo é chamado protocolo SCADA, que como já citado anteriormente é responsável pela comunicação entre os sistemas supervisórios e dispositivos como medidores inteligentes e IEDs. Os protocolo SCADA geralmente têm restrições de tempo mais brandas do que os outros já que incluem a interação do usuário. Portanto, a interface do usuário é parte do sistema supervisório e os atrasos dependem da atividade do usuário. Assim, atrasos de 200 ms a 1000 ms são bem aceitos na rede.

O segundo tipo de protocolo é chamado de protocolo de proteção. Ao contrário do tipo anterior, este tipo de protocolo possui severas limitações de tempo que variam de 3 ms a 100 ms de acordo com os requisitos do cenário. Neste caso, a fim de evitar falhas ou para limitar a interrupção de um serviço, devido a uma falha elétrica, as mensagens de proteção de rede são enviadas depois de um evento elétrico. Falhas podem afetar uma grande parte do sistema elétrico muito rapidamente, assim todas as mensagens de proteção exigem rígidas restrições de tempo. É importante destacar que os dispositivos de proteção (por exemplo, IEDs) podem detectar condições de falha e enviar mensagens de proteção para outro dispositivo (por exemplo, um disjuntor inteligente ou um IED que pode operar um disjuntor) apenas nos sistemas modernos e mais recentes. Nos sistemas tradicionais, um dispositivo de proteção detecta condições de falha e opera diretamente um disjuntor através de cabos de controle, sem uma rede de comunicação.

O terceiro tipo é destinado a medidas e amostragem de valores. A ideia inclui a amostragem de valores instantâneos dos sistemas de potência, principalmente correntes primárias e tensões, e a transmissão através da rede. Estes valores são publicados na rede e dispositivos de proteção ou controle (ou qualquer dispositivo que possa fazer uso deles) são capazes de assiná-los. Valores amostrados são usados pelos dispositivos de proteção e controle para a identificação de falhas elétricas. Portanto, as restrições de tempo são tão rígidas quanto no protocolo de proteção, ou mais, conforme for necessário para a identificação da falha.

As limitações de tempo para envio de mensagens são um dos principais entraves para o uso de criptografia nesse cenário. Em geral, a criptografia ou encriptação é a transformação da informação a partir de um estado compreensivo para um estado aparente absurdo. Assim, a criptografia transmite dados de uma forma particular ao destinatário, de maneira que apenas ele possa processá-los. O remetente de uma mensagem encriptada compartilha, somente com o receptor pretendido, a técnica de decodificação necessária para recuperar a informação original. Medidas criptográficas incluem a criptografia de chave simétrica e criptografia de chave assimétrica. Os métodos mais antigos necessitam de mais recursos computacionais, como AES (*Advanced Encryption Standard*) e DES (*Data Encryption Standard*) [Mishra et al. 2016]. A gestão de chave de segurança é essencial para a criptografia de informações.

No entanto, a criptografia acrescenta atraso na rede de comunicação. Como a codificação e a descodificação são realizadas nos pacotes, o tempo total a partir de um evento e uma operação, por exemplo, pode aumentar consideravelmente. Reconhecendo este fato, a maioria das soluções de criptografia não são adequadas para utilização em protocolos com limitações de tempo rígidas como os protocolos de medidas e amostragem de valores e protocolos de proteção. É necessário que os métodos de criptografia não só satisfaçam requisitos de desempenho em tempo real desses protocolos, mas também garantam a segurança da mensagem. Como existem poucos trabalhos sobre o assunto publicados na literatura [Fangfang et al. 2013], é uma boa oportunidade de pesquisa: um método para proporcionar segurança combinada com a qualidade do serviço. Testes exaustivos devem ser feitos para garantir que as soluções com criptografia não excedam requisitos de atraso em *smart grids*. Em [Fangfang et al. 2013], os autores mostram por simulação com o software OPNET que com um método de criptografia híbrido, é possível. No entanto, testes mais detalhados precisam ser feitos.

Por outro lado, a criptografia pode ser adicionada aos protocolos SCADA, sem problemas, uma vez que este tipo de protocolo não tem muitas limitações de atraso. Vários pesquisadores propuseram métodos de criptografia e esquemas de gerenciamento de chaves para SCADA. Isso ocorre porque os protocolos SCADA não foram projetados considerando a necessidade de segurança. Como mostrado em [Amoah et al. 2016], muitos pesquisadores têm proposto soluções para este fim, mas ainda há muito trabalho a ser feito. Soluções propostas na literatura são muito específicas, com muitas peculiaridades. Algumas soluções são apresentadas a seguir, juntamente com soluções para comunicação segura.

