一年来 iot 前沿论文最新进展

2018.11.03 方建勇

提示：采用手机 safari 微软翻译技术

1. 第 1811.00175[pdf,其他] Cs。铬

   正式验证的硬件软件为远程认证共同设计

   作者:karim el 布赖 say, ivan o.nunes , norrathep rattanavipanon, michael steiner, gene tusdik

   摘要: 在这项工作中，我们通过设计和验证一种名为 vrased:用于简单嵌入式设备的可验证远程验证的体系结构，朝着正式验证 ra 迈出了第一步。vrased 实例化了基于低端嵌入式系统 (例如简单的物联网设备) 的混合 (硬件软件-hw/sw) ra 协同设计 。vrased 提供了与基于 hw 的方法类似的安全级别，同时依靠 sw 将额外的硬件成本降至最低。由于安全属性必须由硬件和软件共同保证，因此验证 vrased 等体系结构是一项具有挑战性的任务，在 ra 的上下文中从未尝试过。我们认为，如本文所述，vrased 是第一个经过正式验证的 ra 计划。据我们所知，我们的努力也对任何安全服务的 hwsw 实施进行了首次正式验证。为了证明 vrased 的实用性，我们在商品平台 (texas 仪器的 msp430) 上对其进行实例化和评估，并将其实施公之于众。我们相信，这项工作展示了混合 ra 的成熟度及其近乎实际采用的准备，标志着嵌入式系统和**物联网**设备在安全性方面取得了重要进展。少

   2018 年 10 月 31 日提交;最初宣布 2018 年 11 月。

2. 建议: 1810.13667[pdf,其他] Cs。铬

   通过对信息流的细粒度控制保护物联网应用的安全

   作者:davino mauro junior,基辅加马, atul prakash

   摘要: 物联网正在迅速发展，许多连接的设备现在已经提供给消费者。随着这一增长，从智能手机管理设备的**物联网**应用引发了重大的安全问题。通常，这些应用是通过敏感凭据 (如电子邮件和密码) 进行保护的，这些凭据需要通过特定的服务器进行验证，因此需要访问 internet 的权限。不幸的是，即使开发人员是善意的，这类应用程序可以是不平凡的安全，以确保用户的凭据不会泄漏到未经授权的服务器在互联网上。例如，如果应用依赖于第三方库 (许多人这样做)，则这些库可能会捕获和泄漏敏感凭据。应用程序中的 bug 还可能导致可利用的漏洞泄漏凭据。本文介绍了我们正在进行的原型工作，该原型使开发人员能够控制应用程序中的信息如何从敏感的 ui 数据流向特定的服务器。我们扩展了 flowfence，以便对敏感的 ui 数据实施细粒度的信息流策略。少

   2018 年 11 月 1 日提交;v1 于 2018 年 10 月 31 日提交;最初宣布 2018 年 10 月。

   评论:接受在十八巴西信息和计算机系统安全问题会议上发表的论文

3. 第 1810.13332[pdf] cs. cy

   通过使用智能容器实现实时可追溯性，改进风险管理

   作者:Siraprapa wattanakul, sébastien henry, mohand lounes bengaha, naporn reeveerakul,yacine ouzrout

摘要: 本研究通过使用从附加在扩展实时数据 (soerd: 例如智能容器、智能托盘等) 的智能对象中获得的链可追溯性数据来改进风险管理，从而提出了应用功能的含义。物流链。学术文献探讨了最近使用可追溯性数据的应用和可追溯性系统中的主要问题。信息是通过使用当前可追溯性数据来分类的，以支持操作、战术和战略层面的风险检测和决策。研究发现，实时数据对各决策级别的运输活动使用产生了重大影响，如食品质量控制和合作伙伴之间的协作规划功能。但是，在汇总各合作伙伴捕获的基于事件的可追溯性数据方面存在一些不确定性，这阻碍了链采用数据使用方式。在工业 4.0 和物联网 (**iot**) 的环境下，so-erd 可通过链实时进行独立的数据跟踪。其数据有可能克服当前问题，改善供应链风险管理。因此，在文献综述的基础上，利用 so-erd 数据揭示了供应链中目前对决策功能的关注，提出了风险管理的意义。其影响可能会对域需求产生影响。少

2018 年 10 月 31 日提交;最初宣布 2018 年 10 月。

期刊介绍:第九届物流与运输国际会议 (iclt 2017), 2017 年 11 月，泰国曼谷。2017 年

4. 第 1810.13068[pdf, ps,其他] cs. it

共生无线电: 被动物联网的一种新的交流模式

作者:龙瑞哲,郭华燕,杨刚, 梁英昌,张瑞

文摘: 本文提出了一种新的无源物联网 (iot) 技术–共生无线电 (sr)，其中一个反向散射器件 (bd) 与一个主要传输集成在一起。主发射机设计用于辅助主发射和 bd 传输，主接收机对来自主发射机和 bd 的信息进行解码。我们认为多输入单输出 (miso) sr 和 bd 传输的符号周期设计为与主系统相同或更长的时间周期，从而导致主系统和 bd 之间的寄生或同源关系传输。我们首先推导出主系统和 bd 传输的可实现速率。然后，我们提出了两个传输波束形成优化问题，即加权求和速率最大化问题和发射功率最小化问题，并应用半定松弛技术解决了这些非凸问题。此外，为了降低解的计算复杂度，提出了一种新的传输波束形成结构。仿真结果表明，在适当设计 bd 传输速率的情况下，所提出的 sr 不仅通过节能的被动后向散射实现了 bd 的机会传输，而且还提高了主系统的可实现速率。适当利用来自 bd 的附加信号路径

2018 年 10 月 30 日提交;最初宣布 2018 年 10 月。

5. 建议: 1810.12735[pdf, ps,其他] Cs。Cl

边缘语言理解

作者:alaa saade, alice coucke, 亚历山大·考利耶, joseph dureau, adreen ball, théodore bluche, david leroy, clément doumouro , thibault gisselbrecht, francesco caltagirone, Thibaut lavril, maël primet

摘要: 我们考虑在**物联网**应用程序典型的小型设备上执行语言理解 (slu) 的问题。我们的贡献是双重的。首先，我们概述了嵌入式、私有设计的 slu 系统的设计，并展示了它的性能与基于云的商业解决方案相当。其次，为了重现重现性，并希望这些数据集能够对 slu 社区有用，我们发布实验中使用的数据集。少

2018 年 10 月 30 日提交;最初宣布 2018 年 10 月。

6. 第 1810.12292[pdf] Cs。直流

物联网云平台: 应用程序开发视角

作者:preeti Agarwal, mansaf alam

摘要: 随着物联网 (**iot**) 设备数量的不断增加，通过这些设备生成的数据也在不断增长。据预测，到 2025 年,**物联网**设备的数量将超过地球上的人类数量。因此，通过这些**物联网**设备

生成的数据将是巨大的。这使得存储量激增。最有希望的解决方案之一是将数据存储在云上。随着**物联网**云平台的数量的增加，市场已经过大。尽管各种**物联网**云平台的可用性非常大，但在文献数据库中几乎没有尝试对其进行分类或比较以供开发的应用程序使用。本文将**物联网**平台分为四类，即：公开交易、开源、开发人员友好和端到端连接。根据给定的一般**物联网**架构，确定并比较了每个类别中的一些流行平台。这项研究对于 **iot** 中的新手和应用程序开发人员根据构建应用程序的要求选择最合适的平台非常有用。少

2018 年 10 月 27 日提交;最初宣布 2018 年 10 月。

7. **第 1810.12260[pdf] Cs。镍**

5g 以外网络的无线太赫兹系统架构

作者:亚历山大·布卢斯托洛斯 a. boulogeorgos, angeliki alsiou, Dimitrios kritharidis，亚历山大·卡齐奥蒂斯，乔治娅·恩图尼, joonaskokkoniemi, janne lethtomaki, markku juntti, dessy yankova, ahmed mokhtar, jean-charlespoint, jose machado, robert elschner, colja schubert, thomas merkle, ricardoferreira, francisco rodrigues, jose lima

摘要：本白皮书重点介绍了 terranova 的系统要求。最初详细介绍了 terranova 技术的关键用例，并介绍了网络体系结构。更详细地说，用例分为两类，即回程和前端和访问和小细胞回程。第一类是光纤扩展器、点对点和冗余应用程序，而后者旨在支持中小型企业 (sme) 的备份连接、物联网 (**iot**) 密集的环境、数据中心、室内无线接入、临时网络和最后一英里接入。然后，它提供了 terranova 系统的网络体系结构以及需要部署的网络元素。使用实例与特定的技术场景相匹配，即室外固定点对点 (P2MP)、室外个体点对点 (p2mp) 和室外 "准" 全向，以及每个方案的关键性能要求被识别。同样，我们提出了突破性的新技术概念，包括完整光和无线链路基带信号处理的联合设计，频率宽带和频谱高效 rf 前端的发展 >275ghz，以及通道建模，波形，天线阵列和多址方案的设计，我们将使用，以满足所提出的要求。接下来，将概述 terranova 系统体系结构中物理 (phy) 层和中等访问控制 (mac) 层所需的新功能。最后，将 terranova 系统的各个使能因素结合起来，为这三种技术方案中的每一个方案开发特定的候选体系结构。少

2018 年 10 月 29 日提交;最初宣布 2018 年 10 月。

评论:73 页, 31 个数字, 7 个表. arxiv 管理说明：文本与 arxiv:1003. 00697 由其他作者

8. **建议: 1810.12035[pdf,其他] Cs。铬**

多伊10.14722/diss.2018.23009

物联网标准化工作中的安全经济学探讨

作者:菲利普·莫格纳, zinaida benenson

摘要：物联网 (**iot**) 传播了由不同制造商连接数十亿异构设备的范式。为了支持**物联网**应用，**物联网**设备之间的通信遵循标准开发组织定义的规范。本文以一个案例研究为例，研究了流行**的物联网**标准 zigbee 所披露的不安全因素，并得出了**物联网**标准化工作中安全经济学的一般经验。我们讨论了主要从经济角度推动**的物联网**标准化工作的动机，在这种情况下，由于消费者不奖励这些努力，因此不认为有必要对安全进行大量投资。通过快速上市、提供功能功能和为互补提供轻松集成，在市场上取得了成功。然而，制造商不仅应考虑经济原因，还应看到他们有责任保护人类和技术基础设施不受不安全**的物联网**产品的威胁。在此背景下，我们提出了一些建议，以加强未来**物联网**标准化工作中的安全设计，从定义精确的安全模型到实施更新策略。少

2018 年 10 月 29 日提交;最初宣布 2018 年 10 月。

评论:ndss 分散物联网安全与标准研讨会 (diss) 2018, 2018 年 2 月 18 日, 美国加利福尼亚州圣地亚哥

9. **建议: 1810.11902[pdf,其他] cs. it**

非理想功率放大器电池供电物联网设备的可靠性感知链路优化

作者:aamir mahood, m. m. aftab hossain , cicek cavdar, mikael Gidlund

摘要: 本文研究了低功耗无线链路的跨层优化, 适用于可靠性感知应用, 同时考虑**了物联网**设备中硬件的约束和非理想特性。具体而言, 我们定义了一个能量消耗 (ec) 模型, 该模型捕获能量成本–收发器电路、功率放大器、数据包错误统计、数据包开销等––在提供有用的数据位时。我们推导了一个理想的和两个现实的非线性功率放大器模型的 ec 模型。为了结合数据包误差统计, 我们以基本函数的形式, 在瑞利块衰落中建立了一种简单的闭式数据包误差率 (per) 逼近方法。利用 ec 模型, 我们推导出能量最佳但可靠性和硬件兼容的条件, 以限制无约束的最优信噪比 (snr) 和有效负载大小。结合这些条件, 我们为资源受限**的物联网设备**开发了一种半解析算法, 以共同优化物理 (调制大小、snr) 和 mac (有效负载大小和重新传输次数) 层的参数。链路距离。我们的结果表明, 尽管可靠性受到限制, 但共同的概念–––更高的 m-与物联网设备中经常使用的 oqpsk 调制相比, 速率调制是短**距离通信**的最佳能量–––优先, 可提供高达 180% 的寿命延长。然而, 可靠性限制降低了它们的范围和能源效率, 而非理想的传统 pa 则将范围进一步缩小了 50%, 并减少了能量增益, 除非使用更好的 pa。少

2018 年 10 月 28 日提交;最初宣布 2018 年 10 月。

10. **第 1810.1729[pdf,其他] Cs。镍**

多组 nb-iot 网络优化的协同深度强化学习

作者:南江,邓燕莎, osvaldo simeone, arumugam nallanathan

摘要: 窄带和物联网 (**nb-iot**) 是一种新兴的基于蜂窝的技术, 它为具有异构需求的设备组的大规模**物联网**无线访问提供了一系列灵活的配置。配置指定分配给每组设备的无线电资源量, 以便随机访问和数据传输。假设不了解流量统计信息, 问题是在每个传输时间间隔 (tti) 以在线方式确定最大限度地提高能够访问和访问的物联网设备的长期平均数量**的配置.** 提供数据。针对优化算法的复杂性, 提出了一种基于 q-w 企业管理 (cma-dqn) 的协同多智能体深神经网络方法, 通过该方法, 每个 dqn 代理独立控制每个组的配置变量。dqn 代理根据有关传输结果的反馈在同一环境中进行合作培训。cma-dqn 被认为大大优于传统的基于负载估计的启发式方法。少

2018 年 11 月 1 日提交;v1 于 2018 年 10 月 27 日提交;最初宣布 2018 年 10 月。

评论:提交供会议出版

11. **第 1810.11006[pdf] Cs。镍**

ofdm 背散射的空间频率特性测量

作者:张晓雪,南环米,新河,杨盘龙, 杜浩华, 侯家辉, 万鹏军

摘要: 正交频分复用 (ofdm) 反向散射系统 (如 wi-fi 反向散射) 由于其无处不在且低成本的特点, 近年来被公认为**物联网**连接的一种有前途的技术。本文研究了考虑不同频段距离和角度的 ofdm 背散射的空间频率特性。我们部署了三种典型方案来执行测量, 以评估从反向散射链路接收到的信号强度。通过所获得的测量数据观察了发射机、标签和接收机之间的距离以及发射机与标签之间的角度的影响。从评价结果中可以发现, 标签的最佳位置要么接近接收机, 要么取决于频带的发射机, 最佳角度是发射机与接收机之间的 90 度。本文为背散射标记在不同频段的空间部署提供了启示, 旨在提高性能, 减少干扰。少

2018 年 10 月 27 日提交;最初宣布 2018 年 10 月。

12. **建议: 1810.11613[pdf,其他] Cs。Sy**

物联网的学习与管理: 适应性和可扩展性的核算

作者:陈天一, sergio barbarossa, xinwang, gegiannakis, zhi-li zhang

摘要: 物联网 (**iot**) 设想了一个联网智能设备的智能基础架构, 提供特定于任务的监控服务。**物联网**的独特特性包括极端的异质性、大量的设备以及部分由于人机交互而产生的不可预知的动态。这就需要在网络设计和管理方面进行根本性的创新。理想情况下, 它应允许高效适应不断变化的环境, 并在受到严格的延迟限制的情况下, 实现可扩展到大量设备的低成本实施。为此, 本文的总体目标是通过在通信、网络、学习和优化方面的联合进步, 概述**物联网**在线学习和管理政策的统一框架。从网络架构的优势点出发, 统一框架利用了一个有前途的雾体系结构, 使智能设备能够在云到事物的连续体中接近地访问网络边缘的云功能。从算法的角度来看, 关键的创新目标是在线方法适应**物联网**动力学中不同程度的非稳定性, 以及它们在有限反馈下的可扩展无模型实现, 这些反馈激励着盲人或土匪方法。拟议的框架旨在提供一个垫脚石, 从而对特定任务的物**联网**学习和管理方案进行系统的设计和分析, 并提供一系列新的研究方向。少

2018 年 10 月 27 日提交;最初宣布 2018 年 10 月。

评论:6 月 15 日提交关于自适应和可扩展通信网络的 ieee 特刊的进展

13. **第 1810.1295[pdf,其他] Cs。Lg**

物联网应用的实时上下文感知学习系统

作者:bhaskar das, jalal almhana

摘要: 我们提出了一个实时上下文感知学习系统以及在移动设备上运行的架构, 为用户提供服务, 并管理**物联网**设备。在该系统中, 在移动设备上运行的应用程序从传感器中收集数据, 了解用户定义的上下文, 进行实时预测, 并相应地管理**物联网**设备。然而, 移动设备的计算能力使得以可接受的精度运行机器学习算法具有挑战性。为了解决这个问题, 一些作者在服务器上运行机器学习算法, 并将结果传输到移动设备。尽管服务器所做的上下文感知预测比移动对应的预测更准确, 但它在很大程度上依赖于将结果传递到设备的网络连接, 这将对实时上下文学习产生负面影响。因此, 在本文中, 我们描述了一种移动设备的上下文学习算法, 该算法对计算资源的要求较低, 并通过从服务器获得的学习参数更新自身来保持预测的准确性定期。实验结果表明, 该算法能实现平均精度高达 97.51%, 而平均执行时间只需要 11 毫秒。少

2018 年 10 月 26 日提交;最初宣布 2018 年 10 月。

评论:34 页, 12 个数字, 期刊文章

14. **第 1810.1287[pdf,其他] Cs。镍**

从边缘卸载执行到云: 基于动态节点红色的方法

作者:román sosa, csaba kiraly , juan d. parra rodriguez

摘要: 雾计算允许使用这样的情况: 在最终设备中产生的数据被存储、处理并直接在网络边缘对其进行操作, 但计算可以通过边缘到云连续体卸载到更强大的实例。在现代多用途**物联网**网关中尤其需要这种卸载机制, 因为在这些网关中, 不同部署的需求和操作条件可能差别很大。为了促进网关的开发和操作, 我们直接实现卸载, 作为嵌入在软件堆栈中的**物联网**快速原型过程的一部分, 基于 node-red。我们使用图像处理示例对实现的方法进行评估,

并根据资源消耗和其他系统指标比较各种卸载策略，突出处理需求和达到的服务级别的差异。少

2018 年 10 月 26 日提交;最初宣布 2018 年 10 月。

评论:第十届 ieee 云计算技术与科学国际会议 (云通信 2018)

15. 第 1810.11175[pdf,其他] Cs。铬

Ircoin: 基于比特币的防漏加密货币，用于物联网中的数据交易

作者:yong yu, yyujieding, yqi zhao, yannan li, xi 去 den , mohsen guizani

文摘: 目前，构成**物联网**的科技 (**iot**) 设备互联网数量已超过 110 亿，而且一直在不断增加。这些设备的普及带来了一种新兴的**物联网**业务模式，称为 "设备即服务" (daas)，使传感器设备能够收集传播到所有感兴趣设备的数据。与其他设备共享数据的设备可能会获得比特币等一些经济回报。但是，侧通道攻击，其目的是利用数据交易执行过程中从**物联网**设备泄漏的一些信息，是可能的，因为大多数**物联网**设备都容易受到攻击或破坏。因此，由于信息泄露 (如在比特币系统中签署比特币交易的私钥) 泄露，在**物联网**环境中安全地实现数据交易具有挑战性。本文提出了一种基于比特币的抗漏加密货币 Ircoin，其中用于对比特币事务进行认证的签名算法具有抗泄漏能力。Ircoin 适用于不可避免的信息泄露的情况，如**物联网**应用。我们的核心贡献是提出了一个有效的基于双线性的连续泄漏弹性 ecdsa 签名。证明了在连续泄漏设置下，在一般双线性群模型中，该签名算法是不可伪造的。理论分析和实施都证明了该方案的实用性。少

