arXiv:2304.00551v1 [cs.RO] 2 Apr 2023

动态群体审查：动态通信网络中恶意机器人的协同检测

Matthew Cavorsi*、Frederik Mallmann-Trenn*、David Salda˜na 和 Stephanie Gil

摘要——大量联网机器人的协同是一项艰巨任务，尤其是在机器人不断移动于环境中且网络内存在恶意攻击的情况下。文献中提出了多种检测恶意机器人的方法，例如消息抽样和可疑行为分析。然而，这些方法要求每个机器人都对网络中的其他所有机器人进行抽样，导致检测过程缓慢，进而降低团队性能。本文提出一种方法，可显著缩短合法机器人识别恶意机器人的检测时间；该方法适用于合法机器人在环境中随机移动的场景。我们的方法借助“Crowd Vetting”这一概念，利用随机遭遇中的观测以及可信邻近机器人的意见，迅速提高恶意机器人检测的准确性。其核心思路是：只要每个合法机器人都能准确估计团队中至少某个固定子集的合法性，它们从可信邻居处获得的二手信息就足以纠正任何误分类，并准确估计团队其他成员的信任度。我们证明，这个固定子集的规模可以表示为图和随机游走的基本性质的函数。此外，我们从形式上证明，随着团队中的机器人数量增加，检测时间仍保持不变。我们推导出一个闭式表达式，用于计算算法成功识别每个机器人真实合法性所需的临界时间步数，使失败概率不超过指定值。我们通过模拟验证了理论结果，结果表明，与未利用可信邻居信息的先前研究相比，本方法可显著缩短检测时间。

I. 引言

多机器人团队能够协作完成单个机器人无法独立完成的众多任务 [1], [2]，例如覆盖或持续监视 [3], [4],、大范围高效探索 [5]，以及群集行为 [6],等。然而，只要任务的成功完成需要多个机器人的协调，就可能出现恶意或不合作的机器人，从而妨碍团队的表现。近期研究利用了“观察型”机器人的概念，并收集信息，以识别可能不可信的机器人 [7],[8], [9], [10], [11], [12]。此类信息下文称为信任观察，其核心原则是：收集更多信息或多条信任观测，可以提高机器人间信任的准确性 [13], [14]。

以往研究从控制视角出发，通过设计策略促使机器人频繁相遇，从而收集信任观测。例如， [15]中的研究为团队设计了特定路线，让其在环境中巡逻，以策略性地增加机器人间交互的机会。然而，这要求机器人相互配合并遵循预定义路线。 [16], [17], [18], [19] 中的论文考虑了将环境离散为多个区域（称为站点）的情形，机器人通过巡逻持续监视这些站点，同时维持各站点上机器人分布的理想状态。在我们先前的工作 [16], 中，我们提出了一种策略，通过采用类似随机游走的随机站点转移规则，鼓励机器人频繁相遇，从而缩短检测时间。然而，该策略要求每个机器人都与其他每个机器人多次相遇，才能形成准确的信任估计。这一过程可能耗时很长，尤其是在机器人或站点数量增加时。

一种名为 *Crowd Vetting* [13] 的最新算法利用了意见动力学 [20], [21], ，其中可信邻居的意见可用于强化机器人对另一机器人的意见。在 Crowd Vetting 算法中，合法机器人共享意见；研究表明，这种做法能够改善其信任估计，同时所需的观测次数少于机器人仅依赖自身观测时的情况

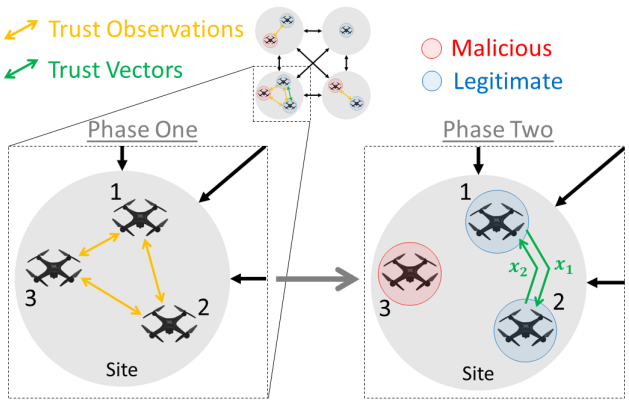


图 1. 动态 Crowd Vetting 算法示意图。阶段 1 中，机器人在站点间移动，同时收集对所遇到的其他机器人的信任观测，并将其存储在本地信任向量中。阶段 2 中，机器人与可信邻居共享其信任向量，以提高正确判定其他机器人可信度的概率。

作者衷心感谢美国空军科学研究办公室提供的部分资助 [，资助编号：FA9550-22-1-0223]，；美国海军研究办公室（ONR）青年研究员计划（YIP）[，资助编号：N00014-21-1-2714]；以及英国工程与自然科学研究委员会（EPSRC）[，资助编号：EP/W005573/1.]。

（*共同第一作者）。Matthew Cavorsi 和 Stephanie Gil 任职于哈佛大学工程与应用科学学院，美国马萨诸塞州剑桥市（电子邮箱：mcavorsi@g.harvard.edu；sgil@seas.harvard.edu）

Frederik Mallmann-Trenn 任职于英国伦敦国王学院信息学系（电子邮件：frederik.mallmann-trenn@kcl.ac.uk）

David Salda˜na 就职于美国宾夕法尼亚州伯利恒利哈伊大学的自主与智能机器人实验室（AIRLab）（电子邮件：saldana@lehigh.edu）

。然而，现有的 Crowd Vetting 算法仅适用于静态网络，在这种网络中，每个机器人随时间推移观测的都是相同的机器人子集。虽然动态网络增加了机器人相遇的多样性，从而暗示利用可信邻居意见可以带来更大的益处，但要规范每对机器人彼此拥有的信任观测数量却变得越来越困难。这带来了新的挑战，因为每个机器人对其他每个机器人拥有的观测数量可能不同，因此机器人之间共享的信息具有不同程度的准确性，难以就信任估计得出任何分析性的性能保证。此外，天真地使用来自不可信来源的间接信息，可能导致错误在团队中传播。

本文的主要贡献是开发了一种称为 动态群体审查 (DCV) 的算法。在动态网络中，该算法允许合法机器人利用可信邻居的二手（间接）意见，从而显著缩短检测时间。我们的 DCV算法分两个阶段进行信任估计。在阶段 1，机器人在各站点之间移动，以估计团队的可信度，并将估计结果存储在一个称为信任向量的向量中。阶段 1 的目标是正确分类团队中至少一个固定子集 的成员。随后，在阶段 2，机器人继续在各站点之间移动，同时与自己信任的其他机器人分享意见，即信任向量。最后，我们证明，只要每个合法机器人在阶段 1 正确分类团队中足够比例的成员，基于共享信息判断信任的相对简单的多数规则算法就足以纠正误分类，并遏制大范围错误信息的传播。此外，我们证明，所需比例可以表示为图和随机游走性质的函数。另外，我们从理论上证明，随着团队中的机器人数量增加，检测时间仍保持不变。这与个体协议 中观察到的时间步数呈对数增长形成对比；在个体协议中，机器人不会利用邻居的意见。

II. 问题表述

考虑一个由 $N_{\mathcal{R}}$ 个机器人组成的团队 $\mathcal{R}=\{1,2,\ldots,N_{\mathcal{R}}\}$，它们在一个由多个区域（也称为站点）构成的离散环境中移动。该环境是一个以无向图 $\mathcal{G}=(\mathcal{V},\mathcal{E})$ 建模的拓扑地图，其中顶点 $\mathcal{V}=\{1,2,\ldots,N_{\mathcal{V}}\}$ 表示站点，边 $\mathcal{E}\subseteq\mathcal{V}\times\mathcal{V}$ 表示站点之间的路径；运算符 $\times$ 表示两个集合的笛卡尔积。如果存在边 $(\iota,\ \omega)\ \in\ \mathcal{E}$，机器人就可以从站点 ι 移动到站点 ω 。此外，机器人始终可以留在当前位置，即对于所有 $\iota\ \in\ \mathcal{V}$，都有 $(\iota,\ \iota)\ \in\ \mathcal{E}$ 。我们假设图 $\mathcal{G}$ 是连通的，因此任意一对站点之间始终存在一条路径。如果机器人位于同一站点，就可以相互通信或观测彼此。机器人 i 的邻域记为 $\mathcal{N}_i(t)$，由机器人 i 在时间步 t 能够观测到的所有机器人 $j\ \in\ \mathcal{R}$ 组成。为便于分析，我们将每个机器人 i 都纳入其自身的邻域 $\mathcal{N}_i(t)$。时间步定义为机器人在相邻站点之间进行状态转移并观测该站点机器人的一次机会；也就是说，任何机器人都可以在任意时间步转移到新站点并获取新的观测。

