Segurança Cibernética em Microrredes: Estado de Arte e Desafios

Bruno O. Zarpellon* Caio Henrique T. Alberto* Jéssica S. Pereira* Juan C. Cebrian* Helmo K. Morales-Paredes*

** Instituto de Ciência e Tecnologia de Sorocaba – ICTS, Universidade Estadual Paulista – UNESP, Sorocaba - SP, CEP 18087-180*

(e-mail: bruno.o.zarpellon@unesp.br; caio.alberto@unesp.br; js.pereira@unesp.br; juan.cebrian@unesp.br; helmo.paredes@unesp.br)

Abstract: The evolution that the world's electric grids have gone through in recent years (becoming intelligent) brings several advantages, such as reduced electric losses, optimization of their operation, greater integration of distributed generations, among others. However, when becoming intelligent networks, electrical networks become extremely dependent on information and communication systems with higher resilient and trustworthy standards. This feature makes the grid vulnerable to cyber-attacks of the most varied types. This bibliographical review proposes to expose some of these possible threats to smart grids, with a particular focus on the so-called microgrids, as well as their characteristics, defense mechanisms and attack detection and possible failure recovery modes.

Resumo: As mudanças pela qual as redes elétricas têm passado nos últimos anos (na direção de se tornarem inteligentes) trazem diversas vantagens, tais como diminuição de perdas elétricas, otimização de seu funcionamento, maior integração da geração de energia distribuída, entre outros. Porém, nessa transição, as redes elétricas passam a depender cada vez mais de informações e sistemas de comunicação confiáveis e resilientes. Isso faz com que as redes passem a ser vulneráveis a ataques cibernéticos dos mais variados tipos. A presente revisão bibliográfica expõe quais são algumas dessas possíveis ameaças às redes elétricas inteligentes, com foco particular nas microrredes, bem como suas características comportamentais, detecção de ataques, mecanismos de defesa e possíveis modos de recuperação de falhas.

Keywords: Cyber security; Microgrids; Smart grids; Cyber-physical systems; Information and Communication Technologies.

Palavras-chaves: Segurança cibernética; Microrredes; Redes elétricas inteligentes; Sistemas Físico Cibernéticos; Tecnologias de Informação e Comunicação.

1. INTRODUÇÃO

A International Energy Agency define rede elétrica inteligente (REI) como uma rede elétrica que utiliza tecnologias digitais avançadas para monitorar e gerenciar o transporte de eletricidade de todas as fontes de geração, visando o atendimento dos consumidores finais de energia (International Energy Agency, 2011). Sendo assim, tal como destacado por Panajotovic et al. (2011) e ENISA (2012), a transição da rede elétrica tradicional para uma REI vem acompanhada da intensa aplicação de tecnologias de informação e comunicação (TICs), que operam de modo a integrar os sistemas de controle e comunicação às redes elétricas, com o objetivo de aproximar os sistemas cibernéticos ao mundo físico e criar uma aderência mais robusta, confiável e resiliente. O uso das TICs melhora o desempenho da rede elétrica, como por exemplo controle dinâmico do uso de energia dos usuários presentes na rede; precificação da energia em tempo real; ou controle do perfil exercido por gerações de energia renováveis de modo a estabilizar a rede quando necessário (U.S. Department of Energy, 2021).

Uma característica importante das REI é a presença dos chamados recursos energéticos distribuídos (REDs), os quais abrangem os diferentes mecanismos para a geração de energia renovável e os sistemas de armazenamento de energia. Na última década, os REDs têm aumentado consideravelmente, principalmente pelas inúmeras vantagens que eles proporcionam tanto à rede elétrica quanto aos consumidores finais, por exemplo, diminuição da emissão de carbono, aumento na estabilidade e confiabilidade da rede (Carvalho e Saleem, 2019). Contudo, como consequência do aumento dos REDs, as redes elétricas precisam se adaptar de forma a atender os problemas operacionais causados pela presença de fluxos de energia bidirecional (Li et al., 2017).

A utilização de REDs nas redes elétricas permite a existência de microrredes localizadas em diversas partes do sistema de distribuição da energia elétrica. De acordo com o Microgrid Exchange Group's Department of Energy and implementation professionals (órgão dos EUA), uma microrrede é definida como: "um grupo de cargas e REDs interconectados, que agem como uma única entidade controlável com relação à rede, com limites elétricos claramente definidos. Ele pode operar tanto conectado à rede como de maneira ilhada, se conectando ou desconectando da rede elétrica" (Ton e Smith, 2012). No contexto das REIs, as microrredes têm sido vistos como uma poderosa plataforma para a construção de sistemas de distribuição elétrica mais eficientes, seguros, sustentáveis, confiáveis e resilientes. Sistemas de controle hierárquicos permitem a integração das microrredes com os REDs (Shahidehpour e Clair, 2012). Com isso, as microrredes

permitem mitigar o impacto negativo causado por interrupções no fornecimento de energia, porque podem operar ilhadas da rede principal quando necessário.

A REI tem como principal função prover eletricidade, de maneira permanente, confiável e segura a seus consumidores (Carvalho e Saleem, 2019). Para o correto funcionamento das REIs, é necessária uma complexa rede de computadores, softwares e interfaces de comunicação (Mantere et al., 2014). Assim como destacado em Yu e Xue (2016), as microrredes podem ser monitoradas e controladas de forma eficiente e confiável utilizando dispositivos eletrônicos inteligentes com base na interação dos sistemas físicos (infraestrutura da rede elétrica) e cibernéticos (sensores, TIC e tecnologias avançadas). Entretanto, existem vulnerabilidades inerentes aos sistemas devido à estreita interconexão entre os componentes cibernéticos e físicos (Nejabatkhah et al., 2021). Nesse sentido, ataques nas redes elétricas podem ter consequências devastadoras. Um exemplo disso, é o ataque cibernético lançado por hackers contra um trecho do setor elétrico da Ucrânia em dezembro de 2015, que deixou cerca de 225.000 consumidores ao longo do país sem energia por mais de seis horas, acarretando uma perda de mais de 130 MW de carga (Whitehead et al., 2017).

