Smart Grid 智能电网, 2022, 12(4), 119-129
Published Online August 2022 in Hans. http://www.hanspub.org/journal/sg
https://doi.org/10.12677/sg.2022.124013

Hans汉斯

智能微网在网络攻击模式下的研究现状及展望

冯宜伟，贾　文

兰州理工大学，电气与信息工程学院，甘肃　兰州

收稿日期：2022年7月22日；录用日期：2022年8月2日；发布日期：2022年8月16日

摘　要

智能微网作为典型的网络物理系统，由于在信息传输，智能控制等方面面临不同类型网络攻击的危险。因此，本文针对网络攻击对系统所带来的危害，首先对两种典型的网络攻击如虚假数据注入和拒绝服务攻击的原理进行综述。其次，根据上述相对应的原理，对于攻击存在时，概述了常用的检测及控制方法如集中式与分布式检测，多智能体一致性协同控制，分布式弹性控制等。最后，对智能微网在不同类型攻击下如何稳定运行进行了总结，并对未来攻击的检测与控制策略进行了展望。

关键词

智能微网，虚假数据注入，拒绝服务攻击，控制策略

Research Status and Prospect of Smart Microgrid in Network Attack Mode

Yiwei Feng, Wen Jia

College of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou Gansu

Received: Jul. 22nd, 2022; accepted: Aug. 2nd, 2022; published: Aug. 16th, 2022

Abstract

As a typical network physical system, smart microgrid is exposed to different types of network attacks due to information transmission and intelligent control. Therefore, aiming at the harm brought by network attacks to the system, this paper firstly reviews the principles of two typical network attacks, such as false data injection and denial of service attack. Secondly, according to the corresponding principle, for the attack, summarizes the commonly used detection and control methods such as centralized and distributed, collaborative multi-agent consistency control, distributed flexible control, etc. Finally, the paper summarizes how to operate the smart microgrid stably under different types of attacks, and prospects the attack detection and control strategies in the future.

文章引用: 冯宜伟, 贾文. 智能微网在网络攻击模式下的研究现状及展望[J]. 智能电网, 2022, 12(4): 119-129.
DOI: 10.12677/sg.2022.124013

Keywords

Smart Microgrid, False Data Injection, Denial of Service Attack, Control Strategy

1. 引言

智能微网是由发电机、负荷和储能组成的局部小型能源电网。随着计算机、通信网络、自动控制等新兴产业的相互交融与促进，信息物理融合网络系统(Cyber-Physical-System, CPS)随之出现，并朝着大规模、智能化的方向发展，智能电网是一种典型的 CPS 系统[1]。然而，通信网络与信息设备之间的缺陷和漏洞使得电力 CPS 中的信息采集、信息传输、智能控制等环节面临着网络攻击的风险，这给智能微网的安全稳定运行带来了新的挑战[2]。而且，智能微网的组件往往是地理分布的，这意味着控制器和控制动作指令的反馈信号需要通过通信网络进行传输[3]。然而，通信网络也带来了潜在的网络威胁。因此，如何确保所提出的控制器在不同类型的网络攻击下的安全性和弹性就显得尤为紧迫和重要。

欺骗和破坏攻击是微电网中常见的两种网络攻击。虚假数据注入(False Date Injection, FDI)攻击是 Liu 等人在 2009 年首次提出的一种针对智能微网网络状态估计的新型网络攻击，是一种典型的欺骗攻击[4]，它会导致系统性能下降，甚至导致系统不稳定和故障。关于 FDI 攻击的相关问题，由于其隐蔽性和潜在的威胁，现有文献主要集中在构建、检测和防御机制[5]。在文献[6]中针对攻击者通过恶意数据攻击触发顺序中断的方式，使用量化影响和系统漏洞的模型来分析攻击机制。该模型提供了一个系统风险评估工具，但没有设计一个保护策略，以防止这种潜在的网络攻击造成的巨大物理损害。在[7]中采用了一种基于自适应卡尔曼滤波的检测方法来检测隐藏的数据注入攻击。与常用的 χ^2 检验、欧几里德检验和残差检测法检测随机攻击相比，该方法能快速检测出隐藏的虚假数据注入攻击。但不考虑自适应阈值，以缩短检测时间。

拒绝服务(Denial of Service, DoS)攻击是一种耗尽资源的攻击，它利用网络协议/软件的缺陷或发送大量无用的请求来耗尽被攻击对象的资源，从而使服务器或者通信网络无法提供正常的服务[8]。文献[9]从攻击者的角度出发，研究了有能量约束的 DoS 攻击者的攻击调度策略和系统状态的估计性能之间的关系，并从理论上证明了使估计协方差最大的攻击策略是发动连续的 DoS 攻击。文献[10]利用两区域负载频率控制系统研究了 DoS 攻击对其控制性能的影响。以上仅仅只讨论了 DoS 攻击下的状态估计和安全控制问题中的一个问题，而状态估计和安全控制是信息物理系统中紧密衔接的两个重要环节，具有高度的耦合性，只有同时确保这两个环节的安全才能保证信息物理系统的安全运行。

综上，本文通过以上网络攻击对智能电网产生影响的相关文献的分析，对 FDI 攻击和 DoS 攻击的基本机理进行了综述，阐述了对这两种攻击的检测与常用的控制方式并分析了不同控制方法的优缺点，最后对攻击存在时以智能微网为研究对象，进行多攻击检测及贴合实际的控制器设计的研究方向进行了展望。

