密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2019, 6(1): 87–99

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

理性密码协议专栏

博弈论与密码协议研究进展*

王 秦[1], 朱建明[2], 高 胜[2]

1. 北京信息科技大学 信息管理学院, 北京 100192
2. 中央财经大学 信息学院, 北京 100081
通信作者: 王秦, E-mail: qwangcufe@163.com

摘 要: 博弈论与密码协议研究的都是互不信任参与方之间的交互问题. 博弈论深化了密码协议的假设条件, 由对诚实或恶意参与方的研究延展到对理性参与方的研究, 对于解决秘密共享、安全多方计算等密码协议问题能够提供重要帮助. 博弈论目前已经成为密码协议研究领域的重要理论和工具之一. 本文对博弈论在密码协议研究中的应用进行了阐释, 在介绍博弈论基本概念的基础上, 主要依据不同的博弈方法对现有文献进行了分类总结, 分别介绍了完全信息静态博弈、完全信息动态博弈、不完全信息静态博弈、不完全信息动态博弈、随机博弈、演化博弈在信息安全研究中的应用, 对密码协议等信息安全问题中的攻防对抗、防御策略选取、定量安全投资、防御者相互依赖、社会最优达成等问题的博弈论建模方法做了简要介绍, 展示了行动次序、不完全信息、系统状态、有限理性等因素在博弈分析中的影响. 本文表明了博弈论的引入对于密码协议研究的重要价值, 也指出了博弈方法本身的局限性以及其他现有研究存在的不足, 并对未来可能的研究方向提供了建议.

关键词: 密码协议; 信息安全; 博弈论; 攻防; 相互依赖性

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000286

中文引用格式: 王秦, 朱建明, 高胜. 博弈论与密码协议研究进展[J]. 密码学报, 2019, 6(1): 87–99.

英文引用格式: WANG Q, ZHU J M, GAO S. Progress in research on game theory and cryptographic protocols[J]. Journal of Cryptologic Research, 2019, 6(1): 87–99.

Progress in Research on Game Theory and Cryptographic Protocols

WANG Qin[1], ZHU Jian-Ming[2], GAO Sheng[2]

1. School of Information Management, Beijing Information Science and Technology University, Beijing 100192, China
2. School of Information, Central University of Finance and Economics, Beijing 100081, China
Corresponding author: WANG Qin, E-mail: qwangcufe@163.com

Abstract: Game theory and cryptographic protocols are both concerned with the interaction among distrustful participants. Game theory deepens the hypothetical conditions of cryptographic protocols,

* 基金项目: 国家重点研发计划 (2017YFB1400700), 国家自然科学基金 (61272398, 61602537, U1509214), 中央财经大学“青年英才”培育支持计划 (QYP1808)

Foundation: National Key Research and Development Program of China (2017YFB1400700), National Natural Science Foundation of China (61272398, 61602537, U1509214), Youth Talent Support Program of Central University of Finance and Economics (QYP1808)

收稿日期: 2018-06-07 定稿日期: 2018-09-04

extending from the study of honest or malicious participants to the study of rational participants, which can provide significant help for solving cryptographic protocols such as secret sharing and secure multi-party computation. Game theory has become one of the important theories and tools in the field of cryptographic protocols. This paper explains the application of game theory in cryptographic protocol research. On the basis of introducing the basic concepts of game theory, the existing literatures are classified and summarized mainly according to different game methods. This paper respectively introduces the application of complete information static game, complete information dynamic game, incomplete information static game, incomplete information dynamic game, stochastic game, and evolutionary game in the study of information security, briefly introduces the game theoretic modeling methods of problems in information security such as cryptographic protocols including the conflicts between attacks and defenses, defense strategy selection, quantitative security investment, interdependence among defenders, and social optimization achievement, and shows the effects of action sequences, incomplete information, system states, limited rationality, and other factors in game theoretic analyses. This paper demonstrates the significant value of the introduction of game theory to cryptographic protocol research, points out the limitations of game theory itself and other existing research deficiencies, and provides suggestions for possible future research directions.

Key words: cryptographic protocol; information security; game theory; attacks and defenses; interdependence

1 引言

随着互联网的快速发展, 越来越多的组织使用信息技术来存储、处理、交换关键信息, 信息已成为当今社会最重要的商业资产之一. 然而, 与信息技术飞速进步相伴随的是信息安全事件的频发及其对经济社会造成的持续严重影响. 根据国家互联网应急中心 (CNCERT/CC) 发布的《2016 年中国互联网网络安全报告》, 2016 年的移动互联网恶意程序捕获数量、网站后门攻击数量以及安全漏洞收录数量较 2015 年均有所上升, 其中移动互联网恶意程序数量增加 39%, 被植入后门的网站数量增加 9.3%, 软硬件漏洞增加 33.9%. 而仅在 2016 年 11 月, 就有 194 万个境内终端感染病毒, 5294 个境内网站被篡改, 5283 个境内网站被植入后门. 在信息安全方面的不够重视, 往往会给企业乃至国家造成极其严重的危害. 这样的例子在国内外安全实践的发展中屡见不鲜. 例如, 由于相关保护措施不力, 索尼影业曾在 2011 年遭遇黑客入侵, 致使 7700 多万个 PlayStation Network 账户被盗. 2014 年该公司再次遭遇大规模黑客攻击, 给公司造成巨额经济损失, 甚至逐渐酿成一起国际政治事件.

密码学是信息安全的基础, 密码协议是信息安全重要的组成部分. 对于信息安全来说, 信息安全技术无疑是最重要的. 甚至很多人认为, 只要有形式化证明了的密码协议和防火墙等安全技术, 系统就一定能达到高度安全. 事实上, 虽然信息安全技术一直扮演着不可或缺的角色, 但是信息安全问题无法通过技术手段彻底解决的, 层出不穷的信息安全事件也印证了这一点. 一方面, 任何技术都可能同时被防御者和攻击者所用, 甚至在现实中攻击者对新技术的采用往往限于防御者, 许多最新的信息安全技术即源于黑客行为. 攻击者占据者对于防御者的天然优势, 防御者在攻击者面前永远属于被动的一方. 攻击行为不仅通常无法事先被判断, 攻击者甚至常常能绕过相关法律和规则实施行动. 一方面, 信息安全必须遵循 “适度安全” 的原则, 防御者无法做到投入所有资源对所有可能的弱点进行保护, 必须根据有限的资源做出最优决策 [1]. 因此, 解决信息安全问题需要综合运用信息技术、经济学和管理学等理论方法.

博弈论是研究决策主体的行为发生相互作用时的决策及其均衡问题的理论, 是研究竞争中参与者为争取最大利益应当如何做出决策的数学方法. 近年来, 博弈论已经成为了信息安全经济学中的主要方法之一. 博弈论擅长刻画的策略依存性可以很好地描述信息安全中的攻防对抗以及防御方之间的互相影响. 博弈论给出了信息安全问题中利益互相冲突依赖的参与方一个定量的决策框架, 这是传统的安全技术方法和其他经济学方法难以做到的 [2].

