应对有限理性对手的 Stackelberg网络阻断

TIEN MAI,新加坡管理大学，新加坡AVINANDAN BOSE,华盛顿大学，美国ARUNESH SINHA, 罗格斯大学，美国THANH H. NGUYEN,俄勒冈大学，美国

本文研究 Stackelberg 网络阻断博弈——这是一类重要的博弈，防御者首先将（随机化的）防御资源分配给图中的一组关键节点，而对手则据此选择攻击这些节点的路径。我们考虑有限理性对手，其响应模型基于经典的基于 logit 的离散选择模型的一种动态形式。我们证明，在理性情形下，为防御者寻找最优阻断策略是 NP-困难的。由此产生的优化问题实际上是非凸的，而且包含对指数数量路径求和的复杂项。为应对这些计算挑战，我们提出了新的高效近似算法，并给出有界的解保证。首先，我们提出一种基于动态规划的多项式时间形式化方法，以解决路径数量呈指数增长的挑战。随后，我们证明，非凸目标函数的梯度也可以在多项式时间内计算，从而能够使用基于梯度的方法高效求解该问题。其次，我们确定了一个凸的受限问题，因此，基于梯度的方法能够找到该受限问题的全局最优解。我们还给出了若干温和条件，在这些条件下，该受限问题能够为原问题提供有界近似。

arXiv:2301.12232v1 [math.OC] 28 Jan 2023

预印本。

1 引言

网络阻断是人工智能领域中一个研究充分的课题。许多实际问题 [Smith 和 Song， 2020], 例如网络系统和非法供应网络中的问题，都可以建模为网络阻断问题。文献中存在许多不同的网络阻断模型，因此，人们采用了多种技术来求解不同类型的这类问题。我们的工作聚焦于一种特定情形：在规模更大的网络中，有一组关键节点 $\mathcal{L}$ 需要保护，而该网络共有 $\mathcal{S}$ 个节点。我们采用一种广泛使用的网络阻断模型 [Fulkerson 和 Harding，1977年，Israeli 和 Wood， 2002], 在该模型中，阻断者（防御者）将有限的防御资源随机分配给 $\mathcal{L}$中的关键节点。对手从起点出发穿越图 s_o，并抵达目的地 s_d。只有当对手经过 $\mathcal{L}$中的任一节点时，才会与防御者发生交互。我们通过领导者—跟随者（Stackelberg）博弈来建模这种交互：防御者先以随机方式分配资源，然后对手据此选择路径。

我们使用动态分位响应模型（这是一类众所周知的动态离散选择模型的实例 [Aguirregabiria 和 Mira，2010，Rust， 1987]）来刻画对手的行为。在该模型中，当前位于节点 s的对手以一定概率选择访问下一个节点 s'，该概率与数值 $\exp\left(\frac{v}{\mu}\right)$成正比，其中 v 是对手选择 s'（在s 的邻居中）所获得的即时效用， μ 是一个常数。在博弈情境中，效用 v 取决于防御者的资源分配，用 x 表示，即 $v(\cdot|\mathrm{x})$。在一项开创性成果中， [Fosgerau 等，2013，Mai 等人 2015], 证明，在某些特定设置下，这种局部的分位响应选择与在网络图上对路径进行分位响应选择直接对应。也就是说，从起点到目的地选择某条路径 τ的概率与 $\exp\left(\frac{U(\tau)}{\mu}\right)$成正比，其中 $U(\tau)$是该路径上各项效用之和。我们使用这种对手响应模型，构建一个优化问题，以计算防御者的最优阻断策略。据我们所知，现有的网络阻断模型都假设对手完全理性，并采用一些线性规划技术来处理 [Smith 等，2009，Smith 和 Song，2020]。我们首次探索使用动态离散选择框架对有限理性对手进行建模，并将防御者的问题表述为非线性优化问题，从而为通过非线性优化技术求解网络阻断问题创造了可能。

尽管对手响应的闭式结果在数学上颇具意义，但它也带来了计算挑战，因为计算任何此类概率都需要对从起点到目的地的指数数量的路径进行推理。本文证明，在有限理性对手的博弈设定下，为防御者寻找最优阻断策略是 NP-困难的。因此，我们采用以下新颖高效的近似算法，解决防御者面临的这一复杂非凸优化问题。

首先，我们提出一种高效的动态规划方法，用于计算目标函数（防御者期望效用）以及优化目标函数的梯度，尽管这些项涉及对指数级数量的路径求和。该方法通过利用不同路径之间与对手效用相关项的递归关系来实现，这些递归关系涉及防御者的最优阻断策略计算。通过采用动态规划，我们可以使用梯度下降方法，在每一步都高效地进行计算，以优化防御者策略。

其次，尽管上述提出的方法在计算上高效，但由于防御者优化问题的非凸性，它无法保证全局最优性。因此，我们确定了一个受限问题，在该问题中，对手只能访问 L 中的一个节点（任意一个），并证明在这一限制下，优化问题是凸的。因此，可以利用第一部分中介绍的高效梯度下降，以一种易于处理的方式对该受限问题求得最优解

贡献。我们进一步确定了两个特定于问题的项的条件 β_1，β_2（方程 8），使得如果 β_1，β_2 较小，则上述受限问题的解能够为原始的非受限问题提供较为接近的近似保证。

符号说明：粗体字符表示矩阵、向量或集合，a_i 表示可索引的$\mathbf{a}$的第 i个元素。对于任意 $m \in \mathbb{N}$，我们使用 $[m]$表示集合$\{1, \ldots\ldots, m\}$。

2 相关工作

动态离散选择模型。我们采用动态离散选择（DDC）框架对对手的有限理性行为进行建模。自 [Rust, 1987], 的开创性工作以来，DDC模型得到了广泛研究和应用，用于分析序贯前瞻选择行为，并被应用于多个领域，例如生育和儿童死亡率 [Wolpin, 1984], 、工作匹配和职业选择 [Miller, 1984], 、公交车发动机更换 [Rust, 1987], 以及路径选择分析 [Fosgerau 等，2013、Mai等, 2015]。在现有的DDC模型中，基于 Logit 的 DDC因其具有闭式表达而广受欢迎 [Rust, 1987]。该模型可被视为广为人知的多项 Logit（或分位响应）模型的动态版本 [McFadden，1981、Train, 2003]。在交通建模，尤其是路径选择分析中，基于 Logit 的 DDC模型被应用于无折扣无限时域的马尔可夫决策过程中，以构建预测人们有限理性路径选择行为的模型 [Fosgerau等人，2013、Mai等, 2015]。正如 [Zimmermann和Frejinger, 2020], 所强调的，这类路径选择模型与随机最短路径问题 [Bertsekas和Tsitsiklis, 1991]具有协同关系。

网络阻断。我们的工作与研究充分的最短路径阻断问题密切相关 [Fulkerson 和 Harding, 1977年，Israeli 和 Wood, 2002] ，也可以视为其有界理性版本。具有完全理性对手的最短路径阻断问题及其他网络阻断问题通常都是 NP-困难的，并且与双层优化 [Dempe 等, 2015] 以及鲁棒优化 [Ben-Tal 和 Nemirovski, 2002]领域有着密切联系。关于全面综述，请参阅 [Smith 和 Song, 2020]。如前所述，现有的网络阻断模型考虑的是完全理性对手 [Smith 等, 2009年，Smith 和 Song, 2020]。另一方面，我们探索采用动态离散选择框架对有界理性对手进行建模，这使防御者面临的难题变得更具挑战性，因为其中涉及复杂的非线性优化。此外，还有其他一些变体模型：问题数据对博弈参与者而言并非完全已知 [Cormican 等, 1998], ；博弈参与者反复交替采取行动 [Sefair 和 Smith, 2016], ；或者涉及在线学习[Borrero 等, 2016]。这些模型为未来研究提供了很有前景的方向。

网络安全博弈及其他。我们的工作也与针对分位响应对手的静态斯塔克尔伯格安全博弈模型有关 [Černỳ等人，2021年，Haghtalab等人，2016年，Mai和Sinha，2022年，Milec等人，2020年，Yang等人, 2011, 2012]。在名为网络安全博弈的动态模型中 [Jain等人, 2011], 其设定与我们的工作不同：在该研究中，理性对手旨在到达一个目标后停止，而在我们的工作中，有限理性对手可以攻击多个目标。沿着这一方向的其他相关工作仅考虑零和网络安全博弈设定；它们尝试运用博弈论或机器学习技术开发可扩展的博弈论算法 [Xue等人, 2022, 2021]。另有研究探讨了网络安全博弈中的分位响应类型松弛方法，其重点是智能预测与优化 [Wang等人, 2020], 然而，优化部分采用标准非线性求解器（如序列二次规划）完成，且不提供任何保证。

此外，还有其他与我们工作相关的博弈模型，其共同点是博弈参与者在基于图的环境中行动，包括追逃博弈和安全巡逻博弈 [Basilico 等人，2017年，2009年，Zhang 等人, 2019]。然而，这些现有研究并未考虑攻击者的

有限理性。这些研究中的策略空间也具有不同的特征，其中将实时信息或警报信号等纳入博弈参与者策略的定义。

3 问题表述

我们的网络阻断问题是一个具有单个对手的主从博弈。该博弈在一个网络（图）上进行。我们将该问题表述为一个双参与者网络阻断博弈，其中节点集合记为 S。跟随者（对手）沿该网络选择一条路径，该路径从如下所述的分布中采样得到。设 L 为关键节点集合（即网络中节点的子集），防御者可以对这些节点进行干预或修改。从领导者（防御者）的角度来看，目标是向节点 $s \in \mathrm{L}$ 分配 M 资源；每一种这样的分配都是防御者的一种纯策略。此外，节点和资源具有不同的种类，因此某一种类的节点只能由同一种类的资源进行保护。设有 K 种节点及其对应的资源。设每一种资源的数量 k为 M_k，因此 $\sum_{k\in[K]} M_k = M$。此外，设 $\{\mathrm{L}_k\}_{k\in[K]}$为节点集合 L 按节点种类划分得到的一个划分。

混合策略是一种随机分配，其结果是以边际概率 x_s 覆盖节点 s（使用 $\mathbf{x} = \{x_s,\ s \in \mathrm{L}\}$），并满足以下限制：$\sum_{s\in\mathcal{L}_k} x_s \le M_k$ 对于所有 $k \in [K]$，进而影响对手的路径选择概率。给定一个节点 $s \in \mathrm{S}$，如果对手经过该节点，则防御者将获得节点特定奖励 $r^l(s, x_s)$。防御者遵循阻断策略 $\mathbf{x}$ 时的期望奖励可计算如下：

$$\mathcal{F}^l(\mathbf{x}) = \sum_{s\in\mathcal{L}} r^l(s, x_s) P_s^f(\mathbf{x}),$$

其中 $P_s^f(\mathbf{x})$ 是跟随者（对手）穿过节点 s的概率，计算如下：

$$P_s^f(\mathbf{x}) = \sum_{\tau\in\Omega, \tau\ni s} \prod_{(s_t, s_{t+1})\in\tau} \pi^f(s_{t+1}|s_t, \mathbf{x}),$$

其中，Ω 是所有可能路径的集合，$\pi^f(s_{t+1}|s_t, \mathbf{x})$ 是对手的随机路径选择策略。请注意，对手行动时，防御者的阻断行动 $\mathbf{x}$ 是固定的，且对手知晓该行动。$P_s^f(\mathbf{x})$ 的方程本质上是对手实际沿着每条经过节点 $s(\tau \ni s)$ 的轨迹 τ移动的概率之和。因此，对手的策略具有马尔可夫性质。寻找最优防御者阻断策略的优化问题可表述如下：

$$\begin{aligned} \max_{\mathbf{x}} \quad & \mathcal{F}^l(\mathbf{x}) = \sum_{s\in\mathcal{L}} r^l(s, x_s) P_s^f(\mathbf{x}) \qquad \text{(OPT)} \\ \text{subject to} \quad & \sum_{s\in\mathcal{L}_k} x_s \le M_k,\ \forall k \in [K] \text{ and } x_s \in [L^x, U^x],\ \forall s \in \mathcal{L}, \end{aligned}$$

通常是非凸的。在此，$[L^x, U^x]$分别表示关键集 L 中每个节点的覆盖概率所需的下界和上界。

网络阻断博弈中的有限理性对手行为。我们使用动态离散选择框架（具体而言，使用基于Logit的递归路径选择模型 [Fosgerau等人， 2013]）来建模对手的有限理性行为。形式化地说，考虑一个网络 (S, A)，其中 S 是节点集合 $\mathrm{S} = \{1, 2, \ldots, |\mathrm{S}|\}$，A 是弧集合。此外，令 v 为对手的效用矩阵，即每个 $v(s; \mathrm{x})$ 表示在领导者策略 x 给定时，访问节点 $s \in \mathrm{S}$ 的即时效用。起点 $s_o \in \mathrm{S}$ 是给定的起始节点。在我们的问题中，我们还假设存在一个汇点（或目的地）节点 $s_d \in \mathrm{S}$，对手将

最终到达该节点。它可以是网络中的一个实际节点，也可以是代表对手最终状态的虚拟节点。

在基于 Logit 的动态离散选择框架（或动态量化响应）下，我们假设对手以有限理性的方式作出响应。设 $U(\tau|s_0、\mathbf{x}) = \sum_{s\in\tau} v(s;\mathbf{x})$ 表示从 s_0开始时的确定性长期效用；如果 $s_0 = s_o$，则简单记作 $U(\tau|\mathbf{x})$。在这一设定下，一个已知性质是：有限理性的对手所选择的策略等价于在所有可能路径上采用静态多项 Logit（MNL）离散选择模型（或 Logit 量化响应模型） [Fosgerau等人， 2013]。更确切地说，给定 $\mathbf{x}$，对手沿着路径 τ 行进的概率可计算如下 [Fosgerau等人， 2013]:

$$P(\tau) = \frac{\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{Z}, \text{ where } Z = \sum_{\tau\in\Omega} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right), \tag{1}$$

其中 Ω 是所有可能路径的集合， μ 是控制跟随者理性程度的参数。因此，我们可以将基于 Logit 的动态离散选择公式视为从源点 s_o 到目的地 s_d的最短加权路径问题的软版本。根据对手行为模型，可以如下计算对手的期望效用：

$$\mathcal{E}^f(\mathbf{x}) = \sum_{\tau\in\Omega} P(\tau)U(\tau;\mathbf{x})$$

这是对所有路径取期望。我们给出以下命题，说明当 μ趋近于零时，对手的期望效用趋近于累积效用的最大值（即最小路径权重）（为简洁起见，我们省略固定的$\mathbf{x}$ ）。

命题 1. 令 $\tau^* = argmax_{\tau\in\Omega} U(\tau)$ （即能够使对手效用最高的最优路径），并令 $L^* = \max_\tau |U(\tau)|$。此外，令 $\Omega^* = \{\tau;\ U(\tau) = U(\tau^*)\}$ （即效用相同且最高的所有路径的集合），并令 $\alpha = U(\tau^*) - \max_{\tau\in\Omega\setminus\Omega^*} U(\tau)$ （即对手选择次优路径而非最优路径时所承受的效用损失）。那么可得：

$$|\mathcal{E}^f - U(\tau^*)| \le \frac{L^* + 1}{1 + \frac{|\Omega^*|}{|\Omega\setminus\Omega^*|}\exp\left(\frac{\alpha}{\mu}\right)}.$$

因此，$\lim_{\mu\to 0} \mathcal{E}^f = U(\tau^*)$.[1]

根据上述命题， $\mu = 0$ 会导出一个效用最大化的（理性）对手。我们的定理 2 表明，对于理性 OPT而言，这是 NP-困难的，因此本文其余部分将着重讨论近似方法（并给出有界的解保证）。

