arXiv:2301.10704v1 [cs.MA] 25 Jan 2023

HOLA ROBOTS：利用共同观测和限制视界的公告缓解多机器人系统中的计划偏离攻击

预印本

Kacper Wardega
波士顿大学
波士顿
USA
ktw@bu.edu

Max von Hippel
东北大学
波士顿
USA
vonhippel.m@northeastern.edu

Roberto Tron
波士顿大学
波士顿
USA
tron@bu.edu

Cristina Nita-Rotaru
东北大学
波士顿
USA
c.nitarotaru@northeastern.edu

Wenchao Li
波士顿大学
波士顿
USA
wenchao@bu.edu

2023年1月26日

摘要

新兴的多机器人系统依赖人类与机器人之间的协作，机器人则按照自动生成的运动计划行动，以完成应用层任务。鉴于机器人在靠近人类和昂贵基础设施的环境中运行时必须满足安全要求，了解并缓解此类系统因被攻陷的机器人偏离指定计划而产生的安全漏洞至关重要。我们关注集中式系统，其中中央实体（中央执行器）负责制定运动计划并将其发送给机器人；机器人按照计划行动时，会报告自己的位置。中央执行器通过比较机器人的预期位置与其自行报告的位置，检查机器人是否遵循指定计划。我们指出，这种自报告监控机制容易受到计划偏离攻击：被攻陷的机器人不遵循指定计划，同时试图通过谎报位置来掩饰自己的行动。我们提出了针对计划偏离攻击的双管齐下缓解方案：1. 一种攻击检测技术，利用机器人的本地感知能力来报告对其他机器人的观测，并结合中央执行器生成的协同观测计划；2. 一种预防技术，中央执行器向机器人发布限制视界的公告，以减少它们对全局运动计划中前方步骤的即时了解。在大规模自动化仓库基准测试中，我们表明，即使攻击者已攻陷多个机器人，我们的方案仍能提供针对隐蔽攻击者的攻击预防保证。

1 引言

在本文中，我们研究遵循集中式执行模型 [H¨onig 等人（2019）], 的多机器人系统（MRS）中的攻击与防御。这种模型代表了在已知的结构化环境中实行集中管理与控制的多机器人系统。系统由外部应用程序、执行任务的机器人，以及负责为每个机器人确定并传输运动计划的中央实体（中央执行器，CE）组成。理想情况下，中央执行器会将机器人的预期位置与其自我报告的位置进行比较，从而检测由故障导致的计划外偏离。遗憾的是，被攻陷的机器人若偏离运动计划并试图穿越环境中的禁入区域，仅凭机器人对位置的自我报告无法检测到它们，

因为被攻陷的机器人可以在报告中撒谎，以免被发现。我们将此类蓄意偏离称为计划偏离攻击，并在本文中重点研究这类攻击。

计划偏离攻击此前由 [Wardega et al.(2019)], 提出，该研究建议利用其他机器人的共同观测来检测偏离。具体而言，以检测约束的形式化规范为核心的基于逻辑的规划，可生成运动计划，使其隐含的共同观测调度能够确保检测到单个被攻陷的机器人。然而，这类计划并不一定存在，而且基于逻辑的规划问题难以求解，因此这种方法无法扩展到实际的多机器人系统部署。更重要的是， [Wardega et al.(2019)] 的方法无法推广到多个被攻陷的机器人。我们根据对攻击者的两点观察来设计解决方案，以应对上述问题：1. 攻击者利用中央执行器（CE）提供的运动计划信息，确定如何前往禁区；2. 攻击者谎报自己的位置，试图躲过中央执行器的检测。我们方法的核心思想是一种新颖的限制视界的公告 （HoLA）机制：我们限制在任意时刻向机器人发布的运动规划信息量，以阻碍攻击者策划成功攻击，同时尽可能多地发送规划步骤。中央执行器通过一种高效的 验证算法实现这一机制，该算法会检查计划发布的公告是否能使隐蔽攻击者因信息不足而无法前往禁区；在最坏情况下，只会发布一个步骤。本文的贡献如下：

- 我们对计划偏离攻击进行了形式化刻画，其核心是隐蔽攻击者 只有在确信自己能够在不被发现的情况下朝禁入区域移动时，才会偏离计划。
- 我们提出了一种缓解计划偏离攻击的方案 HoLA，该方案将共同观测调度与发布限制视界的公告相结合，以防止隐蔽攻击者发动攻击。
- 我们提供了形式化保证，证明限制视界的公告能够阻止已控制多台机器人的隐蔽攻击者发动攻击。
- 我们提出了一种高效计算最长限制视界公告的过程。我们评估了验证的计算开销，并表明该过程能够良好地扩展至包含大量机器人的实例；该过程具有机器人级并行性，在单核上运行时，验证包含 100 台机器人的场景所需时间不超过 2 分钟。

2 问题表述

我们关注集中式多机器人系统模型，该模型由机器人集合 (R) 和中央实体 （中央执行器）组成，中央实体负责与机器人通信并对其进行管理。中央执行器接收待由机器人在环境中执行的应用任务队列作为输入，计算执行这些应用任务的多机器人运动计划 x，随后迭代地向机器人公告部分运动计划 $\alpha(t)$。中央执行器确保运动计划遵守安全约束，即环境中标记为机器人禁入的位置。这些位置可能由多种原因导致，例如有人在环境中移动、机器人出现定位故障、环境中存在不安全状况等。环境建模为图 $G = (V, E)$，随时间变化的越界位置记为 $V_{\text{forbidden}}(t) \subset V$。集中式多机器人系统模型中的运动计划正式定义如下 [Stern 等人（2019）]。

定义 1（多智能体路径查找计划）。环境 $G = (V, E)$ 中，机器人 R 的多机器人路径规划方案是一个有限序列 $\{x_t\}$，其元素为 $x_t \in V^R$，其中序列 $x^i = \{x_t^i\}$ 是机器人 $i \in R$ 的单机器人方案，并且满足以下约束：对于所有 t 以及所有 $i, j \in R$：1. 每个 x^i 都是 G 上的一段游走。2. 机器人不会同时占据同一位置。3. 机器人不会同时经过同一条边。

中央执行器发布的公告是多机器人路径规划前缀，即 $\alpha(t) \preceq x$，定义如下。

定义 2（多机器人路径规划前缀和延续）。设 x 和 y 是两个多智能体路径规划方案。若 y 是 x 的一个 多机器人路径规划前缀，则称 y 是 x 的一个 多机器人路径规划前缀；等价地，若 x 是 y 的一个 多机器人路径延续，则称 x 是 y 的一个 多机器人路径延续，记作 $y \preceq x$，当且仅当 y^i 对所有 $i \in R$ 都是 x^i 的前缀。

攻击者模型。假设攻击者攻陷了一部分 $A \subseteq R$ 机器人，意图破坏系统，并使 A中的机器人违反中央执行器（CE）的安全约束而不被发现。被攻陷的机器人可以完整获知 CE 发布的运动规划公告 α（t），但它们不知道还有哪些其他机器人被攻陷，也无法相互协调，因此必须独立行动。我们不考虑攻击者之间的强协调，因为在集中式环境中，机器人之间的协议内通信受到监控，而且机器人在一个会使此类网络通信被发现的区域内移动。我们还假设机器人无法利用其他侧信道进行通信。被攻陷的机器人偏离名义规划实施恶意行为后，CE 不容易察觉，因为被攻陷的机器人