博弈论和密码协议处理的都是互不信任团体之间的交互问题 [3]. 博弈论的理性假设为密码协议的研

究提供了新的思路. 博弈论的引入对预测密码协议中参与方的行为和涉及更加安全有效的密码协议具有重要意义. 本文对博弈论在密码协议等信息安全研究中的应用进行了综述, 依据不同博弈类型, 试图分析其在密码协议设计、攻防对抗、防御策略选取、定量安全投资、防御者相互依赖、社会最优达成等信息安全问题中的应用.

以下各节的内容安排如下: 第2节简要描述了本文要用到的博弈论基本概念; 第3节介绍了完全信息静态博弈、完全信息动态博弈、不完全信息静态博弈、不完全信息动态博弈、随机博弈、演化博弈在密码协议等信息安全研究中的应用; 第4节指出了当前研究存在的不足和未来的研究方向.

2 博弈论概述

博弈论是研究相互影响的决策主体如何进行决策以及达成均衡的学科. 在博弈中, 博弈是指参与人在考虑其他参与人行动的情况下, 基于收益最大化原则选择相应行动. 自上世纪四十年代诞生以来, 博弈论经过不断发展已经成为经济学的一个重要分支.

博弈论的基本概念包括参与人、行动、支付、战略等. 参与人是指博弈中的决策实体. 参与人可以指代人、机器、团体等. 行动是指参与人在博弈某个时点做出的决策. 支付是指参与人依据自身行动以及其他参与人行动而得到的回报. 战略是指参与人在博弈中的行动计划.

一般而言, 一个博弈可以表述为如下形式 [4]:

$$G=\{S_1,S_2,\cdots,S_n;u_1,u_2,\cdots,u_n\},i=1,2,\cdots,n$$

其中, S_i 为参与人 i 的策略集, 有 $s_i\in S_i$. 参与人 i 的支付函数 $u_i(s_1,s_2,\cdots,s_n)$ 为所有参与人策略的函数.

博弈有多种分类方法. 根据参与人对其他参与人的了解程度, 博弈可以分为完全信息博弈和不完全信息博弈. 完全信息博弈中所有参与人对其他参与人的战略空间、支付函数等信息有充足的了解. 不完全信息博弈中至少有一个参与人对至少其他一个参与人的战略空间或支付函数等信息不了解. 根据参与人的行动的时序性, 博弈可以分为静态博弈和动态博弈. 静态博弈是一次性博弈, 参与人同时做出行动. 动态博弈包含多个阶段, 参与人的行动有先后之分. 这两种分类标准结合可以将博弈论分为完全信息静态博弈、完全信息动态博弈、不完全信息静态博弈和不完全信息动态博弈.

随机博弈也称马尔可夫博弈, 是马尔可夫决策过程在多主体环境下的扩展形式. 随机博弈的主要元素包括状态集、行动集、状态转移函数、支付函数等. 每一阶段参与人的支付由当前状态和参与人行动共同决定, 博弈根据当前状态和参与人行动以一定概率过渡到下一状态. 随机博弈从定义上属于动态博弈, 然而相较传统博弈形式, 随机博弈擅长描述多主体间较大行动空间和较长规划周期的博弈问题, 这使得随机博弈在信息安全领域有较为广泛的应用. 尤其是随机博弈与网络模型以及学习算法的结合使得随机博弈模型十分适合处理网络安全中复杂的动态问题. 本文将单独对随机博弈在信息安全研究中的应用进行说明.

演化博弈论改变了传统博弈论关于参与人完全理性的假设, 将关注点放在长期形成的演化稳定策略. 演化博弈论模仿了达尔文竞争的思想, 认为不同的战略将在长期经过生存和繁殖并达到均衡. 演化博弈论中加入了复制动态这一关键概念, 即更具适应性的个体如何在群体中不断扩张. 演化博弈论正被越来越多地应用于经济学、社会学等领域中.

3 博弈论在密码协议等信息安全研究中的应用

在总结现有文献的基础上, 表1展示了博弈论在密码协议等信息安全领域的应用.

信息安全攻防策略分析是博弈论应用的重要方面, 包含了各种博弈论方法的运用, 分析情境包括入侵检测系统、无线传感器网络、信息战、容忍入侵系统等等. 作为信息安全主要工具, 针对入侵检测系统的分析在这一部分占据了主要部分, 具体研究问题包括响应策略、资源配置、恶意软件监测器放置等.

表 1 现有文献分类比较

Table 1 Classification and comparison of present literatures

研究对象	研究对象	文献	博弈论方法
信息安全攻防博弈	入侵检测系统	[6]	完全信息动态博弈
		[7]	不完全信息静态博弈、不完全信息动态博弈
		[8–10]	不完全信息动态博弈
		[11–14]	随机博弈
		[15]	演化博弈
	信息战	[16]	完全信息静态博弈
	容忍入侵系统	[17]	随机博弈
	企业网络	[18]	随机博弈
	智能电网	[19]	随机博弈
	自适应软件系统	[20]	随机博弈
	自组织网络	[21]	演化博弈
	无线传感器网络	[22, 23]	演化博弈
	其他一般意义下的攻防对抗研究	[1]	完全信息静态博弈
		[24]	完全信息静态博弈
		[25]	完全信息静态博弈
		[26]	完全信息动态博弈
		[27]	不完全信息静态博弈
		[28, 29]	不完全信息动态博弈
		[13, 30–32]	随机博弈
		[33]	演化博弈
信息安全防御者相互依赖关系博弈	外部性	[34–40]	完全信息静态博弈
	不确定性	[41–43]	不完全信息静态博弈
密码协议	安全多方计算	[44]	完全信息静态博弈
		[45–47]	不完全信息动态博弈
	秘密共享	[45, 46, 48]	不完全信息动态博弈
	其他一般意义下的安全协议设计	[49]	不完全信息动态博弈

信息安全防御者相互依赖关系博弈的研究主要包括对外部性和不确定性的研究, 这一部分使用的研究方法为静态博弈. 信息安全具有公共物品的属性, 各个防御主体的安全投资可能会相互影响. 总体的安全程度取决于每个主体, 当安全程度不高时, 所有主体都会受害. Kunreuther 等首先于 2003 年率先提出了一般意义下的相互依赖安全问题 [5]. 作者假设存在多个自私的参与者, 他们可以选择投资于安全或维持现状. 这些个体都想在一定风险水平下投资最少, 而风险不仅取决于自己的投资情况, 也取决于其他参与者的投资情况. 可以证明, 包含两个直至多个参与者的情况下, 所有个体间只存在两种纳什均衡: 全部投资或全部不投资.

与经济学中对公共物品的研究一样, 相互依赖环境下防御者有投资不足的倾向, 难以达到全局最优, 需要采取奖励、惩罚等手段消除这种外部性. 另外, 相互依赖环境下也存在关于其他主体安全投资以及被攻击概率等的不确定性问题, 这种影响适合使用不完全信息博弈来刻画.