2018 年 10 月 25 日提交;最初宣布 2018 年 10 月。

评论:9 页, 3 个数字, 1 个表

16. 建议: 1810.761[pdf,其他] cs. it

面向可持续物联网的低功耗广域网络

作者:秦志金,李国宝,叶丽 , 朱莉 a.麦孔，倪强

摘要: 低功耗广域 (lpwa) 网络正受到广泛关注，因为它们能够提供低成本和大规模连接到分布在广泛地理区域的物联网 (**iot**) 设备。本文简要概述了现有的 lpwa 技术，并提供了有用的见解，以帮助大规模部署 lpwa 网络。特别是，我们首先回顾了 lpwa 网络目前在技术基础知识和大规模部署潜力方面的竞争候选项，如窄带**物联网**(nb-iot) 和远程 (lora)。然后，我们在 lpwa 网络上提供两个实现示例。通过对现场测试结果的分析，我们找出了阻碍 lpwa 技术从理论走向广泛实践的几个挑战。少

2018 年 10 月 25 日提交;最初宣布 2018 年 10 月。

评论:本文已被 ieee 无线通信所接受

17. 建议: 1810.10746[pdf] Cs。铬

为智能电网中支持云的物联网实现高效、安全的数据采集

作者:关志涛,李静,吴龙飞, 张悦,吴军,杜晓江

摘要: 云支持的物联网 (Cloud-supported) 已广泛应用于智能电网系统中。**物联网**前端负责数据采集和状态监控，而大量数据则存储在云服务器中并对其进行管理。在数据采集和传输过程中实现数据安全和系统效率具有重要意义和挑战性，因为电网相关数据是敏感的、巨大的。本文提出了一种基于 cp-abe (基于密码文本策略属性加密) 的高效、安全的数据采集方案。从终端获取的数据将被划分为块，并按相应的访问子树按顺序进行加密，从而可以并行处理数据加密和数据传输。此外，我们还使用阈值秘密共享方法保护有关访问树的信息，从而保护具有未经授权属性集的用户的数据隐私和完整性。形式化分析表明，该方案

能够满足智能电网中云支持物联网的安全要求 。数值分析和实验结果表明，与其他常用方法相比，该方案能有效地降低时间成本。少

2018 年 10 月 25 日提交;最初宣布 2018 年 10 月。

18. **建议: 1810.723[pdf, ps,其他] cs. cy**

基于众源和云空气质量指标的城市医疗大数据系统

作者:min chen, jun yang, long hu , m. shamim hossain, ghulam muhammad

摘要: 日益加速的全球化进程使一半以上的人口能够生活在城市中。因此，城市空气质量对越来越多的城市居民的健康状况产生了至关重要的影响。本文以通过气象站点、移动众包和**物联网**传感采集的城市空气质量数据为基础，结合用户的身体信号，提出了一个名为 uh-bigdatasays 的城市医疗大数据系统。本文首先介绍了一种将多源空气质量数据集成到人工智能智能城市服务数据准备中的方法。然后，随着空气质量意识医疗应用的部署，建立了 uh-bigdatass 的试验台。最后，我们在呼吸道疾病、户外旅行、睡眠质量等方面为城市居民提供健康指导。uh-bigdatays 的最终目标是让城市居民过上更健康的生活。少

2018 年 10 月 25 日提交;最初宣布 2018 年 10 月。

19. **建议: 1810.10697[pdf] Cs。镍**

comtic：设备到设备云中任务分配的组合双竞价

作者:翟玉通,黄柳生,陈龙,肖宁,耿阳耿阳

摘要: 随着物联网 (**iot**) 技术的发展，移动设备的功能大大提高。然而，在大数据时代，在一台设备上完成任务仍然是一项挑战。众包作为一项新兴技术，利用大量设备来方便大规模的传感任务，越来越受到人们的关注。现有的大多数作品要么假定设备愿意利用集中式机制进行合作，要么设计使用双重拍卖的激励算法。当前者缺乏集中控制器时，这是不实际的，也不适合于卖方设备也对后者的资源有限的情况。本文提出了一种真实的激励机制，并对设备对设备 (d2d) 云中的人群传感任务分配进行了组合双重竞价，在这种机制中，具有密集传感任务的单个移动设备可以租用一组空闲相邻设备。有了这种新机制，时间关键传感任务可以在分布式性质下及时处理。证明了所提出的机制是真实的、个体理性的、预算平衡的、计算效率的。仿真结果表明，与现有的双拍卖方案和集中式最大匹配算法相比，组合双拍卖机制分别获得了 26.3% 和 15.8% 的收益。少

2018 年 10 月 24 日提交;最初宣布 2018 年 10 月。

评论:17 页, 7 个数字，被第 18 届并行处理算法和体系结构国际会议 (ica3pp 2018)接受

20. **建议: 1810.10458[pdf,其他] Cs。镍**

基于无线供电的 csmama/ca 物联网网络中的比例公平性

作者:陈晓民,詹舒，王克志, 徐方民,曹悦

文摘: 本文考虑在基于 802.11 的无线供电**物**联网网络中部署混合无线数据电源接入点。在每个设备的能量中性和 cpu 能力的限制下，考虑了**跨物联网**节点的吞吐量的比例公平分配。无线供电和数据通信资源的联合优化考虑了 csmaca/ca 随机通道访问功能，例如回退过程、冲突、协议开销。数值结果表明，优化后的解决方案可以有效地平衡节点间的单个吞吐量，同时在能量约束下按比例提高总体吞吐量。少

2018 年 10 月 24 日提交;最初宣布 2018 年 10 月。

评论:2018 年全球公司接受

21. **建议: 1810.10322[pdf] cs. cy**

多伊10.1049/cp.2018.0003

物联网网络风险的经济影响-分析过去和现在，预测物联网风险分析和物联网网络保险的未来发展

作者:佩塔尔·拉丹廖夫

摘要:本文重点介绍了物联网 (**iot**) 的当前演变及其与工业 4.0 (i4.0) 领域相关的网络风险。我们报告了一项定性实证研究的结果，该研究将学术文献与 14-i4.0 框架和倡议联系起来。

2018 年 10 月 13 日提交;最初宣布 2018 年 10 月。

评论:https://ieeexplore.ieee.org/document/8379690. arxiv 管理说明: 与 arxiv:1809. 05229 大量文本重叠

22. **第 1810.10139[pdf,其他] Cs。镍**

基于认知无线电的区块链网络中的联合交易传输与信道选择: 一种深层强化学习方法

作者:nguyen cong luong, tranthe anh, huynh thi thanh binh, dusitniyato, dongin kim, ying-chang liang

摘要: 为了确保数据聚合、数据存储和数据处理都以分散但可信的方式进行，我们建议将区块链与挖掘池一起用于支持基于认知无线电网络的**物联网**服务。因此，辅助用户可以将其传感数据，即事务，发送到挖掘池。经过矿工的验证后，交易记录将添加到块中。然而，在主通道的动态和挖掘池的 mempool 状态的不确定性下，辅助用户很难确定最佳的事务传输策略。本文提出利用深度强化学习算法，为二次用户推导出最优的事务传输策略。具体来说，我们采用双深度 q 网络 (ddqn)，允许辅助用户学习最佳策略。仿真结果表明，所提出的深度强化学习算法在奖励和学习速度方面优于传统的 q 学习方案。少

2018 年 10 月 23 日提交;最初宣布 2018 年 10 月。

23. **建议: 1810.09551[pdf,其他] Cs。铬**

多伊10.114/3281411.3281440

物联网: 强化物联网系统的安全性

作者:dang tu nguyen, chengyusong, zzyyun qian 仙, srikanth v. krishnamurthy, edward j. m. colbert,patrick mcdaniel

摘要: 当今的**物联网**系统包括与传感器和执行器交互的事件驱动智能应用程序 (应用程序)。**特定于物联网**系统的一个问题是，错误的应用程序、不可预见的不良应用交互或设备/通信故障可能会导致不安全和危险的物理状态。检测导致此类状态的缺陷需要全面查看已安装的应用、组件设备及其配置，更重要的是，需要全面了解它们的交互方式。本文设计了 iotsan，这是一个新的实用系统，它将模型检查作为一个构建块，通过识别可能导致系统进入不安全状态的事件来揭示 "交互级" 缺陷。在构建 iotsan 时，我们设计了针对**物联网**系统定制的新技术，以缓解与模型检查相关的状态爆炸。iotsan 还会自动将**物联网**应用转换为适合模型检查的格式。最后，为了了解检测到的漏洞的根本原因，我们设计了一种归因机制来识别有问题和潜在的恶意应用。我们在三星智能物品平台上对 iotsan 进行评估。从 76 个手动配置的系统中, iotsan 检测到 147 个漏洞。我们还评估 ittsan 与恶意智能事物应用程序从以前的努力。iotsan 检测到潜在的安全违规，并有效地将这些应用归因于恶意。少

2018 年 10 月 27 日提交;v1 于 2018 年 10 月 22 日提交;最初宣布 2018 年 10 月。

评论:2018 年第 14 届中新文件的项目

24. **建议: 1810.08870[pdf, ps,其他] cs. it**

物联网的联合接收机设计

作者:王坤

摘要: 物联网 (**iot**) 是一个不断增长的连接、收集和交换数据的对象网络。为了实现连接一切的使命，物理层沟通是不可或缺的。在这项工作中，我们提出了一个新的**接收**器定制的物联网通信的特点。具体来说，我们的设计适用于**物联网**应用中中小型数据包的零星传输。通过新接收机的接头设计，保证了强大的可靠性，并有望节能。少

2018 年 10 月 20 日提交;最初宣布 2018 年 10 月。

评论:9 页，学术文章

25. 第 1810.086009[pdf] Cs。Lg

一种基于堆叠的自动编码器神经网络的在线状态监测异常检测自动特征提取方法

作者:mohendra roy, sumon kumar bose, bapi kar , prdeep kumar gopalakrishnan, arindam basu

文摘: 状态监测是各大过程工业的日常任务之一。电机、齿轮、轴承等机械部件是加工行业的主要部件，其中的任何故障都可能导致整个工艺的全面停机，从而造成严重损失。因此，在其发生之前预测任何接近的缺陷都是非常关键的。为此目的有几种方法，目前正在为更好和有效的模型进行许多研究。然而，它们大多是基于对原始传感器信号的处理，这是繁琐而昂贵的。最近，基于特征的状态监测有所增加，只从原始信号中提取有用的特征，并解释为预测故障。其中大多数是手工制作的功能，这些功能是根据原始数据的性质手动获取的。这当然需要事先了解数据的性质和相关流程。这将限制特征提取过程。然而，基于自动编码器的特征提取方法的最新发展为传统的手工制作方法提供了一种替代方法;然而，它们大多被限制在图像和音频处理领域。在本工作中，我们开发了一种基于传统自动编码器堆栈和在线顺序极端学习机 (oselm) 网络的在线状态监测的自动特征提取方法。该方法的性能与传统特征提取方法相当。该方法可实现 100% 的检测精度，用于确定美国宇航局轴承数据集的轴承健康状态。该方法的简单设计对于基于物联网 (**iot**) 的预测解决方案的简单硬件实现具有广阔的应用前景。少

2018 年 10 月 18 日提交;最初宣布 2018 年 10 月。

评论:本文已提交给 ieee-ssci 2018 会议

26. 第 1810.08415[pdf,其他] Cs。铬

物联网: 确保边缘网络中的物联网通信

作者:ibbad hafeez, markku antikainen, aaron yiding, sasu tarkoma

摘要: **物联网**设备的日益普及使其成为攻击者的利润目标。由于不安全的产品开发实践，这些设备通常容易受到非常小的攻击，并且很容易受到损害。由于**物联网**设备的数量众多且异质性，因此无法使用传统的端点和网络安全解决方案来保护**物联网**生态系统的安全。为了应对边缘网络中保护**物联网**设备的挑战和要求，我们提出**了物联网**管理员，这是一个能够实时保护网络免受任何恶意活动攻击的新型系统。该系统使用轻量级异常检测技术，在使用网关上可用的有限资源的同时，保护设备到设备和设备对基础结构的通信。它使用未标记的网络数据来区分在网络中观察到的良性和恶意流量模式。通过真实世界测试台进行的详细评估表明,**物联网**管理员检测到任何设备以高精度 (0.982) 和低假阳性率 (0.01) 生成恶意流量。结果表明,**物联网**管理员重量轻、响应迅速，能够有效地处理复杂的 d2d 交互，而无需显式攻击签名或复杂的硬件。少

2018 年 10 月 19 日提交;最初宣布 2018 年 10 月。

评论:20 页, 9 个数字, 4 个表

27. 第 1810.08260[pdf,其他] Cs。直流

合并: 互联测试生态系统的体系结构

作者:ryan good 老人, lincoln thurlow, srivatsan ravi

摘要: 在网络安全研究界, 没有一刀切的解决方案来将来自不同专用测试台的大量异构资源和实验能力合并到集成实验中。目前网络实验的环境多种多样, 包括许多领域, 包括关键基础设施、企业 it、网络物理系统、蜂窝网络、汽车平台、**物联网**和工业控制系统。现有的联合测试平台在设计上与预定义的适用域相限制, 缺乏集成大量异构设备或工具的系统能力, 无法将其有效用于实验。我们开发了合并体系结构, 以逻辑上集中的方式动态集成不同的测试平台, 使研究人员能够有效地发现和使用由不断发展的分布式生态系统提供的资源和功能用于开发严格和高保真网络安全实验的试验台。少

2018 年 10 月 18 日提交;最初宣布 2018 年 10 月。

28. 第 1810.08125[pdf,其他] 反渗透委员会

机器人系统的程序配置访问控制

作者:ruffin white, gianluca Caiazza, henrik i. christensen, agostino cortesi

摘要: 机器人系统以及相关中间件基础结构的安全性是工业和国内**物联网**的一个关键问题, 需要在整个开发生命周期中不断进行评估。下一代开源机器人软件堆栈 ros2 现在的目标是支持安全 dds, 为社区提供安全的真实世界机器人部署的宝贵工具。在本文中, 我们介绍了一个框架, 用于为机器人软件提供过程访问控制策略, 以及验证生成的传输工件和决策点实现的合规性。少

2018 年 10 月 18 日提交;最初宣布 2018 年 10 月。

杂志编号: 2018 ieee®智能机器人和系统国际会议 (iros)

29. 建议: 1810.07862[pdf,其他] Cs。镍

深度强化学习在通信与网络中的应用综述

作者:阮从联、丁泰黄、石民、杜希特·尼亚托、王平、梁英昌、 董英金

文摘: 本文对深层强化学习在通信和网络中的应用进行了全面的文献综述。现代网络, 如物**联网** (**iot**) 和无人机 (uav) 网络, 变得更加分散和自主。在这种网络中, 网络实体需要在本地做出决策, 以便在网络环境不确定的情况下最大限度地提高网络性能。强化学习已被有效地利用, 使网络实体能够获得最佳政策, 例如, 考虑到它们在国家和行动空间较小时的状态, 包括决定或行动。然而, 在复杂的大规模网络中, 状态和作用空间通常很大, 强化学习可能无法在合理的时间内找到最优的策略。因此, 为了克服这些不足, 开发了深度强化学习, 将强化学习与深度学习结合起来。在本次调查中, 我们首先给出了从基本概念到高级模型中深入强化学习的教程。然后, 我们回顾了为解决通信和联网方面新出现的问题而提出的深入强化学习方法。这些问题包括动态网络访问、数据速率控制、无线缓存、数据卸载、网络安全和连接保护, 这些都是下一代网络 (如 5g 及更高) 的重要组成部分。此外, 我们还介绍了深度强化学习在流量路由、资源共享和数据收集中的应用。最后, 重点介绍了应用深度强化学习的重要挑战、开放问题和未来的研究方向。少

2018 年 10 月 17 日提交;最初宣布 2018 年 10 月。

评论:37 页, 13 个数字, 6 个表格, 174 份参考文件

30. 建议: 1810.07829[pdf] cs. cy

质量 4.0: 让我们获得数字化-第四次工业革命正在重塑我们对质量的看法的许多方式

作者:nicole m. radziwill

摘要: 技术格局比以往任何时候都更加丰富和有希望。在许多方面，云计算、大数据、虚拟现实 (vr)、增强现实 (ar)、区块链、添加剂制造、人工智能 (ai)、机器学习 (ml)、互联网协议版本 6 (ipv6)、网络物理系统和互联网事物(iot) 都代表着新的领域。这些技术有助于提高产品和服务质量以及组织绩效。在许多地区，互联网现在就像电力一样无处不在。组件相对便宜。一个强大的开源软件库生态系统意味着工程师解决问题的速度比 20 年前快 100 倍。这种数字化转型正引领我们走向互联智能自动化：智能、超连接代理部署在人类和机器合作的环境中，并利用数据来实现共享目标。这不是世界上第一次工业革命。事实上，这是它的第四次，它将带来的破坏性变化表明，我们需要对质量有新的看法来适应它。少

2018 年 10 月 17 日提交;最初宣布 2018 年 10 月。

日记本参考:radziwill, nicole m. (2018 年 10 月)。让我们了解数字：第四次工业革命正在重塑我们对质量的看法的许多方式。质量进步, asq，第 24-29 页

31. 建议: 1810.0753[pdf, ps,其他] Cs。直流

在物联网网关上实现多容器部署

作者:kodolui, csaba kiraly

摘要: 高级物联网 (iot) 应用中的严格延迟要求以及云数据中心的负载增加，促使人们转向更加分散的方法，实现了物联网数据的存储和处理通过部署多功能物联网网关，更贴近终端设备。但是，这些网关的资源受限性质和多样性对开发可广泛部署的应用程序构成了挑战。通过容器化 (一种轻量级虚拟化形式) 来克服这一挑战，它为广泛的硬件体系结构和物联网网关上的操作系统无关的应用程序部署提供了支持。本文讨论了容器化的体系结构方面，并研究了可用的容器化工具在物联网网关上下文中部署多容器的适用性。我们将容器化呈现在 agile 的背景下，这是一个基于多容器和微服务的物联网网关开源框架，是作为 horizon 2020 项目的一部分而开发的。我们对容器化服务进行研究，以执行设备发现、数据管理和云集成等常见网关功能，揭示了为物联网网关提供容器化环境在使用基础方面的优势用于容器内和跨容器性能优化的图像层次结构和图像分层。我们在本文的一组基准实验中对这些结果进行了说明。少

2018 年 10 月 4 日提交;最初宣布 2018 年 10 月。

评论:7 页, 6 个数字

32. 建议: 1810.07751[pdf,其他] Cs。直流

超越边缘的智能：对间歇嵌入式系统的推理

作者:graham gobieski, nathan beckmann, brandon lucia

摘要: 能量采集技术为未来的物联网应用提供了一个很有前途的平台。然而，由于在这些设备中，通信非常昂贵，应用程序将需要 "超越边缘" 的推理，以避免将宝贵的能量浪费在毫无意义的通信上。我们证明了应用程序性能对推理精度具有高度敏感的特性。不幸的是，准确的推理需要大量的计算和记忆，能量收集系统受到严重的资源限制。此外，能量收集系统间歇性地运行，经常停电，造成腐败，阻碍前进。本文克服了这些挑战，首次全面演示了能量采集系统的 dnn 推理。我们设计并实现了 sonic，这是一个具有专门 dnn 推理支持的间歇性感知软件系统。sonic 引入了循环延续，这是一种新的技术，极大地降低了保证像 dnn 推理这样的环路重代码的正确间歇性执行的成本。为了构建一个完整的系统，我们进一步介绍了 genesis，这是一种自动压缩网络以优化推理精度和能量的工具, tils，利用一些微控制器中可用的 simd 硬件来提高能效。sonic 和 tails 都保证了正确的间歇性执行，

