Smart Grid Security Applied to the Brazilian Scenario: A Visual Approach

Marcos Rogozinski, Rodrigo F. Calili

***Abstract*—Many countries are experiencing a transformation from the traditional generation power system into a smart grid which incorporates communication and data processing technologies. New services become possible and are important to improve the system operation, but there is a large increase in data gathering. This new paradigm increases the complexity of the network and brings new security issues. This article simplifies the understanding of security in power networks by surveying one** hundred and eight recent studies in smart grid security, mapping graphically the **type of risk they represent to their location in the smart grid, organizing them by the lifecycle of smart grid data as proposed by [1], and comparing the ideal case to the current Brazilian scenario.**

***Index Terms*—Security, Smart Grids**

I. Introdução

As redes de fornecimento de energia elétrica vem sofrendo uma grande mudança em todo o mundo com a implantação, principalmente, de medidores inteligentes de energia. Esses medidores podem medir o consumo em intervalos curtos de tempo, fazer medições mais abrangentes e ter a capacidade de armazenamento, processamento e transmissão de dados. Essas novas funcionalidades aliados aos dispositivos domésticos inteligentes, ao barateamento da geração de energia por fontes renováveis e à maior capacidade de armazenamento de energia por baterias e veículos elétricos transformam a tradicional rede elétrica, em que a energia flui de forma unidirecional dos grandes geradores de energia para o consumidor final, em uma rede mais complexa composta de provedores de energia de diversos tamanhos com energia e dados fluindo de forma bidirecional. Essa nova estrutura de rede, ainda em processo de formação em todo o mundo, pode ser chamada de Rede Elétrica Inteligente (REI).

A troca de dados entre os diversos participantes de uma REI cria a necessidade de uma complexa rede de telecomunicação e da padronização na troca de mensagens entre os diferentes atores conectados à rede. Múltiplos equipamentos são responsáveis por gerar, transmitir, receber, armazenar, processar e analisar dados. Assim, o controle sobre o acesso aos dados e à informação por ele gerada se torna crucial para o funcionamento da rede. Segundo [2], a comunicação entre equipamentos e o processamento dos dados assumem um papel tão importante quanto os elementos convencionais das redes de distribuição. É necessário, portanto, que a segurança de uma REI não seja vista somente do ponto de vista físico do fluxo de energia, mas de uma forma mais ampla, que possa abranger o novo fluxo de dados em todo o seu ciclo de vida.

O objetivo deste trabalho é organizar visualmente os temas que tratam de questões de segurança em uma REI com base no ciclo de vida dos dados na rede e vincular cada estágio desse ciclo de vida aos atores e respectivos equipamentos relacionados. Para cada tema trabalhado serão apresentados os riscos correspondentes e listados estudos que tratam de forma mais aprofundada cada tema.

Após a compilação de todos os temas relevantes, é apresentada uma representação visual do cenário atual da rede elétrica no Brasil, considerando os temas pertinentes. A partir desta figura é possível selecionar os estudos que podem contribuir para o estágio atual das redes elétricas neste país, comparando com estado ideal de um cenário de implantação de redes elétricas inteligentes.

Esse trabalho parte da organização das vulnerabilidades de uma REI a partir dos estágios do ciclo de vida dos dados na rede apresentados em [1].

Primeiramente, foram organizados visualmente todos os elementos de uma REI, sendo agrupados os principais tópicos de segurança com base nos estágios do ciclo de vida dos dados na rede. Cada tópico foi então vinculado com seu posicionamento na REI. Para o design deste esquema foram utilizados modelos propostos por [3] e [4].

A partir deste esquema, cada estágio é analisado e são listados estudos que tratam de suas vulnerabilidades, dos seus riscos, das possíveis soluções e dos processos que são impactados em caso de um cyber ataque.

Além desta introdução, na seção 2 é explicada a metodologia utilizada para a seleção dos estudos trabalhados. Na seção 3 é apresentado o conceito de ciclo de vida dos dados e é mostrada de forma visual a sua ligação com os diversos elementos de uma REI. Cada estágio do ciclo de vida dos dados é então detalhado com base em suas questões de segurança e são listados os estudos pertinentes a cada temática apresentada. Na seção 4 é apresentado o cenário brasileiro atual e a sua representação visual, possibilitando a comparação com a representação de uma REI feita na seção 3. Por fim, na seção 5, chega-se a conclusão do trabalho, fazendo a indicação de novos desdobramentos deste.

M. Rogozinski, Pontifícia Universidade Católica do Rio de Janeiro, RJ, Brasil (email: rogozinski@gmail.com).

R. F. Calili, Pontifícia Universidade Católica do Rio de Janeiro, RJ, Brasil (email: calili@puc-rio.br).

II. Metodologia

Para a compilação dos trabalhos constantes na literatura relacionada a cada tema de segurança, foi feita inicialmente a escolha de cinco surveys sobre segurança em REIs. Para a seleção desses artigos foi utilizada a base de dados Scopus com buscas pelos termos "survey AND smart AND grid AND (security OR attack OR issues)". Os artigos [1], [5], [6], [7] e [8] foram selecionados por serem os artigos mais recentes encontrados que tratavam especificamente de segurança em REIs. Com base nesses artigos, foi feita a categorização dos principais temas tratados em segurança de REIs e foram selecionados 108 dos estudos citados nos artigos que melhor representavam cada um desses temas.

III. O Ciclo de Vida dos Dados em uma REI

O ciclo de vida dos dados em uma REI é composto por quatro estágios sequenciais: geração, aquisição, armazenamento e processamento, podendo deste último ser separado o estágio de análise dos dados. Para esse estudo, será considerada a análise dos dados separadamente, a fim de visualizar mais facilmente os atores com que se relaciona e os ataques que lhe causam impacto, já que esse estágio pode ser muito importante como forma de tratar ou prevenir ataques à rede.

A Fig. 1 mostra os estágios do ciclo de vida dos dados de forma sequencial e divide cada estágio do ciclo nos seus tópicos mais relevantes. Cada tópico recebe uma cor que o relaciona com o estágio a que pertence e um código que será utilizado posteriomente na Fig. 2, Fig. 3 e na listagem de estudos para localizar o tópico dentro do esquema de uma REI. O estágio de geração de dados foi dividido pelo tipo de fonte geradora destes, o estágio de aquisição dos dados foi dividido pelo tipo de tecnologia utilizado e o estágio de processamento dos dados foi dividido pelo serviço influenciado, tendo o furto de energia influência sobre todos os serviços prestados.

A visualização das questões de segurança tendo como base o ciclo de vida dos dados em uma REI se torna interessante principalmente por explicitar o encadeamento de eventos em uma eventual falha do sistema. Entretanto, não se deve tomar essa sequência como fixa. O armazenamento, o processamento e a análise podem estar presentes em todos os pontos do ciclo de vida dos dados em uma REI. Um medidor inteligente, por exemplo, pode armazenar e processar os dados imediatamente após a sua geração, com o objetivo de trazer mais segurança aos dados antes da sua aquisição por outros equipamentos da rede.

A Fig. 2 mostra a estrutura de uma REI, detalhando o fluxo de energia, o fluxo dos dados, os atores, algumas das principais formas de comunicação, algumas das principais infraestruturas e tecnologias envolvidas. Além disso a localização dentro da rede dos principais estágios do ciclo de vida dos dados em uma REI é apresentada.

