**隐私保护数据库辅助工业物联网频谱接入：分布式学习方法**

|  |  |
| --- | --- |
| **摘要——在智能工业环境部署中，工业物联网（IIoT）展示了其巨大的价值。随着工业物联网的蓬勃发展，动态频谱共享应运而生，并被视为工业物联网光谱存储有发展前景的解决方案。与此同时，网络物理安全仍然是工业物联网系统可靠运行的最大焦点。在本文中，我们将思考在基于接收信号强度（RSS）之敌对位置攻击下的工业物联网动态频谱接入。我们使用实用有效的功率微扰降低工业物联网设备面临的本地化威胁，并将隐私保护频谱共享当作随机信道选择博弈。为实现功率微扰的随机性，我们开发了一种双时标分布式学习算法。该算法几乎必定能够汇聚该博弈的相关均衡集合。数值结果表现出了算法收敛性，并证实双时标学习过程有效地降低了功率微扰带来的网络吞吐量。**  **索引词——频谱接入、ICPS安全、分布式算法、博弈理论。**  **1. 简介** | 图1：无人地面派送系统遭受基于接收信号强度（RSS）之敌对位置攻击的示意图。该系统有由两家公司（以不同颜色表示）的机器人车辆组成。d1、d2、d3分别为在三个不同位置测得RSS预测距离，将通过三边测量法对目标进行定位。  近年来，无线通讯、工业控制、人工智能及大数据等技术进步，推动了现代工业环境的创新。在下一代网络物理系统（CPS）[2]的支持下，工业物联网（IIoT）已成为智能电网、智能工厂、智能物流管理和智能运输系统等智能工业应用的重要组成部分[3]。在这些运用中，相互连接的物联网设备不断地将实时工业数据发送至工业物联网网关，后者又将数据传送至云/雾服务器进行后续处理和分析[4]。  随着工业物联网设备规模的扩大，产生的大量工业数据对带宽资源提出了更多的要求，使得工业频谱管理面临重大挑战。为解决频谱短缺的问题，人们引进了数据库辅助频谱接入，由地理位置数据库告知工业物联网动态的可用频谱，使其随机进入空闲的许可信道[5][6]。动态频谱接入面临的关键挑战仍然是如何分布式地协调频谱共享，以有效地降低进入相同空闲信道的设备之间的互相干扰[6]。为实现这一目的，采用了博弈理论模型来解决动态频谱进行问题。在该模型中，将设备视为自私的博弈者，它们通过有策略地做出进入信道的决定，实现回报的最大化[7]。 |

1 例如，通过RF指纹技术[29]，接收者可通过分析信号模拟部件的瑕疵来识别无线卡。

2 在全文中，我们使用的术语“用户”和“博弈者”可以相互替换。

3 在相同组内，两个用户之间的信息交流，可以通过共同的控制信道来实现。

|  |  |
| --- | --- |
| 除频谱紧缺外，网络物理安全仍然是工业物联网可靠运行的另一挑战。作为工业网络物理系统的主要组成部分，工业物联网综合了控制、联网和计算部件，为安全及敏感数据的产生、收集和交换提供了基本支持。由于其至关重要性，工业物联网成为网络物理攻击的有吸引力的重要目标[8]。尽管在网络攻击和相关防御方面已有大量的研究，对工业物联网之物理层面攻击的关注却相对较少。作为主要弱点，物联网设备的地理位置信息一旦受到泄漏，将致使设备面临极大危险，极其危险工业物联网的可靠性和安全性。  在本文中，我们考虑了一种实用的基于接收信号强度（RSS）的敌对位置攻击，该攻击在精确定位无线物联网设备方面十分有效[9]。如图1所示，在获得攻击对象附近范围内若干RSS测量距离的情况下，对手可以十分容易地使用现有的三边测量法进行定位攻击[10]。与使用其他物理层信息（例如，到达时间（TOA）、到达时间差（TDOA）和到达角度（AOA）[11]）的定位方法相比，基于RSS的定位既不需要复杂的硬件，也不需要与攻击对象的主动通信，而对手却可以在实践中十分容易地实施。  