arXiv:2301.06977v1 [cs.RO] 17 Jan 2023

群体规模下的拜占庭容错能力：基于机器人间指控的去中心化阻止列表协议

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18日

摘要

加权均值子序列约简（W-MSR）算法是去中心化多机器人系统拜占庭容错设计中最先进的方法，其原理是丢弃通过线性共识协议（LCP）接收到的离群值。尽管 W-MSR 提供了充分理解的理论保证，将稳健的网络连通性与底层共识的收敛联系起来，但该方法存在若干局限，阻碍其规模化应用：1. 必须预先知道需要容忍的拜占庭机器人数量 F；2. 要求每个机器人维持 $2F+1$ 个邻居，这对于大型 F 并不现实；3. 要求$F+1$ 机器人独立测量共识属性，才能改变机器人群的决策，这阻碍了信息传播；4. W-MSR 专用于 LCP，无法推广到未通过 LCP 实现的应用中。本文提出一种基于机器人间指控的去中心化阻止列表协议（DBP）。指控基于本地观察到的不当行为而提出，并由协作机器人在网络中共享；随后，这些指控作为图匹配算法的输入，用于计算阻止列表。DBP 可推广至未通过 LCP 实现的应用，能够适应拜占庭机器人的数量，并在降低相较于 W-MSR 所需网络连通性的同时，实现多机器人系统中的快速信息传播。对于 LCP 类应用，DBP 将 W-MSR 的最坏情况连通性要求从 $(2F+1)$-连通降至 $(F+1)$-连通，并将传播新信息所需的最少协作观察者数量从 $F+1$ 降至仅需 1 名观察者。我们通过协作目标跟踪、时间同步和定位案例研究进行实证验证，证明我们提出的拜占庭容错方法可扩展至数百个机器人。

1 引言

目前应用于工业领域的多机器人系统（MRS）采用结构化部署环境和高度集中的设计 [Verma and Ranga(2021)]。集中协调有利于多机器人系统的所有关键组成部分——任务分配、执行、故障检测与恢复；而结构化环境则允许采取严格的物理安全措施。相比之下，在非结构化环境中涌现的多机器人系统应用（例如巡逻、搜救、覆盖、

形状形成和集体运输）通常因通信限制而不适合采用集中式方法 [Gielis et al.(2022)]。因此，针对非结构化环境中故障和/或恶意机器人的负面影响而采取的去中心化方法，已受到广泛关注，尤其是因为大量攻击已被证明会破坏多机器人系统的功能和安全性，例如传感器扰动和拒绝服务（DoS） [Djouadi et al.(2015), Zhou et al.(2020), Liu et al.(2021)], 执行器干扰 [Guo et al.(2018)], 网络拒绝服务攻击 [Yaacoub et al.(2022)], 或 Sybil／虚假身份攻击 [Gil et al.(2017), Mallmann-Trenn et al.(2021)]。鉴于攻击方式众多，理解多机器人系统抵御拜占庭攻击者的韧性至关重要——也就是说，若允许机器人中的某个未知子集在物理行动和通信方面表现得与协作机器人任意不同，系统将如何应对。

未考虑拜占庭故障的多机器人系统实现通常十分脆弱，只要有一个机器人遭到破坏，系统就会彻底失效。例如，在我们的案例研究中，拜占庭机器人可能会导致机器人群中的机器人追随虚假目标，或在时间同步或定位方面产生任意大的误差。目前，针对拜占庭容错多机器人系统提出的主要方法是加权均值子序列缩减（W-MSR）算法 [LeBlanc 等人（2013年）、Saulnier 等人（2017年）、Mitra 等人（2019年）]。W-MSR 易于实现，且其理论保证已得到充分理解。然而，W-MSR 只能用于通过线性共识协议（LCP）实现的多机器人系统应用；其性能不会随系统中机器人数量的增加而扩展，并且可容忍的拜占庭机器人数量 F 必须事先确定。假设机器人通过 LCP 就环境的某项物理属性达成集体决策。在 W-MSR 中， F 的取值决定了机器人在线性共识的每次更新中应舍弃多少个离群值；每个机器人至少需要 $2F+1$ 个邻居才能更新其局部共识变量，并且至少需要 $F+1$ 个协作机器人独立直接测量相关物理量。如果 F 的取值小于拜占庭机器人的数量，那么 W-MSR 提供的缓解效果便会失效。当 F 较大时，网络连通性要求以及维持 $F+1$ 个协作观测者所需的后勤工作，使 W-MSR 难以实际应用。

在这项工作中，我们提出了去中心化阻止列表协议 (DBP)，这是一种受点对点网络启发、基于机器人间指控的拜占庭容错方法。协作机器人利用局部观测检测有不当行为的对等节点，并据此提出指控。指控在协作机器人之间传播，随后每个机器人独立使用匹配算法处理这些指控，以计算阻止列表。我们推导出一组必要且充分的条件，规定必须提出哪些指控，以及多机器人系统（MRS）须具备何种连通性，才能确保协作机器人最终阻止所有拜占庭机器人，并减轻其影响。具体而言，我们证明，对于满足时变网络中类似（$F+1$）连通性要求的封闭式多机器人系统，阻止所有拜占庭机器人的条件等价于系统内所提指控满足霍尔婚姻定理。除了 W-MSR 要求事先知道可容忍的拜占庭机器人数量外，我们还指出，W-MSR 在实际应用中无法随机器人数量扩展。我们通过目标跟踪和时间同步应用的实证结果表明，情况确实如此；相比之下，我们提出的方法能够自适应地扩展至数百个机器人／攻击者，而相关工作所处理的机器人群不超过 20 个机器人，且仅包含一两个攻击者。对于未基于线性一致性协议（LCP）实现的多机器人系统，例如协作定位，W-MSR 无法提供拜占庭容错能力。我们使用所提出的方法实现了拜占庭容错协作定位，作为概念验证；据我们所知，这是首个成功实现去中心化且具备拜占庭容错能力的协作定位技术。

2 背景与相关工作

W-MSR。对于拜占庭容错去中心化多机器人系统，理解最为透彻的方法或许是 W-MSR 算法。W-MSR 可应用于基于线性一致性协议实现的多机器人系统应用中。线性一致性协议是一种针对实值变量的分布式一致性算法，在该算法中，每个时间步，机器人都会将其局部变量更新为邻居广播值的凸组合，即

$$x_i(t) = \sum_{j \in \mathcal{N}_G(i)} \alpha_j x_j(t-1) \text{ where } \sum \alpha_j = 1$$

而 $\mathcal{N}_G(i)$ 是连通图 G 中 i 的邻居。 [LeBlanc 等人(2013)] 首次提出了用于拜占庭容错能力的 W-MSR，该算法在 LCP 的每个时间步丢弃收到的 F 个最高值和 F 个最低值，并证明，即使存在多达 F 个拜占庭机器人，系统仍能收敛这一性质等价于一种图鲁棒性。具体而言，如果机器人的连通图至少是 $(2F+1)$-顶点连通的，那么共识将收敛到协作机器人初始值的凸包内某个值。W-MSR 已应用于多种场景，例如群集 [Saulnier 等人(2017)] 和状态估计 [Mitra 等人(2019)]。 [Salda˜na 等人(2017)] 提出了将 W-MSR 算法扩展到时变网络的方法，其中有界时间窗口内连通图的并集具有鲁棒性； [Amirian 和 Shamaghdari(2021)] 则将其扩展到事件驱动控制。 [Guerrero-Bonilla 等人(2017)] 提出了构建 W-MSR 算法所需鲁棒图拓扑的方法。