信息安全博弈论在密码协议中的应用主要体现在秘密共享和安全多方计算问题的协议设计上, 使用的主要方法为不完全信息动态博弈. 传统的密码协议都假定参与方或者诚实、或者恶意. 其中诚实的参与方在通信过程中总是遵守协议, 而邪恶的参与方总是使用各种手段欺诈其他参与方而违背协议. 博弈论的观点认为所有参与方都是理性的, 即保证自身利益最大化. 与此相反, 密码协议中并不排斥非理性行为. 这是博弈论与安全多方计算的最大区别. 关于博弈论与密码协议 (以安全多方计算问题为例) 的比较可以参见表2 所示.

表 2 密码协议与博弈论的比较

Table 2 Comparison of cryptographic protocols and game theory

对比项	密码协议	博弈论
动机	在模型之外	博弈支付
参与方	完全诚实或恶意	理性
解决方案	安全协议	均衡
隐私	目标	工具
提前结束	可能	不会

典型的秘密共享问题是指秘密份额被分发给参与者, 只有一定数量以上的参与者才能重构出秘密. 安全多方计算问题中参与者只能接受自己的私密输入, 并不能从他人的输入中获得任何额外信息. 在安全多方计算问题的博弈形式中, 参与者的类型是其输入, 每个参与者试图猜测输出. 他们都想得到正确的输出, 而不希望其他参与者得到正确输出. 另外, 参与者也希望尽可能少地泄露自己的输入, 尽可能多地得到其他参与者的输入. 博弈论通过为理性参与者设计安全协议给安全多方计算问题提供解决方案.

下面以不同博弈论方法为依据介绍博弈论在信息安全研究中的应用.

3.1 完全信息静态博弈

作为信息安全相互依赖关系中的主要模型, 文献 [34] 首次将共同贡献模型、最弱环模型和最佳防御模型引入到信息安全领域的分析中. 在共同贡献模型中, 系统的防御水平取决于各主体贡献之和, 相应地, 在最弱环模型和最佳防御模型中, 系统的防御水平分别取决于防御水平最低和防御水平最高的主体. 对于纳什均衡的研究发现, 在共同贡献模型和最佳防御模型中, 系统可靠性取决于具有最高收益成本比的主体, 在最弱环模型中系统可靠性取决于具有最低收益成本比的主体, 而其他个体都将采取 “搭便车” 的行动. 而关于社会最优的分析表明, 搭便车的行为会导致主体的安全贡献低于社会最优条件下要求的安全贡献水平. 此类相互依赖安全博弈的比较如表3 所示.

文献 [35] 在继承文献 [34] 的基础上, 加入了对保险的分析, 并且提出了最弱目标安全博弈, 即攻击者只对防御水平最低的个体进行攻击. 结果表明在纳什均衡下, 最弱目标安全博弈中主体的投资水平社会最优下的水平. 文献 [36] 基于最弱环模型和共同贡献模型分析了互联网服务提供商如何使用基于结果或贡献的奖惩措施提高整个系统的安全水平.

文献 [37] 考虑了相互依赖条件下的信息安全投资博弈. 作者假设病毒可以通过直接和间接两种方式传染, 而企业的信息安全投资只能消除直接传染的风险. 通过分析单次侵入和多次侵入假设下的参与方支

表 3 相互依赖安全博弈类型比较

Table 3 Comparison of different types of interdependent security games

博弈类型	描述	参考文献
共同贡献安全博弈	系统的防御水平取决于个体贡献之和	[5,26,27,34,35]
最弱环安全博弈	系统的防御水平取决于防御水平最低的个体	[5,27,34,35]
最佳防御安全博弈	系统的防御水平取决于防御水平最高的个体	[5,26,27,34]
最弱目标安全博弈	攻击者只对防御水平最低的个体进行攻击	[5]

付和均衡情况, 作者指出无论是单次入侵还是多次入侵, 博弈只存在两种均衡, 即全部投资或全部不投资.

文献 [38] 重点关注了攻击类型在信息安全投资博弈中的影响. 作者假设公司面对目标攻击或随机攻击, 分别分析了在两种攻击类型下最优信息安全投资水平与潜在损失、内在脆弱性和网络脆弱性之间的关系, 还讨论了责任和安全信息共享这两种机制对安全投资的影响.

安全市场具有柠檬市场的特点, 文献 [39] 指出安全审计可以改善参与方之间的信息不对称问题, 并且可以帮助参与方发出可信信号, 解决参与方之间的协调问题. 作者建立的博弈论模型刻画了信息安全审计的完全性, 信息安全投资对于降低风险的作用以及参与方之间的相互依赖情况. 对于均衡结果的分析表明, 安全审计必须针对特定情境展开, 并且基本的审计水平在多数情况下可能是无效的.

文献 [1] 研究了攻击者和防御者之间的完全信息静态博弈模型, 讨论了零和与非零和博弈情况下的最优防御策略选取算法. 作者还通过改进传统的攻击图模型提出了网络防御图模型, 并且分析了攻防策略的分类方法和成本收益情况.

文献 [24] 提出了一种新的网络安全风险评估方法. 文中使用博弈论建立了防御者与攻击者之间的对抗模型. 防御者有两个行动可以选择, 即保护知识财产或不保护知识财产, 攻击者可以选择不采取行动、开发知识财产或者以一定概率攻击知识财产. 文章对该模型以及基于部分可观测马尔可夫决策过程建立的攻击模型进行了定量分析.

文献 [16] 将信息战刻画为攻防双方的博弈. 文中列举了几个例子来说明参与方如何根据不同情境使用纯策略或混合策略等问题.

文献 [50] 使用博弈论和马尔科夫决策过程等方法来研究传感器网络的入侵检测问题. 文中将入侵检测问题建模为包含攻击者和传感器网络两个参与方的非零和博弈. 文中指出使用博弈论模型可以提高成功识别的几率.

文献 [25] 使用博弈论研究了基于问题机制抵御泛洪攻击的方法. 在这一模型中, 服务器并不区分合法用户或非法用户. 每当客户端发出连接请求时, 服务器先生成一个 “问题”. 只有当客户端回答正确时, 服务器才会分配资源与之建立连接. 问题的质量是决定这一机制是否成功的重要因素. 此外, 对问题数据库的防御和维护也是需要重点考虑的问题.

文献 [40] 研究了作为自私参与方的信息安全投资的效率问题. 文中使用无政府状态的代价 (POA), 即最坏情况下的纳什均衡结果和社会最优结果之比来衡量这一效率, 并进一步提出了加权 POA 的概念. 文中的完全信息静态博弈模型假定参与方的安全投资互相影响, 作者分析了其纯策略纳什均衡下的情况.

安全多方求和属于安全多方计算的基本操作. 文献 [44] 改变传统安全求和方法中参与方行为良好的假定, 分别分析了完全信息静态博弈下不成提供数据以及共谋下的均衡情况, 提出了一种安全求和算法, 结果表明算法可以很好地保护隐私.

3.2 完全信息动态博弈

文献 [40] 中在对完全信息静态博弈模型下的假定做出小幅修改后, 进一步提出了重复博弈, 分析了社会最优子博弈精炼纳什均衡下的效率问题. 文中指出虽然重复博弈下更有可能达成合作, 但也需要参与方之间更多的沟通和协调.