O presente trabalho realiza uma revisão bibliográfica sobre a segurança cibernética em redes elétricas inteligentes, com foco especial em microrredes, procurando contribuir como uma base para o entendimento delas. Além disso são apresentadas algumas de suas principais vulnerabilidades e técnicas de defesa, e as leis nacionais e internacionais que regulamentam a segurança dessas Microrredes. Este trabalho procura também levantar uma discussão sobre a situação atual da segurança das microrredes, bem como panoramas para o futuro deste campo de pesquisa.

2. VISÃO GERAL DAS MICRORREDES

É importante destacar que, embora existam diversas definições sobre conceito de microrrede, elas ainda precisam atingir um consenso. Isso acontece principalmente porque existem características particulares em cada sistema elétrico de cada país. Contudo, algumas características podem ser destacadas, em Li et al. (2017), os autores definem uma microrrede como um sistema de energia em pequena escala que agrupa REDs e cargas dentro de uma área local. Os REDs incluem unidades de geração de energia renovável, dispositivos de armazenamento, geradores convencionais e veículos elétricos. As microrredes podem ter seu sistema elétrico implementado e operado como corrente alternada (CA), corrente contínua (CC) ou um híbrido das duas. No Brasil, a Agência Nacional de Energia Elétrica (ANEEL) utiliza a seguinte definição: “Microrrede é uma rede de distribuição de energia elétrica que pode operar isoladamente do sistema de distribuição, atendida diretamente por uma unidade de geração distribuída”. Estas definições são complementares e permitem um entendimento claro do que é uma Microrrede é constituída.

Em relação aos componentes de uma microrrede, aqueles que estão mais sujeitos a ataques cibernéticos são os medidores inteligentes e os inversores inteligentes. Os medidores inteligentes podem ser definidos como o dispositivo eletrônico que realiza o monitoramento e o registro da energia uso por meios digitais e sem interrupção. Diferente do sistema de medição convencional, onde as leituras devem ser coletadas pelos prestadores do serviço, os medidores inteligentes encaminham as leituras de forma autônoma para seus prestadores de serviços para faturamento imparcial e livre de erros. O medidor inteligente captura e registra a frequência, bem como a tensão e os dados elétricos, e suporta a comunicação no padrão bidirecional existente entre a central e o sistema de medidores. Os dados gerados pelo medidor inteligente consistem em informações de timestamp, identificador de medidor único, valores de consumo de eletricidade etc. O medidor inteligente também permite controlar a carga remotamente, tendo a capacidade de governar vários dispositivos utilitários a fim de equilibrar a carga e as demandas (Khadar et al., 2017). Algumas vantagens de seu uso são: a detecção mais rápida de falta de energia, resposta e restauração; manter os clientes mais bem informados sobre o status da rede elétrica; e a melhoria da resiliência contra interrupções de energia (Yeung e Jung, 2013). Por sua vez, os inversores inteligentes podem ser definidos como inversores com funções avançadas de controle que podem ser usados para ajudar na operação da rede (Standard IEC/TR 61850-90-7, 2013). O papel de um inversor inteligente em uma microrrede é operar como uma interface entre os pontos de geração e consumo de energia, não se limitando à conversão CA-CC ou vice-versa, mas também a controlar o fluxo de energia, detectar falhas, desconectar quando necessário e outras funções. Portanto, pode-se afirmar que os inversores são os componentes de pensamento e processamento de uma microrrede, que coletam dados e as configuram a fim de operar em um ambiente seguro, controlado e eficaz (Arbab-Zavar et al., 2019).

2.1 Microrredes e sistemas físico cibernéticos

As microrredes podem ser entendidas como sistemas físico cibernéticos, dominadas por elementos de conversão eletrônica de potência, que, por sua vez, são utilizados na interface entre os geradores distribuídos, os sistemas de armazenamentos e as cargas. Sendo assim, seus componentes elétricos estão estreitamente interligados pelas TICs. Com isso, suas operações estão fortemente acopladas à funcionalidade do sistema cibernético (Nejabatkhah et al., 2021), como por exemplo a capacidade de detectar as transformações nos processos físicos e reagir em tempo real para garantir os requisitos funcionais e de segurança do sistema (Guzman et al., 2020).

Existem diferentes perspectivas sobre como diferenciar a estrutura funcional de uma microrrede. Para classificar de maneira mais clara a informação destas estruturas, além de apresentar de maneira mais compreensível as divisões que um sistema de potência possui, alguns autores consideram que o uso de uma abordagem por camadas pode ser seguida (Carpintero-Rentería et al., 2019). De acordo com Li et al. (2017), os modelos físicos das microrredes possuem quatro camadas que diferenciam seus componentes de acordo com sua função na rede de maneira geral: processo físico, dispositivos de campo, rede de comunicação e centro de controle.

