基于贝叶斯序贯博弈模型的智能电网信息物理安全分析

李 军[1] 李 韬[2]

摘 要 智能电网是利用信息技术优化从供应者到消费者的电力传输和配电网络. 作为一种信息物理系统 (Cyber-physical system, CPS), 智能电网由物理设备和负责数据计算与通信的网络组成. 智能电网的诸多安全问题会出现在通信网络和物理设备这两个层面, 例如注入坏数据和收集客户隐私信息的网络攻击, 攻击电网物理设备的物理攻击等. 本文主要研究了智能电网的系统管理员 (防护者) 如何确定攻击者类型, 从而选择最优防护策略的问题. 提出了一种贝叶斯序贯博弈模型以确定攻击者的类型, 根据序贯博弈树得到博弈双方的均衡策略. 首先, 对类型不确定的攻击者和防护者构建静态贝叶斯博弈模型, 通过海萨尼转换将不完全信息博弈转换成完全信息博弈, 得到贝叶斯纳什均衡解, 进而确定攻击者的类型. 其次, 考虑攻击者和防护者之间的序贯博弈模型, 它能够有效地帮助防护者进行决策分析. 通过逆向归纳法分别对两种类型的攻击者和防护者之间的博弈树进行分析, 得到博弈树的均衡路径, 进而得到攻击者的最优攻击策略和防护者的最优防护策略. 分析表明, 贝叶斯序贯博弈模型能够使防护者确定攻击者的类型, 并且选择最优防护策略, 从而为涉及智能电网信息安全的相关研究提供参考.

关键词 信息物理系统, 智能电网安全, 网络攻击, 物理攻击, 贝叶斯序贯博弈

引用格式 李军, 李韬. 基于贝叶斯序贯博弈模型的智能电网信息物理安全分析. 自动化学报, 2019, **45**(1): 98−109

DOI 10.16383/j.aas.2018.c180336

Cyber-physical Security Analysis of Smart Grids With Bayesian Sequential Game Models

LI Jun[1] LI Tao[2]

Abstract A smart grid is a network which uses communication and information technologies to optimize the transmission and distribution of power from suppliers to consumers. As a kind of cyber-physical system (CPS), a smart grid consists of the network part of data computing and communication and the physical part of all devices. Many security issues arise in both components of the grid, such as injecting bad data, collecting customer privacy information (cyber attacks) and attacking the grid physical devices (physical attacks). In this paper, we study how the system administrator (defender) can determine the type of attack and make optimal protection strategy. We propose a Bayesian sequential game model to defermine the type of attack, and analyze the equilibrium strategy of both game sides according to the sequential game tree. Firstly, we construct a static Bayesian game model between the attacker of an indeterminate type and the defender. We transform the incomplete information game into a complete information game through Harsanyi transformation, and analyze the Bayesian Nash equilibrium to determine the type of attacker. Secondly, we consider the sequential game model between attackers and defenders, which can effectively help defender to make decision in dynamic networks. Through the backward induction, the game tree is analyzed between two types of attackers and defenders, respectively. Then we obtain the equilibrium path of the game tree and make the optimal strategies for both players. It is shown that the defender can determine the type of attacker and make the optimal strategy by the Bayesian sequential game model, which provides a reference for the security research on smart grids.

Key words Cyber-physical system (CPS), smart grid security, cyber attack, physical attack, Bayesian sequential game

Citation Li Jun, Li Tao. Cyber-physical security analysis of smart grids with Bayesian sequential game models. *Acta Automatica Sinica*, 2019, **45**(1): 98−109

收稿日期 2018-05-29 录用日期 2018-09-14
Manuscript received May 29, 2018; accepted September 14, 2018
国家自然科学基金 (61522310) 资助
Supported by National Natural Science Foundation of China (61522310)
本文责任编委 孙秋野
Recommended by Associate Editor SUN Qiu-Ye
1. 上海大学机电工程与自动化学院 上海 200444 2. 华东师范大学数学科学学院, 上海市核心数学与实践重点实验室 上海 200241
1. School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444 2. Key Laboratory of Pure Mathematics and Mathematical Practice, School of Mathematical Sciences, East China Normal University, Shanghai 200241

计算机、网络通信和控制技术作为近 30 年来信息技术产业发展的核心和动力, 引起了人类社会生活的巨大变革. 然而, 人与自然万物, 以及改造自然的机器之间, 尚缺乏有效地交互协同的作用方式, 需要统一的混合系统框架, 通过对质量流、能量流、信息流的协调管控, 推动计算机、网络通信和控制技术的协同变革和演进融合. 在这一背景下, 信息物理系统 (Cyber-physical systems, CPS)[1−3] 应运而生. 信息物理系统这一概念是由美国科学家 Gill 于

2006 年在美国国家科学基金委员会上提出的[4], 被认为有望成为继计算机、互联网之后世界信息技术的第三次浪潮, 其核心是 3Cs (Computation, communication, control) 的融合. 智能电网作为一种信息物理系统[5], 将 3Cs 技术融合贯穿于发电、输电、配电和用电四大环节, 用以提升电网的各项性能指标, 包括稳定性、有效性、可靠性、安全性等. 对于发电环节而言, 由于风能、太阳能等可再生能源的接入, 导致了电网系统的不确定性增大, 影响了电网的稳定性. CPS 可以协调多能源介质的生产、存储和使用, 确保电网稳定运行, 实现安全节能优化目标. 在输电环节, CPS 可以帮助构建输电线路智能化无人机巡检, 精确导航与控制技术、长距离实时稳定通信技术和计算中心实时数据分析, 确保线路巡检诊断精确可靠. 在智能配电环节, 融合了 3Cs 技术的智能电表通过与配电侧的互联, 给用户提供实时电价, 以实现负载优化调度. 在用电环节, CPS 及相关技术可以准确预测用户用电消费行为及需求, 实时感知、计算并响应调控用电变化, 实现全系统的智能优化和精准控制, 极大地提高了电力的安全生产和消费的效率[6−7].

智能电网承诺提供更高的效率和可靠性, 以及更节约的配电和输电的方法. 这些提升方法依赖于新技术和电力网络中心建立的互联机制, 同时也依赖于不同组件的合作和大量的数据分析. 随着新技术和更容易获取的能源数据的使用, 智能电网将受到多种攻击的威胁, 安全性变得尤为重要. 智能电网可分为网络基础设施和物理基础设施[8−9] 两个主要组件. 网络基础设施包括服务器、数据库、人机接口 (Human machine interface, HMI)、远程终端设备 (Remote terminal unite, RTU)、可编程逻辑控制器 (Programmable logic controller, PLC) 以及监测控制和数据采集 (Supervisory control and data acquisition, SCADA) 系统等. 物理基础设施包括负责发电、输电、配电、用电的物理设备等. 对应于智能电网的这两个主要组件, 攻击者有网络攻击和物理攻击两种类型. 网络攻击者通过攻击智能电网的网络系统, 获得未经授权的特权来控制物理过程的功能. 物理攻击者通过攻击智能电网的物理设备, 导致电网在发电、输电、配电、用电等环节中断以及电力系统拓扑结构的改变等[10−11]. 当系统受到攻击时, 若系统管理员 (防护者) 事先不确定攻击者的类型, 则无法给出最优防护策略. 针对这种问题, 本文提出了一种贝叶斯序贯博弈模型, 可以确定攻击者的类型, 从而选择最优防护策略, 为系统管理员及时提供决策分析, 保持智能电网的安全运行.

目前对于智能电网的安全性研究大部分关注的是网络安全方面, 包括智能电网的安全需求、目标、可能存在的漏洞、攻击和解决方案等[12−13]. 由于智能电网在网络方面容易受到攻击, 导致系统运行不可靠, 对消费者和公司都造成危害, 所以智能电网的分布式通信、普适计算和传感技术都需要一个安全的网络框架. 孙秋野等[14] 指出, 能源互联网作为一个融合信息系统与物理能源系统的综合复杂网络, 控制优化相对复杂, 且因与互联网的相似性, 使得能源互联网信息物理安全将成为网络研究热点问题之一. Luo 等[15] 研究了虚假数据注入攻击下, 大规模智能电网系统的网络安全问题, 提出了一种基于观测器的算法, 通过使用实时同步相量测量来检测和隔离网络攻击. Yan 等[16] 对智能电网的通信安全进行了研究, 总结了智能电网通信过程中的网络安全需求和漏洞, 并调查了当前网络安全解决方案. Hasan 等[17] 研究了资源受限的智能电网中的网络安全规划问题, 为能源 SCADA 系统提出了一个基于中心的信任系统配置方案, 利用中心性测量提升安全保护. Mo 等[18] 考虑了如何结合物理系统安全和网络安全建立一个科学的信息物理安全系统, 确保智能电网安全运行. 虽然单一网络攻击和单一物理攻击方面的安全性研究已经取得显著成绩, 但是对于同时存在网络攻击和物理攻击的混合攻击情形, 现有的研究还比较缺乏.

