arXiv:2302.01975v1 [math.OC] 3 Feb 2023

有限理性参与者与多个攻击者情境下的攻击计划拦截：一种对抗性风险分析方法

Eric DuBois、Ashley Peper 和 Laura A. Albert*威
斯康星大学麦迪逊分校工业与系统工程程系，
University Avenue 1513号，麦迪逊，威斯康星州
53706 邮箱： laura@engr.wisc.edu

2023年2月

摘要

网络安全规划支持在资源受限环境中选择和实施安全控制措施，以管理风险。为此，在建模工作中需要考虑具有不同战略成熟度的自适应对手，从而支持风险管理。然而，文献中的大多数模型只考虑理性或非战略性的对手。因此，我们研究如何为防御决策提供依据，以缓解有限理性参与者带来的风险，尤其关注制定综合性相互依赖的规划决策。为实现这一目标，我们引入一种建模框架，用于选择安全缓解措施组合，以阻断对抗性攻击计划，并采用结构化方法开展风险分析。我们的方法结合对抗性风险分析与认知层级理论，研究一个最大可靠性路径阻断问题，其中包含一名单一防御者和多个具有不同目标及战略成熟度的攻击者。我们不再枚举所有可能的攻击和防御方案，而是引入一种基于整数规划和近似算法的求解技术，迭代求解防御者问题和攻击者问题。一个案例研究展示了所提出的模型，并为防御规划提供了有益见解。

*通讯作者

关键词： 网络安全；对抗性风险分析；网络阻断

1 引言

由于对数字连接日益增长的依赖以及不断增加的威胁，网络安全已成为世界各国政府和组织高度关注的问题。网络攻击日益普遍，2016年给美国经济造成了570亿至1090亿美元的损失（经济顾问委员会，2018年），并影响了整个经济体系中的各类系统，包括医疗保健（Kruse等，2017年）、能源（Wang和Lu，2013年）以及工业控制（Knowles等，2015年）。目前存在许多可用于缓解这些风险的安全控制措施（Ross等，2021年）。网络安全规划要求定期选择安全控制措施组合（例如每年选择一次），使组织能够管理与已出现的漏洞相关的风险。然而，鉴于许多组织在资源受限环境中运营，在选择和部署安全控制措施方面常常面临困难（Stevens等，2020年）。

越来越多的文献采用风险分析技术，通过对安全控制措施进行战略性优先排序来管理网络安全风险。一些研究将攻击者建模为非战略性参与者，利用概率分布，并依据成本效益对安全控制措施进行排序（Hubbard and Seiersen, 2016）。研究者日益采用结构化方法对安全控制措施进行优先排序，以便在目标明确、威胁场景清晰的情况下辅助规划工作（NIST 2018）；其中，攻击图用于表示已知漏洞并直观展示潜在的缓解措施（Lallie et al., 2020）。近期研究采用整数规划（Zheng et al., 2019）和鲁棒优化（Zheng and Albert, 2019b），基于攻击图并通过结构化方法来选择安全缓解措施；然而，这些论文假设攻击者要么不具备战略性，要么只能选择最坏情况场景。

文献中有一系列论文明确通过应用对抗性风险分析（ARA），在网络安全规划中考虑自适应对手。在这些模型中，单一防御者（即安全规划者）会选择安全控制措施，以便在自适应对手试图绕过任何新部署的安全控制措施时仍能发挥良好效果。ARA框架用途广泛，并催生了能够涵盖多种情形和假设的防御者-攻击者模型（Banks et al., 2020）。因此，ARA已应用于许多

这类防御者-攻击者模型，并用于各种安全情境（Rios and Rios Insua, 2012）；此外，它还被扩展到包含多个意图程度各异的对手的网络安全模型中（Rios Insua et al., 2021）。ARA方法的一个局限是需要枚举所有可能的攻击和防御（Banks et al., 2020），Wang and Banks（2011）是一个例外。因此，当实际操作中无法枚举网络安全攻击与防御选项时，ARA算法将难以处理。Zheng and Albert（2019a）试图克服这一挑战，他们引入了一种结构，该结构基于网络阻断模型，通过延缓多个攻击者的攻击计划来简化计算需求。网络阻断模型引入的结构使得可以使用整数规划算法求解防御者与攻击者的策略。

我们在先前工作的基础上，提出一个对抗风险分析（ARA）框架，将有限理性的参与者纳入考量，其中包括一名防御者和多个对手，以指导安全控制措施的选择，从而阻止对抗性攻击计划。虽然我们的方法以网络安全规划为出发点，但也可广泛应用于安全情境中，适用于参与者在多层防御系统中试图最大化或最小化攻击概率的情况。

1.1 方法

在我们所研究的网络安全规划问题中，防御者需要在规划期内，通过选择预算范围内的安全控制措施组合，尽可能降低多个战略成熟度各异的攻击者成功攻击的概率。我们调整了一个对抗风险分析（ARA）框架（Rios Insua et al., 2021），以刻画防御者和攻击者均为有限理性参与者时，安全控制措施组合的战略性选择。这种建模方法有助于我们针对一系列攻击者制定防御决策和规划，从而更准确地反映所建模的系统（Scheibehenne et al., 2010）。由于新的漏洞会定期出现，网络安全规划也应定期开展（例如每年一次），本文提出的方法可为这一过程提供帮助。

攻击建模是网络安全规划中的重要步骤。在漏洞分析中，可以通过成功实施攻击所需的各个步骤来描述漏洞（Schneier，1999），从而为表示攻击场景提供一种结构化方法。在图结构中，节点表示攻击状态（例如，攻击类型的选择、攻击目标或攻击里程碑），边则表示攻击中的中间利用。对手完成一次漏洞利用的难度

通过成功遍历一条弧的条件概率来表示。从根节点到叶节点的路径对应于针对系统的一次攻击，因此，我们将攻击视为图中从源节点到汇节点的一条路径。鉴于对手众多，他们对漏洞的了解程度和能力各不相同，攻击图的拓扑结构和参数可能因对手而异。

对手成功实施攻击中所有漏洞利用的概率，体现为其沿所选路径穿越网络的概率。安全控制措施通过降低单个漏洞利用（即被穿越的弧）完成的概率，与攻击图产生相互作用。安全控制措施可能促使对手选择其他路径。防御者利用其私有信息以及其认为攻击者会选择的攻击图中的路径，来决定选择哪些安全控制措施。

这些策略性互动促使我们将最大可靠性路径阻断问题应用于所研究的规划问题。网络阻断模型（包括最大可靠性路径阻断模型）已被广泛用于描述攻击者-防御者博弈，通常假设有两名参与者且决策者是理性的（Smith and Song，2020年）。尽管有些论文放宽了共享信息的假设（例如，Salmer´on（2012年）），以及参与者对网络中穿越边的概率具有共享信念这一假设（例如，Morton等人（2007年）），但尚无研究考虑有限理性参与者。本文旨在弥补这一差距。

我们将 Rios Insua 等人（2021年）提出的对抗性风险分析（ARA）框架中的理念加以改编，并应用于最大可靠性网络阻断问题，以支持网络安全规划中的决策。对抗性风险分析方法使我们能够考虑并非理性且战略成熟度各不相同的对手；这些都是当前应用场景的重要特征。具体而言，我们运用认知层级理论（Camerer等人，2004年）和级别 k 思维，对有限理性的参与者进行建模（Stahl and Wilson，1995年）。

为说明本文采用的方法，考虑以下单一防御者面对两种对手类型的示例。在该示例中，对手试图窃取服务器；此示例改编自 Bistarelli等人（2006年）。图1展示了所研究的攻击图，包括漏洞利用，以及窃取服务器（到达顶端节点）的两条路径。共有三种安全控制措施（m_1、 m_2和 m_3），分别标注在其阻断的弧旁。为便于说明

起见，我们假设防御者可以选择一种控制措施。未受阻断时的遍历概率标注在各弧旁，使用安全控制措施时受阻断后的遍历概率则列在括号中。在没有任何安全控制措施的情况下，通往“窃取服务器”节点的左侧和右侧路径的遍历概率分别为0.09和0.102。

在此示例中，一名战略成熟度较低、忽视可能的安全防御措施的机会主义攻击者会选择右侧路径，因为该路径未受阻拦的通行概率更高。若防御者只预判这类攻击者发起的攻击，就会选择 m_3，因为这项缓解措施能最大程度地降低右侧路径的通行概率。战略性稍强的攻击者会预判到 m_3 将被部署，因此会选择左侧路径。这会促使战略性更强的防御者选择控制措施 m_2 ，以防御只尝试走左侧路径的攻击者。如果防御者预判到这两类攻击者，其中25%具有一定战略性并选择左侧路径，75%

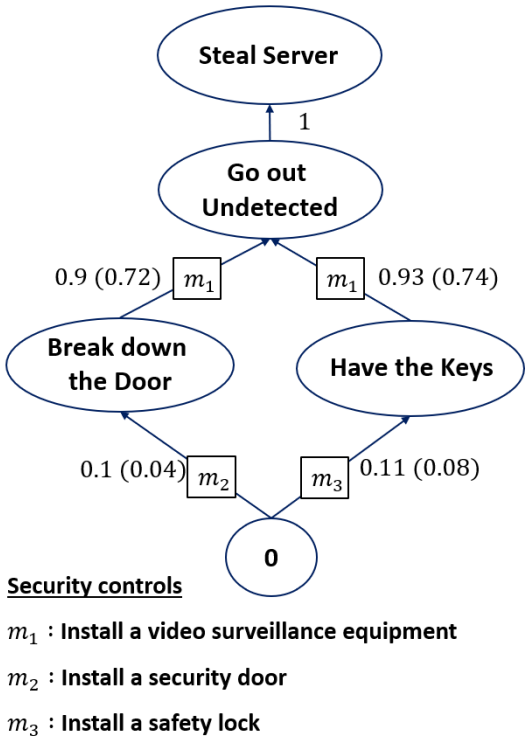


图1：一个包含三项安全控制措施的单一攻击图示例

则是机会主义者并尝试走右侧路径，那么防御者会选择缓解措施 m_1。

这个基于单个攻击图的简单示例表明，考虑多个有限理性攻击者的方法可以为防御规划决策提供有用的信息。一般而言，有许多攻击图能够刻画各种攻击向量，以及对抗目标和能力。安全控制措施可以针对特定漏洞利用并使其延迟，例如m_2 前例中的做法；也可以在控制措施具有广泛适用性的情况下应对多种漏洞利用，例如部署多因素身份验证或员工培训计划。Singhal 和 Ou（2017年）以及 Lallie 等人（2020年）提供了有关如何构建攻击图的更多指导。