而不会在不同的电源系统中进行任何手动调谐或性能损失。在市售微控制器上的三个神经网络中, sonic & amp; tails 比最先进的微控制器分别减少了 6.9x 和 12.2x 的推理能量。少

2018 年 9 月 28 日提交;最初宣布 2018 年 10 月。

33. **第: 1810.0730[pdf,其他] Cs。镍**

mqtt 的 basic 的实现与分析

作者:puneet kumar , behnam dezfouli

摘要: 传输和安全层协议对于确保双方之间可靠和安全的通信至关重要。这些协议必须是轻量级的, 因为**物联网**设备通常受到资源限制。遗憾的是, 现有的传输和安全层协议 (即 tcp/tls 和 TCP/TLS) 在**物联网**应用程序中使用时, 在连接开销、延迟和连接迁移方面存在不足。本文在研究了这些缺点的根本原因后, 展示了在**物联网**场景中使用 basic 如何获得更高的性能。基于这些观察结果, 并考虑到 mqtt 作为**物联网**应用层协议的普及, 我们将 mqtt 与 quic 集成。通过介绍开发的主要 api 和功能, 我们解释了连接建立和消息交换功能的工作原理。我们使用有线、无线和远程测试台评估了 mqttwquic 与 mqttwtcp 的性能。结果表明, mqttwsequic 将与经纪商交换的数据包数量减少了 56% 的连接开销。此外, 通过消除半开放连接, mqtwxquic 将处理器和内存使用率分别降低了 81% 和 48%。此外, 通过消除线头阻塞问题, 传递延迟最多减少 55%。我们还表明, 当发生连接迁移时, mqtwyquic 所经历的吞吐量下降大大低于 mqttwsp。少

2018 年 10 月 17 日提交;最初宣布 2018 年 10 月。

报告编号:scu-siolab-mqttquic-2018

34. **第 1810.07120[pdf, ps,其他] Cs。镍**

电视白空间联网的综合调查

作者:mahbubur rahman, Abusayeed Saifullah

摘要: 2008 年联邦通信委员会 (fcc) 在美国的裁决为电视空白频谱的无证运营提供了新的机会。电视空白上的网络协议通过提供更多的可用性、更宽的带宽和更远距离的通信, 有望克服现有短距离多跳无线体系结构和协议的缺点。电视空白协议是用于传感和监控、物联网 (**iot**)、无线宽带接入、实时、智能和互联社区以及智能公用事业应用的使能技术。在本文中, 我们对过去十年建立的协议以及新的挑战和今后工作的方向进行了回顾。据我们所知, 这是首次全面调查, 介绍和比较电视空白上的现有网络协议。少

2018 年 10 月 26 日提交;v1 于 2018 年 10 月 16 日提交;最初宣布 2018 年 10 月。

评论:19 页

35. **第 1810.7058[pdf,其他] Cs。铬**

屏蔽散点图: 通过反向散射帮助提高物联网安全性

作者:罗志清,王伟,曲军,姜涛,张谦

摘要: 轻量级协议和低功耗无线电技术为促进物联网 (**iot**) 进入我们的日常生活提供了许多机会, 而其简约的设计也使**物联网**设备容易受到许多主动攻击由于缺乏复杂的安全协议。最近的进展主张使用天线阵列来提取细粒度物理层特征, 以减轻这些主动攻击。然而, 它在**物联网**设备负担不起的能耗和硬件成本方面增加了负担。为了克服这种困境, 我们提出了 shieldcatter, 这是一个轻量级系统, 可将无电池的反向散射标签附加到单天线设备上, 以保护系统免受主动攻击。shieldcatter 的关键见解是有意创建多路径传播签名, 并谨慎部署反向散点图标记。这些签名可用于构造敏感的配置文件, 以确定信号到达的位置, 从而检测威胁。我们使用 usrp 和环境反向散射标签对 shieldcatter 进行原型设计, 以便在各种环

境中评估我们的系统。实验结果表明，即使攻击者距离合法设备仅 15 厘米，仅有三个反向散射标记的 shieldcatter 也能减轻 97% 的欺骗攻击尝试，同时仅在 7% 的合法的流量。少

2018 年 10 月 16 日提交;最初宣布 2018 年 10 月。

36. **修订: 1810.0870[pdf,其他] cs et**

网络物理系统的弹性物联网路线图

作者:denise ratasich, faiq khalid , florian geissler, radu grosu, muhammad shafique , ezio bartocci

摘要: 物联网 (**iot**) 是一个无处不在的系统，连接许多不同的设备----事物----可以从远处访问。由于有可能从远处监控物理环境，即**物联网**包含网络物理系统 (cps)，可靠性和安全性这两个概念紧密地交织在一起。动态性、异质性和复杂性的增加增加了系统的脆弱性，并对其对故障的反应能力提出了挑战。本文总结了现有的异常检测、容错和自愈调查的最新情况，并添加了许多其他适用于**实现物联网**弹性的方法。我们特别关注确保网络中数据完整性的非侵入性方法。此外，本文还提出了构建具有弹性**的 cps 物联网的**主要挑战。它进一步总结了我们的解决方案、正在进行的工作以及针对 "cps 值得信赖的**物联网**" 项目的未来工作。最终，此框架将应用于传输域中智能传感器基础结构的选定用例。少

2018 年 10 月 16 日提交;最初宣布 2018 年 10 月。

评论:预打印 (2018-09-25)

37. **第 1810.06057[pdf,其他] Cs。镍**

多伊 10.114/3278161.3278166

5g 应用程序: 要求、挑战和展望

作者:aaron yiding, maryjn janssen

摘要: 物联网 (**iot**) 应用对移动网络容量的需求不断增长，因此需要更好地了解 5g 网络的潜力和局限性。垂直应用领域，如智能移动、能源网络、工业**物联网**应用和 ar/vr 增强服务，都对 5g 网络的使用提出了不同的要求。某些应用程序需要低延迟，而其他应用程序则需要高带宽或安全支持。本文的目的是确定需求并了解 5g 驱动应用程序的局限性。我们回顾了应用领域，并列出了 5g 网络上提出的典型挑战和要求。一个主要的挑战将是开发一个能够动态适应波动的流量模式的网络体系结构，并适应各种技术，如边缘计算、基于区块链的分布式分类帐、软件定义的网络和虚拟。为了激发未来的研究，我们揭示了开放的问题，并强调需要使用 5g 应用程序进行试点，并采取切实的步骤，了解 5g 网络的配置以及在多个垂直行业中使用应用程序的情况。少

2018 年 10 月 14 日提交;最初宣布 2018 年 10 月。

评论:2018 年国际国际贸易研究中心会议出版物的作者版本

38. **建议: 1810.05937[pdf,其他] Cs。直流**

物联网应用程序的端到端服务级别协议规范

作者:awatif alqahtani, yinhaoli, pankesh patel, ellissolaiman, rajiv ranjan

摘要: 物联网 (**iot**) 承诺帮助解决与我们在智能城市、医疗保健监控和环境监控等应用领域的福祉相关的广泛问题。**物联网**利用边缘和云计算提供的计算能力和灵活性，带来了新的无线传感器使用案例。但是，此类应用程序中使用的软件和硬件资源必须正确且最佳地运行。特别是在资源故障可能非常关键的应用程序中。需要以反映物联网应用

程序域端到端性质的标准方式指定此类应用程序的性能要求 (sla)，这将考虑服务**质量** (qos)每个层中的指标，包括边缘、网络网关和云。在本文中，我们提出了一个概念模型，它捕获 sla 的关键实体及其关系，作为端到端 sla 规范和组合的前一步。服务级别目标 (slo) 术语也被视为表示 qos 约束。此外，我们还提出了一种新的 sla 语法，该语法考虑了工作流活动和**物联网**应用程序的多层次性质。因此，我们开发了一个用于 sla 规范和组合的工具，该工具可用作以机器可读格式生成 sla 的模板。我们通过包含 sla 语言比较分析的文献调查，并通过反映可用性研究的用户满意度结果，展示了建议的规范语言的有效性。少

2018 年 10 月 13 日提交;最初宣布 2018 年 10 月。

39. **建议: 1810.05891[pdf, ps,其他] cs. it**

无线供电物联网网络中的资源分配

作者:刘晓兰,秦志金,高悦，朱莉 a. 麦孔

文摘: 本文研究了无线供电**物联网**网络上行传输的有效资源分配。lora 被作为焦点网络的示例，但这项工作可以很容易地推广到其他无线电。在大量用户之间分配有限的资源，如频谱和能源资源，面临着严峻的挑战。我们首先考虑对无线供电用户进行分组，对于分配给同一通道的用户，将研究功率分配，以提高每个用户的吞吐量。具体而言，用户分组问题已被表述为多对一匹配游戏，将用户和频道视为两组自私的玩家，旨在最大限度地发挥各自的效用。针对用户分组问题，提出了一种低复杂度高效信道分配算法 (ecaa)。此外，还采用马尔可夫决策过程 (mdp) 对不可预知的能量到达和信道条件不确定性进行建模，提出了一种功率分配算法，以最大限度地提高在有限范围内的时间插槽累积吞吐量。通过这样做，我们可以将信道访问和动态功率分配决策进行本地分发给用户。仿真结果表明，与蛮力穷演法相比，所提出的 ecaa 方案能够在计算复杂度更低的情况下实现近乎最优的性能。仿真结果表明，与集中式离线方案相比，每个用户的分布式最优功率分配策略都有更好的性能。少

2018 年 10 月 21 日提交;v1 于 2018 年 10 月 13 日提交;最初宣布 2018 年 10 月。

评论:11 页, 8 个数字

40. **第: 1810.05886[pdf,其他] cs. it**

物联网网络中无线供电环境反向散射通信的最优时间调度方案

作者:刘晓兰,高悦,胡凤业

摘要: 本文研究了通过最大限度地提高频谱传感、射频能量采集 (rfh) 和环境反向散射通信 (abcom) 等不同模块的时间调度的优化方案。物联网 (**iot**)。我们首先考虑使用频谱传感与能量检测技术来检测高功率环境射频信号，然后与它们一起执行 rfh 和 abcom。具体而言，为了提高频谱传感效率，采用压缩传感的方法对宽带射频信号进行检测。提出了一个优化时间调度参数和功率分配比的联合优化问题，即由于 reh 和 abcom 同时工作而出现功率分配比。此外，还提出了一种通过分析后散射通信的中断概率来求反向散射通信的频谱传感阈值的方法。数值结果表明，利用频谱传感实现了传输速率较大的最优方案。证实了基于压缩传感的方法效率更高，随着网络运行时间的增加，其优越性变得更加明显。此外，还得到了最优调度参数和功率分配比。通过仿真，分析了后散射通信的中断概率，得到了用于后散射通信的频谱传感阈值。少

2018 年 10 月 13 日提交;最初宣布 2018 年 10 月。

评论:9 页, 13 位数字，物联网杂志

41. **第 1810.0804[pdf, ps,其他] Cs。镍**

通过 hetnet 中的上行链路资源分配和用户关联实现用户传输功率最小化

作者:umar bin farooq, umair sajid hashmi, junaid qadir, aliimran , adnan noor mian

摘要: 蜂窝物联网 (**iot**) 的普及与日俱增，数十亿的**物联网**设备将连接到互联网。其中许多设备的电池寿命有限，传输功率受到限制。蜂窝网络中的高用户功耗限制了 5g 中许多**物联网**设备的部署。为了能够纳入这些设备，5g 应辅之以降低用户功耗的战略和方案。因此，我们提出了一种新的联合上行用户关联和资源分配方案，在满足服务质量的同时，最大限度地降低用户的传输功率。我们分析了我们的双层异构网络 (hetnet) 方案，显示了我们算法的平均发射功率为-2.8 dbm 和 8.2 dbm，而在最先进的最大参考信号接收功率 (rsrp) 和信道单个偏移 (cio) 中，平均发射功率为 20 dbm 基于关联方案。少

2018 年 10 月 13 日提交;最初宣布 2018 年 10 月。

42. **第: 1810.05789[pdf,其他] cse**

交错中断驱动物联网项目的分析与分解

作者:孙玉霞,宋国,张成志,唐勇

摘要: 在物联网 (**iot**) 社区中，无线传感器网络 (wsn) 是实现无处不在的环境感知并为应用提供可靠服务的关键技术。无线传感器网络程序通常是中断驱动的，通过中断过程实例 (ipi，即中断处理逻辑的执行) 的协作来实现这些功能。然而，由于无线传感器网络程序的并发模型复杂，ipi 是复杂的交错，程序行为很难从源代码中断言。因此，为了提高无线传感器网络程序的软件质量，分离交错执行并开发各种基于 ipi 的程序分析技术 (包括离线和在线分析技术) 具有重要意义。作为这些技术的共同基础，迫切需要一种通用的高效实时算法来识别 ipi。但是，现有的实例识别方法不能满足需求。在本文中，我们首先正式定义了 ipi 的概念。接下来，我们提出了一种通用的 ipi 识别算法，并证明了该算法的正确性、实时性和有效性。我们还进行了比较实验，说明我们的算法在时间和空间上都比现有算法更有效。随着理论分析和实证研究的展示，我们的算法为基于 ipi 的物联网环境下无线传感器网络程序分析提供了基础。少

2018 年 10 月 12 日提交;最初宣布 2018 年 10 月。

43. **决议: 181005309[pdf, ps,其他] cs. it**

上行链路物联网流量的时空模型: 调度与随机存取悖论

作者:mohammad Gharbieh, hesham elsawy, hho-chanyang, ahmed bader , mohamed-slim alouini

摘要: 物联网 (**iot**) 是任何东西都将连接的范例。处理**物联网**预期生成的上行链路 (ul) 流量激增的主要方法有两种，即计划 ul (sc-ul) 和随机访问上行链路 (ra-ul) 传输。sc-ul 被认为是控制服务质量 (qos) 级别的可行工具，同时在任何 ul 传输之前在调度请求中产生一些开销。另一方面，ra-ul 是一种简单的单相传输策略。虽然这显然消除了调度开销，但对 ra-ul 的可扩展性了解甚少。在这一关键的结合点，迫切需要分析这两种范例的可伸缩性。为此，本文建立了一个时空数学框架，对 RA-UL 和 ra-ul 的性能进行了分析和评价。所开发的范式共同运用随机几何和排队理论。基于这样的框架，我们表明，"调度与随机访问悖论" 的答案实际上取决于操作场景。特别是，ra-ul 方案提供了较低的访问延迟，但可扩展性有限，即无法支持大量**物联网**设备。另一方面，sc-ul 传输更适合更高的设备强度和流量。少

2018 年 10 月 11 日提交;最初宣布 2018 年 10 月。

44. **第: 1810.04645[pdf,其他] Cs。镍**

工业物联网的安全性：以信息为中心的网络的案例

作者:michael frey, cenk gündoan, peter kietzmann, martine lenders, hauke petersen, thomas c.schmidt, felix Shzu-Juraschek, matthias wählisch

摘要: 工业生产工厂传统上包括用于监控或记录流程的传感器，以及在出现错误配置、故障或危险事件时能够采取纠正措施的执行器。随着**物联网**的出现，嵌入式控制器将这些 "东西" 连接到本地网络，这些网络通常是低功耗无线网络，并且通过网关从全球互联网连接到一些云。工业**物联网**中的网络传感器和执行器构成了一个关键子系统，同时经常在恶劣条件下运行。目前正在辩论如何以安全和有保障的方式处理关键工业部件的联网问题。本文分析了 icn 在为工业安全系统中的约束控制器提供安全、可靠的网络解决方案方面的潜力。我们展示了广泛的工业环境 (如炼油厂) 中的危险气体传感，并与基于 ip 的方法 (如 coap 和 mqtt) 进行了比较。我们的研究结果表明，以内容为中心的安全模型以及增强的 dos 电阻是在安全关键**型工业物联网**中部署以信息为中心的网络的重要论据。对用于内容安全的 riot 操作系统上的加密工作的评估揭示了它在常见部署方案中的可行性。少

2018 年 10 月 10 日提交;最初宣布 2018 年 10 月。

45. **第: 1810.4442[pdf,其他] Cs。镍**

边缘切削吞吐量：在雾计算中的应用感知位置

作者:francescomaria faticanti, francesco de pellegrini, domenico siracusa, daniele santoro, silvio creti

摘要: 雾计算将云计算技术扩展到基础架构的边缘，使**物联网**应用程序能够以更低的延迟、位置感知和动态计算访问对象的数据。通过将工作负载从中央云转移到边缘设备，雾计算克服了通信瓶颈，避免了向中央云的原始数据传输，从而为下一代**基于物联网**的应用程序铺平了道路。本文研究了雾计算中应用的调度和放置，这是确保相关利益相关者盈利的关键。我们考虑这样一种情况，即新兴的微服务体系结构允许将应用程序设计为耦合微服务模块的级联。它导致了一个混合整数非线性问题，涉及对应用程序数据流和计算位置的约束。由于原问题的复杂性，我们采用了简化的版本，这是进一步解决使用贪婪算法。该算法是 fogatlas 平台的核心放置逻辑，fogas 平台是基于现有虚拟化技术的模糊计算平台。广泛的数值结果验证了该模型和所建议解决方案的可扩展性，表明它的性能接近于最佳解决方案，并且在我们的实际实现中，它相对于服务应用程序的数量进行了很好的扩展。少

2018 年 10 月 10 日提交;最初宣布 2018 年 10 月。

46. **第 1810.04408[pdf, ps,其他] cs. it**

物联网的频谱共享：一项调查

作者:张英昌,肖明

摘要: 物联网 (**iot**) 是一个很有前途的模式，可在 5g 及更高的地方容纳大规模的设备连接。为了为未来**的物联网**铺平道路，应该提前规划频谱。由于可用频谱资源的稀缺性，频谱共享是**物联网**的理想解决方案。特别是，移动运营商倾向于利用当前蜂窝网络的现有标准和基础设施，并在许可的蜂窝频谱内部署**物联网**。然而，专有公司更愿意在无证范围内部署**物联网,**以避免任何许可费。在本文中，我们提供了一项关于在许可的蜂窝频谱和未授权频谱中部署的流行**物联网**技术的调查。值得注意的是，重点将放在频谱共享解决方案上，包括共享频谱、干扰模型和干扰管理。为此，我们讨论了不同**物联网**技

术的优点和缺点。最后，我们确定了未来**物联网**面临的挑战，并提出了潜在的研究方向。少

2018 年 10 月 10 日提交;最初宣布 2018 年 10 月。

47. **第: 1810.04118[pdf,其他] Cs。镍**

多伊 10.1109/JIOT.2017.2712560

支持物联网和智慧城市服务的半监督深度强化学习

作者:Mohsen mohamadi, ala al-fuqaha, mohsen guizani, jun-seok oh

摘要: 智能服务是智能城市和物联网 (**iot**) 生态系统的重要组成部分，在这些生态系统中，通过感官数据获得和改善服务背后的智能。提供大量培训数据并不总是可行的;因此，我们需要考虑其他方法，以纳入未标记的数据以及。近年来，深度强化学习 (drl) 在多个应用领域取得了巨大的成功。它是一种适用于**物联网**和智能城市方案的方法，在这种情况下，自动生成的数据可以通过用户的反馈进行部分标记，以便进行培训。本文提出了一种适合智能城市应用的半监督深层强化学习模型，该模型同时消耗标记和未标记的数据，以提高学习代理的性能和准确性。该模型利用变分自动编码器 (vae) 作为推断引擎，用于推广最优策略。据我们所知，所提出的模型是首次将深度强化学习扩展到半监督范式的研究。作为智能城市应用的案例研究，我们关注智能建筑，并将该模型应用于基于 ble 信号强度的室内定位问题。室内本地化是智能城市服务的主要组成部分，因为人们在室内环境中花费大量时间。我们的模型学习了最佳的行动策略，从而对目标位置进行了密切的估计，与监督下的 drl 模型相比，与目标的距离提高了 23%，获得的奖励至少增加了 67%。少

