第XX卷 第XX期 XXXX年XX月XX日
DOI：10.7500/AEPS20240116004
电力系统自动化
Automation of Electric Power Systems
Vol. XX No. XX XX XX, XXXX

电力信息物理系统需求操控攻击策略及防护分析

严 康[1,3]，陆艺丹[2,3]，白晓清[4]，李 滨[4]
（1. 清华大学电机工程与应用电子技术系，北京市 100084；
2. 广西电网有限责任公司电力科学研究院，广西壮族自治区南宁市 530023；
3. 湖南大学电气与信息学院，湖南省长沙市 410082；
4. 广西电力系统最优化与节能技术重点实验室（广西大学），广西壮族自治区南宁市 530004）

摘要：随着大规模配电网用户侧电力异构物联设备（简称配电网用户侧物联设备）接入电力系统，互联网中用户负荷控制业务的主导地位愈加明显。由此，电力系统存在一条跨越信息物理空间的攻击路径——需求操控攻击，致使电力系统面临一种新型的网络安全威胁。在此背景下，研究需求操控攻击策略对于电力系统抵御该类网络攻击具有重要的指导意义。首先，文中阐述了黑客如何利用配电网用户侧物联设备实施需求操控攻击以及其特点，并基于负荷特征和电力设备运行特征制定电力系统中异常负荷规模约束。然后，以低攻击代价诱导传输线路故障为目的探讨需求操控攻击策略，分析了在该类需求操控攻击情景下传输线路的脆弱性。最后，通过多场景下的多个IEEE节点系统仿真验证了需求操控攻击可以在低代价的条件下影响电力系统运行安全。

关键词：配电网；信息物理系统；异构设备；可控负荷；用户侧；物联网

0 引言

电力系统作为国家关键基础设施，一直都是恐怖分子和敌对势力的重要目标之一[1]。2015年，乌克兰电网被黑客利用恶意软件Black Energy入侵，导致大规模停电事故[2]。2019年，委内瑞拉古里水电站被类似Stuxnet的病毒攻击，致使22个州停电[3]。可见，设备的网络安全已经成为了影响电力系统运行的关键要素之一。因此，有必要基于攻击者视角开展针对电力系统网络攻击方式和行为特征的研究，有助于电力安全从业人员识别电力系统潜在的安全威胁。

在此背景下，针对电力系统网络安全开展了大量基于攻击者视角的攻击策略研究。由于传统互联网中的用户负荷控制业务比例较低，研究主要集中于输电侧和电网侧电力物联设备。例如，针对自动发电控制（automatic generation control，AGC）装置，黑客可以通过恶意控制[4]和虚假数据注入[5]等方式导致频率失稳。文献[6]针对数据采集与监控（supervisory control and data acquisition，SCADA）系统制定了以最大运行成本为目标的负荷重分配攻击策略。文献[7]提出了物理攻击协同的概念，扩大了负荷重分配攻击的恶性影响。然而，随着越来越多的空调等智能电器以及老旧电器通过智能开关（统称为配电网用户侧物联设备）[8]接入电力系统，考虑配电网用户侧物联设备终端（简称终端）在开放环境中具有可控性和响应灵敏等特性，电力系统出现了一类新的信息物理攻击方式——需求操控（manipulation of demand，MAD）攻击[9]。

由于需求侧功率变化不受控于SCADA系统，黑客可通过恶意操控终端运行功率调节关键位置的可控负荷，进而影响电力系统的运行。文献[10-11]将异常负荷作为参数考虑，证明了大规模异常可控负荷对10 kV线路供电可靠性[10]和电能质量[11]的恶性影响。文献[12-13]依据“肉鸡”（即被黑客远程控制的配电网用户侧物联设备）的额定功率和数目量化异常负荷，分别论证大规模异常“同投”/“同退”可控负荷给电力系统频率带来的安全影响，其中，“同投”指攻击者向“肉鸡”下达增加运行功率的控制指令，造成负骤增的攻击形式；“同退”指攻击者向“肉鸡”下达减小运行功率的控制指令，造成负荷骤减的攻击形式。例如，黑客可利用250万“肉鸡”造成欧洲电网频率失稳[13]。然而，上述文献的异常负荷量化方法未考虑“肉鸡”的动态响应特性和状态特征，

收稿日期：2024-01-16；修回日期：2024-12-16。
上网日期：XXXX-XX-XX。
国家资助博士后研究人员计划资助项目（GZC20240788）；国家自然科学基金资助项目（51967001）。

且忽略了配电线路过流保护装置等对潜在异常负荷规模的影响，难以准确量化异常负荷，更无法衡量现阶段以及未来MAD攻击对电力系统的恶性影响。此外，在考虑低频减载、高频切机等装置动作的前提下[14]，黑客也可实施针对电力系统潮流的MAD攻击，给电力系统的可靠性带来严重的安全隐患，但现有研究缺乏对该类MAD攻击的考虑[15]。

针对上述问题，为更好地了解MAD攻击产生的潜在恶性影响，提出了一种针对电力系统线路潮流的低代价MAD攻击策略。首先，揭示黑客如何利用配电网用户侧物联设备实施MAD攻击，并以负荷特征和电力设备运行特征为基础分析MAD攻击中的异常负荷潜在规模从而给出相应的约束。然后，在最大化线路潮流的攻击前提下，以“肉鸡”操控数目最小化为目标进行建模，量化了低代价MAD攻击给电力系统带来的安全影响。最后，对所提MAD攻击策略进行求解，验证了攻击策略的有效性。

1 需求操控攻击

为更好地了解MAD攻击，本章介绍黑客如何利用配电网用户侧物联设备实施针对电力系统线路潮流的MAD攻击流程，并阐述MAD攻击的特点。

1.1 需求操控攻击的实施

与分布式拒绝服务（distributed denial of service，DDoS）[16]攻击相同，MAD攻击也是基于“肉鸡”的集群效应。终端作为信息域和物理域的交互节点，黑客可以将信息域中设备的网络安全风险传递至电力系统[17]，实现跨越信息物理空间的MAD攻击。由于终端具有分布广泛的特点，基于配电网用户侧物联设备的MAD攻击示意图如图1所示。

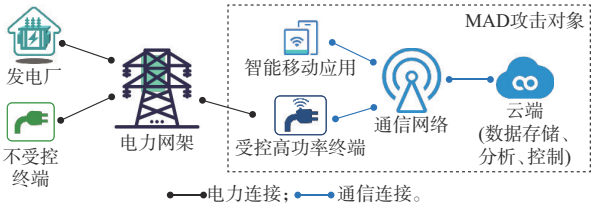


图1 MAD攻击示意图

Fig. 1 Schematic diagram of MAD attacks

首先，黑客可利用配电网用户侧物联设备各组件（云端、终端、移动应用）网络安全防护的薄弱环节和通信网络安全的脆弱性[9]获取目标位置上终端的控制权限；然后，感染互联网环境中的其他设备；最后，形成了一个高度受黑客控制的“肉鸡”网络。与DDoS攻击不同，MAD攻击中的“肉鸡”网络还需要确定“肉鸡”的地理位置。目前，识别“肉鸡”地理位置的方法如下：

1）通过因特网协议（IP）地址进行甄选。Maxmind、百度以及其他数据库可以提供IP地址所对应高精度的地理位置[18]。

2）通过Wi-Fi定位进行甄选。几乎所有的终端均配有Wi-Fi接收器，可以根据Wi-Fi接入点的基本服务集标识（basic service set identifier，BSSID）码进行准确地理定位[19]。

物理域中，在特定的时间节点，黑客向“肉鸡”网络发送改变其运行功率的控制指令（例如，更改空调设定温度等），即可形成异常负荷。由图1可知，由于终端是在电力系统的低压侧接入，异常负荷对电力系统的安全影响是从低电压等级传递至高电压等级。当黑客意图改变电力系统不同位置的可控负荷时，操控各10 kV线路中“肉鸡”网络的运行功率即可在所连电压等级110 kV及以上的变电站中形成异常负荷矩阵$\boldsymbol{D}^{\mathrm{a}}$。此时，输电网中线路潮流矩阵$\boldsymbol{F}_{\mathrm{l}}$上升为$\boldsymbol{F}_{\mathrm{l,a}}$，极有可能致使线路潮流越限，影响电力系统运行的可靠性[20]。

为了防范MAD攻击，本文立足于终端的瞬时功率变化所带来的安全影响，研究MAD攻击，并揭示黑客在“肉鸡”上的恶意行为特征。作为一种特殊的网络攻击形式，针对实施MAD攻击的黑客，本文作以下假设：

1）黑客具备一定的电力专业知识，了解电力系统运行方式、网架结构、经济调度结果等[21-22]；

2）黑客具备一定的信息安全专业知识，可以通过恶意软件、伪造控制指令等手段入侵不同变电站中的接入终端[23]，并可利用对“肉鸡”进行恶意行为试验获取该终端的运行参数[24]等；

3）黑客的“肉鸡”网络分布应具有地缘性，即不同级别黑客的终端“肉鸡”涉及的变电站数目不同；

4）在具备一定攻击资源的前提下，黑客应通过最小攻击代价实现最为恶劣的MAD攻击，即造成目标传输线路最大过载的前提下避免“肉鸡”过多地暴露。

1.2 需求操控攻击的特点

根据网络攻击对象分布的差异，本文将电力系统网络攻击分为以下3类，详见表1。

可见，与类型Ⅰ和类型Ⅱ的网络攻击相比，MAD攻击具有以下特点：

1）设备自身安全防护水平弱。受限于终端运行参数和存储空间，配电网用户侧物联设备各组件的通信通常使用轻量级加密算法和认证机制，其网络安全防护水平远低于网络攻击类型Ⅰ中的AGC装

表1　电力系统网络攻击类型
Table 1　Types of cyber attacks in power system

类型	分布	典型对象	安全防护	攻击路径	攻击方式
类型Ⅰ	发电侧	AGC装置	二次系统安全防护体系、256 bit加密算法等	互联网→专网	机组异常出力等
类型Ⅱ	电网侧	SCADA系统	二次系统安全防护体系、256 bit加密算法等	互联网→专网	虚假数据攻击等
类型Ⅲ	用户侧	配电网用户侧物联设备	轻量级加密算法、轻量级认证机制等	互联网	MAD攻击等

置和类型Ⅱ中的SCADA系统；

2）网络攻击路径差异。与类型Ⅰ和类型Ⅱ的网络攻击相比，MAD攻击的对象由电力专网中的电力物联设备转变为互联网中的配电网用户侧物联设备。由于二次系统安全防护体系并未覆盖配电网用户侧物联设备，黑客不需要突破电力二次系统安全防护体系中的物理隔离装置和入侵检测系统等安全防护措施[25]，仅需要通过互联网即可实现MAD攻击，极大增加了黑客实现电力系统网络攻击的可能性，示意图如附录A图A1所示。