O centro de controle (CdC) de uma microrrede troca continuamente informações com dispositivos de campo usando protocolos dedicados sobre a rede de comunicação. Os sensores fazem medições contínuas dos processos físicos a fim de monitorar o estado operacional da microrrede (tensão, corrente, frequência, entre outros) e as condições ambientais (por exemplo, temperatura ou umidade). O CdC periodicamente requisita os dados dos sensores através do sistema SCADA e depois processa as medições em tempo real usando um conjunto de aplicações do sistema de gerenciamento de energia (estimativa do estado, despacho econômico, gerenciamento da demanda). Ao executar estas aplicações, o CdC consegue otimizar os horários de geração dos REDs, manter estabilidade da frequência e tensão, e fornecer serviços de energia de alta qualidade para clientes em qualquer condição operacional. Nesse sentido, o CdC, quando necessário, envia sinais de controle (abertura/fechamento de interruptores de linha, ajuste das configurações de potência de saída dos REDs, resposta à demanda sinais) através do sistema SCADA para instruir as funções de dispositivos de campo, que são implementadas por atuadores no processo físico (Li et al., 2017).

Em geral, os ataques cibernéticos podem afetar quatro aspectos centrais dos sistemas de energia (Nguyen et al., 2020):

- Estimativas de estado: dados falsos na rede podem ocasionar estimativas de estado erradas que resultam em planos de contingência falhos, podendo haver falta de energia inesperada em caso de desligamento de algum ponto da rede.
- Controle automático de geração: um ataque de energia falsa afeta o processo de definição das rotas de energia (em condições normais esse processo determina as rotas de energia ideais para demanda de carga e geração). Quando os dados são adulterados, esse processo fica comprometido, podendo gerar mensagens de demanda de energia e necessidade de fornecimento que não sejam reais (Liang et al., 2017).
- Controle de tensão: caso o ataque seja realizado em algum ponto de acesso do sistema SCADA, lançando ações de controle, pode-se comprometer os dados das medidas reais como ângulo e magnitude de tensão de barras do sistema, afetando diretamente a segurança física dos sistemas de energia (Liang et al., 2017).
- Mercado de energia: a estimativa de estado também é explorada no despacho econômico de restrição de segurança para o estabelecimento do mercado de energia elétrica em tempo real. Esta questão pode ser considerada como uma motivação para que o adversário ataque furtivamente esta estimativa de estado, alterando os valores do preço marginal local da energia no mercado de eletricidade em tempo real (Ganjkhani et al., 2019), de modo a favorecê-lo com preços mais baixos de energia.

3. AMEAÇAS CIBERNÉTICAS NAS MICRORREDES

De acordo com o *National Intitute of Standards and Technology* (NIST), uma ameaça cibernética é: "qualquer circunstância ou evento com potencial para afetar negativamente as operações ou ativos organizacionais, indivíduos, outras organizações, ou a nação através de um sistema de informação via acesso não autorizado, destruição, divulgação, ou modificação de informações, e/ou negação de serviço" (NIST, 2012). Nesse sentido, vulnerabilidades cibernéticas são falhas ou fraquezas de um sistema que foi exposto a ameaças e podem existir no sistema cibernético da microrrede, desde os sistemas de informação internos, à rede de comunicação, e até os dispositivos de campo, sendo potencialmente exploradas por atacantes para obter um meio de acesso não autorizado ao sistema cibernético de uma microrrede, para comprometer suas operações.

3.1 Vulnerabilidade das Microrredes

Atualmente as redes de potência são compostas pela parte física do sistema elétrico e pelo sistema de comunicação. Ambos apresentam diferentes vulnerabilidades que podem ser comprometidas em um ataque cibernético (Nguyen et al., 2020). De acordo com Li et al. (2017), os requerimentos básicos de segurança cibernética de qualquer rede elétrica são, respectivamente de acordo com sua prioridade:

- Disponibilidade: se refere a garantir que os dados são acessíveis e atualizados. Qualquer latência ou perda de sincronização pode prejudicar a consciência situacional e impactar o desempenho operacional da microrrede.
- Integridade: se refere a garantir que os dados são confiáveis e precisos. Os dados devem sempre representar as informações reais sob todas as condições operacionais.
- Confidencialidade: se refere a proteger os dados de serem acessados e compreendidos por pessoas não autorizadas.

Os ataques cibernéticos podem tomar diversas formas, mas os cinco tipos de ataques mais comuns são descritos a seguir:

- *Denial of service* (DoS): sobrecarga intencional do sistema de comunicação para restringir o acesso a usuários legítimos da rede, causando lentidão e congestionamento da rede (Nguyen et al., 2020; Mirkovic e Reiher, 2004).
- *False data injection attack* (FDIA): injeção de dados falsos utilizando a linha de comunicação entre sensores físicos e o centro de controle (Liang et al., 2017). Esse tipo de ataque pode resultar em cenários diferentes, desde roubo de energia a erros de cálculo da tarifa local e até danos físicos à rede de potência, dependendo das intenções do intruso (Nguyen et al., 2020).
- Roubo de energia: inserção de *Malware* ou *Worms* para o roubo de certificados de segurança da rede (Mousavian et al., 2018).
- *Man-in-the-middle* (MITM): neste ataque o invasor ganha acesso aos sistemas de comunicação para manipular os dados trocados entre dois dispositivos da rede (Carvalho e Saleem, 2019).

- *Eavesdropping*: neste ataque, o invasor tenta adquirir dados válidos e informações sobre o sistema. Assim que a informação é adquirida, ele pode usá-la para outros propósitos maliciosos ou ataques cibernéticos (Carvalho e Saleem, 2019).

3.1.1 Vulnerabilidade nos Medidores e Inversores Inteligentes

Como os medidores inteligentes são o ponto de conexão entre as concessionárias e os clientes, eles são um componente vital ao monitorar e transmitir os parâmetros de uso elétrico. Se estes equipamentos forem passíveis de ataques, podem ocorrer desastres, já que os operadores da rede carecem das informações mais básicas e essenciais sobre o consumo de energia no nível de distribuição (McLaughlin et al., 2013). Os ataques a medidores inteligentes podem ser ataques físicos ou ataques nos sistemas de comunicações. Os autores em (Kondoro et al., 2018) realizam um estudo de caso de três ataques que podem afetar medidores inteligentes (roubo de energia, perda de privacidade e negação localizada de energia).