2. 网络中的攻击类型

智能微网旨在实现分布式电源的灵活、高效应用，解决数量庞大、形式多样的分布式电源并网问题

开发和延伸微电网能够充分促进分布式电源与可再生能源的大规模接入，实现对负荷多种能源形式的高可靠供给。微电网的类型主要有交流，直流和交直流等，而最常见的为直流微网，如图 1 所示。

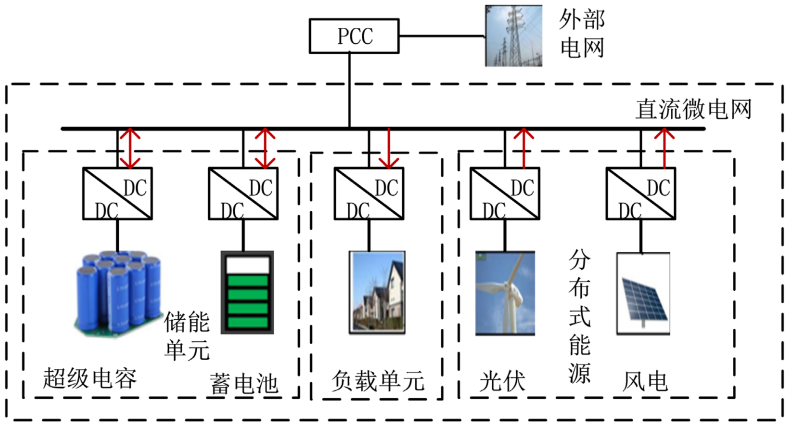

Figure 1. Smart microgrid composition
图 1. 智能微网组成

智能微网分层控制框架在直流微网中得到了广泛的应用，包括内部电流电压控制、下垂控制和二次控制。针对智能微网的普遍使用，它所面临的安全问题也引起了注意，如图 2 所示，FDI 和 DoS 攻击是最常见的两种对智能微网造成的网络攻击。而智能电网的网络安全立足于攻击者与守卫者的博弈过程，良好的控制策略的实施依赖于对攻击行为机理的了解，本节对攻击类型的原理进行详细的介绍。

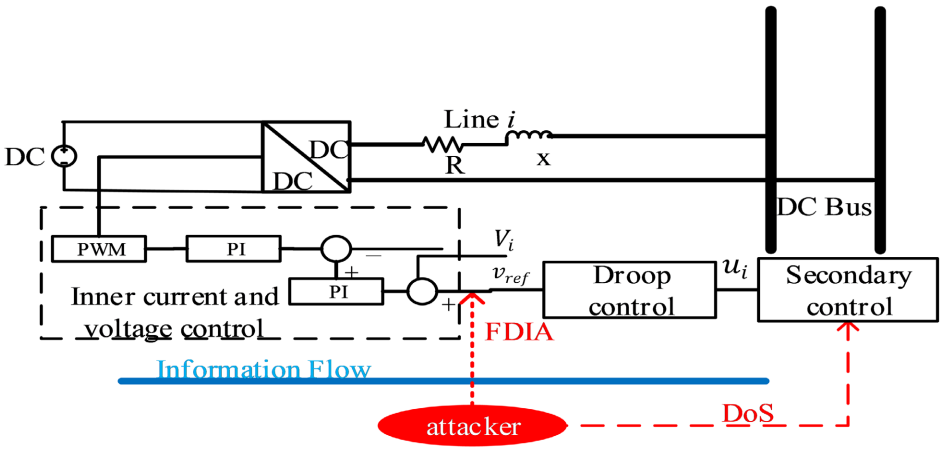

Figure 2. Types of network attacks
图 2. 网络攻击的类型

2.1. 拒绝服务攻击

DoS 攻击会造成系统资源不能用和传输信息丢失。到目前为止，一些数学模型被用来定量分析网络攻击导致的系统性能下降，如排队模型、伯努利模型或马尔可夫模型。本文考虑了一种通用的 DoS 攻击模型，该模型利用了 DoS 的两个典型特征，即 DoS 的频率和持续时间，而不需要对潜在的攻击策略提出任何要求，适用于各种 DoS 攻击[11]。为了定量描述 DoS 攻击的影响，让 $(d_n, d_n+g_n) \triangleq D_n\ (d_n \geq 0, n \in N)$ 表示无攻击区间，此区间内干扰攻击信号停止且通信正常，且让 $(d_n+g_n, d_{n+1}) \triangleq G_n\ (d_n+g_n < d_{n+1}, n \in N)$ 在这个区间内，攻击信号活跃，信号不能被传输。为了便于描述，我们使用来 $S_{Dos}(t)$ 表示 DoS 攻击信号：

$$S_{Dos}(t)=\begin{cases}0 & (d_n,d_n+g_n)\\ 1 & (d_n+g_n,d_{n+1})\end{cases} \tag{1}$$

首先考虑 DoS 攻击发生的频率，让 $v_n=\left((d_{n+1}+g_{n+1})-(d_n+g_n),n\in N\right)$ 表示任意两个连续 DoS 攻击之间经过的时间，我们发现，如果所有 $n\in N$ 的 $v_n<h$ (DoS 可以与采样频率 h 相同的速率发生)，那么无论采取何种策略，系统稳定性都会丧失。因此，为了获得稳定性，DoS 攻击发生的频率必须比采样频率小得多。表达这一要求的方法是通过平均滞留时间的概念[12]。对于 DoS 攻击信号 $S_{Dos}(t)$，$\forall t\geq 0$，设 $n(t)$表示在间隔[0, t]上发生的 DoS 关闭/打开转换的次数。根据文献[11]，DoS 攻击频率为：存在两个实标量 $\chi\geq 0$ 和 $\tau_v>0$，对于所有的 $t\geq 0$：