文献 [6] 提出了公司和用户之间的完全信息动态博弈模型, 用以分析入侵检测系统的价值. 博弈被分为两个阶段. 在第一阶段, 公司决定是否采用入侵检测系统. 在第二阶段, 公司决定是否对入侵检测系统进行配置, 用户选择其攻击策略.

文献 [51] 研究了对于网络入侵的自动响应问题. 文中提出的斯塔克尔伯格博弈模型被用于用户的注册登录过程. 文中对于小型网络使用马尔可夫决策方法做出最优响应, 对于大型网络使用模糊规则集做出最优响应.

文献 [26] 将对攻击者有限理性的假设纳入网络安全博弈研究. 由于现实中的网络及其复杂, 攻击者很难对网络全局有清晰的了解, 因此引入有限理性的假设十分必要. 文中将攻击者和防御者的交互建模为斯塔克尔伯格博弈模型. 博弈在图上进行. 攻击者的纯策略由从起始节点到目标节点的所有路径组成. 防御者安排有限资源在边上设置检查点. 若攻击者选择的路径已经被检查点覆盖, 则防御者得到奖励, 攻击者受到惩罚. 否则攻击者得到奖励, 防御者受到惩罚. 文中假设博弈是非零和的. 由于攻击者会监控防御者的战略, 防御者必须随机选择战略, 即使用混合战略来应对. 文中假设攻击者可以观测到防御者的资源总数和每条边被覆盖的概率. 文中提出了几种不同的攻击者行为模型, 并研究了如何计算防御者的最优战略.

文献 [34] 还考虑了参与方序贯行动的情形, 并假设后行动者可以观察到先行动者的选择. 文中指出为了保证达到最高安全水平, 必须保证具有最低收益成本比的主体率先行动.

3.3 不完全信息静态博弈

文献 [27] 建立了推断攻击者意图、目标和战略的一般博弈模型. 作为示例, 文中的贝叶斯博弈模型中假设主体有两个类型, 即好或坏, 并且该类型是主体的私人知识. 博弈包含有限个阶段, 每个阶段主体和防御系统同时行动. 文中证明即使只有很少的信息, 该模型也能得出满意的结果.

由于网络的复杂性, 现实用户可能并不了解网络的结构信息以及其他用户的安全贡献. 并且用户出于自私性可能并不愿意分享自己的安全贡献信息. 文献 [41] 分析了考虑拓扑信息不确定性的安全投资博弈模型. 文中把网络用户之间的交互建模为不完全信息静态博弈模型. 模型假设用户只知道自己的度信息, 但并不知道邻居的度信息. 用户的战略是自己的安全投资. 用户的支付取决于与邻居用户投资之和或者其中的最大投资有关. 文中证明了单调对称贝叶斯纳什均衡的存在, 并且证明了连接程度更高的用户可能会付出更少的安全投资而获得更高的效用.

文献 [42] 分别比较了共同贡献模型、最弱环模型和最佳防御模型三种安全博弈模型不确定性的代价. 在完全信息状态下, 所有主体的被攻击概率是共同知识; 在不完全信息状态下, 每个主体只知道自己被攻击的概率以及其他主体被攻击的概率分布. 与其他衡量效率的标准类似, 作者使用在完全信息状态和不完全信息状态下支付的最大差别来衡量不确定性的代价. 根据这一思想, 作者提出了最大差别、收益比、成本比等三种标准.

文献 [43] 分析了相互依赖安全博弈中的不确定性问题. 作者假设每个主体只知道风险参数的概率分布, 分别分析了在同质主体和异质主体假设下的贝叶斯纳什均衡. 作者发现在同质主体的假设下, 较低的感染风险可能会导致更高的威胁概率, 较高的感染风险可能会导致更低的威胁概率.

文献 [7] 研究了自组织网络中的入侵检测问题. 由于自组织网络固有的能量约束, 传统的对入侵检测系统保持始终打开状态的选择可能并不有效. 作者假设防御者并不知对手的类型是常规的还是恶意的, 并分别提出了不完全信息静态博弈模型和不完全信息动态博弈模型, 分析了其贝叶斯纳什均衡和精炼贝叶斯均衡. 在不完全信息静态博弈模型中, 作者得出当防御者认为对手为恶意的概率较大时, 博弈会达成混合策略贝叶斯纳什均衡, 否则会达成纯策略贝叶斯纳什均衡.

3.4 不完全信息动态博弈

文献 [7] 中不完全信息动态博弈模型和不完全信息静态博弈模型的假定类似. 对于不完全信息静态博弈模型很难准确给定信念, 而不完全信息静态博弈模型中防御者可以不断调整自己的信念. 作者指出后者是更加现实的模型. 作者在模型基础上进一步提出了贝叶斯混合检测方法, 即使用轻量级监控系统估计对手行动, 而重量级监控系统被留到最后使用. 作者指出这一方法有助于减少能量消耗, 提高检测效果.

文献 [52] 将自组织网络中攻击者和入侵检测系统之间的交互建模为信号传递博弈. 攻击者的行动可以视作信号, 入侵检测系统基于对攻击者的信念处理信号.

文献 [28] 也使用信号传递博弈来建模网络中攻击者和防御者之间的交互. 防御者使用蜜罐技术来保护其网络. 防御者可以选择将蜜罐伪装成正常的系统, 或者将正常的系统伪装成蜜罐. 攻击者可以成功攻击正常的系统, 但并不能成功攻击蜜罐. 如果攻击者攻击蜜罐, 则防御者观察到攻击者的动作并可以在随后提高防御. 作者分析了该模型的精炼贝叶斯均衡, 并用两个案例分析展示了防御者采用欺骗战略的好处.

文献 [8] 提出了分布式入侵检测系统的一般模型, 并基于博弈论提出了两个不同的方案, 即安全预警系统模型和安全攻击博弈模型. 其中, 前者使用合作博弈来建模, 后者使用非零和不完全信息动态博弈来建模. 文献 [9] 基于文献 [8] 中的模型研究了攻击者和入侵检测系统之间的动态博弈, 分别研究了有限博弈和无限博弈的形式. 作者建立了一套定量化的数学模型来处理入侵检测中的资源分配问题. 文献 [10] 中作者将访问控制系统的入侵响应视作资源分配问题. 作者将系统管理员用来响应攻击的时间作为稀缺资源来考虑, 提出了一套结合了神经网络和线性规划方法的资源分配算法. 文中的博弈模型是在文献 [9] 中模型的基础上经过修改发展而来的.

文献 [29] 研究了攻击者和防御者之间的不完全信息非零和博弈. 攻击者可以选择攻击或者不攻击, 防御者可以选择防御或者不防御. 双方对对方的支付函数都不了解, 只能根据对方的行动调整自己的战略. 作者基于虚拟对策博弈构建模型, 并对模型进行了仿真分析.

