# 针对电力系统薄弱状态的自动攻击策略

汤 奕*，张顺道

(东南大学电气工程学院 南京 210096)

【摘要】针对目标电力系统发起的网络攻击能够以较少的攻击资源造成极大的破坏效果，从攻击者视角出发，提出一种针对电力系统薄弱状态的网络攻击策略。首先基于电网拓扑数据建立关联矩阵，通过线性规划模型计算不同信息获取量下攻击造成的减载量；然后提出以最大化攻击效果为目的的自动攻击策略。通过在不同场景下的仿真分析验证了该策略的有效性。

**关 键 词** 攻击策略； 网络攻击； 电力系统； 薄弱状态

**中图分类号** TM711 **文献标志码** A doi:10.12178/1001-0548.2021402

# Automatic Attack Strategy for Weak State of Power System

TANG Yi* and ZHANG Shundao

(School of Electrical Engineering, Southeast University Nanjing 210096)

**Abstract** The network attacks against the power system of hostile countries can cause great damage with less attack resources. From the perspective of attackers, this paper proposes a network attack strategy for weak state of power system. Firstly, tthe correlation matrix based on the grid topology data is established, and the load shedding caused by the attack under different information acquisition amounts is calculated through the linear programming model. Then an automatic attack strategy is proposed to maximize the attack effect. The effectiveness of the proposed strategy is verified by simulation analysis in different scenarios.

**Key words** attack strategy; network attack; power system; weak state

随着信息通信技术的飞速发展，通信网络与电力网络深度融合，推动电力系统的高度自动化与智能化。电力系统逐渐演变为信息物理高度耦合的电力信息物理系统 (cyber physical power system, CPPS)[1]。

电力信息物理融合发展一方面提高了电力系统的运行效率。大量通信设备在电力系统中被广泛使用，使得电网调度中心可以通过以相量测量单元 (phasor measurement unit, PMU) 为代表的量测感知单元实时获取全面的电力系统运行信息[2]，以支撑各类运行控制业务[3]。另一方面，在电力信息物理融合发展中，信息层、物理层以及信息物理耦合层会出现诸多漏洞，利用这些漏洞对目标地区进行网络攻击，可影响其社会生活、生产行为[1]。各种分布式终端和新能源设备的接入给电力系统引入许多不确定因素，多类型通信方式也给电网带来安全风险，为网络攻击提供了途径[4-7]。电力系统发电、输电、配电、变电和用电等各个环节均可成为攻击对象，通过破坏 CPPS 的“保密性”“完整性”和“可用性”来实现对电力系统的攻击[8-11]。国际上已出现专门针对电力系统的网络攻击，如乌克兰遭受恶意攻击导致大停电事故，委内瑞拉遭受网络攻击导致多地停电事故，伊朗纳坦兹核电站遭受蓄意破坏导致停运事故。美国为开展电力等领域的网络攻击与防卫研究，已专门组建编制 6000 人的网络司令部[12-14]。

虽然电网有较为完备的安全稳定控制系统，但受到人为或自然灾害等因素的影响，有时会处于薄弱状态，攻击者对其进行有效利用可获得良好的攻击收益。这种情景的形成主要是因为在电力系统正常状态下发起网络攻击时，如果攻击方式、类型比较单一化，则会被电力系统中表征稳态性能的充裕度和表征动态性能的安全性削弱攻击效果，偏离预

收稿日期：2021－07－21；修回日期：2021－12－21

作者简介：汤奕 (1977－)，男，博士，教授，主要从事电力系统稳定分析、电力信息物理系统方面的研究.

*通信作者：汤奕，E-mail：1187517275@qq.com

期收益目标[15]；而与之相比，对处于薄弱状态下的电力系统进行网络攻击，利用电网的薄弱状态消耗N－1准则的裕度和部分防御资源，在此基础上，网络攻击造成的分布式连锁型故障能够进一步加剧电力系统不稳定因素引起的动荡，这种攻击方式使得攻击者可以通过相应的策略选取，以较低的攻击成本对电网造成较大的经济损失，并威胁电网的安全稳定运行。文献 [16] 基于电力系统静态安全域分析的思想建立关键线路评估模型，提出电力系统关键线路的辨识方法，指出少数线路在电力系统大规模停电中起关键作用。文献 [17] 从攻击者视角提出一种基于攻击损益原则的跨空间连锁故障选择排序方法，揭示电网信息物理系统中由信息攻击引发跨空间连锁故障的演化过程及爆发可能性，虽然有提及掌握部分资源情况下对攻击目标的破坏行为，但是没有对资源、信息受限情况展开分析。文献 [18] 提出针对不确定事件直接搜索的搜索算法，快速搜索出可构成威胁的连锁故障。针对电力系统的网络攻击具有明确的目的性，实施攻击的方式呈现多样性，以上研究主要侧重于电力系统正常状态下进行攻击，缺乏对电网的薄弱状态进行有效利用，很多情形下攻击者难以获取完全信息，这些都会影响攻击效果。

