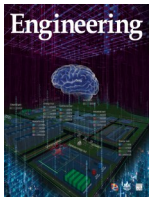
Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng



Research
Active Support of Power System to Energy Transition—Article

互联微电网可编程自适应安全扫描

姜自民[a]，唐泽帆[a]，张鹏[a,*]，秦彦源[b]

[a] Department of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY 11794, USA
[b] Department of Computer Science and Engineering, University of Connecticut, Storrs, CT 06269, USA

ARTICLE INFO

Article history:
Received 21 July 2020
Revised 14 November 2020
Accepted 29 March 2021
Available online 24 June 2021

关键词
互联微电网
可编程自适应安全扫描
协同检测
软件定义网络

摘要

现代微电网的重要特征是其核心的分布式能源和控制系统普遍依赖网络通信和软件系统。信息与物理系统的集成使得微电网获得了极佳的分布可控性、可扩展性和可观性；然而，恶意网络攻击者由此亦可以利用微电网信息物理系统中各种潜在的漏洞对微电网实施破坏。本文提出一种可编程自适应安全扫描（PASS）技术，用以保护电力电子化微电网系统免受各类电力机器人（power bot）的攻击。这一新技术尤其可以有效抵御三种危害性较大的攻击，即控制器操纵攻击、重放攻击和注入攻击。可编程自适应扫描融合软件定义网络与新的协同检测方法；这一新的安全措施可以使得微电网的互联具有超高的弹性和安全性、低成本与高度自动化等优点。协同检测结合了主动同步扫描和混沌检测两类新技术，可以有效识别电力机器人攻击的类型并对各类攻击快速定位，且不会中断或影响互联微电网的正常运行。可编程自适应安全扫描技术的有效性和实用性在大量实验中得到了确证。

1. 引言

互联微电网（NM）不仅可以灵活地容纳分布式能源（DER），而且可以自主协作地运行，“损有余而补不足”，以克服可能存在的功率不足问题，防止停电[1–2]。作为一种典型的信息物理系统，NM愈加依赖用计算机网络技术进行管理协调操作，处理突发事件并促进微电网应用的实施[3]。然而，这也带来了潜在的漏洞[4]。保证监测NM运行状态的传感器测量的大量重要数据以及用于完成不同微电网应用的各种控制信号的机密性、完整性和可用性，才能实现NM安全可靠运行[5]。此外，因DER由独立的微电网所有者拥有和运营，其分布式和即插即用的特性给运行带来了新的挑战，而NM运营商没有足够的能力管理高DER安全等级。NM必须应对一系列新的技术挑战，以管控新出现的风险，特别是制定新的对策，以识别和降低以DER为目标进行的攻击[6]对微电网运营造成的威胁，也就是利用网络机器人，即由远程攻击者控制的DER设备[1]。因此，为了应对这些挑战，NM运营商需要实施新方案以检测对独立拥有的微电网的网络攻击。

作为NM的基本组件，DER不仅可以发电，而且通过有线和（或）无线连接，可以用作多功能变换器的先进管理工具[7]。此种DER的广泛应用以及信息和操作技术的增加，极大地扩展了网络的连通性，从而扩大了网络攻击面。为了使系统达到更为灵活、可靠和有弹性的目标，一

* Corresponding author.
E-mail address: p.zhang@stonybrook.edu(P. Zhang)

英文原文：Engineering 2021, 7(8): 1087–1100
引用本文：Zimin Jiang, Zefan Tang, Peng Zhang, Yanyuan Qin. Programmable Adaptive Security Scanning for NetworkedMicrogrids. *Engineering*, https://doi.org/10.1016/j.eng.2021.06.007.

些逆变器会集成网络元素，包括各种通信和计算的基础设施[8]。然而，这些不可避免地增加部分DER逆变器遭受网络攻击的风险，甚至会出现损坏整个DER逆变器的情况。因此，攻击者并不仅限于攻击基于通信的微电网功能或应用。DER逆变器的某些对通信的依赖性较低的功能或控制，如下垂控制，也可能受到影响[9]。通过破坏DER逆变器，攻击者可以使微电网严重恶化或崩溃，造成电力系统的重大损失。近年来产生了几种不同的攻击方法，其中网络机器人攻击由于具有复杂性和严重破坏性，对逆变器的可靠运行构成了严重威胁[10,11]。单一的攻击环境下，如简单地修改逆变器控制器的参数很容易被检测[1,12]。然而在混合网络攻击环境下，这些方法却不适用。

在实际中，攻击者并不受限于规定的攻击方案。结合复杂、协调和同时攻击的攻击方案会造成更严重的破坏[13,14]。攻击检测必须利用特定的方法识别出恶意的微电网攻击，然后采取有效的对策，消除其对微电网稳定可靠运行的不利影响。最近关于联合攻击检测的工作主要集中在对高级计量架构相关功能的虚假数据传输、欺骗和拒绝服务攻击[15]，如负载频率控制。这些研究运用了残差或状态估计方法，包括卡尔曼滤波[16]、状态预测[17]、数字水印[10]和数据驱动技术的使用[18,19]。对系统模型和参数的高依赖性是基于模型的注入攻击和重放攻击检测方法的主要缺点。这些参数中存在的微小不确定性也会导致检测性能的降低[20]。此外，巨大的计算复杂度也阻碍了这些算法的应用性和可扩展性，特别是当迭代过程发散时。固定阈值的设置，尤其是当NM经历动态或负载变化时，也可能导致错误的攻击检测。虽然数据驱动的方法降低了由参数和建模的不确定性引起的误检测，但这需要大量的训练样本和较长时间的训练过程，难以适用于针对DER的网络攻击的检测，尽管这些方法可以很好地检测选定的样本，但并不适用于所有的情况，并且逆变器控制器的模型和参数也在不断变化[21]。因此，现有的大多数依赖模型、参数或数据的方法很难适用于在动态网络环境下检测更为复杂的网络机器人攻击，这些攻击以具有更高隐私性和不同控制策略的DER控制器[22]为目标。

与此同时，采用先进的通信基础设施和网络管理技术为NM提供了显著的效益[1,8]，软件定义网络（SDN）是一种促进可编程、可扩展和快速响应操作的NM的创新技术。SDN的引入有利于DER与各种通信技术的融合，直接实现网络可编程性、全系统通信可视化以及增强网络安全性和系统弹性[24]。此外，通过实施不同具有发展前景的防御算法，SDN彻底改变了互联中网络攻击的检测和解决办法[8,25]。然而，已有研究中没有提出能够检测和减轻多个网络机器人攻击NM的SDN集成方案。

为了解决上述问题，本研究侧重于利用知情方案检测和减少网络机器人攻击。本研究考虑了三种最常见的攻击类型，即控制器操纵（拓扑修改和参数覆盖）、重放攻击和注入攻击，设计了一种可编程自适应安全扫描（PASS）架构。该方法结合SDN技术和一种新的协同检测方法，能够以一种简化、省时和自主的方式实现可编程、可扩展和超弹性的NM。这种协同检测方法有两个实时检测器，可以在不受攻击方案限制的情况下识别网络机器人对DER控制器的攻击。本研究的关键内容如下：

（1）设计了一种新的支持SDN的PASS架构，用于实时检测DER逆变器上的网络机器人的攻击，具有良好的灵活性、可扩展性和超弹性；

（2）设计了一种由两个检测器组成的新型协同检测方法以有效检测网络机器人的攻击；

（3）推导了采用下垂控制的NM的PASS检测规则，并给出了区分攻击方案的动态探测信号和检测器的协调方法；

（4）进行了大量的仿真模拟研究，以验证PASS在保护NM方面的有效性和实用性。

本文其余内容安排如下：第2节介绍了PASS的总体架构；第3节介绍了两种检测器的协调检测方法和检测原理；第4节中通过测试验证了所提出的PASS方法的有效性和实用性；第5节对全文进行了总结。

2. 支持SDN的PASS架构

PASS框架如图1所示，由三层组成：①物理NM中的DER；②NM控制中心（NMCC）和支持SDN的网络层，用于监测运行状态、发送关键控制信号和生成可编程探测信号；③网络机器人攻击检测层，利用具有安全性、可编程性和弹性的SDN网络识别对DER逆变器的攻击。NMCC负责运行和控制NM并协调各种微电网应用，包括通过生成和传递可编程探测信号来实现PASS。具体来说，所有DER的运行状态（连接或退出）和逆变器控制器的响应都通过SDN网络进行持续监测并传输回NMCC，随后NMCC向DER发送控制和探测信号，用于处理NM操作和安全扫描。

如图1所示，逻辑集中的SDN控制器是实现PASS的基础。它提供高级的通信网络可视化和管理，以及详细的网络状况可视化，其中包括容量利用率和通信路径的选择。其动态可编程性和直接网络控制能力适应NM的特点，有利于促进PASS与NM的集成[1,8,26]，这主要由于

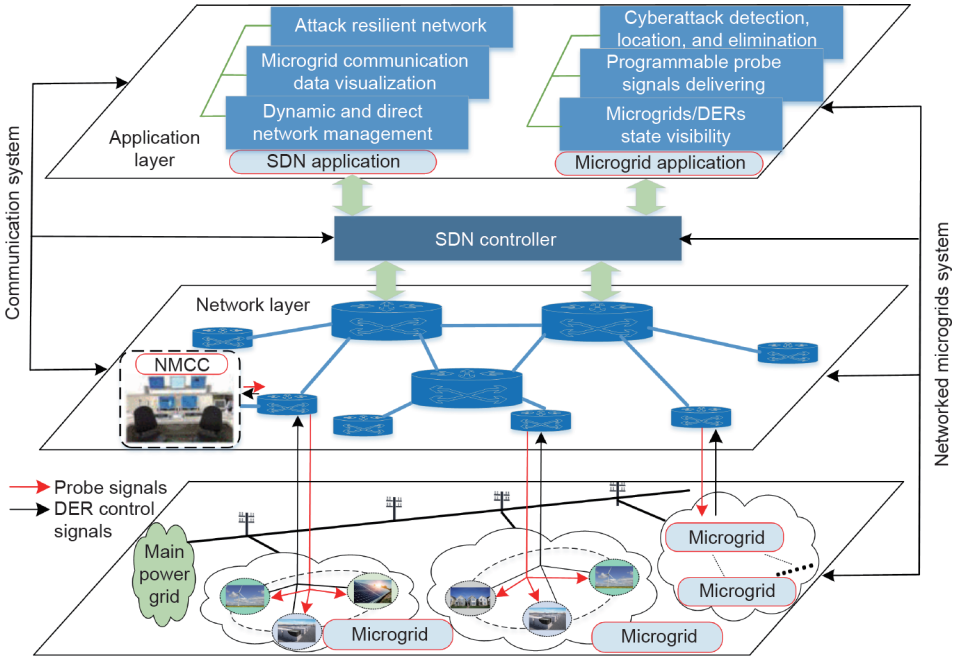


图1. PASS架构。

以下两个方面：

（1）弹性通信网络。通过重新配置交换机，SDN使控制和探测信号的按需通信路径完好无损，从而在通信攻击发生时或由于微电网的应用，如即插即用，造成拓扑变化时建立备选路径。