Os estágios foram subdivididos nos tópicos apresentados na Fig. 1 e posicionados no ponto ou pontos do fluxo de dados correspondentes à sua maior influência. O estágio de geração de dados, por exemplo, foi dividido pela fonte geradora dos dados e cada divisão ganhou um código de identificação (GE1, GE2, GE3 e GE4). Cada código foi posicionado no esquema da REI em seu local de geração mais provável. Foram considerados os principais pontos de cada fase do ciclo dos dados na rede, mas a variedade de locais em que poderiam ser indicados é imensa, devido a complexidade dessa rede. Não foram consideradas neste estudo as questões relacionadas à internet, pois apesar de possuir objetos em comum com os outros meios de comunicação utilizados na REI, já existe uma vasta literatura voltada especificamente para ela.

Nas subseções a seguir, cada um dos estágios do ciclo de vida dos dados (Fig. 1) serão apresentados, sendo separados por tema e autores, evidenciando em que fase da rede elétrica estes estudos foram feitos.

A. Geração de Dados

1) Considerações gerais sobre a geração dos dados: Em uma rede elétrica tradicional os dados de consumo são coletados mensalmente, em muitos casos ainda de forma presencial. Com a implantação de medidores inteligentes esses dados passam a ser gerados em intervalos de horas ou minutos, e além dos dados de consumo, outras informações podem ser produzidas, como o monitoramento de interrupções, o controle de reativos, o monitoramento da tensão e frequência da rede elétrica, a avaliação das distorções harmônicas entre outros [2]. Com o desenvolvimento dessa rede, surgem outros tipos de dados que passam a ganhar cada vez mais importância. Dispositivos domésticos inteligentes e carros elétricos passam a se comunicar com a rede principal gerando dados em tempo real. Diversos serviços passam a poder ser oferecidos pelos fornecedores de energia e por

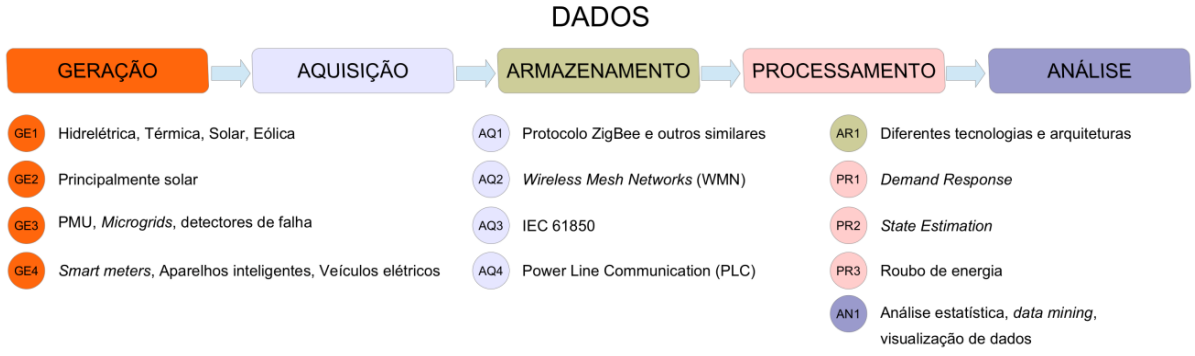

Fig. 1. O ciclo de vida dos dados e a subdivisão em tópicos para cada um dos seus estágios

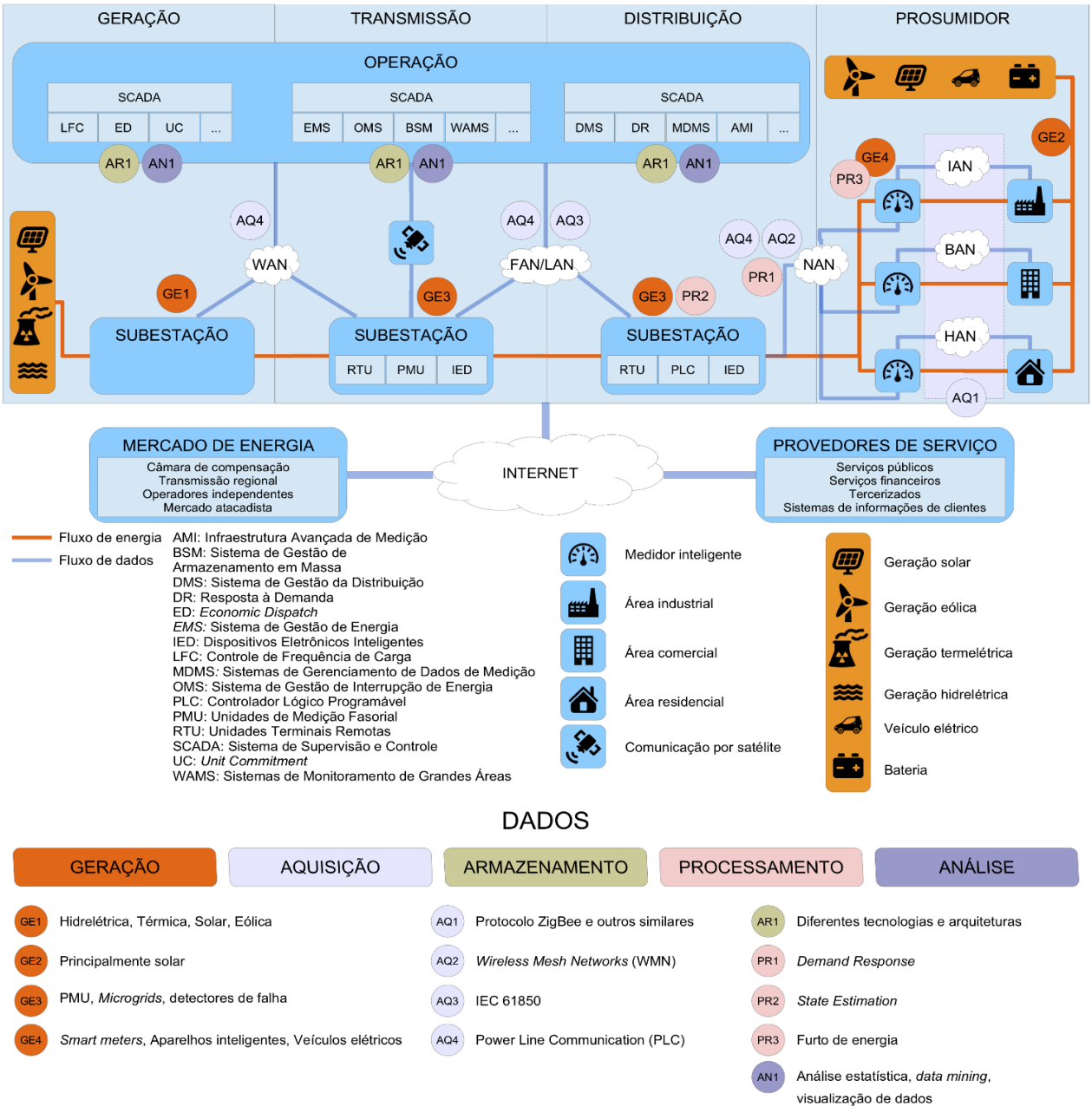

Fig. 2. Estrutura de uma REI com o fluxo de energia e fluxo de dados. Os círculos coloridos indicam o posicionamento dentro da rede de cada estágio do ciclo de vida dos dados e os principais temas de segurança vinculados

terceiros, incluindo o de previsão de demanda de energia, que necessita de dados externos como os meteorológicos, sociais e econômicos, e dados históricos e em tempo real da própria rede. Há, portanto, uma quantidade massiva e extremamente variada de dados gerados que passa a ter relevância e precisa ser considerada, principalmente pelo fato de que um dado que é alterado ou perdido em sua geração pode afetar todo o seu ciclo de vida e o de outros dados que dependem dele.