1.2 贡献

总之，本文做出了以下贡献：

- 我们在对抗风险分析框架下，将安全控制投资问题建模为最大可靠性路径阻断博弈。博弈参与者包括一名防御者和多个攻击者，他们均具有有限理性，但战略成熟度各不相同。我们将防御者问题和攻击者问题建模为混合整数规划模型。

- 我们介绍基于混合整数规划算法和近似算法的求解技术。我们迭代求解防御者问题和攻击者问题，并在每次迭代后更新各模型的输入。我们证明，防御者问题等价于一个带预算约束的子模最大化问题，因此可以使用启发式方法识别至少达到最优解值 $1 - 1/e$ 的解。

- 我们将该建模方法应用于一项案例研究。我们确定了不同战略成熟度级别下的解，并考察了防御者对攻击者战略成熟度判断失误所产生的影响。

本文结构如下。我们首先在第 2 节回顾相关文献。第 3 节介绍对抗风险分析框架。第 4 节介绍从攻击者和防御者视角刻画最大可靠性路径阻断问题的混合整数规划模型。第5节介绍近似算法，第 6 节介绍对抗风险分析算法。第 7 节展示并分析案例研究及其他计算结果。第 8 节总结全文。

2 文献综述

本文探讨的主题涉及多个不同的研究领域，包括对抗性风险分析、有限理性思维、安全控制投资和最大可靠性路径阻断。我们总结了文献中最相关的论文。

2.1 对抗风险分析

对抗风险分析已广泛应用于安全领域（Rios and Rios Insua，2012年）。多篇论文将ARA框架用于网络安全，重点关注防御者—攻击者博弈（Wang et al.，2019）、内部人员威胁建模（Joshi et al.，2020年），以及对抗性机器学习和数据操纵（Caballero et al.，2021年）。Rios Insua et al.（2021年）将ARA框架应用于网络安全资源分配问题，以制定防御行动组合，其中包括购买网络保险，并同时纳入蓄意威胁和非蓄意威胁。

与大多数对抗风险分析（ARA）模型一样，Rios Insua et al. (2021年) 枚举所有可能的攻击和防御。Cano et al. (2016) 同样将对抗风险分析（ARA）应用于网络安全场景，通过枚举具体的攻击和防御，确定最优的安全资源分配，以尽量减少对机场运营的干扰。就我们所知，只有 Wang and Banks (2011) 考虑了攻击和防御不进行枚举的 ARA框架。他们研究了车队通过网络的最优路径，其中攻击者在网络内的节点处放置了若干简易爆炸装置（IEDs）。防御者的目标是使路径成本最小化。通过使用网络模型，他们简洁地表示了许多可能的车队路径。由于 Wang and Banks (2011) 利用其成本函数的可加性来高效求解问题，因此无法将其求解方法应用于我们的问题。不同于现有文献，我们考虑通过拦截攻击计划来支持网络安全规划，并引入一种基于整数规划和近似算法的防御者与攻击者问题求解方法，因为枚举攻击和防御选项是不可行的。

2.2 有限理性

我们在 Rothschild 等人（2012年）的研究基础上开展工作，他们提出了一种在 ARA框架中应用有限理性，具体而言是级别 k 思考的算法。级别 k 思考始于非策略性0级思考者，他们的行动不考虑其他参与者。相比之下，在级别 k思考中，级别 k 参与者仅针对级别 $k-1$ 对手进行优化；而认知层级理论则假设，级别 k 思考者会针对从0级到级别 $k-1$ 的参与者分布进行优化（Camerer等人，2004年）。鉴于防御者需要面对多个攻击者的情形，我们使用这一方法对防御者进行建模。尽管级别 k 思考和认知层级理论的逻辑

在理论上会导致无限回归，但实证研究发现，大多数人的思考不会超出2级或3级（Lee 和 Wolpert，2012年）。高层级思考者（$k > 0$）假设其对手是级别 $k-1$ 思考者，例如，1级参与者针对0级参与者进行优化，2级参与者针对1级参与者进行优化，依此类推。Rothschild 等人（2012年）通过递归构建关于参与者所采用攻击或防御的信念分布，创建了一种确定级别 k 对手策略的算法。在对手中考虑有限理性是本文的一个新颖方面。据我们所知，本文首次在网络阻断所涉及的相互依赖的防御决策中考虑有限理性参与者。

2.3 安全控制措施组合选择

一部分文献研究了在有限预算下如何投资于安全控制措施（Fielder 等人，2016年；Zheng and Albert，2019b）。许多模型考虑的是非策略性攻击，因此不一定会选择能够充分防御自适应对手的控制措施（Zheng 等人，2019年）。非策略性攻击（也称为机会主义攻击或非定向攻击）无论防御者的安全决策如何，都会大致以相同的方式并以相同的频率持续实施。例如，采用决策理论框架的模型假设，防御者的决策不会影响每种攻击方法的发生频率（Cavusoglu 等人，2008年）。尽管一些研究试图在存在策略性攻击者和自然灾害的情况下分配预算（Zhuang 和 Bier，2007年），但该领域的论文都没有考虑如何在存在多个有限理性对手的情况下选择安全防御措施组合。

2.4 最大可靠性路径阻断

网络阻断模型已广泛应用于基础设施保护和韧性问题，用于指导如何保护系统中的关键组件，从而降低最坏情况下的脆弱性。网络阻断问题通常被建模为防御者—攻击者博弈中的斯塔克尔伯格博弈或古诺博弈模型，并且通常假设有两名参与者和理性决策者。Smith and Song（2020年）对这一领域进行了近期综述。最短路径阻断问题可用于对攻击或项目进行建模：攻击者试图缩短完成攻击（穿越网络）所需的时间，而防御者则试图通过阻断网络中的

（延长）边来尽可能拖延攻击（Israeli 和 Wood，2002年）。最短路径阻断问题与最大可靠性阻断问题是等价的表述（Morton等人，2007年）。网络阻断模型已扩展到包含不完美信息和私有信息（Salmer´on，2012年）。多位研究者建议扩展网络阻断模型，以考虑有限理性参与者（Zhang等人，2018年）以及其他更贴近现实的特征，从而助力防御规划（Albert等人，2023年）。

一系列论文研究如何阻断攻击图，以为网络安全防御规划工作提供依据。Nandi 等人（2016）提出了一种双层防御者—攻击者模型，通过阻断攻击图，帮助组织选择并部署安全对策。Letchford 和 Vorobeychik（2013）提出了另一种斯塔克尔伯格博弈：防御者试图阻断攻击计划，并放宽了博弈为零和博弈的假设。Zheng and Albert（2019a）提出了一种双层网络阻断模型，旨在不确定性条件下，确定一组安全控制措施，从而最大限度地延缓多个攻击者发起的大量对抗性网络攻击。

总之，本文将对抗风险分析和认知层级理论与网络阻断建模相结合，为网络安全防御规划提供依据，从而丰富了现有文献。

3 对抗风险分析框架

本节介绍本文采用的对抗风险分析框架，以及我们如何对有限理性参与者进行建模。对抗风险分析从一名参与者的视角出发——在本文中，这名参与者是防御者——并根据其对其他参与者将采取何种行动或作出何种反应的判断，为该参与者寻求最优行动。

3.1 博弈中的参与者互动

最大可靠性网络阻断建模方法考虑的是单一防御者与多个攻击者之间的一次性交锋。对于案例研究中所考虑的网络安全投资决策，这种设定是合理的，因为规划者必须保护信息系统免受多种攻击。在我们的方法中，攻击者并不知道防御者选择了哪些安全控制措施。攻击者试图根据其感知到的防御情况，最大限度地提高攻击成功的概率，

而防御者则力求阻止攻击。关于防御者预算和安全控制成本的信念是有限且离散的。

现在我们描述所考虑的博弈的一般形式。攻击者集合中的每个攻击者都会选择一种攻击方法和一个目标，以使其成功概率最大化，这一概率决定了其可靠性。这等同于选择一条穿过网络的路径。通过选择路径，攻击者选定其经过的边集合，而该集合决定了路径的可靠性。防御者通过选择控制措施，降低这些措施所覆盖的每条边的可靠性。防御者选择一个控制措施组合，使攻击被阻止的条件概率最大化，同时受预算约束。

网络结构的大部分信息被视为共享信念，而网络参数（例如边可靠性）则属于私人信念。具体而言，我们假设所有参与者共享节点、边和可能的控制措施集合。这等同于假设防御者了解攻击者可能考虑的所有威胁。该方法依据已知漏洞为防御规划提供依据，也可以更新以纳入新发现的漏洞。博弈中的其他信息可能是私有的，包括边可靠性、控制措施降低这些可靠性的有效性、来自每个攻击者的攻击比例、实施控制措施的成本，以及防御者预算。

3.2 有限理性参与者

从防御者的角度来看，攻击者可能具有不同级别的战略成熟度。因此，级别为 k 的防御者会针对级别为 0、1、..... $k-1$ 的攻击者进行规划。攻击者策略表示一条路径。防御者策略是一个组合，由一组总成本不超过预算的控制措施构成。

由于我们正在寻求最优防御，因此需要找出从 k 防御者到最高级别 K（即防御者等级）的策略，以及从 k 攻击者到最高级别 $K-1$的策略。随着算法的推进，会记录较低级别攻击者和防御者的策略，从而为不同战略成熟度的防御者等级提供一套相应的组合方案。通过分析这套方案中的各种组合，我们可以更明智地决定：当面对更加或不那么“成熟”的攻击者时，防御者态势应如何变化。

计算每种类型的不同级别 k 攻击者策略的基本算法如下。我们将在第5节中详细阐述这一算法。我们从有关系统的信息和信念开始。首先从 $k=0$ 开始，为非策略型参与者构建0级攻击者和防御者策略。然后将 k 的值增加1，并使用第4.2节介绍的防御者程序 $OptDef$，计算 k 级防御者的最优组合。如果最高级别防御者 K的策略已经计算完毕，则算法终止。否则，我们使用第4.1节介绍的攻击者程序 $OptAtt$，计算 k 级攻击者的最优攻击路径。我们将 k 增加1，重复这一步骤，并求解防御者问题和攻击者问题，直到算法终止。

