Capítulo 3

Comunicação em Redes Elétricas Inteligentes: Eficiência, Confiabilidade, Segurança e Escalabilidade

Pedro Henrique V. Guimarães, Andrés Murillo, Martin Andreoni, Diogo M. F. Mattos, Lyno Henrique G. Ferraz, Fabio Antonio V. Pinto[1], Luís Henrique M. K. Costa e Otto Carlos M. B. Duarte

GTA/PEE-COPPE/DEL-Poli - Universidade Federal do Rio de Janeiro - RJ, Brasil
[1]Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - RJ, Brasil

Resumo

O modelo de redes elétricas inteligentes, conhecidas como Smart Grids, representa uma evolução do sistema elétrico atual. A ideia chave consiste em agregar inteligência à rede elétrica, através de tecnologias de comunicação e computação que permitem coletar dados em tempo real, monitorar e controlar a rede elétrica de forma autônoma. O objetivo principal é garantir maior confiabilidade, eficiência e qualidade do sistema de energia. Neste novo paradigma, os consumidores, as concessionárias e diversos outros atores têm acesso às comunicações e, portanto, existem ameaças e riscos de segurança que devem ser avaliados. Esse minicurso aborda os elementos básicos, inclusive o carro elétrico, do sistema elétrico inteligente, focando nas ameaças e nos desafios relacionados à segurança da comunicação. São apresentados projetos e iniciativas de pesquisa aplicadas às redes elétricas inteligentes, no Brasil e no exterior, assim como uma plataforma de testes baseada em virtualização.

Abstract

Smart grids represent an evolution of the current electrical system. Their key idea is to add intelligence to the power grid, through computing and communication technologies which enable real-time data collection, and autonomous monitoring and control of the grid. The main goal is to ensure greater reliability, efficiency, and quality to the power system. In this new paradigm, there are threats and cyber-security risks that must be evaluated. This short course discusses the basic elements of the smart grid, including electric cars, focusing on the threats and challenges related to cyber-security. We present projects and initiatives applied to smart grids in Brazil and abroad, as well as a virtualization-based testbed.

Este trabalho utilizou recursos da CAPES, CNPq, CTIC, FAPERJ, FINEP, FUJB, FUNTTEL e UOL.

3.1. Introdução

A rede elétrica convencional consiste em um fluxo de energia unidirecional que parte das geradoras para os consumidores. A energia é produzida em grandes plantas de geração, transmitida até as centrais de distribuição localizadas em regiões próximas dos consumidores e, finalmente, distribuída aos consumidores. As redes elétricas inteligentes, ou *smart grids*, referem-se ao uso intensivo de modernas técnicas de comunicação e de informação para garantir maior confiabilidade e oferecer mais qualidade ao sistema de energia elétrica. Nas redes elétricas inteligentes os fluxos de energia e de comunicação são bidirecionais. O consumidor poderá gerar e "vender" energia, criando a nova figura do "prossumidor", ou seja, o produtor e consumidor de energia ao mesmo tempo. O objetivo principal das redes elétricas inteligentes é melhorar a confiabilidade, a eficiência e a qualidade da energia elétrica modernizando e digitalizando os dispositivos e equipamentos, integrando os sistemas de geração, transmissão e distribuição, monitorando de forma acurada com coleta de dados exaustiva, automatizando o controle e a operação do sistema para evitar falhas humanas, provendo agilidade e autocura para reação rápida de forma a evitar interrupções ou restringir a área afetada, entre outros. As redes elétricas inteligentes trarão outros benefícios como geração distribuída e a incorporação da energia com fontes renováveis, as microrredes, a maior participação do consumidor e o carro elétrico.

Confiabilidade, Eficiência e Qualidade da Energia Elétrica

A confiabilidade é fundamental para a rede elétrica. Os sistemas elétricos devem operar em conformidade com o funcionamento esperado. Por confiabilidade, entende-se que as falhas, que porventura venham a ocorrer no sistema, ocorram com baixíssima probabilidade e, se algum componente falhar, que o impacto para o sistema seja minimizado e o componente que falhou restaurado em tempo mínimo [Wenye et al., 2011]. No cenário brasileiro, o Operador Nacional do Sistema (ONS) define os procedimentos para restauração do sistema elétrico depois de uma falha, que variam de acordo com a área geográfica e a disponibilidade de fontes de energia [Gomes et al., 2004]. O Sistema Interligado Nacional (SIN) é um sistema de coordenação e controle do sistema de geração e transmissão elétrica do Brasil. O SIN é um sistema hidrotérmico formado pelas empresas das regiões Sul, Sudeste, Centro-Oeste, Nordeste e parte da região Norte. A produção de energia elétrica é predominantemente de usinas hidrelétricas de múltiplos proprietários estatais e privados. Apenas 3,4% da capacidade de produção de eletricidade do Brasil encontra-se fora do SIN, em pequenos sistemas isolados, localizados principalmente na região amazônica [ONS, 2013]. A Figura 3.1 mostra as diferentes linhas de transmissão de alta tensão dentro do país (de 138, 230, 345, 440, 500 e 750 kV), além das projeções de futuras linhas e os centros hidrelétricos conectados pelo SIN. O ONS opera o SIN e tem como objetivo garantir a confiabilidade, a continuidade, a economicidade no atendimento de energia elétrica.

O apagão (*blackout*) é o evento mais alarmante de constatação de falta de qualidade do sistema elétrico, pois envolve enormes perdas financeiras e evidencia a vulnerabilidade do sistema elétrico. O apagão consiste na perda completa de fornecimento de energia elétrica em uma determinada área. Infelizmente, o Brasil ocupa uma posição de destaque negativo no cenário mundial, pois é o país campeão em número de apagões de grandes dimensões com três apagões entre os dez mais importantes apagões registrados

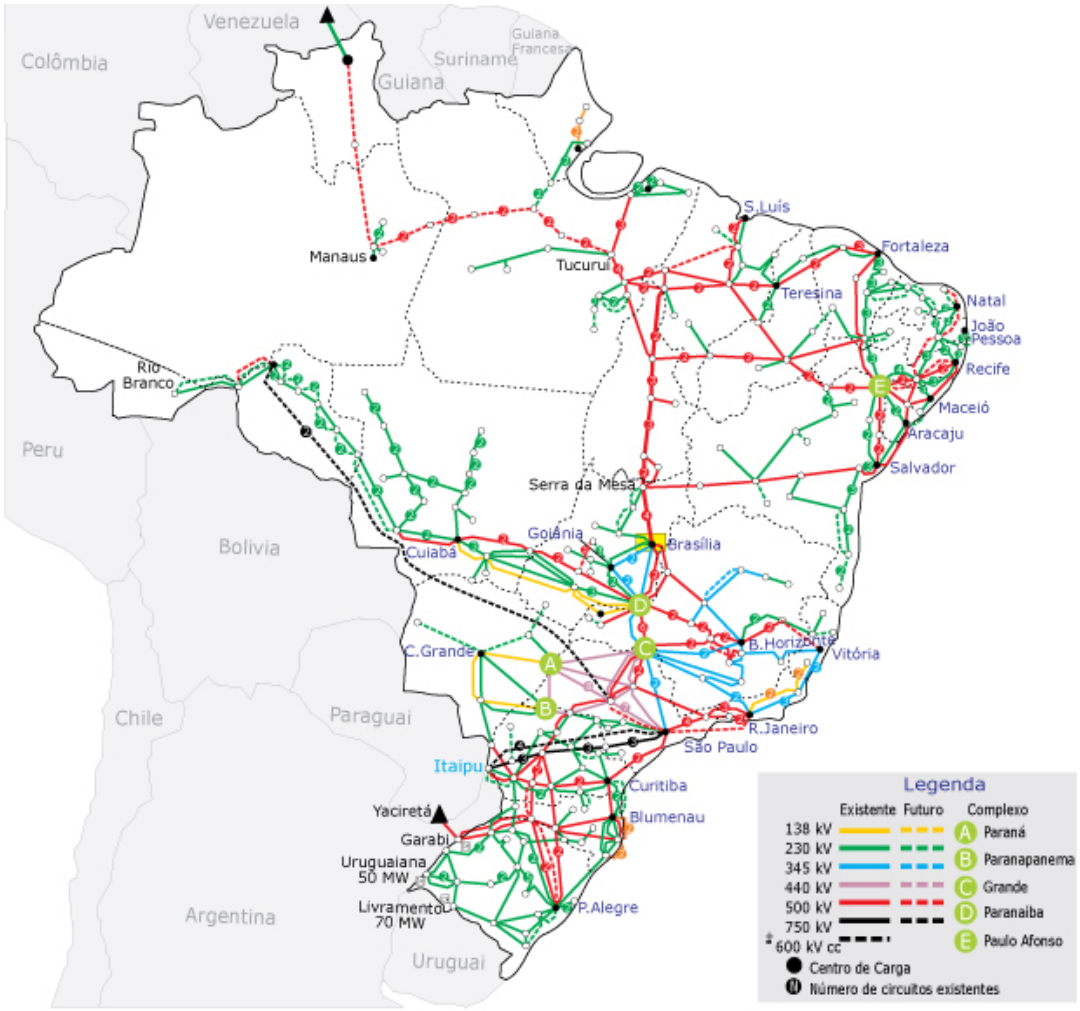


Figura 3.1. Esquema do Sistema Interligado Nacional (SIN). Linhas de transmissão, centros de carga e complexos hidrelétricos no país. Fonte [ONS, 2013].

até hoje, conforme mostra a Tabela 3.1. O maior, em 1997, afetou 97 milhões de pessoas durante 5 horas; o segundo, no ano de 2009 afetou, no Brasil e no Paraguai, 87 milhões de pessoas por até 7 horas; e finalmente, o apagão de 2011 afetou por 16 horas mais de 53 milhões de pessoas [CRO, 2011]. O apagão normalmente não é um evento isolado e costuma ser uma sequência de eventos causados por uma combinação de falhas e deficiências, que em cascata terminam por colapsar o sistema elétrico. As principais causas de apagões são: causas humanas - devido a demanda súbita de energia, falhas humanas e ataques cibernéticos; causas materiais – devido a obsolescência, falta de manutenção e danos materiais nas transmissões elétricas, nas subestações ou no sistema de distribuição; e causas ambientais - desastres naturais (enchentes, terremotos, tsunamis, furacões, raios etc.), contatos das linhas com árvores, etc.

Nos Estados Unidos, em 2003, um apagão afetou 50 milhões de pessoas com uma perda de energia elétrica de 65 GW [Bialek, 2007]. Em algumas partes, a energia elétrica só conseguiu ser restaurada quatro dias depois do início do apagão. O Departamento de Energia (DOE) dos Estados Unidos estima que o prejuízo total foi da ordem

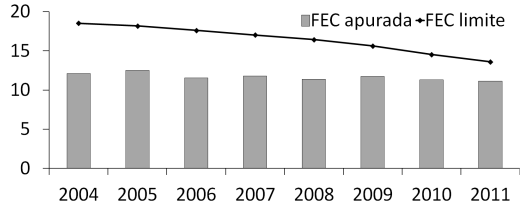
Tabela 3.1. Maiores apagões no mundo desde 1980 [CRO, 2011].

Países	Data	Causas	Duração	Habitantes afetados
Nova Zelândia	20/02/1988	Falhas técnicas	4 semanas	70.000.000
Brasil	11/03/1999	Eventos naturais	5 horas	97.000.000
Índia	02/01/2001	Falhas técnicas	12 horas	226.000.000
Estados Unidos e Canadá	14/08/2003	Falhas técnicas e de comunicação	4 dias	50.000.000
Itália	28/09/2003	Falhas técnicas	18 horas	56.000.000
Espanha	29/11/2004	Falhas humanas e técnicas	5 apagões em 10 dias	2.000.000
Indonésia	18/08/2005	Falhas técnicas	7 horas	100.000.000
Sudoeste da Europa	04/11/2006	Falhas humanas e de comunicação	2 horas	15.000.000
Brasil e Paraguai	10/11/2009	Eventos naturais	25 minutos a 7 horas	87.000.000
Brasil	04/02/2011	Falhas técnicas	16 horas	53.000.000

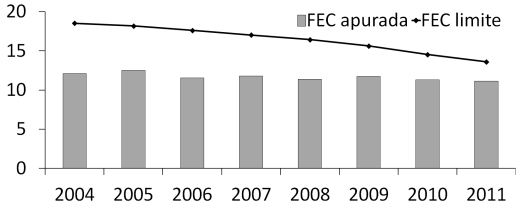
de seis bilhões de dólares. As causas principais do apagão foram falhas materiais e de comunicação tais como: o funcionamento errado de equipamentos críticos; sistemas de alarme e simuladores do sistema elétrico, que falharam durante várias etapas do apagão; e uma comunicação inadequada entre os operadores que os levou a tomadas de decisões erradas ao procurarem responder aos eventos iniciais do apagão.

Em 10 de agosto de 1996, a parte oeste da América do Norte, controlada pelo *Western Electricity Coordinating Council* (WECC), sofreu um apagão causado por falha de comunicação e coordenação entre os operadores da rede elétrica. O apagão, naquela ocasião, foi iniciado a partir de uma série de desligamentos planejados de equipamentos de alta-tensão. Embora planejado, o desligamento desses equipamentos gerou sobrecarga na parte do sul da região controlada pelo WECC. Com isso, ocorreu uma degradação gradual da rede elétrica, até que a maior linha de transmissão da rede caiu e esse evento se alastrou, gerando um apagão. Todo o sistema elétrico colapsou em menos de 6 min [Zima et al., 2005]. Esse caso evidencia que a confiabilidade da rede elétrica se beneficiaria da introdução de tecnologias de coordenação, controle e comunicação entre os diversos pontos da rede em tempo real para reagir a eventos em cadeia. Além do apagão (*blackout*) existe também a queda de tensão (*brownout*) intencional ou não intencional que ocorre com a redução da carga em emergências, procedimento utilizado por administradores de sistemas de energia como medida preventiva ao apagão total.

A Agência Nacional de Energia Elétrica (ANEEL) comprova uma qualidade muito baixa da energia elétrica oferecida. Duas medidas são utilizadas: a Duração Equivalente de Interrupção por Unidade Consumidora (DEC) e a Frequência Equivalente de Interrupção por Unidade Consumidora (FEC). A Figura 3.2 mostra o comportamento anual da FEC e da DEC no Brasil desde o ano de 2004. Pode-se observar que de 2009 a 2011 a DEC apurada ultrapassou os limites anuais estabelecidos pela ANEEL, apesar de a meta da FEC ter sido alcançada em todos os anos. Isto indica que embora as quedas de



(a) Duração Equivalente de Interrupção por Unidade Consumidora (DEC).



(b) Frequência Equivalente de Interrupção por Unidade Consumidora (FEC).

Figura 3.2. Comportamento anual das métricas DEC e FEC no Brasil desde o ano 2004 [ANEEL, 2012].

energia tenham sido dentro do previsto, sua duração foi superior às metas estabelecidas. A Figura 3.3 mostra que a América Latina apresenta uma duração média de interrupção muito alta, de aproximadamente 8 horas. A confiabilidade almejada para o fornecimento de energia elétrico é muito alta, os famosos "cinco noves" (99,999%): isto que equivale a pouco mais de cinco minutos de interrupção de energia anual. O comportamento insatisfatório da FEC e da DEC são fatores impeditivos para que certas companhias invistam e instalem suas fábricas no Brasil.

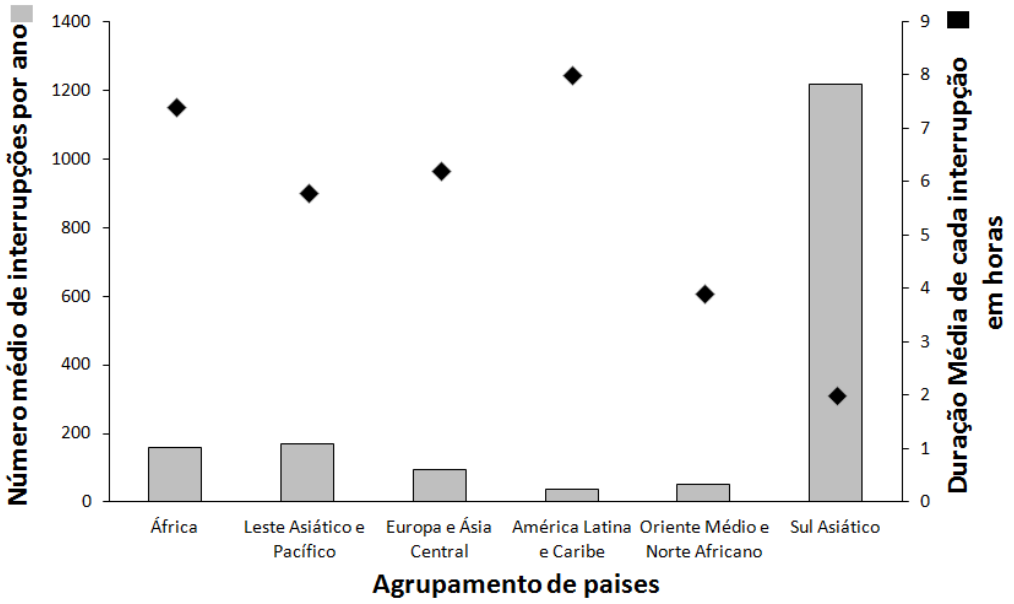


Figura 3.3. Interrupções de energia por ano e duração em horas. Ano 2009. Fonte [WorldBank, 2009].

A eficiência é outra característica que deve ser melhorada com as redes elétricas inteligentes. Hoje, a rede elétrica conta com perdas técnicas e a perdas não técnicas, estas últimas também conhecidas como "gatos". As redes elétricas inteligentes também prometem resolver o problema dos "gatos", que no Brasil chegam a 20% de prejuízo para as concessinárias.

A confiabilidade das redes elétricas está associada, então, à confiabilidade da rede

de comunicação e à confiabilidade dos sistemas de monitoramento e controle. A operação correta dos sistemas de monitoramento e controle de energia, por sua vez, depende de que as comunicações entre os dispositivos eletrônicos inteligentes (IEDs – *Intelligent Electronic Devices*) ocorram como esperado. Assim, a confiabilidade das redes elétricas inteligentes será obtida com o uso intensivo de tecnologias de comunicações e de processamento de dados na geração, transmissão e distribuição de energia. Dessa forma, as redes elétricas inteligentes trazem para as redes elétricas atuais a capacidade de autorecuperação, a tolerância a ataques externos, o aumento da qualidade da energia, a inclusão de novas fontes e demandas de energia, a resposta dinâmica da rede à demanda de energia dos consumidores e a viabilização de mercados mais competitivos de energia e a microgeração de energia [Falcão, 2010].

As redes de comunicação são elementos chave para a oferta de confiabilidade mas, ao mesmo tempo, podem ser causadoras de mais interrupções e apagões. O acesso dos consumidores e de novos diferentes atores às redes elétricas inteligentes traz consigo o risco dos ataques cibernéticos. A rede de comunicação, desde a sua concepção, deve prever o risco de ataques cibernéticos e garantir a segurança necessária ao sistema elétrico.

Fontes Renováveis

A introdução de fontes de energia renováveis na matriz energética dos países tem como principal motivação uma maior diversificação da matriz energética e, consequentemente, uma menor dependência do combustível fóssil cuja produção está concentrada em poucos países. A produção de combustível fóssil deve começar a declinar e existem estimativas que indicam que a produção não dura por mais 80 anos. Além disso, o preço do combustível fóssil tem se mostrado muito volátil. Por fim, o mais importante é o desafio climático do planeta, que tem como principal vilão a emissão de carbono devido aos combustíveis fósseis. Assim, as fontes de energia renováveis, ou energia "verde", vêm recebendo muita atenção e investimentos crescentes nos últimos anos. Novas fontes de energia renováveis baseadas no vento, raios solares, marés, ou ainda efeitos geotérmicos estão sendo utilizadas, além da convencional energia hidrelétrica. Infelizmente, as novas fontes de energia renováveis ainda não são economicamente competitivas e necessitam de subsídios governamentais.

Uma particularidade do Brasil é que a matriz energética é uma das mais "limpas" do mundo, com quase 80% de energia gerada por hidrelétricas. O Brasil também é referência em fonte renovável de biomassa, devido ao programa avançado de produção de etanol que foi iniciado durante a primeira crise do petróleo nos anos 70 com o programa ProÁlcool de 1974.

A **energia eólica** é a energia produzida a partir do vento através da captação por turbinas eólicas tanto em terra (*onshore*), quanto em fazendas eólicas em regiões mais afastadas da costa, no mar (*offshore*). Ela é considerada uma das mais promissoras fontes naturais de energia, porque é renovável, limpa e amplamente distribuída globalmente. O Brasil possui um enorme potencial eólico, estimado em 140 GW, mas atualmente a capacidade instalada é de apenas 1 GW, ou menos de 1% do potencial. A **energia solar** é a energia luminosa ou térmica captada do Sol. O Sol é uma enorme fonte de energia uma vez que a Terra recebe 174 petawatts (PW) de radiação solar na camada superior de sua atmosfera. Apenas uma pequeníssima parte da energia solar é aproveitada, pois tem como

Tabela 3.2. Investimento e Custo da Geração por Tecnologia. Países da Organização para a Cooperação e Desenvolvimento Econômico [Barroso et al., 2010].

	2008		2030	
	Investimento (USD/kW)	Custo (USD/MWh)	Investimento (USD/kW)	Custo (USD/MWh)
Nuclear	1600-5900	42-137	3200-4500	55-80
Hidrelétrica	2960-3670	50-140	2550-3150	35-120
Biomassa	1970-2600	45-105	1940-2570	40-100
Eólica *Onshore*	1900-3700	50-234	1440-1600	70-85
Geotérmica	3470-4060	65-80	3020-3540	55-70
Captura e Armazenamento de CO_2	3223-6268	67-142	1400	94-104
Gás Natural	520-1800	76-120	900	78
Energia Solar Concentrada	3470-4500	136-243	1730-2160	70-220
Eólica *Offshore*	2890-3200	146-261	2280-2530	80-95
Maremotriz	5150-5420	195-220	2240-2390	100-115
Solar Fotovoltaica	5730-6800	333-600	2010-2400	140-305

desvantagens o preço elevado do painel solar, o custo energético alto para fabricação do painel, a variação da geração de energia e, principalmente, a diminuição de geração de energia, com chuvas e nuvens, e ausência de geração à noite. A **energia geotérmica** é a energia obtida a partir do calor proveniente do interior da Terra. O calor da Terra, embora exista em toda parte, está mais perto da superfície em algumas regiões nas quais com furos de 1 centena de metros é possível alcançar calor útil para geração de energia, o que torna mais fácil a sua utilização. No entanto, na maior parte do mundo, furos de quilômetros de profundidade são necessários para encontrar calor significativo. A **energia das correntes marítimas** é obtida através do aproveitamento da energia cinética. Embora não seja ainda muito explorada atualmente, esta energia tem um grande potencial pelas correntes serem mais previsíveis do que o vento. A **energia das ondas** provém do aproveitamento das ondas oceânicas. A **energia maremotriz** é a energia obtida pelas marés através da movimentação da água dos oceanos. Dois tipos de energia maremotriz podem ser obtidas: energia cinética das correntes devido às marés e energia potencial pela diferença de altura entre as marés alta e baixa. A **energia azul** é a energia obtida da diferença de concentração de sal entre a água do mar e a do rio com o uso de eletrodiálise reversa (EDR) (ou osmose) com membranas específicas para cada tipo de íon. A comparação entre o investimento de instalação e o custo de geração para cada tecnologia de geração é apresentada na Tabela 3.2.

Microrredes e Geração Distribuída

Microrredes (*microgrids*) são uma forma eficiente de se conectar fontes de energia de diferentes tipos e capacidades [Falcão, 2010]. As microrredes são sistemas de energia compostas por pequenos ou médios geradores, chamados Geradores Distribuídos (GD), dispositivos de armazenamento de energia, sistemas de controle e um sistema de distribuição de média ou baixa tensão. As microrredes têm o potencial de melhorar sig-

nificativamente a confiabilidade do fornecimento de energia elétrica, pois baseiam-se no pressuposto de que a maior parte da geração de energia está restrita a uma área menor e mais próxima do consumidor. As microrredes podem operar conectadas ao sistema principal de energia ou operar de forma isolada, o modo ilha [Borges e Cantarino, 2011]. O modo ilha das microrredes permite que os geradores distribuídos entreguem a energia necessária para as cargas da microrrede sem usar a energia elétrica da rede principal. Este modo pode ser usado em caso de falhas ou, se no sistema de energia existem aplicações tipo resposta à demanda, para reduzir os gastos de energia quando o preço da energia é elevado. Assim, as microrredes proverão um fornecimento elétrico de maior confiabilidade [Molina e Mercado, 2011].

As microrredes apresentam diversos impactos na operação do sistema, principalmente quanto ao controle da rede e de equipamentos de proteção. A situação é ainda mais crítica quando as microrredes contam com recursos de geração de energia intermitentes, como por exemplo a geração eólica [Leite et al., 2006]. A geração intermitente não garante o fluxo contínuo de energia e nem garante que o pico de consumo de energia na microrrede ocorra no momento do pico de geração da fonte intermitente [Martins e Borges, 2011]. Borges e Cantarino apresentam um modelo para avaliação da confiabilidade de microrredes com geração distribuída com base em recursos renováveis de energia [Borges e Cantarino, 2011]. São propostos modelos estocásticos para representar a disponibilidade de geração de energia de fontes intermitentes e o armazenamento de energia é explorado como forma de reduzir a intermitência dessas fontes. Sendo assim, as microrredes são parte das redes elétricas inteligentes e contribuem para a garantia da confiabilidade da rede como um todo, já que tendem a ser autossuficientes para a geração e consumo de energia, diminuindo a sobrecarga no restante da rede elétrica. O estado-da-arte em modelos de confiabilidade para redes elétricas de distribuição considerando fontes de energia renováveis pode ser encontrado em [Borges, 2012].