综上所述，与过去针对电力系统的网络攻击不同，由于电力二次系统安全防护体系无法针对基于配电网用户侧物联设备的MAD攻击进行主动防御，并且需求侧功率变化并不受控于SCADA系统，MAD攻击给电力系统网络安全防护带来了全新的挑战。

2　异常负荷规模约束

目前，MAD攻击研究中的异常负荷量化仅考虑了终端“肉鸡”的额定运行功率和数目。在实际运行中，终端的运行功率与终端的响应模型、状态和室外环境有关，异常负荷的规模还与配电网线路过流保护装置有关。基于上述考虑，本章计及负荷特征以及电力设备运行特征，给出变电站异常负荷规模的计算方法，建立MAD攻击模型中的异常负荷规模约束。

2.1　终端响应模型

由于电动汽车的运行参数和存储空间远大于其余终端，电动汽车网络安全防护措施的强度远好于其余终端，更难被转换为“肉鸡”。同时，电动汽车需要根据用户的需求手动接入电力系统，并非实时接入。因此，根据设备的渗透率以及普及率（见附录A表A1），本节着重介绍定频空调（fixed-frequency air conditioner，FAC）、变频空调（inverter air conditioner，IAC）、电热水器和洗衣机等典型终端的响应模型。

1）FAC

根据等效热参数模型来模拟FAC的热动力过程，FAC制冷装置的关停和开启时长与空调运行参数的关系为[26]：

$$\begin{cases} H^{\mathrm{ac,off}} = R^{\mathrm{ac}} C^{\mathrm{ac}} \ln \dfrac{T^{\mathrm{ac,min}} - T^{\mathrm{out}}}{T^{\mathrm{ac,max}} - T^{\mathrm{out}}} \\ H^{\mathrm{ac,on}} = R^{\mathrm{ac}} C^{\mathrm{ac}} \ln \dfrac{T^{\mathrm{ac,min}} + \eta^{\mathrm{ac}} D^{\mathrm{ac,d,r}} R^{\mathrm{ac}} - T^{\mathrm{out}}}{T^{\mathrm{ac,max}} + \eta^{\mathrm{ac}} D^{\mathrm{ac,d,r}} R^{\mathrm{ac}} - T^{\mathrm{out}}} \end{cases} \tag{1}$$

式中：$H^{\mathrm{ac,off}}$和$H^{\mathrm{ac,on}}$分别为FAC制冷装置在稳态时一个控制周期内的关停时长和开启时长；R^{ac}为房间等效热阻；C^{ac}为房间等效电容；$T^{\mathrm{ac,min}}$为室内最低温度，$T^{\mathrm{ac,min}} = T^{\mathrm{ac,set}} - 1$，$T^{\mathrm{ac,set}}$为FAC设定温度；$T^{\mathrm{ac,max}}$为室内最高温度，$T^{\mathrm{ac,max}} = T^{\mathrm{ac,set}} + 1$；$T^{\mathrm{out}}$为室外温度；$\eta^{\mathrm{ac}}$为制冷系数；$D^{\mathrm{ac,d,r}}$为FAC的最大运行功率。

单台FAC的运行功率$D^{\mathrm{ac,d}}$为：

$$D^{\mathrm{ac,d}} = D^{\mathrm{ac,d,r}} \frac{H^{\mathrm{ac,on}}}{H^{\mathrm{ac,on}} + H^{\mathrm{ac,off}}} \tag{2}$$

2）IAC

IAC与FAC的不同点在于室内的温度控制原理，IAC是根据调节压缩机的频率来改变制冷量，使得室内温度基本维持在设定温度。单台IAC的运行功率$D^{\mathrm{ac,b}}$为[27]：

$$D^{\mathrm{ac,b}} = \begin{cases} D^{\mathrm{ac,b,r}} & T^{\mathrm{in}} \in [T^{\mathrm{ac,set}} + T^{\mathrm{D}}, T^{\mathrm{out}}] \\ D^{\mathrm{ac,b,r}} + \beta (T^{\mathrm{in}} - T^{\mathrm{ac,set}} - T^{\mathrm{D}}) & \\ & T^{\mathrm{in}} \in [T^{\mathrm{ac,set}}, T^{\mathrm{ac,set}} + T^{\mathrm{D}}) \\ 0 & T^{\mathrm{in}} \in [T^{\mathrm{r,min}}, T^{\mathrm{ac,set}}) \end{cases} \tag{3}$$

式中：$D^{\mathrm{ac,b,r}}$为IAC制冷装置的最大运行功率；T^{in}为室内温度；T^{D}为变频空调控制的大死区温差；β为IAC功率变化系数；$T^{\mathrm{r,min}}$为使用IAC的室内最低温度，$T^{\mathrm{r,min}} = T^{\mathrm{ac,set}} - T^{\mathrm{d}}$，$T^{\mathrm{d}}$为IAC控制的死区温差。

3）电热水器

电热水器在加热时主回路供电，运行功率为最大运行功率；不加热时，仅通过控制回路对热水器内温度进行监测，运行功率可忽略不计。根据文献[28]得到电热水器制热装置的关停时长和开启时长与电热水器运行参数的关系式为：

$$\begin{cases} H^{\mathrm{w,off}} = R^{\mathrm{w}} C^{\mathrm{w}} \ln \dfrac{T^{\mathrm{w,min}} - T^{\mathrm{w,out}}}{T^{\mathrm{w,max}} - T^{\mathrm{w,out}}} \\ H^{\mathrm{w,on}} = R^{\mathrm{w}} C^{\mathrm{w}} \ln \dfrac{T^{\mathrm{w,min}} - Q^{\mathrm{w,h}} R^{\mathrm{w}} - T^{\mathrm{w,out}}}{T^{\mathrm{w,max}} - Q^{\mathrm{w,h}} R^{\mathrm{w}} - T^{\mathrm{w,out}}} \end{cases} \tag{4}$$

式中：$H^{\mathrm{w,on}}$和$H^{\mathrm{w,off}}$分别为电热水器加热装置在稳态时一个控制周期内的开启时长和关停时长；R^{w}和C^{w}分别为电热水器水箱的等效热阻和等效电容；

$T^{w,min}$为水温下限，$T^{w,min}=T^{w,set}-T^{w,d}$，$T^{w,set}$为电热水器的设定温度，$T^{w,d}$为电热水器控制的死区温差；$T^{w,max}$为水温上限，$T^{w,max}=T^{w,set}+T^{w,d}$；$T^{w,out}$为室外水温；$Q^{w,h}$为电热水器加热等效功率，$Q^{w,h}=\eta^{w}D^{w,r}$，$\eta^{w}$和$D^{w,r}$分别为电热水器的制热系数和最大运行功率。

单台电热水器的运行功率D^{w}为：

$$D^{w}=D^{w,r}\frac{H^{w,on}}{H^{w,on}+H^{w,off}} \tag{5}$$

4)洗衣机

洗衣机在工作时的运行功率为额定运行功率(即最大运行功率)，待机时的运行功率为0，其运行功率D^{ws}为：

$$D^{ws}=D^{ws,r} \tag{6}$$

式中：$D^{ws,r}$为洗衣机最大运行功率。

2.2 各状态可操控终端数目

在MAD攻击中，需要考虑变电站接入的终端数目。根据配电网的结构(见附录A图A2)，本节以10 kV线路为基础[29]，并引入相关系数以推算变电站中各状态的接入终端数目，具体计算公式为：

$$[\boldsymbol{N}_i^{I},\boldsymbol{N}_i^{O}]=\mathrm{diag}(\boldsymbol{N}_i)[\boldsymbol{\mu}_i^{I},\boldsymbol{\mu}_i^{O}] \tag{7}$$

式中：$\boldsymbol{N}_i^{I}$和$\boldsymbol{N}_i^{O}$分别为变电站i所连接的10 kV线路中的待机终端数目向量和运行终端数目向量；$\mathrm{diag}(\boldsymbol{N}_i)$为变电站$i$所连接的10 kV线路中的终端数目的对角阵；$\boldsymbol{\mu}_i^{I}$和$\boldsymbol{\mu}_i^{O}$分别为线路中终端的待机系数向量和运行系数向量。

在实际情况中，黑客难以准确操控变电站中所有的接入终端。由于攻击的随机性，黑客可操控的终端中待机、运行比例应与接入终端中的比例相同，线路中可操控终端数目为：

$$[\boldsymbol{N}_i^{a,I},\boldsymbol{N}_i^{a,O}]=\mathrm{diag}(\boldsymbol{\alpha}_i)[\boldsymbol{N}_i^{I},\boldsymbol{N}_i^{O}] \tag{8}$$

式中：$\boldsymbol{N}_i^{a,I}$和$\boldsymbol{N}_i^{a,O}$分别为线路中的待机“肉鸡”数目向量和运行“肉鸡”数目向量；$\boldsymbol{\alpha}_i$为黑客对变电站i所连接的10 kV线路中的终端控制系数矩阵。

2.3 10 kV线路异常负荷规模

当黑客对变电站中的“肉鸡”网络发送恶意控制指令时，10 kV线路h中异常负荷的计算公式为：

$$\begin{cases}D_{i,h}^{a,max,1}=\gamma[(\boldsymbol{K}_{i,h}^{a,I})^{T}\boldsymbol{D}_{i,h}^{I,+}+(\boldsymbol{K}_{i,h}^{a,O})^{T}\boldsymbol{D}_{i,h}^{O,+}]\\ D_{i,h}^{a,min}=\gamma[(\boldsymbol{K}_{i,h}^{a,I})^{T}\boldsymbol{D}_{i,h}^{I,-}+(\boldsymbol{K}_{i,h}^{a,O})^{T}\boldsymbol{D}_{i,h}^{O,-}]\end{cases} \tag{9}$$

式中：$D_{i,h}^{a,max,1}$为变电站i所连接的10 kV线路h中异常负荷的潜在最大值；$D_{i,h}^{a,min}$为变电站i所连接的10 kV线路h中异常负荷的最小值；γ为线损修正系数，本文取1.03；$\boldsymbol{K}_{i,h}^{a,I}$为变电站$i$所连接的10 kV线路$h$中待机终端的可操控状态的0-1向量，其元素的值为0表示不被黑客操控，值为1表示被黑客操控；$\boldsymbol{K}_{i,h}^{a,O}$为变电站$i$所连接的10 kV线路$h$中运行终端可操控状态的0-1向量；$\boldsymbol{D}_{i,h}^{I,+}$为变电站$i$所连接的10 kV线路$h$中待机终端的负荷“同投”攻击功率最大值向量；$\boldsymbol{D}_{i,h}^{O,+}$为变电站$i$所连接的10 kV线路$h$中运行终端的负荷“同投”攻击功率最大值向量；$\boldsymbol{D}_{i,h}^{I,-}$为变电站$i$所连接的10 kV线路$h$中待机终端的负荷“同退”攻击功率最大值向量；$\boldsymbol{D}_{i,h}^{O,-}$为变电站$i$所连接的10 kV线路$h$中运行终端的负荷“同退”攻击功率最大值向量。其中，$\boldsymbol{N}_i^{a,I}+\boldsymbol{N}_i^{a,O}=\boldsymbol{1}^{T}\boldsymbol{K}_{i,h}^{a,I}+\boldsymbol{1}^{T}\boldsymbol{K}_{i,h}^{a,O}$，$\boldsymbol{N}_{i,h}^{a,I}$和$\boldsymbol{N}_{i,h}^{a,O}$分别为线路$h$中待机“肉鸡”数目和运行“肉鸡”数目，$\boldsymbol{1}$为元素全为1的向量。

