引用格式:胡一帆,丁玮,张国敏,等.基于智能电网量测集受控随机化的移动目标防御方法[J].信息对抗技术,2024,3(2):46-53.[HU Yifan, ZHANG Guomin, WANG Xiulei, et al. Moving target defense method based on controlled measurement set randomization in smart grid[J]. Information Countermeasure Technology, 2024, 3(2):46-53.(in Chinese)]

基于智能电网量测集受控随机化的移动目标防御方法

胡一帆[1],丁 玮[2],张国敏[1*],王秀磊[1*],邢长友[1],
许 博[1],丁 科[1],石伟宏[3]

(1. 陆军工程大学指挥控制工程学院,江苏南京 210007; 2. 军事科学院系统工程研究院,北京 100088;
3. 国防科技大学电子科学学院,湖南长沙 410073)

摘 要 信息物理协同攻击利用网络攻击掩盖或者延长物理攻击的影响,对智能电网造成了极大威胁。为阻止协同的虚假数据注入攻击,暴露物理攻击的影响,提出了一种基于量测集受控随机化的移动目标防御方法。首先,形式化描述了量测值的选择需要满足的约束;其次,采用随机的量测集进行状态估计,使得攻击者关于电网的先验知识失效;最后,使用MATPOWER模拟器在IEEE标准系统上进行了大量的仿真,实验结果表明,该方法可以防止50%以上的状态被攻击。

关键词 智能电网;信息物理协同攻击;虚假数据注入;移动目标防御;状态估计

中图分类号 TP 393 **文章编号** 2097-163X(2024)02-0046-08

文献标志码 A **DOI** 10.12399/j.issn.2097-163x.2024.02.005

Moving target defense method based on controlled measurement set randomization in smart grid

HU Yifan[1], DING Wei[2], ZHANG Guomin[1*], WANG Xiulei[1*],
XING Changyou[1], XU Bo[1], DING Ke[1], SHI Weihong[3]

(1. College of Command and Control Engineering, Army Engineering University, Nanjing 210007, China;
2. Systems Engineering Institute, Academy of Military Sciences, Beijing 100088, China;
3. College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China)

Abstract Coordinated cyber-physical attacks (CCPA) utilize network attacks to mask or prolong the impact of physical attacks, which can pose a great threat to smart grid. To prevent the coordinated false data injection(FDI) attacks and expose the impact of physical attacks, a moving target defense(MTD) method based on controlled measurement set randomization was proposed. Firstly, the constraints that need to be met in the selection of measurements were formally described. Secondly, a random set of measurements was adopted for state estimation, which can invalidate the attacker's prior acquired knowledge regarding power grids. Finally, extensive simulations were performed on the standard IEEE systems using the MATPOWER simulator, and results have shown that the proposed approach can prevent more

收稿日期:2023-08-14 **修回日期**:2023-10-29

通信作者:张国敏,E-mail:zhang_gmwn@163.com;王秀磊,E-mail:xiuleiwang1988@126.com

基金项目:江苏省自然科学基金青年基金资助项目(SBK2020043435);陆军工程大学基础前沿科技创新项目(KYZYJKQTZQ23003)

than 50% of the states from being attacked.

Keywords　smart grid；CCPA；FDI；MTD；state estimation

0　引言

智能电网是一种典型的信息物理系统(cyber-physical system，CPS)，可能会遭受信息物理协同攻击(coordinated cyber-physical attack，CCPA)的威胁。例如，2015 年 12 月乌克兰电网攻击：攻击者通过打开断路器断开了一组输电线路(物理攻击)，导致了持续数小时涉及 22.5 万用户的大规模停电，同时采用电话洪泛和 KillDisk 服务器清除(网络攻击)来掩盖系统故障并延长中断时间[1]。CCPA 涉及 2 种攻击形式——物理攻击和网络攻击，物理攻击针对特定的物理基础设施，对电网造成直接破坏；而网络攻击针对从现场设备传输到控制中心的量测值，具有掩盖物理攻击影响的效果。

CCPA 的概念在文献[2]中首次被提出——在断开一部分输电线路的同时，中断量测数据从相量测量单元(phasor measurement unit，PMU)到控制中心的传输；此外，文献[2]还提出仅利用攻击区域外的可用信息来恢复相角和检测断开线路的方法。然而，现有研究均假设攻击者能够直接对从 PMU 采集到的量测数据进行篡改，没有考虑信息层故障在通信网络中扩散到指定的量测设备这一阶段的拓扑传染机制。冯晓萌等[3]在传统的虚假数据注入(false data injection，FDI)攻击的上层首次引入了蠕虫传播模型，实现了跨空间协同攻击的耦合建模，并采用 Q 学习算法求解该模型下的最优协同攻击策略。