在降低物理层面定位攻击方面，人们努力采取了各种应对措施，例如，使用定向天线限制传输范围[12]，以及通过设备层面的合作创建虚拟位置以迷惑对手等[13]。但是，这些方法的成本可能很高，且很难广泛用于系统部署，原因是物联网设备通常尺寸较小，计算及能源资源有限。因此，我们考虑使用轻质的功率微扰方法应对基于RSS的位置攻击[14]。背后的思想是，对物联网设备的传输功率级增添随机噪音，旨为有效地降低对手定位的准确性[15]。  尽管具有实用性和有效性，随机功率微扰法也造成物联网设备干扰评估的不准确性，从而不可避免地导致频谱共享系统的性能退化（例如，吞吐量减少）。出于该动机，本研究的目的是为工业物联网开发一个有效的频谱共享方案，通过传输功率微扰同时保护设备的位置隐私。  接下来[16]，我们将隐私保护频谱接入问题表达为随机博弈，物联网设备动态地更新其信道选择，以实现其使用的最大化，见第III-A节详述。我们基于相关均衡（CE）的表征分析博弈的动态。特别地，我们考虑了相关均衡，即纳什均衡的一般化，允许博弈者之间的依赖关系，且易于修订，实现分布式实现[17]。 | 为实现在随机功率微扰的影响下，取得信道选择博弈的相关均衡，在本研究中，我们设计了一种双时标分布式学习算法。特别地，在较慢的时标，各物联网设备会根据*经修订反悔规则*[18]利用本地维持的估计效用改变其信道选择策略。在较快的时标，通过学习过程保持更新估计效用，以实现功率微拢的随机性，并方便了在较慢时标上更有效的策略学习。我们发现，在温和条件下，在学习时标上，用户联合行动的经验频率构成一个相关均衡集合。仿真结果显示，在随机功率微扰下，我们的双时标学习算法胜于仅涉及信道选择之策略适应的单时标学习算法。这证实，所提议的双时标学习算法有助于实现系统吞吐量和位置隐私之间的平衡。  我们的贡献总结如下：   * 我们识别了数据库辅助频谱接入中针对物联网设备的基于RSS之敌对位置攻击的问题，并考虑了采用轻质功率微扰方法降低定位的精确性。 * 我们通过建立隐私保护信道选择博弈模型，共同研究了动态频谱接入和位置隐私保护。在该博弈中，物联网设备使用扰动传输功率级并有策略地做出信道选择，以使用效用的最大化。 * 我们提出了基于反悔学习规则的双时标学习算法。该算法微弱地汇集了相关均衡的集合，且在降低随机功率微扰引起的系统吞吐量退化方面，它胜于单一时标学习方法。   本文的余下内容安排如下。我们首先在第II节讨论了相关的工作。在第III节，我们描述了隐私保护频谱共享方案的系统模型。在第IV节，我们呈现了对策论的问题公式化，并引进了无反悔学习规则。在第V节，我们为隐私保护频谱共享提议了一种双时标学习算法。在第VI节，我们评估了所提议算法的有效性和效果。在第VII节，我们得出了本文的结论。  II. 相关的工作  频谱管理技术已被广泛用于智能工业物联网设计，以满足数据通信的高QoS要求，这有助于建立传感器、致动器和系统之间的强大相互联系。例如，Cao等[19]利用线性状态动力学探索了多信道的随机接入，以增强网络物理系统的状态估计性能。在[20]中，Chiwewe等就基于认知无线电工业无线传感器网络中的频谱管理，概述了各种不同技术，并为频谱共享方案探索了对策论模型的应用。 |

|  |  |
| --- | --- |