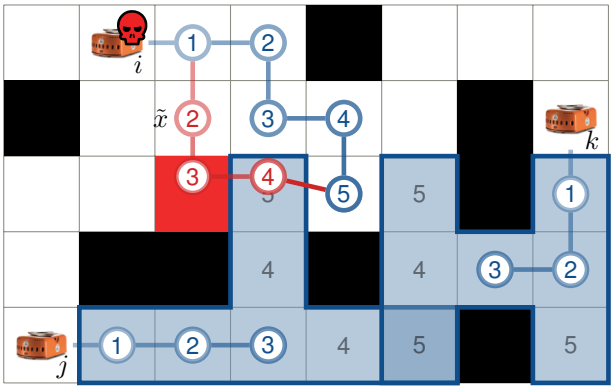


图1：被攻陷的机器人 i 在时间步（1，5）计算出了一个禁止的多智能体路径查找偏离 $\tilde{x}$ （红色路径）。然而，隐蔽攻击者发现，从中央执行器的多智能体路径查找计划已公布部分（蓝色路径）出发，存在一种可能的延续（蓝色阴影区域），会导致中央执行器通过共同观测检测到偏离：如果机器人 j在时间步3向北移动，那么 j 就会在一个不应出现 i 的位置观测到 i 。因此，隐蔽攻击者选择不实施计划偏离攻击。

可以向 CE 谎报自身情况。我们将此类恶意偏离称为计划偏离攻击，将那些还试图使机器人进入 $V_{\text{forbidden}}(t)$ 中某个禁区的偏离称为禁止的计划偏离攻击。我们将在下文对这些威胁进行形式化定义。

定义3 （计划偏离攻击）。 设 x 是机器人集合 R 在地图 $G=(V,\ E)$ 上的一个多智能体路径查找计划。若 $\tilde{x}$满足 $(\forall j,\ t)$ $(x_t^j \neq \tilde{x}_t^j \Leftrightarrow (j=i,\ s<t<f))$ ，则称 $\tilde{x}$是机器人 $i \in R$在时间步 $(s,\ f)$ 相对于 x的多智能体路径查找偏离。

定义4 （禁用计划偏离攻击）。 机器人 i 在 (s, f) 上的多智能体路径寻找偏离 $\tilde{x}$ 是一种禁用 偏离，简称为 $\mathcal{F}(\tilde{x}, x, i, s, f)$，如果满足 $(\exists t \in (s, f))$ s.t. $(\tilde{x}_t^i \in V_{\text{forbidden}}(t))$。

未检测到的计划偏离。假设在时间 t 之前没有尝试过计划偏离攻击，因此真实系统状态 $\tilde{x}_t$ 与中央执行器的预期 x_t 相符。被攻陷的机器人 $a \in A$ 可以通过选择不同的动作 $(x_t^a, \tilde{x}_{t+1}^a) \in E$ s.t. $\tilde{x}_{t+1}^a \neq x_{t+1}^a$，选择偏离计划。为了掩盖偏离已经发生，被攻陷的机器人会伪造其自我报告，并向中央执行器声称自己已移动到名义位置。若 a 没有与未被攻陷的机器人发生碰撞，即 $\tilde{x}$ 仍是多智能体路径查找计划，且 a 没有导致未被攻陷的机器人 $i \neq a$ 无法执行某个动作，即 $\tilde{x}$ 是机器人 i 相对于 x 的多智能体路径寻找偏离，那么很容易看出，机器人发出的自我报告均不会发生变化。这类计划偏离称为未检测到的计划偏离。

隐蔽攻击者。这类攻击者利用其对当前已公告的多智能体路径查找前缀 $\alpha(t)$ 的了解，判断是否存在一个多智能体路径查找计划 $\tilde{x}$，能够确保其构成相对于真实计划 $x, x \succeq \alpha(t)$ 的禁用且未被检测到的偏离。具体而言，隐蔽攻击者需要确保存在一个从 $\tilde{x}_t$ 出发的多智能体路径延续 $\tilde{x}$，使得 $\tilde{x}$ 在实际执行偏离之前，是相对于 x 在 $(t,\ f)$ 上的禁用且未被检测到的多智能体路径偏离。实际上，只要攻击者掌握了足够多关于 x 的信息，就能轻松验证这一点；如果公告 $\alpha(t)$ 展示了计划的较长时域，隐蔽攻击者 a 就能利用 $\alpha(t)$ 轻松求解单机器人规划问题 [Choset 等人（ 2005 ），以避免与其他机器人发生冲突 $i \neq a$。

安全感知执行问题。出于多种原因，中央执行器希望尽可能多地公告多智能体路径查找计划，例如考虑到网络延迟、竞争，或对网络故障和运动故障的鲁棒性 [Atzmon 等人（2020）]。因此，在每个时刻 t，中央执行器的目标是最大化 $|\alpha(t)|$，同时满足以下约束：未知的、遭到入侵的隐蔽攻击者子集 $A \subseteq R$ 无法实施禁止的计划偏离攻击。

3 缓解计划偏离攻击

本节介绍一种针对集中式多机器人系统中的计划偏离攻击的解决方案。我们的方法由两个核心组件构成：共同观测和限制视界的公告。

3.1 协同观测计划

为了减少未被中央执行器检测到的多智能体路径寻找偏离，我们建议在发送给中央执行器的自我报告中加入对其他机器人的共同观测。通常，机器人的机载感知能力仅用于在故障场景中避免碰撞。然而，我们发现，利用传感器报告所有机器人间观测，可显著提升安全性。

我们的方法是在机器人 i于时间 t, $\tilde{\beta}(t)^i$的自我报告中，除了报告动作成功情况外，还包括 i 在时间 t对其他机器人的所有观测。例如，假设机器人 i 位于位置 v，机器人 j位于位置 w，且（v, w）$\in E^*$（换言之，i 可以从其观测点观测到 j）。那么，$\tilde{\beta}(t)^i = \{\tilde{x}^i_{t+1} = x^i_{t+1}, \tilde{x}^j_t = w\}$，也就是说："$i$ 报告称 i 已成功移动到 x^i_{t+1}，并且 i 在时间 t于位置 w观测到了 j。"我们注意到，这种方法可以直接推广到配备固定观察器（摄像机）或完全可信智能体的环境中。

定义 5（基于共同观测的检测）。设 x 为一个多智能体路径查找计划，β 为成功执行 x所隐含的定位和共同观测自我报告：

$$\beta(t) := \{\{\tilde{x}^i_{t+1} = x^i_{t+1}\} \cup \{(i, j, \tilde{x}^j_t) : j \in R \setminus i \wedge (\tilde{x}^i_t, \tilde{x}^j_t) \in E^*\}\}_{i \in R}$$

如果任何机器人 $i \in R$ 未能执行某个动作、未能观测到本应观测到的机器人，或观测到了本不应观测到的机器人，那么 i 发送给中央执行器 CE 的自我报告 $\tilde{\beta}(t)^i$ 将与 $\beta(t)^i$ 不符，从而在 CE 中触发基于共同观测的检测。

3.2 视野限制型多智能体路径规划公告

现在，针对给定的一般多智能体路径查找计划，我们着重探讨如何增加针对采用基于机器人共同观测的缓解机制的系统的攻击规划问题的难度。核心思路如下：中央执行器可以通过阻止攻击者轻易计算出禁止且未被检测到的计划偏离攻击，来提升系统的安全性。实现这一目标最简单的方法，是限制攻击者能够获取的多智能体路径查找计划信息量，也就是在每个时刻限制可获取的未来规划信息量，$\alpha(t)$。

限制隐蔽攻击者。再次考虑针对隐蔽攻击者 $a \in A$ 的攻击规划问题。由于隐蔽攻击者只有在能确保攻击成功且不被发现时才会尝试实施计划偏离攻击，因此攻击者掌握的计划信息量至关重要——如果 $\alpha(t)$提供了较长时域的规划信息，那么攻击规划问题本质上就是一个图可达性问题。形式上，当存在针对 a 的禁止且未被检测到的偏离，且该偏离发生在（t, f）上，其中 f 小于 $\alpha(t)$ 中最短单智能体计划的长度，即 $f < \min_i|\alpha(t)^i|$时，便属于这种情况。然而，如果 $\alpha(t)$未透露如此多的信息，攻击规划问题就会困难得多。这是因为攻击者需要计算一种偏离，它不仅是被禁止的，而且对于 $\alpha(t)$ 的所有可能多智能体路径延续，都能保证不会被检测到。反过来说，这意味着，要缓解隐蔽攻击者发起的攻击，只需证明：对于从 x 出发、针对 a 的每一种禁止偏离，都存在一种来自 $\alpha(t)$ 的延续会导致检测；在这种情况下，隐蔽攻击者就会放弃偏离计划。这促使我们为多智能体路径查找计划 x 提出一类能够确保抵御隐蔽攻击者的公告策略：