如果让 CCPA 中协同的网络攻击失效，那么物理攻击造成的破坏就会迅速败露，系统将采取保护动作减少损失。近年来，针对 CCPA 的安全措施，专注于预防和检测其中的网络攻击——FDI 攻击。由于 FDI 攻击实际是一种针对量测值的恶意篡改，有研究者认为可采用 PMU 来保护某些量测值。PMU 用于进行同步相量的测量和输出以及进行动态记录，可判断量测值是否被篡改。PEI 等[4]提出了一种基于 PMU 预先部署的贪婪算法，优先选择保护一些最为脆弱的节点，再保护其他相对脆弱的节点。XIA 等[5]设计了基于子空间投影的检测算法，并提出 PMU 的准最优放置策略，以提高算法对 FDI 攻击的检测性能。然而，由于需要保护的量测设备数量较多，且 PMU 的价格也不低，导致部署这种安全防护措施的成本过高。因此，研究者致力于寻求成本更低的方法。近几年，移动目标防御(moving target defense，MTD)作为一种经济、高效的防御技术逐渐应用在智能电网中。RAHMAN 等[6]首次将通过改变输电线路的参数来达到防御效果的策略定义为 MTD，并认为输电线路参数的改变不能影响最优电力潮流(optimal power flow，OPF)的输出结果，也不能使得某些输电线路的电力流过载，因此，只能选择某些特定的输电线路来改变参数。LAKSHMINARAYANA 等[7]首次将 MTD 用于防御 CCPA，并在文献[8]中进行扩展，通过对某些输电线路的导纳进行主动扰动，使攻击者难以设计协同的 FDI 攻击，从而导致 CCPA 的攻击环路中断。CHEN 等[9]提出一种可以检测 CCPA 的 MTD 方法，该方法应用卷积神经网络(convolutional neural network，CNN)从受损量测值中定位线路中断的位置(定位物理攻击)。然而，这种改变输电线路参数的方法会引入对电力系统的物理扰动，可能会影响状态估计的准确性。

攻击者发起 FDI 攻击必须基于其获取的电网知识，包括网络拓扑结构(如节点之间的连通性)、输电线路的电抗和用于状态估计的量测集。本文通过随机化状态估计使用的量测集使攻击者的先验知识失效，从而降低 FDI 攻击的成功率。与基于输电线路变参的 MTD 方法不同[6-9]，本文将受控随机化应用于状态估计的量测集来缓解 FDI 攻击，主要有 2 个优势：一是不需要部署额外的物理设备，实施成本较低；二是未改变物理参数，不会对系统造成物理影响。

1　系统模型

在文献[10]中，针对电网状态估计的攻击基于直流(direct current，DC)模型，这种模型相对简单，比较适合进行基本分析，且预期结果在交流(alternating current，AC)模型中表现得更好。

1.1　电网模型

在 DC 模型中，由于输电线路的阻抗完全由

电抗决定，功率平衡方程可简化表示。将连接节点 k 和 j 的输电线路记为 $k-j$，则通过输电线路 $k-j$ 的有功潮流为：

$$P_{kj}=D_{kj}(\theta_k-\theta_j) \tag{1}$$

式中，D_{kj} 表示输电线路 $k-j$ 的导纳（阻抗的倒数），θ_k 表示节点 k 的电压相角。

1.2 状态估计和坏数据检测

电力系统中的状态估计就是通过 m 个量测值 $\boldsymbol{z}=[z_1,z_2,\cdots,z_m]^{\mathrm{T}}$ 来估计 $n(n<m)$ 个系统状态变量 $\boldsymbol{x}=[x_1,x_2,\cdots,x_n]^{\mathrm{T}}$，满足如下关系：

$$\boldsymbol{z}=\boldsymbol{h}(\boldsymbol{x})+\boldsymbol{e} \tag{2}$$

式中，$\boldsymbol{h}(\boldsymbol{x})=[h_1(\boldsymbol{x}_1,\cdots,\boldsymbol{x}_n),\cdots,h_m(\boldsymbol{x}_1,\cdots,\boldsymbol{x}_n)]^{\mathrm{T}}$，$\boldsymbol{e}$ 表示量测噪声向量。式(2)在 DC 模型中可表示为 $\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{e}$，其中 $\boldsymbol{H}=[h_{k,j}]_{m\times n}$ 是雅克比矩阵。

状态估计的计算通常基于最大似然（maximum likelihood，ML）方法[11]，即量测误差均值为 0 且服从正态分布时，状态估计的结果可表示为：

$$\hat{\boldsymbol{x}}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{z} \tag{3}$$