4 模型构建

本节基于最大可靠性网络阻断问题，构建一个同时行动的单防御者多攻击者博弈。为此，我们分别从攻击者视角的优化问题 $OptAtt$ 和防御者视角的优化问题 $OptDef$ 出发。该博弈包含一名单一防御者和一个攻击者集合 $\mathcal{A}$。不失一般性，每名攻击者都从超级源节点 1 出发，穿过图到达超级汇节点 n。每名攻击者都会选择一条最大可靠性路径，即根据其对防御者决策的认知，认为自己能够成功穿过图的概率最高的路径。

反映防御者和攻击者信念的记号分别带有 D 和 A 下标/上标。根据战略成熟度级别更新的信念带有 k 上标。表示决策变量的记号不显式包含 k、 D 或 A。表1总结了与参数、参与者信念以及决策变量相关的记号。为清晰起见，我们用拉丁字母表示变量和共享信息，用希腊字母表示信念。

4.1 攻击者问题

现在我们考虑攻击者问题。我们考虑一个由有限节点集 N 和有向边 E组成的有向无环图 $G=(N,E)$。离开和进入节点$i \in N$ 的边集分别记为 E_i^+和 E_i^-。不失一般性，我们假设集合

表1：符号说明

集合：防御者与攻击者的共同信息

$\mathcal{A}$	=	攻击者
N	=	节点
E	=	边
$E_i^+ \left(E_i^-\right) \subseteq E$	=	离开（进入）节点 $i \in N$ 的边
M	=	控制措施集合
$M_{ij} \subseteq M$	=	阻断边的控制措施子集（$i,\ j$） $\in E$
$P_{(i)}$	=	从源节点到节点 $i \in N$ 的路径集合

级别 k 攻击者 $A \in \mathcal{A}$ 决策

攻击者变量

u_{ij} $=\begin{cases} 1, \text{如果边 } (i,j) \in E \text{ 位于攻击者路径上；否则为 } 0 \end{cases}$ q_{ij} = 攻击者 $A \in \mathcal{A}$ 的攻击到达边 (i,j) 的概率 $\in E$

$\Longrightarrow$ 级别 k'（含 $k' > k$）防御者信念

$\psi_D^{k'}(i,\ j,\ A)$ = 级别为 $k' > k$ 的防御者认为级别为 k 的攻击者$A \in \mathcal{A}$ 尝试穿越边 $(i,\ j) \in E_i^+$（在攻击者到达节点 i 的条件下）的条件概率。

防御者 D 信念

$\delta_D(i,\ j,\ A)$ = 攻击者 $A \in \mathcal{A}$ 穿越未拦截边 $(i,\ j) \in E$ 的可靠性$\delta_D(i,\ j,\ A)$ = 攻击者 $A \in \mathcal{A}$ 穿越已拦截边 $(i,\ j) \in E$ 的可靠性 $\theta_D(A)$ = 攻击者 A 发动攻击的条件概率β_D = 防御者预算$\kappa_D(m)$ = 控制措施的成本 $m \in M$

级别 k 防御者决策

防御者变量

w_m $=\begin{cases} 1, \text{若选择控制措施 } m \in M \text{ 则为 } 0, \text{否则} \end{cases}$ x_{ij} $=\begin{cases} 1, \text{若边 } (i,\ j) \in E \text{ 被覆盖则为 } 0, \text{否则} \end{cases}$ $y_{ij}(A)$ = 攻击者到达未拦截边 $(i,\ j) \in E$ $\tilde{y}_{ij}(A)$ = 攻击者到达已拦截边 $(i,\ j) \in E$的概率

$\Longrightarrow$ 级别 $k+1$ 攻击者信念

$\Omega_A^k = \{\omega_1, ..., \omega_m\}$ = 级别为 k 的防御者$\delta_A^{k+1}(i,j|\Omega_A^k)$ 选择的组合 = 级别为 $k+1$ 的攻击者使用组合 Ω_A^k 时，边 (i,j) 的可靠性 $\in E$

节点 $\{1,...,n\} \in N$的排列顺序满足 $i < j, \forall (i,j) \in E$.

0级攻击者并非策略性的。我们假设，0级攻击者 A 采用短视贪心策略来选择路径。在这种方法中，边可靠性取未受阻断时的值，即对于所有 $(i,j) \in E$，均为 $\delta(i,j,A)$；每个0级攻击者都会从每个节点选择未受阻断可靠性最高的边，若有并列则随机选择。也可以使用其他方法来设定0级攻击者路径。

我们考虑级别为 k 的攻击者所走攻击路径的可靠性。级别为 k 的攻击者 A 认为，级别为 k-1 的防御者已选择组合 $\Omega_A^{k-1} = \{\omega_1, ..., \omega_m\}$。攻击者认为，边 $(i,j) \in E$的可靠性为 $\delta_A^k(i,j|\Omega_A^{k-1})$，即采用组合 Ω_A^{k-1} 时的可靠性。我们假设，不同边的 $\delta_A^k(i,j|\Omega_A^{k-1})$ 值相互独立。给定 Ω_A^{k-1} 后，攻击者认为固定路径 p 的可靠性为 $\prod_{(i,j)\in p} \delta_A^k(i,j|\Omega_A^{k-1})$。每个策略性攻击者都力求最大化其攻击成功的条件概率。利用基于递归的标准方法（Ahuja等人，1993），我们可以用以下一对线性不等式表示攻击到达边 (i,j) 的概率，该概率记为 $q_{j\ell}$:

$$
\begin{aligned}
q_{j\ell} \leq & u_{j\ell} \\
q_{j\ell} \leq & \sum_{(i,j)\in E_j^-} \delta_A^k(i,j|\Omega_A^{k-1}) q_{ij},
\end{aligned}
$$

其中，攻击者所选路径的特征向量为 $u \in \{0,1\}^{|E|}$；若边 $(i,\ j)$ 位于该路径中，则 $u_{ij} = 1$，否则为 $u_{ij} = 0$。

使用这些示例 表述中，我们提出了级别 k 攻击者 $A \in \mathcal{A}$ 的 $OptAtt$ 公式 a

最大可靠路径问题：

$$z_A^k = \max \sum_{(i,n)\in E_n^-} \delta_A^k(i,j|\Omega_A^{k-1}) q_{in} \tag{1}$$

$$\text{s.t.} \sum_{(1,i)\in E_1^+} u_{1i} \le 1 \tag{2}$$

$$\sum_{(i,j)\in E_i^+} u_{ij} \le \sum_{(j,i)\in E_i^-} u_{ji}, \qquad \forall i \in N \setminus \{1\} \tag{3}$$

$$q_{ij} \le u_{ij}, \qquad \forall (i,j) \in E \tag{4}$$

$$q_{j\ell} \le \sum_{(i,j)\in E_j^-} \delta_A^k(i,j|\Omega_A^{k-1}) q_{ij}, \qquad \forall j \in N \setminus \{1\}, (j,\ell) \in E_j^+ \tag{5}$$

$$u_{ij} \in \{0,1\}, \qquad \forall (i,j) \in E \tag{6}$$

$$q_{ij} \ge 0, \qquad \forall i \in N, (i,j) \in E \tag{7}$$

目标函数 (1) 要求攻击者最大化其攻击成功的概率。约束 (2) – (3) 确保 u_{ij} 变量正确定义一条路径。约束 (2) 仅允许攻击者选择一条攻击路径，约束集合 (3) 则保持每个节点流入和流出的平衡。约束集合 (4) – (5) 用于确定攻击成功的概率。约束集合 (4) 只允许攻击沿攻击路径推进。约束集合 (5) 平衡每个节点流入和流出的攻击概率流。约束集合 (6) 和 (7) 分别要求变量取二进制值和非负值。*OptAtt* 是一种规范形式的最大可靠路径问题；对边可靠性进行负对数变换后，可将其转化为最短路径问题，并使用 Dijkstra算法为每个攻击者求解（Morton等人，2007年）。

针对每个攻击者求解 *OptAtt* 后，我们利用求解结果构建防御者对各攻击者将采取的路径的信念 $A \in \mathcal{A}$ 。回顾一下，级别为 k' 的防御者要防御一组攻击者 $\mathcal{A}$，这些攻击者的复杂程度 k可能各不相同，其中 $0 \le k < k'$。因此，级别为 k 的攻击者 $A \in \mathcal{A}$ 的 *OptAtt* 求解结果可用于构建级别为 k' 的防御者的信念，其中 $k+1 \le k' \le K$。为此，我们从 *OptAtt* 的求解变量 u_{ij} 中推导出级别为 k 的攻击者 A 所采取的路径，并将其转换为级别为 k' 的防御者的信念参数。级别为 k' 的防御者认为，攻击者 A 在到达节点后选择边的条件概率

$(i,\ j) \in E$ 在到达节点 i 后为

$$\psi_D^{k'}(i,j,A) = u_{ij},\ \forall (i,j) \in E. \tag{8}$$

虽然我们没有在*OptAtt*中的攻击者变量里明确建模级别 k，但在设置$\psi_D^{k'}(i,\ j,\ A)$的值时，攻击者的级别会被隐式保留。

4.2 防御者问题

现在我们考虑防御者问题。防御者通过从集合 M中选择控制措施，使攻击被阻止的概率最大化。每项控制措施 $m \in M$ 的成本为 $\kappa_D(m)$，且受防御者预算 β_D的约束。控制措施 m阻断一组边，从而降低该集合中所有边的可靠性。子集 $M_{ij} \subseteq M$ 包含所有阻断边$(i,\ j)$的控制措施。这种方法与经典最大可靠性阻断问题略有不同，在后者中，防御者直接阻断网络中的边。我们将预算和成本视为信念，因为攻击者可能不知道它们的值。我们假设0级防御者不选择任何控制措施。

防御者认为，攻击者 $A \in \mathcal{A}$ 尝试发动攻击的条件概率为 $\theta_D(A)$。我们假设该概率由外生因素决定，可能来源于专家意见或风险评估。防御者面临多个具有不同级别 k'的攻击者，其 $0 \le k' \le k-1$体现在 $\psi_D^k(i,j,A)$的值中。每次攻击都遵循一条固定路径 p，并以给定概率~发生，该概率取决于防御者的级别。对于攻击者 A，如果边(i,j)分别被阻断或未被阻断，防御者具有信念概率 $\delta_D(i,j,A)$和 $\delta_D(i,j,A)$，这些概率反映了该边的可靠性。我们假设这些信念概率的实现彼此独立。我们~进一步假设，概率 $\delta_D(i,j,A)$和 $\delta_D(i,j,A)$在不同边之间相互独立。