定义 6（视野限制型多智能体路径规划公告）。设 x 是 R在 G 上的多智能体路径查找计划，α 是针对 x的公告序列，β_x 是 x所隐含的机器人自我报告序列。那么，当且仅当.....时，α 是针对 x 的视野限制型多智能体路径规划公告

$$(\forall \tilde{x}, i \in R, t, f \in \mathbb{N})(\exists y)(\mathcal{F}(\tilde{x}, x, i, t, f) \Rightarrow y \succeq \alpha(t) \wedge \beta_y^{R\setminus\{i\}} \neq \beta_{\tilde{x}}^{R\setminus\{i\}})$$

也就是说，当且仅当公告 α 在任何时候都未透露足够的信息，使攻击者能够确定某个给定的禁止的多智能体路径查找偏离不会被中央执行器检测到时，我们才认为这些公告具有时域限制性；这是因为存在从 α（t）开始的某种延续 y，使得由 y 导致的自我报告与该偏离导致的自我报告不匹配。对于给定的时间 t，如果不存在任何满足 $|\alpha$（t）$| < |\alpha^*$（t）$|$、α^*（t）$\preceq x$的 α^*（t），且 α^*（t）具有时域限制性，那么我们称 α（t）为最大长度视野限制型公告。

定理1（来自隐蔽攻击者的有保障的安全性）。设 x 为一个多智能体路径查找计划，并假设中央执行器使用针对 x的时域限制型多智能体路径查找公告 α。那么，没有被隐蔽攻击者攻陷的机器人会尝试实施计划偏离攻击。

3.3 时域限制公告的综合

在我们的方法中，中央执行器首先利用传统的、未考虑安全性的多智能体路径规划求解器，计算出一个成本优化的多智能体路径查找计划，这与典型部署中的做法相同。然而，在后处理步骤中，我们会先验证式 6 是否成立，然后再确定公告 α。如果无法验证这些公告是否具有限制时域的性质，我们就会尝试通过迭代选择信息量较低的公告来解决问题，直至找到最大长度的视野限制型公告。

我们在设计验证程序时面临的主要挑战，是多智能体路径查找本身的计算复杂度；众所周知，该问题是NP困难 [Yu 和 LaValle(2013)]。因此，对于拥有不完备信息的隐蔽攻击者而言，完整的攻击规划算法在计算上难以实现，因为它需要枚举多智能体路径查找计划的延续。这促使我们转而专注于为限制视界公告检查问题（式6）开发一种不完备但可靠且高效的验证程序。我们的解决方案是非确定性共同观测枚举，如算法1所示。我们的算法基于多智能体路径规划的一种抽象，该抽象允许机器人在 G 上进行非确定性移动。我们的抽象允许未被攻陷的机器人忽略多智能体路径查找计划的顶点约束和边约束，从而能够高效地同时探索从当前 $\alpha(t)$ 出发的多种多智能体路径查找计划延续的共同观测调度。尽管我们的抽象确实对多智能体路径查找计划延续集合进行了过近似，但我们可以证明，该抽象保留了成对共同观测的可能性。也就是说，如果在该抽象下，机器人 i 有可能在时间 t 于位置 v 观测到机器人 j，那么就存在某种多智能体路径查找计划延续，使得 j 在时间 t 于位置 v 被观测到。抽象的这一性质确保了算法1的可靠性，因为算法1本质上是在非确定性移动抽象下，通过观测区域的补集来验证是否不存在禁区偏离。

算法1的输入为集中式多机器人系统实例 $G = (V,\ E)$、$S = (V,\ E^*)$、$V_{\text{forbidden}}(t)$，以及中央执行器计划从当前时刻 t 到未来时刻 f 发布的公告序列，$\{\alpha(s)\}_{s\in[t,f]}$。我们依次将每个机器人 $a \in R$ 设为被攻陷的机器人；根据攻击者独立性，从 a的角度来看，其他 $R\setminus a$都可能未被攻陷。现在，我们遍历 $s \in [t, f]$，并尝试验证 $\alpha(s)$所包含的信息不足以揭示针对机器人 a、始于时刻 s的禁止且未被检测到的计划偏离攻击。验证 $\alpha(s)$分为两个阶段：(1) 计算最早时刻 $u^* > s$ 以及一个位置 l_{obs}，在该处 a 可能被 $R \setminus \{a\}$ 中的某个机器人观测到；(2) 证明对于 a，在 $(s,\ u^*)$上不存在被禁止且未被检测到的偏离。

由于 $\alpha(s)$ 只会向 $i \in R$ 透露截至时间 $|\alpha(s)^i|$ 的部分规划信息，因此，为了考虑给定机器人未来状态未知的情况，我们允许其在 G 上以非确定性方式移动 $u > |\alpha(s)^i|$ 个时间步。我们将 $i \in R$ 在时间 u 以（非）确定性方式占据的位置集合记为 X_u^i。非确定性移动智能体的动力学如下：

> 1. 对于所有 $i \in R$, $X_u^i = \{\alpha(s)_u^i\}$ 且 $u \le |\alpha(s)^i|$ 的情况，即机器人在位置由 $\alpha(s)$ 指定的时间内确定性移动。2. 对于 $u > |\alpha(s)^i|$, $X_u^i \leftarrow \mathcal{N}_G(X_{u-1}^i)$ 的情况，即非确定性移动的机器人沿着 G 中的所有边，从先前占据的位置集合出发移动。3. 对于 $u > |\alpha(s)^i|$，从 X_u^i 中移除所有被其他机器人 $R \setminus \{i\}$ 确定性占据的位置，以及会在 $R \setminus \{i\}$ 与确定性移动的机器人发生顶点冲突或边冲突的位置。冲突位置存储在集合 C 中；当存在没有子节点（可用动作）的 $c \in X_{u-1}^i$ 时，就会将新的冲突更新至该集合。每当发现新的冲突时，都会重新启动对 $\alpha(s)$ 的验证。4. 非确定性移动的被攻陷机器人 a 不能移动到非确定性移动机器人在 $R \setminus \{a\}$ 中 先前 占据的任何位置，因此从 X_u^a 中移除所有也包含在 $X_{u-1}^{R\setminus\{a\}}$ 中的元素。5. $R\setminus\{a\}$ 中非确定性移动的机器人不能移动到被 a 以非确定性方式占据的任何位置，因此从 $X_u^{R\setminus\{a\}}$ 中移除所有也包含在 X_u^a 中的元素。6. 非确定性移动的被攻陷机器人 a 不能移动到 $R \setminus \{a\}$ 中非确定性移动的机器人所占据的任何位置，因此从 X_u^a 中移除所有也包含在 $X_u^{R\setminus\{a\}}$ 中的元素。

非确定性动力学演化至 $u = s + 1$、.....、u^*，其中 u^* 是满足以下条件的第一个时间步：$\exists l_{\text{obs}} \in X_{u^*}^a$ 满足 $l_{\text{obs}} \in \mathcal{N}_S(X_{u^*}^{R\setminus\{a\}})$，即在 $R \setminus \{a\}$ 中，另一台机器人在 a 上存在一种可能的观测，由此结束验证 $\alpha(s)$ 的第一阶段。对于第二阶段，我们只需从源顶点 $\alpha(s)_s^a$ 在 G 上进行图搜索，检查是否存在针对 a 的多智能体路径寻找偏离 $\tilde{x}$，使得在 $(s,\ u^*)$ 上，对于所有 $u \in (s,\ u^*)$，$\tilde{x}_u^a \notin \mathcal{N}_S(X_u^{R\setminus\{a\}})$。如果没有找到这样的偏离，则返回 true，这表示存在从 $\alpha(s)$ 出发的延续，使得在该延续中，a 在 $(s,\ u^*)$ 上不存在被禁止的未检测多智能体路径寻找偏离。如果对每个 $i \in R$ 都验证了每个 $\alpha(s)$，则公告$\{\alpha(s)\}_{s\in[t,f]}$ 被验证为视野限制型多智能体路径规划公告。

