arXiv:2301.03302v1 [eess.SY] 9 Jan 2023

动态弹性多智能体系统中考虑簇形成网络效应的滚动时域博弈

Yurid Nugraha [a]、Ahmet Cetinkaya [b]、Tomohisa Hayakawa [a]、Hideaki Ishii [c]、Quanyan Zhu [d]

[a] *Department of Systems and Control Engineering, Tokyo Institute of Technology, Tokyo 152-8552, Japan*

[b] *Department of Functional Control Systems, Shibaura Institute of Technology, Tokyo, 135-8548, Japa*
n[c] *Department of Computer Science, Tokyo Insitute of Technology, Yokohama 226-8502, Japan*
[d] *Departm*

A
ent of Electrical and Computer Engineering, New York University, Brooklyn NY, 11201, *US*

摘要

针对多智能体一致性场景下的弹性图，建立了一个双人博弈论问题。攻击者可以通过发射干扰信号禁用网络中的部分边，目的是将智能体划分为多个簇；作为回应，防御者则通过提高通信信号的传输功率来恢复部分边。具体而言，我们考虑攻击者与防御者之间的重复博弈，并基于同时考虑智能体状态和簇规模（称为网络效应）的效用函数，以滚动时域方式推导两名参与者的最优策略。每个离散时间步中，参与者用于传输信号的行动受到能量约束，但对攻击者的约束较为宽松。本文推导了智能体一致性的必要条件和充分条件，这些条件受能量约束影响。此外，还刻画了遭受攻击和边恢复后，智能体在无限时间时形成的簇数。文中给出了仿真结果，以展示参与者的行动对簇形成的影响，并说明不同的时域参数下参与者的表现。

Key words: 多智能体系统、网络安全、博弈论、一致性、簇形成、网络效应/网络外部性

1 引言

大型网络化系统在电网和交通系统等关键基础设施的多个领域中迅速得到应用。这类系统可视为多智能体系统，其中多个能够做出局部决策的智能体通过网络进行交互并交换信息，以实现共同目标 [2]。无线通信在网络功能实现中发挥着重要作用，但也容易受到恶意对手发起的网络攻击 [11, 25]。

文献 [3, 5, 28] 研究了多智能体系统一致性问题中的干扰攻击。攻击者与其他保护网络的参与者之间的非合作博弈被广泛用于分析安全问题，包括干扰攻击 [12, 17] 和注入攻击 [18, 24, 26]。

在干扰攻击的建模中，很自然地会考虑干扰者/攻击者受到能量约束，因此，如果其未连接到能量源，就不可能始终攻击网络的所有通信链路 [4,5]。在博弈论方法中，这一约束对于刻画参与者的策略行为至关重要 [17]。

当网络中的链路遭到攻击时，智能体可能会与其他智能体断开连接，从而形成若干由相互连接的智能体组成的群组或簇。

Email addresses: yurid@dsl.sc.e.titech.ac.jp (Yurid Nugraha), ahmet@shibaura-it.ac.jp (AhmetCetinkaya), hayakawa@sc.e.titech.ac.jp (Tomohisa Hayakawa), ishii@c.titech.ac.jp (Hideaki Ishii), quanyan.zhu@nyu.edu (Quanyan Zhu).

work [13] 提出了网络效应/网络外部性的概念，指某一簇中智能体的效用取决于属于该特定簇的其他智能体的数量。这一概念已被用于分析智能体在社交网络和计算机网络等网络中的分组，如 [10,16]中所述。

滚动时域控制已被用于处理具有不确定性的系统。在网络化控制的背景下也对其进行了研究 [15, 30], ，其中可能存在与网络中智能体之间通信相关的额外不确定性。在非合作安全博弈设定下也讨论了滚动时域方法 [34, 35], ，其中时域长度会影响系统的韧性。滚动时域方法还被用于处理系统中的约束，例如，具有避障约束的智能体 [14, 27]。

本文考虑一个双参与者博弈设定下的安全问题：攻击者通过攻击通信链路，试图破坏智能体之间的通信；防御者则尝试恢复部分遭到攻击的链路。我们基于 [6, 20], 对该问题进行建模，利用图连通性刻画博弈及参与者的策略。本文中的博弈在多智能体一致性的背景下，沿离散时间反复进行。

由于这些持续不断的攻击与恢复，在一致性协议下，网络中的智能体会形成不同的簇，各簇的智能体状态也各不相同。例如， [1, 7, 29],研究了多智能体系统中的簇形成，其中某些智能体之间可能存在敌对关系。本文从不同的角度出发，基于博弈论建模探讨聚类问题。具体而言，博弈参与者考虑网络效应/网络外部性 [13] ，以在智能体之间形成簇。他们的效用取决于网络如何被划分为若干智能体组，也取决于参与者的行动如何影响各时刻智能体的状态。在这一设定下，簇的数量和规模受攻击强度的影响：攻击者越强，越有能力将智能体分隔成数量更多、规模更小的簇，反之亦然。

在弹性网络设定中，通常会有一位网络管理者知晓即将发生的攻击，因为智能体始终尝试与邻居智能体通信，因此一旦发现某些邻居不再发送任何信号，便能迅速察觉。随后，网络管理者会设法制定防御计划，以便快速从此类攻击中恢复，并抵御后续攻击。

从攻击者的角度来看，攻击者通常也知道网络中哪些边最脆弱，以及网络管理者的实力如何例如，管理者剩余的资源。因此，我们认为这种序贯模型可以应用于多种现实场景。

本文的主要贡献是引入一种随时间反复进行的重复博弈，用以建模网络安全背景下攻击者与防御者之间的决策过程。接下来，自然需要探究此类博弈如何影响网络以及智能体的状态演化。鉴于一致性协议的特征简单，我们将其作为研究对象；在没有攻击的情况下，所有智能体都应收敛。更具体地说，与 [6, 20], 相比，我们的贡献有三点：(i) 为攻击者的干扰信号强度引入了更多选项；(ii) 博弈包含多个攻击-恢复动作，因此策略更为复杂；(iii) 我们为参与者考虑了滚动时域方法，使他们能够在获得系统状态的新信息后调整策略。

更具体地说，攻击者现在可以通过更强的攻击信号禁用链路，使防御者无法恢复这些链路（决定哪些边将受到更强攻击信号的攻击，与决定哪些边将受到普通攻击信号的攻击同时进行）；这一特点的灵感来自 [32, 33]。实际中，攻击者可以发射更强的干扰信号，这需要消耗更多资源，并导致信干噪比（SINR）大幅降低，因此防御者无法凭借有限的恢复能力恢复这些链路上的通信。另一方面，我们考虑由多个部分组成的博弈；参与者在任何时刻决定策略时，都需要考虑未来效用和能量约束。与单步情形相比，这种设定使参与者能够考虑得更长远，并优先争取长期收益。随着时间推移，参与者会根据滚动时域方法重新计算策略，并可覆盖原有策略。 [19], 讨论了一种不采用滚动时域的相关建模，其中参与者无法更改早先确定的策略。

本文组织如下。第 2 节介绍攻击—恢复序列、智能体之间的簇形成以及参与者的能耗模型框架。第 3 节讨论重复博弈滚动时域方法中的博弈效用函数，而第4节刻画博弈结构。第 5 节分析智能体之间一致性的一些条件，这些条件与底层图的参数和参与者的能量约束有关。随后，我们在第 6 节讨论未达成一致性时智能体的簇形成。第 7 节讨论特定条件下博弈的均衡刻画。我们

随后在第8节给出关于一致性和簇形成的数值示例，并在第 9 节总结全文。本文的会议版本发表于 [21], ，其中我们考虑了参与者更新其策略频率受到更多限制的情形。

本文使用的符号基本上是标准的。我们用 $|\cdot|$ 表示集合的基数。向下取整函数和向上取整函数分别记为 $\lfloor\cdot\rfloor$ 和 $\lceil\cdot\rceil$。正整数集和非负整数集分别记为 $\mathbb{N}$ 和 $\mathbb{N}_0$。

2 一致性动态下多智能体系统的攻击/恢复刻画

我们考虑一个由 n 个智能体组成的多智能体系统，这些智能体在遭受干扰攻击时以离散时间相互通信。智能体通过在通信网络上彼此交互，力求收敛到一致性状态。正常运行时的网络拓扑由一个无向连通图 $\mathcal{G} = (\mathcal{V}, \mathcal{E})$给出。该图由顶点集 $\mathcal{V}$和边集 $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$组成，分别表示智能体和通信链路。连通图 $\mathcal{G}$ 的边连通度 [2] 记为 λ。

每个智能体 i 在时间 $k \in \mathbb{N}_0$ 的标量状态 $x_i[k]$ 遵循以下离散时间更新规则：

$$x_i[k+1] = x_i[k] + u_i[k], \quad x[0] = x_0, \tag{1}$$

其中， $u_i[k]$ 表示施加于智能体 i的控制输入。我们假设 $u_i[k]$ 由智能体 i 与其邻居智能体之间状态差的加权和构成，这种形式常用于例如 [8], ，其定义如下：

$$u_i[k] = \sum_{j \in \mathcal{N}_i[k]} a_{ij}(x_j[k] - x_i[k]), \tag{2}$$

其中， $\mathcal{N}_i[k]$ 表示在时间 k能够与智能体 i 通信的智能体集合， a_{ij} 表示边（i， j） $\in \mathcal{E}$ 的权重，使得 $\Sigma_{j=1,\ j\neq i}^{n} a_{ij} < 1$， $i \in \mathcal{V}$ ，以确保智能体在没有任何攻击的情况下实现一致性。

我们假设，对某条边发动的干扰攻击会影响由该受攻击边连接的两个智能体之间的通信。因此，集合 $\mathcal{N}_i[k]$ 可能发生变化，最终的通信拓扑在时间 k 可能变得不连通。这类干扰攻击表示为从 $\mathcal{G}$ 中移除边。另一方面，系统中有一名防御者，可能有能力维持智能体之间的通信，例如要求智能体发送更强的通信信号，以克服干扰信号。这一行动表示为重建部分受攻击边。

基于这一系列攻击与恢复，我们根据网络中的通信链路，将攻击-恢复过程刻画为攻击者与防御者之间的双人博弈。换言之，如果一组智能体能够从攻击者造成的损害中恢复，则刻画该网络化系统的图具有弹性。然而，在某些情况下，如果干扰信号足够强，使防御者无法恢复，该图的弹性水平可能会降低。需要注意的是，为了实现一致性，智能体不必始终保持连接。

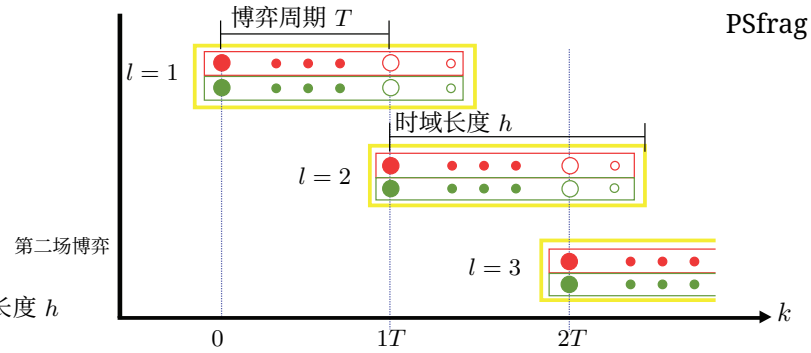
本文考虑攻击者拥有两种不同强度的干扰信号：强干扰信号和常规干扰信号。防御者只能恢复遭到常规强度攻击的边。在以下小节中，我们首先描述攻击与恢复的序列，并说明需要对参与者的能量和计算能力施加的一些约束，以及问题目标的构建方式。

2.1 攻击-恢复序列

在我们的设定中，在每个离散时间 k，参与者（攻击者和防御者）分两个阶段决定攻击/恢复某些边，先由攻击者行动，再由防御者行动。具体而言，在时间 k ，攻击者使用常规干扰信号删除边 $\mathcal{E}_k^{\mathrm{A}} \subseteq \mathcal{E}$ ，并使用强干扰信号删除边 $\overline{\mathcal{E}}_k^{\mathrm{A}} \subseteq \mathcal{E}$ ，从而攻击 $\mathcal{G}$ ，其强度分别为 $\mathcal{E}_k^{\mathrm{A}} \cap \overline{\mathcal{E}}_k^{\mathrm{A}} = \emptyset$；而防御者恢复 $\mathcal{E}_k^{\mathrm{D}} \subseteq \mathcal{E}_k^{\mathrm{A}}$。如前所述，防御者无法恢复遭到强干扰信号攻击的边，即 $\mathcal{E}_k^{\mathrm{D}} \cap \overline{\mathcal{E}}_k^{\mathrm{A}} = \emptyset$。经过攻击和随后的恢复，网络在时间 k 从 $\mathcal{G}$ 变为 $\mathcal{G}_k^{\mathrm{A}} := (\mathcal{V}, \mathcal{E} \setminus (\mathcal{E}_k^{\mathrm{A}} \cup \overline{\mathcal{E}}_k^{\mathrm{A}}))$，并进一步变为 $\mathcal{G}_k^{\mathrm{D}} := (\mathcal{V}, (\mathcal{E} \setminus (\mathcal{E}_k^{\mathrm{A}} \cup \overline{\mathcal{E}}_k^{\mathrm{A}})) \cup \mathcal{E}_k^{\mathrm{D}})$。随后，智能体基于由此得到的图 $\mathcal{G}_k^{\mathrm{D}}$ 与其邻居 $\mathcal{N}_i[k]$ 通信。