| 沿着不同的路径，工业网络物理安全问题最近引起了工业界和学术界的极大关注，都在努力聚焦针对工业网络物理系统的网络攻击。在[21]，作者提出了一个网络物理系统安全框架，该框架可区分CPS系统中的网络、网络物理和物理部件。另外，作者还调查了潜在及报告的攻击，以及现有解决方案。特别地，在[21]，作者聚焦了智能电网系统中智能电表的数据隐私弱点，并充分探讨了最前沿的缓解方案。在[23]，作者探讨了智能医疗保健及运输系统等新兴城市应用内的安全与隐私挑战。  相比之下，本研究中考虑的敌对位置攻击是一种通常以无线传感器网络为目标的典型物理层面攻击[14]。对应对此等威胁，一个主要的方法是使传输信号的信息模糊化，因为对手可能利用该传输信号推测用户的位置。在[14]和[15]，设计了移动设备，以有策略地减少可联合实施基于RSS位置攻击的对手数量，或降低对手定位的精确度。在[24]，Wang等聚焦了定向天线的设计，以解决物理层面位置隐私的攻击。在[25]，Gao等考虑了在与我们相似的认知无线电网络中的位置隐私保护。但是，他们考虑的不是基于RSS的攻击，而是可以通过用户所用信道推测其二次用户位置的攻击模型。对于该威胁，缓解方案是选择支持最稳定信道的信道。  与多数现有工程不同，在本文中，我们共同考虑了频谱管理和位置隐私保护。双时标学习算法的提出受到了[26]的启发，后者使用强化学习算法研究去中心化小细胞网络中的干扰缓解问题。与我们最相关的工作可能是[1]，它使用对策模型调查了社会感知动态频谱接入情景下的位置隐私保护。在本研究中，我们考虑了一种不同的均衡标准（例如，相关均衡），它通过放宽对博弈者信道选择策略的独立性假设，对[1]中考虑的纳什均衡进行一般化。此外，物联网设备设计的策略是遵循反悔规则，而遵循非[1]中使用的随机虚构对策动态。  **III. 位置隐私保护频谱共享的系统模型**  **A. 基本设置**  根据FCC[28]的新近规定，在数据库辅助频谱接入，各空白空间用户将首先向数据库发送频谱接入请求，数据库将告知该用户某特定位置的空闲TV信道。我们考虑某频谱接入网络拥有主信道（例如，TV信道）集体A={1，2，……，M}。另外，次用户（例如，物联网设备）集合V={1，2，……N}的用户在信道未被许可用户占用时试图接入此等信道。特别地，各用户可以接入数据库显示的可用信道子 | 集合，显然，在次用户之间缺乏适当协调的情况下，信道使用可能会发生冲突，且产生的干扰可能严重降低网络性能。  相应地，数据库辅助频谱接入归根性结底是，在随时间变化的信道占用及干扰环境下，次用户之间的动态信道分配协调。为获取物联网设备之间的物理耦合，我们假设了一个物理干扰模型。特别地，我们用表示用户已接入的信道，并在其通信链接上将信道表示为。然后，我们以表示用户与用户n之间干扰链路上信道增益。用户n链路上信道的噪音表示为。用户n的信号噪声干扰比（SINR）可表示为：    其中，为用户n使用的传输功率；当用户m和用户n接入相同的信道（例如，）时，指示函数等于1，否则，等于0。我们以W表示带宽，并将用户n的个体效用定义为功率水平为时的吞吐量，    我们也假设全部物联网设备均可根据功能或所有权归为不同组。在图1所示的无人交付系统的例子中，无人驾驶车辆的群内关系以不同颜色表示。对于各个用户，我们以表示与用户n同组的其他用户集合，并将其组的效用定义为其个体效用加其组邻居的效用总合，并使用加权系数，例如，    我们使用此等组效用模型来获取相同组内同类物联网设备之间的基本社会耦合。直观地，值越大，设备n与相关组之间的社会联系越大。  **B. 针对基于RSS位置隐私攻击的随机功率微扰**  *1）基于RSS位置隐私攻击：*在本研究中，我们考虑了一种PHY层敌对模型，该模型使用基于接收信号强度（RSS）定位技术来攻击用户的位置隐私。基于RSS的位置捕获传输的信号，并根据信号传播模型[14]、[15]建立距离与RSS之间的映射。如图1所示，各对手可以收集来自目标用户之传输信号的RSS水平的序列，并使用最大似然估计获得估计的距离[30]。然后，利用估计距离及对手对应物理位置的集合，通过三边测量法共同确定目标用户的合适位置。 |

|  |  |
| --- | --- |