Participação do Consumidor e Aplicações de Resposta à Demanda

As redes elétricas inteligentes permitirão uma maior participação do consumidor, que pode obter em tempo *quase* real dados do seu consumo e do custo da energia. Espera-se uma maior conscientização do consumidor que pode ter como consequência uma maior participação e responsabilidade no fornecimento e no uso da energia elétrica. Neste sentido, as aplicações de Resposta à Demanda (*Demand Response Application* - DR) objetivam prover confiabilidade à rede elétrica através de uma série de ações que visam reduzir a carga da rede nas horas de pico, quando a concessionária está perto da sua capacidade máxima [NIST7628, 2010a]. As ações podem ser de iniciativa tanto do consumidor quanto da própria concessionária [Berger e Iniewski, 2012].

O Controle Direto de Carga (*Direct Load Control - DLC*) é uma aplicação em que as concessionárias enviam comandos para desligar alguns eletrodomésticos (como o ar condicionado ou o aquecedor de água) durante eventos de picos de demanda que podem afetar a rede [USFERC, 2012]. Diferentes esquemas de controle podem ser usados pela concessionária para decidir como desligar os equipamentos [Ruiz et al., 2009, Kondoh, 2011]. Nos Estados Unidos, a implantação de DLC, em 2012, foi a estratégia com maior impacto na redução de picos de demanda de consumo [USFERC, 2012].

No estado da Califórnia, várias aplicações baseadas em ações iniciadas pelo con-

sumidor estão sendo implantadas [PG&E, 2013]. As aplicações são: preço pelo horário de uso, preço por dia de pico e programa de base interruptível. O preço pelo horário de uso é uma aplicação em que o preço da energia não é fixo, mas varia em um conjunto de valores dependendo da época do ano e da hora do dia. O preço por dia de pico consiste, em certos dias, durante certas horas, em uma taxa extra que é cobrada dos consumidores pelo uso de energia. O programa de base interruptível é um programa em que os consumidores recebem um incentivo econômico se reduzirem o consumo durante um evento prejudicial à rede elétrica. O uso de aplicações de resposta à demanda na Califórnia promoveu a redução de 10% do custo da energia [Marris, 2008].

Carro Elétrico

Uma importante evolução do uso de energia são os carros elétricos. Carros elétricos podem ser conectados em diferentes pontos da rede. Os carros elétricos apresentam dois comportamentos importantes para as redes elétricas inteligentes, o armazenamento de energia, sob a forma de baterias, e a migração de energia elétrica. Os carros elétricos agem na rede elétrica tanto como consumidores, ao carregarem as suas baterias, como produtores, ao fornecerem energia às redes elétricas inteligentes. Simultaneamente, os carros agem também como mecanismos de distribuição de energia, permitindo a migração de energia, já que um carro que foi carregado em determinada região, onde por exemplo o custo da energia é mais barato, pode migrar para outra região em que o custo da energia é mais caro e passar a fornecer energia para a rede. Como gerenciar o consumo desses carros, de tal forma a evitar picos de demanda provocados pela introdução dos carros elétricos no sistema elétrico e de forma a otimizar o custo da energia durante a carga dos carros elétricos é um dos desafios das redes elétricas inteligentes. Além disso, carros que possuem mais de uma fonte de energia podem gerar e fornecer energia para o sistema elétrico de uma casa ou um prédio [Sorebo e Echols, 2012].

Organização do Minicurso

O restante desse minicurso está organizado da seguinte forma. A Seção 3.2 ressalta os principais componentes de uma rede elétrica inteligente, tais como a arquitetura da rede, os sistemas de controle e os principais protocolos de comunicação. Os requisitos e desafios de segurança das redes elétricas inteligentes são discutidos na Seção 3.3. Os projetos de pesquisa e os desafios em redes elétricas inteligentes são explorados na Seção 3.4, que apresenta também algumas propostas para aplicação e testes nas redes de comunicação das redes elétricas inteligentes. Por fim, a Seção 3.5 conclui o minicurso e apresenta perspectivas futuras na área de pesquisa.

3.2. Características e Componentes das Redes Elétricas Inteligentes

A transmissão elétrica é feita através de linhas de transmissão de alta tensão a partir das geradoras de energia até as linhas de baixa tensão que chegam às residências dos consumidores finais. Entre esses dois pontos da rede elétrica, existem as subestações, cujo papel é converter as altas tensões para tensões cada vez mais baixas, até que atinja os consumidores finais. As redes elétricas inteligentes trazem mais automação para a transmissão de energia. As redes elétricas inteligentes propõem a maior automação das subestações utilizando Dispositivos Eletrônicos Inteligentes (*Intelligent Electronic Devices* - IEDs) e Unidades Terminais Remotas (*Remote Terminal Units* - RTUs) para melho-

rar a capacidade de controle e monitoramento de dados. Novos protocolos de comunicação para essa automação vem sendo propostos, o principal deles é o padrão IEC 61850 [Berger e Iniewski, 2012].

As geradoras de energia normalmente encontram-se distantes dos consumidores. Assim, a energia precisa ser transmitida das plantas de geração até os centros de distribuição locais. A energia é transmitida em alta tensão para que a corrente seja baixa e reduza-se a perda de energia nas linhas de transmissão. Os centros de distribuição baixam a tensão para finalmente distribuir a energia aos consumidores [Sorebo e Echols, 2012]. O esquema tradicional das redes elétricas é mostrado na Figura 3.4.

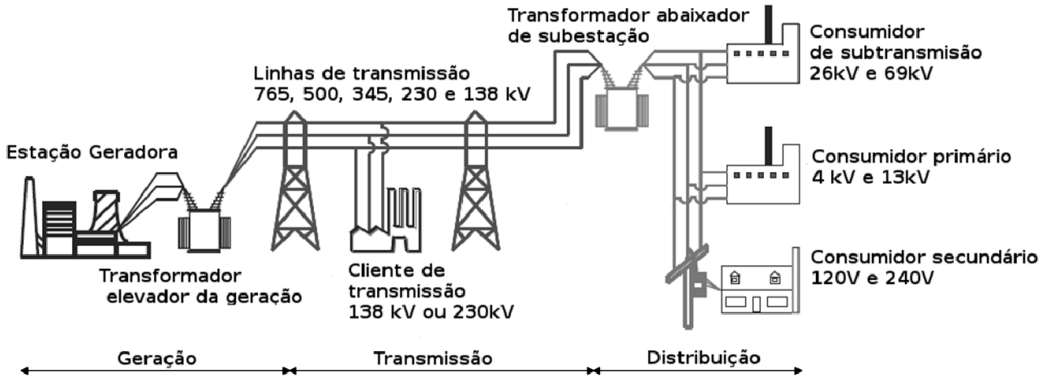


Figura 3.4. Esquema básico do Sistema Elétrico. Adaptado de [US-CPSOTF, 2004].

A geração, a transmissão e a distribuição da energia elétrica, assim como o controle do sistema são os componentes básicos do sistema elétrico atual. Contudo, com as redes elétricas inteligentes, outros atores surgem para melhorar a confiabilidade, a eficiência, a qualidade e a interação com os consumidores. O *National Institute of Standards and Technology* (NIST) [NIST2013, 2013] propõe um modelo conceitual de redes elétricas inteligentes composto de sete domínios de atores, que possuem objetivos ou que executam aplicações similares. Estes domínios são: geração de energia, transmissão, distribuição, consumidores, operação da rede elétrica, provedores de serviço e mercado de energia [NIST7628, 2010a]. Cada um desses domínios possui um ou mais atores que se interconectam com outros atores de outros domínios, de modo que cada conexão possui especificidades, como diferentes protocolos e requisitos de latência e banda [Wenye et al., 2011]. Assim, os domínios se comunicam para coordenar as diversas funções do sistema elétrico. A Figura 3.5 apresenta a visão geral dos domínios e a comunicação entre eles.

O fluxo de energia elétrica segue da geração para os consumidores, compreendendo os domínios geração de energia, transmissão, distribuição e consumidores. A rede elétrica inteligente permite fluxos bidirecionais de energia criando a figura do "prossumidor". Os fluxos de informação também são bidirecionais e englobam todos os domínios para garantir a interoperabilidade dos diversos serviços das redes elétrica inteligentes. O domínio de operação comunica-se com todos os outros domínios para adquirir diferentes tipos de informação e, como consequência, garantir o controle e a operação confiável e

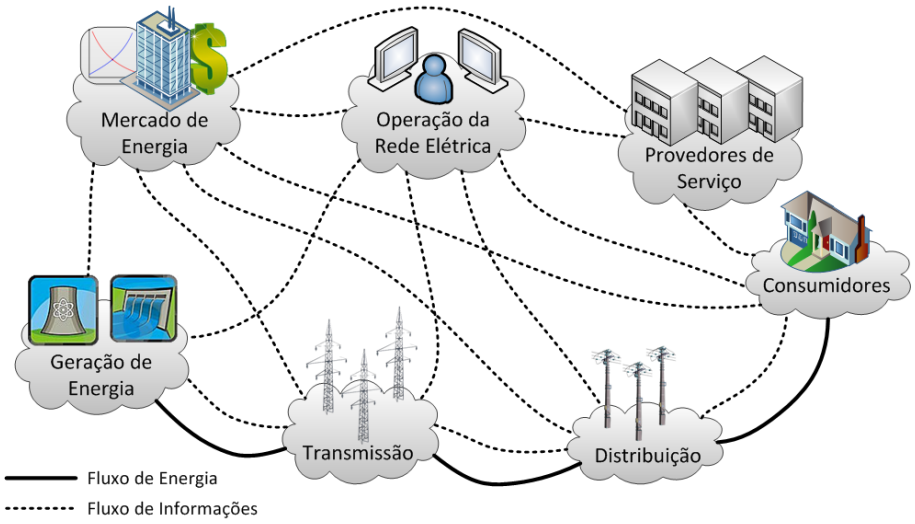


Figura 3.5. Os domínios de atores das redes elétricas inteligentes e a comunicação entre eles. Adaptado de [NIST7628, 2010a].

eficiente das redes elétricas inteligentes. O domínio de geração de energia é composto pelas grandes plantas de geração e armazenamento de energia. Portanto, esse domínio conecta-se com os domínios de operação da rede elétrica e mercado de energia para controle e notificação de capacidade ou de escassez de energia. Os domínios de transmissão e distribuição são constituídos basicamente de subestações e linhas de transmissão de energia e, então esses domínios comunicam-se principalmente com o domínio de operação. Além disso, o domínio de distribuição também coleta informações dos medidores inteligentes (*smart meters*) do domínio de consumidores. O domínio de mercado é responsável pelo balanceamento de oferta e demanda de energia e, portanto, o domínio de mercado coleta e envia informações de oferta e demanda aos domínios de geração, provedores de serviços e operação da rede elétrica inteligente. O domínio de consumidores agrega diversas funcionalidades como consumo, geração de energia em pequena escala e armazenamento energético. Esse domínio se comunica com os domínios de operação da rede elétrica e domínio de mercado. Por fim, o domínio de provedor de serviços comunica-se com o domínio de consumidores para tarifação, operação das aplicações de resposta à demanda e operação de serviços de terceiros. O domínio de provedor de serviços também se comunica com o domínio de mercado e domínio de operação da rede elétrica para obter informações de medições e controle de da rede elétrica.

A confiabilidade, a eficiência e também a segurança do sistema de comunicação, que interconecta os diferentes atores e que interconecta diferentes entidades de um mesmo ator, são essenciais. As redes de comunicação podem cobrir longas, médias ou pequenas distâncias, podem ter requisitos diferentes de vazão e atraso e podem interconectar alguns ou milhões de dispositivos com ou sem restrições de capacidade de processamento. Assim, diversas tecnologias de redes de comunicação são usadas para atender os diferentes requisitos [Wenye e Zhuo, 2013]. A Figura 3.6 mostra as redes de comunicação entre os domínios. A rede de longo alcance é utilizada para a comunicação inter-domínio entre dispositivos e serviços localizados em redes locais diferentes. A rede de longo alcance

pode ser usada para a aquisição de dados e controle remoto de centros de operação da rede elétrica com as subestações da transmissão e distribuição e comunicação com os domínios de mercados de energia e de provedores de serviços. A infraestrutura da rede de longo alcance contém elementos encaminhadores de tráfego de alta capacidade para a comunicação entre os diversos atores e *gateways*[1] para a interface com as redes locais.

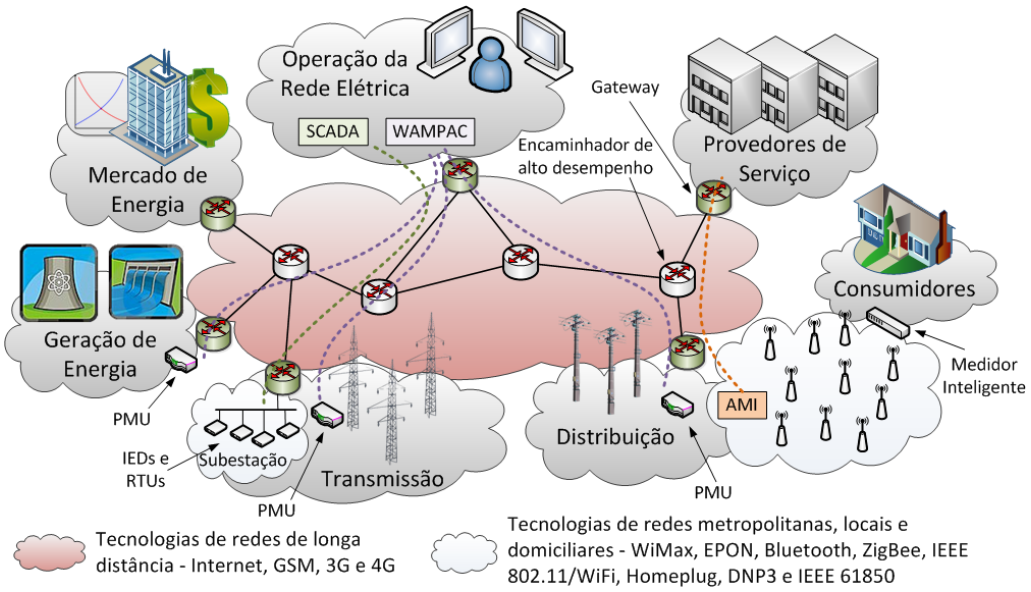


Figura 3.6. Arquitetura de comunicação entre os domínios de atores das redes elétricas inteligentes. Uma tecnologia de rede de longo alcance permite a comunicação entre atores geograficamente dispersos em uma vasta área, enquanto que as tecnologias de redes para distâncias médias e redes locais possibilitam a interconexão local de dispositivos. As técnicas de acesso ao meio, assim como o meio físico, também diferem para atender requisitos de vazão, atraso, mobilidade e escala.

Conectadas à rede de longo alcance pelos *gateways*, as redes de média distância e as redes locais são utilizadas para comunicação intra-domínio de dispositivos instalados na infraestrutura elétrica como dispositivos eletrônicos inteligentes, sensores e medidores inteligentes [Berger e Iniewski, 2012]. As redes de médias distâncias e redes locais contêm elementos encaminhadores estruturados e elementos encaminhadores *ad hoc* para o estabelecimento da comunicação sem a necessidade da criação de uma infraestrutura. Alguns dispositivos das redes elétricas inteligentes que são interconectados pelas redes de média distância e redes locais podem ter restrições capacidade de processamento e também de velocidade de comunicação e, além disso, o número de dispositivos a serem interconectados pode ser muito elevado e os requisitos de comunicação também podem ter restrições de atraso e de garantia de banda. Portanto, estas características tornam os sistemas de comunicação desafiadores. O sistema de comunicações da rede elétrica inteligente envolve então diversas tecnologias de rede que vão das redes de longa distância (*Wide Area Network* - WAN), tais como, a rede Internet, o GSM (*Global System for Mobile Communications*), 3G e 4G; as redes metropolitanas, as redes locais (*Local Area*

[1] *Gateways* são elementos que interconectam duas redes com tecnologias diferentes.

Network - LAN) e as redes domiciliares (*Home Area Network* - HAN), tais como, WiMax, EPON (*Ethernet Passive Optical Network*), Bluetooth, ZigBee, IEEE 802.11/WiFi, Homeplug e as redes específicas de subestações de energia elétrica, tais como DNP3 e IEEE 61850.

O sistema de Controle Supervisório e Aquisição de Dados (*Supervisory Control And Data Acquisition* - SCADA) é um exemplo de sistema que opera sobre as redes de comunicação. Apesar de o SCADA ser um dos atores do domínio de operação da rede elétrica, ele opera remotamente os dispositivos de subestações do domínio de transmissão e distribuição através da rede de longo alcance. O SCADA controla e coleta dados dos IEDs e RTUs das subestações e linhas de transmissão. Um dos principais avanços no sistema elétrico inteligente é a coleta de medidas sincrofasoriais de tensão e corrente, além da frequência obtidas pelos equipamentos de medição fasorial (*Phasor Measurement Units* - PMUs). Assim, o sistema de monitoramento, proteção e controle de longa distância (*Wide-Area Monitoring, Protection, And Control* - WAMPAC) permitirá um controle fino do sistema elétrico e proverá maior confiabilidade, evitando apagões generalizados. Para realizar o WAMPAC, o domínio de transmissão instala diversas PMUs na rede elétrica para obter medidas geolocalizadas dos fasores de corrente, tensão e frequência com uma taxa de amostragem de até 120 Hz. Assim, as PMUs espalhadas na rede elétrica geram um grande volume de dados com restrições de atraso, que trafega pela rede de longo alcance até atores do domínio de operação. Outro componente fundamental nas redes elétricas inteligentes é a medição em tempo *quase* real do consumo de energia de todos os usuários da rede elétrica através de infraestruturas avançadas de medição (*Advanced Metering Infrastructure* - AMI). As AMIs formam redes de comunicação de médias distâncias e locais para a transferência dos dados de um grande número de medidores inteligentes de consumidores até agregadores de dados. Por conectarem a rede elétrica e os usuários finais, o domínio de distribuição é responsável por instalar as redes locais da AMI. A automação e controle dos diversos componentes exige uma diversidade de equipamentos que devem se comunicar, e onde cada comunicação possui requisitos variados. Dessa maneira, padrões e protocolos de comunicação foram propostos para assegurar a interoperabilidade, como o IEEE 1815 [IEEE1815, 2012] e o IEC 61850 [IEC61850, 2010].

3.2.1. Infraestrutura Avançada de Medição

A infraestrutura avançada de medição (AMI) é composta do *hardware* e do *software* necessário para criar uma rede de comunicação entre medidores inteligentes e provedores de serviços e, entre eles, as concessionárias [USDOE, 2008]. Com a AMI, os consumidores têm mais informações sobre a rede elétrica e preços da energia em tempo real, podendo tomar decisões baseadas nessas informações. As concessionárias e as distribuidoras de energia, por outro lado, podem coletar informações sobre o consumo e tomar decisões baseando-se no estado calculado em tempo real da rede elétrica. Além disso, novos modelos de negócios podem utilizar informações da distribuição de energia e oferecer serviços para os consumidores finais. Alguns exemplos são:

- acesso à informação de consumo e controle de utensílios em domicílios inteligentes (*smart houses*) através da Internet [Warmer et al., 2009], permitindo controle do

consumo em função dos preços de diferentes concessionárias;

- cálculo automático da conta de seus consumidores;
- detecção de falhas na rede elétrica;
- consumidores finais podem conectar placas fotovoltaicas ou carros elétricos em suas casas, fornecer energia para a rede de distribuição e ganhar benefícios, como por exemplo, abatimento do valor gerado na conta de energia.

Os medidores inteligentes permitem a tarifação remota e produzem informações mais detalhadas sobre a demanda de energia dos consumidores. Medidores inteligentes são capazes de monitorar o consumo de energia de cada consumidor e disponibilizar esses dados virtualmente em tempo real. Os medidores inteligentes oferecem comunicação entre concessionárias e consumidores e permitem a esses consumidores acompanhar o consumo de energia através de aplicações. As concessionárias podem acompanhar o consumo e detectar falhas ou roubos na distribuição de energia. Os *gateways* de consumidores são responsáveis pela comunicação com utensílios inteligentes dentro das instalações desses consumidores, conectando a rede de média ou longa distância com uma rede local. Esses *gateways* podem se comunicar através de redes domiciliares com eletrodomésticos inteligentes, ligando-os ou desligando-os, e assim controlar a carga, levar em conta a tarifação em função do horário de consumo, a geração de energia pelo consumidor ou ainda permitir que consumidores acompanhem o consumo através da Internet, por exemplo. O *gateway* pode inclusive ser integrado ao medidor inteligente.

As concessionárias são as responsáveis por conectar todos os elementos dessa rede de comunicação. Concessionárias contam com Sistemas de Gerenciamento de Dados de Medidores (MDMS - *Meter Data Management Systems*). Esses sistemas se comunicam com medidores inteligentes, *gateways* e provedores de serviços que surgem com o novo modelo de negócios de redes elétricas inteligentes. Algumas das funcionalidades que os Sistemas de Gerenciamento de Dados de Medidores trazem são:

- controle de demanda e resposta: concessionárias poderão indiretamente controlar a demanda por energia de seus consumidores através de incentivos financeiros. Medidores inteligentes podem realizar multitarifação visando maior controle sobre os picos de consumo de energia, que podem levar a "apagões" na rede elétrica;
- coleta e análise de medidas: medidores inteligentes podem realizar muitas medidas, monitorando em tempo real a demanda de energia. Essa informação é analisada e pode ser utilizada por concessionárias para fazer previsões mais precisas do consumo de energia, facilitando o planejamento da geração;
- monitoramento da qualidade de energia: com a AMI, medir a qualidade da energia sendo fornecida para seus clientes é mais fácil.

O principal desafio da AMI é conectar esses novos equipamentos inteligentes, sem tornar muito dispendiosa a infraestrutura física. As propostas visam adicionar poucos elementos de rede novos e aproveitar muita da infraestrutura de comunicação e elétrica

já existente. A comunicação entre os diversos elementos é feita através de diferentes tecnologias, tais como: redes sem-fio *WiFi*, *ZigBee* para os equipamentos dentro de redes domiciliares e locais e, para redes de longas distâncias, 3G, *Power Line Communications* (PLC) ou a infraestrutura atual da Internet [Ma et al., 2013, Khalifa et al., 2011].

3.2.2. *Supervisory Control And Data Acquisition* - SCADA

O sistema de Controle Supervisório e Aquisição de Dados (*Supervisory Control And Data Acquisition* - SCADA) foi projetado para ser usado em sistemas produtivos industriais, gerenciando e controlando a comunicação entre dispositivos de computação, sensores e atuadores, além de proporcionar o controle de processos industriais a partir de uma interface homem-máquina (*Human-Machine Interface* - HMI) [Gomez, 2002]. Subjacente ao sistema SCADA, há uma rede de comunicação que interconecta um conjunto de dispositivos de campo, tais como sensores e atuadores. Os dispositivos são monitorados e controlados através do sistema SCADA por um computador pessoal ou um controlador lógico programável (*Programmable Logic Controller* - PLC). Portanto, o sistema SCADA tem como objetivo principal o monitoramento e o controle de uma instalação industrial, normalmente dispersa em uma vasta área, a partir de um centro de controle que normalmente está localizado em uma instalação física remota. Os centros de controle concentram servidores de dados, estações de interface homem-máquina e outros servidores para auxiliar os operadores na gestão global da rede da instalação industrial [Igure et al., 2006].

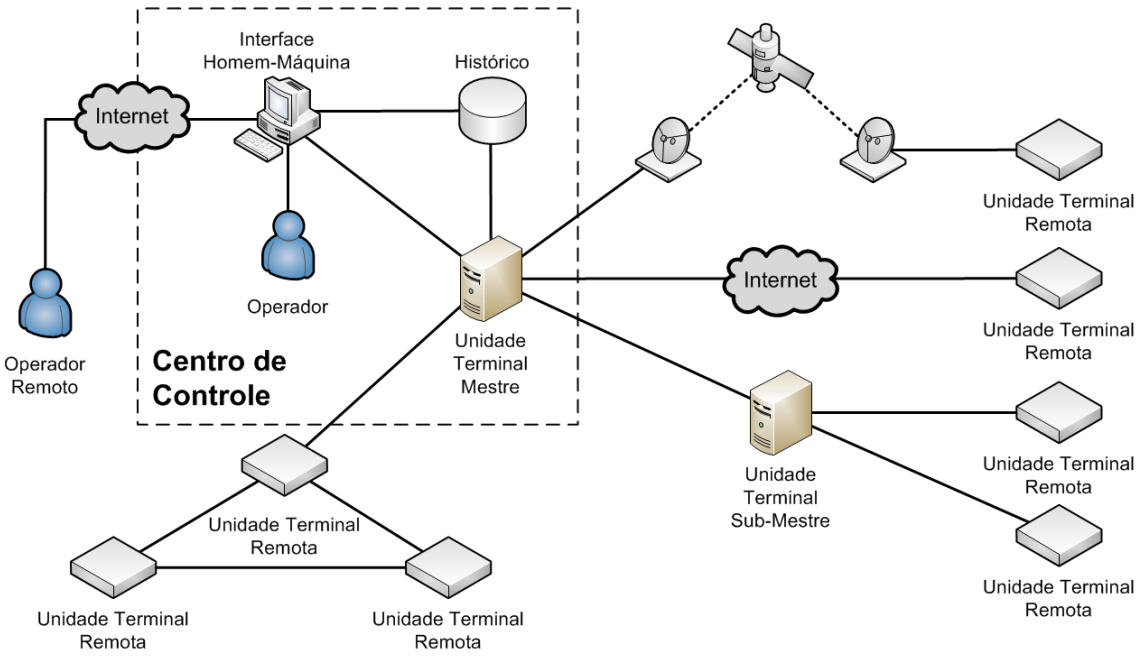


Figura 3.7. Arquitetura do sistema SCADA. As Unidades Terminais Remotas (RTUs) podem se conectar à Unidade Mestre através de diversas tecnologias de rede.

