基于蠕虫传播和 FDI 的电力信息物理协同攻击策略

冯晓萌 [1] 孙秋野 [1] 王冰玉 [1] 高嘉文 [1]

摘 要 随着信息技术与现代电力系统的结合日趋紧密, 通信系统异常和网络攻击均可能影响到电力系统的安全稳定运行. 为了研究工控蠕虫病毒对电网带来的安全隐患, 本文首次建立了基于马尔科夫决策过程 (Markov decision process, MDP) 的电力信息物理系统跨空间协同攻击模型, 该模型同时考虑通信设备漏洞被利用的难易程度为代价以及对电力网络的破坏程度为收益两方面因素, 能够更有效地识别系统潜在风险. 其次, 采用 Q 学习算法求解在该模型下的最优攻击策略, 并依据电力系统状态估计的误差值来评定该攻击行为对电力系统造成的破坏程度. 最后, 本文在通信 8 节点−电力 14 节点的耦合系统上进行联合仿真, 对比结果表明相较单一攻击方式, 协同攻击对电网的破坏程度更大. 与传统的不考虑通信网络的电力层攻击研究相比, 本模型辨识出的薄弱节点也考虑了信息层的关键节点的影响, 对防御资源的分配有指导作用.

关键词 SIR 蠕虫模型, 虚假数据注入, 信息物理联合仿真, 电力系统状态估计, Q 学习

引用格式 冯晓萌, 孙秋野, 王冰玉, 高嘉文. 基于蠕虫传播和 FDI 的电力信息物理协同攻击策略. 自动化学报, 2022, **48**(10): 2429−2441

DOI 10.16383/j.aas.c190574

The Coordinated Cyber Physical Power Attack Strategy Based on Worm Propagation and False Data Injection

FENG Xiao-Meng[1] SUN Qiu-Ye[1] WANG Bing-Yu[1] GAO Jia-Wen[1]

Abstract With the deep integration of information technologies in modern power systems, cyber system anomalies and network attacks can threaten the safety and stability of power system operation. To study the security risks of the power system caused by the latest industrial control worm, a coordinated cyber-physical power attack model based on the Markov decision process (MDP) is proposed in this paper. Then, the Q-learning algorithm is adopted to search for the optimal attack strategy in the proposed model, and the error of state estimation result induced by the attacks is devised to quantify the potential physical influences-attack benefits. Eventually, numerical joint simulation experiments are conducted on the 8CYBER_NODE-14BUS coupling test system, and the results show that the coordinated attack model proposed in this paper is more destructive. Compared with the traditional isolated physical attack without considering the cyber network, the identified weak nodes can also consider the influence of the cyber devices and guide the allocation of defense resources.

Key words SIR worm model, false data injection attack, cyber-physical joint simulation, power system state estimation, Q-learning

Citation Feng Xiao-Meng, Sun Qiu-Ye, Wang Bing-Yu, Gao Jia-Wen. The coordinated cyber physical power attack strategy based on worm propagation and false data injection. *Acta Automatica Sinica*, 2022, **48**(10): 2429−2441

随着电力系统和通信技术的高度耦合[1−2], 远程攻击者可以利用漏洞入侵信息网络引起通信故障, 进一步导致电力系统连锁故障. 近年来, 针对电力系统的攻击事件频繁发生, 如 2019 年 3 月, 委内瑞拉的古里水电站遭到反派黑客的网络攻击. 2019 年 7 月, 美国纽约曼哈顿发生了大规模停电事故. 因此, 电力系统的网络安全问题逐渐成为研究焦点.

现阶段针对电力系统网络攻击的相关研究可以根据攻击阶段的不同, 分为 2 类: 第 1 类是在侵入电力系统前, 研究针对通信层的攻击, 即远程攻击者采取何种网络攻击方式入侵通信网络. 这类研究在计算机科学领域已经相对完善, 一般采用攻击树模型[3] 和复杂网络理论两种方法对不同种类的攻击方法进行建模, 如蠕虫攻击[4]、木马攻击和网络监听等. 这类攻击不考虑从通信网络侵入后对电力系统造成的破坏. 第 2 类是在成功侵入后, 研究针对电

收稿日期 2019-08-09 录用日期 2020-04-07
Manuscript received August 9, 2019; accepted April 7, 2020
国家自然科学基金重点项目 (61433004), 国家自然科学基金 (61573094) 资助
Supported by Key Program of National Natural Science Foundation of China (61433004) and National Natural Science Foundation of China (61573094)
本文责任编委 孙健
Recommended by Associate Editor SUN Jian
1. 东北大学信息科学与工程学院 沈阳 110819
1. College of Information Science and Engineering, Northeastern University, Shenyang 110819

力层的攻击, 即攻击者采用何种攻击行为破坏电力系统. 这类研究主要是围绕如何篡改量测数据, 从而躲避检测机理, 对电力系统造成更严重破坏展开. 主要包括: 虚假数据注入攻击 (False data injection, FDI)[5−7]、负载重分配攻击 (Load redistribution, LR)[8] 和拒绝服务攻击[9] 等. 这类攻击不考虑攻击者利用通信设备上漏洞的难易程度和攻击代价. 上述两类研究都相对独立, 不能将攻击者如何侵入系统, 和侵入后的攻击行为两个阶段联合为一个整体, 实现跨空间攻击过程. 为了探索两个阶段攻击行为的耦合过程, 信息物理协同攻击逐渐受到国内外学者关注. 与传统的网络或物理攻击相比, 协同攻击的特点是同时考虑 (由于物理攻击) 对电力系统造成的破坏性, 和 (由于网络攻击) 对通信数据造成的不准确性 (篡改量测数据、开关状态等)[10]. 协同攻击的最新示例是 2015 年 12 月对乌克兰电网的攻击, 该攻击使几台断路器 (即物理攻击) 断开, 导致大约 225 000 名客户断电. 在攻击过程中, 针对电力客户服务的分布式拒绝服务攻击[11] 和 KillDisk 服务器擦除 (即网络攻击) 被用来掩盖紧急情况并延长中断时间[12].

现阶段对信息物理协同攻击的研究处于初步阶段, 主要分为 2 类: 1) 攻击者能够通过网络攻击对物理攻击行为进行遮掩, 欺骗检测机制. 例如, 通过 FDI 攻击, 修改线路的开断信息和量测数据, 从而掩盖和误导调度中心错误指令. 2) 攻击者通过分析信息物理耦合网络的特征和双向跨空间级联故障传播特性, 对耦合系统存在的漏洞进行分析, 制定更有效的攻击方案[13−15]. 文献 [16] 提出了一种电力信息物理协同攻击分析模型, 侧重于考虑攻击者和调度中心的交互关系. 文献 [17−18] 分别分析了在可观察和不可观察条件下攻击者通过改变拓扑信息来掩盖物理攻击行为. 文献 [19] 提出了一种在攻击者通过修改 PMU (Phasor measurement unit) 的量测数据后引起电力系统的状态估计结果出现误差的情形下, 电力系统的脆弱性评判指标. 文献 [20] 提出了攻击者共谋理论, 某通信节点的量测数据和与它邻接的其他通信节点, 即共谋者的数据同时被篡改后, 更容易避开检测装置的检测机制.

当黑客进行协同攻击时会根据电力系统的网络结构、设备特性和破坏情况反馈制定最优的攻击策略. 为了解决求最优解时出现的维度灾难、不连续可微函数不可解等问题, 引入了人工智能算法[21]. 因为电力信息物理系统在信息物理协同攻击下的系统运行状态符合马尔科夫决策过程, 提出了一种基于 Q 学习方法求解的最佳攻击策略[22]. 文献 [19] 使用马尔科夫决策过程来模拟在电力信息物理系统中的攻击风险传播过程, 并分析攻击者的攻击路线选择策略, 以获得最佳的回报效益. 此外, 从攻防双方的角度出发, 文献 [23−24] 建立了基于随机博弈的攻防模型, 能够给防御资源分配起到指导作用.

类比电力系统中的级联故障[25], 通信网络中故障的传播也具有一定的拓扑传染特性[13]. 上述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, 未实现跨空间协同攻击的耦合建模. 因此, 本文主要工作如下: 1) 本文提出了基于马尔科夫决策过程的协同攻击模型, 其在传统的虚假数据注入攻击的上层首次引入了蠕虫传播模型 (Susceptible infected recovered model, SIR), 实现了通信−电力双层攻击的耦合建模. 2) 在信息层采用漏洞评分标准 (Common vulnerability scoring system, CVSS) 中的 “漏洞利用难度”字段量化攻击者对攻击的难易程度, 即攻击成本. 在物理层依据全量测状态估计的误差值评定该攻击行为对电力系统造成的破坏程度, 即攻击收益. 3) 使用 Q 学习方法对该模型下攻击者最优协同攻击策略进行求解, 目标函数定义为破坏电力设备的攻击收益和入侵通信层设备的攻击成本比值的积累奖励. 4) 使用网络模拟器 (Network simulator 2, NS2) 和 MATLAB 进行通信 8 节点−电力 IEEE 14 节点的联合仿真实验, 模拟攻击者跨空间渗透的攻击过程, 并分析了在该最优攻击策略下相关设备被攻击的可能性. 仿真结果表明, 较单层攻击模式, 本文所提的协同攻击模型攻击破坏性更强. 本文进一步分析了最优攻击策略下相关设备被攻击的可能性, 能更有效地发现电网薄弱环节.

1 电力信息物理跨空间协同攻击模型

近年来数例典型电网破坏事件[12, 26] 的流程可以概括为: 远程黑客利用 PC 机或可编程逻辑控制器 (Programmable logic controller, PLC) 中的系统漏洞注入病毒; 该病毒在通信设备中级联渗透; 扩散到指定功能的通讯设备或调度中心; 随后通过修改量测数据和控制命令使得电力系统瘫痪.