算法 1非确定性共观测枚举

1: **过程** VERIFY(G, S, V_{forb}, α, s, a) 2: $u \leftarrow s$ ▷ 时间偏移
3: $X_u^R \leftarrow \alpha(s)_u^R$ ▷ 每个机器人的初始可达集
4: 执行 5: $X_{u+1}^R \leftarrow$ REACHABLE($\alpha(s)$ G, X_u^R, u, C) 6: $X_{u+1}^a \leftarrow X_{u+1}^a \setminus X_u^{R\setminus\{a\}}$7: $X_{u+1}^{R\setminus\{a\}} \leftarrow X_{u+1}^{R\setminus\{a\}} \setminus X_{u+1}^a$8: $X_{u+1}^a \leftarrow X_{u+1}^a \setminus X_{u+1}^{R\setminus\{a\}}$ 9 $u \leftarrow u+1$: : 当 10 $X_u^a \cap \mathcal{N}_S(X_u^{R\setminus\{a\}}) \neq \{\}$11: $u^* \leftarrow u$12: $Q \leftarrow X_{u^*}^a \cap \mathcal{N}_G($ $X_{u^*}^{R\setminus\{a\}}$) 13: 返回 $\bigvee_{q\in Q} \neg$ATTACKEXISTS($a, G, V_{\text{forb}}, X, s,$ u^*, q) 14: 结束过程 15: 过程 REACHABLE(x, G, X, t, C) 16: $X_{\text{next}} \leftarrow \{\}$17: 对 $v \in X$ 执行 18: $X_{\text{next}} \leftarrow X_{\text{next}} \cup$ MOVEROBOT(x, G, v, t, C) 19: 结束循环 20: 返回 X_{next}21: 结束过程 22: 过程 MOVEROBOT(x, G, v, t, C) 23: 如果 $\exists r \in R, v = x_t^r \wedge |x^r| > t+1$ 则 24: 返回 $\{x_{t+1}^r\}$ ▷ 已知 r 的前缀
25: **结束条件判断**26: 返回 $\leftarrow \mathcal{N}_G(v) \setminus \{x_{t+1}^r :$ $r \in R \wedge |x^r| > t+1\}$27: **如果** $v \notin$ 返回**则** ▷避免边冲突
28: 返回 $\leftarrow$ 返回 $\setminus \{x_t^r :\ r \in R \wedge x_{t+1}^r = v\}$29: 结束条件判断 30: 返回 $\leftarrow$ 返回 $\setminus \{v : (v, t+1) \in C\}$ 31: 如果 |返回| $= 0$ 则 32: $C \leftarrow C \cup \{(v, t)\}$33: 引发冲突 34: 结束条件判断 35: 返回返回值 36: 结束过程 37: 过程 ATTACKEXISTS($a, G, V_{\text{forb}}, X, s, u^*, q$) 38: A $\leftarrow X_t^a$39: B $\leftarrow \{\}$40: 对于 $u = s+1,.. ., u^*$ 执行 41: A $\leftarrow \mathcal{N}_G(A) \setminus \mathcal{N}_S(X_u^{R\setminus\{a\}})$ 42: B $\leftarrow \mathcal{N}_G($ $B) \setminus \mathcal{N}_S(X_u^{R\setminus\{a\}})$ 43: B $\leftarrow$ B $\cup$ (A $\cap V_{\text{forb}}$) 44: 结束循环 45: 返回 $q \in B$46: 结束过程

定理 2（非确定性共同观测枚举的可靠性）。设 x 为一个多智能体路径查找计划，α 为针对 x 的一系列公告。则如果算法1返回 true，那么 α 就是针对 x 的限制时域的多智能体路径寻找公告。

证明。式（6）等价于以下陈述：对于在 $(s,\ f)$ 上针对 $a \in R$ 的所有禁止的多智能体路径偏离 $\tilde{x}$，都存在一个 $\alpha(s)$ 的多智能体路径延续 y，使得如果 y 是中央执行器的多智能体路径查找计划，则执行攻击 $\tilde{x}$ 将触发基于共同观测的检测。令 $\{X_u\}_{u>s}$ 表示由算法1计算得到的、从时间 s 开始各机器人的（非）确定性可达集序列。我们首先证明一个引理，说明算法1的非确定性移动抽象相对于共同观测可能性的可靠性：

引理 1（非确定性抽象保留共同观测的可能性）。设 $q \in X_u^a$。若 $q \in \mathcal{N}_S(X_u^{R\setminus\{a\}})$，则存在一个多智能体路径延续 y, $y \succeq \alpha(s)$，使得 $y_u^a \in \mathcal{N}_S(y_u^{R\setminus\{a\}})$。换言之，如果

在非确定性抽象下， a 有可能在时间 u 于位置 q被观测到，那么就存在一个从 $\alpha(s)$开始的多智能体路径延续，其中 a 在时间 u于位置 q被观测到。

引理 1 的证明：首先，由于对于所有 $i \in R$， X_u^i 中不存在不属于 $\mathcal{N}_G(X_{u-1}^i)$ 的元素，因此，通过从某个 X_{u-1}^i 中的位置沿着 E 中的一条边移动一步，即可到达 X_u^i 中的所有位置。此外，由于 X_u^i 中的元素不在冲突集 C中，因此相对于已知前缀 $\alpha(s)$，存在一条从 $\alpha(s)_s^i$ 到 X_u^i 中每个元素的、位于 G 上的无冲突路径。由于不确定性移动的 a 不允许移动到 $X^{R\setminus\{a\}}$中的任何元素，因此对于所有 $q \in X_u^a$，存在一个 $y \succeq \alpha(s)$，使得 $y_u^a = q$。至于 $R\setminus\{a\}$中其他机器人的不确定性移动对，抽象并未明确阻止顶点冲突和边冲突。然而，由于 $X_u^{R\setminus\{a\}}$中的元素不在冲突集 C中，因此某个机器人$i \in R\setminus\{a\}$ 可以占据 $X_u^{R\setminus\{a\}}$中的每个元素，而不会与确定性移动的机器人发生冲突。同理，由于 $R\setminus\{a\}$ 中的不确定性移动机器人不允许移动到 X^a中的任何元素，我们得出结论：阻止机器人 $i \in R\setminus\{a\}$ 到达 X_u^i 中某个位置的唯一冲突，是与另一个不确定性移动机器人 $j \in R\setminus\{a,i\}$发生的冲突。因此，对于所有 $p \in X_u^i$，要么存在一个 $y \succeq \alpha(s)$，使得 $y_u^i = p$；要么存在一个 $y \succeq \alpha(s)$ $j \in R\setminus\{a,i\}$，使得 $y_u^j = p$。我们得出结论，对于所有 $q \in X_u^a$、 $p \in X_u^{R\setminus\{a\}}$，存在一个 $y \succeq \alpha(s)$、 $i \in R\setminus\{a\}$，使得 $y_u^a = q$且 $y_u^i = p$。 ■