Sistemas SCADA apresentam uma arquitetura hierárquica, conforme mostrado na Figura 3.7. Um sistema SCADA consiste de dispositivos como a unidade terminal mestre (*Master Terminal Unit* - MTU), a interface homem máquina (HMI) e unidades terminais remotas (*Remote Terminal Units* - RTU) [Donghyun et al., 2010]. A unidade terminal

mestre é a raiz de todo o sistema SCADA, assim, a estrutura de um sistema SCADA geralmente se constitui de uma unidade terminal mestre se comunicando com unidades terminais sub-mestre (SUB-MTU) e com unidades terminais remotas. A unidade terminal remota é um dispositivo composto por sensores para a aquisição de dados, por um componente para realizar a comunicação e por outro componente responsável por executar os comandos vindos da MTU. Outro dispositivo que compõe a arquitetura dos sistemas SCADA é a interface homem máquina que permite que o operador interaja com o sistema. Na Figura 3.7, o centro de controle é a parte da rede do sistema SCADA que é considerada fisicamente segura, então, tudo o que se encontra fora desse perímetro de segurança deve ser considerado inseguro e, portanto, deve ser protegido contra adulteração (*tampering*) [Donghyun et al., 2009].

A topologia da rede nos sistemas SCADA tende a ser estática, ou seja, há poucas alterações na rede já estabelecida e, portanto, os caminhos para a comunicação entre nós são conhecidos *a priori*. Vale ressaltar que a comunicação entre as unidades terminais remotas e a unidade terminal mestre pode ocorrer através de diversas redes de acesso de tecnologias diferentes, tais como através da Internet, de rádio, de satélites ou de Ethernet. A interconexão entre duas redes de sistema SCADA, ou duas instalações monitoradas pelo sistema SCADA, ou ainda entre uma rede do sistema SCADA e a rede corporativa é realizada através de sistemas intermediários ou nós chamados *gateways*, conforme mostrado na Figura 3.8. Assim, um *gateway* interfaceia redes de sistema SCADA, próprias das instalações industriais, com redes baseadas em IP. O gateway faz a conversão de protocolos e realiza o cache de objetos de dados que são trocados entre as diferentes redes [Igure et al., 2006].

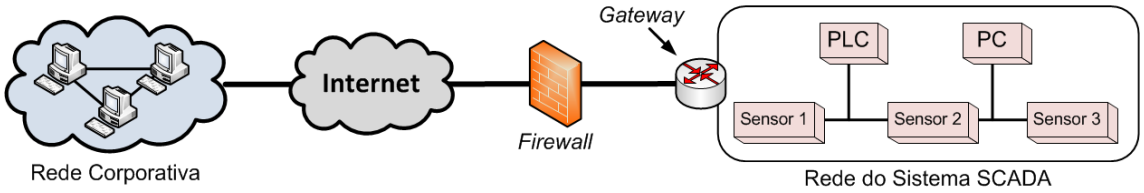


Figura 3.8. Interconexão da rede do sistema SCADA com a rede corporativa. A rede do sistema SCADA é protegida por um *Firewall* e a tradução de protocolos é feita pelo *gateway*.

A comunicação típica de uma rede do sistema SCADA segue o modelo mestre e escravo para a troca de mensagens de controle. Um dispositivo mestre, como um computador pessoal ou um controlador lógico programável, é aquele que controla a operação de outro dispositivo, chamado escravo. Um dispositivo escravo é geralmente um sensor simples ou atuador, que pode enviar mensagens para o dispositivo de controle e executa ações de controle enviadas por um dispositivo mestre. Outro tipo de mensagem comum em redes do sistema SCADA é a comunicação entre dispositivos pares e, para acomodar esse requisito, os protocolos usados na rede SCADA, como o PROFIBUS e DNP3, têm um modelo de comunicação híbrida que inclui um modelo de comunicação par-a-par (*peer-to-peer*) entre dois dispositivos mestres e outro modelo de comunicação cliente-servidor entre dispositivos mestre e escravos. Alguns dispositivos também podem se comunicar apenas através de mensagens de alarme e mensagens de estado. A rede do sistema SCADA baseia-se na ideia de que os dispositivos compartilham um barra-

mento comum e, portanto, o protocolo da rede do sistema SCADA provê diferenciação de serviço, atribuindo prioridades de mensagens para distinguir as mensagens críticas das não críticas [Igure et al., 2006].

O sistema SCADA é um dos elementos mais importantes de controle das redes elétricas atuais e possui papel de destaque nas redes elétricas inteligentes. O SCADA aplicado às redes elétricas consiste em monitorar e controlar sensores e atuadores geograficamente distribuídos em subestações e também coletar os dados gerados pelas subestações através de um nó remoto de controle. Nesse caso, os sensores nas subestações geram dados que são enviados à Unidade Terminal Remota (*Remote Terminal Unit* - RTU), que coleta os dados gerados e os encaminha para o centro de operações do SCADA. No centro de operações, os dados são disponibilizados aos operadores através de interfaces homem-máquina. O SCADA permite ainda aplicar algoritmos de detecção de dados falsos e análise de dados coletados na rede elétrica. As mensagens trocadas entre os sensores e atuadores e a RTU, assim como as mensagens trocadas entre RTU e centro de operações, não apresentam restrições fortes de atraso [IEEE1815, 2012, Dawson et al., 2006].

3.2.3. *Wide-Area Monitoring, Protection, And Control* – WAMPAC

O sistema de monitoramento, proteção e controle em longa distância (*Wide-Area Monitoring, Protection, And Control* - WAMPAC) é caracterizado pelo uso de informações sincrofasoriais globais do sistema elétrico, obtidas em tempo real, sincronizadas em relação ao Sistema de Posicionamento Global (*Global Positioning System* - GPS) e transferidas por um sistema de comunicação para uma localização remota. O principal objetivo do WAMPAC é aumentar a confiabilidade do sistema elétrico, já que monitora a dinâmica do sistema de transmissão e distribuição de energia, em tempo real, identificando as instabilidades no sistema e perturbações na rede elétrica e contendo a propagação destes distúrbios [Terzija et al., 2011]. A principal tecnologia do WAMPAC é a SMT (*Synchronized Mesurement Technology*), medição sincronizada de fase, tensão e corrente coletadas em diversos pontos de uma rede elétrica. Esta medição sincronizada permite inferir o estado global da rede em tempo real. A referência de tempo global obtida do GPS garante a sincronização das medidas. A Unidade de Medição Fasorial (*Phasor Measurement Unit* – PMU) é o elemento responsável por realizar as medições. Assim, os blocos fundamentais da SMT são as PMUs, os concentradores de dados e as redes de comunicação subjacentes a essas tecnologias [Zima et al., 2005].

As PMUs medem os valores dos fasores de tensão e corrente, assim como a frequência, e os associam à referência de tempo fornecida pelo GPS. Os dados são transmitidos pelas PMUs para concentradores de dados fasoriais (*Phasor Data Concentrators* - PDC) [Zima et al., 2005]. Os PDCs são nós responsáveis por coletar os dados das PMUs, agregá-los e transmiti-los para os centros de controle. Cada distribuidora de energia detém o controle de um determinado conjunto de concentradores de dados fasoriais. Contudo, a visão global da rede elétrica provida pelo WAMPAC depende de os PDCs das distribuidoras se comunicarem com um centro de controle responsável por agregar as medições das PMUs de todas as distribuidoras que atendem uma grande área. Uma proposta para coletar os dados das diferentes distribuidoras é criar um "super coletor de dados" que é responsável por coletar os dados dos coletores de dados de cada distribuidora em uma região [Terzija et al., 2011]. O super coletor de dados é capaz de atender diferentes proto-

colos de comunicação, para poder interoperar com diferentes coletores de dados, e é capaz de fornecer todos os dados coletados a um único coletor de dados de uma dada distribuidora de energia para que a distribuidora possa entender o estado da rede elétrica mesmo em uma região que esteja fora da sua área de controle. A conexão entre os elementos do WAMPAC pode ser através de diferentes meios físicos, como enlaces de micro-ondas, redes ópticas, conexões discadas, ou até mesmo através de redes privadas virtuais sobre a Internet. A Figura 3.9 mostra a arquitetura genérica do sistema WAMPAC.

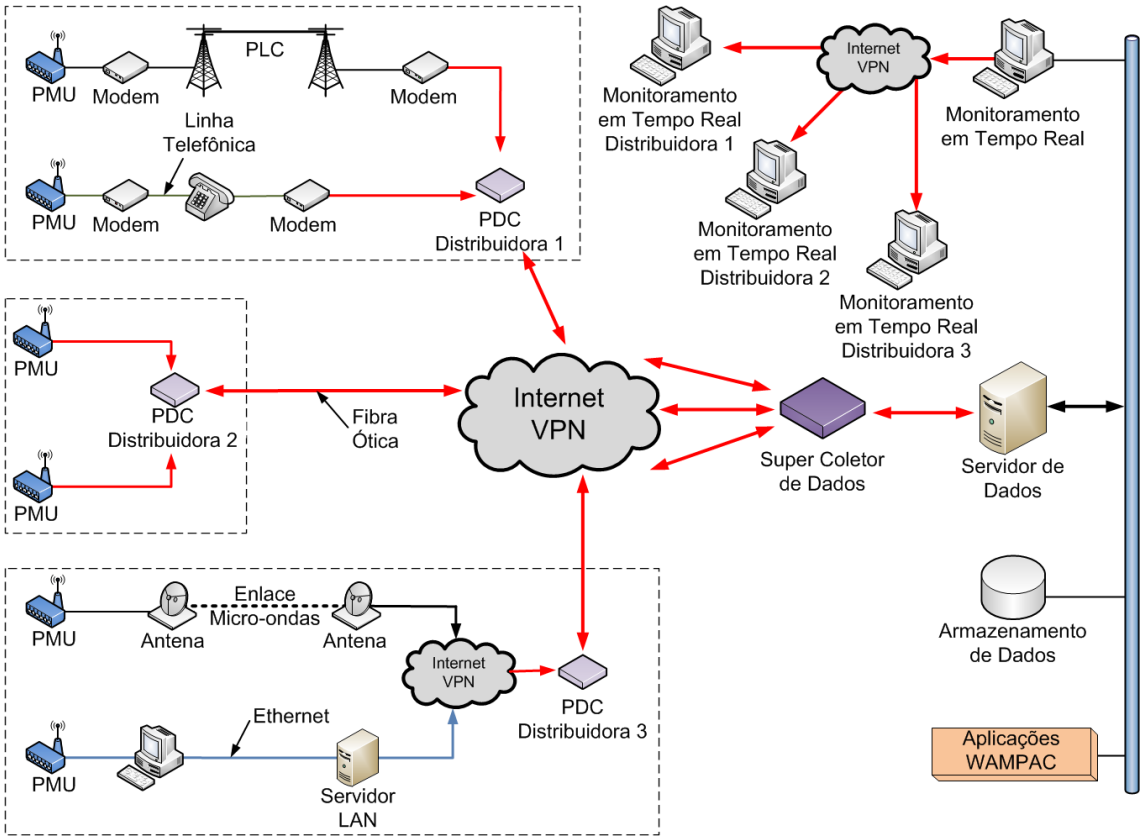


Figura 3.9. Arquitetura genérica do sistema WAMPAC. Cada distribuidora de energia tem a sua própria infraestrutura de coleta de dados das PMUs. Os dados coletados são enviados aos PDC de cada distribuidora e então enviados ao Servidor de Dados centralizado que tem a visão global do estado da rede elétrica.

Atualmente, o estado global do sistema elétrico é obtido pelo sistema SCADA e os Sistemas de Gerenciamento de Energia (*Energy Management System* - EMS) clássicos usados nas subestações de distribuição. Estes sistemas normalmente executam medições do estado da rede elétrica a uma frequência muito baixa, com períodos da ordem de segundos ou até minutos dependendo da aplicação. As medições coletadas não possuem uma referência de tempo comum e se restringem às áreas de controle regional de cada sistema. O conceito de WAMPAC estende o controle exercido por sistemas SCADA e EMS para uma área mais ampla, com coleta de dados em tempo real, associada a informações geográficas e a uma referência de tempo global sincronizado. Vale ressaltar que o posicionamento das PMUs na rede elétrica é definido como um problema de otimização da visibilidade e da estimação do estado do sistema elétrico [Morris et al., 2012, Terzija et al., 2011, Mao et al., 2005].

Os sistemas que implementam o WAMPAC têm como principais objetivos monitorar, proteger e controlar a rede elétrica em áreas maiores do que o controle regional exercido por sistemas SCADA ou EMS. Assim, a ideia central do controle exercido pelo WAMPAC é que uma falha ou perturbação em uma área possa ser identificada em tempo real e que medidas corretivas ou, em último caso, de contenção possam ter tomadas, evitando assim apagões em cascata. Dado que o estado da rede elétrica é estimado em tempo real com o WAMPAC, padrões de falhas são identificados na área em que se iniciam e não se propagam para o restante da rede. Outro objetivo do WAMPAC é permitir que as distribuidoras de energia elétrica executem aplicações com o conhecimento global da rede, tais como o registro dinâmico de eventos, a modelagem da rede em tempo real para adequar geração e demanda de energia e o monitoramento da diferença de ângulo de fase entre barramentos diferentes em tempo real [Terzija et al., 2011]. Contudo, as tecnologias que permitem a realização do WAMPAC ainda apresentam alguns desafios de segurança.

3.2.4. Protocolos de Comunicação das Redes Elétricas Inteligentes

A comunicação entre os sistemas de controle e os dispositivos de campo em uma rede elétrica inteligente segue protocolos e normas já definidos. Essa seção apresenta as duas principais normas, IEEE 1815 e IEC 61850.

Padrão IEEE 1815 - *Distributed Network Protocol Version 3*

O padrão IEEE 1815, também conhecido como *Distributed Network Protocol Version 3* (DNP3), define um conjunto de protocolos de comunicação usado em sistemas de automação de processos [IEEE1815, 2012]. Ele foi desenvolvido para a comunicação entre equipamentos de aquisição de dados e controle, sendo muito usado em sistemas SCADA. O método de acesso do DNP3 é determinístico e do tipo mestre-escravo, garantindo uma transferência confiável em meios físicos com banda estreita [Gao et al., 2013]. O protocolo define o formato das mensagens trocadas entre duas entidades, assim como a semântica dessas mensagens. Atualmente, o DNP3 é muito adotado pelas companhias elétricas para a automação de subestações, ou seja para as comunicações entre os centros de controle e os dispositivos elétricos inteligentes (IEDs) dentro de uma subestação.

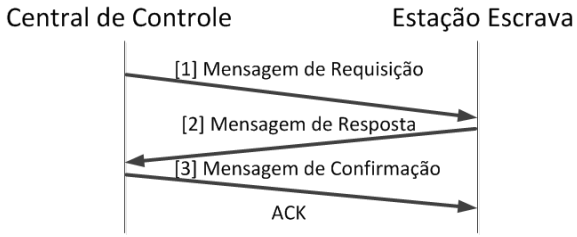


Figura 3.10. Diagrama de tempo de mensagens do DNP3: requisição da estação de controle, resposta da estação-escrava e confirmação de recebimento da estação de controle.

Existem dois tipos de comunicação no DNP3, a requisição-resposta e as respostas não-solicitadas. A comunicação orientada a requisição-resposta define mensagens de requisição de dados que são enviadas das estações de controle para as estações escravas e então as estações escravas respondem às requisições recebidas, como visto na Figura 3.10.

Já na comunicação orientada a respostas não-solicitadas, estações escravas enviam mensagens diretamente às suas estações de controle sem que haja uma requisição prévia. Esse modelo de comunicação permite que estações escravas enviem alarmes ou mensagens de erro para suas estações de controle, ilustrado pela Figura 3.11.

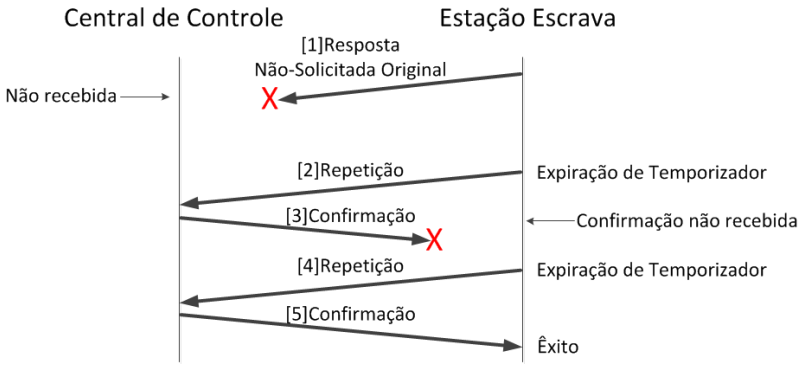


Figura 3.11. Diagrama de tempo de mensagens de resposta não-solicitada do DNP3 com exemplos de erros de transmissão: estação escrava envia resposta não-solicitada e a central de controle envia uma mensagem de confirmação do recebimento. A imagem mostra como cada entidade reage à perda de mensagens repetindo após estouro do temporizador.

No DNP3, o reconhecimento de recebimento de pacotes é feito por uma função da camada de aplicação, chamada de função de transporte (*transport function*). A norma IEEE 1815 também define uma interface para gerenciar a conexão utilizando a pilha de protocolos TCP/IP. Essa extensão permite que o DNP3 se conecte com a rede corporativa, usufrua de protocolos de comunicação suportados na Internet e tenha uma comunicação confiável fim-a-fim com o TCP.

Padrão IEC 61850

O padrão IEC 61850 é um conjunto de normas que definem uma arquitetura de referência para a automação de subestações de sistemas elétricos [IEC61850, 2010]. A comunicação entre elementos das subestações é mapeada em diversos protocolos que têm como objetivo garantir a interoperabilidade dos elementos dos Sistemas de Automação de Subestações (*Substation Automation Systems* – SAS). Os principais objetivos dos SAS são controle, supervisão, proteção e monitoramento dos equipamentos da rede.

A norma também prevê uma linguagem para configuração de subestações (*Substation Configuration Language* – SCL). O modelo de subestação é composto por três níveis (Figura 3.12): o nível de processo, composto por sensores e atuadores responsáveis por monitorar e controlar um determinado processo na subestação; o nível de vão, composto por IEDs responsáveis pelo controle entre processos e proteção da subestação; e o nível de estação, composto por computadores capazes de controlar e monitorar o funcionamento da subestação. Uma das características mais importantes do IEC 61850 é a diferenciação de exigências de atraso sobre os diferentes tipos de mensagens.

A norma define sete tipos de mensagens para troca de informações entre os dispositivos de uma subestação, conforme a Figura 3.13. As três mensagens mais importantes da norma IEC 61850 são:

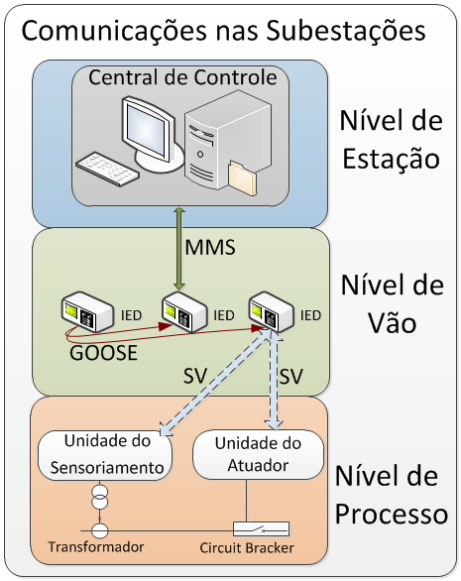


Figura 3.12. Modelo conceitual em três camadas descrito pelo IEC 61850 e troca de mensagens entre IEDs e Centrais de Controle.

- *Generic Substation Events* (GSE) e *Generic Object Oriented Substation Event* (GOOSE): mensagens para troca de dados e de controle com restrições de tempo máximo de entrega entre IEDs dentro da própria subestação. Essas mensagens são enviadas em *multicast* na camada de enlace;

- *Manufacturing Message Specification* (MMS): mensagens sem restrições de atraso trocadas através da pilha TCP/IP. Essas mensagens são trocadas por sistemas SCADA assincronamente com IEDs nas subestações;

- *Sampled Value* (SV): valores amostrados, como corrente e tensão do transformador, são enviados nas mensagens SV que possuem restrições de tempo, pois o conjunto de valores amostrados será usado no receptor para "reconstruir" o valor original da grandeza medida;

Interface de Serviço de Comunicação Abstrato

A norma IEC 61850 define o ASCI (*Abstract Service Communication Interface*) que é um método para descrever os dispositivos do sistema de energia. O ASCI define os serviços e as respostas a esses serviços, isto é, as funções e os parâmetros de cada serviço que possibilita que todos IEDs se comportem da mesma maneira da perspectiva da rede. Esse serviço abstrato permite o isolamento dos dados, para que eles possam ser mapeados por outros protocolos de comunicações ou possamm ser inseridas futuras tecnologias como serviços web, etc. O ASCI foi projetado considerando as qualidades definidas no capítulo de arquitetura da NIST [NIST7628, 2010a].

Um importante serviço do ASCI é chamado de auto-descrição. Nesse serviço, um dispositivo pode dizer ao seu mestre que tipo de dado vai ser transmitido e, com essa informação, o mestre pode se configurar para receber distintos tipos de informação

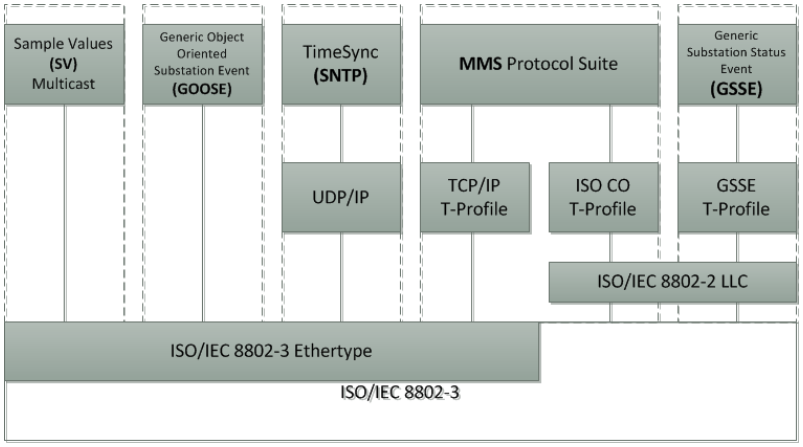


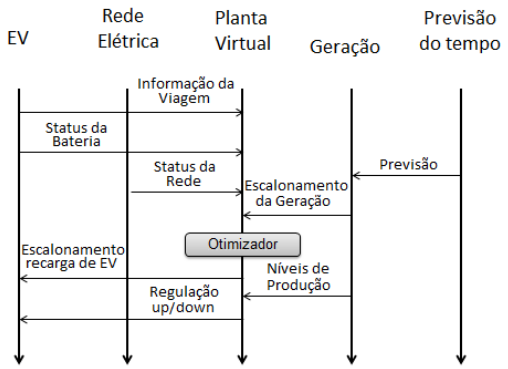
Figura 3.13. Os diferentes tipos de mensagens no IEC 61850, e as camadas utilizadas para a comunicação de esses mensagens.

pelos diferentes IEDs, sem a necessidade de uma configuração manual. Consequentemente, comparado com outros protocolos [Gunther, 2011], existe uma economia de 75% do tempo de configuração além da redução de erros, permitindo que a configuração de um sistema seja *plug-and-play*.

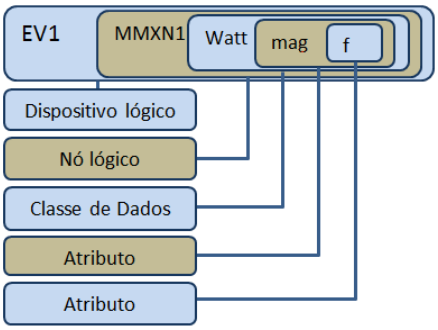
Veículos Elétricos: a emenda IEC 61850-7-420 e o protocolo SIP

Uma proposta para resolver requisitos de escalabilidade e promover suporte à mobilidade para o abastecimento dos veículos elétricos é combinação dos protocolos SIP (*Session Initiation Protocol*) e IEC 61850-7-420 [Bernhard et al., 2010]. A entidade do agregador surge com o nome de Planta Virtual de Energia de Veículo Elétrico (EV-VPP - *Electric Vehicle Virtual Power Plant*) e tem como funções a comunicação com a geração para o fornecimento de energia suficiente ao veículo para a próxima viagem, a minimização do custo de abastecimento observando as restrições e picos de energia da rede. A Planta Virtual de energia atua como um mediador entre a geração de energia e os consumidores, em particular os veículos elétricos. Baseando-se em predições de viagens anteriores dos veículos, o comportamento de carga pode ser antecipado, otimizado e alinhado com as previsões de flutuação de produção de energia, mostrado na Figura 3.14(a).

É sugerida como um módulo-núcleo da Planta Virtual, a figura do Otimizador. Como mostra a figura abaixo o Otimizador recebe informações de previsão de viagem e o status de carga da bateria de cada veículo elétrico. Com base nessas informações, o otimizador calcula o volume de carga necessária a cada veículo para o percurso desejado. Torna-se intuitivo que a tarefa a ser executada pelo Otimizador seja elaborar e resolver um problema de otimização, tendo como insumos de entrada: informações da distância de percurso, status da bateria dos veículos, as restrições da rede elétrica (balanceamento de produção de energia e demanda de energia), o escalonamento da produção de energia, que por sua vez irá depender das condições do tempo, etc. Como exemplo de objetivo pode-se citar a minimização do custo total de energia entregue aos veículos elétricos ou ainda a tentativa de equalizar o total de energia entregue na recarga dos veículos com a energia gerada.



(a) Otimizador da recarga de veículos elétricos.



(b) Exemplo do caminho de um objeto no padrão IEC 61850.