2) Riscos de segurança: Boa parte dos riscos de segurança vinculados à geração dos dados são atrelados à alterações e manipulações nos medidores de energia, sensores, unidades de medição fasorial (PMUs), sistemas de controle industrial etc. Essas alterações podem ocorrer de forma não intencional (como por exemplo, a influência climática e as falhas técnicas) ou por manipulação intencional dos equipamentos.

Uma outra categoria de riscos é vinculada com a manipulação na comunicação dos dados no momento da geração. Esses riscos incluem a interceptação de sinais de rádio, a falta de segurança na comunicação de PMUs via TCP/IP (*Transmission Control Protocol/Internet Protocol*), e a falta de segurança na comunicação de *microgrids* via IP (*Internet Protocol*).

É importante notar que nas redes elétricas, apesar da confiabilidade da informação ser importante, é ainda mais fundamental manter a integridade e disponibilidade dos dados para evitar a interrupção do serviço [9].

Na Tabela I são listados os estudos relacionados ao estágio de geração de dados, agrupados pelo tema trabalhado em cada um destes estudos e vinculados aos códigos apresentados na Fig. 2, para facilitar sua localização dentro de uma REI.

B.Aquisição de Dados

1) Considerações gerais sobre a aquisição dos dados: Conforme visto no capítulo anterior, o desenvolvimento das Redes Elétricas Inteligentes amplia os equipamentos geradores de dados relevantes para a rede. A comunicação necessária para a integração desses dados se torna bastante complexa, principalmente nos casos em que a sincronia das informações influenciam no resultado final da informação que será gerada. É importante também notar que a diversidade dos tipos de comunicação e protocolos utilizados torna a questão da integração e segurança desses dados um assunto bastante amplo, porém de importância fundamental, já que é a base para diversos serviços de monitoramento como informações de consumo, balanceamento de carga, alocação de recursos entre outros.

2) Riscos de segurança: Os estudos relacionados à aquisição de dados focam principalmente na privacidade dos dados, já que nessa fase são comuns os ataques visando ao furto ou à manipulação dos dados. Outros estudos focam na criação de protocolos que facilitem a troca de informações entre os diversos atores da rede facilitando a integração dos equipamentos e, em muitos casos, embutindo privacidade e segurança na comunicação.

TABELA I
ESTUDOS RELACIONADOS AOS RISCOS DE GERAÇÃO DE DADOS EM REDES ELÉTRICAS INTELIGENTES

Área	Tema	Código	Estudos
Geração de energia	Falhas nos equipamentos de geração de energia	GE1, GE2	[10], [11], [12], [13], [14]
	Mecanismos de detecção de eventos que possam produzir efeitos em cascata	GE1	[15], [16]
	Fatores de segurança na geração de energia	GE1	[17], [18], [19]
	Fatores de segurança na geração de energia, incluindo de fontes renováveis	GE1, GE2	[20]
Transmissão e distribuição de energia	Desafios de segurança em sistemas embarcados	GE3	[21]
	Ataques à PMUs	GE3	[22], [23], [24],[25]
	Ataques à AMI	GE3	[26],[27],[28]
	Vulnerabilidades em *microgrids*	GE3	[29],[30]
Controle de carga	Questões de segurança e ataques em medidores inteligentes	GE4	[31], [32], [33], [34], [35]
	Ataques ao sistema SCADA	GE3	[36], [37], [38],[39]
	Criptografia em dispositivos para redes inteligentes	GE4	[40], [41]
	Segurança e privacidade em transações na infraestrutura para carros elétricos	GE4	[42]

Vários protocolos de comunicação podem ser utilizados nas diferentes necessidades apresentadas por uma REI, a Tabela II agrupa os principais protocolos encontrados em REIs no momento desta publicação.

As tecnologias de comunicação sem fio ZigBee (IEEE 802.15.4), Wi-Fi (IEEE 802.11) e WiMAX (IEEE 802.16) cobrem áreas de até 50 m, 100 m e 100 km com taxa de transferência de dados de 50 kb/s, 150 Mb/s e 288.8 Mb/s, respectivamente. Em geral, a comunicação sem fio é bastante susceptível a sofrer interferências externas [43].

O IEC 61850 é um padrão aberto para comunicação via Ethernet entre as subestações, garantindo a interoperabilidade entre os diversos Dispositivos Eletrônicos Inteligentes (IED) utilizados [44].

A comunicação via PLC (Power Line Comunication), utiliza a rede de de distribuição e transmissão de energia instalada para a comunicação de dados. A sua taxa de transferência de dados é inversamente proporcional à distância percorrida pelo dado. Entre os principais problemas que apresenta estão a perda de dados, a atenuação e distorção do sinal, ruídos, interferências e congestionamento do canal de comunicação [43].

C.Armazenamento de Dados

1) Considerações gerais sobre o armazenamento dos dados: O armazenamento dos dados é de fundamental importância para serviços que tenham como base o histórico dos dados e a combinação de informações de diversas fontes,

TABELA II
ESTUDOS RELACIONADOS AOS RISCOS DE AQUISIÇÃO DE DADOS EM REDES ELÉTRICAS INTELIGENTES

Área	Tema	Código	Estudos
Protocolos	*ZigBee*	AQ1	[45], [46], [47]
	Wireless Mesh Networks (WMN)	AQ2	[48], [49], [50], [51], [52]
	IEC 61850	AQ3	[53], [54], [55]
	Power Line Communication (PLC)	AQ4	[56], [57]
	Outros protocolos	AQ1, AQ2, AQ3, AQ4	[58], [59], [60]
Privacidade	*Compressive sensing* (CS)	AQ1, AQ2, AQ3, AQ4	[61]
	Intrusion Detection and Prevention Systems (IDPS)	AQ1, AQ2, AQ3, AQ4	[62]
	Aquisição de dados de medidores inteligentes	AQ1	[63], [64], [65], [66],[67],[68]
	Aquisição de dados de sensores em casas inteligentes	AQ1	[69]

como é o caso da detecção de falhas, Resposta à Demanda, predição de geração de energia, análise de consumidores, cobrança entre outros. Dependendo da necessidade os dados podem ser armazenados no próprio equipamento gerador da informação, como medidores inteligentes ou dispositivos domésticos inteligentes, além de poderem ser armazenados em grandes bancos de dados. Devido ao grande volume e complexidade dos dados, diferentes tecnologias e arquiteturas devem ser estudadas para o uso em cada caso, optando-se pelo armazenamento centralizado ou distribuído, e por bases de dados relacionais ou chave-valor, ou ainda pelo uso de sistemas híbridos. Sistemas de banco de dados paralelos e distribuídos tem se tornado cada vez mais populares em REIs devido a natureza distribuída da rede elétrica, dispersa geograficamente e em grande escala [1].

2) Riscos de segurança: Assim como a aquisição de dados, o armazenamento também pode receber ataques objetivando o furto ou a manipulação de dados, aumentando os riscos de confidencialidade, integridade e disponibilidade. É objeto de muitos estudos existentes na literatura avaliar impacto do controle de acesso aos dados, da criptografia da base de dados e do correto dimensionamento do sistema, com a finalidade de evitar que o excesso de dados constantes no sistema e que são enviados pelos equipamentos da rede não causem um estouro ou uma falha de funcionamento nos servidores.