$$n(t)\leq \chi+\frac{t}{\tau_v} \tag{2}$$

除了 DoS 攻击频率受到限制外，还需要限制干扰攻击者的 DoS 攻击持续时间，即中断通信的间隔长度。考虑序列 (d_n+g_n)，定义 $E(t)=\left[\bigcup_{n=1}^{n(t)-1}G_n\right]\cup\left[d_{n(t)}+g_{n(t)},\min\left(d_{n(t)+1},t\right)\right]$ 表示截止到当前时间 t 的 DoS 攻击总间隔时间。则 DoS 攻击持续时间为:存在两个实标量 $\kappa\geq 0$ 和 $\Gamma>1$，对于所有的 $t\geq 0$：

$$\left|E(t)\right|\leq \kappa+\frac{t}{\Gamma} \tag{3}$$

针对上述 DoS 的基本原理，文献[13]研究了具有多个非线性恒功率负载和间歇性 DoS 攻击的直流微电网的事件触发控制器设计问题，如图 3 所示。然而，无线传感器的寿命还可以通过考虑能量收入来进一步延长，如何研究带有能量采集传感器的非线性直流微电网的事件触发镇定问题是本文未考虑的。

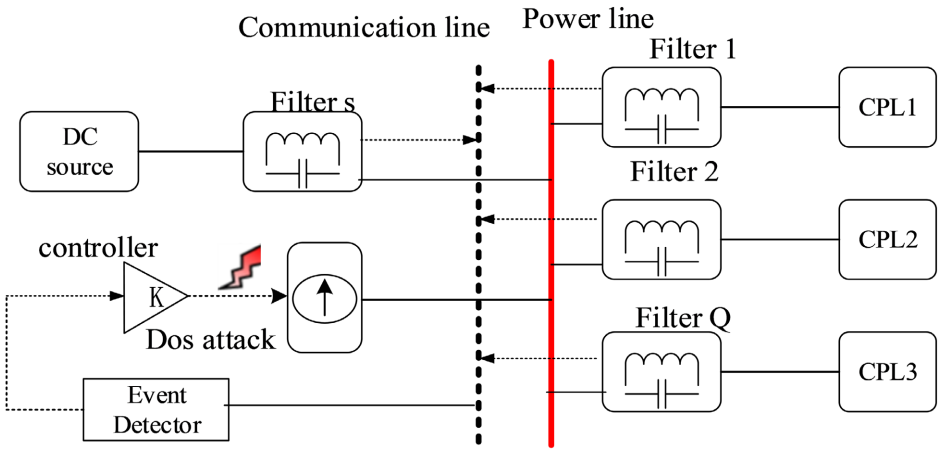

Figure 3. Event trigger control
图 3. 事件触发控制

2.2. 虚假数据注入攻击

虚假数据注入攻击利用电网状态估计中基于残差的不良数据检测漏洞，通过向数据采集与监控系统(Supervisory Control And Data Acquisition, SCADA)系统中注入虚假数据，达到修改电力系统的量测值和状态变量，控制智能微网的运行状态或者获取经济利益等不法目的[14]。

图 4 是虚假数据注入时整个智能微网运行的简化图，FDI 攻击是通过攻击量测系统，直接影响系统的状态估计模块。

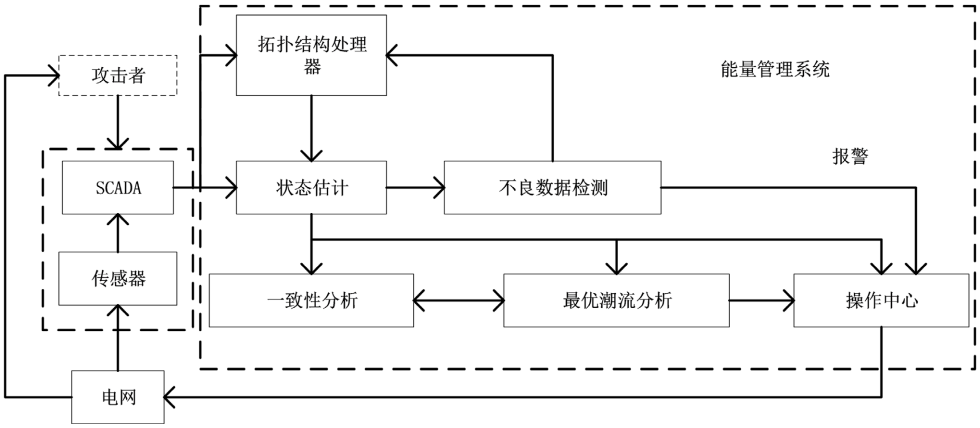

Figure 4. Simplified operation diagram of smart microgrid
图 4. 智能微网运行简化图

考虑一个 n 点系统，假设系统的量测值与状态变量之间满足如下关系：

$$z=\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix}=\begin{bmatrix} h_1\left(x_1x_2x_{2n-1}\right) \\ h_2\left(x_1x_2x_{2n-1}\right) \\ \vdots \\ h_m\left(x_1x_2x_{2n-1}\right) \end{bmatrix}+\begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix}=h\left(x\right)+e \tag{4}$$

式中 z 为量测向量，且 $z\in R^{m\times 1}, m>\left(2n-1\right)\times 1$，$e$ 为量测误差向量，x 为微网状态变量，幅值 $h\left(x\right)$ 是量测值与状态变量之间的计算函数关系。