式中，$\boldsymbol{W}$ 是一个对角加权矩阵，其元素为量测噪声方差的倒数。

作为系统的自检机制，坏数据检测器（bad data detection，BDD）通过比较残差来检测错误的量测值，残差可以定义为：

$$r=\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}\| \tag{4}$$

若残差超过预定义的阈值 τ，则会触发 BDD 报警。通过设置检测阈值 τ，可以将假阳（false positive，FP）率调整到足够小，甚至接近于 0。

1.3 隐蔽攻击条件

若注入量测值的攻击向量为 $\boldsymbol{a}\in\mathbf{R}^m$ 时，则被篡改的量测向量可以表示为：

$$\boldsymbol{z}_a=\boldsymbol{z}+\boldsymbol{a} \tag{5}$$

大多数攻击向量无法绕过 BDD，除非满足 $\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}$ 的形式，其中 $\boldsymbol{c}\in\mathbf{R}^m$。

1.4 协同攻击条件

当电网的拓扑结构和潮流发生改变后，量测值会发生变化，此时 BDD 会检测到异常。为了掩盖物理攻击的影响，攻击者会构造协同的 FDI 攻击，抵消掉 BDD 的残差。

当一组输电线路受到物理攻击 p 而中断时，被篡改的量测向量可表示为：

$$\boldsymbol{z}_{\mathrm{p}}=\boldsymbol{z}+\boldsymbol{a}_{\mathrm{p}} \tag{6}$$

式中，$\boldsymbol{a}_{\mathrm{p}}=\boldsymbol{H}\Delta\boldsymbol{x}+\Delta\boldsymbol{H}\boldsymbol{x}_{\mathrm{p}}$，$\Delta\boldsymbol{H}=\boldsymbol{H}-\boldsymbol{H}_{\mathrm{p}}$。为了绕过 BDD，协同的 FDI 攻击必须满足 $\boldsymbol{a}=\Delta\boldsymbol{H}\boldsymbol{x}_{\mathrm{p}}$[12]。

1.5 环境变量介绍

FDI 攻击受到以下环境变量的影响：1）访问能力。当一些访问信道被加密或一些量测值被保护时，攻击者无法访问所有的量测数据。此外，由于传感器分布广泛，对所有的传感器组织攻击所花费的成本或工作量将非常巨大。因此，攻击者只能以部分量测值为目标，并且访问能力受到攻击者的资源限制。2）先验知识。电力系统的状态估计是基于电网的拓扑结构以及从不同线路和节点采集的一组量测值，攻击者提前获取的知识对于成功的 FDI 攻击至关重要，包括节点之间的连接和输电线路的电气参数（如导纳等）。此外，攻击者还需要知晓状态估计使用了哪些量测值。3）防护对象。攻击者的目的通常是破坏对系统有特定影响的一组状态，例如掩盖系统故障，但是无法攻击受到保护的量测值。

2 MTD 方法

2.1 MTD 的概念

MTD 的基本思想是通过增加系统的随机性、减少系统的可预见性来对抗同类型攻击，通过有效降低系统的确定性、相似性和静态性来显著增加攻击成本。MTD 通常的实现方式是通过变换系统配置，缩短系统配置属性信息的有效期，使得攻击者不能在有限时间内完成目标探测和攻击代码开发，同时降低收集的历史信息的有效性，使探测到的信息在攻击期间已失效。攻击面变换是 MTD 的主要手段，根据文献[13]的定义，系统的攻击面是指系统资源的一个子集，该子集可以被攻击者利用进行系统攻击破坏活动。因此，通过持续变换系统呈现在攻击者面前的攻击面，可以增加攻击者想要探测目标脆弱性的代价，从而有效降低系统被攻击的成功率。

2.2 MTD 工作机制

本文提出的 MTD 工作机制如图 1 所示，其主要步骤如下：

步骤 1 随机选择一组量测值作为状态估计的测量集，这组量测值通过一直被求解直到系统是可观测的。

步骤 2 攻击者基于原始的量测集发起 FDI 攻击，未能操纵状态估计的结果。

步骤 3 状态估计可以检测到异常数据，因

为量测残差超出了正常范围。

步骤 4　控制中心触发应急响应机制，采取了故障恢复保护动作。

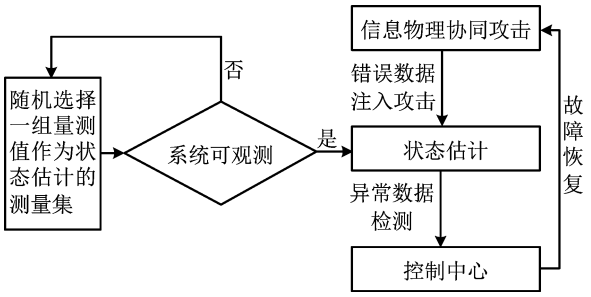


图 1　移动目标防御的工作机制

Fig. 1　The working mechanism of MTD

2.3　量测选择的随机化方法

根据 BDD 算法，状态估计并没有使用所有的量测值，因为有些量测值的噪声太大，可以忽略不计。一般来说，状态估计使用的量测集通常是固定的。攻击者为了构造攻击 $\boldsymbol{a}=\Delta\boldsymbol{H}\boldsymbol{x}_{\mathrm{p}}$，必须知晓状态估计所采用的量测集，否则就无法精确地识别一组所需的量测值，导致缺失一个或多个量测值或者包含没有必要的量测值。因此，如果增加攻击者关于量测集信息的不确定性，例如，随机选取量测值组成一组量测集，那么攻击的形式 $\boldsymbol{a}=\Delta\boldsymbol{H}\boldsymbol{x}_{\mathrm{p}}$ 将很难实现。