基于上述分析，本文提出一种针对电力系统薄弱状态的自动攻击策略，根据已掌握的部分或者全部稳控业务信息确定可攻击范围[19]，通过攻击成功状态与攻击成功后电力系统中其他线路处于正常或断线状态的排列组合构建电力系统攻击成功状态空间，在对电力系统是否处于薄弱状态做出判别后，依据已经确定的攻击范围，对电力系统攻击成功状态空间进行遍历，模拟攻击发起后电力系统变化，通过线性规划计算出在线路由于攻击成功而断线时可产生的减载量，遵循最大化原则筛选出严重故障情况下可获得的攻击收益并确定攻击位置等攻击信息。

# 1　严重故障搜索

作为攻击方预设达成的期望目标，实现攻击效果最大化是严重故障搜索算法的执行方向，针对资源耗尽型 DOS(denial- of-service) 攻击技术[20]，在对攻击类型、组合、信息状态等维度进行考虑的基础上研究电网严重故障搜索算法。

如图 1 所示，在面向电力系统的网络攻击手段中，拒绝服务式攻击 DOS 能对远程调度控制中心的通信网络进行破坏，使电力通信业务中断，并发展成设备故障，这种最为直接的攻击手段具有很强的破坏性。DOS 攻击能够对目标 CPPS 信息侧存在的网络协议漏洞进行挖掘，通过消耗其网络带宽、允许链接和通信进程等网络资源，使网络失去通信[20-21]；对通信节点实施 DOS 攻击还会引发 CPPS 分层控制结构的调度数据网的区域性瘫痪，即便提升通信数据计算处理速度、提高带宽通信能力，也无法避免 DOS 攻击造成的破坏性。具备有限的容错能力是 CPPS 本身负荷频率控制系统的一个基本特点，可通过有差调节维持一定的稳定性；但当 DOS 攻击引起断网等事故时，电力系统稳定性遭到严重破坏，尤其是在分布式 DOS 攻击方式下，为维持部分重要电力业务，电力系统会采取切负荷等防御手段。

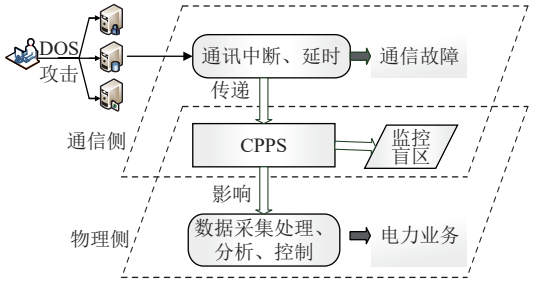


图 1　面向电力网络的 DOS 攻击影响示意图

## 1.1　可行性分析

由前述内容可知，资源耗尽型网络攻击技术能够通过削弱或破坏二次系统的正常功能来达到攻击的目的，而当 SCADA 系统、WAMS(wide area measurement system)、AMI(advanced metering infrastructure) 等二次系统发生故障或遭受恶意攻击时，CPPS 出现信息中断、延迟、篡改等情况，会导致控制中心下达错误指令，使决策单元误动或退出运行，从而对电力系统造成严重故障，使其一次系统的完整性遭到破坏[8]。

另一方面，电力系统中为确保电网的安全稳定运行，普遍遵循N－1安全准则对安全稳定设备进行配置；即在正常运行方式下电力系统中任意一元件 (如线路、发电机、变压器等) 出现异常或因故障断开后，电力系统应能保持稳定运行和正常供电、其他元件不过负荷、电压和频率均在允许范围内的规范要求[22]。目前电力系统主要采用N－1仿真校验作为最为有效的电网安全性评价手段，在电网

运行中，行之有效的电网安全管理理念与基于N－1安全准则的安全稳定预控密不可分[23]。但电力系统在N－$n$故障的可靠裕度方面存在成本–收益冲突的问题，即N－$n$故障发生概率极小，若以此为标准来确定电力系统的可靠裕度会导致成本过高，而普遍采用N－1准则，故在处理N－$n$故障时的处置策略较为被动，缺乏灵活性。针对电力系统这一特点，在电力系统薄弱状态下发起网络攻击，可在原有故障基础上引发N－$n$多重故障，达到连锁故障的效果，此时网络攻击对已经处于薄弱状态下的电力系统造成的破坏力，远高于其对电力系统处于正常状态下造成的破坏力。因此可以通过攻击处于薄弱状态时的电网，以达到攻击者期望的较为良好的攻击效果。

### 1.2 搜索模型

严重故障搜索模型以传统电力系统N－$n$故障为研究导向，以N－1故障为研究基础，以获得最佳攻击收益的目标，使用减载量作为攻击收益量化数据，采用线性规划模型分析数据。严重故障搜索分为两个阶段实施。