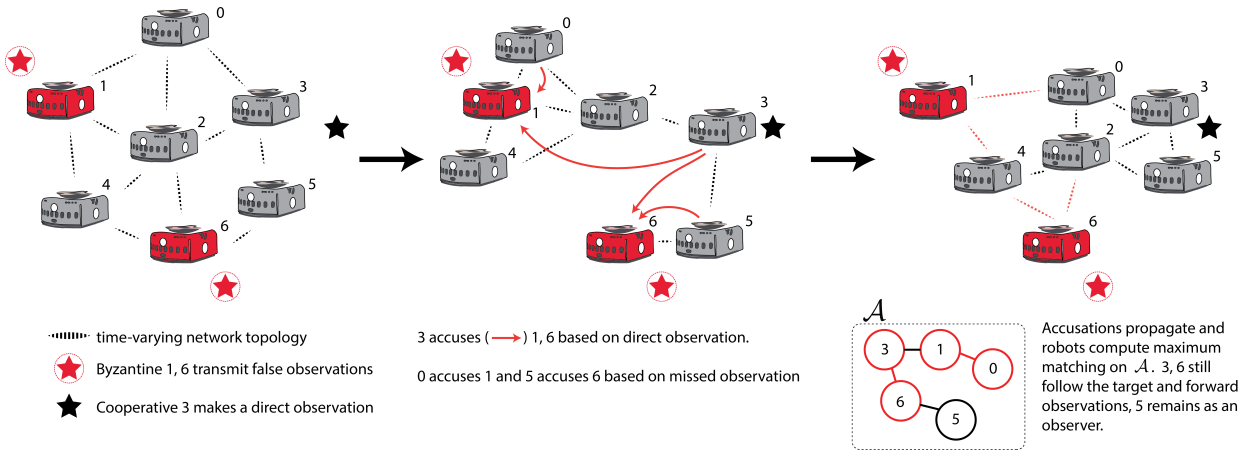

图 1：在第 5.1 节探讨的目标跟踪案例研究中，DBP 用于为一个简单的七机器人（其中两个为拜占庭机器人）场景提供拜占庭容错能力。拜占庭机器人 1 和 6 传输了虚假目标观测（红色星形），而协作机器人 3 直接观测到了目标（黑色星形）。协作机器人根据最近观测者的位置，向推测的目标位置移动。机器人 0 和 5 分别到达了机器人 1 和 6 报告的虚假位置，并根据本应进行却未能获得的观测，对这些观测者提出指控。与此同时，机器人 3 因机器人 1 和 6 的观测与其直接观测相矛盾，也对二者提出指控。指控在协作机器人之间传播，最终每个协作机器人都拥有记作 $\mathcal{A}$ 的指控图。每个机器人都使用 Edmonds 算法独立计算最大匹配 $\{(3,\ 6),\ (0,\ 1)\}$（红色边），因此机器人 0、1、3 和 6 的观测被屏蔽。其他协作机器人仍信任机器人 2、4 和 5 的观测。注意，机器人 0 和 3 仍继续协作，向目标移动，并转发来自未被屏蔽观测者的观测。

区块链。分布式账本技术（例如区块链）也因其可能提供韧性保证而受到广泛关注。针对与本文所考虑的类似场景，[Strobel 等人(2018)] 提议在一项多机器人系统集体决策研究中使用以太坊区块链。[Pacheco 等人(2020)] 探讨了基于区块链实现共识的方法。关于区块链在机器人应用中的研究（包括多机器人系统和机器人群），请参阅近期综述 [Aditya 等人(2021)]。

机器人间观测。在多智能体系统中，利用机器人间观测检测不当行为并建立信任，是一种常见做法。与我们利用指控计算阻止列表的工作不同，[Ashkenazi 等人（2019）] 提出，协作机器人在观察到机器人行为不当时，应采取物理行动将其隔离。例如，在协作巡逻案例研究中，协作机器人会包围并阻碍那些被观察到未沿正确轨迹行进的机器人。更常见的做法是将机器人间观测作为声誉机制的输入，由机器人维护同伴的实值声誉分数。例如，[Fagiolini 等人（2007）] 介绍了一项网联车辆案例研究，其中机器人利用部分信息判断其局部邻居是否不合作；后续工作 [Arrichiello 等人（2015）]则提出了一种适用于多机器人系统的自适应阈值执行器故障检测策略。[Pierson 和 Schwager（2016）], 探讨了将声誉分数用作协作覆盖问题的输入，而 [Cheng 等人（2021）] 则为多机器人系统提出了通用信任框架，并以智能交叉路口管理为案例进行研究。声誉机制也可以与共识结合，例如，[Fagiolini 等人（2008）] 提出让机器人就其他机器人的声誉值达成共识。归根结底，声誉机制继承了 W-MSR 的缺点：$F+1$ 在从系统中移除不当行为机器人影响力之前，协作机器人必须先为每个不当行为机器人赋予较低的声誉；此外，共识变量（即声誉分数）的数量会随着机器人群规模线性增长。

多机器人系统安全。除上述直接相关的研究外，我们的工作也受到更广泛的多机器人系统安全研究推动。关于多机器人系统中尚未解决的安全问题及针对各类问题的缓解建议，请参阅 [Bijani and Robertson（2014）] 的全面综述；关于不确定或对抗性运行环境下多机器人系统近期方法的讨论，请参阅 [Zhou and Tokekar（2021年）]。去中心化多机器人系统的攻击面广泛；[Guo 等人（2018）] 针对各种入侵场景测试了受信息物理系统启发的异常检测方法，例如车轮干扰、激光雷达拒绝服务攻击、车轮编码器逻辑故障等；[Djouadi 等人（2015）] 则分析了有界传感器攻击。我们工作的创新之处在于，对协作定位的拜占庭弹性进行了概念验证。拜占庭定位是一项具有挑战性的问题，[Weber 等人（2020）] 推导出了拜占庭定位在

集中式设置下可解的条件；与 W-MSR 类似，拜占庭定位要求机器人间测量的图结构满足鲁棒性。

女巫攻击。文献对某些威胁模型给予了特别关注。 [Zhou 等人（2020）], 提出了在拒绝服务攻击下高效调度多机器人系统的方法， [Liu 等人（2021）] 则将其扩展到了去中心化环境。在我们的工作中，我们假设多机器人系统免受女巫攻击，因为中央信任机构会为所有机器人签发身份。我们认为，对于封闭式 多机器人系统而言，通过中央机构确保系统具备抗女巫攻击能力是合理的假设；在这类系统中，机器人集合不会随时间变化。不过，面向多机器人系统的去中心化身份管理和抗女巫攻击能力仍是一个活跃的研究领域，与我们的研究方向正交。 [Gil 等人（2017）]首次提出利用机器人间的无线电信号检测女巫身份；随后， [Mallmann-Trenn 等人（2021）]将同一技术应用于女巫威胁模型下的协作集群场景。文献中还提出了其他受物理学启发、特定于应用的方法，例如防御针对众包交通信号灯的女巫攻击 [Shoukry 等人（2018）]。先前的研究还提出将女巫攻击防御作为 W-MSR 算法的一个组成部分 [Renganathan 和 Summers（2017）]。