例如，IEEE 14 节点系统共计有 54 个量测值可用于状态估计，包括通过 20 条输电线路的正向和反向潮流以及 14 个节点的功耗。假设状态估计采用包含 30 个量测值的固定集合 B，其余量测值作为保留。为了增加量测集的不确定性，可从保留的量测值中再选取 7 个作为备选集 A，再从 $A\cup B$ 中重新选择 30 个量测值作为一组新的量测集。但是，新的量测集必须能够观测到系统，也就是说，系统的所有未知状态都可以从量测集中唯一地计算出来。

2.4　量测选择的形式化模型

假设电网共有 l 条输电线路和 b 个节点，则有 $m=2l+b$ 个量测值可用于状态估计，即通过每条输电线路的正向和反向潮流以及每个节点的功耗。

正向和反向潮流分别对应于 $\boldsymbol{H}$ 的第 1 个 l 行和第 2 个 l 行。输电线路 i 的潮流和与其连接的节点的状态可关联为：

$$\forall 1\leqslant i\leqslant l, P_i^{\mathrm{L}}=d_i(\theta_{\mathrm{f}_i}-\theta_{\mathrm{e}_i}) \tag{7}$$

式中，P_i^{L} 表示通过输电线路 i 的潮流，d_i 表示输电线路 i 的导纳，θ_j 表示节点 j 的电压相角，f_i 和 e_i 分别表示输电线路 i 的潮流的 2 个相反方向。

节点的功耗对应于 $\boldsymbol{H}$ 的最后 n 行。节点 j 的功耗和通过输电线路到该节点的潮流可关联为：

$$\forall 1\leqslant j\leqslant b, P_j^{\mathrm{B}}=\sum_{i\in L_{j,\mathrm{in}}}P_i^{\mathrm{L}}-\sum_{i\in L_{j,\mathrm{out}}}P_i^{\mathrm{L}} \tag{8}$$

式中，P_j^{B} 表示节点 j 的功耗，$L_{j,\mathrm{in}}$ 和 $L_{j,\mathrm{out}}$ 分别表示通过输电线路进、出节点 j 的潮流的集合。

从根本上说，状态估计就是通过求解所有量测值的方程得到每个节点的电压相角 θ，即 $\boldsymbol{H}$ 的每一行对应一个功率方程，利用量测集对这些方程进行求解。如果量测集能够通过式(7)～(8)求解未知状态，那么电力系统是可观测的。因此，式(7)～(8)可作为可观测性约束。若被使用的量测值对应的潮流或功耗为 0，则有：

$$\begin{cases}\forall 1\leqslant i\leqslant l, & (t_i\vee t_{l+i})\rightarrow(P_i^{\mathrm{L}}=0)\\ \forall 1\leqslant j\leqslant b, & t_{2l+j}\rightarrow(P_j^{\mathrm{L}}=0)\end{cases} \tag{9}$$

式中，t_i 表示量测值 i 是否被使用，其下标 i，$l+i$ 和 $2l+j$ 分别表示正向潮流、反向潮流和节点的功耗对应 $\boldsymbol{H}$ 中的位置。

如果量测集可以观测到系统，那么将每个量测值都假定为 0，求解出的状态一定是相同的。据此反推，如果至少存在 1 个不同于其他状态的状态，那么这个量测集就不能观测到系统，即：

$$\exists 1\leqslant j_1, j_2\leqslant b, j_1\neq j_2, \theta_{j_1}\neq\theta_{j_2} \tag{10}$$

基于这种方法，可以验证量测集能否观测到系统。

2.5　量测选择对攻击的影响

在物理攻击断开一组输电线路后，电网拓扑结构发生改变，影响了某些线路的潮流和某些节点的功耗。为了掩盖物理攻击的影响，攻击者需要发起协同的 FDI 攻击操纵状态估计的结果，让控制中心误认为系统运行正常。当某些线路的潮流和某些节点的功耗被改变后，若攻击者对量测值 i 注入特定的错误数据，则有：

$$\begin{cases}\forall 1\leqslant i\leqslant l,\\ \quad(\Delta P_i^{\mathrm{L}}\neq 0)\rightarrow(t_i\rightarrow a_i)\wedge(t_{l+i}\rightarrow a_{l+i})\\ \forall 1\leqslant j\leqslant b,\\ \quad(\Delta P_j^{\mathrm{B}}\neq 0)\rightarrow(t_{2l+j}\rightarrow a_{2l+j})\end{cases} \tag{11}$$