近年来使用博弈论分析智能电网安全的研究越来越多[19]. Hewett 等[20] 在攻击者和安全管理者之间构建了双人非零和的完全信息动态博弈, 通过逆向归纳法求出纳什均衡解. 当系统遭遇攻击时, 防护者根据纳什均衡解能够及时地做出准确的决策. Maharjan 等[21] 提出了一种公用事业公司和终端用户之间的斯塔克伯格博弈方法, 分析了智能电网的需求响应管理, 最大化事业公司的收入和每个用户的收益. Ma 等[22] 利用多动态博弈策略分析电力市场中的拥塞攻击. 攻击者通过拥塞攻击减少携带测量信息的信道数量来操纵区域边际价格, 从而获得盈利. 防护者能够保证采用有限数量的信道就可以进行信息交付. Sanjab 等[23] 研究了智能电网中多个数据注入攻击者和一个电网防护者之间的博弈, 利用分布式学习算法求解博弈的均衡解, 最大化攻击者的收益, 最小化防护者的损失. 博弈论分析智能电网的安全, 实际上就是研究攻击者和防护者之间的相互作用, 通过求解博弈均衡解来预测个体的行为[24]. 袁勇等[25] 研究了一类带有时间偏好的单边双类型不完全信息轮流出价议价模型, 运用单阶段偏离法则分析了议价博弈的合并均衡与分离均衡, 并证明了议价博弈将唯一地实现合并均衡. 针对高级计量基础设施 (Advanced metering infrastructure, AMI) 网络中的分布式拒绝服务攻击, Wang 等[26] 将蜜罐技术 (Honeypot technology)

引入 AMI 网络中作为诱饵系统来检测和收集攻击信息, 分析了攻击者和防御者之间的相互作用, 并为双方推导出最佳策略.

以上针对智能电网安全性的研究, 大都没有考虑同时存在网络攻击和物理攻击两种类型攻击者的情形. 针对系统管理员 (防护者) 如何确定攻击者的类型, 从而选择最优防护策略的安全问题, 本文提出一种贝叶斯序贯博弈模型来确定攻击者的类型, 从而选择最优防护策略, 为系统管理员 (防护者) 及时地提供决策分析. 首先, 对事先不确定类型的攻击者和防护者构建静态贝叶斯博弈模型. 通过海萨尼转换, 使得防护者知道攻击者类型的概率分布, 将不完全信息博弈转换成完全信息博弈进行分析. 防护者以 μ 的概率知道攻击者类型是网络攻击, 其中 μ 可以通过智能电网的网络组件和物理组件占整个电网系统的比值计算. 经过贝叶斯博弈分析, 可以根据攻击者类型为网络攻击的概率和贝叶斯纳什均衡解, 确定攻击者的类型. 其次, 考虑了攻击者和防护者之间的序贯博弈模型, 能够有效地帮助防护者进行决策分析. 利用逆向归纳法分别对两种类型的攻击者和防护者之间的序贯博弈树进行分析, 根据均衡路径选择最优策略. 通过贝叶斯博弈和序贯博弈树分析, 确定攻击者的类型, 并且根据均衡路径可以得到攻击者的相对最优攻击策略和防护者的相对最优防护策略, 为保证智能电网的安全运行提供参考.

本文结构安排如下: 第 1 节介绍两种类型攻击者和防护者之间的静态贝叶斯博弈模型, 通过海萨尼转换将不完全信息博弈转换成完全信息博弈, 通过贝叶斯博弈模型的分析, 确定攻击者的类型; 第 2 节介绍序贯博弈的模型和求解均衡路径的数值算法; 第 3 节给出两种类型攻击者和防护者之间的数值算法分析, 根据求解的均衡路径得出攻击者的最优攻击策略和防护者的最优防护策略; 第 4 节是对全文的总结和对未来研究的展望.

1 攻击者和防护者的静态贝叶斯博弈

用 G 表示一个博弈: 如 G 有 n 个博弈方, 每个博弈方的全部可选策略的集合称为 "策略空间", 分别用 $S_1, \cdots, S_n$ 表示. $s_{ij} \in S_i$ 表示博弈方 i 的第 j 个策略, 其中 j 可以取有限个值 (有限策略博弈), 也可以取无限个值 (无限策略博弈); 博弈方 i 的收益用 U_i 表示, U_i 是各博弈方策略的多元函数. n 个博弈方的标准式博弈 G 通常记为 $G = \{S_1, \cdots, S_n; U_1, \cdots, U_n\}$[27].

1.1 博弈模型

当系统受到攻击时, 不同类型的攻击者获得的收益不同, 防护者对于攻击者的收益没有准确的认识, 所以是不完全信息博弈. 本文首先研究两种类型攻击者和防护者之间的双人非合作静态贝叶斯博弈. 入侵检测系统对于智能电网的安全防护有着重要作用, 当系统受到攻击时, 可以有效地检测到攻击, 从而系统防护者可以及时地选择防护策略. 为了能够更好地防护智能电网的安全, 电网的每个组件都应该配备一个入侵检测系统, 并且入侵检测系统保持运行状态. 从系统使用的角度来看, 永远在线运行并不是一个有效的选择, 因为智能电网的网络组件通常是资源受限的[28]. 静态贝叶斯博弈模型可以帮助系统防护者进行决策分析, 提升入侵检测系统的检测效率.

用 M_i 表示攻击者, θ 表示攻击者的类型, $\theta = 1$ 表示网络攻击, $\theta = 0$ 表示物理攻击, 每个类型的策略包括 {攻击, 不攻击}. M_j 表示系统防护者, 它的策略包括 {防护, 不防护}. α 表示入侵检测系统的检测率; β 表示误报率; ω 表示防护者的安全值; $c_{ic} > 0$ 表示网络攻击的成本; $c_{ip} > 0$ 表示物理攻击的成本; $c_d > 0$ 表示防护者的成本, 其中 $\alpha, \beta \in [0, 1]$.

假设 1. 防护者的安全值 ω 满足

$$\omega > \max(c_{ic}, c_{ip}, c_d)$$

在资源受限的网络中, 防护者安全值是系统受保护的能源资产, 防护成本可以根据系统采取防护策略的能量消耗来确定, 攻击成本可以根据攻击者采取攻击策略的能量消耗来确定. 若 ω 不满足假设 1, 那么攻击者就没有动机采取攻击策略, 防护者也没有动机采取防护策略. 当 $\theta = 1$ 时, 攻击者类型为网络攻击, 攻击者和防护者的策略组合为 (攻击, 不防护) 时, 攻击者成功攻击了系统, 系统防护者的损失为 ω, 即攻击者的收益为 $\omega - c_{ic}$, 防护者的收益为 $-\omega$. 策略组合为 (攻击, 防护) 时, 防护者的收益是检测到攻击的期望收益减去防护成本, 即 $\alpha\omega - (1 - \alpha)\omega - c_d = (2\alpha - 1)\omega - c_d$, 其中 $1 - \alpha$ 表示入侵检测系统的漏检率. 另外, 攻击者的收益是防护者损失的收益减去攻击成本, 即 $(1 - 2\alpha)\omega - c_{ic}$. 策略组合为 (不攻击, 防护) 时, 由于入侵检测系统的误报产生损失值 $-\beta\omega$, 所以防护者的收益为 $-\beta\omega - c_d$, 攻击者的收益为 0, 如表 1 所示. 其中收益组合的前半部分表示攻击者的收益, 后半部分表示防护者的收益. 当 $\theta = 0$ 时, 攻击者类型为物理攻击, 同理可以求解出攻击者和防护者的收益情况, 如表 2 所示.

1.2 贝叶斯纳什均衡分析

不同类型的攻击者和防护者之间相互作用, 得出的均衡解可能不同. 防护者对于攻击者类型的知识不能准确了解, 属于不完全信息博弈. 在 1967 年之前, 信息不完全的情况, 博弈论是无法解决的, 因

表 1　攻击者类型为网络攻击

Table 1　The type of attacker is a cyber attack

	防护	不防护
攻击	$(1-2\alpha)\omega-c_{ic}$, $(2\alpha-1)\omega-c_d$	$\omega-c_{ic}$, $-\omega$
不攻击	0, $-\beta\omega-c_d$	0, 0

表 2　攻击者类型为物理攻击

Table 2　The type of attacker is a physical attack

	防护	不防护
攻击	$(1-2\alpha)\omega-c_{ip}$, $(2\alpha-1)\omega-c_d$	$\omega-c_{ip}$, $-\omega$
不攻击	0, $-\beta\omega-c_d$	0, 0

为当你还不知道对手为何物时, 无法选择自己的最优策略. 在 1967 年, 海萨尼 (Harsanyi) 提出了海萨尼转换的方法[27], 将不完全信息博弈转换成完全但不完美信息博弈, 防护者知道攻击者两种类型的分布概率, 从而进行分析.