Por sua vez, os inversores inteligentes também são vulneráveis a ataques cibernéticos físicos e em seus sistemas de comunicação. De acordo com os autores em (Surya et al., 2021), estes ataques podem ser classificados como ataques a disponibilidade de dados, ataques a integridade dos dados e ataques a confidencialidade dos dados. No ataque a disponibilidade de dados, os atacantes fazem com que os dados necessários à rede não estejam disponíveis nos momentos de transientes ou ilhamento; no ataque a integridade de dados, os atacantes manipulam as medidas na rede de comunicação, de modo a gerar desbalanço na tensão e variações na frequência no inversor, impedindo sua sincronização com a rede; por fim, nos ataques a confidencialidade de dados, os atacantes não causam danos ao funcionamento da rede, mas obtêm acesso aos dados dos usuários dela (por exemplo suas identidades e uso de energia). Na referência (Liu et al., 2016) é apresentado um estudo de caso que aborda ataques nas redes de comunicação de inversores inteligentes, de modo a comprometer seu controle de frequência na microrrede.

3.2 Detecção de ataques cibernéticos

Um fator importante da resiliência das microrredes é a sua capacidade de detectar ataques que porventura estejam acontecendo, de modo que seu controle interno possa atuar para mitigar os possíveis danos causados por esses ataques. Em Tan et al. (2020), os autores realizaram uma pesquisa sobre métodos para detecção de ataques cibernéticos em sistemas físico cibernéticos. Os principais métodos de detecção abordados pelos autores em Tan et al. (2020) envolvem três frentes: detecção de ataques contra sensores e atuadores, detecção de ataques em sistemas não lineares (que possuem propriedades não lineares devido a suas características e ambiente externo) e detecção de ataques na presença de ruído/perturbações (gerados pelo *jitter* na amostragem e acionamentos irregulares e erros de sincronização entre os componentes do sistema físico cibernético analisado) e erros na modelagem do sistema. Todos se baseiam na estimativa de estado do sistema.

Os autores Musleh et al. (2020) apresentam em seu trabalho formas de detecção de ataques de injeção falsa de dados em redes elétricas inteligentes, podendo ser estas, métodos de detecção baseados em modelos de operação da rede e algoritmos de detecção orientados por dados.

Li et al. (2017) e Nejabatkhah et al. (2021) também abordam de maneira superficial alguns modelos de detecção de ataques em microrredes, como o uso de rede definida por software para construção de técnicas de detecção de intrusos e detectores estáticos e dinâmicos de ataques.

4. GERENCIAMENTO DO RISCO CIBERNÉTICO NAS MICRORREDES

Neste item serão apresentados os aspectos da microrrede frente a ataques cibernéticos, como por exemplo sua resiliência, métodos e modelos de proteção e estratégias para recuperação de seu funcionamento quando sofrendo um ataque bem-sucedido.

4.1 Resiliência das redes de energia a ataques cibernéticos

A resiliência de um sistema de energia se baseia na habilidade do sistema de lidar com eventos extremos de baixa probabilidade e alto risco, incluindo desastres naturais extremos e ataques cibernéticos (Bie et al., 2017). A eficiência de uma infraestrutura resiliente depende em sua habilidade de antecipar, absorver, se adaptar ou rapidamente se recuperar de um evento potencialmente perturbador (Presidential Policy Directive 21, 2013).

A Fig. 1(a) apresenta a performance de recuperação de uma microrrede dividida em 4 etapas. A 1ª etapa é a operação normal do sistema antes da perturbação, a 2ª etapa é o acontecimento de alguma perturbação na rede, a 3ª etapa é a preparação do sistema para retornar ao estado normal de operação novamente e na 4ª etapa finalmente acontece a ação de recuperação do sistema. Quando se compara com a Fig. 1(b), é possível perceber que a 3ª etapa não está presente, isso acontece porque a resiliência do sistema é maior, ou seja, assim que a perturbação acontece, a microrrede se adapta e se recupera com maior velocidade do que no primeiro caso. Na Fig 1(b), pode-se observar que uma resposta proativa e estratégia de recuperação implementada de forma automática pode minimizar ou mesmo evitar o tempo de preparação quando o evento atinge a rede elétrica, aumentando a resiliência do sistema (Nguyen et al., 2020).

4.2 Proteção contra os ataques cibernéticos

Em uma microrrede com sistemas centralizados, a efetivação de ataques seria relativamente mais simples. Uma solução para essa situação, muito utilizada em redes estadunidenses para defesa contra os ataques terroristas é a distribuição dos recursos existentes em vários nós, dificultando o processo de derrubar esse tipo de rede. Isso é possível pois esse tipo de sistema pode ser subdividido em partes ainda menores, podendo atuar de forma autônoma ou também em colaboração, mas permanecendo isoladas (S&C Electric Company, 2019).

Outra arquitetura possível envolve o uso de equipamentos de reserva, que serão acionados de imediato após a falha do equipamento primário. Um exemplo disso seria um software de gerenciamento para painéis fotovoltaicos, onde, caso ele sofra um ataque, a microrrede pode ser programada para que a

geração de energia não seja interrompida e busque como solução outras fontes, como armazenamento ou até cogeração térmica (S&C Electric Company, 2019).