为了避免10 kV线路过载运行，变压器通常设有过载保护开关，其过载保护装置的动作电流通常设置为线路额定电流的1.25倍。当黑客所操控的异常负荷致使10 kV线路传输电流超过保护装置动作电流时，过流保护装置动作，将造成线路供电中断，即无法形成负荷“同投”攻击。综上，10 kV线路的负荷“同投”攻击功率阈值$D_{i,h}^{a,max,2}$为：

$$D_{i,h}^{a,max,2}=\sigma D_{i,h}^{rated}-D_{i,h}^{base} \tag{10}$$

式中：σ为黑客负荷“同投”攻击系数，本文设置为1.25；$D_{i,h}^{rated}$为变电站i所连接的10 kV线路h的传输容量；$D_{i,h}^{base}$为变电站i所连接的10 kV线路h的传输功率。

变电站i所连接的10 kV线路h中异常负荷的最大值$D_{i,h}^{a,max}$为：

$$D_{i,h}^{a,max}=\min(D_{i,h}^{a,max,1},D_{i,h}^{a,max,2}) \tag{11}$$

2.4 变电站异常负荷规模约束

在考虑负荷特征和电力设备运行特征的前提下，各变电站的潜在异常负荷的取值区间为：

$$[D_i^{a,min},D_i^{a,max}]=\left[\sum_{h\in H}D_{i,h}^{a,min},\sum_{h\in H}D_{i,h}^{a,max}\right] \tag{12}$$

式中：$D_i^{a,min}$为变电站i的异常负荷最小值；$D_i^{a,max}$为变电站i的异常负荷最大值；H为线路集合。

在MAD攻击中，各变电站的异常负荷向量应满足：

$$\boldsymbol{D}^{a,min}\leqslant\boldsymbol{D}^{a}\leqslant\boldsymbol{D}^{a,max} \tag{13}$$

式中：$\boldsymbol{D}^{a}$为变电站的异常负荷向量；$\boldsymbol{D}^{a,max}$为异常负荷向量的最大值；$\boldsymbol{D}^{a,min}$为异常负荷向量的最小值。

在实际情况中，黑客的攻击资源通常是有限的，故黑客构建“肉鸡”网络的入侵特征(即可操控的可控负荷所分布的变电站数目)是有限的。设R为黑客实施该类MAD攻击策略需要涉及的变电站数目，相关关系式为：

$$\boldsymbol{1}^{T}\boldsymbol{\delta}^{a}\leqslant R \tag{14}$$

$$D_i=0\Leftrightarrow D_i^{a}=0\Leftrightarrow\delta_i^{a}=0 \tag{15}$$

式中：$\boldsymbol{\delta}^{\mathrm{a}}$为变电站的攻击状态的0-1向量；$D_i$为变电站$i$的负荷；$D_i^{\mathrm{a}}$为黑客在变电站$i$中所形成的异常负荷；$\delta_i^{\mathrm{a}}$为变电站$i$攻击状态的0-1变量，值为0表示变电站$i$关联的互联网可控负荷无法被操控，值为1表示可控负荷可以被操控。

3　低代价的需求操控攻击策略

在实际生产中，电力系统依据经济调度结果实时运行，执行区间为15 min。由于终端响应特性灵活，黑客操控可控负荷时刻、异常负荷产生时刻和线路潮流变化时刻同可以认为属于同一个时间断面。黑客可以在经济调度区间内操控可控负荷，导致在调度区间内的目标线路潮流过载，影响电力系统运行的可靠性，MAD攻击影响示意图如图2所示。

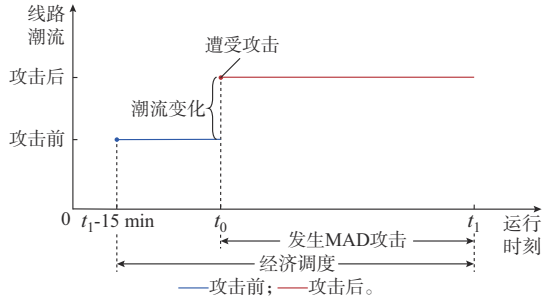


图2　MAD攻击影响示意图

Fig. 2　Schematic diagram of impact of MAD attack

低代价MAD攻击策略应达到以下目标：1）应在攻击资源有限的前提下，尽可能地造成目标传输线路过载运行；2）应确保高功率“肉鸡”率先响应的攻击策略，实现操控“肉鸡”数目最小，避免“肉鸡”过度暴露；3）异常负荷不会致使高频切机、低频减载等装置动作。针对电力系统经济调度场景中的线路潮流，本章提出一种低代价的MAD攻击策略。

3.1　变电站异常负荷形成策略

首先，MAD攻击策略需要确定黑客在输电网各变电站中产生的异常负荷。该阶段的目标是使传输线路k的潮流过载程度最大[30]。以在各变电站中产生的异常负荷为决策变量，基于线路传输功率约束和异常负荷规模约束建立该阶段的攻击策略，具体如下：

$$\max \left| F_k^{\mathrm{l.a}} \right| \tag{16}$$

$$\text{s.t.}\quad \mathbf{1}^{\mathrm{T}}\boldsymbol{D}^{\mathrm{a}} \leqslant 0.1(\mathbf{1}^{\mathrm{T}}\boldsymbol{D}) \tag{17}$$

$$\boldsymbol{F}^{\mathrm{l.a}} = \boldsymbol{S}_{\mathrm{F}}[\boldsymbol{K}_{\mathrm{P}}\boldsymbol{F}^{\mathrm{G}} - \boldsymbol{K}_{\mathrm{D}}(\boldsymbol{D}+\boldsymbol{D}^{\mathrm{a}})] \tag{18}$$

$$\boldsymbol{F}^{\mathrm{G}} \in \arg\ \min\ \boldsymbol{C}^{\mathrm{G}}\boldsymbol{F}^{\mathrm{G}} \tag{19}$$

$$\mathbf{1}^{\mathrm{T}}\boldsymbol{F}^{\mathrm{G}} = \mathbf{1}^{\mathrm{T}}(\boldsymbol{D}+\boldsymbol{D})^{\mathrm{a}} \tag{20}$$

$$\boldsymbol{F}^{\mathrm{G,min}} \leqslant \boldsymbol{F}^{\mathrm{G}} \leqslant \boldsymbol{F}^{\mathrm{G,max}} \tag{21}$$

式中：$F_k^{\mathrm{l.a}}$为MAD攻击后的输电网第k条线路潮流；$\boldsymbol{D}$为变电站的负荷向量；$\boldsymbol{F}^{\mathrm{l.a}}$为MAD攻击后的输电网线路潮流向量；$\boldsymbol{S}_{\mathrm{F}}$为线路潮流转移因子矩阵；$\boldsymbol{K}_{\mathrm{P}}$为变电站-发电机组连接矩阵；$\boldsymbol{F}^{\mathrm{G}}$为经济调度场景下发电机组出力向量；$\boldsymbol{C}^{\mathrm{G}}$为发电机组成本向量；$\boldsymbol{F}^{\mathrm{G,min}}$为发电机组出力最小值向量；$\boldsymbol{F}^{\mathrm{G,max}}$为发电机组出力最大值向量；$\boldsymbol{K}_{\mathrm{D}}$为变电站-负荷的连接矩阵。式(1)—式(15)确保了各变电站的所形成异常负荷规模量化的合理性，即所形成的异常负荷应满足攻击资源；(16)用于描述黑客的攻击意图；(17)确保了整体负荷波动不会触动低频减载、高频切机等装置动作；(18)计算了被攻击后的线路潮流；(19)反映了电力系统当前的运行方式。

3.2　“肉鸡”操控策略

MAD攻击策略其次需确定10 kV线路中“肉鸡”的操控状态。首先，根据3.1节所述的变电站异常负荷形成策略，得到各变电站需产生的异常负荷，作为该阶段攻击策略的输入。其次，为合理优化有效的MAD攻击策略，该阶段的MAD攻击应以攻击代价最小为目标，即操控“肉鸡”的数目最小化。此外，为避免“肉鸡”所产生的异常负荷触发10 kV线路过流保护装置动作，从而导致MAD攻击失效，在约束中考虑了10 kV线路传输功率和过流保护装置的动作电流。最后，基于上述的目标函数和约束条件，建立“肉鸡”操控策略，确定受控终端操控状态，最终形成有效的MAD攻击，具体模型为：

$$\min\ N_{i,h}^{\mathrm{a,c}} \tag{22}$$

s.t.

$$N_{i,h}^{\mathrm{a,c}} = \mathbf{1}^{\mathrm{T}}[\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,I}})\boldsymbol{K}_{i,h}^{\mathrm{a,I}}] + \mathbf{1}^{\mathrm{T}}[\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,O}})\boldsymbol{K}_{i,h}^{\mathrm{a,O}}] \tag{23}$$

$$D_{i,h}^{\mathrm{a,c}} = [\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,I}})\boldsymbol{K}_{i,h}^{\mathrm{a,I}}]^{\mathrm{T}}\boldsymbol{D}_{i,h}^{\mathrm{l},+} + [\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,O}})\boldsymbol{K}_{i,h}^{\mathrm{a,O}}]^{\mathrm{T}}\boldsymbol{D}_{i,h}^{\mathrm{O},+} \quad D_{i,h}^{\mathrm{a,c}} \geqslant 0 \tag{24}$$

$$D_{i,h}^{\mathrm{a,c}} = [\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,I}})\boldsymbol{K}_{i,h}^{\mathrm{a,I}}]^{\mathrm{T}}\boldsymbol{D}_{i,h}^{\mathrm{l},-} + [\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,O}})\boldsymbol{K}_{i,h}^{\mathrm{a,O}}]^{\mathrm{T}}\boldsymbol{D}_{i,h}^{\mathrm{O},-} \quad D_{i,h}^{\mathrm{a,c}} < 0 \tag{25}$$

$$\frac{D_{i,h}^{\mathrm{a,c}}}{\sum_{h\in H} D_{i,h}^{\mathrm{a,c}}} = \frac{D_{i,h}^{\mathrm{a,max}}}{\sum_{h\in H} D_{i,h}^{\mathrm{a,max}}} \quad D_{i,h}^{\mathrm{a,c}} \geqslant 0 \tag{26}$$

$$\frac{D_{i,h}^{\mathrm{a,c}}}{\sum_{h\in H} D_{i,h}^{\mathrm{a,c}}} = \frac{D_{i,h}^{\mathrm{a,min}}}{\sum_{h\in H} D_{i,h}^{\mathrm{a,min}}} \quad D_{i,h}^{\mathrm{a,c}} < 0 \tag{27}$$

$$D_i^{\mathrm{a}} = \sum_{h\in H} D_{i,h}^{\mathrm{a}} \tag{28}$$

式中：$N_{i,h}^{\mathrm{a,c}}$为变电站i的10 kV线路h中操控“肉鸡”的数目；$\boldsymbol{K}_{i,h}^{\mathrm{a,c,I}}$为10 kV线路$h$中待机“肉鸡”的操控的0-1矩阵，其中，矩阵元素的值为1表示在该MAD