2018 年 10 月 9 日提交;最初宣布 2018 年 10 月。

评论:11 页, 7 个数字。接受在 ieee 物联网杂志上发表

日记本参考:ieee 物联网杂志，第 5 卷，第 2 期, 2018 年

48. **第: 1810.3822[pdf,其他] Cs。镍**

用于控制物联网物理系统的软件定义体系结构

作者:ala ' darabseh, nikk 组织 m. freris

摘要: 基于软件定义的原则，我们提出了一个完整的网络物理系统 (cps) 和物联网 (**iot**) 应用架构，并强调了与可扩展性、灵活性、鲁棒性、互操作性、和网络安全。我们的设计特别利用智能代理所拥有的计算单元，这些单元可用于分散控制和网络内数据处理。我们以系统可编程的方式描述吸收一组组件 (如传感器、执行器、控制器和协调器) 的数据流、通信流和控制流。我们特别致力于分散决策，将控制扩展到多个层次。此外，我们还提出了一个中间件层，用于封装在高度动态环境中实现时间关键的操作的单元和服务。我们进一步发现了网络攻击的多种漏洞，并集成了软件定义的解决方案，以实现恢复能力、检测和恢复。在这一权限中，几个控制人员合作，以自我调整的方式识别和应对安全威胁和异常情况。最后，我们说明了数值模拟，以支持 cps 和**物联网**软件定义设计的优点。少

2018 年 10 月 9 日提交;最初宣布 2018 年 10 月。

49. **第: 1810.2749[pdf,其他] Cs。直流**

演示摘要: 用于指定物联网应用的服务级别协议的工具包

作者:awatif alqahtani, pankesh patel, ellis solaiman, rajiv ranjan

摘要: 今天，我们看到物联网 (**iot**) 在各种应用领域的应用，如医疗保健、智能家居、智能汽车和智能城市的智能 x 应用。基于**物联网**和云计算的应用程序数量预计将在未来几年内迅速增加。基于**物联网**的服务必须满足保证的服务质量 (qos) 水平，以满足用户的期望。通过使用服务级别协议 (sla) 指定 qos 约束来确保 qos 至关重要。因此，作为实现 sla 管理的第一步，必须以机器可读的格式提供 sla 规范。在本文中，我们演示了一个用于**为物联网**应用创建 sla 规范的工具包。该工具包用于简化**捕获物联网**应用程序需求的过程。我们展示了使用远程运行状况监视服务 (rhms) 使用的工具包的演示。该工具包支持以下方面: (1) 在应用程序级别指定**物联网**应用程序的服务层目标 (slo);(2) 指定**物联网**应用程序的工作流程活动;(3) 将每个活动映射到所需的软硬件资源，并指定 slo 的约束和所需硬件和软件的其他配置相关指标;(4) 以 json 格式创建组合的 sla。少

2018 年 10 月 5 日提交;最初宣布 2018 年 10 月。

50. 建议: 1810.02090[pdf] Cs。铬

shakedown: 基于编译器的移动目标保护，用于工业物联网设备上的面向回报的编程攻击

作者:fady copty, francisco hernandez, dov murik, olmo rayón

摘要: 网络犯罪分子使用面向返回的编程技术来攻击系统和**物联网**设备。虽然防御已经开发出来，但并非所有防御都适用于受约束的设备。我们介绍 shakedown，这是一个编译时随机生成工具，它创建了多个版本的二进制文件，每个版本都有不同的内存布局。针对一个设备开发的攻击将无法在另一个具有不同内存布局的设备上工作。我们在工业**物联网**设备上测试了 shakedown，并显示其正常功能在漏洞被阻止时保持不变。少

2018 年 10 月 11 日提交;v1 于 2018 年 10 月 4 日提交;最初宣布 2018 年 10 月。

评论:第一次 smesec 研讨会-希腊伊拉克利翁 (2018 年)

51. 建议: 1810.01839[pdf,其他] Cs。直流

多伊 10.1109/CloudCom.2016.0082

cloud4iot: 面向物联网的异构、分布式和自主云平台

作者:daniele pizzolli, giuseppecossu, daniele santoro, luca capra, corentin dupont, dukas charalampos, francesco de pellegrini, fabio antonelli, silvio 克雷蒂

摘要: 我们引入 cloud4iot，这是一个提供**自动部署**、编排和动态配置的平台，支持用于数据处理和分析的软件组件和数据密集型应用程序，从而实现即插即用集成新的传感器对象和动态工作负载可扩展性。cloud4iot 在**物联网**环境中实现了基础架构作为代码的概念: 它使**物联网**运营具有云服务的灵活性和弹性。此外，它还按照**物联网**技术的要求，将传统的集中式云架构转变为更分散和分散的计算范式，缩小了云计算与**物联网**生态系统之间的差距。因此, cloud4iot 的作用类似于雾计算、云或移动边缘云等解决方案所涵盖的角色。Cloud4IoThosts 的分层架构是一个中央云平台和多个支持专用设备的远程边缘云模块，即**物联网**网关，通过这些模块，平台可以访问新的传感器对象。总体而言，该平台的设计是为了支持**基于物联网**和数据密集型应用程序可能对低延迟、受限可用带宽或数据局部性提出特定要求的系统。cloud4iot 是基于几种开源技术构建的，用于集装箱化和**物联网**标准、协议和服务的实施。我们介绍了该平台的实现，并在两个不同的用例中进行了演示。少

2018 年 10 月 3 日提交;最初宣布 2018 年 10 月。

评论:这篇文章已被 ieee 接受出版

52. **第: 1810.01070[pdf] Cs。Hc**

游戏控制器: 用于增强数字游戏的中间件到程序输入

作者:kazutaka kuihara, nobuhiro doi

摘要: 本研究提出中间件--gamecoliglerizer, 它允许用户将物联网 (**iot**) 设备、web 服务和人工智能 (ai) 的应用的流程结合起来, 并将它们转换为游戏控制操作, 将其转换为增强现有的数字游戏。该系统通过使用各种设备和信息来源作为游戏的输入, 促进了新娱乐形式的轻松尝试和错误开发和游戏化的配置。GameControllerizer 由一个可视化的编程元素组成, 该元素使用 node-red 工具, 允许用户轻松地编程, 将不同格式的信息转换为游戏的输入, 并包含一个游戏输入仿真元素, 其中硬件和基于软件的仿真为游戏设备生成输入。业绩评估和各种使用案例的建议提供了该系统有用性的证据。少

2018 年 10 月 2 日提交;最初宣布 2018 年 10 月。

53. **建议: 1810.01069[pdf,其他] Cs。简历**

云追逐者: 低计算功率器件的实时深度学习计算机视觉

作者:罗正义,奥斯汀·斯莫尔,利亚姆·杜根,斯蒂芬·莱恩

摘要: 物联网 (**iot**) 设备、移动电话和机器人系统由于其有限的计算能力, 往往被剥夺了深度学习算法的强大功能。然而, 为了提供应急、家庭援助、监控等时间关键服务, 这些设备往往需要对其相机数据进行实时分析。本文试图通过利用云的计算能力, 提供一种可行的方法, 将基于高性能深度学习的计算机视觉算法与低资源、低功耗设备集成。通过将计算工作卸载到云, 无需专用硬件就可以在现有的低计算能力设备上启用深层神经网络。基于树莓派的机器人 "云追逐者" 旨在展示使用云计算执行实时视觉任务的强大功能。此外, 为了减少延迟和提高实时性能, 提出了将实时视频帧传输到云中的压缩算法并进行了评估。少

2018 年 10 月 2 日提交;最初宣布 2018 年 10 月。

评论:2008 年第十一届机器视觉国际会议

54. **第: 1810.447[pdf,其他] Cs。镍**

探索 nb-iot 的性能边界

作者:borja martíez, fer 兰 adelantado, andrea bartoli, xavier vilajosana

文摘: **nb-iot** 刚刚成为 lpwan 社区。与大多数竞争对手不同的是,**nb-iot** 并不是真正从干净的床单中诞生的。事实上, 它与 lte 紧密相连, 它从 lte 继承了它的许多特征, 这些特征无疑制约了它的行为。本文从用户的角度对该技术的核心特征进行了实证研究, 分析了能耗、可靠性和延迟等关键特征。结果表明, 其在能源方面的性能是可比的, 甚至比 lora 这样的 lpwan 参考技术 (lra) 平均优于, 其额外的好处是保证交付。然而, 在能源支出和网络延迟方面观察到的高度变异性使人们对其是否适合某些应用提出了疑问, 特别是那些受服务级协议制约的应用。少

2018 年 10 月 1 日提交;最初宣布 2018 年 10 月。

55. **第 1810.0027[pdf,其他] Cs。镍**

多址边缘计算的五大驱动力

作者:madhusanka liyanage, pawani porambage, aaron yi ding

摘要: 多址边缘计算 (mec) 技术的出现旨在将云计算能力扩展到无线接入网络的边缘。mec 提供对无线网络资源的实时、高带宽、低延迟访问，使运营商能够将其网络开放到新的生态系统和价值链。此外，它还将为未来第五代 (5g) 无线系统的设计提供新的见解。本文介绍了五项关键技术，包括网络功能优化 (nfv)、软件定义网络 (sdn)、网络切片、以信息为中心的网络 (icn) 和物联网 (**iot**)，这些技术强化了 mec 及其采用。我们的目标是在 5g 环境中提供 mec 和这五种驱动技术之间的关联性，同时确定开放的挑战、未来的方向和有形的集成路径。少

2018 年 10 月 1 日提交;最初宣布 2018 年 10 月。

评论:提交给 ieee 通信杂志

56. **第: 1810.00773[pdf,其他] Cs。镍**

mqtt +: 增强的语法和代理功能，用于数据筛选、处理和聚合

作者:riccardo giambona, alessandro e. c.redondi , matteo cesana

文摘: 在过去的几年里，消息队列遥测传输 (mqtt) 发布/订阅协议成为**物联网**、m2m 和无线传感器网络应用的实际标准通信协议。这种流行主要是由于客户端的协议极其简单，适用于低成本和资源受限的边缘设备。其他不错的功能包括非常低的协议开销，非常适合有限的带宽方案，支持不同的服务质量 (qos) 和许多其他。但是，当边缘设备有兴趣对多个客户端发布的数据执行处理操作时，使用 mqtt 可能会导致最终设备的网络带宽使用率高和能耗高，这在资源中是不可接受的受约束的方案。为了克服这些问题，本文提出了 mqtt +，它提供了一种增强的协议语法，并通过数据过滤、处理和聚合功能丰富了 pub/sub 代理。mqtt + 从开源 mqtt 代理开始实现，并在不同的应用程序方案中进行评估。少

2018 年 10 月 1 日提交;最初宣布 2018 年 10 月。

57. **建议: 1810.00720[pdf,其他] cs. it**

物联网网络联合活动检测与信道估计: 相位转换与计算估计交易

作者:姜涛,石元明,张军,哈立德 b.

摘要: 对于物联网 (**iot**) 网络而言，大规模设备连接是一个关键的通信挑战，因为它由大量具有零星流量的设备组成。在每个一致性块中，服务基站需要识别有源设备，估计其通道状态信息，以便进行有效的通信。利用数据传输的稀疏模式，提出了一种结构群稀疏估计方法，用于同时检测有源器件并估计相应的信道。此方法显著减少了签名序列长度，同时支持大规模**的物联网**访问。为了确定最优签名序列长度，我们研究了群稀疏估计问题的相变行为}。具体而言，当签名序列长度超过阈值时，可以很有可能成功地估计用户活动;否则，它失败的概率很高。利用圆锥积分几何理论对相变区的位置和宽度进行了表征。我们进一步开发了一种平滑方法，在给定的时间预算下解决高维结构化估计问题。这是通过在平滑参数、签名序列长度和估计精度等方面对收敛速度进行尖锐的表征来实现的，从而在估计精度和计算成本之间进行权衡。数值结果说明了我们理论结果的准确性和平滑技术的好处。少

2018 年 10 月 1 日提交;最初宣布 2018 年 10 月。

58. **建议: 1810.00349[pdf,其他] Cs。铬**

idmob: 区块链上的物联网数据市场

作者:kazm röfat zylmaz, mehmet doáan, arda yurdakul

摘要: 如今，物联网 (**iot**) 设备是数据生成的强大动力，其数量不断增加，并具有广泛的渗透率。同样，人工智能 (ai) 和机器学习 (ml) 解决方案也正被集成到各种服务中，使产品变得更加 "智能"。这些技术的核心是 "数据"。**物联网**设备供应商应该能够跟上不断提高的吞吐量，并提出新的业务模式。另一方面，如果培训数据多样化且丰富，ai/ml 解决方案将产生更好的结果。在本文中，我们提出了一个基于区块链、分散和无信任的数据市场，在这个**市场上，物联网**设备供应商和 ai/ml 解决方案提供商可以进行交互和协作。通过促进透明的数据交换平台，将使获得同意的数据的机会民主化，针对最终用户的服务种类将增加。提出的数据市场是作为一个智能合同在以太区块链上实现的，群被用作分布式存储平台。少

2018 年 9 月 30 日提交;最初宣布 2018 年 10 月。

评论:在 2018 年 6 月 20 日至 22 日举行的区块链技术密码谷会议 (cvcbbt 2018) 上提交-已出版版本可能有所不同

59. 第 1810.00300 [pdf, ps,其他] Cs。镍

多伊 10.1109/TGCN.2018.2873783

认知-lpwan：在混合低功耗广域网中实现智能无线服务

作者:陈敏,苗一明,辛健,王晓飞,伊兹托克·胡马尔

摘要: 物联网 (**iot**) 通信技术的不断发展和人工智能 (ai) 的逐渐成熟，带来了强大的认知计算能力。用户现在可以在智能城市、绿色**物联网**和异构网络中获得高效、便捷的智能服务。ai 已应用于各个领域，包括智能家庭、先进的医疗、自动驾驶和情感互动。本文重点介绍了当前的无线通信技术，包括蜂窝通信技术 (4g、5g)、具有无照频谱的低功耗广域 (lpwa) 技术 (lora、sigfox) 和 3gpp 支持的其他 lpwa 技术与授权频谱 (ec-gsm、lte-m、nb-iot) 合作。我们提出了一个认知低功耗广域网络 (认知-lpwan) 架构，以保障异构**物联网**中稳定高效的通信。为了确保用户能够高效、方便地使用 ai，我们实现了各种 lpwa 技术来保护网络层。此外，为了平衡异构**物联网**设备的需求和通信延迟和能耗，我们从交通控制的角度出发，提出了支持 ui 的 lpwa 混合方法。该算法为无线通信技术、智能应用和服务的选择提供了智能控制。作为一个例子，我们考虑了 aiwac 情感交互系统，建立了认知-lpwan，并测试了提出的启用 ai 的 lpwa 混合方法。实验结果表明，该方案能够满足通信延迟应用的要求。认知-lpwan 选择适当的通信技术，以获得更好的交互体验。少

2018 年 9 月 29 日提交;最初宣布 2018 年 10 月。

日记本参考:2018 年 ieee 绿色通信和网络交易

60. 第 1810.00281 [pdf,其他] cs. cy

基于社区的物联网安全

作者:朱全燕,斯特凡·拉斯,彼得·沙特纳

摘要: 随着越来越多的设备可以连接到互联网，服务的数量却急剧增加，但也有很多威胁。安全往往是功能和舒适性背后的次要问题，但问题已经得到承认。尽管如此，随着许多**物联网**设备的部署，安全性将逐步实现，并通过应用程序和**物联网**软件的更新、修补程序和新版本实现。虽然这些更新可以安全地从应用商店中检索，但问题是通过越狱的设备和互联网上出现的各种不受信任的来源引发的。既然黑客攻击通常是社区的努力？如今，安全也可能成为社区的目标。挑战是多方面的,**物联网**设备安全性薄弱或缺失的一个原因是其计算能力薄弱。在本章中，我们讨论了一种基于社区的安全机制，在

这种机制中，设备在安全软件管理中相互帮助。我们讨论了社区形成的游戏理论方法和在**物联网**设备社区内完成正版软件部署的轻量级加密方法。少

2018 年 9 月 29 日提交;最初宣布 2018 年 10 月。

61. 第 1810.00179[pdf,其他] Cs。直流

多伊 10.1109/CloudCom.2017.62

雾：在雾计算环境中的工作负载业务流程的平台

作者:daniele santoro, daniel zozin, daniele pizzolli, francesco de pellegrini, silvio Cretti

摘要: 本文介绍了基于开源技术的架构框架和软件平台 fgy。fgy 负责协调应用程序工作负载、协商资源并支持多层、分布式、异构和分散的云计算系统的**物联网**操作。fogy 是为 5g 网络和**物联网**等新兴领域量身定制的，这些领域要求按照 fog 计算模式，将资源和服务分布在靠近数据源和用户的位置。fagy 为基础设施所有者和租户 (即应用程序提供商) 提供了一个平台，提供协商、调度和工作负载放置的功能，同时考虑到传统要求 (例如基于 ram、cpu、磁盘) 和非传统的 (例如基于网络) 以及对地点和访问权的多样化限制。在不久的将来，fgy 模型也可以考虑资源的经济学和定价问题。figgy 在基础设施所有者和租户的需求之间找到权衡的能力，在满足应用程序要求的同时高效和优化地使用基础设施，并通过视频中的三个用例得到证明监控和车辆跟踪环境。少

2018 年 9 月 29 日提交;最初宣布 2018 年 10 月。

评论:这篇文章已被 ieee 接受出版

62. 第 xiv:1800.11120[pdf,其他] Cs。镍

music 的案例：移动城市传感应用的可编程物联网框架

作者:shiva r. iyer, soumie kumar, kate boxer, fatima zarinni, lakshminarayanan subramanian

文摘: 本文介绍了 music 的案例，这是一个用于构建分布式移动物联网应用的城市传感分布式**移动物**联网框架。移动城市传感、推理和控制 (music) 框架是针对静态或移动传感器的分布式集合共同完成城市传感任务的情况而进行的背景。music 平台专为以城市为中心的传感应用而设计，如用于道路交通监测的移动电话上的位置传感、空气质量传感和使用远程摄像机进行城市质量监测。这个可编程系统在一个高级别，由几个小传感器放置在一个城市的移动车辆和一个集中控制器，作出传感的决定，以实现某些明确的目标，如改善空间覆盖的传感和热点的检测。该系统是可编程的，因为我们的框架允许一个人通过编写用于传感的自定义控制逻辑来创建自定义智能系统。我们的贡献有两个方面--后端软件堆栈，可实现分布式设备和可编程性的集中控制，以及在实际功耗和网络约束的情况下实现智能控制的算法。我们简要介绍了建立在 music 堆栈之上的三种不同的城市传感应用。少