在此博弈中，参与者试图就受攻击/恢复的边 $(\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}})$ 和 $\mathcal{E}_k^{\mathrm{D}}$选择最佳策略，以最大化各自的效用函数。这里，每经过 T 个时间步进行一轮博弈，第 l轮博弈的时域为 h 步，起始时间为（$l-1$）T，结束时间为（$l-1$）$T+h-1$，其中 $l \in \mathbb{N}$ 和$1 \leq T \leq h$。参与者以滚动时域的方式做出决策；在（$l-1$）T时为未来时间获得的最优策略，可能会在下一轮博弈开始、参与者于时间 lT 重新计算策略时被覆盖。图1展示了随时间推移的上述序列，其中包含 $h = 8$ 和 $T = 4$；实心圆表示已实施的策略，空心圆

Edge



PSfrag 替换

图1. 参与者采用滚动时域方法在离散时间 k 上进行博弈的示意图。

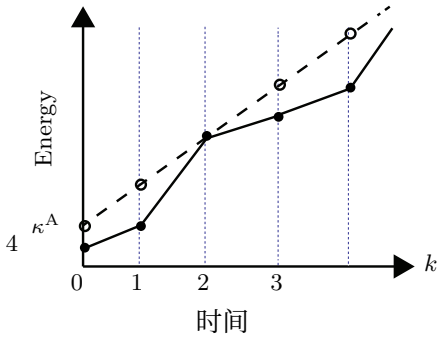


图2. 公式中考虑的攻击者能量约束。虚线表示可用于消耗的供给能量总量。表示参与者实际消耗能量的实心圆应位于虚线下方。

表示被舍弃的博弈策略。在此设定中，时域长度 h 表示计算能力，即参与者能够为多远的未来规划策略；而博弈周期$T \leq h$ 表示参与者的适应能力，即参与者在不更新的情况下应用已获得策略的时长（ T 越短，参与者的适应能力越强）。第4节将更详细地讨论滚动时域博弈结构。

2.2 能量约束

攻击者和防御者的行动受到其能源资源约束的影响。假设参与者获得的供给能量总量随时间线性增长；此外，参与者消耗的能量与攻击／恢复边的数量成正比。这里假设参与者初始分别拥有一定量的能量 κ^{A} 和κ^{D}，分别对应攻击者和防御者。此外，假设参与者能够无线地向阻碍／维持智能体间通信信号的设备供能，因此，每个离散时间步向这些设备供能的速率受常数值 ρ^{A} 和 ρ^{D} 限制。假设这些设备的电池容量无限，因此参与者可以分别以线性速率 ρ^{A} 或 ρ^{D}持续为其供能。

对于攻击者，对 $\overline{\mathcal{E}}_k^{\mathrm{A}}$ 实施强攻击时，每条边每单位时间消耗 $\overline{\beta}^{\mathrm{A}}$ >0能量；对 $\mathcal{E}_k^{\mathrm{A}}$实施普通攻击时，每条边消耗 $\beta^{\mathrm{A}} > 0$ 成本，其中 $\overline{\beta}^{\mathrm{A}} > \beta^{\mathrm{A}}$。攻击者使用的总能量受以下约束:

$$\sum_{m=0}^{k} (\overline{\beta}^{\mathrm{A}} |\overline{\mathcal{E}}_m^{\mathrm{A}}| + \beta^{\mathrm{A}} |\mathcal{E}_m^{\mathrm{A}}|) \leq \kappa^{\mathrm{A}} + \rho^{\mathrm{A}} k \tag{3}$$

对于任意时间 k，其中 $\kappa^{\mathrm{A}} \geq \rho^{\mathrm{A}} > 0$。这意味着攻击者消耗的总能量不能超过

由初始能量 κ^{A} 与截至时间 k 的供给能量 $\rho^{\mathrm{A}} k$ 之和所表示的可用能量。该能量约束限制了攻击者能够攻击的边数。注意，攻击者的可用能量在每个 k 增加 ρ^{A} 。条件 $\kappa^{\mathrm{A}} \geq \rho^{\mathrm{A}}$ 使攻击者在时间 $k = 0$ 至少拥有相同的攻击能力。

图2展示了攻击者的能量约束，其中斜率为 ρ^{A} 的虚线表示供给的总能量，实心圆表示已消耗的总能量。一个临界情况是 $\beta^{\mathrm{A}} < \rho^{\mathrm{A}}$，因为攻击者可能在所有时刻至少攻击一条边。这将影响智能体的一致性和簇形成，稍后将对此进行讨论。

防御者的能量约束与以下形式类似 (3):

$$\sum_{m=0}^{k} \beta^{\mathrm{D}} |\mathcal{E}_m^{\mathrm{D}}| \leq \kappa^{\mathrm{D}} + \rho^{\mathrm{D}} k, \tag{4}$$

其中 $\kappa^{\mathrm{D}} \geq \rho^{\mathrm{D}} > 0$ 且 $\beta^{\mathrm{D}} > 0$。注意，左侧只有一项，因为智能体只有一种恢复信号。

3 考虑簇形成和智能体组索引的效用函数

在我们的博弈设定中，攻击者试图使图不连通，从而将智能体分成若干簇。在这里，我们介绍一些与智能体分组/聚类相关的概念。在给定的子图 $\mathcal{G}' = (\mathcal{V}, \mathcal{E}')$中，智能体可能被划分为 $\pi(\mathcal{G}')$ 个群组，其中群组 $\mathcal{V}'_1$、$\mathcal{V}'_2$、…、$\mathcal{V}'_{\pi(\mathcal{G}')}$ 是 $\mathcal{V}$ 的一个划分，且 $\cup_{p=1}^{\pi(\mathcal{G}')} \mathcal{V}'_p = \mathcal{V}$ 和 $\mathcal{V}'_p \cap \mathcal{V}'_q = \emptyset$，如果 $p \neq q$。不同群组之间不存在相连的边，即$e_{i',j'} \notin \mathcal{E}'$、$\forall i' \in \mathcal{V}'_p$、$j' \in \mathcal{V}'_q$。我们还将无限时间时处于相同状态的每个智能体子集称为一个簇——

簇，即 $\lim_{k\to\infty}(x_i[k]-x_j[k])=0$ 意味着智能体 i 和 j 属于同一个簇。PSfrag 替换 项

在所考虑的博弈中，攻击者和防御者都关注每个组中的智能体数量。具体而言，我们遵循网络效应/网络外部性 [13],的概念，即某个组中智能体的效用取决于属于该特定组的其他智能体数量。在这个博弈中，攻击者希望隔离智能体，使每个组中的智能体更少；而防御者则希望尽可能多的智能体处于同一组中。然后，我们用函数 $c(\cdot)$ 表示图 $\mathcal{G}'$ 中的分组程度，并将其称为智能体组索引，定义如下：

$$c(\mathcal{G}') := \sum_{p=1}^{\overline{n}(\mathcal{G}')} |\mathcal{V}'_p|^2 - |\mathcal{V}|^2 \quad (\leq 0). \tag{5}$$

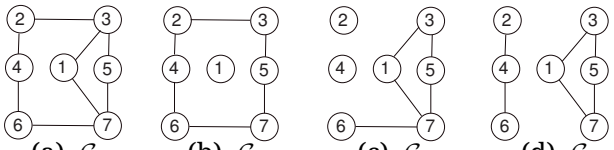
如果 $\mathcal{G}'$ 连通，则 $c(\mathcal{G}')$ 的值为 0，因为此时只有一个组（即 $\overline{n}(\mathcal{G}')=1$）。$c(\mathcal{G}')$ 的值越大（越接近 0），意味着图$\mathcal{G}'$中的组越少，和/或每个组中的智能体越多。图3展示了一些图的智能体组索引。有趣的是，尽管$\mathcal{G}_{\mathrm{C}}$ 的组更多，$c(\mathcal{G}_{\mathrm{D}})$ 仍小于 $c(\mathcal{G}_{\mathrm{C}})$。这是因为，与 $\mathcal{G}_{\mathrm{D}}$的情况相比，$\mathcal{G}_{\mathrm{C}}$ 中最大的簇由更多智能体构成。因此，对于试图减少单个簇中智能体数量的攻击者而言，$\mathcal{G}_{\mathrm{D}}$ 优于 $\mathcal{G}_{\mathrm{C}}$。

在我们的问题设定中，参与者在发动攻击/恢复时，也会考虑其行动对智能体状态的影响。例如，攻击者可能希望将状态值差异较大的智能体分到不同组中。我们将智能体的状态差异 z_k 定义为

$$z_k(\overline{\mathcal{E}}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{A}}, \mathcal{E}_k^{\mathrm{D}}) := x^{\mathrm{T}}[k+1] L_{\mathrm{c}} x[k+1], \tag{6}$$

其中，为简单起见，L_{c}是具有 n 个智能体的完全图的拉普拉斯矩阵。也就是说，(6)表示所有智能体对的状态差平方和。这意味着任意一对智能体之间的所有状态差异都具有相同的权重，因此参与者不会优先考虑智能体之间的任何连接。

遭受攻击和恢复的边（$\overline{\mathcal{E}}_k^{\mathrm{A}}$、$\mathcal{E}_k^{\mathrm{A}}$、$\mathcal{E}_k^{\mathrm{D}}$）将按照（1）和（2）影响 $x[k+1]$，进而影响 z_k的值。请注意，即使在攻击下某些智能体与其他智能体断开连接，z_k 的值也会随时间 [2] 单调不增。对智能体状态差异的这种平方和刻画很常见，与我们先前针对连续时间设定的工作 [19] 基本相同；在此，我们将其扩展为适用于离散时间



(a) $\mathcal{G}_{\mathrm{A}}$ (b) $\mathcal{G}_{\mathrm{B}}$ (c) $\mathcal{G}_{\mathrm{C}}$ (d) $\mathcal{G}_{\mathrm{D}}$

图3. 图及其智能体组指标：(a) $c(\mathcal{G}_{\mathrm{A}})=0$，(b) $c(\mathcal{G}_{\mathrm{B}})=-12$，(c) $c(\mathcal{G}_{\mathrm{C}})=-22$，以及 (d) $c(\mathcal{G}_{\mathrm{D}})=-24$。注意，即使群组数量更多，$c(\mathcal{G}_{\mathrm{C}})$ 仍大于 $c(\mathcal{G}_{\mathrm{D}})$。

通过考虑提前一个时间步的状态进行设置$k+1$。

现在，我们将式 (5) 和式 (6) 中的两个度量结合起来，以零和方式构造该博弈的效用函数。具体而言，对于从时间 $k=(l-1)T$ 开始的第 l 个博弈，攻击者和防御者的效用函数考虑智能体组索引 $c(\cdot)$，以及从时间 $(l-1)T$ 到 $(l-1)T+h-1$、时域长度为 h 的区间内智能体状态的差异 z_k。对于权重 a、$b\geq 0$，第 l 个博弈中攻击者的效用 U_l^{A} 和防御者的效用 U_l^{D} 分别定义为

$$U_l^{\mathrm{A}} := \sum_{k=(l-1)T}^{(l-1)T+h-1} (a z_k - b c(\mathcal{G}_k^{\mathrm{D}})), \tag{7}$$

$$U_l^{\mathrm{D}} := -U_l^{\mathrm{A}}. \tag{8}$$

在我们的设定中，双方参与者都试图在每场博弈开始时最大化各自的效用 l。a和 b 的取值代表参与者对长期智能体聚类或短期智能体分组的偏好。a 的值越高，表示参与者越倾向于关注智能体状态及后续的簇形成；而 b 的值越高，则表示他们越倾向于关注智能体分组。我们假设双方参与者都了解底层拓扑 $\mathcal{G}$ 以及所有智能体的状态 $x_i[k]$。

4 滚动时域博弈结构

我们希望找到第 3 节所述博弈的子博弈完美均衡 [9] 。为此，我们将博弈划分为若干子博弈／决策点。子博弈完美均衡必须在每个子博弈中都是均衡。每位参与者的最优策略通过逆向归纳法求得，即从最小的子博弈开始寻找均衡。当参与者的策略产生相同效用时，就会触发平局判定条件。在这种情况下，我们假设参与者会选择节省能量，少攻击／恢复一些边；但如果他们有足够的能量在后续每一步中攻击／恢复所有边，则会选择攻击／恢复更多边。

由于滚动时域方法的性质，

从第 l次博弈中获得的策略，即受攻击边和恢复边，仅从时间（$l-1$）T至$lT-1$开始应用。具体而言，在时间（$l-1$）T至（$l-1$）$T+h-1$的第 l次博弈中，双方参与者的策略表示为（（$\overline{\mathcal{E}}_l^{\mathrm{A}}$,1,$\mathcal{E}_l^{\mathrm{A}}$,1,$\mathcal{E}_l^{\mathrm{D}}$,1）.....，（$\overline{\mathcal{E}}_l^{\mathrm{A}}$,$_h$,$\mathcal{E}_l^{\mathrm{A}}$,$_h$,$\mathcal{E}_l^{\mathrm{D}}$,$_h$）），其中（$\overline{\mathcal{E}}_{l\,\alpha}^{\mathrm{A}}$,$\mathcal{E}_{l}^{\mathrm{A}}$,$_\alpha$,$\mathcal{E}_{l}^{\mathrm{D}}$,$_\alpha$）表示在具有 $\alpha\in\{1,\dots,h\}$的第 l次博弈中第α步的策略。请注意，此处用两个下标表示策略，分别代表沿时间轴的博弈序号和步序号。在上述策略集合中，仅应用（（$\overline{\mathcal{E}}_l^{\mathrm{A}}$,1,$\mathcal{E}_l^{\mathrm{A}}$,1,$\mathcal{E}_l^{\mathrm{D}}$,1）.....，（$\overline{\mathcal{E}}_l^{\mathrm{A}}$,$_T$,$\mathcal{E}_l^{\mathrm{A}}$,$_T$,$\mathcal{E}_l^{\mathrm{D}}$,$_T$））。回想一下，$h$ 被取为大于或等于T。因此，对于时间（$l-1$）T至 $lT-1$的第 l次博弈，所应用的策略写作（（$\overline{\mathcal{E}}^{\mathrm{A}}$（$_{l-1}$）$_T$,$\mathcal{E}^{\mathrm{A}}_{(l-1)T}$,$\mathcal{E}^{\mathrm{D}}_{(l-1)T}$）.....，（$\overline{\mathcal{E}}^{\mathrm{A}}_{lT-1}$,$\mathcal{E}^{\mathrm{A}}_{lT-1}$,$\mathcal{E}^{\mathrm{D}}_{lT-1}$））：=（（$\overline{\mathcal{E}}_l^{\mathrm{A}}$,1,$\mathcal{E}_l^{\mathrm{A}}$,1,$\mathcal{E}_l^{\mathrm{D}}$,1）.....，（$\overline{\mathcal{E}}_l^{\mathrm{A}}$,$_T$,$\mathcal{E}_l^{\mathrm{A}}$,$_T$,$\mathcal{E}_l^{\mathrm{D}}$,$_T$））。