A. 背景

1) 在动态网络中收集信任观测：本文研究这样一类问题：团队中可能有一个未知子集是恶意的，记为 $\mathcal{M}\ \subset\ \mathcal{R}$；而合法 机器人 $\mathcal{L}\ =\ \mathcal{R}\backslash\mathcal{M}$ 可以利用彼此的观测（我们称之为信任观测）来验证信息以及邻近机器人的合法性。机器人 j 对机器人 i的信任观测记为 $\alpha_{i,j}(t)$，它表示对机器人 j合法性的一种带噪声且不完美的测量。 [1] 我们假设，对于任意机器人对 (i,j) 以及任意时刻 t，信任观测彼此独立；并且机器人只有在彼此为邻居时才能相互收集观测，即 $j\ \in\ \mathcal{N}_i(t)$。此外，尽管我们不对信任观测的分布作任何假设，但出于分析目的，我们对其期望施加了特定假设。与文献 [7], [13], [14], 类似，我们假设信任观测满足

$$\mathbb{E}\left[\,\alpha_{i,j}(t)\mid j\in\mathcal{L}\,\right]\geq 1/2+\varepsilon_{\alpha},\tag{1}$$

and

$$\mathbb{E}\left[\,\alpha_{i,j}(t)\mid j\in\mathcal{M}\,\right]\leq 1/2-\varepsilon_{\alpha},\tag{2}$$

其中，数值 $\varepsilon_{\alpha}\in(0,\ 1/2]$ 表示观测的质量。数值较低的 $\varepsilon_{\alpha}\approx 0$ 表示该观测完全模糊不清，而当观测具有 $\varepsilon_{\alpha}\approx 1/2$时，则几乎可以确定传输机器人的合法性。在 [16],中，每个机器人都维护一个信任向量，记作$\mathbf{x}_i(t)$。信任向量的目的是存储团队中其他每个机器人的正确合法性信息：向量$\mathbf{x}_i(t)$的 j^{th} 项（记作 $[\mathbf{x}_i]_j(t)$)中，1表示机器人 i 认为机器人 j 值得信任，而 $[\mathbf{x}_i]_j(t)\ =\ 0$ 则表示其他情况。由于信任观测$\alpha_{i,\ j}(t)$被假定为含有噪声，因此，每个机器人都需要对其邻居进行多次观测，才能对其信任向量的有效性形成一定的置信度。在 [16] 中，每个机器人对其他每个机器人所需观测的具体数量记作 n_{α}，并假定该数量是任意但已知的。本文将通过分析确定，在使用我们提出的算法时，为达到期望的成功概率 $1-\delta/N_{\mathcal{R}}$，所需的适当观测数量 n_{α}；该成功概率对应于用户设定的失败概率 δ。我们旨在最大限度地减少所需的信任观测数量，以及收集这些观测所需的时间窗口 T，并采用*Crowd Vetting* 算法。

[1]此类观测的一个例子见于 [14] [7], [13], 中的研究。在这些研究中，信任观测具有随机性，并由无线传输的物理属性决定。

2）Crowd Vetting 算法：Crowd Vetting 算法 [13] 利用意见动力学，使机器人能够与其可信邻居共享信任向量，从而不仅使所有合法邻居就其信任向量达成一致，还能提高所达成的信任向量正确的概率。然而，当前形式的 Crowd Vetting 算法仅适用于所有机器人在每个时间步都与同一组邻居通信的情况（静态通信网络）。目标是让所有合法机器人就最终的信任向量$\mathbf{x}_i^*$达成一致，使得对于每个机器人 $j \in \mathcal{R}$,

$$[\mathbf{x}_i^*]_j = \begin{cases} 1, & \text{if } j \in \mathcal{L}, \\ 0, & \text{if } j \in \mathcal{M}. \end{cases} \tag{3}$$

为此，每个机器人 $i \in \mathcal{L}$ 都会收集其他每个机器人的 n_α 信任观测，并根据这些观测形成一个中间信任向量。然后，每个机器人将其中间信任向量分享给其可信邻居，并根据自身与可信邻居的意见采用多数规则，判定是否信任其他机器人。本文将 Crowd Vetting 算法扩展到机器人会移动的场景中，因此机器人在每个时间步都可能与不同的机器人相遇。

3) 图上的随机游走：本文的结果在一定程度上取决于站点图的拓扑结构，以及合法机器人在站点间移动时所进行的随机游走。我们将合法机器人 i的轨迹定义为一组状态，记作 $\chi_i(1)\ \chi_i(2) \ldots, \chi_i(t_f)$，这些状态对应于从任意起始时间 $t = 1$ 到任意结束时间 $t = t_f$期间，该机器人在每个时间步所处的站点。机器人的轨迹取决于它在站点图上执行的随机游走。我们假设机器人执行的随机游走是不可约且非周期的，因此具有唯一的平稳分布 π。我们将机器人相互收集信任观测所需的时间表示为图的相遇时间（记作 T_{meet}）、图的命中时间（记作 T_{hit}）以及图的混合时间（记作 T_{mix}）的函数。有关这些量的直观解释，请参见 [22]。相遇时间定义为 $T_{\text{meet}} = \max_{\iota,\omega} T_{\text{meet}}(\iota, \omega)$，其中 $T_{\text{meet}}(\iota, \omega)$ 是从节点 ι 和 ω 出发的随机游走相遇所需时间的期望值。如果机器人 i和 j 执行的两次随机游走在某个时间 κ满足 $\chi_i(\kappa) = \chi_j(\kappa)$，我们就称它们相遇。命中时间定义为 $T_{\text{hit}} = \max_{\iota,\omega} T_{\text{hit}}(\iota, \omega)$，其中$T_{\text{hit}}(\iota, \omega)$ 是从节点 ι 出发的随机游走到达节点 ω所需时间的期望值。相遇时间和命中时间是研究充分的马尔可夫链量，有兴趣的读者可在[23, 第 169]页找到常见图的相关界限。此外，我们使用[24, 定理 3.1] 和 [25, 定理 1], , 分别计算了模拟中所用图的命中时间和相遇时间。最后，混合时间 T_{mix} 是机器人所处站点的分布随时间近似收敛至平稳分布 π所需的时间。

B. 问题陈述

本文将 Crowd Vetting 算法扩展为支持动态场景，例如移动机器人邻居集合可能随时间变化的情况。当对站点转移进行建模的图 $\mathcal{G}$是连通图时， [26]已证明所有机器人 $i \in \mathcal{L}$ 最终都会访问图中的每个站点 $\mathcal{G}$。这意味着，只要时间窗口 $t = \{t_0, t_0 + T\}$足够长，每个机器人都会遇到所有其他机器人；该时间窗口的长度为从某个任意初始时刻 t_0起经过的时间 T 。

问题 1. 给定期望的失败概率 δ 和信任观测 $\alpha_{i,\ j}(t)$ 满足 (1) 和(2)，设计一种算法，以缩短时间窗口 T 的长度$t \in \{t_0, t_0 + T\}$，使所有机器人 $i \in \mathcal{L}$以至少 $1 - \delta/N_{\mathcal{R}}$ 的概率返回正确的最终信任向量 $\mathbf{x}_i^*$ 。

III. 算法

为了将 Crowd Vetting 算法扩展到支持动态场景，我们首先引入时间窗口邻域 这一概念，用于捕捉机器人在时间窗口 T内相遇的历史。

定义1（时间窗口邻域）。机器人 i 的时间窗口邻域定义为其在时间窗口 T 内所有邻居集合的并集，即$\mathcal{N}_i^T(t) = \bigcup_{\kappa=t-T}^{t} \mathcal{N}_i(\kappa)$，对任意 $t > T$ 均成立。

在时间窗口邻域中，由于每个机器人的邻居可能在每个时间步发生变化，因此很难确保机器人能够足够多次地收集到其他所有机器人的信任观测。接下来，我们介绍一种仅使用每个机器人对其他机器人的个体（直接）观测来估计信任向量的过程，称为个体协议。