1) 攻击类型分为以考虑发电机为主要因素的网络攻击和以考虑支路为主要因素的网络攻击，通过对预攻击的发电机和支路进行设置，形成攻击组合，根据已获取的目标电网拓扑信息构筑节点–线路关联矩阵，如图 2 所示。对电力系统攻击成功状态空间进行搜索，依据搜索得到的减载量筛选出严重故障并标记出其对应的攻击目标。

$$
\begin{array}{c}
\text{节点} \\
\begin{array}{c} \\ \text{线路} \end{array}
\begin{array}{c}
\begin{array}{ccccccc} N_1 & \cdots & N_i & \cdots & N_n \end{array} \\
\begin{bmatrix}
X_{11} & \cdots & X_{1j} & \cdots & X_{1n} \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
X_{i1} & \cdots & X_{ij} & \cdots & X_{in} \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
X_{n1} & \cdots & X_{nj} & \cdots & X_{nn}
\end{bmatrix}
\end{array}
\begin{array}{c} L_1 \\ \vdots \\ L_i \\ \vdots \\ L_n \end{array}
\end{array}
$$

图 2 线路–节点关联矩阵

2) 在阶段 1) 的基础上，将信息状态纳入考虑，如图 3 所示。此处信息状态主要指：被攻击方 (防御方) 受到攻击后依据正常故障处置办法，通过调用备用发电容量和重合闸等手段来发送负荷修复指令的信息收发状态。对信息状态进行攻击，使其丧失故障后的负荷修复能力，此时得到的减载量为最终减载量 (或称延缓减载量)。

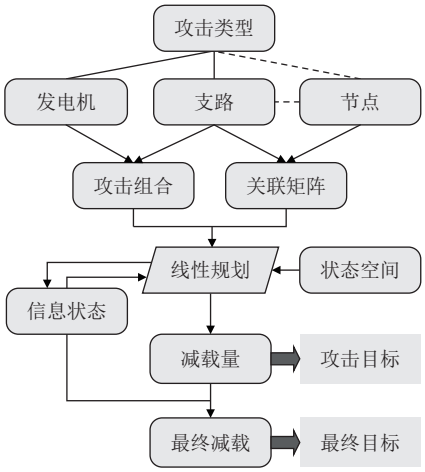


图 3 故障搜索流程图

### 1.3 收益量化

通过负荷减载量化攻击电网获得的攻击收益，针对线路、发电机、节点的电力系统攻击能够改变电网拓扑结构并使电网偏离正常状态，假设电力系统为减小攻击带来的危害，以牺牲部分负荷来维持其自身处于正常运行状态，在各场景下最小减载量为：

$$\min\ f = \sum_{i \in N} D_i \tag{1}$$

式中，$N$ 为电力系统所包含节点；$i$ 为节点下标；$f$ 为电网总的减载量；$D_i$ 为序号为 $i$ 的节点减载量。

为得到最小减载量，需建立直流潮流模型，节点电压相角为线路功率的主要影响变量，线路潮流与线路阻抗和节点相角关系为：

$$P_l = \frac{E_l}{x_l} \sum_{i \in N} H_i \delta_i \quad l \in L \tag{2}$$

式中，$L$ 为电网中的支路总集；$l$ 为支路在总集中的排列序号；$P_l$ 为支路 $l$ 上流通的潮流；$E_l$ 代表支路 $l$ 通态或断态，即为 0 或 1；$x_l$ 代表支路 $l$ 的阻抗值；$\boldsymbol{H}$ 为节点–线路关联矩阵；$\boldsymbol{\delta}$为相角矩阵。

电力系统中潮流服从功率平衡条件，节点负荷和流入流出功率之间的约束为：

$$\sum_{m \in M} B_m P_m - \sum_{i \in N} H_i P_i = Q_i - D_i \tag{3}$$

式中，$M$ 为电网中发电机总集；$m$ 为发电机在总集中的排列序号，$B_m$ 为发电机 $m$ 处于停机或者运行状态；$P_m$ 为发电机 $m$ 的有功出力；$Q_i$ 为节点 $i$ 上的负荷量。

支路上的潮流、发电机的发电功率、节点上的切负荷量都要受到各自的上下限制约，不能超出约

束范围：

$$-P_l^{\max} \leqslant P_l \leqslant P_l^{\max} \quad l \in W \tag{4}$$

$$P_m^{\min} \leqslant P_m \leqslant P_m^{\max} \quad m \in M \tag{5}$$

$$0 \leqslant D_i \leqslant Q_i \quad i \in N \tag{6}$$

式中，$P_l^{\max}$为支路 $l$ 上的流通功率上限值；$P_m^{\max}$为发电机 $m$ 的发电出力上限值；$P_m^{\min}$为发电机 $m$ 的发电出力下限值。