| *2）随机功率微扰：*为应对基于RSS的位置隐私攻击，我们使用了一种本地随机功率微扰方法，旨为将不确定性引入对手的定位结果[15]。为实现这一目的，允许各用户故意动态且随机地改变其传输功率水平。在对手那里，获得的RSS噪声测量可能有效地放大目标用户位置的不确定位置，从而降低定位的精确度。  为避免对主用户产生额外的干扰，我们将随机功率微扰部件限制为负偏压。特别地，用户n的微扰传输功率由确定，即常规传输功率水平和微扰项的总和，并产生以下单侧截断指数分布，其pdf如下：    其中，表示最大微扰水平。如果超出该水平，则对于正常的数据传输，物联网设备的SINR可能不可接受。参数描绘了用户指定的“期望”功率微扰水平，在第VI节中，我们将进一步讨论。  **IV. 隐私保护频谱共享**  在本节，我们将频谱共享问题当作一个随机信道选择博弈，并引入无反悔规则。该规则能够分布式地计算出非合作博弈中的相关均衡。  **A. 频谱共享的随机信道选择博弈**  在我们的研究中，我们建立了一场随机信道选择博弈。在该博弈中，物联网用户为自私的博弈者，并有策略地不断地与其他博奕者相互发生作用，旨为在长远上实现其预期组效用的最大化2。各博奕者的行动空间是用户n能够接入的可用信道的集合。我们用表示全部用户的共同频谱接入档案，其中，。为方便评估各用户的预期组效用，我们以表示用户n的混合策略空间，以表示用记n的混合策略，且的概率分布表示选择信道的概率。因此，全部博弈者的联合混合策略为，除用户n之外的博奕者的联合策略可按照惯例表示为 | 。我们继续以表示所采取的联合行动的概率。  总而言之，我们将隐私保护频谱共享问题当作一场非合作博弈，并以三元组表示。在我们的研究中，考虑的均衡标准是相关均衡。它通过允许博弈者策略相互依赖，对纳什均衡予以概括。从数学角度，相关均衡是凸多胞形，其极端点与纳什均衡集合相对应。因此，一般来讲，相比纳什均衡，在相关均衡下能够取得更好的整体性能。相关均衡的正式定义如下：  **定义1**（相关均衡）。*的概率分布是博弈的相关均衡（CE）。如果则预期组效用满足以下条件：*    **评注。**为切实理解相关均衡，可以将视为受信任频谱数据库提供的策略建议。在隐含假定其他用户的策略均遵守该建议的情况下，遵守该建议最符合各用户的利益。换句话说，如果某用户独立偏离CE，则无法取得更好的预期组效用。  **定理。***（CE的存在）在随机信道选择博弈中，至少存在一个CE。*  由于我们的信道选择博弈由有限的博弈者集合和行动集合组成，因此，它属于有限博弈，并确定拥有非空的相关均衡[17]。  **B. 无反悔匹配规则**  在本节，我们简要介绍了用于分布式搜索非合作博弈之相关均衡的无反悔匹配规则[27]。按照这样的规则，使用反悔测量对博弈者行为调整之损益予以量化。关键的思路是让各用户从各特定行动中学习反悔，以随着时间推移最大程度降低平均反悔。  特别地，对于各用户，假设其对手的行动为，则在时间t之前，当前行动下的平均组效用与任何其他行动下的平均组效用之间的差异可计算为： |

|  |  |
| --- | --- |
| 其中，第二个术语是对时间t之前用户n感知的平均组效用的量化；而第一个术语表示当做出行动时，假定该用户每次均选择时能够取得的平均效用。那么，用户n对在先前博弈中选择行动而非的“反悔”，可表示为=。直觉地，用户n会反悔其他行动是否会为其带来更高的效用。  基于在时间t的反悔测量，用户n根据以下概率策略改进其行动：    在这里，变更至替换行动与相应反悔测量相成比例。参数选择较大值，以保证在当前选择的信道始终有剩余的实证概率。较高的值降低了切换至其他信道的概率，因此，可视为“惯性”参数。然后，随用户在时间步t+1更新其反悔测量，推进算法。