Na Tabela III, os estudos são organizados em três grandes temas. O tema autenticação e controle de acesso trata principalmente dos diferentes privilégios de acesso aos dados de cada ator participante da rede (administradores, operadores, engenheiros etc) e da importância da criptografia para a proteção desses acessos. O armazenamento na nuvem aumenta a exposição dos dados e este tema aborda questões de integridade, confidencialidade e disponibilidade dos dados armazenados. O tema sobre modificação maliciosa dos dados e suas consequências trata dos impactos causados em diferentes partes da rede pela manipulação indevida dos dados armazenados.

TABELA III
ESTUDOS RELACIONADOS AOS RISCOS DE ARMAZENAMENTO DE DADOS EM REDES ELÉTRICAS INTELIGENTES

Tema	Código	Estudos
Autenticação e controle de acesso	AR1	[70], [71], [72], [73]
Questões específicas para armazenamento na nuvem	AR1	[74]
Modificação maliciosa de dados armazenados e consequências na rede	AR1	[75], [76]

D.Processamento de Dados

1) Considerações gerais sobre o processamento dos dados: Diversos equipamentos são responsáveis por processar os dados em uma REI, cada um com o objetivo específico de atender a um ou mais serviços. Neste estudo, seguindo a lógica de [1], os estudos foram divididos em dois serviços que ganham enormemente com os diversos dados que surgem com a implantação de uma REI, a Resposta à Demanda e a Estimação de Estado. Além deles, são apresentados estudos que falam sobre furto de energia elétrica, problema tão antigo quanto as primeiras redes elétricas, mas que tende a aumentar com o controle financeiro sendo efetuado a distância.

O serviço de Resposta à Demanda utiliza dados de medidores inteligentes e informações de sinalizadores de preços para sugerir ou alterar o padrão de consumo dos consumidores finais [1]. Já o serviço de Estimação de Estado controla processos críticos como a análise de contingência, o despacho econômico de energia, a definição de preços em tempo real entre outros [1]. Atualmente o processo de Estimação de Estado é centralizado no controle de operações com métodos de detecção de dados falsos. Com a introdução dos *prosumers* e o aumento exponencial de geração de dados na REI, o método utilizado tradicionalmente se torna impraticável.

2) Riscos de segurança: Na fase de processamento dos dados, a manipulação dos dados é sempre o fator de maior preocupação, seja por falha de equipamentos ou intervenções maliciosas.

No caso do serviço de Resposta à Demanda, são considerados os diversos níveis de segurança como a confidencialidade, a integridade, a disponibilidade, a autenticidade, a rastreabilidade das operações e as possíveis auditorias das operações realizadas. O *OpenADR* é um protocolo desenvolvido especificamente para facilitar a comunicação entre os diversos atores do serviço de Resposta à Demanda, facilitando o desenvolvimento de novas aplicações.

Para o serviço de Estimação de Estado, as questões estudadas estão principalmente relacionadas com *data injection.* Neste tipo de ataque de violação de integridade, geralmente os dados são corrompidos ou são introduzidos dados falsos com a finalidade de comprometer a acurácia do serviço [6]. Técnicas de processamento e análise de dados podem reduzir os danos causados através da detecção de falhas e dados falsos.

Para o furto de energia, além da manipulação dos dados persistem os tradicionais problemas de furto físico, como o desvio de energia e a manipulação física do leitor. Os estudos listados na Tabela IV focam nos métodos utilizados para detecção de furto de energia utilizando o processamento de dados de uma única fonte de dados ou pela combinação de dados de múltiplas fontes. As soluções baseadas em uma única fonte de dados tratam somente dos dados de consumo gerados pelos medidores inteligentes, enquanto as soluções baseadas em múltiplas fontes consideram também outras fontes de dados, como os medidores dos transformadores de distribuição, os registros de auditoria dos medidores, os sensores anti-adulteração dos medidores entre outros. Em outro tema, são tratados formas de processamento dos dados que garantam a privacidade na leitura de medidores inteligentes.

TABELA IV
ESTUDOS RELACIONADOS AOS RISCOS DE PROCESSAMENTO DE DADOS EM REDES ELÉTRICAS INTELIGENTES

Área	Tema	Código	Estudos
Resposta à Demanda	*OpenADR*	PR1	[77], [78]
	Requerimentos e questões de segurança	PR1	[77]
	Privacidade	PR1	[79], [80], [81]
	Estabilidade	PR1	[82], [83]
Estimação de Estado	Ataques de *data injection*	PR2	[84], [85], [86], [87], [88], [89], [90], [91], [92]
	Novas formulações de Estimação de Estado que minimizam dados falsos	PR2	[93], [94], [95], [96], [97]
Furto de energia	Fonte única	PR3	[98], [99], [100]
	Múltiplas fontes	PR3	[101], [102], [103]
	Privacidade	PR3	[104], [105]

TABELA V
ESTUDOS RELACIONADOS À ANÁLISE DE DADOS

Tema	Métodos de Análise	Código	Estudos
Geração distribuída	*Skewness*, *kurtosis estimators*, *cumulative sum control chart*	AN1	[106]
SCADA	*Conditional Covariance Test*, *Markov graph*	AN1	[107], [108]
AMI	*Markov chain*, *Hoeffiding tree*	AN1	[109], [110]
Geração de energia	*Feature extraction*, técnicas de classificação de dados	AN1	[111], [112], [113]
Sistemas de transmissão	*Rule-based expert system*, *commom path mining*	AN1	[114]
Rede como um todo		AN1	[115], [116], [117]

E. Análise de Dados

1) Considerações gerais sobre a análise dos dados: A análise de dados não constitui um problema de segurança, mas uma possível solução para detecção de falhas, furtos e intervenções maliciosas. Muitos dos estudos já citados utilizam a análise de dados para resolução de problemas de segurança, principalmente na fase de processamento dos dados. A aquisição massiva de dados em uma REI com seus múltiplos geradores de dados abre possibilidades para a análise de *big data* com o intuito de solucionar problemas de falha ou manipulação dos dados. Assim, podem ser utilizados algoritmos de classificação de padrão, de previsão ou otimização que visam identificar padrões de fraude na rede como um todo.

A Tabela V, lista os estudos relacionados à análise de dados para diversos componentes de uma REI e indica na coluna de Métodos de Análise alguns dos métodos estudados para cada situação, conforme indicado em [1].

Em [118] é proposta a classificação dos estudos de análise de dados em análise estatística, mineração de dados e visualização de dados. Na análise estatística ([106],[108],[110]) o objetivo é usar a teoria estatística para modelar aleatoriedade e incerteza, a mineração de dados ([112],[114],[109],[111]) busca descobrir padrões e relações em conjuntos de dados e a visualização de dados ([107],[113],[115],[116],[117]) busca representar os dados de forma gráfica para que possam ser melhor analisados e tratados [1].

IV. APLICAÇÃO DA ABORDAGEM VISUAL AO CENÁRIO BRASILEIRO ATUAL

A transformação da rede brasileira de energia elétrica em uma REI completa, como apresentada na Fig. 2, ainda se encontra em estágio inicial. Conforme [119], o país conta com vários projetos pilotos elaborados pelas concessionárias de energia elétrica, utilizando recursos do programa de Pesquisa Desenvolvimento e Inovação da ANEEL (Agência Nacional de Energia Elétrica), o que tem servido para avaliar as redes inteligentes sem afetar o equilíbrio econômico-financeiro empresarial e a regulação atual do setor. Ainda é necessária a realização das definições legais e regulamentação do tema para que uma implantação de redes inteligentes no Brasil seja feita em grande escala.

O trabalho [120], que é um dos produtos gerados no P&D Estratégico ANEEL – Programa Brasileiro de Redes Inteligentes, apresenta a situação atual da rede brasileira de energia elétrica e uma visualização do possível estado da rede no futuro. Na Fig. 3 é apresentado o cenário atual adaptado do esquema exposto na Fig. 2 e do trabalho [120], com os respectivos problemas de segurança e suas ligações com os estudos listados neste artigo.