攻击者的类型包括网络攻击 (Cyber attack) 和物理攻击 (Physical attack), 每个类型的策略包括 {攻击 (Attack), 不攻击 (No attack)}. 防护者的策略包括 {防护 (Defend), 不防护 (No defend)}, N 是一个决定攻击类型的自然节点. 根据表 1 和表 2 的收益矩阵可得出贝叶斯博弈的扩展式, 如图 1 所示. 防护者有概率 μ 知道攻击者的类型是网络攻击, 并且博弈双方是理性的, 攻击者希望获得最大的收益, 防护者希望损失最小.

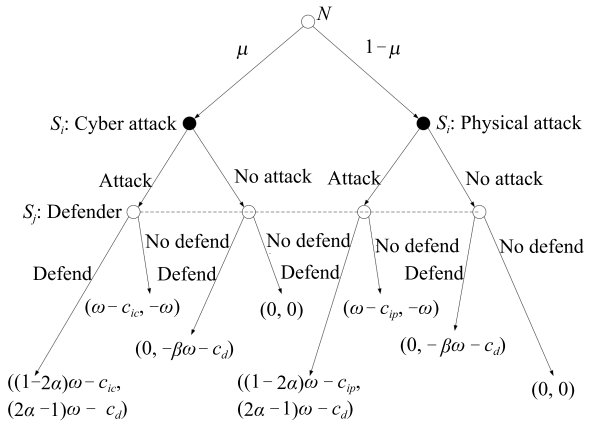

图 1　贝叶斯博弈的扩展式

Fig. 1　The Bayesian game in an extensive form

定义 1. 占优策略[27]. 用 s_{i1} 和 s_{i2} 表示博弈方 i 的两个可行策略, 如果对其他博弈方可能的策略组合 s_{-i}, 博弈方 i 选择 s_{i1} 的收益大于选择 s_{i2} 的收益, 即 $U_{i1}(s_{i1}, s_{-i}) \geq U_{i2}(s_{i2}, s_{-i})$, 则称 s_{i1} 为相对于 s_{i2} 的占优策略.

定义 2. 贝叶斯纳什均衡[27]. n 人不完全信息静态博弈 $G = \{S_1, \cdots, S_n; \theta_1, \cdots, \theta_n; p_1, \cdots, p_n; U_1, \cdots, U_n\}$ 的纯策略贝叶斯纳什均衡是一个类型依存战略组合 $\{s_i^*(\theta_i), i = 1, \cdots, n\}$, 其中每个参与人 i 在给定自己的类型 θ_i 和其他参与人类型依存战略 $s_{-i}^*(\theta_{-i})$ 的情况下最大化自己的期望效用函数 U_i. 若对于所有的 i, $s_i \in S_i(\theta_i)$, $s_i^*(\theta_i) \in \arg\max_{s_i} \sum p_i(\theta_{-i}|\theta_i) U_i(s_i, s_{-i}^*(\theta_{-i}); \theta_i, \theta_{-i})$, 战略组合 $s^* = (s_1^*(\theta_1), \cdots, s_n^*(\theta_n))$ 是一个纯策略的贝叶斯纳什均衡. 若博弈方 i 的策略空间为 $\{s_{i1}, \cdots, s_{ik}\}$, 那么概率分布 $p_i = (p_{i1}, \cdots, p_{ik})$ 称为 i 的一个混合策略, 其中 $p_{ik} = p(s_{ik})$ 是博弈方 i 选择策略 s_{ik} 的概率, $0 \leq p_{ij} \leq 1$, $j = 1, \cdots, k$, 并且 $p_{i1} + \cdots + p_{ik} = 1$. 如果对于所有的 i 的期望效用, $U_i(p_i^*, p_{-i}^*) \geq U_i(p_i, p_{-i}^*)$, 那么混合战略组合 $p^* = (p_1^*, \cdots, p_n^*)$ 是一个混合策略的贝叶斯纳什均衡.

定理 1. 纳什均衡的存在性[29]. 在 n 个博弈方参与的标准博弈 $G = \{S_1, \cdots, S_n; U_1, \cdots, U_n\}$ 中, 如果 n 是有限的, 且每个博弈方的策略集合 S_i 也是有限的, 则该博弈至少存在一个纳什均衡, 均衡可能包含混合策略.

用 $(X; Y)$ 表示攻击者的纯策略, $((X; Y), Z, \mu)$ 表示贝叶斯纳什均衡, 其中 X 表示攻击者类型为网络攻击的策略, Y 表示攻击者类型为物理攻击的策略, Z 表示防护者策略, μ 表示攻击者类型为网络攻击的概率.

两种类型的攻击者的纯策略包含了四种情况: (攻击; 攻击)、(攻击; 不攻击)、(不攻击; 攻击)、(不攻击; 不攻击). 当攻击者类型不确定时, 我们通过贝叶斯博弈的扩展式 (图 1), 可以计算出攻击者纯策略组合下的防护者的期望收益, 其中防护者采取防护策略的期望收益表示为 $\mathrm{E}(d)$, 采取不防护策略的期望收益表示为 $\mathrm{E}(nd)$. 攻击者类型为网络攻击时, 采取攻击策略的期望收益为 $\mathrm{E}_c(a)$, 采取不攻击的期望收益为 $\mathrm{E}_c(na)$. 攻击者类型为物理攻击时, 采取攻击策略的期望收益为 $\mathrm{E}_p(a)$, 采取不攻击的期望收益为 $\mathrm{E}_p(na)$. 当 $\mathrm{E}(d) = \mathrm{E}(nd)$ 时, 可以求出混合策略中攻击均衡策略的概率; 当 $\mathrm{E}_c(a) = \mathrm{E}_c(na)$ 和 $\mathrm{E}_p(a) = \mathrm{E}_p(na)$ 时, 可以求出混合策略中防护均衡策略的概率. 对两种类型攻击者和防护者之间的双人非合作静态贝叶斯博弈, 本文有如下定理.

定理 2. 若假设 1 成立, 当攻击者的纯策略为 (攻击; 攻击) 和 (不攻击; 不攻击) 时, 不存在纯策略的贝叶斯纳什均衡和混合策略的贝叶斯纳什均衡.

证明.

1) 当攻击者的纯策略为 (攻击; 攻击) 时, 防护

者采取防护策略的期望收益为

$$\begin{aligned}\mathrm{E}(d) = {} & \mu((2\alpha-1)\omega - c_d) + \\ & (1-\mu)((2\alpha-1)\omega - c_d) = \\ & (2\alpha-1)\omega - c_d\end{aligned} \tag{1}$$

防护者采取不防护策略的期望收益为

$$\mathrm{E}(nd) = -\omega \tag{2}$$

此时, 防护者的纯策略 {防护, 不防护} 的期望收益都与 μ 无关. 所以 ((攻击; 攻击), 防护) 和 ((攻击; 攻击), 不防护) 都不是纯策略的贝叶斯纳什均衡和混合策略的贝叶斯纳什均衡.

2) 当攻击者的纯策略为 (不攻击; 不攻击) 时, 防护者采取防护策略的期望收益为

$$\begin{aligned}\mathrm{E}(d) = {} & \mu(-\beta\omega - c_d) + \\ & (1-\mu)(-\beta\omega - c_d) = \\ & -\beta\omega - c_d\end{aligned} \tag{3}$$

防护者采取不防护策略的期望收益为

$$\mathrm{E}(nd) = 0 \tag{4}$$

此时, 防护者的纯策略 {防护, 不防护} 期望收益都与 μ 无关. 并且 $\mathrm{E}(d) < \mathrm{E}(nd)$, 防护者采取的占优策略是不防护, 然而攻击者采取相应的最优策略是 (攻击; 攻击). 所以 ((不攻击; 不攻击), 不防护) 不是纯策略的贝叶斯纳什均衡和混合策略的贝叶斯纳什均衡. □

定理 3. 若假设 1 成立, 当 $\mu > (\beta\omega + c_d)/((2\alpha + \beta)\omega)$ 时, 在 $c_{ic} < (1-2\alpha)\omega < c_{ip}$ 的情况下, 存在纯策略的贝叶斯纳什均衡, 此时攻击者的类型为网络攻击; 当 $\mu \le (\beta\omega + c_d)/((2\alpha + \beta)\omega)$ 时, 存在混合策略的贝叶斯纳什均衡, 此时攻击者的类型为网络攻击.

证明.

1) 当攻击者的纯策略为 (攻击; 不攻击) 时, 防护者采取防护策略的期望收益为

$$\begin{aligned}\mathrm{E}(d) = {} & \mu((2\alpha-1)\omega - c_d) + \\ & (1-\mu)(-\beta\omega - c_d) = \\ & (2\alpha+\beta-1)\mu\omega - (\beta\omega + c_d)\end{aligned} \tag{5}$$

防护者采取不防护策略的期望收益为

$$\mathrm{E}(nd) = -\mu\omega \tag{6}$$

当 $\mu > (\beta\omega + c_d)/((2\alpha + \beta)\omega)$ 时, $\mathrm{E}(d) > \mathrm{E}(nd)$, 防护者采取的占优策略是防护. 假设 $c_{ic} < (1-2\alpha)\omega < c_{ip}$, 攻击者采取相应的最优策略是 (攻击; 不攻击). 因此当 $\mu > (\beta\omega + c_d)/((2\alpha + \beta)\omega)$ 和 $c_{ic} < (1-2\alpha)\omega < c_{ip}$ 时, ((攻击; 不攻击), 防护, μ) 是纯策略的贝叶斯纳什均衡, 否则不存在. 当 $\mu \le (\beta\omega + c_d)/((2\alpha + \beta)\omega)$ 时, $\mathrm{E}(d) < \mathrm{E}(nd)$, 防护者采取的占优策略是不防护. 然而攻击者采取相应的最优策略是 (攻击; 攻击), 所以 ((攻击; 不攻击), 不防护, μ) 不是纯策略的贝叶斯纳什均衡.