如图 1 所示, 电力信息物理系统由电力系统网架结构和通信网络组成. 量测装置 PMU 将潮流和线路开关状态信息传输给由通信设备 (如 PLC) 组成的通信网络, 接着传输至调度中心. 调度中心利用状态估计筛查量测数据, 并进行潮流调度. 基于

此, 本文提出了一种信息物理协同攻击模型, 该模型实现了跨空间双层攻击的耦合建模, 在上层通信层攻击模型建立为蠕虫传播模型, 下层电力层采用虚假数据注入的攻击方式. 通信−电力两层之间以电力母线上装置的量测装置 PMU 与 PLC 等通信设备相连接. 该协同攻击的攻击原理为: 远程攻击者发起蠕虫病毒感染通信网络中的 PLC 等通讯设备. 一旦感染成功, 被感染的通讯设备所收集到的 PMU 量测数据有一定概率被注入虚假数据, 进而导致电力系统状态估计值出现误差, 从而引发连锁故障.

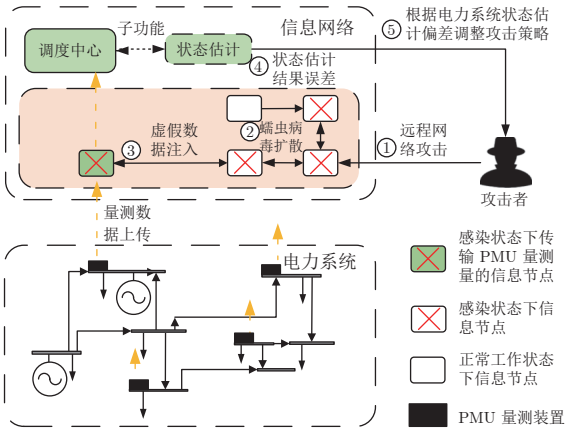


图 1　电力信息物理协同攻击示意图

Fig. 1　Diagram of electrical cyber-physical cooperative attacks

由此, 本节首先对通信层和物理层攻击模式分层建模. 然后根据网络攻击从信息系统渗透到物理系统的跨空间传播方式, 提出了一种基于马尔科夫过程的协同攻击模型. 为了便于表述, 在下文中, 将通信网络 (C-net) 中负责传输 PMU 量测数据的通信设备定义为信息节点 C-n, 节点数目为 N^c. 将电力网络 (G-net) 中的母线抽象定义为电力节点 Bus-n, 节点数目为 N^g.

1.1　通信层攻击模型

本节使用 SIR 传染病模型对蠕虫病毒在通信层设备间的传播机制进行建模, 并采用 CVSS 漏洞评分标准来定义攻击者成本函数.

1.1.1　蠕虫传播模型

首例工业控制蠕虫病毒 Stuxnet[27] 被证实能在边缘通信设备, 如 PLC 中单独传播, 不需要借助任何 PC 机. 文献 [4] 对工控网络中 PLC 病毒传播机理进行建模, 但仅分析了病毒在信息设备的传播机理. 文献 [28] 使用元胞自动机建模定性分析了电力信息系统中信息安全风险跨空间传播的基本原理, 但并没有给出具体模型. 本文采用 SIR 传染病模型对蠕虫病毒在电力通信网络中的传播机理进行建模. 在该模型下通信设备 i 的状态有 3 种: 1) 易感染态 ($\mathcal{S}$): 易感染态也是正常状态, 处于该状态的设备上存在安全漏洞, 但还没有被感染节点扫描到. 2) 感染态 ($\mathcal{I}$): 此类设备已经成为蠕虫节点, 将会扫描与它拓扑相连的其他易感染态节点并将其感染. 3) 免疫态 ($\mathcal{R}$): 此类节点的安全漏洞已经被修复, 在该状态下对蠕虫节点的扩散免疫. 通信网络中 3 种节点的状态转移过程如图 2 所示, 一旦某通信设备被感染成为蠕虫节点, 那么攻击者可以获取该设备的权限, 对该设备存储和传输的 PMU 量测数据进行篡改.

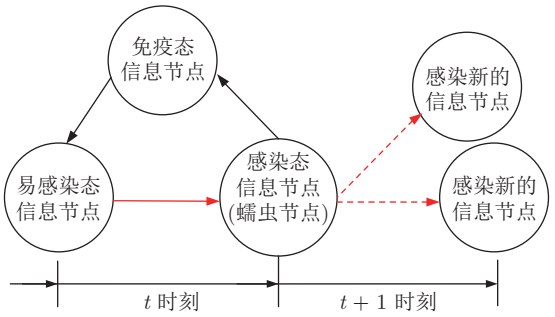


图 2　通信网络的 SIR 蠕虫扩散模型状态转换图

Fig. 2　SIR worm diffusion model state transition diagram of the cyber network

如图 2 所示, 通信网络的设备状态转变和前一时刻状态的关联度较高. 基于本模型的各个通信设备 i 从 t 时刻的状态到 $t+1$ 时刻的状态的状态转移概率为

$$P(s_i^{c'}|s_i^c)=\begin{cases}P_{\mathcal{S}\to\mathcal{I}}^t, & \text{若 } s_i^c=\mathcal{S} \text{ 且 } s_i^{c'}=\mathcal{I}\\ 1-P_{\mathcal{S}\to\mathcal{I}}^t, & \text{若 } s_i^c=\mathcal{S} \text{ 且 } s_i^{c'}=\mathcal{S}\\ P_{\mathcal{I}\to\mathcal{R}}^t, & \text{若 } s_i^c=\mathcal{I} \text{ 且 } s_i^{c'}=\mathcal{R}\\ 1-P_{\mathcal{I}\to\mathcal{R}}^t, & \text{若 } s_i^c=\mathcal{I} \text{ 且 } s_i^{c'}=\mathcal{I}\\ P_{\mathcal{R}\to\mathcal{S}}^t, & \text{若 } s_i^c=\mathcal{R} \text{ 且 } s_i^{c'}=\mathcal{S}\\ 1-P_{\mathcal{R}\to\mathcal{S}}^t, & \text{若 } s_i^c=\mathcal{R} \text{ 且 } s_i^{c'}=\mathcal{R}\end{cases}\tag{1}$$

其中, 通信设备 i 在 t 时刻为易感染态 ($\mathcal{S}$) 且 $t+1$ 时刻为感染态 ($\mathcal{I}$) 时, 状态转移概率为 $P_{\mathcal{S}\to\mathcal{I}}^t$, 其他同理. 该转移概率与通信网络当前的拓扑结构, 数据包传输情况以及各个设备当前的感染情况有关. 其中拓扑结构与网络中节点的度有关, 本文将 k_i^c 定义为信息节点 i 的度, 表示该节点与 k_i^c 个信息

节点邻接. 第 i 个信息节点在 t 时刻状态转移概率计算式为

$$P^t_{S->I}(i) = |\Theta_i|\eta\Delta t\beta \tag{2}$$

$$P^t_{R->S}(i) = \varsigma \tag{3}$$

$$P^t_{I->R}(i) = \nu \tag{4}$$

其中, $|\Theta_i|$ 代表与信息节点 i 相连接的蠕虫节点的个数. η 是蠕虫病毒节点可以在 1 s 内扫描的邻接设备的数量, 该参数受限于扫描方法的性能和网络带宽. 在理想的情况下, 一般取实际网络带宽的上限. 本节假设在同一个通信网络中全网蠕虫节点的值相同. Δt 表示扫描周期, 这里设一般取为秒级. β 代表通信设备扫描到一次之后被成功感染的概率. ς 代表从免疫态 ($\mathcal{R}$) 到易感染态 ($\mathcal{S}$) 的恢复率, 该参数是由病毒实时更新速度和补丁失效情况决定. 同理, ν 代表通信设备状态从感染态 ($\mathcal{I}$) 转移到免疫态 ($\mathcal{R}$) 的移除率, 该参数是由漏洞补丁的更新速度和感染区域隔离情况等决定.

在实际情形中, 攻击者通过监听和流量监测等手段并不能完全掌握观测到整个信息层设备的状态, 只能掌握部分可观的网络结构、蠕虫节点的总数量和被监听的节点的连接信息, 不能掌握正常节点和蠕虫节点的拓扑关联信息. 下面对 $|\Theta_i|$ 进行估算, 进而求解状态转移概率. 本文根据已知参数估计通信网络的平均度估计各个信息节点的邻接情况.

通过攻击者检测到的相关信息, 预估计出的度为 k 的信息节点的数为 N^c_k, 其中蠕虫节点的个数为 I^c_k. 令 $\lambda^c(k) = N^c_k/N^c$ 表示该网络中的度分布, 即节点度的散布情况. 也就是说, 在网络中随机抽取某信息节点的度是 k 的概率为 $\lambda^c(k)$. 令 $\langle k\rangle^c$ 代表平均度, 可计算为

$$\langle k\rangle^c = \sum_{k=0}^{k^c_{\max}} [k \times \lambda^c(k)] \tag{5}$$

其中, $k^c_{\max}$ 表示 C _ net 中的设备与其他设备邻接的最大度. 令 ψ^c 表示与易感染态节点相邻的节点是蠕虫节点的概率, 可计算为

$$\psi^c(t) = \frac{1}{\langle k\rangle^c}\sum_{k=0}^{k^c_{\max}}\left[k \times \lambda^c(k) \times \frac{I^c_k(t)}{N^c}\right] \tag{6}$$

由此, $|\Theta_i|$ 可以表示为

$$|\Theta_i| = k^c_i \times \psi^c(t) \tag{7}$$

在该模型下可以模拟蠕虫病毒在通信网络中的传播机理. 在这种动态的状态转化过程中, 各个通信设备的攻击成本也随着状态转移概率动态变化.