定理 2。 防御者阻断问题 (OPT) 是 *NP*-困难的，适用于 $\mu = 0$。

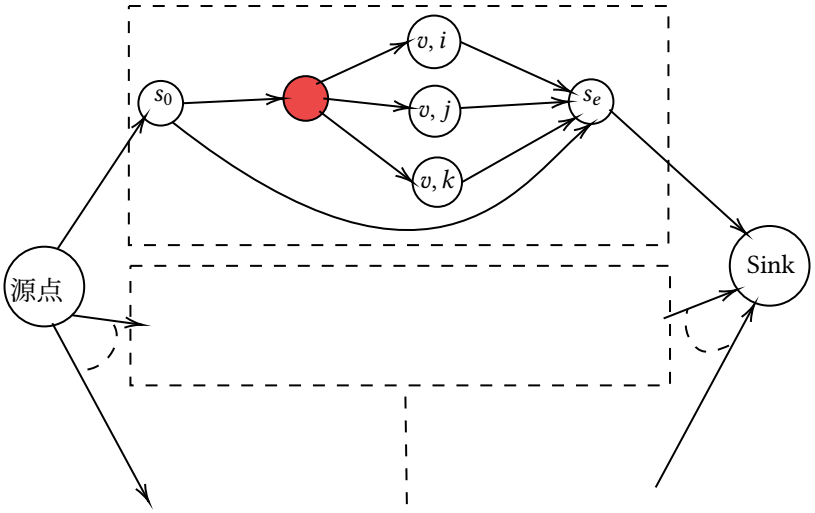
证明。我们将其归约为精确 3-覆盖问题：给定 m 个元素 {1、……、 m}，以及由 n 个子集组成的集合 {S_1、……、 S_n}，其中 $S_v \subset$ {1、……、 m}，每个子集的大小均为 3，即 $|S_v| = 3$ 对于 $v \in$ {1、……、 n}，判定问题是是否存在一个使每个元素恰好出现一次的覆盖。这是一个已知的 NP-困难问题。此外，显然任何有效的覆盖都必须包含 $m/3$ 个子集。

给定 *3*-覆盖问题的博弈实例构造。给定一个精确 3-覆盖问题，我们按如下方式构造网络安全博弈的实例：关键节点可以属于 $m + 1$ 种类型，其中前 m种类型标记为 1、……、 m，最后一种类型标记为红色。此外，共有 $n - m/3 + m$ 个防御者资源。在这些资源中， $n - m/3$ 个资源记为

[1]所有未在正文中给出的证明均包含在附录中。

by R_1、……、$R_{n-m/3}$，可以防御红色类型的节点（我们称这些为红色资源）。剩余的 m个资源记为 r_1、……、r_m，其中资源 r_j可以防御类型为 j的节点。

我们构造 n个子图——每个子图都对应于下图所示的一个子集 $S_v = \{i, j, k\}$。S_v对应的子图包含一个红色关键节点，以及三个分别标记为（v, i），（v, j），（v, k）的关键节点，其类型分别为 i, j, k。子图中有一个起始非关键节点 s_0和一个末尾非关键节点 s_e。此外，s_0与 s_e之间还有一条直接相连的边，称为虚拟边。我们可以通过创建一个源节点，并将该源节点连接到每个子图中的所有 s_0，再创建一个汇点，并将每个子图中的所有 s_e连接到该汇点，从而将所有 n个子图连接起来（如下图所示）。



对于任意节点，p表示防御者保护该节点的概率。我们将对手针对关键节点的收益设为 $u_a(p) = -50p + 50(1-p) - Kp\log p = 50 - 100p - Kp\log p$，其中常数 $K = {}^{100}\log\left({}^{n-m}/_{n-m^{3+1}/3+0.5}\right) > 0$。攻击者跳过所有关键节点的收益通过每个子图中的底部边为 0。另一方面，当对手访问关键节点时，防御者收益设为 $u_d(p) = -100(1-p) - \epsilon$，其中 $\epsilon > 0$为某个较小值。因此，只要攻击者经过任何关键节点，防御者收益就始终严格为负。当对手没有访问任何关键节点时，防御者收益为 0。这意味着，防御者的任何最优策略所能带来的最大收益都至多为 0。

问题归约。我们声称，当且仅当存在一个精确3覆盖时，相应网络阻断博弈中防御者的最优期望收益为 0。

首先，假设存在一个精确3覆盖，接下来我们证明，以下策略可使防御者的收益为 0：（i）防御者将 $n - m/3$ 个红色资源 R_1、……、$R_{n-m/3}$ 分配给对应于非覆盖子集的 $n-m/3$ 个子图中的红色节点；（ii）对于对应于覆盖中子集的 $m/3$ 个子图，防御者将 m 个资源 r_1、……、r_m 分配给每个子图中的三个节点。这保证了在每个子图 S_v中，红色节点或三个节点（v，i）、（v，j）、（v，k）会受到完全保护。给定防御者的这一策略，我们注意到，任意非虚拟路径上恰有两个关键节点：其中一个节点以概率 1 受到防御者保护，另一个关键节点受保护的概率为 0。因此，如果对手选择这条路径，对手从这两个节点获得的总期望收益将等于 $-50 + 50 = 0$（因为当 p 为 0 或 1 时，$p\log p = 0$）。按照 Leitmann 的做法，在平局时优先考虑防御者 [， 1978], 对手将选择一条底部虚拟边，

因此防御者的期望收益为零。正如我们之前所讨论的，防御者能够获得的最大收益至多为 0。因此，上述策略是防御者的最优策略，可使防御者获得最大收益 0。

接下来，假设防御者获得的最优期望收益为 0，且均衡策略是一个针对每个关键节点的概率值向量 $\mathbf{p}^*$。由于期望收益为 0，对手必然选择了一条底部边。让我们分析一条经过关键节点的路径：该路径在红色节点上的取值为 $p^*_{v,r}$，在另一种类型为 i的节点上的取值为 $p^*_{v,i}$。对手选择该路径时的收益为 $100 - 100(p^*_{v,r} + p^*_{v,i}) - Kp^*_{v,r}\log p^*_{v,r} - Kp^*_{v,i}\log p^*_{v,i}$。由于对手选择的是底部边，对手在该路径上的收益必须为 ≤ 0。或者，通过移项并除以 100，

$$p^*_{v,r}(1 + (K/100)\log p^*_{v,r}) + p^*_{v,i}(1 + (K/100)\log p^*_{v,i}) \geq 1 \tag{2}$$

根据式 2，我们将证明，红色节点恰好在$m/3$个子图中未被覆盖（即，$p^*_{v,r} = 0$）。首先，由于我们有 $n - m/3$ 个防御者资源可以覆盖红色节点，而总共有 n 个红色节点（即，每个 n 子图中有一个红色节点），因此未被覆盖的红色节点数量（即，$p^*_{v,r} = 0$）为 $\leq m/3$。此外，我们将通过反证法证明，对于 $< m/3$个子图，$p^*_{v,r} = 0$ 的另一种情况不可能发生。为进行反证，假设$p^*_{v,r} = 0$ 在 $< m/3$个子图中，或者换言之，$p^*_{v,r} > 0$ 在 $\geq n - m/3 + 1$ 个图中。下文将证明，这一假设会导致矛盾，因此该假设不成立。

我们注意到 $p^*_{v,\,i}$（$1 +$（$K/100$） 对数 $p^*_{v,\,i}$） ≤ 1。因此，根据式 2，可得：

$$p^*_{v,r}(1 + (K/100)\log p^*_r) \geq 0 \tag{3}$$

设 $P \subset \{1, \ldots\ldots, n\}$ 为满足 $p^*_{v,\,r} > 0$ 对于 $v \in P$ 的子集（根据我们的假设 $|P| \geq n - m/3 + 1$）。对于任意这样的 $p^*_{v,\,r} > 0$ 满足 $v \in P$，根据式 3，必有 $1 + (K/100)\log p^*_{v,\,r} \geq 0$，整理后得到 $p^*_{v,\,r} \geq \exp(-100/K)$。对所有 $v \in P$ 求和，可得

$$\sum_{v \in P} p^*_{v,r} \geq |P| \exp(-100/K)$$

上式左侧为 $\sum_{v \in P} p^*_{v,\,r} \leq n - m/3$（因为 $p^*_{v,\,r} = 0$ 对于 $v \notin P$，且只有 $n - m/3$ 个红色资源）。令 $K = \frac{100}{\log\left(\frac{n-m}{n-m}^{3+1}/3+0.5\right)}$，并利用 $|P| \geq n - m/3 + 1$ 这一事实，可得右侧为 $\geq n - m/3 + 0.5$。这就产生了矛盾。因此，假设对于 $< m/3$ 个子图，$p^*_{v,\,r} = 0$ 不成立。

因此，红色节点恰好在 $m/3$ 个子图中未被覆盖（即 $p^*_{v,\,r} = 0$）。我们注意到，如果$p^*_{v,\,r} = 0$，那么为了满足式 2，$p^*_{v,\,i} = 1$。对于同一子图 $S_v = \{i, j, k\}$ 中的其他非虚拟路径，依照相同的推理，如果 $p^*_{v,\,r} = 0$，那么 $p^*_{v,\,i} = p^*_{v,\,j} = p^*_{v,\,k} = 1$。请记住，$m$ 个（非红色）防御者资源中的每个防御者资源 r_j 只能保护一个 j 类型的节点。这意味着这些 $m/3$ 个子图中的 m 个非红色节点属于不同类型。因此，我们得到了原始 3-覆盖问题的一个满足条件的覆盖——该覆盖中的每个子集都包含三个元素，分别对应于上述 $m/3$ 个子图之一中的三个非红色节点。□

4 基于梯度的二分搜索算法

总体而言，如（OPT）中所表述的为防御者寻找最优阻断策略的问题在计算上颇具挑战性，因为（OPT）中的目标函数不仅涉及网络中指数数量的路径，而且还是非凸的。我们首先提出一种新的基于梯度的二分搜索算法，以高效求解（OPT）。我们的算法包含三个关键步骤：（i）我们使用二分搜索将原始分式（OPT）化简为一个更简单的非分式问题；（ii）我们通过构建动态规划，给出目标函数一种非平凡的紧凑表示，以处理原始目标函数表述中涉及的指数数量的路径；（iii）我们采用基于梯度上升的方法，高效求解该

由此得到的紧凑优化问题。需要注意的是，由于我们的问题是非凸的，我们基于梯度的方法无法保证获得全局最优解。因此，我们将在第OPT节中为（5）提出新的有保证的近似解。

本质上，我们将（OPT）的目标函数重写如下：

$$\mathcal{F}^l(\mathbf{x}) = \sum_{s\in\mathcal{L}} r^l(s,x_s)P_s^f(\mathbf{x}) = \sum_{s\in\mathcal{L}}\sum_{\substack{\tau\in\Omega\\ \tau\ni s}} r^l(s,x_s)P(\tau) = \frac{\sum_{s\in\mathcal{L}}\sum_{\tau\ni s} r^l(s,x_s)\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau'\in\Omega}\exp\left(\frac{U(\tau';\mathbf{x})}{\mu}\right)}. \quad (4)$$

$\mathcal{F}^l$（$\mathbf{x}$）具有分式非凸形式。简化这种结构的一种典型方法是使用 Dinkelbach变换和二分搜索算法 [Dinkelbach, 1967] 将原问题转化为一系列更简单的问题。我们使用二分搜索将（OPT）等价地表示为：

$$\max_{\delta}\left\{\delta \,\middle|\, \exists\mathbf{x}\ \text{s.t.}\ \mathcal{F}^l(\mathbf{x}) \geq \delta\right\} \Leftrightarrow \max_{\delta}\left\{\delta \,\middle|\, \max_{\mathbf{x}}\{g(\mathbf{x},\delta)\} \geq 0\right\},$$

其中，所得目标函数为：

$$g(\mathbf{x},\delta) = \sum_{s\in\mathcal{L}}\sum_{\substack{\tau\in\Omega\\ \tau\ni s}} r^l(s,x_s)\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) - \delta\left(\sum_{\tau'\in\Omega}\exp\left(\frac{U(\tau';\mathbf{x})}{\mu}\right)\right) \quad (5)$$

总体而言，g（$\mathbf{x}$ δ）仍然是非凸的，但不再是分式形式。由于 g（$\mathbf{x}$ δ）可微，因此可以通过基于梯度的方法求解该最大化问题的局部最大值。其中一个关键挑战是计算 g（$\mathbf{x}$ δ）；如果采用朴素方法，则需要枚举 Ω 上指数数量的路径。下面我们将展示，g（$\mathbf{x}$ δ）具有紧凑形式，因此可以通过动态规划高效地计算 g（$\mathbf{x}$ δ）及其梯度。

4.1 紧凑表示：处理指数数量的路径

为了对 g（$\mathbf{x}$ δ）进行紧凑表示，我们引入以下新术语：

$$Z_s = \sum_{\tau\in\Omega^{s_d}(s)}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right),\ \forall s\in\mathcal{S}, \qquad Y_{s'}^{s} = \sum_{\tau\in\Omega(s',s)}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)$$

其中，Ω^{s_d}（s）是从 s到目的地 s_d的所有路径的集合，而 Ω（s'，s）是对于任意 s，$s'\in$S，从 s'到 s的所有路径的集合。

给定这些新术语，目标函数 g（$\mathbf{x}$ δ）可以重新表述如下：

$$g(\mathbf{x},\delta) = \sum\nolimits_{s\in\mathcal{L}} r^l(s,x_s)Y_{s_o}^{s}Z_s - \delta Z_{s_o}, \quad (6)$$

其中，s_o是起点，而 Ω（s_o，s）是从 s_o到 s的所有路径的集合。

尽管这些新术语在 Ω^{s_d}（s）和 Ω（s'，s）中，对于所有s，s'仍然涉及指数数量的路径，但我们证明，可以通过动态规划高效地计算这些术语。本质上，Z_s、$\forall s\in$S，可以递归计算如下：

$$Z_s = \begin{cases}\sum_{s'\in N(s)}\exp\left(\frac{v(s;\mathbf{x})}{\mu}\right)Z_{s'} & \text{if } s\neq s_d\\ 1 & \text{if } s = s_d,\end{cases}$$

其中，$N(s)$ $=\{s'\in$S$|(s,$ $s')$ $\in$A$\}$ 表示从节点 $s\in$S 出发通过一跳可以到达的所有可能后续节点的集合。设 $\mathbf{M}$为一个大小为 $|$S$|\times|$S$|$的矩阵，其元素对于所有$s\in$S $s'\in N(s)$均为 $M_{ss'} = \exp\left(\frac{v(s|}{\mu}\right)\mathbf{x})$，则 $\mathbf{Z}$ $=\{Z_s,$ $s\in$S$\}$ 是以下线性系统 $\mathbf{Z}$ $=\mathbf{M}\mathbf{Z}$ $+\mathbf{b}$ 的一个解，其中 $\mathbf{b}$ 是一个大小为 $|$S$|$ 的向量，除 b_{s_d} = 1外其余元素均为零。

此外，$\mathbf{Y}^s = \{Y^s_{s'}\}_{s'}$ 也可以递归定义如下：

$$Y^s_{s'} = \begin{cases} \sum_{s'' \in N(s')} \left(\exp\left(\frac{v(s';\mathbf{x})}{\mu} \right) \right) Y_{s''} & \text{if } s' \neq s \\ 1 & \text{if } s' = s. \end{cases}$$

类似于上述针对$\mathbf{Z}$的技术，可以看出$\mathbf{Y}^s$是线性系统$\mathbf{Y}^s = \mathbf{M}\mathbf{Y}^s + \mathbf{b}^s$的一个解，其中$\mathbf{b}^s$的大小为 $|\mathbb{S}|$，除 $b^s_s = 1$外，其余位置均为零。

由于 Y^s和 Z 分别是线性系统 $\mathrm{Y}^s = \mathrm{M}\mathrm{Y}^s + \mathrm{b}^s$和 $\mathrm{Z} = \mathrm{M}\mathrm{Z} + \mathrm{b}$ 的解，$\forall s \in \mathrm{S}$，因此可以通过求解 $|\mathrm{L}| + 1$ 个线性方程组来计算目标函数 $g(\mathrm{x}\ \delta)$。最后可以看出，上述所有线性系统都依赖于公共矩阵 M。我们可以将它们合并为一个线性系统。设 H 为一个大小为 $(|\mathrm{S}|) \times (|\mathrm{L}| + 1)$ 的矩阵，其中第 1 列至第 $|\mathrm{L}|$列是向量 $\mathrm{Y}^s, s \in \mathrm{L}$，最后一列是 Z。设 B 为一个大小为 $(|\mathrm{S}|) \times (|\mathrm{L}| + 1)$ 的矩阵，其中第 1 列至第 $|\mathrm{L}|$列是向量 $\mathrm{b}^s, s \in \mathrm{L}$，最后一列是 b。可以看出，H 是线性系统 $(\mathrm{I} - \mathrm{M})\mathrm{H} = \mathrm{B}$ 的一个解。因此，通常只需求解一个线性系统，即可得到所有 Y^s 和 Z。当 L 的规模增大时，这种方法应当仍具可扩展性。

4.2 基于梯度的优化

如前所述，我们旨在采用基于梯度的方法求解以下优化问题（这是对原问题应用二分搜索后得到的结果（OPT）：

$$\max_{\mathbf{x}} \{g(\mathbf{x}, \delta)\}$$

为此，关键是计算梯度 $\left\{ \frac{\partial g(\mathbf{x},\delta)}{\partial x_s} \right\}$。根据公式 6，计算该梯度需要对矩阵 $\mathbf{Z}$ 和 $\{\mathbf{Y}^s\}$（或等价地，对矩阵 $\mathbf{H}$）进行求导。我们首先给出命题3：