A implantação das soluções relacionadas à REI no Brasil são motivados por velhos problemas enfrentados pelas distribuidoras do país, como as perdas técnicas e não técnicas (fraude e inadimplência), a interrupção de energia, as flutuações de tensão e a alta demanda de energia no horário de pico. Assim, as soluções ainda são simples, quais sejam: a instalação de medidores inteligentes para mitigar os problemas relacionados ao furto de energia e reduzir a inadimplência; a instalação na média tensão de chaves, dispositivos de manobras e disjuntores telecomandados para redução de interrupção de grandes blocos de carga; a implantação de mecanismos de tarifa binômia para os consumidores de grades cargas e maior nível tensão, possibilitando uma redução da demanda no horário de ponta, por conta do estabelecimento de tarifas diferenciadas nestes horários.

É importante notar a presença dos prosumidores no cenário brasileiro, já que em 2012 a Resolução Normativa nº 482 da ANEEL definiu as regras que permitem ao consumidor gerar a própria energia, fornecer o excedente de geração para a rede pública e ganhar créditos na forma de desconto na conta de energia.

O desenvolvimento de uma rede descentralizada, com maior poder de participação do consumidor e com maior oferta de serviços ainda é incipiente no país, mas grande parte dos

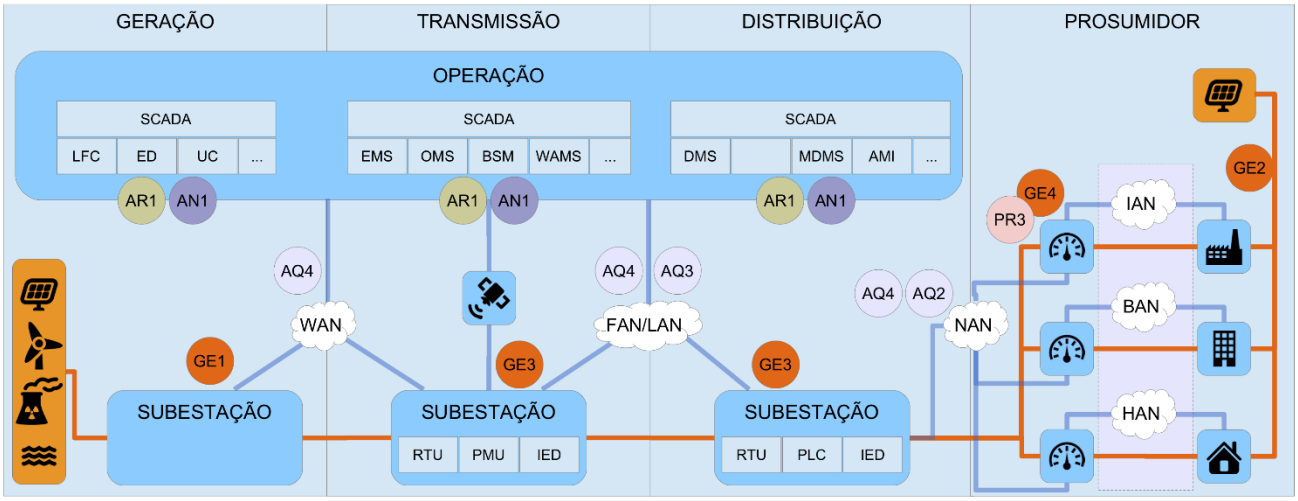

Fig. 3. Visualização do esquema apresentado na Fig. 2 com base na situação atual brasileira. Os espaços em branco marcam a posição dos itens correspondentes da Fig. 2 que não se aplicam a este cenário.

estudos apresentados neste artigo podem ser aproveitados no cenário atual. A situação futura da rede elétrica brasileira apresentada em [120] se aproxima cada vez mais do esquema apresentado na Fig. 2, com a interoperabilidade entre todos os atores da rede e a inclusão de novos atores, como os Veículos Elétricos Plugáveis. Caso esta tendência seja mantida, todos os estudos apresentados neste artigo terão utilidade na mitigação de riscos para o setor elétrico brasileiro.

Para que o cenário apresentado na Fig. 2 seja alcançado, é muito importante que haja uma mudança regulatória no setor de energia no Brasil, pois o arcabouço normativo atual não incentiva as distribuidoras a investir em tecnologias disruptivas e que possam, de fato, reduzir os velhos problemas enfrentados por estas empresas e que impactam no dia a dia dos seus clientes.

V. Conclusão e Trabalhos Futuros

Este trabalho apresentou de forma visual as questões de segurança que surgem com o desenvolvimento das Redes Elétricas Inteligentes. Foi elaborado um esquema representativo de uma REI e nele foram posicionados os principais tópicos de segurança, divididos com base no ciclo de vida dos dados. Cento e oito estudos recentes sobre segurança em REIs foram avaliados, organizados por temas e vinculados aos tópicos deste esquema, permitindo um melhor entendimento da influência exercida por cada um dentro da rede. O esquema apresentado serviu como base para apresentar o cenário atual de energia elétrica no Brasil, facilitando a busca por estudos pertinentes e a comparação com o cenário ideal. Além disso, a metodologia apresentada neste trabalho pode servir como base para acompanhar o desenvolvimento das questões de segurança na rede elétrica de qualquer país e permitir a organização de estudos correlatos, ajudando na sua classificação, na comparação com outros estudos e na visualização do seu posicionamento dentro de uma REI.

Referências

[1] S. Tan, D. De, W. Song, J. Yang and S. K. Das, "Survey of Security Advances in Smart Grid: A Data Driven Approach," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 397-422, Firstquarter 2017.

[2] W. F. Correia, and R. F. Calili, “Inclusão de métodos estatísticos como apoio ao faturamento de energia realizado por medidores inteligentes.” M.S. thesis, Dept. Metrologia, Pontifícia Universidade Católica do Rio de Janeiro, 2018.

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

[4] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," in IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 13-27, 12 2016.

[5] M. Z. Gunduz e R. Das, “Cyber-security on smart grid: Threats and potential solutions”, Computer Networks, vol. 169, p. 107094, mar. 2020.

[6] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, “Cyber-security in smart grid: Survey and challenges,” Computers & Electrical Engineering, vol. 67, pp. 469–482, Apr. 2018.

[7] B. B. Gupta and T. Akhtar, “A survey on smart power grid: frameworks, tools, security issues, and solutions,” Annals of Telecommunications, vol. 72, no. 9–10, pp. 517–549, Sep. 2017.

[8] L. Kotut and L. A. Wahsheh, "Survey of Cyber Security Challenges and Solutions in Smart Grids," 2016 Cybersecurity Symposium (CYBERSEC), Coeur d'Alene, ID, 2016, pp. 32-37.

[9] Y. Lopes, T. Bornia, V. Farias, N. C. Fernandes, and D. C. Muchaluat-Saade, “Desafios de Segurança e Confiabilidade na Comunicação para Smart Grids“ ch 4. 2016. Presented at Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg). [Online]. Available: http://sbseg2016.ic.uff.br/pt/files/MC4-SBSeg2016.pdf

[10] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): ‘Cyber-attack against Ukrainian critical infrastructure’. Alert (IR-ALERT- H-16-056-01), 2016. [Online]. Available: https://www.ics-cert.us-cert.gov/alerts/IR- ALERT-H-16-056-01

[11] "Head of Turkish grid operator resigns after blackout," Deutsche Welle. June 4, 2015. [Online]. Available: http://www.dw.com/en/head-of-turkish- grid-operator-resigns-after-blackout/a-18363453

[12] PB Power, "OFGEM Report on Support Investigations into Recent Blackouts in London and West Midlands," February 2004. [Online].