Figura 3.14. Protocolo de recarga e otimização da recarga de veículos elétricos. Os veículos são representados como objetos do padrão IEC 61850.

Os padrões propostos de comunicação entre veículos e a Planta Virtual possuem forte semelhança com os já estabelecidos protocolos de voz sobre IP e mensagem instantânea. Nos serviços de voz sobre IP, o cliente se registra e estabelece uma sessão com outro(s) usuário(s). Em paralelo aos dados de voz, é transmitida a sinalização adicional para a manutenção da comunicação. Um padrão típico para um procedimento de carga de veículo elétrico consiste em:

1. O veículo se registra com a Planta Virtual quando se conecta com a unidade de carregamento;
2. O veículo elétrico envia informações sobre a viagem pretendida e seu status de bateria;
3. O veículo recebe seu plano de carga para a próxima operação de carga;
4. O veículo fica alcançável para a planta virtual e vice-versa permitindo atualizações no plano de carga e sendo também capaz de receber mensagens para participação no balanceamento da rede de energia elétrica. É interessante notar que ocorre até então uma comunicação de natureza intermitente;
5. O veículo se desconecta, as informações e medidas são enviadas para a Planta Virtual antes do de-registro da Planta Virtual.

O SIP (*Session Initiation Protocol*) é um protocolo bastante usado na sinalização de sessões de voz sobre IP (VoIP - *Voice over* IP) e mensagens instantâneas (IM – *Instant Messaging*) [Bernhard et al., 2010]. O SIP é adequado para o estabelecimento de uma sessão entre a unidade de carregamento e a Planta Virtual. Além disso, outras motivações para o uso do SIP são o suporte à mobilidade, confiabilidade e escalabilidade, uma vez que uma quantidade grande de veículos irá ser gerenciada. Os dados de registro e a sinalização necessária para o estabelecimento da sessão são realizados em um canal de comunicação fora da banda principal. A troca de dados, incluindo as informações sobre

os planos de abastecimento, estado da bateria e dados de viagem, percurso, são realizados em um canal separado estabelecido via SIP.

O modelo adotado para a transferência de dados é o protocolo IEC 61850. Ele foi originalmente pensado para promover a interoperabilidade entre diferentes dispositivos em subestações. O padrão define dispositivos lógicos que são representações virtuais de um dispositivo físico dentro do ambiente da subestação no caso. Um dispositivo lógico contém um ou mais nós lógicos representando vários componentes pertencentes ao dispositivo físico. Nesse modelo um servidor tem a função de estabelecer uma comunicação a um dispositivo na rede elétrica, estabelecendo um endereço IP e uma porta. Um servidor contém um ou mais dispositivos lógicos, por exemplo, uma planta eólica, solar ou carros elétricos, representando uma visão lógica da rede ou de parte dela. Por sua vez, cada dispositivo lógico contém certo número de nós lógicos que descreve aspectos do dispositivo. Nota-se que este padrão, mais especificamente a emenda IEC 61850-7-420 que engloba as fontes de energia distribuídas, usa um modelo hierárquico, em árvore, para a descrição de modelos de energia. No exemplo da Figura 3.14(b), o dispositivo lógico `EV1` (veículo elétrico 1) engloba o nó lógico `MMXN1`. A parte `MMXN` se refere ao tipo do nó e deve conter todas as classes do nó lógico em questão. As classes de dados representam informações significativas dos nós lógicos. Um atributo pode tanto ser um tipo como FLOAT32, INT24 ou BOOLEAN.

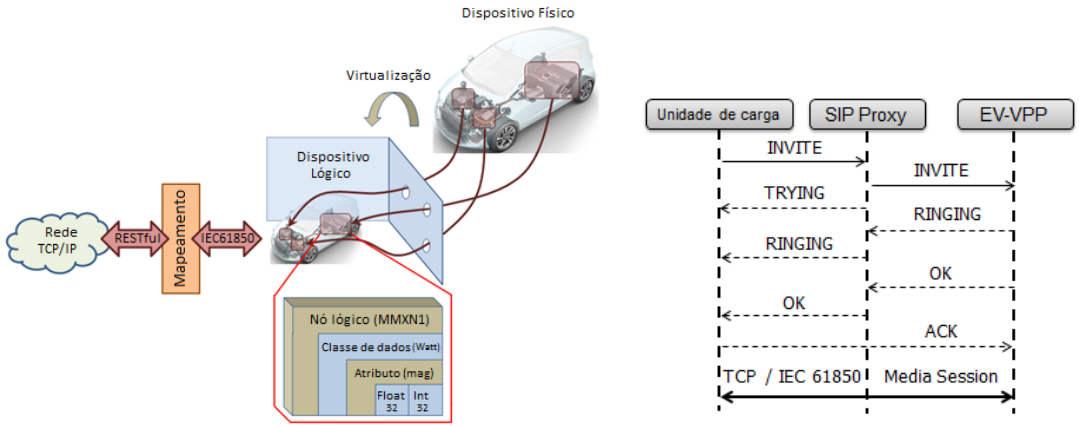
Nesse modelo hierárquico de dados qualquer objeto ou dado pode ser diretamente acessado pelo seu caminho, devido ao fato de que a estrutura de dados se dá em árvore, como um caminho de sistema de arquivos ou uma URL. Assim para acessar o atributo `f` do veículo elétrico `EV1` a referência a esse objeto pode ser descrita por:

```
EV1/MMXN1.Watt.mag.f
```

O caminho acima pode ser mapeado em uma URL: `http://hostname/device/node/class/attribute`. Incuída na especificação IEC 61850, esse método chama-se Abstract Communication Service Interface (ACSI), de acordo com a Figura 3.15(a) pode ser mapeado em REST. O REST tem como atrativo expor recursos no serviço RESTful usando URL únicas. Os serviços RESTful utiliza os métodos HTTP (GET, POST, PUT, DELETE...) para leitura, criação, atualização e destruição dos recursos, respectivamente. A Figura 3.15(a) mostra o mapeamento.

Quando um veículo elétrico se conecta a um ponto de carga, uma vez aberta a sessão entre o agregador e o veículo, os dados de carga (estado de carga, limites de potência e capacidade da bateria) podem ser trocados via protocolo IEC 61850. O procedimento de estabelecimento de uma sessão com a EV-VPP, como mostra a Figura 3.15(b), se inicia no envio de uma mensagem INVITE. Uma vez que a mensagem foi aceita, sinalizado por parte da planta virtual por meio da mensagem OK, a unidade de carga, cumprindo o critério da autenticação de três vias, envia uma mensagem ACK e em seguida estabelece-se a comunicação por meio do protocolo IEC 61850, possibilitando a carga no veículo. A sessão permanece ativa durante todo o período de carregamento.

Qualquer renegociação que for necessária para qualquer informação de alteração no escalonamento do abastecimento, por exemplo, se a tarifa se tornou mais cara, ou se o plano da próxima viagem do veículo foi alterado é enviado uma mensagem de re-INVITE para que possam ser renegociados os novos valores. Para finalizar o procedimento de



(a) Mapeamento entre URL e o atributo do veículo elétrico. (b) Mensagens SIP para o estabelecimento da sessão de carregamento.

Figura 3.15. O objeto do veículo elétrico segundo o padrão IEC 61850 e a troca de mensagens SIP para o estabelecimento da sessão de recarga. Após o estabelecimento da sessão, o protcolo IEC 61850 é usado para controlar o fornecimento de carga.

carga, uma vez que se chegou a quantidade contratada ou até a plena carga, é enviada uma mensagem BYE. Vale a pena ressaltar que a mensagem de BYE pode ser enviada por ambas as partes. Assim são trocadas as informações de energia transferida, valor da conta, tempo de abastecimento, dentre outras. Uma vez recebida a mensagem de reconhecimento, desconecta-se o plug e segue-se a viagem, como ilustrado pela Figura 3.16.

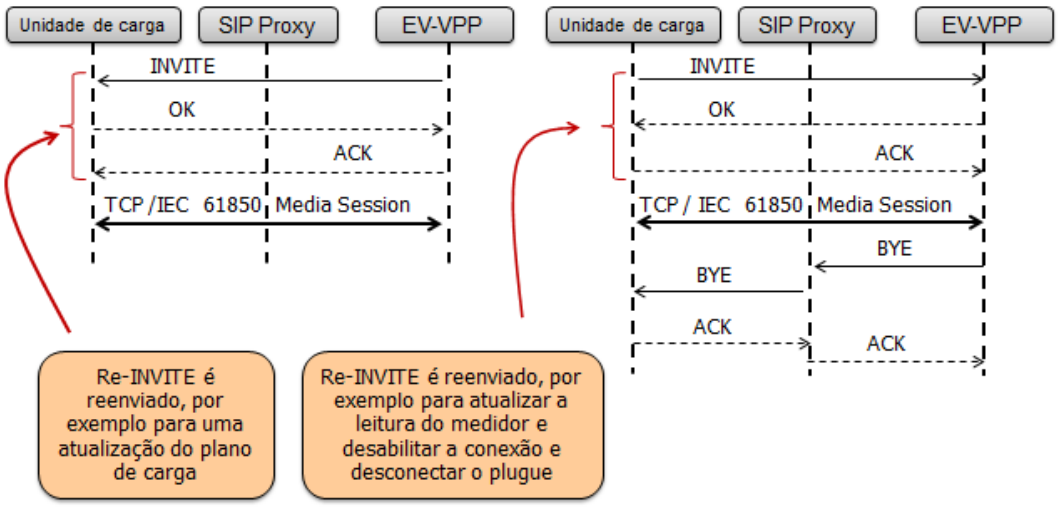


Figura 3.16. Mudança nas condições de contratação da carga na rede elétrica implicam no envio de uma mensagem de re-INVITE para o restabelecimento da sessão SIP.

O proprietário do veículo é redirecionado ao seu agregador de origem e isso permite que o SIP se encarregue adequadamente da questão da mobilidade, uma vez que

o proprietário pode se encontrar em um ponto de recarga longínquo e fora da área de operação da sua concessionária de energia. Uma vez estabelecida a sessão, o protocolo IEC 61850 se encarrega efetivamente da troca de dados.

Compração entre IEC 61850 e DNP3

A comparação entre o DNP3 e o IEC 61850 não é trivial. O DNP3 é um padrão bem antigo e já bem estabelecido como um conjunto de protocolos de comunicação usado em sistemas de automação de processos, em especial, nos sistemas de automação elétricos e de distribuição de água. O IEC 61850 é um padrão bem amis recente e objetiva a automação de subestações elétricas. O padrão IEC 61850 também compreende modelos abstratos de dados que podem ser mapeados em protocolos de comunicação, tais como MMS, GOOSE e SMV. Ambos os conjuntos de protocolos têm como motivador a padronização da comunicação entre os sistemas de controles e sensores e atuadores.

Os protocolos do DNP3 foram inicialmente projetados para serem usados em enlaces seriais com comunicação mestre-escrevo, nos quais O canal de comunicação possuia banda estreita e, portanto, os requisitos eram para mecanismos que melhor aproveitassem a banda do canal. Os protocolos foram projetados considerando-se também que o meio de comunicação está sujeito a interferências e distorções. Para prover a confiabilidade necessária mesmo em ambientes adversos e sujeitos a degradação pelo tempo, o protocolo DNP3 se serve de bits de paridade (*Cyclic Redundancy Check* – CRC) para detectar erros nas mensagens. Por sua vez, os protocolos do padrão IEC 61850 foram projetados para cenários em que as subestações automatizadas se comunicam através de redes Ethernet com banda larga de transmissão de dados. Os protocolos do padrão IEC 61850 se baseiam nas pilhas de protocolos do modelo *Open System Interconnection* (OSI) e da Internet. Assim, os protocolos do DNP3 compreendem protocolos da camada física, do enlace serial, e de aplicação, além de uma pseudo-camada de transporte. Os protocolos do IEC 61850 executam sobre a camada de enlace provida pelo protocolo Ethernet. Quando executado em perfis cliente-servidor, os protocolos do IEC 61850 executam a camada de sessão sobre a pilha TCP/IP.

Outra diferença importante entre os protocolos do DNP3 e do IEC 61850 é que enquanto o DNP3 provê um uso eficiente e otimizado do envio de dados na rede, já que só envia dados dos sensores para o centro de controle quando há uma alteração significativa do estado, os protocolos do IEC 61850 baseiam a organização dos dados em capacidades de representar dados abstratos e, portanto, não é tão eficiente no uso do meio quanto o DNP3 já que não define *a priori* os dados a serem enviados. Assim, o DNP3 consiste na especificação do protocolo que definie os bytes enviados e recebidos, os formatos dos dados e o tempo de cada mensagem, já o IEC 61850 define a arquitetura e os requisitos para a automação de uma subestação, apresenta definições abstratas de objetos e serviços que devem ser usadas como base para implementação de objetos e serviços reais e, ainda, define o mapeamento dos objetos abstratos para protocolos específicos como MMS e Ethernet.

Comparando-se os perfis de uso dos protocolos, ambos permitem comunicação direta, ou seja, orientada à comunicação entre duas entidades, e comunicação em difusão, quando uma entidade se comunica com várias ao mesmo tempo. Para a comunicação direta, a pilha de protocolo DNP3 usa o esquema mestre-escravo para fazer a comunicação

par-a-par. A comunicação par-a-par no DNP3 pode ser realizada sobre a pilha TCP/IP, em que uma entidade abre uma conexão TCP diretamente com outra entidade. No entanto, sobre a pilha TCP/IP, o DNP3 executa a pilha de protocolos seriais, ou seja, a camada de dados e de aplicação que o DNP3 define. O padrão IEC 61850 realiza a comunicação direta através de mensagens MMS e, para tanto, implementa as camadas de apresentação, sessão e aplicação sobre a pilha TCP/IP. Vale ressaltar que ao usar o DNP3 sobre a pilha TCP/IP, não há a necessidade de usar as mensagens de confirmação de recepção de dados, previstas no protocolo, pois o TCP já provê o serviço de comunicação confiável fim-a-fim. O MMS não implementa a confirmação do recebimento de dados, pois é previsto para ser usado sobre a pilha TCP/IP.

Quanto ao perfil de comunicação em difusão, a pilha de protocolos DNP3 pode ser usada diretamente sobre um enlace serial, como previsto no protocolo inicialmente, ou pode ser encapsulado em um pacote UDP sobre IP. Já o padrão IEC 61850 prevê dois tipos de mensagens de múltiplos destinatários, as mensagens GOOSE e as GSSE. Ambas são enviadas diretamente sobre o Ethernet que já provê meios para envio de mensagens em difusão, endereços Ethernet *multicast* e *broadcast*. Destaca-se que as mensagens GOOSE e GSSE são especificadas para serem entregues em uma rede local em um tempo máximo de 4 ms. Contudo, o protocolo Ethernet não garante o tempo máximo de entrega das mensagens.

Tendo em consideração os serviços providos pelos protocolos IEC 61850 e DNP3, verifica-se que ambos provêm primitivas de serviços para monitoração e controle suficientes para diversas aplicações. Contudo, o IEC 61850 destaca-se por oferecer primitivas de descoberta de novos objetos e primitivas de autoconfiguração. Essas duas primitivas permitem que os protocolos do IEC 61850 apresentem menor tempo para a configuração de um novo equipamento em relação ao DNP3. Contudo, esse benefício é acompanhado de um maior custo dos equipamentos que usam os protocolos IEC 61850, com lógica mais complexa, em relação aos que usam o DNP3, mais simples.

Na descrição dos modelos de objetos suportados tanto pelo DNP3 quanto pelo IEC 61850, guardada as devidas proporções, ambos permitem representar dados discretos, digitais, analógicos, contadores e pontos flutuantes. Ambos ainda permitem marcar mensagens com etiquetas de qualidade e envio de mensagens com marcação de tempo.

Tabela 3.3. IEEE 1815-DNP3 e IEC 61850: Comparação de Protocolos de Comunicação de Subestações.

	IEEE P1815-DNP3	IEC 61850
Comandos	Sem *timestamp*	Sim
Medidas	Sim	Sim
Auditoria de Falhas	Não	Sim
Interoperabilidade	Não	Sim
Transmissão de Dados	Mestre/Escravo	Orientado a eventos
Comunicação Subestação e Central de controle	Sim	Sim

No geral, o protocolo DNP3 foi proposto para agir como meio de coleta de

informações do sistema SCADA. Contudo, o padrão IEC 61850 apresenta-se como uma opção de substituição ao DNP3, com a principal vantagem de permitir transportar objetos de dados mais complexos e menos estruturados do que os do DNP3. A adoção do IEC 61850, no entanto, está condicionada à evolução da banda disponível para a comunicação entre subestações, já que o uso do enlace é menos eficiente do que o DNP3. A tabela 3.3 apresenta um resumo da comparação entre os protocolos.

3.3. Segurança em Redes Elétricas Inteligentes

As redes elétricas inteligentes oferecerão maior confiabilidade e qualidade através de um controle mais robusto e automatizado devido a um sistema avançado de comunicação entre os diferentes atores do sistema elétrico, inclusive com a participação dos consumidores finais. Assim, os sistemas de comunicação que interconectam os diferentes atores são sofisticados e requerem um maior grau de conectividade. Nesse novo cenário, tanto os consumidores, com os seus medidores inteligentes e as suas redes domiciliares, quanto as concessionárias responsáveis pelo sistema elétrico e outros provedores de serviços estão suscetíveis a ataques, assim como também podem ser fontes de ataques intencionais, ou não, ao sistema de comunicação. A introdução de uma infraestrutura de comunicação mais conectada no controle da rede elétrica expõe a rede de controle, que é crítica em segurança, a uma miríade de problemas de segurança já conhecidos da Internet [Igure et al., 2006, Wenye e Zhuo, 2013]. Portanto, a segurança das redes de comunicação depende de mecanismos de proteção contra ataques à infraestrutura de comunicação. Os apagões que hoje são acidentais e causados por falhas materiais e humanana, podem passar a ser "intencionais"' e provocados remotamente pou um usuário que adquiriu acesso è rede de controle. Surge a possibilidade dos ataques cibernéticos.

Os ataques podem ser classificados em dois tipos de comportamentos: egoísta e malicioso. Consumidores com comportamento egoístas são consumidores legítimos que tentam obter alguma vantagem em relação a recursos de rede através da violação dos protocolos de comunicação. Os consumidores maliciosos adquirem, modificam, interferem ou interrompem ilegalmente o fluxo de informações na rede. O comportamento malicioso é mais crítico que o comportamento egoísta, pois os dispositivos eletrônicos inteligentes (*Inteligent Eletronic Device* – IED) são usados para monitorar e controlar serviços em que a confiabilidade e integridade dos dados é essencial. Portanto, atacantes maliciosos podem induzir danos catastróficos ao fornecimento de energia e gerar apagões generalizados com inserção de dados falsos de controle na rede de comunicação da rede elétrica inteligente. As ameaças nesse novo modelo de rede elétrica podem ser:

- atacantes individuais que visam reduzir o valor de suas contas de energia, interromper ou prejudicar outros consumidores, obter lucros com venda de *softwares* maliciosos, entre outros;

- grupos criminosos com estrutura capaz de gerar grandes prejuízos, de oferecer serviços ilegais, etc;

- desenvolvedores de *spyware/malware* que podem contaminar os equipamentos e bisbilhotar as características dos consumidores;

- *phisher* que conseguiriam senhas e informações dos consumidores;
- operadores de *bots* que podem causar apagões (*blackout*) enviando inúmeras informações falsas de consumo, uma vez que os equipamentos inteligentes podem ser corrompidos e ficarem sob comando de um operador;
- espiões industriais que podem obter informações valiosas de concorrentes;
- sabotadores que podem causar danos ao sistema uma vez que são consumidores legítimos;
- terroristas que podem provocar apagões (*blackout*) e danos materiais;
- agentes de serviços de inteligência estrangeiros que podem identificar pontos críticos do sistema elétrico de um país.

Os principais pontos a serem abordados são as estratégias de segurança baseadas em ações de prevenção, detecção, resposta e regeneração. Métodos seguros de comunicação, verificação de integridade, autenticação e autorização vão ser abordados e discutidos para garantir a confiabilidade e a robustez ao serviço de energia elétrica.

3.3.1. Requisitos de Segurança em Redes Elétricas Inteligentes

Os principais requisitos de segurança para a rede de comunicação das redes elétricas inteligentes são a disponibilidade, a integridade, a privacidade, a autenticação, a autorização, a auditoria, o não repúdio e a confiança entre os componentes da rede [Mo et al., 2012, Wenye e Zhuo, 2013] que são definidos a seguir.

Disponibilidade refere-se a assegurar que consumidores ou sistemas não possam negar o acesso aos serviços de rede aos consumidores e sistemas legítimos. A disponibilidade aplica-se aos sistemas de comunicação internos a uma planta de geração, transmissão e distribuição de energia, aos sistemas de monitoramento e controle, assim como aos sistemas de comunicação entre os sistemas de controle internos e outros elementos externos. Ataques contra disponibilidade são chamado de Ataques de Negação de Serviço (*Denial of Service* - DoS) e têm como objetivo interferir, retardar ou impedir a comunicação entre elementos da rede elétrica inteligente [Wenye e Zhuo, 2013, Mo et al., 2012].

Diferentemente de uma rede de comunicação convencional, muitas mensagens da rede de comunicação da rede elétrica inteligente são críticas quanto a garantia que deve ser entregue de forma íntegra e também em relação ao tempo máximo de entrega. Assim, versões mais fracas de ataques de negação de serviço que apenas retardem intencionalmente a transferência de uma mensagem crítica em atraso, para violar a sua exigência de tempo, podem ser suficientes para gerar impactos catastróficos para as infraestruturas de energia.

Ataques de negação de serviço podem ser realizados em todas as camadas da rede de comunicação. Na camada física, o ataque de negação de serviço simples e eficaz é o ataque de interferência no canal (*channel jamming*). Na camada de enlace o atacante pode modificar deliberadamente, não respeitando, os parâmetros do protocolo de acesso ao meio da camada de enlace do seu dispositivo para ter melhores condições de acesso

ao meio físico, ao custo da degradação do desempenho dos outros nós que compartilham o meio. Outro possível ataque é a personificação (*spoofing*) de outro nó legítimo na camada de enlace, aproveitando a não proteção dos campos de endereço em um quadro sa sub-camada *Medium Access Control* (MAC) para enviar informações falsas para outros dispositivos. Um possível exemplo de DoS é um nó malicioso transmitir pacotes ARP (*Address Resolution Protocol*) forjados para desligar todos os dispositivos eletrônicos inteligentes (IEDs) conectados a uma subestação. Na camada de rede e de transporte, é comum o uso da pilha de protocolos de comunicação TCP/IP da Internet [Gomez, 2002, Igure et al., 2006]. Ataques de negação de serviço nas camadas TCP/IP podem degradar o desempenho da comunicação fim-a-fim [Moreira et al., 2012], tal como inundações de tráfego a partir de fontes distribuídas [Laufer et al., 2011, Moreira et al., 2010].

Na camada de aplicação os ataques de negação de serviço têm por objetivo exaurir os recursos de um computador, seja de processamento, de memória ou de banda passante da rede. Assim, uma forma de atacar um dispositivo é inundá-lo de requisições computacionalmente custosas. Como em redes elétricas inteligentes alguns dispositivos apresentam recursos computacionais muito limitados, esses dispositivos são potenciais vítimas de DoS.

Autenticação refere-se à determinação da identidade real de um participante em um sistema de comunicação e o consequente mapeamento desta identidade para uma representação interna ao sistema através da qual o consumidor é reconhecido. Autenticação é fundamental e outros requisitos de segurança dependem da autenticação como, por exemplo, a autorização, para distinguir os consumidores legítimos dos ilegítimos com base na autenticação.

Integridade refere-se a identificar que modificações, injeção, repetição e atraso proposital de mensagens feitas por consumidores ou sistemas não autorizados. Os ataques à integridade podem objetivar tanto informações dos consumidores, como a informação do preço pago pela energia ou a quantidade de energia consumida, assim como, também, pode objetivar corromper informações de operação da rede, como a informação de coleta de dados de sensores na rede elétrica. Um exemplo de ataque à integridade da rede elétrica inteligente é a injeção de mensagens com preços negativos na rede de comunicação por um atacante. Esse ataque pode causar um pico de utilização de eletricidade como inúmeros dispositivos ligando simultaneamente para aproveitar o preço baixo. Outro ponto importante é de se garantir a integridade do *software* dos dispositivos eletrônicos inteligentes (IEDs), pois um *software* malicioso pode controlar todos os dispositivos e componentes da rede elétrica, contituindo os "bots elétricos".

Privacidade ou confidencialidade refere-se a garantir que um atacante não é capaz de obter informações não autorizadas a partir da rede de comunicação. Ataques à privacidade têm o objetivo principal de espionar canais de comunicação das redes elétricas para a aquisição de informações desejadas, como o número da conta de um cliente, o seu consumo de energia e o tipo de tráfego. Exemplos de ataques incluem escuta de canal (*eavesdropping*) e analisadores de tráfego. Esses dois ataques citados apresentam um efeito negligenciável sobre a funcionalidade de redes de comunicação das redes elétricas, mas as informações coletadas dos consumidores podem impactar o consumidor, já que as informações de consumo de energia fornecem padrões de uso de aparelhos individuais,

que podem revelar as atividades pessoais e o comportamento dos consumidores de energia através do monitoramento não intrusivo dessas medidas.

Autorização ou controle de acesso refere-se a preservar o acesso do sistema de comunicação somente para pessoas ou sistemas que sejam legítimos, impedindo o acesso das demais pessoas ou sistemas que não tenham permissão para acessá-lo. A autorização refere-se aos mecanismos que distinguem entre consumidores legítimos e ilegítimos. Evidentemente, que as companhias que tem o acesso ao controle do sistema elétrico terão definir uma política bem determinada e eficaz de controle de acesso.

Auditoria refere-se à capacidade de reconstruir o histórico completo do comportamento do sistema a partir de registros de todas as ações relevantes executadas. O objetivo da auditoria é descobrir as razões para o mau funcionamento de um sistema após a ocorrência de um determinado fato e estabelecer as consequências desse fato.