为推导 *OptDef* 公式，注意，级别为 k 的防御者的组合会阻断一组边 $S \subseteq E$。此外，令 $P(i)$ 表示从源节点 1 通往节点 $i > 1$ 的路径集合。那么，成功攻击的条件概率为

$$\sum_{A \in \mathcal{A}} \theta_D(A) \sum_{p \in P(n)} \psi_D^k(p,A) \prod_{(i,j) \in p \setminus S} \delta_D(i,j,A) \prod_{(i,j) \in p \cap S} \tilde{\delta}_D(i,j,A). \tag{9}$$

从任意节点 $i \in N$ 到汇节点 n 的最大概率路径不取决于

用于到达 i 的路径。因此，可将式 (9) 改写为

$$\sum_{A\in\mathcal{A}} \theta_D(A) \sum_{p\in P(n)} \prod_{(i,j)\in p} \psi_D^k(i,j,A) \Big(\delta_D(i,j,A)(1-x_{ij}) + \tilde{\delta}_D(i,j,A)x_{ij}\Big) \tag{10}$$

防御者认为，若边 $(j,\ell) \in E$未被封锁，攻击者 A 尝试经过该边的概率为 $y_{ij}(A)$；若该边被封锁，概率则为 $\tilde{y}_{j\ell}(A)$。这些都是防御者模型中的决策变量。我们递归地定义 $y_{j\ell}(A)$ 和 $\tilde{y}_{j\ell}(A)$ 如下：

$$y_{j\ell}(A) = (1-x_{j\ell})\psi_D^k(j,\ell,A) \sum_{(i,j)\in E_j^-} \Big(\delta_D(i,j,A)y_{ij}(A) + \tilde{\delta}_D(i,j,A)\tilde{y}_{ij}(A)\Big)$$

$$\tilde{y}_{j\ell}(A) = x_{j\ell}\psi_D^k(j,\ell,A) \sum_{(i,j)\in E_j^-} \Big(\delta_D(i,j,A)y_{ij}(A) + \tilde{\delta}_D(i,j,A)\tilde{y}_{ij}(A)\Big).$$

综合这些方程，我们引入 *OptDef* 表述：

$$z_D^k = 1 - \min \sum_{A\in\mathcal{A}} \theta_D(A) \sum_{(i,n)\in E_n^-} \Big(\delta_D(i,n,A)y_{in}(A) + \tilde{\delta}_D(i,n,A)\tilde{y}_{in}(A)\Big) \tag{11}$$

$$\text{s.t. } y_{1i}(A) + \tilde{y}_{1i}(A) \geq \psi_D^k(1,i,A), \qquad \forall A\in\mathcal{A}, (1,i)\in E_1^+ \tag{12}$$

$$y_{j\ell}(A) + \tilde{y}_{j\ell}(A) \geq \psi_D^k(j,\ell,A) \sum_{(i,j)\in E_j^-} \Big(\delta_D(i,j,A)y_{ij}(A) + \tilde{\delta}_D(i,j,A)\tilde{y}_{ij}(A)\Big), \quad \forall A\in\mathcal{A}, j\in N\setminus\{1,n\}, (j,\ell)\in E_j^+ \tag{13}$$

$$\tilde{y}_{ij}(A) \leq \sum_{m\in M_{ij}} w_m, \qquad \forall A\in\mathcal{A}, (i,j)\in E \tag{14}$$

$$\sum_{m\in M} \kappa_D(m)w_m \leq \beta_D \tag{15}$$

$$y_{ij}(A), \tilde{y}_{ij}(A) \geq 0, \qquad \forall A\in\mathcal{A},\ (i,j)\in E \tag{16}$$

$$w_m \in \{0,1\}, \qquad \forall m\in M \tag{17}$$

级别为 k 的防御者会最大化阻止攻击的条件概率（11）；这等同于最小化攻击成功的条件概率，而攻击成功发生在攻击者穿越网络时。约束集合（12）确保每个攻击者都会尝试发动攻击。约束集合（13）作为流量平衡方程，用于确定攻击

从每个攻击者到达每条边的概率。具体而言，该概率等于攻击到达边的起始节点的概率，乘以攻击随后沿该边继续前进的条件概率。约束集合（14）规定，只有选择了能够阻断某条边的控制措施，才能阻断该边。约束（15）规定，防御者选择的控制措施数量不得超过其预算允许的数量。最后两个约束集合（16）和（17）确保相应变量为非负数和二进制变量。

对级别 k 防御者问题的求解结果，会影响级别 $k+1$ 攻击者对防御者边可靠性的信念。具体而言，Ω_A^k 定义为集合 $\{m \in M: \quad w_m = 1\}$，且对于每个 $(i, \ j) \in E$

$$\delta_A(i,j|\Omega_A^k) = \begin{cases} \delta_D(i,j,A), & \text{if } x_{ij} = 0 \\ \tilde{\delta}_D(i,j,A), & \text{if } x_{ij} = 1. \end{cases} \tag{18}$$

5 防御者问题的近似

对于大规模问题实例，求解 *OptDef* 以找到最优解可能在计算上十分困难。不过，我们证明存在一种近似算法，能够提供具有 $1-1/e$ 性能保证的解。为此，我们证明 *OptDef* 等价于一个带背包约束的非负次模最大化问题。对于该问题，启发式算法可在多项式时间内找到至少达到最优解值 $(1-1/e)$ 的解（Sviridenko，2004年）。对于相关问题——即带基数约束的子模函数最大化问题——也有类似结果（Nemhauser 等人，1978年）。稍后在第 7 节中，我们将证明，在实践中，这种近似算法通常能找到其值极其接近最优解值的解。该近似算法可通过为混合整数规划求解器提供热启动，缩短求解 *OptDef* 所需的时间。

我们将 Khuller等人（1999）的启发式算法应用于 *OptDef*。首先，我们选择价值最大的控制措施集合 $S_1 \subset M$，其中 $|S_1| \leq 2$。接下来，我们枚举所有满足预算约束的、基数为 3 的控制措施集合 $\mathcal{S}_{\in}$，即对于每个满足 $|S_2| = 3$ 的控制措施集合 $S_2 \in \mathcal{S}_{\in}$，都有 $\sum_{m \in S_2} \kappa_D(m) \leq \beta_D$。然后，我们贪心地扩充这些集合，直到

预算耗尽或没有可用的控制措施为止。也就是说，对于定义在集合 M 上的次模函数 f，如果元素 $m^* \in M \setminus S_2$ 满足预算约束（即 $\kappa_D(m^*) + \sum_{m \in S_2} \kappa_D(m) \leq \beta_D$），我们就将其添加进去；该元素满足

$$m^* \in \arg\max_{m \in M \setminus S_2} \frac{f(S_2 \cup \{m\}) - f(S_2)}{\kappa_D(m)}. \tag{19}$$

然后， $S_2 \leftarrow S_2 \cup m^*$ 并重复此过程，直到无法再选取新元素。令以此方式完成的最大值集合为 S_3。如果 $f(S_1) \geq f(S_3)$，则算法返回 S_1.；否则返回 S_3.

定理 1 表明，给定一组被拦截边时，成功攻击的条件概率（即 *OptDef* 目标函数值的补数）是一个超模函数。

定理 1。令 S 为一组被拦截边$(i, j) \in E$，并令

$$0 \leq \tilde{\delta}_D(i, j, A) \leq \delta_D(i, j, A), \forall (i, j) \in E, A \in \mathcal{A}.$$

那么，对于任意路径 $p \in P$ 和攻击者 $A \in \mathcal{A}$,

$$g(S, p, A) = \prod_{(i,j) \in p \setminus S} \delta_D(i, j, A) \prod_{(i,j) \in p \cap S} \tilde{\delta}_D(i, j, A)$$

是关于 S 的非增超模函数。

证明。 我们首先证明 $g(S, p, A)$ 关于 S 单调不增。首先注意到，由于 $g(S, p, A)$ 是一组取值介于 0 和 1 之间的数的乘积，因此 $0 \leq g(S, p, A) \leq 1$。对于边集$S_1 \subseteq S_2 \subseteq E$，我们有

$$\begin{aligned}
g(S_2, p, A) &= \prod_{(i,j) \in p \setminus S_2} \delta_D(i, j, A) \prod_{(i,j) \in p \cap S_2} \tilde{\delta}_D(i, j, A) \\
&= \prod_{(i,j) \in p \cap (S_2 \setminus S_1)} \frac{\delta_D(i, j, A) \tilde{\delta}_D(i, j, A)}{\delta_D(i, j, A) \tilde{\delta}_D(i, j, A)} \prod_{(i,j) \in p \setminus S_2} \delta_D(i, j, A) \prod_{(i,j) \in p \cap S_2} \tilde{\delta}_D(i, j, A) \\
&= \prod_{(i,j) \in p \cap (S_2 \setminus S_1)} \frac{\tilde{\delta}_D(i, j, A)}{\delta_D(i, j, A)} \prod_{(i,j) \in p \setminus S_1} \delta_D(i, j, A) \prod_{(i,j) \in p \cap S_1} \tilde{\delta}_D(i, j, A) \\
&= \left(\prod_{(i,j) \in p \cap (S_2 \setminus S_1)} \frac{\tilde{\delta}_D(i, j, A)}{\delta_D(i, j, A)} \right) g(S_1, p, A).
\end{aligned} \tag{20}$$

˜由于 $0 \leq \delta_D(i,j,A) \leq \delta_D(i,j,A)\ \forall (i,j) \in E$，由 (20) 可知 $g(S,p,A)$ 关于 S 单调不增。

我们现在证明 明 $g(S,\ p,\ A)$ 是超模函数，方法是证明对所有 $(i_1,\ j_1)$，$(i_2,\ j_2) \in E$ tha t

$$\begin{aligned} & g(S,p,A) + g(S \cup \{(i_1,j_1),(i_2,j_2)\},p,A) \\ & -g(S \cup \{(i_1,j_1)\},p,A) - g(S \cup \{(i_2,j_2)\},p,A) \geq 0. \end{aligned} \tag{21}$$