A. 个体协议

在我们先前的工作 [16], 中，当机器人需要估计其邻居的合法性时，它们会通过频繁地在站点之间转移来收集信任观测，这种方式称为快速转移状态。在本工作中，我们将分析重点放在这种快速转移状态上，并将机器人 i在快速转移状态下使用的转移矩阵记为 $\mathbf{P}_i$。我们将快速转移状态定义为一种惰性随机游走

$$[\mathbf{P}_i]_{\iota,\omega} := \begin{cases} \frac{1}{2}, & \iota = \omega, \\ \frac{1}{2 \cdot \sum_{\{\omega \mid (\iota,\omega) \in \mathcal{E}\}} 1}, & (\iota, \omega) \in \mathcal{E}, \\ 0, & \text{otherwise}, \end{cases} \tag{4}$$

其中 $[\mathbf{P}_i]_{\iota,\ \omega}$ 表示矩阵 $\mathbf{P}_i$ 的第（ι，ω）个元素。我们注意到，所有机器人 $i \in \mathcal{L}$ 使用的快速转移矩阵 $\mathbf{P}_i$ 都相同，因为它们都在同一个站点图上进行随机游走；但我们保留索引 i ，以明确这是机器人 i 使用的转移矩阵，因为后续分析通常从特定机器人 $i \in \mathcal{L}$ 的视角进行。此外，机器人 $j \in \mathcal{M}$ 不一定会使用式（4）中设计的快速转移矩阵。

机器人在环境中移动时，会收集邻居的信任观测。令向量 $\mathbf{o}_{i,\ j}$ 为一个 $\eta_{i,\ j} \times 1$ 向量，其中包含机器人 i 在时间窗口 T 内收集的关于机器人 j 的所有信任观测，其中 $\eta_{i,\ j} \leq T$ 表示这一对机器人收集的观测总数。然后，机器人 i 根据向量$\mathbf{o}_{i,\ j}$ 确定一个值 $\beta_{i,\ j}(t)$，称为信任函数，如下所示：

$$\beta_{i,j}[t] = \sum_{\kappa=1}^{\eta_{i,j}} \left([\mathbf{o}_{i,j}]_\kappa - \frac{1}{2} \right), \tag{5}$$

其中 $[\mathbf{o}_{i,\ j}]_\kappa$ 是向量 $\mathbf{o}_{i,\ j}$中的 κ^{th} 项。根据 (1) 和 (2)，我们知道，若 $j \in \mathcal{M}$，则$\alpha_{i,\ j}(t) < \frac{1}{2}$ 在期望上成立，因此根据期望的线性性，对 (5) 中的求和可得 [14], ，$\beta_{i,\ j}(t) < 0$ 在期望上成立。同理，若 $j \in \mathcal{L}$，则$\beta_{i,\ j}(t) > 0$ 在期望上成立。因此，每个机器人$i \in \mathcal{L}$ 使用信任函数$\beta_{i,\ j}(t)$ 构建其中间信任向量 $\mathbf{x}_i(t)$，其中

$$[\mathbf{x}_i]_j(t) = \begin{cases} 1, & \text{if } \beta_{i,j}(t) \geq 0, \\ 0, & \text{if } \beta_{i,j}(t) < 0. \end{cases} \tag{6}$$

使用个体信任观测估计每个机器人的合法性的完整流程如算法 1 所述。该算法要求机器人按照 (4) 中的转移矩阵 $\mathbf{P}_i$，在站点之间状态转移 $\tau_{\text{ind}} = \frac{4}{\varepsilon_\alpha^2}\log(2N_{\mathcal{R}}^3/\delta)$ T_{meet} 个时间步，目的是为其他每个机器人至少收集 n_α 个信任观测。未能彼此收集至少 n_α 个信任观测的机器人默认选择不信任对方。我们推导出这一持续时间 τ_{ind} 和观测数量 n_α，并在第四节说明这会带来 $1 - \delta/N_{\mathcal{R}}$ 的成功概率。

算法 1 机器人的个体协议 i **(个体)**
输入：时间窗口 τ_{ind} (定理 1)，转移矩阵 $\mathbf{P}_i$ 式 (4) 中的观测数量 n_α (定理 1)
输出：信任向量$\mathbf{x}_i(t)$

1：使用式 (4) 中的快速转移矩阵 $\mathbf{P}_i$，收集邻近机器人的信任观测，持续 τ_{ind} 个时间步。记录在此期间每个机器人收集到的观测总数 $\eta_{i,\ j}$。2：计算信任向量 $\mathbf{x}_i(t) \in \{0,1\}^{N_{\mathcal{R}}}$：对于每个$j \in \mathcal{R}$，如果收集到的机器人 j 的观测数量至少为 n_α，则使用式 (6) 计算该项 $[\mathbf{x}_i]_j(t)$；否则 $[\mathbf{x}_i]_j(t) = 0$。设置 $[\mathbf{x}_i]_i(t) = 1$。

B. 动态 *Crowd Vetting* 算法

DCV算法旨在利用可信邻居意见，通过要求机器人只需进行足够长时间的状态转移，以收集网络中一个子集的 n_α条观测，而非整个网络的观测，从而缩短达到至少 $1 - \delta/N_{\mathcal{R}}$ 成功概率所需的时间 τ_{ind}。将机器人 i 在时间 t 的可信邻域定义为

$$\Theta_i^T(t) := \{j \in \mathcal{N}_i^T(t) \mid [\mathbf{x}_i]_j(t) = 1\}. \tag{7}$$

运行DCV算法的流程见算法2。与个体协议类似，该算法要求每个合法机器人在式（4）中使用状态转移矩阵$\mathbf{P}_i$。此次，机器人分两个阶段在站点之间进行状态转移，时长为$\tau = \min\left\{ f(N_{\mathcal{R}}, |\mathcal{L}|, \delta)T_{\text{hit}}, \frac{4}{\varepsilon_\alpha^2}\log(4N_{\mathcal{R}}^3/\delta T_{\text{meet}} \right\})$ 个时间步，目标是收集整个团队中一个较大子集的至少 n_α条信任观测，其中$f(N_{\mathcal{R}}, |\mathcal{L}|, \delta) = 26(1-1/e)^2 n_\alpha$，$n_\alpha = \frac{8}{0.1\varepsilon_\alpha^2}\log\left(\frac{e^{2e}N_{\mathcal{R}}}{0.1\delta|\mathcal{L}|}\right)$，且$e$为欧拉常数。我们在第四节推导所需的时长 τ和观测数量 n_α，并证明其可使成功概率达到 $1 - \delta/N_{\mathcal{R}}$。

算法2 用于机器人的DCV算法 i
输入：时间窗口 τ （命题 1），转移矩阵$\mathbf{P}_i$ 式（4）中的观测数量 n_α （命题 1）
输出：最终信任向量$\mathbf{x}_i^*$

阶段 1：1：使用 Individual(τ, P_i, n_α) 计算中间信任向量 $\mathbf{x}_i(t) \in \{0,1\}^{N_{\mathcal{R}}}$。阶段 2：2：在收集所有可信邻居$j \in \{\mathcal{N}_i(t)|$[的中间信任向量 $\mathbf{x}_j(t)$的同时，再进行 τ 个时间步的状态转移 $j \in \{\mathcal{N}_i(t)|[\mathbf{x}_i]_j(t) = 1\}$。3：计算最终信任向量 $\mathbf{x}_i^* \in \{0,1\}^{N_{\mathcal{R}}}$：通过多数规则为每个条目 $[\mathbf{x}_i^*]_k$赋值，即，如果$\left(\sum_{j\in\Theta_i^\tau(t)}[\mathbf{x}_j]_k(t)\right) \geq \frac{|\Theta_i^\tau|}{2}$($t$ |)，则为 $[\mathbf{x}_i^*]_k = 1$；否则为 $[\mathbf{x}_i^*]_k = 0$。

算法2通过在阶段 1 缩短运行个体协议的时间，并在阶段 2 利用可信邻居的意见来强化自身意见，使机器人更快地获得最终信任向量。这样，机器人无需充分观察**每个**其他机器人的可信度，因为它们可以依靠可信邻居提供有关自己尚未充分接触过的机器人的信息。

IV. 分析

本节的组织方式与第三节类似。首先，我们对机器人使用个体协议（算法 1）估计所有其他机器人的真实合法性所需的时间进行理论分析。然后，我们分析机器人使用所提出的 DCV 算法（算法2）估计所有其他机器人的真实合法性所需的时间，并展示与个体协议相比所需时间的缩短（基于先前的工作 [16]）。