攻击中待机“肉鸡”被操控，值为0表示该“肉鸡”不被操控；$\boldsymbol{K}_{i,h}^{\mathrm{a,c,O}}$为设备运行终端的操控的0-1矩阵；$D_{i,h}^{\mathrm{a,c}}$为10 kV线路$h$中由MAD攻击产生的异常负荷。式(22)用于描述黑客操控的终端数目最少。在避免各10 kV线路发生负荷明显异常以及触发线路过流保护装置动作的前提下，式(23)—式(28)确保各10 kV线路中所形成的异常负荷满足变电站异常负荷形成策略的要求。

3.3 仿真流程

本文所提针对电力系统低代价的MAD攻击策略仿真流程图如附录A图A3所示，具体步骤如下：

步骤1：初始化。设定模型的基本参数，建立大规模配电网用户侧物联设备接入场景下的电力系统潮流计算模型。

步骤2：确定异常负荷规模约束。根据“肉鸡”动态响应特性以及状态特征，计算线路h中异常负荷的潜在最大值$D_{i,h}^{\mathrm{a,max,1}}$和异常负荷的最小值$D_{i,h}^{\mathrm{a,min}}$；根据10 kV线路过流保护装置动作特征，计算10 kV线路h中的负荷“同投”攻击功率阈值$D_{i,h}^{\mathrm{a,max,2}}$；最后，根据式(12)—式(15)，得到变电站的异常负荷规模约束。

步骤3：设定攻击对象。将高负载传输线路设定为攻击对象。

步骤4：计算变电站异常负荷并衡量攻击效果。考虑攻击资源限制以及步骤2中异常负荷规模约束，根据3.1节所述的变电站异常负荷形成策略计算变电站异常负荷$\boldsymbol{D}^{\mathrm{a}}$，并引入线路故障概率$P_k^{\mathrm{l}}$用于评价攻击效果[31-32]。其中，$P_k^{\mathrm{l}}$的计算公式为：

$$P_k^{\mathrm{l}}=\begin{cases}0 & F_k^{\mathrm{l,a}}<F_k^{\mathrm{l,r}}\\ \dfrac{F_k^{\mathrm{l,a}}-F_k^{\mathrm{l,r}}}{F_k^{\mathrm{l,max}}-F_k^{\mathrm{l,r}}} & F_k^{\mathrm{l,r}}\leqslant F_k^{\mathrm{l,a}}\leqslant F_k^{\mathrm{l,max}}\\ 1 & F_k^{\mathrm{l,a}}>F_k^{\mathrm{l,max}}\end{cases}\tag{29}$$

式中：$F_k^{\mathrm{l,r}}$为传输线路k的容量；$F_k^{\mathrm{l,max}}$为传输线路k的极限容量，$F_k^{\mathrm{l,max}}=1.4F_k^{\mathrm{l,r}}$。

步骤5：确定终端操控状态。基于步骤4中的$\boldsymbol{D}^{\mathrm{a}}$，根据3.2节所述终端“肉鸡”操控策略求解变电站10 kV线路h中待机“肉鸡”的操控状态向量$\boldsymbol{K}_{i,h}^{\mathrm{a,c,I}}$和运行“肉鸡”的操控状态向量$\boldsymbol{K}_{i,h}^{\mathrm{a,c,O}}$。

4 仿真算例

为了验证本文所提低代价MAD攻击策略的有效性，以多个IEEE节点系统为例进行仿真分析。仿真算例的测试环境为MATLAB R2018b，CPU的型号为Intel Core i7-8750H，主频为2.3 GHz，内存容量为16 GB。

4.1 仿真参数

假设IEEE 14节点系统中传输线路1的容量为160 MW，其余传输线路的容量为60 MW。各变电站负荷、10 kV线路的情况如附录B表B1所示。其中，10 kV线路的容量为8 MW，且负荷为均匀分布。

由文献[26]可知，10 kV线路接入的空调数量为6 000台，由此推算各终端数量如表2所示。其中，场景1中空调的渗透率设置为60%、电热水器的渗透率设置为42%、洗衣机的渗透率设置为17%[32]；场景2中各智能终端的渗透率均设置为80%。FAC、IAC的室外温度设置为40 ℃，设定温度为26 ℃。电热水器的室外水温设置为30 ℃，设定温度为45 ℃。洗衣机的运行数据取自目前销售市场中主流洗衣机的典型值。在攻击场景1中，基于附录B表B2所述的终端异常行为，“同投”和“同退”攻击功率的情况如表2所示。

表2 典型终端运行数据

Table 2 Operation data of typical terminals

终端	场景1数量/台	场景2数量/台	攻击功率/kW			同时系数
			待机“同投”	运行“同投”	运行“同退”	
FAC	1 512	2 016	2.5	0.68	0.94	0.50
IAC	2 088	2 784	2.5	2.50	0.40	0.50
电热水器	252	480	4.5	1.42	0.59	0.20
洗衣机	255	1 200	0.8	0	0.80	0.25

由表2可知，对于待机“同投”攻击，待机“肉鸡”可产生的异常负荷与最大运行功率相同。然而，运行“肉鸡”可产生的异常负荷与最大运行功率并不完全相同。在室外温度为40℃的场景下，FAC的运行功率为0.94 kW，为最大运行功率的37.6%；运行FAC可生成的异常负荷为0.68 kW，为最大运行功率的26.8%。在室外水温为30℃的场景下，电热水器的运行功率为0.59 kW，为最大运行功率的13.1%；运行电热水器可产生的异常负荷为1.42 kW。针对运行“同退”攻击，FAC、IAC、电热水器的攻击功率分别为0.94、0.40、0.59 kW。综上，考虑“肉鸡”响应模型以及运行状态的动态异常负荷量化方法可以更为准确地量化“肉鸡”可产生的异常负荷。

4.2 场景1中的需求操控攻击策略

4.2.1 计算变电站异常负荷规模

考虑负荷特征和电力设备运行特征，各变电站的负荷“同投”和“同退”攻击功率最大值如图3所示。

在不考虑10 kV线路过流保护装置的前提下，

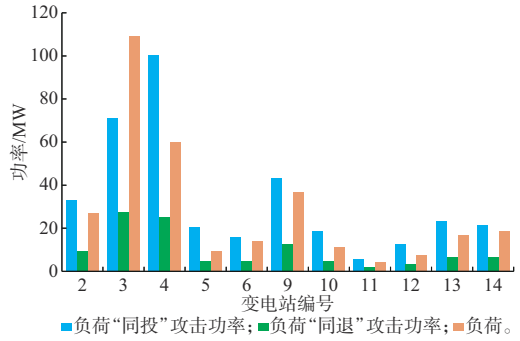


图3　变电站潜在的异常负荷
Fig. 3　Potential abnormal loads of substations

变电站3的负荷“同投”攻击功率最大值应为139.75 MW。由图3可知，在考虑10 kV线路的过流保护装置的前提下，变电站3的负荷“同投”攻击功率降至70.93 MW。原因为“同投”攻击功率可能致使过流保护装置动作，线路发生停电事故。以变电站3中的10 kV线路11为例，其负荷为6.95 MW。当黑客对所有可操控终端发送提升运行功率的控制指令时，线路负荷将升至15.51 MW，运行电流为895.47 A，远高于动作电流(577 A)，过流保护装置动作，切除负荷6.95 MW，预计10 kV线路11的负荷由15.51 MW降至−6.95 MW。对于变电站2(负荷“同投”攻击功率最大值详见附录B表B3)，其“同投”攻击功率最大值由48.68 MW降至32.87 MW。对于10 kV线路6，当负荷“同投”攻击功率的最大值为7.66 MW时，线路运行电流升至727.34 A，高于动作电流，攻击失败。综上，在考虑负荷特征和电力设备运行特征等因素的前提下，本文所提策略可以准确地反应目前系统异常负荷规模，避免错误估计MAD攻击所带来的安全影响。

4.2.2　计算变电站异常负荷

本文所提MAD攻击策略给传输线路带来的安全影响详见附录B表B4。由表B4可知，随着攻击资源的不断增加，本文所提MAD攻击策略会扩大异常负荷对传输线路的安全影响，最多可以给6条传输线路带来过载风险、2条传输线路带来故障风险。

本节以传输线路3为攻击目标的MAD攻击作为典型，阐述黑客如何利用配电网用户侧物联设备实现所提低代价MAD攻击策略。在此背景下，各传输线路的线路潮流如表3所示。其中，$F_l^{\mathrm{a},1}$为R=4时的线路潮流，$F_l^{\mathrm{a},2}$为R=11时的线路潮流。

在R=4时，黑客对变电站2、4、9进行负荷“同退”攻击，负荷“同退”攻击功率分别为6.72、17.69、8.83 MW；对变电站3实施负荷“同投”攻击，负荷

表3　场景1中的传输线路潮流
Table 3　Power flow of transmission lines in scenario 1

传输线路编号	潮流/MW		
	F_l	$F_l^{\mathrm{a},1}$	$F_l^{\mathrm{a},2}$
1	123.25	148.40	149.65
2	60.00	65.83	65.11
3	60.00	90.74	93.74
4	48.86	50.38	50.68
5	35.02	34.63	32.59
6	−19.07	−53.09	−56.26
7	−60.00	−67.95	−77.61
8	16.57	12.21	5.92
9	13.46	10.96	7.35
10	25.52	23.56	13.89
11	12.08	10.90	11.36
12	10.04	9.87	7.59
13	23.45	22.84	18.38
14	−20.00	−20.00	−20.00
15	36.57	32.21	25.92
16	3.54	4.72	−0.22
17	9.62	10.41	5.45
18	−7.70	−6.53	−8.23
19	2.42	2.25	2.27
20	8.99	8.22	8.44

“同投”攻击功率为64.75 MW。由表3可知，在此攻击场景下，传输线路3的潮流发生严重越限，其潮流由60.00 MW升至90.74 MW，故障概率为1。同时，传输线路7的潮流由60.00 MW升至67.95 MW，传输线路2的潮流由60.00 MW升至66.37 MW，故障概率分别为33.12%和26.54%，增加了电力系统的运行风险。