1.1.2 攻击者成本函数

攻击者的攻击成本与设备主机上的漏洞的利用难度成正比. 某一通信设备的攻击成本由该设备上最薄弱的漏洞利用难度决定. 本文参考漏洞评估系统 (CVSS) 中网络漏洞评价指标的 “利用复杂性” 分数, 对漏洞难度量化. “利用复杂性” 值越大, 该漏洞被利用的难度就越大. 此外, 通信设备中的相关漏洞参数由工业互联网安全响应数据库[20] 中提供. 攻击者在 t 时刻攻击第 i 个通信设备的攻击成本为

$$C_i(t) = \frac{g^i_{\text{com}}(t)}{\sum\limits_{j=0}^{N^c} g^j_{\text{com}}(t)} \tag{8}$$

其中, g^i_{com} 代表第 i 个节点利用复杂性分数, 它随着攻击者对通信网络的渗透程度变化. 其动态变化由下式计算

$$g^i_{\text{com}}(t) = \begin{cases} 0, & i \notin \phi_V(t) \\ g^i_{\text{com}}, & i \in \phi_V(t) \end{cases} \tag{9}$$

其中, $\phi_V(t)$ 代表暴露给攻击者的扫描目标集, 即攻击者可以通过当前信息网络的渗透状态能够选择的下一个阶段攻击的目标节点的集合. 本文使用动态攻击图 $G = (\phi_V(t), \phi_E(t))$ 来记录攻击者的扫描目标集和渗透路径. $\phi_E(t)$ 代表攻击者掌握的当前扫描目标集能够利用的渗透路径. 攻击图节点集 $\phi_V(t)$ 和边集 $\phi_E(t)$ 的初值为攻击者在最开始时能利用的扫描网络. 当蠕虫病毒扫描网络时, 只能感染扫描集中的设备. 一旦某设备 i 被感染, 那么与其相邻的节点 j, 即满足 $l_{c,ij}$=1, 会被加入 $\phi_V(t)$, 见式 (17). 同时, 节点 i 和 j 的连接线将被添加到 $\phi_E(t)$ 中. 每一次攻击结束后, 更新整个动态攻击图的拓扑.

1.2 电力层攻击模型

本节定义了电力系统全量测状态估计遭受 FDI 攻击后的错误估计结果和原始估计结果的均方误差 (Root mean squared error, RMSE) 作为攻击者攻击回报函数. 分析了攻击者在篡改量测数据时, 要同时更新共谋者的相关数据, 以此躲避检测器检测机理.

1.2.1 电力系统的 FDI 攻击

无论攻击者对信息层设备的渗透严重程度如何, 其最终目标都是通过对量测装置、相关的控制设备和通信网络注入错误数据, 进而导致电力系统状态估计器产生错误的状态估计结果, 最终对电力系统相关应用业务造成危害.

本文采用电力系统全量测状态估计方法[29], 该方法中电力系统状态估计的量测值包括 SCADA 量测值和 PMU 量测值. 从攻击动机方面, 相比于 SCADA 量测数据, PMU 量测量误差更小, 精度更高, 还包括独有的相角量测数据, 具有很高的攻击价值. 从攻击难度方面, 考虑电力系统调度的分区机制, SCADA 在一区, 防御最严密, 攻入难度较大, 而与 PMU 量测量相关的通信设备由于在终端, 攻入难度相对较小. 综上, PMU 量测量更容易成为攻击者的攻击目标[30−31]. 基于此, 针对全量测状态估计方法的电力系统虚假数据注入攻击过程如下:

步骤 1. 首先使用传统的状态估计模型求解, 即使用 SCADA 量测数据计算加权最小二乘估计方法求解状态估计结果 $\boldsymbol{x}^{(1)}=[\boldsymbol{\theta},\boldsymbol{V}]^{\mathrm{T}}$.

步骤 2. 引入 PMU 的量测值进行全量测状态估计

$$\begin{bmatrix}\boldsymbol{x}^{(1)}\\ \boldsymbol{z}^{g}\end{bmatrix}=\begin{bmatrix}\boldsymbol{I}_{2N^{g}}\\ \boldsymbol{H}_{z}\end{bmatrix}\left[\boldsymbol{x}^{(2)}\right]+[\boldsymbol{\omega}] \tag{10}$$

其中, 全部量测值包括原始的状态估计结果 $\boldsymbol{x}^{(1)}$ 和 $\boldsymbol{z}^{g}$. 在本文中, $\boldsymbol{z}^{g}$ 定义为 PMU 的量测值, 个数为 N^{g}, 包括电压相量的幅值 $\boldsymbol{V}$ 和相位角 $\boldsymbol{\theta}$. $I_{N^{g}}$ 为 N^{g} 阶单位矩阵, H_{z} 为布尔矩阵[29]. $\boldsymbol{x}^{(1)}=[\boldsymbol{\theta}',\boldsymbol{V}']^{\mathrm{T}}$ 是基于 SCADA 和 PMU 量测量的全系统状态估计结果. $\boldsymbol{\omega}$ 为仪表量测误差, 它是独立于状态量 $\boldsymbol{x}$, 服从均值为 0, 标准方差为 2% 的高斯分布[32].

步骤 3. 令 $\boldsymbol{e}_{z}=[e_{\theta 1},\cdots,e_{\theta N^{z}},e_{V1},\cdots,e_{VN^{z}}]^{\mathrm{T}}$ 表示注入 $\boldsymbol{z}^{g}$ 的虚假数据向量, 估计器将获得错误估计结果, 即

$$\begin{bmatrix}\boldsymbol{x}^{(1)}\\ \hat{\boldsymbol{z}}^{g}\end{bmatrix}=\begin{bmatrix}\boldsymbol{x}^{(1)}\\ \boldsymbol{z}^{g}+\boldsymbol{e}_{z}\end{bmatrix}+[\boldsymbol{\omega}]=\begin{bmatrix}I_{2N^{g}}\\ H_{z}\end{bmatrix}[\boldsymbol{x}^{(2)}+\boldsymbol{e}_{xz}]+[\boldsymbol{\omega}] \tag{11}$$

其中, $\hat{\boldsymbol{z}}^{g}=[\hat{\theta}_{1},\hat{\theta}_{2},\cdots,\hat{\theta}_{N^{z}},\hat{V}_{1},\hat{V}_{2},\cdots,\hat{V}_{N^{z}}]^{\mathrm{T}}$ 表示被注入虚假数据之后传输给估计器的量测值, $\boldsymbol{e}_{xz}=[\boldsymbol{e}_{x\theta},\boldsymbol{e}_{xV}]^{\mathrm{T}}$ 是由虚假数据注入攻击导致的估计器求解出的状态量的误差.

步骤 4. $\boldsymbol{x}^{(2)}$ 采用加权最小二乘法通过迭代求解如下

$$[\boldsymbol{e}_{xz}]=[G_{2}]^{-1}\left[R_{2}^{-1}H_{2}\right]^{\mathrm{T}}[\hat{\boldsymbol{z}}^{g}]-\left[\boldsymbol{x}^{(2)}\right] \tag{12}$$

其中, $[G_{2}]=[H_{2}]^{\mathrm{T}}[R_{2}]^{-1}[H_{2}]$ 为增益矩阵, $H_{2}=\begin{bmatrix}I_{2N^{g}}\\ H_{z}\end{bmatrix}$, $[R_{2}]=\begin{bmatrix}\mathrm{cov}(\boldsymbol{x}^{(1)}) & 0\\ 0 & R_{\mathrm{pmu}}\end{bmatrix}$, R_{pmu} 是 PMU 量测量的协方差矩阵.

1.2.2　“共谋” 躲避检测机理

对电力节点 j 的第 l 个量测值 z_{jl} 注入虚假数据后, 该错误量测数据被检测器检测出的概率与检测算法和该节点周围邻接节点的量测值被篡改的个数有关[33]. 该节点周围邻接节点的量测值被篡改的个数越多, 对该节点注入恶意数据后被检测出来的概率越小, 即攻击者共谋理论. 本节对这个特性进行定性分析检测器检测概率, 某个电力节点 j 数据被篡改后, 被检测出来的概率为

$$P_{j}^{\mathrm{fail}}(t)=\kappa[k_{j}^{g}\times\psi^{g}(t)]=\kappa\left[k_{j}^{g}\frac{1}{\langle k\rangle^{g}}\sum_{k_{j}=0}^{k_{\max}^{g}}k_{j}^{g}\times\lambda^{g}(k_{j})\times I_{k_{j}}^{g}(t)\right] \tag{13}$$

其中, κ 是检测系数, 由检测方法所决定. k_{j}^{g} 表示电力节点 j 的度, 即 $k_{j}^{g}=\sum_{i=1}^{N^{g}}l_{g,ji}$, $l_{g,ji}$ 代表电力线路的邻接关系, 见式 (17). ψ^{g} 表示与任意电力节点相邻的电力节点的量测数据已经被篡改概率. $k_{\max}^{g}$ 代表 G-net 中的设备与其他设备邻接的最大度. $\langle k\rangle^{g}$ 代表整个电力网络中节点的平均度. I_{m}^{g} 表示度为 m 的、并且其上量测数据已被篡改了的母线节点的总数. $P^{g}(m)=N_{m}^{g}/N^{g}$ 代表整个电力网络中节点度分布, 为度为 m 的节点的总数与电力网络所有节点的总数的比值.

$$\langle k\rangle^{g}=\sum_{j=0}^{k_{\max}^{g}}k_{j}^{g}\times\lambda^{g}(k_{j}^{g}) \tag{14}$$

1.2.3　攻击者回报函数

假设攻击者某一次的攻击行为成功地避开了检测机制, 将合适的虚假数据注入系统的量测装置并且造成估计的状态结果的偏差, 则攻击者可以通过本次攻击行为获得回报. 对于某一个电力节点 j 的数据被篡改之后, 攻击者攻击回报为电压偏差和电流偏差, 即

$$(B_{Vj},B_{\theta j})=\left(\frac{\left|V_{xj}-\hat{V}_{xj}\right|}{V_{xj}},\frac{\left|\theta_{xj}-\hat{\theta}_{xj}\right|}{\theta_{xj}}\right) \tag{15}$$

其中, V_{xj},θ_{xj} 分别是原始估计结果, 而 $\hat{V}_{xj},\hat{\theta}_{xj}$ 是错误的估计结果. 针对整个电力网络, 攻击者的攻击收益为全局状态估计结果的均方根误差, 即

$$B(t)=\sqrt{\frac{1}{N^{g}}\sum_{j=0}^{N^{g}}(B_{\theta j}^{2}(t)+B_{Vj}^{2}(t))} \tag{16}$$

攻击者通过修改部分通信设备的量测值后, 使得全局的状态估计结果和原始估计结果产生的均方

根误差 (RMSE) 定义为攻击者的回报函数.