Available: https://www.ofgem.gov.uk/ofgem-publications/37665/sectoralinvestigations-18.pdf

[13] Swiss Federal Office of Energy, "Report on the blackout in Italy on 28 September 2003," November, 2003. [Online]. Available: http://www.bfe.admin.ch/php/modules/publikationen/stream.php?extlang=en&name=en_109363212.pdf

[14] "The South Australia blackout: Once in 50-year storm lashes state", The Sydney Morning Herald, September 28, 2016. [Online]. Available: http://www.smh.com.au/national/south-australia-blackout-once-in- 50year-storm-lashes-state-20160928-grqpks.html

[15] S. Ruj and A. Pal, "Analyzing Cascading Failures in Smart Grids under Random and Targeted Attacks," 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, Victoria, BC, 2014, pp. 226-233.

[16] U.S.-Canada Power System Outage Task Force, "Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations". 2004

[17] "Smart grid and cyber security for energy assurance," Nat. Assoc. State Energy Officials, Arlington, TX, USA, Tech. Rep. DE-OE0000119, 2011.

[18] K. Morison, Lei Wang and P. Kundur, "Power system security assessment," in IEEE Power and Energy Magazine, vol. 2, no. 5, pp. 30-39, Sept.-Oct. 2004.

[19] "Green paper—Towards a European strategy for the security of energy supply," European Commission, Tech. Rep. B. COM(2000) 769 Final, 2000.

[20] B. Johansson, "Security aspects of future renewable energy systems–A short overview," Energy, vol. 61, pp. 598–605, Nov. 2013.

[21] A. Kanuparthi, R. Karri, and S. Addepalli, "Hardware and embedded security in the context of internet of things," in Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles - CyCAR '13, 2013.

[22] Z. Zhang, S. Gong, A. D. Dimitrovski and H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis," in IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 87-98, March 2013.

[23] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela and A. D. Domı´nguez-Garcı´a, "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units," in IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 3253-3262, Aug. 2013.

[24] W. Stallings, "Network and Internetwork Security: Principles and Practice," Upper Saddle River, NJ, USA: Prentice-Hall, 1995.

[25] Y. Wang, T. T. Gamage, e C. H. Hauser, "Security Implications of Transport Layer Protocols in Power Grid Synchrophasor Data Communication", IEEE Transactions on Smart Grid, p. 1–10, 2015, doi: 10.1109/tsg.2015.2499766.

[26] A. Ghosal e M. Conti, "Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey", IEEE Communications Surveys & Tutorials, vol. 21, no 3, pp. 2831–2848, 2019.

[27] F. M. Cleveland, "Cyber security issues for Advanced Metering Infrasttructure (AMI)", in 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008, doi: 10.1109/pes.2008.4596535.

[28] P. Yi, T. Zhu, Q. Zhang, Y. Wu and J. Li, "A denial of service attack in advanced metering infrastructure network," 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, 2014, pp. 1029-1034.

[29] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2013-5472, Jul. 2013.

[30] R. E. Perez-Guzman, Y. Salgueiro-Sicilia, e M. Rivera, "Communication systems and security issues in smart microgrids", in 2017 IEEE Southern Power Electronics Conference (SPEC), 2017, doi: 10.1109/spec.2017.8333659.

[31] K. Sharma and L. Mohan Saini, "Performance analysis of smart metering for smart grid: An overview," Renewable and Sustainable Energy Reviews, vol. 49, pp. 720–735, Sep. 2015.

[32] A. Alnasser and N.-E. Rikli, "Design of a trust security model for smart meters in an urban power grid network," in Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks - Q2SWinet '14, 2014.

[33] Ye Yan, R. Q. Hu, S. K. Das, H. Sharif, and Yi Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," in IEEE Network, vol. 27, no. 4, pp. 64–71, 2013.

[34] S. M. Amin, "Smart grid: overview, issues and opportunities. Advances and challenges in sensing, modeling, simulation, optimisation and control", in Eur J Control, vol. 17, issues 5–6, pp. 547-567. 2011.

[35] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, 2010, pp. 238-243.

[36] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933–1954, 2014.

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

[38] S. East, J. Butts, M. Papa, and S. Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol," in IFIP Advances in Information and Communication Technology, Springer Berlin Heidelberg, 2009, pp. 67–81.

[39] T. A. Rizzetti, P. Wessel, A. S. Rodrigues, B. M. da Silva, R. Milbradt, e L. N. Canha, "Cyber security and communications network on SCADA systems in the context of Smart Grids", in 2015 50th International Universities Power Engineering Conference (UPEC), 2015.

[40] W. Fangfang, W. Huazhong, C. Dongqing and P. Yong, "Substation Communication Security Research Based on Hybrid Encryption of DES and RSA," 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Beijing, 2013, pp. 437-441.

[41] R. Abercrombie et al., "Secure cryptographic key management system (CKMS) considerations for smart grid devices," in Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '11, 2011.

[42] H. Nicanfar, P. TalebiFard, S. Hosseininezhad, V. C. M. Leung, and M. Damm, "Security and privacy of electric vehicles in the smart grid context," in Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications - DIVANet '13, 2013.

[43] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, and C.-F. Covrig, "A survey on the critical issues in smart grid technologies," Renewable and Sustainable Energy Reviews, vol. 54, pp. 396–405, Feb. 2016.

[44] M. Emmanuel and R. Rayudu, "Communication technologies for smart grid applications: A survey," Journal of Network and Computer Applications, vol. 74, pp. 133–148, Oct. 2016.

[45] P. Yi, A. Iwayemi and C. Zhou, "Developing ZigBee Deployment Guideline Under WiFi Interference for Smart Grid Applications," in IEEE Transactions on Smart Grid, vol. 2, no. 1, pp. 110-120, March 2011.

[46] M. Armel, "ZigBee overview, lecture notes, the George Washington University," George Washington University, Tech. Rep., 2007.

[47] S. C. Ergen, "ZigBee/IEEE 802.15.4 summary," Univ. California at Berkeley, Berkeley, CA, USA, Tech. Rep., 2004.

[48] K. Gai, M. Qiu, Z. Ming, H. Zhao and L. Qiu, "Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2431-2439, Sept. 2017.

[49] Reyes H, Kaabouch N. Jamming and lost link detection in wireless networks with fuzzy logic. Int J Sci Eng Res 2013;4(February(2)):1–7.H. R. Moncayo, and N. Kaabouch, "Jamming and Lost Link Detection in Wireless Networks with Fuzzy Logic," in International Journal of Scientific and Engineering Research, vol. 4. Feb. 2013.

[50] B. A. Akyol, H. Kirkham, S. L. Clements, and M. D. Hadley, "A Survey of Wireless Communications for the Electric Power System," Office of Scientific and Technical Information (OSTI), Jan. 2010.

[51] Y. Liu, P. Ning, H. Dai and A. Liu, "Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication," 2010 Proceedings IEEE INFOCOM, San Diego, CA, 2010, pp. 1-9.

[52] P. Zhang, O. Elkeelany and L. McDaniel, "An implementation of secured Smart Grid Ethernet communications using AES," Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon), Concord, NC, 2010, pp. 394-397.

[53] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh and J. Tan, "An Intrusion Detection System for IEC61850 Automated Substations," in IEEE Transactions on Power Delivery, vol. 25, no. 4, pp. 2376-2383, Oct. 2010.