## 2　薄弱状态下自动攻击研究方法

电力系统薄弱状态指电力系统偏离正常运行的状态。为获得高于在电力系统处于正常状态时的攻击收益，利用电网处于薄弱状态对电力系统进行攻击。为达到这一攻击目的，需要把目标电力系统实时数据信息与正常状态数据信息进行比对，通过异常数据信息来辨别电力系统是否处于薄弱状态，并确定电力系统是否已出现N－1故障。攻击者利用所掌握目标电力系统部分节点配备的 PMU 稳定控制业务数据信息，形成可观测的攻击实施区间，对其中的单个或几个线路进行网络攻击，构成N－$b$故障，对电力系统攻击成功状态空间进行遍历，通过线性规划计算出线路由于攻击成功而断线时可产生的减载量，遵循最大化原则筛选出严重故障情况下可获得的减载量以及攻击位置等信息，从而获得针对电力系统薄弱状态下的自动攻击策略。

### 2.1　攻击者掌握完全信息

为提高攻击成功率，攻击方事先应通过各种手段来获取目标电力系统的相关信息。当攻击方掌握目标电力系统的完全信息时，攻击区间达到最大，同时与选定攻击类型相对应的攻击组合数量也达到最大。

利用掌握目标电力系统的完全信息对处于薄弱状态下电网发起攻击的策略方法分为 6 个步骤，对应的具体流程如图 4 所示。

1) 在薄弱状态基础上，使目标电力系统出现连锁故障，并以此为目标确定攻击方向，开始运行程序；

2) 将目标电力系统实时数据信息同正常数据进行对比，判别电网是否处于薄弱状态。此处仅做数据比对，不需要做大量计算，运算速度快，所以既能以一个时间断面静态进行，也可动态循环扫描；

3) 当电力系统被识别为薄弱状态，标记为N－1故障后，确立故障类型、位置，为严重故障搜索做准备；若不处于故障状态则返回至实时数据和正常数据对比阶段；

4) 在进行严重故障搜索时，需要把N－1故障的故障类型、位置纳入考虑，以此为基础形成攻击空间，并对攻击空间进行遍历，以减载量作为衡量攻击效果的量化数据，通过严重故障搜索算法得出此时处于薄弱状态下的电力系统的最优可攻击目标组合；

5) 判别目标电力系统的减载量或减载百分比是否符合收益判据，即攻击收益是否符合攻击收益预期。若不符合预期时，则自动忽略本次电网薄弱状态，转至实时数据与正常数据对比处，继续寻找下一个电力系统薄弱状态；

6) 当攻击收益符合预期时，确立减载百分比，并标记对应的攻击组合、类型，形成新的攻击方案。

在电力系统处于薄弱状态后，修改电力网拓扑信息，形成新的网络攻击状态空间，根据严重故障搜索算法，对攻击状态空间遍历，得到符合攻击收益条件的攻击区间，由此形成自动攻击策略。

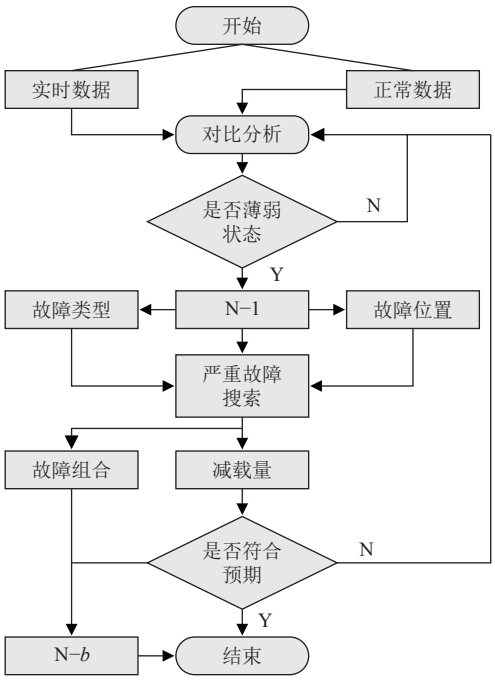


图 4　完全信息时攻击策略

### 2.2　攻击者掌握非完全信息

当攻击方未获得目标电力系统的全部 PMU 稳控信息数据时，如图 5 所示，此时处于不完全信息状态，即为可用攻击信息受限[20]。有限的攻击资源

表现为可攻击的目标数量有限，有限的可用攻击信息意味着攻击范围有限，在有限的攻击范围内，寻找使攻击收益最大化的攻击目标，需要考虑线路、节点等在不同场景下的组合问题，这样攻击者通过严重故障搜索结果对攻击资源进行配置，在电网中多处发起针对线路、发电机、变压器等元件的分布式攻击，在单位时间内使电力系统出现多重故障，迫使电力系统因无法同时承受多处攻击造成的破坏，采取诸如切负荷等临时稳定控制的处置办法。