文献 [45] 说明了将理性条件加入对秘密共享和安全多方计算的研究中. 作者假设参与方倾向于自己获取秘密, 并且有尽可能少的其他参与方获取秘密. 只有当自己的效用提高时, 参与方才会遵守协议. 作者证明不发送秘密份额是弱占优策略. 并且, 在使用随机机制的情况下其计算可以在常数时间内完成.

文献 [46] 研究了秘密共享和安全多方计算的公平协议问题. 作者假设对于输入分布函数和参与方效用只有不完全信息, 分别分析了联播信道和非联播信道下的协议设计. 其设计的协议可以进行任意轮迭代, 不受逆向归纳的影响.

文献 [49] 基于扩展式博弈建立安全协议模型, 通过分析博弈过程, 可以很好地预测各方的策略选择及其原因.

文献 [48] 分析了博弈论环境下的秘密分发机制和秘密重构机制. 作者在秘密分发机制中引入了理性第三方的概念, 并设计了一个秘密重构机制以解决参与方的合作问题.

文献 [47] 尝试在理性密码协议与传统博弈论之间建立联系, 作者考虑了计算成本, 证明了防范秘密攻击的两方安全计算是计算博弈中可忽略的调解人的通用实现.

3.5 随机博弈

文献 [30] 将网络中攻击者与管理员之间的交互建模为非零和随机博弈. 作者将网络建模为外部世界、Web 服务器、文件服务器、工作站之间交互的环境. 外部世界可以通过防火墙与 Web 服务器进行联系, Web 服务器、文件服务器、工作站三者之间可以互相联系. 作者使用非线性规划方法对纳什均衡求解. 通过设置不同的初始条件, 作者得到了三个纳什均衡, 并对均衡结果进行了讨论.

文献 [31] 改变了文献 [30] 中完美信息的假定, 将攻击者和防御者之间的交互建模为非完美信息博弈模型. 作者指出现实中参与方通常使用传感器来判断系统状态, 因此论文假定参与方在某一特定时刻以一定的错误概率知晓系统的真实状态. 文中提出的基于博弈论的半自动化防御架构包含三个主要组件: 博弈代理和中央博弈协调者的集合, 管理控制台以及动态蜜罐. 系统管理员使用奖惩结合的措施来引导攻击者行为. 作者还提出了一系列对模型的扩展来应对可能的挑战.

文献 [11] 将攻击者和入侵检测系统之间的交互建模为随机博弈模型. 攻击者试图对系统进行非授权访问或者发起拒绝服务攻击, 入侵检测系统分配系统资源搜集信息来检测并做出响应. 作者假设每个参与方并不知道其他参与方的行动和系统的演进状态, 只能基于自身成本和关于系统和其他参与方的有限观测进行决策.

文献 [12] 基于线性影响网络模型建立了攻击者和入侵检测系统之间的零和随机博弈模型. 作者使用加权有向图来表示网络中节点安全资产和脆弱性的相互关系. 线性影响网络的加入也有助于使用计算机程序对博弈求解.

文献 [17] 研究了入侵者和容忍入侵系统之间的零和随机博弈模型. 作者分析了系统可用性、完整性、机密性的平均失效时间, 以及攻击意愿、攻击收益和行动策略之间的关系.

文献 [18] 研究了网络中参与方之间的随机博弈网模型. 由于随机博弈存在无法反映复杂网络结构等缺点, 作者提出的模型结合了 Petri 网技术. 论文的结果被用于企业网络的安全分析中.

文献 [53] 基于马尔可夫博弈提出了一种新型的风险评估模型. 传统的风险评估方法无法考虑未来的安全状态. 作者提出的模型可以考虑未来可能的风险对当前风险评估的影响, 其影响随距离当前时间的增长而下降. 模型使用马尔可夫链来描述威胁传播过程以及系统管理员对系统脆弱性的修复过程. 一方面,

针对脆弱性的威胁会导致风险, 并且风险随威胁的传播而增大; 另一方面, 风险会因系统管理员的修复行动而变小. 模型模拟了威胁和脆弱性之间的关系. 作者还设计了一套风险评估平台来验证模型的有效性.

文献 [32] 提出了一种攻击者和网络之间零和马尔可夫博弈模型的分解求解方法. 模型假设攻击者无法观察到网络状态. 由于均衡战略随博弈阶段数呈指数级增长, 作者利用其嵌套信息结构将博弈分解为若干个子博弈, 并使用逆向归纳法来求解博弈. 作者表明通过计算每个阶段一个信息集上的单值函数, 博弈能被有效求解.

文献 [19] 研究了智能电网关键基础设施保护问题, 建立了智能电网保护者和攻击者之间的马尔可夫博弈模型. 为了解决博弈模型的可扩展性问题, 作者提出了一种剪枝算法在计算时间和计算精确度之间进行平衡.

文献 [13] 从数据融合和自适应控制的角度研究了对网络安全系统的评估和保护. 由于攻击工具和技术正变得越来越复杂, 下一代网络管理和入侵检测系统要求能融合短期传感器数据和长期知识数据库中的数据来提供决策支持. 作者提出了一种基于马尔可夫博弈的自适应数据融合方法. 作者假设参与方之间并不了解对方的成本函数, 并使用马尔可夫博弈方法估计对网络攻击类型的信念.

文献 [14] 使用攻击者和入侵检测系统之间的零和马尔可夫博弈模型研究了恶意软件监测器的放置问题. 恶意软件监测器的放置在基于网络的入侵检测系统设计中十分重要. 检测器可以被用作已有网络部件, 也可以被用作单独的设备. 通过对模型最优战略的求解和仿真分析, 作者说明了如何在网络环境中更好地使用恶意软件检测器.

文献 [20] 研究了攻击者和自适应管理器之间的零和马尔可夫博弈模型. 自适应管理器可以在动态攻击场景中不断修正自己的战略. 作者研究了如何将模型应用于 IBM 公司提出的 MAPE-K 参考模型中, 并使用动态应用层拒绝服务攻击案例仿真证明了模型的适用性.

3.6 演化博弈

文献 [21] 使用演化博弈论研究了 AODV 路由协议下自私节点的动态合作行为. 在数据转发的过程中, 节点可能会由于自私性丢包导致数据传输率下降. 作者提出了一个重复包转发框架, 并使用遗传算法学习和预测最优响应. 包转发路径上的每一节点都会通过直接监控学习邻居节点行动, 基于博弈模型预测邻居节点行动, 并选择最适合的节点将数据包转发出去. 仿真结果证明通过使用演化战略和信任评价机制, 节点之间可以达到最大化的合作.

文献 [22] 基于博弈论和模糊逻辑提出了一种自适应协调器选择算法. 文中的博弈模型包含两部分: 针对动态防御的随机博弈和针对协调器选择的演化博弈. 在演化博弈框架中, 参与方为网络中的节点, 协调器选择战略为来自不同邻居的估计信息的本地组合. 模糊逻辑被用于构建选择协调器的状态估计算法.