（2）实时通信网络验证。PASS和常规NM操作的时间关键特性都与完全连续的可访问通信网络相关。通过开发利用SDN提供的可编程和动态配置功能的自愈通信网络，由SDN提供的网络可见性和数据流可视化即使在网络故障和拥堵等异常的情况下，也能确保数据包成功发送到目标DER。

整个PASS流程总结如下：

（1）在正常情况，即无攻击情况下，在NMCC内部根据两个协同检测方法检测器的输出结果建立检测规则，如下一节所述。

（2）NMCC通过安全的SDN网络向DER控制器发送某些低幅值的正弦波探测信号。一旦信号被DER控制器接收，它的响应会通过SDN网络同步发送到NMCC。

（3）在NMCC内部进行协同检测，利用每个DER接收到的信息计算检测结果。

（4）将计算得到的检测结果与检测规则进行对比。一旦发生较大偏差，则检测到攻击。利用两种协同检测方法的检测器可以识别攻击类型。

具体来说，在NMCC中进行实时DER状态的可视化，以确定是否应该产生和传递新的探测信号。当微电网经历动态变化，如DER的连接/断开、控制策略变化以及微电网拓扑结构的变化时，应在进行攻击检测之前对检测程序进行相应调整。当DER连接时，应执行两个附加步骤：①对合适的探测信号进行编程；②对DER逆变器的探测信号和控制信号的路径进行配置。若是DER断开，NMCC则终止整个过程。当控制策略发生变化时，应根据新的控制策略重新创建检测规则，并对探测信号进行重新编程。当微电网拓扑发生变化时，在进行检测程序之前，还应对通信网络进行重新配置，确保DER与NMCC之间存在可靠的通信。

SDN的可编程性可以改变扫描频率和目标微电网，并且可以通过结合其他检测方法轻松扩展PASS。

3. DER逆变器控制器的协同检测方法

恶意攻击者可以同时发起不同的攻击来破坏DER。本文研究了基于下垂控制的NM中最常见的三种网络机器人攻击，即控制器操纵（拓扑修改和参数覆盖）、重放攻击和注入攻击。攻击者可以修改逆变器控制器的拓扑结构和参数，并操纵不同DER之间交换的数据。图2给出了三种网络机器人的攻击类型和已建立的网络安全检测方法。

为有效识别上述三类攻击，设计的协同检测方法使用了两个实时检测器：同步检测器（SD）[11]和杜芬振荡检测器（DOD）[27]。为确保实时检测网络机器人攻击和DER的正常运行，本研究将两个低幅值的正弦信号组合

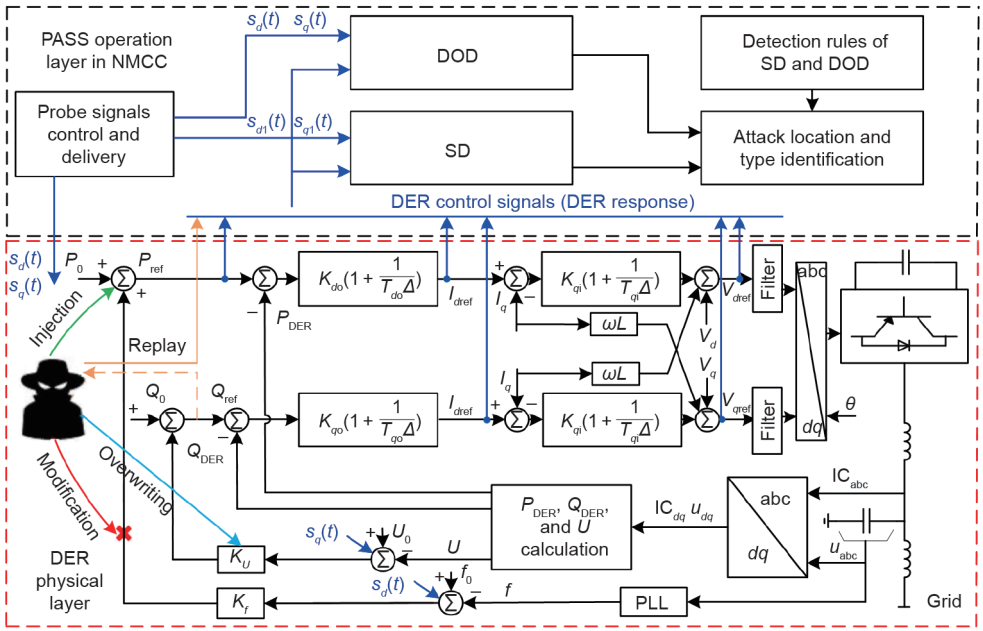


图2. 网络机器人对基于下垂控制的DER逆变器的攻击。DOD：杜芬振荡检测器；SD：同步检测器；u：瞬时电压；IC：瞬时电流；a、b、c：三相；d：直轴；q：交轴；PLL：锁相环；θ：电压相位；ω：角频率；f：电网频率；f_0：频率的初始运行值；U_0：电压初始运行值；U：电压均方根（rms）；I：电流均方根（rms）；Δ：拉普拉斯算子；PWM：脉宽调制；P：有功功率；Q：无功功率；P_0、Q_0：DER的初始有功和无功输出功率；V：参考电压；K_{do}、K_{qo}、K_{di}、K_{qi}：内外环控制器参数；K_U、K_f：下垂控制器参数；T_{do}、T_{qo}、T_{di}、T_{qi}：内外环控制器的时间常数；ref：参考。

作为探测信号，该探测信号须具有以下两个特点：①探测信号对DER逆变器的性能没有影响；②探测信号由于可编程特性不易被窃听。为了避免出现的对DER的扰动，探测信号的设计需具有三个特征，可以用数学表示为：①$s(t) = s(t+NT)$，其中，N为整数，②$\|s(f)\| \leqslant \varepsilon$和$\int_t^{t+T} s(t)\mathrm{d}t = 0$，其中，$t$为时间轴上的任意特定时刻，$T$为连续信号$s(t)$的周期，$\|*\|$是频率$f$处谐波的$L_2$范数，$\varepsilon$为小阈值。设计的探测信号要确保在一个周期内对目标DER的影响为零；换言之，探测信号不会改变DER控制器的整体性能，因此也可以避免对物理系统的扰动[1,11]。图2中的探测信号$s_d(t)$和$s_q(t)$表示如下：

$$s_d(t) = s_{d1}(t) + s_{d2}(t) = \alpha_{d1}\sin(\omega_{d1}t) + \alpha_{d2}\sin(\omega_{d2}t) \quad (1)$$

$$s_q(t) = s_{q1}(t) + s_{q2}(t) = \alpha_{q1}\sin(\omega_{q1}t) + \alpha_{q2}\sin(\omega_{q2}t) \quad (2)$$

其中，α_{dj}和α_{qj}为振幅；ω_{dj}和ω_{qj}（$j=1$或2）分别为正弦信号的频率。$s_{d1}(t)$和$s_{q1}(t)$通过同步检测器检测修改和重写攻击。$s_{d2}(t)$和$s_{q2}(t)$通过DOD检测重放和注入攻击。为确保没有干扰，ω_{d2}和ω_{q2}应分别为ω_{d1}和ω_{q1}的整数倍（≥2）。

检测这三种类型的攻击的协同性主要分为两个方面：①可编程探测信号与相应探测器之间的协同；②两个探测器的协调以识别攻击类型。需要说明的是本研究中设计的两个检测器在不需要系统模型和参数、计算复杂度和数据处理负担的情况下，仍能够有效地识别攻击，这些将在后续小节中进行讨论。

3.1. 同步检测器及其检测规则

（1）用于基于下垂控制的DER的检测器：下垂控制可以实现并网和孤岛运行之间的灵活切换。下垂系数对维持额定频率和电压十分重要。因此，对下垂控制器的攻击具有威胁性，因为它会导致NM立即恶化甚至崩溃。本节以f-P和U-Q型下垂控制器的检测为例，建立同步检测器的检测规则。值得注意的是，该方法适用于应用广泛且具有不同控制策略的dq双环控制器，相应的检测规则可用如下公式进行推导。

同步探测器实时工作以获取检测信号：

$$D = \frac{1}{T}\int_t^{t+T} s(t)\cdot r(t)\mathrm{d}t \quad (3)$$

其中，$s(t)$表示$s_{d1}(t)$或$s_{q1}(t)$；$r(t)$表示DER响应，即P_{dref}、Q_{dref}、I_{dref}、I_{qref}、V_{dref}或V_{qref}。D是检测信号，即D_f、D_U、D_{do}、D_{qo}、D_{di}或D_{qi}。下标代表的含义已在图2的标题中给出。