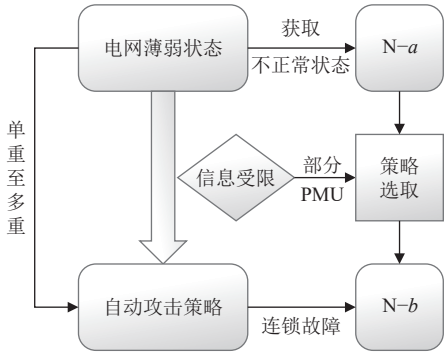


图 5 非完全信息时攻击策略

在这种非完全信息情况下，根据已知 PMU 稳控信息构成的攻击区间为完全信息时的攻击空间的子区间；攻击组合形成的集合为完全信息时攻击组合形成的集合的子集；完全信息时的攻击收益为不完全信息时的攻击收益上限；非完全信息时自动攻击策略的最终目的同完全信息时一致：得到符合攻击者期望的攻击区间。攻击者不仅要依据完全信息时的自动攻击策略设计攻击流程，还需要充分考虑信息受限时的攻击范围；在完全信息情况下与在非完全信息情况下，虽然都是通过薄弱状态来形成连锁故障，但在信息受限时，由于已获取的可用攻击信息不同，这就会导致不同场景下形成的攻击范围不同，从而取得的攻击效果也不同，攻击效果呈现出不确定性、随机性、分散性，这与完全信息时攻击效果的确定性、集中性形成鲜明对比。不过单就某一确定的非完全信息时的攻击场景而言，其攻击效果又会相似于完全信息时的攻击场景。

## 3 算例分析

以 IEEE39 节点系统为例验证本文所提方法。基于已获取的 PMU 部署信息数据确定攻击场景，IEEE39 节点系统如图 6 所示。

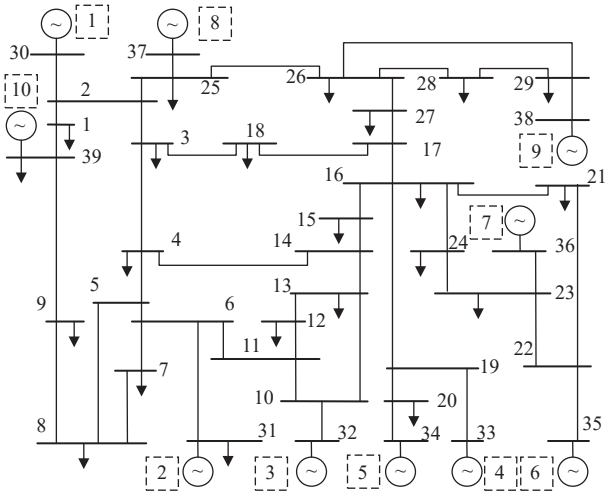

图 6 IEEE39 节点系统图

### 3.1 考虑单重故障至双重连锁故障的攻击场景

在由N－1电网薄弱状态到N－2故障状态的攻击场景中，假设因为信息受限，攻击方只知道部分 PMU 部署信息，通过监测电力系统，识别出电力系统出现单重故障，确认电力系统处于薄弱状态后，根据已知 PMU 数据信息形成攻击范围，对攻击范围内所有支路通断状态进行遍历并修改部分数据，形成N－2故障，在此场景中，假设已识别出 IEEE39 节点系统中 37 支路发生故障。在众多攻击场景中选取 8 个子场景进行比对。结果如图 7 和表 1 示。

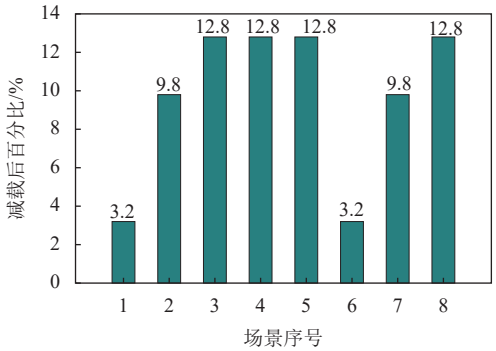


图 7 事故减载前各攻击场景下减载比重

表 1 事故减载前 IEEE 39 节点部分 PMU 位置

| 场景序号 | PMU位置 | 被攻击线路 |
|---|---|---|
| 1 | 5 | 8 |
| 2 | 2，5 | 5 |
| 3 | 2，5，10 | 20 |
| 4 | 2，10 | 20 |
| 5 | 5，10 | 20 |
| 6 | 5，15 | 8 |
| 7 | 2，15 | 5 |
| 8 | 10，15 | 20 |