我们通过一个 $h=2$ and $T=1$ or 2 的示例，探讨如何找到最优边。在这种情况下，对于时间上第 l 次博弈（$l-1$）T 和（$l-1$）$T+1$，参与者的最优策略为

$$\mathcal{E}^{\mathrm{D}*}_{l,2}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,2},\mathcal{E}^{\mathrm{A}}_{l,2})\in\arg\max_{\mathcal{E}^{\mathrm{D}}_{l,2}} U^{\mathrm{D}}_{l,2},\tag{9}$$

$$(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1}),\mathcal{E}^{\mathrm{A}*}_{l,2}(\mathcal{E}^{\mathrm{D}}_{l,1}))\in\arg\max_{(\overline{\mathcal{E}}^{\mathrm{A}}_{l,2},\mathcal{E}^{\mathrm{A}}_{l,2})} U^{\mathrm{A}}_{l,2},\tag{10}$$

$$\mathcal{E}^{\mathrm{D}*}_{l,1}(\overline{\mathcal{E}}^{\mathrm{A}}_{l,1},\mathcal{E}^{\mathrm{A}}_{l,1})\in\arg\max_{\mathcal{E}^{\mathrm{D}}_{l,1}} U^{\mathrm{D}}_{l},\tag{11}$$

$$(\overline{\mathcal{E}}^{\mathrm{A}*}_{l,1},\mathcal{E}^{\mathrm{A}*}_{l,1})\in\arg\max_{(\overline{\mathcal{E}}^{\mathrm{A}}_{l,1},\mathcal{E}^{\mathrm{A}}_{l,1})} U^{\mathrm{A}}_{l},\tag{12}$$

其中，U_l^{A}、$_\alpha$ 和 U_l^{D}、$_\alpha$ 分别定义为 U_l^{A} 和 U_l^{D} 的组成部分，它们是从第 α 步计算到第 l 次博弈的最后一步（第 h 步）得出的，即 UAl、$_\alpha=-U_l^{\mathrm{D}}$、$_\alpha$:= $\sum^{(l-1)T+h-1}$ $_{(l-1)T+\alpha-1}$($az_k-bc(\mathcal{G}_k^{\mathrm{D}})$)。在这种 $h=2$ 情况下，函数 U_l^{A},2 和 U_l^{D},2 仅基于 $k=(l-1)T+1$ 处的 az_k 和 $b\mathcal{G}_k^{\mathrm{D}}$ 值。注意，为了求得（$\overline{\mathcal{E}}^{\mathrm{A}*}_{l\,1}$，，$\mathcal{E}^{\mathrm{A}*}_{l\,1}$，），需要预先得到 $\mathcal{E}^{\mathrm{D}*}_{l\,1}$，（$\overline{\mathcal{E}}_l^{\mathrm{A}}$,1,$\mathcal{E}_l^{\mathrm{A}}$,1）。同样，为了求得 $\mathcal{E}^{\mathrm{D}*}_{l\,1}$，，需要预先得到（$\overline{\mathcal{E}}^{\mathrm{A}*}_{l\,2}$，（$\mathcal{E}_l^{\mathrm{D}}$,1）$\mathcal{E}^{\mathrm{A}*}_{l\,2}$，（$\mathcal{E}_l^{\mathrm{D}}$,1））。类似地，为了求得（$\overline{\mathcal{E}}^{\mathrm{A}*}_{l\,2}$，，$\mathcal{E}^{\mathrm{A}*}_{l\,2}$，），必须预先得到边 $\mathcal{E}^{\mathrm{D}*}_{l\,2}$，（$\overline{\mathcal{E}}^{\mathrm{A}}_{l\,2}$，，$\mathcal{E}^{\mathrm{A}}_{l}$,2）。注意，推导上述最优策略时须满足能量约束 (3) 和 (4)。

对于 $h>2$，参与者的最优策略由 $2h$ 个部分组成，类似于式（9）–（12）中的部分；一个时间步包含两个与参与者人数相对应的策略部分。参与者在第 l 场博弈 $l\in\mathbb{N}$ 的每个时间 $k=(l-1)T$ 求解这些策略。对于 $T=h$，参与者没有机会覆盖自己的策略，因此博弈不再具有滚动时域特性。

由于边的选择是有限的，我们将通过计算所有可能的组合来求出参与者的最优策略。根据上述指定的优化问题，参与者最多需要考察 $3^{|\mathcal{E}|}2^{|\mathcal{E}|}h$ 种受攻击边与恢复边的组合，以评估效用，因为他们还必须预见对手的响应。请注意，攻击者对一条边有三种可能的行动：不攻击、使用普通信号攻击，以及使用强信号攻击；而防御者只有两种行动：恢复或不恢复。由此可见，计算量会随着底层图中边的数量呈指数级增长。为了解决可扩展性问题，我们可以先找出更容易遭受攻击的边，即一旦受到攻击便会形成新群组的边，并仅将这些边纳入策略选择范围。

我们先前的工作 [19, 20] 研究了连续时间下的相关博弈，其中发起攻击/防御行动的时机也是决策变量的一部分。这一因素使问题的建模变得复杂，也增加了研究时域内博弈的难度。本文简化了时机问题，转而引入滚动时域特性。这样一来，参与者便能在更长的时间范围内考虑簇形成；当对手阻碍智能体之间达成一致性时，这一点尤为重要。

在这种滚动时域设置下，参与者需要了解对手在博弈前一步采取的行动，才能确定自己在博弈树中的位置，即自己正在参与哪个子博弈。例如，如果防御者不知道哪些边之前遭到了攻击，就无法正确计算效用函数 (8) 的值。

5 一致性分析

本节考察博弈结构和参与者的能量约束对一致性的影响。

我们首先分析参与者满足特定能量条件的情形。具体而言，如果某个参与者拥有足够的能量，能够从博弈的某一步开始攻击/恢复所有边，那么在之后的步骤中，该参与者将用尽所有能量，尽可能多地攻击/恢复边。下文将对此进行正式证明。为简单起见，我们将防御者在第 l 次博弈之前消耗的总能量记为 $\tilde{\beta}_l^{\mathrm{D}}$: $=\sum_{k=0}^{(l-1)T-1}\beta^{\mathrm{D}}|\mathcal{E}_k^{\mathrm{D}}|$，将防御者在第 l 次博弈的第 1 步至第 α 步可能消耗的总能量记为 $\hat{}\beta_\alpha^{\mathrm{D}}$: $=\sum_{m=1}^{\alpha}\beta^{\mathrm{D}}|\mathcal{E}_{l\,,\,m}^{\mathrm{D}}|$；这里稍微滥用一下记号，省略左侧的索引 l。类似地，对于攻击者，我们记为 $\tilde{\beta}_l^{\mathrm{A}}$: $=\sum_{m=0}^{(l-1)T-1}(\beta^{\mathrm{A}}|\mathcal{E}_m^{\mathrm{A}}|+\overline{\beta}^{\mathrm{A}}|\overline{\mathcal{E}}_m^{\mathrm{A}}|)$ 和 $\hat{}\beta_\alpha^{\mathrm{A}}$:=$\sum_{m=1}^{\alpha}$($\beta^{\mathrm{A}}|\mathcal{E}_{l\,,\,m}^{\mathrm{A}}|+\overline{\beta}^{\mathrm{A}}|\overline{\mathcal{E}}_{l\,,\,m}^{\mathrm{A}}|$)。

我们在引理 1（分别为引理 2）中讨论满足第 2 节所述特定能量条件时，防御者（分别为攻击者）在博弈第 α 步的最优策略。对防御者（分别为攻击者）最优策略的这一刻画，将有助于获得一致性不发生的必要（分别为充分）条件。

5.1 无法达成一致性的必要条件

本小节讨论智能体在无限长时间内彼此分离为不同簇、但未能达成整体一致性的必要条件。我们首先在引理1和引理2中讨论满足特定条件时，防御者在某些博弈中的最优策略。引理1阐述了在满足特定能量条件时，防御者在第 l 个博弈的任意一步采取的最优策略。

引理 1 若防御者在第 l 个博弈的第 α 步之前消耗的总能量 $\tilde{\beta}_l^{\mathrm{D}} + \hat{}\beta_{\hat{\alpha}-1}^{\mathrm{D}}$ 满足

$$\begin{aligned}&\tilde{\beta}_l^{\mathrm{D}} + \hat{\beta}_{\hat{\alpha}-1}^{\mathrm{D}}\\&\le \kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T + \hat{\alpha} - 1) - (h - \hat{\alpha} + 1)|\mathcal{E}|\beta^{\mathrm{D}},\end{aligned} \tag{13}$$

则对于所有 $\alpha \ge \hat{}\alpha$，$\mathcal{E}_{l,\ \alpha}^{\mathrm{D}*} = \mathcal{E}_{l,\ \alpha}^{\mathrm{A}*}$，即防御者将从第 α 步起恢复所有常规攻击的边。

证明。我们首先考察第 l 个博弈的最后一步（第 h 步）。由于该博弈的时域为 h 步，博弈的最后一步对应于最后一个决策点，此时参与者的策略无法影响同一博弈前几步中已经作出的决策。因此，在第 l 个博弈的最后一步，参与者不会通过减少攻击或恢复的边数来节省能量。

根据防御者的能量约束 (4)，显然，在任意时间 k，防御者恢复的边集合都有界，为 $|\mathcal{E}_k^{\mathrm{D}}| \le \frac{\kappa^{\mathrm{D}} + \rho^{\mathrm{D}} k - \sum_{m=0}^{k-1} \beta^{\mathrm{D}}|\mathcal{E}_m^{\mathrm{D}}|}{\beta^{\mathrm{D}}}$。因此，在第 h 步，恢复边满足 $|\mathcal{E}_{l,\ h}^{\mathrm{D}}| \le |\mathcal{E}_{l,\ h}^{\mathrm{D}\prime}|$ 其中 $|\mathcal{E}_{l,\ h}^{\mathrm{D}\prime}| := \min\{\lfloor \frac{\kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T + h - 1) - (\tilde{\beta}_l^{\mathrm{D}} + \hat{}\beta_{h-1}^{\mathrm{D}})}{\beta^{\mathrm{D}}} \rfloor, |\mathcal{E}_{l,\ h}^{\mathrm{A}*}|\}$。

根据哪些边通常受到攻击，防御者可能无法恢复最大数量的边 $|\mathcal{E}_{l,h}^{\mathrm{D}\prime}|$。如果在给定通常受到攻击的边 $\mathcal{E}_{l,h}^{\mathrm{A}}$，时，防御者的最优策略不是恢复 $|\mathcal{E}_{l,h}^{\mathrm{D}\prime}|$ 条边，即恢复较少的边，那么防御者将能够获得更高的效用 $U_{l,h}^{\mathrm{D}}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{D}}) > U\mathrm{D}_{l,h}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{D}\prime})$。然而，在 (13) 中，$\alpha = h$ 防御者拥有足够高的能量，因此效用变为 $U_{l,h}^{\mathrm{D}}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{D}}) > U_{l,h}^{\mathrm{D}}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}, \mathcal{E}_{l,h}^{\mathrm{A}}) = U\mathrm{D}_{l,h}(\overline{\mathcal{E}}_{l,h}^{\mathrm{A}}, \emptyset, \emptyset)$。由此可得只要防御者拥有足够的能量，就会在第 h 步恢复所有通常受到攻击的最优边，即 $\mathcal{E}_{l,h}^{\mathrm{D}*} = \mathcal{E}_{l,h}^{\mathrm{A}*}$。

接下来，我们研究这一性质对第 l 个博弈前面各步的影响。由于当 $\kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T + h - 1) - (\tilde{\beta}_l^{\mathrm{D}} + \hat{}\beta_{h-1}^{\mathrm{D}}) \ge \beta^{\mathrm{D}}|\mathcal{E}|$ 时，防御者在第 h 步的策略不受其在前一步（即第 $(h-1)$ 步）策略的影响，因此，防御者在第 $(h-1)$ 步无需为了节省能量而减少恢复的边数；这是因为它在第 h 步已经有足够的能量来恢复 $\mathcal{E}_{l,\ h}^{\mathrm{A}*}$。