在R=11时，传输线路3的潮流升至93.74 MW；传输线路7的潮流升至77.61 MW，为最大传输功率的1.29倍；传输线路2的潮流为65.11 MW。根据式(29)可得，在R=11时，传输线路2、3、7的故障概率从0%分别增至21.29%、100.00%、73.37%，对电力系统的安全运行造成了极大威胁。可见，黑客可以通过改变“肉鸡”运行功率对电力系统造成一定规模的扰动，严重影响电力系统的运行安全。同时，对于目标传输线路，黑客仅需要掌握关键变电站的攻击资源，即可影响其线路潮流，威胁电力系统的运行安全。

4.2.3　确定“肉鸡”操控状态

本节以变电站3中的“肉鸡”操控状态为例，进一步阐述所提的MAD攻击策略。在R=4时，各10 kV线路运行状态如附录B表B5所示，攻击后各

10 kV线路的传输功率如图B1所示。由表B5可知，各10 kV线路中的平均操控数量为1 263台；攻击后的最大传输功率为9.74 MW，发生在线路11中，低于保护装置动作阈值10 MW；最小的线路传输功率为9.60 MW，发生在线路8中。在线路8中，黑客利用171台电热水器、1 393台智能空调造成数值为4.37 MW的异常“同投”负荷，致使线路传输功率由5.22 MW升至9.60 MW。在线路11中，黑客利用191台智能电热水器和741台智能空调造成线路传输功率升至9.74 MW。

由附录B图B1可知，在随机攻击策略（详见附录C）的影响下，6条10 kV线路触发过流保护装置动作，变电站3的负荷“同投”攻击功率由64.95 MW降至−1.06 MW，负荷“同投”攻击失败。各10 kV线路中异常“同投”负荷的标准差为1.003，高于本文所提MAD攻击策略的标准差（0.427）。在随机攻击策略中，最大的“同投”负荷为5.29 MW，发生在线路11；线路传输功率升至12.24 MW，触发过流保护装置动作，异常负荷由5.29 MW变为−6.95 MW。最小的“同投”负荷为2.30 MW，发生在线路3，线路传输功率由6.17 MW升至8.47 MW，负荷“同投”攻击成功。因此，在避免各10 kV线路过流保护装置动作的前提下，低代价MAD攻击策略通过高功率“肉鸡”率先响应的原则确保了“肉鸡”操控数量的最小化，实现了低代价MAD攻击。

4.3 场景2中的需求操控攻击策略

随着配电网用户侧物联设备渗透率的不断增加，MAD攻击带来的安全影响也随之扩大。如附录B图B2可知，在场景2中，一旦黑客掌握6个关键变电站的攻击资源，即可使2条传输线路故障、7条传输线路过载。其中，传输线路3和传输线路7存在故障风险。在此背景下，本节分别在攻击资源为5和11的前提下，以传输线路3和传输线路7为攻击目标，阐述所提的低代价MAD攻击策略，部分结果如表B6所示。

由附录B表B6可知，在R=5时，MAD攻击后的传输线路3的潮流为93.99 MW，为最大传输功率的1.566倍，故障概率为100%。原因为传输线路3连接的是变电站2和变电站3，变电站3的负荷“同投”攻击功率为70.93 MW，变电站2的负荷“同退”功率为10.02 MW。可见，选择线路3作为攻击目标的MAD攻击策略具有很好的效果。在R=11时，攻击后的传输线路7的潮流最大，为最大传输功率的1.690倍，故障概率为100%。原因为传输线路7连接变电站4和变电站5，变电站4和变电站5关联的传输线路有8条（线路2、线路4至线路10），且靠近电力系统的负荷中心（变电站3和变电站4）。故选择线路7作为攻击目标的MAD攻击策略同样具有较好的效果。可见，本文所提MAD攻击策略可以准确反映不同攻击资源在电力系统面临MAD攻击时传输线路的脆弱性，为电力系统进行主动防御提供了有效的参考。

4.4 安全影响延展性分析

本节进一步验证所提低代价MAD攻击策略的有效性，分别以IEEE 39节点、48节点、72节点、118节点系统为例进行仿真分析，IEEE标准系统数据（网络拓扑参数、发电机与负荷数据）均来自Matpower 6.0，配电网用户侧物联设备接入数量和渗透率与3.3.2节中的场景2相同，各10 kV线路的控制系数均设置为1。不同场景下故障线路和过载线路数量如图4所示，其中，IEEE 39节点系统中的R为2，IEEE 48节点系统中的R为4，IEEE 72节点系统中的R为7，IEEE 118节点系统中的R为10。

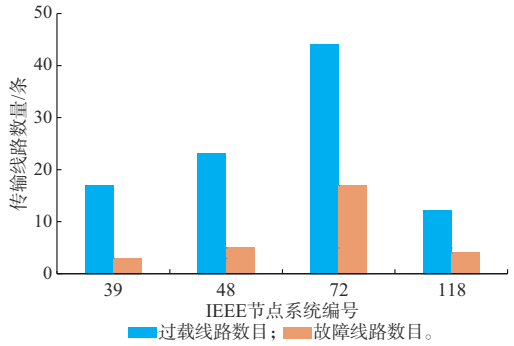


图4 MAD攻击对各系统的安全影响
Fig. 4 Security impacts of MAD attacks on various systems

根据图4可知，在不同的IEEE节点系统中，所提低代价MAD攻击策略均有良好的效果。当R=2时，IEEE 39节点系统中有21条传输线路存在过载运行的风险，3条传输线路存在故障风险，占比分别为45.65%和6.52%；当R=4时，IEEE 48节点系统中有23条传输线路存在过载运行的风险，4条传输线路存在故障的风险；当R=7时，IEEE 72节点系统中有44条传输线路存在过载运行风险，17条传输线路存在故障的风险；当R=10时，IEEE 118节点系统有12条传输线路存在过载运行的风险，4条传输线路存在故障的风险。上述数据表明在配电网用户侧物联设备高渗透率的场景中，在掌握关键攻击资源的前提下，MAD攻击可以给电力系统运行带来严重的安全隐患。

4.5 现阶段安全防护分析

根据上述仿真结果，所提MAD攻击策略可以

给电力系统运行安全带来极大影响。由第1章可知，MAD攻击主要分为构建“肉鸡”网络和产生异常负荷2个关键阶段，需要分别阐述在这2个阶段电网公司的安全防护现状，并分析电网公司现阶段如何针对MAD攻击构建安全防护策略。在黑客构建“肉鸡”网络的过程中，由于电力二次系统安全防护体系并未覆盖配电网用户侧物联设备，导致电网公司无法实时监测设备终端，不利于电网公司黑客入侵终端过程中识别潜在“肉鸡”；在异常负荷的产生过程中，由于设备的异构性，电网公司亦无法操控异常设备终端，致使异常负荷持续产生。可见，目前电网公司缺乏针对MAD攻击的主动防御手段。但由于电网公司配备了发电机组出力、负荷控制等措施，以维持电力系统受扰后稳定运行和不发生大面积停电，这些措施同样能够缓解因MAD攻击造成线路潮流严重越限。在此背景下，考虑发电机、负荷、储能装置的调控能力，构建安全防护策略（详见附录C），针对场景2中$R=5$的MAD攻击，在线路潮流的具体效用见附录B表B7。

由附录B表B7可知，所提安全防护策略可以有效缓解MAD攻击对线路潮流的恶性影响。受到MAD攻击后，安全从业人员向变电站2和变电站3所关联的储能装置发送控制指令，分别执行17.63 MW的放电指令和30.00 MW的充电指令；向变电站3发送数值为33.55 MW的切负荷指令；向发电机1发送出力减少9.11 MW的控制指令。在此背景下，传输线路3的潮流从93.99 MW降至60.00MW，故障概率为0；传输线路2和传输线路7的故障概率分别从25.25%和56.37%降至0。线路潮流下降至安全区间，但由于电力安全从业人员对发电机、储能装置、负荷进行了紧急控制，电力系统运行成本由61 807.32元/h升至102 087.37元/h，上升了40 280.05元/h，上升比例为65.17%。主动防御和所提安全防护策略的差异性如表4所示。

1）由于配电网用户侧物联设备的异构性，现有的安全防护体系并不能识别、调控异常设备终端，更无法避免异常负荷的产生和检测该类型负荷，不利于预防MAD攻击。

2）基于发电机、负荷、储能装置控制的MAD攻击安全防护策略要求负荷、发电机组具备足够的调控能力，否则可能无法进行有效的安全防御。

3）所产生异常负荷致使电力系统运行成本的迅速上升，可衍生针对系统运行成本的MAD攻击形式。

由表4可知，在调控能力充足的前提下，电网公司在MAD攻击发生后，可通过发电机、负荷、储能装置的调控能力缓解MAD攻击给电力系统带来的恶性影响。但由于在信息域中无法实时监控配电网用户侧物联设备，电力系统无法避免异常负荷的产生，攻击者可在社会域、物理域中衍生出不同攻击目的的MAD攻击形式，不利于实现针对MAD攻击的主动防御。附录C为分别对配电网用户侧物联设备厂商和电网公司针对MAD攻击的防护对策，以期实现逐步实现针对MAD攻击的主动防御。

表4　主动防御和所提安全防护策略的差异性
Table 4　Differences between active defense and proposed security defense strategies

项目	影响电力系统前		影响电力系统后	
	设备入侵是否可识别	“肉鸡”是否可复原	运行成本控制	是否满足线路潮流安全
主动防御模型	是	是	波动小	是
所提安全防护策略	否	否	波动大	是（有足够的调节能力）

5　结语

随着越来越多的配电网用户侧物联设备接入电力系统，本文分析了不触发低频减载、高频切机等装置因MAD攻击产生的安全影响。首先，基于负荷特征和电力设备运行特征等因素得到异常负荷约束。然后，以黑客低代价攻击成本造成目标线路潮流过载水平最大为思路，建立低代价MAD攻击策略；仿真结果表明，本文所提MAD攻击策略可以引起传输线路潮流越限的情况发生，严重影响电力系统的安全运行。最后，本文分析了现阶段电网公司如何避免该类MAD攻击带来的恶性影响，对配电网用户侧物联设备厂商和电网公司提出了针对MAD攻击的防护对策，。

目前，相关研究尚处在初级阶段，只基于攻击者视角考虑负荷特征和电力设备运行特征等因素作用下的MAD攻击对电力系统传输线路造成的安全影响。电力系统如何识别系统遭受MAD攻击并及时做出相应的主动防御策略等问题还有待完善，需要进一步研究对MAD攻击的主动防御模型。

附录见本刊网络版（http://www.aeps-info.com/aeps/ch/index.aspx），扫英文摘要后二维码可以阅读网络全文。

参考文献

[1] 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 Yi, CHEN Qian, LI Mengya, et al. Overview on cyber-attacks against cyber physical power system[J]. Automation of