命题 3。 如果网络无环，那么 $(\boldsymbol{I} - \boldsymbol{M})$ 可逆。

命题 3 表明 $(\mathbf{I} - \mathbf{M})$ 可逆，因此我们可以计算矩阵 $\mathbf{H}$：

$$\mathbf{H} = (\mathbf{I} - \mathbf{M})^{-1}\mathbf{B}.$$

分别对两边关于 x_j、 $j \in \mathrm{L}$ 求导，可得：

$$\mathbf{J}^{\mathbf{H},j} = (\mathbf{I} - \mathbf{M})^{-1}\mathbf{J}^{\mathbf{M},j}(\mathbf{I} - \mathbf{M})^{-1}\mathbf{B} = (\mathbf{I} - \mathbf{M})^{-1}\mathbf{J}^{\mathbf{M},j}\mathbf{H},\ \forall j \in \mathcal{L},$$

其中，$\mathrm{J}^{\mathbf{H},j}$和$\mathrm{J}^{\mathbf{M},j}$是H和M关于$x_j$的梯度矩阵，即$\mathrm{J}^{\mathbf{H},j}$是一个尺寸为$|\mathbb{S}| \times (|\mathbb{L}| + 1)$的矩阵，其元素为$\mathrm{J}^{\mathbf{H},j}_{ss'} = \partial H_{ss'}, / \partial x_j$；$\mathrm{J}^{\mathbf{M},j}$是一个尺寸为$(|\mathbb{S}| \times |\mathbb{S}|)$的矩阵，其元素为$\mathrm{J}^{\mathbf{M},j}_{ss'} = \partial M_{ss'}, / \partial x_j$，适用于任意 $j \in \mathrm{L}$。设$\mathrm{R}^l(\mathbf{x})$是一个尺寸为 $1 \times |\mathbb{L}|$的矩阵，其元素为 $r^l(s, x_s)$，适用于 $s \in \mathrm{L}$。我们用$A_{S,T}$表示 A的一个子矩阵，该子矩阵取自集合 S 中的行和集合 T中的列。如果 S或T是单元素集合，例如 $S = \{s_o\}$或 $T = |\mathbb{L}| + 1$，则将其写作 s_o或 $|\mathbb{L}| + 1$。

因此，我们现在可以按如下方式计算所需的梯度：

$$\begin{aligned} \frac{\partial g(\mathbf{x}, \delta)}{\partial x_s} &= (\mathbf{R}^l(\mathbf{x}) \circ \mathbf{J}^{\mathbf{H},s}_{s_o,\mathcal{L}} + \mathbf{J}^{R,s} \circ \mathbf{H}_{s_o,\mathcal{L}}) \times \mathbf{H}_{\mathcal{L},|\mathcal{L}|+1} \\ &\quad + (\mathbf{R}^l(\mathbf{x}) \circ \mathbf{H}_{s_o,\mathcal{L}}) \times \mathbf{J}^{\mathbf{H},j}_{\mathcal{L},|\mathcal{L}|+1} - \delta \mathbf{J}^{\mathbf{H}}_{s_o,|\mathcal{L}|+1}, \forall s \in \mathcal{L} \end{aligned} \tag{7}$$

其中 $\circ$ 表示注：Hadamard乘积。我们总结了优化 $g(\mathbf{x}\ \delta)$ 的主要步骤，见算法 1 .

备注1。 上述基于梯度的方法只能保证得到局部最优解。其复杂度由矩阵求逆或求解线性方程组决定；在最坏情况下，该复杂度为 $O(|\mathcal{S}|^3)$。梯度下降循环运行 $O(1/\epsilon)$ 次，以提供加性 ϵ近似。因此，总复杂度为 $O((1/\epsilon)\ |\mathcal{S}||\mathcal{A}|)$。在实践中，可以使用自动微分技术求得梯度，相比直接使用 $\boldsymbol{J}^{\boldsymbol{H},\ j}$ 的公式，速度会显著提升。

算法 1： 最大化 $g(\boldsymbol{x}\ \delta)$

当 未收敛时**执行**
  给定$\mathbf{x}$，求解系统$\mathbf{H} = (\mathbf{I} - \mathbf{M})^{-1}\mathbf{B}$ 和$\mathbf{J}_H{}^j = (\mathbf{I} - \mathbf{M})^{-1}\mathbf{J}_M{}^j\mathbf{H}$，对所有 j
  计算 $g(\mathbf{x}\ \delta)$ 和 $\frac{\partial g(\mathbf{x}\ \delta)}{\partial x_s}$ 使用式6、7。
  使用投影梯度法更新$\mathbf{x}$
end

5 有保证的近似解

如前文所述，尽管我们可以处理指数数量的路径，但由于（OPT）的非凸性，我们的基于梯度的方法无法保证找到全局最优解。在本节中，我们基于算法1提出能够提供近似保证的结果。对于这种近似，我们需要对效用函数作出假设，即效用具有线性形式：$v(s; \mathbf{x}) = w_s^f x_s + t_s^f$和 $r^l(s; \mathbf{x}) = r^l(s, x_s) = w_s^l x_s + t_s^l$，其中 w_s^f、 t_s^f、 w_s^l、 t_s^l为某些常数。我们还假设 $w_s^f < 0$和 $w_s^l > 0$，即在节点 s投入更多资源 x_s会降低对手的效用，并为防御者提供更多奖励。这种设置对于安全场景而言十分直观，见 Mai 和 Sinha，2022年，Yang等人， 2012]。

下面我们首先介绍一个受限阻断问题，该问题可以使用我们高效的基于梯度下降的方法，以最优且易处理的方式求解。然后，我们给出关于其解与原问题之间联系的重要理论结果。进一步地，我们通过二分搜索方法证明，受限阻断问题可以在保证解界的情况下以高得多的效率求解。

受限阻断问题。 令 $\Delta(s)$ 表示穿过 s 且不穿过 L 中任何其他节点的路径集合。我们考虑以下受限阻断问题：

$$\max_{\mathbf{x}} \widetilde{\mathcal{F}}(\mathbf{x}) = \frac{\sum_{s\in\mathcal{L}} \sum_{\tau\in\Delta(s)} r^l(s, x_s) \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{s\in\mathcal{L}} \sum_{\tau\in\Delta(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)} \qquad \text{(Approx-OPT)}$$

$$\text{subject to } \sum\nolimits_{s\in\mathcal{L}_k} x_s \le M_k,\ \forall k \in [K],\ \text{and } x_s \in [L^x, U^x],\ \forall s \in \mathcal{L}.$$

直观而言，在（Approx-OPT）中，对手的路径选择被限制在网络中的一个路径子空间内，这些路径仅穿过 L 中的一个关键节点。我们将 $\mathrm{X} = \{\mathbf{x} \in \mathbb{R}^{|\mathcal{L}|} |\ \sum_{s\in\mathcal{L}_k} x_s \le M_k,\ \forall k \in [K],\ x_s \in [L^x, U^x],\ \forall s \in \mathrm{L}\}$ 记为防御者阻断策略$\mathbf{x}$的可行集。

5.1 与原问题的解的关系 (OPT)

给定受限问题（Approx-OPT），我们现在从理论上分析其与我们原问题（OPT）的解的关系，即为防御者寻找最优阻断策略的问题。

5.1.1 **主要结果。** 给定一个关键节点 $s \in \mathrm{L}$，令 $\Delta^+(s)$表示经过 s 以及 L 中至少另一个关键节点的路径集合。令 β_1、 $\beta_2 > 0$满足：

$$\begin{aligned}
\beta_1 &= \max_{\mathbf{x}} \max_{s\in\mathcal{L}} \left\{ \frac{\sum_{\tau\in\Delta^+(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau\in\Delta(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)} \right\} \\
\beta_2 &= \max_{\mathbf{x}} \left\{ \frac{\sum_{\tau\in\bigcup_s\{\Delta^+(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau\in\bigcup_s\{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)} \right\},
\end{aligned} \tag{8}$$

直观地说，当对手的路径选择被限制在 Approx-OPT 中所述的受限路径空间内时， β_1 和 β_2 刻画了对手行为的最大变化。若 L 中任意两个关键节点之间的通行成本较高，则预计 β_1 和 β_2 的值较小。也就是说，对于任意 s、 $s' \in$ L，若$\sum_{\tau\in\Omega}(s$、 $s')$ exp $\left(\frac{U(\tau}{\mu}\right) \to 0$;x)，则$\beta_1$、 $\beta_2 \to 0$，其中 $\Omega(s$、 $s')$表示从 s到 s'的所有路径的集合。我们的主要理论结果见定理 4 和定理 5。

定理4。 令$\boldsymbol{x}^*$为(Approx-OPT)的最优解：$\max_{\boldsymbol{x}\in\mathcal{X}} \widetilde{\mathcal{F}}(\boldsymbol{x})$以及 $\kappa = \max_{\boldsymbol{x}\in\mathcal{X}} \sum_{s\in\mathcal{L}} |r^l(s, x_s)|$ 防御者在关键节点处可能获得的最大绝对奖励，我们有：

$$\mathcal{F}^l(\boldsymbol{x}^*) \geq \frac{\max_{\boldsymbol{x}\in\mathcal{X}}\{\mathcal{F}^l(\boldsymbol{x})\}}{(1+\beta_1)(1+\beta_2)} - \kappa\frac{\beta_1+\beta_2+\beta_1\beta_2}{(1+\beta_1)(1+\beta_2)}.$$

注意， $\max_{\mathbf{x}\in\mathcal{X}}\{\mathcal{F}^l(\mathbf{x})\}$是用于寻找最优阻断策略的原始（OPT）。如前所述，当任意两个关键节点之间的旅行成本较高时， β_1 和 β_2 趋近于零，这意味着定理4 中的不等式右侧将达到（OPT）的最优解。

现在，如果我们只能近似求解（Approx-OPT），我们仍然可以估计原始（OPT）的近似界，如定理5所示。

定理 ~第 5 节。 给定 $\epsilon > 0$，令 $\boldsymbol{x}^*$ 为满足以下条件的解：$\mathcal{F}(\boldsymbol{x}^*) \geq (1-\epsilon)\max_{\boldsymbol{x}}\mathcal{F}(\boldsymbol{x})$，我们有：

$$\mathcal{F}^l(\boldsymbol{x}^*) \geq \frac{(1-\epsilon)\max_{\boldsymbol{x}}\{\mathcal{F}^l(\boldsymbol{x})\}}{(1+\beta_1)(1+\beta_2)} - \kappa\frac{\epsilon+\beta_1+\beta_2+\beta_1\beta_2}{(1+\beta_1)(1+\beta_2)}.$$

~ ~此外，如果 $\boldsymbol{x}^*$ 是一个带有加性误差 $\epsilon > 0$ 的近似解，即 $\mathcal{F}(\boldsymbol{x}^*) \geq \max_{\boldsymbol{x}}$ $\mathcal{F}(\boldsymbol{x}) - \epsilon$，则可得到以下界：

$$\mathcal{F}^l(\boldsymbol{x}^*) \geq \frac{1}{\eta}\max_{\boldsymbol{x}}\{\mathcal{F}^l(\boldsymbol{x})\} - \kappa\frac{\eta-1}{\eta},$$

其中 $\eta = (1+\beta_1)(1+\beta_2)\left(1 + \frac{\epsilon}{\kappa + \min_{\mathbf{x}\in\mathcal{X}}}\right)$ F($\boldsymbol{x}$)。

5.1.2 证明概要。 这些定理的证明基于两个重要引理，具体如下所述。引理 1 仅适用于所有防御者奖励 $r^l(s, x_s)$ 均为非负的情况。然后，我们在引理 2 中处理一般情况。直观地说，这两个引理展示了：对于任意给定的防御者阻断策略 $\mathbf{x}$，原问题（OPT）与受限问题（Approx-OPT）之间，在防御者效用（即目标函数 $F^l(\mathbf{x})$ 和 $\widetilde{F}(\mathbf{x})$）方面的关系。

引理1. 若 $r^l(s, x_s) \geq 0$ 对于任意 $\boldsymbol{x} \in \mathcal{X}$成立，则对于任意 $\boldsymbol{x}$，

$$\frac{1}{1+\beta_2}\widetilde{\mathcal{F}}(\boldsymbol{x}) \leq \mathcal{F}^l(\boldsymbol{x}) \leq (1+\beta_1)\widetilde{F}(\boldsymbol{x}).$$

处理 $r^l(s, x_s)$ 可能取负值的情形更具挑战性。以下引理给出了这种情况下的一般不等式。

引理2. 若选择 $\kappa = \sum_{s\in\mathcal{L}}\max_{\boldsymbol{x}}\left|r^l(s, x_s)\right|$，则对于任意 $\boldsymbol{x} \in \mathcal{X}$，

$$\frac{1}{1+\beta_2}\left(\widetilde{\mathcal{F}}(\boldsymbol{x}) + \kappa\right) \leq \mathcal{F}^l(\boldsymbol{x}) + \kappa \leq (1+\beta_1)\left(\widetilde{\mathcal{F}}(\boldsymbol{x}) + \kappa\right).$$

定理4 和定理5 的证明可由上述引理直接得到 .

完成定理的证明4. 根据引理 2，我们得到：

$$\frac{1}{1+\beta_2}\max_{\mathbf{x}}\left(\widetilde{\mathcal{F}}(\mathbf{x}) + \kappa\right) \leq \max_{\mathbf{x}}\left(\mathcal{F}^l(\mathbf{x}) + \kappa\right) \leq (1+\beta_1)\max_{\mathbf{x}}\left(\widetilde{\mathcal{F}}(\mathbf{x}) + \kappa\right), \tag{9}$$

从而得到以下不等式链：

$$\frac{1}{1+\beta_2}\left(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa\right) \le \left(\mathcal{F}^l(\mathbf{x}^*)+\kappa\right) \le \max_{\mathbf{x}}(\mathcal{F}^l(\mathbf{x})+\kappa) \le (1+\beta_1)\left(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa\right).$$

其中，$\mathbf{x}^*$ 是 (Approx-OPT 的最优防御策略解。由于 $\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa$、$\mathcal{F}^l(\mathbf{x}^*)+\kappa$和 $\max_{\mathbf{x}}(\mathcal{F}^l(\mathbf{x})+\kappa)$ 均为正数，因此我们有：

$$\frac{\mathcal{F}^l(\mathbf{x}^*)+\kappa}{\max_{\mathbf{x}}(\mathcal{F}^l(\mathbf{x})+\kappa)} \ge \frac{\frac{1}{1+\beta_2}\left(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa\right)}{(1+\beta_1)\left(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa\right)} = \frac{1}{(1+\beta_1)(1+\beta_2)}$$

$$\text{which implies: } \mathcal{F}^l(\mathbf{x}^*)+\kappa \ge \frac{\max_{\mathbf{x}\in\mathcal{X}}\{\mathcal{F}^l(\mathbf{x})\}}{(1+\beta_1)(1+\beta_2)} + \frac{\kappa}{(1+\beta_1)(1+\beta_2)}$$

$$\text{or equivalently, } \mathcal{F}^l(\mathbf{x}^*) \ge \frac{\max_{\mathbf{x}\in\mathcal{X}}\{\mathcal{F}^l(\mathbf{x})\}}{(1+\beta_1)(1+\beta_2)} - \kappa\frac{\beta_1+\beta_2+\beta_1\beta_2}{(1+\beta_1)(1+\beta_2)}$$

由此得证。 □

$\widetilde{}$定理 5 的证明。若 $\mathbf{x}^*$ 是满足 $\mathcal{F}(\mathbf{x}^*) \ge \widetilde{}(1-\epsilon)\max_{\mathbf{x}}\mathcal{F}(\mathbf{x})$的阻断策略解，则利用 (9)，可得到以下不等式链：

$$\begin{aligned}\frac{1}{1+\beta_2}\left(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa\right) &\le \frac{1}{1+\beta_2}\max_{\mathbf{x}}\left(\widetilde{\mathcal{F}}(\mathbf{x})+\kappa\right) \le \max_{\mathbf{x}}\left(\mathcal{F}^l(\mathbf{x})+\kappa\right) \\ &\le (1+\beta_1)\max_{\mathbf{x}}\left(\widetilde{\mathcal{F}}(\mathbf{x})+\kappa\right) \le (1+\beta_1)\left(\frac{1}{1-\epsilon}\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa\right) \\ &\le \frac{1+\beta_1}{1-\epsilon}(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa)\end{aligned} \tag{10}$$