1.3 信息物理协同攻击模型

本节通过马尔科夫决策过程模拟恶意入侵者在动态环境中的攻击行为和电力信息物理系统的状态随时间演变过程. 在遭受协同攻击后, 电力信息物理系统在 t 时刻的系统状态与 $t-1$ 时刻的系统状态具有很高的纵向关联度. 也就是说, 在协同攻击下电力信息物理系统的状态演化过程具有马尔科夫性, 因而本节建立基于马尔科夫决策过程的电力信息–物理双层协同攻击模型.

1.3.1 信息–物理脆弱性邻接矩阵

如图 3 所示, 定义电力信息–物理脆弱性邻接矩阵 $\boldsymbol{L}$:

$$\boldsymbol{L}=\begin{bmatrix}\boldsymbol{L}_c & \boldsymbol{L}_f\\ \boldsymbol{L}_f^{\mathrm{T}} & \boldsymbol{L}_g\end{bmatrix}_{(N^c+N^g)\times(N^c+N^g)} \tag{17}$$

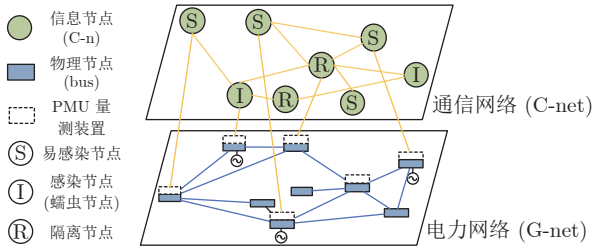


图 3 电力信息物理耦合网络

Fig. 3 The network of cyber-physical power coupling system

其中, 脆弱性邻接矩阵的元素主要有 4 类: 1) 通信–通信节点连接矩阵 $\boldsymbol{L}_c$: 其中元素 $L_{c,ij}$ 代表攻击者可以利用信息节点 i 上的漏洞, 并进一步感染信息节点 j. 2) 通信–物理节点连接矩阵 $\boldsymbol{L}_f$: $L_{f,ij}$ 表示母线 i 和 j 之间的传输线从控制中心向物理设备发送控制命令的过程. 3) 物理–物理节点连接矩阵 $\boldsymbol{L}_g$: $L_{g,ij}$ 表示电力母线 i 和 j 之间的传输线. 4) 物理–信息节点连接矩阵 $\boldsymbol{L}_f^{\mathrm{T}}$: $L_{f,ij}^{\mathrm{T}}$ 表示信息节点 i 可以接收并传输物理设备 j 的相关量测值. 当节点 i 和节点 j 之间存在传输线路时, $L_{ij}=1$. 相反, 当节点 i 和 j 之间不存在传输线路时, $L_{ij}=0$.

1.3.2 信息–物理双层耦合建模

如图 4 所示, 当前攻击者可模拟控制中心的功能, 进行状态估计求得奖励回报值 Reward, 从而制定更精确更有效的攻击策略[6, 34]. 由此, 针对该类攻击者的攻击策略所制定的防御策略更具有研究意义. 基于此, 本节给出在上文所提出的信息物理协同攻击下跨空间渗透和反馈决策机理. 首先, 根据攻击策略 π 发动攻击行为 Action, 感染相关的通信层设备, 使其从正常态 $\mathcal{S}$ 变为感染态 $\mathcal{I}$, 并在通信网络中扩散; 然后, 感染态的信息节点将从 PMU 中收集到的量测值 $\boldsymbol{z}^g(t)$ 进行篡改, 使其变为错误的量测值 $\hat{\boldsymbol{z}}^g(t)$; 随后, 状态估计器使用错误的量测值估计出错误的状态量 $\boldsymbol{x}^{(2)}(t)+\boldsymbol{e}_{xz}$, 计算状态量的误差, 该误差值作为奖励回报值 Reward 反馈给攻击者; 最后, 攻击者会根据相应的回报值调整接下来

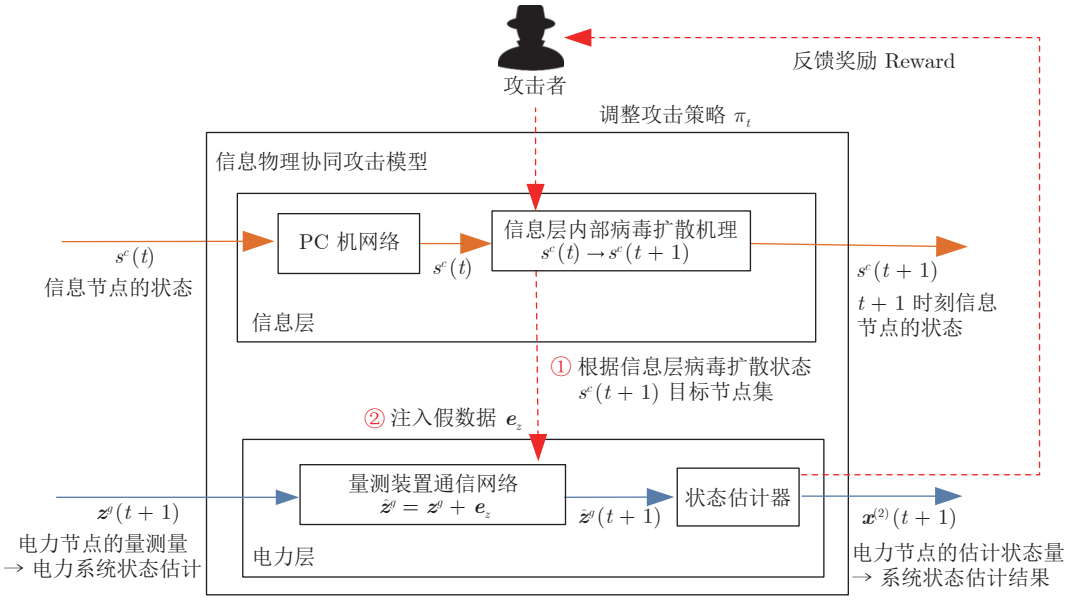


图 4 信息物理协同攻击下跨空间渗透和反馈决策机理

Fig. 4 Cross-space penetration and feedback decision mechanism under cyber-physical collaborative attack

的攻击行为, 通过不断地模拟, 修正策略, 最终得到使得目标函数最大的最优攻击策略. 其中, 感染态的信息节点对邻接的 PMU 量测值注入虚假数据的函数为

$$\begin{cases} \hat{\boldsymbol{z}}^g(t)=\boldsymbol{z}^g(t)+\left\{\begin{bmatrix}1\\1\end{bmatrix}\otimes(\boldsymbol{L}_z\times(\boldsymbol{L}_f^{\mathrm{T}}\times\boldsymbol{\Lambda}))\right\}\circ\boldsymbol{e}_z \\ \begin{bmatrix}\boldsymbol{x}^{(1)}\\ \hat{\boldsymbol{z}}^g(t)\end{bmatrix}=\begin{bmatrix}I_{N^g}\\ H_z\end{bmatrix}[\boldsymbol{x}^{(2)}(t)+\boldsymbol{e}_{xz}] \end{cases} \tag{18}$$

其中, 通信系统当前的信息节点感染状态用 $\boldsymbol{\Lambda}=[l_{s_1^c=I},\, l_{s_2^c=I},\, \cdots,\, l_{s_{N^c}^c=I}]^{\mathrm{T}}$ 表示, 可由式 (1) 求得. $\otimes$ 和 $\circ$ 分别是克罗内克积和哈达玛积. 表示通信−电力设备连接矩阵, $\boldsymbol{L}_{f(N^c\times N^g)}$ 可由式 (17) 求得. $\boldsymbol{L}_{z(N^z\times N^g)}$ 为 N^g 个母线节点标号和 N^z 个安置 PMU 设备的母线的标号对应关系 (标号从小到大), 即 $l_{z,\,ij}=1$ 表示 N^g 中第 j 个标号对应 N^z 中第 i 个标号. 对 l_x, 当 x 判断为真时, $l_x=1$, 当 x 判断为假时, $l_x=0$. 当通信设备 i 的状态为感染态 ($\mathcal{I}$) 时, 即 $s_i^c=I$ 时, $l_{s_i^c=I}$ 为 1. $\boldsymbol{x}^{(1)}$, $\boldsymbol{e}_{xz}$ 分别是式 (11) 中 PMU 前一阶段的估计值和估计误差. 每次攻击行为结束后造成的状态值的误差 $\boldsymbol{e}_{xz}$ 能够反馈给攻击者, 攻击者会根据这个反馈值不断修正当前的攻击策略, 最终求得最优的攻击策略.

由于 PMU 的采样频率很高, 大约为 30 次/s, 而大多数研究表明攻击者攻击间隔 Δt 大约是秒级. 为了解决注入假数据时刻和 PMU 采样时刻并不一致的问题, 本文采用基础的 PMU 缓存的方法, 即当攻击者在 t 时刻对 PMU 量测量注入假数据时, 直接选取 PMU 缓存器中距离 t 时刻最近时刻的存储数据篡改. 由此, 这里根据攻击间隔对原本离散的 PMU 采样值进一步离散化.