（2）检测规则：给定DER控制器的拓扑结构和参数，就可以得到检测信号。以D_{di}为例，表示如下：

$$
\begin{aligned}
D_{di} &= \frac{1}{T}\int_{t}^{t+T} s_{d1}(t)\cdot V_{d\mathrm{ref}}\,\mathrm{d}t \\
&= \frac{1}{T}\int_{t}^{t+T} s_{d1}(t)\cdot[(I_{d\mathrm{ref}}-I_d)K_{di}(1+\frac{1}{T_{di}s})-I_q\omega L+V_d]\,\mathrm{d}t \\
&= \frac{1}{T}\int_{t}^{t+T} s_{d1}(t)\cdot[(I_{d\mathrm{ref}}-I_d)K_{di}(1+\frac{1}{T_{di}s})]\,\mathrm{d}t+\frac{1}{T}\int_{t}^{t+T} s_{d1}(t)\cdot(-I_q\omega L+V_d)\mathrm{d}t \\
&= \frac{1}{T}\int_{t}^{t+T} s_{d1}(t)\cdot[(I_{d\mathrm{ref}}-I_d)K_{di}(1+\frac{1}{T_{di}s})]\,\mathrm{d}t+0 \\
&= \frac{K_fK_{do}K_{di}}{T}\int_{t}^{t+T} s_{d1}^2(t)(1+\frac{1}{T_{do}s})(1+\frac{1}{T_{di}s})\mathrm{d}t+\frac{K_fK_{do}K_{di}}{T}(1+\frac{1}{T_{do}s})(1+\frac{1}{T_{di}s})\int_{t}^{t+T} s_{d1}(t)s_{d2}\,\mathrm{d}t \\
&= \frac{\alpha_{d1}^2\cdot K_f\cdot K_{do}\cdot K_{di}}{2}(1-\frac{1}{T_{do}T_{di}\omega_{d1}^2})
\end{aligned}
\tag{4}
$$

其中，T为$s_{d1}(t)$的周期，记$\omega_{d2}=N\omega_{d1}$，其中N为整数，且$N\geqslant 2$。因此$\frac{1}{T}\int_{t}^{t+T} s_{d1}(t)\cdot s_{d2}(t)\mathrm{d}t=0$，同理，正常运行状态下的$D_f$、$D_U$、$D_{do}$、$D_{qo}$和$D_{qi}$可以推导如下：

$$D_f=\frac{1}{T}\int_{t}^{t+T} s_{d1}(t)P_{\mathrm{ref}}\,\mathrm{d}t=\frac{\alpha_{d1}^2K_f}{2} \tag{5}$$

$$D_U=\frac{1}{T}\int_{t}^{t+T} s_{q1}(t)Q_{\mathrm{ref}}\,\mathrm{d}t=\frac{\alpha_{q1}^2K_U}{2} \tag{6}$$

$$D_{do}=\frac{1}{T}\int_{t}^{t+T} s_{d1}(t)I_{d\mathrm{ref}}\,\mathrm{d}t=\frac{\alpha_{d1}^2K_fK_{do}}{2} \tag{7}$$

$$D_{qo}=\frac{1}{T}\int_{t}^{t+T} s_{q1}(t)I_{q\mathrm{ref}}\,\mathrm{d}t=\frac{\alpha_{q1}^2K_UK_{qo}}{2} \tag{8}$$

$$D_{qi}=\frac{1}{T}\int_{t}^{t+T} s_{q1}(t)\cdot V_{q\mathrm{ref}}\,\mathrm{d}t=\frac{\alpha_{q1}^2\cdot K_f\cdot K_{qo}\cdot K_{qi}}{2}(1-\frac{1}{T_{qo}T_{qi}\omega_{q1}^2}) \tag{9}$$

从公式（4）～（9）可得，每个D仅由控制器系数和探测信号的幅值或频率决定。任何改变控制器系数的攻击都会导致检测结果异常。在等式（3）中设计的探测器只需要控制器的响应，因此不会影响DER的私密性。

当所有DER控制器完好时，检测信号的稳态值D_f、D_U、D_{do}、D_{qo}、D_{di}和D_{qi}分别等于公式（4）～（9）中的值。一旦发起攻击，计算值将偏离既定的范围。相应地，①拓扑修改和②控制器参数覆盖/更改两类控制器操纵攻击下的异常值汇总如表1所示。表1所示的值是假定在特定攻击稳态下类似公式（4）～（9）推导得到的。由于攻击导致的扰动，这些值可能不等于实际的检测值。表1清楚地显示了两种控制器操纵攻击对所有可能位置的检测值的相应变化。将检测异常值与公式（4）～（9）和表1中的攻击类型进行比较，可以识别出这两种控制器的操纵攻击类型及其位置。

3.2. DOD及其检测规则

从DER发送给NMCC的数据和反向发送的控制信号都有可能暴露给攻击者。在本小节中，我们将介绍第二种检测器，即DOD，它通过与SD相协调，用于检测重放攻击和注入攻击。攻击者可以发起重放攻击，即通过先复制其记录的响应，然后将其重复或延迟发送给NMCC使SD失灵，因为NMCC无法收到实际的逆变器控制器响应。注入攻击可以通过向DER控制器注入附加恶意信号或直接将恶意信号注入检测层来破坏微电网的稳定运行或者使SD失效。

DOD的原理是在DER控制信号上叠加动态弱信号。DOD能够检测到幅值很低的微弱的正弦信号，并且不受噪声影响[27−29]。在本研究中，$s_{d2}(t)$和$s_{q2}(t)$的频率和幅值可以动态调整以构造认证信号，然后由杜芬振荡器检测该认证信号。任何记录的逆变器响应的重放都会改变预定的动态认证信号并进而改变相应的DOD运行模式，从而被检测出来。相反，虽然注入攻击由于DOD的选择性而对其运行模式没有影响，但仍会被SD检测到[27]，因此可以通过两个检测器的协同作用来识别这两类攻击。

（1）DOD：正常杜芬方程如下所示[29]：

$$\frac{\mathrm{d}^2x}{\mathrm{d}t^2}+\delta\frac{\mathrm{d}x}{\mathrm{d}t}-x+x^3=\gamma\cos(t), \tag{10}$$

其中，δ为阻尼比，多项式“$-x+x^3$”为非线性恢复力，$\gamma\cos(t)$为周期驱动力或参考信号。如果δ固定，γ增大，系统状态由无序运动变为大周期运动。当γ达到信号幅度阈值（本研究中δ为0.5时，γ为0.82）时，系统进入临界状态，此时杜芬振荡器变得非常敏感[28]。为了获得γ_c，可以增大驱动力幅度，观察杜芬振荡器系统的相位轨迹。只有当待检测信号与驱动力频率相同时，杜芬振荡器相位轨迹才会迅速进入周期状态；否则，系统仍然是无序的。这是杜芬振荡器的选择性，可用于检测重放攻击，如下所示。

表1 DER受攻击下的同步检测器的值

Controllers under attack	Attack types	D_f	D_U	D_{do}	D_{qo}	D_{di}	D_{qi}
Droop loop	①	0	0	0	0	0	0
	②	$\frac{\alpha_{d1}^2 K_f'}{2}$	$\frac{\alpha_{q1}^2 K_U'}{2}$	$\frac{\alpha_{d1}^2 K_f' K_{do}}{2}$	$\frac{\alpha_{q1}^2 K_U' K_{qo}}{2}$	$\frac{\alpha_{d1}^2 K_f' K_{do} K_{di}}{2}\left(1-\frac{1}{T_{do}T_{di}\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2 K_U' K_{qo} K_{qi}}{2}\left(1-\frac{1}{T_{qo}T_{qi}\omega_{q1}^2}\right)$
Outer loop	①	$\frac{\alpha_{d1}^2 K_f}{2}$	$\frac{\alpha_{q1}^2 K_U}{2}$	0	0	0	0
	②	$\frac{\alpha_{d1}^2 K_f}{2}$	$\frac{\alpha_{q1}^2 K_U}{2}$	$\frac{\alpha_{d1}^2 K_f K_{do}'}{2}$	$\frac{\alpha_{q1}^2 K_U K_{qo}'}{2}$	$\frac{\alpha_{d1}^2 K_f K_{do}' K_{di}}{2}\left(1-\frac{1}{T_{do}'T_{di}\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2 K_U K_{qo}' K_{qi}}{2}\left(1-\frac{1}{T_{qo}'T_{qi}\omega_{q1}^2}\right)$
Inner loop	①	$\frac{\alpha_{d1}^2 K_f}{2}$	$\frac{\alpha_{q1}^2 K_U}{2}$	$\frac{\alpha_{d1}^2 K_f K_{do}}{2}$	$\frac{\alpha_{q1}^2 K_U K_{qo}}{2}$	0	0
	②	$\frac{\alpha_{d1}^2 K_f}{2}$	$\frac{\alpha_{q1}^2 K_U}{2}$	$\frac{\alpha_{d1}^2 K_f K_{do}}{2}$	$\frac{\alpha_{q1}^2 K_U K_{qo}}{2}$	$\frac{\alpha_{d1}^2 K_f K_{do} K_{di}'}{2}\left(1-\frac{1}{T_{do}T_{di}'\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2 K_U K_{qo} K_{qi}'}{2}\left(1-\frac{1}{T_{qo}T_{qi}'\omega_{q1}^2}\right)$
Droop and outer loop	①	0	0	0	0	0	0
	②	$\frac{\alpha_{d1}^2 K_f'}{2}$	$\frac{\alpha_{q1}^2 K_U'}{2}$	$\frac{\alpha_{d1}^2 K_f' K_{do}'}{2}$	$\frac{\alpha_{q1}^2 K_U' K_{qo}'}{2}$	$\frac{\alpha_{d1}^2 K_f' K_{do}' K_{di}}{2}\left(1-\frac{1}{T_{do}'T_{di}\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2 K_U' K_{qo}' K_{qi}}{2}\left(1-\frac{1}{T_{qo}'T_{qi}\omega_{q1}^2}\right)$
Droop and inner loop	①	0	0	0	0	0	0
	②	$\frac{\alpha_{d1}^2 K_f'}{2}$	$\frac{\alpha_{q1}^2 K_U'}{2}$	$\frac{\alpha_{d1}^2 K_f' K_{do}}{2}$	$\frac{\alpha_{q1}^2 K_U' K_{qo}}{2}$	$\frac{\alpha_{d1}^2 K_f' K_{do} K_{di}'}{2}\left(1-\frac{1}{T_{do}T_{di}'\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2 K_U' K_{qo} K_{qi}'}{2}\left(1-\frac{1}{T_{qo}T_{qi}'\omega_{q1}^2}\right)$
Outer and inner loop	①	$\frac{\alpha_{d1}^2 K_f}{2}$	$\frac{\alpha_{q1}^2 K_U}{2}$	0	0	0	0
	②	$\frac{\alpha_{d1}^2 K_f}{2}$	$\frac{\alpha_{q1}^2 K_U}{2}$	$\frac{\alpha_{d1}^2 K_f K_{do}'}{2}$	$\frac{\alpha_{q1}^2 K_U K_{qo}'}{2}$	$\frac{\alpha_{d1}^2 K_f K_{do}' K_{di}'}{2}\left(1-\frac{1}{T_{do}'T_{di}'\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2 K_U K_{qo}' K_{qi}'}{2}\left(1-\frac{1}{T_{qo}'T_{qi}'\omega_{q1}^2}\right)$
Droop, outer, and inner loop	①	0	0	0	0	0	0
	②	$\frac{\alpha_{d1}^2 K_f'}{2}$	$\frac{\alpha_{q1}^2 K_U'}{2}$	$\frac{\alpha_{d1}^2 K_f' K_{do}'}{2}$	$\frac{\alpha_{q1}^2 K_U' K_{qo}'}{2}$	$\frac{\alpha_{d1}^2 K_f' K_{do}' K_{di}'}{2}\left(1-\frac{1}{T_{do}'T_{di}'\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2 K_U' K_{qo}' K_{qi}'}{2}\left(1-\frac{1}{T_{qo}'T_{qi}'\omega_{q1}^2}\right)$