Não repúdio refere-se ao fato de prover provas irrefutáveis para que o autor de uma ação não negue ter realizado a ação, mesmo que este não esteja cooperando. Esse requisito é importante em regulamentação e a sua violação tipicamente implica em consequências legais ou comerciais.

Confiança é definida como uma crença de uma entidade sobre a outra parte, seja uma pessoa, uma organização ou de um dispositivo, com base num conjunto de regras bem estabelecidas e as suas expectativas de comportamento [Velloso et al., 2010].

3.3.2. Segurança da Infraestrutura Avançada de Medição

No Brasil, um dos problemas mais recorrentes na distribuição de energia é o furto. A Light estima que em 2010 mais de 5300 GWh foram perdidos, representando mais de um bilhão de reais [Light, 2010]. Esses ataques são atualmente feitos à infraestrutura física da distribuição elétrica. A adoção de redes elétricas inteligentes pode facilitar essas atividades uma vez que os ataques podem ser feitos remotamente e com outras motivações além do furto de energia [McDaniel e McLaughlin, 2009]. Esses ataques podem ser motivados por indivíduos querendo diminuir a sua conta de luz, por criminosos visando lucrar com a venda de energia roubada, por atacantes visando prejudicar ou roubar dados sobre os hábitos de consumidores ou mesmo por ataques ao sistema elétrico de um país [McDaniel e McLaughlin, 2009, Cleveland, 2008].

As principais questões e requisitos de segurança para a Infraestrutura Avançada de Medição (*Advanced Metering Infrastructure* - AMI) são a confidencialidade, a autenticidade, a integridade, a disponibilidade e o não repúdio [Cleveland, 2008]. A AMI conecta medidores e *gateways* de redes domiciliares a uma rede de comunicação externa. Nesse cenário, informações pessoais podem ser roubadas, afetando seriamente a privacidade dos consumidores. A autenticidade das entidades nessa rede de comunicação é fundamental, pois o dado só tem valor para a infraestrutura de medição se a sua fonte for autêntica, por exemplo, um medidor inteligente legítimo. A integridade dos dados também é mandatória e qualquer alteração nos dados devem ser detectadas. A disponibilidade da medição deve ser garantida, ou seja, os dados devem estar acessíveis pelas entidades autorizadas no momento em que elas solicitarem. Uma entidade não pode negar que pediu um dado ou realizou uma medida para garantir o não repúdio. McLaughlin

et al. apresentam modelos de ataques à nova infraestrutura de medição do consumo de energia que são [McLaughlin et al., 2010]:

- falsificação de medidores através do roubo da chave criptográfica que lhes correspondem. Esse tipo de ataque pode ser visto como o primeiro passo para os outros tipos de ataques;
- ataques físicos aos medidores inteligentes: i) pela rede elétrica; ii) pelo próprio consumidor que faz uma ligação entre a entrada e a saída do medidor, ou iii) ataques mais sofisticados sobre o seu *hardware* ou *software*;
- interposição na comunicação das medidas (*man-in-the-middle*), que podem guardar as mensagens trocadas na rede (*logging*) ou forjar mensagens;
- simulação de medidores inteligentes em computadores criando os *meter bots*, para orquestrar ataques sobre a rede de distribuição, como ataques de negação de serviços [McDaniel e McLaughlin, 2009].

A confiança de clientes na nova infraestrutura de distribuição é fundamental para a sua adoção. A *Pacific Gas and Electricity* recebeu reclamações de cobranças excessivas de clientes que adotaram medidores inteligentes [Varodayan e Gao, 2010]. Prover uma arquitetura segura para o medidor inteligente é mandatório. Câmara propõe uma arquitetura para medidores inteligentes que são compostos por microcontroladores seguros [Câmara, 2011]. Os medidores coletam dados dos sensores conectados à rede elétrica e assinam esses dados antes de enviá-los para a concessionária ou guardá-los na memória do próprio medidor. A proposta é uma arquitetura segura que oferece novos serviços para o consumidor e a concessionária: a tarifação em função do horário e uma interface que possibilita aos consumidores verificarem o seu consumo.

Para que os medidores possam realizar a multitarifação, um contador agindo como o relógio, deve estar presente na arquitetura [Khalifa et al., 2011]. Esse relógio é conhecido como RTC (*Real Time Clock*) e precisa se sincronizar periodicamente com o horário no restante da infraestrutura. O RTC tem uma função fundamental em todo o funcionamento do medidor inteligente, permitindo o cálculo local das tarifas com a multitarifação, o registro de eventos relevantes com seus respectivos horários e outras atividades. Câmara propõe que o RTC seja incluído dentro do microcontrolador seguro presente no medidor, garantindo assim a integridade das medidas [Câmara, 2011]. Todas as atividades relevantes dentro do medidor devem ser registradas juntamente com uma estampa de tempo *timestamp* assinada pelo microcontrolador seguro. Esse modelo de arquitetura permite que o medidor inteligente atinja as exigências de segurança.

Privacidade na Infraestrutura Avançada de Medição

As informações coletadas em uma AMI podem revelar informações mais detalhadas sobre as atividades dos consumidores usando técnicas como a NALM (*Non Intrusive Appliance Load Monitoring*) [Quinn, Elias Leake, 2009]. Com NALM as informações entregues por um medidor inteligente podem ser comparadas com perfis conhecidos de eletrodomésticos para inferir o momento em cada eletrodoméstico está em uso. A Figura 3.17 apresenta os resultados do uso de NALM, usando medidas enviadas por um medidor inteligente a cada 15 minutos, em um intervalo de 24 horas. Informações tão detalhadas podem revelar as atividades cotidianas dos consumidores, o que cria preocupações sobre a privacidade das informações transmitidas através da AMI pelos medidores inteligentes.

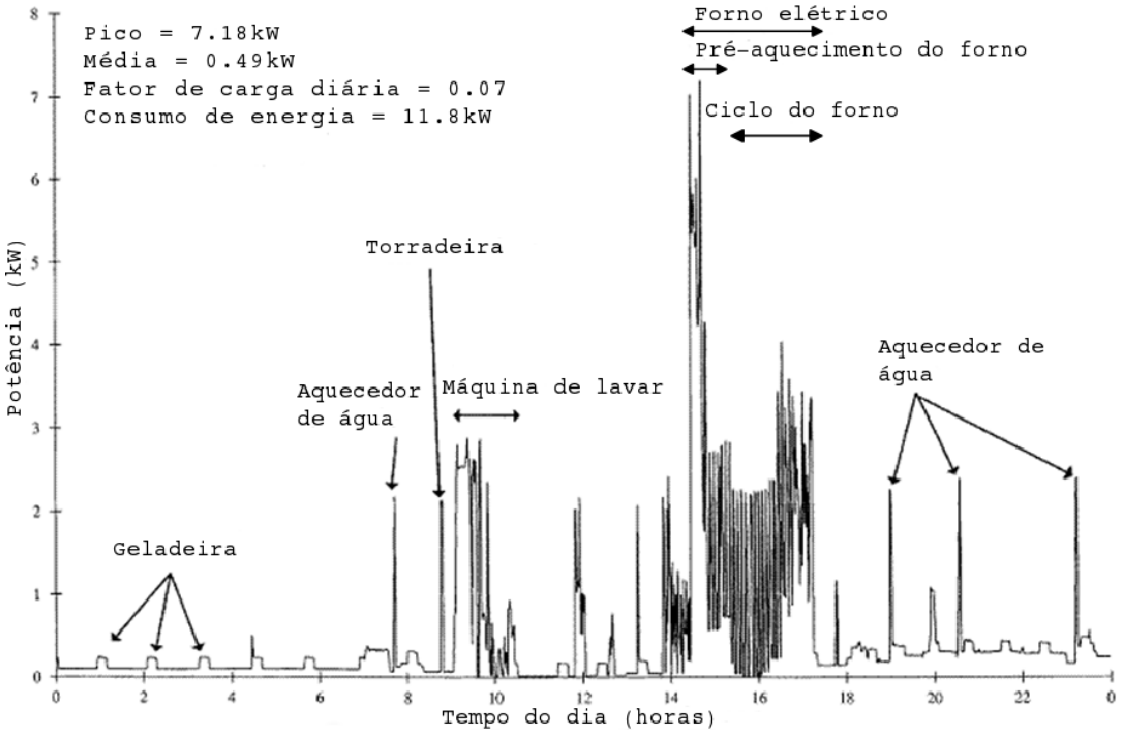


Figura 3.17. Uso de NALM (*Non Intrusive Appliance Load Monitoring*) para mapear atividades pessoais com informações de uso de energia enviadas na rede por um medidor inteligente. Figura Adaptada de [NIST7628, 2010b].

SmartPrivacy é um modelo conceitual de privacidade em AMI, baseado no NISTIR 7628 [Cavoukian et al., 2010]. Esse modelo propõe:

- toda informação divulgada para uma terceira entidade deve ser minimizada. Esses dados devem ser divulgados apenas para realizar serviços relevantes;
- canais seguros de transmissão devem ser definidos para assegurar que apenas entidades autorizadas tenham acesso à informação;
- terceiras entidades não devem pedir dados dos consumidores para concessionárias;

- terceiras entidades não devem correlacionar dados obtidos de outras fontes sem o consentimento prévio dos consumidores.

Outra proposta além de canais seguros fim-a-fim é a agregação de dados na AMI. Os dados coletados são enviados para agregadores que processam essas informações. Uma proposta para construir um canal seguro e permitir a agregação dos dados é o uso de criptografia homomórfica [Mármol et al., 2012]. Cada medidor inteligente tem uma chave e envia a sua chave para um agregador. O agregador por sua vez cria uma chave de grupo baseada em todas as chaves recebidas e repassa para os provedores de serviços. No entanto, um medidor inteligente malicioso pode não divulgar a sua chave e não precisa assim enviar os seus dados. Outra proposta é a criação de uma *spanning tree* para rotear os medidores para seus devidos agregadores, utilizando-se criptografia homomórfica [Bartoli et al., 2010].

A utilização de técnicas de ofuscação também garante um grau de privacidade dos dados enviados por medidores inteligentes. Ofuscação está associada ao conceito de obscuridade da informação ou falta de clareza de informação. Na Ciência da Computação, ofuscação é o ato de tornar a mensagem confusa ou difícil de interpretar para proteger o conteúdo da mensagem. Define-se um procedimento que torna a mensagem incompreensível, mas preservando o conteúdo da mensagem. Um exemplo é retirar o espaçamento entre palavras de um texto de uma mensagem, que evita ataques de força bruta que buscam extrair informações do texto da mensagem como mineração de dados [Chakraborty et al., 2012]. Em redes elétricas inteligentes, a ofuscação está associada a esconder informações dos consumidores para garantir sua privacidade. Kim *et al.* tornam as atividades diárias medidas por medidores inteligentes ininteligível para as concessionárias ou provedores de serviço com um estimador de estado cooperativo [Kim et al., 2011b]. Os autores consideram uma medição como função linear do vetor de fases dos circuitos de um domicílio somada com um ruído de medição e modelam um estimador do vetor de fases dos circuitos. Em seguida, define-se um conjunto de vetores que não alteram o resultado do estimador do vetor de fases dos circuitos e um conjunto especial de coeficientes para multiplicar esses vetores. Para ofuscar a medição, cada medidor soma um dos vetores multiplicado por um coeficiente à sua medição instantânea e enviam o resultado para as concessionárias ou provedores de serviços. Em seguida, concessionárias ou provedores de serviços somam tais valores para obter a medição agregada. Apesar da escolha dos coeficientes envolver um procedimento de otimização, esse método utiliza somente operações de soma e multiplicação de matrizes.

3.3.3. Ameaças de Segurança no Sistema SCADA

Os sistemas SCADA eram presumidamente seguros. A princípio a única falha de segurança que o SCADA estaria sujeito era a sabotagem dos equipamentos físicos. Atualmente, a conexão entre sistemas SCADA é realizada através de redes, como a Internet, por exemplo, expondo as vulnerabilidades do sistema ao mundo externo do ambiente seguro da planta controlada. Os ataques à segurança do sistema SCADA são comuns aos sistemas computacionais como um todo, já que o SCADA não foi projetado para ser executado em um ambiente inseguro [INL, 2001]. A segurança do SCADA se baseava no controle de acesso às instalações físicas em que estavam os componentes do sistema SCADA. As

vulnerabilidades permitem que um atacante que tenha acesso à rede do sistema SCADA possa atacar todos os elementos independentemente de onde estejam.

Como em qualquer sistema de computação, as principais vulnerabilidades do SCADA estão no *hardware*, no *software*, na integridade dos dados ou na rede. A principal vulnerabilidade de *hardware* é que as informações estão sujeitas a interceptação, pois as informações não são criptografadas e geralmente trafegam em enlaces de comunicação expostos. Nesse caso, uma medida de combate a essa vulnerabilidade é proteger o acesso físico aos enlaces de comunicação da rede do sistema SCADA. Outra vulnerabilidade do *hardware* do SCADA é a limitação de recursos de capacidade de processamento e memória dos sensores e das unidades terminais remotas (RTUs). Um atacante pode aproveitar dessa limitação para realizar a interrupção total ou aumentar o atraso na aquisição de dados no SCADA. As vulnerabilidades de *software* do SCADA também são similares que as de qualquer outro *software*, tais como interrupção, interceptação e modificação do aplicativo. Como em qualquer outro *software*, atacantes podem se aproveitar de vulnerabilidades publicadas em sítios de Internet para atacar sistemas SCADA desatualizados [INL, 2001]. Outra vulnerabilidade do SCADA é que a integridade dos dados trafegados é apenas assegurada por um código detector de erros CRC [Wright et al., 2004]. Assim, sistemas criptográficos têm sido propostos para SCADA [Igure et al., 2006]. Outro desafio em prover criptografia em SCADA é o gerenciamento de chaves [Dawson et al., 2006, Donghyun et al., 2009, Beaver et al., 2002]. Também, vulnerabilidades na rede afetam o sistema SCADA. A segurança da rede do sistema SCADA se baseia em protocolos proprietários e, então, é protegido por obscuridade, já que os protocolos não são divulgados, e por premissa, o atacante não tem acesso à rede física.

As ameaças de segurança ao sistema SCADA dividem-se em três grandes desafios. O primeiro desafio é controlar o acesso às redes do sistema SCADA. O segundo desafio é garantir a segurança na rede de comunicação do sistema SCADA, desenvolvendo mecanismos e ferramentas segurança eficazes, para garantir autenticidade, integridade dos dados e detectar intrusões além de outras atividades suspeitas na rede. O terceiro desafio é melhorar a gestão da segurança da rede do sistema SCADA.

Controle de Acesso - O sistema SCADA deve ser capaz de permitir que somente quem seja autorizado tenha acesso à rede do sistema SCADA. Isso é um desafio para a maioria dos sistemas SCADA atuais, pois os sistemas de controle são acessíveis aos operadores através de um nó *gateway* que conecta a rede do sistema SCADA à Internet. Contudo, em grande parte das implementações, o nó *gateway* não é a única forma de acesso dos nós da rede SCADA à Internet [Igure et al., 2006]. Um complicador ainda maior do controle de acesso aos nós SCADA é que o protocolo de tradução entre os protocolos da rede SCADA e a Internet não incorporam características de segurança. Assim, uma das propostas para se assegurar o controle de acesso às redes do sistema SCADA é implementar mecanismos de controle de acesso baseados em cartões inteligentes [Sauter e Schwaiger, 2002].

***Firewall* e Sistemas de Detecção de Intrusão** - O *firewall* bloqueia o tráfego não autorizado de entrar na rede protegida. O sistema de detecção de intrusão (*Intrusion Detection System* - IDS) gera alarmes e bloqueia quando o comportamento de um sistema foge do padrão ou apresenta alguma assinatura, padrão previamente conhecido, do ataque. Essas duas ferramentas são importantes para garantir a segurança em uma rede do sistema

SCADA. Uma proposta de arquitetura de segurança para redes do sistema SCADA baseia-se na definição de um *firewall* de 3 zonas para maior eficácia de filtragem. A arquitetura de 3 zonas divide a rede em três entidades física e logicamente separadas: a rede do sistema SCADA ou rede de controle de processo, a rede corporativa ou a rede da empresa e, por fim, uma zona desmilitarizada como uma passagem entre as outras duas zonas [Igure et al., 2006]. *Firewalls* apresentam melhores resultados quando em conjunto com sistemas de detecção de intrusão. Contudo, o desenvolvimento de regras de IDS para evitar ataques requer o conhecimento das vulnerabilidades nos protocolos e/ou padrões de ataque. Este conhecimento é desenvolvido através de estudos de vulnerabilidade de protocolos SCADA.

Criptografia e Gerência de Chaves - Atualmente, os protocolos usados na rede do sistema SCADA não suportam qualquer tipo de criptografia, pois a rede do sistema SCADA é uma rede dedicada e desconectada das demais. As mensagens são, portanto, transmitidas em claro. A adição de primitivas de criptografia nos protocolos de rede do sistema SCADA é um desafio, pois os nós apresentam restrições como capacidade computacional limitada, baixa taxa de transmissão de dados e a necessidade de respostas em tempo real a partir dos dispositivos da rede. Estas restrições dificultam a implementação de esquemas criptográficos complexos [Igure et al., 2006]. Algumas propostas de soluções de criptografia são incompletas, já que não realizam o gerenciamento eficiente de chaves [Beaver et al., 2002, Dawson et al., 2006, Donghyun et al., 2009, Donghyun et al., 2010].

Segurança dos Dispositivos e do Sistema Operacional - A segurança do sistema SCADA depende da segurança dos dispositivos na rede e muitos nós executam sistemas operacionais de tempo real (*Real Time Operational System* - RTOS) e outros softwares de controle de tempo real. Contudo, ao comparar os sistemas operacionais normais e sistemas operacionais de tempo real, estes são mais susceptíveis ao ataque de negação de serviço (DoS) porque mesmo pequenas interrupções no funcionamento do dispositivo podem levar a uma perda significativa da disponibilidade do sistema em uma aplicação em tempo real [Igure et al., 2006]. Outro ponto de vulnerabilidade em dispositivos é que no monitoramento de redes de distribuição de energia elétrica não é prático fornecer proteção física para cada nó, o que resulta em muitos nós não estarem seguros quanto a adulterações. Atacantes podem ganhar acesso físico irrestrito a esses nós, comprometendo-os e, assim, o atacante pode obter acesso ao resto da rede [Igure et al., 2006].

A principal fonte de vulnerabilidades na rede do sistema SCADA vem da sua conexão com redes externas, e esse cenário vai continuar a crescer, levando a um risco ainda maior de ataques cibernéticos e a consequente necessidade de melhorar a segurança da rede do sistema SCADA. Atualmente, existem iniciativas de organizações para padronizar e melhorar a segurança da rede SCADA, embora ainda esbarrem em desafios técnicos [Igure et al., 2006].

Em resumo, as vulnerabilidades do sistema SCADA são basicamente as vulnerabilidades de qualquer sistema de computação, somadas ao complicador de que os dados tratados no sistema são de alta importância e a adulteração ou a quebra de privacidade desses dados podem ter consequências catastróficas para o sistema controlado. Outro ponto característico de vulnerabilidade do sistema SCADA é o fator humano. O controle do sistema muitas vezes é realizado por um operador humano que está sujeito a falhas

de operação e à quebra de privacidade do sistema, como, por exemplo, cedendo senha de acesso a outro operador não autorizado.

3.3.4. Ameaças de Segurança ao WAMPAC

O protocolo de comunicação mais comum utilizado entre PMU e PDC é o padrão IEEE C37.118 para a transmissão de dados. Contudo, as mensagens utilizadas nesse protocolo não possuem mecanismos de verificação de integridade e de garantia de confidencialidade [Morris et al., 2012]. Atualmente, há um projeto, *draft*, do padrão IEC 61850-90-5 que inclui uma assinatura digital para fornecer autenticação, para detectar falhas na integridade e, ainda, inclui criptografia opcional para garantir a confidencialidade das mensagens.

O WAMPAC está sujeito a ameaças de segurança às Unidades de Medição Fasorial. Morris *et al.* ressaltam algumas ameaças virtuais que o WAMPAC está sujeito, tais como, ataques de reconhecimento (*Reconnaissance Attack*), de negação de serviço (*Denial of Service* - DoS) e de injeção de pacote [Morris et al., 2012]:

- o ataque de reconhecimento consiste em o atacante identificar os sistemas conectados e, em seguida, recolher configurações e padrões de comunicação dos sistemas conectados, tais como aprender quais são as portas abertas, identificar a versão do sistema operacional remoto e identificar a versão dos aplicativos que implementam as pilhas de protocolos de rede no sistema remoto. Essas informações recolhidas pelo ataque de reconhecimento se constituem em uma ameaça, pois permitem que o atacante planeje um ataque específico para o sistema já reconhecido. Um exemplo de ataque de reconhecimento é o atacante que escuta um tráfego não criptografado entre PMUs e PDCs, como no protocolo IEEE C37.118, para identificar quais as coordenadas geográficas fornecidas pelo GPS da localização das PMUs;

- o ataque de injeção de pacotes pode ser classificado em dois subgrupos:

  a Injeção de Medições de Sensores consiste em injetar medidas falsas na rede, induzindo o sistema de controle a calcular um estado do sistema elétrico inconsistente, errado e, por consequência, levando o sistema de controle a tomar medidas não adequadas ao estado corrente do sistema elétrico;

  a Injeção de Comandos insere comandos falsos no sistema de controle. A injeção de comandos pode se dar através de um atacante enviando dados na rede como se fosse o comando de controle enviado por operadores humanos agindo nos sistemas supervisórios ou, outra possibilidade, é o atacante alterar os dados de Dispositivos Eletrônicos Inteligentes (IEDs) ou de Unidades Terminais Remotas (RTUs) que executam ações de controle, de modo que ao executar uma ação, esses elementos executem a ação definida pelo atacante.

- o ataque de negação de serviço (DoS) consiste em exaurir os recursos de comunicação entre a unidade terminal remota (RTU) e o terminal mestre ou a estação com interface homem-máquina. Normalmente este ataque é realizado inserindo um grande volume de tráfego para um dos dispositivos mestres ou RTU e, como esses dispositivos têm memória muito limitada, os dispositivos interrompem o funcionamento ou reiniciam.

3.3.5. Autenticação e Gerenciamento de Chaves em Redes Elétricas Inteligentes

A autenticação de todos os dispositivos que trocam informações e o gerenciamento de identidades nas redes elétricas inteligentes é fundamental porque afetam o funcionamento da rede elétrica [Wenye e Zhuo, 2013]. Portanto, a integração do sistema com a interconexão de milhões dispositivos de medição e controle é crucial para garantir a estabilidade geral do sistema de energia. No entanto, o contexto de redes elétricas inteligentes impõem algumas restrições que tornam a autenticação um desafio ainda maior [NIST7628, 2010a]. Os principais desafios são quantidade de dispositivos, que chegam a milhões, a limitada capacidade de processamento e de armazenamento de alguns dos dispositivos e a pequena banda passante de alguns canais de comunicação, o que impede esquemas de segurança que requerem muita troca de informação.

A autenticação com chaves simétricas requer que entidades pares possuam uma mesma chave secreta para assinar as mensagens. Como só a entidade par possui a chave secreta, a assinatura só pode ser verificada pela entidade par. Um dos desafios associados à autenticação com chaves simétricas é a distribuição das chaves secretas de maneira segura. Além disso, o gerenciamento de identidades baseado em chaves simétricas é inadequado quando se tem uma grande quantidade de dispositivos comunicantes, pois requer o armazenamento de uma chave secreta para cada conexão segura.

Na autenticação com chaves assimétricas, cada entidade possui um par de chaves pública/privada, de modo que um texto criptografado pela chave privada só pode ser decriptografado pela correspondente chave pública e vice-versa. Já que a assinatura é realizada pela criptografia com a chave privada, qualquer entidade que possuir a chave pública correspondente pode certificar a autenticidade da mensagem. O desafio da autenticação com chaves assimétricas reside na associação de uma identidade digital com sua chave pública. No gerenciamento de identidades com infraestrutura de chaves públicas (ICP), os dispositivos obtêm um certificado digital que garante as identidades digitais e contém chaves para a comunicação segura. A ICP define um conjunto de *hardware*, *software*, políticas e procedimentos para gerenciar certificados digitais [Chokhani e Ford, 2003], que vinculam uma chave pública da criptografia assimétrica a alguma informação acerca da identidade, como um endereço IP (*Internet Protocol*) de um serviço, um número de série de um dispositivo, um registro de um consumidor, entre outros. Os certificados digitais são assinados pela autoridade certificadora (AC), uma entidade confiável cuja chave pública é conhecida por todos os consumidores da ICP. Uma AC também gera certificados para ACs encarregadas formando uma cadeia de certificados, para distribuir a carga de gerenciamento de certificados. Assim, um consumidor da ICP pode verificar a assinatura de um certificado diretamente com chave pública da AC conhecida, ou obter e verificar a cadeia de certificados até a AC conhecida.

Os desafios inerentes aos modelos de infraestrutura de chaves públicas (ICP) são agravados no contexto das redes elétricas inteligentes por causa da sobrecarga causada em determinadas tarefas pelo grande número de dispositivos como, por exemplo, a revogação de certificados digitais devido à perda de dispositivos, mau funcionamento e comportamento malicioso. Uma das abordagens de revogação de certificados digitais é o protocolo de estados em tempo real de certificados (*Online Certificate Status Protocol* - OCSP), que oferece um serviço de revogação de certificados em tempo real [Myers et al., 1999].