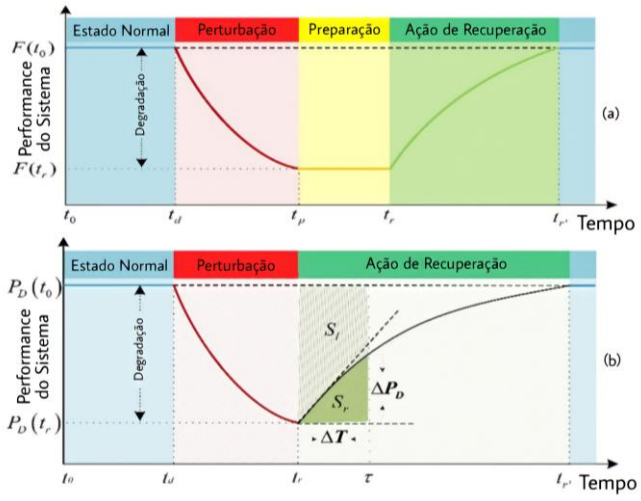

Fig. 1 Performance de recuperação da Microrrede. (a) Microrrede comum, (b) Microrrede resiliente; adaptado de (Nguyen et al., 2020).

Por fim, pode-se descentralizar também o sistema de gestão central da microrrede. Essa proteção, garante que caso haja um ataque cibernético de modo que afete um controlador da rede, outro controlador reserva assumiria de imediato toda a gestão da rede. Assim, é garantido, o tempo mínimo necessário para que os gestores da rede identifiquem, tratem e resolvem a falha sem que ocorram prejuízos no fornecimento a instalações e servidores (S&C Electric Company, 2019).

Portanto é muito importante o bom conhecimento da arquitetura da rede, verificando suas limitações, qualidade dos equipamentos e identificação de como o inimigo pode atacar a rede para definição de uma melhor forma de defesa. É importante entender também, que muitas dessas microrredes foram projetadas e construídas antes mesmos da existência de ataques cibernéticos, e que a grande maioria delas ainda trabalha com uma arquitetura centralizada.

Algumas contramedidas para ataques possíveis, retiradas de Ahmed e Pathan (2020), são listadas na tabela 1. Essas medidas estão direcionadas aos dois tipos de ataques mais comuns utilizados por hackers (DoS e FDIA). Para ambos, o intuito das contramedidas abordadas está no ato de interromper o ataque, devolver a origem ou até descobrir o ponto em questão. Para o DoS e para o caso de devolver o ataque até a origem, pode-se citar medidas como *Pushback*. No âmbito de descobrir a origem, pode-se utilizar o rastreamento de pacotes IP, D-WARD e o DefCOM (uma evolução do D-WARD). Em comparação ao FDIA, a maiorias das contramedidas possuem funções que variam de parâmetros de medição sobre dados falsos e reais (Autenticação Hop by Hop, Blockchain, Distância de KLD) até filtragens (Filtro de Kalman).

5. LEGISLAÇÃO VIGENTE

Segundo a ANEEL as distribuidoras são avaliadas em diversos aspectos no fornecimento de energia elétrica. Essas avaliações seguem padrões definidos nos Procedimento de Redes de Distribuição (PRODIST). Entre eles, está a qualidade do serviço e do produto oferecidos, sendo que a qualidade compreende a avaliação das interrupções no fornecimento de energia elétrica (ANEEL, 2021). Os indicadores destacados no PRODIST são fundamentais para garantir a prestação de serviços de qualidade através de fiscalizações rigorosas, sendo que as empresas que descumprem as normas estabelecidas podem sofrer punições que vão desde advertência e multas até a cassação da concessão. O processo administrativo punitivo de fiscalização da ANEEL é regido pela Resolução nº 846, de 11 de junho de 2019.

O ordenamento jurídico brasileiro respalda através de seus preceitos jurídicos a segurança cibernética. O decreto nº 10.222/2020 dispõe a respeito da Estratégia Nacional de Segurança Cibernética. Nesse sentido, os órgãos e entidades da administração pública federal serão responsáveis na gestão da implementação das ações estratégias previstas para publicação no sítio eletrônico do gabinete de segurança institucional da presidência da república. Ademais, o Decreto nº 9.637/2018 prevê a Política Nacional de Segurança da Informação, com o intuito de contemplar a defesa cibernética, a segurança da informação sigilosa, a proteção contra vazamento de dados e a segurança das infraestruturas críticas.

Em consonância, o direito internacional também regulamenta a proteção de dados com o intuito de promover a segurança cibernética. Em 2000, o Canadá adotou a legislação conhecida como *Personal Information Protection and Electronic Documents Act*. Além disso, no EUA, no estado da Califórnia entrou em vigor a legislação *California Consumer Privacy Act*, inspirada no Regulamento Geral sobre a Proteção de Dados 2016/679, que se trata de um regulamento do direito europeu sobre a privacidade e proteção de dados.

6. DISCUSSÃO

A segurança cibernética em microrredes é um assunto complexo e multidisciplinar, com desdobramentos econômicos e sociais. Sua complexidade deriva da interação entre os sistemas físicos com os sistemas cibernéticos, que inserem comunicação de dados entre os componentes das redes, além dos impactos e motivações para ataques. Cada um dos sistemas, físico e cibernético, possui vulnerabilidades específicas e sua atuação em conjunto cria vulnerabilidades inerentes à sua atuação.

Alguns dos principais problemas de vulnerabilidade são: os dispositivos suscetíveis a adulterações e ataques (como medidores e inversores inteligentes, redes de comunicações, protocolos adotados nas comunicações), a exposição das microrredes a comunicações com a internet e serviços externos; os centros de controles e utilização de dispositivos datados e que não possuem segurança embutida. Da mesma forma como foi destacado em Jamil et al. (2021), cada um destes pontos apresenta suas vulnerabilidades específicas, que podem ser exploradas por agentes maliciosos da rede, os quais podem realizar ataques por motivos diversos como terrorismo, ativismo político, retaliação ou roubo de energia. Este último é um problema que merece uma atenção especial em se tratando do cenário brasileiro de eletricidade, pois é o mais comum, bastante frequente e impactante, como pode ser identificado pelo relatório de perdas de energia elétrica de distribuição da ANEEL (2019).