[54] Y. Liang and R. H. Campbell, “Understanding and simulating the IEC 61850 standard,” Dept. Comput. Sci., Univ. Illinois at Urbana-Champaign, Champaign, IL, USA, Tech. Rep., 2008.

[55] T. Kostic, O. Preiss, and C. Frei, “Understanding and using the IEC 61850: a case for meta-modelling,” Computer Standards & Interfaces, vol. 27, no. 6, pp. 679–695, Jun. 2005.

[56] M. Yigit, V. C. Gungor, G. Tuna, M. Rangoussi, and E. Fadel, “Power line communication technologies for smart grid applications: A review of advances and challenges,” Computer Networks, vol. 70, pp. 366–383, Sep. 2014.

[57] S. Galli, A. Scaglione and Z. Wang, "Power Line Communications and the Smart Grid," 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, 2010, pp. 303-308.

[58] S. Uludag, K. Lui, W. Ren and K. Nahrstedt, "Secure and Scalable Data Collection With Time Minimization in the Smart Grid," in IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 43-54, Jan. 2016.

[59] G. Dan, K.-S. Lui, R. Tabassum, Q. Zhu, and K. Nahrstedt, “SELINDA: A secure, scalable and light-weight data collection protocol for smart grids,” in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Vancouver, BC, Canada, Oct. 2013, pp. 480–485.

[60] Y.-J. Kim, V. Kolesnikov, H. Kim, and M. Thottan, “SSTP: A scalable and secure transport protocol for smart grid data collection,” in 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2011.

[61] G. Li and Y. Wang, "A Compressive Sensing Based Secure Data Transmission Scheme," 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, 2013, pp. 1272-1275.

[62] P. I. Radoglou-Grammatikis e P. G. Sarigiannidis, “Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems”, IEEE Access, vol. 7, pp. 46595–46620, 2019.

[63] L. Yang, H. Xue, and F. Li, “Privacy-preserving data sharing in smart grid systems,” in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Venice, Italy, Nov. 2014, pp. 878–883.

[64] N. Yukun, T. Xiaobin, C. Shi, W. Haifeng, Y. Kai and B. Zhiyong, "A security privacy protection scheme for data collection of smart meters based on homomorphic encryption," Eurocon 2013, Zagreb, 2013, pp. 1401-1405.

[65] Z. Erkin, J. R. Troncoso-pastoriza, R. L. Lagendijk and F. Perez-Gonzalez, "Privacy-preserving data aggregation in smart metering systems: an overview," in IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 75-86, March 2013.

[66] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris and D. Barthel, "Secure Lossless Aggregation for Smart Grid M2M Networks," 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, 2010, pp. 333-338.

[67] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, e A. Martin, “Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues”, IEEE Communications Surveys & Tutorials, vol. 21, no 3, pp. 2886–2927, 2019.

[68] M. Yesilbudak e I. Colak, “Main Barriers and Solution Proposals for Communication Networks and Information Security in Smart Grids”, in 2018 International Conference on Smart Grid (icSmartGrid), 2018, doi: 10.1109/isgwcp.2018.8634478.

[69] A. Chakravorty, T. Wlodarczyk, and C. Rong, “Privacy preserving data analytics for smart homes,” in Proc. IEEE Security Privacy Workshops (SPW), San Francisco, CA, USA, May 2013, pp. 23–27.

[70] X. Li, X. Liang, R. Lu, X. Shen, X. Lin and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," in IEEE Communications Magazine, vol. 50, no. 8, pp. 38-45, August 2012

[71] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu and X. S. Shen, "A Lightweight Message Authentication Scheme for Smart Grid Communications," in IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 675-685, Dec. 2011.

[72] Q. Li and G. Cao, "Multicast Authentication in the Smart Grid With One-Time Signature," in IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 686-696, Dec. 2011.

[73] H. Cheung, A. Hamlyn, T. Mander, C. Yang and R. Cheung, "Role-based model security access control for smart power-grids computer networks," 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, 2008, pp. 1-7.

[74] Y. Simmhan, A. G. Kumbhare, B. Cao and V. Prasanna, "An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds," 2011 IEEE 4th International Conference on Cloud Computing, Washington, DC, 2011, pp. 582-589.

[75] A. Anwar and A. Mahmood, “Cyber security of smart grid infrastructure,” in The State of the Art in Intrusion Prevention and Detection. Boca Raton, FL, USA: CRC Press, 2014, pp. 449–472.

[76] J. Valenzuela, J. Wang and N. Bissinger, "Real-time intrusion detection in power system operations," in IEEE Transactions on Power Systems, vol. 28, no. 2, pp. 1052-1062, May 2013.

[77] A. Paverd, A. Martin, and I. Brown, “Security and Privacy in Smart Grid Demand Response Systems,” in Lecture Notes in Computer Science, Springer International Publishing, 2014, pp. 1–15.

[78] A. Mohan and D. Mashima, “Towards secure demand-response systems on the cloud,” in Proc. IEEE Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS), Marina Del Rey, CA, USA, May 2014, pp. 361–366.

[79] H. Li, X. Lin, H. Yang, X. Liang, R. Lu and X. Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2053-2064, Aug. 2014.

[80] M. Zhu, "Distributed demand response algorithms against semi-honest adversaries," 2014 IEEE PES General Meeting | Conference & Exposition, National Harbor, MD, 2014, pp. 1-5.

[81] X. Liang, X. Li, R. Lu, X. Lin and X. Shen, "UDP: Usage-Based Dynamic Pricing With Privacy Preservation for Smart Grid," in IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 141-150, March 2013.

[82] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing and T. Basar, "Dependable Demand Response Management in the Smart Grid: A Stackelberg Game Approach," in IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 120-132, March 2013.

[83] H. H. Nguyen, R. Tan and D. K. Y. Yau, "Safety-assured collaborative load management in smart grids," 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), Berlin, 2014, pp. 151-162.

[84] H. Sedghi and E. Jonckheere, "Statistical Structure Learning to Ensure Data Integrity in Smart Grid," in IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 1924-1933, July 2015.

[85] D. B. Rawat and C. Bajracharya, "Detection of False Data Injection Attacks in Smart Grid Communication Systems," in IEEE Signal Processing Letters, vol. 22, no. 10, pp. 1652-1656, Oct. 2015.

[86] D. Wang et al., “Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids,” Energies, vol. 7, no. 3, pp. 1517–1538, 2014. [Online]. Available: http://www.mdpi.com/1996- 1073/7/3/1517

[87] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar and K. Poolla, "Smart Grid Data Integrity Attacks," in IEEE Transactions on Smart Grid, vol. 4, no. 3, pp. 1244-1253, Sept. 2013.

[88] Y. Huang et al., "Bad data injection in smart grid: attack and defense mechanisms," in IEEE Communications Magazine, vol. 51, no. 1, pp. 27-33, January 2013.

[89] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni and H. V. Poor, "Sparse Attack Construction and State Estimation in the Smart Grid: Centralized and Distributed Models," in IEEE Journal on Selected Areas in Communications, vol. 31, no. 7, pp. 1306-1318, July 2013.

[90] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," in IEEE Signal Processing Magazine, vol. 29, no. 5, pp. 106-115, Sept. 2012.

[91] O. Kosut, L. Jia, R. J. Thomas and L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, 2010, pp. 220-225.

[92] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” in Proc. 16th ACM Conf. Comput. Commun. Security, 2009, pp. 34–35.

[93] P. Chavali and A. Nehorai, "Distributed Power System State Estimation Using Factor Graphs," in IEEE Transactions on Signal Processing, vol. 63, no. 11, pp. 2864-2876, June1, 2015.