2) 在攻击者的纯策略为 (攻击; 不攻击) 的情况下, 当 $\mu \le (\beta\omega + c_d)/((2\alpha + \beta)\omega)$ 时, 不存在纯策略的贝叶斯纳什均衡, 由定理 1 可知, 博弈存在混合策略的贝叶斯纳什均衡. 假设攻击者的类型为网络攻击时, 采取攻击策略的概率为 p_1, 采取不攻击策略的概率为 $1-p_1$; 攻击者的类型为物理攻击时, 采取不攻击策略. 防护者采取防护的概率 q_1, 不防护的概率为 $1-q_1$.

防护者采取防护策略的期望收益为

$$\begin{aligned}\mathrm{E}(d) = {} & \mu p_1((2\alpha-1)\omega - c_d) + \mu(1-p_1)\times \\ & (-\beta\omega - c_d) + (1-\mu)(-\beta\omega - c_d) = \\ & \mu p_1\omega(2\alpha+\beta-1) - (\beta\omega + c_d)\end{aligned} \tag{7}$$

防护者采取不防护策略的期望收益为

$$\mathrm{E}(nd) = -\mu p_1\omega \tag{8}$$

攻击者的类型为网络攻击, 采取攻击的期望收益为

$$\begin{aligned}\mathrm{E}_c(a) = {} & \mu q_1((1-2\alpha)\omega - c_{ic}) + \\ & \mu(1-q_1)(\omega - c_{ic}) = \\ & -2\alpha\omega\mu q_1 + \mu(\omega - c_{ic})\end{aligned} \tag{9}$$

攻击者的类型为网络攻击, 采取不攻击的期望收益为

$$\mathrm{E}_c(na) = 0 \tag{10}$$

当 $\mathrm{E}(d) = \mathrm{E}(nd)$ 时, 可以得出攻击者类型为网络攻击时, 采取攻击均衡策略的概率为 $p_1^* = (\beta\omega + c_d)/((2\alpha + \beta)\mu\omega)$. 当 $\mathrm{E}_c(a) = \mathrm{E}_c(na)$ 时, 可以得出防护者采取防护均衡策略的概率 $q_1^* = (\omega - c_{ic})/2\alpha\omega$. 由此可知, 当 $\mu \le (\beta\omega + c_d)/((2\alpha + \beta)\omega)$ 时 ((以 p_1^* 的概率攻击; 不攻击), 以 q_1^* 的概率防护, μ) 是混合策略的贝叶斯纳什均衡. □

定理 4. 若假设 1 成立, 当 $\mu < (2\alpha\omega - c_d)/((2\alpha + \beta)\omega)$ 时, 在 $c_{ip} < (1-2\alpha)\omega < c_{ic}$ 的情况下, 存在纯策略的贝叶斯纳什均衡, 此时攻击者的类型为物理攻击; 当 $\mu \ge (2\alpha\omega - c_d)/((2\alpha + \beta)\omega)$ 时, 存在混合策略的贝叶斯纳什均衡, 此时攻击者的类型为物理攻击.

证明.

1) 当攻击者的纯策略为 (不攻击; 攻击) 时, 防护者采取防护策略的期望收益为

$$\begin{aligned}\mathrm{E}(d) = {} & \mu(-\beta\omega - c_d) + \\ & (1-\mu)((2\alpha-1)\omega - c_d) = \\ & (2\alpha-1)\omega - c_d - \mu\omega(2\alpha+\beta-1)\end{aligned} \tag{11}$$

防护者采取不防护策略的期望收益为

$$\mathrm{E}(nd) = \mu\omega - \omega \tag{12}$$

当 $\mu < (2\alpha\omega - c_d)/((2\alpha+\beta)\omega)$ 时, $\mathrm{E}(d) > \mathrm{E}(nd)$, 防护者采取的占优策略是防护. 假设 $c_{ip} < (1-2\alpha)\omega < c_{ic}$, 攻击者采取相应的最优策略是 (不攻击; 攻击). 因此当 $\mu < (2\alpha\omega - c_d)/((2\alpha+\beta)\omega)$ 和 $c_{ip} < (1-2\alpha)\omega < c_{ic}$ 时 ((不攻击; 攻击), 防护, μ) 是纯策略的贝叶斯纳什均衡, 否则不存在. 当 $\mu \geq (2\alpha\omega - c_d)/((2\alpha+\beta)\omega)$ 时, $\mathrm{E}(d) < \mathrm{E}(nd)$, 防护者采取的占优策略是不防护. 然而攻击者采取相应的最优策略是 (攻击; 攻击), 所以 ((不攻击; 攻击), 不防护, μ) 不是纯策略的贝叶斯纳什均衡.

2) 在攻击者的纯策略为 (不攻击; 攻击) 的情况下, 当 $\mu \geq (2\alpha\omega - c_d)/((2\alpha+\beta)\omega)$ 时, 不存在纯策略的贝叶斯纳什均衡, 由定理 1 可知, 博弈存在混合策略的贝叶斯纳什均衡. 假设攻击者类型为物理攻击, 采取攻击策略的概率为 p_2, 采取不攻击策略的概率为 $1-p_2$; 攻击者类型为网络攻击时采取不攻击策略. 防护者采取防护策略的概率 q_2, 采取不防护策略的概率为 $1-q_2$.

防护者采取防护策略的期望收益为

$$\begin{aligned}\mathrm{E}(d) = {} & \mu(-\beta\omega - c_d) + \\ & (1-\mu)p_2((2\alpha-1)\omega - c_d) + \\ & (1-\mu)(1-p_2)(-\beta\omega - c_d) = \\ & (2\alpha+\beta-1)(1-\mu)\omega p_2 - (\beta\omega + c_d)\end{aligned} \tag{13}$$

防护者采取不防护策略的期望收益为

$$\mathrm{E}(nd) = (\mu-1)\omega p_2 \tag{14}$$

攻击者类型物理攻击时, 采取攻击策略的期望收益为

$$\begin{aligned}\mathrm{E}_p(a) = {} & (1-\mu)q_2((1-2\alpha)\omega - c_{ip}) + \\ & (1-\mu)(1-q_2)(\omega - c_{ip}) = \\ & 2\alpha\omega q_2(\mu-1) + (1-\mu)(\omega - c_{ip}) = \\ & (\mu-1)(2\alpha\omega q_2 - \omega + c_{ip})\end{aligned} \tag{15}$$

攻击者类型物理攻击时, 采取不攻击策略的期望收益为

$$\mathrm{E}_p(na) = 0 \tag{16}$$

当 $\mathrm{E}(d) = \mathrm{E}(nd)$ 时, 可以得出攻击者类型为物理攻击时, 采取攻击均衡策略的概率为 $p_2^* = (\beta\omega + c_d)/((2\alpha+\beta)(1-\mu)\omega)$. 当 $\mathrm{E}_p(a) = \mathrm{E}_p(na)$ 时, 可以得出防护者采取防护均衡策略的概率 $q_2^* = (\omega - c_{ip})/2\alpha\omega$. 由此可知, 当 $\mu \geq (2\alpha\omega - c_d)/((2\alpha+\beta)\omega)$ 时, ((不攻击; 以 p_2^* 的概率攻击), 以 q_2^* 的概率防护, μ) 是混合策略的贝叶斯纳什衡. □

静态贝叶斯博弈模型广泛地应用于多攻击者类型的网络中, 例如 DOS 攻击 (Denial of service attacks), 路由中断攻击 (Routing disruption attacks). 为了能够更好地防护智能电网的安全, 入侵检测系统总是保持运行状态. 从系统使用的角度来看, 持续运行并不是一个最有效的选择, 因为电网的网络组件通常是资源受限的. 静态贝叶斯博弈模型可以根据贝叶斯纳什均衡解帮助系统防护者进行决策分析, 提升入侵检测系统的检测效率. 由定理 3 和定理 4 可知, 本文根据攻击者类型为网络攻击的概率和贝叶斯纳什均衡解, 可以确定攻击者的类型. 对于攻击者类型不确定的问题, 可以通过智能电网的网络组件占整个电网系统的比例来计算攻击者类型为网络攻击的概率.