我们利用 (20) 对 (21) 左侧进行代数化简：

$$\begin{aligned} & g(S,p,A) + g(S \cup \{(i_1,j_1),(i_2,j_2)\},p,A) - g(S \cup \{(i_1,j_1)\},p,A) - g(S \cup \{(i_2,j_2)\},p,A) \\ =& g(S,p,A)\left(1 + \frac{\tilde{\delta}_D(i_1,j_1,A)\tilde{\delta}_D(i_2,j_2,A)}{\delta_D(i_1,j_1,A)\delta_D(i_2,j_2,A)} - \frac{\tilde{\delta}_D(i_1,j_1,A)}{\delta_D(i_1,j_1,A)} - \frac{\tilde{\delta}_D(i_2,j_2,A)}{\delta_D(i_2,j_2,A)}\right) \\ =& g(S,p,A)\left(1 - \frac{\tilde{\delta}_D(i_2,j_2,A)}{\delta_D(i_2,j_2,A)}\right)\left(1 - \frac{\tilde{\delta}_D(i_1,j_1,A)}{\delta_D(i_1,j_1,A)}\right). \end{aligned} \tag{22}$$

˜由于，$0 \leq \delta_D(i,\ j,\ A) \leq \delta_D(i,\ j,\ A)\ \forall (i,\ j) \in E$，我们得到以下三个不等式：

$$\begin{aligned} g(S,p,A) &\geq 0, \\ 1 - \frac{\tilde{\delta}_D(i_2,j_2,A)}{\delta_D(i_2,j_2,A)} &\geq 0, \\ 1 - \frac{\tilde{\delta}_D(i_1,j_1,A)}{\delta_D(i_1,j_1,A)} &\geq 0. \end{aligned}$$

将这三个不等式与 (22) 结合可得 (21)。因此，$g(S,\ p,\ A)$ 是一个单调不增的超模函数。 ■

定理 1 的推论是，*OptDef* 目标函数是一个非负次模函数。接下来，我们证明 *OptDef* 是一个受背包约束的非负子模最大化问题。

定理 2。*OptDef* 是一个非负的子模最大化问题，且受背包约束限制。

证明。我们首先重新表述 (10)，它等价于目标函数 (11) 和约束 (12) – (13) 的补集。然后，某次

攻击被阻止的概率，根据定理 1 中 $g(S,p,A)$ 的定义，为

$$1-\sum_{A\in\mathcal{A}}\theta_D(A)\sum_{p\in P(n)}g(S,p,A)\prod_{(i,j)\in p}\psi_D(i,j,A). \tag{23}$$

其中， S 是防御者的组合所拦截的边集合。请注意，在此表述中，$\prod_{(i,j)\in p}\psi_D(i,j,A)$是一个常数。超模函数的非负加权和也是超模函数，因此将 (23) 中的函数乘以 -1 并减去 1 后，所得函数是次模函数。所得值介于 0 和 1 之间，因为它表示一个概率。

*OptDef*的其余约束，即约束 (14)–(15)，仅仅是在控制措施集合上定义一个背包约束。由于 S 随控制措施的增加而非递减，这等价于对 S施加背包约束。因此，我们得到了所需结论。 ■

定理 2 有两个推论。第一，本节前文介绍的 Khuller 等人（1999）的算法能够识别出具有保证的 $1-1/e$ 近似比的解。第二个推论是，可以使用计算效率更高的贪心算法（同样由 Khuller 等人（1999）提出）来识别近似比为$1-1/\sqrt{e}$的解。贪心算法从空控制措施集合开始，并按照 (19) 贪心地扩充该集合，直到预算用尽或可用控制措施耗尽。随后，它将这个贪心选出的集合与价值最高的单元素集合进行比较，并选择目标函数值较高的那个。

–

6 迭代式ARA算法

我们正式介绍一种迭代算法，用于求解攻击者和防御者问题中所有 k 值对应的$OptAtt$ 和 $OptDef$ 。

1. 初始化：提供数据。

   必须提供表1中给出的若干集合和信念，包括防御者的级别（K）、攻击者集合（$\mathcal{A}$）、节点集合（N）和边集合（E）、控制措施集合（M）、边的可靠度$\tilde{}$（δ_D（i,j,A）、 δ_D（i,j,A）$\forall$（i,j） $\in E, A\in\mathcal{A}$）、防御者预算（β_D）、控制措施的成本（κ_D（m） $\forall m\in M$）以及攻击者分布（θ_D（A） $\forall A\in\mathcal{A}$）。

2. 确定0级攻击者和防御者的解决方案：

我们假设，0级攻击者 A 会采取一条按第4.1节所述贪心构造的路径 p 。对于所有认为攻击者 A 处于0级的防御者 $k' > 0$，这会产生 $\psi_D^{k'}(i,\ j,\ A) = 1$，如果 $(i,\ j) \in p$，并产生 $\psi_D^{k'}(i,\ j,\ A) = 0$，如果 $(i,\ j) \notin p$。

我们假设0级防御者不会选择任何控制措施，因此0级防御者的解为 $\Omega_A^0 = \emptyset$，其中 $\delta_A^1(i,\ j|\Omega_A^0) = \delta_D(i,\ j,\ A)$，对每个攻击者 $A \in \mathcal{A}$均如此。

3. 对于 $k = 1,\ 2, \ldots\ldots,\ K-1$:

- 使用 Dijkstra算法求解 $OptAtt$： 对于每个级别为 k 的攻击者 A ，我们根据（1）–（7）求解 $OptAtt$，以获得攻击路径 p ；该路径使用 Dijkstra算法，按第4.1节所述求得。使用u_{ij} 的值，通过（8）为每个 $k < k' \leq K$ 设置 $\psi_D^{k'}(i,\ j,\ A),\ (i,\ j) \in E$。

- 求解$OptDef$ ，以确定级别为 k 的防御者。我们建议采用以下两种方法：– 使用公式 (11) – (17) 给出的混合整数规划公式，将$OptDef$ 求至最优。– 使用第5节介绍的近似算法或贪心算法，求出近似解，使其与最优解值的差距分别在 $(1-1/e)$ 或 $(1-1/\sqrt{e})$ 以内。给定$OptDef$的一个解，令 $\Omega_A^k = \{m \in M \mid w_m = 1\}$。然后使用 (18) 为所有级别为 $k+1$ 的攻击者 $A \in \mathcal{A}$ 设置$\delta_A^{k+1}(i,j|\Omega_A^k)$ 的值。

–

4. 最后再求解一次$OptDef$ ，以获得级别为 K 的防御者的解。

为说明该算法，我们重新审视第1.1节中引入的示例。同样，我们假设防御者的预算只允许其选择一项控制措施。接下来，我们依次运行该算法，分别求出级别为1–4的防御者的OptDef解。对于级别从 $k = 1$ 到 $k = 4$的每个 k防御者，我们假设防御者要防御级别低于 k的攻击者所构成的均匀分布。我们报告两种模型的攻击成功概率，以便直接比较表2中的$OptAtt$ 和$OptDef$ 解。

我们首先考虑0级攻击者，他们采用贪心策略选择右侧路径，攻击成功概率为0.102。0级防御者不选择任何控制措施。1级攻击者针对0级防御者进行优化，再次选择右侧路径，攻击成功概率仍为0.102，因为在所有边均未拦截的情况下，这是可靠性最高的路径。

我们继续逐级考虑攻击者和防御者，直至达到所需的防御者等级。接下来，我们求解针对0级攻击者进行优化的1级防御者的$OptDef$。1级防御者选择能最大程度降低0级攻击者所选路径可靠性的控制措施，即控制措施 m_3。这使$OptDef$攻击成功概率达到0.074。随后，2级攻击者选择左侧路径，攻击成功概率为0.09。2级防御者针对0级和1级攻击者进行优化；两者都选择右侧路径，因此防御者再次选择 m_3，使攻击成功概率达到0.074。基于此，3级攻击者选择右侧路径，攻击成功概率为0.102。

接下来，我们考虑3级防御者，其防御对象是0至2级攻击者，其中两名选择右侧路径，一名选择左侧路径。3级防御者选择 m_1 ，使$OptDef$攻击成功概率达到0.078。4级防御者则防御所有0至3级攻击者，其中两名经过左侧路径，另两名经过右侧路径。在这种情况下，m_2 成为最优控制措施选择，由此得到最终的$OptDef$攻击成功概率0.069。在这个例子中，我们看到防御者会根据其对攻击者所选路径的判断来调整控制决策。

表2：示例 $OptAtt$ 和$OptDef$针对不同级别攻击者和防御者的解决方案 s

攻击者			防御者		
k	Path 已选择	*OptAtt* 攻击成功概率	k	缓解措施 已选择	*OptDef* 攻击成功概率
0	右	0.102	0	N/A	N/A
1	右	0.102	1	m_3	0.074
2	Left	0.09	2	m_3	0.074
3	右	0.102	3	m_1	0.078
–	–	–	4	m_2	0.069

请注意，ARA算法会得出一系列针对$OptDef$的解，这些解分别对应 0、1、..... K 名防御者。因此，我们的方法为决策者提供了一组解，而非单个“良好”解，这有利于防御规划。

7 计算结果

本节基于 DuBois（2020）介绍的信息安全投资案例研究，给出模型和算法的计算结果。在该案例研究中，我们根据特定的参数化结构生成随机数据，并能够调整该结构，以控制问题的规模和复杂度。我们将介绍如何构建这一结构以及所用的参数。随后，我们改变问题实例的规模，以评估近似算法的性能。

在该案例研究中，每个问题实例由一个网络构成，该网络由一个源节点、一个汇节点和 ℓ 个节点“层”组成。每一层都是一个节点集合，其中的节点只与下一层中的节点相连。为简化起见，我们假设每层包含相同数量的节点，因此形成了一个拥有大量互连关系和路径的结构。图2展示了一个所研究网络的示例，其中包含两层，每层有三个节点。穿过该网络的一条路径包含每层中的一个节点。源节点通过可靠度为 1 的不可阻断边与第一组中的每个节点相连。分别从集合 1、.....、$\ell - 1$ 中的每个节点出发，有三条边连接到集合 2、.....、ℓ中的节点。