4.4.2. Solução de Padronização para a Segurança em Subestações

Devido a razões históricas, as questões de segurança cibernética não fazem parte dos protocolos industriais. DNP3, 60870-5 e IEC 61850 foram publicados quando a segurança não era uma grande preocupação industrial. Para superar este problema, o IEC padrão 62351 foi desenvolvido pelo Comitê de IEC Técnica (TC) 57, a fim de fornecer os requisitos de segurança em redes de automação de energia. Na verdade, a IEC 62351 já utiliza os métodos atuais, tanto quanto possível. Por exemplo, utiliza o protocolo TLS (*Transport Layer Security*), a fim de preservar a integridade das mensagens de acordo com um esquema forte de gestão de identidade. Além disso, ele propõe o uso de RBAC (*Role-Based Access Control*). Isto significa que não só pretende identificar de forma se-

gura todas as entidades do sistema, mas também definir políticas de controle de acesso baseadas na função da entidade no sistema. Os objetivos do padrão também incluem integridade, confidencialidade, prevenção de falsificação, detecção de intrusão, autenticação por meio de certificados digitais, e assim por diante. Este padrão é dividido em 10 partes, como ilustrado na Figura 4.12.

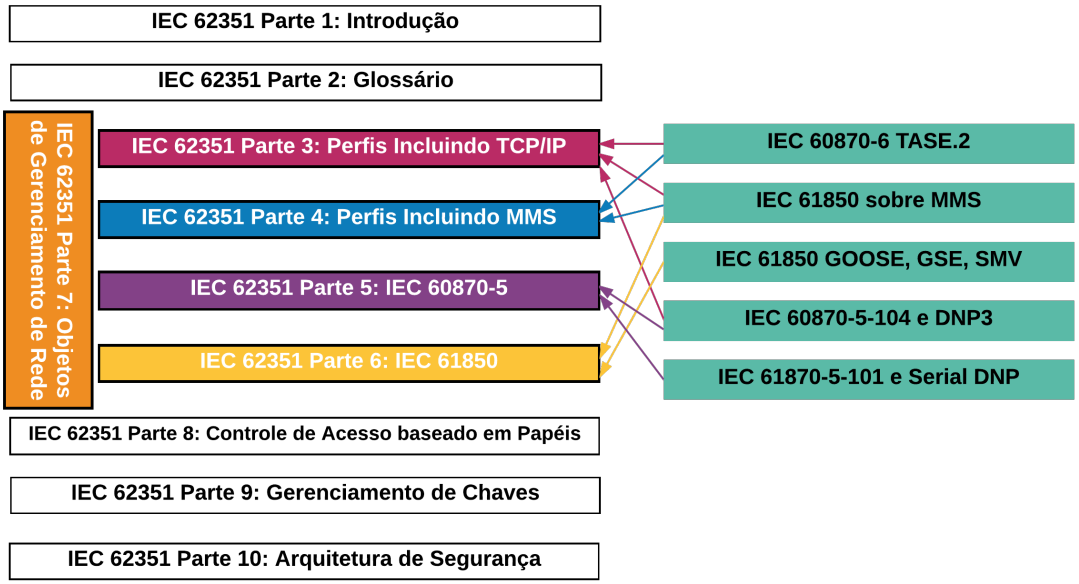


Figura 4.12. Estrutura da norma IEC 62351.

Uma solução bem conhecida já aplicada é um Sistema de Detecção de Intrusão (*Intrusion Detection System* - IDS). A finalidade de um IDS é detectar comportamento anormal na rede digitalizando pacotes e gerando alertas para os operadores. IDS são normalmente classificados como *network-based* ou *host-based*. Um IDS baseado em rede monitora o tráfego de rede local e tem acesso a todos os pacotes transmitidos, enquanto um IDS baseado em host analisa os pacotes em um ou mais servidores individualmente [Sun et al. 2016]. Um trabalho recente de Mishra et al. [Mishra et al. 2016] demonstrou um método ideal para a digitalização de pacotes como uma defesa contra ataques a preços acessíveis, oferecendo segurança, sem comprometer os requisitos rigorosos de QoS.