因此，

$$\begin{aligned}&\frac{1}{1+\beta_2}\left(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa\right) \le \mathcal{F}^l(\mathbf{x}^*)+\kappa \le \max_{\mathbf{x}}\left(\mathcal{F}^l(\mathbf{x})+\kappa\right) \le \frac{1+\beta_1}{1-\epsilon}(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa) \\ \implies &\frac{\mathcal{F}^l(\mathbf{x}^*)+\kappa}{\max_{\mathbf{x}}\{\mathcal{F}^l(\mathbf{x})+\kappa\}} \ge \frac{1-\epsilon}{(1+\beta_1)(1+\beta_2)},\end{aligned} \tag{11}$$

由此进一步得到：

$$\mathcal{F}^l(\mathbf{x}^*) \ge \frac{(1-\epsilon)\max_{\mathbf{x}}\{\mathcal{F}^l(\mathbf{x})\}}{(1+\beta_1)(1+\beta_2)} - \kappa\frac{\epsilon+\beta_1+\beta_2+\beta_1\beta_2}{(1+\beta_1)(1+\beta_2)},$$

如所需。

$\widetilde{}$对于加性误差 $\mathrm{F}(\mathbf{x}^*) \ge \max_{\mathbf{x}}\mathrm{F}(\mathbf{x}) - \epsilon$，类似地，我们可以写为：

$$\begin{aligned}\frac{1}{1+\beta_2}\left(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa\right) &\le \mathcal{F}^l(\mathbf{x}^*)+\kappa \le \max_{\mathbf{x}}\left(\mathcal{F}^l(\mathbf{x})+\kappa\right) \\ &\le (1+\beta_1)\max_{\mathbf{x}}\left(\widetilde{\mathcal{F}}(\mathbf{x})+\kappa\right) \le (1+\beta_1)\left(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\epsilon+\kappa\right),\end{aligned}$$

由此可得：

$$\begin{aligned}&\frac{\mathcal{F}^l(\mathbf{x}^*)+\kappa}{\max_{\mathbf{x}}\{\mathcal{F}^l(\mathbf{x})+\kappa\}} \ge \frac{1}{(1+\beta_1)(1+\beta_2)}\frac{1}{1+\epsilon/(\widetilde{\mathcal{F}}(\mathbf{x}^*)+\kappa)} \ge \frac{1}{\eta} \\ &\Rightarrow \mathcal{F}^l(\mathbf{x}^*) \ge \frac{1}{\eta}\max_{\mathbf{x}}\{\mathcal{F}^l(\mathbf{x})\} - \kappa\frac{\eta-1}{\eta},\end{aligned}$$

正如所期望的那样，由此完成了我们的证明。 □

5.2 求解限制性拦截问题 （Approx-OPT）

为了解决受限问题，我们还提出采用二分搜索方法。二分搜索每一步产生的子问题可表述如下：

$$\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x},\delta) = \sum_{s\in\mathcal{L}}\sum_{\tau\in\Delta(s)} r^l(s,x_s)\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) - \delta\left(\sum_{s\in\mathcal{L}}\sum_{\tau\in\Delta(s)}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)\right). \quad \text{(sub-Approx)}$$

本节其余部分将介绍我们关于（sub-Approx）所依赖的关键性质的理论结果，以及用于求解（sub-Approx）的新精确解和近似解。

5.2.1 （sub-Approx）的单峰性。 下面我们给出定理6，该定理表明，我们可以使用基于梯度的方法来获得（sub-Approx）的唯一全局最优解。

定理6。 （sub-Approx） 问题具有单峰性；也就是说，（***sub-Approx***）的任意局部最优解$\boldsymbol{x}^*$ （sub-Approx）也是全局最优的。

证明概要。证明可分为两个主要步骤：

步骤 1：证明 (sub-Approx) 可以转化为一个（严格）凸优化问题。这一步通过变量变换完成。回顾一下，对手效用 $v(s;\mathrm{x}) = v(s,x_s) = w^f x_s + t^f$，防御者效用 $r^l(s;\mathrm{x}) = r^l(s,x_s) = w^l x_s + t^l$，其中 $w^f < 0$ 且 $w_l > 0$。本质上，我们对所有关键节点 $s \in \mathrm{L}$ 引入一个新变量 $y_s = \exp\left(\frac{v(s,x_s)}{\mu}\right)$。我们将证明，(sub-Approx) 的目标函数 $\widetilde{g}(\mathrm{x}\ \delta)$ 可以改写为关于 $\{y_s\}$ 的严格凹函数。

对于每条轨迹 $\tau \in \Delta(s)$，令 $V^s(\tau) = \sum_{s'\in\tau,\, s'\neq s} v(s';\mathrm{x})$，或等价地，$V^s(\tau) = U(\tau;\mathrm{x}) - v(s;\mathrm{x})$，它表示轨迹 τ 上除节点 s 以外所有节点的累积对手效用。我们看到，$V^s(\tau)$ 与每个关键节点 $s \in \mathrm{L}$ 处的防御者覆盖概率 x_s 无关（根据 $\Delta(s)$ 的定义）。因此，我们可以将 (sub-Approx) 的目标函数 $\widetilde{g}(\mathrm{x}\ \delta)$ 重写如下：

$$\widetilde{g}(\mathbf{x},\delta) = \sum_{s\in\mathcal{L}} r^l(s,x_s)\exp\left(\frac{v(s;\mathbf{x})}{\mu}\right)H(s) - \delta\left(\sum_{s\in\mathcal{L}}\exp\left(\frac{v(s;\mathbf{x})}{\mu}\right)H(s)\right).$$

其中 $H(s) = \sum_{\tau\in\Delta(s)}\exp(V^s(\tau)/\mu)$。因此，我们可以将 $\widetilde{g}(\mathbf{x}\ \delta)$ 写成关于 $\mathbf{y}$ 的函数，如下所示：

$$\begin{aligned}\widetilde{g}(\mathbf{y},\delta) &= \sum_{s\in\mathcal{L}}\left(\left(\mu\log(y_s) - t^f\right)\frac{w^l}{w^f} + t^l\right)y_s H(s) - \delta\left(\sum_{s\in\mathcal{L}} y_s H(s)\right)\\ &= \sum_{s\in\mathcal{L}}\mu\frac{w^l}{w^f}H(s)\log(y_s)y_s - y_s H(s)\left(\mu\frac{t^f w^l}{w^f} + t^l + \delta\right). \end{aligned} \tag{12}$$

由于 $w^f/w^l \le 0$，可以证明每个分量 $\mu\frac{w^l}{w^f}H(s)\log(y_s)y_s$ 关于 y_s 都是凹函数，因此，对于所有关键节点 s，$\widetilde{g}(\mathbf{y}\ \delta)$ 关于 $\mathbf{y}$ 是严格凹函数。此外，对于任意 $k \in [K]$，约束 $\sum_{s\in\mathcal{L}_k} x_s \le M_k$ 变为 $\sum_{s\in\mathcal{L}_k}\frac{\mu\log(y_s) - t^f}{w^f} \le M_k$，由于 $w^f < 0$，该函数是凸函数。

步骤 ***2***：通过变量变换下的 ***KKT***条件对应关系证明全局最优性. 按照**步骤 1**中给出的变量变换，为方便表述，定义 $\widehat{x}_s(\cdot): \mathbb{R}\to\mathbb{R}$ 和 $\widehat{y}_s(\cdot): \mathbb{R}\to\mathbb{R}$，使得：

$$\widehat{y}_s(x_s) = \exp\left(\frac{v(s,x_s)}{\mu}\right)$$
$$\widehat{x}_s(y_s) = \frac{\mu\log(y_s) - t^f}{w^f},$$

即从$\mathbf{x}_s$到$\mathbf{y}_s$的映射，反之亦然。

回顾一下，防御者的可行策略空间为 $\mathcal{X} = \{\mathbf{x}: \ \sum_{s\in\mathcal{L}_k} x_s \le M_k, \ \forall k, \ x_s \in [L^x, U^x]\}$因此，我们可以将（sub-Approx）的拉格朗日对偶写成如下形式：

$$L^g(\mathbf{x}, \boldsymbol{\gamma}, \boldsymbol{\eta}^1, \boldsymbol{\eta}^2) = \widetilde{g}(\mathbf{x}, \delta) - \sum_k \gamma_k \left(\sum_{s\in\mathcal{L}_k} x_s - M_k \right) - \sum_s \eta_s^1 (x_s - U^x) + \sum_s \eta^2 (x_s - L^x).$$

由于$\mathbf{x}^*$是（sub-Approx）的局部最优解，KKT 条件表明存在对偶变量$\boldsymbol{\gamma}^*$、$\boldsymbol{\eta}^{1*}$、$\boldsymbol{\eta}^{1*} \ge 0$，使得以下约束得到满足：

$$\begin{cases} \frac{\widetilde{g}(\mathbf{x}^*,\delta)}{\partial x_s} - \gamma_k^* - \eta_s^{1*} + \eta_s^{2*} = 0, \text{ where } k \text{ such that } s \in \mathcal{L}_k \\ \gamma_k^* \left(\sum_{s\in\mathcal{L}_k} x_s - M_k \right) = 0, \ \forall k \\ \eta_s^{1*}(x_s^* - U^x) = 0 \\ \eta_s^{2*}(x_s^* - L^x) = 0 \\ L^x \le x_s^* \le U^x \\ \sum_{s\in\mathcal{L}_k} x_s - M_k, \ \forall k \end{cases} \tag{13}$$

根据方差变换 y_s =指数函数$\left({}_{(w^f x_s + t^f)_\mu} \right)$，令 y_s^* =指数函数$\left({}_{(w^f x_s^* + t^f)_\mu} \right)$以及 $x_s = \widehat{x}_s(y_s)$ =μ对数$\left(\frac{y_s}{w^f} - t^f \right)$对所有 $s \in \mathcal{L}$，我们可以将（13）等价地写为：

$$\begin{cases} \frac{\widetilde{g}(\mathbf{x}^*,\delta)}{\partial x_s} \frac{\partial \widehat{x}_s(y_s^*)}{\partial y_s} - \gamma_k^* \frac{\partial \widehat{x}_s(y_s^*)}{\partial y_s} - \eta_s^{1*} \frac{\partial \widehat{x}_s(y_s^*)}{\partial y_s} + \eta_s^{2*} \frac{\partial \widehat{x}_s(y_s^*)}{\partial y_s} = 0 \\ \gamma_k^* \left(\sum_{s\in\mathcal{L}} \frac{\mu \log(y_s^*) - t^f}{w^f} - M \right) = 0, \ \forall k \\ \eta_s^{1*} \left(\frac{\mu \log(y_s^*) - t^f}{w^f} - U^x) \right) = 0 \\ \eta_s^{2*} \left(\frac{\mu \log(y_s^*) - t^f}{w^f} - L^x \right) = 0 \\ L^x \le \frac{\mu \log(y_s^*) - t^f}{w^f} \le U^x \\ \sum_{s\in\mathcal{L}_k} \frac{\mu \log(y_s^*) - t^f}{w^f} \le M_k, \ \forall k. \end{cases} \tag{14}$$

(14) 中的第一个条件可等价地写为：

$$\frac{\widetilde{g}(\mathbf{y}^*, \delta)}{\partial y_s} - \gamma_k^* \mathbb{I}[s \in \mathcal{L}_k] \frac{\partial \widehat{x}_s(y_s^*)}{\partial y_s} - \eta_s^{1*} \frac{\partial \widehat{x}_s(y_s^*)}{\partial y_s} + \eta_s^{2*} \frac{\partial \widehat{x}_s(y_s^*)}{\partial y_s} = 0,$$

其中，$\mathbb{I}[\cdot]$是指示函数。这意味着$\mathbf{y}^*$、$\boldsymbol{\gamma}^*$、$\boldsymbol{\eta}^{1*}$、$\boldsymbol{\eta}^{1*}$也满足以下（严格）凸优化问题的 KKT 条件（即 **Step1** 中所讨论的变量变换所得的问题）。

$$\begin{aligned} \max_{\mathbf{y}} \quad & \widetilde{g}(\mathbf{y}, \delta) \\ \text{subject to} \quad & \sum_{s\in\mathcal{L}_k} \widehat{x}_s(y_s) \le M_k, \ \forall k \text{ and } \widehat{x}_s(y_s) \in [L^x, U^x]. \end{aligned} \tag{15}$$

因此，$\mathbf{y}^*$是（15）的唯一全局最优解，这也意味着$\mathbf{x}^*$也是（sub-Approx）的全局最优解，正如所期望的那样。□

5.2.2 精确解。根据定理6，我们可以使用基于梯度的方法求得（sub-Approx）的唯一全局最优解。计算上的挑战在于，目标函数$\widetilde{g}$（$\mathbf{x}$ δ）仍然涉及指数数量的路径。我们的思路是将 $\widetilde{g}$（$\mathbf{x}$ δ）分解为多个项（每一项对应一个关键节点 $s \in \mathcal{L}$），并使用动态规划计算这些项。具体而言，我们通过保留节点 $s \in \mathcal{L}$ 并移除其他所有

节点$\mathcal{L}$来创建新的图。通过这样做，我们可以使用第 Δ（s）节中的方法精确处理 Δ（s）。为便于说明，令$\mathcal{G}(s)$表示从图$\mathcal{G}$ 中删除集合$\mathcal{L}$ 中的所有节点（节点 s除外）后得到的子图。由于我们将处理多个图，因此下文将任意图$\mathcal{G}$ 中的所有路径记为 $\Omega(\mathcal{G})$。下面的命题表明，$\widetilde{g}$（$\mathbf{x}$ δ）可以分解为若干项，并且这些项可基于子图$\mathcal{G}(s)$、 $\forall s \in \mathcal{S}$高效计算。

命题 7。 $\widetilde{g}$（$\boldsymbol{x}$ δ） 可写为如下形式：

$$\sum_{s\in\mathcal{L}}\left(\sum_{\tau\in\Omega(\mathcal{G}(s))\tau\ni s}\left[r^{l}(s,x_s)\exp\left(\frac{U(\tau;\boldsymbol{x})}{\mu}\right)-\delta\exp\left(\frac{U(\tau;\boldsymbol{x})}{\mu}\right)\right]\right) \tag{16}$$

给定任意子图 $\mathcal{G}(s)$，中的项 $\widetilde{g}(\mathbf{x}$ $\delta)$ （以及它们的梯度）可以通过求解线性方程组来计算，类似于第 1 节的算法 4.1中所述的方法。我们在下面的算法 2 中求解整个问题。

算法2： 求解(OPT) 通过受限阻断问题(Approx-OPT)

- 创建 $\mathcal{G}(s)$ 对所有 $s \in \mathcal{L}$ - 使用二分搜索求解（Approx-OPT）。在二分搜索的每一步，利用式（$\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x}$ $\delta)$ 中的重构，使用基于梯度的方法进行优化。- 使用原始网络重新求解（OPT），以改进上述步骤得到的解。

5.2.3 高效近似解。 回顾一下，在前面的章节中，我们提供了：(i)一种求解原始阻断问题（OPT）的新算法——该算法效率较高，但只能保证得到局部最优解；以及 (ii)一种求解受限阻断问题（Approx-OPT）的新算法（算法 2）——该算法能够为（Approx-OPT）提供全局最优解，从而保证得到（OPT）的有界近似解（定理 4&5）。然而，当$|\mathcal{L}|$ 较大时，由于该算法需要 $|\mathcal{L}|$ 个子图，因此在实际实现中可能无法很好地扩展。

因此，在本节中，我们提出一种兼具高效性并能保证（OPT）有界近似解的新算法。我们的主要思路可概括如下：(a)我们确定一种图修改，并使用第 4节所述的算法，基于修改后的图求解（OPT）；(b)尽管 (a)无法保证得到（OPT）的全局最优解，但我们从理论上证明，由此得到的解是（Approx-OPT）的有界近似解（定理 8）；(c)最后，借助定理 5和定理 8中的结论，我们得到定理 9，证明由 (a) 得到的解同样是（OPT）的有界近似解。下面将详细阐述我们的思路。

网络修改。 本质上，我们通过提高 L 中任意一对节点之间的通行成本来修改原始网络 G，使得 β_1 和 β_2 变得任意小。值得注意的是，对于任意 $\epsilon' > 0$，我们总能修改 L 中各节点对之间的通行成本，从而得到一个修改后的网络 G′，使其满足以下条件：

$$\max_{\mathbf{x}}\max_{s\in\mathcal{L}}\left\{\frac{\sum_{\tau\in\Delta^{+}(s)}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau\in\Omega,\tau\ni s}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}\right\}\leq\epsilon' \tag{17}$$

$$\max_{\mathbf{x}}\left\{\frac{\sum_{\tau\in\bigcup_s\{\Delta^{+}(s)\}}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau\in\Omega}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}\right\}\leq\epsilon'. \tag{18}$$