3 威胁模型

我们考虑一个群体机器人系统，其中机器人通过时变网络拓扑 $G[t] = (V, E[t])$ 相连。每个机器人都有一个由可信中央机构在部署时颁发的身份，并利用该身份向邻居发送签名消息，以及验证接收消息的真实性。假设部分机器人被拜占庭对手控制，但具体是哪些机器人尚不确定。我们将协作机器人称为 $\mathcal{C} \in V$，将拜占庭机器人称为 $\bar{\mathcal{C}} = V \setminus \mathcal{C}$，并假设集合 V 和 $\mathcal{C}$ 是固定的，即多机器人系统是封闭的。我们假设存在一个强对手：拜占庭机器人可以在线集中协调彼此的行动，详细了解系统实现（例如机器人能力和应用细节），向协作机器人发送任意消息，并表现出任意物理行为。拜占庭机器人的目标是破坏多机器人系统的应用；具体目标和攻击策略取决于应用。第 5 节中的每个案例研究都会说明攻击者的目标和策略。由于机器人使用信任机构颁发的身份进行通信，我们假设对手无法发动女巫攻击，因为它无法伪造能被 $\mathcal{C}$ 接受的欺诈身份。然而，身份（密钥）已遭泄露的机器人可被对手用来发送误导性消息。因此，机器人群中密钥已被 $\bar{\mathcal{C}}$ 泄露的任何机器人都被视为 $\mathcal{C}$的一部分。

4 去中心化阻止列表协议

去中心化阻止列表协议（DBP）是一种群体阻止列表算法，能够适应拜占庭对手的存在。DBP 可作为 W-MSR 的替代方案，但对网络连通性的要求较低，且无需提前获知 F。DBP 具有适应性，因此对鲁棒网络拓扑的要求会随拜占庭机器人的实际数量而变化。即使实际的拜占庭机器人数量较少，W-MSR 对连通性的要求仍会随参数 F变化。图 1 展示了 DBP 在目标跟踪场景中的工作方式。协作机器人根据本地观测结果指控不当行为的对等节点。指控通过泛洪在网络中传播，并作为匹配算法的输入，由该算法生成阻止列表。

DBP 依赖泛洪这一网络通信原语，协作机器人始终会重新广播（转发）收到的消息。DBP 中的消息是由发起泛洪的机器人签名的指控。指控 $\text{Acc}_i(j)$ 是与应用无关的消息，其有效载荷仅为发起者 i 希望指控的机器人的身份 j。决定是否以及何时发出指控的具体规则取决于应用。指控用于消除拜占庭节点对群体应用的影响。每个机器人 i 都会在本地维护其收到的指控集合 $R_i[t]$。机器人 i 将使用任意确定性最大匹配算法（例如 Edmonds [Edmonds（1965年）]）在本地计算一个子集 $R_i^*[t] \subseteq R_i[t]$，以形成阻止列表。本节余下部分将假设机器人采用可靠的 指控机制：

定义 1（可靠指控）。 如果协作机器人 i 提出指控 $Acc_i(j)$，那么 $Acc_i(j)$ 是可靠的，当且仅当 $d \bar{\mathcal{C}}$仅当 $j \in \mathcal{C}$。

备注 1。在存在 $\bar{\mathcal{C}}$拜占庭机器人时，收到消息 $Acc_i(j)$ 意味着 $i \in \bar{\mathcal{C}} \vee j \in \mathcal{C}$。原因是，如果 $i \in \mathcal{C}$，那么 $j \in \mathcal{C}$ 指控的可靠性。在另一种情况下，$i \in \bar{\mathcal{C}}$。

匹配。重要的是，所收到的指控集合 $R_i[t]$ 具有由指控可靠性赋予的结构。给定一个无向图 $G = (V = X \cup Y, E)$，其中 X, Y互不相交，若 X 是 G中的独立顶点集，则称 G 为 X-半二部图 。若子集 $\mathcal{M}$ 是 G中的独立边集，则称子集 $\mathcal{M} \subseteq E$ 为 G 上的匹配 。给定一个

匹配 $\mathcal{M}$，我们用 $V_{\mathcal{M}}$ 表示 $\mathcal{M}$中的匹配顶点。如果无法向匹配 $\mathcal{M}$中添加更多边，则称 $\mathcal{M}$ 为极大匹配。如果不存在满足$|V_{\mathcal{M}^*}| > |V_{\mathcal{M}}|$的匹配 $\mathcal{M}^*$，则称 $\mathcal{M}$ 为基数最大匹配，或最大匹配。给定一个子集 $S \subseteq V$，若匹配 $\mathcal{M}$ 满足 $S \subseteq V_{\mathcal{M}}$，则称其为 S-完美匹配 。以下条件使我们能够将最大匹配与完美匹配的概念联系起来：

定义 2 (霍尔婚姻定理**)**。 给定 $G = (X \cup Y, E)$，使得 G 是 X-半二分图，则存在一个 Y-完美匹配，当且仅当 $\forall S \subseteq Y, |S| \leq |\mathcal{N}_G(S) \cap X|$。此外，任意最大匹配都是 Y-完美的。

指控图。现在令 $\mathcal{A}_k[t]$ 为边为 (i, j) 的指控图，当且仅当 $\text{Acc}_i(j) \in R_k[t]$。正如我们在备注 1 中指出的，每项指控都可以视为一个析取命题——$\text{Acc}_i(j)$ 可理解为“i 是拜占庭的，或 j 是¯拜占庭的（也可能两者都是）”。因此，$\mathcal{A}_k[t]$ 是 $\mathcal{C}$-半二分图，且 M 上的任意匹配都满足 $|V_M| \leq 2|\mathcal{C}|$。当且仅当霍尔婚配条件对 $\mathcal{C}$ 上的 $\mathcal{A}_k[t]$ 成立时，该不等式取等号——在这种情况下，¯ ¯最大匹配 M 是带有 $|V_M| = 2|\mathcal{C}|$的 $\mathcal{C}$-完美匹配。机器人 k 选择将 $R_k^*[t]$ 设为 $\mathcal{A}_k[t]$上的最大匹配的匹配顶点——与这些匹配顶点对应的机器人就是 k 将阻止的对象。图 1 中以“$\mathcal{A}$”展示了一个指控图及其对应的最大匹配示例。

网络泛洪。只有当所需的指控确实在 $\mathcal{C}$ 中的机器人之间传播时，这一匹配结果才有用。给定时变有向图 $G[t] = (V, E[t])$，考虑一次网络泛洪的执行：节点 $v \in V$ 在时刻 τ 发起泛洪，向其邻居 $\mathcal{N}_{G[\tau]}(v)$ 发送消息。当 v 的邻居向各自的邻居发送消息时，泛洪继续进行，因此在时刻 $\tau + 2$，$\mathcal{N}_{G[\tau+1]}(\mathcal{N}_{G[\tau]}(v))$ 将收到该消息。依此类推，对于正整数 s，泛洪的 s-前沿为

$$\mathcal{N}^s_{G[\tau]}(v) := \mathcal{N}_{G[\tau+s-1]}(\mathcal{N}_{G[\tau+s-2]}(\cdots \mathcal{N}_{G[\tau]}(v)))$$

因此，泛洪的 s-闭包为以下集合的并集

$$\mathcal{N}^{s^*}_{G[\tau]}(v) := \mathcal{N}^0_{G[\tau]} \cup \cdots \cup \mathcal{N}^s_{G[\tau]}$$

如果对于任意初始节点 v 和起始时间 τ，都存在一个正整数 s，使得 $\mathcal{N}^{s^*}_{G[\tau]}(v) = V$，那么我们称 $G[t]$ 是可泛洪的。到目前为止，我们假设节点可以多次重新传输消息。如果将重新传输次数限制为 n，且仍存在一个 s，使得以类似方式定义的 (n, s)-闭包等于 V，那么我们称 $G[t]$ 是 n-可泛洪的。如果 $|V| \geq k$，并且从 V 中移除任意一组 k 个节点后，$G[t]$ 仍然是 n-可泛洪的，那么我们称 $G[t]$ 是 (k, n)-可泛洪的。最终，我们现在可以指出，即使存在多达 F 个拜占庭机器人，协作节点也终将听到所有指控，并拥有相同的指控图：

