Mais segurança nas REDES ENERGÉTICAS

Estudo destaca os riscos dos ataques de injeção de dados falsos, estratégia que dispensa conhecimento profundo do sistema-alvo

» RAFAELA BOMFIM*

A crescente digitalização das redes elétricas, impulsionada pela expansão de fontes de energia distribuídas como baterias e painéis solares, trouxe também novos riscos cibernéticos. Um estudo publicado na revista *Engineering* chama atenção para uma ameaça em ascensão: os ataques de injeção de dados falsos (FDIAs), capazes de comprometer a estabilidade e o controle dessas redes. Com a presença de baterias e painéis solares, os sistemas elétricos passaram a depender de dados informatizados para operar com eficiência. Essa dependência expõe vulnerabilidades, como o acesso às informações de controle. Na tentativa de resguardar o sistema, pesquisadores trabalham para evitar que um FDIA distorça informações essenciais, provoque falhas operacionais e afete diretamente a confiabilidade da rede.

Os pesquisadores identificaram um novo tipo de ataque, o chamado FDIA de caixa-preta. Ao contrário das abordagens convencionais, que atuam na transmissão de dados, esse método atinge diretamente os dispositivos de medição. Usando uma rede adversária generativa (GAN), a incursão é executada de forma discreta, sem necessidade de conhecer a fundo o sistema, o que a torna ainda mais perigosa em aplicações reais.

Rodolfo da Silva Villaça, doutor em engenharia elétrica e professor da Universidade Federal do Espírito Santo (UFES), detalha o funcionamento da denominada "técnica da caixa-preta". "É um método de ataque cibernético em que a ação não se baseia no conhecimento do funcionamento interno do sistema-alvo, no caso, o sistema elétrico. Em vez disso, essa técnica se concentra na manipulação das entradas e saídas observáveis do sistema para atingir seus objetivos, manipulando diretamente os módulos de medição de fontes de energia distribuídas."

Contra-ataque

A estratégia do desenvolvimento de uma técnica estima os parâmetros dos controladores e filtros usados nas fontes de energia distribuídas, permitindo que a reação ocorra com maior precisão, reduzindo falhas e aumentando sua eficiência. Em testes realizados em um sistema de 39 barramentos da Nova Inglaterra, o impacto foi claro. A exatidão do modelo TSP diminuiu de 98,75% para 56% os danos causados à confiabilidade das redes inteligentes. O método utiliza diferentes configurações, incluindo diversas arquiteturas de redes neurais e sistemas-padrão do IEEE (Instituto de Engenheiros Eletricistas e Eletrônicos).

O método utiliza ajustes em tempo real e integração física para gerar vetores de ataque que se assemelham muito a dados operacionais legítimos, desafiando a detecção de sistemas convencionais para diferenciar das falhas originais dos equipamentos ou variações operacionais transitórias. Para executar a tarefa, é aplicado um modelo A3D que usa autocodificadores baseados em atenção para identificar anomalias, reconstruindo condições operacionais normais e comparando-as com as atuais.

Os resultados mostraram que o vetor de ataque consegue enganar uma ampla variedade de alvos, afetando tanto infraestruturas menores e também maiores. O que reforça a urgência de desenvolver mecanismos de proteção mais eficazes, capazes de lidar com ameaças em escala. Segundo o pesquisador Villaça, embora as soluções de segurança estejam avançando, os ataques continuam evoluindo com rapidez. "As tecnologias de defesa cibernética têm progredido, mas os métodos de ataque também ficam mais sofisticados, criando um cenário de constante disputa. Em áreas críticas como o setor elétrico, as ameaças muitas vezes se desenvolvem mais rápido do que as soluções. Por isso, é fundamental investir em inteligência artificial e adotar uma postura preventiva na proteção das redes inteligentes."

***Estagiária sob a supervisão de Renata Giraldi**

MPF

Sala de controle, com rede computadorizada interligada

Três perguntas para

HELDER ROBERTO DE OLIVEIRA ROCHA, doutor em computação científica e sistemas de potência e professor do Departamento de Engenharia Elétrica da Universidade Federal do Espírito Santo (UFES)

O Brasil está preparado para implementar soluções eficazes contra os ataques cibernéticos descritos no estudo, como os que envolvem integração de sistemas de energia renovável?