K' represents the modified parameters of DER controllers by attackers (K). Attack types: ① topology modification; ② controller parameter overwrighting/changing.

为了检测认证探测信号，杜芬振荡器必须有一个输入信号（参考信号）。待检测的探测信号可视为参考信号的扰动。这两个信号的频率和幅度在NMCC内动态协调。根据DOD相位轨迹变化可以确定检测到的信号是否包含从NMCC发出的探测信号。杜芬振荡器不受噪声影响，因为它只影响局部轨迹，没有状态转换。

使用方程（10）检测不同频率的信号，须进行频率变换。定义$y = \mathrm{d}x/\mathrm{d}t = \dot{x}$，方程（10）可以改写为：

$$\dot{x} = y, \tag{11}$$

$$\dot{y} = -\delta y + x - x^3 + \gamma\cos(t). \tag{12}$$

令$t = \omega\tau$（τ是转换的中间变量），下列方程成立：

$$x(t) = x(\omega\tau) = x_*(\tau), \tag{13}$$

$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = \frac{\mathrm{d}x(\omega\tau)}{\mathrm{d}(\omega\tau)} = \frac{1}{\omega}\frac{\mathrm{d}x(\omega\tau)}{\mathrm{d}\tau} = \frac{1}{\omega}\frac{\mathrm{d}x_*(\tau)}{\mathrm{d}\tau}, \tag{14}$$

$$\frac{\mathrm{d}^2x(t)}{\mathrm{d}t^2} = \frac{\mathrm{d}^2x(\omega\tau)}{\mathrm{d}(\omega\tau)^2} = \frac{1}{\omega^2}\frac{\mathrm{d}^2x(\omega\tau)}{\mathrm{d}\tau^2} = \frac{1}{\omega^2}\frac{\mathrm{d}^2x_*(\tau)}{\mathrm{d}\tau^2}. \tag{15}$$

用方程（11）和（12）替换方程（13）~（15），省略下标x_*，适用于不同频率的方程如下：

$$\dot{x} = \omega y, \tag{16}$$

$$\dot{y} = \omega(-\delta y + x - x^3 + \gamma\cos(\omega t) + \Delta\gamma_t), \tag{17}$$

其中，$\Delta\gamma_t$为输入信号，包括探测信号和噪声。因为方程（16）和方程（17）从方程（10）导出，所以其系统特性和临界值不变。因此，在滤除直流（DC）分量后，可以将DER控制信号注入方程（16）和方程（17）检测重放攻击。

为了说明杜芬振荡器的工作原理，图3给出了杜芬振荡器的两个状态，其中从轨迹中的运动点到(−1,0)和(1,0)的距离之和用于快速自动状态识别。比较两种状态下的l，

可以看出大周期状态下 l 总是大于3，而混沌状态下的 l 介于2~4之间。因此，本研究使用了一个阈值，即 $l = 2.5$ 来识别状态，如图3中红色虚线所示。一旦 l 小于2.5，就可以确定杜芬振荡器处于混沌状态；否则，杜芬振荡器处于大周期状态。

（2）检测规则：设置杜芬振荡器参考信号使其处于混沌运动状态。将探测信号 $s_{d2}(t)$ 和 $s_{q2}(t)$ 与参考信号协调的幅值编译为每0.05 s或0.1 s改变一次，使振荡器在两种运动状态之间交替运行，如图4所示。由于频率小于或等于0.1 s，重放和注入攻击者注入杜芬检测器的信号与在NMCC中产生的信号不同。因此，NMCC预先定义的运行状态将因其灵敏度和选择性而被破坏，因此可以检测重放和注入攻击。

3.3. 攻击类型和位置的检测规则

NMCC向DER传送可编程探测信号。与上述两种检测器配合，根据算法1给出的协同检测方法的检测规则可以确定攻击类型。根据检测结果的异常值可以识别攻击位置。特别是对于同时注入和覆盖攻击的检测规则，随着注入信号的类型不同而略有不同。如果注入的信号是直流分量，则无法用算法1识别同时攻击，因为检测结果与仅覆盖攻击下的检测结果相同。考虑到注入的信号可以看作是每个控制回路的对应参考，NMCC持续监测每个回路的控制信号，这些信号也是每个回路的响应，因此通过比较每个回路的响应与正常控制下的响应，NMCC可以很容易地识别出同时发生的攻击。如果控制器响应正常，而同步检测器检测结果偏离正常值，则说明只发生了覆盖攻击。如果控制器响应异常，而检测值正常，则只发生了注入攻击。如果控制器响应和检测值都出现异常，则表示发生了注入攻击和覆盖攻击。如果注入信号不是直流分量，因其检测结果与仅进行覆盖攻击的检测结果不同，则可以

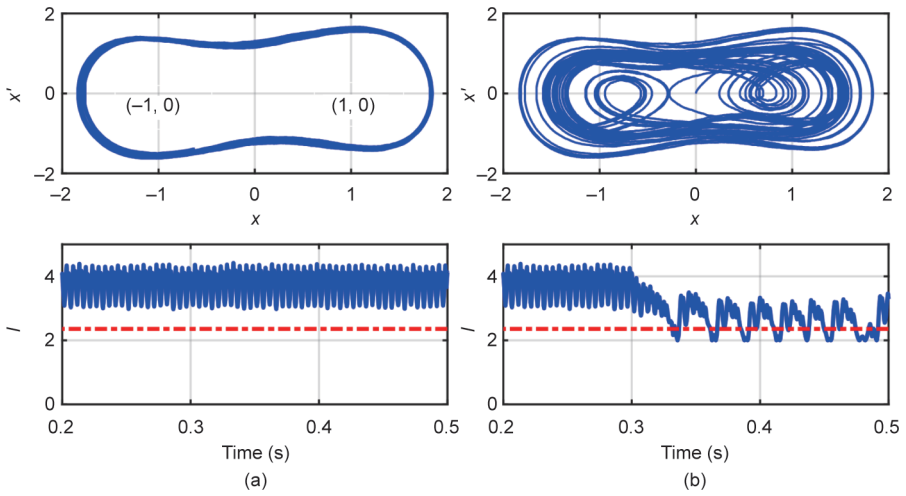


图3. 两个杜芬振荡器状态。（a）周期运动；（b）无序运动。x：杜芬振荡器方程的变量；x'：x 的导数。

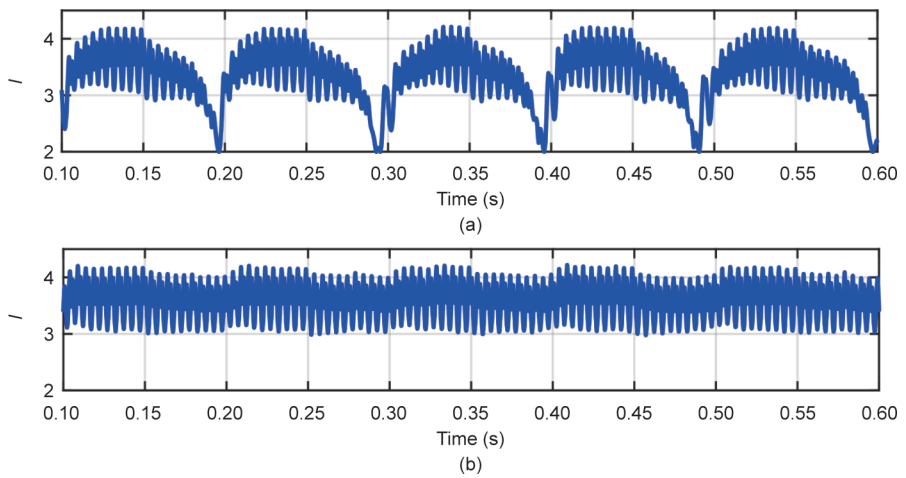


图4. 用于检测攻击的杜芬振荡器。（a）DOD的交替运动状态；（b）DOD的大周期运动状态。

通过直流分量注入攻击的方法或算法1识别攻击类型。

算法1 攻击类型的检测规则

for all values of D_f, D_U, D_{do}, D_{qo}, D_{di}, D_{qi} **do**
  if there exists 0 **then**
    Topologies modification attack detected;
  else
    if D_f, D_U, D_{do}, D_{qo}, D_{di}, D_{qi} *are normal* **then**
      if *Duffing detectors results are normal* **then**
        There are no attacks.
      else
        Replay attacks detected.
      end
    else
      if D_f, D_U, D_{do}, D_{qo}, D_{di}, D_{qi} *are normal* **then**
        Injection attacks detected.
      else
        Parameters overwriting attacks detected.
      end
    end
  end
end