定理2的证明：现在令 u^*、 l_{obs} 分别为根据算法1计算出的、在 a 上首次可能观测的时间和位置。令 $\tilde{x}$ 为 a 在$(s, s+k)$上、 $k > 1$的任意一种禁止的多智能体路径查找偏离。情形I， $\tilde{x}_{u^*}^a \neq l_{obs}$：由引理1可立即得出， $\exists y \succeq \alpha(s)$ $i \in R\setminus a$ 使得 $l_{\text{obs}} \in \mathcal{N}_S(y_{u^*}^i)$。因此， a 错过了一次观测，从而在中央执行器中触发基于共同观测的检测。情形II(a)， $\tilde{x}_{u^*}^a = l_{obs}$ 且 $\exists u \in (t, u^*)$使得 $\tilde{x}_u^a \in \mathcal{N}_S(X_u^{R\setminus\{a\}})$：在这种情况下，同样可由引理1立即得出， $\exists y \succeq \alpha(s)$ $i \in R\setminus\{a\}$ 使得 $\tilde{x}_u^a \in \mathcal{N}_S(y_u^i)$。然而，由于$u < u^*$，这与 a 上的首次可能观测发生在时间 u^*相矛盾。因此， a 导致了一次意外观测，从而在中央执行器中触发基于共同观测的检测。情形II(b)， $\tilde{x}_{u^*}^a = l_{obs}$ 且$(\neg\exists u \in (t, u^*)$使得$\tilde{x}_u^a \in \mathcal{N}_S(X_u^{R\setminus\{a\}})$：仅剩下这样的禁止偏离： a 没有错过时间 u^*的计划观测，也没有在时间 $u \in (t, u^*)$引入意外观测。该算法执行图搜索，以检查是否存在此类偏离。 ■

□

算法1的计算复杂度为 $\mathcal{O}(RV)$，因为该过程会在攻击者的可达集与任一防御者的可达集相交时终止——总共有 R 个集合，每个集合的最大基数为 V。每个潜在攻击者 a 和公告 $\{\alpha(s)\}_{s\in[t,f]}$ 都可以并行验证，从而高效地计算出最大长度的时域限制型公告。

4 实验结果

在上一节中，我们提出了一种缓解计划偏离攻击的策略，该策略依赖于机器人的共同观测，并限制在任意时刻所披露的规划信息量。本文将回答以下研究问题：

RQ1 与仅通过定位自报告检测问题的集中式多机器人系统相比，HoLA在安全性方面有何优势?

RQ2 与非安全感知的集中式多机器人系统相比，HoLA带来的开销是多少？**RQ3** 一般MAPF计划中的机器人共同观测具有什么特性会导致安全漏洞？**RQ4** 机器人共同观测在安全性方面有何优势？引入机器人共同观测后，在不使用限制视界的公告的情况下，我们缓解计划偏离攻击的能力会受到怎样的影响？**RQ5** 增量式计划的公告计划会如何影响攻击的有效性？**RQ6** 典型的集中式多机器人系统部署可能采用的公告方案存在哪些安全漏洞?

4.1 实验设置

环境。多智能体路径规划方案使用 ECBS 算法 [Barer等人（2014）], 计算。ECBS 是一种高效且有界次优的图式多智能体路径规划求解器（因此适用于集中式多机器人系统），用于一组包含 100 个标准多智能体路径规划四邻接网格基准实例 [H¨onig（2021）]。这些多智能体路径查找实例均可求解（即存在可求解该实例的多智能体路径查找计划），由随机生成的四邻接 32×32 网格构成，机器人数量为 10、20、.....或 100，且

~200 包含障碍物。我们假设每个机器人都能感知相邻方格；也就是说，每个机器人的传感器模型 S 与可达性图 G 相同。假设机器人在网格上彼此相邻时能够相互观测。我们使用 Rust 编程语言实现公告安全验证；运行时间是在 4GHz 的 Intel Core i7-6700 处理器上测得的。可在
https://github.com/gitsper/hola-announce 获取用于复现实验的源代码
执行场景。有两个因素会影响公告计划：1. 公告中包含多少个提前步骤；2. 一次从中央执行器向机器人发送的通信中包含多少条公告。提前步骤的数量体现了安全性与任务计算延迟之间的权衡：为提高安全性，公告应仅包含一个步骤，但这会导致机器人团队完成任务所需的时间增加。我们使用以下符号表示：

- $(p,\ k)$-公告：规定中央执行器每 p 个时间步发布一条新公告，并且每条公告包含接下来 k 个步骤的规划信息。

隐蔽攻击者指标。我们考虑隐蔽攻击者攻陷名义执行场景时的安全性。我们不进行仿真，而是针对每个场景，从10个不同的机器人中随机选择一个作为隐蔽攻击者，并从网格中的10个位置中随机选择一个标记为禁区位置，然后使用算法1检查公告是否相对于被攻陷的机器人和禁区位置具有限制时域的作用。我们使用以下指标：

- 安全隐蔽场景是指在给定一组可能场景的情况下，可由算法1验证为能够防范隐蔽攻击者的场景比例，也是衡量该案例容易受到隐蔽攻击者攻击程度的指标。

一个多智能体路径查找实例及其对应的由 ECBS 计算出的多智能体路径查找计划、共同观测调度和公告调度构成一个执行场景，简称场景。

大胆攻击者指标。在每个场景中，我们还会考察一种非隐蔽型攻击者（即大胆攻击者）的行为。这种攻击者即使不确定攻击是否会构成被禁止且未被检测到的偏离，也可能尝试发动攻击。大胆攻击者的偏离行为会持续到 $V_{\text{forbidden}}$，并根据 $\alpha(t)$ 中的信息，尽可能匹配共同观测调度，但不会推理从 $\alpha(t)$ 开始的后续延续。我们模拟大胆攻击者 100 次，每次随机选择 10 个不同机器人中的一个来扮演攻击角色，并随机选择网格中的 10 个位置之一，将其标记为禁区位置。我们对各场景中的指标取平均值。对于大胆攻击者，我们无法验证计划是否安全，因此 CE 会尝试进行检测，但无法保证检测成功。我们使用以下指标来衡量攻击及其检测情况：

- 大胆型攻击成功率是被攻陷的机器人执行禁区偏离的仿真所占比例，也是衡量被攻陷机器人在各场景集合中相对危险程度的指标。
- 大胆型漏检率是阳性案例中中央执行器基于我们的自我报告检测机制未报告异常的比例，也是衡量中央执行器漏检多少次禁区偏离的指标。

4.2 HoLA 的安全收益

本文的核心论点是，仅依靠机器人对自身定位的自我报告，根本不足以检测或阻止集中式多机器人系统中的恶意行为。因此，本文的主要贡献是 HoLA：一种利用机器人共同观测和限制视界的公告为中央执行器提供安全保障的安全措施。借助 HoLA，中央执行器可以计算并发布最大公告，从而保证系统中的所有隐蔽攻击都会被阻止。此外，HoLA 通过同时增加攻击规划问题的难度并收集协同观测报告，帮助检测系统中的非隐蔽攻击者。为证明 HoLA 的必要性（**RQ1**），我们考虑一个大胆攻击者，并比较两种中央执行器实现：1. 仅采用基于定位的检测，并向机器人发布完整的多智能体路径查找计划（无缓解措施）；2. HoLA：采用基于共同观测的检测，由中央执行器发布最大长度公告，并已通过算法 1 验证这些公告能够阻止所有隐蔽攻击。

在图2中，我们展示了大胆攻击者的漏检率随执行场景中的机器人数量 $|R|$ 变化的情况。我们观察到，当中央执行器不采取任何缓解措施时，大胆攻击者造成的几乎所有禁区偏离都会被中央执行器漏检，这凸显了基于定位的检测方法并不充分。相比之下，采用 HoLA 后，不仅所有隐蔽攻击都能得到确切防范，中央执行器漏检的大胆型攻击也大幅减少；当 $|R| = 100$ 时，大胆型攻击的漏检率最终仅为 22%。在检测方面，HoLA 始终优于未采取缓解措施的中央执行器；

对于较大的 $|R|$，大胆型攻击的漏检率更低，这是因为在更拥挤的环境中，机器人之间进行共同观测的频率更高。我们注意到，在某些场景下，大胆攻击者必定能在不被 HoLA 检测到的情况下得手，例如被攻陷的机器人靠近禁区且远离其他机器人时。