A. 个体协议

我们首先推导个体协议返回正确最终信任向量$\mathbf{x}_i(t)$所需的时间，其中 $i \in \mathcal{L}$ 对所有对象均成立。

定理 1. 给定用户指定的失败概率 $\delta > 0$、相遇时间为 T_{meet} 的站点拓扑 $\mathcal{G}$，以及满足(1) 和(2)的信任观测 $\alpha_{i,\ j}(t)$。如果所有合法机器人

$i \in \mathcal{L}$使用具有$\mathbf{P}_i$转移矩阵的个体协议（算法*1*），该转移矩阵见(4)，经过 $\tau_{ind} = \frac{4\log(2N_{\mathcal{R}}^3/\delta)}{\varepsilon_\alpha^2}$ ~~T_{meet}~~个时间步，并获得每个其他机器人的 $n_\alpha = \log(2N_{\mathcal{R}}^3/\delta)/(2\varepsilon_\alpha^2)$个观测，那么最终信任向量$\mathbf{x}_i(t)$对于所有 $i \in \mathcal{L}$ 都将以至少 $1 - \frac{\delta}{N_{\mathcal{R}}}$ 的概率正确。

证明。考虑任意合法机器人 $i \in \mathcal{L}$。根据附录 A 中的引理 2，如果机器人 i 收集了关于机器人 j的$n_\alpha = \log(2N_{\mathcal{R}}^3/\delta)/(2\varepsilon_\alpha^2)$条信任观测，则它将以至少 $1-\delta/(2N_{\mathcal{R}}^3)$ 的概率正确地判定另一机器人 j。

如果 $j \in \mathcal{M}$，则有两种情况：1）如果机器人 i 与机器人 j 相遇至少 n_α 次，则正确判定机器人 j 的概率同样至少为 $1-\delta/(2N_{\mathcal{R}}^3)$。2）如果机器人 i 与机器人 j 相遇次数较少，则默认情况下，机器人 i会正确地决定不信任机器人 j。对 $\mathcal{L} \times (\mathcal{L} \cup \mathcal{M})$ 中所有机器人对应用并集界 [27]，可得失败概率至多为 $|\mathcal{L} \times (\mathcal{L} \cup \mathcal{M})| \cdot \frac{\delta}{2N_{\mathcal{R}}^3}$。这里，算子 $\times$ 表示两个集合的笛卡尔积。

下面还需证明，在 $\frac{4\log(2N_{\mathcal{R}}^3/\delta)}{\varepsilon_\alpha^2}$ T_{meet} 个时间步内，机器人 i 与任意机器人~~$j \in \mathcal{L}$~~ 至少相遇 n_α 次。根据马尔可夫不等式 [28,第 3 章，无论机器人 i 和机器人 j 从哪些站点出发，它们在 $2T_{\text{meet}}$ 个时间步后相遇的概率至少为 $1/2$。在经过 $\frac{4\log(2N_{\mathcal{R}}^3/\delta)}{\varepsilon_\alpha^2} T_{\text{meet}} = 8n_\alpha T_{\text{meet}}$ 个时间步后，预期相遇次数至少为 $\mu \geq 2n_\alpha$。因此，根据切尔诺夫界（附录 A 中的命题 2），令 $\gamma = 1/2$，可得相遇次数 X，

$$\begin{aligned}\mathbb{P}[X \leq (1-\gamma)\mu] = \mathbb{P}[X \leq n_\alpha] &\leq e^{-\gamma^2\mu/2} \\ &\leq e^{-n_\alpha/4} \leq \frac{\delta}{2N_{\mathcal{R}}^3}.\end{aligned} \tag{8}$$

对所有合法机器人对应用并集界，可得失败概率至多为 $|\mathcal{L} \times \mathcal{L}| \cdot \frac{\delta}{2N_{\mathcal{R}}^3}$。

将机器人误分类和收集到的信任观测数量不足所对应的失败概率相加，得到$|\mathcal{L} \times (\mathcal{L} \cup \mathcal{M})| \cdot \frac{\delta}{2N_{\mathcal{R}}^3} + |\mathcal{L} \times \mathcal{L}| \cdot \frac{\delta}{2N_{\mathcal{R}}^3} \leq \frac{\delta}{N_{\mathcal{R}}}$。 □

我们注意到，定理 1 的界在以下意义下是紧的：存在一类无限多个图，使得所有机器人对至少相遇 $\Omega(\log N_{\mathcal{R}})$ 次所需的时间不低于 $\Omega(T_{\text{meet}} \log N_{\mathcal{R}})$。不同站点数量构成的路径图就是一个例子。

B. 动态 Crowd Vetting 算法

接下来我们给出本文的主要结果，即 DCV算法返回所有 $i \in \mathcal{L}$的正确最终信任向量 $\mathbf{x}_i^*$所需的时间。首先，设

$$q = \frac{\delta\rho_1}{e^{2e}} \frac{|\mathcal{L}|}{N_{\mathcal{R}}}, \tag{9}$$

$$n_\alpha = \frac{8}{\rho_1\varepsilon_\alpha^2} \log\left(\frac{1}{q}\right), \tag{10}$$

$$f(N_{\mathcal{R}}, |\mathcal{L}|, \delta) = \frac{26}{(1-1/e)^2} n_\alpha. \tag{11}$$

定理 2。给定用户指定的失败概率 $\delta > 0$、具有命中时间 T_{hit} 和相遇时间 T_{meet}的站点拓扑 $\mathcal{G}$，以及满足(1) 和(2)的信任观测$\alpha_{i,\ j}(t)$。如果所有合法机器人 $i \in \mathcal{L}$ 都使用 *DCV*（算法*2*），采用(4) 中的转移矩阵 $\mathbf{P}_i$ 以及(10)中给出的 n_α 观测，那么最终信任向量 $\mathbf{x}_i^*$将对所有 $i \in \mathcal{L}$ 都正确，所需时间为 $O(\min\{T_{hit}\log(\frac{N_{\mathcal{R}}}{\delta|\mathcal{L}|}),\ T_{meet}\log(\frac{N_{\mathcal{R}}}{\delta})\})$，且概率至少为 $1 - \frac{\delta}{N_{\mathcal{R}}}$。

为证明定理 2，我们首先定义一个事件 E；若该事件成立，则所有最终信任向量都确定性地正确。事件 E 由四个条件组成，每个条件都要求一定比例的 $\rho_1, \rho_2, \rho_3, \rho_4$合法机器人满足相应条件。

令 E 表示如下事件：对于每个合法机器人 $i \in \mathcal{L}$，以下所有性质均成立：

1) 机器人 i 在阶段 1 中至少与 $(1-\rho_1)|\mathcal{L}|$ 个合法机器人各相遇 n_α 次。2) 机器人 i 在阶段 1 中对合法机器人的误分类不超过 $\rho_2|\mathcal{L}|$ 次。3) 机器人 i 在阶段 1 中对恶意机器人的误分类不超过 $\rho_3|\mathcal{L}|$ 次。4) 机器人 i 在阶段 2 中至少与 $(1-\rho_4)|\mathcal{L}|$ 个合法机器人各相遇一次。

事件 E 的四项性质如图 2 所示。

我们通过证明以下两点来证明定理 2：当事件 E成立时，所有最终信任向量均正确（这一点将在引理 1 中证明）；事件 E 成立的概率至少为$1-\delta/N_{\mathcal{R}}$（这一点将在命题 1 中证明）。

引理 1。假设事件 E 成立，且 $1 > 3\rho_2 + \rho_3 + \rho_4$，其中 ρ_2、ρ_3、$\rho_4 \geq 0$。若采用参数为 $\tau =$最小值 $\left\{f(N_{\mathcal{R}}, |\mathcal{L}|, \delta)T_{hit}, \frac{4\text{对数}(4N_{\mathcal{R}}^3/\delta}{\varepsilon_\alpha^2} T_{meet}\right\}$ 的 *DCV*算法，其中 $f(N_{\mathcal{R}}, |\mathcal{L}|, \delta)$ 由(11)给出，则任意合法机器人 i