提醒一下， $\Delta^+(s)$ 是所有经过 s 且至少还经过 L 中另一个节点的路径集合，而 Ω 是所有路径的集合。我们将二分搜索步骤中关于修改后的网络 G′的 (OPT) 的目标函数 (5) 记为 $g(\mathrm{x}\ \delta|\mathrm{G}')$。我们可以通过梯度下降来优化 $g(\mathrm{x}\ \delta|\mathrm{G}')$。问题 $\max_{\mathbf{x}} g(\mathrm{x}\ \delta|\mathrm{G}')$ 并非凸问题，但我们可以给出以下强有力的保证。

解的理论界。我们先定义：

$$\rho^s = \sum_{\tau\in\Omega,\tau\ni s} \exp\left(\frac{U(\tau; L^x\mathbf{e})}{\mu}\right),\ \forall s \in \mathcal{L}$$

$$\rho = \sum_{\tau\in\Omega} \exp\left(\frac{U(\tau; L^x\mathbf{e})}{\mu}\right)$$

其中$\mathbf{e}$ 是一个大小为 |L|的全 1 向量。请注意， L^x和 U^x分别是防御者在每个关键节点 $s \in$ L处资源覆盖 x_s 的下界和上界。此外，对手和防御者的效用函数具有如下线性形式： $v(s;\mathbf{x}) = v(s, x_s) = w_s^f x_s + t_s^f$和$r^l(s;\mathbf{x}) = r^l(s, x_s) = w_s^l x_s + t_s^l$，其中常数为 $w_s^f, t_s^f, w_s^l, t_s^l$，且 $w_s^f < 0$和 $w_s^l > 0$。

定理 8。 若我们运行二分搜索来求解(OPT)，使用修改后的网络$\mathcal{G}'$并得到$(\boldsymbol{x}\ \delta)$，则受限问题(Approx-OPT)的性能界如下：

$$\widetilde{\mathcal{F}}(\bar{\mathbf{x}}) \geq \max_{\boldsymbol{x}}\{\widetilde{F}(\boldsymbol{x})\} - \frac{\epsilon'(\mathcal{H}+2C)}{\sum_{s\in\mathcal{L}}\sum_{\tau\in\Delta(s)}\exp\left(\frac{U(\tau;U^x\boldsymbol{e})}{\mu}\right)} \tag{19}$$

其中常数$C = \left(\kappa \max_s\{\rho^s\} + \delta\rho\right)$。

证明概要。 我们的证明依赖于以下两个引理。引理 3 说明二分搜索步骤的目标函数之间的关系 $g(\mathbf{x}\ \delta|\mathcal{G}')$对应于（OPT）中使用修改后的 $\mathcal{G}'$的步骤，以及受限问题（Approx-OPT）中使用原始图 $\mathcal{G}$的二分搜索步骤 $\widetilde{g}(\mathbf{x}\ \delta)$ 的目标函数。

引理 3。 对于任意$(\boldsymbol{x}\ \delta)$，有：

$$|g(\boldsymbol{x}, \delta|\mathcal{G}') - \widetilde{g}(\boldsymbol{x}, \delta)| \leq \epsilon'\left(\kappa \max_s\{\rho^s\} + \delta\rho\right).$$

给定 δ，下面的引理 4 表明，$\max_{\mathbf{x}} g(\mathrm{x}\ \delta|\mathrm{G}')$ 的任意局部最优解（即（OPT）中使用修改后的 G′的二分步骤）都位于（sub-Approx）的最优解的 O (ϵ') 邻域内：（sub-Approx）：$\max_{\mathbf{x}} \widetilde{g}(\mathrm{x}\ \delta)$，即受限问题（Approx-OPT）中使用原始图 G 的二分步骤。为证明该引理，我们证明：对于 $\max_{\mathbf{x}} g(\mathrm{x}\ \delta|\mathrm{G}')$ 的任意局部最优解 x，都存在一个单峰函数（即经过变量变换后变为严格凹函数，如定理6的证明中所述），它位于 $\widetilde{g}(\mathrm{x}\ \delta)$ 的 O (ϵ') 邻域内，且 x 是其全局最优解。

引理 4。 令$\boldsymbol{x}$为给定 δ 下$\max_{\boldsymbol{x}} g(\boldsymbol{x}\ \delta|\mathcal{G}')$的局部最优解，则有：

$$\max_{\boldsymbol{x}}\{\widetilde{g}(\boldsymbol{x}, \delta)\} - \widetilde{g}(\bar{\mathbf{x}}, \delta) \leq \epsilon'\mathcal{H},$$

$$where\ \mathcal{H} = 2\left(\mu\rho^j + \frac{\kappa}{|w_j^f|}\max_s\{\rho^s\} + \delta\rho\right)\exp\left(\frac{w_j^f(L^x - U^x)}{\mu}\right).$$

令 $(\mathbf{x}^*, \delta^*)$ 为通过二分法（即二分搜索）求解受限阻断问题（Approx-OPT）得到的输出。基于上述两个引理，我们现在尝试界定间隙 $|\delta - \delta^*|$（基于此，我们可以界定 $\max_{\mathbf{x}\in\mathcal{X}} \mathcal{F}(\mathbf{x}) - \mathcal{F}(\mathbf{x})$，具体说明将在后文给出）。

首先，由于$\bar{\mathbf{x}}\ \delta)$ 是通过二分搜索求解 (OPT) 得到的输出，使用的是修改后的网络 $\mathcal{G}'$，因此我们有$|g(\mathbf{x}\ \delta|\mathcal{G}')| \leq \xi$，其中 ξ是一个正的常数，取决于二分

搜索的精度。事实上，这个常数可以任意小，因此为简洁起见，我们可以在后续证明中将其省略——也就是说，接下来我们只考虑$|g(\mathbf{x}\ \delta|\mathcal{G}')| = 0$。现在，根据引理 3，我们有：

$$|g(\overline{\mathbf{x}}, \overline{\delta}|\mathcal{G}') - \widetilde{g}(\overline{\mathbf{x}}, \overline{\delta})| \leq \epsilon' \left(\kappa \max_s\{\rho^s\} + \overline{\delta}\rho\right) = \epsilon' C \tag{20}$$

由于 $|g(\overline{\mathbf{x}}\ \overline{\delta}|\mathcal{G}')| = 0$，我们有 $|\widetilde{g}(\overline{\mathbf{x}}\ \overline{\delta})| \leq \epsilon' C$。

另一方面，由于$(\mathbf{x}^*,\ \delta^*)$ 是对（Approx-OPT）进行二分搜索的结果，因此我们有：$\widetilde{g}(\mathbf{x}^*,\ \delta^*) = 0$ 且 $\delta^* = \max_{\mathbf{x}\in\mathcal{X}} F(\mathbf{x})$。我们记：

$$\widetilde{K}(\delta) = \max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x}, \delta)$$

其中 $\widetilde{K}(\delta)$ 在 δ中单调递减。此外，$K(\delta^*) = \widetilde{g}(\mathbf{x}^*,\ \delta^*) = 0$。根据引理4：

$$\widetilde{K}(\overline{\delta}) - \epsilon'\mathcal{H} \leq \widetilde{g}(\overline{\mathbf{x}}, \overline{\delta}) \leq \widetilde{K}(\overline{\delta}). \tag{21}$$

因此，我们得到以下不等式链：

$$\epsilon'\mathcal{H} \geq |\widetilde{K}(\overline{\delta}) - \widetilde{g}(\overline{\mathbf{x}}, \overline{\delta})| \overset{(a)}{\geq} |\widetilde{K}(\overline{\delta})| - |\widetilde{g}(\overline{\mathbf{x}}, \overline{\delta})| \geq |\widetilde{K}(\overline{\delta})| - \epsilon' C \tag{22}$$

$$\implies |\widetilde{K}(\overline{\delta})| \leq \epsilon'(\mathcal{H} + C) \tag{23}$$

其中，$a(K)$ 是根据三角不等式得出的。我们还可以得到 $\delta^*(=0)$，因此：

$$|\widetilde{K}(\overline{\delta}) - \widetilde{K}(\delta^*)| \leq \epsilon'(\mathcal{H} + C)$$

由于 $K(\delta)$ 关于 δ 可微，根据中值定理，存在 $\alpha \in [\delta, \delta^*]$ 使得：

$$|\widetilde{K}(\overline{\delta}) - \widetilde{K}(\delta^*)| = \widetilde{K}'(\alpha)|\overline{\delta} - \delta^*| \leq \epsilon'(\mathcal{H} + C). \tag{24}$$

我们将 $\widetilde{\mathbf{x}}$ 记为 $K(\alpha) = \max_{\mathbf{x}\in\mathcal{X}}\{\widetilde{g}(\mathbf{x}\ \alpha)\}$ 的解。根据 Danskin 定理，我们可以如下计算梯度 $K\prime(\alpha)$：

$$|\widetilde{K}'(\alpha)| = \left(\sum_{s\in\mathcal{L}}\sum_{\tau\in\Delta(s)} \exp\left(\frac{U(\tau;\widetilde{\mathbf{x}})}{\mu}\right)\right) \geq \sum_{s\in\mathcal{L}}\sum_{\tau\in\Delta(s)} \exp\left(\frac{U(\tau;U^x\mathbf{e})}{\mu}\right) \overset{\text{def}}{=} \lambda,$$

结合（24），我们得到以下界：

$$0 \leq \delta^* - \overline{\delta} \leq \frac{\epsilon'(\mathcal{H} + C)}{\lambda}. \tag{25}$$

已知上述关于 $\delta^* - \delta$ 的界，现在我们将对 $\max_{\mathbf{x}\in\mathcal{X}}\mathcal{F}(\mathbf{x}) - \mathcal{F}(\mathbf{x})$ 进行界定。根据上述不等式 $|\widetilde{g}(\mathbf{x}\ \delta)| \leq \epsilon' C$（公式 20）的断言，我们有：

$$\left|\sum_{s\in\mathcal{L}}\sum_{\tau\in\Delta(s)} r^l(s, \overline{x}_s) \exp\left(\frac{U(\tau;\overline{\mathbf{x}})}{\mu}\right) - \overline{\delta}\left(\sum_{s\in\mathcal{L}}\sum_{\tau\in\Delta(s)} \exp\left(\frac{U(\tau;\overline{\mathbf{x}})}{\mu}\right)\right)\right| \leq \epsilon' C$$

这意味着

$$\left|\widetilde{\mathcal{F}}(\overline{\mathbf{x}}) - \overline{\delta}\right| \leq \frac{\epsilon' C}{\sum_{s\in\mathcal{L}}\sum_{\tau\in\Delta(s)} \exp\left(\frac{U(\tau;\overline{\mathbf{x}})}{\mu}\right)} \leq \frac{\epsilon' C}{\lambda} \implies \widetilde{\mathcal{F}}(\overline{\mathbf{x}}) \geq \overline{\delta} - \frac{\epsilon' C}{\lambda}$$

因此，我们得到以下界：

$$\delta^* = \max_{\mathbf{x}\in\mathcal{X}} \widetilde{\mathcal{F}}(\mathbf{x}) \geq \widetilde{\mathcal{F}}(\overline{\mathbf{x}}) \geq \overline{\delta} - \frac{\epsilon' C}{\lambda} \implies \max_{\mathbf{x}\in\mathcal{X}} \widetilde{\mathcal{F}}(\mathbf{x}) - \widetilde{\mathcal{F}}(\overline{\mathbf{x}}) \leq \delta^* - \overline{\delta} + \frac{\epsilon' C}{\lambda} \leq \frac{\epsilon'(\mathcal{H} + 2C)}{\lambda}.$$

由此完成我们的证明。 □

最后，我们给出关于原问题（OPT）的理论界。本质上，定理9 是定理5 和定理8结合以下常数直接得到的结果：

$$\mathcal{U} = \frac{\mathcal{H} + 2C}{(\min_{\mathbf{x}\in\mathcal{X}} \widetilde{\mathcal{F}}(\mathbf{x}) + \kappa) \sum_{s\in\mathcal{L}} \sum_{\tau\in\Delta(s)} \exp\left(\frac{U(\tau;U^x\mathbf{e})}{\mu}\right)}.$$

定理 9。 如果我们针对修改后的网络 (OPT) 运行二分搜索以求解 $\mathcal{G}'$ 并获得 $(\boldsymbol{x}\ \delta)$，则可保证以下性能界：

$$\mathcal{F}^l(\overline{\boldsymbol{x}}) \geq \frac{1}{\overline{\eta}} \max_{\boldsymbol{x}}\{\mathcal{F}^l(\boldsymbol{x})\} - \kappa\frac{\overline{\eta}-1}{\overline{\eta}},$$

其中 $\underline{\eta} = (1+\beta_1)(1+\beta_2)\left(1+\epsilon\prime\mathcal{U}\right)$，其中 $\mathcal{U}$ 是一个与 ϵ'、β_1、β_2 无关的常数。

在结束之前，我们在算法 3 中给出近似方案的主要步骤。

算法 3： 通过受限阻断问题 (OPT) 求解 (Approx-OPT)

/* 通过近似求解 (Approx-OPT) 来求解 (sub-Approx) */
- 通过提高 L 中任意节点对之间的行驶成本来创建 G′
- 使用修改后的图 OPT，通过算法 1 求解 $\mathcal{G}'$
/* 改进 */
恢复原始图 $\mathcal{G}$ 并重新求解 OPT，以改进上述步骤获得的解。

注 2。 如果 β_1、β_2 和 ϵ' 较小，那么 η 将接近 1，$\boldsymbol{x}$ 也将接近原始拦截问题的最优解。注意，在实际情况下，如果对手在关键节点之间行驶的成本很高（例如，关键节点彼此相距较远），β_1、β_2 将会很小。此外，如果能够很好地识别关键节点之间行驶的主要路径，就可以轻松提高这些路径的成本，使 ϵ' 任意小。

6 数值实验

为展示我们提出的算法的有效性，我们在合成数据上进行了实验。

6.1 实验设置

数据生成：我们生成包含 $|\mathbb{S}|$ 个顶点、边概率为 p 的随机图（无环）。我们随机选择 $|\mathbb{L}|$ 个顶点（源点和目的地除外）作为可被攻击的关键节点。我们设置 $|\mathbb{L}| = 0.8\times|\mathbb{S}|$。此外，防御者权重 $\{(w_j^l, t_j^l)|j \in [|\mathbb{L}|]\}$ 从区间 $[0,1]$ 中均匀随机生成，对手权重 $\{(w_j^f, t_j^f)|j \in [|\mathbb{S}|]\}$ 从区间 $[-1,0]$ 中随机生成。

基线方法： 我们通过从网络中采样路径，近似计算方程4 中对指数级数量路径的求和，并对该表达式执行梯度下降，以估计最优决策变量。有关路径采样方式的详细信息见附录。我们使用随机采样的 1000 条路径来估计基线目标函数。为确保公平性，所有算法均使用相同数量的训练轮次。此外，由于算法 2包含两个梯度循环，我们确保算法 2 中的循环总数与基线方法和算法 1相同。对于我们所考虑的最大图规模（规模 $|\mathcal{S}| = 100$），所有方法的运行时间均少于五分钟。所有实验均在配备 128GB 随机存取存储器的 2.1 GHz 中央处理器上运行。

6.2 数值结果

如表 1所示，我们注意到，与我们提出的方法相比，基线方法的解质量较差。此外，我们的实验也验证了算法 2所推导出的保证所带来的益处。

	节点数（$\|S\|$）				
方法	20	40	60	80	100
基线方法	93.44 ± 3.12	94.38 ± 3.27	96.88 ± 2.18	94.72 ± 2.25	96.76 ± 2.53
算法 1	94.36 ± 2.69	98.10 ± 1.98	99.76 ± 0.16	99.48 ± 0.45	99.99 ± 0.00

表 1. 通过各种方法得到的最优解的目标值占算法 2 得到的最优目标值的百分比。我们使用 $p = 0.8$, $\mu = 2$, $|\mathcal{L}| = 0.8|\mathcal{S}|$。每种设置下均随机生成了 20 个数据集，并报告均值和标准差。

7 结论

网络阻断博弈问题一开始就面临着一系列看似难以解决的挑战。在本研究中，我们通过提供能够求解一类具有近似保证的网络阻断问题的方法，应对其中一些挑战。近似保证的质量取决于具体问题，但在大量随机采样的问题中，我们的方法在经验表现上优于基线方法。我们也是首批研究以下类型网络阻断问题中的动态分位响应模型的研究者：[Fulkerson 和 Harding，1977 年，Israeli 和 Wood， 2002]。我们认为，这项建模与方法论方面的贡献为未来诸多可能的研究方向提供了启示，例如，识别能够使我们的近似保证表现良好的图的性质，或研究一种变体，其中对手的目标是最大化通过网络的流量。

参考文献

Victor Aguirregabiria and Pedro Mira. 2010年. 动态离散选择结构模型：综述. 计量经济学杂志 156, 1 (2010年), 38–67. Nicola Basilico, Giuseppe De Nittis, and Nicola Gatti. 2017 年 . 具有空间不确定警报信号的对抗式巡逻 . 人工智能 246 (2017 年), 220–257. Nicola Basilico, Nicola Gatti, and Francesco Amigoni. 2009 年 . 在具有任意拓扑结构的环境中进行机器人巡逻的领导者—跟随者策略. In 自主智能体与多智能体系统国际联合会议 *(AAMAS)*. 57–64. Aharon Ben-Tal and Arkadi Nemirovski. 2002年. 鲁棒优化——方法论与应用. 《数学规划》 92, 3 (2002 年), 453–480. Dimitri P Bertsekas and John N Tsitsiklis. 1991 年 . 随机最短路径问题分析 . 运筹学数学 16, 3 (1991年), 580–595. Juan S Borrero, Oleg A Prokopyev, and Denis Sauré. 2016年. 不完全信息下的序贯最短路径阻断. 决策分析 13, 1 (2016年), 68–98. Stephen Boyd, Stephen P Boyd, and Lieven Vandenberghe. 2004年. 凸优化. 剑桥大学出版社. Jakub Černỳ, Viliam Lisỳ, Branislav Bošanskỳ, and Bo An. 2021年. 用于计算量化斯塔克尔伯格均衡的 Dinkelbach 型算法. In 第二十九届国际人工智能联合会议论文集. 246–253. Kelly J Cormican, David P Morton, and R Kevin Wood. 1998年. 随机网络阻断. 运筹学 46, 2 (1998年), 184–197. Stephan Dempe, Vyacheslav Kalashnikov, Gerardo A Pérez-Valdés, and Nataliya Kalashnykova. 2015年. 双层规划问题. 能源系统. 施普林格，柏林 10 (2015年), 978–3. Werner Dinkelbach. 1967年. 非线性分式规划. 管理科学 13, 7 (1967年), 492–498.