Electric Power Systems, 2016, 40(17): 59-69.
[2] 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,2016,40(5):145-147.
GUO Qinglai, XIN Shujun, WANG Jianhui, et al. Comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine's blackout [J]. Automation of Electric Power Systems, 2016, 40(5): 145-147.
[3] 安天研究院,广东省电力系统网络安全企业重点实验室.委内瑞拉大规模停电事件的初步分析与思考启示[J].信息安全与通信保密,2019,17(5):28-39.
ANTIY Institute, CSGITSEC. Preliminary analysis and reflections on Venezuela's power outage [J]. Information Security and Communications Privacy, 2019, 17(5): 28-39.
[4] WU Y D, WEI Z, WENG J, et al. Resonance attacks on load frequency control of smart grids [J]. IEEE Transactions on Smart Grid, 9(5): 4490-4502.
[5] TAN R, NGUYEN H H, FOO E Y S, et al. Modeling and mitigating impact of false data injection attacks on automatic generation control [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(7): 1609-1624.
[6] YUAN Y L, LI Z Y, REN K. Modeling load redistribution attacks in power systems [J]. IEEE Transactions on Smart Grid, 2011, 2(2): 382-390.
[7] 阮振,吕林,刘友波,等.考虑负荷数据虚假注入的电力信息物理系统协同攻击模型[J].电力自动化设备,2019,39(2):181-187.
RUAN Zhen, LÜ Lin, LIU Youbo, et al. Coordinated attack model of cyber-physical power system considering false load data injection [J]. Electric Power Automation Equipment, 2019, 39(2): 181-187.
[8] 严康,陆艺丹,于宗超,等.配电网用户侧异构电力物联设备安全研究综述及展望[J].电力自动化设备,2023,43(3):146-158.
YAN Kang, LU Yidan, YU Zongchao, et al. Review and prospect of research on security of user-side heterogeneous power IoT devices in distribution network [J]. Electric Power Automation Equipment, 2023, 43(3): 146-158.
[9] SOLTAN S, MITTAL P, and POOR H V. P. BlackIoT: IoT botnet of high wattage devices can disrupt the power grid [EB/OL]. [2024-01-16]. https://www. usenix. org/conference/usenixsecurity18/presentation/soltan.
[10] 吴亦贝,李俊娥,陈洵,等.大规模可控负荷被恶意控制场景下配电网风险分析[J].电力系统自动化,2018,42(10):30-37.
WU Yibei, LI Jun'e, CHEN Xiong, et al. Risk analysis of distribution network with large-scale controllable loads with attacks [J]. Automation of Electric Power Systems, 2018, 42(10): 30-37.
[11] DVORKIN Y, GARG S. IoT-enabled distributed cyber-attacks on transmission and distribution grids[C]// 2017 North American Power Symposium (NAPS), September 17-19, 2017, Morgantown, USA.
[12] AMINI S, PASQUALETTI F, MOHSENIAN-RAD H. Dynamic load altering attacks against power system stability: attack models and protection schemes [J]. IEEE Transactions on Smart Grid, 9(4): 2862-2872.
[13] DABROWSKI A, ULLRICH J, WEIPPL E R. Grid shock: coordinated load-changing attacks on power grids: the non-smart power grid is vulnerable to cyber attacks as well [C]// Proceedings of the 33rd Annual Computer Security Applications Conference, December 4-8, 2017, Orlando, USA.
[14] 张子扬,张宁,杜尔顺,等.双高电力系统频率安全问题评述及其应对措施[J].中国电机工程学报,2022,42(1):1-25.
ZHANG Ziyang, ZHANG Ning, DU Ershun, et al. Review and countermeasures on frequency security issues of power systems with high shares of renewables and power electronics [J]. Proceedings of the CSEE, 2022, 42(1): 1-25.
[15] MALIK N S, COLLINS R. The cyberattack that crippled gas 803 pipelines is now hitting another industry [EB/OL]. [2024-01-16]. https://www.bloomberg.com/news/articles/2018-04-80504/cyberattack-bleedsinto-utility-space-as-duke-sees-billing-delay.
[16] 严康,陆艺丹,覃芳璐,等.配电网用户侧异构电力物联设备网络风险量化评估[J].电力系统保护与控制,2023,51(11):64-76.
YAN Kang, LU Yidan, QIN Fanglu, et al. Network security risk assessment of UPIDs in the distribution system [J]. Power System Protection and Control, 2023, 51(11): 64-76.
[17] 伍志韬,杜伟,刘蕾蕾,等.恶意攻击下的电力耦合网络风险传播模型研究[J].电网技术,2020,44(6):2045-2052.
WU Zhitao, DU Wei, LIU Leilei, et al. Risk propagation model of power coupled networks under malicious attack [J]. Power System Technology, 2020, 44(6): 2045-2052.
[18] GeoIP products of MaxMind [EB/OL]. [2024-01-16]. http://dev.maxmind.com/geoip.
[19] Wiggle: wireless network mapping [EB/OL]. [2024-01-16]. https://wigle.net.
[20] CHE L, LIU X, LI Z Y. Screening hidden $N-k$ line contingencies in smart grids using a multi-stage model [J]. IEEE Transactions on Smart Grid, 10(2): 1280-1289.
[21] SHEKARI T, CÁRDENAS A, BEYAH R. MaDIoT 2.0: modern high-wattage IoT botnet attacks and defenses [C]// Proceedings of the 31st USENIX Security Symposium, August 10-12, 2022, Boston, USA:3539-3556.
[22] HUANG B, CARDENAS A A, BALDICK R, et al. Not everything is dark and gloomy [C]// Proceedings of the 28th USENIX Conference on Security Symposium, August 14-16, 2019, Santa Clara, USA: 1115-1132.
[23] Cloud giants likely to beef up bandwidth to fight IoT botnets [EB/OL]. [2024-01-16]. http://www. iotworldtoday. com/2016/11/01/cloud-giants-likely-beef-bandwidth-fight-iotbotnets.
[24] ADEPU S, KANDASAMY N K, MATHUR A. EPIC: an electric power testbed for research and training in cyber physical systems security [EB/OL]. [2024-01-16]. https://link.springer.com/chapter/10.1007/978-3-030-12786-2_3.
[25] 国家能源局.电力二次系统安全管理若干规定[EB/OL]. [2024-01-16]. http://zfxxgk. nea. gov. cn/2022-10/17/c_1310677191.htm.
National Energy Administration. Several provisions on the safety management of electric power secondary system [EB/OL]. [2024-01-16]. http://zfxxgk.nea.gov.cn/2022-10/17/c_

1310677191.htm.

[26] 武昕，梁凯鑫，焦点，等．面向清洁能源跟踪的空调分组协同方法[J]．电力系统自动化，2020，44(11)：68-77.
WU Xin，LIANG Kaixin，JIAO Dian，et al. Collaborative method of air conditioner grouping for clean energy tracking[J]. Automation of Electric Power Systems，2020，44(11)：68-77.

[27] 李滨，黎智能，陈碧云．电力市场中配电网的空调群调控策略[J]．电力系统自动化，2019，43(15)：124-131.
LI Bin，LI Zhineng，CHEN Biyun. Air conditioning group dispatch control strategy of distribution network in electricity market[J]. Automation of Electric Power Systems，2019，43(15)：124-131.

[28] 郝文斌，李银奇，张毓格，等．基于需求侧响应的家庭电热水器优化调度[J]．电力系统保护与控制，2019，47(2)：95-100.
HAO Wenbin，LI Yinqi，ZHANG Yuge，et al. Household electric water heater load scheduling based on demand response [J]. Power System Protection and Control，2019，47(2)：95-100.

[29] CARRERAS B A，LYNCH V E，DOBSON I，et al. Critical points and transitions in an electric power transmission model for cascading failure blackouts[J]. Chaos，2002，12(4)：985-994.

[30] 蒲天骄，刘克文，陈乃仕，等．基于主动配电网的城市能源互联网体系架构及其关键技术[J]．中国电机工程学报，2015，35(14)：3511-3521.
PU Tianjiao，LIU Kewen，CHEN Naishi，et al. Design of ADN based urban energy Internet architecture and its technological issues[J]. Proceedings of the CSEE，2015，35(14)：3511-3521.

[31] 蔡晔，刘放，曹一家，等．电力信息物理系统低代价多阶段高危攻击策略研究[J]．电力系统自动化，2021，45(20)：1-8.
CAI Ye，LIU Fang，CAO Yijia，et al. Research on low-cost multi-stage high-risk attack strategy for power cyber-physical system[J]. Automation of Electric Power Systems，2021，45(20)：1-8.

[32] 2023年智能家电发展趋势预测：政策刺激行业消费，市场规模不断增[EB/OL]．[2024-01-16]．https://baijiahao.baidu.com/s?id=1774451393313987498&wfr=spider&for=pc.
Trend forecast of smart home appliances in 2023：policies to stimulate industry consumption，increasing market size[EB/OL]．[2024-01-16]．https://baijiahao. baidu. com/s? id=1774451393313987498&wfr=spider&for=pc.

严　康(1993—)，男，通信作者，博士，主要研究方向：电力系统信息物理安全。E-mail：yankang124@163.com

陆艺丹(1993—)，女，博士，主要研究方向：新型电力系统规划与运行。E-mail：lyd112@hnu.edu.cn

白晓清(1969—)，女，教授，博士生导师，主要研究方向：电力系统最优化等。E-mail：baixq@gxu.edu.cn

（编辑　杨松迎）

Demand Manipulation Attack Strategy and Analysis of Its Defence for Cyber-Physical Power System

YAN Kang[1,3]，*LU Yidan*[2,3]，*BAI Xiaoqing*[4]，*LI Bin*[4]

(1. Department of Electrical Engineering Tsinghua University，Beijing 100084，China；
2. Electric Power Research Institute of Guangxi Power Grid Company Limited，Nanning 530023，China；
3. College of Electrical and Information Engineering，Hunan University，Changsha 410082，China；
4. Guangxi Key Laboratory of Power System Optimization and Energy Technology (Guangxi University)，Nanning 530004，China)

Abstract: With large-scale distribution network user-side heterogeneous power Internet of Things devices (referred to as distribution network user-side IoT devices，UPIDs) integrating into power systems，the dominance of load control service for users on the Internet is becoming increasingly obvious. Thus，there is a cross cyber-physical domain attack path in power systems，manipulation of demand (MAD) attacks，which causes the power system to face a new type of cybersecurity threat. In this background，the research on MAD attack strategy has important guiding significance for power systems to resist such type of cyber attack. Firstly，this paper describes how hackers use distribution network UPIDs to carry out MAD attacks and their characteristics，and further gives constraints of abnormal loads in the power system based on the operation characteristics of loads and power equipment. Then，the MAD attack strategy to induce transmission line fault under the low-cost condition is proposed，pointing out the vulnerability of transmission lines in power systems under this type of MAD attack scenario. Finally，multiple IEEE node system simulations under multiple scenarios verify that MAD attacks can affect power system operation security at a low cost.