在电力系统处于薄弱状态 (37 支路断开) 时，从已知 PMU 数量不同时和已知 PMU 数量相同时两个方向分析。

如图 7 与表 1 数据所示，在子场景 1、2、3 中，减载百分比随着可获取 PMU 数量的增加而增加，表明攻击收益与已知信息量呈正相关。在子场景 2、4、5、6、7、8 中，PMU 数量相等，但减载百分比却不一样，表明信息量相同时，不同组合得到的结果也不一样。从图 7 中可以看出，在子场景 3、4、5、8 中，减载比重明显高于其他场景，再结合表 1 中被攻击线路一列数据进行分析，可以得出此时支路 20 为关键支路，该攻击点与 10 节点处设置的 PMU 密切相关。

如果攻击方处于完全信息情况下，对处于正常状态的电力系统进行全面的N－2严重故障搜索，攻击者得到的攻击线路组合为线路 20 和线路 37，可等效为线路 37 故障时线路 20 为关键线路，和前述从N－1电网薄弱状态到N－2故障状态的攻击场景中获得的结论一致，这表明，无论是通过单重故障攻击诱使处于薄弱状态下的电力系统发生双重故障，还是直接使电力系统发生双重故障，得到的攻击效果一致。但攻击子场景 2、4、5、7、8 表明如果攻击方掌握的信息不完全则不一定能达到该效果，这是由于掌握的信息有限，有限信息集作为完全信息集 (母集) 的子集，只包含有完全信息集中的部分元素，不一定包含关键元素，元素的不同组合构成的子集，会对自动攻击策略产生影响。另外，经过检查发现线路 20 对应 IEEE39节点系统中 10–32 支路，32 节点上只连接 3 号发电机与线路 20，故对线路 20 发起攻击得到的攻击效果等同于直接攻击 3 号发电机。

### 3.2　考虑事故处理的攻击场景

处于薄弱状态时，电力系统稳控业务依据事故处置办法处理引起电网不稳定的因素，在其进行事故处理前后，攻击的效果存在差异，事故处理过程中出现的减载量使这种差异具体化。在 3.1 中因为未区分在事故减载前攻击与在事故减载后攻击的区别，只对事故减载前攻击场景进行算例分析。此处补充事故减载后攻击场景，假设条件同前面一样，得到的攻击收益结果如图 8 与表 2 示。

从图 8 可以看出，在电力系统对人为因素或者自然灾害引起的单重故障调用N－1准则进行减载处理后，通过严重故障搜索对攻击范围进行遍历并修改部分数据，形成N－2严重故障，在各个子场景下得到的攻击收益结果普遍小于图 7 所示的攻击收益结果。

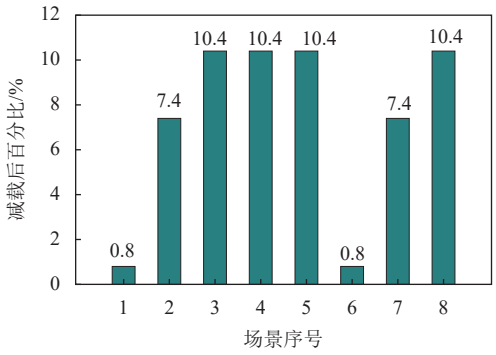


图 8　事故减载后各场景下减载比重

**表 2　事故减载前 IEEE 39 节点部分 PMU 位置**

| 场景序号 | PMU位置 | 被攻击线路 |
|---|---|---|
| 1 | 5 | 8 |
| 2 | 2，5 | 5 |
| 3 | 2，5，10 | 20 |
| 4 | 2，10 | 20 |
| 5 | 5，10 | 20 |
| 6 | 5，15 | 8 |
| 7 | 2，15 | 5 |
| 8 | 10，15 | 20 |

因此，在攻击手段允许的情况下，攻击方应尽可能选取事故减载前攻击的攻击方式，这样得到的收益效果更符合用较低的攻击成本获得更高的攻击收益的目标。

### 3.3　考虑节点母线故障的攻击场景

通常 PMU 设置在节点母线，攻击方掌握部分 PMU 信息就意味着可以将节点作为攻击对象。假设已识别出 IEEE39 节点系统中 37 支路发生故障，在电力系统处于薄弱状态下选择节点作为攻击对象的场景，结果如图 9 与表 3 示。

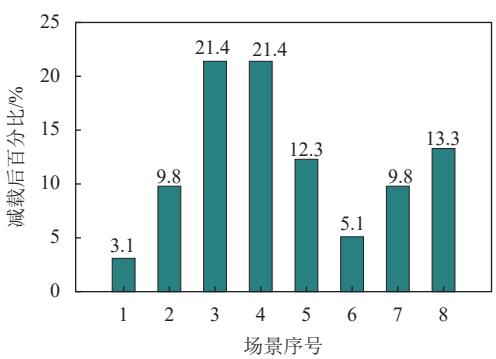


图 9　考虑节点时各攻击场景下减载比重

**表 3 考虑节点时 IEEE 39 节点部分 PMU 位置**

| 场景序号 | PMU位置 | 被攻击线路 |
|---|---|---|
| 1 | 5 | 8，10，11 |
| 2 | 2，5 | 1，3，4，5，8，10，11 |
| 3 | 2，5，10 | 1，3，4，5，8，10，11，18，19，20 |
| 4 | 2，10 | 1，3，4，5，18，19，20 |
| 5 | 5，10 | 8，10，11，18，19，20 |
| 6 | 5，15 | 8，10，11，24，25 |
| 7 | 2，15 | 1，3，4，5，24，25 |
| 8 | 10，15 | 18，19，20，24，25 |