Com OCSP, um dispositivo consulta o estado de identidade no serviço de revogação, o qual responde um dos seguintes estados para a identidade “boa”, “revogada” ou “desconhecida”. Por se tratar de um serviço essencial para o funcionamento correto das redes elétricas, ele deve estar sempre disponível, deve ser capaz de atender a todas as consultas de identidade de todos os dispositivos em tempo hábil e deve se proteger de todos os ataques de negação de serviço. Esses requisitos devem ser assegurados, pois a falha de uma consulta pode bloquear a realização de uma operação crítica como o redirecionamento de energia no caso de falhas nas linhas de transmissão e, por fim, resultar na interrupção do abastecimento energético.

Uma alternativa para a revogação de certificados é utilizar uma lista de certificados revogados (LCR), na qual se inclui um registro para cada identidade digital comprometida [Housley et al., 2002]. Os certificados devem ser renovados após uma data limite de validade e os certificados revogados ainda válidos devem permanecer na LCR até passar a validade. Portanto, o balanceamento do período de validade de certificados e o tamanho da LCR impõe algumas restrições. O tamanho da LCR pode crescer muito caso o período de validade de um certificado digital seja grande, pois acarreta em um grande período de permanência de chaves revogadas na lista de certificados revogados. Por outro lado, ao se procurar manter uma LCR de tamanho pequeno, diminuindo o período de validade, acarreta-se uma sobrecarga de controle para a renovação dos certificados. Em redes elétricas inteligentes, o elevado número de dispositivos resulta em uma maior dificuldade de obter um compromisso entre o tamanho das listas de revogação de certificados e a sobrecarga de controle para renovar certificados se o período de validade do certificado é reduzido. Além dos problemas técnicos têm os problemas operacionais, pois uma concessionária tem que custear o gerenciamento da infraestrutura de chave pública. Os custos atuais não se adequam ao cenário das redes elétricas inteligentes, pois o gerenciamento de identidades hoje requer um funcionário para cada 10.000 medidores e isto resultaria no custo inaceitável de 500 profissionais para 5 milhões de medidores inteligentes [Khurana et al., 2010]. Assim, o gerenciamento de ICPs necessita procedimentos automatizados e modelos de integração de múltiplas ICPs [Baumeister, 2011].

No modelo de listas de certificados confiáveis (*Certificate Trust List*) utilizado pela maioria dos navegadores de Internet, uma autoridade publicadora divulga uma lista com os certificados das autoridades certificadoras (AC) confiáveis. Consumidores, serviços e dispositivos utilizam essa lista para autenticar qualquer certificado ou cadeia de certificados, cujo certificado raiz esteja presente na lista. Esse modelo possui alta disponibilidade e garante operação em tempo real, pois requer pouca interação entre seus componentes, utilizando principalmente armazenamentos locais da lista. Entretanto, ao usar uma lista estática, esse modelo não possui muita flexibilidade e as modificações na lista precisam ser atualizadas em todos os dispositivos. Ademais, a lista de pode ser muito extensa se cada organização agir como sua própria autoridade certificadora (AC) raiz, dificultando ainda mais a gerência. O modelo de infraestrutura de chaves públicas (ICP) hierárquico utiliza uma única AC raiz que emite certificados para ACs encarregadas, e assim por diante até a emissão de certificados para os dispositivos, serviços e consumidores. Esse modelo ajuda a identificar a cadeia de confiança e de validação de certificados, e permite a emissão de certificados em domínios a fim de tornar modelo escalável. A estrutura hierarquizada impõe a interoperabilidade entre elementos da cadeia, então é fácil gerar

políticas, procedimentos e nomes padronizados. Apesar da possibilidade de ACs encarregadas operarem independentemente por longos períodos, caso a AC raiz for comprometida, todo o sistema fica comprometido. O modelo de ICP em malha procura eliminar o ponto único de falha do modelo hierárquico e, portanto, cada organização é responsável pela própria solução ICP, e realiza uma certificação cruzada com organizações com quem desejam se comunicar. Esse modelo é bem flexível, pois permite que cada organização possua a solução de ICP mais adequada. Além disso, a natureza distribuída desse modelo cria uma fonte distribuída de confiança que torna o sistema mais disponível, e resistente a ataques e desastres naturais. Entretanto, a ausência de agentes centralizadores que estabeleçam diretrizes causa uma maior complexidade nas relações entre organizações de interoperabilidade e política de segurança, como a avaliação do nível de confiança de outras organizações, o endereçamento estruturado de identidades e a descoberta das cadeias de confiança resultando em maiores atrasos para validação de certificados.

O modelo de ICP em ponte, assim como no modelo em malha, cada organização é responsável por sua própria solução de ICP, mas ao invés da certificação cruzada com cada organização par, as organizações usam uma ponte para fazer a certificação cruzada. A ponte gerencia as relações entre organizações e usa mapeamentos de políticas para interoperabilidade de organizações. As desvantagens desse modelo são a criação de ponto único de falha e complexidade da descoberta das cadeias de confiança como o modelo de ICP em malha. No entanto, esse modelo pode ser adequado para as redes elétricas inteligentes, pois combina a flexibilidade de fonte distribuída de confiança com a eficiência do gerenciamento centralizado [Baumeister, 2011].

Fouda *et al.* apresentam um esquema de autenticação para medidores inteligentes que utiliza o protocolo de Diffie-Hellman para a geração de chaves compartilhadas para serem utilizadas na assinatura com *hash* [Fouda et al., 2011]. Com o protocolo Diffie-Hellman, duas entidades pares geram uma chave comum a partir de chaves secretas próprias e informações públicas [Mahalanobis, 2005]. Por sua vez, a assinatura com *hash* é realizada com a inclusão no final da mensagem do *hash* da mensagem mais a chave comum. A entidade par que possuir a chave comum realiza a mesma operação para comprovar o *hash* da mensagem. Esse de autenticação possui baixa complexidade computacional, portanto é indicado para mensagem com baixa tolerância de atrasos [IEC, 2007]. Os autores argumentam ainda que a troca inicial de mensagem possa ser assegurada por chaves assimétricas e mecanismos de gerenciamento de identidades como a ICP.

Uma forma de evitar a dificuldade da associação de identidades digitais com chaves públicas é através da utilização da criptografia baseada em identidades, na qual o identificador de um consumidor é usado na composição da própria chave pública e assim evita o uso de certificados digitais [Hoeper e Gong, 2006]. Nesse esquema, uma entidade Geradora de Chaves Privadas (GCP) possui uma com uma chave privada mestra e uma chave pública universalmente conhecida, que é utilizada na composição das chaves públicas das entidades junto com os identificadores das próprias entidades [Ferraz, 2011]. So *et al.* propõem usar a criptografia baseada em identidades para a comunicação fim-a-fim em redes elétricas inteligentes [So et al., 2010]. Esse esquema diminui a responsabilidade do emissor em relação à ICP, pois o emissor não precisa obter um certificado para a comunicação com cada par. O emissor também não precisa obter novos certificados dos pares após a expiração, pois a validade pode estar embutida na chave pública das entida-

des. O emissor pode exigir que o receptor renove sua chave ao usar o identificador do receptor com uma marca de tempo. Além disso, o emissor pode gerar uma chave compartilhada com um par sem uma troca inicial de mensagens. Dessa maneira, esse esquema é escalável ao evitar trocas de mensagens de controle ao antes de enviar uma mensagem segura. Por outro lado, a GCP deve ser uma entidade muito confiável, pois como ela gera as chaves privadas das entidades, ela tem acesso a todas as chaves e pode decriptografar e assinar todas as mensagens. Dessa maneira, a GCP pode ser representada por uma autoridade reguladora governamental, assumindo que seja altamente segura. Além disso, a geração de chaves privadas pode ser distribuída em diversos servidores, de modo que cada um tenha somente uma parte da chave privada mestra. Para tornar a chave privada mestra ainda mais segura ela pode ter curta validade para diminuir a chance de comprometê-la. O esquema de criptografia baseada em identidades possui alguns dos mesmos desafios de ICP, como a revogação de chaves de entidades e a renovação das chaves da GCP.

3.3.6. Relatório NISTIR 7628 - Diretrizes de Segurança Cibernética

O NISTIR 7628 é um relatório feito pelo *National Institute of Standards and Technology* (NIST) que prevê a descrição da arquitetura de alto nível das redes elétricas inteligentes [NIST7628, 2010a]. O relátorio foi elaborado pelo *Cipher Security Working Group (CSWG) of the Smart Grid Interoperability Panel (SGIP)*, que tem 500 participantes de diversos setores acadêmicos e industriais. O NISTIR 7628 descreve uma abordagem a problemas de segurança e os objetivos e requisitos de segurança em comunicações em uma rede elétrica inteligente.

O NISTIR 7628 está composto por três volumes, em que o primeiro volume descreve a metodologia usada pelo CSWG para definir os requerimentos de segurança. O relatório também apresenta uma arquitetura de referência de alto nível e requisitos de latência para algumas aplicações. O primeiro volume termina com uma discussão sobre temas criptográficos e de gerenciamento de chaves.

A arquitetura de alto nível é composta por domínios, atores e interfaces. Os domínios apresentados são: geração, transmissão, distribuição, consumidores, mercados, operadores e provedores de serviços.

Domínios são compostos por grupos de atores com objetivos similares e participando de aplicações similares. Atores executam ações e trocam informações com outros componentes da rede elétrica inteligente, como por exemplo, medidores inteligentes. Uma organização pode ter múltiplos atores através de vários domínios. Os atores comunicam entre si usando interfaces. No NISTIR 7628 as interfaces são agrupadas em categorias e são avaliados os requisitos de segurança para essas categorias.

A discussão do relatório sobre criptografia determina que os medidores inteligentes e alguns equipamentos, como IEDs, tenham recursos computacionais limitados. Além disso, os IEDs participaram de aplicações com fortes requesitos de tempo, assim, o relatório discute os desafios de segurança que representa adaptar e desenvolver sistemas para este tipo de dispositivos. Segundo o relatório, estratégias tradicionais como a infraestrutura de chaves públicas (ICP) podem não resultar apropriadas devido a problemas com listas de revogação.

O segundo volume discute temas de privacidade em redes elétricas inteligentes que foram tratados na Seção 3.3.2, sobre a privacidade na infrastrutura avançada de medição.

O terceiro volume conclui com uma compilação de análises e referências usadas para criar os requisitos de segurança. O terceiro volume ainda apresenta um capítulo de desafios em pesquisa e desenvolvimento que devem ser atingidos para oferecer uma rede elétrica segura. As discussões no presente minicurso abordam esses desafios.

O relatório NISTIR 7628 define que os objetivos de segurança em redes elétricas inteligentes devem ser:

disponibilidade - oferecer o acesso sincronizado e confiável à informação e seu uso. A perda de disponibilidade é o impedimento do acesso a uma determinada informação;

integridade - guardar a informação contra qualquer modificação ou destruição imprópria e garantir o não-repúdio e autenticidade de uma informação. A modificação imprópria de informações pode levar a decisões tomadas erradamente sobre o gerenciamento da energia;

confidencialidade - acesso à informação preservando-se restrições de autorização.

Requerimentos de segurança do NISTIR 7628

Os requerimentos do NISTIR estão divididos em três categorias: de governo, de risco e de cumprimento (GRC), técnicos comuns e técnicos únicos. Os requerimentos GRC devem ser implantados no nível organizacional, como, por exemplo, a definição de políticas e procedimentos de controle de acesso. Os requerimentos técnicos comuns devem ser aplicados em todas as interfaces como, por exemplo, a limitação do número de tentativas mal sucedidas de *login*. Os requerimentos técnicos únicos são específicos de um conjunto determinado de categorias de interfaces.

Cada requerimento define um conjunto específico de atividades de segurança que devem ser realizadas pelas organizações. No requerimento é indicado o nível de impacto nos objetivos de segurança cibernética nas redes elétricas inteligentes. Os níveis de impacto são: baixo, médio e alto. Um impacto baixo implica em um efeito adverso **limitado**, um impacto médio implica um efeito adverso **sério** e um impacto alto implica um efeito adverso **catastrófico**.

Como exemplo, a comunicação entre um equipamento RTU de transmissão e um sistema SCADA é identificado no NISTIR 7628 como uma interface de categoria 1, o que implica que é uma interface com alta disponibilidade e com restrições computacionais e/ou de largura de banda. O comprometimento neste tipo de interface causaria um impacto baixo na confidencialidade e impactos altos na integridade e na disponibilidade. Usando estes níveis de impacto os requerimentos únicos definidos para esta interface são controle de acesso, identificação e autenticação, proteção do sistema de informação e da comunicação.

- **Controle de acesso** - algumas ações específicas podem ser realizadas sem identificição ou autenticação do consumidor.
- **Identificação e Autenticação** - os consumidores devem ser globalmente identifica-

dos e autenticados; os dispositivos devem ser globalmente identificados e autenticados; o mecanismo de autenticação não deve prover informação que permita a um consumidor não autorizado comprometer o mecanismo de autenticação;

- **Proteção do Sistema de Informação e da Comunicação** - o sistema de informação tem mecanismos para isolar funções seguras e não seguras, limita ou mitiga os efeitos de negação de serviço, os dispositivos de borda de rede filtram certos tipos de pacotes para proteger a rede interna e o sistema de informação utiliza mecanismos de criptografia para asegurar a integridade da informação e a confidencialidade da informação. O sistema de informação utiliza técnicas de verificação para detectar alterações e erros no *software* utilizado pelos equipamentos.

3.3.7. Segurança dos Protocolos DNP3 e IEC 61850

O protocolo DNP3 prevê um mecanismo de autenticação próprio na camada de aplicação. Uma das partes, a estação de controle ou a estação escrava, inicia a conexão e envia uma mensagem. O receptor da mensagem responde com um desafio para a outra entidade. Essa entidade deve gerar um *keyed-hash message authentication code* (HMAC) com o desafio mais a chave secreta que as duas partes conhecem. Ao receber a resposta, o emissor do desafio verifica se o valor recebido está correto, caso esteja, o receptor responde à primeira mensagem como previsto no protocolo. Para economizar banda, o protocolo também prevê um "modo agressivo", em que parte da mensagem age também como desafio. O emissor calcula o HMAC dessa mensagem com a chave conhecida e envia. Caso esteja correto, o receptor responde de acordo com o protocolo. O modo agressivo não é tão seguro, pois apenas uma parte da mensagem está sendo gerada aleatoriamente para servir de desafio. Apesar disso, a norma considera que o modo agressivo é suficientemente seguro e define que todas as entidades devem suportar esse modo.

A norma IEEE1815 também define protocolos de troca de chaves. Pela norma, cada entidade tem dois tipos de chaves: a chave de sessão, com duração de horas até semanas e a chave de atualização, com duração de meses ou anos. A chave de sessão é utilizada na autenticação enquanto que a chave de atualização é utilizada para criptografar as mensagens do protocolo de troca das chaves de sessão. A troca da chave de atualização é feita por meios externos aos protocolos definidos na norma [Gilchrist, 2008, IEEE1815, 2012].

O uso de protocolos de segurança como o TLS/SSL é recomendado quando as mensagens trafegam sobre TCP/IP para garantir a confidencialidade do conteúdo das mensagens.

Na especificação de segurança do protocolo DNP3 [Gilchrist, 2008], define-se o uso de autoridades certificadoras para a troca de chaves. A troca de chaves por certificados permite um gerenciamento de chaves de sessão de forma mais confiável. Majdalawieh *et al.* descrevem o DNPSec, um protocolo de segurança para camada de enlace que garante confidencialidade, pois o conteúdo da mensagem deve ser criptografado por uma chave DES e a integridade é garantida através do envio de um *hash* da mensagem em anexo [Majdalawieh et al., 2006].

Falk discute ameaças ao padrão IEC 61850 que são o acesso desautorizado, o roubo de identidade na rede do sistema SCADA, a reutilização, a interceptação (*ea-*

vesdropping) e a manipulação de mensagens. Para resolver esses problemas, mecanismos de confidencialidade, autenticação e integridade devem ser adicionados às mensagens [Falk, 2008, Klein, 2009].

A série de padrões IEC 62351 [IEC, 2007] define mecanismos de segurança para protocolos de comunicação, como por exemplo o IEC 61850. Esses protocolos trocam diferentes tipos de informação como amostras feitas pelos dispositivos elétricos inteligentes (*Intelligent Electric Devices* - IEDs), mensagens de eventos ocorridos nas subestações e mensagens de comandos. A IEC 62351-7 desenvolve um modelo abstrato de elementos que participam das redes elétricas inteligentes. Essa norma desenvolve objetos de dados para gerenciamento de redes e sistemas (*Network and System Management* – NSM).

IEC 62351-3 recomenda o uso de protocolos de segurança para troca de mensagens, como o TLS (*Transport Layer Security*). Apesar disso, em [Wenye e Zhuo, 2013] é indicado que a autenticação por troca de chaves públicas sugerida nessa norma não atende às aplicações em que o tempo é crítico e um dos terminais tem pouco poder computacional, por exemplo, um sensor. Essa autenticação pode gerar um ataque de negação de serviços em redes elétricas inteligentes. O atacante pode causar o atraso de mensagens que devam atender requisitos críticos de tempo.

IEC 62351-4 dedica-se às mensagens MMS (*Manugecturing Message System*). Esse padrão sugere o uso de HMACs (*Hash Message Authentication Code*) para MMS (ISO 9506). HMACs garantem a autenticação do emissor da mensagem, assim com a integridade de seu conteúdo, mesmo para aplicações com requisitos críticos de tempo.

IEC 62351-5 define que as mensagens devem seguir por um canal seguro SSL/TLS, enquanto a IEC 62351-6 assegura que as mensagens GOOSE necessariamente devem ser marcada com uma etiqueta de VLAN (802.1Q) para terem os seus requisitos de tempo crítico respeitados e, além disso, inserem um HMAC nas mensagens GOOSE.

Há a proposta de que o padrão IEC 62351 seja atualizada para novos estudos de casos de redes elétricas inteligentes [Steffen et al., 2010]. Esses casos são derivados da participação de consumidores e de cálculos de demanda e resposta da rede.

3.4. Projetos de Pesquisa, Desafios e Propostas para Redes Elétricas Inteligentes

Esta seção descreve alguns projetos de pesquisa nacionais e internacionais, apresenta alguns importantes desafios e apresenta algumas propostas do Grupo de Teleinformática e Automação (GTA) para redes elétricas inteligentes.

3.4.1. Projetos de Pesquisa

Múltiplos projetos sobre redes elétricas inteligentes têm sido apresentados atualmente em diferentes partes do Brasil, desde regulações até implementações. Existem projetos pilotos das concessionárias de distribuição como a Cidade Inteligente de Búzios, feita pela AMPLA/ENDESA ou Projeto Smart Grids pela AES Eletropaulo, etc. Também existem implantações de distintas tecnologias como, por exemplo, sistemas de medições centralizados (medidores inteligentes) ou iluminação eficiente. Paralelamente alguns organismos do estado estão fazendo regulações distintas como especificações de medidores

inteligentes ou regulamentações da microgeração. Além das concessionárias, diversas universidades do país pesquisam soluções nas diversas áreas das redes elétricas inteligentes como Eletrônica de Potência, Telecomunicações, Controle, etc. Seguem abaixo algumas iniciativas mais focadas em segurança e no contexto deste minicurso, assim como alguns desafios e propostas para experimentar e avaliar o desempenho e a segurança das redes de comunicações, que constituem os primeiros passos para a implementação das redes elétricas inteligentes no Brasil.

3.4.1.1. Iniciativas Internacionais

O *Pacific Northwest Smart Grid Demonstration Project* [PNSGD, 2013] é um dos maiores projetos piloto de redes elétricas inteligentes dos EUA. Um dos 16 projetos financiados pelo Departamento de Energia do governo americano, o projeto envolve mais de 60.000 clientes em cinco estados americanos. Nos próximos dois anos, o projeto se concentrará em coletar e analisar dados de utilização de energia. As 11 concessionárias participantes irão analisar os benefícios da utilização da rede elétrica inteligente localmente em suas cidades e no nível regional. A ideia é investigar como uma rede elétrica inteligente pode entregar energia de forma mais eficiente e como se pode aumentar a utilização de fontes de energia eólicas.

O *Trustworthy Cyber Infrastructure for the Power Grid* [TCIPG, 2013] é um projeto liderado pela *University of Illinois at Urbana-Champaign* que busca definir uma infraestrutura segura para as redes elétricas inteligentes. Dentro deste projeto, uma equipe do *Los Alamos National Laboratory* obteve sucesso ao demonstrar a proteção de dados de controle através de criptografia quântica. Dados de controle da rede inteligente devem ser transmitidos de forma segura e sem atraso, dado que principalmente com as fontes renováveis, a geração de energia pode variar em curtos períodos de tempo. Utilizando criptografia quântica, estes requisitos podem ser atendidos. Fótons são usados para produzir números aleatórios de forma segura, compartilhados pelos consumidores. Estes números aleatórios podem então ser usados para autenticar e criptografar os comandos de dados e de controle da rede inteligente. Uma vez que os números aleatórios foram produzidos de forma segura, eles podem ser usados como material criptográfico para algoritmos de autenticação e criptografia. O laboratório produziu um pequeno transmissor óptico que pode ser utilizado para transmitir os fótons utilizados na geração do número aleatório, além dos pacotes de dados e comandos, usando a mesma fibra óptica.

No Japão, uma iniciativa conhecida como *Digital Grid* [Rikiya, 2010] é uma das mais inovadoras em redes elétricas inteligentes. O Japão decidiu abandonar, a médio prazo, a energia nuclear. Assim, no caso do Japão a exploração de fontes de energia renováveis e a implantação de uma rede elétrica inteligente tornaram-se cruciais. As concessionárias de energia tem por objetivo regular a frequência e voltagem na rede, mantendo um equilíbrio o mais fino possível entre a geração de energia e o consumo. Como numerosas fontes de geração de pequeno porte em vez de grandes plantas de geração de energia é uma característica de muitas fontes de energia renovável, a busca desse equilíbrio torna-se um desafio. Um grupo de empresas japonesas busca uma solução diferente para a rede elétrica inteligente, inspirada da rede de comutação de pacotes da Internet. A ideia

básica do que foi chamado a *Digital Grid* é uma arquitetura baseada na Internet, em que existiriam "pacotes de energia" virtuais. A ideia é subdividir a rede elétrica atual, completamente sincronizada, por células autônomas, de tamanhos variados, interconectadas. O equivalente de um endereço IP seria associado a geradores, conversores de potência, fazendas eólicas, fontes de energia solar e outros elementos dentro das células. O equivalente do roteador seria o *Digital Grid Router* (DGR). DGRs teriam o papel de gerenciar e regular as demandas de energia elétrica, através de conexões assíncronas entre as células, realizadas pelo roteador. A inteligência do DGR está em conhecer quanto determinado cliente pretende consumir em uma janela de tempo no futuro, identificar as fontes de energia disponíveis para esta demanda, e realizar a interconexão no tempo devido.

3.4.1.2. Iniciativas Nacionais

O projeto Cidade Inteligente [CIB, 2013] liderado pela empresa Ampla em Búzios, no estado do Rio de Janeiro, visa implantar uma infraestrutura de rede elétrica inteligente na cidade litorânea. A Ampla é a concessionária de energia elétrica que atende boa pare do interior do estado do Rio de Janeiro. O projeto conta com recursos da ordem de R$ 30 milhões. O objetivo principal é racionalizar o consumo de energia na cidade. O projeto pretende implantar a cobrança de tarifa diferenciada por horário, a modernização da iluminação pública com utilização de luminárias com LEDs, luminárias com microgeração eólica e pontos de iluminação telecomandados. Todas estas iniciativas pretendem aumentar a economia de energia elétrica. Além disso, fases futuras do projeto preveem a utilização de veículos elétricos. A Ampla é controlada pela empresa espanhola Endesa, que possui projeto semelhante em Málaga, na Espanha.

A Light, concessionária de energia elétrica na cidade do Rio de Janeiro, possui um programa denominado Smart Grid Light [SGL, 2013], cujo piloto envolve a implantação de medidores inteligentes em um grupo de consumidores da empresa. Um dos aspectos do programa é o acompanhamento do perfil de consumo de energia dos clientes. Com isto, podem-se detectar pontos de desperdício e horários de pico de consumo, permitindo planejar a distribuição de energia de forma mais eficiente. Por outro lado, outro aspecto importante é a segurança das medições. A utilização de medidores inteligentes seguros é importante para a concessionária, permitindo, por exemplo, diminuir perdas não técnicas, também conhecidas como "gatos". Também é importante para o consumidor, que deve ser capaz de verificar o seu consumo e a cobrança correta por parte da concessionária.

A empresa AES Eletropaulo investe em programa de implantação de infraestrutura de medição inteligente no estado de São Paulo [Eletropaulo, 2013]. Através da utilização de novas tecnologias, principalmente sem fio, a empresa pretende reduzir os custos de operação e as perdas não técnicas. Por exemplo, em parceria com a empresa *Spring Wireless*, a AES Eletropaulo desenvolveu um sistema automatizado que utiliza mensagens SMS para alguns serviços simples, como solicitação de segunda via de fatura ou religação de energia. A utilização de mensagens SMS reduz custos, pois evita que uma parte das chamadas sejam feitas para o seu *call center*. Além disso, a Eletropaulo fez uma parceria com uma empresa nacional desenvolvedora de medidores inteligentes.

3.4.2. Gerenciamento de Identidades e Controle de Acesso usando Microcontroladores Seguros

Com a adoção das redes elétricas inteligentes, vai haver uma maior comunicação entre as diferentes entidades que coordenam o sistema elétrico e novas formas de coordenar as atividades no sistema elétrico vão ser possíveis.

As redes elétricas inteligentes são compostas por diversas entidades (ou atores) atuando nos diferentes domínios definidos pela NIST [NIST7628, 2010a]. Josang *et al.* apresentam quatro modelos de gerenciamento de identidades e comparam as exigências de confiança para cada modelo [Jøsang et al., 2005]. Cada identidade é dividida em identificador, um elemento de informação que permite identificar unicamente uma entidade e credenciais, elementos de informação que permitem à entidade identificada comprovar que ela é autêntica. Os modelos propostos seguem a classificação de gerenciamento de identidades: isolado, federado, centralizado e centralizado no consumidor.