为了简化和便于我们分析计算，我们将交流模型的非线性量测模型转换为局部线性关系，即直流近似模型的量测方程直流中有功功率量测模型的矩阵表达式：

$$z=\boldsymbol{H}x+e \tag{5}$$

$\boldsymbol{H}$ 矩阵非零元素的数值是与各个支路上电抗的倒数有关，是一个雅可比矩阵，通过对交流非线性方程的 $h\left(x\right)$ 对各个状态变量求偏导数所得：

$$\boldsymbol{H}=\frac{\partial h\left(x\right)}{\partial x}=\begin{bmatrix} \frac{\partial h_1\left(x\right)}{\partial x_1} & \frac{\partial h_1\left(x\right)}{\partial x_2} & \cdots & \frac{\partial h_1\left(x\right)}{\partial x_{n-1}} \\ \frac{\partial h_2\left(x\right)}{\partial x_1} & \frac{\partial h_2\left(x\right)}{\partial x_2} & \cdots & \frac{\partial h_2\left(x\right)}{\partial x_{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial h_m\left(x\right)}{\partial x_1} & \frac{\partial h_m\left(x\right)}{\partial x_2} & \cdots & \frac{\partial h_m\left(x\right)}{\partial x_{n-1}} \end{bmatrix} \tag{6}$$

$\boldsymbol{H}$ 是一个 $m\times\left(n-1\right)$ 维矩阵。针对上述量测方程模型(6)，将对系统进行状态估计，通过迭代逼近的方法使得方程组收敛，得到状态变量的估计值。加权最小二乘估计方法是电力系统状态估计中最常用的方法之一，它无需知道需要估计变量的统计特性，可以通过依据量测估计值 $\boldsymbol{H}\hat{x}$ 与量测值 z 之差的平方和最小的估计准则对系统未知变量进行估计。该方法假定量测误差 e 服从理想正态分布，$E\left(e_i=0, i=1,\cdots,m\right)$ 且 $E\left[e_i,e_j\right]=0$，则最终估计结果具备最优一致且无偏的统计特性。基于此，定义量测残差为：

$$y\left(x\right)=z-\boldsymbol{H}\hat{x} \tag{7}$$

其中，$\hat{x}$ 为估计状态变量。则优化目标函数可定义为：

$$\hat{x} = \arg\min \sum_{i=1}^{m} \boldsymbol{W} \left(z_i - \boldsymbol{H}x \right)^2 \tag{8}$$

其中，$\boldsymbol{W} = \boldsymbol{R}^{-1}$ 是量测量的权值矩阵，$\boldsymbol{R}$ 为量测量的误差方差矩阵，是一个对角阵。于是，最终得到节点状态变量的最优解为：

$$\hat{x} = \left(\boldsymbol{H}^{\mathrm{T}} \boldsymbol{W} \boldsymbol{H} \right)^{-1} \boldsymbol{H}^{\mathrm{T}} \boldsymbol{W} z \tag{9}$$

由于远程终端单元传感器采集到的数据存在干扰或者人为破坏以及物理设备老化等产生故障等原因，采集的量测数据中很可能存在不良数据，于是需要对量测值进行状态估计。在系统的状态估计通常采用量测值残差(线性模型)进行不良数据检测，表达式如下：

$$r = z - \boldsymbol{H}\hat{x} \tag{10}$$

检测虚假数据的判据是：$\|r\| < \tau$，τ 为判据的阈值。如果 $\|r\| < \tau$ 成立，则没有虚假数据，否则就要剔除相应的虚假数据并重新进行状态估计，直到通过虚假数据检测为止。

FDI 攻击在信息层入侵智能电网，以 z_a 表示被攻击后的系统量测值，$a = \begin{bmatrix} a_1 & a_2 & \cdots & a_m \end{bmatrix}^{\mathrm{T}}$ 表示数据注入的虚假数据向量。则实际的量测数据为 $z_a = z + a$；FDI 引起状态变量的误差向量 $c = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \end{bmatrix}^{\mathrm{T}}$，此时估计的状态变量为：

$$\hat{x}_a = \hat{x} + c \tag{11}$$

攻击后的残差表达式为：

$$\|r\| = \|z_a - \boldsymbol{H}\hat{x}_a\| = \|z + a - \boldsymbol{H}\left(\hat{x} + c\right)\| = \|z - \boldsymbol{H}\hat{x} + a - \boldsymbol{H}c\| \tag{12}$$

显然，当 $a = \boldsymbol{H}c$ 时，由下式成立。

$$\|r\| = \|z_a - \boldsymbol{H}\hat{x}_a\| = \|z - \boldsymbol{H}\hat{x}\| < \tau \tag{13}$$

上式说明注入的虚假数据就顺利通过最大标准化残差检验了，攻击者可以将量测值和状态变量改为任意值，从而给电力系统状态估计造成不可估计得损失，攻击成功。

典型的虚假数据注入攻击需要两个条件：一是攻击者要掌握系统拓扑信息矩阵；二是攻击者要控制所有的测量单元，满足这两个条件时攻击者才能达到任意篡改状态估计结果的目的[15]。文献[16]针对一个智能的、隐形的 FDI 可以严重危害微电网的稳定性，特别是在实际控制数据的知识边缘下，提出了一种基于 UIO 和 LQR 联合的最优弹性控制器，所提出的双层控制算法包括用户界面检测、微电网状态估计和充电站微电网频率偏差抑制，如图 5 所示。