2　序贯博弈模型和数值算法

2.1　序贯博弈模型

关于智能电网的网络安全和物理安全的研究, 分别是网络攻击和防护者、物理攻击和防护者之间的一个双人博弈; 当攻击者的类型确定时, 博弈方对另外一方的特征、战略空间及支付函数有准确的知识, 是一个完全信息的博弈; 攻击者和防护者轮流选择策略, 是一个连续的博弈; 因此攻击者和防护者之间的博弈是一个双人完全信息下的序贯博弈[19]. 对于序贯博弈, 通常使用博弈树的方法进行分析. 树形图称为博弈的扩展式, 表明所有博弈方可选择的所有可能策略, 并给出博弈的所有可能的收益结果. 攻击者和防护者之间依次轮流选择策略, 当前状态的收益只依赖于上一个状态的收益, 这反映了收益行为是一个马尔科夫过程 (Markov process)[30].

用 $U_h(S,a)$ 表示当前状态博弈方 S 的收益情况, 那么当前收益是上一状态的收益 $U_{h-1}(S,a')$ 加上行为函数收益 $A(S,a,d)$, 计算公式为

$$U_h(S,a) = U_{h-1}(S,a') + A(S,a,d) \tag{17}$$

其中, d 表示博弈树的深度, a 表示博弈方 S 的行为策略, 由于攻击者和防护者是轮流采取策略, 所以 a' 表示博弈方 S 的对手的策略. 若行为函数收益中的 a 是攻击者的策略, 当博弈方 S 为攻击者时, 它会

获得一个线性的增益影响; 当博弈方 S 为防护者时, 它会有指数级的损失影响. 若 a 是防护者的策略, 当博弈方 S 为攻击者时, 它没有收益; 当博弈方 S 为防护者时, 它会有线性的增益影响, 如表 3 所示.

表 3 行为函数收益

Table 3 The payoff of the behavioral function

$A(S,a,d)$	a 为攻击者策略	a 为防护者策略
S 为攻击者	$d \times Impact(a)$	0
S 为防护者	$-Impact(a)^d$	$d \times Impact(a)$

下面计算策略 a 对博弈方产生的影响函数 $Impact(a)$, 它由智能电网的保密性 (Confidentiality)、完整性 (Integrity)、可用性 (Availability) 和安全性 (Safety) 组成, 分别用 $C(a)$, $I(a)$, $A(a)$, $SF(a)$ 表示, 并且根据重要性赋予的权值分别为 ω_C, ω_I, ω_A, ω_{SF}. 其中 $Impact(a)$ 定义如下:

$$Impact(a) = \omega_C C(a) + \omega_I I(a) + \omega_A A(a) + \omega_{SF} SF(a) \tag{18}$$

2.2 数值算法

为了能够对确定类型的攻击者和防护者之间的序贯博弈进行分析, 本文提出了一种数值算法, 通过逆向归纳法对序贯博弈模型的博弈树进行分析. 将博弈树的每个决策结点看成一个子博弈的初始结点, 每个决策结点和它的后续分支构成一个子博弈. 在每个子博弈中求出纳什均衡, 这些纳什均衡的战略组合是子博弈精炼纳什均衡. 如果一个博弈有几个子博弈, 一个特定的纳什均衡决定了原博弈树上唯一的路径, 这条路径称为均衡路径. 为了求解子博弈精炼纳什均衡, 通过逆向归纳法从最后一个子博弈开始, 依次向前求解每个子博弈的纳什均衡. 根据博弈树的均衡路径, 可以得出博弈双方的最优策略, 以下是数值算法的步骤:

算法 1. 数值算法

步骤 1. 设置初值:

ω_C, ω_I, ω_A, ω_{SF}, $C(a)$, $I(a)$, $A(a)$, $SF(a)$

步骤 2. 构建博弈树:

每个决策节点表示攻击者和防护者的轮次, 每条分支表示攻击者和防护者的策略; 博弈树的高度为 d.

步骤 3. 收益值:

根据式 (18) 求出策略 a 的 $Impact(a)$; 根据式 (17) 和表 3 可以求出博弈树每个决策节点的收益值, 初始收益值都为 (0, 0), 前者为攻击者的收益, 后者为防护者的收益.

步骤 4. 迭代:

for $i = d$; $i \geq 0$; $i--$ **do**
  if 决策节点为攻击者轮次 **then**
    比较后续分支的攻击者收益值, 保留收益值较大的行为策略;
  end if
  if 决策节点为防护者轮次 **then**
    比较后续分支的防护者收益值, 保留收益值较大的行为策略;
  end if
end for

3 序贯博弈模型的数值算法分析

经过静态贝叶斯博弈模型分析后, 攻击者的类型确定, 接下来分别对两种类型的攻击者和防护者进行序贯博弈数值算法分析, 通过算法求出均衡路径, 根据均衡路径可以得出攻击者的最优攻击策略和防护者的最优防护策略.

3.1 两种类型的攻击者

随着新技术的应用和更容易获取的能源数据的使用, 智能电网有可能受到多种漏洞和攻击的威胁. 为了能够清晰地了解攻击者的策略, 下面介绍三种网络攻击和三种物理攻击.

1) 网络类型的攻击者: 攻击智能电网的网络组件.

干扰攻击 (Jamming): 智能电网的通信系统较容易受到攻击, 例如拒绝服务攻击. 干扰攻击作为拒绝服务攻击的一种, 干扰和阻塞了系统组件之间的信息交换、数据测量和控制输入, 对数据的完整性造成了损害[31].

窃听攻击 (Eavesdropping): 对手可以通过监控网络流量来获取敏感信息, 披露智能电网控制结构以及未来的价格信息, 从而导致用户隐私泄露. 这种窃听可以用来收集更多的信息, 进行更多的犯罪. 例如, 攻击者可以收集和检查网络流量, 从通信模式中推断出信息, 甚至加密的通信也容易受到流量分析的攻击.

数据注入攻击 (Data injection): 攻击者向目标地区当前或者未来的价格中注入虚假信息, 使得地区的电力需求变化而造成损失, 以及将错误的电表信息发送给智能电网公司, 造成公司的经济损失. 数据注入攻击也会改变电力市场的状态估计值, 通过电网拓扑的知识, 可以看出在当今的监控和数据采集 (SCADA) 系统中, 错误的数据注入攻击可以绕开不良数据检测[32].

2) 物理类型的攻击者: 攻击智能电网的物理组件.

恐怖袭击 (Terrorist): 第一起恐怖袭击事件发生在 2014 年的也门, 袭击者发射火箭摧毁输电塔, 造成也门全国停电和 2 400 万人受伤[11]. 再如狙击手攻击美国加利福尼亚州输电变电站的电力系统变压器, 改变电力系统的拓扑结构, 导致了直接停电并引发连锁故障[33].

盗窃攻击 (Steal): 攻击者盗窃铜线和金属设备, 损害了电网的完整性, 造成大片区域的停电事故. 例如, 盗窃造成了美国西弗吉尼亚州 3 000 人的停电事故[11].

自然灾害攻击 (Natural disaster): 自然灾害会损害智能电网的物理设备, 造成大片区域的停电, 显示了智能电网组件的物理暴露和不可靠性的影响. 树木的过度生长和倒塌也会对电网输电线路造成攻击, 例如过度生长的树木造成了美国俄亥俄州北部 5 000 万人的大面积停电[34].

3.2　网络攻击和防护者的序贯博弈数值分析

为了保证智能电网安全、可扩展和可靠地运行, 各国提出了一些框架和指导方针[35]. 美国国家标准与技术研究院提出, 为了智能电网的安全, 应满足三个安全需求: 保密性 (Confidentiality)、完整性 (Integrity) 和可用性 (Availability). 由于智能电网组件的不同性质, 以及与物理世界的直接互动, 安全性 (Safety) 要求也是至关重要的. 美国 2004 年 2 月出版的《联邦信息和信息系统安全分类标准》(Federal information processing standard 199, FIPS 199) 对每个安全需求都规定了低、中、高影响级. 由于安全性的重要性, 本文也规定了低、中、高影响级. 对于智能电网的网络安全, 数据的完整性是最重要的, 其次是数据的可用性, 最后是保密性和安全性. 本文假设网络安全需求的权值分别为 $\omega_I = 0.4$, $\omega_A = 0.3$, $\omega_C = 0.2$, $\omega_{SF} = 0.1$. 网络攻击中的干扰攻击 (Jamming)、窃听攻击 (Eavesdropping)、数据注入攻击 (Data injection) 分别用 a_{cj}, a_{ce} 和 a_{cd} 表示, 其中 a_{cno} 表示不攻击策略. 智能电网的防护者也会采取相应的策略, 例如密钥管理 (Key management)、干扰防护 (Jamming defense), 用 $d_{\langle km,jd\rangle}$ 表示, 其中 d_{cno} 表示不防护策略. 根据这些网络攻击对智能电网的影响, 确定攻击策略的影响级, 其中影响级低、中、高分别用 l, m, h 表示 ($l < m < h$). 根据式 (18) 可计算出行为策略 a 的影响函数, 如表 4 所示. 网络攻击者和防护者之间进行序贯博弈, 通过数值算法对网络攻击的序贯博弈树进行分析, 博弈双方轮流采取行动, 通常是攻击者先采取行动.