现在，我们推导出，如果在第（$h-1$）步中 $\kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T + h - 2) - (\tilde{\beta}_l^{\mathrm{D}} + \hat{}\beta_{h-2}^{\mathrm{D}}) \ge 2\beta^{\mathrm{D}}|\mathcal{E}|$，那么防御者也会恢复 $\mathcal{E}_{l,\ h-1}^{\mathrm{D}*} = \mathcal{E}_{l,\ h-1}^{\mathrm{A}*}$。因此，要在步骤 $\alpha \ge \hat{}\alpha$ 恢复所有受攻击边，只需防御者的能量满足（13），使得 $\kappa^{\mathrm{D}} + \rho^{\mathrm{D}}((l-1)T + \alpha - 1) \ge \tilde{\beta}_l^{\mathrm{D}} + \hat{}\beta_{\alpha-1}^{\mathrm{D}} + \beta^{\mathrm{D}}|\mathcal{E}|$，即在防御者恢复所有边时，能量约束（4）的最坏情况始终在 $\alpha \ge \hat{}\alpha$ 时得到满足。□

从上述证明中可以看出，即使满足（13），如果防御者的策略仍是不恢复所有常规攻击的边，即 $\mathcal{E}_{l,\alpha}^{\mathrm{A}} = \hat{}\mathcal{E}^{\mathrm{A}} \ne \mathcal{E}_{l,\alpha}^{\mathrm{D}}$，那么攻击者一开始就不会攻击 $\hat{}\mathcal{E}^{\mathrm{A}}$ 这一组边。这是因为攻击 $\hat{}\mathcal{E}^{\mathrm{A}}$（并考虑 $\mathcal{E}_{l,\alpha}^{\mathrm{D}} \ne \hat{}\mathcal{E}^{\mathrm{A}}$）后，攻击者在步骤 $\alpha \ge \hat{}\alpha$ 的效用变为 $U\mathrm{A}_{l,\alpha}(\cdot, \hat{}\mathcal{E}^{\mathrm{A}}, \mathcal{E}_{l,\ \alpha}^{\mathrm{D}} \ne \hat{}\mathcal{E}^{\mathrm{A}}) < U_{l,\alpha}^{\mathrm{A}}(\cdot, \emptyset, \emptyset)$，因为 $U_{l,\alpha}^{\mathrm{D}}(\cdot, \hat{}\mathcal{E}^{\mathrm{A}}, \mathcal{E}_{l,\alpha}^{\mathrm{D}} \ne \hat{}\mathcal{E}^{\mathrm{A}}) > U\mathrm{D}_{l,\alpha}(\cdot, \emptyset, \emptyset) = U\mathrm{D}_{l,\alpha}(\cdot, \hat{}\mathcal{E}^{\mathrm{A}}, \hat{}\mathcal{E}^{\mathrm{A}})$ 且 $U_l^{\mathrm{D}} = -U_l^{\mathrm{A}}$。

我们还指出，为了得出防御者的相同最优策略，不等式 (13) 右侧的量 $(h - \alpha + 1)|\mathcal{E}|$ 可以放宽为攻击者根据其能量条件从第 $\hat{}\alpha$ 步到第 h 步所能攻击的边数上限。然而，这一边数可能每局博弈都会变化，因而难以简洁地表示该不等式。

引理 2 给出了一个时间区间，在该区间内，至少有一次选择在发送普通信号时不进行攻击或恢复非零边是最优的。

引理 2 每隔 $\lceil \frac{h|\mathcal{E}|\beta^{\mathrm{D}} - \rho^{\mathrm{D}}}{\rho^{\mathrm{D}} T} + 1 \rceil$ 个时间步，$\mathcal{E}_k^{\mathrm{D}} \ne \emptyset$ 或 $\mathcal{E}_k^{\mathrm{A}} = \emptyset$ 至少会发生一次。

证明。由引理 1 可知，在索引为 l'、且对 $\alpha = 1$ 满足 (13) 的博弈中，防御者总会恢复在第 1 步中受到常规攻击的边，即 $\mathcal{E}_{l',\ 1}^{\mathrm{D}} \ne \emptyset$ 如果 $\mathcal{E}_{l',\ 1}^{\mathrm{A}} \ne \emptyset$。接下来，我们考察在哪些博弈中，对 $\alpha = 1$ 满足不等式 (13)。由于防御者每次 k 都会获得 ρ^{D}，如果 $\mathcal{E}_k^{\mathrm{D}} = \emptyset$，对于

任意 $k \in \{0, \ldots, (l'-1)T-1\}$，则第 l' 个博弈第一步的 (13) 可写为 $\kappa^{\mathrm{D}}+\rho^{\mathrm{D}}(\ l'-1\ T \leq h|\mathcal{E}|\cdot$。以 $\kappa^{\mathrm{D}}=\rho^{\mathrm{D}}$ 作为最坏情况，左边变为 $\rho^{\mathrm{D}}(1+(l'-1)T)\ \beta^{\mathrm{D}}$，于是得到 $l' \geq \lceil \frac{h|\mathcal{E}|\beta^{\mathrm{D}}-\rho^{\mathrm{D}}}{\rho^{\mathrm{D}}T}+1 \rceil$。

请注意，对于任意 $k \in \{(j-1)(l'-1)T, \ldots, j(l'-1)T-1\}, j \in \mathbb{N}$，当防御者未恢复任何边时，上述事实成立。如果防御者在任意 $k \in \{0, \ldots, (l'-1)T-1\}$ 恢复了一条或多条受攻击边，那么上述结果可能不成立，即防御者可能无法恢复所有 $\mathcal{E}_{l'}^{\mathrm{A}}$。然而可以推出，在时间 $k \in \{(j-1)(l'-1)T, \ldots, j(l'-1)T-1\}$ 期间，以下情况至少发生一次：1）防御者恢复非零条边（$\mathcal{E}_k^{\mathrm{D}} \neq \emptyset$）；或 2）攻击者未使用普通信号攻击任何边（$\mathcal{E}_k^{\mathrm{A}} = \emptyset$）。□

上面的引理1和引理2表明，防御者保证每隔一定时间就能从普通攻击中恢复。因此，攻击者需要对某些边发动强力攻击，以阻止恢复，从而将智能体分隔到不同的簇中，下面将对此进行讨论。

以下两个结果给出了一致性无法实现的必要条件。命题3考虑更一般的条件，而定理4则针对导致条件更严格的效用函数，考虑一种更具体的情形。回想一下，λ 表示 $\mathcal{G}$的连通度。

命题3 一致性无法实现的必要条件是 $\lfloor \rho^{\mathrm{A}}/\beta^{\mathrm{A}} \rfloor \geq \lambda$。

证明。在推导这一必要条件时，我们假设防御者在任意时间k都不会进行恢复。若防御者未进行任何恢复（$\mathcal{E}_k^{\mathrm{D}} = \emptyset$），攻击者必须在任意时间 k 至少攻击 λ 条带有普通信号（所需能量较少）的边，才能使 $\mathcal{G}_k^{\mathrm{D}}$始终不连通。否则，图 $\mathcal{G}_k^{\mathrm{D}}$ 在某些时间步会连通，这意味着仍然会达到一致性。

如果攻击者始终使用常规干扰信号攻击 λ 条边，能量约束(3)将变为$(\beta^{\mathrm{A}}\lambda - \rho^{\mathrm{A}})k \leq \kappa^{\mathrm{A}}$。因此，必须满足条件 $\rho^{\mathrm{A}}/\beta^{\mathrm{A}} \geq \lambda$，才能确保攻击者对于所有 k都能使 $\mathcal{G}_k^{\mathrm{D}}$不连通。注意，如果在没有恢复的情况下，攻击者没有足够的能量使 $\mathcal{G}_k^{\mathrm{D}}$不连通，那么面对防御者的恢复时，它肯定也无法使 $\mathcal{G}_k^{\mathrm{D}}$ 不连通。□

现在，我们将式（7）、（8）中的效用函数类限制为权重中的 $b=0$。这意味着参与者不会考虑图中的智能体组索引，而只考虑一致性状态。在这种情况下，攻击者可能需要更多能量来阻止达成一致性，正如下一个定理所示。

定理4 假设 $b=0$。一致性不发生的必要条件是 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq \lambda$。

证明。我们通过逆否命题进行证明；特别地，当 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$时，我们证明一致性始终会发生。

我们首先假设攻击者始终试图强力攻击λ 条边，以使图 $\mathcal{G}_k^{\mathrm{D}}$不连通。根据(3)，攻击者在时间 k 的能量约束变为 $(\overline{\beta}^{\mathrm{A}}\lambda - \rho^{\mathrm{A}})k \leq \kappa^{\mathrm{A}}$。如果 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$，则当 k 足够大时，该不等式不成立，因为$\overline{\beta}^{\mathrm{A}}\lambda - \rho^{\mathrm{A}}$ 变为正值，而 κ^{A} 是有限的。因此，当 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$时，攻击者无法始终强力攻击 λ 条边，而被迫改用常规干扰信号进行攻击，以使图不连通。

接下来，根据上述引理 2，我们证明：如果边遭到常规攻击，那么存在一个时间区间，在此期间防御者总会进行恢复，即在给定 $\mathcal{E}_{l'}^{\mathrm{A}} \neq \emptyset$ 的情况下，$\mathcal{E}_{l'}^{\mathrm{D}} \neq \emptyset$ 是最优的。

根据 (7)、(8) 中的定义，在给定 $b=0$ 的情况下，可以看出，智能体彼此越接近，防御者获得的效用越高。这意味着，当需要恢复的边数非零时（在上述描述的时间 $jl'T$ ），防御者会恢复连接距离较远的智能体的边。具体而言，对于某个 $i \in \mathbb{N}$，在区间 $[jl'T, (j+i)l'T]$ 内，存在一个时间步，使得 $U_l^{\mathrm{D}}(\mathcal{E}_k^{\mathrm{D}} = \mathcal{E}_1) \geq U_{\mathrm{D}l}(\mathcal{E}_2)$，其中边 $\mathcal{E}_1$ 连接的智能体，其状态间距大于由 $\mathcal{E}_2$ 连接的智能体。由此可知，进行恢复时，防御者总会选择彼此断连且距离较远的智能体。由于智能体通过 (1) 中的共识协议进行通信时，其状态会逐渐接近，因此，当恢复边所连接的智能体状态足够接近时，防御者将选择恢复其他边。因此，若 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$，则存在 $i \in \mathbb{N}$，使得在时间区间 $[j(l'-1)T$ 内，各图的边的并所构成的图（即图的并）$(\mathcal{V}, \bigcup((\mathcal{E} \setminus (\overline{\mathcal{E}}_k^{\mathrm{A}} \cup \mathcal{E}_k^{\mathrm{A}})) \cup \mathcal{E}_k^{\mathrm{D}}), (j+i)(l'-1)T])$ 成为连通图，其中 $l' = \lceil \frac{h|\mathcal{E}|\beta^{\mathrm{D}}-\rho^{\mathrm{D}}}{\rho^{\mathrm{D}}T}+1 \rceil$ 如上述引理 2 所述。这些区间 $[j(l'-1)T, (j+i)(l'-1)T]$ 会无限次出现，因为防御者的能量上界随时间不断增加。

文献 [31] 表明，采用协议 (1) 时，只要有界时间区间内各图的并集构成连通图，智能体就能在时变图中实现一致性。这意味着，只要

$(\mathcal{V}, \bigcup((\mathcal{E}\setminus(\overline{\mathcal{E}}_k^{\mathrm{A}}\cup\mathcal{E}_k^{\mathrm{A}}))\cup\mathcal{E}_k^{\mathrm{D}}))$ 在$[l_i', l_i'+1, \ldots, l_{i+j}']$上连通，就能实现一致性。因此，若 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < \lambda$，则可实现一致性。□

定理4中的结果仅适用于 $b=0$，因为在$b>0$ 的情况下，防御者可以选择恢复连接状态相似的智能体的边，以最大化 c（$\mathcal{G}_k^{\mathrm{D}}$）（而不是恢复连接状态差异更大的智能体的边）。在这种情况下，网络可能仍然是不连通的，因此智能体可能会收敛到不同的状态。正如我们从这些结果中看到的，权重值会影响防止一致性所需的条件，而权重对充分条件（稍后讨论）的影响则不那么直接。a 和 b 的取值对一致性的影响见第8节。

5.2 防止一致性的充分条件

下一个结果给出了防止一致性的充分条件。该结果表明，在给定网络拓扑 $\mathcal{G}$的情况下，如果攻击者具有足够大的充能速率 ρ^{A}，则可以防止一致性。首先，我们给出关于攻击者在某些能量条件下的最优策略的引理5，这与上面对防御者情形的讨论类似。

引理 5 攻击者的最优策略为 $\overline{\mathcal{E}}_l^{\mathrm{A}*,\ \alpha} = \mathcal{E}$ 如果

- 攻击者的充能速率满足 $\rho_{\mathrm{A}}/\overline{\beta}_{\mathrm{A}} \geq |\mathcal{E}|$，或者
- 攻击者在第 l 次博弈的第 α 步之前消耗的总能量 $\tilde{\beta}_{\mathrm{A}\ l} + \hat{}\beta_{\mathrm{A}\alpha-1}$ 满足

$$\tilde{\beta}_l^{\mathrm{A}} + \hat{\beta}_{\alpha-1}^{\mathrm{A}} \leq \kappa^{\mathrm{A}} + \rho^{\mathrm{A}}((l-1)T+\alpha-1) - (h-\alpha+1)\overline{\beta}^{\mathrm{A}}|\mathcal{E}|. \tag{14}$$