1.3.3　攻击者的目标函数

攻击者的最终目标为: 从初始状态在时间 T 内采取策略 π 后, 能够获得期望的 Reward 值达到最大. 即对电力网络的破坏程度与对通信设备的利用成本的比值的累积和 W 达到最大, 定义其最大值为

$$\max W=\mathrm{E}\left[\frac{1}{T}\sum_{t=0}^{T}\left(\frac{B(t)}{C(t)}\right)\right]=\mathrm{E}\left[\frac{1}{T}\sum_{t=0}^{T}\left(\frac{\sqrt{\frac{1}{N^g}\sum\limits_{j=0}^{N^g}B_j(t)}}{\sum\limits_{i=0}^{N^c}P_i^{\mathrm{act}}C_i(t)}\right)\right] \tag{19}$$

电力网络的约束条件为

$$P_j^{\min}\le\Gamma^{\mathrm{T}}D\sin(\Gamma\theta)\le P_j^{\max} \tag{20}$$

$$V_j^{\min}\le\hat{V}_j\le V_j^{\max} \tag{21}$$

$$\theta_j^{\min}\le\hat{\theta}_j\le\theta_j^{\max} \tag{22}$$

$$\Gamma^{\mathrm{T}}D\sin(\Gamma\theta)-P_j=0 \tag{23}$$

信息网络的约束条件为

$$\|\pi\|_0=n \tag{24}$$

$$\sum_{i=0}^{N^c}P_i^{\mathrm{act}}=1 \tag{25}$$

其中, $B(t)$表示攻击者在时间 t 的攻击收益, 由式 (16) 求得. $C(t)$ 表示攻击者的攻击成本, 定义为 $C=\sum_{i=0}^{N^c}P_i^{\mathrm{act}}C_i(t)$, 其中 $C_i(t)$ 由式 (8) 求得. 式 (20) ~ (23) 是关于电力系统的约束条件. Γ 是智能电网拓扑的关联矩阵, D 是线路导纳的对角矩阵. 此外, 式 (24) 和式 (25) 是网络设备的限制. 由于资源有限, 在攻击持续时间 $[1:T]$ 期间只能执行 n 次攻击动作, $\|\pi\|_0$ 代表策略 π 的 0 范数. 攻击者发动某次攻击之后信息节点 i 的攻击概率为 P_i^{act}, 其概率和为 1. 该目标函数同时考虑了电力系统和通信网络的耦合影响.

1.3.4　协同攻击建模

本节将通信−电力协同攻击建立成一个四元组 $(\boldsymbol{S},\,\boldsymbol{A},\,R,\,P)$ 的马尔科夫决策过程.

1) 状态集合 $\boldsymbol{S}=\{s_{\mathrm{I}},\, s_{\mathrm{II}},\, s_{\mathrm{III}},\, \cdots,\, s_{\mathcal{N}_S}\}$: 表示马尔科夫模型中的状态集, 其中任一状态 s 由 N^c 个通信设备的状态和 N^g 个物理设备的状态两部分组成, 分别用 s^c 和 s^g 表示. s^c 表示通信设备的状态, 该状态包括易感染态、感染态和恢复态, 见式 (1).

$$s^c=[s_1^c,\, s_2^c,\, \cdots,\, s_{N^c}^c]^{\mathrm{T}} \tag{26}$$

s^g 用来表示电力系统各个母线的电压状态量. 定义 N_θ^g 和 N_V^g 分别表示电压相角和幅值的离散状态的总数. 然后, $\hat{\theta}_j$ 和 $\hat{V}_j$ 的离散值 $\overline{\theta}_j$ 和 $\overline{V}_j$ 表示为

$$\overline{\theta}_j=\theta_j^{\min}+(q-1)\times\frac{\Delta\theta_j}{N_\theta^g} \tag{27}$$

此时, $\hat{\theta}_j\in[\theta_j^{\min}+(q-1)\times\dfrac{\Delta\theta_j}{N_\theta^g},\, \theta_j^{\min}+q\times\dfrac{\Delta\theta_j}{N_\theta^g})$.

$$\overline{V}_j=V_j^{\min}+(q-1)\times\frac{\Delta V_j}{N_V^g} \tag{28}$$

此时, $\hat{V}_j\in[V_j^{\min}+(q-1)\times\dfrac{\Delta V_j}{N_V^g},\ V_j^{\min}+q\times\dfrac{\Delta V_j}{N_V^g})$.

式 (27) 中, $\theta_j^{\min}$ 表示电压幅值量测值 $\hat{\theta}_j$ 的下界, $\theta_j^{\max}$ 表示电压幅值量测值 $\hat{\theta}_j$ 的上界, $\Delta\theta_j=\theta_j^{\max}-\theta_j^{\min}$; 式 (28) 中, $\hat{V}_j$ 同理. 离散量 $q^\theta\in\{1,\, \cdots,\, N_\theta^g\}$

且 $q^V \in \{1, \cdots, N_V^g\}$. s^g 表示离散化后的错误的量测值, 即

$$s^g = [\bar{\theta}_1, \bar{\theta}_2, \cdots, \bar{\theta}_{N^g}, \bar{V}_1, \bar{V}_2, \cdots, \bar{V}_{N^g}]^{\mathrm{T}} \tag{29}$$

因此, 系统状态表示为

$$s = \{s^c, s^g\} \tag{30}$$

2) 动作集合 $\boldsymbol{A} = \{a_{\mathrm{I}}, a_{\mathrm{II}}, a_{\mathrm{III}}, \cdots, a_{\mathcal{N}_A}\}$: 表示攻击者能够采取攻击的动作集, 针对每一个系统状态 s 均有响应的动作集 $\varphi(\pi(s))$. 攻击者的某次攻击动作 a 是对所有的通信设备的攻击概率分布, 即

$$a = [P_1^{\mathrm{act}}, P_2^{\mathrm{act}}, \cdots, P_{N^c}^{\mathrm{act}}]^{\mathrm{T}} \tag{31}$$

其中, 不在扫描集 $\phi_V(t)$ 中的通信设备的攻击概率为 0. 因为在 t 时刻攻击者无法直接或间接的扫描到该设备, 所以并不能对该设备上的漏洞加以利用. 在每个攻击时间, 选择目标节点 i 进行攻击的概率为 P_i^{act}.

3) 状态转移概率 P: 从 t 时刻的状态 s 转换到 $t+1$ 时刻的状态 s' 需要经过一个过渡状态 $\tilde{s}$, 该状态表示该时间间隔内信息层设备的病毒扩散过程结束, 但该攻击效果还没有渗透到物理设备. 由式 (18) 可以得出 $\tilde{s} \to s'$ 时信息层发生状态改变后对物理层的渗透影响. 处于状态 s 的系统采取动作 a 后状态转移到 s' 的概率定义为 $P(s'|s, a)$. $P(s'|s, a)$ 包括两部分, 分别是攻击行为 a 造成的通信层设备感染概率 $P(\tilde{s}|s, a)$ 和电力层设备注入虚假数据后不能被检测概率 $P(s'|\tilde{s})$. 值得注意的是, 这里 s' 仅与 $\tilde{s}$ 有关, 与 a 无关.

$$P(s'|s, a) = P(\tilde{s}|s, a) \times P(s'|\tilde{s}) \tag{32}$$

对受到攻击者攻击行为 a 之后的信息层设备状态转移概率和攻击者攻击概率求和, 分别可由式 (1) 和式 (32) 求得

$$P(\tilde{s}|s, a) = \prod_{i=1}^{N^c} [P(s_i^{c\prime}|s_i^c) + P_i^{\mathrm{act}}] \tag{33}$$

攻击者发动攻击后成功避开检测装置, 即攻击行为在电力层成功渗透的概率为

$$P(s'|\tilde{s}) = \prod_{j=1}^{N^g} [1 - P_j^{\mathrm{fail}}(t)] \tag{34}$$

其中, $P_j^{\mathrm{fail}}(t)$ 参考式 (13), 最终的状态转移概率由两层转移概率做积求得.

4) 奖励回报值 $R(s, a)$: 表示系统在 t 时刻 s 状态时采取 a 行动后转移到 $t+1$ 时刻 s' 状态后整个 $[0, t+1]$ 时间段内的预期奖励回报. 其定义为这段期间内攻击者的攻击成本与攻击收益的比值累积和, 即

$$R(s, a) = \mathrm{E}\left[\frac{1}{t+1}\sum_{t=0}^{t+1}\left(\frac{B(s, a)}{C(s, a)}\right)\right] = \sum_{s' \in s_{\mathcal{N}_S}} P(s'|s, a)R(s'|s, a) \tag{35}$$

2 基于 Q-learning 的模型求解

本文使用 Q 学习求解所提的协同攻击模型下的最优攻击策略. 首先采用 Q-learning 的方法根据攻击者目标函数求得最优策略. 目标函数可由式 (19) 求得. 最后分析在该最优攻击策略下各个电力设备被攻击的可能性, 由此可以识别电力系统的薄弱节点.

2.1 Q-learning 求解过程

基于 Q-learning 的攻击者最优攻击路径求解的基本思路为: 攻击者根据 Reward 奖励值反馈或惩罚刺激下, 逐步修正自己的攻击策略 π, 最终求解在有限攻击资源下最大化预期总奖励的最优攻击策略, 即

$$Q_\pi = \sum_{t=0}^{T} \gamma^{t-1} R(s, \pi(s)) \tag{36}$$

其中, γ 为折算因子, $\gamma \in [0, 1)$. 由于信息网络路由选择概率和网络延迟等原因, 其中求解 $R(s, \pi(s))$ 所需要的 $P(\tilde{s}|s, a)$ 不能直接求得, 见式 (32). 所以本文使用 NS2 软件通过蒙特卡洛方法模拟大量的信息网络状态过程求得. 接下来, 在 s 下最优攻击策略 π^* 可以通过下式计算:

$$\pi^*(s) = \arg\max_a Q^*(s, a) \tag{37}$$

为了避免局部最优的出现, 许多随机动作序列将被搜索以更新 Q 表, 在此期间, 攻击者动作序列最终会被修改为最佳攻击策略, 即

$$Q(s, a) \leftarrow (1-\alpha) \times Q(s, a) + \alpha \times [R(s, a) + \gamma \times \max_a Q(s', a)] \tag{38}$$

其中, α 是学习速率. 最终, 该最优攻击策略相当于攻击者的一个预判行为, 通过该预判行为可以分析哪些电力元件成为攻击者攻击目标的可能性更大, 能够对防御资源的分配起到指导作用.

在制定状态−动作 Q 矩阵时, 由于变量之间存在关联关系, 所以许多系统状态在整个探索过程中均未出现. 如果使用传统的 Q 矩阵, 随着变量的增加, 状态集和动作集均会呈指数增长, 最终导致运算速率过慢. 因此, 本文将传统的静态稀疏 Q 矩阵

转换为动态更新的满秩 Q 矩阵, 以加快运算速率并节约存储空间.