式中，ΔP_i^{L} 表示通过输电线路 i 的潮流变化量，ΔP_j^{B} 表示节点 j 的功耗变化量，a_i 表示量测值 i

因为攻击而被改变的值。

因此，如果将受控随机化应用于状态估计所使用的量测集，t_i 对于攻击者来说是不确定的，那么 a_i 就很难确定。

3 仿真实验

本文将攻击者分为无知型和智慧型 2 类，前者认为系统没有运行 MTD 且使用一组固定的量测值进行状态估计，后者知道系统运行了 MTD。为了与本文 MTD 方法作对比，仿真实验还考虑了文献[14]中提到的基于输电线路导纳扰动的 MTD 方法，并在不同的场景设定下重复计算 20 次取算术平均值，其中攻击者每次攻击 12 个量测值，且分布在不超过 7 个节点上；防御者每次随机选择 5 条输电线路，且只扰动其中 2 条输电线路的导纳。

本文使用 MATPOWER 模拟器[15]仿真了 3 个不同的 IEEE 标准系统，包括 IEEE 14 节点、IEEE 30 节点和 IEEE 57 节点系统。其中，IEEE 14 节点系统共计 54 个量测值可用于状态估计，随机选取 30 个作为状态估计的量测集；IEEE 30 节点系统共计 112 个量测值可用于状态估计，随机选取 65 个作为状态估计的量测集；IEEE 57 节点系统共计 217 个量测值可用于状态估计，随机选取 120 个作为状态估计的量测集。所有这些量测集都被证明能够观测到系统。

本文将受到攻击的状态数（被 FDI 攻击感染的状态数）占状态总数的百分比作为评估指标。为了保证 FDI 攻击成功，使用可满足性模理论（satisfiability modulo theories，SMT）对 FDI 攻击验证模型[16]进行编码，并使用高效的 SMT 求解器 Z3[17]执行这个模型。如果验证结果是可满足的，那么存在满足条件的攻击向量。

图 2～4 给出了 3 种不同攻防场景下的仿真结果，场景的设置分别考虑了攻击者的访问能力、知识限制和防护对象 3 个环境变量，每种场景只改变一个环境变量，其他环境变量保持原始状态。图 2 和图 3 分别显示了当攻击者的访问能力和知识限制在 40%～100%之间变化时，受到攻击的状态占状态总数的百分比。图 4 显示了当受保护的量测值在 0%～60%变化时，受到攻击的状态占状态总数的百分比。每个场景考虑 4 种不同的攻击案例，涉及 MTD 的应用和攻击者的类型：1）系统没有 MTD 的防护；2）系统部署了导纳扰动策略；3）系统部署了本文 MTD 方法且攻击者知晓量测集；4）系统部署了本文 MTD 方法但攻击者不知晓量测集。