证明。我们首先注意到，在第 l 次博弈的第 h 步中，攻击者不会通过攻击较少的边来节省能量。由于对于任意边 $\overline{\mathcal{E}}_{l\ h}^{\mathrm{A}}, \mathcal{E}_{l\ h}^{\mathrm{A}}, \mathcal{E}_{l\ h}^{\mathrm{D}}$，$z_{l,h}(\mathcal{E},\emptyset,\emptyset) > z_{l,h}(\overline{\mathcal{E}}_{l\ h}^{\mathrm{A}}, \mathcal{E}_{l\ h}^{\mathrm{A}}, \mathcal{E}_{l\ h}^{\mathrm{D}})$ 和 $c(\mathcal{V},\emptyset)) \geq c(\mathcal{V},(\mathcal{E}\setminus(\overline{\mathcal{E}}_{l\ h}^{\mathrm{A}}\cup\mathcal{E}_{l\ h}^{\mathrm{A}})\cup\mathcal{E}_{l\ h}^{\mathrm{D}}))$ 始终成立，因此，如果攻击者对所有边 $\mathcal{E}$ 发动强力攻击，函数U_h^{A}的值始终最高。由此可知，能量充足的攻击者，即满足 $\kappa^{\mathrm{A}} + \rho^{\mathrm{A}}((l-1)T+h-1) - (\tilde{\beta}_l^{\mathrm{A}} + \hat{}\beta_{h-1}^{\mathrm{A}}) \geq \overline{\beta}^{\mathrm{A}}|\mathcal{E}|$ 的攻击者，会选择对所有边发动强信号攻击。

与引理 1 中的证明类似，对于任意步骤 α，不等式 $z_{l,\ \alpha}(\mathcal{E},\emptyset,\emptyset) > z_{l,\ \alpha}(\overline{\mathcal{E}}_{l\ ,\ \alpha}^{\mathrm{A}}, \mathcal{E}_{l\ ,\ \alpha}^{\mathrm{A}}, \mathcal{E}_{l\ ,\ \alpha}^{\mathrm{D}})$ 和 $c((\mathcal{V},\emptyset)) \geq c((\mathcal{V},(\mathcal{E}\setminus(\overline{\mathcal{E}}_{l\ ,\ \alpha}^{\mathrm{A}}\cup\mathcal{E}_{l\ ,\ \alpha}^{\mathrm{A}})\cup\mathcal{E}_{l\ ,\ \alpha}^{\mathrm{D}})))$ 始终成立。因此，只要能量充足，攻击者就会选择在任意步骤 α 攻击所有具有强信号的边。若攻击者的储存能量足够高，即满足 (14)，或者攻击者的充能速率足够高，即 $\rho^{\mathrm{A}} \geq \overline{\beta}^{\mathrm{A}}|\mathcal{E}|$，便可实现这一点。这些条件使攻击者能够强力攻击所有边，同时仍满足上述所有步骤的能量约束 (3)。 □

命题6 所有智能体在无限时间内无法实现一致性的一个充分条件是，攻击者的参数满足 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$。

证明。根据引理 5，在任意一步的博弈中，如果游戏开始时具有足够的充能速率或储存能量，攻击者总会使用强信号攻击所有边α。因此，如果
攻击者的充能速率满足 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$，攻击者将在所有博弈的每一步都使用更强的干扰信号攻击 $\mathcal{E}$，使每个智能体始终彼此分离。因此，会形成 n 个簇，显然无法达成一致性。□

注7 请注意，上述必要条件和充分条件考虑的是式 (6) 中的 $z_k = x^{\mathrm{T}}L_{\mathrm{c}}x$，它是一个非递增函数。也可以考虑其他拉普拉斯矩阵，例如底层图 $\mathcal{G}$ 的拉普拉斯矩阵；然而，函数 z_k 可能不再是非递增的。例如，考虑一个简单的路径图 1-2-3，其初始状态为 $x_0 = [10, 0, -5]^{\mathrm{T}}$，并在状态差异函数 z_k 中采用图 $\mathcal{G}$ 的拉普拉斯矩阵。采用效用函数 (7) 和 (8) 的权重 $a=1$ 和 $b=0$，以及权重为 $a_{12}=0.1$ 和 $a_{23}=0.8$ 的一致性协议 (1) 和 (2)，当 $h=1$ 时，参与者在第一场博弈中的效用为 $U_{1}^{\mathrm{A}} = -U_1^{\mathrm{D}} = 148$（未发起任何攻击），而在攻击两条边时为 $U_1^{\mathrm{A}} = U_{\mathrm{A}_0} = -U_1^{\mathrm{D}} = 125$。这表明，即使攻击者拥有足够大的能量，不攻击任何边实际上也可能是其最优选择。因此，在状态差异函数 z_k 中采用图 $\mathcal{G}$ 的拉普拉斯矩阵时，分析会变得更加复杂，部分理论结果也不再成立，例如命题6中的充分条件。

5.3 必要条件与充分条件之间差距的示例

在本小节中，我们通过一个示例说明定理4中阻止一致性的必要条件与命题6中的充分条件之间的差距。这里假设防御者的充能速率非常高（即，ρ^{D} 远大于 β^{D}），因此它可以在任意 k 内修复所有受到常规攻击的边（请注意，定理4中的条件仅包含攻击者的参数）。这将迫使攻击者

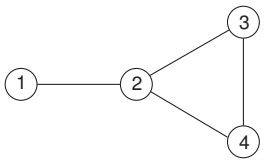


图4。案例研究中使用的图 $\mathcal{G}$ 。

表1 不同 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$ 值下的智能体状态差异

$\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$	z_{20}	一致性
1	0.113	Yes
1.1	0.115	Yes
1.2	1.3405	No
1.4	235.345	No
1.8	706.8	No
2	1354	No

使用强干扰信号发起攻击，以使任意智能体断开连接。

我们考虑图

$$\mathcal{G} \qquad 4, \qquad x[0] \quad =,$$
$$[-5,0,-20,10] \;\; h=2 \qquad \kappa^{\mathrm{A}}=\rho^{\mathrm{A}}$$

如图所示，其中有，，和。效用函数的权重设为 $a=1$ 和 $b=0$。我们测试 $1 \leq \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \leq 2$的各种取值，这意味着攻击者始终可以使用强信号攻击一条边，而不会耗尽能量。因此，为了阻止一致性，攻击者必须始终攻击 e_{12} （ $\mathcal{G}$的最小割边），因为只有攻击这条边才会使图断开。请注意，该比率 $1 \leq \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \leq 2$满足定理4中阻止一致性的必要条件，但不满足命题6中的充分条件。

具体而言，在本例中，我们根据时间 $k=20$ 的智能体状态，测试对于不同的 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$ 值，一致性是否会被阻止。值得注意的是，从表1可以看出，即使 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} < |\mathcal{E}|$ 的值相对较小，攻击者仍然可以阻止一致性。

从本例中可以看出，必要条件与充分条件之间存在差距。需要注意的是，对于连接更紧密的 $\mathcal{G}$，以及由更多智能体组成的网络，这一差距可能更大，通常 $|\mathcal{E}|>> \lambda.$ 。随后，我们将在第8节中提供更详细的示例，说明这些参数值对一致性的影响。

作为本节的最后一个结果，我们指出，对于在 $b=0$ 和 h =1 下的完全图这一特殊情形，即没有滚动时域的单步博弈，定理4中的条件也是充分条件，也就是说，必要条件与充分条件之间不存在差距。

命题8：假设 $b=0$ 和 $h=1$。在完全图 $\mathcal{G}$中，一致性不发生的充分条件是 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq n-1$。

证明。对于 $h=1$，攻击者将在博弈的唯一一步中耗尽所有能量。对于 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq n-1$，攻击者始终能够断开完全图 $\mathcal{G}$。

在完全图 $\mathcal{G}$中，无论智能体的状态如何，每个智能体都与其他所有智能体相连，这意味着攻击者无法优先选择某个智能体将其隔离（与上面的例子不同）。因此，对于 $b=0$，攻击者必定能分离出距离最远的智能体。这意味着，在每场博弈中（以及在每个k），攻击者总是攻击相同的边，从而使 $\mathcal{G}_k^{\mathrm{D}}$在每个时刻都断开。□

我们注意到，对于不同类别的图（包括其他对称图，例如环图或星形图），要推导出更严格的充分条件更具挑战性。这是因为智能体只能直接访问其他部分智能体，因此，基于智能体状态进行簇形成会更加困难。

6 聚类分析

本节推导关于无限时间时形成的智能体簇数量的一些结果。根据命题 6，结果表明一个简单情形：如果攻击者拥有足够的能量，使得 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$，那么攻击者便可以攻击底层拓扑结构 $\mathcal{G}$ 中的所有边，从而使簇的数量为 n （即所有智能体彼此分离）。

下一个结果讨论攻击者的成本和能量补充率与攻击者通过干扰可能形成的最大簇数量之间的关系。本节后续结果中，我们假设 $b=0$。

我们首先定义一个向量，用于表征给定参数 ρ^{A}和 $\overline{\beta}^{\mathrm{A}}$ 时 $\mathcal{G}$ 的最大簇数。具体而言，我们定义一个向量 $\Theta \in \mathbb{R}^{|\mathcal{E}|}$，其元素 Θ_j为：$=\max^{|\mathcal{E}^{\mathrm{A}}|=j} \overline{\pi}(\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}})$，其中 $\overline{\pi}(\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}})$ 表示 $(\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}})$ 的智能体群组数。

命题9 无限时间下形成的簇数量的上界为 $\Theta_{\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor}$。

证明。向量 Θ 由已形成群组的最大数量 $\overline{\pi}(\mathcal{V}, \mathcal{E} \setminus \mathcal{E}^{\mathrm{A}})$构成，给定数量的

受攻击边数作为元素索引。由于需要持续攻击某些边，才能将智能体划分为不同的簇，因此，在无限时间内形成的簇数不会超过给定相同数量强攻击边时任意时刻的群组最大数量 k 。

回顾一下，$\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor$ 是始终能够被强攻击的边数的最大可达值。给定已知的图拓扑 $\mathcal{G}$，我们可以推知，$\Theta_{\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor}$ 给出了无限时间时簇数量的最大值。□

接下来，我们讨论一种特殊情况，即网络中的所有智能体彼此相连。

推论10 在完全图 $\mathcal{G}$中，攻击者无法将智能体划分为超过

$$1+\sum_{j=1}^{(n-1)} \min\Big\{1, \Big\lfloor \frac{2\rho^{\mathrm{A}}}{j\overline{\beta}^{\mathrm{A}}(2n-j-1)} \Big\rfloor \Big\} \qquad (15)$$

个簇。

证明。在完全图中，每个智能体都与其他所有 $n-1$ 智能体相连。根据命题9，我们可以得到完全图 $\mathcal{G}$ 的向量 Θ ，其形式为

$$\Theta = [1, \ldots, 1, 2, \ldots, 2, 3, \ldots, n-1, n]^{\mathrm{T}},$$

其中，第（$n-1$）个条目的值为 2，第（（$n-1$）+（$n-2$））个条目的值为 3，依此类推。这是因为，在完全图 $\mathcal{G}$ 中，攻击者需要攻击（$n-1$）条边才能断开该图，还需要攻击（$n-2$）条边才能将智能体分成三个组，再攻击（$n-3$）条边才能将智能体分成四个组，依此类推，直到（$n-1$）+（$n-2$）+ $\cdots$ + 1 =n（$n-1$）/2 个智能体组成 n 个组。对于完全图，该 Θ矩阵中第$\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor$ 个条目的值可写为式（15）。该值决定了簇数量的上界。□

在命题9中，我们利用图结构的信息来获得向量 Θ。需要指出的是，如果图结构 $\mathcal{G}$ 未知，那么无限时间时的簇数量通常以上界 $\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor + 1$为界。这是因为攻击者在任意时刻连续发动攻击时，至多只能攻击 $\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor$ 条边；而在具有 $\lambda = 1$的最脆弱图中，即树图中，任何被攻击的边都会导致产生一个新的组。为说明 Θ 与 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$之间的关系，我们考察

表2 攻击与恢复动作的可能情况

Case	$c(\mathcal{G}_l^{\mathrm{A},\alpha})$	$c(\mathcal{G}_l^{\mathrm{D},\alpha})$
1	$c(\mathcal{G}_l^{\mathrm{A},\alpha}) = c(\mathcal{G})$	$c(\mathcal{G}_l^{\mathrm{D},\alpha}) = c(\mathcal{G}_l^{\mathrm{A},\alpha})$
2	$c(\mathcal{G}_{l,\alpha}^{\mathrm{A}}) < c(\mathcal{G})$	$c(\mathcal{G}_l^{\mathrm{D},\alpha}) = c(\mathcal{G}_l^{\mathrm{A},\alpha})$
3	$c(\mathcal{G}_{l,\alpha}^{\mathrm{A}}) < c(\mathcal{G})$	$c(\mathcal{G}_{l,\alpha}^{\mathrm{D}}) > c(\mathcal{G}_{l,\alpha}^{\mathrm{A}})$

7 均衡刻画

在这个博弈中，策略选择均为有限形式，即被攻击和恢复的边。在此，我们针对参与者时域长度为 1 的情况，刻画某些情形下参与者的均衡/最优策略；此时，参与者会在每个时间步上以短视方式更新策略。

本节给出 $a = 0$ 时的一些结果，即参与者在确定策略时不考虑智能体状态，而只考虑智能体组索引，因此，同一组中的智能体越多，防御者（攻击者）的效用越高（低）。与 [20], 中的分析类似，我们在此探讨博弈中参与者的一些可能的最优策略候选。然而，由于在此表述中，博弈由多个步组成，因此与 [20] 中由单个步构成的博弈相比，子博弈完美均衡的刻画更为复杂。