2.2　电力元件被攻击的可能性分析

在求得最优策略下, 根据各个电力设备被攻击的可能性, 研究相应节点的特性, 并指导相关的防御行为. 因为马尔科夫决策过程的状态转移概率存在随机性, 所以攻击者采取相同的攻击策略时, 导致电力信息物理系统的破坏程度也存在随机性[19]. 基于此, 首先定义在马尔科夫决策过程中系统状态为 s_X 时, 状态分布概率为

$$H_r(s_X) \approx \frac{\sum\limits_{h_y \in \Phi(h)} l_{s_X \in h_y(\pi^*)}}{\sum\limits_{h_y \in \Phi(h)} \|\pi\|_0} \tag{39}$$

其中, 第 y 次测试时攻击者发动 n 次攻击行为, 这期间的状态转移序列集 $\{s_{y1}, s_{y2}, \cdots, s_{yn}\}$ 用 h_y 来表示. $\Phi(h)$ 代表系统所有状态转移序列集的集合. $h_y(\pi^*)$ 代表最优策略下的序列集. 在测试过程中, 状态的分布概率满足 $\sum_{s_X \in s_{\mathcal{N}_S}} H_r(s_X) = 1$, l_x 和 $\|\pi\|_0$ 可由式 (18) 求得. 接下来, 定义电力母线 j 在攻击者最优策略下的被攻击的可能性为

$$H_b(j) \approx \frac{\sum\limits_{s_X \in \psi(s)} l_{[j \in \varphi(\pi^*(s_X))]} \cdot H_r(s_X)}{\sum\limits_{s_X \in \psi(s)} H_r(s_X)} \tag{40}$$

其中, $\psi(s)$ 代表全部测试结果中出现的系统状态的集合, $\varphi(\pi^*(s_X))$ 表示在 s_X 状态采取最优攻击动作 a^* 之后被成功渗透的电力节点的集合, 如果节点 j 属于该集合, 那么 $l_{[j \in \varphi(\pi^*(s_X))]}$ 的值为 1, 电力节点被攻击的可能性最大, 防御者应该在该节点处分配更多的防御资源.

3　算例分析

3.1　仿真模型与参数设置

如图 5 所示, 本模型在一个通信 8 节点−电力 IEEE14 节点的耦合系统上进行测试, 该算例系统由两部分组成, 上层通信层由 8 个通信设备 C-n 组成, 下层电力层是 IEEE14 节点系统, 该通信网络服务于电力系统的状态估计功能. 当攻击者发动远程网络攻击时, 病毒在通信网络节点之间以蠕虫形式传播, 将虚假数据注入通信设备. 在该算例系统中, 通信网络使用 NS2 软件仿真, 该软件可以考虑更多实际情况, 如链路阻塞、丢包等过程, 仿真结果更加准确. 该算例系统在参数设置时采用 UDP 协议和自带的单播路由协议, 并选择具有代表性的已

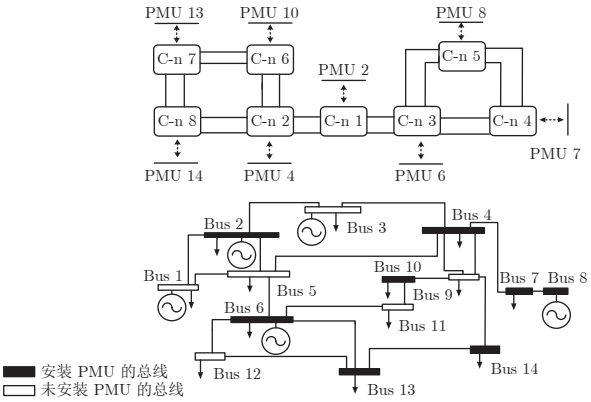


图 5　通信 8 节点−电力 IEEE14 节点耦合系统

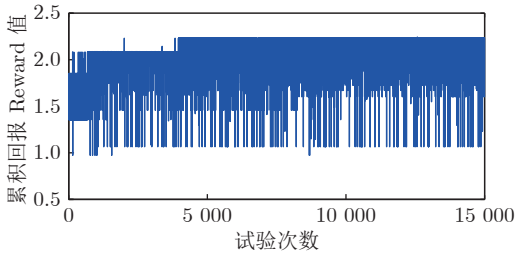
Fig. 5　Cyber 8-Power IEEE14 node coupling system

经公开的 PLC 机上的漏洞, 相关的通信网络参数见附录 A, 其中移除率和恢复率分别为 0.001 和 0.01 (参见文献 [4]). 为了使实验结果更直观, 做出以下假设:

假设 1. 攻击者动作集合均采用单层攻击目标的动作, 即攻击目标为 i 时, $P_i^{\text{act}} = 1$ 且 $P_{i \neq j}^{\text{act}} = 0$.

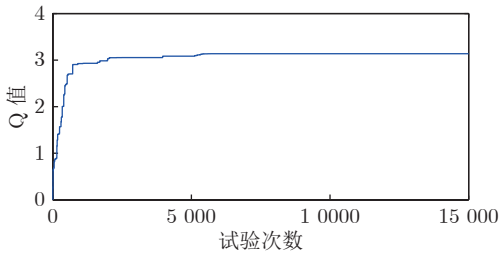
假设 2. 电力节点和信息节点是一一对应的, 电压量测值允许的偏差为 ±5%, 单次修改的虚假数据为原始量测值的 ±1%.

Q-learning 算法的每一个训练周期都是从攻击者发动攻击开始. 在算例系统上进行 15 000 次仿真训练, 每次训练都设置的时间间隔为 $T = 3\Delta t$, 其中攻击间隔取值 $\Delta t = 1$ s[19]. 其目标是寻找最优攻击策略, 以获得最大的积累回报值. 图 6(a) 显示了每



(a) 每个训练周期的积累回报值

(a) Accumulated reward for each trial



(b) 每个训练周期的 Q 值

(b) Q value for each trial

图 6　每个训练周期的累积收益

Fig. 6　Accumulated benefit for each trial

次训练中采用不同的攻击策略的累积奖励. 整个搜索的过程可分为 3 个部分: 起始状况、局部最优和全局最优. 截止到 886 次测试时, 攻击者累积奖励没有显著增加, 保持其初始值为 1.783. 从 887 次训练开始, 积累奖励值从 1.783 迅速增加到 2.156, 即找到了局部最优解. 然后在 3962 次训练时, 累积奖励从 2.156 急剧增加到 2.242, 即找到全局最优解. 3963 次训练之后, 奖励值保持稳定并且仍然是最大值, 这意味着确定了最优攻击策略. 同时, 随着训练次数的增加, 图 6(b) 显示经过大量训练之后 Q 值趋于恒定, 这表明已经搜索到最优的攻击策略.

在本节的算例仿真中, 攻击者最优策略下的攻击序列为 C-n 4→C-n 2→C-n 1, 映射到电力系统中为 Bus 7→Bus 4→Bus 2, 每一次攻击行为之后蠕虫病毒在通信网络的扩散情况如图 7 所示.

图 8 横坐标从左到右分别是初始状况、攻击者第 1 次攻击动作后、第 2 次攻击动作后和第 3 次攻击动作后. 纵坐标表示在最优的攻击策略下估计状态值偏差的百分比, 即式 (16) 的值.

可以推断, 如果只修改一个母线的测量值, 则可能由检测机制检测并且能够被校正; 如果攻击者同时修改某条母线及其相邻母线的测量值, 就会使估计器无法检测到错误数据, 从而使估计误差变大. 在该算例中电力母线 4 受到攻击的可能性最大, 是系统中较为薄弱的环节, 在防御者进行资源分配的时候应该优先考虑.

3.2 结果分析

为了验证本文提出的协同攻击具有更好的攻击效果, 这里对网络攻击、物理攻击和信息物理协同攻击 3 种不同攻击方法的攻击效果进行仿真实验, 对比结果如表 1 所示. 其中, n 表示发动攻击的次数. 网络攻击指的是攻击者的目标是只考虑信息层攻击成本最小, 不考虑电力系统的破坏程度; 物理攻击指的是传统的电力系统攻击研究, 即假设在通信层量测设备能够无差别地被攻击者篡改的条件下, 攻击者目标是对电力系统破坏程度最大.

从表 1 可以看出, 协同攻击在 3 种攻击方法中表现最好, 物理攻击次之, 网络攻击最差. 其中, π^* 表示当前攻击者的最优攻击策略, $\boldsymbol{e}_{xz}$ 表示估计状态值的误差, $f(\Delta V)$ 表示电压幅值偏差百分比的累积量, $f(\Delta\theta)$ 表示电压相位角的偏差百分比的累积量. 需要注意的是, 当攻击者采用网络攻击时, 每个物理节点的攻击回报值设置为 1. 随着攻击时间的增加, 协同攻击的有效性变得更加显著. 由此可见, 当攻击者只考虑利用信息节点漏洞的利用能力时, 虽然受感染的网络节点数量在短时间内增加, 但对电力网络的影响很小. 此外, 单纯的物理攻击可能效果不佳, 这是因为与某些关键电力节点相连接的通信网络节点在通信层难以得到利用.