M. Fosgerau, E. Frejinger, and A. Karlström. 2013年. 选择集不受限制的基于链接的网络路径选择模型. 《交通研究*B*辑》 56 (2013年), 70–80. Delbert Ray Fulkerson and Gary C Harding. 1977年. 在预算约束下最大化最小源汇路径. 《数学规划》 13, 1 (1977年), 116–118. Nika Haghtalab, Fei Fang, Thanh H. Nguyen, Arunesh Sinha, Ariel D. Procaccia, and Milind Tambe. 2016年. 三种成功策略：学习安全博弈中的对手模型. In 第二十五届国际人工智能联合会议 *(IJCAI)*. Eitan Israeli and R Kevin Wood. 2002年. 最短路径网络阻断. 《*Networks*：国际期刊》 40, 2 (2002年), 97–111. Manish Jain, Dmytro Korzhyk, Ondřej Vaněk, Vincent Conitzer, Michal Pěchouček, and Milind Tambe. 2011年. 用于图上零和安全博弈的双重预言机算法. In 第十届国际自主智能体与多智能体系统会议论文集，第*1*卷. 327–334. George Leitmann. 1978. 关于广义 Stackelberg 策略. 《优化理论与应用杂志》 26, 4 (1978), 637–643. Tien Mai, Mogens Fosgerau, and Emma Frejinger. 2015年. 用于路径选择分析的嵌套递归Logit模型. 《交通研究*B*辑》 75, 0 (2015年), 100 – 112. Tien Mai and Arunesh Sinha. 2022年. 选择并非独立：采用嵌套量化响应模型的 Stackelberg 安全博弈.(2022年). In 第三十六届 *AAAI* 人工智能会议论文集，温哥华，加拿大. 1–9. Daniel McFadden. 1981年. 概率选择的计量经济模型. In 计量经济应用中的离散数据结构分析, C. Manski and D. McFadden (Ed.). 麻省理工学院出版社, 第5章, 198–272. David Milec, Jakub Černỳ, Viliam Lisỳ, and Bo An. 2020年. 在大型双人博弈中利用量化对手的复杂性与算法. *arXiv* 预印本 *arXiv:2009.14521* (2020年). Robert A Miller. 1984年. 工作匹配与职业选择. 《政治经济学杂志》 (1984年), 1086–1120. John Rust. 1987年. GMC 公交车发动机的最优更换：Harold Zurcher 的实证模型. 《计量经济学》 55, 5 (1987年), 999–1033. Jorge A Sefair and J Cole Smith. 2016年. 动态最短路径阻断. 《*Networks*》 68, 4 (2016年), 315–330. J Cole Smith, Churlzu Lim, and Aydın Alptekinoğlu. 2009年. 针对捕食者的新产品引入：一种双层混合整数规划方法. 《海军研究后勤》 56, 8 (2009年), 714–729. J Cole Smith and Yongjia Song. 2020年. 网络阻断模型与算法综述 . 《欧洲运筹学杂志》 283, 3 (2020 年), 797–811. Kenneth Train. 2003 年 . 带模拟的离散选择方法. 剑桥大学出版社. Kai Wang, Andrew Perrault, Aditya Mate, and Milind Tambe. 2020年. 面向博弈的对手模型可扩展学习：网络安全博弈中的从数据到决策. In *AAMAS*. 1449–1457. Kenneth I Wolpin. 1984年. 生育与儿童死亡率的可估计动态随机模型. 《政治经济学杂志》 (1984年), 852–874. Wanqi Xue, Bo An, and Chai Kiat Yeo. 2022年. NSGZero：通过神经蒙特卡洛树搜索，在大规模网络安全博弈中高效学习不可利用策略. *arXiv* 电子预印本 (2022年), arXiv–2201. Wanqi Xue, Youzhi Zhang, Shuxin Li, Xinrun Wang, Bo An, and Chai Kiat Yeo. 2021年. 通过神经虚拟自博弈求解大规模扩展式网络安全博弈. *arXiv* 预印本 *arXiv:2106.00897* (2021年). Rong Yang, Christopher Kiekintveld, Fernando Ordonez, Milind Tambe, and Richard John. 2011年. 改进针对人类对手的安全博弈资源分配策略. In 第二十二届国际人工智能联合会议. Rong Yang, Fernando Ordonez, and Milind Tambe. 2012年. 计算安全博弈中针对量化响应的最优策略. In *AAMAS*. 847–854. Youzhi Zhang, Qingyu Guo, Bo An, Long Tran-Thanh, and Nicholas R Jennings. 2019年. 借助实时信息对城市罪犯进行最优阻断. In *AAAI*人工智能会议论文集, Vol. 33. 1262–1269. Maëlle Zimmermann and Emma Frejinger. 2020年. 用于分析和预测路径选择行为的递归模型教程. 《*EURO*交通与物流杂志》 9, 2 (2020年), 100004.

A 详细证明

A.1 命题1的证明

证明。我们将对手的期望效用重写如下：

$$\begin{aligned}
\mathcal{E}^f &= \sum_{\tau\in\Omega} U(\tau)\frac{\exp\left(\frac{U(\tau)}{\mu}\right)}{\sum_{\tau'}\exp\left(\frac{U(\tau')}{\mu}\right)} \\
&= \sum_{\tau\in\Omega^*} U(\tau)\frac{\exp\left(\frac{U(\tau)}{\mu}\right)}{\sum\limits_{\tau'\in\Omega^*}\exp\left(\frac{U(\tau')}{\mu}\right)+\sum\limits_{\tau'\in\Omega\setminus\Omega^*}\exp\left(\frac{U(\tau')}{\mu}\right)} \\
&+ \sum_{\tau\in\Omega\setminus\Omega^*} U(\tau)\frac{\exp\left(\frac{U(\tau)}{\mu}\right)}{\sum\limits_{\tau'\in\Omega^*}\exp\left(\frac{U(\tau')}{\mu}\right)+\sum\limits_{\tau'\in\Omega\setminus\Omega^*}\exp\left(\frac{U(\tau')}{\mu}\right)} \\
&= \frac{U(\tau^*)|\Omega^*|}{|\Omega^*|+\sum\limits_{\tau'\in\Omega\setminus\Omega^*}\exp\left(\frac{U(\tau')-U(\tau^*)}{\mu}\right)} + \sum_{\tau\in\Omega\setminus\Omega^*}\frac{U(\tau)\exp\left(\frac{U(\tau)-U(\tau^*)}{\mu}\right)}{|\Omega^*|+\sum\limits_{\tau'\in\Omega\setminus\Omega^*}\exp\left(\frac{U(\tau')-U(\tau^*)}{\mu}\right)}
\end{aligned} \tag{26}$$

为简化记号，令 $\mathrm{T}=\sum_{\tau'\in\Omega\setminus\Omega^*}\exp\left(\frac{U(\tau')-U\ \tau^*}{\mu}\right)()$。我们有：

$$0 \le \mathcal{T} \le |\Omega\setminus\Omega^*|\exp\left(-\frac{\alpha}{\mu}\right) \tag{27}$$

由（26），可得：

$$\begin{aligned}
|\mathcal{E}^f - U(\tau^*)| &\le \frac{\mathcal{T}}{|\Omega^*|+\mathcal{T}} + \left|\sum_{\tau\in\Omega\setminus\Omega^*}\frac{U(\tau)\exp\left(\frac{U(\tau)-U(\tau^*)}{\mu}\right)}{|\Omega^*|+\mathcal{T}}\right| \\
&\le \frac{\mathcal{T}}{|\Omega^*|+\mathcal{T}} + L^*\left|\frac{\mathcal{T}}{|\Omega^*|+\mathcal{T}}\right| \\
&= (L^*+1)\frac{1}{1+\frac{|\Omega^*|}{\mathcal{T}}} \overset{(i)}{\le} \frac{L^*+1}{1+\frac{|\Omega^*|}{|\Omega\setminus\Omega^*|}\exp\left(\frac{\alpha}{\mu}\right)},
\end{aligned}$$

其中 (i) 由（27）得出。由此我们得到所需的不等式。极限 $\lim_{\mu\to 0}\mathcal{E}^f = U(\tau^*)$ 正是该不等式的直接结果，从而完成证明。 □

A.2 命题3的证明

证明。对于任意 $n\in\mathbb{N}$，考虑 $\mathbf{M}^n = \underbrace{\mathbf{M}\times\mathbf{M}\times\ldots\mathbf{M}}_{n\text{ times}}$，其元素为

$$\mathbf{M}^n_{ss'} = \sum_{(s_0,s_1,\ldots,s_n)\in\mathcal{S}^{n+1}}\left(\prod_{i=0}^{n-1} M_{s_i s_{i+1}}\right)$$

回顾一下，$M_{ss'} = \exp\left(\frac{v(s)}{\mu}\right)$ if $s'\in N(s)$ 以及 $M_{ss'}=0$ otherwise。我们看到，如果 $n>|\mathrm{S}|$，那么对于任意序列 $(s_0,\ \underbrace{s_1、\ldots\ldots、\ s_n}_{s_0=s,s_n=s'})$，至少存在一对 $s_j = s_k, 0\le j,\ k\le n$。由于该网络是

无环的，因此至少存在一对 $(s_j,\ s_{j+1})$ 使得 $M_{s_j s_{j+1}} = 0$，从而得到 $\mathbf{M}^n_{ss'} = \sum_{(s_0,\ s_1、\ \ldots\ldots、\ s_n) \in \mathcal{S}^{n+1}} \left(\prod_{i=0}^{n-1} M_{s_i s_{i+1}}\right) = 0$ 对于任意 $s,\ s' \in \mathrm{S}$。因此，如果 $n > |\mathrm{S}|$，则有 $\mathbf{M}^n = \mathbf{0}$。我们选取 $s_0=s,\ s_n=s' n > |\mathrm{S}|$ 并记作

$$(\mathbf{I} - \mathbf{M}) \left(\sum_{t=0}^{n-1} \mathbf{M}^t \right) = (\mathbf{I} - \mathbf{M}^n) = \mathbf{I},$$

这意味着 $\det(\mathbf{I} - \mathbf{M}) \neq 0$，或者等价地，$\mathbf{I} - \mathbf{M}$ 是可逆的，正如所要求的那样。 □

A.3 引理1的证明

证明。回顾一下，我们已将 β_1 和 β_2 定义如下：

$$\beta_1 = \max_{\mathbf{x}} \max_{s \in \mathcal{L}} \left\{ \frac{\sum_{\tau \in \Delta^+(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau \in \Delta(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)} \right\}, \quad \beta_2 = \max_{\mathbf{x}} \left\{ \frac{\sum_{\tau \in \bigcup_s \{\Delta^+(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau \in \bigcup_s \{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)} \right\},$$

对于任意 防御者策略 $x \in \mathrm{X}$，我们可以将防御者的期望效用重新写成如下形式：

$$\mathcal{F}^l(\mathbf{x}) = \frac{\sum_{s \in \mathcal{L}} r^l(s, x_s) \left(\sum_{\tau \in \Delta(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) + \sum_{\tau \in \Delta^+(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \right)}{\sum_{\tau \in \bigcup_s \{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) + \sum_{\tau \in \bigcup_s \{\Delta^+(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)} \stackrel{\text{def}}{=} \frac{\mathcal{U}}{\mathcal{V}} \tag{28}$$

根据 β_1 的定义，我们得到：

$$\sum_{\tau \in \Delta^+(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \leq \beta_1 \sum_{\tau \in \Delta(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)$$

$$\Longrightarrow \mathcal{U} \leq \sum_{s \in \mathcal{L}} r^l(s, x_s) \left(\sum_{\tau \in \Delta(s)} (1 + \beta_1) \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \right)$$

此外，我们有：$\mathrm{V} \geq \sum_{\tau \in \bigcup_s \{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)$。因此，我们得到以下不等式：

$$\mathcal{F}^l(\mathbf{x}) \leq \frac{\sum_{s \in \mathcal{L}} r^l(s, x_s) \left(\sum_{\tau \in \Delta(s)} (1 + \beta_1) \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \right)}{\sum_{\tau \in \bigcup_s \{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)} = (1 + \beta_1) \widetilde{\mathcal{F}}(\mathbf{x}) \tag{*}$$

另一方面，根据 β_2 的定义，我们得到：

$$\sum_{\tau \in \bigcup_s \{\Delta^+(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \leq \beta_2 \sum_{\tau \in \bigcup_s \{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)$$

$$\Longrightarrow \mathcal{V} \leq \sum_{\tau \in \bigcup_s \{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) (1 + \beta_2)$$

此外，我们有：$\mathrm{U} \geq \sum_{s \in \mathcal{L}} r^l(s, x_s) \left(\sum_{\tau \in \Delta(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \right)$。因此，我们得到：

$$\mathcal{F}^l(\mathbf{x}) \geq \frac{\sum_{s \in \mathcal{L}} r^l(s, x_s) \left(\sum_{\tau \in \Delta(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \right)}{\sum_{\tau \in \bigcup_s \{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) (1 + \beta_2)} = \frac{1}{1 + \beta_2} \widetilde{\mathcal{F}}(\mathbf{x}) \tag{**}$$

结合（*）和（**）即可完成我们的证明。 □

A.4 引理2的证明

证明。 我们沿用引理 1证明中 U 和 V 的定义。与引理 1的证明类似，根据 β_1的定义，我们得到：

$$\sum_{\tau\in\Delta^+(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \leq \beta_1 \sum_{\tau\in\Delta(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)$$

此外，根据定义 $\kappa = \sum_{s\in\mathcal{L}} \max_{\mathbf{x}} |r^l(s,x_s)|$，我们有 $r^l(s,x_s) + \kappa \geq 0$ 对于任意$\mathbf{x} \in \mathrm{X}$。因此，我们可以写为：

$$\begin{aligned}\mathcal{U} + \kappa\mathcal{V} &= \sum_{s\in\mathcal{L}} \left(r^l(s,x_s)+\kappa\right)\left(\sum_{\tau\in\Delta(s)\bigcup\Delta^+(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)\right)\\ &\leq \sum_{s\in\mathcal{L}} \left(r^l(s,x_s)+\kappa\right)\left(\sum_{\tau\in\Delta(s)} (1+\beta_1)\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)\right)\end{aligned}$$

此外，我们有：$\mathrm{V} \geq \sum_{\tau\in\bigcup_s\{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)$。因此，我们得到以下不等式：

$$\begin{aligned}\mathcal{F}^l(\mathbf{x}) + \kappa = \frac{\mathcal{U}+\kappa\mathcal{V}}{\mathcal{V}} &\leq \frac{\sum_{s\in\mathcal{L}} \left(r^l(s,x_s)+\kappa\right)\left(\sum_{\tau\in\Delta(s)}(1+\beta_1)\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)\right)}{\sum_{\tau\in\bigcup_s\{\Delta(s)\}}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}\\ &= (1+\beta_1)\left(\widetilde{\mathcal{F}}(\mathbf{x})+\kappa\right) \qquad (29)\end{aligned}$$