[94] Y. Mo and B. Sinopoli, "Secure Estimation in the Presence of Integrity Attacks," in IEEE Transactions on Automatic Control, vol. 60, no. 4, pp. 1145-1151, April 2015.

[95] J. Zhang, G. Welch, N. Ramakrishnan, and S. Rahman, “Kalman Filters for Dynamic and Secure Smart Grid State Estimation,” Intelligent Industrial Systems, vol. 1, no. 1, pp. 29–36, May 2015.
[96] M. Göl and A. Abur, "LAV Based Robust State Estimation for Systems Measured by PMUs," in IEEE Transactions on Smart Grid, vol. 5, no. 4, pp. 1808-1814, July 2014.
[97] Y. Weng, R. Negi, and M. Ilic, “Historical data-driven state estimation for electric power systems,” in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Vancouver, BC, Canada, Oct. 2013, pp. 97–102.
[98] S. Salinas, C. Luo, W. Liao, and P. Li, “State estimation for energy theft detection in microgrids,” in Proc. 9th Int. Conf. Commun. Netw. China (CHINACOM), Maoming, China, Aug. 2014, pp. 96–101.
[99] A. Cardenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, “A game theory model for electricity theft detection and privacy- aware control in ami systems,” in Proc. 50th Annu. Allerton Conf. Commun. Control Comput. (Allerton), Monticello, IL, USA, Oct. 2012, pp. 1830–1837.
[100] D. Mashima and A. A. Cárdenas, “Evaluating Electricity Theft Detectors in Smart Grid Networks,” in Research in Attacks, Intrusions, and Defenses, Springer Berlin Heidelberg, 2012, pp. 210–229.
[101] P. Jokar, N. Arianpoo and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers’ Consumption Patterns," in IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 216-226, Jan. 2016.
[102] S. Sahoo, D. Nikovski, T. Muso and K. Tsuru, "Electricity theft detection using smart meter data," 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, 2015, pp. 1-5.
[103] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier and S. Zonouz, "A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures," in IEEE Journal on Selected Areas in Communications, vol. 31, no. 7, pp. 1319-1330, July 2013.
[104] S. A. Salinas and P. Li, "Privacy-Preserving Energy Theft Detection in Microgrids: A State Estimation Approach," in IEEE Transactions on Power Systems, vol. 31, no. 2, pp. 883-894, March 2016.
[105] S. Salinas, M. Li and P. Li, "Privacy-Preserving Energy Theft Detection in Smart Grids: A P2P Computing Approach," in IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 257-267, September 2013.
[106] I. M. Moreno-Garcia et al., “Intelligent electronic device for smart grid: Statistical approach applied to event detection,” in Proc. 38th Annu. Conf. IEEE Ind. Electron. Soc. (IECON), Montreal, QC, Canada, Oct. 2012, pp. 5221–5226.
[107] W. J. Matuszak, L. DiPippo, and Y. L. Sun, “Cybersave: Situational awareness visualization for cyber security of smart grid systems,” in Proc. 10th Workshop Visualization Cyber Security (VizSec), Atlanta, GA, USA, 2013, pp. 25–32. [Online]. Available: http://doi.acm.org/10.1145/2517957.2517961
[108] H. Sedghi and E. Jonckheere, "Statistical structure learning of smart grid for detection of false data injection," 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, 2013, pp. 1-5.
[109] M. A. Faisal, Z. Aung, J. R. Williams and A. Sanchez, "Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study," in IEEE Systems Journal, vol. 9, no. 1, pp. 31-44, March 2015.
[110] M. Q. Ali and E. Al-Shaer, “Configuration-based IDS for advanced metering infrastructure,” in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS ’13, 2013.
[111] S. Pan, T. Morris, and U. Adhikari, “Developing a hybrid intrusion detection system using data mining for power systems,” in IEEE Trans. Smart Grid, vol. 6, no. 6, pp. 3104–3113, Nov. 2015.
[112] W. Hurst, M. Merabti, and P. Fergus, “Big data analysis techniques for cyber-threat detection in critical infrastructures,” in Proc. 28th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA), Victoria, BC, Canada, May 2014, pp. 916–921.
[113] M. Steiger, T. May, J. Davey, and J. Kohlhammer, “Smart grid monitoring through visual analysis,” in Proc. 4th IEEE/PES Innov. Smart Grid Technol. Europe (ISGT EUROPE), Kongens Lyngby, Denmark, Oct. 2013, pp. 1–5.
[114] T. Popovic, M. Kezunovic, and B. Krstajic, “Smart grid data analytics for digital protective relay event recordings,” Information Systems Frontiers, vol. 17, no. 3, pp. 591–600, Jun. 2013.
[115] D. Gurugubelli, C. Foreman, and D. Ebert, “Achieving a cyber-secure smart grid through situation aware visual analytics,” in Proc. Center Educ. Res. Inf. Assurance Security, 2015, p. 11.
[116] M. Angelini, D. D. Santis, and G. Santucci, “Toward geographical visualizations for hierarchical security data,” in Proc. IEEE Symp. Visualization Cyber Security (VizSec), Paris, France, Nov. 2014, p. 9.
[117] P. Chopade, K. M. Flurchick, M. Bikdash, and I. Kateeb, “Modeling and visualization of smart power grid: Real time contingency and security aspects,” in Proc. IEEE Southeastcon, Orlando, FL, USA, Mar. 2012, pp. 1–6.
[118] H. Hu, Y. Wen, T.-S. Chua, and X. Li, “Toward scalable systems for big data analytics: A technology tutorial,” IEEE Access, vol. 2, pp. 652–687, 2014.
[119] M. A. Limberger, R. F. Calili, and R. C. Souza, “Estudo da tarifa branca para a classe residencial pela medição de consumo de energia e de pesquisa de posses e hábitos.”, M.S. thesis, Dept. Metrologia, Pontifícia Universidade Católica do Rio de Janeiro, 2014.
[120] J. C. Dutra, M. C. Pinheiro, N. F. Leite et al., “Redes elétricas inteligentes no Brasil. Subsídios para um Plano Nacional de Implantação”. P&D ANEEL, ABRADEE, APTEL, CEMIG e SYNERGIA, 2011.

Marcos Rogozinski nasceu no Rio de Janeiro, RJ, Brasil em 1974. É graduado em Music Production & Engineering pela Berklee College Of Music, Boston, MA, EUA em 1997 e graduação em Sistemas de Informação pela Universidade Estácio de Sá, Rio de Janeiro, RJ, Brasil em 2015. Atualmente é mestrando do curso de Pós-Graduação em Metrologia, Qualidade e Inovação da Pontifícia Universidade Católica do Rio de Janeiro, Brasil.

Rodrigo F. Calili nasceu em São Paulo, SP, Brasil em 1976. É graduado em Engenharia Elétrica pela Universidade Federal de Juiz de Fora, Minas Gerais, Brasil em 2003, tem mestrado e doutorado em Engenharia Elétrica pela Pontifícia Universidade Católica do Rio de Janeiro, Brasil (2006 e 2013, respectivamente), tendo cursado parte de seu doutorado na École des Mines em Paris. Tem Pós-doutorado em Metrologia pela PUC-Rio, Rio de Janeiro, Brasil em 2016. Desde 2016 é professor assistente do Programa de Pós-Graduação em Metrologia e do Mestrado Profissional de Engenharia Urbana e Ambiental da PUC-Rio. Doutor Calili já publicou mais de 60 artigos em congressos, periódicos, jornais e revistas.