对于各联合行动，我们以表示时隙t产生的经验分布，表达如下：    众所周知，对于非合作博弈，当博弈者根据无反悔匹配规则更新策略时，经验分布汇聚（概率1）为相关均衡的集合，其中，[27]。  有两个挑战阻碍了我们直接使用无反悔规则解决我们的随机信道选择博弈。首先，由于使用随机功率微扰程序，各用户的组效用受到随机噪声的干扰，并不可避免地导致不准确的“反悔”测量及该博弈可能有问题的相关均衡。  而且，根据（6），要计算未能选择信道产生的反悔，用户n需要每次评估在时间步采取行动时， 的潜在可感知的组效用。这不并可行，因为用户n并不拥有其他用户个人效用函数及其选择的信道的全局信息。  为解决这两大挑战，在下一节，我们设计了一个双时标学习算法。用户可以通过该算法“更快地”学习其嘈杂的组效用，并与此同时，根据“更慢”学习过程中的的以下经修订基于反悔原则的适用其信道选择策略。  **V. 隐私保护频谱共享之发布式基于反悔的学习**  在本节，我们引入了双时标分布式算法，以发现我们信道选择博弈中的相关均衡，并提供温和条件下长期弱收敛的理论分析。 | **A. 双时标基于反悔的学习算法**  如算法1所概述，学习算法包含“更快”和“更慢”学习过程。特别地，在更快的时标，在各时间步嘈杂效用情况下，各用户不断更新与各可用信道对应的预期组效用。在校准至维持的预期组效用的同时，各用户在“更慢”的时标，通过遵循基于反悔的学习规则变更其策略。接下来，我们将分别进一步详述“更快”和“更慢”学习过程。  1）更快时标上的效用学习：在“更快”学习过程，用户n维持一个矢量=，各因素表示在时间步t采取行动时的预期组效用。随着时间的推移，预期的组效用更新如下：    其中，表示学习速率。特别地，对于各用户n，是通过第一次测量其收到的干扰并查询各用户收到的而取得，再根据（3）进行合计。注意，在各迭代t，只有矢量的元素得到实际更新。通过这种递归效用学习过程，用户n能够渐进地形成对预期组效用的精确评估，确保了较慢时标上策略学习能够最终达到CE集合。  **算法1** 双时标分布式学习算法  1. **初始化**：对于各用户n，  2. 初始化及反悔测量。  3. 随机选择一个信道，初始概率为。  4. 设置学习速率和；设置参数。  5. **初始化结束**  6. 各平行用户**循环**。  7. “更快”学习过程：  8. 测量收到的干扰，并按照（2）计算个人的吞土量。  9. 查询邻居的个体效用，并按照（3）计算即时的组效用。  10. 按照（9）更新预期效用的预测。  11. “更慢”学习过程：  12. 根据（11）计算即时反悔，并根据（10）计算反悔测量。  13. 根据（12）更新信道选择策略，并基于随机选择一个信道。  14. 。  15. **结束循环** |

|  |  |
| --- | --- |
| *2）更慢时标上的策略适应：*在更慢时标，我们实施了一个经修正的基于反悔的学习程序。该程序系基于第IV-B节所述标准无反悔规则而开发的。  尤其是，各用户n按照以下公式递归地更新各替换行动和当前行动之间的平均组效用差异：    其中，定义为在时间t采取行动而非行动的即时反悔。学习速率决定了基于反悔的策略学习的时标，且该速率应当根据设置，以保证收敛至CE，见详下文讨论。注意，（10）对（6）进行一般化，并可归纳为（6），学习速率设为1/t。  如上节所述，在时间t采取替换行动时，如果不知道其他用户的行动和基个体效用函数，则很难计算可感知效用。因此，我们求助于经修订的无反悔匹配规则[18]，并以估计项替代明确的可感知效用。其中，和为选择考虑中两行动的概率。尤其是，用户n根据以下公式计算其在时间t时的即时反悔：    然后，我们再次将采取行动而非行动的“反悔”测量定义为= 。简单地说，反悔测量定义了和之间平均组效用的差异。