2018 年 9 月 28 日提交;最初宣布 2018 年 9 月。

评论:8 页两列格式，包括参考，5 个数字，5 个代码列表，格式化的提交

63. 第 xiv:1809.775[pdf,其他] Cs。铬

自动僵尸捕手：基于块链的物联网 p2p 僵尸网络检测

作者:gokhan sagirlar, barbara carminati , elena ferrari

摘要: 通常，僵尸网络是被入侵的互联网计算机的集合，由攻击者出于恶意目的进行控制。为了提高攻击的成功机会和防御机制的恢复能力，现代僵尸网络通常采用分散的

p2p 结构。在这里,**物联网**设备发挥着至关重要的作用，成为恶意方执行攻击的主要工具之一。值得注意的例子是 ddos 对 krebs 的安全和 dyn 的攻击，这些攻击是由**僵尸网络的物联网**设备执行的。我们向**检测物联网**中的 p2p 僵尸网络迈出了第一步，提出了 autobcatcher 的建议，其设计是出于同一僵尸网络的机器人经常相互通信并形成社区的考虑。因此，autbotcatcher 的目的是动态分析根据 iot 设备的**网络**流量形成的设备社区，以检测僵尸网络。autofcatcher 利用许可的拜占庭容错 (bft) 区块链，将其作为状态转换机器，允许一组事先确定的当事方在没有信任的情况下进行协作，以便执行协作和动态僵尸网络检测。收集和审核**物联网**设备的网络流量，将其作为区块链交易。本文重点介绍了 autbotcatcher 的设计，首先定义了 autbotcatcher 的区块链结构，然后讨论了其组成。少

2018 年 9 月 27 日提交;最初宣布 2018 年 9 月。

评论:出版于 ieee cic 2018

64. **第: 1809.10492[pdf,其他] Cs。铬**

雾计算对物联网安全的影响

作者:ismail butun, alparslan sari, patrik sterberg

摘要: 最近,**物联网**设备和传感器的使用迅速增加，这也导致数据生成 (信息和日志)、带宽使用和相关现象的增加。据我们所知，雾计算与**物联网**集成的标准定义正在出现。这种整合将为研究人员带来许多机会，特别是在构建网络安全相关解决方案的同时。在本研究中，我们调查了雾计算与**物联网**的集成及其含义。我们的目标是找出并强调**问题，特别是物联网使用雾**计算时出现的与安全相关的问题。根据我们的发现，尽管这种集成似乎不是微不足道和复杂的，但它的好处比影响更多。少

2018 年 9 月 27 日提交;最初宣布 2018 年 9 月。

评论:5 页，会议论文，将刊登在《 2019 年 icce 论文集》上, ieee 第 37 届消费电子国际会议 (icce), 2019 年 1 月 11 日至 13 日，拉斯维加斯，美国 nv

65. **第 1809. 10387[pdf,其他] Cs。铬**

多伊 10.1109/TSUSC.2018.2808455

使用蓝牙识别可穿戴设备

作者:hidayet aksu, a. selcuk Uluagac, elizabeth s.bentley

摘要: 随着可穿戴设备 (如智能手机) 在消费电子市场的兴起，确保这些可穿戴设备的安全至关重要。但是，当前的安全机制仅侧重于验证用户而不是设备本身。事实上，可穿戴设备可以是 (1) 具有正确凭据的未经授权的可穿戴设备，可访问有价值的系统和网络, (2) 被动内部人或外部可穿戴设备，或 (3) 信息泄漏的可穿戴设备。通过机器学习进行指纹识别可以提供必要的网络威胁情报来解决所有这些网络攻击。在本文中，我们介绍了一种以蓝牙经典协议为中心的可穿戴式指纹技术，这是可穿戴设备和其他**物联网**设备常用的协议。具体而言，我们提出了一个非侵入性可穿戴设备识别框架，该框架在分类过程的训练阶段采用了 20 种不同的机器学习 (ml) 算法，并为测试阶段选择了性能最佳的算法。此外，我们还评估了拟议的可穿戴指纹技术在真正的可穿戴设备上的性能，包括各种现成的智能手机。我们的评估证明了该技术提供可靠的网络威胁情报的可行性。具体而言，我们的详细精度结果显示，使用蓝牙经典协议识别可穿戴设备的精度平均为 98.5%、98.3% 和召回率。少

2018 年 9 月 27 日提交;最初宣布 2018 年 9 月。

评论:15 页, 10 个数字

日记本参考:ieee 可持续计算交易, 2018

66. 决议: 1809.10289[pdf,其他] cs. it

高斯跟踪中的依赖性导致的隐私渐近损失

作者:nazanin takbiri, ramin soltani, dennis l.goeckel, amir houmansadr, hossein Pishro-Nik

摘要: 物联网 (**iot**) 的快速增长要求采用隐私保护技术来保护用户的敏感信息。即使用户跟踪是匿名的, 也可以使用统计匹配来推断敏感信息。在前面的工作中, 我们已经为用户跟踪是离散随机变量的实例化, 并且对手只知道依赖关系图的结构, 即是否连接了每对用户的情况建立了隐私要求。本文考虑了数据跟踪是高斯随机变量的实例化, 对手不仅知道图的结构, 而且知道成对相关系数的情况。我们建立了匿名化的要求, 以阻止这种统计匹配, 这表明 (重大) 的程度, 在多大程度上, 对等相关系数的知识进一步大大有助于对手打破用户匿名。少

2018 年 9 月 26 日提交;最初宣布 2018 年 9 月。

评论:提交给 ieee 无线通信和网络会议

67. 第 1809.10134[pdf,其他] Cs。铬

物联网中间件的中介策略和执行监视器

作者:juan carlos fuentes carranza, phillip w. l. fong

摘要: 基于事件的系统是许多基于云的物联网 (**iot**) 平台的核心。这种 broker 体系结构风格和发布者-订阅服务器设计模式的组合为智能设备之间的通信和协调提供了一种方式。这些基于云**的物联网**框架的当前设计缺乏以下措施: (i) 保护设备免受恶意云断开连接的影响, (ii) 在通信方之间实施信息流控制, 以及 (iii) 在被破坏的设备的存在。在这项工作中, 我们建议扩展 fiege 等人基于模块化事件的系统架构, 以纳入中介策略和执行监视器, 从而应对上述三种保护挑战。我们形式化了保护方案的操作语义, 探讨了如何利用该方案来实施 blp 风格的信息流控制和 rbac 风格的保护域, 在开源的 mqtt 经纪商中实现了该方案, 并对保护机制对性能的影响。少

2018 年 9 月 27 日提交;v1 于 2018 年 9 月 26 日提交;最初宣布 2018 年 9 月。

68. 第 xiv:1809. 099772[pdf,其他] Cs。直流

物联网、雾与云连续: 集成与挑战

作者:luiz f. bittencourt, roger immich, rivs sakellariou, nelson l.s. da fonseca , edmundor. m. madeira, marilia cururado, leandrovas, luiz da silva, craig lee, omer rana

摘要: 预计未来十年, 物联网对计算能力和存储的需求仍将呈上升趋势。因此, 网络边缘的设备生成的数据量也将增加。虽然云计算已经成为获取计算和存储作为对许多应用程序的服务的一种既定而有效的方式, 但它可能不适合**处理来自物联网**设备的大量数据并在很大程度上实现异构应用要求。雾计算是在**物联网**和云之间发展起来的, 它提供了一种计算能力层次结构, 可以从**物联网**设备收集、聚合和处理数据。将雾和云结合起来可能会减少向云的数据传输和通信瓶颈, 也有助于减少延迟, 因为雾计算资源存在于更接近边缘的地方。本文研究了这个**物联网**-flo-cloud 生态系统, 并从不同的方面提供了文献综述: 如何组织它, 如何处理管理问题, 以及应用程序如何从中受益。最后, 我们提出了**物联网**-flo-cloud 基础架构中尚未解决的具有挑战性的问题。少

2018 年 9 月 26 日提交;最初宣布 2018 年 9 月。

评论:预印版本-将发表在 elsevier 的物联网杂志

69. 第 1809. 09870[pdf,其他] cs. cy

一种基于角色的在物联网中协调紧急配置的方法

作者:radu-casian mihailescu, romina spalazzese, clclt heyer, paul davdsson

摘要: 物联网 (**iot**) 被设想为一个全球互联的网络，支持无处不在的机器对机器 (m2m) 通信。由于在未来几年将连接数十亿的传感器和设备,**物联网**被认为具有巨大的潜力，可以影响我们的生活方式，也可以影响我们的工作方式。但是，连接方面本身只考虑底层的 m2m 基础结构。为了正确支持工程**物联网**系统和应用程序，以无缝、自适应和动态的方式协调异构的 "事物" 是关键，这样系统就可以表现出目标导向的行为并采取适当的行动.然而，事物之间的这种形式的交互需要采取以用户为中心的方法，绝不逃避用户的要求。为此，上下文化是该系统的一个重要功能，使其能够推断用户活动，并在没有有意命令的情况下提示用户提供相关信息和互动。在本文中，我们提出了一个基于角色的连接系统应急配置模型，作为对**物联网**系统进行建模、管理和推理的一种方法，包括用户与它们的交互。我们特别注重集成用户视角，以指导新出现的配置，从而使系统目标与用户的意图保持一致。我们讨论了相关的科学和技术挑战，并提供了几个应用案例，概述了紧急配置的概念。少

2018 年 9 月 26 日提交;最初宣布 2018 年 9 月。

评论:第二次代理商互联网国际研讨会论文集 @AAMAS2017

70. 第 1809. 09846[pdf] Cs。Hc

共睡: 设计基于工作场所的健康计划，以提高对睡眠不足的认识

作者:bing zhai, yu guan , kyle montague, stuart nicolson, patrick olivier, jason ellis

摘要: 睡眠不足是一个公共卫生问题。睡眠不足不仅会损害我们的身体免疫系统，还会降低他们保持认知能力的能力。在以工作为基础的健康方案中，对睡眠不足的认识没有得到广泛调查。在这项研究中，该项目与当地一家制造公司的 9 名参与者进行了合作，以提高这一认识。通过部署探头和访谈，确定了睡眠不足的常见原因。这项研究产生了智能**物联网**工作场所的设计理念，以跟踪和分享白天与睡眠相关的活动。通过自下而上的设计方法，参与者从不同的权力关系角度考虑睡眠数据的使用，包括意外使用睡眠进行疲劳风险管理和评价员工绩效。少

2018 年 9 月 26 日提交;最初宣布 2018 年 9 月。

评论:11 页, 3 个数字

71. 第 1809.09520[pdf,其他] Cs。Sy

多伊 10.1109/JIOT.2018.2868226

以物联网设备的收费服务质量保证获得最大化

作者:文芳,张庆清,刘明清,刘庆文, 夏鹏飞

摘要: 谐振波束充电 (rbc) 是一种很有前途的无线功率传输 (wpt) 技术，可为物联网 (**iot**) 设备提供远程、高功率、移动和安全的无线功率。点对点 (ptmp) rbc 系统可以同时为多个接收器充电，类似于 wifi 通信。为了保证每个接收者的充电服务质量 (qocs)，最大限度地提高 ptmp rbc 服务的整体收益，我们制定了充电定价策略 (cps)，并开发了高优先充电 (hpc) 调度算法来控制充电顺序和功率分配。每个接收器都被分配一个优先级，该优先级根据其充电状态 (soc) 和指定的充电功率动态更新。优先级较高的接收器计划在每个时段收费。提出了基于接收机 soc、放电能量和各种相关参数的

hpc 算法伪编码。通过仿真分析，证明了 hpc 算法比循环充电 (rrc) 调度算法能获得更好的 qocs 和收益。在性能评价的基础上，我们说明了改进 ptmp rbc 服务的方法是: 1) 将接收机数量限制在合理的范围内, 2) 尽可能延长充电时间。总之, hpc 调度算法提供了一种实用的策略，可以利用每个接收者的 qocs 保证，最大限度地提高 ptmp rbc 服务的收益。少

2018 年 9 月 25 日提交;最初宣布 2018 年 9 月。

72. 第 xiv: 180909 470[pdf, ps,其他] Cs。镍

SS5G: 延迟和节能 lora 网络的碰撞解决协议

作者:nancy el rachkidy,亚历山大 guitton, megumi kaneko

摘要: 未来的 5g 和物联网 (**iot**) 应用将严重依赖低功耗无线局域网 (lpwan) 等远程通信技术。特别是，建立在 lora 物理层上的 lorwan 正在聚集来自学术界和业界的越来越多的兴趣，以实现低成本、节能的**物联网**无线传感器网络，例如在广泛领域进行环境监测。虽然它的通信范围可能会上升到 20 公里，但在 lorwan 中，可实现的比特率被限制在每秒几千比特。在发生碰撞的情况下，由于数据包丢失和重新传输，感知速率进一步降低。首先，为了减轻碰撞的有害影响，我们提出了一种解码算法，能够解析多个叠加的 lora 信号。我们提出的方法利用了叠加信号的轻微去同步和 lora 物理层的具体特征。其次，我们设计了一个完整的 mac 协议，实现了碰撞分辨率。仿真结果表明，该方法在系统吞吐量、能效和时延等方面均优于传统的 lorwan。这些结果表明，我们的方案非常适合 5g 和**物联网**系统，因为它们的主要目标之一是在这些性能目标之间提供最佳的权衡。少

2018 年 9 月 21 日提交;最初宣布 2018 年 9 月。

评论:arxiv 管理说明: 文本与 arxiv:1804.00503 重叠

73. 第 1809. 09379[pdf,其他] Cs。Sy

多伊 10.1109/JIOT.2018.2853546

物联网器件谐振梁充电中的公平调度

作者:文芳,张庆清,刘庆文,吴军,夏鹏飞

摘要: 谐振波束充电 (rbc) 是一种无线功率传输 (wpt) 技术，它可以为物联网 (**iot**) 设备提供大功率、远距离、移动和安全的无线充电。支持多个**物联网**设备同时充电是 rbc 系统的一大特点。为了优化多用户充电性能，应安排传输功率同时为所有**物联网**设备充电。为了保持所有**物联网**设备的工作时间尽可能长，为了公平起见，我们提出了第一接入第一收费 (ffc) 调度算法。然后，定量地制定了算法实现的调度参数。最后，考虑接收机数、发射功率和充电时间的影响，分析了 ffc 调度算法的性能。在分析的基础上，总结了提高多 **iot** 设备 wpt 性能的方法，包括限制接收机数量、增加传输功率、延长充电时间、提高单用户的充电效率。ffc 调度算法的设计和分析为多用户 rbc 系统提供了一个公平的 wpt 解决方案。少

2018 年 9 月 25 日提交;最初宣布 2018 年 9 月。

74. 建议: 1809. 9364[pdf,其他] Cs。Sy

多伊 10.1109/JIOT.2018.2867457，我的时间，我的

智能无线功率传输中的自适应谐振波束充电

作者:张庆清,文芳,熊明良,刘庆文，吴军,夏鹏飞

摘要: 谐振束充电 (rbc) 作为一种远程大功率无线功率传输 (wpt) 技术，可以为物联网 (**iot**) 中的设备远距离传输功率级功率。由于其开环架构, rbc 面临着提供动态电流和电压以优化电池充电性能的挑战。在 rbc 中，电池过充可能会导致能源浪费、热效应，甚至安全问题。另一方面，电池电量不足可能会导致充电时间延长和显著降低电池容量。本文提出了一种用于电池充电优化的自适应谐振光束充电 (arbc) 系统。基于 rbc, arbc 使用反馈系统根据电池首选充电值动态控制所提供的电源。此外，为了将接收到的电流和电压转换为与电池首选充电值相匹配, arbc 采用直流电流直流 (dc-dc) 转换电路。利用 rbc 功率传输的分析模型，得到了 arbc 近似线性闭式功率传输的端到端功率传输关系。因此，接收器上的电池首选充电电源可以映射到发射器上提供的电源，以进行反馈控制。数值计算表明，与 rbc 相比, arbc 可节省 61% 的电池充电能量和 53%-60% 的供电能量。此外，当 wpt 效率低下时, arbc 比 rbc 具有较高的节能增益。wpt 中的 arbc 类似于无线通信中的链路自适应。他们都在各自的领域发挥着重要作用。少

2018 年 9 月 25 日提交;最初宣布 2018 年 9 月。

评论:12 页, 24 位数字, ieee 物联网杂志

日记本参考:ieee 物联网杂志, 2018

75. 第 1809. 09315[pdf,其他] Cs。燃气轮机

基于物联网的众包的预算可行同行评级机制

作者:vikash kumar singh, sajal mukhopadhyay, fatos xhafa, aniruddh sharma

文摘 我们开发并扩展了最近在 "众包" 中设计异构任务分配问题机制的一系列工作。我们认为预算中的市场包括多个任务请求者和多个**物联网**设备作为任务执行器;每个任务请求者都被赋予了一个单独的任务以及公开的预算。此外，每个 **iot** 设备都有用于执行任务和质量的估值，这些成本是私有的。在这种情况下，目标是为每个任务**选择物联网**设备的子集，以便在达到阈值质量的同时，在分配的预算配额范围内支付的总款项。为了确定**物联网**设备的未知质量，我们使用了对等分级的概念。在本文中，我们精心构建了一个真实的预算可行机制;即 tube-tap 针对正在调查的问题，这也使我们能够获得有关**物联网**设备质量的真实信息。进行模拟是为了衡量我们提出的机制的有效性。少

2018 年 10 月 17 日提交;v1 于 2018 年 9 月 25 日提交;最初宣布 2018 年 9 月。

评论:在版本 2 中，错误已修复

76. 第 xiv: 1809.09038[pdf,其他] Cs。铭

spx: 为边缘计算保留端到端安全性

作者:ketan bhardwaj, shh myingwei h, ada gavrilovska, tesoo kim, chingyu song

摘要: 除了点解决方案之外，边缘计算的愿景是使 web 服务能够在移动网络边缘的多租户基础架构中部署其边缘功能。但是，由于一个关键问题，边缘函数可能会变得无用: web 服务是通过端到端加密连接提供的，因此边缘函数不能在不影响安全性或降低性能的情况下对加密通信进行操作。此问题的任何解决方案都必须与现有协议 (如 tls) 以及新出现的客户端和**物联网**设备安全协议进行互操作。边缘函数必须对客户端终结点保持不可见，但可能需要从其服务端 web 服务进行显式控制。最后，解决方案必须在开销边距范围内运行，这并不排除边缘的好处。为了解决这个问题，本文提出了 spx--一种边缘就绪和端到端安全协议扩展的解决方案，它可以有效地维护端到端 (e3 个) 安全语义。使用 spx 原型，我们允许边缘函数对加密流量进行操作，同时确保安全

协议的安全语义仍然有效。spx 使用英特尔 sgx 将通信通道与远程认证绑定，并提供一种解决方案，该解决方案不仅可以抵御潜在的攻击，还可以导致性能低下，也不会要求最终用户方面进行任何更改或中断与现有协议的互操作性。少

2018 年 9 月 24 日提交;最初宣布 2018 年 9 月。

评论:12 页, 19 位数字

77. 第 1809. 08783[pdf,其他] Cs。Lg

使用足迹产生的地震信号进行人员识别

作者:bodhibrata mukhopadhyay, sahil anchal, subrat kar

文摘: 基于足迹的生物识别系统也许是唯一不妨碍个人自然运动的人的识别技术。与所有其他生物鉴别系统相比，这显然是一个优势，这些系统需要大量的人为干预，并在一定程度上侵犯个人的隐私。本文提出了一种利用广泛分布于不同地域的检波器 (振动传感器) 实现基于足迹的生物识别系统的雾计算体系。结果存储在物联网 (**iot**) 云中。我们在一个本地数据库 (由我们创建) 上测试了我们的生物识别系统，该数据库包含来自 8 人的 46000 足迹事件，并且在每个样本的 1、5 和 10 足迹的情况下实现了 73%、90% 和 95% 的精度。我们还提出了一种基于追求的数据压缩技术 ds8bp，用于向雾中无线传输足迹事件。ds8bp 将原始足迹事件 (采样在 8 khz 时采样) 压缩 10 倍，并起到平滑滤镜的作用。这些实验结果描述了我们的技术在人的识别和访问控制系统领域的高可行性。少