4.4.3. Soluções de Segurança para AMI

Soluções de segurança para AMI estão em discussão e há um elevado número de propostas sobre a forma de garantir a segurança na rede. Nesta seção, vamos mostrar soluções e sistemas de proteção para os ataques contra estruturas cibernéticas internas de uma rede de distribuição e os desafios de melhorar a segurança neste cenário.

O ataque de bloqueio de sinal foi apresentado como uma ameaça à disponibilidade da rede elétrica. Alguns estudos propõem soluções para este tipo de ataque à rede sem fio, a maioria deles são técnicas baseadas em salto de frequência. Por exemplo, há uma proposta que sugere o uso de múltiplos canais de frequências alternativas [Aravinthan et al. 2011]. Se os medidores detectarem interferências no canal atual, to-

dos os medidores se movem através de uma sequência aleatória pré-definida e comum de canais. Quando um medidor completa o processo de autenticação, recebe a sequência de saltos de frequência através de um canal encriptado. Outra proposta consiste em um esquema aleatório de espalhamento espectral designado por FQR (*Frequência Quorum Rendezvous*) [Lee et al. 2011]. FQR explora um sistema de quorum que permite que cada nó construa uma sequência de saltos de forma independente durante a fase de estabelecimento de chave. A propriedade de intersecção do sistema de quorum garante que um par de nós se encontre dentro de um período limitado de tempo, durante o qual eles compartilham uma chave comum usada para comunicações futuras de espalhamento espectral. Este mecanismo não só evita interferência, mas também espionagem através de escuta do canal sem fio.

A prevenção de fraudes e injeção de dados falsos pode ser alcançada com forte criptografia fim a fim em canais de comunicação da rede HAN (*Home Area Network*) e AMI. Como as restrições de atraso para esta aplicação não são críticas, muitas opções de criptografia fim a fim utilizadas na Internet estão facilmente disponíveis. Uma lista de trabalhos relacionados com a prevenção de ataque com dados falsos podem ser encontrados em [Sharma and Saini 2015]. Autenticação também é de grande importância, uma vez que dados falsos ou medidores fraudulentos podem ser inseridos na rede dando ao invasor a capacidade de executar comandos e degradar serviços. Nicanfar et al. [Nicanfar et al. 2014] apresentam uma rede inteligente de autenticação mútua (SGMA) que fornece uma autenticação eficiente entre medidor inteligente e servidor de autenticação usando senhas, e um protocolo de rede inteligente de gerenciamento de chaves (SGKM) utilizando a infraestrutura de chave pública (PKI). Também foram propostas novas melhorias para proteger a privacidade do usuário. Neste caso, um mecanismo obscurece parcialmente o perfil de carga do usuário usando uma bateria recarregável, e protege a privacidade do usuário [Varodayan and Khisti 2011]. O consumo relatado pelo medidor inteligente para a empresa concessionária é uma combinação de aparelhos e o consumo da bateria. A qualquer momento, a bateria pode realizar uma combinação das seguintes ações (ou nenhuma delas) sujeitas à sua capacidade: transmitir energia diretamente do utilitário para os aparelhos; armazenar energia da concessionária para uso futuro; entregar a energia armazenada anteriormente para os aparelhos. Desta forma, o carregamento e a descarregamento de uma bateria pode manipular a carga de saída, obscurecendo a informação do consumidor real. Outras soluções para a privacidade são baseadas em esquemas de gerenciamento de chaves para proteger o conteúdo que está sendo transmitido no interior da casa entre o medidor e o sistema de controle [Kazienko et al. 2015].

4.5. Direções para Futuras Pesquisas

Neste capítulo, vulnerabilidades tanto de cliente e medidores inteligentes quanto de subestações e centros de controle foram abordadas. Os ataques e ameaças e as suas consequências foram descritos. Além disso, as possíveis soluções encontradas na literatura foram destacadas, o que pode nos ajudar a alcançar uma rede inteligente segura. No entanto, a implantação de uma rede segura de comunicação para *smart grid* ainda é um enorme desafio. Algumas linhas de pesquisa incluem:

- Propostas como IEC 62351 prometem resultados, mas elas exigem testes exausti-

vos e experimentações. Elas devem ser testadas com protocolos industriais para atestar que a qualidade dos serviços exigida por aplicações de energia não seja afetada. Além disso, a proposta padrão está sendo atualizada com novos métodos ou evolução dos métodos já conhecidos, o que confirma a necessidade de avaliação constante.