O Brasil ainda enfrenta desafios na implementação de medidas robustas contra ataques cibernéticos, especialmente devido à heterogeneidade da infraestrutura elétrica e à falta de regulamentação específica para a segurança do setor. Com a crescente adoção de fontes renováveis, que frequentemente dependem de sistemas descentralizados e da Internet das Coisas (IoT), a necessidade de proteção se torna ainda mais crítica. Para enfrentar essas ameaças de maneira eficiente, o país precisa investir mais em pesquisa, capacitação e regulamentação. As concessionárias de energia têm financiado pesquisas em universidades brasileiras sobre o tema. No entanto, tenho observado que, em quase todos os editais de projetos das concessionárias, há foco em inteligência artificial, enquanto poucos são voltados para a cibersegurança e a prevenção de ataques cibernéticos.

Como as redes adversárias generativas (GAN) para criar ataques furtivos podem afetar a operação de sistemas de energia no Brasil. tanto nas grandes cidades, como em áreas remotas?

Esses ataques podem causar um blecaute total no Brasil ou blecautes direcionados para determinadas cidades, e a restauração da rede pode levar dias, resultando em grandes prejuízos financeiros. Em áreas remotas com sistemas de energia distribuída, os ataques cibernéticos são mais fáceis de serem inseridos devido à menor proteção, embora também sejam menos visadas. Para mitigar esse risco, a implementação de sistemas de detecção baseados em IA, capazes de distinguir padrões artificiais de padrões naturais, torna-se essencial. As redes GAN podem ser utilizadas tanto para atacar quanto para proteger a infraestrutura elétrica. Essas redes são compostas por duas partes: uma responsável por gerar ataques e outra por identificá-los. Enquanto agentes mal-intencionados buscam aprimorar geradores de ataques cada vez mais sofisticados, os operadores do sistema elétrico precisam desenvolver identificadores eficientes para detectar e neutralizar essas ameaças.

A pesquisa mostra que os algoritmos de previsão de estabilidade transitória (TSP) são fundamentais para a operação das redes inteligentes. É possível aperfeiçoar a precisão e a segurança deles para evitar manipulações externas?

Podemos aprimorar a precisão e a segurança dos algoritmos de previsão de estabilidade transitória baseados em caixa-preta por meio da incorporação de técnicas como o aprendizado federado, que possibilita o treinamento distribuído sem a necessidade de compartilhar dados sensíveis. Além disso, a implementação de métodos robustos de detecção de anomalias, estimação dos dados de rede e mecanismos avançados de criptografia pode reduzir significativamente o risco de manipulação externa.

SUSTENTABILIDADE

Baterias de lítio e íons reutilizáveis

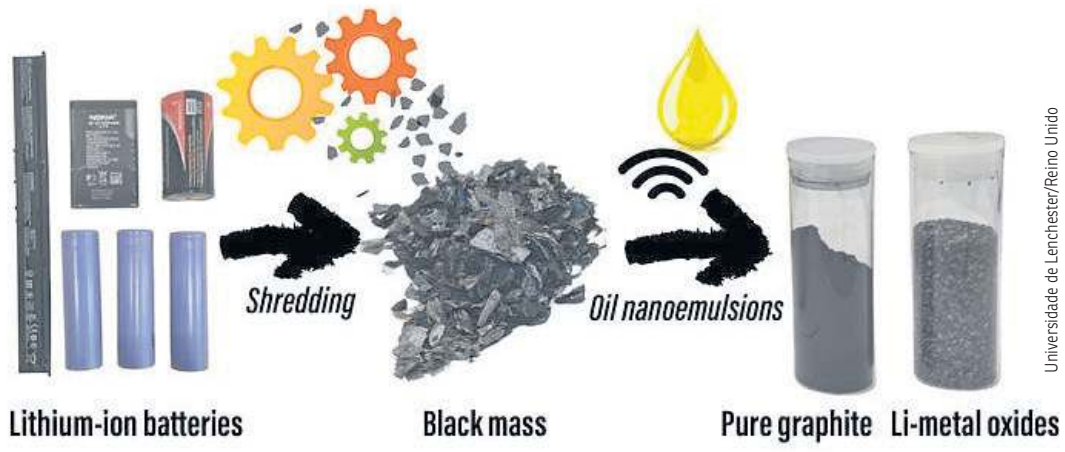
Com uma técnica inovadora e materiais específicos, pesquisadores das áreas de química e física da Universidade de Leicester, do Reino Unido, recuperaram metais em baterias já usadas. A iniciativa permitiu o reuso, o que antes era improvável. Para restaurar a chamada "massa negra", formada por íons de lítio, a base foi a água de torneira e temperatura ambiente e, em poucos minutos, o resultado apareceu. A substância, uma mistura de ânodo, cátodo e outros materiais de baixo valor, é transformada em óxidos metálicos puros, como lítio, níquel e cobalto (NMC).