在每个博弈的第 α 步中，函数 $c(\cdot)$ 有三种可能情况，如表2所示（情况1、情况2和情况3）。根据此表，我们刻画了两位参与者在各情况下的最优策略：

- 情况1：当 $c(\mathcal{G}) = c(\mathcal{G}_{\mathrm{D}l,\alpha})$ 时，攻击者在一个时间步内的效用为 $c(\mathcal{G})$，这意味着攻击者不应使用普通信号或强信号攻击任何边，且两位参与者的效用均为零。此情况下参与者的策略称为组合策略 1。
- 情况2：当 $c(\mathcal{G}_{\mathrm{D}l,\alpha}) = c(\mathcal{G}_{\mathrm{A}l,\alpha})$ 时，防御者不会恢复任何遭到攻击的边，而攻击者应使用强信号或普通信号攻击一些边。此情况下参与者的策略归类为组合策略 2。
- 情况3：此时，双方都会攻击或恢复非零数量的边。具体而言，攻击者会使用普通信号进行攻击，并可能使用强信号。参与者在此处采用的策略称为组合策略 3。

参见上一节中的图4。这里，$\Theta = [2, 2, 3, 4]^{\mathrm{T}}$，而对于 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} = 1$，$\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor + 1$ 的取值分别为 2、3、4、5；对于 2、3 和 4 亦然。注意，对于 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$ 的任意取值，不等式 $\Theta_{\lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor} \leq \lfloor \rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \rfloor + 1$ 始终成立，这表明了解图结构有助于更准确地估计簇数量的上界。

接下来，我们将在下文的命题 11 中讨论该博弈的均衡。为简单起见，我们仅考虑 $h=1$ 的情形。对于 $h=1$ 的情形，可基于此处的刻画来分析 $h>1$ 的情形。

命题 11 具有 $h=1$ 的参与者的最优策略满足以下条件：

(1) Combined Strategy 1 if $\tilde{\beta}_l^{\mathrm{A}}+\beta^{\mathrm{A}}>\kappa^{\mathrm{A}}+\rho^{\mathrm{A}}(l-1)T$,
(2) Otherwise,
  (a) Combined Strategy 2 if
    (i) $\tilde{\beta}_l^{\mathrm{D}}+\beta^{\mathrm{D}}>\kappa^{\mathrm{D}}+\rho^{\mathrm{D}}(l-1)T$, *or*
    (ii) $\tilde{\beta}_l^{\mathrm{D}}+\beta^{\mathrm{D}}\leq\kappa^{\mathrm{D}}+\rho^{\mathrm{D}}(l-1)T$ *and* $U_l^{\mathrm{A}}(\lfloor(\kappa^{\mathrm{A}}+\rho^{\mathrm{A}}(l-1)T-\tilde{\beta}_l^{\mathrm{A}})/\overline{\beta}^{\mathrm{A}}\rfloor,\emptyset,\emptyset)=\max_{\overline{\mathcal{E}}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}}}U_l^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}})$,
  (b) Combined Strategy 3 if $\tilde{\beta}_l^{\mathrm{D}}+\beta^{\mathrm{D}}\leq\kappa^{\mathrm{D}}+\rho^{\mathrm{D}}(l-1)T$ *and* $U_l^{\mathrm{A}}(\lfloor(\kappa^{\mathrm{A}}+\rho^{\mathrm{A}}(l-1)T-\tilde{\beta}_l^{\mathrm{A}})/\overline{\beta}^{\mathrm{A}}\rfloor,\emptyset,\emptyset)\neq\max_{\overline{\mathcal{E}}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}}}U_l^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}})$.

证明。对于 $a=0$，我们注意到，只要能量充足，防御者总能在最后一步从最优攻击中恢复，这意味着当 $\tilde{\beta}_l^{\mathrm{D}}+\beta^{\mathrm{D}}\leq\kappa^{\mathrm{D}}+\rho^{\mathrm{D}}((l-1)T)$ 满足时，对于 $h=1$，防御者总能恢复。与防御者类似，在 $h=1$ 的情况下，攻击者不进行攻击即可获得最低效用，即零。因此，只要能量足够，攻击者至少会攻击一条边。我们将在下文逐一证明命题中的各项陈述。

(1)：现在我们假设 $\tilde{\beta}_l^{\mathrm{A}}+\beta^{\mathrm{A}}>\kappa^{\mathrm{A}}+\rho^{\mathrm{A}}((l-1)T)$（陈述中的第 (1) 点）成立，即攻击者甚至没有足够的能量以普通方式攻击一条边。在这种情况下，组合策略 1 是最优策略，因为别无选择，即攻击者无法使用普通信号攻击任何一条边。在证明的其余部分，我们假设 $\tilde{\beta}_l^{\mathrm{A}}+\beta^{\mathrm{A}}\leq\kappa^{\mathrm{A}}+\rho^{\mathrm{A}}((l-1)T)$ 成立。

(2a(i))：接下来，我们给出组合策略 2 的条件。与上文讨论的攻击者类似，我们观察到，如果 $\tilde{\beta}_l^{\mathrm{D}}+\beta^{\mathrm{D}}>\kappa^{\mathrm{D}}+\rho^{\mathrm{D}}((l-1)T)$，防御者就无法恢复任何边，这意味着 $c(\mathcal{G}_l^{\mathrm{A}},\alpha)<c(\mathcal{G})$ 且 $c(\mathcal{G}_l^{\mathrm{D}},\alpha)=c(\mathcal{G}_l^{\mathrm{A}},\alpha)$（对应点 $(2a(i))$）。

(2a(ii))：接下来我们假设满足 $\tilde{\beta}_l^{\mathrm{D}}+\beta^{\mathrm{D}}\leq\kappa^{\mathrm{D}}+\rho^{\mathrm{D}}((l-1)T)$。由此可知，只要防御者拥有足够的能量，攻击者就需要用强信号攻击非零数量的边，才能满足 $c(\mathcal{G}_l^{\mathrm{A}},\alpha)<c(\mathcal{G})$ 和 $c(\mathcal{G}_l^{\mathrm{D}},\alpha)=c(\mathcal{G}_l^{\mathrm{A}},\alpha)$。为了使组合策略 2 达到最优，攻击者需要强力攻击边，而完全不使用普通信号进行攻击，即 $\mathcal{E}_k^{\mathrm{A}}=\emptyset$。因此，$\overline{\beta}^{\mathrm{A}}$ 需要足够低，才能使强攻击具有可行性。具体而言，$U_l^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}\prime},\emptyset,\emptyset)=\max_{\overline{\mathcal{E}}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}}}U_l^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}})$，其中 $|\overline{\mathcal{E}}_k^{\mathrm{A}\prime}|=\lfloor(\kappa^{\mathrm{A}}+\rho^{\mathrm{A}}((l-1)T)-\tilde{\beta}_l^{\mathrm{A}})/\overline{\beta}^{\mathrm{A}}\rfloor$ 表示攻击者强力攻击的边数上限。这对应于点 $(2a(ii))$。

(2b)：因此，如果 $\tilde{\beta}_l^{\mathrm{D}}+\beta^{\mathrm{D}}\leq\kappa^{\mathrm{D}}+\rho^{\mathrm{D}}((l-1)T)$ 和 $U_l^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}\prime},\emptyset,\emptyset)\neq\max_{\overline{\mathcal{E}}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}}}U_l^{\mathrm{A}}(\overline{\mathcal{E}}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{A}},\mathcal{E}_k^{\mathrm{D}})$ 成立，那么攻击者通常会攻击非零条边，防御者也会恢复非零条边，这意味着组合策略 3 是最优的（点 $2b$）。□

注 12 命题 11 中对最优策略的刻画，同样适用于比式 (5) 中定义的 $c(\mathcal{G})$ 更一般的一类智能体组指标，只要效用函数结构 (7) 和 (8) 保持不变。具体而言，它适用于属于以下类别的指标：

$$\mathcal{C}:=\{\tilde{c}:2^{\mathcal{V}}\times2^{\mathcal{E}}\to\mathbb{R}:\tilde{c}((\mathcal{V},\overline{\mathcal{E}}\cup\mathcal{E}'))\geq\tilde{c}((\mathcal{V},\overline{\mathcal{E}})),\ \overline{\mathcal{E}},\mathcal{E}'\subseteq\mathcal{E}\}. \tag{16}$$

条件 $\tilde{c}((\mathcal{V},\overline{\mathcal{E}}\cup\mathcal{E}'))\geq\tilde{c}((\mathcal{V},\overline{\mathcal{E}}))$ 意味着，不发动攻击会使攻击者的 $\tilde{c}(\mathcal{G}_l^{\mathrm{A}},\alpha)$ 取得最大值。类似地，对于防御者，该条件意味着在遭受攻击后不进行恢复会使 $\tilde{c}(\mathcal{G}_l^{\mathrm{D}},\alpha)$ 取得最小值。该条件是确保命题 11 所述均衡的必要条件，因为它保证只要参与者有足够的能量，攻击或恢复非零条数的边（对应于组合策略 3）始终是其最优选择。

一般而言，由于上述讨论的情况都只涉及一步，对于更长的 $h>1$，最优策略将表现为一组组合策略。例如，如果 $h=3$，最优策略序列可能为{组合策略 1、组合策略 2、组合策略 2}。另一方面，对于 $a>0$，命题 11 中的条件会变得更加难以刻画，因为攻击更多的边并不一定会带来尽可能高的效用。

8 仿真结果

8.1 不同参数下的一致性与聚类

此处展示效用函数的不同权重和初始状态如何影响一致性。

8.1.1 改变权重 a和 b

我们考虑初始状态为 $x_0=[1,0.75,0.75,-1]^{\mathrm{T}}$ 的 4智能体线形/路径图 1–2–3–4。参数

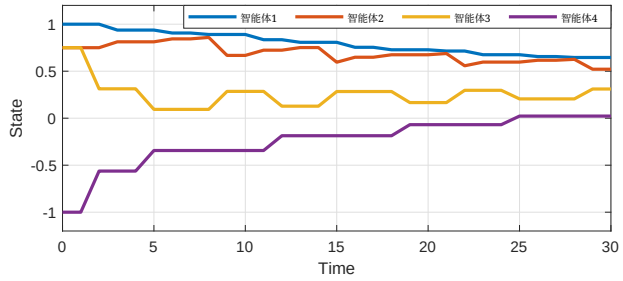


图5. 智能体状态与 $a = 0.1$ and $b = 0.9$

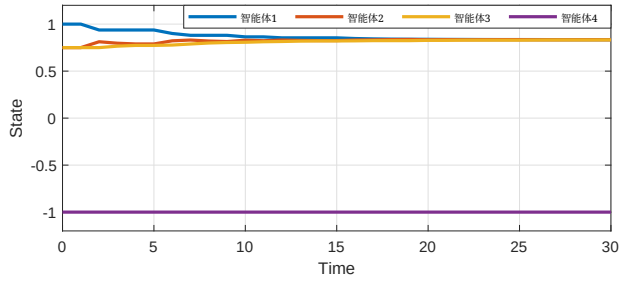


图6. 智能体状态与 $a = 0.9$ 和 $b = 0.1$

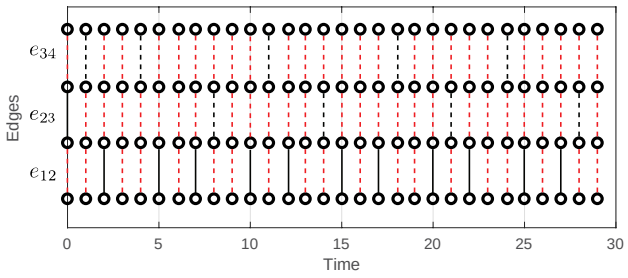


图7. 攻击和恢复的边与 $a = 0.1$ 和 $b = 0.9$

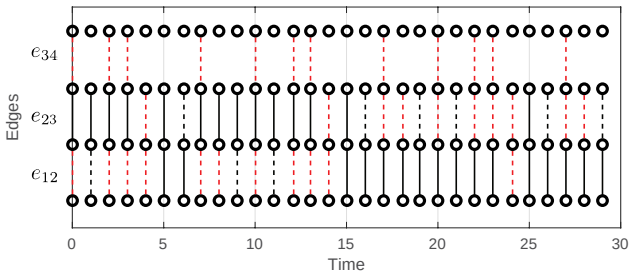


图8. 攻击和恢复的边与 $a = 0.9$ 和 $b = 0.1$

为 $\beta^{\mathrm{A}} = \beta^{\mathrm{D}} = 1$, $h = \overline{\beta}^{\mathrm{A}} = 2$, $\kappa^{\mathrm{A}} = \rho^{\mathrm{A}} = 2.6$, $\rho^{\mathrm{D}} = 0.3$ 和 $\kappa^{\mathrm{D}} = 0.8$，这些参数满足命题3中防止一致性的必要条件，但不满足命题6中的充分条件。在 $b = 1 - a$ 的情况下，图5和图6分别展示了较小 a （取值为 a =0.1）和较大 a （取值为 $a = 0.9$）时的智能体状态。图7和图8展示了 $\mathcal{G}_k^{\mathrm{D}}$ 随离散时间变化的边状态 k。其中，对应边上没有线表示该边受到强攻击；同样，红色虚线表示受到常规攻击，黑色虚线表示已恢复，黑色实线表示未受攻击。

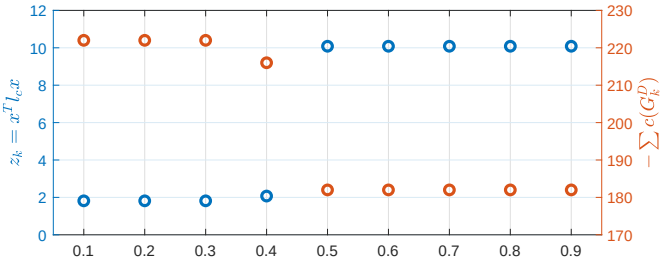


图9. z_k 和 $-\sum c\ (\mathcal{G}_k^{\mathrm{D}})$ 与 a的比较（$k = 20$）

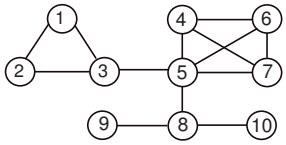


图10. 第8.1.2节仿真所用的图

我们观察到，当 a较小时，攻击者更常将智能体划分为更多群组，这一点可从图7中更多的红色虚线看出。因此，尽管满足命题3中的条件，攻击者仍未能阻止智能体之间达成一致性（图5）。另一方面，当 a较大时，与 a较小的情况相比，攻击者更专注于扩大智能体状态之间的差异，同时将智能体划分为较少的群组。图8展示了这些特点，其中边 e_{34}上没有黑线，因此图6中的智能体无法达成一致性。