假设攻击者第一阶段采取的策略为 $\{a_{ce}, a_{cno}\}$, 第二阶段采取策略 $\{a_{cj}, a_{cd}\}$; 防护者采取的策略为 $\{d_{\langle km,jd\rangle}, d_{cno}\}$. 博弈树的收益结果根据式 (17) 和表 3 进行计算, 表示为 (攻击者收益, 防护者收益), 其中根节点的初始收益为 (0, 0), 实心圆表示攻击者轮次, 空心圆表示防护者轮次. 网络攻击的序贯博弈树如图 2 所示.

首先从博弈树高度为 2 的最左侧子博弈开始, 比较收益 $(1.6l+m+1.4h, -(0.3l+0.3m+0.4h)^3 - 0.1l + 1.1m)$ 和 $(1.3l + m + 1.7h, -(0.2l + 0.3m + 0.5h)^3 - 0.1l + 1.1m)$, 此时是攻击者轮次, 并且 $1.6l + m + 1.4h < 1.3l + m + 1.7h$, 所以攻击者的最优策略是 a_{cd}, 收益为 $(1.3l + m + 1.7h, -(0.2l + 0.3m + 0.5h)^3 - 0.1l + 1.1m)$. 同理可以求出博弈树高度为 2 的其余三个子博弈的最优策略和收益分别为 a_{cd} 和 $(1.3l + m + 1.7h, -(0.2l + 0.3m + 0.5h)^3 - 0.7l - 0.1m - 0.2h)$, a_{cd} 和 $(0.6l + 0.9m + 1.5h, -(0.2l + 0.3m + 0.5h)^3 + 0.6l + 1.2m + 0.2h)$, a_{cd} 和 $(0.6l + 0.9m + 1.5h, -(0.2l + 0.3m + 0.5h)^3)$.

其次从博弈树高度为 1 的左侧子博弈分析, 比较收益 $(1.3l + m + 1.7h, -(0.2l + 0.3m + 0.5h)^3 - 0.1l + 1.1m)$ 和 $(1.3l + m + 1.7h, -(0.2l + 0.3m + 0.5h)^3 - 0.7l - 0.1m - 0.2h)$, 此时是防护者的轮次, 并且 $-(0.2l + 0.3m + 0.5h)^3 - 0.1l + 1.1m > -(0.2l + 0.3m + 0.5h)^3 - 0.7l - 0.1m - 0.2h$, 所以防护者采取防护策略 $d_{\langle km,jd\rangle}$, 收益为 $(1.3l + m + 1.7h, -(0.2l+0.3m+0.5h)^3 - 0.1l + 1.1m)$. 同理可求出博弈树高度为 1 的右侧子博弈最优策略和收益为 $d_{\langle km,jd\rangle}$ 和 $(0.6l + 0.9m + 1.5h, -(0.2l + 0.3m + 0.5h)^3 + 0.6l + 1.2m + 0.2h)$.

最后对博弈树高度为 0 的子博弈进行分析, 比较收益 $(1.3l + m + 1.7h, -(0.2l + 0.3m + 0.5h)^3 - 0.1l + 1.1m)$ 和 $(0.6l + 0.9m + 1.5h, -(0.2l + 0.3m + 0.5h)^3 + 0.6l + 1.2m + 0.2h)$, 此时是攻击者轮次, 并且 $1.3l + m + 1.7h > 0.6l + 0.9m + 1.5h$, 所以攻击者采取 a_{ce}, 收益为 $(1.3l + m + 1.7h, -(0.2l + 0.3m + 0.5h)^3 - 0.1l + 1.1m)$.

经过分析, 攻击者的类型为网络攻击时, 博弈树的均衡路径如图 2 所示, 攻击者的最优策略是 a_{ce} 和 a_{cd}, 防护者的最优策略是 $d_{\langle km,jd\rangle}$.

3.3　物理攻击和防护者的序贯博弈数值分析

智能电网遭受物理攻击时, 也会对网络造成影响, 例如攻击智能电表会导致用户数据丢失, 使得电网公司损失利益. 所以影响函数 $Impact(a)$ 也是由智能电网的保密性 (Confidentiality)、完整性 (Integrity)、可用性 (Availability)、安全性 (Safety) 组成. 对于智能电网的物理设备的安全, 完整性 (Integrity) 和可用性 (Availability) 同时重要, 其次是保密性 (Confidentiality)、安全性 (Safety). 本文根据物理安全需求的重要性来分配权值, 分别为 $\omega_I =$

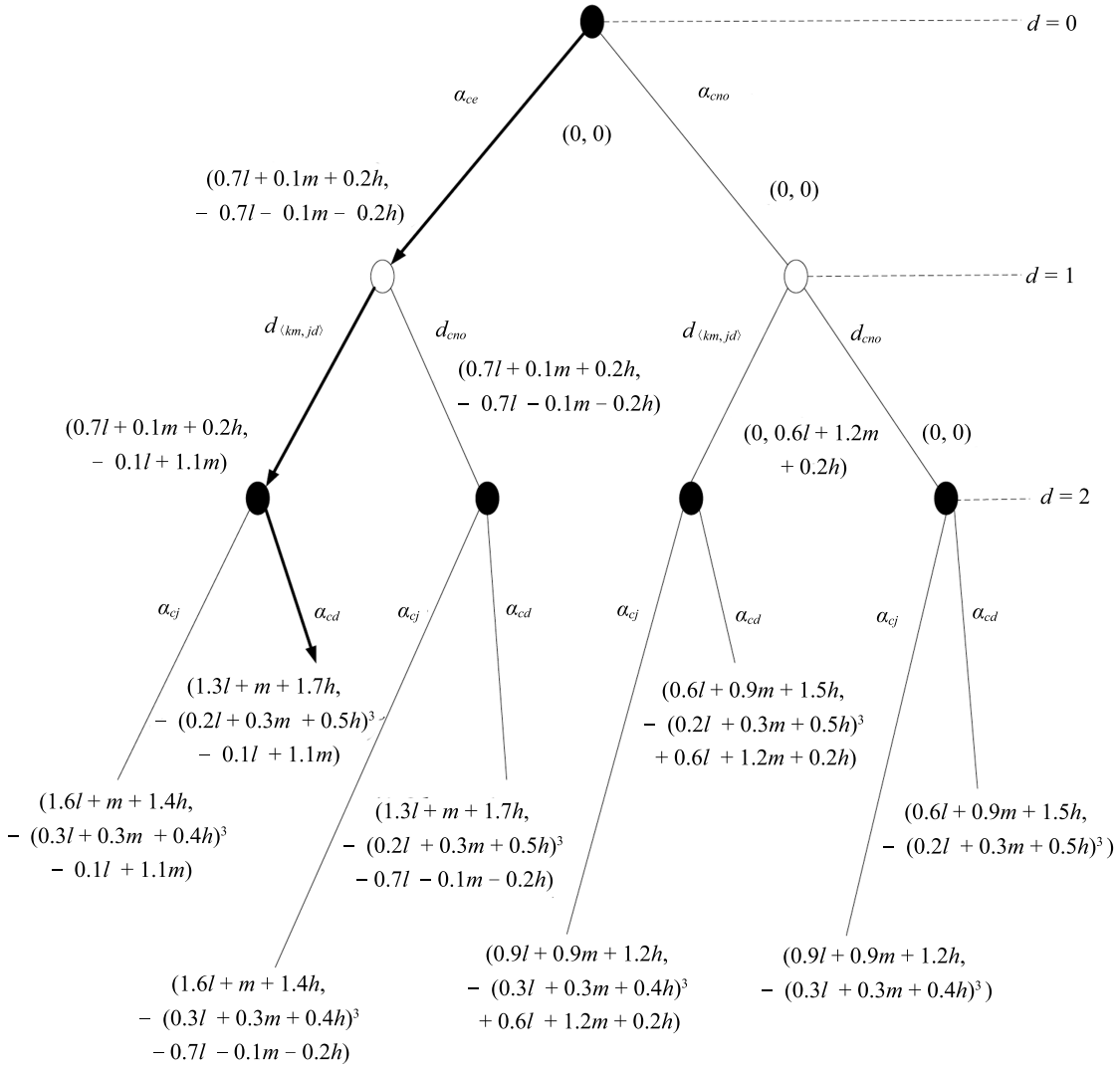

图 2 网络攻击的序贯博弈树

Fig. 2 The sequential game tree for cyber attacks

0.4, $\omega_A = 0.4$, $\omega_C = 0.1$, $\omega_{SF} = 0.1$. 物理攻击中的恐怖袭击 (Terrorist)、盗窃攻击 (Steal)、自然灾害攻击 (Natural disaster) 分别用 a_{pt}, a_{ps} 和 a_{pn} 表示, 其中 a_{pno} 表示不攻击策略. 智能电网的防护者也会采取相应的策略, 例如意外事故分析 (Contingency analysis)、监控物理访问 (Monitor physical access), 用 $d_{\langle ca,mp\rangle}$ 表示, 其中 d_{pno} 表示不防护策略. 根据式 (18) 可计算出行为策略 a 的影响函数, 如表 5 所示.