定理 1 （最终区块列表共识）。 设 $G[t]$ 为机器人群 V 的时变 （F，n）-可泛洪网络拓扑。若 $|\bar{\mathcal{C}}| \leq F$，则存在 $\exists \tau \in \mathbb{Z}^+$、$\mathcal{A} \forall i \in \mathcal{C}$、$s \geq \tau$，使得 $\mathcal{A} = \mathcal{A}_i[s]$。

证明。 根据（F，n）-可泛洪的定义， V 发出的所有指控最终都会传达到所有 $\mathcal{C}$，因为即使最多有 F 个拜占庭节点不转发指控，协作机器人也能确保指控最终传达到所有 $\mathcal{C}$ 。由于多机器人系统是封闭的，可能的指控数量有限（上限为 $2|\mathcal{C}| + |\bar{\mathcal{C}}|^2$），因此存在一个时间 τ，此后不会再有新的指控。由于每个协作机器人都使用相同的确定性算法，在指控图上计算最大匹配，因此每个协作机器人最终都会计算出相同的最大匹配，并得出相同的待阻止机器人列表。 □

如果假设 $G[t]$ 是 (F, n)-可泛洪的条件不成立，那么某些协作机器人可能无法收到某些指控。如果 $R_k[t]$ 最终未能在所有 k之间达成一致，那么即使全局范围内提出的指控数量已足以满足霍尔婚配条件，也可能无法阻止所有不协作机器人。不过，只要 k的本地指控图 $\mathcal{A}_k[t]$ 满足霍尔婚配条件，¯所有 $\mathcal{C}$ 最终都会被 k 阻止，但阻止列表中匹配到的协作机器人可能与其他阻止列表中的不同。

5 案例研究

我们在 ARGOS [Pinciroli 等人（2012）], 这一多物理场机器人模拟器中对 TurtleBot 进行仿真实验。该模拟器能够高效地模拟大规模机器人群。机器人配备了无线电，可向 4 米范围内的邻近机器人发送信息；还配备了全向摄像头，用于检测附近目标并避障，观测距离为 ≈ 0.9 米。机器人控制器以 30 Hz 运行。重现我们实验的源代码可在 https://github.com/gitsper/decentralized-blocklist-protocol 找到。

5.1 目标跟踪

应用概述。在群体目标跟踪中，机器人的目标是找到并协同跟踪一个最高速度为 d 的移动目标。在我们的实验设置中，目标是一台带有黄色灯光的机器人——距离目标 r 以内的机器人可以看到灯光，并对目标进行直接观测。为了让整个机器人群都能跟踪目标，即使那些无法直接观测到目标的机器人也能参与其中，机器人会广播包含以下内容的目标观测消息：

1. 观察者唯一标识符 2. 观测时间
3. 目标的观测位置

在每个时间步，机器人会按照观测时间对收到的观测消息进行排序，并选择最新的一条发送给邻居。机器人会跟踪某条观测消息已被发送的次数，并在发送固定的有限次数后停止共享该消息。多次发送同一条观测消息，旨在应对与邻近机器人之间时变的连接性。除应用消息外，还使用 DBP 来减轻拜占庭机器人的影响。机器人会删除来自被阻止的观测者标识符的观测消息，且不会转发这些消息。旧的观测消息会定期从本地缓存中删除。

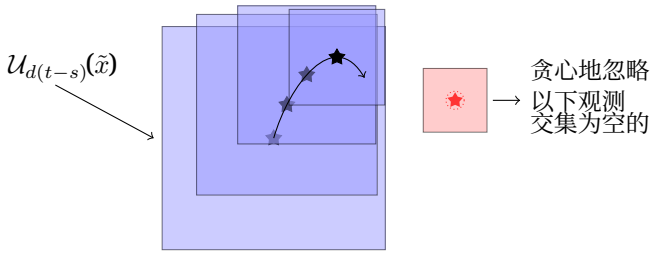

图2：基于观测的目标跟踪设置，可与 DBP 配合使用。未直接观测到目标的机器人会按接收观测的时间先后排序，并根据经过时间，为每条包含目标的观测计算一个包围盒。对这些包围盒应用集合交算子进行归约，可得出机器人对目标当前位置的信念。冲突观测（即导致交集为空的观测）会被丢弃，本轮迭代随之结束。

控制器。对于直接观测到目标的机器人，它们会计算一个从当前位置指向目标的航向向量，并朝目标移动。未直接观测到目标的机器人则依靠接收到的观测消息来计算其航向向量。我们用 $\mathcal{U}_d(c)$ 表示以 c 为中心、边长为 $2d$ 的闭正方形。给定一条时间为 s 且观测到目标位置为 $\tilde{x}$的观测消息，其隐含的信念是集合$\mathcal{U}_{d(t-s)}(\tilde{x})$在当前时刻 $t > s$包含目标。首先，接收到的观测消息按时间排序（s_1，$\tilde{x}_1$），（s_2，$\tilde{x}_2$）……，其中 $s_1 \geq s_2 \geq \cdots$。为计算航向向量，机器人会迭代地取交集

$$\mathcal{U}_{d(t-s_1)}(\tilde{x}_1) \cap \mathcal{U}_{d(t-s_2)}(\tilde{x}_2) \cap \cdots$$

如果在迭代过程中交集变为空集，则丢弃导致该情况的观测，并结束迭代。机器人将交集的中心视为其估计的目标位置，并用它计算航向向量。控制过程如图 2 所示。为简化集合交集的计算，这里使用包围盒而非圆。

指控规则。收到新的观测消息后，机器人会根据四条针对目标跟踪的指控规则发起 DBP 指控。给定机器人 j 在时间 s对 $\tilde{x}$ 进行的观测，令 $\Delta t = t - s$为经过时间，$\Delta p_i = \|p_i[t] - \tilde{x}\|$ 为从 i的位置 $p_i[t]$ 到观测目标的距离，c 为一个常数，表示消息在网络中传输速度的上限（在我们的实验设置中为 4 米/时间步）。当满足 $r + c\Delta t < \Delta p_i$时，触发第一条指控规则，因为这意味着观测必须以超出可能范围的速度在网络中传输。满足 $\Delta p_i < r - d\Delta t$ 且i 未直接观测到目标时，触发第二条指控规则——如果收到的观测属实，i 本应进行观测，却漏掉了。满足 $\Delta p_i > r + d\Delta t$ 但确实有 i进行了直接观测时，触发第三条指控规则；在这种情况下，目标不可能在收到观测的位置和 i 当前观测到它的位置之间移动得如此之快。最后一条指控规则用于检测单个观测者产生的振荡。如果 i过去收到过来自 j 的观测，就会考虑来自 j 的、关于 $\tilde{x}_{\text{old}}$ 且时间为 s_{old}的最近一次先前观测；若 $\|\tilde{x} - \tilde{x}_{\text{old}}\| > d\,(s - s_{\text{old}})$，则会指控 j。在这种情况下，j的观测从根本上与 x的最大变化率不一致。

实验设置。我们将基于 DBP 的拜占庭容错目标跟踪与最先进的 W-MSR 方法进行比较。除了无需预先知道需要容忍的拜占庭机器人数量，且网络连通性要求较低之外，我们的方法只需一台未受阻的协作机器人观测移动目标；而当目标移动时，W-MSR 需要 $F+1$ 台协作观察者来改变协作机器人之间的共识。我们模拟 $|\mathcal{C}| = 200$ 台和 $|\mathcal{C}| = 100$ 台机器人，以比较跟踪性能。拜占庭机器人可以发送内容任意的观测消息和指控。在我们的场景中，拜占庭机器人的行为是在环境中均匀散布，并持续广播虚假观测——每台拜占庭机器人都会选择一个距离自身 ~ 0.4米、沿远离原点方向的位置作为广播观测。这种拜占庭策略试图通过促使协作机器人向远离原点的方向分散来降低网络连通性，同时又不违反网络指控规则中的速度限制。