可以发现，由场景 1、2、3 知攻击收益与已知信息量呈正相关。由场景 2、4、5、7、8 知信息量相同时，不同组合得到的结果也不一样，总体上，与收益趋势有关的结论与前面相似。但在一些场景下，如 PMU 所在位置为 2，5，10 时，3.3 节得到的攻击收益明显高于 3.1 节中对应场景的攻击收益。这是因为电力系统出于经济性考虑一般会在单条线路的一端设有 PMU，节点母线与多个线路连接，使得一个 PMU 控制多条线路，在该 PMU 受到攻击时，与之相连接的线路会受到波及，若把攻击节点等效为攻击支路，则相当于同时使多条线路受损，故在子场景相同时，与 3.1 节相比，3.3 节得到的攻击收益一般较高。

## 4 结 束 语

针对目标电力系统的网络攻击已经对 CPPS 安全稳定造成较为严重的破坏，本文从攻击者角度研究了利用电力系统处于薄弱状态时开展的自动攻击策略，基于直流潮流模型，提出在信息受限的情况下通过严重故障搜索寻找使目标电网受损的严重故障。本文以 IEEE39 节点系统为检验标准，对 N－1故障至N－2故障、考虑事故处理、考虑节点母线故障等不同场景进行仿真，并对得到的结果进行分析比较。多个场景中的数据表明，攻击方在不完全信息下，获取的可利用信息量越大，攻击产生的减载量越大，获得的攻击收益越高。

本文仅从 CPPS 的电力物理侧针对电力系统薄弱状态下的攻击进行研究，对建立电力系统的安全防御措施提供一定的借鉴意义。未来将从物理侧与信息侧交互攻击、电网偶发事故应急处理后发起攻击、纵向短路故障等角度展开进一步的研究。

## 参 考 文 献

[1] HUA Y , LIU Y , PENG Z . Efficient eigen-analysis for large delayed cyber-physical power system using explicit infinitesimal generator discretization[J]. IEEE Transactions on Power Systems, 2016, 31(3): 2361-2370.

[2] CHEN C, WANG J, LI Z, et al. PMU uncertainty quantification in voltage stability analysis[J]. IEEE Transactions on Power Systems, 2015, 30(4): 2196-2197.

[3] SARMA N, RAJU V V, RAO K. Design of telemetering configuration for energy management systems[J]. IEEE Transactions on Power Systems, 2002, 9(1): 381-387.

[4] 陈武晖, 陈文淦, 薛安成. 面向协同信息攻击的物理电力系统安全风险评估与防御资源分配[J]. 电网技术, 2019, 43(7): 2353-2360.
CHEN W H, WU W G, XUE A C. Security risk assessment and defense resource allocation of power system under synergetic cyber attacks[J]. Power System Technology, 2019, 43(7): 2353-2360.

[5] OYEWOLE P A, JAYAWEERA D. Power system security with cyber-physical power system operation[J]. IEEE Access, 2020, 8: 179970-179982.

[6] DAI J , QIU J , WU J , et al. A vulnerability assessment method of cyber physical power system considering power-grid infrastructures failure[C]//2019 IEEE Sustainable Power and Energy Conference (iSPEC). [S.l.]: IEEE, 2019: 129-132.

[7] 汤奕, 陈倩, 李梦雅, 等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化, 2016, 40(17): 59-69.
TANG Y, CHEN Q, LI M Y, et al. Overview on cyber-attacks against cyber physical power system[J]. Automation of Electric Power Systems, 2016, 40(17): 59-69.

[8] ABEDI A, HESAMZADEH M R, ROMERIO F. An ACOPF-based bilevel optimization approach for vulnerability assessment of a power system[J]. International Journal of Electrical Power & Energy Systems, 2021, 125: 78-85.

[9] SPERSTAD I B, SOLVANG E H, JAKOBSEN S H. A graph-based modelling framework for vulnerability analysis of critical sequences of events in power systems[J]. International Journal of Electrical Power & Energy Systems, 2021, 125: 32-37.