- A padronização é também uma preocupação principal. A arquitetura de rede inteligente é complexa e composta por diferentes tipos de domínios e redes. O sucesso da implantação comercial das redes elétricas inteligentes depende de mecanismos padrão que permitam que diferentes fornecedores possam interoperar em um formato uniforme. Um padrão universal pode ser utilizado a fim de proporcionar interoperabilidade, a flexibilidade, a redução de custos, e assim por diante. A utilização do mesmo modelo de informação irá melhorar a comunicação e, principalmente, pesquisas de segurança. Há indícios de uso do IEC 61850, no entanto ainda existem muitas questões a serem avaliadas.

- O estabelecimento de uma estrutura universal para comunicação segura das redes inteligentes é muito importante. Esta estrutura deve levar em consideração a proteção "defesa em profundidade"[Lüders 2011]. Assim, cada camada de comunicação deve ser tratada, bem como o hardware e software. Técnicas de segurança de TI tradicionais também devem ser abordadas no contexto de redes inteligentes, incluindo questões como:

  - Um processo fácil e barato para aplicar *patches* de segurança em IEDs e medidores inteligentes;
  - A utilização de estruturas de gerenciamento de identidade para fornecer autenticação e autorização segura;
  - O uso de sistemas de gerenciamento de configuração para IEDs e medidores inteligentes;
  - A utilização de novos *firewalls* e técnicas de detecção de intrusão em subestações e redes de AMI.
  - O uso de técnicas de *big data* para descobrir informações importantes entre os dados coletados de medidores inteligentes para ajudar a descobrir *botnets*, roubo de energia, e até mesmo ações de terrorismo.

- A proposta de métodos de autenticação e integridade mais seguras para a comunicação *multicast*, sem incorrer nos requisitos de alto poder de processamento ou elevados atrasos de comunicação. Isto é de especial importância para proporcionar uma comunicação entre IEDs que seja mais resistente contra os invasores externos e internos.

- A proposta de uma solução completa, que compreende a interoperabilidade entre diferentes sistemas de criptografia, também é necessária. Diferentes tecnologias de comunicação e protocolos são usados na infraestrutura de rede inteligente que resulta em requisitos de criptografia exclusivos para cada um. Uma abordagem segura e interoperável é essencial.

- O equilíbrio entre a disponibilidade da informação e preservação da privacidade não é trivial e é uma direção de pesquisa muito interessante. Enquanto um grande conjunto de informações resulta em decisões mais inteligentes e melhores otimizações, também representa uma ameaça à privacidade do usuário. Informações de medidores inteligentes tornam possível inferir o comportamento do consumidor, o que possivelmente ofenderá os consumidores.

4.6. Conclusão

O avanço da comunicação para *smart grid* estabelece novos desafios de segurança. Como o cenário em subestações e na mudança dos sistemas de distribuição, velhos conceitos caíram por terra. Atualmente, atacantes são uma realidade para redes de campo em subestações, mesmo com o uso de firewalls, redes privadas virtuais (VPN), sistemas de detecção de intrusão (IDS), e algumas técnicas de criptografia.

Não há solução definitiva para a segurança nas redes de comunicação de *smart grid*, bem como esta solução completa não existe para a Internet também. A segurança deve sempre evoluir, porque os *hackers* estão sempre à procura de novas brechas. Processos legados para gerenciar redes ICS já não são aceitáveis. Práticas como a não utilização de *firewalls*, não usar anti-vírus, não aplicação de *patches*, usar configurações padrão e contas padrão, a não utilização de certificação digital, etc. já não são aceitáveis. Além disso, os fornecedores devem assumir a responsabilidade para o desenvolvimento de dispositivos seguros e robustos. Muito esforço tem sido colocado nos últimos anos para o desenvolvimento de dispositivos que sejam seguros contra explosões ou falhas no sistema elétrico e que sejam robustos a diferentes cenários de falhas de energia. No entanto, esses dispositivos não são testados em casos de abuso e não podem ser considerados seguros.

Muitas dessas observações partem do fato de que existem muitos especialistas em segurança de rede de TI, mas apenas alguns que entender tanto de segurança de rede e sistemas de controle industrial. Assim, existe uma forte necessidade de formar mais profissionais capacitados para trabalhar nesta área multidisciplinar.