我们首先分配边，确保每个节点都有一条入边和一条出边，然后随机分配其余边。随后，我们为每条边随机分配可靠度，并将生成的每个可靠度视为常量。未阻断可靠度在 0 到 1 之间均匀取值，即 $\delta(i,\ j) \sim U(0,1]$。阻断后可靠度是未阻断值的一个随机˜(0，1)比例，即 $\delta(i,\ j) \sim U(0,\ 1] \cdot \delta(i,\ j)$。最后，不可阻断边将第 ℓ层的每个节点连接到汇节点，其可靠度为 $U(0.5,\ 1]$。我们选定若干个可能的控制措施以及防御者的预算，然后使用指定成本范围内的均匀分布，随机确定这些控制措施各自的成本。对于基数预算约束，成本恰好为 1；对于背包约束，成本服从 $U[0.5, 1.5]$ 分布，以确保在两种情况下每项控制措施的平均成本均为 1.0。随后，为每项控制措施随机分配一组要阻断的边。为此，我们首先指定一个参数 α，表示任意一项控制措施所覆盖边的平均比例。如果采用基数预算约束，我们就遍历每项控制措施的所有边，并以 α 的概率将每条边分配给该控制措施。如果采用背包约束，我们会通过考虑成本来调整将每条边分配给某项控制措施的概率

对于控制措施，我们会通过考虑成本来调整将边分配给该控制措施的概率。令 Δ_m 为控制措施 m 的成本减去平均成本后，再除以可能成本范围所得的值。在我们的情形中，成本取自范围 $[0.5, 1.5]$，这等价于 $\Delta_m = \kappa_D(m) - 1$。然后，我们以 $\alpha(1 + \alpha_2\Delta_m)$ 的概率将边分配给控制措施 m，其中 α_2 表示成本对缓解质量的影响程度。

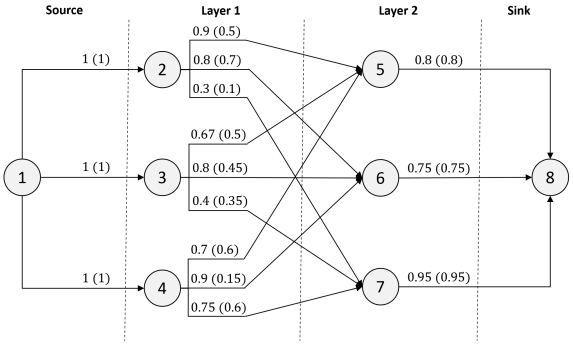


图2：包含两层的合成网络结构简单示例。沿每条边标示了边未受攻击（受到攻击）时的示例可靠度，$\delta_{ij}(i,\ j,\ A)$ $\left(\tilde{\delta}_{ij}(i,\ j,\ A)\right)$

在我们的案例研究中，我们为一个包含 $\ell = 5$ 层、每层5个节点的图生成了一个问题实例。为了更清晰地展示控制措施之间的权衡，我们对防御者预算采用了基数约束，即防御者可以从10项控制措施中选择4项。每项控制措施均随机生成，旨在覆盖约15%的边（$\alpha = 0.15$）。虽然防御者等级的现实取值为4，但为了研究一系列防御方案，我们将防御者等级的上限设为 $K = 10$ 。每个防御者等级 $k \leq K$ 都假设攻击者等级在 $0 \leq k' < k$上服从均匀分布。

我们使用第 6 节中的算法求解该案例研究；对于防御者的每个级别，我们都使用 Gurobi 9.1.1 将 *OptDef* 求至最优。该计算在一台配备 Intel(R) Core(TM) i7-8650U CPU @1.90GHz 2.11GHz 处理器和 16GB 随机存取存储器的计算机上完成，完整运行该算法耗时 1.36 秒。

ARA算法在 k的所有级别中总共求解防御者问题 11 次，从而在得出 $K = 10$ 级防御者的最终解之前，生成多个可能的防御者解。表 3 报告了从 0 到 10 级的各级防御者 k所选择的控制措施组合。请注意，根据假设，0级防御者不选择任何控制措施。表 3 显示，有些控制措施在任何防御者的解中都未被选用，例如 m_1、 m_6、 m_7和 m_8。

其他控制措施相互配合，能更好地防范攻击者可能采取的不同路径，或更多种类的路径（例如，控制措施 m_2、 m_3和 m_4）。控制措施 m_5 和 m_9 分别由级别至少为 3 级和 5 级的防御者选择，这表明某些控制措施只有对策略性更强的防御者（他们认为自己面对的是更具策略性的攻击者）才具有吸引力。

表 3：防御者为不同 k 级别选择的组合表

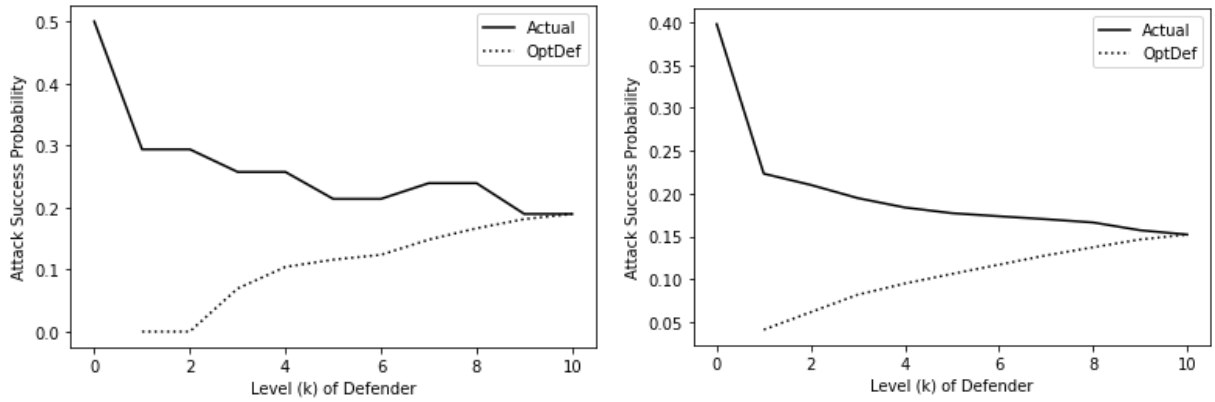
	控制措施									
防御者等级	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}
0	-	-	-	-	-	-	-	-	-	-
1	-	✓	✓	✓	-	-	-	-	-	✓
2	-	✓	✓	✓	-	-	-	-	-	✓
3	-	✓	-	✓	✓	-	-	-	-	✓
4	-	✓	-	✓	✓	-	-	-	-	✓
5	-	✓	-	✓	✓	-	-	-	✓	-
6	-	✓	-	✓	✓	-	-	-	✓	-
7	-	✓	✓	-	✓	-	-	-	✓	-
8	-	✓	✓	-	✓	-	-	-	✓	-
9	-	-	✓	✓	✓	-	-	-	✓	-
10	-	-	✓	✓	✓	-	-	-	✓	-

接下来，我们考察攻击成功概率，即成功攻击的平均概率，以及*OptDef* 目标函数值的补数。我们报告级别为 $0-9$ 的防御者在攻击者级别服从均匀分布 $0-9$ 时的攻击成功概率。图3从防御者和攻击者双方的角度报告了攻击成功概率。首先，报告与*OptDef* 对应的攻击成功概率（虚线），该概率反映了根据防御者对攻击者的认知所估算的攻击成功概率。其次，报告的是针对同一攻击者集合，根据其实际战略成熟度级别回溯得出的实际攻击成功概率（实线）。这些数值有所不同，因为级别低于 10 的防御者无法识别级别为 9（或更高）的攻击者的真实战略成熟度级别。

图3(a)展示了单个问题实例的结果，图3(b)展示了对100个与示例问题规模相同的问题实例取平均后的结果。在两幅图中，与 *OptDef* 相关的攻击成功概率均随 k 增加而上升。这是因为，更具策略性的防御者会为更具策略性的攻击者选择控制措施，而后者更有能力规避防御。我们观察到，实际攻击成功概率高于与 *OptDef*相关的攻击成功概率，因为级别为 $k<10$ 的防御者认为某些攻击者的策略性低于

其实际水平，从而导致所认为的攻击成功概率不准确。当防御者的信念与现实相符时，两条线会收敛到同一点；在我们的示例中，这发生在防御者处于 $k = 10$级别时。图3(a)表明，对于任何特定的问题实例，实际攻击成功概率并不总是随 k 增加而降低。这种影响是由 k级别更高的攻击者造成的。由于防御者无法准确假设攻击者分布，攻击者可能会针对高策略水平防御者找到更多可靠路径。

图3(b)展示了*OptDef* 对应的攻击成功概率，以及在100个相同规模的随机生成的问题实例中取平均后的实际值。图3(b)中的总体趋势与图3(a)相似，显示平均实际攻击成功概率随 k单调递减。这表明，*OptDef*提供的解平均而言能为更具策略性的防御者提供更好的防御。



(a) 示例案例　　(b) 对100个实例取平均

图3：两条曲线分别展示了0至9级攻击者针对 $k < 10$级防御者的平均攻击成功率，以及 $k < 10$ 级防御者的OptDef值（0至 k级攻击者均匀分布时的攻击成功率）。

接下来，我们考察防御者的控制措施组合所产生的影响，以及该组合应对战略成熟度不同的攻击者时的表现。与之前一样，我们考虑级别为0至9的防御者。我们研究两组攻击者对这些防御者的攻击表现：低级别（级别 $0-4$）和高级别（级别 $5-9$）。我们还报告所有攻击者（级别 $0-9$）的表现，以供比较。请注意，级别为 $0-9$ 的攻击者这一情形与图3中考察的情形一致。与之前一样，在每种情形下，攻击者的实际级别均服从离散均匀分布。每位防御者都假设攻击者的级别在所有低于自身级别的级别 k 中均匀分布。5级防御者认为自己正在防御低级别的 $0-4$ 攻击者，而