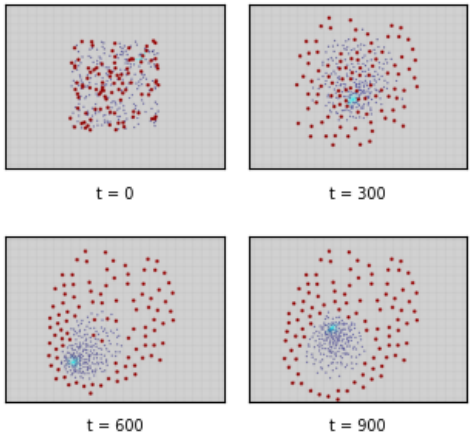

图 3：ARGOS 中基于 DBP 的目标跟踪视图。拜占庭机器人以红色圆形标出，目标的直接观测以青色显示。

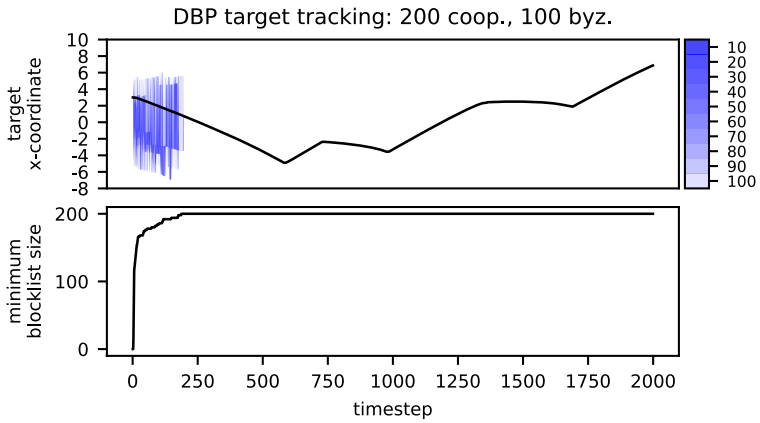

图 4：基于 DBP 的目标跟踪性能。上图中，黑色曲线表示移动目标的真实 x 坐标，蓝色阴影区域表示围绕中位数的信念范围（以百分位数表示）。下图绘制的是 $\min_i R_i^*[t]$，即最小封锁名单大小。在时间步 ~ 200，每个协作机器人都已将所有拜占庭机器人列入阻止列表；随着拜占庭节点的影响被消除，协作机器人几乎可以无误差地跟踪目标。

实验结果。图 4 使用分位数热图汇总了每个协作机器人对目标 x 坐标的信念。信念范围逐渐缩小，直到约 $t = 400$，此时所有拜占庭机器人都已被屏蔽，执行进入拜占庭影响全部消除的阶段。图 3 展示了在 ARGOS 仿真器中进行的 DBP 目标跟踪实验。基线 W-MSR 算法要求预先选定韧性参数 F。如果 F 选得太小，W-MSR 的理论保证

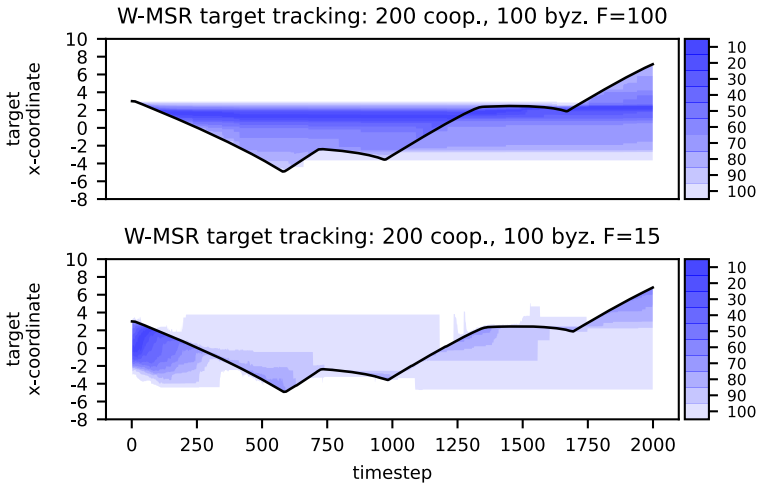

图 5：基于 W-MSR 的目标跟踪性能。当韧性参数为 $F = 100$ （上图）时，为了保证安全性，由于高连通性和同步的观察者要求，移动目标的信息无法在协作机器人之间传播。相比之下，$F = 15$ （下图）不保证安全性，但允许部分机器人成功跟踪目标。然而，拜占庭节点的影响始终无法消除。

就会失效，因此拜占庭机器人可能会破坏协作机器人的共识。具体而言，机器人群中拜占庭机器人密度较低的部分可能仍能成功跟踪目标，但拥有超过 F 个拜占庭邻居的协作机器人会受到攻击影响。每个受攻击影响的协作机器人都会反过来加剧攻击，因为其局部值会逐渐接近攻击者的值——图 5 底部的$F = 15 < |\mathcal{C}|$展示了这一情形。然而，W-MSR 无法扩展到较大的 F，因为机器人无法实现如此高的网络连通性，也无法拥有如此多的协作观察者。图 5 顶部的¯展示了大规模-F情形，其中有 $F = 100 = |\mathcal{C}|$。

5.2 时间同步

应用概述。对于此任务，机器人的目标是在环境中移动的同时，协作地将各自的本地时钟与通用参考时钟同步。一部分机器人被指定为锚点——这些机器人会定期对参考时钟时间进行高精度观测。与目标跟踪应用一样，锚点会广播包含以下内容的观测消息：

1. 观测者唯一标识符
2. 观测时间

在每个时间步，非锚点机器人按观测时间降序排列收到的观测消息，并选取最大值转发给邻居；同时使用 DBP 删除来自被屏蔽观测者的观测消息，并有选择地不转发这些消息。

控制器。在收到新观测消息的时间步，非锚点机器人只需将本地时钟设置为其观测消息列表中的最大观测时间，以此更新本地时钟。如果某个时间步内没有收到新观测消息，非锚点机器人 i的本地时钟会通过加上一个从分布 $1 + \mu_i + U[-0.05, 0.05]$中抽取的数值来更新，其中 $U[a, b]$ 是定义在 $[a, b]$ 上的均匀分布，而 μ_i 是在模拟开始时从 $U[-0.01, 0.01]$中抽取的。此更新行为旨在模拟未收到新观测消息时的随机游走时钟漂移。

指控规则。每当锚点机器人收到一条新的观测消息，如果观测时间大于锚点的本地时间，就会指控消息来源。该指控规则背后的直觉是，收到的观测时间与锚点本地时间之间的差值只能为负数——如果观测者是协作节点，那么该差值应对应于观测消息沿最短路径到达接收锚点所经过的跳数。如果差值为正数，则意味着观测者的本地时钟超前，这违反了协作锚点对参考时间进行高精度观测的假设。

实验设置。我们将基于 DBP 的拜占庭容错时间同步方法与最先进的、基于 W-MSR 的方法进行比较。我们模拟 $|\mathcal{C}| = 100$ （其中 50 个充当锚点，观测周期为 100 个时间步）和 $|\mathcal{C}| = 45$ 个机器人，以比较同步性能。拜占庭机器人可以发送任意观测消息，包括冒充锚点。实验中，拜占庭节点的行为与协作机器人相同，穿行于环境中，同时以与协作锚点相同的周期广播虚假的参考时钟观测。这些虚假观测等于真实参考时钟值加上$+1000$ 个时间步的攻击偏移量。这种拜占庭对手的选择旨在通过迫使非锚点采用过大的本地时钟值来破坏协作节点的时间同步；过小的值会被协作机器人忽略，因为每个非锚点总是将本地时钟设置为观测到的最大时钟值。