4. 测试和验证

如图5所示，本文通过典型的NM系统测试和验证了PASS方法在检测Power bot攻击方面的有效性和实用性。测试系统由六个微电网组成，并在孤岛模式下运行。本文在MATLAB/Simulink中对NM建模，设定仿真时间步长为50 μs。在NMCC内对探测信号进行编程，并通过Mininet [30]中模拟的SDN传送到目标DER。在4.1节和4.2节中本研究验证了单一攻击下两个检测器的有效性。然后，在4.3节中评估了两个检测器在复杂攻击下的性能。最后，在4.4节中验证了本文所提出的协同检测方法的有效性。

为了清晰地说明本文提出的基于SDN的实现方法，我们介绍了测试环境设置、网络连接和系统运行过程的详细信息。PASS测试环境由微电网模拟器、SDN模拟器和NMCC组成。图6为三个组件的网络连接以及在NMCC中运行的协同检测方法的流程图。

该NM测试系统包括6个运行的微电网，并在MATLAB/Simulink中进行开发和编译，如图6所示。系统采用内置的Simulink发送器和接收器模块进行通信。六个微电网的互联网协议（IP）地址设置为10.0.0.1至10.0.0.6。

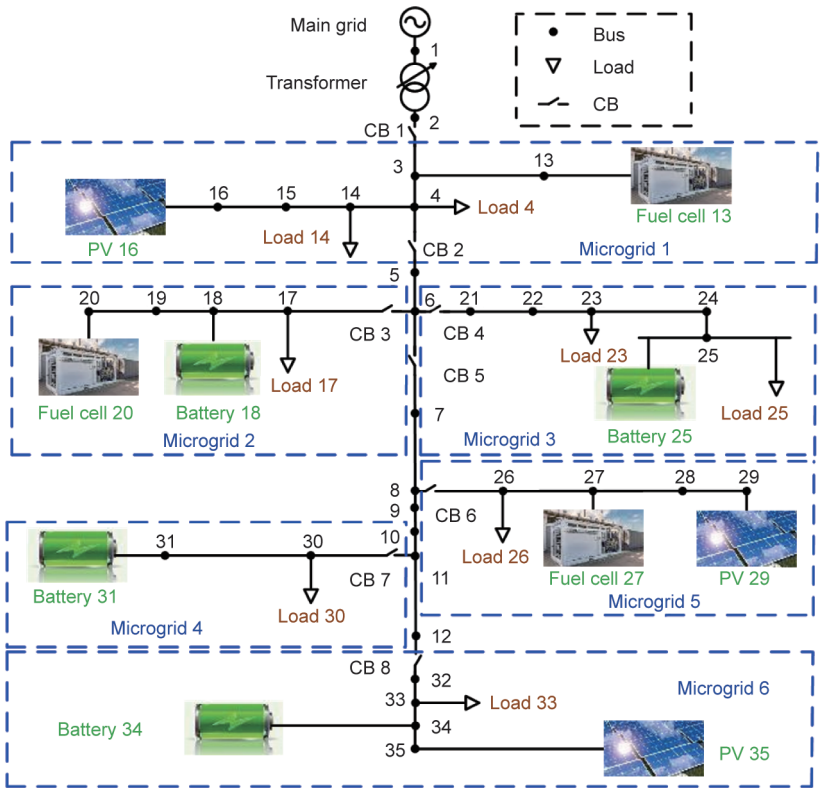


图5. 用于验证协同检测的联网微电网。CB：断路器；PV：光伏。1~35为总线号。

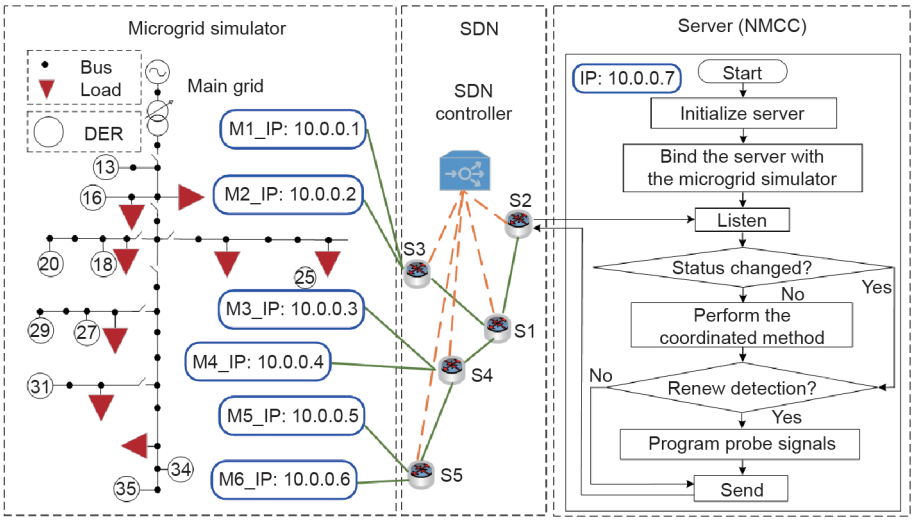


图6. PASS仿真系统的网络连接。M1~M6是六个微电网；S1~S5是五个交换机；IP：互联网协议。

DER逆变器控制信号测量通过SDN传输并发送到NMCC，其IP地址为10.0.0.7。NMCC在远程服务器上运行，该服务器可以接收DER运行状态（连接或断开）和逆变器控制信号，并将可编程探测信号发送回MATLAB/Simulink，通过协同检测方法、编译和发送探测信号来执行PASS方法。服务器连接模拟器后，进入监听模式，接收目的IP和端口与服务器匹配的数据包，然后进行PASS测试。图6中间显示了用于网络化微电网系统的SDN拓扑，其中包括五个交换机和一个SDN OpenFlow控制器Ryu [30]。SDN网络在Mininet环境中运行。在Mininet中，每条链路的带宽一般设置为每秒1亿比特（Gbps）。用户数据报协议（UDP）[31]通过Mininet [32]在NM和NMCC之间传输数据包。

4.1. 修改和覆盖攻击的同步检测器的验证

（1）修改攻击：本测试案例中，微电网4中电池31的逆变器外环功率控制器在1.10 s发生修改攻击（图5）。本测试通过两个子案例演示了使用和不使用同步检测器时测试系统的性能。当激活检测器时，$\alpha_{d1} = \alpha_{q1} = 0.06$，并且$\omega_d = \omega_q = 1256\ \text{rad}\cdot\text{s}^{-1}$ (1 rad = 180°/π)。图7说明了母线20和31处的电流响应（三相：a、b和c）以及关闭同步检测器时基于下垂控制的DER的输出功率。图8显示了受保护下的三相电流和功率响应。电池31的D_{do}的变化如图9所示。

如图6至图8所示，当D_{do}达到零时，同步检测器在$t = 1.11$ s处检测到修改攻击，并且立即打开断路器（CB）7以断开微电网4并隔离攻击。

（2）覆盖攻击：本测试案例中，在$t = 1.10$ s时对微电网1中燃料电池13的下垂控制器进行覆盖攻击（图5）。本实验还提供了测试系统的运行情况以验证SD功效。在没有SD的情况下，母线13和27的电流响应以及下垂控制的DER的输出功率如图10所示。SD投入使用时，27号母线的电流响应和下垂控制DER的输出功率如图11所示。攻击在$t = 1.12$ s时被识别，D_{do}明显偏离正常值，如图12所示。

从图7至图12可知，在没有SD的情况下，修改和覆盖攻击的影响迅速蔓延到NM，并且NM性能严重恶化（图7和图10）。使用SD可以识别攻击，并减轻其对NM的影响（图8和图11）。这验证了SD在防御Power bot攻击方面的有效性。

攻击前实际的D_{do}值与检测函数计算的值近似相等。由图9和图12可知，两种情况下的D_{do}值分别为3.63和1.44，与计算值3.60和1.44非常接近。微电网4断开后，D_{do}值连续变化。这些值与表1中所示的检测值并不一致，这是因为断开的微电网运行异常，而表1的值代表检测规则的稳态情况。在实际应用中，一旦检测结果偏离正常值一定程度后，即大于正常运行状态值的1.5倍或小于0.5倍，就应发出攻击警报。为了保护更关键的DER，可以设置更窄的警报阈值。

4.2. 重放攻击DOD的验证

（1）重放攻击：在本测试案例中，通过注入记录的正常运行数据，对微电网6中电池34的内环控制器发起重放攻击。当DOD被激活时，$\alpha_{d2} = \alpha_{q2} = 0.01$并且DOD状态在NMCC中被编译为每0.1 s改变一次频率。记录信号的频率与NMCC产生的动态变化的信号不匹配。因此，