4.3 公告安全验证的开销

我们的解决方案提出，中央执行器应使用算法1来验证所选的 α 是否为时域限制型多智能体路径查找公告。验证程序的计算开销取决于机器人数量 $|R|$。我们的场景集包含机器人数量在10至100之间的实例，多智能体路径查找的最大长度为70个时间步（平均长度为49个时间步）。在所有场景中，我们都使用算法1依次验证每个机器人；验证耗时从未超过6分钟。对于 $|R| = 10$，平均耗时为48秒；对于 $|R| = 100$，为2.11分钟。由于每个机器人的公告都是独立验证的，因此计算过程可并行化。作为比较，在我们的基准测试中，多智能体路径查找实例使用ECBS进行规划（次优界为1.3）最多耗时1分钟；而在我们的8核CPU上，验证程序最多耗时6分钟。$/8 = 45$秒。

4.4 一般MAPF计划的安全性

我们旨在了解一般MAPF计划的哪些特性会提升或削弱 HoLA 下场景的安全性（**RQ3**）。从攻击者的角度来看，偏离检测计划之所以安全，是因为攻击者连续两次观测之间不存在未被检测到的禁用计划偏离。我们进行了以下实验：运行攻击场景，模拟大胆型攻击者，并改变公告中包含的前瞻步数；然后根据攻击者连续两次观测之间最多相隔的时间步数对场景进行分类，我们将其称为最大观测间隔时间。

在图 3 中，我们绘制了大胆型攻击的攻击成功率。结果显示，连续两次观测之间最多相隔较少（< 15）个时间步的攻击者，其攻击成功率低于 10%；而连续两次观测间隔较大（> 25）的攻击者，攻击成功率则显著高于平均水平，当最大观测间隔时间为 40 个时间步时，攻击成功率达到 $\sim 70\%$。通过跟踪对隐蔽型攻击者进行验证的安全场景，也证实了最大观测间隔时间增加与安全性降低之间的相关性：我们发现，至少每 10 个时间步就被观测一次的攻击者，其场景安全率为 100%；超过这一间隔后，安全场景的比例呈下降趋势，最终在观测最少的隐蔽型攻击者中降至 81%。

4.5 消融研究：机器人协同观测的安全效益

在第 3.1 节中，我们声称，仅包含定位信息的机器人自我报告不足以提供安全保证。我们通过实验结果支持这一论断（**RQ4**）。我们考虑一个大胆攻击者，并比较两种 CE实现：一种仅采用基于定位的检测，另一种采用基于共同观测的检测；同时，我们改变每条公告中可用信息的数量，即公告包含多少步的前瞻信息。若不使用共同观测，要触发 CE 检测，被攻陷的机器人就必须与未被攻陷的机器人发生碰撞，或者占据原本应由未被攻陷的机器人占据的位置。对于使用共同观测的情况，如果报告的共同观测与 CE 的预期不符（见定义 5），也会触发检测。

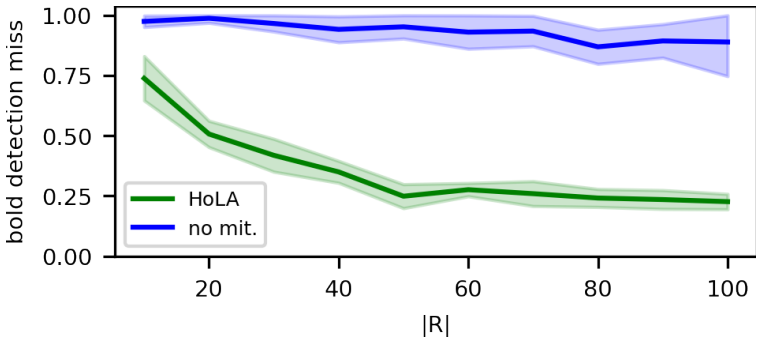


图 2：当中央执行器仅采用基于定位的检测（无缓解措施）或采用 HoLA 时，大胆攻击者的大胆型检测漏检率。在 HoLA 情况下，中央执行器会收集协同观测报告，并且公告的最大长度经验证符合时域限制。

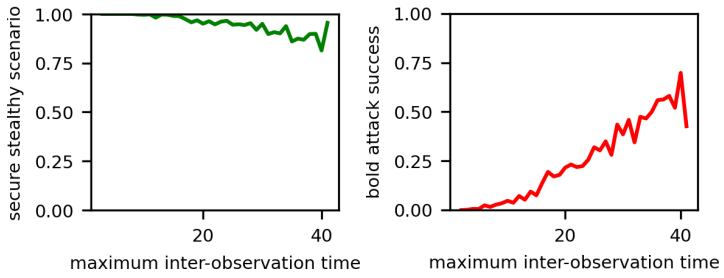


图3：对于大胆攻击者，攻击成功率；对于隐蔽攻击者，在一般*MAPF*计划（即无法确定这些计划是否能检测偏离，因为它们并非为此目的生成）下的安全场景数量，随机器人处于未观测状态的时间（最大观测间隔时间）变化。

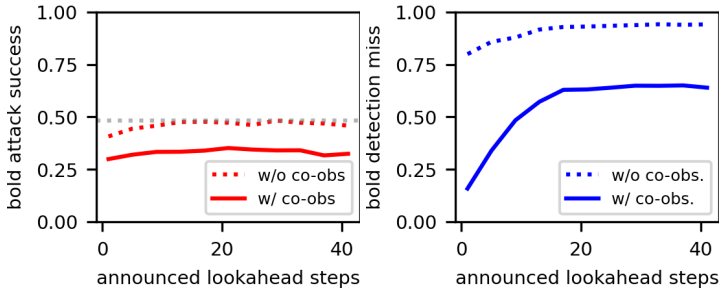


图4：启用共同观测和未启用共同观测时，大胆攻击者的攻击成功率和漏检率。此时中央执行器使用（1，k）公告计划；其中，k表示前瞻步数。在某些场景中，攻击不可行，因此大胆攻击成功率的上界以灰色虚线标出。

在图 4 中，我们展示了大胆攻击者的攻击成功率和漏检情况随 k（公告中包含的前瞻步数）的变化。我们观察到，在采用最小公告（$k = 1$）的情况下，对于不使用共同观测的设置，CE 的漏检率为 80%；而采用机器人协同观测时，CE 的漏检率仅为 16%。随着公告包含的信息增多（k 大于 25），不使用共同观测的 CE 的漏检率接近 94%，而收集共同观测的 CE 的漏检率则接近 64%。在不使用共同观测和使用共同观测的情况下，大胆攻击者的成功率分别从约 46% 降至 33%。

4.6 消融研究：公告计划对安全性的影响

我们在第3.2节指出，公告计划会影响场景的安全性：信息量更大的公告计划会缩小攻击者认为可能被禁止且未被检测到的计划偏离集合（**RQ5**）。然而，我们没有理论保证：(1) 算法1能够证明更多信息量较少的场景具有时域限制；(2) 信息量较少的公告在理论上增加了大胆攻击者的攻击规划难度，这是否会对应于攻击成功率和隐蔽性的可测量下降。

我们按照参数 k 对图 5 中的结果进行分类，该参数表示一条公告中的前瞻步数；根据公告的单调性，(1，k)-公告所含信息少于 (1，$k+1$)-公告，而 (k，k)-公告所含信息少于 (1，k)-公告。对于隐蔽攻击者的安全性验证（见图 5），我们确实观察到 k 与安全场景之间存在负相关：例如，在所有 (1，k)-公告场景中，最少 ($k = 1$) 条公告时，安全场景约占 98%；随着 k 增加，这一比例降至约 90%。我们还发现，环境中的智能体密度会显著影响我们使用算法1验证安全性的能力随 k 增加而迅速下降的程度。例如，在机器人数量较少的场景中，$|R| = 10$ 时安全场景比例降至约 70%；而在 $|R| > 70$ 的场景中，安全场景比例则不低于 95%。除了证明我们提出的方法能够验证大多数针对隐蔽攻击者的场景的安全性外，我们还注意到，未被攻陷的机器人密度增加，有助于提升我们验证系统安全性的能力。