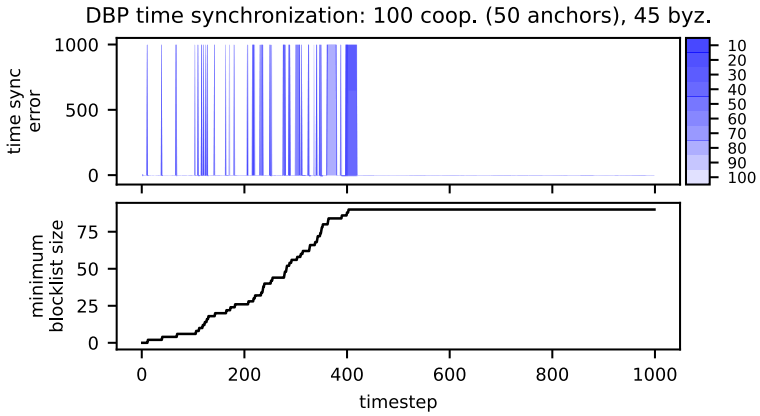

图6：基于 DBP 的时间同步性能。图中上方显示的是协作机器人的本地时钟相对于全局参考时钟的误差。每当拜占庭机器人发起攻击，误差就会飙升至攻击者的偏移量。时间步 ~ 400 之后，所有拜占庭节点均已被阻止，跟踪误差保持在正常水平。

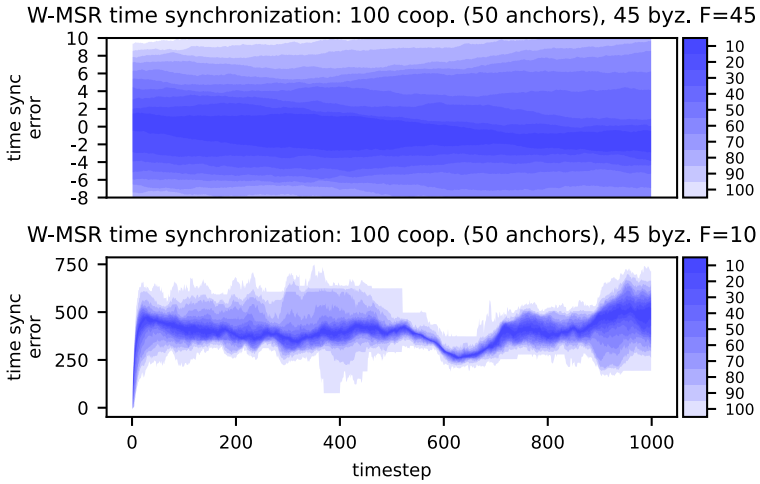

图7：基于 W-MSR 的时间同步性能。与目标跟踪案例研究一样，$F = |\mathcal{C}| = 45$可保证安全性，但相应的连通性要求会阻碍收敛。相反，较低的 $F = 10$ 则允许共识收敛，但代价是拜占庭节点能够对协作机器人的本地时钟值造成不利影响。

实验结果。图 6 展示了仿真过程中协作型非锚点机器人的时间同步误差（本地时间与参考时间之差）。我们观察到，拜占庭机器人能够通过发送虚假的参考时间观测值，将同步误差推至 $+1000$ 个时间步的攻击偏移量，直到时间步 ~ 400。此时，每个协作机器人都已屏蔽所有拜占庭机器人，攻击者的影响也被成功消除。与目标跟踪案例研究一样，W-MSR基线要求预先选择韧性参数 F。如果 F 选得太小，例如图 7 底部所示的 $F = 10$，那么

拜占庭机器人就会影响共识，协作机器人得到的本地时钟值会介于¯攻击偏移量与参考时间之间。如果 F 选得足够大，以抵御 $|\mathcal{C}| = 45$ 个攻击者，那么非锚点机器人所需的连通性和同时观测要求就过高，无法根据邻居的观测值更新本地¯时钟。图 7 顶部展示了大-F 取值范围的情况，其中 $F = 45 = |\mathcal{C}|$。

5.3 协作定位

应用概述。在协作定位任务中，机器人会在未知和／或动态环境中移动，并利用本地机器人间距离测量来估计其在全局坐标系中的位置。为便于完成此任务，部分机器人充当锚点，并定期对自身位置进行高精度观测（例如，作为静态预置锚点，或配备全球定位系统的移动机器人）。与目标跟踪和时间同步应用不同，非锚点机器人也会广播包含其定位信念的定位消息。定位消息包含：

- 发送方的唯一标识符
- 发送方的本地时间
- 发送者所信任的定位，以包围盒表示
- 锚点标志，当且仅当发送者是锚点时设为启用– 如果锚点标志未启用，则为最近收到的锚定位消息

非锚点机器人最初对自身定位没有任何信念。一旦形成定位信念（起初只有锚点机器人具备），非锚点机器人便开始定期向邻居广播定位消息。只有发送者是锚点时，锚点标志才会启用。除非非锚点发送的消息附带一条锚点标志已启用的定位消息，否则该消息将被忽略。

控制器。在收到定位消息的时间步，非锚点机器人会按照底层锚消息的时间对收到的定位消息排序（时间最近的排在最前），然后使用稳定排序，按照锚点标志排序（锚消息排在最前）。排序完成后，机器人遍历收到的定位消息，并对每条定位信念与经传输范围扩张后的区域求交集，c，再加上机器人每个时间步可移动的最大距离，d。如果遍历过程中交集变为空集，则丢弃最后一条定位消息并结束遍历。最终得到的交集即为表示机器人新定位信念的包围盒。在下一个时间步，机器人将发送其定位信念，并附带遍历过程中遇到的最近一条锚消息（这可能是来自锚点的直接传输，也可能是作为非锚点消息附件传来的锚消息）。该算法的运行过程如图 8 所示。DBP 用于删除并忽略来自被阻止发送者的消息。

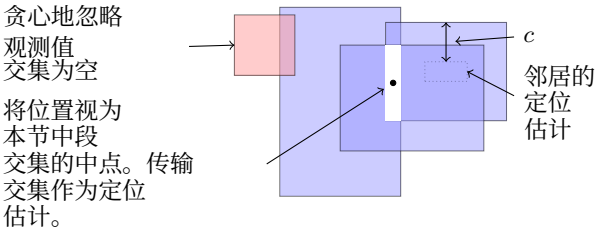

图8：与 DBP 配合使用的基于观测的协作定位设置。非锚点机器人根据从邻居处接收的定位估计来估算自身位置。估计范围按传输距离进行扩展，然后通过集合交算子缩小范围，以计算定位信念。定位估计按照其所依据的锚消息的时效排序，直接从锚点发送的估计具有优先权。

指控规则。收到的定位消息需接受两项指控规则的检验。第一项规则适用于锚机器人接收来自其他锚点的定位消息时，无论这些消息是直接收到的，还是作为非锚点定位消息的附件收到的。假设另一锚点 j 声称自己在时间 s位于 $\tilde{p}_j$，令 $\Delta t = t - s$ 表示经过时间，且$\Delta x_i = \|\tilde{p}_j - p_i\|$。若 $c\Delta t < \Delta x_i$，接收方锚点 i 就会指控 j；换言之，如果锚点 j的定位消息在网络中的传输速度快于物理上可能的速度，就会触发指控。第二项指控规则可由所有机器人（包括非锚机器人）提出。该规则指出，任何收到的非锚点定位消息与其附带的锚消息之间，都应满足第一项规则。如果机器人的能力更强，这些简单的指控规则还可以扩展。例如，如果机器人能够测量与发送方距离的下界，锚点便能够