2018 年 9 月 24 日提交;最初宣布 2018 年 9 月。

78. 第: 189.07928[pdf, ps,其他] Cs。镍

操纵攻击下物联网网络数据完整性的理论研究前景

作者:mehrdad salimitari, shameek bhattacharjee, mainak chatterjee

摘要: 随着物**联网** (**iot**) 和网络物理系统变得越来越普遍，并且是我们日常生活中不可或缺的一部分，因此我们能够信任此类系统的数据聚合非常重要。然而，对可信度的解释是有背景的，并根据有关应用程序的风险容忍度态度以及与信任模型所依据的证据相关的不同程度的不确定性而有所不同。因此，数据完整性评分机制应有适应不同风险态度和不确定性的规定。本文提出了一个贝叶斯推理模型和一个数据完整性评分的前景理论框架，该模型在操纵数据的对手面前量化了从**物联网**设备收集的数据的可信度。我们认为是一个不完善的异常监视机制，用于监视从每个设备发送的数据，并将结果归类为未被泄露、泄露和无法推断。这些结果被概念化为贝叶斯推理模型的多项式假设，具有三个参数，然后用于计算关于聚合数据的可靠性的实用值。我们使用前景理论启发的方法来量化此数据完整性分数，并评估来自**物联网**框架的聚合数据的可信度。此外，我们还利用传统的预期效用理论对该系统进行了建模，并将结果与利用前景理论得到的结果进行了比较。由于决策是基于数据的融合方式，我们提出了两种测量模型--一种是乐观的，另一种是保守的。通过大量的仿真实验验证了该框架的有效性。我们展示了在攻击强度和检测不准确等多种系统因素下数据完整性得分的变化情况。少

2018 年 9 月 20 日提交;最初宣布 2018 年 9 月。

评论:本文提交给 ieee 关于可靠和安全计算的事务

79. 第十四条: 189.07914[pdf,其他] Cs。铬

基于云的物联网加密数据智能处理的安全短语搜索

作者:孟申,马宝丽,朱丽,杜晓江，徐克

摘要: 短语搜索允许检索包含精确短语的文档，这在基于云**的物联网的**许多机器学习应用程序 (如智能医疗数据分析) 中发挥着重要作用。为了防止敏感信息被服务提供商泄露，文档 (例如诊所记录) 通常在外包给云之前由数据所有者进行加密。然而，这使得搜索操作成为一项极具挑战性的任务。现有的多关键字搜索操作的可搜索加密方案无法执行短语搜索，因为它们无法确定查询短语中多个关键字在云服务器端加密数据上的位置关系。本文提出了一种高效**的基于云的物联网**智能加密数据处理隐私保护短语搜索方案 p3。我们的方案利用同态加密和双线性映射来确定多个查询关键字在加密数据上的位置关系。它还利用概率陷阱门生成算法来保护用户的搜索模式。全面的安全分析证明了 p3 所实现的安全保障。我们实现了一个原型，并对真实世界的数据集进行了广泛的实验。评价结果表明，与现有的多关键字搜索方案相比，p3 可以通过适度的开销大大提高搜索精度。少

2018 年 9 月 20 日提交;最初宣布 2018 年 9 月。

80. **第: 189.07855[pdf,其他] Cs。镍**

ee-bsmu: 智能城市智能通信节能基站监控单元

作者:syed waqas haider shah, ahmad talal riaz

摘要: 物联网 (**iot**) 几乎应用于我们日常生活的各个方面，并被广泛用于智能城市应用。为了监控环境并为公民提供服务,**物联网**使用各种设备来感知、驱动、发送数据、接收数据。各种传感器正在进行传感，这些数据通过通信系统存储在云中。移动通信是将数据从终端设备传输到云的主要参与者之一。随着对移动通信需求的增加，部署了更多的基站 (bs)，以促进服务。除了传统服务外，移动通信系统还经过即兴**提供支持物联网**设备等较新的服务。因此，为了提供高效的碳排放服务，传递基站的智能性是非常重要的。在这项工作中，我们提出了一个基站监测单元 (bsmu)，以提高 bs 的智能，一个基站监测单元用于收集、计算和传输数据，并在 bsmu 中嵌入一个智能单元使用 mapreduce 算法和 hdfs 减少要传输到分布式云的文件的大小，在该云中，分布式云用于存储数据并向管理员发送有关异常的通知。因此，提出的 bsmu 实现了改进的服务质量 (qos) 的 bs，最大限度地减少了资源使用和碳排放。少

2018 年 9 月 5 日提交;最初宣布 2018 年 9 月。

评论:7 页, 4 个数字

81. **第: 189.07655[pdf,其他] Cs。铬**

使用 ethereum、s 群和 lora 设计基于区块链的物联网基础架构

作者:kazm röfat zylmaz, arda yurdakul

摘要: 如今,**物联网**设备在生活各个方面的数量呈指数级增长。我们生活的城市越来越聪明，并以一种背景的方式向我们通报我们的环境。但是，除了存储和挖掘数据以提供更高质量的**物联网**服务的问题外，部署、管理和收集这些设备中的数据也面临着重大挑战。区块链技术，即使在今天的新生形式，包含了支柱，以创建一个共同的，分布式的，不可信赖的和自主的基础设施系统。本文介绍了一个标准化**的物联网**基础架构;其中数据存储在一个抗 ddos、容错、分布式存储服务中，数据访问由分散的、不可信任的区块链管理。图解系统以 lora 为新兴网络技术，群以分布式数据存储，以太作为区块链平台。这样的数据后端将确保高可用性和最小的安全风险，同时用单一的 "智能合同" 取代传统的后端系统。少

2018 年 9 月 22 日提交;v1 于 2018 年 9 月 20 日提交;最初宣布 2018 年 9 月。

评论:接受在 ieee 消费电子杂志上发布 22.04.2018-已发布的版本可能会有所不同

82. 第 xiv:1809. 06962[pdf,其他] Cs。铬

面向安全和隐私的商品物联网应用的程序分析：挑战与机遇

作者:z. berkay celik, earlence fernandes, eric paley, gang tan, patrick mcdaniel

摘要: 物联网 (**iot**) 的最新发展为智能家居、个人监控设备和增强的制造等无数领域提供了支持。**物联网**现在已经普及---几乎在每一个可以想象的领域都部署了新的应用程序，从而采用了基于设备的交互和自动化。程序分析对于识别**物联网**漏洞至关重要，但物**联网**中程序分析的应用和范围在很大程度上仍未被技术界探索。在本文中，我们研究**了物联网**中的隐私和安全问题，这些问题需要程序分析技术，重点是针对这些系统和防御措施的已识别攻击。基于对五个**物联网**编程平台的研究，我们确定了程序分析和安全社区工作所产生的关键见解，并将程序分析技术的有效性与安全和隐私问题联系起来。最后，我们研究了最近的**物联网**分析系统并对其实现进行了探讨。通过这些探索，我们强调了在校准将使用**物联网**系统的环境方面的主要挑战和机遇。少

2018 年 10 月 12 日提交;v1 于 2018 年 9 月 18 日提交;最初宣布 2018 年 9 月。

评论:部分流更新，并修复写入问题

83. 第 xiv:1809.06699[pdf,其他] cs. it

用于临时活动的下无人机单元：无人机高度和空中通道环境的影响

作者:周晓辉,萨勒曼，郭静, 哈利姆·亚尼科莫洛

摘要: 提供与大量设备的无缝连接是物联网 (**iot**) 网络面临的最大挑战之一。使用无人机作为空中基站 (abs) 为地面设备或用户提供覆盖，被认为是**物联网**网络的一个有希望的解决方案。在本文中，我们考虑建立一个带有底层 abs 的通信网络，为体育赛事或体育场内的音乐会等临时活动提供报道。利用随机几何，我们提出了一个通用的分析框架来计算空中和地面蜂窝系统的上行和下行覆盖概率。我们的框架适用于任何指定了视线 (los) 和非视线 (nlos) 链接的概率函数的空中通道模型。考虑两种常用的空中通道模型，通过蒙特卡罗模拟验证了分析结果的准确性。我们的研究结果显示了不同的空中通道环境 (即郊区、城市、密集的城市和高层城市) 对上行和下行覆盖概率的不小影响，并为最佳 abs 部署高度提供了设计指南。少

2018 年 10 月 8 日提交;v1 于 2018 年 9 月 17 日提交;最初宣布 2018 年 9 月。

评论:这项工作被接受出现在 ieee 物联网杂志关于无人机对物联网的特刊上。版权可以在不通知的情况下转让，之后此版本可能不再可访问。arxiv 管理说明：文本与 arxiv:1801 1.05948 重叠

84. 第 xiv:1809.06624[pdf,其他] Cs。镍

多伊 10.1109/NFV-SDN.2017.8169876

在 6tisch 工业物联网网络中使用第 2 层切片隔离 sdn 控制流量

作者:michael baddeley, reza nejabati, george oikonomou, sedat gormus, mahesh sooriyabandara, dimitra simaeonidou

摘要: ieee 最近在 ieee 802.15.4 调度频道跳跃 (tsch) 和 ietf 6tisch 工作组 (wg) 中进行的标准化工作旨在跨受限的物联网 (wg) 提供确定性通信和资源的有效分配 (**物联网**) 网络，尤其是在工业**物联网**(iiot) 方案中。在 6tic 中，软件定义网络 (sdn) 已被确定为在许多关键情况下提供集中控制的手段。然而，在低功耗和损耗网络 (lln) 中实现集中式 sdn 体系结构面临着相当大的挑战：不仅控制器流量由于链接不可靠和网络争用而抖动，而且 sdn 产生的开销也可能带来严重影响其他流量的性能。本文建议

使用 6tisch 轨道，即用于跨 tsch 网络创建专用转发路径的第 2 层切片机制，以隔离 sdn 控制开销。这不仅可以防止控制流影响其他数据流的性能，而且 6tisch 轨道的属性允许确定性、低延迟的 sdn 控制器通信。使用 contiki os 的轻量级 sdn 实现，我们首先演示了 sdn 控制流量对 6tisch 网络中应用程序数据流的影响。然后，我们通过沿 sdn 控制路径分配专用资源来划分网络，轨道为降低 ieee 802.15.4-2015 tsch 网络中 sdn 控制开销的成本提供了有效的方法。少

2018 年 9 月 18 日提交;最初宣布 2018 年 9 月。

85. 第 1809. 06551 [pdf] cs. cy

基于块链的智能工业网络 (dsdin)

作者:barco you , matthias hub, muszheyou , bo xu, Mengzhe , ivan uemlianin

摘要: 过去由于技术限制，制造业出现了集中化，工厂 (特别是大型制造商) 收集了几乎所有的制造资源，包括: 技术、原材料、设备、工人、市场信息等。然而，这种集中生产成本高昂、效率低下和不灵活，难以应对迅速变化、多样化和个性化的用户需求。本文介绍了一个智能工业网络 (dsdin)，它提供了一个完全分布式的制造网络，每个人都可以通过权力下放而参与制造，而不是中间环节，使他们能够快速获得他们希望获得授权、认可并以低成本方式获得回报的产品或服务，包括提供创造性的想法、设计或设备、原材料或体力)。dsdin 是一个基于区块**链的物联网**和 ai 技术平台，也是一个基于**物联网**的智能服务标准。由于 dsdin 形成的智能网络，制造中心不再是工厂，实际上没有制造中心。dsdin 为人员和事物 (包括原材料、设备、成品/半成品等) 提供多参与式对等网络。通过网络传输的信息称为智能服务算法 (isa)。用户可以通过 isa 向设备发送流程模型、公式或控制参数, dsdin 中的每个事务都是 isa 定义的智能服务。少

2018 年 9 月 18 日提交;最初宣布 2018 年 9 月。

86. 第 xiv:1809. 005:04 [pdf] cs. cy

物联网杯中的一场风暴: 网络物理社交机器的出现

作者:aastha madaan, jason r. c.护士, david de roure, kieron o ' hara, wendy hall, sadie creese

摘要: 社交机器的概念正越来越多地被用来描述网络上的各种社会认知空间。社交机器是使用网络数字技术的人类集体，它启动了现实世界的过程和活动，包括人类沟通、互动和知识创造。因此，它们在 web 上不断出现和褪色。物联网 (**iot**) 传感器和设备的采用使人与机器之间的关系变得更加复杂。这些器件的规模、自动化、连续传感和驱动能力为人与机器之间的关系增加了一个额外的维度，因此很难在系统或概念层面上理解它们的演变。本文介绍了这些新的社会技术系统，我们将其称为网络物理社交机器，通过不同的范例，并考虑了安全和隐私的相关挑战。少

2018 年 9 月 16 日提交;最初宣布 2018 年 9 月。

评论:14 页, 4 个数字

报告编号:ssr-3250383

87. 第 189.05613 [pdf, ps,其他] Cs。镍

物联网网络的区块链和共识协议概述

作者:mehrdad salimitari, mainak chatterjee

摘要: 区块链作为加密货币的基础技术的成功也为其在其他应用领域的应用开辟了可能性。区块链在其他领域的潜在用途的主要优势在于其固有的安全机制和对不同攻击

的免疫力。区块链依靠一种一致的方法来商定任何新的数据。目前用于不同加密货币的区块链的大多数共识方法都需要很高的计算能力，因此不适合于资源受限的系统。在本文中，我们讨论和研究了适用于资源受限**的物联网**设备和网络的各种基于区块链的共识方法。典型**的物联网**网络由多个设备组成，这些设备的计算和通信能力有限。大多数情况下，这些设备无法执行密集计算，并且缺乏带宽。因此，我们讨论了可以采取的措施，以减少基本共识方法的计算能力和收敛时间。我们还讨论了公共区块链的一些替代方案，如私有区块链和纠结，以及它们在**物联网**网络中的潜在采用。此外，我们还讨论了现有的共识方法和区块链实现，并探讨了利用它们实现基于物联网的**区块链**网络的可能性。并提出了一些公开研究的挑战。少

2018 年 9 月 14 日提交;最初宣布 2018 年 9 月。

评论:它被提交给 ieee 网络杂志

88. 第 xiv:1809.05604[pdf,其他] Cs。镍

多伊 10.1109/METROI4.2018.8428309

工业 lora 传感器网络的自校准轻量化同步算法

作者:luca tessaro, cristiano Raffaldi, maurizio rossi, davde brunelli

摘要: 在工业物联网时代，无线传感器和执行器网络的发展势头越来越大。来自制造链中传感器的闭环数据的使用扩展了无线传感器网络 wsn 的常见监控场景，在该场景中只记录了数据。本文提出了一种在最先进的**物联网**无线电 (如 lora) 上实现的 tdma 的精确定时同步，该同步在工业环境中具有很高的鲁棒性，是一个很好的解决方案。实验结果表明，如何调节漂移校正，并将同步误差控制在要求范围内。少

2018 年 9 月 14 日提交;最初宣布 2018 年 9 月。

89. 第 xiv:1809. 00556[pdf,其他] Cs。铬

多伊 10.1109/JIOT.2018.2877749

危险游戏: 对智能玩具威胁的分类和评价

作者:sharon shasha, moustafa mahmoud, mohammad mannan, amr youssef

摘要: 智能玩具已经占据了越来越多的玩具市场份额，并且在有孩子的家庭中越来越普遍。智能玩具是物联网 (**iot**) 设备的一个子集，包含传感器、执行器和/或人工智能功能。他们经常通过配套应用直接或间接地拥有互联网连接，并收集有关其用户和环境的信息。最近的研究发现，许多智能玩具存在安全缺陷，导致严重的隐私泄露，或允许跟踪儿童的实际位置。这种性质的一些广为流传的发现促使世界各国政府采取行动，禁止其中一些玩具。与其他**物联网**设备相比，智能玩具由于其容易受到攻击的用户群而带来独特的风险，我们的工作旨在定义这些风险并评估针对这些风险的玩具子集。我们提供智能玩具特有威胁的分类，以团结和补充现有的临时分析，并帮助对其他智能玩具进行全面评估。我们的威胁分类框架解决了潜在的安全和隐私缺陷，这些缺陷可能导致私人信息泄露或允许对手控制玩具来引诱、伤害或困扰儿童。使用此框架，我们对 11 个智能玩具及其配套应用进行了彻底的实验分析。我们的系统分析发现，目前的几个玩具仍然使儿童面临多个威胁，攻击者通过物理的，附近的，或远程访问玩具。少

2018 年 10 月 25 日提交;v1 于 2018 年 9 月 14 日提交;最初宣布 2018 年 9 月。

评论:ieee 物联网杂志, 2018 年 10 月接受 (提前访问网址: https://ieeexplore.ieee.org/document/8502818)

90. 第 xiv:1809.05250[pdf,其他] Cs。Lg

高维设置下的实时非参数异常检测

作者:mehmet necip kult, yyin yilmaz, xiadong wang

摘要: 及时可靠地检测突发异常，例如故障、入侵/攻击，对于实时监控和安全许多现代系统 (如智能电网和物**联网 (iot**) 网络) 至关重要，这些系统能够产生故障、入侵/攻击。高维数据。基于这一目标，我们提出了有效且可扩展的高维环境中实时异常检测算法。我们提出的算法是非参数化 (无模型)，因为标称和异常的多变量数据分布都被假定为未知。我们提取有用的单变量汇总统计，并在一维空间中执行异常检测任务。我们将异常建模为持久异常值，并建议通过类似于累积和 (cusum) 的算法来检测异常。如果观测到的数据流具有较低的内在维数，我们发现一个低维子流，其中嵌入标称数据，然后评估按顺序获取的数据是否持续偏离标称子流形。此外，在一般情况下，我们通过几何熵最小化 (gem) 方法确定标称数据的接受区域，然后评估按顺序观察到的数据是否持续下降到接受区域之外。在提出的 cusum-s 算法的平均虚警周期上，我们提供了一个渐近下限。此外，我们还提供了一个充分的条件，可以渐近地保证该算法的决策统计在没有异常的情况下不会出现差异。数值研究表明，在各种高维环境中，该方案在快速、准确地检测变化异常方面是有效的。少

2018 年 9 月 14 日提交;最初宣布 2018 年 9 月。

91. 决议: 1809. 05229[pdf] cs. cy

多伊10.1016/J.COMPIND.2018.08.002

物联网网络风险评估的未来发展

作者:petar radanliev, david charles de roure, razvan nicolescu, michael huth, rafael mantilla montalvo, stacy cannady, peter burnap

文摘: 本文重点介绍了物联网 (**iot**) 及其相关网络风险载体和顶点的经济影响评估--**对物联网**垂直领域的重新解释。我们适应 **iot** 模型 (衡量给定时间段内可能最大损失的成熟模型) 和 micromort 模型 (一种广泛使用的模型，通过死亡率风险单位预测不确定性)。由此产生的用于计算**物联网风险的**新**物联网** micromort 将使用 bullguard 物联网扫描仪 (超过 310,000, 000 次扫描) 和 garner 在**物联网**连接设备上的报告中获得真实数据的测试和验证。提出了物**联网**网络风险的现状和**未来物联网**网络风险的预测两个计算。因此，我们的工作推动了整合网络风险影响评估的努力，并更好地了解**了物联网**网络风险的经济影响评估。少

2018 年 9 月 13 日提交;最初宣布 2018 年 9 月。

评论:http://doi.org/10.1016/J.COMPIND.2018.08.002

92. 第 xiv: 1809.05142[pdf,其他] Cs。Lg

南洋理工大学节能的深层学习与博弈研究

作者:ioannis c. konstantakopoulos , andrew r. barkan , shiying he, tanya veeravalli, huihan liu, costas spanos