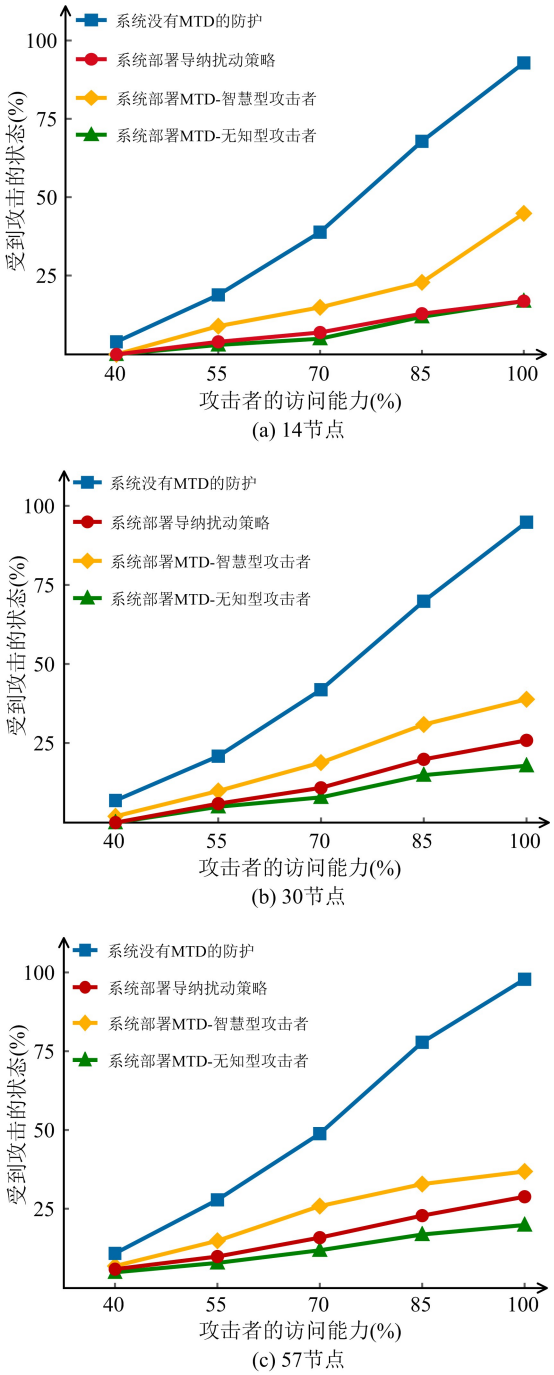


图 2 在攻击者访问能力不同时的攻击测试

Fig. 2 Attack tests under different access capabilities of attackers

3.1 攻击者的访问能力不同（场景Ⅰ）

图 2 展示了在场景Ⅰ下 3 个 IEEE 标准系统的仿真结果。总体而言，攻击者的访问能力对受到攻击的状态占比有显著影响，即攻击者的访问能力越强，FDI 攻击的成功率越高。在相同的访问能力下，当系统没有 MTD 的防护时，受到攻击

的状态占比最高；当系统部署了本文 MTD 方法时，受到攻击的状态占比下降至少 50%，且在对抗无知型攻击者时效果更好，这是因为如果攻击者知晓 MTD 方法在运行，他们会在构造攻击向量时涉及尽可能多的量测值来提高攻击的成功率。

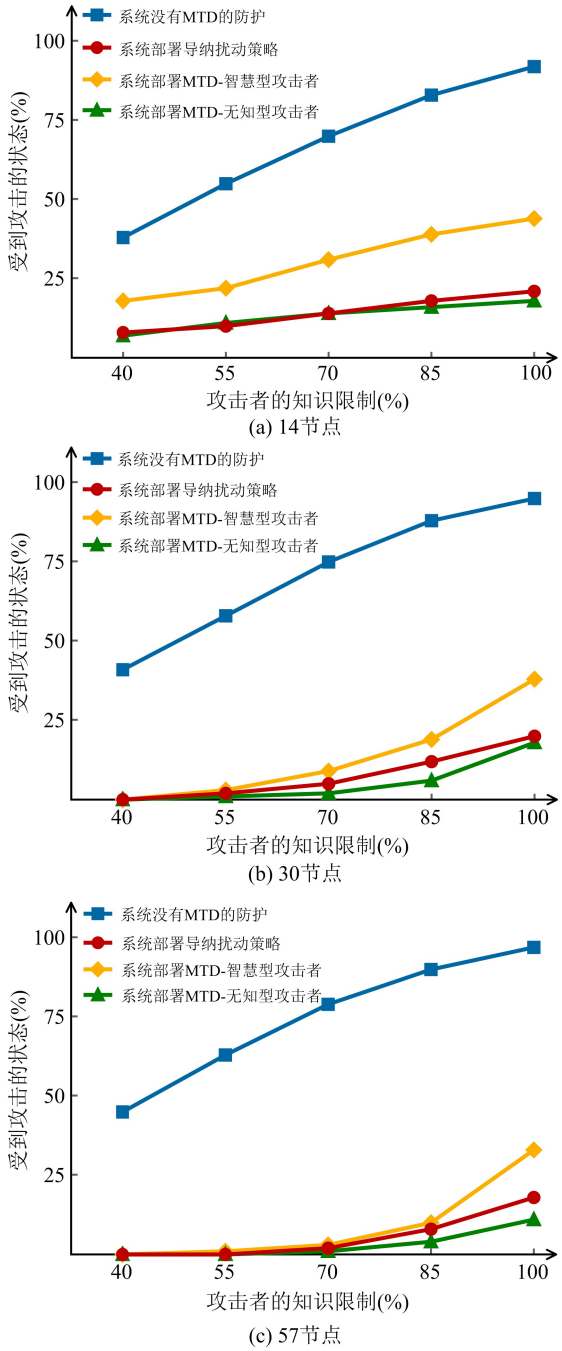


图 3　在攻击者知识限制不同时的攻击测试

Fig. 3　Attack tests under different knowledge limitations of attackers

3.2　攻击者的先验知识不同（场景 Ⅱ）

图 3 展示了在场景 Ⅱ 下 3 个 IEEE 标准系统的仿真结果。总体而言，随着攻击者知识限制的上升，受到攻击的状态的相对数量也会提高。在相同的知识限制下，被攻击状态占比在案例 1 中仍然是最高的，且在案例 3 和 4 中仍然可以减少 50%以上。特别地，当本文 MTD 方法对抗智慧型攻击者时，知识限制对受到攻击的状态占比有显著影响，这是因为攻击者会利用其所有关于量测集的知识来确保 FDI 攻击的成功。当攻击者的知识限制低于 80%时，在 30 节点和 57 节点系统中的攻击成功率是非常低的。