文献 [23] 提出了一种无线传感器网络的安全速率博弈, 其目的是最大化传感器节点安全速率并最小化数据传输能量消耗. 作者将经典窃听信道扩展到簇状无线传感器网络, 以获得安全速率的对应计算公式. 作者构建的演化博弈模型反映了传感器节点和能量消耗成本之间的交互联系. 通过求解演化稳定策略, 作者解释了传感器节点如何选择战略, 并提出了一个对应的安全速率自适应算法.

文献 [33] 研究了信息安全攻防对抗的演化博弈模型. 模型中防御者可以选择投资或不投资, 攻击者可以选择攻击或不攻击. 防御者的投资行动可以抵御攻击并给其带来一定的商誉无形资产, 但必须付出投资成本. 通过对演化稳定策略的分析, 作者指出了投资成本在影响投资行动中的关键作用.

文献 [15] 研究了入侵者和入侵检测系统之间的演化博弈模型. 作者假设如果入侵者入侵, 入侵检测系统做出正确响应, 则入侵者将在付出入侵成本的同时受到惩罚, 入侵检测系统将获得收益. 作者分析了博弈的演化稳定策略, 并指出了使用演化博弈论分析入侵检测系统的好处.

4 总结

本文介绍了使用博弈论研究密码协议等信息安全问题的优势, 考察了完全信息静态博弈、完全信息动态博弈、不完全信息静态博弈、不完全信息动态博弈、随机博弈、演化博弈等不同类型的博弈模型在信息安全研究中的应用. 当前研究仍存在一些不足. 现实中安全环境极其复杂, 攻击概率、风险损失等参数通常难以估计, 并且当前形势下攻击手段越来越多样化, 更给建模带来难度以外. 因此, 基于博弈论的信息

安全研究需要更先进的安全参数刻画方法作为支撑. 此外, 由于博弈论自身的理论特性, 使用博弈论对信息安全进行研究可能还会出现以下问题:

第一, 许多信息安全博弈模型存在多个纳什均衡, 不同的均衡间参与方的支付可能差异很大, 会导致模型的可靠程度大幅下降. 此外, 一些较为复杂的博弈模型对均衡战略的求解往往十分困难, 使得必须付出一定代价对求解过程进行简化.

第二, 攻击者和防御者都可能同时采取多个行动, 但目前使用博弈论同时刻画多个行动仍然存在困难.

第三, 在现实中, 参与方采取行动以及系统状态转换都需要一定时间, 而博弈论通常假定其立即完成, 忽略这种时间影响可能会使模型与现实情况产生巨大偏差. 事实上, 参与方采取行动所需的时间一般很不规律, 而在复杂度较高的场景下, 不同的时间长度对于最优行动的计算影响很大.

第四, 博弈论只能处理建立在已知行动集上的问题. 而在现实中, 随着攻击的深入和时间的推移, 攻击者可能采用新的方法发动攻击, 防御者也必须对这种可能性做出防范.

鉴于现有研究存在的不足, 今后可以考虑从以下方向展开研究:

第一, 对攻击者的刻画. 攻击者发动攻击的原因是多种多样的, 可能是为了谋取经济利益, 获得同行尊重, 或者仅仅是为了满足某种满足感或者尝试某种最新技术. 即使仅仅为了谋取经济利益, 对于不同攻击者的计量标准往往也并不相同. 在具体情景下, 攻击者的目标可以是某一单一目标, 也可以是多种目标的组合. 甚至随着时间的推移, 攻击者还可能改变目标. 现有研究对于攻击者的建模通常较为简单, 比如将攻击者的效用简单等同于防御者的损失. 因此需要开发针对攻击者效用的新的计量方法, 考虑更为复杂的博弈模型.

第二, 基于网络拓扑的研究. 可以将博弈参与方视为计算机网络中的节点. 网络拓扑使得博弈参与方之间存在着复杂的相互影响关系, 不同网络的拓扑特征使其具有不同的鲁棒性. 然而, 简单地借用传统网络模型并不能准确地刻画计算机网络. 当前还很少有研究考虑网络拓扑的影响, 需要开发新的方法针对计算机网络进行研究.

第三, 实证研究的加入. 对各种风险参数评估的困难既降低了防御者投资信息安全的动力, 增大了攻击者成功的机会, 也降低了博弈模型的可信度. 需要建立行业统一的大规模数据集以供研究者和实践者分析使用. 可以利用机器学习等方法基于这些数据进行风险评估和决策制定.

第四, 对于信息安全投资的建模. 当前研究一般假定信息安全投资要么是离散的要么是连续的. 但是, 现实中信息安全投资通常是多维的, 管理者一般将信息安全预算分散于设备购置、员工培训、网络保险购买等上面. 对于信息安全投资需要更加复杂的建模方式.

第五, 与机制设计理论的结合. 通过调整相关参数等手段, 可以使用机制设计理论研究如何将博弈导向更令决策者满意的均衡. 机制设计理论可以在安全协议设计中扮演重要作用.

由于作者精力所限, 一些重要的文章可能没有被包括在内. 此外, 由于基于博弈论的密码协议等研究刚刚起步, 相关参考文献有限, 本文只是对这一领域所做的探索性分析, 作者期待以后有文章能对这一主题进行更加系统的阐述.

References

[1] JIANG W, FANG B X, TIAN Z H, et al. Evaluating network security and optimal active defense based on attack-defense game model[J]. Chinese Journal of Computers, 2009, 32(04): 817–827. [DOI: 10.3724/SP.J.1016.2009.00817]
姜伟, 方滨兴, 田志宏, 等. 基于攻防博弈模型的网络安全测评和最优主动防御 [J]. 计算机学报, 2009, 32(04): 817–827. [DOI: 10.3724/SP.J.1016.2009.00817]

[2] ZHU J M, WANG Q. Analysis of cyberspace security based on game theory[J]. Chinese Journal of Network and Information Security, 2015, 1(1): 43–49. [DOI: 10.11959/j.issn.2096-109x.2015.00006]
朱建明, 王秦. 基于博弈论的网络空间安全若干问题分析 [J]. 网络与信息安全学报, 2015, 1(1): 43–49. [DOI: 10.11959/j.issn.2096-109x.2015.00006]

[3] ZHU J M, TIAN Y L. Game Theory and Information Security[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2015: Chapter 1.
朱建明, 田有亮. 博弈论与信息安全 [M]. 北京: 北京邮电大学出版社, 2015: 第一章.