另一方面，根据我们的选择 κ，我们有：

$$\begin{aligned}\kappa \geq \sum_{s\in\mathcal{L}} |r^l(s,x_s)| &\geq \sum_{s\in\mathcal{L}} |r^l(s,x_s)| \frac{\sum_{\tau\in\Delta(s)}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau\in\bigcup_{s'}\{\Delta(s')\}}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}\\ \Longrightarrow \sum_{s\in\mathcal{L}} \left(r^l(s,x_s)+\kappa\right)&\left(\sum_{\tau\in\Delta(s)}\exp\left(\frac{U(\tau;\mathbf{x}))}{\mu}\right)\right) \geq 0\end{aligned}$$

此外，根据 β_2 的定义，我们得到：

$$\begin{aligned}&\sum_{\tau\in\bigcup_s\{\Delta^+(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \leq \beta_2 \sum_{\tau\in\bigcup_s\{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)\\ \Longrightarrow \mathcal{V} &\leq \sum_{\tau\in\bigcup_s\{\Delta(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)(1+\beta_2)\end{aligned}$$

因此，我们得到以下不等式，

$$\begin{aligned}\mathcal{F}^l(\mathbf{x}) + \kappa &\geq \frac{\sum_{s\in\mathcal{L}}(r^l(s,x_s)+\kappa)\left(\sum_{\tau\in\Delta(s)}\exp\left(\frac{U(\tau;\mathbf{x}))}{\mu}\right)\right)}{\mathcal{V}}\\ &\geq \frac{\sum_{s\in\mathcal{L}}(r^l(s,x_s)+\kappa)\left(\sum_{\tau\in\Delta(s)}\exp\left(\frac{U(\tau;\mathbf{x}))}{\mu}\right)\right)}{\sum_{\tau\in\bigcup_s\{\Delta(s)\}}\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)(1+\beta_2)} = \frac{1}{1+\beta_2}(\widetilde{\mathcal{F}}(\mathbf{x})+\kappa). \qquad (30)\end{aligned}$$

结合（29）和（30）即可得到所需的不等式。 □

A.5 引理3的证明

证明。注意到 $\{\tau; \tau \in \Omega, \ \tau \ni s\} = \Delta^+(s) \cup \Delta(s)$ 与 $\Delta^+(s) \ \Delta(s)$ 不相交，我们可以将 $g(\mathbf{x}\ \delta|\mathcal{G}')$ 分解为两个独立的项，如下所示：

$$\begin{aligned} g(\mathbf{x}, \delta|\mathcal{G}') &= \sum_{s\in\mathcal{L}} \sum_{\substack{\tau\in\Omega \\ \tau\ni s}} r_s^f(x_s) \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) - \delta\left(\sum_{\tau'\in\Omega} \exp\left(\frac{U(\tau';\mathbf{x})}{\mu}\right)\right) \\ &= \widetilde{g}(\mathbf{x}, \delta) + \mathcal{T}(\mathbf{x}, \delta), \end{aligned} \tag{31}$$

其中第二项：

$$\mathcal{T}(\mathbf{x}, \delta) = \sum_{s\in\mathcal{L}} r_s^f(x_s) \sum_{\tau\in\Delta^+(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) - \delta\left(\sum_{\tau\in\bigcup_{s\in\mathcal{L}}\Delta^+(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)\right).$$

此外，请记住我们对 ρ^s 和 ρ 的定义：

$$\rho^s = \sum_{\tau\in\Omega,\tau\ni s} \exp\left(\frac{U(\tau;L^x\mathbf{e})}{\mu}\right), \ \forall s \in \mathcal{L} \qquad\qquad \rho = \sum_{\tau\in\Omega} \exp\left(\frac{U(\tau;L^x\mathbf{e})}{\mu}\right)$$

根据公式（17）和（18），我们得到：

$$\max_{\mathbf{x}} \max_{s\in\mathcal{L}} \left\{ \frac{\sum_{\tau\in\Delta^+(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau\in\Omega,\tau\ni s} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)} \right\} \le \epsilon' \implies \sum_{\tau\in\Delta^+(s)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \le \epsilon'\rho^s, \ \forall \mathbf{x} \in \mathcal{X}, s \in \mathcal{L} \tag{32}$$

$$\max_{\mathbf{x}} \left\{ \frac{\sum_{\tau\in\bigcup_s\{\Delta^+(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau\in\Omega} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)} \right\} \le \epsilon' \implies \sum_{\tau\in\bigcup_s\{\Delta^+(s)\}} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \le \epsilon'\rho, \ \forall \mathbf{x} \in \mathcal{X}. \tag{33}$$

利用这些不等式，我们得到：

$$|\mathcal{T}(\mathbf{x}, \delta)| \le \sum_{s\in\mathcal{L}} |r_s^f(x_s)|\epsilon'\rho^s + \delta\epsilon'\rho \le \epsilon'\left(\kappa \max_s\{\rho^s\} + \delta\rho\right). \tag{34}$$

这就完成了我们的证明。 □

A.6 引理4的证明

证明。我们重用引理 3 中所述的 $g(\mathbf{x}\ \delta|\mathcal{G}')$ 分解。对 $\mathcal{T}(\mathbf{x}\ \delta)$ 关于 $x_j, j \in \mathcal{L}$ 求导，我们得到：

$$\begin{aligned} \frac{\partial\mathcal{T}(\mathbf{x}, \delta)}{\partial x_j} &= w_j^f \sum_{\tau\in\Delta^+(j)} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) + \frac{1}{\mu} \sum_{s\in\mathcal{L}} r_s^f(x_s) \sum_{\tau\in\Delta^+(s),\tau\ni j} w_j^f \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right) \\ &\quad - \frac{\delta}{\mu}\left(\sum_{\tau\in\bigcup_{s\in\mathcal{L}}\Delta^+(s),\tau\ni j} w_j^f \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)\right). \end{aligned}$$

因此，利用（32）和（33），我们得到不等式：

$$\left|\frac{\partial\mathcal{T}(\mathbf{x}, \delta)}{\partial x_j}\right| \le \epsilon'\left(|w_j^f|\rho^j + \frac{\kappa}{\mu}\max_s\{\rho^s\} + \frac{\delta}{\mu}|w_j^f|\rho\right). \tag{35}$$

Now, 考虑问题 $\max_{\mathbf{x}}\{g(\mathbf{x}\ \delta|\mathrm{G}')|\mathbf{x}\ \in \mathrm{X}\}$。我们将其构造为拉格朗日对偶形式：

$$L^{\mathcal{G}'}(\mathbf{x},\boldsymbol{\gamma},\boldsymbol{\eta}) = g(\mathbf{x},\delta|\mathcal{G}') - \sum_{k\in[K]}\gamma_k\left(\sum_{s\in\mathcal{L}_k}x_s - M_k\right) - \sum_s \eta_s^1(x_s - U^x) + \sum_s \eta_s^2(x_s - L^x).$$

如果$\mathbf{x}$是 $\max_{\mathbf{x}}\{g(\mathbf{x}\ \delta|\mathrm{G}')|\mathbf{x}\ \in \mathrm{X}\}$ 的驻点，那么 KKT 条件意味着存在$\boldsymbol{\gamma}^*, \boldsymbol{\eta}^{1*}, \boldsymbol{\eta}^{2*}$，使得：

$$\frac{\partial g(\overline{\mathbf{x}},\delta|\mathcal{G}')}{\partial x_j} - \sum_{k\in[K]}\gamma_k^*\mathbb{I}[j\in\mathcal{L}_k] - \eta_j^{1*} + \eta_j^{2*} = 0,$$

其中 $\mathbb{I}[\cdot]$是指示函数。注意，$\frac{\partial g(\mathbf{x}\ \delta|}{\partial x_j}' = \frac{\partial \widetilde{g}(\mathbf{x}\ \delta)}{\partial x_j} + \frac{\partial \mathcal{T}(\mathbf{x}\ \delta)}{\partial x_j}$。因此，由式（35）可得：

$$\begin{aligned}
&\left|\frac{\partial \widetilde{g}(\overline{\mathbf{x}},\delta)}{\partial x_j} - \sum_{k\in[K]}\gamma_k^*\mathbb{I}[j\in\mathcal{L}_k] - \eta_j^{1*} + \eta_j^{2*}\right| \\
&\le \left|\frac{\partial g(\overline{\mathbf{x}},\delta|\mathcal{G}')}{\partial x_j} - \sum_{k\in[K]}\gamma_k^*\mathbb{I}[j\in\mathcal{L}_k] - \eta_j^{1*} + \eta_j^{2*}\right| + \left|\frac{\partial\mathcal{T}(\mathbf{x},\delta)}{\partial x_j}\right| \\
&\le \epsilon'\left(|w_j^f|\rho^j + \frac{\kappa}{\mu}\max_s\{\rho^s\} + \frac{\delta}{\mu}|w_j^f|\rho\right). \qquad (36)
\end{aligned}$$

现在定义函数 $\widehat{G}(\mathbf{x}\ \delta)$ 如下：

$$\widehat{G}(\mathbf{x},\delta) = \widetilde{g}(\mathbf{x},\delta) + \sum_{s\in\mathcal{L}}\alpha_s\exp\left(\frac{w_s^f x_s + t_s^f}{\mu}\right),$$

其中，$\alpha_s, \forall s \in \mathrm{L}$ 的取值如下：

$$\alpha_s = -\frac{\frac{\partial\widetilde{g}(\overline{\mathbf{x}},\delta)}{\partial x_s} - \sum_{k\in[K]}\gamma_k^*\mathbb{I}[j\in\mathcal{L}_k] - \eta_j^{1*} + \eta_j^{2*}}{\frac{w_s^f}{\mu}\exp\left(\frac{w_s^f x_s + t_s^f}{\mu}\right)}.$$

给定按上述方式定义的 α_s，可得以下方程：

$$\frac{\partial\widehat{G}(\overline{\mathbf{x}},\delta)}{\partial x_j} - \sum_{k\in[K]}\gamma_k^*\mathbb{I}[j\in\mathcal{L}_k] - \eta_j^{1*} + \eta_j^{2*} = 0,\ \forall j\in\mathcal{L}. \qquad (37)$$

在下文中，我们首先尝试对每个防御者策略 x 界定 $\left|\widehat{G}(\mathrm{x}\ \delta) - \widetilde{g}(\mathrm{x}\ \delta)\right|$ 之间的差距。随后，我们结合 $G(\mathrm{x}\ \delta)$ 的单峰性，利用这一界来界定差距$\lrcorner\max_{\mathbf{x}\in\mathcal{X}}\widetilde{g}(\mathrm{x}\ \delta) - \widetilde{g}(\mathrm{x}\ \delta)|$。正如我们将在后文中展示的，$G(\mathrm{x}\ \delta)$ 的单峰性是基于方程37以及定理6证明中使用的变量转换技巧得到证明的。

Boun弥补差距 $\left|\widehat{G}(\boldsymbol{x}\ \delta) - \widetilde{g}(\boldsymbol{x}\ \delta)\right|$。对 $\widehat{G}(\mathbf{x}\ \delta)$关于$x_j$求导，可得 t:

$$\frac{\partial\widehat{G}(\mathbf{x},\delta)}{\partial x_j} = \frac{\widetilde{g}(\mathbf{x},\delta)}{\partial x_j} + \frac{\alpha_j w_j^f}{\mu}\exp\left(\frac{w_j^f + t_j^f}{\mu}\right).$$

结合（36）-（37），我们可以得到 α_j， $\forall j \in \mathcal{L}$的如下界：

$$\begin{aligned}
&\left|\frac{\alpha_j w_j^f}{\mu}\exp\left(\frac{w_j^f \overline{x}_j + t_j^f}{\mu}\right)\right| = \left|\frac{\partial \widehat{G}(\overline{\mathbf{x}},\delta)}{\partial x_j} - \frac{\widetilde{g}(\overline{\mathbf{x}},\delta)}{\partial x_j}\right| \\
&\leq \left|\frac{\partial \widehat{G}(\overline{\mathbf{x}},\delta)}{\partial x_j} - \sum_{k\in[K]} \gamma_k^* \mathbb{I}[j\in\mathcal{L}_k] - \eta_j^{1*} + \eta_j^{2*}\right| + \left|\frac{\partial \widetilde{g}(\overline{\mathbf{x}},\delta)}{\partial x_j} - \sum_{k\in[K]} \gamma_k^* \mathbb{I}[j\in\mathcal{L}_k] - \eta_j^{1*} + \eta_j^{2*}\right| \\
&\leq \epsilon'\left(|w_j^f|\rho^j + \frac{\kappa}{\mu}\max_s\{\rho^s\} + \frac{\delta}{\mu}|w_j^f|\rho\right) \qquad (38)
\end{aligned}$$

这意味着：

$$\left|\alpha_j \exp\left(\frac{w_j^f \overline{x}_j + t_j^f}{\mu}\right)\right| \leq \epsilon'\mu\left(\rho^j + \frac{\kappa}{\mu|w_j^f|}\max_s\{\rho^s\} + \frac{\delta}{\mu}\rho\right). \qquad (39)$$

将上述不等式与 $G(\mathbf{x}\ \delta)$ 的定义相结合，可得到对于所有防御者策略 $\mathbf{x} \in \mathrm{X}$ 都成立的以下不等式：

$$\begin{aligned}
\left|\widehat{G}(\mathbf{x},\delta) - \widetilde{g}(\mathbf{x},\delta)\right| &\leq \sum_{j\in\mathcal{L}}\left|\alpha_j \exp\left(\frac{(w_j^f x_j + t_j^f)}{\mu}\right)\right| \\
&\leq \sum_{j\in\mathcal{L}}\left|\alpha_j \exp\left(\frac{w_j^f \overline{x}_j + t_j^f}{\mu}\right)\exp\left(\frac{w_j^f (x_j - \overline{x}_j)}{\mu}\right)\right| \\
&\leq \epsilon'\left(\mu\rho^j + \frac{\kappa}{|w_j^f|}\max_s\{\rho^s\} + \delta\rho\right)\exp\left(\frac{w_j^f (L^x - U^x)}{\mu}\right).
\end{aligned}$$

上界 $|\max_{\boldsymbol{x}\in\mathcal{X}} \widetilde{g}(\boldsymbol{x}\ \delta) - \widetilde{g}(\boldsymbol{x}\ \delta)|$。为简化记号，定义 $\mathrm{H} = 2\left(\mu\rho^j + \frac{\kappa}{|w_j^f|}\max_s\{\rho^s\} + \delta\rho\right)\exp\left(\frac{w_j^f (L^x - U^x)}{\mu}\right)$。我们有以下几点说明：

(i) 根据 (37)，我们可以看到，x 是最大化问题 $\max_{\mathbf{x}\in\mathcal{X}}\{G(\mathrm{x}\ \delta)\}$ 的驻点，并且 $\boldsymbol{\gamma}^*, \boldsymbol{\eta}^{1*}$, $\boldsymbol{\eta}^{2*}$ 是相应的 KKT乘子。(ii) 通过证明定理6时使用的变量变换，函数 $G(\mathrm{x}\ \delta)$ 变为 $\widetilde{g}(\mathrm{x(y)}\ \delta) + \sum_{s\in\mathrm{L}} \alpha_s y_s$，因此 $G(\mathrm{x(y)}\ \delta)$ 关于 y 严格凹。与定理6类似，$G(\mathrm{x}\ \delta)$ 是单峰的（即任何局部最优解都是全局最优解）。

因此，$\mathbf{x}$ 也是 $\max_{\mathbf{x}\in\mathcal{X}} G(\mathbf{x}\ \delta)$ 的最优解。因此，我们现在可以将差距 $|\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x}\ \delta) - \widetilde{g}(\mathbf{x}\ \delta)|$ 界定如下：

$$\begin{aligned}
|\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x},\delta) - \widetilde{g}(\overline{\mathbf{x}},\delta)| &\leq |\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x},\delta) - \widehat{G}(\overline{\mathbf{x}},\delta)| + |\widehat{G}(\overline{\mathbf{x}},\delta) - \widetilde{g}(\overline{\mathbf{x}},\delta)| \\
&\leq |\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x},\delta) - \max_{\mathbf{x}\in\mathcal{X}} \widehat{G}(\mathbf{x},\delta)| + \frac{\epsilon'\mathcal{H}}{2}. \qquad (40)
\end{aligned}$$