This work is supported by State-funded Postdoctoral Researcher Program (No. GZC20240788) and National Natural Science Foundation of China (No. 51967001).

Key words: distribution system；cyber-physical system；heterogeneous device；controlled load；user-side；Internet of Things

附录 A

1)电力系统网络攻击示意图

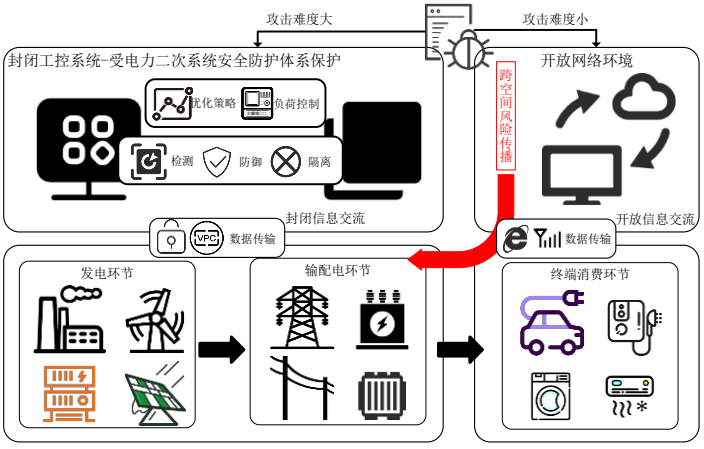


图 A1　电力系统网络攻击示意图
Fig. A1　Schematic diagram of cyberattacks for power systems

2)典型配电网用户侧物联设备

表 A1　典型配电网用户侧物联设备
Table A1　Typical UPIDs

设备	2024 年上半年全渠道数据	功率(kW)
空调	空调市场销售量达到了 3315 万台；	2.5kW/台
电热水器	电储水热水器销售量达到了 826 万台；	4.5kW/台
电动汽车	新能源汽车销售量达到了 494.4 万台；	7kW/辆
洗衣机	洗衣机销售量达到了 1909 万台。	0.8kW/台

3)配电网结构示意图

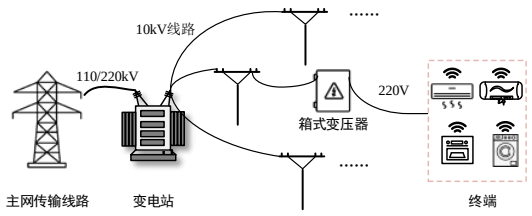
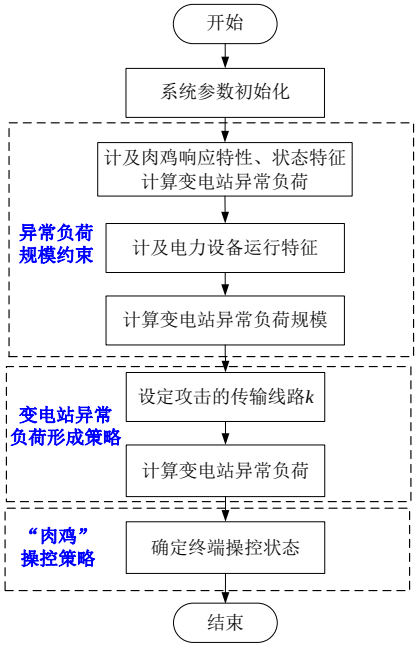


图 A2　配电网结构示意图
Fig. A2　Schematic diagram of distribution systems

4）低代价MAD攻击策略仿真流程图



图A3　低代价MAD攻击策略仿真流程图
Fig. A3　Schematic diagram of low-cost MAD attacks

附录B

1)仿真系统参数

表B1 系统参数
Table B1 System parameters

变电站编号	负荷/MW	10kV线路数目/条	变电站编号	负荷/MW	10kV线路数目/条
1	-	-	8	-	-
2	27.13	6	9	36.87	8
3	109.07	18	10	11.25	3
4	59.75-	16	11	4.37	1
5	9.5	3	12	7.63	2
6	14	3	13	16.87	4
7	-	-	14	18.62	4

2)终端上黑客恶意行为

表B2 黑恶在终端上的恶意行为
Table B2 Malicious behaviors on UPIDs

终端	恶意行为	
	“同投”攻击	“同退”攻击
空调	开启待机空调;降低运行空调设定温度为16℃;	关闭运行空调;
电热水器	开启待机电热水器;提高运行电热水器设定温度为75℃;	关闭运行电热水器;
洗衣机	开启待机洗衣机。	关闭运行洗衣机。

3)“同投”攻击功率

表B3 变电站2中10kV线路负荷“同投”攻击功率
Table B3 Simultaneously increasing attack power of 10 kV lines in Sub 2

线路	1	2	3
运行功率(MW)	4.32	4.47	4.11
同投功率(MW)	5.68	5.53	5.89
线路	4	5	6
运行功率(MW)	4.72	4.57	4.93
同投功率(MW)	5.28	5.43	5.07

4)所提MAD攻击策略的安全影响

5)变电站3中10kV线路运行状态

6)变电站3中10kV线路传输功率

7)过载和故障线路数目对比

8)场景2中部分线路潮流

表中,$F_l^{a,3}$是目标为传输线路3的MAD攻击影响下线路潮流,$F_l^{a,4}$是目标为传输线路7的MAD攻击影响下线路潮流,单位为MW。

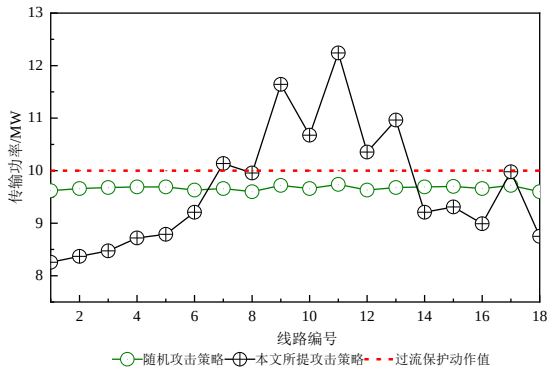
9)场景2中部分线路潮流

表B4　所提MAD攻击策略的安全影响
Table B4　Security impacts of proposed MAD attack strategy

R	仅考虑负荷“同投”影响的MAD攻击策略		本文所提MAD攻击策略	
	过载数目	故障数目	过载数目	故障数目
1	3	0	3	0
2	3	0	4	0
3	3	0	4	1
4	3	0	5	2
5	3	0	5	2
6	3	0	6	2
7	3	0	6	2
8	3	0	6	2
9	3	0	6	2
10	3	0	6	2
11	3	0	6	2

表B5　变电站3中10kV线路运行状态
Table B5　Operating status of 10kV lines in Sub 3

线路	$F_{i,h}$	$F_{i,h}^{a}$	数目	线路	$F_{i,h}$	$F_{i,h}^{a}$	数目
1	5.52	4.10	1441	10	5.94	3.72	1308
2	5.92	3.74	1315	11	6.95	2.79	932
3	6.17	3.51	1234	12	5.62	4.01	1421
4	6.27	3.42	1190	13	6.24	3.44	1193
5	6.34	3.35	1165	14	6.31	3.38	1184
6	5.63	4.00	1418	15	6.41	3.29	1148
7	5.96	3.70	1316	16	5.91	3.75	1318
8	5.22	4.38	1564	17	6.72	3.00	1022
9	6.63	3.09	1054	18	5.31	4.29	1514



图B1　变电站3中10kV线路传输功率
Fig. B1　Transmission power of 10kV lines in Sub 3

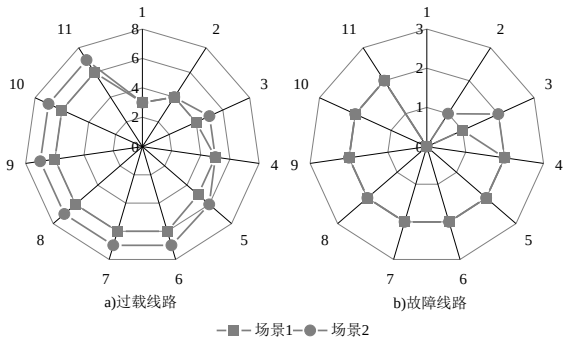


图 B2　过载和故障线路数目对比
Fig. B2　Comparison of overload and fault line quantity

表 B6　场景 2 中部分线路潮流
Table B6　Power flow of part transmission lines in Scenario 2

线路	初始	R=5		R=11	
	F_l	$F_l^{\mathrm{a},3}$	$F_l^{\mathrm{a},4}$	$F_l^{\mathrm{a},3}$	$F_l^{\mathrm{a},4}$
2	60	66.05	73.93	65.22	71.74
3	60	**93.99**	56.05	**94.70**	63.31
4	48.86	51.22	68.49	54.09	66.99
7	-60	-73.53	**－93.08**	-85.27	**－－101.45**

表 B7　安全防护策略效用
Table B7　Effectiveness of proposed security defense strategy

线路	$F_l^{\max}$	$F_l^{\mathrm{a},2}$	F_l^{c}	线路	$F_l^{\max}$	$F_l^{\mathrm{a},2}$	F_l^{c}
1	160	148.70	118.92	11	60	13.61	13.19
2	60	66.06	54.23	12	60	8.94	8.92
3	60	93.99	60.00	13	60	19.59	19.49
4	60	51.22	42.05	14	60	-20.00	-19.00
5	60	34.13	29.09	15	60	34.34	35.45
6	60	-56.00	-26.10	16	60	2.02	3.02
7	60	-73.53	-55.93	17	60	7.64	8.76
8	60	14.34	16.45	18	60	-9.23	-8.23
9	60	12.19	13.20	19	60	1.32	1.29
10	60	22.08	22.80	20	60	10.99	10.86

附录 C

1）MAD 攻击策略

$$\max \left| F_k^{\mathrm{l.a}} \right| \tag{C1}$$

约束条件

$$\mathbf{1}^{\mathrm{T}} \boldsymbol{D}^{\mathrm{a}} \leqslant 0.1(\mathbf{1}^{\mathrm{T}} \boldsymbol{D}) \tag{C2}$$

$$\boldsymbol{F}^{\mathrm{l.a}} = \mathrm{SF}\left[\mathrm{KP} \cdot \boldsymbol{F}^{\mathrm{G}} - \mathrm{KD}(\boldsymbol{D} + \boldsymbol{D}^{\mathrm{a}})\right] \tag{C3}$$

$$0 \leqslant \boldsymbol{D}^{\mathrm{a}} \leqslant \boldsymbol{D}^{\mathrm{a,max}} \tag{C4}$$

$$F^{\mathrm{G}}\in\arg\ \min\ \boldsymbol{C}^{\mathrm{T}}F^{\mathrm{G}} \tag{C5}$$

$$\mathbf{1}^{\mathrm{T}}F^{\mathrm{G}}=\mathbf{1}^{\mathrm{T}}(\boldsymbol{D}+\boldsymbol{D}^{\mathrm{a}}) \tag{C6}$$

$$F^{\mathrm{G,min}}\leqslant F^{\mathrm{G}}\leqslant F^{\mathrm{G,max}} \tag{C7}$$