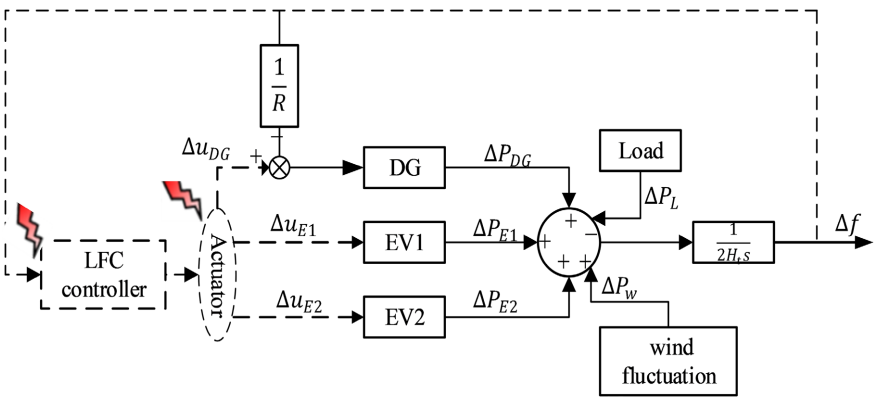

Figure 5. Optimal elastic controller based on UIO and LQR
图 5. 基于 UIO 和 LQR 联合的最优弹性控制器

文献[17]针对攻击试图忽略智能微网中的平均电压调节和电流共享，提出了一种合作机制，用于检测潜在的欺骗性网络攻击，对于隐形攻击到欺骗分布式观察者的不稳定性的表述和相关的范围，提出了一种针对每个 agent 的协作漏洞因子(cooperative vulnerability factor, CVF)框架，该框架能够准确识别不同场景下被攻击的 agent，如图 6 所示。

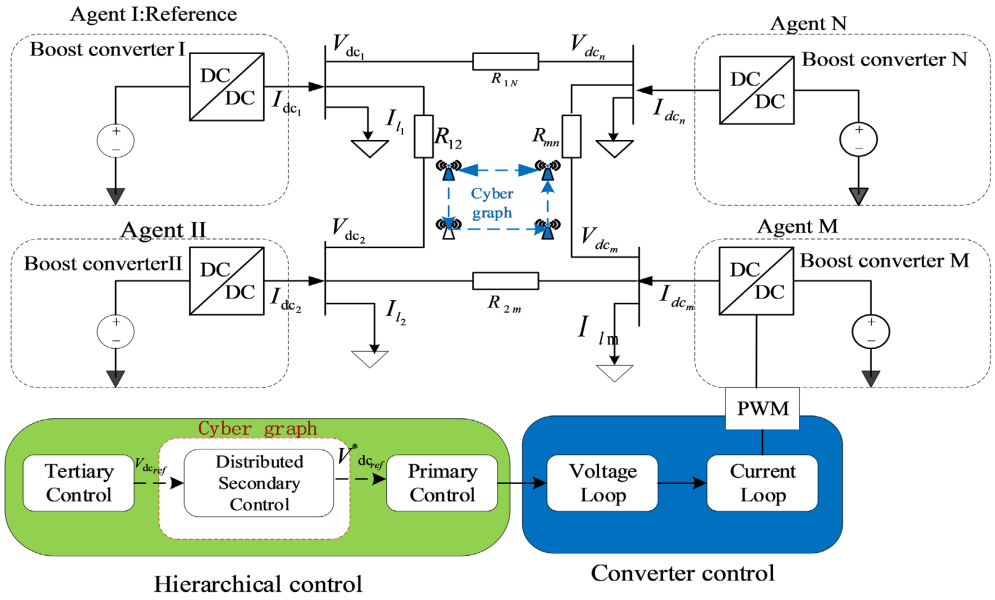

Figure 6. CVF method detects hidden attacks
图 6. CVF 方法检测隐藏攻击

3. 网络攻击模式下的控制与检测策略分析

基于以上对常用的两种攻击类型的原理进行综述后，当他们存在智能微网，破坏系统稳定性时，对它们采取相应的控制与及时检测出它们，减少对系统的损害就显得尤为重要，下面介绍目前常见的几种方法。

3.1. 基于多智能体一致性算法的协同控制

智能微网作为集成多种分布式电源(Distributed Generator, DG)的有效方式，受到广泛关注。协同分布式电源出力，实现微电网安全稳定运行对促进可再生能源开发和利用具有重要意义。多智能体一致性算法，利用智能体之间的互相通讯使智能体的状态趋于一致，为微网中分布式电源的协同控制提供了可行方案。在过去的许多研究中，研究者们假设多智能体系所处的环境是理想的，即多智能体系统不会受到网络攻击的影响。然而，多智能体系统对于通信网络的依赖性使其暴露在了网络攻击的威胁中。因此在设计多智能体系统时，考虑网络攻击所带来的影响非常有必要。文献[18]研究了 DoS 攻击下模糊非线性多智能体系统的脉冲一致性问题。通过构造不连续的李雅普诺夫函数，得到了在 DoS 攻击下保证非线性 T-S 模糊多智能体系统一致性的充分条件。与现有 DoS 攻击下多智能体系统脉冲共识的结果不同，本文提出的方法可以灵活地处理通信中断和拓扑切换问题。文献[19]研究了一类切换非线性多智能体系统的输出一致性问题，其中分别考虑了通信信道和智能体执行器中的拒绝服务攻击和故障。网络攻击会破坏通信通道，导致共识性能下降，甚至无法达成共识。与现有关于网络攻击下多智能体系统一致性的研究结果相比，本文的多智能体动力学描述为高阶异构切换非线性系统。网络攻击、执行器故障、异步切换以