我们考虑以下两种情况：

- $\widehat{\ }$若 $\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x}\ \delta) \geq \max_{\mathbf{x}\in\mathcal{X}} G(\mathbf{x}\ \delta)$。令 $\mathbf{x}^*$ 为 $\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x}\ \delta)$ 的最优解，则有

$$\begin{aligned}|\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x},\delta) - \max_{\mathbf{x}\in\mathcal{X}} \widehat{G}(\mathbf{x},\delta)| &= \widetilde{g}(\mathbf{x}^*,\delta) - \max_{\mathbf{x}\in\mathcal{X}} \widehat{G}(\mathbf{x},\delta) \\ &\leq \widetilde{g}(\mathbf{x}^*,\delta) - \widehat{G}(\mathbf{x}^*,\delta) \\ &\leq \frac{\epsilon'\mathcal{H}}{2}\end{aligned} \tag{41}$$

- 如果 $\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x}\ \delta) < \max_{\mathbf{x}\in\mathcal{X}} \widehat{G}(\mathbf{x}\ \delta)$, 那么我们有

$$\begin{aligned}|\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x},\delta) - \max_{\mathbf{x}\in\mathcal{X}} \widehat{G}(\mathbf{x},\delta)| &= \max_{\mathbf{x}\in\mathcal{X}} \widehat{G}(\mathbf{x},\delta) - \max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x},\delta) \\ &\leq \widehat{G}(\overline{\mathbf{x}},\delta) - \widetilde{g}(\overline{\mathbf{x}},\delta) \\ &\leq \frac{\epsilon'\mathcal{H}}{2}\end{aligned} \tag{42}$$

结合（40）-（41）-（42），我们得到：

$$|\max_{\mathbf{x}\in\mathcal{X}} \widetilde{g}(\mathbf{x},\delta) - \widetilde{g}(\overline{\mathbf{x}},\delta)| \leq \epsilon'\mathcal{H}$$

这就是所需的不等式，从而完成我们的证明。

□

B 实验细节

对于基线方法，为了采样路径，将资源分配$\mathbf{x}$ 分配给 L，并将跟随者最初放置在起点 s_o。其下一个节点 s_1 从分布 $\pi^f(s|s_0,\mathbf{x}) = \exp\left(\frac{v_{s\ \mu}}{\sum_{s\in N} Z_{s(:\mathbf{x})'(s_0)} \exp\left(\frac{v_{(\prime;\mathbf{x})}}{\mu}\right) Z_{s'}}\right)$ 中采样，其中 $s \in$ {nodes having an edge to s_0}，而 $N(s_0)$ 是从 s_0出发的出节点集合。类似地，$s_2, \ldots$ 等会被采样，直到到达目的地 s_d。每次迭代会重复采样 1000 次，然后取平均值以获得目标函数。基于梯度，会更新资源分配$\mathbf{x}$，从而改变转移概率，并重复该过程直到收敛。对$\mathbf{x}$ 进行了十种不同的初始化，并报告损失最低的种子。

C 零和博弈模型

C.1 问题表述

本节讨论一种常用于对抗性场景的零和博弈模型，其中防御者的目标是最小化对手的期望效用。对手的期望效用可按如下方式计算：

$$\mathcal{E}^f(\mathbf{x}) = \sum_{\tau\in\Omega} U(\tau;\mathbf{x}) \frac{\exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)}{\sum_{\tau'\in\Omega} \exp\left(\frac{U(\tau';\mathbf{x})}{\mu}\right)}$$

零和博弈模型可表述如下：

$$\min_{\mathbf{x}\in\mathcal{X}} \quad \mathcal{E}^f(\mathbf{x}) \tag{OPT-zerosum}$$

它在$\mathbf{x}$上通常是非凸的。由于它与论文正文中讨论的非零和博弈模型具有相同的结构，我们基于受限

问题仍然适用。这里，我们不直接求解非凸问题（OPT-零和），而是提出优化以下对数和目标函数，该目标函数更易处理

$$\Gamma(\mathbf{x}) = \mu \log\left(\sum_{\tau\in\Omega} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)\right)$$

可以看出， Γ(x)具有几何规划的对数和指数凸形式，因此它是凸的 [Boyd etal., 2004]。根据第 4.1 节的结果，我们进一步得出， Γ(x)可以通过求解一个线性方程组来计算，而这可以在多项式时间内完成。因此，优化问题 $\max_{\mathbf{x}} \Gamma(\mathbf{x})$可以在多项式时间内求解。下面我们讨论 (OPT-zerosum)、另一种表述形式 $\max_{\mathbf{x}} \Gamma(\mathbf{x})$ 与经典最短路径网络阻断问题之间的联系 [Israeli 和 Wood，2002年，Smith and Song, 2020]。为便于说明这一点，我们考虑以下最短路径网络阻断问题：

$$\min_{\mathbf{x}\in\mathcal{X}} \quad \Big\{T(\mathbf{x}) = \max_{\tau\in\Omega} \quad U(\tau;\mathbf{x})\Big\}. \tag{OPT-shortest-path}$$

众所周知，上述最短路径网络阻断问题可以表述为混合整数线性规划，并且是 NP-困难的 [Israeli 和 Wood， 2002]。我们首先在引理 $\Gamma(\mathbf{x})$ 与 $T(\mathbf{x})$ 之间，针对任意 $\mathbf{x} \in \mathcal{X}$，给出上界。下文的引理 5 将证明这一点

引理 *5.* 对于 $x \in X$，令 $\tau^* = argmax_{\tau\in\Omega} U(\tau; x)$（即能带来最高对手效用的最佳轨迹）， $\Omega^* = \{\tau | U(\tau; x) = U(\tau^*; x)\}$（即所有具有相同最高效用的轨迹的集合），以及 $\alpha = \{U(\tau^*; x) - max_{\tau\in\Omega\setminus\Omega^*} U(\tau; x)\}$，则有：

$$|\Gamma(\boldsymbol{x}) - T(\boldsymbol{x})| \le \mu \log\left(|\Omega^*| + \frac{|\Omega\setminus\Omega^*|}{\exp(\alpha/\mu)}\right).$$

因此，极限$_{\mu\to 0} \Gamma(\boldsymbol{x}) = U(\tau^*)$。

证明。我们可以写成：

$$\begin{aligned}
\Gamma(\mathbf{x}) &= \mu \log\left(\sum_{\tau\in\Omega} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)\right) \\
&= \mu \log\left(|\Omega^*| \exp\left(\frac{U(\tau^*;\mathbf{x})}{\mu}\right) + \sum_{\tau\in\Omega\setminus\Omega^*} \exp\left(\frac{U(\tau;\mathbf{x})}{\mu}\right)\right) \\
&\le \mu \log\left(|\Omega^*| \exp\left(\frac{U(\tau^*;\mathbf{x})}{\mu}\right) + (|\Omega\setminus\Omega^*|) \exp\left(\frac{U(\tau^*;\mathbf{x}) - \alpha}{\mu}\right)\right) \\
&= U(\tau^*;\mathbf{x}) + \mu \log\left(|\Omega^*| + (|\Omega\setminus\Omega^*|) \exp\left(\frac{-\alpha}{\mu}\right)\right)
\end{aligned} \tag{43}$$

此外，我们有 $\Gamma(\mathbf{x}) \ge U(\tau^*;\mathbf{x})$. 将其与 (43) 结合，我们得到所需的不等式。极限 $\lim_{\mu\to 0} \Gamma(\mathbf{x}) = U(\tau^*)$ 只是由这个等式直接得到的结果，从而完成了我们的证明。 □

结合引理 5 与命题 1，我们得到 $|\mathcal{E}^f(\mathbf{x}) - \Gamma(\mathbf{x})|$

引理 6。 令 $L^* = \max_{\tau\in\Omega,\ x\in\mathcal{X}} |U(\tau;\ \boldsymbol{x})|$，我们有

$$|\mathcal{E}^f(\boldsymbol{x}) - \Gamma(\boldsymbol{x})| \le \frac{L^* + 1}{1 + \frac{|\Omega^*|}{|\Omega\setminus\Omega^*|} \exp\left(\frac{\alpha}{\mu}\right)} + \mu \log\left(|\Omega^*| + \frac{|\Omega\setminus\Omega^*|}{\exp\left(\frac{\alpha}{\mu}\right)}\right)$$

现在，我们可以评估由以下替代公式 $\max_{\mathbf{x}} \Gamma(\mathbf{x})$以及零和博弈公式（OPT-zerosum）和（OPT-shortest-path）给出的解的质量。令 $\Gamma^* = \max_{\mathbf{x}} \Gamma(\mathbf{x})$、$\mathcal{E}^*$、$T^*$ 分别表示（OPT-zerosum）、（OPT-shortest-path）的最优值，并且 $\mathbf{x}$ 是以下问题的最优解：$\max_{\mathbf{x}} \Gamma(\mathbf{x})$。给定任意 $\mathbf{x} \in \mathcal{X}$，令：

$$\alpha(\mathbf{x}) = \max_{\tau \in \Omega} U(\tau; \mathbf{x}) - \max\{U(\tau; \mathbf{x}) | \ \tau \in \Omega,\ U(\tau; \mathbf{x}) < \max_{\tau \in \Omega} U(\tau; \mathbf{x})\}$$

直观地说，$\alpha(\mathbf{x})$ 表示对手选择次优轨迹而非最优轨迹时在效用上的对手损失。此外，令 $C(\mathbf{x})$ 表示 Ω 中最优路径的数量，即 $C(\mathbf{x}) = |\operatorname{argmax}_{\tau \in \Omega} U(\tau; \mathbf{x})|$。我们得到以下结果，它们将凸问题 $\max_{\mathbf{x}} \Gamma(\mathbf{x})$ 与两种基线方法（即经典最短路径网络阻断及其有界理性版本）之间的差距界定为 μ 的函数。这些结果表明，当 μ 趋于零时，$\max_{\mathbf{x}} \Gamma(\mathbf{x})$ 的最优值和最优解将分别收敛到 (OPT-shortest-path) 和 (OPT-zerosum) 的最优值和最优解。

命题10。令 $\boldsymbol{x}^* = argmax_{\boldsymbol{x}} \Gamma(\boldsymbol{x})$ 且

$$\begin{aligned} \kappa_1(\mu) &= \max_{\boldsymbol{x}} \left\{ \mu \log \left(|C(\boldsymbol{x}) + \frac{|\Omega| - |C(\boldsymbol{x})}{\exp\left(\frac{\alpha(\boldsymbol{x})}{\mu}\right)} \right) \right\} \\ \kappa_2(\mu) &= \kappa_1(\mu) + \max_{\boldsymbol{x}} \left\{ \mu \frac{L^* + 1}{1 + \frac{|C(\boldsymbol{x})}{|\Omega| - |C(\boldsymbol{x})} \exp\left(\frac{\alpha(\boldsymbol{x})}{\mu}\right)} \right\} \end{aligned} \tag{44}$$

以下结果成立

(i) $|\Gamma^* - T^*| \le \kappa_1(\mu)$，且 $|T(\boldsymbol{x}^*) - \max_{\boldsymbol{x}}\{T(\boldsymbol{x})\}| \le 2\kappa_1(\mu)$

(ii) $|\Gamma^* - \mathrm{E}^*| \le \kappa_2(\mu)$，且 $|\mathrm{E}^f(\boldsymbol{x}^*) - \max_{\boldsymbol{x}}\{\mathrm{E}^f(\boldsymbol{x})\}| \le 2\kappa_2(\mu)$

(iii) $\lim_{\mu \to 0} \kappa_1(\mu) = \kappa_2(\mu) = 0$

证明。对于 (i)，我们首先注意到 $\Gamma(\mathbf{x}) \le T(\mathbf{x})$ 对任意 $\mathbf{x} \in \mathcal{X}$。因此 $\Gamma^* \le T^*$。令 $\mathbf{x}$ 为 (OPT-shortest-path) 的最优解，我们写出：

$$\begin{aligned} |\Gamma^* - T^*| = T^* - \Gamma^* &= T(\overline{\mathbf{x}}) - \max_{\mathbf{x}} \Gamma(\mathbf{x}) \\ &\le T(\overline{\mathbf{x}}) - \Gamma(\overline{\mathbf{x}}) \\ &\overset{(a)}{\le} \kappa_1(\mu). \end{aligned}$$

其中 (a) 是由命题 1得出的。此外，考虑间隙 $|T(\mathbf{x}^*) - \max_{\mathbf{x}} T(\mathbf{x})|$，我们得到以下一系列不等式

$$\begin{aligned} |T(\mathbf{x}^*) - \max_{\mathbf{x}}\{T(\mathbf{x})\}| &\le |T(\mathbf{x}^*) - \max_{\mathbf{x}}\{\Gamma(\mathbf{x})\}| + |\Gamma^* - T^*| \\ &= |T(\mathbf{x}^*) - \Gamma(\mathbf{x}^*)| + |\Gamma^* - T^*| \\ &\le 2\kappa_1(\mu). \end{aligned}$$

对于 (ii)，设 $\widehat{\mathbf{x}}$ 是 (OPT-zerosum) 的一个最优解。类似地，我们可以写出

$$\begin{aligned} |\Gamma^* - \mathcal{E}^*| = \mathcal{E}^* - \Gamma^* &= \mathcal{E}^f(\widehat{\mathbf{x}}) - \max_{\mathbf{x}} \Gamma(\mathbf{x}) \\ &\le \mathcal{E}^f(\widehat{\mathbf{x}}) - \Gamma(\widehat{\mathbf{x}}) \\ &\overset{(b)}{\le} \kappa_2(\mu). \end{aligned} \tag{45}$$

	节点数（|S|）				
方法	20	40	60	80	100
基线方法	99.95 ± 0.00	99.88 ± 0.07	99.74 ± 0.18	99.69 ± 0.23	99.07 ± 0.52

表 2. 使用我们处理指数数量路径的方法所获得的最优目标值，与基线方法获得的最优解目标值之比（百分比）。我们使用 $p = 0.8$，$\mu = 2$。每种设置下随机生成 20 个数据集，并报告均值和标准差。

其中（b）这由引理 6 得出。此外，考虑差距 $|\mathcal{E}^f(\mathbf{x}^*) - \max_{\mathbf{x}} \mathcal{E}^f(\mathbf{x})|$，我们写作

$$\begin{aligned}|\mathcal{E}^f(\mathbf{x}^*) - \max_{\mathbf{x}}\{\mathcal{E}^f(\mathbf{x})\}| &\le |\mathcal{E}^f(\mathbf{x}^*) - \max_{\mathbf{x}}\{\Gamma(\mathbf{x})\}| + |\Gamma^* - \mathcal{E}^*| \\ &= |\mathcal{E}^f(\mathbf{x}^*) - \Gamma(\mathbf{x}^*)| + |\Gamma^* - \mathcal{E}^*| \\ &\le 2\kappa_2(\mu).\end{aligned}$$

显然，极限 $\lim_{\mu\to 0} \kappa_1(\mu) = \kappa_2(\mu) = 0$ 均成立，由此完成证明。 □

事实上，我们可以通过调整 μ 来控制对手的理性程度，即当 $\mu \to 0$ 时，对手会更加理性（若 $\mu = 0$ 则完全理性），而当 $\mu \to \infty$ 时则会变得不理性。

C.2 零和博弈的实验结果

注意，由于对数和替代形式$\min_{\mathbf{x}}\{\Gamma(\mathbf{x})\}$ 是一个凸问题，因此基线方法以及在我们提出的方法基础上使用梯度下降来处理第 4 节中指数数量的路径，都能够将其求解至最优。然而，从表 2 可以看出，随着图规模 $|\mathcal{S}|$ 增大，基线方法的表现略有下降，这是因为基线方法中的目标函数通过采样进行估计，而且路径数量会随着 $|\mathcal{S}|$呈指数级增长。

随着对手的理性程度提高（对应于 μ 的降低），我们预期最优防御者收益会下降，因为对手能够以更高的概率选择最优路径。此外，对于零和博弈，根据命题 10 中的保证，我们可以断言，最优解将收敛于（OPT-shortest-path）的解。图1展示了收益下降和收敛现象。

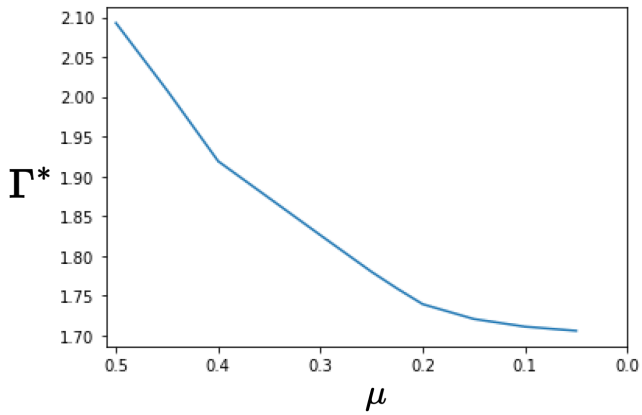


图 1. 对于固定的合成数据集（$|S| = 50$，p=0.8），最优值 Γ^* 随 μ 的变化。