接下来，我们在图9中比较不同 a 和 $b = 1 - a$ 下的最优状态差异 z_k（$\overline{\mathcal{E}}_k^{\mathrm{A}*}$， $\mathcal{E}_k^{\mathrm{A}*}$， $\mathcal{E}_k^{\mathrm{D}*}$）和智能体组索引 $c\ (\mathcal{G}_k^{\mathrm{D}})$。我们观察到， a越大，攻击者越能成功阻止智能体之间达成一致性（表现为 z_k的值较大），时间为 $k = 20$。另一方面，当 a 较小（对应于 b较大）时，攻击者以较低的 z_k为代价，获得较高的 $c\ (\mathcal{G}_k^{\mathrm{D}})$，这意味着攻击者未能阻止一致性。值得注意的是，对于某些不同的a， z_k和 $\sum c\ (\mathcal{G}_k^{\mathrm{D}})$的值几乎保持不变，这意味着权重 a 和b 存在一个临界值，该值决定了无限时间下的一致性和簇的数量；在这种情况下， a的临界值位于 $0.4 < a < 0.5$。

8.1.2 变化的初始状态 x_0

我们还考察初始状态 x_0 对智能体的智能体-组索引的影响。我们考虑图10所示的图，该图由10个智能体组成。除初始状态外，所有参数均设为相同，并满足命题3中的条件。具体而言，我们设定 $\beta^{\mathrm{A}} = \beta^{\mathrm{D}} = 1$、$\overline{\beta}^{\mathrm{A}} = 2$、$\kappa^{\mathrm{A}} = \rho^{\mathrm{A}} = 2.1$、$\kappa^{\mathrm{D}} = \rho^{\mathrm{D}} =$为0.7，以及 $a = 1 - b = 0.9$。初始状态 x_0 不同时智能体的状态轨迹如图11–13所示。这里我们考虑初始状态 x_0 的三种情况：

(1) $x_0 = [1, 0.9, 0.8, 0.4, 0.44, 0.35, 0.48, 0.2, 0.19, 0.28]^{\mathrm{T}}$, (2) $x_0 = [1, 0.9, 0.8, 0.4, 0.44, 0.35, 0.48, -0.5, -0.1, -0.2]^{\mathrm{T}}$, (3) $x_0 = [0.6, 0.5, 0.8, 0.4, 0.44, 0.35, 0.48, 0.58, 0.8, 0.75]^{\mathrm{T}}$。

请注意，在情况（1）中，智能体1–3的初始状态彼此更接近，且与其他智能体相距较远。同样，在情况（2）中，智能体8–10的初始状态与其他智能体不同。然而，在情况（3）中，智能体状态在范围 $[0.35, 0.8]$内近似均匀分布，因此攻击者很难将它们划分为多个簇。

从图11可以看出，在情况（1）中，与其他智能体连接较弱（仅通过一条边连接）的智能体1–3被分到同一组，并收敛到相同状态。这是通过攻击连接智能体3和5的边实现的。另一方面，在图12所示的情况（2）中，由于连接智能体5和8的边持续遭到攻击，智能体8–10与其他智能体分离。显然，在情况（1）和（2）中，攻击者更容易将智能体分开，因为它们的初始状态形成的簇与网络拓扑结构相吻合。

然而，在情况（3）中，初始状态值并不具备这类性质，因此状态最终收敛到同一数值，如图13所示。在这次仿真中，攻击者无法始终有效地攻击某些边；因此，智能体没有被划分为簇，系统也就达成了一致性。如上文第8.1.1节所述，攻击者或许可以通过更高的权重 a 阻止一致性。

为得到图11–13，我们求解组合优化问题，以确定参与者的最优策略。需要指出的是，该问题的计算复杂度取决于 $\mathcal{G}$的边数 $\mathcal{E}$。我们通过忽略一些显然不是最优的边组合，降低了计算复杂度；例如，只攻击连接智能体4和7的边并不能使图断开，因此不可能是攻击者的最佳行动。

8.1.3 变化的能量和成本参数

下面继续讨论攻击者的充能速率 ρ^{A} 以及攻击单位成本 β^{A} 和 $\overline{\beta}^{\mathrm{A}}$对一致性和簇形成的影响。回顾第5节和第6节中的理论结果，利用 ρ^{A}与 $\overline{\beta}^{\mathrm{A}}$ 以及 ρ^{A} 与 β^{A} 的比值，可以推导出防止达成一致性的必要条件和充分条件，以及无限时间内形成的簇数量的上界。

假设 $b = 0$，如命题9所述，簇的数量由 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}}$ 决定。我们在图14中展示了底层图 $\mathcal{G}$ 的不同拓扑结构下簇的数量。我们考虑具有

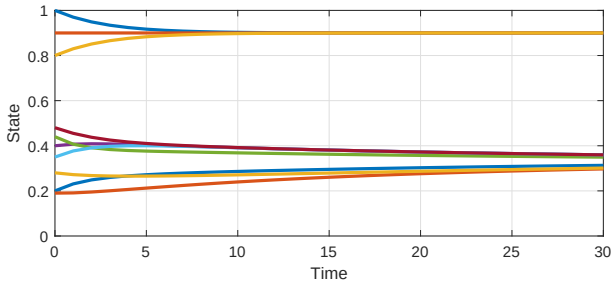


图11. 情况1中的智能体状态

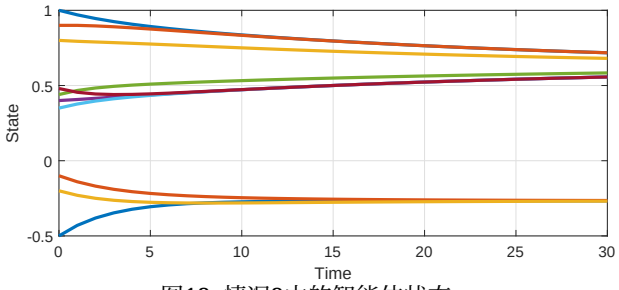


图12. 情况2中的智能体状态

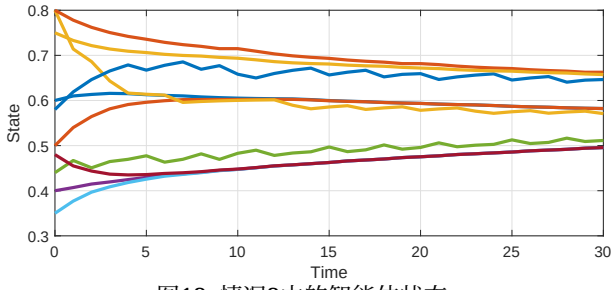


图13. 情况3中的智能体状态

$n = 5$，边的位置安排使其形成最连通的拓扑结构，即在边数 $|\mathcal{E}|$相同的情况下使 λ最大。请注意，对于 $n = 5$，底层图 $\mathcal{G}$ 中最多有 $n(n-1)/2 = 10$ 条边（完全图 $\mathcal{G}$ 即为这种情况）。我们观察到，对于 $\rho^{\mathrm{A}}/\overline{\beta}^{\mathrm{A}} \geq |\mathcal{E}|$，智能体被分成5个簇（所有智能体彼此分离），如图左上方标记为“5”的区域所示，这与命题6推导出的结果一致；而在右下方标记为“1”的区域，智能体则收敛到同一个簇。显然，在连通性更强的图中，智能体更有可能收敛到较少的簇。

8.2 不同时间范围长度和博弈周期下的玩家表现

在本小节中，我们评估参与者在不同的时域长度 h 和博弈周期 T下的表现。为评估参与者的表现，我们引入实际效用 $\hat{U}^{\mathrm{A}k} := az_k(\overline{\mathcal{E}}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{D}*}) - bc(\mathcal{G}_k^{\mathrm{D}*})$ 和 $\hat{U}_k^{\mathrm{D}} := -az_k(\overline{\mathcal{E}}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{A}*}, \mathcal{E}_k^{\mathrm{D}*}) + bc(\mathcal{G}_k^{\mathrm{D}*})$，其中$\mathcal{G}_k^{\mathrm{D}*} = (\mathcal{V}, ((\mathcal{E} \setminus (\overline{\mathcal{E}}_k^{\mathrm{A}*} \cup \mathcal{E}_k^{\mathrm{A}*})) \cup \mathcal{E}_k^{\mathrm{D}*})$。这些是效用函数 h 和 T中的元素，

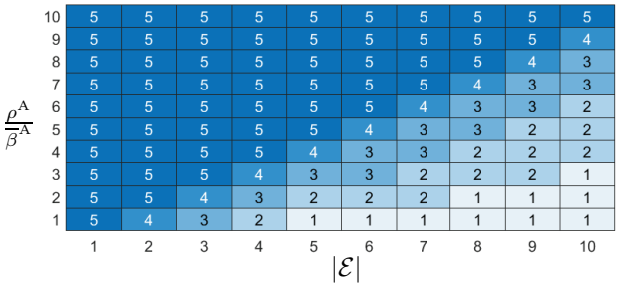


图14. 当 $k=50$ 为 $b=0$ 时的簇数量。所使用的底层图均包含5个智能体，最多有10条边。

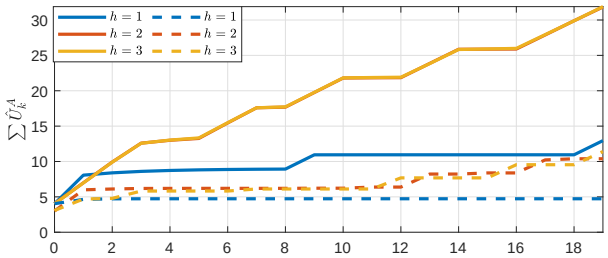


图15. 在路径图（实线）和完全图（虚线）中，h 取不同值时的 $\sum_k \hat{U}_k^{\mathrm{A}}$。路径图中 $h=2$ 和 $h=3$ 的实际效用几乎相同。

对应于博弈索引为 $l=\lfloor k/T \rfloor+1$ 的博弈中的第 α 步（$\alpha = k \bmod T+1$），此时采用所获得的策略 $(\overline{\mathcal{E}}^{\mathrm{A}*}{}_{(l-1)T+\alpha-1}, \mathcal{E}^{\mathrm{A}*}_{(l-1)T+\alpha-1}, \mathcal{E}^{\mathrm{D}*}_{(l-1)T+\alpha-1}) = (\overline{\mathcal{E}}^{\mathrm{A}*}_{l\,\alpha}, \mathcal{E}^{\mathrm{A}*}_{l\,\alpha}, \mathcal{E}^{\mathrm{D}*}_{l\,\alpha})$。由于 $U_l^{\mathrm{A}} = -U_l^{\mathrm{D}}$，攻击者的实际效用越高，防御者的实际效用就越低。请注意，h和 T 的值在参与者之间是一致的。

在本小节中，我们考虑式（2）中的权重 $a_{ij}=\hat{a}$、$\hat{a}<1/n$，这意味着不同智能体的收敛速度因其邻居数量而异。此外，我们考虑智能体的多种初始状态 x_0，以便更准确地评估攻击者的表现以及实际效用的模式 $\hat{U}_k^{\mathrm{A}}$。在本次仿真中，我们为每个智能体使用多达1000个随机生成的初始状态，取值范围为 -1 至1。本小节中，我们使用参数 $n=3$、$\rho^{\mathrm{A}}=1.1$、$\kappa^{\mathrm{A}}=7$、$\overline{\beta}^{\mathrm{A}}=2\beta^{\mathrm{A}}=1$。

8.2.1 不同视界长度下的参与者表现

现在，我们考虑网络为路径图和完全图时，时域长度 h 变化的情况。请注意，攻击者和防御者的 h 值仍然相同。图15展示了攻击者所获得的效用 $\hat{U}_k^{\mathrm{A}}$ 随 h 变化的演变情况（每个 h对应$T=1$）。

表3 路径图中 $\mathcal{G}$ 在 $h=2$ 和 $h=3$之间的最优动作及由此产生的效用差异

初始状态	$\lvert\overline{\mathcal{E}}_0^{\mathrm{A}*}\rvert$		$\sum_{k=0}^{19}\hat{U}_k^{\mathrm{A}}$	
	$h=2$	$h=3$	$h=2$	$h=3$
$[0.824,\ -0.798,\ -0.413]^{\mathrm{T}}$	2	2	37.74	
$[-0.983,\ 0.649,\ 0.535]^{\mathrm{T}}$	2	2	39.89	
$[-0.787,\ -0.786,\ -0.265]^{\mathrm{T}}$	2	1	28.41	30.00
$[0.624,\ 0.629,\ -0.821]^{\mathrm{T}}$	2	1	37.92	43.45

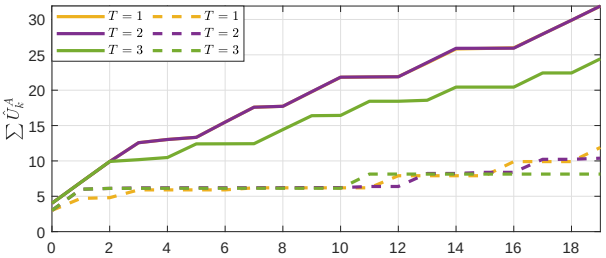


图 16. 路径图（实线）和完全图（虚线）中的 $\sum_k \hat{U}_k^{\mathrm{A}}$随 T 变化的情况。路径图中 $T=1$ 和 $T=2$ 的实际效用几乎相同。