我们观察到，k (p，k)-公告的前瞻参数与大胆攻击者的 CE 检测漏检率之间存在正相关关系（图 5）。具体而言，最小公告（$k = 1$）对应的漏检

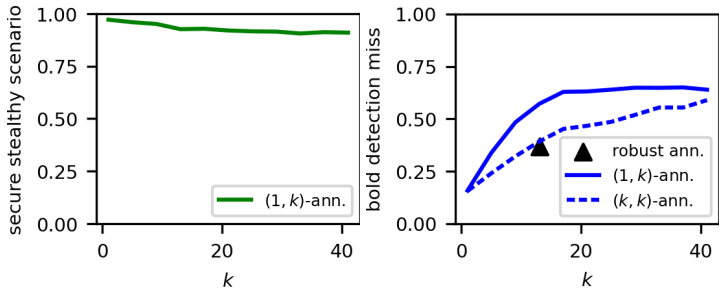


图 5：隐蔽攻击者的安全场景，以及大胆攻击者的漏检情况。比较 CE 使用 $(1, k)$-公告或 (k, k)-公告的场景；前者在每个时间步公告接下来的 k 步，后者每隔 k 步公告一次接下来的 k 步。我们还绘制了鲁棒公告方案的漏检率与平均前瞻范围之间的关系。

率低于 20%，但在测试过的信息量最大的公告下，漏检率最高接近 60%。结果表明，尽管限制公告不会改变大胆攻击者可采取的行为集合，但实际上，攻击者在选择计划偏离时所经历的歧义增加，会对大胆攻击者的隐蔽性产生显著影响。

合成公告类别有助于展示信息披露与安全之间的关系，但这些类别无法直接与典型多机器人系统（MRS）部署中可能采用的其他公告方案进行比较（**RQ6**）。作为比较，我们考虑根据运动计划计算鲁棒公告的场景，方法遵循 [Honig 等人（2019）]。由于鲁棒公告的前缀长度会动态变化，且各机器人各不相同，因此我们测量每个机器人的平均前缀长度，即综合所有计划、时间和机器人的数据，衡量关于特定机器人的未来规划信息的典型可用量。我们发现，平均前瞻范围约为 13 个时间步；对于鲁棒公告方案，CE 的漏检率约为 37%（图 5）。结果表明，从安全角度来看，鲁棒公告方案与 (k, k)-公告类别相当相似（因为 (13,13)-公告的漏检率相近）。

5 相关工作

巡逻。与我们的工作最相关的是，在对抗性多机器人巡逻（MRP）博弈的背景下，研究了机器人在实体安全场景中的应用。在这类博弈中，多机器人系统需要经过编程，以最大限度地检测试图闯入禁区的入侵者 [Agmon et al.(2008)]。对手可能掌握零、一部分或全部系统知识 [Agmon et al.(2011)]；入侵检测可以采用集中式或分布式方式 [Fagiolini et al.(2007), Fagiolini et al.(2008)]；检测器除了巡逻机器人外，也可能使用固定传感器 [Kim et al.(2008)]。MRP 与我们的工作有几方面不同。在 MRP 中，巡逻机器人的唯一目标是巡逻，并且假定巡逻机器人值得信任，而入侵者是外部人员；相比之下，在我们的设定中，机器人的首要目标是执行应用任务，机器人可能遭到入侵，而“入侵者”（试图闯入禁区的机器人）则是内部人员。

鲁棒多智能体路径查找。以往关于多智能体路径查找的研究提出了不同的公告计划，以便在发生智能体故障或运动延迟时能够更灵活地重新规划 [H¨onig 等人（2019），Atzmon 等人（2020）], ，或实现容错机器人规划 [Yang 等人（2011），Arrichiello 等人（2015）]。本文聚焦于缓解计划偏离攻击，因此我们的公告计划侧重于为安全目的渐进式披露信息。近期关于多机器人监控的研究探讨了被攻陷的机器人如何有效地拒绝服务，例如在 [Liu 等人（2021）],中，针对被攻陷机器人的韧性被建模为一个鲁棒任务调度问题。

机器人应用安全。多项研究探讨了机器人和多智能体安全； [Bijani and Robertson(2014), Yaacoub et al.(2021)]综述了相关研究。Bicchi *et. al.* [Bicchi et al.(2008)] 以及 Renganathan 和 Summers [Renganathan and Summers(2017)]从通信层面分析了机器人网络安全；Portugal *et. al.* [Portugal et al.(2017)]在有人在回路的场景下对此进行了研究；Morante、Victores 和 Balaguer [Morante et al.(2015)]则对此进行了广泛探讨。多项研究探讨了机器人与物理环境交互所产生的安全问题，例如工厂装配线所用类型的机械臂存在的漏洞 [Quarta et al.(2017)], 、机器人传感器存在的漏洞 [Choi et al.(2020)], 以及执行器存在的漏洞 [Guo et al.(2018)]。一些研究展示了攻击者如何利用机器人操作系统中的软件漏洞

系统（ROS）发动攻击，并提出相应的安全增强措施 [Dieber et al.(2016), Rivera et al.(2019)]。所提出的防御措施侧重于软件本身，而非机器人应用本身。

路由协议中的基于位置的攻击。 [Shoukry 等人（2018）] 提出了一种能够抵御女巫攻击的交通流量估计与路由算法，该算法利用传感基础设施提供的信息，以及车辆的动力学和相互距离。其他研究则利用系统的物理属性构建能够抵御攻击的网络协议 [Gil 等人（2017）]。这种情况下的场景与我们的问题截然不同：我们的系统中有一个中央实体 CE 负责规划和检测，而机器人在移动方式上受到限制。

6 结论

本文重点研究了如何利用机器人协同观测和增量式计划发布来缓解计划偏离攻击。攻击者有两个目标：一是朝禁区移动，二是不被中央实体检测到。我们利用共同观测来限制攻击者谎报其位置的能力；同时限制增量式计划公告的规模，使攻击者难以有把握地提前规划。我们根据攻击者是否希望不被检测到，将其分为两类：“隐蔽型”和“大胆型”。我们证明，对于一类隐蔽攻击者，我们的方案能够阻止攻击。对于大胆攻击者，我们通过实验表明，我们的方案能显著提高对攻击的检测率。我们的方案开销也很小，因此适用于由几十到数百个机器人组成的群体。