Tabela 1. Contramedidas indicadas para ataques do tipo FDIA e DDoS

Sistemas e tecnologias específicas de proteção de microrredes		
Detecção FDIA	**Distância de KLD (*Kullback-Luibler*)**	Medição utilizada como parâmetro para distinção de medições reais obtidas por sensores em comparação com medidas injetadas por ciberataques. Essa contramedida age de forma que variações em distribuições de probabilidade são evidenciadas através de históricos de dados da plataforma.
	Ruído gaussiano colorido	Modelo que consiste na utilização de um GLRT (Teste de Razão de Verossimilhança Generalizada), com o intuito de detectar possíveis ataques.
	Autenticação de *Hop-by-Hop*	Trata-se de uma medida utilizada, que baseia sua medição no número de nós atingidos quando os mesmos excedem um limite predeterminado, a fim de identificar um ataque FDIA.
	Filtro de Kalman	Trata-se de um estudo que utiliza como medida a distância eucliadiana a fim de identificar FDIA.
	Blockchain	Muito utilizado baseando sua métrica em natureza descentralizada, autenticação criptográfica e mecanismos de consenso.
	Outros mecanismos	Aprendizado profundo da FDIA, otimização esparsa, correlações espaço-temporais, sistema de controle gaussiano invariante no tempo, medição de informação incompleta, criptografia de chave pública.
Ataques DDOS	**Novo sistema de rastreamento de pacotes IP**	Sistema que determina a origem de cada pacote recebido pela vítima do ataque. Dessa forma, a análise é feita em cima das assinaturas inseridas por cada roteador que o pacote percorreu no seu caminho até a vítima.
	Pushback	Consiste na medida de empurrar o tráfego de volta à origem.
	D-WARD	Consiste em um sistema que coleta informações de tráfego bidirecional (fonte e destino), para comparar com informações de tráfego utilizadas como referências (tráfegos reais, duvidosos e de ataques), e assim pré-determinar taxas que ofereçam limites a fim de detectar os ataques.
	NetBouncer	Mecanismo focado na legitimidade e veracidade de um cliente, assim permitindo seu tráfego. Utilizando vários tipos de teste usuário/cliente para checar sua veracidade, uma vez confirmado a posição do cliente, ele é adicionado a uma lista de clientes legítimos, no qual possui preferência sobre aqueles que ainda não foram legitimados. Caso o criminoso cibernético decida forjar uma autenticação, após um certo período a assinatura expira, sendo necessária uma nova.
	DefCOM	Mecanismo que detecta o ataque e limita o tráfego de forma que apenas o tráfego legítimo passe. Funciona baseado em 3 nós: geradores de alerta que identificam os ataques, limitadores de taxa de tráfego e classificadores que desempenham a função de verificar e separar os pacotes reais de suspeitos. Em resumo, o DefCOM identifica ataques, limita utilizando taxas específicas e bloqueia tráfegos suspeitos. O DefCOM, utiliza o D-WARD como mecanismo de apoio a fim de melhoria e classificação dos resultados.
	Outros mecanismos	SOS (constatação dos pontos de acesso por parte dos clientes a fim de verificar legitimidade), COSSACK (análises e medições em tráfegos suspeitos baseados em históricos), PI (inserção de identificadores de percurso a fim de evitar pacotes falsos), SIFF (divisão do tráfego em privilegiado e não privilegiado utilizando permissões) e HCF (filtro de contagem de saltos, contabilizando passagem por roteadores através de análise do TTL).

Nesse sentido, maiores estudos devem ser realizados em diversas frentes, de maneira diversificada com o intuito de obter de uma rede elétrica extremamente segura. Algumas destas frentes são: mecanismos de proteção e detecção de ataques, desenvolvimento de medidas de segurança para os protocolos de comunicação adotados (como por exemplo criptografia de dados, métodos de conferência da integridade destes dados), gerenciamento de riscos quando a ocorrência de ataques não pode ser evitada, recuperação da rede e soluções para isolamento ou reparo dos trechos comprometidos, técnicas de controle descentralizadas (ação que pode evitar o comprometimento da rede como um todo quando seu centro de controle é comprometido), confiabilidade dos controles adotados nas microrredes, análise de controles e mecanismos de segurança necessários quando a microrrede opera conectada à rede principal ou de maneira ilhada, e avaliação de riscos.

Outro ponto muito importante são os bancos de ensaios (simuladores de ataques), vitais para o entendimento do comportamento do sistema sob ataques, bem como os impactos destes no sistema, pois a realização de testes de ataques não é plausível nos sistemas reais. No geral, esses bancos têm de ser virtuais por praticidade, o que leva a outro ponto de estudos e melhorias: softwares que possam ser utilizados em conjunto de modo a replicar de maneira fiel o comportamento do sistema físico cibernético da microrrede, por exemplo durante a troca de dados ou a sincronização do mundo cibernético com o físico (Canaan et al., 2020).

Além de estudos nas tecnologias, as normas atuais vigentes também precisam passar por profundos estudos e reformulações de modo a estarem de acordo com o funcionamento das microrredes e as necessidades básicas de segurança que cada participante desta rede tem de atender para participar da mesma de maneira não prejudicial.