Referências

[1646 2004] 1646, I. (2004). Ieee standard communication delivery time performance requirements for electric power substation automation.

[Amoah et al. 2016] Amoah, R., Camtepe, S., and Foo, E. (2016). Securing dnp3 broadcast communications in scada systems. *IEEE Transactions on Industrial Informatics*, 12(4):1474–1485.

[Aravinthan et al. 2011] Aravinthan, V., Namboodiri, V., Sunku, S., and Jewell, W. (2011). Wireless ami application and security for controlled home area networks. In *2011 IEEE Power and Energy Society General Meeting*, pages 1–8. IEEE.

[Assante 2016] Assante, M. (2016). Confirmation of a coordinated attack on the ukrainian power grid. *Online]: https://ics. sans. org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainianpower-grid*.

[Bayat et al. 2015] Bayat, M., Arkian, H. R., and Aref, M. R. (2015). A revocable attribute based data sharing scheme resilient to dos attacks in smart grid. *Wireless Networks*, 21(3):871–881.

[Bayod-Rújula 2009] Bayod-Rújula, A. A. (2009). Future development of the electricity systems with distributed generation. *Energy*, 34(3):377 – 383. {WESC} 2006 6th World Energy System Conference Advances in Energy Studies 5th workshop on Advances, Innovation and Visions in Energy and Energy-related Environmental and Socio-Economic Issues.

[Budka et al. 2010] Budka, K., Deshpande, J., Hobby, J., Kim, Y.-J., Kolesnikov, V., Lee, W., Reddington, T., Thottan, M., White, C., Choi, J.-I., Hong, J., Kim, J., Ko, W., Nam, Y.-W., and Sohn, S.-Y. (2010). GERI - Bell Labs smart grid research focus: Economic modeling, networking, and security & privacy. In *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 208–213.

[Budka et al. 2014] Budka, K. C., Deshpande, J. G., Thottan, M., et al. (2014). Communication networks for smart grids. In *Computer Communications and Networks*. Springer.

[Cheung et al. 2007] Cheung, H., Hamlyn, A., Wang, L., Yang, C., and Cheung, R. (2007). Computer network security strategy for coordinated distribution system operations. In *Power Engineering, 2007 Large Engineering Systems Conference on*, pages 279–283.

[Chim et al. 2011] Chim, T., Yiu, S., Hui, L., and Li, V. (2011). PASS: Privacy-preserving authentication scheme for smart grid network. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 196 –201.

[Cleveland 2008] Cleveland, F. (2008). Cyber security issues for advanced metering infrasttructure (AMI). In *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, pages 1 – 5.

[DoE 2010] DoE (2010). Communication requirements of smart grid. U.S. Department of Energy (DoE).

[East et al. 2009] East, S., Butts, J., Papa, M., and Shenoi, S. (2009). A taxonomy of attacks on the dnp3 protocol. In *International Conference on Critical Infrastructure Protection*, pages 67–81. Springer.

[EPRI 2009] EPRI (2009). Report to nist on the smart grid interoperability standards roadmap. Electric Power Research Institute.

[Falliere et al. 2011] Falliere, N., Murchu, L. O., and Chien, E. (2011). W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5:6.

[Fangfang et al. 2013] Fangfang, W., Huazhong, W., Dongqing, C., and Yong, P. (2013). Substation communication security research based on hybrid encryption of des and rsa. In *Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on*, pages 437–441. IEEE.

[Finster and Baumgart 2015] Finster, S. and Baumgart, I. (2015). Privacy-aware smart metering: A survey. *IEEE Communications Surveys & Tutorials*, 17(2):1088–1101.

[Giani et al. 2011] Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., and Poolla, K. (2011). Smart grid data integrity attacks: Characterizations and countermeasures. *Cyber and Physical Security and Privacy*, pages 232–237.

[Greveler et al. 2012] Greveler, U., Glösekötterz, P., Justusy, B., and Loehr, D. (2012). Multimedia content identification through smart meter power usage profiles. In *Proceedings of the International Conference on Information and Knowledge Engineering (IKE)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[Group 2010] Group, C. S. W. (2010). The smart grid interoperability panel - guidelines for smart grid cyber security. NISTIR 7628, pp. 1-597.

[Gungor et al. 2011] Gungor, V., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., and Hancke, G. (2011). Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, 7(4):529–539.

[IEC 2007] IEC (1988- 2007). IEC 60870-5: Telecontrol equipment and systems - Part 5: Transmission protocols. Technical report, International Electrotechnical Commission.