及系统的高度复杂性使现有的共识算法失效。针对网络攻击下多智能体系统的输出一致性问题，提出了一种新的控制方案。利用图论、切换系统理论和李雅普诺夫函数方法，给出了是否能达到一致目标的充分条件。

3.2. 基于智能微网的弹性分布式控制

为解决数量庞大、相对分散且形式多样的分布式电源并网带来的稳定运行问题，各种控制理论逐渐被应用到微电网控制中。相比于集中式控制，分布式控制所具有的去中心化、可扩展性以及高可靠性，更适合管理地域分散、不断渗透的分布式电源。但是，较为依赖通信网络的分布式控制方式，更容易受到网络攻击的影响。其中，FDIA 是一种常见且隐蔽性强的攻击形式，其通过破坏控制系统的数据真实性扰乱控制目标，进而破坏微电网的稳定运行。文献[20]中，分析了网络攻击对通信链路，本地控制器和主控制器的影响，提出了一种网络攻击弹性分布式控制策略，其中，每个参与者都可以及时，经济地检测并隔离损坏的链接和控制器。所提出的控制策略对时变攻击信号和连续攻击有效，同时保留了 MG 的操作优势。微电网的分布式控制方法依托稀疏通信网络，在受到网络攻击后可能严重影响控制效果，甚至造成系统失稳。考虑 FDI 攻击，文献[21]针对分布式控制方式下的孤岛交流微电网，建立了 FDI 攻击的数学模型；其次，分析了系统受到 FDI 攻击后的脆弱性，并在此基础上，基于自适应控制原理提出了抵御 FDI 攻击的微电网分布式韧性控制方法，该方法能够在有界或无界的 FDI 攻击下使微电网实现既定控制目标，并具有良好的动态性能；然后，通过李雅普诺夫理论对分布式韧性控制器进行了严格的收敛性证明。

3.3. 网络攻击检测

网络物理系统(CPS)由于其在许多领域的潜在应用而受到了广泛的关注。但是，对通信网络的强烈依赖使 CPS 容易受到故意的网络攻击。因此，已经提出了许多攻击检测方法以增强 CPS 的安全性。根据控制信息的知识，CPS 的控制器分为集中式和分布式控制器。现有的集中式攻击检测方法主要有：1) 线性时不变系统，2) 执行器和传感器攻击，3) 非线性系统和 4) 带有噪声的系统。此外，根据不同的解耦方法，分布式攻击检测主要有奇异值分解，故障检测与识别方法，迭代法。

目前文献中关于攻击检测方法的研究成果大多基于集中式结构。然而，近年来，分布式控制系统由于其较低的计算复杂度和使用较少的网络资源而成为流行，因此分布式系统的攻击检测方法值得进一步研究。除此之外，在真实场景中，多个传感器或通信链路可能同时受到攻击，特别是在考虑传感器数量较多的情况下，然而，大多数的检测方法都假设系统中存在单次攻击，尽管基于多攻击检测的方法具有重要的工程意义，但在这一研究领域仍存在许多挑战。目前针对单个常见系统的攻击检测方法进行了深入研究。但是，这些方法对于计算资源和通信带宽受限的大规模网络物理系统是不可取的。因此，在设计攻击检测算法时还应考虑可扩展性。大多数现有文献只提供能够检测一种特定攻击的方法。但是，它们可能无法对付其他类型的攻击。因此，设计能够应对各种攻击的算法是极其重要的。

3.4. 其他控制方法

针对一类控制通讯信道受到攻击下直流微电网系统母线电压波动问题，滑模控制能够克服系统的不确定性，对干扰和未建模动态具有很强的鲁棒性，尤其是对非线性系统的控制具有良好的控制效果。由于变结构控制系统算法简单，响应速度快，对外界噪声干扰和参数摄动具有鲁棒性，能够实现动态控制与快速响应。如文献[22]，在直流微电网系统中引入蓄电池储能系统并构建系统数学模型。然后，设计积分滑模控制策略，来控制储能系统注入镇定电流以稳定直流母线电压，从而抑制非线性扰动和虚假数据注入攻击对系统性能的影响。同时，借助适当的 Lyapunov 泛函，得到确保滑动模态渐近稳定和滑模面可

达性的充分条件，保证直流微电网系统能够实现对负载需求的迅速响应及稳定运行。事件触发是在一些特定的，由系统稳定关系决定的一些特定时刻，去计算或改变控制输入。一般由两部分组成，第一是反馈控制器，第二是触发条件。针对非线性网络控制系统存在的拒绝服务(DoS)攻击，文献[23]设计一种具有动态事件触发策略的 H_∞ 安全控制器。首先，将 DoS 攻击引起的丢包影响作为触发条件的不确定性，针对这个不确定性以及在静态事件触发中引入一个内部动态参数，设计动态事件触发机制，在此基础上设计具有 H_∞ 性能的安全控制器。文献[24]通过分析 FDIA 对电压稳定性影响的基础上，采用静止无功补偿器信号(CSSVC)和节点电压稳定性指数(NVSI)来确定电力系统中节点的脆弱性水平。文献[25]中，提出了一种在直流状态估计中新型 FDIA 检测机制，表达式为(6)和(10)，采用双层非线性优化模型。基于信号处理的方法 DWT 来分解特定级别的估计状态，用改进的基于 EIM 的降维方法来减少训练检测模型的时间消耗。但未考虑在交流状态估计利用 FDIA 行为来分析攻击特性与电力系统复杂性之间的关系。文献[26]中攻击者在有限的能量预算下，以最大化 DoS 攻击对电力系统远程状态估计的影响。然而，上述只讨论了针对状态估计的 DoS 攻击，其目的是破坏系统的安全性和稳定性，未考虑如何设计最优的 DoS 策略来破坏电力系统的经济性能。文献[27]从防御角度，设计了事件/自触发控制策略。文献[28]中，针对孤岛微电网在随机拒绝服务攻击下的随机稳定性，提出了一种依赖模式的弹性控制器即二次频率控制方法来减轻 DoS 造成的影响。文献[29]中，在间歇性拒绝服务攻击下的网络物理微电网系统稳定性分析中，为了清楚的解释攻击引起的通信时延对微电网稳定性的影响，对此，提出了一种风险评估方法来研究 DoS 攻击下的稳定性。但未考虑攻击的有效性和成本及攻击下的微电网的电压和频率变化。