Por fim, é importante destacar que a evolução das REIs para microrredes é não só uma tendência como o futuro. Sua evolução vem acompanhada de percalços, mas a resolução destes é a chave para uma distribuição de energia elétrica de melhor qualidade para todos. Os aspectos de evolução no quesito de segurança cibernética dessas redes para o futuro partem da identificação de rumos e perspectivas para a segurança das microrredes. Alguns desses rumos sugeridos pela literatura e que podem ser destacados são: autenticação de dispositivos na rede, investigação e melhoria de custos de arquiteturas de dispositivos com maior resistência a adulteração e sobrevivência, uso do protocolo internet IPv6 e 5G para segurança da microrrede, segmentação e virtualização do sistemas, gerenciamento de resiliência e suporte inteligente de decisões, autenticação e controle de usuários, detecção de intrusos sem comprometimento dos requerimentos de disponibilidade da microrrede, criptografia avançada para

segurança de microrredes, entre outros (Jamil et al., 2021). Além disso, é sempre importante frisar que, as próprias ameaças cibernéticas às quais estas microrredes estão expostas, evoluem e se tornam mais acessíveis com o avanço da tecnologia, tornando o estudo desta ciência ainda mais dinâmico e desafiador, pois as tecnologias e mecanismos de defesa precisam evoluir conjuntamente, de maneira a se adaptar às novas ameaças que possam surgir.

7. CONCLUSÕES

As microrredes têm se apresentado como uma excelente alternativa para o futuro da produção e distribuição de energia elétrica. Sua integração com mecanismos de tecnologia de informação e comunicação e recursos de energia distribuída tornam a rede mais confiável, robusta, menos poluente e fazem com que ela trabalhe de maneira inteligente, trazendo vantagem para todos os participantes, concessionária de energia elétrica e consumidores finais.

Porém, a inserção dos mecanismos de TIC traz vulnerabilidades as redes. Os conhecimentos de segurança cibernética de redes elétricas inteligentes têm se tornado cada vez mais relevantes em um contexto mundial, vide o quão danosos os ataques às redes elétricas podem vir a ser para os usuários da rede e concessionárias, já que os sistemas de distribuição de energia elétrica são parte das chamadas infraestruturas críticas da sociedade atual e precisam trabalhar com disponibilidade de serviço e integridade de dados o tempo todo. Sendo assim, com a constante evolução dos ataques cibernéticos, é necessário também evoluir nos estudos para evitar esses ataques, ou mitigá-los quando uma completa defesa não for possível. Ou seja, mesmo com o foco cada vez maior à segurança cibernética das microrredes, ainda existem extensos pontos a serem estudados de modo a dar continuidade a este tema. Alguns aspectos podem ser priorizados como tornar os protocolos de comunicação mais seguros ou elaborar estratégias eficientes para "enganar' possíveis atacantes. A implementação dessas estratégias leva à elaboração de mecanismos de defesa inovadores que impeçam ataques até então desconhecidos pela rede elétrica.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio do CNPq, Processo No. 309297/2021-4, da FAPESP, Processo No. 2016/08645-9 e da CAPES, código financeiro 001.

REFERÊNCIAS

Agência Nacional de Energia Elétrica – Aneel. Indicadores. Disponível em: www.aneel.gov.br/indicadores (acessado em 8 de Outubro 2021).

Agência Nacional de Energia Elétrica – Aneel. Micro-rede. Disponível em: www.aneel.gov.br/ (acessado em 6 de Outubro 2021).

Agência Nacional de Energia Elétrica – Aneel. Procedimentos de Distribuição de Energia Elétrica no Sistema Nacional – PRODIST, Módulo 8 – Qualidade de Energia Elétrica. Disponível em: www.aneel.gov.br/ (acessado em 8 de Outubro 2021).

Agência Nacional de Energia Elétrica – Aneel. Relatório Perdas de Energia Elétrica na Distribuição, Edição 01/2019. Disponível em: www.aneel.gov.br/ (acessado em 25 de Novembro 2021).

Ahmed, M. e Pathan, A. S. K. (2020). False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling*, Volume 8.

Arbab-Zavar, B., Palacios-Garcia, E. J., Vasquez, J. C., Guerrero, J. M. (2019). Smart Inverters for Microgrid Applications: A Review. *Energies 2019*, 12, 840, doi: 10.3390/en12050840.

Bie, Z., Lin, Y., Li, G. e Li, F. (2017). Battling the extreme: a study on the power system resilience. *Proceedings of the IEEE*, Volume 105 (no. 7), pp. 1253-1266.

Canaan B., Colicchio B. e Ould Abdeslam D. (2020). Microgrid Cyber-Security: Review and Challenges toward Resilience, *Applied Sciences*, 10(16):5649, doi: 10.3390/app10165649

Carpintero-Rentería, M., Santos-Martín, D., Guerrero, J.M. (2019). Microgrids Literature Review through a Layers Structure. *Energies 2019*, 12, 4381, doi: 10.3390/en12224381.

Carvalho, R. S. e Saleem, D. (2019). Recommended functionalities for improving cybersecurity of distributed energy resources. *Resilience Week (RWS)*, pp. 226-231.

European Network and Information Security Agency (ENISA). (2012). Smart Grid Security. Annex II – Security aspects of the smart grid.

Ganjkhani, M., Fallah, S. N., Badakhshan, S., Band, S. e Chau, K. W. (2019). A Novel Detection Algorithm to Identify False Data Injection Attacks on Power System State Estimation. *Energies*, Volume 12, doi: 10.3390/en12112209.

Guzman, N. H. C., Wied, M., Kozine, I. e Lundteigen, M. A. (2020). Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Systems Engineering*, Volume 23, pp. 189–210, doi: 10.1002/sys.21509.

International Electrotechnical Commission (IEC) (2013). Communication Networks and systems for Power Utility Automation, Part 90-7: Object Models for Power Converters in Distributed Energy Resources (DER) Systems. *Standard IEC/TR 61850-90-7*.