[IEC 2013] IEC (2002- 2013). IEC 61850: Communication networks and systems for power utility automation. Technical Report IEC 61850, International Electrotechnical Commission.

[IEC 2009] IEC, T. (2009). 57. communication networks and systems in substations–part 7–420: basic communication structure–distributed energy resources logical nodes. *Int. Electrotech. Comm.*

[IEEE 2012] IEEE (2012). Ieee standard for electric power systems communications-distributed network protocol (dnp3). pages 1–821. IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010).

[Kazienko et al. 2015] Kazienko, J. F., Moraes, I. M., Albuquerque, C. V., et al. (2015). On the performance of a secure storage mechanism for key distribution architectures in wireless sensor networks. *International Journal of Distributed Sensor Networks*, 2015:1.

[Khaitan et al. 2015] Khaitan, S. K., McCalley, J. D., and Liu, C. C. (2015). *Cyber Physical Systems Approach to Smart Electric Power Grid*. Springer.

[Kounev et al. 2016] Kounev, V., Lévesque, M., Tipper, D., and Gomes, T. (2016). Reliable communication networks for smart grid transmission systems. *Journal of Network and Systems Management*, pages 1–24.

[Kush et al. 2014] Kush, N., Ahmed, E., Branagan, M., and Foo, E. (2014). Poisoned goose: exploiting the goose protocol. In *Proceedings of the Twelfth Australasian Information Security Conference-Volume 149*, pages 17–22. Australian Computer Society, Inc.

[Lee et al. 2011] Lee, E.-K., Oh, S. Y., and Gerla, M. (2011). Frequency quorum rendezvous for fast and resilient key establishment under jamming attack. *ACM SIGMOBILE Mobile Computing and Communications Review*, 14(4):1–3.

[Li and Han 2011] Li, H. and Han, Z. (2011). Manipulating the electricity power market via jamming the price signaling in smart grid. In *2011 IEEE GLOBECOM Workshops (GC Wkshps)*, pages 1168–1172. IEEE.

[Li et al. 2015] Li, Q., Ross, C., Yang, J., Di, J., Balda, J. C., and Mantooth, H. A. (2015). The effects of flooding attacks on time-critical communications in the smart grid. In *Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society*, pages 1–5. IEEE.

[Lopes et al. 2015a] Lopes, Y., Fernandes, N. C., and Muchaluat-Saade, D. C. (2015a). Geração Distribuída de Energia: Desafios e Perspectivas em Redes de Comunicação. In *Minicursos do XXXIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 55–109. Sociedade Brasileira de Computação (SBC), "Vitória, Espírito Santo, Brasil", 1 edition.

[Lopes et al. 2012] Lopes, Y., Frazão, R. H., Molano, D. A., dos Santos, M. A., Calhau, F. G. a., Bastos, C. A. M., Martins, J. S. B., and Fernandes, N. C. (2012). Smart Grid e IEC 61850: Novos Desafios em Redes e Telecomunicações para o Sistema Elétrico. In *Minicursos do XXX Simpósio Brasileiro de Telecomunicações*, pages 1–44. 1 edition.

[Lopes et al. 2015b] Lopes, Y., Muchaluat-Saade, D. C., Fernandes, N. C., and Fortes, M. Z. (2015b). Geese: A traffic generator for performance and security evaluation of iec 61850 networks. In *2015 IEEE 24th International Symposium on Industrial Electronics (ISIE)*, pages 687–692. IEEE.

[Lüders 2011] Lüders, S. (2011). Why control system cybersecurity sucks. GovCERT.NL Symposium.

[McDaniel and McLaughlin 2009] McDaniel, P. and McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security and Privacy*, 7(3):75–77.

[Mishra et al. 2016] Mishra, S., Dinh, T. N., Thai, M. T., Seo, J., and Shin, I. (2016). Optimal packet scan against malicious attacks in smart grids. *Theoretical Computer Science*, 609:606–619.

[Molina-Markham et al. 2010] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., and Irwin, D. (2010). Private memoirs of a smart meter. In *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*, pages 61–66. ACM.

[Neuman and Tan 2011] Neuman, C. and Tan, K. (2011). Mediating cyber and physical threat propagation in secure smart grid architectures. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 238–243.