摘要: 以智能基础设施应用的形式实施智能建筑技术，通过利用人在环战略，具有提高可持续性和能源效率的巨大潜力。然而，人类对生活条件的偏好通常是未知和异质的，表现为对建筑物的控制投入。此外，建筑物的住户通常缺乏必要的独立动力，无法在控制智能建筑基础设施方面发挥贡献和发挥关键作用。此外，负责提高运营效率的决策者仍然不知道真正的人类行动及其与传感器驱动平台的整合。通过将用户交互建模为非合作玩家之间的顺序离散游戏，我们引入了一种博弈化方法来支持用户参与和集成在以人为中心的网络物理系统中。我们建议设计和实施大规模网络游戏，目的是通过利用

尖端的物联网 (**iot**) 传感器和网络物理系统传感器/驱动平台。一个基准效用学习框架，它对经典的离散选择模型采用鲁棒估计，为派生的高维不平衡数据提供了支持。为了提高预测性能，我们利用深度双向递归神经网络的深度学习端到端培训，扩展了基准效用学习方案。我们将建议的方法应用于南洋理工大学住宅智能建筑住户的社交游戏实验中的高维数据。我们使用乘员检索到的资源 (如照明和 acb) 操作，模拟了由估计效用函数定义的游戏。少

2018 年 9 月 25 日提交;v1 于 2018 年 9 月 13 日提交;最初宣布 2018 年 9 月。

评论:16 页，较短的版本提交到应用能源杂志

93. 第 xiv:180 9.04966[pdf,其他] Cs。铬

用于 5g 物联网支持的防滑安全助听器的实时轻量级混沌加密

作者:ahsan adeel, jawad ahmad, amir hussain

摘要: 已知现有的仅有音频的助听器在存在巨大噪音的嘈杂情况下表现不佳。新一代视听 (唇读驱动) 助听器是实现更易于理解的音频的主要推动因素。然而，高数据速率、低延迟、低计算复杂性和隐私是成功部署此类高级助听器的主要瓶颈。为了应对这些挑战，我们设想将 5g 云无线接入网、物联网 (**iot**) 和强大的隐私算法集成在一起，以充分受益于这些技术所提供的可能性。设想的 5g **物联网**支持安全的视听 (av) 助听器传输加密的压缩 av 信息，并接收加密的增强的重建语音实时，完全解决网络安全攻击，如位置隐私和窃听。对于安全实现，使用了实时轻量级 av 加密。为了增强语音，云中接收到的 av 信息被用来利用深度学习和分析声学建模 (基于滤波的方法) 来过滤噪声音频。为了卸载计算复杂性和实时优化问题，该框架在云的后台运行深入学习和大数据优化过程。具体而言，在这项工作中，报告了三个关键贡献: (1) 5g **iot** 支持安全视听助听器框架，旨在实现高达 5 毫秒的往返延迟，100 mbps 数据空间 (2) 实时轻量化视听加密 (3) 在云中进行语音增强的唇读驱动的深度学习方法。从语音增强和 av 加密两方面的关键分析表明，所设想的技术在获得高质量的语音重建和安全的移动 av 助听器通信方面具有潜力。少

2018 年 9 月 13 日提交;最初宣布 2018 年 9 月。

类:D.4.6;c.2;i.2;I.2.7;I.2。6

94. 第 xiv:180 9.04583[pdf,其他] Cs。铬

对 mhealths 数据进行高效且保留基于语音的搜索

作者:mohammad hadian, thamer altuwaiyan, xiaohui liang, wei li

摘要: 作为智能个人助理，家庭**物联网**设备在医疗系统中发挥着重要作用。它们通常带有支持语音的功能，为老年人、残疾人和患者增加了额外的可用性和便利。在本文中，我们提出了一个有效的和隐私保护的语音搜索方案，以提高效率和隐私的家庭医疗应用程序。我们考虑的是一个应用场景，患者使用这些设备记录他们的声音并将其上传到服务器，并且护理人员根据语音内容、情绪、语调和背景声音搜索患者感兴趣的声音。我们的方案保留了语音数据的丰富性和隐私性，并实现了准确和高效的基于语音的搜索，而在当前使用语音识别的系统中，语音数据的丰富性和隐私性受到损害。具体而言，我们的方案通过采用同态加密来实现隐私;只有加密的语音数据被上载到无法访问原始语音数据的服务器。此外，我们的方案使服务器能够根据语音特征的相似性，有选择地准确地响应照顾者对语音数据的查询。通过实际实验对我们的方案进行了评价，并表明我们的方案即使有隐私保护，也能成功地匹配相似的语音数据，平均准确率为 80.8。少

2018 年 9 月 12 日提交;最初宣布 2018 年 9 月。

95. 第 xiv:1809.04143[pdf,其他] Cs。镍

kratos: 用于 lpwan 快速研究的开源硬件软件平台

作者:rajeev piyare, amy l. murphy, michele magno, luca benini

摘要: 远程 (lora) 无线电技术最近在**物联网**领域获得了势头，允许低功耗通信跨越数公里的距离。因此，部署的 lora 网络越来越多。然而，商用 lora 设备价格昂贵且适当，从而造成进入的障碍，并可能减缓新应用程序的开发和部署。使用开源硬件和软件平台将使更多的开发人员能够测试和构建智能设备，从而实现更好的整体开发生态系统、更低的进入壁垒以及**物联网**应用数量的快速增长。针对这一目标，本文介绍了 kratos 的设计、实现和评估, kraos 是一个运行 contikios 的低成本 lora 平台。我们的硬件和软件设计都作为开源发布给了研究界。少

2018 年 9 月 11 日提交;最初宣布 2018 年 9 月。

评论:2018 年在 wimob 接受

96. 第 xiv:1809.04142[pdf,其他] Cs。镍

按需 tdma，用于利用 lora 和唤醒接收器进行节能数据采集

作者:rajeev piyare, amy l. murphy, michele magno, luca benini

摘要: lora 等低功耗和远程通信技术由于能够以毫瓦的功耗覆盖公里范围，在物**联网**应用中越来越受欢迎。lora 的主要缺点之一是网络中设备数量增加时的数据延迟和交通拥堵。特别是，延迟的产生是由于 lora 终端节点的极端占空比循环，以降低整体能耗。为了克服这一缺点，我们提出了一种异构网络体系结构和一种节能的按需 tdma 通信方案，以提高标准 lora 网络的设备寿命和数据延迟。我们将微瓦唤醒接收器的功能结合在一起，实现超低功耗状态和纯异步通信，并结合 lora 的远程连接。实验结果表明，数据可靠性为 100%，往返延迟约为毫秒，末端设备在活动时耗散小于 46 mj，在不活动期间消耗 1.83μw，在 1200 mJ 锂电池上持续长达 3 年。少

2018 年 9 月 11 日提交;最初宣布 2018 年 9 月。

评论:2018 年在 wimob 接受

97. 第 1809. 002702[pdf,其他] Cs。铬

区块链自动智能合同安全测试的实证脆弱性分析

作者:reza m. parizi, ali dehghantanha, kim-kwang raymond choo, amritraj singh

摘要: 新兴的区块链技术支持分散计算范式的转变，是一个迅速逼近的现象。虽然区块链主要被认为是比特币的基础，但由于引入了智能合同，它的应用已经远远超出了加密货币的范围。智能合同是自我执行的软件，它驻留和运行在托管区块链上。使用基于区块链的智能合同进行安全和透明的管理，以管理 internet 支持的环境 (主要**是物联网**) 中的交互 (身份验证、连接和事务)，是研究和实践的一个特殊领域。但是，编写可信和安全的智能协定可能具有极大的挑战性，因为底层域特定语言的语义和可测试性很复杂。有一些引人注目的事件表明，连锁智能合同可能包含各种代码安全漏洞，从而引发财务伤害。当涉及到智能合同的安全性时，具有编写合同能力的开发人员应该能够测试他们的代码，诊断安全漏洞，然后再将其部署到区块链上的不可变环境中。但是，智能合同的安全测试工具只有少数。这意味着，现有的自动智能合同安全测试研究还不够充分，仍处于起步阶段。我们的具体目标是更容易地实现区块链智能合同在安全和隐私方面的应用，我们应该首先了解它们的漏洞，然后才能广泛实施。因此，本文的目的

是对当前静态智能合同安全测试工具进行意义深远的实验评估，对于最广泛使用的区块链、ethereum 及其特定领域的编程语言,提供了第一个.. 。少

2018 年 9 月 7 日提交;最初宣布 2018 年 9 月。

98. 第 xiv:1809. 02234[pdf] Cs。镍

在 lorawan 上的插槽 aloha 叠加: 一种分布式同步方法

作者:托马索·波洛内利,达维德·布鲁内利,卢卡贝尼尼

摘要: lorawan 是**物联网**应用中最有前途的标准之一。然而，每个网关的终端设备密度高，网关和终端设备之间缺乏有效的同步方案，这些网络的可扩展性受到挑战。在本文中，我们建议使用 slotted-aloloha (s-aloha) 而不是 lora 使用的经典 aloha 方法来管理 lorawan 网络的通信。实现是标准 lorwan 之上的覆盖层;因此，无需对预先存在的 lrawan 固件和库进行修改。我们的方法基于一种适用于低成本**物联网**终端节点的新型分布式同步服务。我们的同步服务支持的 s-aloha 显著提高了传统 lorawan 网络在数据包丢失率和网络吞吐量方面的性能。少

2018 年 9 月 6 日提交;最初宣布 2018 年 9 月。

评论:4 页, 8 个数字

99. 第: 1809. 01974[pdf] cs. cy

多伊 10.1109/FAS-W.2018.00031

管理和保存数据以衡量生活质量的愿景和挑战

作者:vero Estrada-Galinanes, ketarzyna wac

摘要: 与健康有关的数据分析在自我认识、疾病预防、诊断和生活质量评估中发挥着重要作用。随着数据驱动解决方案的出现，无数的应用和物联网 (**iot**) 设备 (可穿戴设备、家用医疗传感器等) 为数据收集提供了便利，并通过中央管理提供了云存储。最近，封锁链和其他分布式分类账成为基于分散组织系统的替代存储选项。我们将关注人类数据出血问题，并认为，如果忽视个人、社区和社会价值观，集中式或分散式系统组织都不是数据驱动创新的灵丹妙药。这份立场文件的目的是阐述保护隐私的战略，以及鼓励数据共享和支持开放数据，而不需要研究人员使用复杂的访问协议。我们的主要贡献是概述了一个以生活质量 (qol) 数据为重点的自我监管的开放健康档案 (oha) 系统的设计。少

2018 年 9 月 6 日提交;最初宣布 2018 年 9 月。

评论:dss 2018: 数据驱动的自我调节系统

期刊参考: 2018 年 ieee 第三届关于自我基础和应用的国际研讨会 *

100. 第 09iv:1800.00986[pdf] cs. cy

物联网智能照明的发展趋势

作者:豪尔赫·希盖拉、 aleix llenas、 josep carreras

摘要: 智能照明是一个基本概念，它将三个主要方面联系起来: 固态照明 (ssl) 技术、先进的控制和遵循全球标准的通用通信接口。然而，这种概念化是不断发展的，以符合在物联网 (**iot**) 生态系统中工作的下一代设备的准则。现代智能照明系统基于发光二极管 (led) 技术，涉及具有动态光谱光再现和高级传感功能等功能的高级驱动器。最终的特点是提供额外的高级服务，作为光通信的枢纽，允许在室内环境中与传统 wi-fi 网关共存。在此背景下，照明系统正在不断发展，以支持与**物联网**生态系统兼容的不同无线通信接口。ssl 系统的市场趋势预测连接的**物联网**照明控制系统将加速扩展，在不同

的市场中，从智能家居和工业环境。这些系统提供了前所未有的高级功能，如光源的高级频谱控制，以及包括几个通信接口。这些接口主要是有线、射频（rf）和光无线通信（owc）接口，用于传感和可见光通信（vlc）等高级服务。本文介绍了如何利用不同**的以物联网**为中心的照明架构，针对不同应用设计和实现**基于物联网**的智能照明系统。最后，在考虑到商业智能照明平台的情况下，解释了与互操作性和 web 服务有关的不同标准和方面。少

2018 年 8 月 29 日提交;最初宣布 2018 年 9 月。

评论:24 页，5 个数字，2 个表

101. **第 09iv:1800.00966[pdf，ps,其他] cs. it**

具有高能效的移动边缘计算卸载适用于具有共享数据的应用程序

作者:何祥宇,洪兴,岳晨，arumugam nallanathan

摘要：移动边缘计算卸载（meco）已被认为是一个很有希望的解决方案，通过将计算任务卸载到蜂窝网络边缘（**也**称为 {\em} 来减轻资源有限的知识（iot）设备互联网的负担云})。具体而言，虚拟现实（vr）和增强现实（ar）等延迟关键应用程序具有固有的协作属性，因为部分输入输出数据由邻近的不同用户共享。在本文中，我们考虑了一个多用户雾计算系统，在该系统中，运行具有共享数据的应用程序的多个单天线移动用户可以在（部分）将其各自的任务卸载到附近的单天线云中进行选择。远程执行和执行纯本地计算。移动用户的能量最小化被表述为一个凸问题，受总计算延迟约束、单个数据下载的总能量约束以及局部计算的计算频率约束的影响。经典拉格朗日二元性可以用来寻找最优解。基于半封闭表单解决方案，共享数据被证明只由其中一个移动用户而不是多个移动用户传输。此外，与那些没有考虑共享数据属性或移动用户本地计算能力的基线算法相比，所提出的联合计算卸载和通信资源分配提供了大量的能量储蓄。少

2018 年 9 月 4 日提交;最初宣布 2018 年 9 月。

评论:6 页，3 个数字，接受 ieee 全球 2018 年

102. **第 09iv:1800.00745[pdf,其他] Cs。铬**

物联网：智能环境的数字取证框架

作者:leonardo babun，amit kumar sikder，abbas acar，a. selcuk Uluagac

摘要：**物联网**设备和传感器以合作的方式得到了利用，从而实现了智能环境的概念。在这些智能设置中，由于设备之间的交互和用户的日常活动，会生成大量数据。此类数据包含有关智能环境中发生的事件和操作的有价值的取证信息，如果进行分析，可能有助于追究违反安全策略者的责任。在本文中，我们介绍了 ittots，这是一种适用于智能家居和智能办公室等智能环境的新型数字法医框架。iotdots 有两个主要组件：iotdots-修饰符和 iotdots-antier。在编译时，iotdos-reudoder 执行智能应用的源代码分析，检测与相关信息，并自动插入跟踪日志。然后，在运行时，日志存储到 iotdots 数据库中。后来，在进行法医调查的情况下，iotdos-anicer 采用数据处理和机器学习技术，从设备活动中提取有价值和可用的法医信息。为了测试 iotdots 的性能，我们在一个现实的智能办公环境中测试了 i 衔接 dots，共有 22 个设备和传感器。评估结果表明，i 衔接 dots 在检测用户活动方面平均可达到 98% 以上的精度，在智能环境中检测用户、设备和应用的行为时的精度可达到 96% 以上。最后，iotdots 性能不会给智能设备带来开销，也不会给云服务器带来最小的开销。少

2018 年 9 月 3 日提交;最初宣布 2018 年 9 月。

103. **第 09iv:1800.0043[pdf] cs. it**

迈向智能边缘：无线通信与机器学习

作者:朱光旭,刘东珠,杜玉清，你,张军，黄开斌

摘要：人工智能（ai）最近的复兴正在使几乎每一个科学和技术分支发生革命性的变化。考虑到无处不在的智能移动设备和物联网（**iot**）设备，预计大多数智能应用将部署在无线网络的边缘。这一趋势在实现"智能边缘"以支持各种边缘设备上支持 ai 的应用程序方面产生了浓厚的兴趣。因此，出现了一个新的研究领域，称为边缘学习，它跨越和彻底改变了两个学科：无线通信和机器学习。边缘学习的一个主要主题是克服每个边缘设备的有限计算能力以及有限的数据。这是通过利用移动边缘计算（mec）平台和利用分布在大量边缘设备上的海量数据来实现的。在这样的系统中，从分布式数据中学习和边缘服务器和设备之间的通信是两个关键和耦合的方面，它们的融合带来了许多新的研究挑战。本文提出了一套新的边缘学习无线通信设计原则，统称为学习驱动通信。提供了示例来证明这些设计原则的有效性，并确定了独特的研究机会。少

2018 年 9 月 2 日提交;最初宣布 2018 年 9 月。

评论:提交给 ieee 以供可能的出版

104. **第：1809.00238[pdf,其他] Cs。Sd**

面向智慧城市噪声分类的机器学习驱动物联网解决方案

作者:yasser alsouda, sabri pllana, arianit kuri

文摘：我们提出了一种基于机器学习的方法，使用低功耗和廉价的**物联网**单元进行噪声分类。我们使用 mel-fuser 系数进行音频特征提取，并使用受监督的分类算法（即支持向量机和 k 最近的邻居）进行噪声分类。我们通过实验评估我们的方法，该数据集大约有 3000 个声音样本，分为八个声音类（如汽车喇叭、千斤顶或街道音乐）。我们探索了支持向量机和 k 最近邻域算法的参数空间，以估计所研究数据集中声音样本分类的最佳参数值。我们实现了 85%--100% 范围内的噪声分类精度。对于具有 3000 多个声音样本特征的数据集，在 raspberry pi zero w 上对我们最近的邻居（k = 1）实现的培训和测试不到一秒。少

2018 年 9 月 1 日提交;最初宣布 2018 年 9 月。

105. **第 1808.10529[pdf] Cs。铬**

了解物联网（iot）中的安全要求和挑战：回顾

作者:faraz idris khan, sufian hameed

摘要：物联网（**iot**）是通过在各种使用互联网相互通信的低功耗嵌入式设备之间自由流动信息的理念实现的。据预测,**物联网**将得到广泛部署，并将在生活的各个领域中找到适用性。**物联网**的需求最近引起了极大的关注，组织对**物联网**模式将产生的数据的业务价值感到兴奋。另一方面,**物联网**对最终用户有各种安全和隐私问题，限制了其扩散。在本文中，我们确定、分类和讨论了各种安全挑战和解决这些挑战的最新工作。少

2018 年 8 月 30 日提交;最初宣布 2018 年 8 月。

106. **第 1808.10217[pdf,其他] Cs。镍**

具有链的无线供电物联网（iot）人群传感系统中的竞争数据交易

作者:冯少汉,王文波,都喜尼亚托，董英金,王平

摘要：随着智能**物联网**设备在互联网边缘的爆炸式增长，在移动设备上嵌入传感器以进行海量数据收集和集体环境传感已被视为**物联网**的经济高效的解决方案应用。然而，现有**的物联网**平台和框架依赖于专用中间件进行（半）集中任务调度、数据存储和激励

提供。因此，它们通常部署成本很高，对不同需求的适应性有限，并且面临一系列数据安全和隐私问题。在本文中，我们采用无许可区块链，构建了一个纯分散的平台，用于在无线供电的**物联网**人群传感系统中进行数据存储和交易。在该系统中,**物联网**传感器使用从 rf 能量信标无线传输的电力，用于数据传感和传输到接入点。然后将数据转发到分布式分类帐服务的区块链，即数据事务验证、记录和维护。由于无线传输的耦合干扰和区块链分布式分类帐服务产生的交易费用，合理的传感器必须决定其传输速率，以最大限度地提高个人效用。因此，我们建立了一个不合作的博弈模型来分析传感器之间的竞争情况。我们为纳什均衡的存在提供了分析条件，并对博弈中的平衡策略给出了一系列有见地的数值结果。少