然后，使用权重使即时组效用正常化，使括号内的两项可以相比较。  通过反悔测量，各用户按照以下更新其策略：    其中，，表示用户组效用的上界。由于是无限的，要确保，我们采用加权反悔项和的最小值。在策略得到更新的情况下，各用户调整信道选择，并在下一时间步更新其反馈测量。  注意，通过引入参数，策略更新规则（12）使开发和利用达到权衡。在一方面，导致更大“反悔”的替换行动被选中的可能性更大，这可视为寻求更加策略的利用过程。在另一方面，各替换行动被选中的概率至少为，使策略开发有了可能。结果是，可以足够多次地访问各 | 用户N  更慢策略适应公式（10）（11）（12）  更快效用学习公式（9）  用户1  环境  图2：在时间t效用学习（在更快时标上）和策略适应（在更慢时标上）的耦合  个行动，而这是策略适应和效用学习收敛的必要条件。按照标准，我们设置了一个逐渐减少的权得（其中，），以确保策略适应的收敛。出于澄清目的，我们使用图2来说明任一时间步t两个学习过程的耦合。简单地说，在提议的基于反悔的双时标学习算法中，用户在更变策略并造成信道选择的更大反悔的同时，同步地学习其长期组效用。在各个迭代，各用户使用其维持的平均反悔矩阵，计算即时反悔测量，导致计算复杂性。接下来，我们将评估我们所提议学习算法的收敛性能。  **B. 收敛性分析**  在本节，我们分析算法1的收敛行为。我们利用标准随机逼近理论的双时标扩展来展示博弈至相关均衡集合的弱收敛。思路是，让效用学习和基于反悔的策略适应以不同的步长计划同时进行，使基于反悔的策略学习在较慢但有效的时标上进行，并将效用学习看作准静态。我们的主要结果见以下定理。  **假设1。**对于各用户，均满足条件C1-C3：    **定理2。***（算法1的收敛）让作为经验分布，定义见（8）。当满足（10）中的和假设1时，算法1几乎确定地收敛至博弈的CE 集合，其中，= 。尤其是，我们有，* |

|  |  |
| --- | --- |
| 和    其中，为用户n采取行动而其他人策略为时的预期组效用。  本证明的主要思路是，先引入离散学习过程（9）和（10）的持续时间插值过程。该离散学习过程视为半流的渐进假轨道，并与两个学习动态所定义的微分包含相对应[13]。因此，可以通过微分包含研究序列和的极限行为。通过结合异步随机逼近框架[32]，在假设1的情况下，我们可以获取同时进行的两个学习过程的渐进弱收敛。由于缺乏篇幅有限，我们将详细的证明附于线上附录[33]。  **VI. 性能评估**  在本节，我们评估为隐私保护频谱共享而提议的双时标分布式学习算法的性能。  **A. 模拟设定**  我们考虑了一个数据库辅助频谱接入网络。该网络N=80台物联网设备，且随机散布在1km X 1km的正方形区域内，并拟相同概率归为两个分组中的任意一组。对于各次用户n，我们将受微扰前的传微功率设为，将可用的信道设为，其中，默认。我们考虑了一个瑞雷衰落通道环境。用户n和m之间的信道增益与其物理距离成反比例，路径损耗因子。对于使用信道的各用户n，基背景干扰功率统一分配至[-100，-90]dBm的间距中。无论任一分组，其各个用户的权得因子均以均匀分布产生，其中默认。  在我们的实验中，我们让每个用户随机微扰其传输功率水平，以应对基于RSS的位置攻击（见第III-B的介绍）。其中，各用户的隐私保护水平按照功率微扰的期望值予以量化。根据（4），我们能够将功率微扰项的期望值表达式导出为。其中，。我们默认设定，，以使得微扰水平约为-6mW。对于双时标学习算法，我们在算法1中设学习速率为，。超级参数值则通过调整确定，使之满足C1-C3的条件。此外，我们让，如[18]中所用。 | **B. 结果与讨论**  *1）收敛性能：*我们首先检查了我们算法的收敛性能。