O foco principal de modelos de gerenciamento de identidades mais integrados deve ser a autenticação segura, ou seja, o gerenciamento e distribuição de credenciais de forma segura entre as entidades. Sauter e Schwaiger abordam o problema de gerenciamento e distribuição de credenciais para autenticação via Internet em uma FAN (*Field Area Network*). Essas redes são utilizadas em plantas industriais e permitem a operação de processos industriais. A proposta consiste em utilizar cartões inteligentes para gerar e armazenar chaves. Cartões inteligentes contêm microcontroladores e aplicações, podendo executar operações criptográficas em seu interior. Essa funcionalidade permite ao cartão inteligente gerar chaves e guardá-las sem que essas sejam reveladas a qualquer outra entidade. Na arquitetura proposta, o cartão é responsável por construir um MAC dos comandos enviados através da Internet para uma FAN. Esse MAC autentica o consumidor e garante a integridade da mensagem [Sauter e Schwaiger, 2002].

Existem diversos protocolos de aplicação para gerenciamento de identidades federado, centralizado ou mesmo centrado no consumidor. Para garantir a segurança, seja qual for o modelo de gerenciamento de identidades escolhido, a distribuição de credenciais e a autenticação devem ser feitas utilizando-se microcontroladores seguros. Um desses protocolos é o OpenID, que permite consumidores se autenticarem e abrirem sessões em um provedor de identidades. Nesse sentido, o Grupo de Teleinformática e Automação usa cartões inteligentes para verificar se o consumidor é legítimo e o autentica através de um provedor de identidades [Guimarães, 2012].

3.4.3. Desafios dos Veículos Elétricos e Armazenamento de Energia

O advento dos veículos elétricos descortina um novo e desafiante cenário onde observamos o armazenamento de energia através das baterias e a possibilidade desses veículos atuarem não só como consumidores de energia, mas também como fontes de energia distribuídas quando estacionados. O aumento da frota de veículos elétricos no mercado irá viabilizar um balanceamento de carga e descarga das baterias dos veículos em momentos convenientes. Nos instantes em que se observam picos de consumo na rede, devido a um aumento da demanda, veículos que se encontram estacionados podem funcionar como fontes de energia, fornecendo carga através das baterias à rede, operação conhecida na literatura como V2G (*Vehicle to Grid*) [Garcia-Valle e Lopes, 2012] e assim

suavizando os picos de consumo e aliviando a geração das fontes tradicionais de energia. Nos momentos em que o consumo total de energia cai, geralmente à noite, e quando a maioria dos veículos se encontra estacionada nas residências, faz-se o carregamento das baterias, operação conhecida como G2V (*Grid to Vehicle*). Acrescenta-se a esse novo paradigma o fato de a tarifação de energia apresentar diferenciações no preço em relação ao horário do dia, incentivando o consumidor a drenar energia da rede em horários em que a tarifa encontra-se a preços módicos e possibilitando também a venda de energia à rede elétrica nos momentos em que a rede elétrica encontra-se sob picos de consumo de energia. Várias propostas surgem no intuito de promover a comunicação entre veículos elétricos e a rede no sentido de gerenciar e controlar os processos de carga (G2V) e descarga (V2G). Uma proposta em veículos inteligente é o controle em que a comunicação não envolve diretamente o proprietário do veículo e a rede, surgindo entre estes a figura de um intermediador denominado agregador, entidade com a função de agrupar e controlar um grande grupo de veículos [Erietta et al., 2011]. O agregador surge com a funcionalidade de controlar de forma inteligente as operações de carga de bateria de um grupo de veículos elétricos (operação G2V) e no fluxo inverso, do grupo de veículos à rede (operação V2G). A Figura 3.18 ilustra a arquitetura com o agregador que é a entidade entre o veículo e a rede e com enlace de comunicação com o operador da rede elétrica, conhecido como centro de controle. Essa arquitetura se encarrega de estabelecer um sistema de comunicação capaz de conduzir informação e sinais de controle entre os veículos elétricos e o agregador e entre este último e o centro de controle. A Figura 3.18 ilustra a arquitetura com o agregador. O agregador é a entidade entre o veículo e a rede e com enlace de comunicação com o operador da rede elétrica, conhecido como centro de controle. Essa arquitetura se encarrega de estabelecer um sistema de comunicação capaz de conduzir informação e sinais de controle entre os veículos elétricos e o agregador e entre este último e o centro de controle. Nos últimos anos surgiram várias tecnologias de comunicação sem fio que possibilitam o emprego na comunicação entre as entidades descritas. Dois diferentes protocolos são propostos para a comunicação, o IEEE 802.16d-Fixed WiMax, para o enlace entre o centro de controle e o agregador, e o IEEE 802.11p para comunicação entre o agregador e os veículos elétricos [Erietta et al., 2011]. O WiMax possibilita o uso eficiente da banda numa ampla faixa de frequências e pode ser usado também como uma solução para internet de banda larga. Já o IEEE802.11p vem sendo muito usado na indústria automobilística principalmente na categoria de veículos de luxo como ferramenta importante em serviços de prevenção de colisão e frenagem de emergência. O IEEE 802.11p possibilita a comunicação entre os veículos elétricos e o agregador.

O centro de controle pode ser encarado como o Operador do Sistema de Distribuição (OSD) ou o Operador do Sistema de Transmissão (OST). É vantajoso que a comunicação que ocorre entre o centro de controle e o agregador permita ao primeiro delegar a este último as funções de tarifação aos veículos. Vale ressaltar que os agregadores atuam em um ambiente competitivo e ofereceria incentivos aos consumidores (veículos elétricos) às operações V2G ou G2V. Assim, os veículos elétricos responderiam proporcionalmente de acordo com suas necessidades de carga ou descarga de baterias. A comunicação entre agregador e veículos tem requisitos cruciais:

- Baixa latência - os veículos devem ter resposta rápida aos comandos vindos (envi-

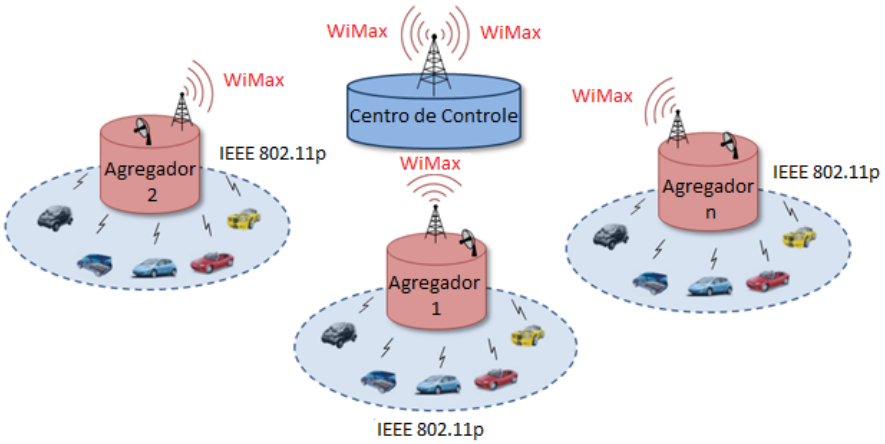


Figura 3.18. Agregador como um agente intermediário entre o centro de controle e os veículos elétricos.

ados) do (ao) centro de controle e encaminhados pelo (ao) agregador para que se associem ao posto de carga para operação V2G (G2V);

- Rápida autenticação e criptografia – devido à velocidade (mobilidade) dos veículos e o alcance de comunicação limitado, torna-se premente a necessidade de troca rápida de informações de autenticação e dados de forma eficaz e segura;

- Banda larga – devido ao grande número de veículos que podem estar conectados ao agregador, um grande volume de dados pode ser observado nos momentos de maior atividade;

- Interoperabilidade – os investimentos em infraestrutura de carga/descarga só trarão retorno se as interfaces de conexão e protocolos de troca de dados estiverem bem definidos.

Com a integração de veículos elétricos à rede elétrica há uma constante preocupação na previsão do número e os perfis de consumo de carga destes em relação aos horários do dia. Nos horários de maior consumo, a rede encontra-se sob grande possibilidade de congestionamento logo, se houver alguma ferramenta capaz de executar algum tipo de previsão em relação à quantidade de veículos que irá se conectar à rede e seus perfis de consumo, isso irá fornecer subsídios para que a central de controle possa antecipar cenários auxiliando no processo de produção de energia. É necessário considerar ainda que a tarifa de energia influenciará o processo de carga, proporcionando ao proprietário do veículo que opte pelo consumo nos horários de menor pico de energia e incentivando a venda de energia nos horários de maior pico. Uma proposta de otimização dos horários de carga de veículos elétricos baseia-se em um modelo de previsão baseado na estatística das chegadas dos veículos elétricos nos pontos de carga, baseado em teoria de filas [Mahnoosh Alizadeh, 2011]. O modelo adotado define 2 cenários: o primeiro, menos realista, considera que os veículos serão sempre atendidos pelos pontos de carga,

o modelo adotado no modelo de filas é o de infinitos servidores, ou seja, todo veículo que chega à rede será atendido. Com base na quantidade de veículos que chega aos pontos de carga, podemos aferir o grau de consumo de energia no momento t_i, o que permite prever o consumo do momento t_{i+1}. O segundo modelo, mais realista em relação ao primeiro, considera que os veículos podem se conectar a rede optando por consumir energia de fontes renováveis ou de fontes tradicionais. Nesse caso o modelo de infinitos servidores não se aplica mais. Em cada momento é previsto o grau de congestionamento do sistema e, no momento em que for verificado esse estado, o controle de operação do sistema envia mensagens a todos os veículos que não podem ser atendidos naquele momento para que optem carregar seus veículos em outro momento.

3.4.4. Plataforma de Teste para Redes Elétricas Inteligentes

A análise, a simulação e a experimentação de propostas de redes de comunicação para redes elétricas inteligentes é um desafio, pois depende de equipamentos especializados, diferentes pilhas de protocolos específicas. No caso específico da experimentação, esta atividade é essencial mas requer uma dispendiosa infraestrutura de rede de comunicação que reflita aproximadamente a vasta área coberta e o grande número de nós da rede elétrica inteligente.

Lu, Wang e Ma propõem uma infraestrutura de testes para redes elétricas inteligentes baseada em uma rede de comunicação Ethernet local (LAN) ou em uma rede sem fio local (WLAN) [Xiang et al., 2013]. O sistema proposto, chamado *Green Hub*, objetiva demonstrar a viabilidade de implementação prática de protocolos de comunicação de redes elétricas inteligentes em microrredes. A infraestrutura de testes é composta por equipamentos elétricos ligados a um controlador e cada controlador é conectado à rede de controle definida sobre uma rede local Ethernet. Coletando os dados gerados pelos controladores, há um centro de controle, representado por um computador portátil conectado à rede, que coleta os dados dos equipamentos elétricos e mostra em tempo real. A comunicação entre os controladores dos equipamentos elétricos e o centro de controle é realizada pelo protocolo DNP3. Para tanto, foi usada uma implementação aberta desse protocolo disponível na Internet [Green Energy, 2013]. No entanto, os experimentos realizados no *Green Hub* estão limitados a uma rede local e, assim, não permite que o mesmo centro de controle colete dados de um controlador remoto em outra rede local.

SmartGridLab é uma infraestrutura de testes para redes elétricas inteligentes composta por quatro componentes básicos, fornecedores de energia, consumidores de energia, uma rede de comunicação de medidores inteligentes de consumo de energia e um interruptor inteligente (*Intelligent Power Switch* - IPS) [Gang et al., 2010]. A experiência realizada contou com um gerador eólico e um painel solar como fornecedores de energia, enquanto os interruptores inteligentes e os medidores inteligentes foram desenvolvidos pelos autores. A rede de comunicação usada é uma rede em malha seguindo a especificação IEEE 802.15.4. Contudo, o SmartGridLab também se limita a comunicação local dos componentes e não prevê a comunicação em centros de controle.

Outra importante proposta de infraestrutura de testes para redes elétricas inteligentes, que avalia segurança, combina o uso de elementos elétricos com *software* de simulação para modelar subestações e centros de controle [Hahn et al., 2013]. Na in-

fraestrutura de testes, há uma subestação física, composta de unidades de terminais remotos (RTUs) dedicadas e conectadas a dispositivos elétricos inteligentes (IEDs), e outra subestação modelada por *software* de simulação [Digsilent, 2011]. O centro de controle foi criado usando servidores industriais do sistema SCADA. A rede de comunicação interna à subestação segue o padrão IEC 61850. Uma rede WAN simulada interconecta as duas subestações e o centro de controle. A simulação da rede WAN é realizada pelo *Internet-Scale Event and Attack Generation Environment* (ISEAGE) [Iowa Infas, 2011], que provê um ambiente compatível com a Internet para a realização de ataques virtuais. Para comunicações de longa distância, as subestações se comunicam com o centro de controle usando o protocolo DNP3 encapsulado sobre o IP. Contudo, como a rede de interconexão entre subestações é simulada pelo ISEAGE, não há trafego da Internet compartilhando o meio com o tráfego de controle e, portanto, o ambiente simulado não leva em consideração condições realísticas de atrasos na Internet.

Em termos de área de cobertura, escala e quantidade de equipamentos, os requisitos de uma rede de experimentação para redes elétricas inteligentes se aproximam daqueles encontrados para se testar novas propostas para a Internet do Futuro em um ambiente real. Um ambiente de teste baseado em redes virtuais pode ser uma solução desejável, pois é economicamente viável e funcionalmente segura. O Grupo de Teleinformática e Automação (GTA/UFRJ) possui experiência na aplicação do moderno conceito de virtualização de redes para a experimentação de redes de comunicação. O GTA participa do desenvolvimento do (*Future Internet Testbed with Security* - FITS) [Mattos et al., 2012][Guimarães et al., 2013], que é uma rede de testes interuniversitária para Internet do Futuro que provê isolamento entre as redes virtuais, segurança de acesso e diferenciação de qualidade de serviço. Este conceito de redes virtuais pode ser aplicado e também estendido em redes elétricas inteligentes. Uma proposta de experimentação de redes elétricas inteligentes é usar e estender a plataforma de experimentação FITS, para testar, avaliar e comparar os protocolos de comunicação e os elementos de controle em máquinas virtuais. Para testes de segurança uma plataforma de teste pode ser bastante útil para avaliar a efetividade e o impacto de um ataque e também a eficácia de uma solução de segurança.

Os protocolos de comunicação podem ser implementados em redes virtuais através de versões abertas disponíveis na Internet [Green Energy, 2013] e os centro de controle podem ser implementados através de versões abertas do sistema SCADA. Nós *gateway* do FITS interconectariam os elementos físicos de controle da rede elétrica, assim como a conexão de outros centros de controle físicos, por exemplo, uma implementação fora da rede virtual de um sistema SCADA. Os nós *gateway* conectam uma rede local a uma rede virtual que pode ser estendida através da Internet. Outra vantagem de realizar a experimentação da rede de comunicação das redes elétricas inteligentes sobre o FITS é que diversas propostas de rede de comunicação podem ser experimentadas concomitantemente de maneira isolada [Mattos e Duarte, 2012], ou seja, uma rede não é capaz de interferir nas outras.

3.4.5. Redes Virtuais e Redes Definidas por Software em Redes Elétricas Inteligentes

A tecnologia de redes virtuais desenvolvida no Grupo de Teleinformática e Automação (GTA) que é usada no FITS provê um ambiente de redes virtuais isoladas com

oferta de qualidade de serviço [Fernandes e Duarte, 2011, Mattos e Duarte, 2012]. Redes elétricas inteligentes podem se beneficiar dessa técnica que possibilita a coexistência de diversas redes isoladas e seguras sobre uma mesma infraestrutura física e que atendam as diferentes exigências e restrições dessa rede, como por exemplo, restrições como o atraso máximo para sistemas de controle, como redes isoladas para diferentes provedores de serviço, que é similar ao ambiente multi-inqulinos (*multitenant*), e privacidade para aplicações dos consumidores [Berger e Iniewski, 2012].

O sistema de comunicação de uma rede elétrica inteligente é um sistema complexo formado por diferentes tecnologias de redes e que envolve diferentes requisitos como um grande número de medidores, transferência confiável de um grande volume de dados para controle em tempo real e *hardware* e *software* heterogêneos. Gerenciar e prover segurança a um sistema de comunicação deste porte é um desafio [Xin et al., 2011]. A tecnologia de virtualização de redes permite que diferentes atores do sistema elétrico possam ter as suas próprias "fatias de rede" totalmente isoladas das demais fatias de rede dos demais atores participantes e também possam ser atendidos em demandas específicas de qualidade de serviço da comunicação, como por exemplo, tempo de latência máxima ou diferentes pilhas de protocolos sobre um mesmo substrato físico. Em Redes Elétricas Inteligentes, diversos tipos de organizações dividem uma mesma rede de comunicação, virtualização de redes vem como uma solução para problemas de isolamento e qualidade da comunicação. O baixo custo é a principal vantagem da tecnologia de redes virtuais. Esta tecnologia pode suportar diversas redes executando em paralelo em um mesmo *hardware* e totalmente isoladas uma das outras. Ou seja, mesmo usando o mesmo hardware, uma concessionária possui uma "fatia de rede" e não tem acesso nem aos dados nem ao tráfico das outras. Cada rede virtual tem os seus próprios elementos e arcabouço de controle e monitoramento exercidos por um ator como, por exemplo, uma concessionária, que detém o controle de determinada rede virtual. Além disso a tecnologia desenvolvida pelo GTA permite oferecer diferentes qualidades de serviço para as redes de diferentes atores. Esta mesma tecnologia de redes virtuais pode também ser testada como uma possível solução para um sistema de comunicação virtualizado em redes elétricas inteligentes. Pode-se imaginar o emprego de redes virtuais distintas em cima de um hardware *virtualizado*. A tecnologia de redes virtuais isoladas e com qualidade de serviço desenvolvida pelo GTA permite prover diferentes redes em cima de um mesmo elemento de rede.

Outra característica importante da tecnologia de redes desenvolvida pelo GTA e presente na plataforma de teste FITS é o controle de fluxos centralizado oferecido pela interface de programação de aplicação OpenFlow [McKeown et al., 2008] [Mattos et al., 2011][Pisa et al., 2010]. A centralização do controle de fluxos do OpenFlow pode ser um fator conveniente para se propor a rede de comunicações das mensagens de controle das redes elétricas inteligentes. A plataforma de teste FITS permite criar uma rede baseada em Ethernet inclusive com túneis que interligam "ilhas locais". Esta centralização permite o teste de propostas baseadas na tecnologia de redes definidas por *Software* (*Software Defined Network* - SDN) que permitem um enorme "agilidade" na configuração e reconfiguração da rede. Através da técnica de redes definidas por *software* é possível, de forma centralizada e muito rápida, reconfigurar os *firewalls* de toda a rede elétrica inteligente. A agilidade de configuração também pode ser um aliado importante

em eventos e em catástrofes, uma vez que o redirecionamento do fluxo pode ser feito em tempo *quase* real. A agilidade oferecida pelas redes definidas por *software* pode ser útil também para restringir ataques de segurança, principalmente os ataques de negação de serviço (DoS) pela filtragem das mensagens de DoS.

3.4.6. Computação em Nuvens para Redes Elétricas Inteligentes

A inclusão da comunicação e múltiplos dispositivos inteligentes em redes elétricas inteligentes causa um aumento exponencial dos dados gerados, processados e consumidos, ocasionados pela necessidade de coletar grandes massas de dados em tempo real e emitir comandos remotos. Cada serviço das redes elétricas inteligentes terá um requisito diferenciado de processamento e armazenamento de informações e que varia ao longo do tempo. Dessa maneira, o ambiente de computação em nuvens oferece as condições adequadas às redes elétricas inteligentes, pois são infraestruturas altamente escaláveis e flexíveis em relação a computação, armazenamento e conectividade [Carvalho e Duarte, 2012]. Assim, a escalabilidade e flexibilidade da computação em nuvens possibilitam o desenvolvimento de serviços com capacidade de gerenciar grandes massas de dados com baixos custos, adaptados às necessidades. Além disso, existe uma integração das informações, pois atores distintos acessam os mesmo dados, e geram dados que são consumidos por outros atores. Essa é mais uma motivação para o uso de computação em nuvens, que oferece serviços de compartilhamento e troca de informações de forma facilitada e econômica. Por fim, o uso de computação em nuvens facilita a terceirização de operação e manutenção da infraestrutura, o que permite prestadores de serviços focar em suas atividades e negócios [Fang et al., 2013].

O uso de computação em nuvens oferece uma infraestrutura para o gerenciamento de dados com recursos de armazenamento e processamento, que permite acesso ubíquo às informações garantindo a privacidade e confidencialidade. Usando computação em nuvens é possível replicar de forma consistente os dados em diferentes localidades, o que permite armazenamento próximo ao consumidor de dados para comunicação com baixa latência e aumenta a resiliência geral do sistema devido à replicação. Para suprir as demandas das redes elétricas inteligentes, a nuvem é composta de centros de dados de alta capacidade interconectados que possibilitam o gerenciamento eficiente de grandes massas de dados [Costa et al., 2012]. Além disso, o custo geral de uso de nuvem pode ser otimizado, pois existe uma diversidade de locais de armazenamento e processamento de dados com diferentes preços de operação e comunicação [Fang et al., 2013]. Os serviços das redes elétricas inteligentes são instalados na nuvem que expõe uma interface para enviar e obter dados [Rusitschka et al., 2010]. Assim, a nuvem permite a ampla disponibilidade de informações para que serviços de resposta à demanda possam executar algoritmos para incentivar consumidores economizar energia [Kim et al., 2011a].

A computação em nuvens das redes elétricas inteligentes pode fazer parte da própria infraestrutura da rede de comunicação [Kim et al., 2010]. Nesse modelo, os próprios elementos encaminhadores armazenam os dados, e uma interface de envio e obtenção de dados distribui os dados pelos elementos encaminhadores, o que garante a alta disponibilidade e eficiência de comunicação. O armazenamento de dados na rede pode ser estendido a Redes Orientadas a Informação (*Information Centric Network* - ICN) [de Brito et al., 2013], que permite esquema de endereçamento orientado a nome dos

dados, comunicação eficiente e armazenamento distribuído na rede [Torres et al., 2013], [Guimarães et al., 2013].

3.5. Conclusão e Perspectivas Futuras

As redes elétricas inteligentes são uma promessa de maior eficiência e confiabilidade, graças à incorporação de tecnologias de comunicação e informação às redes elétricas tradicionais. Com a infraestrutura avançada de medição baseada nas redes de comunicação e medidores inteligentes, as concessionárias terão acesso remoto a dados de consumo em tempo *quase* real. Assim, podem-se combater perdas não técnicas ("gatos") de forma mais eficaz e possibilitar previsões de demanda mais precisas. Do ponto de vista do consumidor, os medidores inteligentes permitirão maior conhecimento sobre o seu perfil de consumo e escolha dos horários mais convenientes para ligar aparelhos e consumir energia, de acordo com diferentes tarifas ao longo do dia, ou de que fontes geradoras está produzindo a energia. O usuário pode inclusive comandar à distância o acionamento/desligamento de aparelhos domésticos. Do ponto de vista da geração, transmissão e distribuição de energia, a infraestrutura de comunicação disponível nas redes elétricas inteligentes permite maior confiabilidade porque os dados sensoriados e transmitidos através da rede de comunicação permitirão sistemas completamente automatizados de resposta a falhas da rede. Por outro lado, a agilidade trazida pela infraestrutura de comunicação permitirá também acomodar fontes de microgeração ao sistema elétrico. Fontes de energia renováveis, tais como a eólica ou a solar, tendem a produzir menos energia por unidade de geração que uma planta hidrelétrica ou nuclear, por exemplo. Assim, para gerar a mesma quantidade de energia são necessárias muito mais fontes, distribuídas na rede. A rede elétrica inteligente facilitará o planejamento da geração distribuída de energia. Mais ainda, a rede elétrica inteligente permitirá acomodar consumidores que podem também gerar energia, por exemplo, uma residência de praia com placas solares ou um pequeno gerador eólico pode entregar energia à rede quando sua produção ultrapassa a demanda da sua residência. A capacidade de comunicação da rede elétrica inteligente será necessária para coordenar estas novas fontes de consumo/geração, ou prosumidores.

A capacidade de comunicação das redes elétricas inteligentes traz enormes desafios relacionados à segurança. Mais além, surgem desafios relacionados à enorme quantidade de informação presente na rede elétrica inteligente que não existia na rede elétrica tradicional, além de importantes novos componentes, as fontes de energia renováveis e os veículos elétricos. Além das questões relacionadas à segurança da informação, inerentes aos protocolos de comunicação, a segurança em redes elétricas inteligentes é um desafio mais crítico. A inserção de informação falsa na rede poderia, por exemplo, simular falhas que não ocorreram, enganando o sistema e levando ao acionamento do sistema de proteção e desligamento de parte da rede elétrica de geração, produzindo um apagão. Este tipo de ataque permite até o terrorismo à distância. Em menor escala, a quantidade de informação disponível da rede elétrica inteligente pode também ser usada de forma maliciosa. Por exemplo, a privacidade do consumidor pode ser violada se um terceiro obtiver acesso aos seus dados pessoais de consumo de energia elétrica. A proteção da informação e autenticação dos comandos nas redes elétricas inteligentes constituem portanto um desafio muito importante.

Além da segurança, a capacidade de comunicação e sensoriamento nas redes

elétricas inteligentes se traduz na disponibilidade de enormes massas de dados, que constituem desafios em termos de transmissão, armazenamento e análise de forma a que a informação possa ser utilizada em benefício de empresas e consumidores. Por outro lado, o advento das redes elétricas é acompanhado de novos atores importantes no sistema: além das fontes de energia renováveis, os veículos elétricos também geram desafios. Veículos elétricos são mais "limpos" do ponto de vista energético, mais eficientes que veículos movidos a motores a combustão, no entanto, no momento em que a adoção de veículos elétricos for massiva eles próprios constituirão novos desafios. A frota de veículos elétricos se tornará uma fonte de consumo significativa. Por outro lado, as baterias dos veículos elétricos podem atuar como elementos de armazenamento de energia da rede elétrica inteligente. O planejamento da geração e consumo de energia nas redes elétricas inteligentes do futuro deve levar em conta os veículos elétricos.