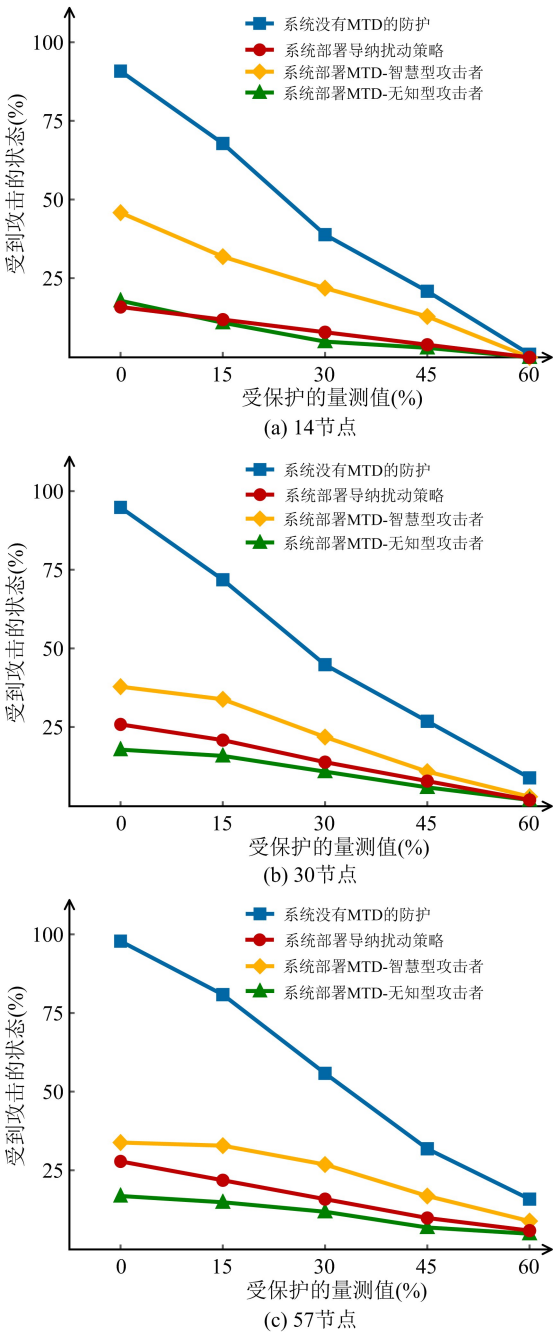


图 4　在受保护的量测值不同时的攻击测试

Fig. 4　Attack tests under different protected measurements

3.3　受保护的量测值不同（场景 Ⅲ）

图 4 展示了在场景 Ⅲ 下 3 个 IEEE 标准系统

的仿真结果。总体而言,受到攻击的状态占比随着受保护的量测值数量的增加而减少。换句话说,受保护的量测值越多,本文 MTD 方法的效果就越好。与未运行 MTD 的系统相比,在部署了本文 MTD 方法的系统中,受到攻击的状态占比降低至少 50%,也能够证明本文 MTD 方法的有效性。

可以观察到在 14 节点系统中,导纳扰动策略的性能表现趋向于当本文 MTD 方法对抗无知型攻击者时的性能表现,在图 3(a)、4(a)和 5(a)中呈现 2 条接近的曲线;当系统规模从 14 节点扩展到 30 节点和 57 节点时,本文 MTD 方法在对抗无知型攻击者时比导纳扰动策略表现得更好一些,且在图 3(b)和(c)中随着攻击者的访问能力百分比的增加,这种优势更明显。此外,系统规模对本文 MTD 方法的影响不大,横向比较实验结果在不同规模的系统中呈现相似的曲线,纵向比较实验结果在不同的场景中只有微小的差异。

4 结束语

本文设计了一种基于量测集受控随机化的 MTD 方法,通过阻止协同的 FDI 攻击,暴露物理攻击的影响使其可以被检测,从而及时发现并阻止 CCPA 进一步扩大影响。为了约束量测值的选择,确保状态估计使用的量测集是可以观测到系统的,本文引入了可观测性约束来构建量测选择的形式化模型。实验结果表明,在相同的环境变量下,本文所提出的 MTD 方法可以防止 50% 以上的状态被攻击。未来的工作将考虑电力系统的损耗和固有的非线性,把现有的工作扩展到 AC 模型中。

参 考 文 献

[1] GJESVIK L, SZULECKI K. Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout [J]. European Security, 2023, 32(1): 104-124.

[2] SOLTAN S, YANNAKAKIS M, ZUSSMAN G. Joint cyber and physical attacks on power grids: graph theoretical approaches for information recovery[J]. Performance Evaluation Review, 2015, 43(1): 361-374.