[4] ZHANG W Y. Game Theory and Information Economics[M]. Shanghai: Truth & Wisdom Press, 2012: Chapter 1.
张维迎. 博弈论与信息经济学 [M]. 上海: 格致出版社, 2012: 第一章.
[5] KUNREUTHER H, HEAL G. Interdependent security[J]. Journal of Risk & Uncertainty, 2003, 26(2–3): 231–249. [DOI: 10.1023/A:1024119208153]
[6] CAVUSOGLU H, MISHRA B, RAGHUNATHAN S. The value of intrusion detection systems in information technology security architecture[J]. Information Systems Research, 2005, 16(1): 28–46. [DOI: 10.1287/isre.1050.0041]
[7] LIU Y, COMANICIU C, MAN H. A Bayesian game approach for intrusion detection in wireless ad hoc networks[C]. In: Proceedings from the 2006 Workshop on Game Theory for Communications and Networks. ACM, 2006: 275–283. [DOI: 10.1145/1190195.1190198]
[8] ALPCAN T, BAŞAR T. A game theoretic approach to decision and analysis in network intrusion detection[C]. In: Proceedings of 42nd IEEE International Conference on Decision and Control, Vol. 3. IEEE, 2003: 2595–2600. [DOI: 10.1109/CDC.2003.1273013]
[9] ALPCAN T, BAŞAR T. A game theoretic analysis of intrusion detection in access control systems[C]. In: Proceedings of 43rd IEEE Conference on Decision and Control (CDC), Vol. 2. IEEE, 2004: 1568–1573. [DOI: 10.1109/CDC.2004.1430267]
[10] BLOEM M, ALPCAN T, BAŞAR T. Intrusion response as a resource allocation problem[C]. In: Proceedings of the 45th IEEE Conference on Decision and Control. IEEE, 2006: 6283–6288. [DOI: 10.1109/CDC.2006.376981]
[11] ALPCAN T, BAŞAR T. An intrusion detection game with limited observations[C]. In: Proceedings of 12th International Symposium on Dynamic Games and Applications. Sophia Antipolis, France, 2006: 222–232.
[12] NGUYEN K C, ALPCAN T, BAŞAR T. Stochastic games for security in networks with interdependent nodes[C]. In: Proceedings of 2009 International Conference on Game Theory for Networks (GameNets' 09). IEEE, 2009: 697–703. [DOI: 10.1109/GAMENETS.2009.5137463]
[13] SHEN D, CHEN G, BLASCH E, et al. Adaptive Markov game theoretic data fusion approach for cyber network defense[C]. In: Proceedings of IEEE Military Communications Conference (MILCOM 2007). IEEE, 2007: 1–7. [DOI: 10.1109/MILCOM.2007.4454758]
[14] SCHMIDT S, ALPCAN T, ALBAYRAK Ş, et al. A malware detector placement game for intrusion detection[C]. In: Critical Information Infrastructures Security—CRITIS 2007. Springer Berlin Heidelberg, 2007: 311–326. [DOI: 10.1007/978-3-540-89173-4_26]
[15] XIA Z C, YIN Y, CHEN X H. An evolutionary game analysis on the response policy of the intrusion detection system[J]. Microcomputer Information, 2009, 2009(33): 60–61.
夏子超, 银鹰, 陈晓桦. 入侵检测系统响应策略的进化博弈论分析 [J]. 微计算机信息, 2009, 2009(33): 60–61.
[16] JORMAKKA J, MÖLSÄ J V E. Modelling information warfare as a game[J]. Journal of Information Warfare, 2005, 4(2): 12–25.
[17] ZHOU H, ZHOU H J, MA J F. Security analysis model of intrusion tolerant systems based on game theory[J]. Journal of Electronics & Information Technology, 2013, 35(8): 1933–1939. [DOI: 10.3724/SP.J.1146.2012.01081]
周华, 周海军, 马建锋. 基于博弈论的入侵容忍系统安全性分析模型 [J]. 电子与信息学报, 2013, 35(8): 1933–1939. [DOI: 10.3724/SP.J.1146.2012.01081]
[18] WANG Y, YU M, LI J, et al. Stochastic game net and applications in security analysis for enterprise network[J]. International Journal of Information Security, 2012, 11(1): 41–52. [DOI: 10.1007/s10207-011-0148-z]
[19] MA C Y T, YAU D K Y, RAO N S V. Scalable solutions of Markov games for smart-grid infrastructure protection[J]. IEEE Transactions on Smart Grid, 2013, 4(1): 47–55. [DOI: 10.1109/TSG.2012.2223243]
[20] EMAMI-TABA M, AMOUI M, TAHVILDARI L. Strategy-aware mitigation using Markov games for dynamic application-layer attacks[C]. In: Proceedings of 2015 IEEE 16th International Symposium on High Assurance Systems Engineering. IEEE, 2015: 134–141. [DOI: 10.1109/HASE.2015.28]
[21] KOMATHY K, NARAYANASAMY P. Secure data forwarding against denial of service attack using trust based evolutionary game[C]. In: Proceedings of Vehicular Technology Conference (VTC Spring 2008). IEEE, 2008: 31–35. [DOI: 10.1109/VETECS.2008.19]
[22] LIU J H, YUE G X, SHEN S G, et al. A game-theoretic response strategy for coordinator attack in wireless sensor networks[J]. The Scientific World Journal, 2014, 2014: 950618. [DOI: 10.1155/2014/950618]
[23] JIANG G, SHEN S, HU K, et al. Evolutionary game-based secrecy rate adaptation in wireless sensor networks[J]. International Journal of Distributed Sensor Networks, 2015, 2015: 1–13. [DOI: 10.1155/2015/975454]
[24] CARIN L, CYBENKO G, HUGHES J. Quantitative evaluation of risk for investment efficient strategies in cybersecurity: The QuERIES methodology[R]. AFRL/WS-07-2145, September 2007.
[25] NEYYAN R, PAUL A, DESHWAL M, et al. Game theory based defense mechanism against flooding attack using

puzzle[C]. In: IJCA Proceedings on Emerging Trends in Computer Science & Information Technology (ETCSIT 2012). 2012: etcsit1001 ETCSIT 5: 6–10.

[26] YANG R, FANG F, JIANG A X, et al. Modeling human bounded rationality to improve defender strategies in network security games[C]. In: Workshop on Human-Agent Interaction Design and Models at AAMAS. Valencia, Spain, June 2012.

[27] LIU P, ZANG W, YU M. Incentive-based modeling and inference of attacker intent, objectives, and strategies[J]. ACM Transactions on Information and System Security (TISSEC), 2005, 8(1): 78–118. [DOI: 10.1145/948109.948135]

[28] CARROLL T E, GROSU D. A game theoretic investigation of deception in network security[J]. Security and Communication Networks, 2011, 4(10): 1162–1172. [DOI: 10.1109/ICCCN.2009.5235344]

[29] NGUYEN K C, ALPCAN T, BAŞAR T. Security games with incomplete information[C]. In: Proceedings of 2009 IEEE International Conference on Communications. IEEE, 2009: 1–6. [DOI: 10.1109/ICC.2009.5199443]

[30] LYE K, WING J M. Game strategies in network security[J]. International Journal of Information Security, 2005, 4(1–2): 71–86. [DOI: 10.1007/s10207-004-0060-x]

[31] SHIVA S, ROY S, DASGUPTA D. Game theory for cyber security[C]. In: Proceedings of the Workshop on Cyber Security & Information Intelligence Research. ACM, 2010: 1–4. [DOI: 10.1145/1852666.1852704]

[32] ZHENG J, CASTANÓN D A. Decomposition techniques for Markov zero-sum games with nested information[C]. In: Proceedings of 52nd IEEE Conference on Decision and Control. IEEE, 2013: 574–581. [DOI: 10.1109/CDC.2013.6759943]

[33] SUN W, KONG X W, HE D Q, et al. Research on attack and defense in information security based on evolutionary game[J]. Information Science, 2008, 26(9): 1408–1412.
孙薇, 孔祥维, 何德全, 等. 基于演化博弈论的信息安全攻防问题研究 [J]. 情报科学, 2008, 26(9): 1408–1412.