A técnica é baseada no sistema de nanoemulsões preparadas com óleo de cozinha e que utiliza ultrassom. Esse sistema adere à superfície do carbono presente na massa negra, formando conglomerados que flutuam na água. Já os óxidos metálicos, por serem hidrofílicos, permanecem na solução e podem ser extraídos com facilidade.

De acordo com os pesquisadores envolvidos, o método apresenta um avanço significativo para a reciclagem sustentável de baterias, reduzindo a necessidade de extrair minérios e de novos recursos, minimizando danos ambientais. A simplicidade do processo facilita sua aplicação em larga escala, tornando a recuperação de metais mais acessível e eficiente para a indústria.

O trabalho se concentra em um projeto-piloto capaz de processar grandes volumes de massa negra. O objetivo é demonstrar sua viabilidade econômica e fornecer material de qualidade para a fabricação de novas baterias. De acordo com os cientistas, essa inovação, desenvolvida pela Universidade de Leicester, representa um avanço significativo na busca por soluções sustentáveis para o gerenciamento de baterias usadas. É que essa tecnologia tem o potencial de reduzir o impacto ambiental da produção e descarte de baterias, além de contribuir para uma economia circular eficiente.

Jake Yang, coautor do estudo, professor de química e física da Universidade de Leicester, está bastante otimista sobre o futuro do projetor. "O próximo passo é escalar isso e colocá-lo como parte de uma linha piloto que estamos desenvolvendo atualmente. Temos certeza de que essa técnica pode ser usada em vários campos onde as fases hidrofílicas e hidrofóbicas precisam ser separadas."



Universidade de Lenchester/Reino Unido

O material usado é transformado na "massa negra" e gera metais puros

A ideia de usar óleo de cozinha e água para reciclar baterias surgiu de tentativa e erro em busca de uma forma para criar energia renovável, segundo o professor do departamento de química e física da Universidade de Leicester, Andy Abbott que participou da pesquisa. "Achamos que os dois materiais que queríamos separar eram muito diferentes em sua hidrofobicidade, mas misturas simples de óleo e água não molharam nenhum dos materiais. Percebemos que precisávamos fazer as gotículas de óleo realmente pequenas e por isso, usamos ultrassom para criar uma nanoemulsão."

Testes

O método desenvolvido em Leicester oferece diversas vantagens em relação às técnicas de reciclagem tradicionais. É mais rápido, simples e barato do que os sistemas já em prática e não requer o uso de altas temperaturas ou ácidos corrosivos. A estrutura cristalina dos materiais recuperados não é danificada, o que permite a sua reutilização direta na fabricação de novas baterias.

Abbott, ressalta que trabalham com parte de um projeto para abordar todos os aspectos da reciclagem. "Devido à escala do problema, sabemos que o processo deve ser simples e barato, caso contrário, os fabricantes continuarão usando material virgem em vez de reciclado. Este é um passo importante devido à sua simplicidade, mas também ao volume que pode ser processado rapidamente e a um baixo custo."

O esforço agora, de acordo com os cientistas, é que essa tecnologia de fato revolucione os processos de reciclagem de baterias de íons de lítio no mundo. Com o crescente número de veículos elétricos e dispositivos eletrônicos, o reuso eficiente é fundamental para a transição para uma economia circular. (**RB**)