假设攻击者第一阶段采取的策略为 $\{a_{ps}, a_{pno}\}$, 第二阶段采取策略 $\{a_{pn}, a_{pt}\}$; 防护者采取的策略为 $\{d_{\langle ca,mp\rangle}, d_{pno}\}$. 博弈树的收益结果根据式 (17) 和表 3 进行计算, 表示为 (攻击者收益, 防护者收益), 其中根节点的初始收益为 (0, 0), 实心圆表示攻击者轮次, 空心圆表示防护者轮次. 物理攻击的序贯博弈树如图 3 所示. 通过数值算法对物理攻击的序贯博弈树进行分析, 求出均衡路径.

首先从博弈树高度为 2 的最左侧子博弈开始, 比较收益 $(1.1l + 2.9m, -(0.1l + 0.9m)^3 - 0.6l + 1.6m)$ 和 $(1.1l + 0.2m + 2.7h, -(0.1l + 0.9h)^3 - 0.6l + 1.6m)$, 此时是攻击者的轮次, 并且 $1.1l + 0.2m + 2.7h > 1.1l + 2.9m$, 所以攻击者的最优策略是 a_{pt}, 收益为 $(1.1l+0.2m+2.7h, -(0.1l+0.9h)^3 - 0.6l + 1.6m)$. 同理求出其余博弈树高度为 2 的子博弈最优策略和收益分别为 a_{pt} 和 $(1.1l + 0.2m + 2.7h, -(0.1l+0.9h)^3 - 0.8l - 0.2m)$, a_{pt} 和 $(0.3l + 2.7h, -(0.1l+0.9h)^3 + 0.2l + 1.8m)$, a_{pt} 和 $(0.3l + 2.7h, -(0.1l + 0.9h)^3)$.

其次对博弈树高度为 1 的左侧子博弈分析, 比较收益 $(1.1l+0.2m+2.7h, -(0.1l+0.9h)^3 - 0.6l + 1.6m)$ 和 $(1.1l+0.2m+2.7h, -(0.1l+0.9h)^3 - 0.8l - 0.2m)$, 此时是防护者轮次, 并且 $-(0.1l+0.9h)^3 -$

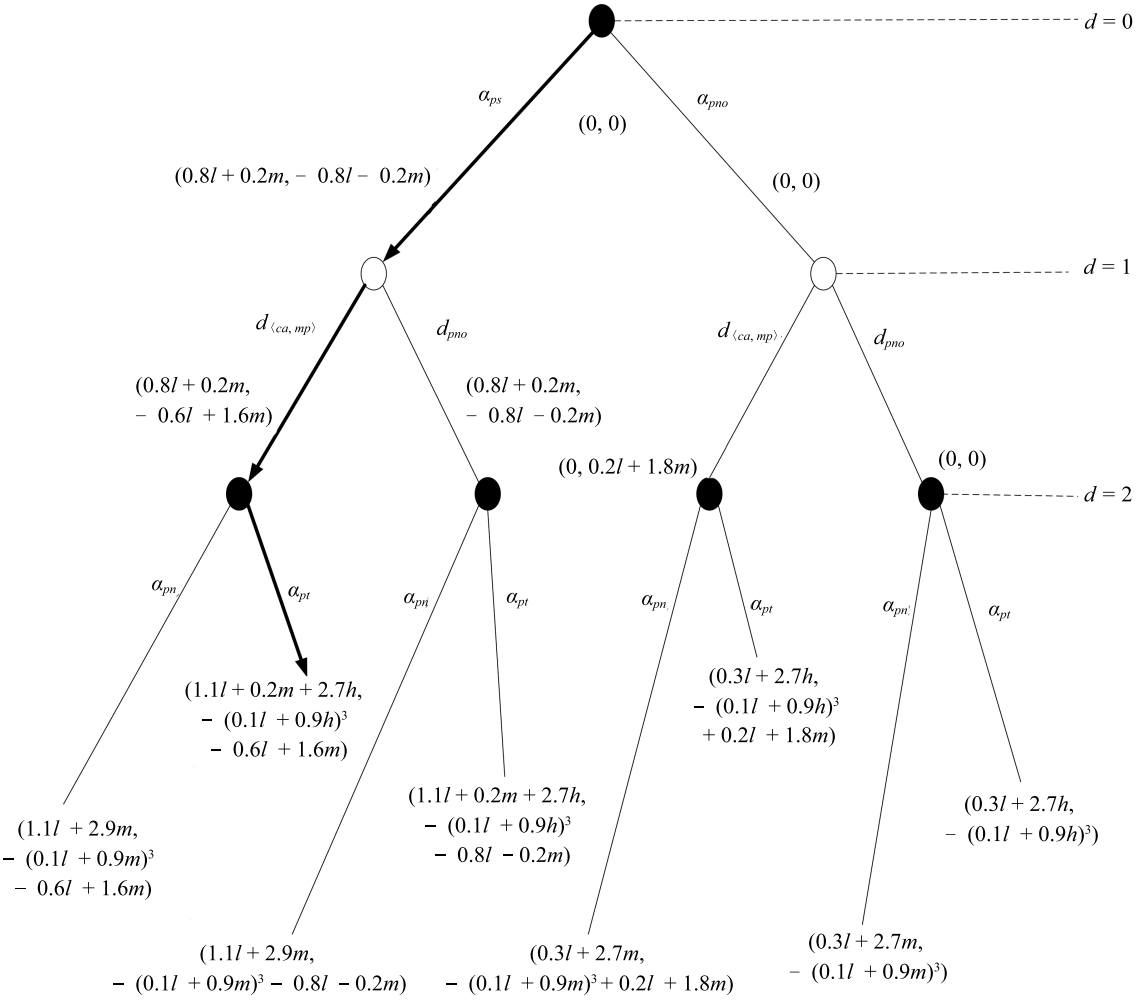

图 3　物理攻击的序贯博弈树

Fig. 3　The sequential game tree for physical attacks

表 4　行为策略 a 的影响函数 (网络攻击)

Table 4　The payoff of the behavioral function (cyber attack)

行为策略 (a)	$C(a)$	$I(a)$	$A(a)$	$SF(a)$	$Impact(a)$
$d_{\langle km,jd\rangle}$	m	m	l	h	$0.3l + 0.6m + 0.1h$
a_{ce}	h	l	l	m	$0.7l + 0.1m + 0.2h$
a_{cj}	l	h	m	l	$0.3l + 0.3m + 0.4h$
a_{cd}	l	h	m	h	$0.2l + 0.3m + 0.5h$

表 5　行为策略 a 的影响函数 (物理攻击)

Table 5　The payoff of the behavioral function (physical attack)

行为策略 (a)	$C(a)$	$I(a)$	$A(a)$	$SF(a)$	$Impact(a)$
$d_{\langle ca,mp\rangle}$	l	m	m	m	$0.1l + 0.9m$
a_{ps}	m	l	l	m	$0.8l + 0.2m$
a_{pn}	l	m	m	m	$0.1l + 0.9m$
a_{pt}	l	h	h	h	$0.1l + 0.9h$

$0.6l + 1.6m > -(0.1l + 0.9h)^3 - 0.8l - 0.2m$, 所以防护者采取的最优策略为 $d_{\langle ca,mp\rangle}$, 收益为 $(1.1l + 0.2m + 2.7h, -(0.1l + 0.9h)^3 - 0.6l + 1.6m)$. 同理求出博弈树高度为 1 的右侧子博弈的最优策略和收益为 $d_{\langle ca,mp\rangle}$ 和 $(0.3l + 2.7h, -(0.1l + 0.9h)^3 + 0.2l + 1.8m)$.

最后对博弈树高度为 0 的子博弈进行分析, 比较收益 $(1.1l+0.2m+2.7h, -(0.1l+0.9h)^3 - 0.6l + 1.6m)$ 和 $(0.3l+2.7h, -(0.1l+0.9h)^3+0.2l+1.8m)$, 此时是攻击者轮次, 并且 $1.1l + 0.2m + 2.7h > 0.3l + 2.7h$, 所以攻击者采取的最优策略为 a_{ps}, 收益为 $(1.1l+0.2m+2.7h, -(0.1l+0.9h)^3 - 0.6l + 1.6m)$.

经过分析, 攻击者的类型为物理攻击时, 博弈树的均衡路径如图 3 所示, 攻击者的最优策略是 a_{ps} 和 a_{pt}, 防护者的最优策略是 $d_{\langle ca,mp\rangle}$.