表 2 对比了在协同攻击和物理攻击下各个电力设备被攻击的可能性, 概率和为 1. 由分析可知, 当考虑到通信层设备的影响时, 与在通信网络中更脆弱的信息设备相连接的电力设备的脆弱性显著增加, 且边缘信息设备的脆弱性与该设备在通信网络中连接度的大小和元件上存在的漏洞的利用难易程度相关. 例如: 采用物理攻击时, 母线 10 的脆弱性最高, 因为连接母线 10 和母线 9 的电力线具有比其他支路更小的电抗. 当虚假数据注入母线 10 的测量值时, 状态估计器的估计结果将具有更大的误差. 当采用协同攻击时, 母线 2 (对应通信设备 1) 的量测值被篡改的概率急剧增加. 主要有两个原因: 1) 母线 2 是电力网络中较为关键的节点; 2) 通信设备 C-n 1 在通信网络中具有较大的连接度, 当其被成功感染时, 其相邻网络设备 C-n 2 和 C-n 3 的攻击概率将显著增加. 随着时间的推进, 与 C-n 2 和 C-n 3

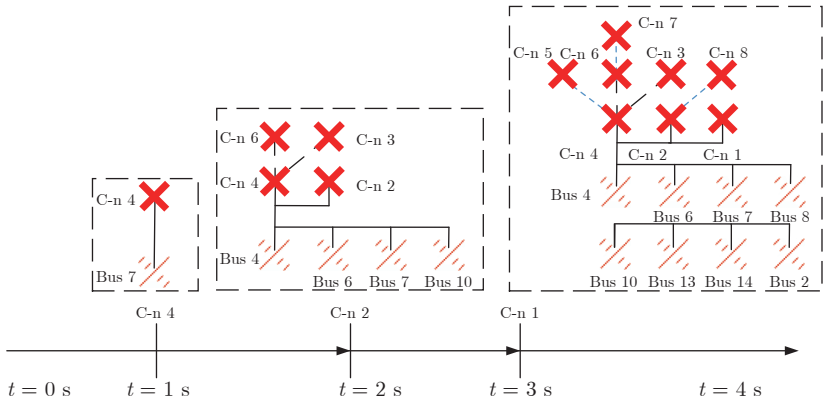


图 7 最优攻击策略下攻击者的攻击序列和病毒扩散序列

Fig. 7 The attack sequence and virus spreading sequence under the optimal attack strategy

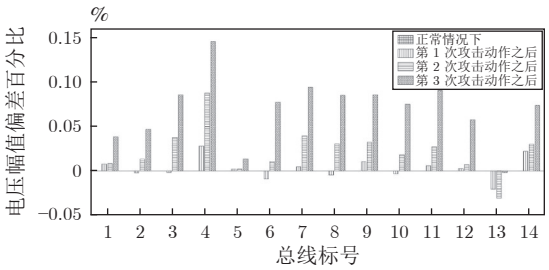


图 8　在最优攻击策略下电压幅值差百分比

Fig. 8　Difference percentage in voltage amplitude under optimal attack strategy

表 1　考虑不同攻击方法下的影响

Table 1　Attack effect under different attack methods

攻击类型	参数	$n=1$	$n=2$	$n=3$
网络攻击	π^*	1	$2\to3$	$2\to3\to4$
	$f(\Delta\theta)$	0.022	0.103	0.2333
	$f(\Delta V)$	0.043	0.115	0.245
物理攻击	π^*	4	$5\to6$	$5\to4\to7$
	$f(\Delta\theta)$	0.035	0.144	0.344
	$f(\Delta V)$	0.061	0.134	0.444
协同攻击	π^*	3	$6\to7$	$2\to4\to8$
	$f(\Delta\theta)$	0.077	0.223	0.523
	$f(\Delta V)$	0.062	0.267	0.667

邻接的通信设备将陆续被感染, 从而扩散到整个通信网络.

3.3　不同参数对攻击效果的影响

本节讨论系统的离散程度和注入虚假数据的正负是否对协同攻击效果有影响.

3.3.1　系统离散程度对攻击结果的影响

对于算例系统, 当各个母线的电压幅度和角度的离散状态的数目 N_V^g 和 N_θ^g 的值在 4 ~ 8 的范围内发生变化时攻击效果如表 3 所示.

由表 3 推断, 当系统状态离散情况发生变化时, 算例系统中每条母线的脆弱性几乎没有变化.

3.3.2　注入虚假数据的正负对攻击结果的影响

对于算例系统, 当 $\boldsymbol{e}_z=[\boldsymbol{e}_\theta,\boldsymbol{e}_V]^{\mathrm{T}}$ 的数值取正值、负值或者混合符号数据时, 攻击效果如图 9 所示.

由图 9 推断, 注入的假数据的符号不同对算例系统中每条物理母线脆弱性影响不大.

表 2　电力设备被攻击可能性分析 (%)

Table 2　The vulnerability analysis of power equipment (%)

通信−电力	节点耦合	协同攻击	物理攻击
C-n 1	Bus 2	31.65	16.66
C-n 2	Bus 4	32.51	16.40
C-n 3	Bus 6	30.60	11.27
C-n 4	Bus 7	0.67	15.26
C-n 5	Bus 8	0.85	5.97
C-n 6	Bus 10	1.00	19.54
C-n 7	Bus 13	1.44	8.70
C-n 8	Bus 14	1.25	6.20

4　结束语

本文从攻击者角度出发, 提出了一种电力信息物理协同攻击模型, 该模型同时考虑通信层设备的攻击难易程度以及对电力物理系统的破坏程度两方面因素. 然后, 本文结合通信层和电力层设备的特性, 制定攻击成本和攻击收益函数, 并定义攻击收益与成本的比值为目标函数. 随后, 采用 Q-learning 求解所提模型下的目标函数最大的最优攻击策略. 最后, 利用通信 8 节点−电力 IEEE14 节点联合仿真算例对单层网络攻击、物理攻击和协同攻击方式的攻击效果进行对比, 并分析了元件被攻击的可能性, 得到的结论如下: 1) 本文所提出的信息物理双层协同攻击模型可以准确地描述攻击行为在电力信息物理系统中的动态攻击效果和级联影响; 2) 通过算例研究, 验证了相较网络攻击和物理攻击, 本文所提的协同攻击由于同时考虑通信层设备的利用难度和电力设备的破坏程度两方面因素的耦合影响, 所以攻击效果更好, 物理攻击次之, 网络攻击效果最差; 3) 由仿真结果分析可得, 由于电力信息物理系统的通信层和电力层设备存在复杂的耦合关系和交互机理, 所以通信层元件利用的难易程度和通信网络结构对电力设备潜在被攻击的可能性存在显著影响.

表 3　系统离散程度不同时电力设备被攻击的可能性分析

Table 3　The vulnerability analysis of power equipment under different discrete degrees of false data

离散状态数目	各个电力设备被攻击的可能性分析 (%)							
母线标号	Bus 2	Bus 4	Bus 6	Bus 7	Bus 8	Bus 10	Bus 13	Bus 14
$N_V^g=N_\theta^g=4$	7.18	20.88	13.36	18.25	6.54	16.03	9.02	6.31
$N_V^g=N_\theta^g=6$	8.31	19.95	12.97	17.66	6.43	17.38	10.50	6.80
$N_V^g=N_\theta^g=8$	8.11	20.45	12.27	17.66	6.97	17.54	9.70	7.20

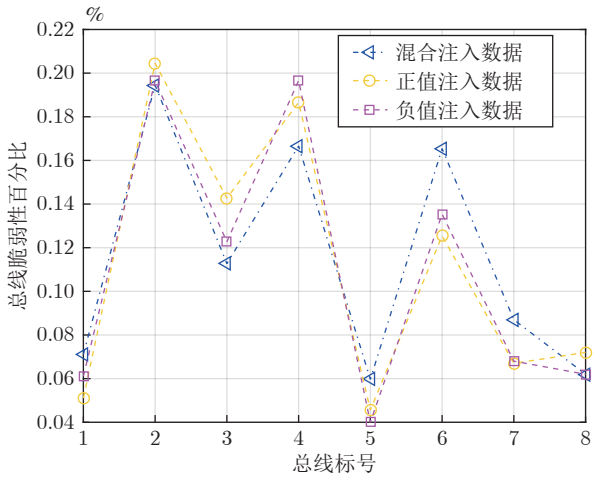


图 9 注入虚假数据取不同符号下电力设备被攻击的可能性分析

Fig. 9 The vulnerability analysis of power equipment under different signs of false data

附录 A

表 A1 NS2 中通信网络的参数配置

Table A1 The parameters of cyber network in NS2

起点	终点	带宽 (Mbps)	时延 (ms)
C-n 1	C-n 2	60	60
C-n 2	C-n 6	60	20
C-n 2	C-n 8	60	20
C-n 7	C-n 8	60	20
C-n 7	C-n 6	60	20
C-n 1	C-n 3	60	60
C-n 3	C-n 4	60	20
C-n 3	C-n 5	60	20
C-n 4	C-n 5	60	20

表 A2 每个通信设备上存在的漏洞的 CVSS 评分

Table A2 The CVSS standards of each cyber node

标号	漏洞 ID 标号	影响度量分数	漏洞利用分数	基础分数
C-n 1	CVE-2016-8366	3.4	3.9	7.3
C-n 2	CVE-2016-8366	3.4	3.9	7.3
C-n 3	CVE-2016-8366	3.4	3.9	7.3
C-n 4	CVE-2017-14470	2.7	2.8	5.5
C-n 5	CVE-2017-14470	2.7	2.8	5.5
C-n 6	CVE-2017-14470	2.7	2.8	5.5
C-n 7	CVE-2018-16210	5.9	3.9	9.8
C-n 8	CVE-2018-16210	5.9	3.9	9.8

References

1 Wang Bing-Yu, Sun Qiu-Ye, Ma Da-Zhong, Huang Bo-Nan. A cyber physical model of the energy internet based on multiple time scales. *Automation of Electric Power Systems*, 2016, **40**(17): 13–21
(王冰玉, 孙秋野, 马大中, 黄博南. 能源互联网多时间尺度的信息物理融合模型. 电力系统自动化, 2016, **40**(17): 13–21)

2 Liu Ting, Tian Jue, Wang Jia-Zhou, Wu Hong-Yu, Sun Li-Min, Zhou Ya-Dong, et al. Integrated security threats and defense of cyber-physical systems. *Acta Automatica Sinica*, 2019, **45**(1): 5–24
(刘烃, 田决, 王稼舟, 吴宏宇, 孙利民, 周亚东, 等. 信息物理融合系统综合安全威胁与防御研究. 自动化学报, 2019, **45**(1): 5–24)

3 Mo Y C, Xing L D, Zhong F R, Zhang Z. Reliability evaluation of network systems with dependent propagated failures using decision diagrams. *IEEE Transactions on Dependable and Secure Computing*, 2016, **13**(6): 672–683