(1)　-(12)，(14)-(15)

式中：$F^{\mathrm{l.a}}$为攻击后的输电网中线路潮流向量；SF为线路潮流转移因子矩阵；KP为发电机组参数矩阵；F^{G}为经济调度场景下发电机组出力向量；$F^{\mathrm{G,min}}$为发电机组最小出力向量；$F^{\mathrm{G,max}}$为发电机组最大出力向量；KD为负荷的单位参数矩阵；$\boldsymbol{D}$为变电站的负荷向量；$\boldsymbol{D}^{\mathrm{a}}$为变电站异常负荷向量；$\boldsymbol{D}^{\mathrm{a,max}}$为黑客的负荷“同投”攻击功率向量。

2)随机攻击策略

$$\min N_{i,h}^{a,c} \tag{C8}$$

约束条件

$$N_{i,h}^{\mathrm{a,c}}=\mathbf{1}^{\mathrm{T}}[\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,I}})\boldsymbol{K}_{i,h}^{\mathrm{a,I}}]+\mathbf{1}^{\mathrm{T}}[\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,O}})\boldsymbol{K}_{i,h}^{\mathrm{a,O}}] \tag{C9}$$

$$D_{i,h}^{\mathrm{a,c}}=[\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,I}})\boldsymbol{K}_{i,h}^{\mathrm{a,I}}]^{\mathrm{T}}\boldsymbol{D}_{i,h}^{\mathrm{I},+}+[\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,O}})\boldsymbol{K}_{i,h}^{\mathrm{a,O}}]^{\mathrm{T}}\boldsymbol{D}_{i,h}^{\mathrm{O},+}\quad D_{i,h}^{\mathrm{a,c}}>0 \tag{C10}$$

$$D_{i,h}^{\mathrm{a,c}}=[\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,I}})\boldsymbol{K}_{i,h}^{\mathrm{a,I}}]^{\mathrm{T}}\boldsymbol{D}_{i,h}^{\mathrm{I},-}+[\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,O}})\boldsymbol{K}_{i,h}^{\mathrm{a,O}}]^{\mathrm{T}}\boldsymbol{D}_{i,h}^{\mathrm{O},-}\quad D_{i,h}^{\mathrm{a,c}}<0 \tag{C11}$$

$$D_{i}^{\mathrm{a}}=\sum_{h}D_{i,h}^{\mathrm{a}} \tag{C12}$$

式中：$N_{i,h}^{\mathrm{a,c}}$为变电站i的10kV线路h中操控终端数目；$\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,I}})$为10kV线路$h$中待机终端的操控的0-1对角阵，其中，1表示在该MAD攻击中待机终端被操控，0则表示该终端不被操控；$\mathrm{diag}(\boldsymbol{K}_{i,h}^{\mathrm{a,c,O}})$为设备运行终端的操控的0-1对角阵；$D_{i,h}^{\mathrm{a,c}}$为10kV线路$h$中由MAD攻击产生的异常负荷。

3)考虑发电机、负荷、储能装置控制的安全防御策略

$$\min\ \boldsymbol{C}_{\mathrm{G}}{}^{\mathrm{T}}F^{\mathrm{G,c}}+\boldsymbol{C}_{\mathrm{Es}}{}^{\mathrm{T}}|\boldsymbol{D}^{\mathrm{Es}}|+\boldsymbol{C}_{\mathrm{S}}{}^{\mathrm{T}}\boldsymbol{D}^{\mathrm{s}} \tag{C13}$$

约束条件

$$\mathbf{1}^{\mathrm{T}}F^{\mathrm{G,c}}=\mathbf{1}^{\mathrm{T}}(\boldsymbol{D}+\boldsymbol{D}^{\mathrm{a}}+\boldsymbol{D}^{\mathrm{Es}}+\boldsymbol{D}^{\mathrm{s}}) \tag{C14}$$

$$F^{\mathrm{l.c}}=\mathrm{SF}[\mathrm{KP}\cdot F^{\mathrm{G,c}}-\mathrm{KD}(\boldsymbol{D}+\boldsymbol{D}^{\mathrm{a}}+\boldsymbol{D}^{\mathrm{Es}}+\boldsymbol{D}^{\mathrm{s}})] \tag{C15}$$

$$F^{\mathrm{G,c,min}}\leqslant F^{\mathrm{G,c}}\leqslant F^{\mathrm{G,c,max}} \tag{C16}$$

$$F^{\mathrm{l,min}}\leqslant F^{\mathrm{l,c}}\leqslant F^{\mathrm{l,max}} \tag{C17}$$

$$D^{\mathrm{Es,min}}\leqslant D^{\mathrm{Es}}\leqslant D^{\mathrm{Es,max}} \tag{C18}$$

$$0\leqslant D^{\mathrm{s}}\leqslant D^{\mathrm{s,max}} \tag{C19}$$

式中：$\boldsymbol{C}_{\mathrm{G}}$为发电机组成本向量；$\boldsymbol{C}_{\mathrm{Es}}$为储能装置成本向量；$\boldsymbol{C}_{\mathrm{S}}$为切负荷成本向量；$F^{\mathrm{G,c}}$为防御策略后发电机组出力向量；$\boldsymbol{D}^{\mathrm{Es}}$为储能装置充放电向量；$\boldsymbol{D}^{\mathrm{s}}$为切负荷向量.$F^{\mathrm{l,c}}$为防御策略后传输线路潮流向量；$F^{\mathrm{G,c,min}}$为防御策略中的发电机组最小出力向量，计算公式为$F^{\mathrm{G,c,min}}=0.9F^{\mathrm{G,c}}$；$F^{\mathrm{G,c,max}}$为防御策略中的发电机组最大出力向量；$D^{\mathrm{Es,min}}$为储能装置最大充电功率向量；$D^{\mathrm{Es,max}}$为储能装置最大放电功率向量；$D^{\mathrm{s,max}}$为变电站最大切负荷向量。附录C式(C13)确保了在遭遇MAD攻击后电力系统运行成本最低，附录C式(C14)确保了电力系统的供需平衡，附录C式(C16)、(C18)和(C19)分别为发电机控制、储能装置控制、切负荷约束，附录C式(C17)确保了传输线路潮流在遭遇所提的MAD攻击策略后在安全的范围内运行。

3)配电网用户侧物联设备厂商安全防护建议

对于设备厂商而言，提升配电网用户侧物联设备的网络安全防护能力成为了应对MAD攻击的关键。由文献[9]可知，黑客可以通过入侵配电网用户侧物联设备的一个组件即可控制其终端。为了更好地预防配电网用户侧物联设备被恶意操控，移动应用、云和终端等组件的安全防护建议如下：

(1)终端受到存储空间和计算能力的限制，仅使用轻量级加密算法或身份验证机制来防止被恶意攻击。由此，设备厂商应加强对轻量级加密算法和认证机制的研究，并且不同的产品应使用不同的轻量级加密方法和认证机制。同时，根据安全事件[33]可知，终端固件中应具有删除默认账户以及密码的机制，从而避免被恶意软件的爆破攻击。

(2)在移动应用开发的过程中,部分程序员可能会存在过分关注代码的实用型而忽视其安全性的现象。厂商在开发过程中,应规定关键函数、SO文件以及DEX文件等加密、混淆比例,以确保移动应用程序能够抵御网络攻击。并且,根据安全事件[34],厂商应对员工进行安全管控,以免泄露移动应用程序的关键信息,如加密算法和消息格式。

(3)云端作为配电网用户侧物联设备的数据中心,储存着大量的用户隐私信息、使用数据以及控制指令等。为了避免大规模终端数据泄露[35],应在网络边缘处部署数据隔离、入侵检测等安全装置,避免黑客通过SQL攻击、XXS攻击等方式轻易地接触数据库。同时,应加强员工身份验证机制,阻断社会工程学攻击发生的可能性。

随着上述所提安全建议的实施,配电网用户侧物联设备网络安全防护能力的进一步提高,潜在"肉鸡"规模也随之下降,我们以场景1中的IEEE14节点系统为例阐述上述安全防护建议带来的影响,所提攻击策略造成故障线路的数目如附录C表C1所述。

表C1 不同"肉鸡"规模造成故障线路的数目

Table C1 Quantity of faulty lines caused by proposed MAD attack strategy with different scales

R	"肉鸡"规模比				
	100%	80%	60%	40%	20%
1	0	0	0	0	0
2	0	0	0	0	0
3	1	1	0	0	0
4	2	1	0	0	0
5	2	2	1	0	0
6	2	2	1	0	0
7	2	2	1	1	0
8	2	2	2	1	0
9	2	2	2	1	0
10	2	2	2	1	0
11	2	2	2	1	0

由附录C表C1可知,当"肉鸡"规模下降为现有规模的0.2倍时,所提的MAD攻击策略无法造成IEEE 14节点系统中任何线路发生故障,MAD攻击所带来的安全威胁显著下降。可见,设备厂商提高配电网用户侧物联设备的网络安全防护能力对电力系统应对MAD攻击起着至关重要的作用。

11)电网公司安全防护建议效用分析

尽管现阶段电网公司可能可以通过发电机、储能装置控制等手段缓解文中所提MAD攻击所带来的恶性影响,但无法避免异常负荷的产生以及可衍生的恶性影响。在此背景下,电网公司如何建立设备的风险管控体系成为了实现主动防御的关键,本节主要从如何降低配电网用户侧物联设备网络风险以及如何对设备终端进行管控等两个方面阐述。

(1)电网公司应联合销售市场监察部门规范接入配电网用户侧物联设备的安全防护能力,及时评估设备带来的网络安全风险,以此形成对设备风险的闭环管理,从而从源头降低网络风险。

(2)在黑客通过恶意软件、伪造的控制指令等方式获取终端控制权限的过程中,由于各组件部署的安全防护,将会出现大量的异常行为,如信息验证错误等。电网公司可以通过建立与云端的协同管控机制,并以存储在云端的设备异常行为为基础识别"肉鸡",在MAD攻击发生时刻通过云端控制指令恢复"肉鸡"状态,减小异同中的异常负荷,从而缓解MAD攻击带来的安全影响。

(3)针对关键变电站所接入的配电网用户侧物联设备,电网公司可以基于零信任安全机制,利用单包授权等技术,建立基于网络定义边界(Software Defined Perimeter, SDP)[36]的防护方案,加强对配电网用户侧物联设备行为的安全认证,避免黑客操控配电网用户侧物联设备。