4. 总结与展望

除了传统的物理攻击之外，层出不穷的新型网络攻击也能给智能微网带来巨大威胁。网络攻击不仅能单独对智能电网造成破坏性影响，也能与物理攻击进行协同以造成更大的灾难性后果。此外，网络攻击还可以保持隐蔽，对微网系统安全形成长期性威胁。虚假数据注入攻击作为一种典型的网络攻击形式，利用了智能电网状态估计算法的漏洞，能以隐蔽的方式对系统造成破坏性影响。拒绝服务攻击作为一种耗尽资源的攻击，它利用网络协议/软件的缺陷或发送大量无用的请求来耗尽被攻击对象的资源，造成系统资源不能使用和传输信息丢失。

根据上述的实际不足和未来发展趋势，总结未来研究重点。首先，现有的关于虚假数据攻击和检测的研究大多采用近似的 DC 潮流模型。交流潮流模型由非线性方程组成，包含有功功率和无功功率，较为复杂和耗时而且交流潮流模型比 DC 模型更精确。另一方面，现有的研究大多集中在集中式的虚假数据检测上，而对分布式的研究较少。因此，有必要从分布式攻击检测、多攻击检测、可扩展攻击检测和其他攻击检测等方面讨论几个潜在的研究方向。

对于 DoS 攻击行为，现有的文献往往会假设 DoS 攻击服从伯努利分布或满足一个 Markov 过程，然而现实中，攻击者可以根据自身的能量约束对 DoS 攻击进行精心的设计，有策略地发动一连串组合式的 DoS 攻击，因此需要进一步研究更一般化的 DoS 攻击模型。虽然现有的针对 DoS 攻击的安全控制策略也具有对 DoS 攻击的鲁棒性，但都相对被动或对 DoS 攻击造成的系统不稳定动态不能得到快速的校正，这往往会较大地牺牲系统的控制性能(如系统的响应速度、稳态误差等)。因此，如何使系统性能在 DoS 攻击下尽可能地减少损失的控制策略值得进一步的研究。

总之，本文主要结合两种常见的网络攻击形式，根据大量的参考文献，概述了目前常用的针对攻击存在时，智能微网为研究对象，设计的控制及检测方法如多智能体一致性协同控制，分布式弹性控制及集中式与分布式两种检测方法。但未来攻击形式的多样化及复杂化，多攻击检测及设计相对应的控制器就变得很有意义。

参考文献

[1] Afshari, A., Karrari, M., Baghaee, H.R., *et al*. (2020) Resilient Synchronization of Voltage/Frequency in AC Microgrids under Deception Attacks. *IEEE Systems Journal*, **15**, 2125-2136. https://doi.org/10.1109/JSYST.2020.2992309

[2] 巴斯替，骆德汉. 智能电网网络安全的发展与挑战[J]. 电工电气, 2019(7): 5-8+54.

[3] Ding, L., Han, Q.L., Wang, L.Y., *et al*. (2018) Distributed Cooperative Optimal Control of DC Microgrids with Communication Delays. *IEEE Transactions on Industrial Informatics*, **14**, 3924-3935. https://doi.org/10.1109/TII.2018.2799239

[4] Liu, Y., Reiter, M.K. and Ning, P. (2009) False Data Injection Attacks Against State Estimation in Electric Power Grids. *Proceedings of the* 2009 *ACM Conference on Computer and Communications Security* (CCS 2009), Chicago, 9-13 November 2009, 21-32. https://doi.org/10.1145/1653662.1653666

[5] Jiwei, T., Buhong, W., Fute, S., *et al*. (2017) Stealthy False Data Injection Attacks Using Matrix Recovery and Independent Component Analysis in Smart Grid. *IOP Conference Series*: *Materials Science and Engineering*, **199**, Article ID: 012034. https://doi.org/10.1088/1757-899X/199/1/012034

[6] Che, L., Liu, X., Li, Z., *et al*. (2019) False Data Injection Attacks Induced Sequential Outages in Power Systems. *IEEE Transactions on Power Systems*, **34**, 1513-1523. https://doi.org/10.1109/TPWRS.2018.2871345

[7] 罗小元，朱鸣皋，王新宇，关新平. 基于自适应卡尔曼滤波器的智能电网隐蔽假数据攻击检测[J]. 信息与控制, 2018, 47(1): 16-21.