4 Yao Y, Sheng C, Fu Q, Liu H X, Wang D J. A propagation model with defensive measures for PLC-PC worms in industrial networks. *Applied Mathematical Modelling*, 2019, **69**: 696–713

5 Wang Xian-Pei, Tian Meng, Dong Zheng-Cheng, Zhu Guo-Wei, Long Jia-Chuan, Dai Dang-Dang, et al. Survey of false data injection attacks in power transmission systems. *Power System Technology*, 2016, **40**(11): 3406–3414
(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. 电网技术, 2016, **40**(11): 3406–3414)

6 Hug G, Giampapa J A. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *IEEE Transactions on Smart Grid*, 2012, **3**(3): 1362–1370

7 Wang Qi, Tai Wei, Tang Yi, Ni Ming. A review on false data injection attack toward cyber-physical power system. *Acta Automatica Sinica*, 2019, **45**(1): 72–83
(王琦, 邰伟, 汤奕, 倪明. 面向电力信息物理系统的虚假数据注入攻击研究综述. 自动化学报, 2019, **45**(1): 72–83)

8 Xiang Y M, Wang L F, Liu N. Coordinated attacks on electric power systems in a cyber-physical environment. *Electric Power Systems Research*, 2017, **149**: 156–168

9 Yang Fei-Sheng, Wang Jing, Pan Quan, Kang Pei-Pei. Resilient event-triggered control of grid cyber-physical systems against cyber attack. *Acta Automatica Sinica*, 2019, **45**(1): 110–119
(杨飞生, 汪璟, 潘泉, 康沛沛. 网络攻击下信息物理融合电力系统的弹性事件触发控制. 自动化学报, 2019, **45**(1): 110–119)

10 Deng R L, Zhuang P, Liang H. CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid. *IEEE Transactions on Smart Grid*, 2017, **8**(5): 2420–2430

11 Guo Qing-Lai, Xin Shu-Jun, Wang Jian-Hui, Sun Hong-Bin. Comprehensive security assessment for a cyber physical energy system: A lesson from Ukraine′s blackout. *Automation of Electric Power Systems*, 2016, **40**(5): 145–147
(郭庆来, 辛蜀骏, 王剑辉, 孙宏斌. 由乌克兰停电事件看信息能源系统综合安全评估. 电力系统自动化, 2016, **40**(5): 145–147)

12 Liang G Q, Weller S R, Zhao J H, Luo F J, Dong Z Y. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 2017, **32**(4): 3317–3318

13 Korkali M, Veneman J G, Tivnan B F, Bagrow J P, Hines P D H. Reducing cascading failure risk by increasing infrastructure network interdependence. *Scientific Reports*, 2017, **7**: Article No. 44499

14 Buldyrev S V, Parshani R, Paul G, Stanley H E, Havlin S. Catastrophic cascade of failures in interdependent networks. *Nature*, 2010, **464**(7291): 1025–1028

15 Tang Yi, Han Xiao, Wu Ying-Jun, Ju Yong, Zhou Xia, Ni Ming. Electric power system vulnerability assessment considering the influence of communication system. *Proceedings of the CSEE*, 2015, **35**(23): 6066–6074
(汤奕, 韩啸, 吴英俊, 鞠勇, 周霞, 倪明. 考虑通信系统影响的电力系统综合脆弱性评估. 中国电机工程学报, 2015, **35**(23): 6066–6074)

16 Tian Meng, Dong Zheng-Cheng, Wang Xian-Pei, Zhao Le, Jian Zi-Ni. Analysis of electrical coordinated cyber physical attacks

under goal conflict. *Power System Technology*, 2019, **43**(7): 2336−2344
(田猛, 董政呈, 王先培, 赵乐, 简子倪. 目标冲突下电力信息物理协同攻击分析. 电网技术, 2019, **43**(7): 2336−2344)

17 Liu X, Li Z Y, Liu X D, Li Z Y. Masking transmission line outages via false data injection attacks. *IEEE Transactions on Information Forensics and Security*, 2016, **11**(7): 1592−1602

18 Zhang J Z, Sankar L. Physical system consequences of unobservable state-and-topology cyber-physical attacks. *IEEE Transactions on Smart Grid*, 2016, **7**(4): 2016−2025

19 Hao Y S, Wang M, Chow J H. Likelihood analysis of cyber data attacks to power systems with Markov decision processes. *IEEE Transactions on Smart Grid*, 2018, **9**(4): 3191−3202

20 Duan J, Chow M Y. A novel data integrity attack on consensus-based distributed energy management algorithm using local information. *IEEE Transactions on Industrial Informatics*, 2019, **15**(3): 1544−1553

21 Sun Qiu-Ye, Yang Ling-Xiao, Zhang Hua-Guang. Smart energy-applications and prospects of artificial intelligence technology in power system. *Control and Decision*, 2018, **33**(5): 938−949
(孙秋野, 杨凌霄, 张化光. 智慧能源−人工智能技术在电力系统中的应用与展望. 控制与决策, 2018, **33**(5): 938−949)

22 Yan J, He H B, Zhong X N, Tang Y F. Q-learning-based vulnerability analysis of smart grid against sequential topology attacks. *IEEE Transactions on Information Forensics and Security*, 2017, **12**(1): 200−210

23 Shi Li-Bao, Jian Zhou. Vulnerability assessment of cyber physical power system based on dynamic attack-defense game model. *Automation of Electric Power Systems*, 2016, **40**(17): 99−105
(石立宝, 简洲. 基于动态攻防博弈的电力信息物理融合系统脆弱性评估. 电力系统自动化, 2016, **40**(17): 99−105)

24 Wei L F, Sarwat A I, Saad W, Biswas S. Stochastic games for power grid protection against coordinated cyber-physical attacks. *IEEE Transactions on Smart Grid*, 2018, **9**(2): 684−694

25 Zhou Yan-Heng, Wu Jun-Yong, Zhang Guang-Tao, Miao Qing, Qu Bo, Hu Yan-Mei. Assessment on power system vulnerability considering cascading failure. *Power System Technology*, 2013, **37**(2): 444−449
(周彦衡, 吴俊勇, 张广韬, 苗青, 屈博, 胡艳梅. 考虑级联故障的电力系统脆弱性评估. 电网技术, 2013, **37**(2): 444−449)

26 Langner R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 2011, **9**(3): 49−51

27 Warda H, Zhioua S, Almulhem A. PLC access control: A security analysis. In: Proceedings of the 2016 World Congress on Industrial Control Systems Security (WCICSS). London, UK: IEEE, 2016.

28 Ye Xia-Ming, Wen Fu-Shuan, Shang Jin-Cheng, He Yang. Propagation mechanism of cyber physical security risks in power systems. *Power System Technology*, 2015, **39**(11): 3072−3079
(叶夏明, 文福拴, 尚金成, 何洋. 电力系统中信息物理安全风险传播机制. 电网技术, 2015, **39**(11): 3072−3079)

29 Tarali A, Abur A. Bad data detection in two-stage state estimation using phasor measurements. In: Proceedings of the 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT). Berlin, Germany: IEEE, 2012.

30 Wang X A, Shi D, Wang J H, Yu Z, Wang Z W. Online identification and data recovery for PMU data manipulation attack. *IEEE Transactions on Smart Grid*, 2019, **10**(6): 5889−5898

31 Beasley C, Zhong X S, Deng J, Brooks R, Venayagamoorthy G K. A survey of electric power synchrophasor network cyber security. In: Proceedings of the 2014 IEEE PES Innovative Smart Grid Technologies, Europe (ISGT). Istanbul, Turkey: IEEE, 2014. 1−5

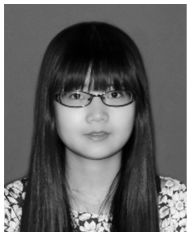
32 Li Qiang, Zhou Jing-Yang, Yu Er-Keng, Liu Shu-Chun, Wang Lei. Power system linear state estimation based on phasor measurement. *Automation of Electric Power Systems*, 2005, **29**(18): 24−28
(李强, 周京阳, 于尔铿, 刘树春, 王磊. 基于相量量测的电力系统线性状态估计. 电力系统自动化, 2005, **29**(18): 24−28)

33 Li P K, Liu Y, Xin H H, Jiang X C. A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks. *IEEE Transactions on Industrial Informatics*, 2018, **14**(10): 4343−4352

34 Liang J W, Sankar L, Kosut O. Vulnerability analysis and consequences of false data injection attack on power system state estimation. *IEEE Transactions on Power Systems*, 2016, **31**(5): 3864−3872

冯晓萌 东北大学信息科学与工程学院硕士研究生. 主要研究方向为电力信息物理系统建模及安全防御.
E-mail: fengxiaomeng12345@outlook.com
(**FENG Xiao-Meng** Master student at the School of Information Science and Engineering, Northeastern University. Her research interest covers cyber security for cyber-physical power system.)

孙秋野 东北大学信息科学与工程学院教授. 主要研究方向为网络控制技术, 分布式控制技术, 分布式优化分析及其在能源互联网、微网、配电网等领域相关应用. 本文通信作者.
E-mail: sunqiuye@mail.neu.edu.cn
(**SUN Qiu-Ye** Professor at the School of Information Science and Engineering, Northeastern University. His research interest covers network control technology, distributed control technology, distributed optimization analysis and various applications in energy internet, microgrid, and power distribution network. Corresponding author of this paper.)



王冰玉 东北大学信息科学与工程学院博士研究生. 主要研究方向为信息物理能源系统, 微电网控制和多智能体系统.
E-mail: 1610266@stu.neu.edu.cn
(**WANG Bing-Yu** Ph.D. candidate at the School of Information Science and Engineering, Northeastern University. Her research interest covers cyber-physical energy system, control strategy of microgrid, and multiagent systems.)

高嘉文 东北大学信息科学与工程学院硕士研究生. 主要研究方向为电力信息物理系统建模及安全防御.
E-mail: helensun0708@outlook.com
(**GAO Jia-Wen** Master student at the School of Information Science and Engineering, Northeastern University. His research interest covers cyber security for cyber-physical power system.)