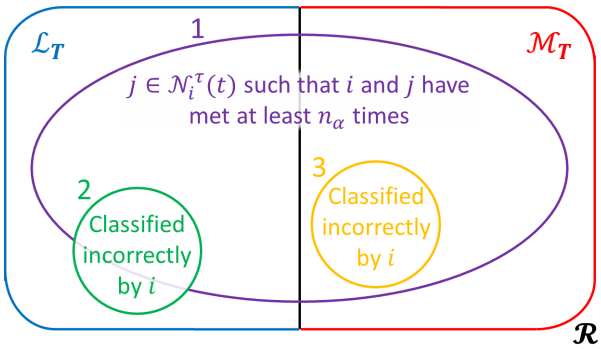


图 2. 事件 E所指定区域的示意图。在所有合法和恶意机器人中，机器人 i 在阶段 1 期间至少相遇 n_α 次的机器人所占比例以紫色表示，对应性质 1。阶段 1 结束后，机器人 i 会误分类一些合法机器人，以绿色表示，对应性质 2。如果机器人 i 将与其至少相遇 n_α 次的另一台机器人误分类，或者由于至少未与该机器人相遇 n_α 次而默认将其归类为恶意机器人，就可能发生这种情况。此外，阶段 1 结束后，机器人 i 会误分类一些恶意机器人，以橙色表示，对应性质 3。只有当机器人 i 至少与某个恶意机器人相遇 n_α 次时，才可能发生这种情况。性质 4 对应机器人 i 在阶段 2 中相遇的机器人。该区域与紫色表示的性质 1 所对应区域相似，不同之处在于，机器人在阶段 2 中只需相遇一次即可纳入该区域。

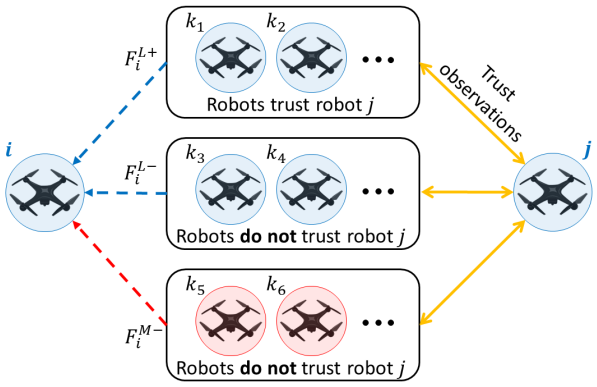


图3。机器人 k与机器人 i分享它们对机器人 j的看法，帮助机器人 i判断机器人 j的可信度。在机器人 k中，有些机器人（F_i^{L+}）是合法的，会向机器人 i提供正确的信息；有些机器人（F_i^{L-}）是合法的，但会错误地分类机器人 j，因此提供错误的信息；还有些机器人（F_i^{M-}）是恶意的，会故意分享错误的信息。当 $F_i^{L+} > F_i^{L-} + F_i^{M-}$ 时，分类才是正确的。

能够正确分类任何其他机器人 j 。

证明。我们分析机器人 $i \in \mathcal{L}$ 如何利用每个可信邻居 $k \in \Theta_i^\tau$ （ t ） $\backslash\{j\}$ 提供的信息来判定另一机器人 j 的可信度。对于任意机器人 j，我们区分两种情况。

对于第一种情况，假设机器人 j 是合法的。设 F_i^{L+} 为机器人 $i \in \mathcal{L}$ 信任、也信任机器人 j，且机器人 i 在阶段 2 遇到的合法机器人数量。这表示阶段 2 结束后，支持机器人 i正确分类机器人 j 的合法机器人数量。要使合法机器人 k 不被计入 F_i^{L+} ，必须发生以下三种情况之一：1）机器人 i 错误地分类了机器人 k；2）机器人 k 错误地分类了机器人 j；或 3）机器人 k 在阶段 2 没有遇到机器人 i 。根据并集界，$F_i^{L+} \geq |L| - 2\rho_2|L| - \rho_4|L| = (1 - 2\rho_2 - \rho_4)|L|$。

令 F_i^{L-} 表示机器人 i信任、但不信任机器人 j，且机器人 i 在阶段 2 遇到的合法机器人数量。这表示在阶段 2 之后，为机器人 i对机器人 j 的错误 分类背书的合法机器人数量。根据并集界，我们有 $F_i^{L-} \leq \rho_2|L|$.

最后，令 F_i^{M-} 表示机器人 i 信任且声称机器人 j 是恶意机器人的恶意机器人数量。这表示在阶段 2 之后，为机器人 i对机器人 j 的错误 分类背书的恶意机器人数量。我们可以假设没有恶意机器人声称自己信任机器人 j。我们有 $F_i^{M-} \leq \rho_3|L|$。

机器人 i 正确分类机器人 j的充分条件是：向机器人 i 提供正确信息的机器人数量，大于向机器人 i 提供错误信息的机器人数量，即 $F_i^{L+} > F_i^{L-} + F_i^{M-}$。由此可得，只要满足 $1 > 3\rho_2 + \rho_3 + \rho_4$，就有 $F_i^{L+} > F_i^{L-} + F_i^{M-}$。因此，对于$\rho_2$、 ρ_3和 ρ_4的任何有效取值，机器人 i 都能正确分类机器人 j 。可信机器人 $k \in \Theta_i^\tau(t)\backslash\{j\}$与机器人 i 分享信息，以帮助机器人 i 对机器人 j 作出判断的过程如图3所示。

对于第二种情况，假设机器人 j 是恶意的。令 F_i^{L+} 表示机器人 i 信任的、将机器人 j 判定为恶意且在阶段 2与机器人 i 会面的合法机器人的数量。我们有，$F_i^{L+} \geq |L| - 2\rho_2|L| - \rho_4|L| = (1 - 2\rho_2 - \rho_4)|L|$。

令 F_i^{L-} 表示机器人 i信任、将机器人 j 分类为合法机器人，且机器人 i 在阶段 2 遇到的合法机器人数量。我们有 $F_i^{L-} \leq \rho_2|L|$。

最后，令 F_i^{M-} 表示机器人 i 信任且声称机器人 j 是合法机器人的恶意机器人数量。我们有 $F_i^{M-} \leq \rho_3|L|$。

显然，只要$1 > 3\rho_2 + \rho_3 + \rho_4$，我们就有 $F_i^{L+} > F_i^{L-} + F_i^{M-}$。因此，对于 ρ_2、 ρ_3和 ρ_4的任意有效取值，机器人 i 都能正确地将机器人 j 分类。

无论哪种情况，机器人 i 都能正确地将机器人 j 分类。 □

命题 *1.* 设 $|\mathcal{L}| \geq 1$、 $\rho_1 = 0.1$、 $\rho_2 = \rho_3 = 0.2$。给定满足 *(1)* 和 *(2)* 的信任观测α_i、$_j(t)$，若所有合法机器人 $i \in \mathcal{L}$ 均使用 *(4)* 中的状态转移矩阵 P_i，则使用参数 $\tau = min\left\{f(N_\mathcal{R}、 |\mathcal{L}|、 \delta)T_{hit}、 {}^4log(\frac{4N_\mathcal{R}^3/\delta}{\varepsilon_\alpha^2} T_{meet})\right\}$ 和 n_α 运行 *DCV*（算法*2*），其中 $f(N_\mathcal{R}、 |\mathcal{L}|、 \delta)$由 *(11)* 给出，$n_\alpha$ 由 *(10)* 给出，可确保事件 E 以至少$1 - \frac{\delta}{N_\mathcal{R}}$的概率成立。

——

备注： 在证明该命题之前，请注意，如果$|\mathcal{M}| = O(|\mathcal{L}|)$，那么 τ的第一项为 $O(T_{\text{hit}})$，因为$N_\mathcal{R}/|\mathcal{L}| \approx 2$；而第二项无论合法机器人所占比例如何，均为 $O(T_{\text{meet}}\log(N_\mathcal{R}))$。

证明。 不失一般性，我们假设 τ 的第一项（即关于命中时间的函数）为最小项。否则，根据成功概率为 $1 - \delta/(2N_\mathcal{R})$的定理 1，证明可直接得出。

考虑任意合法机器人 i 从任意起始时间 $t = 1$ 到任意结束时间 $t = t_f$的轨迹 $\chi_i(1)\ \chi_i(2) \ldots, \chi_i(t_f)$。我们证明，事件 E 的每个性质成立的概率至少为$1 - \delta/(4N_\mathcal{R})$。因此，对全部 4 个性质应用并集界，可得总成功概率至少为 $1 - \delta/N_\mathcal{R}$。我们从性质 1 开始。

a) 性质1：我们首先声称，任意其他合法机器人 j 在经过 $4T_{\text{mix}} + T_{\text{hit}}$ 个时间步后遇到机器人 i 的概率至少为 $(1 - 1/e)^2$,，其中 e 为欧拉常数。为证明这一点，注意到，根据 [29, 引理 A.5]，经过$4T_{\text{mix}}$ 个时间步后，机器人 j 执行的随机游走以至少 $1-1/e$的概率服从平稳分布 π。然后，根据引理 3，经过 T_{hit} 个时间步后，机器人 j 没有遇到机器人 i 的概率至多为 $(1 - 1/T_{\text{hit}})^{T_{\text{hit}}} \leq 1/e$；这里我们利用了，对于 $n \geq 1$, $|x| \leq n$，有 $(1 + x/n)^n \leq e^x$ 。由此可证。