Finalmente, fica claro que modelos de simulação, experimentação e testes são fundamentais para a pesquisa e desenvolvimento de novos mecanismos que solucionem os desafios das redes elétricas inteligentes. Novos modelos matemáticos e de simulação são necessários para entender o comportamento da rede elétrica com novas fontes de geração distribuída e elementos que podem se comportar ora como consumidor ora como produtor de energia. A autenticação por microcontrolador seguro e proposta de redes definidas por *software* devem ser tecnologias chaves a serem utilizadas. A própria infraestrutura de comunicação deverá lidar com um número e variedade maior de atores, em um cenário futurista o consumidor poderia até escolher de que fornecedor comprar a energia elétrica. Assim, não somente como meio de testar novos protocolos de comunicação em uma mesma infraestrutura compartilhada, mas também como ferramenta em que a infraestrutura pode ser compartilhada de forma isolada entre diferentes fornecedores de serviços, a virtualização torna-se uma ferramenta importante para a pesquisa e desenvolvimento em redes elétricas inteligentes.

Referências

[ANEEL, 2012] ANEEL (2012). *Informações Gerenciais*. Agéncia Nacional de Energia Elétrica, http://www.aneel.gov.br/arquivos/PDF/Z_IG_Dez12.pdf. Acessado em março de 2013.

[Barroso et al., 2010] Barroso, L. A., Rudnick, H., Sensfuss, F. e Linares, P. (2010). The green effect. *Power and Energy Magazine, IEEE*, 8(5):22–35.

[Bartoli et al., 2010] Bartoli, A., Hernandez-Serrano, J., Soriano, M., Dohler, M., Kountouris, A. e Barthel, D. (2010). Secure losless aggregation for smart grid M2M networks. Em *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, p. 333–338.

[Baumeister, 2011] Baumeister, T. (2011). Adapting PKI for the smart grid. Em *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, p. 249–254.

[Beaver et al., 2002] Beaver, C., Gallup, D., Neumann, W. e Torgerson, M. (2002). Key management for SCADA. Relatório técnico, Cryptog. Information Sys. Security Dept., Sandia Nat. Labs, Tech. Rep. SAND2001-3252.

[Berger e Iniewski, 2012] Berger, L. T. e Iniewski, K. (2012). *Smart Grid: Applications, Communications and Security*. Wiley.

[Bernhard et al., 2010] Bernhard, J., Carl, B., Olle, S. e Dieter, G. (2010). Architeture and communication of an electric vehicle virtual power plant. Em *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, p. 149–154.

[Bialek, 2007] Bialek, J. W. (2007). Why has it happened again? comparison between the UCTE blackout in 2006 and the blackouts of 2003. Em *IEEE Power Tech, Lausanne*, p. 51–56.

[Borges, 2012] Borges, C. L. T. (2012). An overview of reliability models and methods for distribution systems with renewable energy distributed generation. *Renewable & Sustainable Energy Reviews*, 16(6):4008–4015.

[Borges e Cantarino, 2011] Borges, C. L. T. e Cantarino, E. (2011). Microgrids reliability evaluation with renewable distributed generation and storage systems. Em *IFAC World Congress*, volume 18, p. 11695–11700.

[Câmara, 2011] Câmara, S. (2011). Uma arquitetura de segurança para medidores inteligentes - verificação prática de dados de energia multitarifada. Dissertação de mestrado, Universidade Federal do Rio de Janeiro.

[Carvalho e Duarte, 2012] Carvalho, H. E. T. e Duarte, O. C. M. B. (2012). VOLTAIC: volume optimization layer to assign cloud resources. Em *Proceedings of the 3rd International Conference on Information and Communication Systems*, ICICS'12, p. 3:1–3:7, Irbid, Jordânia. ACM.

[Cavoukian et al., 2010] Cavoukian, A., Polonetsky, J. e Wolf, C. (2010). SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society*, 3(2):275–294.

[Chakraborty et al., 2012] Chakraborty, S., Raghavan, K. R., Srivastava, M. B., Bisdikian, C. e Kaplan, L. M. (2012). Balancing value and risk in information sharing through obfuscation. Em *15th International Conference on Information Fusion (FUSION)*, p. 1615–1622.

[Chokhani e Ford, 2003] Chokhani, S. e Ford, W. (2003). *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. Network Working Group, RFC 3647.

[CIB, 2013] CIB (2013). *Cidade Inteligente Búzios (CIB)*. Ampla, http://www.cidadeinteligentebuzios.com.br. Acessado em março de 2013.

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

[Costa et al., 2012] Costa, L. H. M. K., Amorim, M. D., Campista, M. E. M., Rubinstein, M. G., Florissi, P. e Duarte, O. C. M. B. (2012). Grandes massas de dados na nuvem: Desafios e técnicas para inovação. Em *SBRC 2012*, Ouro Preto, MG, Brazil.

[CRO, 2011] CRO (2011). *Power Blackout Risks, Risk Management Options*. Chief Risk Officers (CRO), http://www.thecroforum.org/. Acessado em março de 2013.

[Dawson et al., 2006] Dawson, R., Boyd, C., Dawson, E. e Nieto, J. M. G. (2006). SKMA: A Key management architecture for SCADA systems. Em *Proceedings of Australasian workshops on Grid computing and e-research*, volume 54 of *ACSW Frontiers'06*, p. 183–192, Darlinghurst, Austrália. Australian Computer Society, Inc.

[de Brito et al., 2013] de Brito, G. M., Velloso, P. B. e Moraes, I. M. (2013). *Information Centric Networks: A New Paradigm for the Internet*. Wiley-ISTE.

[Digsilent, 2011] Digsilent (2011). *Power Factory Software*. Digsilent GmbH, http://www.digsilent.de/. Acessado em março de 2013.

[Donghyun et al., 2009] Donghyun, C., Hakman, K., Dongho, W. e Seungjoo, K. (2009). Advanced Key-management architecture for secure SCADA communications. *IEEE Transactions on Power Delivery*, 24(3):1154–1163.

[Donghyun et al., 2010] Donghyun, C., Sungjin, L., Dongho, W. e Seungjoo, K. (2010). Efficient secure group communications for SCADA. *IEEE Transactions on Power Delivery*, 25(2):714–722.

[Eletropaulo, 2013] Eletropaulo (2013). *Smart Grid AES Eletropaulo*. AES Eletropaulo, http://www.aeseletropaulo.com.br. Acessado em março de 2013.

[Erietta et al., 2011] Erietta, I. Z., George, C. K., Nikolaos, D. H. e Nikolaos, K. U. (2011). An evaluation study of wireless access technologies for V2G communications. Em *IEEE 16th International Conference on Intelligent System Application to Power Systems (ISAP)*, p. 1–7.

[Falcão, 2010] Falcão, D. M. (2010). Integração de tecnologias para viabilização da smart grid. *III Simpósio Brasileiro de Sistemas Elétricos*, p. 1–5.

[Falk, 2008] Falk, H. (2008). Securing IEC 61850. Em *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, p. 1–3.

[Fang et al., 2013] Fang, X., Yang, D. e Xue, G. (2013). Evolving smart grid information management cloudward: A cloud optimization perspective. *IEEE Transactions on Smart Grid*, 4(1).

[Fernandes e Duarte, 2011] Fernandes, N. C. e Duarte, O. C. M. B. (2011). Provendo isolamento e qualidade de serviço em redes virtuais. *XXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC*, p. 1–14.

[Ferraz, 2011] Ferraz, L. H. G. (2011). Um mecanismo de exclusão acurado e preciso baseado em confiança para controle de acesso em redes ad hoc. Dissertação de mestrado, Universidade Federal do Rio de Janeiro.

[Fouda et al., 2011] Fouda, M. M., Fadlullah, Z. M., Kato, N., Lu, R. e Shen, X. (2011). A lightweight message authentication scheme for smart grid communications. *IEEE Transactions on Smart Grid*, 2(4):675 – 685.

[Gang et al., 2010] Gang, L., De, D. e Wen-Zhan, S. (2010). Smartgridlab: A laboratory-based smart grid testbed. Em *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, p. 143–148.

[Gao et al., 2013] Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., Liang, W. e Philip Chen, C. L. (2013). SCADA communication and security issues. *Security and Communication Networks*.

[Garcia-Valle e Lopes, 2012] Garcia-Valle, R. e Lopes, J. A. P. (2012). *Electric Vehicle Integration into Modern Power Networks*. Springer.

[Gilchrist, 2008] Gilchrist, G. (2008). Secure authentication for DNP3. Em *IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, p. 1–3. IEEE.

[Gomes et al., 2004] Gomes, P., Siqueira de Lima, A. C. e Guarin, A. d. P. (2004). Guidelines for power system restoration in the brazilian system. *IEEE Transactions on Power Systems*, 19(2):1159–1164.

[Gomez, 2002] Gomez, J. A. (2002). *Survey of SCADA Systems and Visualization of a Real Life Process*. PhD thesis, Tekniska Högskolan Linköping Universitet.

[Green Energy, 2013] Green Energy (2013). *Distributed Network Protocol 3*. Green Energy Corporation, https://code.google.com/p/dnp3/. Acessado em março de 2013.

[Guimarães, 2012] Guimarães, P. H. V. (2012). Arquitetura de gerenciamento de identidades usando OpenID e cartoes inteligentes. Relatório técnico.

[Guimarães et al., 2013] Guimarães, P. H. V., Ferraz, L. H. G., Torres, J. V., Mattos, D. M. F., Murillo P., A. F., Andreoni, M., Alvarenga, I. D., Rodrigues, C. S. C. e Duarte, O. C. M. B. (2013). Experimenting content-centric networks in the future internet testbed environment. *Aceito para publicação em IEEE International Conference on Communications (ICC)-Workshop on Cloud Convergence*.

[Gunther, 2011] Gunther, E. (2011). *Features and Benefits of IEC 61850*. Enernex, http://www.enernex.com/wp-content/uploads/2012/04/
Features-and-Benefits-of-IEC-61850_web.pdf. Acessado em março de 2013.

[Hahn et al., 2013] Hahn, A., Ashok, A., Sridhar, S. e Govindarasu, M. (2013). Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *Aceito para publicação em IEEE Transactions on Smart Grid*.

[Hoeper e Gong, 2006] Hoeper, K. e Gong, G. (2006). Key revocation for identity-based schemes in mobile ad hoc networks. Em Kunz, T. e Ravi, S., editors, *Ad-Hoc, Mobile, and Wireless Networks*, volume 4104 of *Lecture Notes in Computer Science*, p. 224–237. Springer Berlin Heidelberg.

[Housley et al., 2002] Housley, R., Polk, W., Ford, W. e Solo, D. (2002). *RFC3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Network Working Group, RFC 3280.

[IEC, 2007] IEC (2007). *Power Systems Management and Associated Information Exchange - Data and Communications Security*. International Electrotechnical Commission (IEC).

[IEC61850, 2010] IEC61850 (2010). IEC61850: Communication networks and systems in substation. *International Electrotechnical Commission IEC-61850*, p. 1–1316.

[IEEE1815, 2012] IEEE1815 (2012). IEEE1815: IEEE standard for electric power systems communications - distributed network protocol (DNP3). *IEEE P1815.1/D4.00*, p. 1–775.

[Igure et al., 2006] Igure, V. M., Laughter, S. A. e Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, 25(7):498–506.

[INL, 2001] INL (2001). Vulnerability analysis of energy delivery control systems. Relatório técnico, Idaho National Laboratory INL, Tech. Rep. INL/EXT-10-18381.

[Iowa Infas, 2011] Iowa Infas (2011). *Internet-Scale Event and Attack Generation Environment*. Iowa State University Information Assurance Center InfAs, https://www.iac.iastate.edu/wiki/ISEAGE. Acessado em março de 2013.

[Jøsang et al., 2005] Jøsang, A., Fabre, J., Hay, B., Dalziel, J. e Pope, S. (2005). Trust requirements in identity management. Em *Proceedings of Australasian workshop on Grid computing and e-research*, volume 44, p. 99–108. Australian Computer Society, Inc.

[Khalifa et al., 2011] Khalifa, T., Naik, K. e Nayak, A. (2011). A survey of communication protocols for automatic meter reading applications. *IEEE Communications Surveys & Tutorials*, 13(2):168–182.

[Khurana et al., 2010] Khurana, H., Hadley, M., Ning, L. e Frincke, D. A. (2010). Smart-grid security issues. *IEEE Security Privacy*, 8(1):81–85.

[Kim et al., 2011a] Kim, H., Kim, Y. J., Yang, K. e Thottan, M. (2011a). Cloud-based demand response for smart grid: Architecture and distributed algorithms. Em *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, p. 398–403. IEEE.

[Kim et al., 2011b] Kim, Y., Ngai, E. C. e Srivastava, M. B. (2011b). Cooperative state estimation for preserving privacy of user behaviors in smart grid. Em *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, p. 178–183.

[Kim et al., 2010] Kim, Y.-J., Thottan, M., Kolesnikov, V. e Lee, W. (2010). A secure decentralized data-centric information infrastructure for smart grid. *IEEE Communications Magazine*, 48(11):58–65.

[Klein, 2009] Klein (2009). A secure IEC-61850 toolkit for utility automation. Em *Conference For Homeland Security. CATCH'09. Cybersecurity Applications Technology*, p. 245–250.

[Kondoh, 2011] Kondoh, J. (2011). Direct load control for wind power integration. Em *Power and Energy Society General Meeting*, p. 1–8. IEEE.

[Laufer et al., 2011] Laufer, R. P., Velloso, P. B. e Duarte, O. C. M. B. (2011). A generalized bloom filter to secure distributed network applications. *Computer Networks*, 55(8):1804 – 1819.

[Leite et al., 2006] Leite, A. P., Borges, C. L. T. e Falcão, D. M. (2006). Probabilistic wind farms generation model for reliability studies applied to brazilian sites. *IEEE Transactions on Power Systems*, 21(4):1493–1501.

[Light, 2010] Light (2010). *Light participa de Operação Caça-Furto da Polícia Civil em Jacarepaguá*. Light S.A., http://www.light.com.br/web/aplicacoes/news/institucional/tenoticiasview.asp?mid=8687942772327225&id=6561803D&categoria=6561803D. Acessado em março de 2013.

[Ma et al., 2013] Ma, R., Chen, H. H., Huang, Y. R. e Meng, W. (2013). Smart grid communication: Its challenges and opportunities. *IEEE Transactions on Smart Grid*, 4(1).

[Mahalanobis, 2005] Mahalanobis, A. (2005). *Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups*. PhD thesis, Florida Atlantic University Boca Raton, Florida.

[Mahnoosh Alizadeh, 2011] Mahnoosh Alizadeh, Anna Scaglione, R. J. T. (2011). Direct load management of electric vehicles. Em *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, p. 5964 – 5967.

[Majdalawieh et al., 2006] Majdalawieh, M., Parisi-Presicce, F. e Wijesekera, D. (2006). DNPSec: Distributed network protocol version 3 DNP3 security framework. *Advances in Computer, Information, and Systems Sciences, and Engineering*, p. 227–234.

[Mao et al., 2005] Mao, A., Yu, J. e Guo, Z. (2005). PMU placement and data processing in WAMS that complements SCADA. Em *IEEE Power Engineering Society General Meeting*, volume 1, p. 780–783.

[Marris, 2008] Marris, E. (2008). Energy: Upgrading the grid. *Nature, International weekly journal of science*, 454:570–573.

[Martins e Borges, 2011] Martins, V. F. e Borges, C. L. T. (2011). Active distribution network integrated planning incorporating distributed generation and load response uncertainties. *IEEE Transactions on Power Systems*, 26(4):2164–2172.

[Mattos e Duarte, 2012] Mattos, D. M. F. e Duarte, O. C. M. B. (2012). QFlow: Um sistema com garantia de isolamento e oferta de qualidade de serviço para redes virtualizadas. Em *XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC*.

[Mattos et al., 2011] Mattos, D. M. F., Fernandes, N. C., da Costa, V. T., Cardoso, L. P., Campista, M. E. M., Costa, L. H. M. K. e Duarte, O. C. M. B. (2011). OMNI: Openflow management infrastructure. Em *International Conference on the Network of the Future (NOF)*, p. 52–56. IEEE.

[Mattos et al., 2012] Mattos, D. M. F., Mauricio, L. H., Cardoso, L. P., Alvarenga, I. D., Ferraz, L. H. G. e Duarte, O. C. M. B. (2012). Uma rede de testes interuniversitária a com técnicas de virtualizacao híbridas. *Salão de Ferramentas do XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos-SBRC*.

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

[McKeown et al., 2008] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S. e Turner, J. (2008). OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74.

[McLaughlin et al., 2010] McLaughlin, S., Podkuiko, D. e McDaniel, P. (2010). Energy theft in the advanced metering infrastructure. *Critical Information Infrastructures Security*, p. 176–187.

[Mo et al., 2012] Mo, Y., Huyn-Jin, Kim, T., Brancik, K., Dickinson, D., Lee, H., Perrig, A. e Sinopoli, B. (2012). Cyber-physical security of a smart grid infrastructure. *IEEE Proceedings*, 100(1):195–209.

[Molina e Mercado, 2011] Molina, M. G. e Mercado, P. E. (2011). Power flow stabilization and control of microgrid with wind generation by superconducting magnetic energy storage. *IEEE Transactions on Power Electronics*, 26(3):910–922.

[Moreira et al., 2010] Moreira, M. D. D., Laufer, R. P., Fernandes, N. C. e Duarte, O. C. M. B. (2010). Uma técnica de rastreamento sem estado para identificar a origem de ataques a partir de um único pacote. Em *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSEG 2010*.

[Moreira et al., 2012] Moreira, M. D. D., Laufer, R. P., Velloso, P. B. e Duarte, O. C. M. B. (2012). Capacity and robustness tradeoffs in bloom filters for distributed applications. *IEEE Transactions on Parallel and Distributed Systems*, 23(12):2219–2230.

[Morris et al., 2012] Morris, T. H., Pan, S. e Adhikari, U. (2012). Cyber security recommendations for wide area monitoring, protection, and control systems. Em *IEEE Power and Energy Society General Meeting*, p. 1–6.

[Mármol et al., 2012] Mármol, F. G., Sorge, C., Ugus, O. e Perez, G. M. (2012). Do not snoop my habits: Preserving privacy in the smart grid. *IEEE Communications Magazine*, 50(5):166–172.

[Myers et al., 1999] Myers, M., Ankney, R., Malpani, A., Galperin, S. e Adams, C. (1999). *X.509 Internet Public Key infrastructure online certificate status protocol-OCSP*. Network Working Group, RFC 2560.

[NIST2013, 2013] NIST2013 (2013). *Smart Grid Home page*. http://www.nist.gov/smartgrid/index.cfm. Acessado em março de 2013.

[NIST7628, 2010a] NIST7628 (2010a). NIST7628-guidelines for smart grid cyber security vol. 1, smart grid cyber security strategy, architecture, and high-level requirements. National Institute of Standards and Technology (NIST).

[NIST7628, 2010b] NIST7628 (2010b). NIST7628-guidelines for smart grid cyber security: Vol. 2, privacy and the smart grid. National Institute of Standards and Technology (NIST).

[ONS, 2013] ONS (2013). *Sistema Interligado Nacional*. Operador Nacional do Sistema Elétrico (ONS), http://www.ons.org.br/home/. Acessado em março de 2013.

[PG&E, 2013] PG&E (2013). *Demand Response: Programs for Business to Save Money and Help California Meet Energy Demand*. Pacific Gas and Electric Company, http://www.pge.com/mybusiness/energysavingsrebates/demandresponse/. Acessado em março de 2013.

[Pisa et al., 2010] Pisa, P. S., Fernandes, N. C., Carvalho, H. E. T., Moreira, M. D. D., Campista, M. E. M., Costa, L. H. M. K. e Duarte, O. C. M. B. (2010). Openflow and xen-based Virtual network migration. Em *Communications: Wireless in Developing Countries and Networks of the Future*, p. 170–181. Springer.

[PNSGD, 2013] PNSGD (2013). *The Pacific Northwest Smart Grid Demonstration Project*. Pacific Northwest, http://www.pnwsmartgrid.org/. Acessado em março de 2013.

[Quinn, Elias Leake, 2009] Quinn, Elias Leake (2009). *Smart Metering and Privacy: Existing Laws and Competing Policies*. http://ssrn.com/abstract=1462285. Acessado em março de 2013.

[Rikiya, 2010] Rikiya, A. (2010). Digital grid: Communicative electrical grids of the future. Em *Innovative Smart Grid Technologies Conference Europe (ISGT Europe)*, p. 1–8.

[Ruiz et al., 2009] Ruiz, N., Cobelo, I. e Oyarzabal, J. (2009). A direct load control model for virtual power plant management. *IEEE Transactions on Power Systems*, 24(2):959–966.

[Rusitschka et al., 2010] Rusitschka, S., Eger, K. e Gerdes, C. (2010). Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain. Em *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, p. 483–488. IEEE.

[Sauter e Schwaiger, 2002] Sauter, T. e Schwaiger, C. (2002). Achievement of secure internet access to fieldbus systems. *Microprocessors and Microsystems*, 26(7):331–339.

[SGL, 2013] SGL (2013). *Programa Smart Grid Light*. Light S.A., http://www.smartgridlight.com.br. Acessado em março de 2013.

[So et al., 2010] So, H. K. H., Kwok, S. H. M., Lam, E. Y. e Lui, K.-S. (2010). Zero-configuration identity-based signcryption scheme for smart grid. Em *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, p. 321 –326.

[Sorebo e Echols, 2012] Sorebo, G. N. e Echols, M. C. (2012). *Smart Grid Security: An End-to-End View of Security in the New Electrical Grid*. CRC Press.

[Steffen et al., 2010] Steffen, F., Hans, J. H. e Maik, S. (2010). Enhancing IEC-62351 to improve security for energy automation in smart grid environments. Em *Fifth International Conference on Internet and Web Application Services*.

[TCIPG, 2013] TCIPG (2013). *Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)*. University of Illinois at Urbana-Champaign (UIUC), http://tcipg.org/. Acessado em março de 2013.

[Terzija et al., 2011] Terzija, V., Valverde, G., Cai, D., Regulski, P., Madani, V., Fitch, J., Skok, S., Begovic, M. M. e Phadke, A. (2011). Wide-area monitoring, protection, and control of future electric power networks. *Proceedings of the IEEE*, 99(1):80–93.

[Torres et al., 2013] Torres, J. V., Ferraz, L. H. G. e Duarte, O. C. M. B. (2013). Redes orientadas a conteúdo baseadas em controladores hierárquicos. Em *a ser publicadoXXXI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC*.

[US-CPSOTF, 2004] US-CPSOTF (2004). *Final Report on the August 14, 2003 Blackout in the United Stated and Canada: Causes and Recommendations*. U.S.-Canada Power System Outage Task Force, https://reports.energy.gov/BlackoutFinal-Web.pdf. Acessado em março de 2013.

[USDOE, 2008] USDOE (2008). *AMI System Security Requirements v1.01*. US Department of Energy (USDOE), http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-AMI_System_Security_Requirements_updated.pdf. Acessado em março de 2013.

[USFERC, 2012] USFERC (2012). *Assessment of Demand Response and Advanced Metering*. US Federal Energy Regulatory Commission (USFERC), http://www.ferc.gov/legal/staff-reports/12-20-12-demand-response.pdf. Acessado em março de 2013.

[Varodayan e Gao, 2010] Varodayan, D. P. e Gao, G. X. (2010). Redundant metering for integrity with information theoretic confidentiality. *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, p. 345–349.

[Velloso et al., 2010] Velloso, P. B., Laufer, R. P., Cunha, D. O., Duarte, O. C. M. B. e Pujolle, G. (2010). Trust management in mobile Ad Hoc networks using a scalable maturity-based model. *IEEE Transactions on Network and Service Management*, 7(3):172–185.

[Warmer et al., 2009] Warmer, C., Kok, K., Karnouskos, S., Weidlich, A., Nestle, D., Selzam, P., Ringelstein, J., Dimeas, A. e Drenkard, S. (2009). Web services for integration of smart houses in the smart grid. *Grid-Interop-The road to an interoperable grid, Denver, Colorado, USA*.

[Wenye et al., 2011] Wenye, W., Yi, X. e Mohit, K. (2011). A survey on the communication architectures in smart grid. *Computer Networks*, 55(15):3604–3629.

[Wenye e Zhuo, 2013] Wenye, W. e Zhuo, L. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371. Elsevier.

[WorldBank, 2009] WorldBank (2009). *Energy Strategy Approach Paper Annexes Sustainable Development Network*. Acessado em março de 2013.

[Wright et al., 2004] Wright, A. K., Kinast, J. A. e McCarty, J. (2004). Low-latency cryptographic protection for scada communications. Em Jakobsson, M., Yung, M. e Zhou, J., editors, *Applied Cryptography and Network Security*, volume 3089 of *Lecture Notes in Computer Science*, p. 263–277. Springer Berlin Heidelberg.

[Xiang et al., 2013] Xiang, L., Wenye, W. e Jianfeng, M. (2013). An empirical study of communication infrastructures towards the smart grid: Design, implementation, and evaluation. *IEEE Transactions on Smart Grid*, 4(1):170–183.

[Xin et al., 2011] Xin, Y., Baldine, I., Chase, J., Beyene, T., Parkhurst, B. e Chakrabortty, A. (2011). Virtual smart grid architecture and control framework. Em *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, p. 1–6. IEEE.

[Zima et al., 2005] Zima, M., Larsson, M., Korba, P., Rehtanz, C. e Andersson, G. (2005). Design aspects for wide-area monitoring and control systems. *Proceedings of the IEEE*, 93(5):980–996.