参考文献

[abi(2019)] 2019. 消费机器人是一个处于转型期的市场；智能家居将成为这场变革的核心。https://www.abiresearch.com/press/consumer-robotics-market-transition-smart-home-will-be-heart-change/. 访问日期：2021年4月4日..[iro(2020)] 2020. 历史。https://www.irobot.com/about-irobot/company-information/history. 访问日期：2021年4月4日..[spo(2021)] 2021. Spot。https://www.bostondynamics.com/spot. 访问日期：2021年4月4日..[Agmon 等人（2011）] Noa Agmon、Gal A Kaminka 和 Sarit Kraus。2011。多机器人对抗巡逻：面对全知对手。《人工智能研究期刊》42（2011），887–916。[Agmon 等人（2008）] Noa Agmon、Sarit Kraus 和 Gal A Kaminka。2008。对抗环境中的多机器人周界巡逻。载于*IEEE*机器人与自动化国际会议。IEEE，2339–2345。[Arrichiello 等人（2015）] Filippo Arrichiello、Alessandro Marino 和 Francesco Pierri。2015。联网多机器人系统中基于观测器的分散式故障检测与隔离策略。《*IEEE*控制系统技术汇刊》23，4（2015），1465–1476。[Atzmon 等人（2020）] Dor Atzmon、Roni Stern、Ariel Felner、Glenn Wagner、Roman Bart´ak 和 Neng-Fa Zhou。2020。鲁棒多智能体路径规划与执行。《人工智能研究期刊》67（2020年3月），549–579。[Azadeh 等人（2019）] Kaveh Azadeh、Ren´e De Koster 和 Debjit Roy。2019。机器人化与自动化仓储系统：综述与最新进展。《交通科学》53，4（2019），917–945。[Barer等人（2014）] Max Barer、Guni Sharon、Roni Stern 和 Ariel Felner。2014。多智能体路径规划问题中冲突搜索算法的次优变体。第七届组合搜索年度研讨会论文集（2014）。[Bicchi 等人（2008）] Antonio Bicchi、Antonio Danesi、Gianluca Dini、Silvio La Porta、Lucia Pallottino、Ida M Savino 和 Riccardo Schiavi。2008。异构无线多机器人系统。《*IEEE*机器人与自动化杂志》15，1（2008），62–70。[Bijani 和 Robertson（2014）] Shahriar Bijani 和 David Robertson。2014。开放式多智能体系统中的攻击与安全方法综述。《人工智能评论》42，4（2014），607–636。[Choi 等人（2020）] Hongjun Choi、Sayali Kate、Yousra Aafer、Xiangyu Zhang 和 Dongyan Xu。2020。基于软件的机器人车辆传感器攻击实时恢复。载于第*23*届攻击、入侵与防御研究国际研讨会。349–364。[Choset 等人] Howie M Choset、Kevin M Lynch、Seth Hutchinson、George Kantor、Wolfram Burgard、Lydia Kavraki、Sebastian Thrun 和 Ronald C Arkin。2005。机器人运动原理：理论、算法与实现。麻省理工学院出版社。

[Dieber 等人（2016）] Bernhard Dieber、Severin Kacianka、Stefan Rass 和 Peter Schartner。2016。基于 ROS 的应用的应用层安全。载于智能机器人与系统国际会议。IEEE，4477–4482。[Fagiolini 等人（2008）] Adriano Fagiolini、Marco Pellinacci、Gianni Valenti、Gianluca Dini 和 Antonio Bicchi。2008。面向多机器人系统的基于共识的分布式入侵检测。载于2008年 IEEE 国际机器人与自动化会议。IEEE，120–127。[Fagiolini 等人（2007）] Adriano Fagiolini、Gianni Valenti、Lucia Pallottino、Gianluca Dini 和 Antonio Bicchi。2007。面向安全协作多智能体系统的分散式入侵检测。载于2007年第46届 IEEE 决策与控制会议。IEEE，1553–1558。[Gil 等人（2017）] Stephanie Gil、Swarun Kumar、Mark Mazumder、Dina Katabi 和 Daniela Rus。2017。保障抗欺骗多机器人网络。《Autonomous Robots》41，6（2017），1383–1400。[Guo 等人（2018）] Pinyao Guo、Hunmin Kim、Nurali Virani、Jun Xu、Minghui Zhu 和 Peng Liu。2018。RoboADS：针对移动机器人的传感器和执行器异常行为的异常检测。载于2018年第48届 IEEE/IFIP 可靠系统与网络国际年会（DSN）。IEEE，574–585。[H¨onig（2021）]Wolfgang H¨onig。2021。libMultiRobotPlanning。https://github.com/whoenig/ libMultiRobotPlanning[H¨onig 等人（2019）] Wolfgang H¨onig、Scott Kiesel、Andrew Tinka、Joseph W Durham 和 Nora Ayanian。2019。在仓库中持续且鲁棒地执行多智能体路径寻找调度。《IEEE Robotics and Automation Letters》4，2（2019），1125–1131。[Honig 等人（2019）] Wolfgang Honig、Scott Kiesel、Andrew Tinka、Joseph W. Durham 和 Nora Ayanian。2019。在仓库中持续且鲁棒地执行多智能体路径寻找调度。《IEEE Robotics and Automation Letters》4，2（2021年4月），1125–1131。https://doi.org/10.1109/LRA.2019.2894217[Kim 等人（2008）] Ji Min Kim、Jeong Sik Choi 和 Beom Hee Lee。2008。用于监控和控制安全区域内观测空间的多智能体协同运动规划。《IFAC Proceedings Volumes》41，2（2008），1679–1684。[Li 等人（2021）] Jiaoyang Li、Andrew Tinka、Scott Kiesel、Joseph W Durham、T K Satish Kumar 和 Sven Koenig。2021。大型仓库中的终身多智能体路径寻找。AAAI 人工智能会议论文集（AAAI）（2021）。[Liu 等人（2021）] Jun Liu、Lifeng Zhou、Pratap Tokekar 和 Ryan K Williams。2021。对抗环境中的分布式弹性次模动作选择。《IEEE Robotics and Automation Letters》6，3（2021），5832–5839。[Morante 等人（2015）] Santiago Morante、Juan G Victores 和 Carlos Balaguer。2015。机器人密码安全：机器人为何需要网络安全。《Frontiers in Robotics and AI》2（2015），23。[Portugal 等人（2017）] David Portugal、Samuel Pereira 和 Micael S Couceiro。2017。安全在人机共享环境中的作用：基于 ROS 的监控机器人的案例研究。载于2017年第26届 IEEE 机器人与人类交互通信国际研讨会（RO-MAN）。IEEE，981–986。[Quarta 等人（2017）] Davide Quarta、Marcello Pogliani、Mario Polino、Federico Maggi、Andrea Maria Zanchettin 和 Stefano Zanero。2017。工业机器人控制器的实验性安全分析。载于2017年 IEEE 安全与隐私研讨会（SP）。IEEE，268–286。[Renganathan 和 Summers（2017）] Venkatraman Renganathan 和 Tyler Summers。2017。面向分布式多机器人系统的抗欺骗协同。载于2017年多机器人与多智能体系统国际研讨会（MRS）。IEEE，135–141。[Rivera 等人（2019）] Sean Rivera、Sofiane Lagraa、Cristina Nita-Rotaru、Sheila Becker 和 Radu State。2019。ROS-defender：基于 SDN 的机器人应用安全策略执行。载于2019年 IEEE 安全与隐私研讨会（SPW）。IEEE，114–119。[Shoukry 等人（2018）] Yasser Shoukry、Shaunak Mishra、Zutian Luo 和 Suhas Diggavi。2018。抗女巫攻击的交通网络：一种基于物理的信任传播方法。载于2018年 ACM/IEEE 第九届网络物理系统国际会议（ICCPS）。IEEE，43–54。[Simon（2019）] Matt Simon。2019。在亚马逊仓库里，人类与机器融为一体。https://www.wired.com/story/amazon-warehouse-robots/。访问日期：2021年4月4日..[Stern 等人（2019）] Roni Stern、Nathan R. Sturtevant、Ariel Felner、Sven Koenig、Hang Ma、Thayne T. Walker、Jiaoyang Li、Dor Atzmon、Liron Cohen、T. K. Satish Kumar、Roman Bart´ak 和 Eli Boyarski。2019。多智能体路径寻找：定义、变体与基准。载于第十二届组合搜索年度研讨会。

[Wardega 等人（2019）] Kacper Wardega、Roberto Tron 和 Wenchao Li。2019。多机器人系统抵御物理伪装攻击的韧性。*2019 年 IEEE 安全与隐私研讨会论文集（SPW 2019）*（2019），120–125。[Yaacoub 等人（2021）] Jean-Paul A Yaacoub、Hassan N Noura、Ola Salman 和 Ali Chehab。2021。机器人网络安全：漏洞、攻击、对策与建议。《国际信息安全杂志》（2021），1–44。[Yang 等人（2011）] 杨浩、Marcel Staroswiecki、姜斌和刘建业。2011。一类非线性多智能体系统的容错协同控制。《系统与控制快报》60，4（2011），271–277。[Yu 和 LaValle（2013）] 余晶金和 Steven M LaValle。2013。图上多机器人最优路径规划的结构与难解性。载于第二十七届*AAAI*人工智能会议。