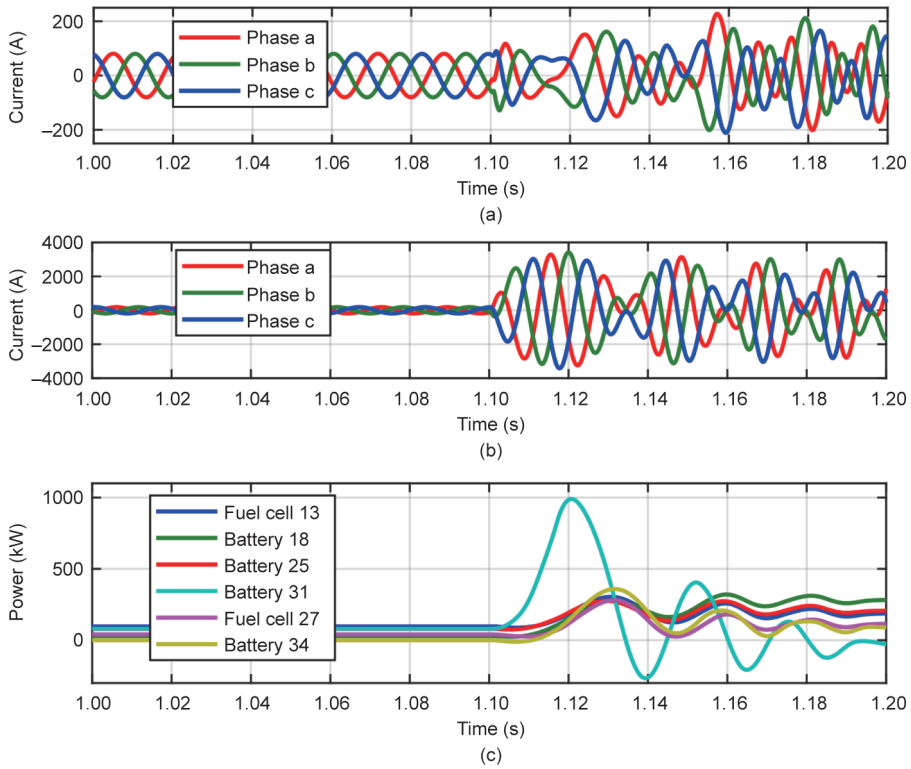


图7. （a）、（b）母线20和31的电流响应；（c）没有SD时修改攻击下的DER功率响应。

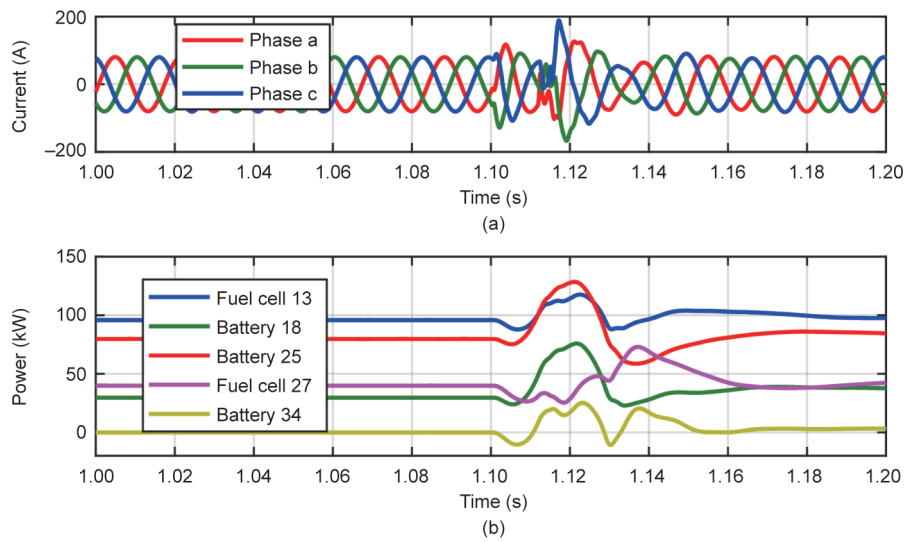


图8. （a）母线20的电流响应；（b）采用SD时的DER输出功率。

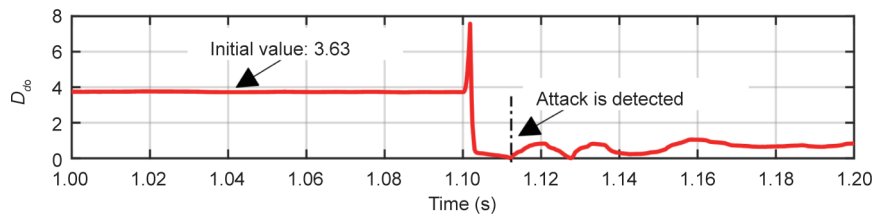


图9. 电池31中D_{do}的检测函数值。

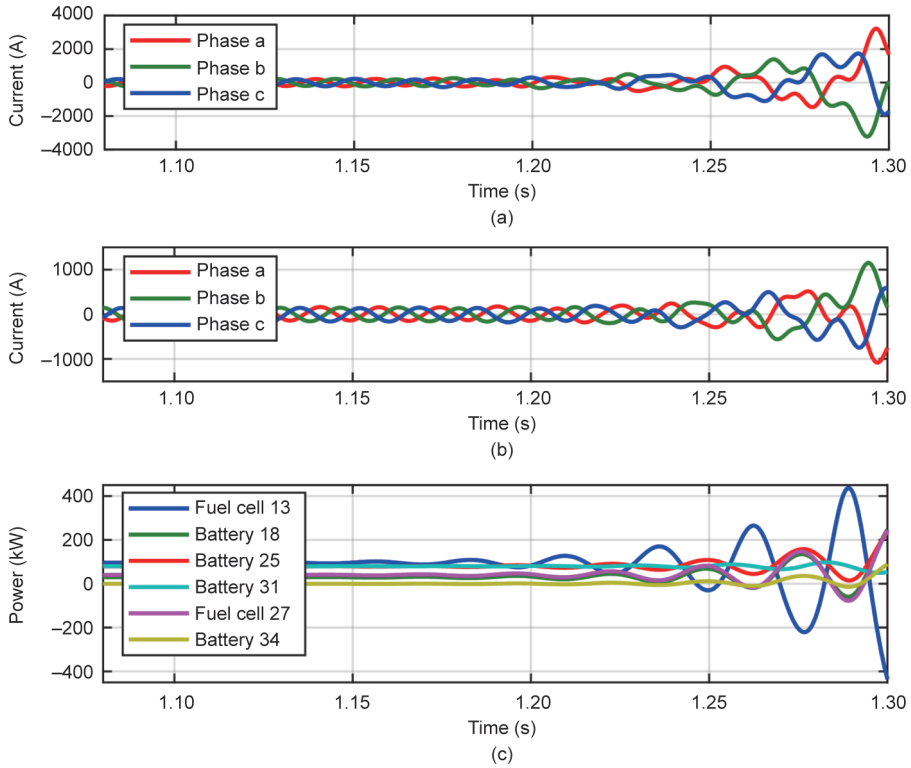


图10. （a）、（b）总线13和27的电流响应；（c）没有SD的DER功率响应。

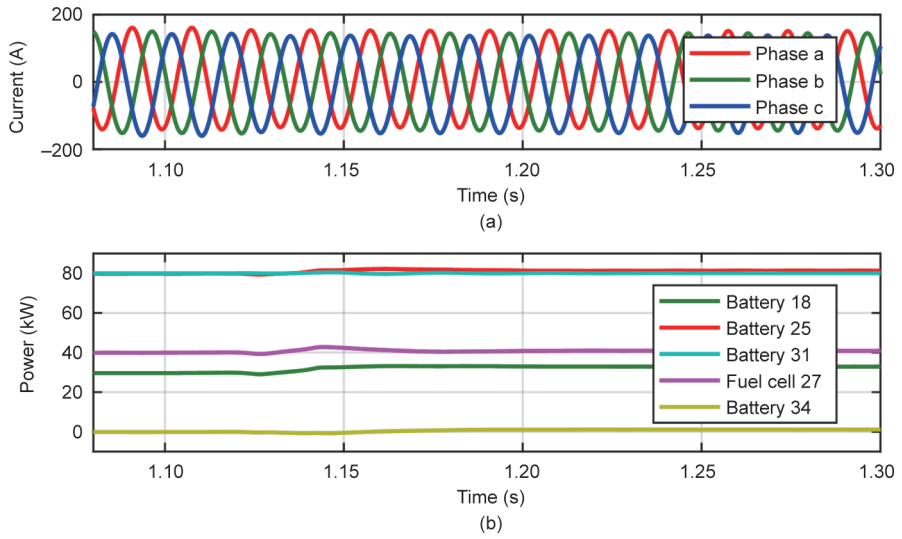


图11. （a）总线27的电流响应；（b）含有SD的DER输出功率。

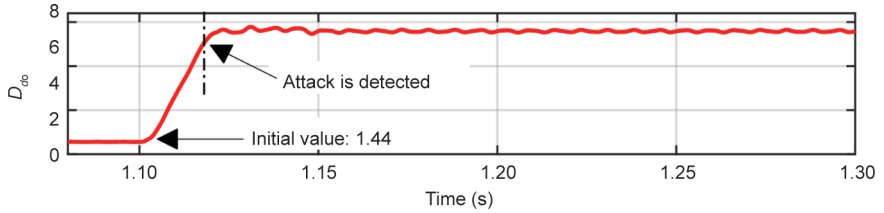


图12. 燃料电池13中D_{do}的检测函数值。

DOD运动状态在重放攻击发生时发生变化。如图13所示，重放攻击发生在$t = 0.9$ s并在$t = 0.94$ s时被检测到。

（2）鲁棒性验证：在实际中，DOD需具备可靠性和稳健性，这说明：①正弦信号α_{d2}和α_{q2}不应影响NM的正

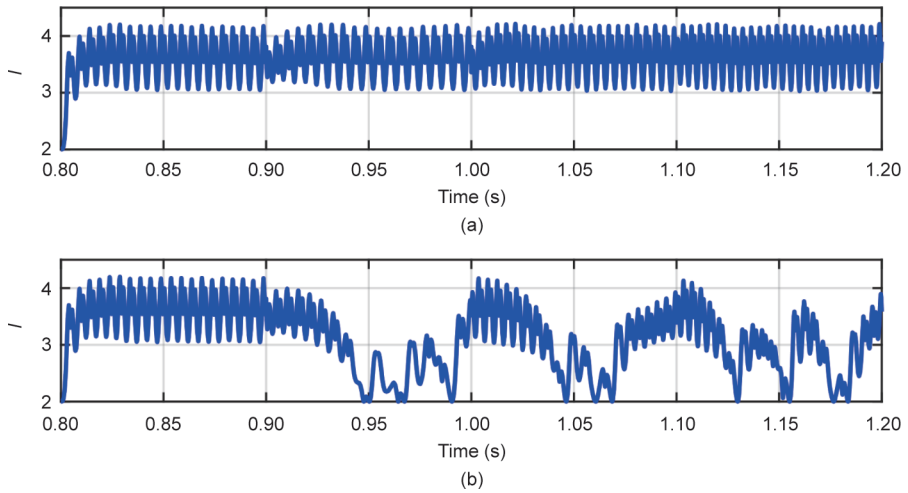


图13. 重放攻击的检测。（a）DOD无重放攻击的运动状态；（b）重放攻击下DOD的运动状态。

常运行，因为信号幅度低于SD探测信号，其影响可以忽略；②DOD能正确检测带有强噪声的弱探测信号。Duffing振荡器可识别的最低正弦信号幅值为0.0001，最低可达到的信噪比（SNR）为−51 dB，如参考文献中所述[27]。为了证明DOD在检测低信噪比弱信号方面的能力，仿真结果如图14所示。