在其他锚点的定位消息本应更早收到的情况下，提出类似的指控。

实验设置。在本案例研究中，无法将 W-MSR 算法选作基线，因为在小规模场景之外，协作定位并非通过线性共识问题来求解；在小规模场景中，每个机器人都能直接观测机器人群中的其他所有机器人。我们通过模拟 ¯来展示我们的方法，以此作为具备拜占庭容错能力的协作定位概念验证。我们模拟 $|\mathcal{C}| = 120$ （其中 80 个充当固定位置的锚点机器人）以及 $|\mathcal{C}| = 50$。拜占庭机器人试图干扰协作非锚点机器人的定位，它们通过获取自身真实位置，并给 x、y 坐标分别加上一个从 [-20,20]米范围内均匀采样的随机攻击偏移量，来发送虚假的锚点定位消息。虚假锚点消息会干扰非锚点机器人的定位消息迭代——由于虚假的锚点定位很可能与附近协作锚点发来的定位消息没有交集，因此会导致协作定位性能下降。

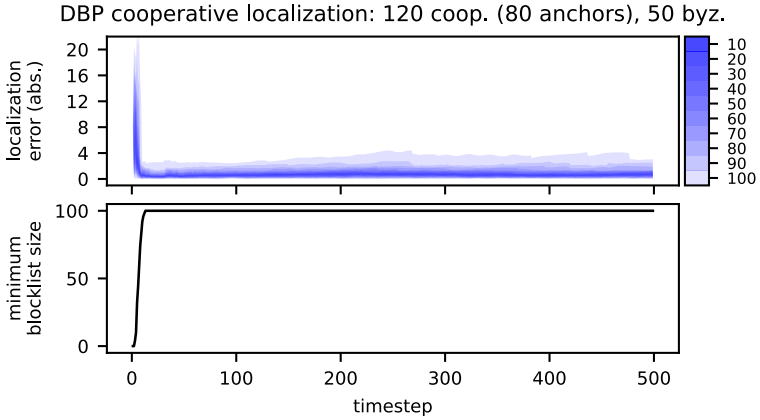

图 9：基于 DBP 的协作定位性能。上图展示了协作机器人对自身位置 x 坐标的估计绝对误差。下图展示了协作机器人阻止列表的最小大小——一旦所有拜占庭节点都被屏蔽，随着拜占庭节点的影响得到抑制，估计误差便恢复至正常值。

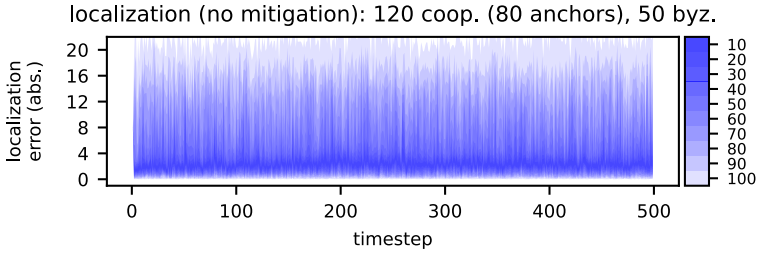

图 10：为支持我们关于 DBP 适用于此任务这一主张，我们展示了拜占庭机器人对协作定位可能造成的影响——拜占庭节点可能导致协作机器人的定位误差任意增大。

实验结果。在图 9 中，我们绘出了协作非锚点机器人在 x 坐标上的绝对误差，即它们认定的 x 坐标与真实值之间的绝对差值。我们观察到，尽管协作非锚点机器人最初的误差可能接近 ~ 20m 的攻击偏移量，但拜占庭机器人很快就会受到协作机器人的指控并被列入阻止列表。拜占庭机器人被阻止后，锚点定位共享算法便能为非锚点机器人提供低误差的协作定位。作为对比，我们还模拟了禁用 DBP 的相同场景，其 x 坐标绝对定位误差如图 10 所示。正如预期，拜占庭机器人会严重干扰定位，导致协作非锚点机器人的误差始终很大，最高可达攻击偏移量。

6 结论

本文提出了一种基于机器人间指控的去中心化阻止列表协议，旨在为多机器人系统提供拜占庭容错能力。我们证明，作为 W-MSR 算法的一种替代方案，我们的方法允许在提出指控期间暂时受到拜占庭影响，但与此同时，它会在检测到拜占庭机器人后作出适应，支持快速信息传播，并可应用于共识以外的领域。根据群体目标跟踪、时间同步和定位案例研究的实证结果，相较于 W-MSR，我们的方法在扩展到大型机器人群时更具实用性，因为它不要求每个协作机器人都拥有 $2F+1$ 个邻居，也不要求有 $F+1$ 名协作观察者才能传播信息。事实上，我们的方法只要求即使存在 F 个拜占庭机器人，消息仍能通过网络泛洪送达，并且来自单个协作机器人的观测结果也能迅速传播至整个机器人群。此外，我们首次证明了该方法能够为大规模去中心化协作定位问题提供拜占庭容错能力。在未来的工作中，我们希望将该方法扩展到指控并非总是可靠的系统，并探索能够优化发现和指控拜占庭机器人速度的群体算法。

参考文献

[Aditya 等人（2021）] USP Srinivas Aditya、Roshan Singh、Pranav Kumar Singh 和 Anshuman Kalla。2021年。《机器人领域的区块链综述：问题、机遇、挑战与未来方向》。《网络与计算机应用期刊》196（2021），103245。[Amirian 和 Shamaghdari（2021）] Neda Amirian 和 Saeed Shamaghdari。2021年。通过事件触发/自触发通信实现多智能体系统的分布式弹性集群控制。《*IET*控制理论与应用》15，4（2021），559–569。https://doi.org/10.1049/cth2.12061 电子版：https://onlinelibrary.wiley.com/doi/pdf/10.1049/cth2.12061。[Arrichiello 等人（2015）] Filippo Arrichiello、Alessandro Marino 和 Francesco Pierri。2015年。网络化多机器人系统中基于观测者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。出版方：IEEE。[Ashkenazi 等人（2019）] Yotam Ashkenazi、Shlomi Dolev、Sayaka Kamei、Fukuhito Ooshita 和 Koichi Wada。2019年。宽恕与遗忘：面对拜占庭机器人的自稳定群体。载于《*2019*年第七届计算与联网国际研讨会研讨会论文集（*CANDARW*）》。188–194。https://doi.org/10.1109/CANDARW.2019.00041[Bijani and Robertson（2014）] Shahriar Bijani 和 David Robertson。2014年。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。出版方：Springer。[Cheng 等人（2021）] Mingxi Cheng、Chenzhong Yin、Junyao Zhang、Shahin Nazarian、Jyotirmoy Deshmukh 和 Paul Bogdan。2021年。多智能体系统通用信任框架。载于《第*20*届自主智能体与多智能体系统国际会议论文集》。332–340。[Djouadi 等人（2015）] Seddik M Djouadi、Alexander M Melin、Erik M Ferragut、Jason A Laska、Jin Dong 和 Anis Drira。2015年。信息物理系统中的有限能量攻击与有界执行器攻击。载于《*2015*年欧洲控制会议（*ECC*）》。IEEE，3659–3664。[Edmonds（1965）] Jack Edmonds。1965年。路径、树与花。《加拿大数学杂志》17（1965），449–467。[Fagiolini 等人（2008）] Adriano Fagiolini、Marco Pellinacci、Gianni Valenti、Gianluca Dini 和 Antonio Bicchi。2008年。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*机器人与自动化国际会议》。120–127。https://doi.org/10.1109/ROBOT.2008.4543196 ISSN：1050-4729。[Fagiolini 等人（2007）] Adriano Fagiolini、Gianni Valenti、Lucia Pallottino、Gianluca Dini 和 Antonio Bicchi。2007年。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。[Gielis 等人（2022）] Jennifer Gielis、Ajay Shankar 和 Amanda Prorok。2022年。多机器人系统通信：批判性综述。《机器人学最新报告》（2022年8月）。https://doi.org/10.1007/s43154-022-00090-9[Gil 等人（2017）] Stephanie Gil、Swarun Kumar、Mark Mazumder、Dina Katabi 和 Daniela Rus。2017年。保障抗欺骗多机器人网络。《自主机器人》41，6（2017），1383–1400。出版方：Springer。