我们调整了b值，以使功率微扰幅度的平均值为-5mW，且最小集体关系强度。我们先在不同数量（M=4，5，6）的可用信道上开展实验。使用网络吞吐量作为性能度量指标。从图3中，我们观察到，所提议的算法通常在1500迭代次数内发生收敛，随着信道数量的增加，收敛时间也更长。可以观察到，改变信道大小并不影响能够取得的最大网络吞吐量，这占可选网络吞吐量的约90%。对于任意选择的用户#10，我们进一步评估了在各可用信道上，其策略的收敛情况，如图3b所示。  网络吞吐量的收敛    可选  正常化的网络吞吐量  迭代  （a）  用户#10的策略的收敛    概率  迭代  （b）  图3：双时标分布式算法的收敛性能  *2）吞吐量-隐私均衡的比较研究：*  接下来，我们研究了在不同功率微扰水平下网络吞吐量和位置隐私之间的均衡。我们使用默认设置和，并在不同功率微扰水平下开展实验。特别地，我们改变了参数b的值，以使微扰功率水平的平均值处于0mW至-9mW之间。出于比较研究的目的，我们考虑了两个基准：（a）单一时标学习算法，仅包含基于第V-A2节所述经修订基于反悔的学习（RBL）的策略适应；（b）双时标学习算法，包含效用学习和遵循随机虚构博弈（SFP）的策略适应[1]。 |

|  |  |
| --- | --- |
| 如图4所示，一般来讲，随着平均功率微扰水平的增加，系统吞吐量会降低。同时，很清楚的是，与同时包含效用学习和策略适应的其他两种方法相比，使用RBL的单一时标学习的吞吐量降低地更快。这表明，使用平行效用学习校准嘈杂效用观察的有效性，这有助于保持位置隐私保护与网络性能（例如，系统吞吐量）之间的平衡。  可以看到，我们所提议算法取得的吞吐量比使用[1]中所述使用双时标学习方法获得的吞吐量平均高出5%。两个研究使用了不同的均衡标准，可以解决这一原因。按照定义，纳什均衡使用的关键假设是，博弈者的策略是相互依赖的。而在本研究中，其考虑的相关均衡通过允许博弈者之间的策略相互独立，而对纳什均衡予以一般化。由于相关均衡在数学上等同于凸多胞形，其极端点对纳什均衡的集合相对应，因此，一般来讲，可以表现出更好的性能。    使用RBL的单时标学习  使用SFP的双时标学习  使用RBL的双时标学习  正常化平均吞吐量  吞吐量VS隐私  集体关系强度的最低价值（）  图4：在不同功率微扰水平下各不同学习算法的性能比较  *3）系统规模和集体关系强度的影响：*我们最后检查了网络对系统性能的影响。我们针对三三种不同网络规模（例如，N=80，100，120）的情景，按照从0.5增加到0.9开展实验。如图5所示，随着系统规模的增大，一般来讲，网络吞吐量也增加。同样，可以看到，随着组内关系的增强，吞吐量也单调地增加。对于N=80，100，120的情景，当从0.5增加至0.9时，取得的性能增益分别为14.5%、15%和16.4%。这表明，如果用户更加选择利他行为，则系统将从中受益。 | 正常化平均吞吐量  吞吐量VS隐私  集体关系强度的最低价值（）  图5：总用户数量N和最低组织内关系强度对网络吞吐量的影响  **VII. 结论**  在本文中，我们研究了工业物联网系统中的数据库辅助频谱共享。为应对基于RSS的位置隐私攻击，使用了随机功率微扰方法来降低对手的定位精确度。我们将隐私保护频谱共享当作存在社会耦合关系的物联网设备之间的随机信道选择博弈。基于无反悔动态，我们开发了一种双时标分布式学习算法。在该算法中，各设备不断地估算其组效用，并改进其策略，以降低反悔。我们提出的算法表明，它能够实现相关均衡集合的弱收敛，且相比仅涉及策略适应的单一时标学习方法，它的表现更为出色。因此，我们的方法可帮助在工业物联网中，在位置隐私保护和增强网络性能之间找到平衡。  **参考文献** |