由于路径图是连通性最弱的图，相较于连通性更强的图，攻击者能够相对轻松地将智能体划分为多个群组。因此，攻击者可能不需要很长的时域长度 h 就能提高效用，因为与完全图的情况相比，它无需节省那么多能量。图15中红色和黄色实线重叠，说明时域长度 $h=3$ 已能达到与 $h=2$相当的效果。另一方面，蓝色实线远低于红色和黄色实线，这表明h 过短会导致攻击者随着时间推移获得更低的效用。

表3展示了路径图中 $\mathcal{G}$ 在 $h=2$ 和$h=3$ 之间一些值得注意的情形下，攻击者策略的差异。这里，我们可以看到，尽管图15中实际效用的曲线非常相似，但路径图中，时域为 $\mathcal{G}$ 时，时域为 $h=2$和 $h=3$ 的攻击者在最优动作上存在差异。我们观察到，当某些智能体的初始状态足够接近时，时域为 $h=2$ 的攻击者会在 $k=0$持续攻击两条边，而时域为 $h=3$的攻击者则选择攻击较少的边以节省能量。在$k=19$，时域为 $h=3$ 的攻击者获得了更高的实际效用，这表明它能够比时域为 $h=2$ 的攻击者更好地利用能量，尽管后者较晚才发起攻击。

另一方面，由于完全图是连通性最强的图，攻击者需要消耗更多能量才能使图断开并获得一些效用。因此，即使 h 更长，$\sum \hat{U}_k^{\mathrm{A}}$ 的差异也比路径图的情况小。这个差异

不过，红色虚线与黄色虚线之间的差异更加明显，这表明攻击者仍能从拥有 $h = 3$ 中获益（而路径图情况下的差异则微乎其微）。攻击者在路径图和完全图中的不同表现 $\mathcal{G}$ 表明，在攻击者的能量参数给定时，对于连通性较弱的图，较长的 h 所带来的效果可能会比连通性较强的图 $\mathcal{G}$ 更早达到饱和。

一般而言，我们观察到，较长的 h 可能会随着时间推移带来更高的攻击者实际效用，因为攻击者在博弈中担任领导者，即攻击者先行动，并能够选择使防御者的最优响应效用最小化的策略。此外，$\sum \hat{U}_k^{\mathrm{A}}$何时增加也呈现出明显的规律；这表明，初始状态的变化可能不会影响攻击者的最优策略，但上文所述的某些情况除外。

我们还注意到，不同 h 的影响也取决于底层图 $\mathcal{G}$。具体而言，在连通性较弱的图 $\mathcal{G}$中，时域非常短甚至可能比在连通性较强的 $\mathcal{G}$中更不利。例如，在图 16 中，路径图中 $\sum \hat{U}_k^{\mathrm{A}}$在 $h = 1$ 和 $h = 2$ 之间的差异，比完全图中明显得多。可能的原因是，在路径图中，攻击者更容易断开所有智能体之间的连接，并在某些时间步形成 n 群组。因此，当 h 足够大时，攻击者可以节省足够的能量，从而更频繁地形成 n 群组。另一方面，我们还观察到，对于路径图而言，将时域长度从 $h = 2$ 增加到 $h = 3$ 对攻击者效用的影响很小，这表明时域长度超过某个值后，再继续增加可能不再有益。正如我们稍后将看到的，改变 T的取值时也会出现类似现象。

8.2.2 不同博弈周期下参与者的表现

接下来，我们通过模拟博弈周期取不同值的情况继续分析 T （对于双方， h 的值均设为 $h = 3$ ，因此假设 $T \leq h$ 始终成立）。$\sum \hat{U}_k^{\mathrm{A}}$ 随时间变化的平均值如图 16 所示。总体而言，无论是在路径图还是完全图中，博弈周期 T 较短的攻击者都有更高的实际效用，尤其是在后期 $\mathcal{G}$。

较短的 T 使攻击者能够更灵活地适应智能体和参与者条件的变化。在此博弈情境下，较短的 T 可能会使攻击者进一步推迟攻击，以便在之后最大化其效用。这反过来会提高攻击者之后的效用，与上文讨论的较长 h 情况类似。请注意，黄色虚线和实线与图15中的黄色线相同；我们可以看到，绿色线和紫色线的差异不像红线和

表4 路径图中受到攻击的边的平均总数 $\mathcal{G}$

h	T	$\sum_{m=0}^{k}\lvert\mathcal{E}_m^{\mathrm{A}*}\rvert$（普通）		$\sum_{m=0}^{k}\lvert\overline{\mathcal{E}}_m^{\mathrm{A}*}\rvert$（强）	
		$k=9$	$k=19$	$k=9$	$k=19$
1	1	7	16	5	6
2		0	0	8	13.959
3		0	0	7.993	13.971
	2	0	0	8	13.970
	3	2.970	4.970	7.003	11.015

图15中的蓝线那样明显，这表明对攻击者而言， T的值较大未必像 h较短那样不利。

表4展示了在 h 和 T 取不同值时，普通和强干扰信号攻击的边的平均数量。值得注意的是，对于 $h > T$，攻击者从不使用普通信号攻击任何边，这表明它倾向于保存能量，以便稍后用于更强力的攻击。因此，使用 $h > T$ 强力攻击的边数多于 $h = T$ 的情况，从而带来如上所述更高的实际效用。我们还可以观察到，在 $h = 3$ 和 $T = 1$ 的情况下，攻击者平均而言在 $k = 19$ 强力攻击的边数多于表4中的其他情况，尽管在 $k = 9$ 攻击的边数略少于 h 和 T 取值较为接近的情况。这表明，当 h 较大且 T 较小时，攻击者倾向于保存更多能量。

9 结论

我们构建了一个关于弹性多智能体系统簇形成的双人博弈，且该博弈随时间进行。参与者会考虑其行动对未来通信拓扑和智能体状态的影响，并根据滚动时域方法调整策略。我们推导了智能体形成簇的必要条件和充分条件。我们讨论了效用函数权重和不同初始状态对簇形成的影响，并评估了时域长度和博弈周期变化对参与者表现的影响。

未来可能的扩展包括：参与者的效用函数不是零和的情形、参与者不具备完全知识的情形，以及每个智能体都能够以分散式方式自行决定策略的情形。我们还在 [22] 中考虑了参与者的时域长度和博弈周期不统一的情形。该情形还可以进一步推广到分散式设置，在其中智能体以异步方式自行决定策略。

此外，考虑参与者可能并不完全了解其他参与者的情形也很有意义。 [23]中探讨了这种不完全信息博弈。

参考文献

[1]C. Altafini. 含对抗性相互作用的网络一致性问题。*IEEE Trans. Autom. Control*，58(4):935–946，2013年。[2] F. Bullo. *Lectures on Network Systems*。Kindle Direct Publishing，2019年。[3] A. Cetinkaya、H. Ishii 和 T. Hayakawa。随机丢包和恶意丢包条件下的网络化控制。*IEEE Trans.Autom. Control*，62:2434–2449，2017年。[4] A. Cetinkaya、H. Ishii 和 T. Hayakawa。时变干扰对网络化镇定的影响。*SIAM J. Control Optim.*，56:2398–2435，2018年。[5] A. Cetinkaya、K. Kikuchi、T. Hayakawa 和 H. Ishii。用于防御多智能体一致性中干扰攻击的随机化传输协议。 *Automatica*，117，2020年。[6] J. Chen、C. Touati 和 Q. Zhu。用于安全且弹性的基础设施网络战略设计的动态博弈方法。*IEEE Trans. Inf. Forensics Security*，15:462–474，2020年。[7] G. De Pasquale 和 M. Elena Valcher。具有合作与对抗关系的智能体集群的一致性。*Automatica*，第110002页，2022年。[8] S. M. Dibaji、H. Ishii 和 R. Tempo。弹性随机量化一致性。*IEEE Trans. Autom. Control*，63(8):2508–2522，2018年。[9] D. Fudenberg 和 J. Tirole。 *Game Theory*。麻省理工学院出版社，1991年。[10]X. Gong、L. Duan、X. Chen 和 J. Zhang。当社交网络效应遇上无线网络中的拥塞效应：数据使用均衡与最优定价。*IEEE J. Sel.Areas Commun.*，35(2):449–462，2017年。[11] H. Ishii 和 Q. Zhu。 *Security and Resilience of Control Systems: Theory and Applications*， *Lecture Notes in Control and Information Sciences*，第489卷。施普林格，2022年。[12]L. Jia、Y. Xu、Y. Sun、S. Feng 和 A. Anpalagan。无线网络抗干扰防御的斯塔克尔伯格博弈方法。 *IEEE Wireless Commun.*，25:120–128，2018年。[13] M. L. Katz 和 C. Shapiro。系统竞争与网络效应。 *Journal of Economic Perspective*，8:93–115，1994年。[14]Y. Kuwata、T. Schouwenaars、A. Richards 和 J. How。用于轨迹规划的鲁棒约束滚动时域控制。载于 *Proc. AIAA Guidance*， *Navigation*， *and Control Conference and Exhibit*，第6079页，2005年。[15] H. Li 和 W. Yan。一般线性多智能体系统中基于滚动时域控制的一致性方案。*Automatica*，56:12–18，2015年。[16] Y. Li、C. A. Courcoubetis、L. Duan 和 R. Weber。具有网络外部性的点对点共享最优定价。*IEEE/ACM Trans. Netw.*，29(1):148–161，2021年。[17]Y. Li、D. E. Quevedo、S. Dey 和 L. Shi。针对远程状态估计的基于信干噪比的拒绝服务攻击：一种博弈论方法。*IEEE Trans. Control Netw. Syst.*，4:632–642，2017年。[18]Y. Li、D. Shi 和 T. Chen。针对网络化控制系统的虚假数据注入攻击：斯塔克尔伯格博弈分析。*IEEE Trans. Autom. Control*，63:3503–3509，2018年。[19]Y. Nugraha、A. Cetinkaya、T. Hayakawa、H. Ishii 和 Q. Zhu。通过动态弹性图博弈实现多智能体一致性中的簇形成。载于 *Proc. IEEE Conf. ControlTech. App.*，第735–740页，2021年。[20]Y. Nugraha、A. Cetinkaya、T. Hayakawa、H. Ishii 和 Q. Zhu。应用于多智能体一致性的动态弹性网络博弈。*IEEE Trans. Control Netw. Syst.*，8:246–259，2021年。[21] Y. Nugraha、A. Cetinkaya、T. Hayakawa、H. Ishii 和 Q. Zhu。弹性多智能体系统簇形成的滚动时域博弈。载于 *Proc. IEEE Conf. Dec.Contr.*，第4829–4834页，2021年。[22] Y. Nugraha、A. Cetinkaya、T. Hayakawa、H. Ishii 和 Q. Zhu。具有非均匀时域的弹性网络滚动时域博弈。*European Journal of Control*，68:100693，2022年。[23] Y. Nugraha、T. Hayakawa、H. Ishii、A. Cetinkaya 和 Q. Zhu。弹性多智能体系统的双人不完全博弈。arXiv:2212.01570。[24]M. Pirani、E. Nekouei、H. Sandberg 和 K. H. Johansson。基于 $\mathcal{H}_2$ 表现指标的一致性动态中攻击者—防御者博弈的图论均衡分析。*IEEE Trans. Netw. Sci. Eng.*，8:1991–2000，2021年。[25] H. Sandberg、S. Amin 和 K. H. Johansson。网络化控制系统信息物理安全特刊。 *IEEEControl Syst. Mag.*，35:20–23，2015年。[26] A. Sanjab 和 W. Saad。针对多个对手的智能电网数据注入攻击：博弈论视角。*IEEE Trans. Smart Grid*，7:2038–2049，2016年。[27]T. Schouwenaars、J. How 和 E. Feron。具有隐式安全保证的滚动时域路径规划。载于 *Proc.American Control Conference*，第5576–5581页，2004年。[28] D. Senejohnny、P. Tesi 和 C. De Persis。用于自触发网络协调的抗干扰算法。*IEEE Trans. Control Netw. Syst.*，5:981–990，2018年。[29] Y. Shang。多智能体系统的弹性簇共识。*IEEE Trans. Syst.*， *Man*， *Cybern.*， *Syst.*，52:346–356，2022年。[30] E. Stefansson、J. F. Fisac、D. Sadigh、S. S. Sastry 和 K. H. Johansson。利用分层动态博弈实现卡车编队行驶中的人机交互。载于 *Proc. European ControlConference*，第3165–3172页，2019年。[31]W. Ren 和 R. W. Beard。动态变化的交互拓扑下多智能体系统中的共识寻求。*IEEE Trans. Autom. Control*，50(5):655–661，2005年。[32]B. Wang、Y. Wu、K.J. Ray Liu 和 T.C. Clancy。认知无线电网络中的抗干扰随机博弈。 *IEEEJ. Sel. Areas Commun.*，29(4):877–889，2011年。[33] D. Yang、G. Xue、J. Zhang、A. Richa 和 X. Fang。应对无线网络中的智能干扰器：一种斯塔克尔伯格博弈方法。 *IEEE Trans. Wireless Commun.*，12:4038–4047，2013年。[34]M. Zhu 和 S. Martinez。信息物理系统中相关攻击的斯塔克尔伯格博弈分析。载于 *Proc.American Control Conference*，第4063–4068页，2011年。[35]M. Zhu 和 S. Martinez。重放攻击下弹性网络化控制系统的表现分析。*IEEE Trans. Autom. Control*，59(3):804–808，2014年。