[8] Srikantha, P. and Kundur, D. (2015) Denial of Service Attacks and Mitigation for Stability in Cyber-Enabled Power Grid. *Innovative Smart Grid Technologies Conference*, Washington DC, 18-20 February 2015, 1-5. https://doi.org/10.1109/ISGT.2015.7131827

[9] Zhang, H., Cheng, P., Shi, L. and Chen, J.M. (2015) Optimal Denial-of-Service Attack Scheduling with Energy Constraint. *IEEE Transactions on Automatic Control*, **60**, 3023-3028. https://doi.org/10.1109/TAC.2015.2409905

[10] Liu, S., Liu, X.P. and Saddik, A.E. (2013) Denial-of-Service (DoS) Attacks on Load Frequency Control in Smart Grids. 2013 *IEEE PES Innovative Smart Grid Technologies Conference*, Washington DC, 24-27 February 2013, 1-6. https://doi.org/10.1109/ISGT.2013.6497846

[11] 郑凯中，樊春霞. 基于事件触发的遥操作系统在 DOS 攻击下的安全控制[J]. 南京邮电大学学报：自然科学版, 2021, 41(2): 77-84.

[12] Persis, C.D. and Tesi, P. (2015) Input-to-State Stabilizing Control Under Denial-of-Service. *IEEE Transactions on Automatic Control*, **60**, 2930-2944. https://doi.org/10.1109/TAC.2015.2416924

[13] Hu, S., Yuan, P., Yue, D., *et al*. (2019) Attack-Resilient Event-Triggered Controller Design of DC Microgrids under DoS Attacks. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, **67**, 699-710. https://doi.org/10.1109/TCSI.2019.2948015

[14] 王先培，田猛，董政呈，朱国威，龙嘉川，代荡荡，等. 输电网虚假数据攻击研究综述[J]. 电网技术，2016, 40(11): 3406-3414.

[15] 田继伟,王布宏，李腾耀，尚福特，曹堃锐. 智能电网虚假数据注入攻击研究进展与展望[J]. 信息安全与技术, 2019, 10(9): 73-84.

[16] Khalghani, M.R., Solanki, J., Solanki, S.K., *et al*. (2020) Resilient Frequency Control Design for Microgrids under False Data Injection. *IEEE Transactions on Industrial Electronics*, **68**, 2151-2162. https://doi.org/10.1109/TIE.2020.2975494

[17] Sahoo, S., Mishra, S., Peng, C.H., *et al*. (2018) A Stealth Cyber Attack Detection Strategy for DC Microgrids. *IEEE Transactions on Power Electronics*, **34**, 8162-8174. https://doi.org/10.1109/TPEL.2018.2879886

[18] Ma, T., Zhang, Z. and Cui, B. (2022) Impulsive Consensus of Nonlinear Fuzzy Multi-Agent Systems under DoS Attack. *Nonlinear Analysis*: *Hybrid Systems*, **44**, Article ID: 101155. https://doi.org/10.1016/j.nahs.2022.101155

[19] Li, S., Zou, W.C., Guo, J. and Xiang, Z.R. (2022) Consensus of Switched Nonlinear Multiagent Systems Subject to Cyber Attacks. *IEEE Systems Journal*. https://doi.org/10.1109/JSYST.2021.3110501

[20] Zhou, Q., Shahidehpour, M., Alabdulwahab, A. and Abusorrah, A. (2020) A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids. *IEEE Transactions on Smart Grid*, **11**, 3690-3701. https://doi.org/10.1109/TSG.2020.2979160

[21] 张露元，许寅，吴翔宇，王思家. 抵御虚假数据注入攻击的交流微电网分布式韧性控制[J/OL]. 电力系统自动化, 2022: 1-19. http://kns.cnki.net/kcms/detail/32.1180.TP.20220702.1235.004.html, 2022-07-13.

[22] 楼琦凯，陈蓓，丁勐，牛玉刚. 虚假数据注入攻击下直流微电网的滑模控制[J/OL]. 控制与决策, 2022: 1-9. https://doi.org/10.13195/j.kzyjc.2021.0606, 2022-07-13.

[23] 黄玲，孙晓宇，蔺小娜，郭婧. 具有 DoS 攻击非线性网络的动态事件触发控制[J/OL]. 控制理论与应用，2022: 1-9. http://kns.cnki.net/kcms/detail/44.1240.TP.20210825.1312.012.html, 2022-07-13.

[24] Xu, R., Rui, W., Guan, Z., *et al*. (2017) Achieving Efficient Detection against False Data Injection Attacks in Smart Grid. *IEEE Access*, **5**, 13787-13798. https://doi.org/10.1109/ACCESS.2017.2728681

[25] Yang, L., Zhang, X., Li, Z., *et al*. (2020) Detecting Bi-Level False Data Injection Attack Based on Time Series Analysis Method in Smart Grid. *Computers & Security*, **96**, Article ID: 101899. https://doi.org/10.1016/j.cose.2020.101899

[26] Zhang, H., Qi, Y., Wu, J., *et al*. (2018) DoS Attack Energy Management against Remote State Estimation. *IEEE Transactions on Control of Network Systems*, **5**, 383-394. https://doi.org/10.1109/TCNS.2016.2614099

[27] Xu, W., Ho, D., Zhong, J., *et al*. (2019) Event/Self-Triggered Control for Leader-Following Consensus over Unreliable Network with DoS Attacks. *IEEE Transactions on Neural Networks and Learning Systems*, **30**, 3137-3149. https://doi.org/10.1109/TNNLS.2018.2890119

[28] Liu, S., Hu, Z., Wang, X., *et al*. (2018) Stochastic Stability Analysis and Control of Secondary Frequency Regulation for Islanded Microgrids Under Random Denial of Service Attacks. *IEEE Transactions on Industrial Informatics*, **15**, 4066-4075. https://doi.org/10.1109/TII.2018.2885170

[29] Rong, F., Huang, X., Sun, J., *et al*. (2017) Stability Analysis of the Cyber Physical Microgrid System under the Intermittent DoS Attacks. *Energies*, **10**, Article No. 680. https://doi.org/10.3390/en10050680