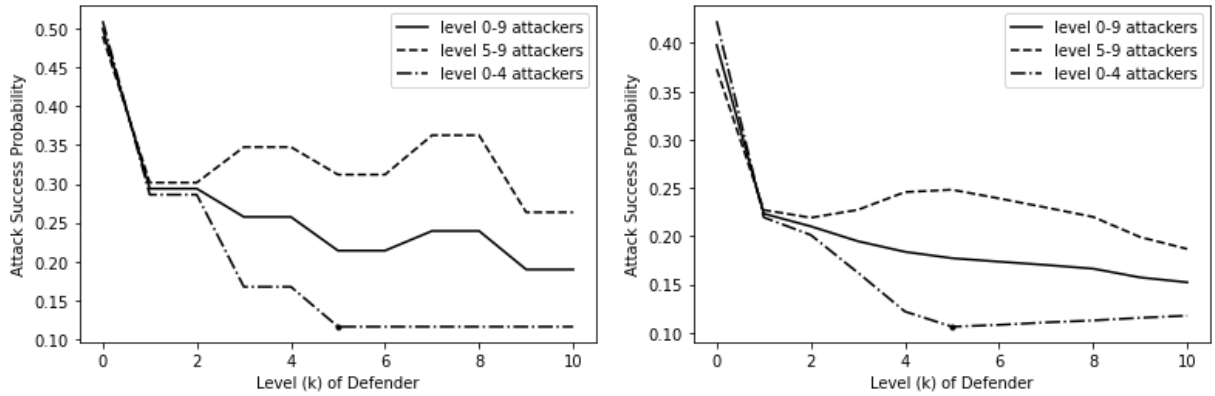
10级防御者认为自己正在防御级别为 $0-9$ 的攻击者。在这两种情形下，防御者的信念都与攻击者的实际级别相符；然而，在其他所有情形下，防御者的信念与攻击者的实际级别均不一致，防御者会在不同程度上高估或低估攻击者的级别。

图4展示了三组攻击者面对防御者时的实际攻击成功概率，其中图4(a)展示了示例问题的实际攻击成功概率，图4(b)展示了对100个问题实例取平均后的实际攻击成功概率。在两幅图中，对于所有防御者等级，等级较高的攻击者往往比等级较低的攻击者更容易成功，这符合预期。我们观察到，面对 $0-4$ 级攻击者时，等级较高的防御者往往能取得较低的攻击成功概率。这表明，即使防御者高估了攻击者的等级（ $6-9$ 级防御者就会出现这种情况），防御措施也可能更有效地对付策略性较弱的攻击者。

相比之下， $5-9$ 级攻击者往往能取得较高的攻击成功概率。在图4(a)中， $5-9$ 级攻击者面对7级和8级防御者时，攻击成功概率最高。这一结果令人意外，其原因是，等级高于防御者的攻击者能够找到防御者防守不力的路径。这表明，与策略水平较低的防御者所选择的防御措施相比，策略水平较高的防御者所选择的防御措施有时反而更难有效应对高策略水平的攻击者。

图4(b)展示了对100个随机生成的问题实例取平均后的结果。总体而言，随着防御者等级提高，针对所有级别为 $0-9$ 的攻击者和低级 $0-4$ 攻击者的攻击成功概率呈下降趋势。针对级别为 $0-4$ 的攻击者，攻击成功概率的下降更为明显。这是因为随着防御者等级提高至5，防御者对攻击者分布的假设越来越准确。等级超过5后，防御者面对级别为 $0-4$ 的攻击者时仍能持续有效防御，而面对级别为$5-9$ 的攻击者时，防御效果大多有所提升。针对高级别 $5-9$ 攻击者的实际攻击成功概率并不会随防御者等级提高而单调下降（也就是说，该概率在防御者等级从2升至5期间反而上升）。这有悖直觉，是由防御者的信念造成的。例如，级别为 $k=5$ 的防御者假设自己面对的是级别为 $0-4$ 的攻击者，因此会针对策略性较弱的攻击者优化防御。随着防御者等级提高至 $k=9$，防御者对付最具策略性的攻击者时会变得更加有效。总体而言，这个例子表明，对于防御者而言，更好的做法是

高估　　攻击者的级别，而不是低估攻击者的级别　　s.



(a) 示例问题　　(b) 对 100 个实例取平均

图4：针对级别为 0 至 9 的防御者，三种攻击者均匀分布下的攻击者成功概率：低级别（0-4）、高级别（5-9）以及两者兼有（0-9）。

为了进一步分析防御者错误判断攻击者复杂程度的影响，我们考虑一名等级为 $k = 10$ 的防御者，其会将攻击者等级统一高估或低估某个偏移量。和之前一样，我们假设攻击者等级真实值为0到9，且服从均匀分布。正偏移表示防御者高估攻击者等级，负偏移表示防御者低估攻击者等级。高估时，防御者无法感知等级高于自身的攻击者，因此在$OptDef$中会假设这类攻击者的等级比自己低一级。同样，低估时，防御者始终假设攻击者的等级至少为0。例如，偏移量为-3的防御者会将感知到的攻击者等级下限设为0，因此只能感知到等级为0至6的攻击者。

图5展示了实际攻击成功概率在 100 个问题实例上的平均值随偏移量的变化。我们观察到，与防御者准确感知攻击者真实级别的情况（偏移量为 0）相比，高估或低估攻击者分布都会导致更高的攻击成功概率；低估攻击者的情况略差于高估。这一观察结果与图4一致。这表明，防御者最好能够“判断正确”，准确建模攻击者；此外，宁可按应对复杂攻击者的方式进行规划，也会带来一定好处。

接下来，我们评估贪心算法（见第5节）所确定解的质量。该算法保证找到的解的目标函数值至少为 $1-1/\sqrt{e}$ 的　　–

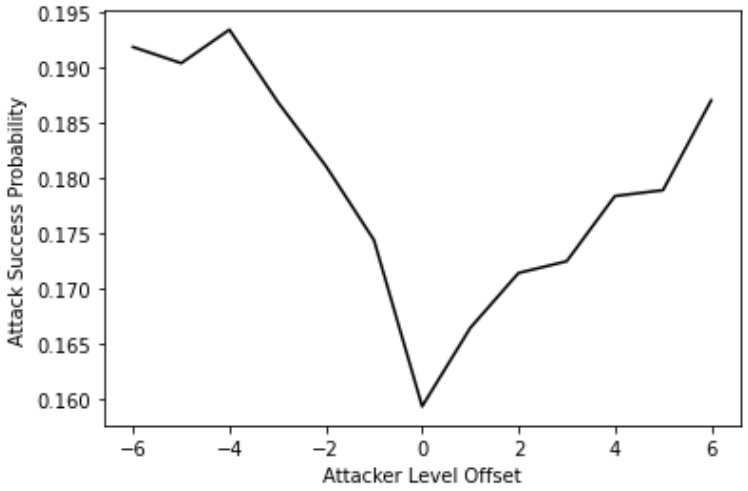


图5：均匀分布的攻击者对10级防御者的攻击成功率；这些防御者认为所有攻击者的级别都偏移了横轴所示的数值。

最优*OptDef* 解值。我们考虑为10级防御者随机生成的问题实例，每个实例的预算均采用背包约束。我们在相同的问题实例上比较贪心算法与精确算法，具体做法如下：首先使用贪心算法，为级别为 $1-9$的防御者确定近似最优的*OptDef*解。然后，对10级防御者的问题实例使用精确算法或贪心算法。

我们随机生成了40个规模各异的问题实例，以评估贪心算法的解质量。表4报告了用于生成每个问题实例的参数，以及精确算法（*OptDef*）和贪心算法对应的 CPU 时间。将 *OptDef* 精确求解至最优所需的 CPU 时间（以秒为单位）包括设置时间（即写入变量和约束的时间）以及求解器时间。同样，实现贪心算法所需的时间包括读取输入和执行算法的时间。表4报告了贪心解值（z_h）与 *OptDef* 的最优解值之比（z_D^*）。结果表明，在所有问题实例中，贪心解与最优解值的差距均在1.7%以内；在40个问题实例中，贪心算法有28个找到了最优解。对于规模较大的问题实例，Gurobi 加载和求解问题实例所需的时间明显长于贪心算法，这为采用贪心算法提供了动力。

表4：满足背包约束的防御者问题各实例的求解时间，以及贪心算法的相对准确度。

层 ℓ	每层节点数 层，$\lvert N_\ell \rvert$	边 $\lvert E \rvert$	控制措施 $\lvert M \rvert$	预算 β	OptDef 时间（秒）	贪心 时间（秒）	Gap z_h / z_D^*
5	15	930	10	5	3.07	0.078	0.983
5	15	930	20	10	2.62	0.236	0.998
10	10	920	10	5	2.47	0.237	0.999
10	10	920	20	10	2.26	0.277	0.999
10	15	2055	12	6	19.9	0.998	0.997
10	15	2055	24	12	6.99	1.07	0.999
10	20	3640	14	7	49.7	2.25	0.998
10	20	3640	30	15	19.1	3.24	1.000
10	25	5675	16	8	66.2	2.12	0.999
10	25	5675	34	17	63.7	6.13	1.000
15	5	360	10	5	0.724	0.075	0.999
15	5	360	20	10	1.16	0.337	1.000
15	10	1420	12	6	8.40	0.328	0.997
15	10	1420	24	12	7.16	1.13	1.000
15	15	3180	14	7	24.0	1.13	0.993
15	15	3180	30	15	22.2	2.48	1.000
15	20	3000	16	8	22.1	1.15	1.000
15	20	3000	34	17	18.8	3.75	1.000
15	20	5640	16	8	68.1	2.36	1.000
15	20	5640	34	17	60.3	8.27	1.000
15	25	4000	18	9	36.7	2.22	0.999
15	25	4000	40	20	41.6	9.74	1.000
15	25	8800	18	9	157.6	4.15	1.000
15	25	8800	40	20	159.1	17.8	1.000
20	10	1920	14	7	12.0	0.717	1.000
20	10	1920	30	15	10.3	2.81	1.000
20	15	4000	16	8	38.7	1.33	1.000
20	15	4000	34	17	34.2	6.66	1.000
20	15	4305	16	8	44.8	1.62	1.000
20	15	4305	34	17	41.8	6.17	1.000
20	20	4000	18	9	12.1	0.637	1.000
20	20	4000	40	20	32.2	7.56	1.000
20	20	7640	18	9	124.6	3.54	1.000
20	20	7640	40	20	107.3	13.8	1.000
20	25	5000	20	10	22.7	1.09	1.000
20	25	5000	44	22	47.6	11.9	1.000
20	25	11925	20	10	95.1	2.83	1.000
20	25	11925	44	22	238.3	28.6	1.000
25	10	2420	16	8	5.96	0.459	1.000
25	10	2420	34	17	15.0	3.29	1.000

8 结论

本文介绍了新的模型和算法，用于确定在面对战略成熟度各异的多个自适应对手时应部署的安全控制措施组合。为指导此类投资，我们将对抗风险分析框架扩展至单一防御者与多个攻击者参与的最大可靠性路径阻断问题。我们假设所有参与者均具有有限理性，并考虑系统信息和参与者信息方面的不确定性。我们提出了攻击者问题和防御者问题的混合整数规划公式，并介绍了一种对抗风险分析算法，用于迭代求解这些模型。我们还提出了一种近似算法，可在保证 $1 - 1/e$ 近似比的前提下，确定防御者问题的近似最优解。