[3] 冯晓萌, 孙秋野, 王冰玉, 等. 基于蠕虫传播和 FDI 的电力信息物理协同攻击策略[J]. 自动化学报, 2022, 48(10): 2429-2441.
FENG Xiaomeng, SUN Qiuye, WANG Bingyu, et al. The coordinated cyber physical power attack strategy based on worm propagation and false data injection [J]. Acta Automatica Sinica, 2022, 48(10): 2429-2441.

[4] PEI C, XIAO Y, LIANG W, et al. PMU placement protection against coordinated false data injection attacks in smart grid[J]. IEEE Transactions on Industry Applications, 2020, 56(4): 4381-4393.

[5] XIA W, HE D M, CHEN J B. On the PMU placement optimization for the detection of false data injection attacks[J]. IEEE Systems Journal, 2023, 17(3): 3794-3797.

[6] RAHMAN M A, AL-SHAER E, BOBBA R B. Moving target defense for hardening the security of the power system state estimation[C]//Proceedings of the 1st ACM Workshop on Moving Target Defense. [S. l.: s. n.], 2014: 59-68.

[7] LAKSHMINARAYANA S, BELMEGA E V, POOR H V. Moving-target defense for detecting coordinated cyber-physical attacks in power grids[C]//Proceedings of 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids. [S. l.]: IEEE, 2019: 560-566.

[8] LAKSHMINARAYANA S, BELMEGA E V, POOR H V. Moving-target defense against cyber-physical attacks in power grids via game theory[J]. IEEE Transactions on Smart Grid, 2021, 12(6): 5244-5257.

[9] CHEN Y X, LAKSHMINARAYANA S, TENG F. Localization of coordinated cyber-physical attacks in power grids using moving target defense and deep learning[C]//Proceedings of 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids. [S. l.]: IEEE, 2022: 387-392.

[10] BOBBA R B, ROGERS K M, WANG Q Y, et al. Detecting false data injection attacks on DC state estimation[C]//Proceedings of Preprints of the 1st Workshop on Secure Control Systems. [S. l.: s. n.], 2010: 1-9.

[11] WOOD A J, WOLLENBERG B F, SHEBLÉ G B. Power generation, operation, and control[M]. [S. l.]: John Wiley & Sons, 2013.

[12] DENG R L, ZHUANG P, LIANG H. CCPA: coordinated cyber-physical attacks and countermeasures in smart grid[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2420-2430.

[13] MANADHATA P K, WING J M. An attack surface metric[J]. IEEE Transactions on Software Engineering, 2011, 37(3): 371-386.

[14] ZHANG Z Y, TIAN Y L, DENG R L, et al. A doub-

le-benefit moving target defense against cyber-physical attacks in smart grid[J]. IEEE Internet of Things Journal, 2022, 9(18): 17912-17925.

[15] ZIMMERMAN R D, MURILLO-SÁNCHEZ C E, THOMAS R J. MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education[J]. IEEE Transactions on Power Systems, 2011, 26(1): 12-19.

[16] RAHMAN M A, AL-SHAER E, RAHMAN M. A. A formal model for verifying stealthy attacks on state estimation in power grids[C]//Proceedings of 2013 IEEE International Conference on Smart Grid Communications. [S. l.]: IEEE, 2013: 414-419.

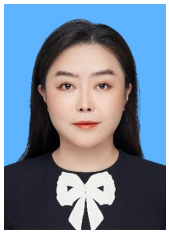
[17] DE MOURA L, BJØRNER N. Z3: an efficient SMT solver[C]//Proceedings of the 14th International Conference on Tools and Algorithms for the Construction and Analysis of Systems. [S. l.]: Springer, 2008: 337-340.

作 者 简 介

胡一帆

男，1991 年生，博士，讲师，研究方向为物联网安全

E-mail：huyifan@aeu.edu.cn



丁　玮

女，1988 年生，助理研究员，研究方向为装备试验鉴定

E-mail：1988dingwei2872@sina.com

张国敏

男，1979 年生，博士，副教授，研究方向为网络空间安全

E-mail：zhang_gmwn@163.com

王秀磊

男，1988 年生，博士，讲师，研究方向为数据安全

E-mail：xiuleiwang1988@126.com

邢长友

男，1982 年生，博士，教授，研究方向为网络空间测绘与对抗、可编程网络、网络功能虚拟化等

E-mail：changyouxing@126.com

许　博

男，1980 年生，博士，副教授，研究方向为网络性能测量

E-mail：xubo820@163.com

丁　科

男，1978 年生，博士，讲师，研究方向为硬件加速计算

E-mail：milod@163.com

石伟宏

男，1983 年生，高级工程师，研究方向为网络信息安全

E-mail：swh2011xy@163.com

责任编辑　安　蓓