International Energy Agency (2011). Technology roadmap smart grid. Disponível em: https://iea.blob.core.windows.net/assets/fe14d871-ebcb-47d3-8582-b3a6be3662ba/smartgrids_roadmap.pdf (acessado em 14 de Setembro 2021).

Jamil N., Qassim Q. S., Bohani F. A., Mansor M. e Ramachandaramurthy V. K. (2021). Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research. *Applied Sciences*, 11(21):9812, doi: 10.3390/app11219812

Khadar, A., Khan, J. A. e Nagaraj, M. S. (2017). Research Advancements Towards in Existing Smart Metering over

Smart Grid. *International Journal of Advanced Computer Science and Applications (IJACSA)*, Volume 8 (no. 5), doi: 10.14569/IJACSA.2017.080511.

Kondoro, A., Ben Dhaou, I., Rwegsira, D., Kelati, A., Tenhunen, H. e Mvungi, N. (2018). A Simulation Model for the Analysis of Security Attacks in Advanced Metering Infrastructure. *2018 IEEE PES/IAS PowerAfrica*, pp. 533-538, doi: 10.1109/PowerAfrica.2018.8521089.B.

Li, Z., Shahidehpour, M. e Aminifar, F. (2017). Cybersecurity in distributed power systems. *Proceedings of the IEEE*, Volume 105 (no. 7), pp. 1367-1388.

Liang, G., Zhao, J., Luo, F., Weller, S. R. e Dong, Z. Y. (2017). A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid*, Volume 8 (no. 4), pp. 1630-1638.

Liu, S., Liu, P. X. e Wang, X. (2016). Effects of cyber attacks on islanded microgrid frequency control. *2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 461-464, doi: 10.1109/CSCWD.2016.7566033.

Mantere, M., Noponen, S., Olli, P. e Salonen, J. (2014). Network security monitoring in a small-scale smart-grid laboratory. *Ninth International Conference on Availability, Reliability and Security*, pp. 310-316.

McLaughlin, S., Holbert, B., Fawaz, A., Berthier, R., Zonouz, S. (2013). A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures. *IEEE J. Sel. Areas Commun.*, Volume 31, no. 7, pp. 1319–1330.

Mirkovic, J. e Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Comput. Commun.*, Review 34 (2), pp. 39–53.

Mousavian, S., Erol-Kantarci, M., Wu, L. e Ortmeyer, T. (2018). A risk-based optimization model for electric vehicle infrastructure response to cyber attacks. *IEEE Transactions on Smart Grid*, Volume 9 (no. 6), pp. 6160-6169.

Musleh, A. S., Chen, G. e Dong, Z. Y. (2020). A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Transactions on Smart Grid*, Volume 11 (no. 3), pp. 2218-2234.

National Intitute of Standards and Technology - NIST SP 00-30, (2012). Guide for conducting risk assessments, Revision 1.

Nejabatkhah, F., Li, Y. W., Liang, H. e Ahrabi, R. R. (2021). Cyber-security of smart microgrids: A survey. *Energies 2021*, Volume 14 (no. 1: 27).

Nguyen, T., Wang, S., Alhazmi, M., Nazemi, M., Estebsari, A. e Dehghanian, P. (2020). Electric power grid resilience to cyber adversaries: State of the art. *IEEE Access*, Volume 8, pp. 87592-87608.

Panajotovic, B., Jankovic, M. e Odadzic, B. (2011). ICT and smart grid. *2011 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS)*, pp. 118-121, doi: 10.1109/TELSKS.2011.6112018.

Pivotto, C. V. C. e Pimenta, L. C. S. (2006). Denial of service - Negação de Serviço. Disponível em: www.gta.ufrj.br/grad/06_1/dos/index.html (acessado em 14 de Setembro 2021).

Presidential Policy Directive (PPD) 21, (2013). The White House, Washington, DC, USA.

S&C Electric Company, (2019). Revista Microgrid Knowledge. Disponível em: www.sandc.com/globalassets/sac-electric/documents/sharepoint/documents---all-documents/documento-tecnico-100-t116p.pdf?dt=637692498243604455 (acessado em 16 de Agosto 2021).

Shahidehpour, M. e Clair, J. F. (2012). A functional microgrid for enhancing reliability, sustainability, and energy efficiency. *The Electricity Journal*, Volume 25 (no. 8), pp. 21-28.

Surya, S., Srinivasan, M. K., Williamson, S. (2021). Technological Perspective of Cyber Secure Smart Inverters Used in Power Distribution System: State of the Art Review. *Appl. Sci. 2021*, 11, 8780, doi: 10.3390/app11188780.

Tan, S., Guerrero, J. M., Xie, P., Han, R. e Vasquez, J. C. (2020). Brief survey on attack detection methods for cyber-physical systems. *IEEE Systems Journal*, Volume 14 (no. 4), pp. 5329-5339.

Ton, D. T. e Smith, M. A. (2012). The U.S. Department of Energy's microgrid initiative. *The Electricity Journal*, Volume 25 (no. 8), pp. 84-94.

U.S. Department of Energy, SmartGrid.gov. *The smart grid*. Disponível em: www.smartgrid.gov/the_smart_grid/smart_grid.html. (acessado em 13 de Setembro 2021).

Whitehead, D. E., Owens, K., Gammel, D. e Smith, J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, pp. 1-8.

Yeung, P. e Jung, M. (2013). Improving Electric Reliability with Smart Meters. *Silver Spring Networks*, White Paper.

Yu, X. e Xue, Y. (2016). Smart Grids: A cyber–physical systems perspective. *Proceedings of the IEEE*, Volume 104 (no. 5), pp. 1058-1070.