这些解为构建分层安全防御的投资提供了参考，且能够有效应对众多对手，其中也包括一些非策略性对手。所提方法的一项实际优势是能够提供一系列投资方案，而非单一方案，从而为决策者提供帮助。该建模方法的另一项优势是允许考虑非策略性攻击者，这可用于模拟自然因素带来的风险；不过，我们并未专门考察自然灾害的影响（Zhuang 和 Bier，2007年）。新漏洞不断出现，因此，组织应定期主动开展风险评估，以指导防御投资和决策。本文提出的方法旨在为这些决策提供帮助。

我们通过一个案例研究展示这些模型和求解技术。该框架表明，防御策略会随着防御者和攻击者各自的战略成熟度级别而变化。研究结果确定了在一系列对手假设下都有效的安全控制措施。与更具战略性的防御者相比，这些方案往往更能防御战略性较弱的攻击者。此外，研究结果表明，防御者高估攻击者的战略成熟度，可能比低估更好。

未来研究有几个方向。首先，采用有限理性参与者的对抗风险分析方法可以扩展到最大可靠性路径阻断问题以外的其他网络阻断模型。其次，可以扩展模型，以适应对网络的了解少于防御者的攻击者；一种可能的方法是在求解攻击者的模型时，移除攻击者不了解的部分网络

。第三，对抗风险分析方法可以根据具体应用，在安全目标与系统性能之间进行权衡。

致谢

第一作者和末位作者的工作部分得到了美国国家科学基金会项目（编号：2000986）的资助。本文中表达的任何观点、研究结果、结论或建议均仅代表作者本人，并不一定反映美国国家科学基金会的观点。作者还要感谢匿名审稿人，他们提出的改进建议使稿件质量得到了显著提升。

参考文献

Ravindra Ahuja、Thomas Magnanti 和 James Orlin。《网络流：理论、算法与应用》。Prentice-Hall, Inc.，第1版，1993年。ISBN 0-13-617549-X。Laura A Albert、Alexander Nikolaev 和 Sheldon H Jacobson。国土安全研究机遇。《IISE Transactions》，55(1):22–31，2023年。David Banks、Vıctor Gallego、Roi Naveiro 和 David Rıos Insua。对抗性风险分析：概述。《Wiley Interdisciplinary Reviews: Computational Statistics》，第 e1530 页，2020年。Stefano Bistarelli、Fabio Fioravanti 和 Pamela Peretti。用于安全投资经济评估的防御树。载于《第一届国际可用性、可靠性与安全会议（ARES'06），奥地利维也纳，2006年4月20—22日论文集》，第8–页。电气电子工程师学会，2006年。William N Caballero、Mark Friend 和 Erik Blasch。多源指挥与控制中的对抗性机器学习与对抗性风险分析。《SPIE会议论文集 11756，信号处理、传感器／信息融合与目标识别 XXX》，11756L:98–108，2021年。C. F. Camerer、T.-H. Ho 和 J.-K. Chong。博弈的认知层级模型。《经济学季刊》，119(3):861–898，2004年。Javier Cano、Alessandro Pollini、Lorenzo Falciani 和 Uˇgur Turhan。通过对抗性风险分析对机场领域当前及新兴威胁进行建模。《风险研究杂志》，19 (7):894–912，2016年。Huseyin Cavusoglu、Srinivasan Raghunathan 和 Wei T. Yue。信息技术安全投资的决策理论与博弈论方法。《管理信息系统杂志》，25(2):281–304，2008年。经济顾问委员会。恶意网络活动对美国经济的成本。技术报告，白宫，华盛顿哥伦比亚特区，2018年。网址：https://www.whitehouse.gov/wp-co

ntent/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy .pdf。Eric DuBois。《应用于国土安全系统的优化模型》。博士论文，威斯康星大学麦迪逊分校，威斯康星州麦迪逊，2020年。Andrew Fielder、Emmanouil Panaousis、Pasquale Malacaria、Chris Hankin 和 Fabrizio Smeraldi。网络安全投资的决策支持方法。《决策支持系统》，86:13–23，2016年。Douglas W Hubbard 和 Richard Seiersen。《如何量化网络安全风险中的任何事物》。John Wiley & Sons，2016年。Eitan Israeli 和 R. Kevin Wood。最短路径网络阻断。《Networks》，40(2):97–111，2002年。Chaitanya Joshi、Jesus Rios Aliaga 和 David Rios Insua。内部人员威胁建模：一种对抗性风险分析方法。《IEEE信息取证与安全汇刊》，16:1131–1142，2020年。Samir Khuller、Anna Moss 和 Joseph Seffi Naor。预算约束最大覆盖问题。《Information Processing Letters》，70(1):39–45，1999年。William Knowles、Daniel Prince、David Hutchison、Jules Ferdinand Pagna Disso 和 Kevin Jones。工业控制系统网络安全管理综述。《国际关键基础设施保护杂志》，9:52–80，2015年。Clemens Scott Kruse、Benjamin Frederick、Taylor Jacobson 和 D. Kyle Monticone。医疗保健领域的网络安全：现代威胁与趋势的系统综述。《Technology and Health Care》，25(1):1–10，2017年。Harjinder Singh Lallie、Kurt Debattista 和 Jay Bal。网络安全中攻击图与攻击树可视化语法综述。《Computer Science Review》，35:100219，2020年。Ritchie Lee 和 David H. Wolpert。空中相遇期间飞行员行为的博弈论建模。载于 Tatiana Valentine Guy、Miroslav K´arn´y 和 David H. Wolpert（编），《不完美决策者的决策》，智能系统参考图书馆第28卷。施普林格，柏林、海德堡，2012年。J. Letchford 和 Y. Vorobeychik。攻击计划的最优阻断。载于《第12届国际自主智能体与多智能体系统会议论文集》，明尼苏达州圣保罗，2013年。David P. Morton、Feng Pan 和 Kevin J. Saeger。核走私阻断模型。《IIE Transactions》，39(1):3–14，2007年。Apurba K Nandi、Hugh R Medal 和 Satish Vadlamani。阻断攻击图以保护组织免受网络攻击：双层防御者–攻击者模型。《Computers & Operations Research》，75:118–131，2016年。美国国家标准与技术研究院。改善关键基础设施网络安全的框架。NIST报告，美国国家标准与技术研究院，华盛顿哥伦比亚特区，2018年。

George L Nemhauser、Laurence A Wolsey 和 Marshall L Fisher。最大化次模集合函数的近似分析——I。数学规划，14(1):265–294，1978年。Jesus Rios 和 David Rios Insua。反恐建模中的对抗性风险分析。风险分析，32(5):894–915，2012年。David Rios Insua、Aitor Couce-Vieira、Jose A Rubio、Wolter Pieters、Katsiaryna Labunets 和 Daniel G. Rasines。网络安全的对抗风险分析框架。风险分析，41 (1):16–36，2021年。Ron Ross、Victoria Pillitteri、Kelley Dempsey、Mark Riddle 和 Gary Guissanie。在非联邦系统和组织中保护受控非机密信息。NIST 特别出版物 800-171v2，美国国家标准与技术研究院，华盛顿哥伦比亚特区，2021年。Casey Rothschild、Laura McLay 和 Seth Guikema。不完全信息下的对抗性风险分析：层级 k 方法。风险分析：国际期刊，32(7):1219–1231，2012年。Javier Salmer´on。网络阻断中的欺骗战术：一种多目标方法。*Networks*，60(1):45–58，2012年。Benjamin Scheibehenne、Rainer Greifeneder 和 Peter M Todd。选择是否会多到令人难以承受？关于选择过载的元分析综述。《消费者研究杂志》，37(3): 409–425，2010年。B. Schneier。攻击树：安全威胁建模。《*Dr. Dobb's* 软件工具杂志》，24 (12):21–29，1999年。A. Singhal 和 X. Ou。使用概率攻击图对企业网络进行安全风险分析。载于 L. Wang、S. Jajodia、A. Singhal、A. Singhal 和 X. Ou（编），《网络安全度量》。施普林格，德国海德堡，2017年。J Cole Smith 和 Yongjia Song。网络阻断模型与算法综述。《欧洲运筹学杂志》，283(3):797–811，2020年。Dale O. Stahl 和 Paul W. Wilson。论参与者对其他参与者的模型：理论与实验性证据。《博弈与经济行为》，10(1):218–254，1995年。Rock Stevens、Josiah Dykstra、Wendy Knox Everette、James Chapman、Garrett Bladow、Alexander Farmer、Kevin Halliday 和 Michelle L Mazurek。合规注意事项：调查与美国数字安全标准相关的安全问题。载于网络与分布式系统安全（*NDSS*）研讨会，加利福尼亚州圣迭戈，2020年。Maxim Sviridenko。关于在背包约束下最大化次模集合函数的说明。《运筹学快报》，32(1):41–43，2004年。Shouqiang Wang 和 David Banks。叛乱活动的网络路由：对抗性风险分析框架。《海军研究后勤》，58(6):595–607，2011年。Wei Wang、Francesco Di Maio 和 Enrico Zio。通过对抗性风险分析分配最优防御资源，以保护信息物理系统免受网络攻击。风险分析，39(12):2766– 2785，2019年。

Wenye Wang 和 Zhuo Lu。智能电网中的网络安全：综述与挑战。计算机网络，57(5):1344–1371，2013年。Jing Zhang、Jun Zhuang 和 Brandon Behlendorf。随机最短路径网络阻断：亚利桑那州—墨西哥边境案例研究。《可靠性工程与系统安全》，179:62–73，2018年。Kaiyue Zheng 和 Laura A Albert。延缓针对关键信息技术基础设施的对抗性攻击的阻断模型。《海军研究后勤》，66(5):411–429，2019a。Kaiyue Zheng 和 Laura A Albert。缓解网络供应链风险的稳健方法。风险分析，39(9):2076–2092，2019b。Kaiyue Zheng、Laura A Albert、James R Luedtke 和 Eli Towle。用于网络安全规划与管理的预算化最大多重覆盖模型。*IISE Transactions*，51(12):1303– 1317，2019年。Jun Zhuang 和 Vicki M Bier。在恐怖主义与自然灾害之间取得平衡——攻击者努力内生的防御策略。运筹学，55(5):976–991，2007年。