现在，我们可以将时间划分为长度为$4T_{\text{mix}} + T_{\text{hit}}$ 的时段，并重复这一试验；注意，每次试验彼此独立。根据 [30], 中的式（10.35），我们有$4T_{\text{mix}} + T_{\text{hit}} \leq 13T_{\text{hit}}$。

设 X 为两台合法机器人之间的相遇次数。经过 $f(N_\mathcal{R}, |\mathcal{L}|, \delta)T_{\text{hit}}$ 个时间步后，两台合法机器人之间的预期相遇次数

为 $\mu \geq (1-1/e)^2 f(N_{\mathcal{R}}, |\mathcal{L}|, \delta)/13 = 2n_\alpha$。根据切尔诺夫界（附录 A 中的命题 2），令 $\gamma = 1/2$，可得合法机器人之间的相遇次数少于 n_α 的概率至多为

$$\begin{aligned}\mathbb{P}[X \leq n_\alpha] &\leq \mathbb{P}\left[X \leq \frac{\mu}{2}\right] \leq e^{-\gamma^2\mu/2} \\ &\leq \exp\left(-\frac{2n_\alpha}{8}\right) \leq q^{2/\rho_1}.\end{aligned} \tag{12}$$

令 Y_j 为指示变量：若合法机器人 j 与合法机器人 i 相遇少于 n_α 次，则其值为 1。需要注意的是，对于任意 j, $k \neq i$ 和 $j \neq k$， Y_j与 Y_k 相互独立，因为我们已提前固定机器人 i 的轨迹。利用这一关键的独立性，我们可以对 $Y = \sum_{j\in\mathcal{L}\setminus\{i\}} Y_j$进行界定，即与机器人 i 相遇少于 n_α 次的合法机器人的数量。为此，我们在$p = q^{2/\rho_1}$的条件下应用命题 3（参见附录 A）。注意，由于$p \leq \rho_1^2/\exp(2e(1-\rho_1))$，我们可以应用命题 3。我们有

$$\mathbb{P}[Y \geq \rho_1|\mathcal{L}|] \leq p^{\rho_1|\mathcal{L}|/2} = q^{|\mathcal{L}|} \leq \frac{\delta}{4|\mathcal{L}|\cdot N_{\mathcal{R}}}, \tag{13}$$

根据引理 4（参见附录 A）。对所有合法机器人 $|\mathcal{L}|$ 应用并集界，可证明事件 E的性质 1 以至少 $1-\delta/(4N_{\mathcal{R}})$ 的概率成立。

b) 性质 2：令 $\mathcal{L}_1$ 为至少与机器人 i 相遇 n_α 次的合法机器人集合。根据引理 2，由于每个机器人 $j \in \mathcal{L}_1$ 至少与机器人 i 相遇 n_α 次，每个机器人$j \in \mathcal{L}_1$ 都将以至少$1-q^{24/\rho_1}$的概率正确地将机器人 i 分类。现在令 $p = q^{24/\rho_1}$。若要将 $\rho_2|\mathcal{L}|$ 个合法机器人误分类，则在 $|\mathcal{L}_1|$中至少有 $\rho_1|\mathcal{L}|$个机器人被误分类。

根据命题 3，代入 $\rho = \frac{\rho_1|\mathcal{L}|}{|\mathcal{L}_1|}$和 $n = |\mathcal{L}_1|$，并取 $p \leq \rho_1^2/\exp(2e(1-\rho_1))$，超过 $\rho_1|\mathcal{L}|$ 个机器人被误分类的概率至多为

$$p^{\rho_1|\mathcal{L}|/2} = q^{12|\mathcal{L}|} \leq \frac{\delta}{4|\mathcal{L}|\cdot N_{\mathcal{R}}}, \tag{14}$$

根据引理 4。

因此，在性质 1 的所有成功会面中，只有 $\rho_1|\mathcal{L}|$ 次会面会被误分类，其概率至多为$1-\delta/(4|\mathcal{L}|\cdot N_{\mathcal{R}})$。所以，误分类机器人 i 的机器人包括与机器人 i 相遇次数少于n_α 次的机器人，以及与机器人 i 至少相遇 n_α 次但仍将其误分类的机器人。这给出 $\rho_1|\mathcal{L}| + \rho_1|\mathcal{L}| = \rho_2|\mathcal{L}|$。对所有 $|\mathcal{L}|$ 个机器人应用并集界，可得性质 2 成立的概率至少为 $1-\delta/(4N_{\mathcal{R}})$。

c) 性质 3：为了使被判定为合法的恶意机器人数量最大化，不失一般性，我们可以假设每个机器人 $j \in \mathcal{M}$ 至少与机器人 i相遇 n_α 次。根据引理 2，机器人 i 将每个恶意机器人 $j \in \mathcal{M}$ 误判的概率至多为 $p = q^{24/\rho_1}$。不失一般性，假设 $|\mathcal{M}| \geq 1$。我们可以在 $\rho = \rho_3|\mathcal{L}|/|\mathcal{M}|$ 和 $n = |\mathcal{M}|$的条件下应用命题 3，其中$p \leq \rho_1^2/\exp(2e(1-\rho_1))$。因此，根据引理 4，超过 $\rho_3|\mathcal{L}| = \rho_3\frac{|\mathcal{L}|}{|\mathcal{M}|}|\mathcal{M}|$ 个恶意机器人被误判的概率至多为 $p^{\rho_3|\mathcal{L}|/2} = q^{24|\mathcal{L}|} \leq \delta/(4|\mathcal{L}|\cdot N_{\mathcal{R}})$，对所有 $|\mathcal{L}|$ 个合法机器人应用并集界，即可完成性质 3 的证明。

d) 性质 4：性质 4 的证明与性质 1 相同，因为 $n_\alpha \geq 1$。

对全部 4 个性质应用并集界，可得总成功概率至少为 $1-\delta/N_{\mathcal{R}}$。 □

根据引理 1，事件 E 会使所有合法机器人正确返回最终信任向量。此外，根据命题 1，事件 E 以至少 $1-\delta/N_{\mathcal{R}}$ 的概率成立，从而证明了定理 2。

需要注意的是，定理 2 的界在以下意义上是紧的：存在一类无限多个图，其所需时间与定理 2 中的所需时间相差至多一个常数因子。在某些图中，例如规模足够大的星形图 $N_{\mathcal{V}}$，满足要求需要 $\Omega(T_{\text{meet}}\log N_{\mathcal{V}}) = \Omega(\log N_{\mathcal{V}})$ 轮次。另一方面，例如在 $N_{\mathcal{V}} \times N_{\mathcal{V}}$ 网格中，则需要 $\Omega(T_{\text{hit}}) = \Omega(N_{\mathcal{V}}^2)$ 轮次。

还值得注意的是，经过 $O(T_{\text{hit}})$ 个时间步后，失败概率在 $|\mathcal{L}|$ 中呈指数级小。由于我们取命中时间与相遇时间乘以 $\log N_{\mathcal{R}}$ 后两者中的较小值，因此不能指望失败概率总是呈指数级小。

V. 仿真

为了评估我们提出的算法，我们开展了一项仿真研究，考察与个体协议相比，在我们提出的方法中利用可信邻居意见来确定正确的信任向量所节省的时间。图 4 中，我们将机器人数量从 4 变化到 128，并检查合法机器人使用个体协议（灰色）和我们提出的 DCV 协议（蓝色）确定正确的信任向量所需的平均时间步数。每次仿真中，我们设置 $|\mathcal{L}| = |\mathcal{M}| = N_{\mathcal{R}}/2$，并针对 $N_{\mathcal{R}}$ 的每个取值运行仿真 100 次。我们还测试了不同的拓扑结构，每个拓扑使用 9 个站点，并在图 4 各子图的左上角标出。左上图采用网格站点拓扑，右上图采用线形拓扑。左下图考察使用 Barab´asi-Albert 模型生成的随机图，其中 $k < N_{\mathcal{V}}$ 个站点最初连接成一条线，其余站点逐个加入，并通过边将其与至多 k 个先前加入的站点相连，这些站点以 $k = 3$ 随机选取。右下图考察使用 Erd¨os-R´enyi 模型生成的随机图，其中每对站点之间以概率 0.2 建立一条边。