4.3. 单一检测器对攻击的检测能力不足

（1）SD故障：在$t = 1.10$ s时，向电池31和18的控制器分别注入具有相同和不同sd1(t)频率的附加信号（图5）。图15分别显示了该过程中D_{do}的变化。如图15所示，微电网2和4由于明显的D_{do}偏差而断开连接。但是事实上，逆变器控制器参数并没有受到攻击。因此，尽管SD可以隔离攻击，但当发生注入攻击时，其无法准确识别攻击类型。

但是，在重放攻击和覆盖攻击下，SD无法检测到它们。在$t = 1.10$ s发起覆盖攻击之前，实际控制信号已经被预先记录的信号替换并报告给NMCC。图16显示了下垂控制的DER的输出功率和电池31中D_{do}的变化。NM性能严重下降并最终崩溃。但是，SD无法及时识别和消除攻击。

（2）DOD的故障：如3.2节中所述，由于其选择性，DOD本身无法确定注入攻击。如图17（a）所示，当燃料电池13受攻击时，其运动状态不改变。因此，它无法识别此攻击。

4.4. 协同检测方法验证

（1）覆盖和注入攻击检测：当燃料电池13中仅发生注入攻击时，D_{do}的变化和DOD的状态如图17（b）所示。在发起注入攻击时，D_{do}发生了变化，而DOD和NM仍保持正常运行。虽然SD被注入攻击所误导，但也可以准确识别攻击类型。

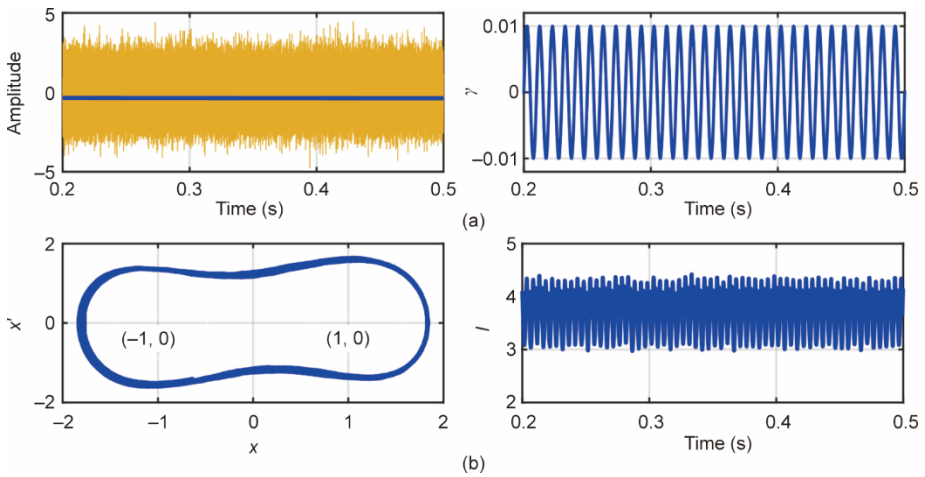


图14. 低SNR弱信号的检测。（a）带有强噪声的弱信号；（b）带噪声的DOD运动状态。

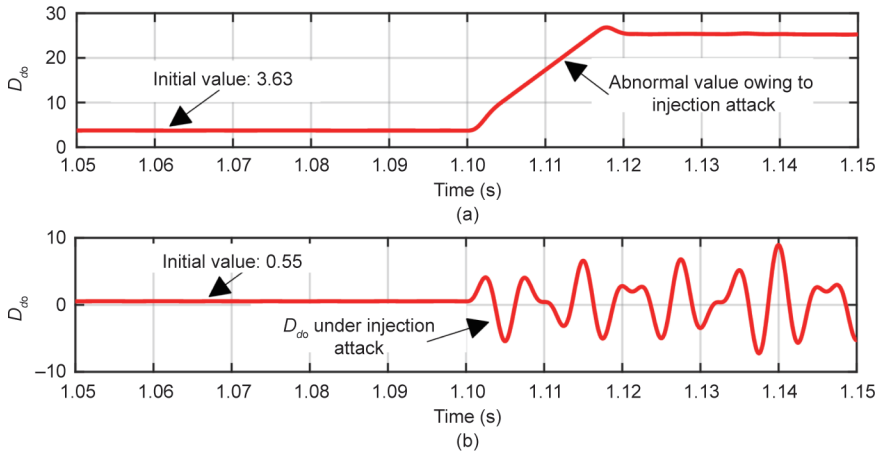


图15. 注入攻击时的电池31中D_{do}的变化（a）、电池18中D_{do}的变化（b）。

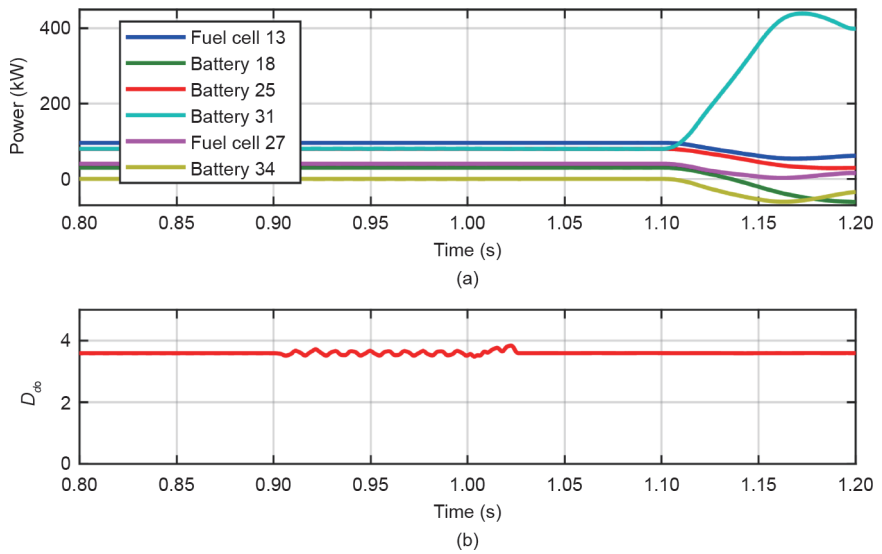


图16. 只有SD时两种攻击下的DER功率响应（a）、电池31的D_{do}（b）。

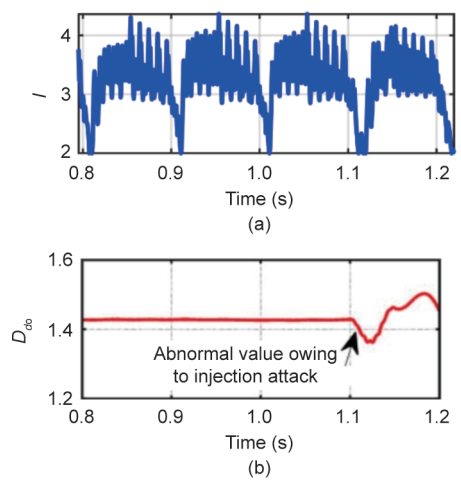


图17. 燃料电池13中DOD（a）和SD（b）的检测结果。

当电池18同时发生覆盖和注入攻击时，不仅D_{do}会偏离正常值，DOD运动状态也会改变，如图18所示。与图15（b）相比，通过两个检测器的配合，可以准确地区分覆盖攻击和注入攻击。

（2）检测修改和重放攻击：通过记录正常操作数据并在t = 1.00 s将它们注入NMCC，电池31中可以发起再攻击。同时，在t = 1.10 s时发起修改攻击。电池31的D_{do}和没有协同检测方法的DER输出功率如图16所示。当激活协同检测时，攻击前后的DOD运动状态和DER输出功率如图19所示。

如图16和图19所示，因为D_{do}在联合攻击期间几乎没有变化，所以无法检测到修改攻击。因此，无法及时隔离微电网以隔离攻击。当应用协调检测方法时，一旦发起重放攻击，Duffing振荡器的运动状态就会发生变化，如图19（a）和（b）所示。可以使用协同检测方法检测攻击，并识别攻击类型。还可以减轻其影响以确保稳定的NM运行，这验证了所建立方法的有效性。