[Guerrero-Bonilla 等人（2017）] Luis Guerrero-Bonilla、Amanda Prorok 和 Vijay Kumar。2017年。弹性机器人团队编队。《IEEE机器人与自动化快报》2，2（2017年4月），841–848。https://doi.org/10.1109/LRA.2017.2654550 会议名称：IEEE机器人与自动化快报。[Guo 等人（2018）] Pinyao Guo、Hunmin Kim、Nurali Virani、Jun Xu、Minghui Zhu 和 Peng Liu。2018年。RoboADS：针对移动机器人传感器与执行器异常行为的异常检测。载于《2018年第48届IEEE/IFIP年度可靠系统与网络国际会议（DSN）》。IEEE，574–585。[LeBlanc 等人（2013）] Heath J. LeBlanc、Haotian Zhang、Xenofon Koutsoukos 和 Shreyas Sundaram。2013年。鲁棒网络中的弹性渐近共识。《IEEE通信领域精选期刊》31，4（2013年4月），766–781。https://doi.org/10.1109/JSAC.2013.130413 会议名称：IEEE通信领域精选期刊。[Liu 等人（2021）] Jun Liu、Lifeng Zhou、Pratap Tokekar 和 Ryan K. Williams。2021年。在对抗环境中进行分布式弹性次模动作选择。《IEEE机器人与自动化快报》6，3（2021年7月），5832–5839。https://doi.org/10.1109/LRA.2021.3080629 arXiv：2105.07305。[Mallmann-Trenn 等人（2021）] Frederik Mallmann-Trenn、Matthew Cavorsi 和 Stephanie Gil。2021年。群体验证：通过协作排斥对手，并将其应用于多机器人集群。《IEEE机器人学汇刊》（2021），1–20。https://doi.org/10.1109/TRO.2021.3089033 会议名称：IEEE机器人学汇刊。[Mitra 等人（2019）] Aritra Mitra、John A. Richards、Saurabh Bagchi 和 Shreyas Sundaram。2019年。移动智能体的弹性分布式状态估计：克服拜占庭对手、通信丢失和间歇测量。《自主机器人》43，3（2019年3月），743–768。https://doi.org/10.1007/s10514-018-9813-7[Pacheco 等人（2020）] Alexandre Pacheco、Volker Strobel 和 Marco Dorigo。2020年。通过自组织网络通信的区块链控制物理机器人群。载于《群体智能国际会议》。Springer，3–15。[Pierson 和 Schwager（2016）] Alyssa Pierson 和 Mac Schwager。2016年。用于鲁棒多机器人传感器覆盖的自适应机器人间信任。载于《机器人学研究》，Masayuki Inaba 和 Peter Corke（编）。第114卷。Springer国际出版公司，Cham，167–183。https://doi.org/10.1007/978-3-319-28872-7_10 丛书名称：Springer高级机器人学丛书。[Pinciroli 等人（2012）] Carlo Pinciroli、Vito Trianni、Rehan O'Grady、Giovanni Pini、Arne Brutschy、Manuele Brambilla、Nithin Mathews、Eliseo Ferrante、Gianni Di Caro、Frederick Ducatelle、Mauro Birattari、Luca Maria Gambardella 和 Marco Dorigo。2012年。ARGoS：面向多机器人系统的模块化并行多引擎模拟器。《群体智能》6，4（2012），271–295。[Renganathan 和 Summers（2017）] Venkatraman Renganathan 和 Tyler Summers。2017年。分布式多机器人系统的抗欺骗协调。载于《2017年多机器人与多智能体系统国际研讨会（MRS）》。IEEE，135–141。[Salda˜na 等人（2017）] David Salda˜na、Amanda Prorok、Shreyas Sundaram、Mario F. M. Campos 和 Vijay Kumar。2017年。时变网络中动态智能体的弹性共识。载于《2017年美国控制会议（ACC）》。252–258。https://doi.org/10.23919/ACC.2017.7962962 ISSN：2378-5861。[Saulnier 等人（2017）] Kelsey Saulnier、David Salda˜na、Amanda Prorok、George J. Pappas 和 Vijay Kumar。2017年。移动机器人团队的弹性集群。《IEEE机器人与自动化快报》2，2（2017年4月），1039–1046。https://doi.org/10.1109/LRA.2017.2655142 会议名称：IEEE机器人与自动化快报。[Shoukry 等人（2018）] Yasser Shoukry、Shaunak Mishra、Zutian Luo 和 Suhas Diggavi。2018年。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年第9届ACM/IEEE网络物理系统国际会议（ICCPS）》。IEEE，43–54。[Strobel 等人（2018）] Volker Strobel、Eduardo Castell´o Ferrer 和 Marco Dorigo。2018年。在群体机器人集体决策场景中通过区块链技术管理拜占庭机器人。载于《第17届自主智能体与多智能体系统国际会议论文集》（瑞典斯德哥尔摩）（AAMAS '18）。自主智能体与多智能体系统国际基金会，美国南卡罗来纳州里奇兰，541–549。[Verma 和 Ranga（2021）] Janardan Kumar Verma 和 Virender Ranga。2021年。多机器人协调分析、分类体系、挑战与未来展望。《智能与机器人系统期刊》102，1（2021年5月），10。https://doi.org/10.1007/s10846-021-01378-2[Weber 等人（2020）] Matthew Weber、Baihong Jin、Gil Lederman、Yasser Shoukry、Edward A. Lee、Sanjit Seshia 和 Alberto Sangiovanni-Vincentelli。2020年。Gordian：用于安全防护的基于形式化推理的离群点检测

定位。《*ACM*网络物理系统汇刊》4, 4（2020年8月），1–27。https://doi.org/10. 1145/3386568[Yaacoub 等人（2022年）] Jean-Paul A. Yaacoub、Hassan N. Noura、Ola Salman 和 Ali Chehab。2022年。机器人网络安全：漏洞、攻击、对策与建议。《国际信息安全杂志》21, 1（2022年2月），115–158。https://doi.org/10.1007/s10207-021-00545-8[Zhou and Tokekar（2021年）] Lifeng Zhou 和 Pratap Tokekar。2021年。不确定且对抗性环境中的多机器人协调与规划。《机器人学最新报告》2, 2（2021年6月），147–157。https: //doi.org/10.1007/s43154-021-00046-5 arXiv: 2105.00389。[Zhou 等人（2020）] Lifeng Zhou、Vasileios Tzoumas、George J. Pappas 和 Pratap Tokekar。2020年。面向多机器人规划的分布式抗攻击次模最大化。载于*2020*年 *IEEE*机器人与自动化国际会议（*ICRA*）。2479–2485。https://doi.org/10.1109/ICRA40945.2020.9197243 ISSN: 2577-087X。