[Nicanfar et al. 2014] Nicanfar, H., Jokar, P., Beznosov, K., and Leung, V. C. (2014). Efficient authentication and key management mechanisms for smart grid communications. *IEEE systems journal*, 8(2):629–640.

[NIST 2010] NIST (2010). Nist 7628 - guidelines for smart grid cyber security vol. 1: smart grid cyber security strategy, architecture, and high-level requirements. National Institute of Standards and Technology.

[Noce et al. 2016] Noce, J., Lopes, Y., Muchaluat-Saade, D. C., Fernandes, N. C., and Albuquerque, C. (2016). Identificando falhas de segurança na rede de comunicação de subestações digitalizadas em redes elétricas inteligentes utilizando GEESE 2.0. In *XXI Congresso Brasileiro de Automática (CBA)*, pages 1–6. SBA.

[Organization 2005] Organization, M. (2005). *Modbus protocol*. www.modbus.org/specs.php.

[Pan et al. 2014] Pan, J., JAIN, R., and Paul, S. (2014). A survey of energy efficiency in buildings and microgrids using networking technologies. *IEEE Communications Surveys Tutorials*, (3):1709–1731.

[Patel et al. 2011] Patel, A., Aparicio, J., Tas, N., Loiacono, M., and Rosca, J. (2011). Assessing communications technology options for smart grid applications. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 126–131.

[PUB 2006] PUB, F. (2006). Minimum security requirements for federal information and information systems.

[Rahimi et al. 2011] Rahimi, S., Chan, A. D., and Goubran, R. A. (2011). Usage monitoring of electrical devices in a smart home. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 5307–5310. IEEE.

[Rahman et al. 2012] Rahman, M., Bera, P., and Al-Shaer, E. (2012). SmartAnalyzer: A noninvasive security threat analyzer for AMI smart grid. In *Proceedings IEEE INFOCOM*, pages 2255 – 2263.

[Rodofile et al. 2015] Rodofile, N., Radke, K., and Foo, E. (2015). Real-time and interactive attacks on dnp3 critical infrastructure using scapy.

[Sharma and Saini 2015] Sharma, K. and Saini, L. M. (2015). Performance analysis of smart metering for smart grid: An overview. *Renewable and Sustainable Energy Reviews*, 49:720–735.

[Siddiqui et al. 2012] Siddiqui, F., Zeadally, S., Alcaraz, C., and Galvao, S. (2012). Smart grid privacy: Issues and solutions. In *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, pages 1–5. IEEE.

[Sun et al. 2016] Sun, C.-C., Liu, C.-C., and Xie, J. (2016). Cyber-physical system security of a power grid: State-of-the-art. *Electronics*, 5(3):40.

[Ur-Rehman et al. 2015] Ur-Rehman, O., Zivic, N., and Ruland, C. (2015). Security issues in smart metering systems. In *Smart Energy Grid Engineering (SEGE), 2015 IEEE International Conference on*, pages 1–7. IEEE.

[Varodayan and Khisti 2011] Varodayan, D. and Khisti, A. (2011). Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage. In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1932–1935. IEEE.

[Wang et al. 2011] Wang, J., Yang, X., and Long, K. (2011). Web DDoS detection schemes based on measuring user's access behavior with large deviation. In *IEEE Global Telecommunications Conference (GLOBECOM 2011)*, pages 1 – 5.

[Wei and Wang 2014] Wei, M. and Wang, W. (2014). Greenbench: A benchmark for observing power grid vulnerability under data-centric threats. In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pages 2625–2633.

[Wei and Wang 2016] Wei, M. and Wang, W. (2016). Data-centric threats and their impacts to real-time communications in smart grid. *Computer Networks*, 104:174–188.

[Wilhoit 2013] Wilhoit, K. (2013). The scada that didn't cry wolf. *Trend Micro Inc., White Paper*.

[Yan et al. 2011] Yan, Y., Qian, Y., and Sharif, H. (2011). A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 909 –914.

[Yoo and Shon 2015] Yoo, H. and Shon, T. (2015). Novel approach for detecting network anomalies for substation automation based on iec 61850. *Multimedia Tools and Applications*, 74(1):303–318.

[Zhu et al. 2011] Zhu, T., Xiao, S., Ping, Y., Towsley, D., and Gong, W. (2011). A secure energy routing mechanism for sharing renewable energy in smart microgrid. In *2011 IEEE International Conference on Smart Grid Communications (IEEE SmartGridComm)*, pages 143–148.