无论站点拓扑如何，与个体协议相比，我们提出的 DCV 算法成功所需的时间步都显著更少。还可以看出，随着机器人数量增加，各协议所需时间步数之间的差距也随之扩大，这表明随着团队规模扩大，DCV算法的表现优于个体协议。我们注意到，在最左侧的图中（对应网格和 Barab´asi-Albert 拓扑），仿真中使用 DCV 算法所需的时间步数实际上会随着机器人数量增加而略微减少。这是因为我们

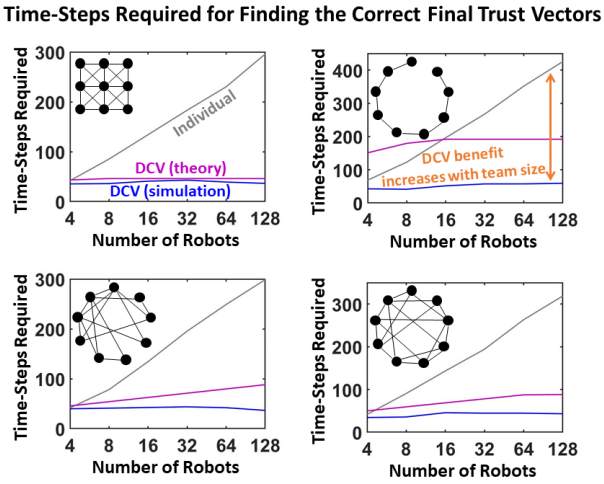


图 4. 在仿真中，机器人使用我们提出的 DCV 协议找到正确最终信任向量所需的时间步数（蓝色），与个体协议（灰色）以及我们根据理论对 DCV 算法的预测（紫色）进行比较。机器人数量在 4 种不同的站点拓扑中变化，每种拓扑均由 9 个站点组成：网格（左上）、线形（右上）、Barab´asi-Albert（左下）和 Erd¨os-R´enyi（右下）。随着机器人数量增加，合法机器人与恶意机器人的比例保持不变。无论站点拓扑如何，随着团队规模增大，两种方法的性能差距都会扩大。

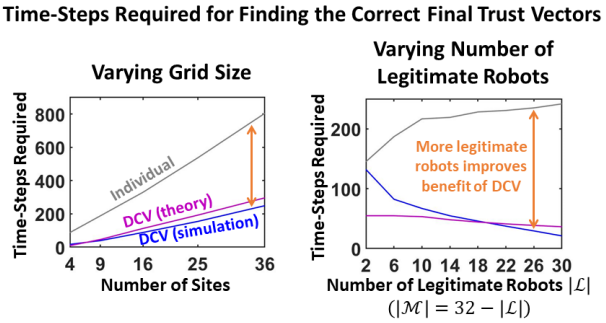


图 5. 在仿真中，机器人使用我们提出的 DCV 协议找到正确的最终信任向量所需的时间步数（蓝色），与个体协议（灰色）以及我们根据 DCV算法理论预测的结果（紫色）进行比较。站点数量沿网格站点拓扑变化（左图）；合法和恶意机器人的数量则在固定网格中变化，网格包含 $N_{\mathcal{V}} = 9$ （右图）。

在找到正确的最终信任向量后便终止仿真。在定理 2 中，我们证明，随着机器人数量增加，使用 DCV 找到正确信任向量所需的时间保持为常数，但找到正确信任向量的概率会随机器人数量增加而提高。这一现象可能导致图 4 最左侧两个图中出现明显的下降。此外，我们还用线条标示理论预测所需的时间步数（紫色），即定理 2 给出的预测。不同站点拓扑的命中时间使用 [24,定理 3.1]，计算，相遇时间则使用 [25, 定理 1]计算。对于通过随机图生成模型生成的 100 种拓扑（Barab´asi-Albert 模型和 Erd¨os-R´enyi 模型），我们对各自的命中时间和相遇时间取平均值，以计算理论预测的这些情形下所需时间。从图 4 可以看出，理论预测所需的时间步数与仿真中实际得到的数量十分接近（相差仅为常数因子）。

在图 5 中，我们改变了网格拓扑中的站点数量（左图），以及合法机器人与恶意机器人的数量（右图）。左图使用了 $N_{\mathcal{R}} = 32$ 台机器人，其中$|\mathcal{L}| = |\mathcal{M}| = N_{\mathcal{R}}/2$。右图使用了包含 $N_{\mathcal{V}} = 9$ 个站点的网格站点拓扑，机器人总数固定为 $N_{\mathcal{R}} = 32$ ，但合法机器人的数量从 $|\mathcal{L}| = 2$ 变化到 $|\mathcal{L}| = 30$ ，其中 $|\mathcal{M}| = N_{\mathcal{R}} - |\mathcal{L}|$。两幅图均显示，随着站点数量增加（左图）以及合法机器人与恶意机器人的比例提高（右图），DCV 算法相对于个体协议的优势都会增大。

VI. 结论

本文提出了一种算法，可利用可信邻居的意见，快速且有效地利用信任观测确定邻近机器人的真实信任，即使机器人处于移动状态且邻居集合随时间变化也不例外。我们证明，该算法不仅有助于合法机器人就其信任向量达成一致，还能通过减少每个机器人必须单独收集观测的时间步总数，缩短正确确定信任向量所需的时间。

参考文献

[1] Z. Yan、N. Jouandeau 和 A. A. Cherif，“多机器人协调：综述与分析”，《国际先进机器人系统杂志》，第 10 卷第 12 期，第 399 页，2013年。[2] Y. Rizk、M. Awad 和 E. W. Tunstel，“协作异构多机器人系统：综述”，《*ACM*计算综述》（*CSUR*），第 52 卷第 2 期，第 1–31 页，2019年。[3] A. Davydov 和 Y. Diaz-Mercado，“多机器人覆盖控制的稀疏结构与最优性”，*IEEE*控制系统快报，第 4 卷第 1 期，第 13–18 页，2019年。[4] M. Boldrer、F. Pasqualetti、L. Palopoli 和 D. Fontanelli，“通过时间反演Kuramoto动力学实现多智能体持续监测”，*IEEE*控制系统快报，2022年。[5] A. Ivanov 和 M. Ca mpbell，“联合探索与跟踪：Jet”，*IEEE*控制系统快报，第 2 卷第 1 期，第 43–48 页，2017年。[6] M. Cavorsi、B. Capelli、L. Sabattini 和 S. Gil，“利用控制屏障函数实现多机器人对抗韧性”，*2022*年*IEEE*机器人学：科学与系统（*RSS*），2022年。[7] S. Gil、S. Kumar、M. Mazumder、D. Katabi 和 D. Rus，“保障抗欺骗多机器人网络”，自主机器人，第 41 卷第 6 期，第 1383–1400 页，2017年。[8] C. Pippin 和 H. Christensen，“多机器人巡逻中的信任建模”，载于*2014*年*I EEE*机器人与自动化国际会议（*ICRA*）。IEEE，2014年，第 59–66 页。[9] J. Xiong 和 K. Jamieson，“SecureArray：利用细粒度物理层信息提升WiFi安全性”，第*19*届年度移动计算与网络国际会议论文集，第 441–452 页，2013年。[10] M. Cheng、C. Yin、J. Zhang、S. Nazarian、J. Deshmukh 和 P. Bogdan，“多智能体系统的通用信任框架”，载于第*20*届自主智能体与多智能体系统国际会议论文集，2021年，第 332–340 页。[11] A. Pierson 和 M. Schwager，“面向鲁棒多机器人传感器覆盖的自适应机器人间信任”，载于国际机器人研究研讨会，2013年。[12] H. Parwana 和 D. Panagou，“面向非合作多智能体系统的基于信任、速率可调的控制屏障函数”，*2022*年*IEEE*决策与控制国际会议，2022年。