[34] VARIAN H. System reliability and free riding[M]. In: CAMP L J, LEWIS S, (eds). Economics of Information Security. Advances in Information Security, Vol. 12. Springer Boston, 2004: 1–15. [DOI: 10.1007/1-4020-8090-5_1]

[35] GROSSKLAGS J, CHRISTIN N, CHUANG J. Secure or insure? A game-theoretic analysis of information security games[C]. In: Proceedings of the 17th International World Wide Web Conference. ACM, 2008: 209–218. [DOI: 10.1145/1367497.1367526]

[36] GROSSKLAGS J, RADOSAVAC S, RDENAS A A, et al. Nudge: Intermediaries' role in interdependent network security[C]. In: Proceedings of the 2010 ACM Symposium on Applied Computing. ACM, 2010: 1879–1880. [DOI: 10.1145/1774088.1774486]

[37] LYU J J, KOU W H, WANG Y Z. An analysis of games of information security investment based on interdependent security[J]. Chinese Journal of Management Science, 2006, 14(03): 7–12. [DOI: 10.3321/j.issn:1003-207X.2006.03.002]
吕俊杰, 邱菀华, 王元卓. 基于相互依赖性的信息安全投资博弈 [J]. 中国管理科学, 2006, 14(03): 7–12. [DOI: 10.3321/j.issn:1003-207X.2006.03.002]

[38] WU Y, FENG G, WANG N, et al. Game of information security investment: Impact of attack types and network vulnerability[J]. Expert Systems with Applications, 2015, 42(15–16): 6132–6146. [DOI: 10.1016/j.eswa.2015.03.033]

[39] BÖHME R. Security audits revisited[C]. In: Financial Cryptography and Data Security—FC 2012. Springer Berlin Heidelberg, 2012: 129–147. [DOI: 10.1007/978-3-642-32946-3_11]

[40] JIANG L, ANANTHARAM V, WALRAND J. How bad are selfish investments in network security?[J]. IEEE/ACM Transactions on Networking, 2011, 19(2): 549–560. [DOI: 10.1109/tnet.2010.2071397]

[41] PAL R, HUI P. Modeling Internet security investments: Tackling topological information uncertainty[C]. In: Decision and Game Theory for Security—GameSec 2011. Springer Berlin Heidelberg, 2011: 239–257. [DOI: 10.1007/978-3-642-25280-8_18]

[42] GROSSKLAGS J, JOHNSON B, CHRISTIN N. The price of uncertainty in security games[M]. In: MOORE T, PYM D, IOANNIDIS C (eds). Economics of Information Security and Privacy. Springer Boston, 2010: 9–32. [DOI: 10.1007/978-1-4419-6967-5_2]

[43] JOHNSON B, GROSSKLAGS J, CHRISTIN N, et al. Uncertainty in interdependent security games[C]. In: Decision and Game Theory for Security—GameSec 2010. Springer Berlin Heidelberg, 2010: 234–244. [DOI: 10.1007/978-3-642-17197-0_16]

[44] ZHANG G R, YIN J. Multi-party secure sum computation based on game theory[J]. Application Research of Computers, 2009, 26(4): 1497–1499. [DOI: 10.3969/j.issn.1001-3695.2009.04.086]
张国荣, 印鉴. 基于博弈论的安全多方求和方法 [J]. 计算机应用研究, 2009, 26(4): 1497–1499. [DOI:

10.3969/j.issn.1001-3695.2009.04.086]
[45] HALPERN J, TEAGUE V. Rational secret sharing and multiparty computation[C]. In: Proceedings of Thirty-sixth ACM Symposium on Theory of Computing. ACM, 2004: 623–632. [DOI: 10.1145/1007352.1007447]
[46] KOL G, NAOR M. Cryptography and game theory: Designing protocols for exchanging information[C]. In: Theory of Cryptography—TCC 2008. Springer Berlin Heidelberg, 2008: 320–339. [DOI: 10.1007/978-3-540-78524-8_18]
[47] LUO X Z, QIAN P D, ZHU Y Q, et al. Secure computation against convert adversaries based on game theory[J]. Journal of Nanjing University of Aeronautics & Astronautics, 2012, 44(1): 70–74. [DOI: 10.3969/j.issn.1005-2615.2012.01.013]
罗喜召, 钱陪德, 朱艳琴, 等. 防范秘密攻击的安全计算的博弈论实现 [J]. 南京航空航天大学学报, 2012, 44(1): 70–74. [DOI: 10.3969/j.issn.1005-2615.2012.01.013]
[48] TIAN Y L, MA J F, PENG C G, et al. Game-theoretic analysis for the secure sharing scheme[J]. Acta Electronica Sinica, 2011, 39(12): 2790–2795.
田有亮, 马建峰, 彭长根, 等. 秘密共享体制的博弈论分析 [J]. 电子学报, 2011, 39(12): 2790–2795.
[49] TIAN Y L, PENG C G, MA J F, et al. Game-theoretic mechanism for cryptographic protocol[J]. Journal of Computer Research and Development, 2014, 51(2): 344–352. [DOI: 10.7544/issn1000-1239.2014.20111375]
田有亮, 彭长根, 马建峰, 等. 安全协议的博弈论机制 [J]. 计算机研究与发展, 2014, 51(2): 344–352. [DOI: 10.7544/issn1000-1239.2014.20111375]
[50] AGAH A, DAS S K, BASU K, et al. Intrusion detection in sensor networks: A non-cooperative game approach[C]. In: Proceedings of IEEE International Symposium on Network Computing & Applications. IEEE, 2004: 343–346. [DOI: 10.1109/NCA.2004.1347798]
[51] ANUVARSHA G, KUMAR R. Intrusion detection and response using game strategy and RRE engine in network security[J]. International Journal of Engineering and Computer Science, 2015, 4(3): 10977–10983.
[52] PATCHA A, PARK J M. A game theoretic approach to modeling intrusion detection in mobile ad hoc networks[C]. In: Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004. IEEE, 2004: 280–284. [DOI: 10.1109/IAW.2004.1437828]
[53] CUI X, TAN X, ZHANG Y, et al. A Markov game theory-based risk assessment model for network information system[C]. In: Proceedings of 2008 International Conference on Computer Science and Software Engineering, Vol. 3. IEEE, 2008: 1057–1061. [DOI: 10.1109/CSSE.2008.949]

作者信息

王秦 (1990–), 甘肃天水人, 博士. 主要研究领域为信息安全的经济学分析.
qwangcufe@163.com

朱建明 (1965–), 山西太原人, 教授, 博士生导师. 主要研究领域为信息安全和电子商务安全.
tyzjm65@163.com

高胜 (1987–), 湖北黄冈人, 博士, 副教授. 主要研究领域为数据安全与隐私保护, 区块链技术与应用.
sgao@cufe.edu.cn