[10] 郭庆来, 辛蜀骏, 王剑辉, 等. 由乌克兰停电事件看信息能源系统综合安全评估[J]. 电力系统自动化, 2016(5): 145-147.
GUO Q L, XIN S J, WANG J H, et al. Comprehensive security assessment for a cyber physical energy system: A lesson from Ukraine's blackout[J]. Automation of Electric Power Systems, 2016(5): 145-147.

[11] 汤奕, 王琦, 倪明, 等. 电力信息物理融合系统中的网络攻击分析[J]. 电力系统自动化, 2016, 40(6): 148-151.
TANG Y, WANG Q, NI M, et al. Analysis of cyber attacks in cyber physical power system[J]. Automation of Electric Power Systems, 2016, 40(6): 148-151.

[12] 邱威, 贺静波, 谭真, 等. 一种用于含直流馈入的受端电网故障筛选与排序方法[J]. 电网技术, 2020, 44(9): 350-358.
QIU W, HE J B, TAN Z, et al. Contingency screening and ranking for receiving-end power grid with infeed HVDC[J]. Power System Technology, 2020, 44(9): 350-

358.

[13] 董朝阳, 赵俊华, 文福拴, 等. 从智能电网到能源互联网: 基本概念与研究框架[J]. 电力系统自动化, 2014, 38(15): 1-11.
DONG C Y, ZHAO J H, WEN F S, et al. From smart grid to energy internet: Basic concepts and research framework[J]. Automation of Electric Power Systems, 2014, 38(15): 1-11.

[14] 苏盛, 吴长江, 马钧, 等. 基于攻击方视角的电力 CPS 网络攻击模式分析[J]. 电网技术, 2014, 38(11): 3115-3120.
SU S, WU C J, MA J, et al. Attacker's perspective based analysis on cyber attack mode to cyber-physical system[J]. Power System Technology, 2014, 38(11): 3115-3120.

[15] 程林, 郭永基. 发输电系统充裕度和安全性算法研究[J]. 电力系统自动化, 2001, 25(19): 23-26.
CHENG L, GUO Y J. New algorithm of adequacy and security evaluation for bulk power system[J]. Automation of Electric Power Systems, 2001, 25(19): 23-26.

[16] 曾凯文, 文劲宇, 程时杰, 等. 复杂电网连锁故障下的关键线路辨识[J]. 中国电机工程学报, 2014, 34(7): 1103-1112.
ZENG K W, WEN J Y, CHENG S J, et al. New algorithm of adequacy and security evaluation for bulk power system[J]. Proceedings of the CSEE, 2014, 34(7): 1103-1112.

[17] 王宇飞, 李俊娥, 邱健, 等. 计及攻击损益的跨空间连锁故障选择排序方法[J]. 电网技术, 2018, 42(12): 3926-3937.
WANG Y F, LI J E, QIU J, et al. A novel selection sorting method of cascading failures across space considering attack gain and cost[J]. Power System Technology, 2018, 42(12): 3926-3937.

[18] 邓慧琼, 艾欣, 张东英, 等. 基于不确定多属性决策理论的电网连锁故障模式搜索方法[J]. 电网技术, 2005(13): 50-55.
DENG H Q, AI X, ZHANG D Y, et al. Search technique for power system cascading outages based on uncertain multiple attribute decision-making[J]. Power System Technology, 2005(13): 50-55.

[19] 庞凯元, 王一铮, 文福拴, 等. 计及通信失效的输电系统信息物理协同恢复策略[J]. 电力系统自动化, 2021, 45(3): 58-67.
PANG K Y, WANG Y Z, WEN F S, et al. Cyber-Physical collaborative restoration strategy for power transmission system with communication failures[J]. Automation of Electric Power Systems, 2021, 45(3): 58-67.

[20] ALENEZI M, REED M J. Efficient AS DoS traceback[C]//2013 International Conference on Computer Applications Technology (ICCAT). [S.l.]: IEEE, 2013: 33-41.

[21] LI W, SRINIVASAN B. Analysis and Improvements over DoS Attacks against IEEE 802.11I standard[C]//The 2nd International Conference on Networks Security Wireless Communications & Trusted Computing. [S.l.]: IEEE, 2010: 251-257.

[22] 孙英云, 游亚雄, 陈颖, 等. 一种考虑 N-1 约束的智能配电网信息网络启发式规划算法[J]. 电力系统自动化, 2014, 38(8): 50-55.
SUN Y Y, YOU Y X, CHEN Y, et al. A heuristic algorithm for network planning of smart distribution network considering N-1 constraint[J]. Automation of Electric Power Systems, 2014, 38(8): 50-55.

[23] 肖峻, 刘世嵩, 李振生, 等. 基于潮流计算的配电网最大供电能力模型[J]. 中国电机工程学报, 2014, 34(31): 5516-5524.
XIAO J, LIU S S, LI Z Z, et al. Model of total supply capability for distribution network based on power flow calculation[J]. Proceedings of the CSEE, 2014, 34(31): 5516-5524.

编　辑　叶　芳