[13] F. Mallmann-Trenn、M. Cavorsi 和 S. Gil，“Crowd Vetting：通过协作拒绝对抗者及其在多机器人集群中的应用”，IEEE机器人学汇刊，第 38 卷第 1 期，第 5–24 页，2021年。[14] M. Yemini、A. Nedi´c、A. J. Goldsmith 和 S. Gil，“信息物理系统中分布式共识的信任与韧性特征分析”，IEEE机器人学汇刊，第 38 卷第 1 期，第 71–91 页，2021年。[15] X. Yu、D. Shishika、D. Saldana 和 M. A. Hsieh，“面向韧性共识的模块化机器人编队与路由”，2020年美国控制会议（ACC），第 2464–2471 页，2020年。[16] M. Cavorsi、N. Jadhav、D. Salda˜na 和 S. Gil，“动态拓扑中的自适应恶意机器人检测”，2022年IEEE决策与控制国际会议（CDC），2022年。[17] S. Berman、A. Hal´asz、M. A. Hsieh 和 V. Kumar，“机器人群任务分配的优化随机策略”，IEEE机器人学汇刊，第 25 卷第 4 期，第 927–937 页，2009年。[18] S. Bandyopadhyay、S.-J. Chung 和 F. Y. Hadaegh，“大规模自主智能体群的概率分布式控制”，IEEE机器人学汇刊，第 33 卷第 5 期，第 1103–1123 页，2017年。[19] I. Jang、H.-S. Shin 和 A. Tsourdos，“用于概率群体分布引导的基于局部信息的控制”，群体智能，第 12 卷第 4 期，第 327–359 页，2018年。[20] D. Acemoglu 和 A. Ozdaglar，“社交网络中的意见动力学与学习”，动态博弈与应用，第 1 卷第 1 期，第 3–49 页，2011年3月。[21] R. Hegselmann、U. Krause 等，“意见动力学与有界信任模型、分析及仿真”，人工社会与社会模拟杂志，第 5 卷第 3 期，2002年。[22] L. Lov´asz，“图上的随机游走”，《组合学：Paul Erdos 八十华诞纪念文集》，第 2 卷，第 1–46 期，第 4 页，1993年。[23] D. Aldous 和 J. Fill，“可逆马尔可夫链与图上的随机游走”，2002年，未发表。http://www.stat.berkeley.edu/~aldous/ RWG/book.html。[24] S. K. Rao，“求解各种图中的击中时间”，统计与概率快报，第 83 卷第 9 期，第 2067–2072 页，2013年。[25] M. George、R. Patel 和 F. Bullo，“多个随机游走的相遇时间”，arXiv预印本 arXiv:1806.08843，2018年。[26] R. A. Horn 和 C. R. Johnson，《矩阵分析》。剑桥大学出版社，2012年。[27] G. Boole，《逻辑的数学分析》。哲学图书馆，1847年。[28] M. Mitzenmacher 和 E. Upfal，《概率与计算：算法与数据分析中的随机化和概率技术》。剑桥大学出版社，2017年。[29] V. Kanade、F. Mallmann-Trenn 和 T. Sauerwald，“关于图中的聚并时间——聚并何时与相遇一样快？”，CoRR，第 abs/1611.02460 卷，2016年。 [在线]。可访问：http://arxiv.org/abs/1611. 02460[30] D. A. Levin、Y. Peres 和 E. L. Wilmer，《马尔可夫链与混合时间》。美国数学学会，2006年。[31] R. I. Oliveira 和 Y. Peres，“图上的随机游走：关于击中、相遇、聚并与返回的新界”，载于2019年第十六届解析算法与组合学研讨会论文集（ANALCO）。SIAM，2019年，第 119–126 页。[32] T. Hagerup 和 C. R¨ub，“切尔诺夫界导论”，信息处理快报，第 33 卷第 6 期，第 305–308 页，1990年。

附录

A. 辅助命题

引理 2（上界 [13]）。 如果机器人 $i \in \mathcal{L}$ 从另一台机器人 j接收到 $n_\alpha = \log(1/\delta)\, 2\varepsilon_\alpha^2$ 条信任观测，那么只需依据观测结果的多数意见，它就能以至少 $(1-\delta)$ 的概率判断机器人 j是合法的还是恶意的：

$$\mathbb{P}\left[\sum_{\kappa=1}^{n_\alpha}\left([\mathbf{o}_{i,j}]_\kappa - \frac{1}{2}\right) > 0 \;\middle|\; j \in \mathcal{L}\right] \geq 1-\delta,$$

and

$$\mathbb{P}\left[\sum_{\kappa=1}^{n_\alpha}\left([\mathbf{o}_{i,j}]_\kappa - \frac{1}{2}\right) < 0 \;\middle|\; j \in \mathcal{M}\right] \geq 1-\delta. \tag{15}$$

命题 2（[28]）。 设 $X_1, \ldots, X_n$ 是相互独立的伯努利随机变量，满足 $X = \sum_i^n X_i$ 和$\mu = \mathbb{E}[X]$。那么，对于任意 $0 < \gamma < 1$,

$$\mathbb{P}[X \leq (1-\gamma)\mu] \leq e^{-\gamma^2\mu/2}. \tag{16}$$

引理 3 ([31,定理 1.3])**.**对于任意 $t \in \mathbb{N}\setminus\{0\}$以及任意序列 $\chi_i(1)\, \chi_i(2) \ldots, \chi_i(t) \in \mathcal{V}$，对于机器人 j从平稳分布 π出发、针对 $\kappa \in \{1, \ldots, t\}$执行的任意惰性随机游走 $\mathbf{P}^{j(\kappa)}$，我们有：

$$\mathbb{P}[\forall \kappa, \chi_j(\kappa) \neq \chi_i(\kappa)] \leq (1 - 1/T_{hit})^\kappa .$$

以下结论由 [13, 定理 4] / [32]的公式 10 推出。

命题 3. 设 $Y = \sum_{i=1}^n Y_i$ 是由 n个独立同分布随机变量之和，满足 $\mathbb{P}[Y_i = 1] = p$且 $\mathbb{P}[Y_i = 0] = 1 - p$满足 $p \leq \rho^2/\exp(2e(1-\rho))$。对于任意 $\rho \in (0,\ 0.8]$，我们有：

$$\mathbb{P}[Y \geq \rho n] \leq p^{\rho n/2}.$$

引理 4. 沿用引理 *1* 和命题 *1* 中的记号。我们有，$q^{|\mathcal{L}|} \leq \frac{\delta}{4N_{\mathcal{R}}|\mathcal{L}|}$。

证明。 设 $\phi = \frac{|\mathcal{L}|}{20N_{\mathcal{R}}}$。由于 $|\mathcal{L}| \geq 1$，且根据q的定义，只需证明

$$\phi^{|\mathcal{L}|} \leq \frac{1}{4N_{\mathcal{R}}|\mathcal{L}|}. \tag{17}$$

因为这样便有 $q^{|\mathcal{L}|} \leq \delta\phi^{|\mathcal{L}|} \leq \frac{\delta}{4N_{\mathcal{R}}|\mathcal{L}|}$。

注意，公式 (17) 等价于证明以下等式

$$\frac{1}{\phi^{|\mathcal{L}|}} = \left(\frac{20N_{\mathcal{R}}}{|\mathcal{L}|}\right)^{|\mathcal{L}|} \geq 4|\mathcal{L}|N_{\mathcal{R}}. \tag{18}$$

现在，我们通过区分以下几种情况来证明公式 (18)。

- $|\mathcal{L}| = 1$: holds trivially.
- $|\mathcal{L}| \in \{2, 3\}$:

$$\left(\frac{20N_{\mathcal{R}}}{|\mathcal{L}|}\right)^{|\mathcal{L}|} > (5N_{\mathcal{R}})^{|\mathcal{L}|} \geq 25N_{\mathcal{R}}^2 \geq 4|\mathcal{L}|N_{\mathcal{R}}.$$

- $|\mathcal{L}| \in \{4, 5, \ldots, \sqrt{N_{\mathcal{R}}}\}$:

$$\left(\frac{20N_{\mathcal{R}}}{|\mathcal{L}|}\right)^{|\mathcal{L}|} \geq (20\sqrt{N_{\mathcal{R}}})^{|\mathcal{L}|} \geq 20^4 N_{\mathcal{R}}^2 \geq 4|\mathcal{L}|N_{\mathcal{R}}.$$

- $|\mathcal{L}| \in \{\sqrt{N_{\mathcal{R}}} + 1, \ldots, N_{\mathcal{R}}\}$:

$$\left(\frac{20N_{\mathcal{R}}}{|\mathcal{L}|}\right)^{|\mathcal{L}|} \geq (20)^{|\mathcal{L}|} \geq 20^{\sqrt{N_{\mathcal{R}}}} \geq 4N_{\mathcal{R}}^2 \geq 4|\mathcal{L}|N_{\mathcal{R}},$$

其中，倒数第二个不等式可通过对两边取对数验证；由此得到$\sqrt{N_{\mathcal{R}}}\log(20) \geq 2\log(2N_{\mathcal{R}})$，其中 $N_{\mathcal{R}} \geq 1$。

□