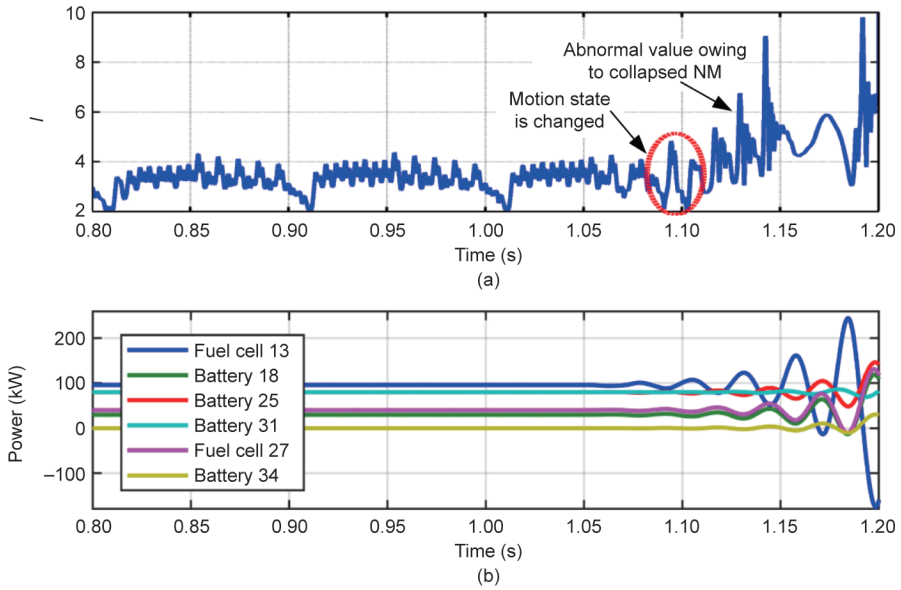


图18. 覆盖和注入攻击下协同检测的有效性。（a）受到攻击的Duffing振荡器的运动状态；（b）DER的功率响应。

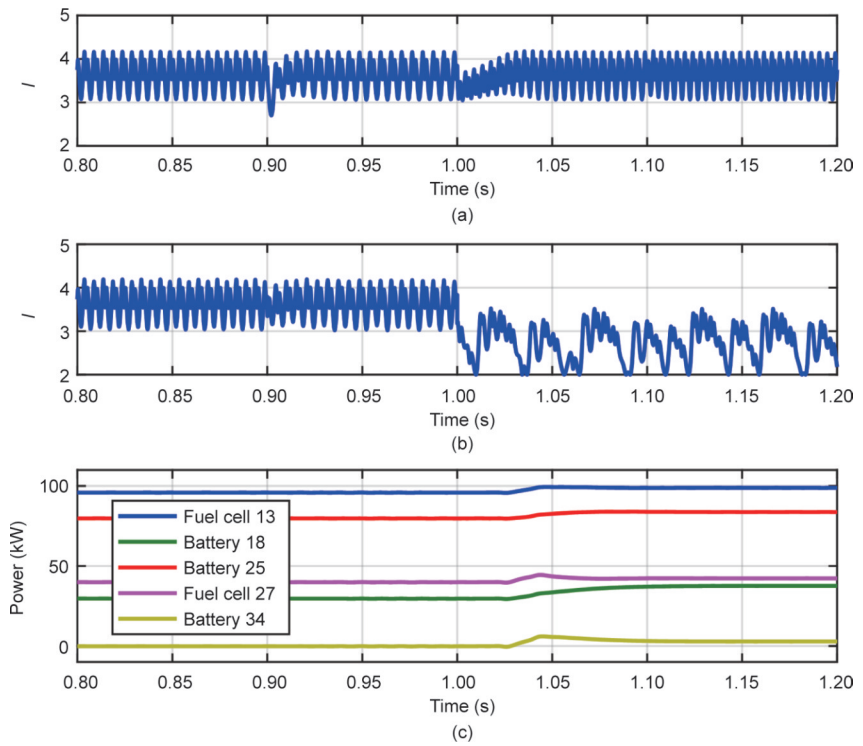


图19. 修改和重放攻击下协同检测的有效性。（a）、（b）分别为正常条件下和攻击下Duffing振荡器的运动状态；（c）DER的功率响应。

从以上仿真来看，当单个检测器被激活时，复杂的恶意攻击不仅会使检测器报告错误的攻击类型，而且会使其变得无法检测。无论恶意攻击者采用何种攻击策略，本研究设计的协同检测方法都能够识别攻击。协调探测信号在NMCC中使用基于SDN的PASS策略进行编程，这对于NM的保护是切实可行且可靠的。

5. 结论

在本研究中，我们提出了一种支持SDN的PASS方法来识别和减轻NM中复杂的网络攻击。不管恶意攻击者采用什么样的攻击方案，探测信号都可以在NMCC中编程并转发到DER控制器以检测复杂的攻击，包括修改攻击、

覆盖攻击、注入攻击和重放攻击。通过协调检测的方法，可以检测出攻击的类型和位置。本研究设计出的可编程策略可以有效实现微电网即插即用功能，大量测试验证了该方法的有效性和可靠性。

Acknowledgements

This work was supported in part by the National Science Foundation, USA under Grant Nos. ECCS-2018492, CNS-2006828, ECCS-2002897, and OIA-2040599.

Compliance with ethics guidelines

Zimin Jiang, Zefan Tang, Peng Zhang, and Yanyuan Qin declare that they have no conflict of interest or financial conflicts to disclose.

References

[1] Zhang P. Networked microgrids. Cambridge: Cambridge University Press; 2021.
[2] Tang Z, Zhang P, Krawec WO, Jiang Z. Programmable quantum networked microgrids. IEEE Trans Quantum Engineer 2020;1:1−13.
[3] Tang Z, Qin Y, Jiang Z, Krawec WO, Zhang P. Quantum-secure microgrid. IEEE Trans Power Syst 2021;36(2):1250−63.
[4] Lu LY, Liu HJ, Zhu H, Chu CC. Intrusion detection in distributed frequency control of isolated microgrids. IEEE Trans Smart Grid 2019;10(6):6502−15.
[5] Farhady H, Lee H, Nakao A. Software-defined networking: a survey. Comput Netw 2015;81:79−95.
[6] Tang Z, Zhang P, Krawec WO. A quantum leap in microgrids security: the prospects of quantum-secure microgrid. IEEE Electrific Mag 2021;9(1):66−73.
[7] Hatziargyriou ND, Kleftakis V, Papadimitriou CN, Messinis G. Microgrids in distribution. In: Liu CC, MaArthur S, Lee SJ, editors. Smart grid handbook. Hoboken: John Wiley & Sons, Ltd.; 2016.
[8] Zhang P, Wang B, Luh PB, Ren L, Qin Y, inventors; University of Connecticut, assignee. Enabling resilient microgrid through ultra-fast programmable network. United States patent US 20170324671. 2017 Apr 28.
[9] Wang L, Qin Y, Tang Z, Zhang P. Software-defined microgrid control: the genesis of decoupled cyber-physical microgrids. IEEE Open Access J Power Energy 2020;7:173−82.
[10] Huang T, Satchidanandan B, Kumar PR, Xie L. An online detection framework for cyber attacks on automatic generation control. IEEE Trans Power Syst 2018; 33(6):6816−27.
[11] Ravichandran MT. Resilientmonitoring and control systems: design, analysis, and performance evaluation [dissertation]. Michigan: University of Michigan; 2015.
[12] Li Y, Zhang P, Zhang L, Wang B. Active synchronous detection of deception attacks in microgrid control systems. IEEE Trans Smart Grid 2017;8(1):373−5.
[13] Pan K, Teixeira A, Cvetkovic M, Palensky P. Cyber risk analysis of combined data attacks against power system state estimation. IEEE Trans Smart Grid 2019;10(3):3044−56.
[14] Skopik F, Smith PD, editors. Smart grid security: innovative solutions for a modernized grid. Burlington: Syngress; 2015.
[15] Kurt MN, Yilmaz Y, Wang X. Real-time detection of hybrid and stealthy cyberattacks in smart grid. IEEE Trans Inform Forensics Security 2019; 14(2): 498−513.
[16] Manandhar K, Cao X, Hu F, Liu Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans Cont Network Syst 2014;1(4):370−9.
[17] Tang Z, Jiao J, Zhang P, Yue M, Chen C, Yan J. Enabling cyberattack-resilient load forecasting through adversarial machine learning. 2020. arXiv:2001.02289.
[18] Tan S, De D, Song WZ, Yang J, Das SK. Survey of security advances in smart grid: a data driven approach. IEEE Comm Surv Tutor 2017;19(1): 397−422.
[19] Musleh AS, Chen G, Dong ZY. A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Trans Smart Grid 2020; 11(3): 2218−34.
[20] Wang J, Qin Y, Tang Z, Zhang P. Software-defined cyber-energy secure underwater wireless power transfer. IEEE J Emerg Sel Topics Ind Electron 2021;2(1):21−31.
[21] He Y, Mendis GJ, Wei J. Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans Smart Grid 2017;8(5):2505−16.
[22] Babahajiani P, Wang L, Liu J, Zhang P. Push-sum-enabled resilient microgrid control. IEEE Trans Smart Grid. In press.
[23] Ren L, Qin Y, Wang B, Zhang P, Luh PB, Jin R. Enabling resilient microgrid through programmable network. IEEE Trans Smart Grid 2017;8(6):2826−36.
[24] Moslemi R, Mesbahi A, Velni JM. A fast, decentralized covariance selectionbased approach to detect cyber attacks in smart grids. IEEE Trans Smart Grid 2018;9(5):4930−41.
[25] Wan W, Bragin MA, Yan B, Qin Y, Philhower J, Zhang P, et al. Distributed and asynchronous active fault management for networked microgrids. IEEE Trans Power Syst 2020;35(5):3857−68.
[26] Kreutz D, Ramos FMV, Esteves Verissimo P, Esteve Rothenberg C, Azodolmolky S, Uhlig S. Software-defined networking: a comprehensive survey. Proc IEEE 2015;103(1):14−76.
[27] Akilli M, Yilmaz N. Study of weak periodic signals in the EEG signals and their relationship with postsynaptic potentials. IEEE Trans Neural Syst Rehabil Eng 2018;26(10):1918−25.
[28] Vahedi H, Gharehpetian GB, Karrari M. Application of duffing oscillators for passive islanding detection of inverter-based distributed generation units. IEEE Trans Power Deliv 2012;27(4):1973−83.
[29] Jalilvand A, Fotoohabadi H. The application of Duffing oscillator in weak signal detection. ECTI Trans Electr Engineer Electron Commun 2011;9(1):1−6.
[30] Fujita T. Introduction to Ryu SDN framework [Internet]. Tokyo: Ryu SDN Framework Community; 2013 Apr 15 [cited 2020 Jul 20]; Available from: https://ryu-sdn.org/slides/ONS2013-april-ryu-intro.pdf.
[31] Wang MH, Chi PW, Guo JW, Lei CL. SDN storage: a stream-based storage system over software-defined networks, In: Proceedings of 2016 IEEE Conference on Computer Communications Workshops; 2016 Apr 10−14; San Francisco, CA, USA; New York: IEEE; 2016. p. 598−9.
[32] Chithaluru P, Prakash R. Simulation on SDN and NFV models through mininet. In: Damka A, editor. Innovations in software-defined networking and network functions virtualization. Hershey: IGI Global; 2018. p. 149−74.