4 结束语

本文针对智能电网的防护者如何确定攻击者类型, 进而选择最优防护策略的安全问题, 提出了一种贝叶斯序贯博弈模型, 为系统防护者及时提供决策分析. 首先, 通过静态贝叶斯博弈模型分析, 根据贝叶斯纳什均衡解和攻击者类型为网络攻击的概率, 确定攻击者的类型. 其次, 通过逆向归纳法对确定类型的攻击者和防护者之间的序贯博弈博弈树进行分析, 根据均衡路径选择博弈双方的最优策略. 通过对攻击者和防护者的静态贝叶斯博弈和序贯博弈树分析, 解决了防护者不确定攻击者类型的安全问题, 并且根据均衡路径得出了攻击者的最优攻击策略和防护者的最优防护策略, 为保证智能电网的安全运行提供了参考. 下一步值得进一步探讨的问题包括建立和分析攻击者和防护者之间的动态贝叶斯博弈模型, 以及扩展序贯博弈模型中的行为函数收益公式等.

References

1 Derler P, Lee E A, Vincentelli A S. Modeling cyber-physical systems. *Proceedings of the IEEE*, 2012, **100**(1): 13−28

2 Mitchell R, Chen I R. Effect of intrusion detection and response on reliability of cyber physical systems. *IEEE Transactions on Reliability*, 2013, **62**(1): 199−210

3 Cao X H, Cheng P, Chen J M, Sam Ge S, Cheng Y, Sun Y X. Cognitive radio based state estimation in cyber-physical systems. *IEEE Journal on Selected Areas in Communications*, 2014, **32**(3): 489−502

4 Baheti R, Gill H. Cyber-physical systems. *The Impact of Control Technology*. Washington D. C., USA: IEEE, 2011. 161−166

5 Cintuglu M H, Mohammed O A, Akkaya K, Uluagac A S. A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys and Tutorials*, 2017, **19**(1): 446−464

6 Liu Y, Peng Y, Wang B L, Yao S R, Liu Z H. Review on cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica*, 2017, **4**(1): 27−40

7 Wen Jing-Rong, Wu Mu-Qing, Su Jing-Fang. Cyber-physical system. *Acta Automatica Sinica*, 2012, **38**(4): 507−517
(温景容, 武穆清, 宿景芳. 信息物理融合系统. 自动化学报, 2012, **38**(4): 507−517)

8 Liu E D, Cheng P. Achieving privacy protection using distributed load scheduling: a randomized approach. *IEEE Transactions on Smart Grid*, 2017, **8**(5): 2460−2473

9 Dai W B, Dubinin V N, Christensen J H, Vyatkin V, Guan X P. Toward self-manageable and adaptive industrial cyber-physical systems with knowledge-driven autonomic service management. *IEEE Transactions on Industrial Informatics*, 2017, **13**(2): 725−736

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 Humayed A, Lin J Q, Li F J, Luo B. Cyber-physical systems security-a survey. *IEEE Internet of Things Journal*, 2017, **4**(6): 1802−1831

12 Tian J, Tan R, Guan X H, Liu T. Enhanced hidden moving target defense in smart grids. *IEEE Transactions on Smart Grid*, DOI: 10.1109/TSG.2018.2791512, 2018.

13 Yang Q Y, Li D H, Yu W, Liu Y K, An D, Yang X Y, et al. Toward data integrity attacks against optimal power flow in smart grid. *IEEE Internet of Things Journal*, 2017, **4**(5): 1726−1738

14 Sun Qiu-Ye, Teng Fei, Zhang Hua-Guang. Energy internet and its key control issues. *Acta Automatica Sinica*, 2017, **43**(2): 176−194
(孙秋野, 滕菲, 张化光. 能源互联网及其关键控制问题. 自动化学报, 2017, **43**(2): 176−194)

15 Luo X Y, Yao Q, Wang X Y, Guan X P. Observer-based cyber attack detection and isolation in smart grids. *International Journal of Electrical Power and Energy Systems*, 2018, **101**: 127−138

16 Yan Y, Qian Y, Sharif H, Tipper D. A survey on cyber security for smart grid communications. *IEEE Communications Surveys and Tutorials*, 2012, **14**(4): 998−1010

17 Hasan M M, Mouftah H T. A study of resource-constrained cyber security planning for smart grid networks. In: Proceedings of the 2016 IEEE Electrical Power and Energy Conference. Ottawa, Canada: IEEE, 2016. 1−6

18 Mo Y L, Kim T H J, Brancik K, Dickinson D, Lee H, Perrig A, et al. Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 2012, **100**(1): 195−209

19 Osborne M J, Rubinstein A. *A Course in Game Theory*. Cambridge: MIT Press, 1994.

20 Hewett R, Rudrapattana S, Kijsanayothin P. Cyber-security analysis of smart grid SCADA systems with game models. In: Proceedings of the 9th Annual Cyber and Information Security Research Conference. Oak Ridge, Tennessee, USA: ACM, 2014. 109−112

21 Maharjan S, Zhu Q Y, Zhang Y, Gjessing S, Basar T. Dependable demand response management in the smart grid: a Stackelberg game approach. *IEEE Transactions on Smart Grid*, 2013, **4**(1): 120−132

22 Ma J H, Liu Y T, Song L Y, Han Z. Multiact dynamic game strategy for jamming attack in electricity market. *IEEE Transactions on Smart Grid*, 2015, **6**(5): 2273−2282

23 Sanjab A, Saad W. Data injection attacks on smart grids with multiple adversaries: a game-theoretic perspective. *IEEE Transactions on Smart Grid*, 2016, **7**(4): 2038−2049

24 Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V, Wu Q S. A survey of game theory as applied to network security. In: Proceedings of the 43rd Hawaii International Conference on System Sciences. Honolulu, HI, USA: IEEE, 2010. 1−10

25 Yuan Yong, Wang Fei-Yue. Sequential equilibrium analysis and computational experiments of a bargaining game with incomplete information. *Acta Automatica Sinica*, 2016, **42**(5): 724−734
(袁勇, 王飞跃. 不完全信息议价博弈的序贯均衡分析与计算实验. 自动化学报, 2016, **42**(5): 724−734)

26 Wang K, Du M, Maharjan S, Sun Y F. Strategic honeypot game model for distributed denial of service attacks in the smart grid. *IEEE Transactions on Smart Grid*, 2017, **8**(5): 2474−2482

27 Zhang Wei-Ying. *Game Theory Information Economics*. Shanghai: Truth and Wisdom Press, Shanghai Joint Publishing, Shanghai People′s Publishing House, 2012.
(张维迎. 博弈论与信息经济学. 上海: 格致出版社, 上海三联书店, 上海人民出版社, 2012.)

28 Lakshmanan K, de Niz D, Rajkumar R, Moreno G. Resource allocation in distributed mixed-criticality cyber-physical systems. In: Proceedings of the 30th International Conference on Distributed Computing Systems. Genova, Italy: IEEE, 2010. 169−178

29 Nash J [Author], Zhang Liang-Qiao, Wang Xiao-Gang [Translator]. *Essays on Game Theory*. Beijing: Capital University of Economics and Business Press, 2015.
(约翰 · 纳什 [著], 张良桥, 王晓刚 [译]. 纳什博弈论论文集. 北京: 首都经济贸易大学出版社, 2015.)

30 Ross S M [Author], Gong Guang-Lu [Translator]. *Stochastic Processes* (2nd edition). Beijing: China Machine Press, 2013.
(罗斯 [著], 龚光鲁 [译]. 随机过程. 第 2 版. 北京: 机械工业出版社, 2013.)

31 Li Y Z, Shi L, Cheng P, Chen J M, Quevedo D E. Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach. *IEEE Transactions on Automatic Control*, 2015, **60**(10): 2831−2836

32 Xie L, Mo Y L, Sinopoli B. False data injection attacks in electricity markets. In: Proceedings of the 1st IEEE International Conference on Smart Grid Communications. Gaithersburg, MD, USA: IEEE, 2010. 226−231

33 Smith R. Assault on California power station raises alarm on potential for terrorism. *Wall Street Journal*, 2014, 1−7

34 Tsang R. Cyberthreats, vulnerabilities and attacks on SCADA networks. University of California, Berkeley, USA, 2010.

35 Lee A. Guidelines for Smart Grid Cyber Security, NIST Interagency/Internal Report (NISTIR)-7628, 2010.

李 军 上海大学机电工程与自动化学院博士研究生. 主要研究方向为信息物理系统, 智能电网安全, 博弈论. 本文通信作者. E-mail: leejun@shu.edu.cn
(**LI Jun** Ph. D. candidate at the School of Mechatronic Engineering and Automation, Shanghai University. His research interest covers cyber-physical system, smart grid security, and game theory. Corresponding author of this paper.)

李 韬 华东师范大学数学科学学院教授. 2009 年获得中国科学院数学与系统科学院博士学位. 主要研究方向为随机系统, 信息−物理多主体系统, 博弈论.
E-mail: tli@math.ecnu.edu.cn
(**LI Tao** Professor at the School of Mathematical Sciences, East China Normal University. He received his Ph. D. degree from the Academy of Mathematics and Systems Science, Chinese Academy of Sciences in 2009. His research interest covers stochastic systems, cyber-physical multi-agent systems, and game theory.)