2018 年 8 月 30 日提交;最初宣布 2018 年 8 月。

评论:提交给 2018 年 ieee 通信系统国际会议

107. 第 1808.10097[pdf,其他] Cs。操作系统

基于 linux 的物联网器件的自骑性能分析与提高

作者:immanuel amirtharaj, tai glot, behnam dezfouli

摘要: 最大限度地减少基于 linux 的设备的能耗是在各种**物联网**方案中实现广泛部署的重要一步。节能方法 (如占空比) 旨在通过限制设备通电的时间来解决这一限制。在这项工作中，我们研究并改进了基于 linux 的**物联网**设备完成其任务所需的时间。我们分析了两个平台 (raspberry pi 3 和零无线) 上的系统启动和关机过程，并通过识别和禁用在用户空间中初始化的耗时或不必要的设备来提高空降循环性能。我们还研究了 sd 卡速度和 sd 卡容量利用率是否会影响启动持续时间和能耗。此外，我们还建议在 \t{systemd} 系统之上构建的 allex，即在用户空间初始化的同时运行用户应用程序。当应用于各种**物联网**应用场景时，我们验证了 pallex 对性能的影响: (i) 捕获图像, (ii) 捕获和加密图像, (iii) 使用最接近 k 的邻居算法捕获和分类图像，以及 (iv) 捕获图像并将其发送到云服务器。结果表明，在这些应用场景中，系统寿命分别提高了 18.3%、16.8%、13.9% 和 30.2%。少

2018 年 8 月 29 日提交;最初宣布 2018 年 8 月。

评论:scu 物联网研究实验室技术报告

报告编号:tr-scu-siotlab-aug2018-pallex

108. 第 1808.0969[pdf] Cs。镍

多伊 10.3390/fi10080068

纳米物、物和事物的互联网: 未来的增长趋势

作者:mahdi h. miraz, maaruf ali , peter s. excell, richard picking

文摘: 对物联网 (**iot**)、物联网 (ioe) 和纳米物联网 (iont) 的现状和未来前景进行了广泛的综述，并进行了总结调查。分析**清楚地区分了物联网**和 ioe，许多评论家错误地认为它们是相同的。在**评估了物联网**、ioe 和 iont 领域当前的发展趋势之后，本文确定了当前和未来最重要的 21 个挑战，以及未来可能扩展其应用程序的方案。尽管这些事态发展可能存在消极方面，但有理由对即将到来的技术普遍持乐观态度。当然，许多繁琐的任务可以由**物联网**设备承担。然而，犯罪活动和其他邪恶活动的危险，加上硬件和软件错误的危险，构成了重大挑战，是进一步研究的优先事项。确定了研究的主要具体优先问题。少

2018 年 8 月 27 日提交;最初宣布 2018 年 8 月。

日记本参考:未来互联网 2018, 10 (8), 68, 可用:
http://www.mdpi.com/1999-5903/10/8/68

109. xiv:1808. 09 390[pdf] Cs。镍

多伊10.5722intunitechopen. 70907

物联网: 技术、应用和标准化

作者:jaydipsen , moonkunlee, sungheonlee, yeongbok choe, menachem domb, arpan pal, hemant kumar rath, samar shailendra , abhijan bhattacharyya, albena mihovska, mahasweta sarkar, hyun jung lee, myungho kim,亚历山德鲁·阿韦里安

摘要: "物联网" (**iot**) 一词是指由相互关联的物理对象和设备组成的生态系统, 这些物理对象和设备可通过 internet 访问, 并且可以相互通信。**物联网**愿景的主要优势在于它在潜在用户日常生活和行为的若干方面产生了并将继续产生的巨大影响。本书介绍了**物联网**领域的一些最新研究工作, 特别是在通信协议、协议和语义的互操作性、信任安全和隐私问题、参考体系结构等方面设计和标准化。它将成为在**物联网**各个领域工作的研究人员、工程师、从业人员以及研究生和博士生的宝贵知识来源。这对研究生院和大学的教职员工也将是有用的。少

2018 年 8 月 25 日提交;最初宣布 2018 年 8 月。

评论:这本书有 137 页。2008 年 8 月, 英特威特, 联合王国, 伦敦出版. 打印国际标准书号 978-1- 78923-548-7, 在线国际标准书号 978-1- 78923-549-4

110. 建议: 1808. 09335[pdf] Cs。哦

相控 mac: 基于 14 topssew 的 8位 gro 相位域 mac 电路, 适用于传感器内计算的深度学习加速器

作者:yoshioka kentaro yoshioka, yosuke toyama, koichiro ban, daisuke yashima, shigeru maya, akihide sai , kohei onizuka

摘要: 提出了一种基于 8 位 mac 电路的相位域 gited-ring-rescorator (gro), 旨在最大限度地减少深度学习加速器的面积和功耗。pmac 仅由数字电池组成, 由于其高效的模拟积累特性, 其功耗明显小于标准数字设计。它所占的面积比传统的模拟设计小 26.6 倍, 与数字 mac 电路相比具有竞争力。pmac 的峰值效率为 14 topsw, 最好是报告, 比传统艺术高 48%。结果说明了异常检测任务的结果, 这是工业**物联网**领域最热门的应用。少

2018 年 8 月 23 日提交;最初宣布 2018 年 8 月。

评论:在 symp 提交。vlsi 2018

111. xiv:1808.08809[pdf, ps,其他] Cs。铬

实体互联网 (ioe): 一种基于区块链的分布式安全范式

作者:罗伯托·萨亚

摘要: 基于无线的解决方案 (如与移动智能设备 (如智能手机和平板电脑) 和物联网 (**iot**) 设备相关的解决方案) 呈指数级增长, 在我们社会的各个领域都带来了无数优势。几十年前, 这种情况将以延迟为主的世界转变为一个以高效实时互动范式为基础的新世界。最近, 加密货币促成了这场技术革命, 其支点是权力下放模式和所谓的区块链基础设施提供的认证功能, 从而有可能对金融进行认证。交易, 匿名。但是, 应该注意到, 这种具有挑战性的情况是如何产生与所涉及的新技术直接相关的新的安全问题的 (例如, 电子商务欺诈、移动僵尸网络攻击、区块链 dos 攻击、加密货币诈骗等)。在这方

面，我们可以承认，科学界的努力通常面向具体的解决办法，而是协同利用所有可用的技术，以便确定更有效的安全模式。本文旨在通过向实体的安全定义互联网（ioe）引入一种新的范式，指出一种能够提高人员和事物安全的可能方法。它是一种人员和事物本地化的机制，它利用了现有大量基于无线的设备和基于区块链的分布式分类帐技术，克服了传统本地化方法的限制，但而不会危及用户隐私。它的操作基于两个核心元素，可互换的角色，实体和跟踪器，这可能是非常常见的元素，如智能手机，平板电脑和**物联网**设备，其实施所需的工作量很小，由于现有的基础设施和设备。少

2018 年 8 月 27 日提交;最初宣布 2018 年 8 月。

评论:30 页, 13 位数字

112. **第 1808.08615[pdf,其他] Cs。简历**

多伊 10.114/3240765 3240833

使用低功耗可穿戴设备的在线人类活动识别

作者:ganapati bhat, ranadeepdeb, vvia vardhan chaurasia, holly shill, umit y. ogras

摘要: 人类活动识别由于其在健康监测和患者康复中的应用，引起了人们的极大兴趣。最近关于 har 的研究主要集中在使用智能手机，因为它的广泛使用。然而，这导致了不方便的使用、传感器选择的有限和资源的低效使用，因为智能手机不是为 har 设计的。本文介绍了第一个既能进行在线训练又能进行推理的 har 框架。该框架从一种新的技术开始，该技术利用基于纹理的拉伸传感器和加速度计的快速傅立叶变换和离散小波变换生成特征。利用这些特点，我们设计了一个人工神经网络分类器，该分类器是利用策略梯度算法在线训练的。在低功耗**物联网**设备（ty-cc2650 mcu）上对 9 个用户进行的实验显示，在识别 6 个活动及其转换时的精度为 97.7%，功耗低于 12.5 mw。少

2018 年 8 月 26 日提交;最初宣布 2018 年 8 月。

评论:本论文已被接受在 iccad 2018 中发表。最终版本将出现在 iccad 2018 的会议记录中

113. **第 1808.08549[pdf,其他] Cs。铬**

物联网的可信和优先感知传感

作者:ihtesham haider, bernhard riner

摘要: 物联网（**iot**）被认为是智能服务的关键使能技术。由于商品设备的广泛使用，安全性和隐私是**物联网**应用面临的严峻挑战。这项工作介绍了两种基于硬件的轻量级安全机制，以确保传感器的感知数据可信度（即感知数据保护和传感器节点保护）和使用隐私（即检测数据的隐私感知报告）。集中式和分散的**物联网**应用。物理上不可克隆的函数（puf）构成了这两个机制的基础。为了证明我们基于 puf 的方法的可行性，我们在三个平台（atmel 8 位 mcu、arm 皮层 m4 32 位 mcu 和 zynq7010 soc）上实现和评估了 puf，具有不同的复杂性。我们还在一个视觉传感器节点上实现了我们的可信传感和隐私感知报告方案（用于集中式应用）和安全节点方案（适用于分散应用），该节点节点由 ov5642 图像传感器和 zynq7010 soc 组成。我们的实验评估显示了我们的安全机制所产生的低开销延迟、存储、硬件和通信。少

2018 年 8 月 26 日提交;最初宣布 2018 年 8 月。

评论:日记本

114. **第 1808.08443[pdf,其他] Cs。铬**

多伊 10.1109/JIOT.2018.2864168

物联网中的隐私：从原则到技术

作者:李超,巴拉吉·帕拉尼萨米

摘要: 无处不在的低成本智能设备的部署和高速无线网络的广泛使用，导致了物联网(**iot**）的快速发展。**物联网**包含了无数未参与传统互联网的物理对象，使它们能够进行交互和合作，从而提供广泛的**物联网**应用。**物联网**中的许多服务可能需要全面了解和分析通过大量物理设备收集的数据，这些设备既挑战了个人信息隐私，也挑战**了物联网**的发展。**物联网**中的信息隐私是一个广泛而复杂的概念，因为它的理解和感知因个人而异，其实施需要立法和技术的努力。本文回顾了隐私法的最新原则、**物联网**的架构以及具有代表性的隐私增强技术（pet）。我们分析如何通过在分层**物联网**架构模型的各个层中仔细实施隐私增强技术（pet）来支持法律原则，以满足与之互动的个人的隐私要求**物联网**系统。我们展示了隐私立法如何映射到隐私原则，这反过来又推动了**在物联网**架构堆栈中应用的必要隐私增强技术的设计。少

2018 年 8 月 25 日提交;最初宣布 2018 年 8 月。

115. 第 1808.08006[pdf,其他] cs.it

通过支持超宽带的蜂窝网络实现高效节能的大规模物联网共享频谱访问

作者:ghaith hattab, danijela cabric

摘要: 提供与大量传感器和机器（通常称为 "**物联网" (iot)**）的连接，已成为第五代新收音机（5g-nr）的重要用例。然而，现有的传输协议（如正交分配或频谱共享）可能会由于拥塞和干扰或资源分割的增加而对蜂窝用户（ue）和**物联网**设备有害。为此，我们考虑为蜂窝网络配备无人驾驶飞行器（uav），例如无人机，作为移动数据聚合器。具体来说，我们提出了**物联网**设备和 ui 之间共享频谱访问的传输协议，其中**物联网**流量由无人机收集，然后聚合到蜂窝网络。利用随机几何，分析了该协议的性能，并与现有协议进行了比较。此外，我们还提出了一个随机优化框架，该框架优化**了物联网**器件的发射功率，以最大限度地提高典型**物联网**器件的平均能效（ee），同时受到 ui 的干扰约束。仿真结果验证了所提出的传输协议和功率控制的有效性，表明**了物联网器件 ee** 的显著改进，与相比，对 ue 频谱效率的降低最小。现有的传输方案。少

2018 年 8 月 24 日提交;最初宣布 2018 年 8 月。

评论:提交给 ieee 无线通信交易

116. 建议: 1808.07432[pdf,其他] Cs。铬

多伊 10.114/3229565.3229567

智能家居物联网的友好型图书馆

作者:trisha datta, noah apthorpe, nick feamster

摘要: 在过去几年中，互联网连接设备的数量和种类大幅增长，给安全和隐私带来了新的挑战。研究表明，网络对手可以使用来自消费者**物联网**设备的流量速率元数据来推断敏感的用户活动。将流量调整为适合独立于用户活动的发行版可以保护隐私，但由于开发人员的工作量和开销带宽成本，这种方法几乎没有被采用。在这里，我们为**物联网**开发人员提供了一个 python 库，以便轻松地将隐私保护流量整形集成到他们的产品中。该库将标准网络功能替换为通过有效负载填充、碎片和随机覆盖流量的组合自动混淆设备流量模式的版本。我们的库成功地保护了用户隐私，并要求大约 4 kbn 的架空带宽为**物联网**设备具有较低的发送率或较高的延迟容忍度。考虑到美国家庭的正常互联网速度，这种开销是合理的，是对现有解决方案带宽要求的一种改进。少

2018 年 8 月 22 日提交;最初宣布 2018 年 8 月。

评论:6 页, 6 个数字

日记本参考:2018 年物联网安全与隐私研讨会论文集, 43-48 页, 2018 年 8 月

117. 第: 1808.07379[pdf] cs. cy

从基于 iot 的智能家居中进行隐私挖掘

作者:李明昌,金春林,奥拉夫

摘要: 最近, 各种智能设备被部署在各种环境中, 以提高人类生活质量。基于**物联网**的重要应用之一是智能家居, 特别是老年人的智能家居。**基于物联网的**智能家居使老年人的健康得到适当的监测和照顾。然而, 由于网络通信不受充分保护或其他原因, 老年人的隐私可能会从智能家居中披露。为了说明这个问题有多严重, 我们在本文中介绍了一种从智能家居中挖掘隐私的隐私挖掘方法 (pma), 方法是对智能家居产生的传感器数据集进行一系列的推导和分析。实验结果表明, pma 能够为智能家居推导出全球传感器拓扑结构, 并在家庭布局方面披露长者的隐私。少

2018 年 9 月 11 日提交;v1 于 2018 年 8 月 18 日提交;最初宣布 2018 年 8 月。

评论:本文件有 11 页和 7 位数字, 已于 2018 年 8 月 13 日被 2018 年 bwcca 接受

118. 第 188.07355[pdf,其他] Cs。镍

碎片是对物联网成功的威胁吗?

作者:mohab aly, foutsekhomh , yann-gaël guéhneuc, hironori washizaki, soumaya yacout

摘要: 当前分布式事物协作的革命被视为**物联网**开发各种服务的第一阶段。这种合作受到当今行业分散的威胁, 因为它带来了难以将各种技术纳入系统所带来的挑战。多样化的网络技术导致互操作性问题, 从而限制了重用数据开发新服务的可能性。必须提供处理数据收集的不同方面, 以便为交互的各种对象提供互操作性;但是, 随着协作设备技术数量的不断增加, 这些方法会在环境中带来严重的性能缺陷, 因此这些方法受到了挑战。少

2018 年 8 月 2 日提交;最初宣布 2018 年 8 月。

评论:16 页, 2 个数字, 物联网杂志 (http://ieee-iotj.org)

119. 第 188.07202[pdf,其他] cs. cy

食品计算综述

作者:关伟清,姜树强,刘林虎,荣瑞,拉梅什·杰恩

摘要: 食物对人类生活非常重要, 对人类的体验也是必不可少的。与食品相关的研究可以支持多种应用和服务, 如引导人类行为、改善人类健康和了解烹饪文化。随着社交网络、移动网络和物联网 (**iot**) 的快速发展, 人们通常会上传、共享和录制食品图像、食谱、烹饪视频和食品日记, 从而产生大规模的食品数据。大规模的粮食数据提供了丰富的食品知识, 可以帮助解决人类社会的许多核心问题。因此, 现在是将与食品计算相关的几个不同问题分组的时候了。食品计算从不同来源获取和分析异质食品数据, 用于食品的感知、识别、检索、推荐和监控。在食品计算中, 采用计算方法来解决医学、生物学、美食和农学领域与食品有关的问题。大规模的食品数据和最近在计算机科学方面的突破正在改变我们分析食品数据的方式。因此, 在食品领域开展了大量工作, 针对不同的面向粮食的任务和应用。然而, 很少有系统的审查, 这些审查很好地塑造了这一领域, 并全面和深入地总结了这一领域目前的努力或详细的未决问题。在本文中, 我们将

食品计算正式化，并对各种新出现的概念、方法和任务进行了全面的概述。我们总结了食品计算的主要挑战和未来方向。这是首次针对食品领域计算技术研究的综合调查，还提供了一系列研究和技术，使在不同食品相关领域工作的研究人员和从业人员受益。少

2018 年 9 月 9 日提交;v1 于 2018 年 8 月 21 日提交;最初宣布 2018 年 8 月。

120. **第: 188.07175[pdf,其他] Cs。铬**

光学模板

作者:joe loughry

摘要: 自 2002 年以来，关于光学 tempet 的研究取得了进展，当时关于这一主题的第一篇论文是独立出现的，在一周内从世界上广泛分离的地方出现。自那时以来，脆弱性随着系统的发展而演变，因此出现了几个新的威胁媒介。尽管以太网的供应链生态系统通过使用标准化的 phy 解决方案，减少了数十亿设备的脆弱性，但包括工业环境中的物联网 (**iot**) 和通用设备在内的其他近期趋势人口、金融部门的高频交易 (hft)、欧洲一般数据保护条例 (gdpr) 和廉价无人机再次使其成为设计隐私新产品时考虑的问题。安全的一般原则之一是，漏洞一旦修复，有时就不会保持这种状态。少

2018 年 8 月 21 日提交;最初宣布 2018 年 8 月。

评论:6 页, 2 个数字; 参加了国际电磁兼容性研讨会和展览 (emc 欧洲 2018), 2018 年 8 月 27 日至 30 日，荷兰阿姆斯特丹

类:C.2.0;D.4.6;e.3;K.6。5

121. **第: 188.07163[pdf, ps,其他] cs. it**

基于符号的 5g 大容量机路通信的非正交多址 (s-noma)

作者:mostafa mohammadkarimi, muhammad ahmad raza, octavia a. dosre

摘要: 在物联网 (**iot**) 中提供数量有限的可用资源的大规模连接问题激发了非正交多重访问 (noma) 解决方案。在本文中，我们将全面回顾基于签名的 noma (s-noma) 计划，将其作为**物联网**的潜在候选方案。s-noma 中的签名表示以非正交方式在可用资源上分布的活动设备的数据流的方式。它可以根据特定于设备的码本结构、延迟模式、扩展序列、交错模式和争用序列进行设计。此外，我们还介绍了用于从接收端的非正交叠加信号解码每个设备的数据的检测算法。在脉冲噪声环境下，模拟了不同 s-noma 方案的误码率，这在机器式通信中具有重要意义。仿真结果表明，在这种情况下，s-noma 方案的性能会降低。最后，提出了面向 s-noma 的物**联网的**研究面临的挑战。少

2018 年 8 月 21 日提交;最初宣布 2018 年 8 月。

122. **第: 1808. 06874[pdf] cse**

基于 nfv 和 sdn 的分布式物联网网关，用于大规模灾难管理

作者:carla mouradian, narjes tahghigh jahromi, roch h. g 二

摘要: 大规模的灾害管理应用是**物联网**的几个现实应用之一。火灾探测和地震预警应用只是两个例子。在此类应用中使用了多个**物联网**设备，例如传感器和机器人。这些传感器和机器人通常是异质的。此外，在灾害情况下，现有通信基础设施可能会完全或部分被破坏，使移动临时网络成为提供连接的唯一替代方案。利用这些应用程序带来了新的挑战，例如需要动态、灵活和分布式网关，这些网关可以容纳新的应用程序和新**的物联网**设备。网络功能虚拟化 (nfv) 和软件定义网络 (sdn) 是新兴的范例，可以帮助克服这些挑战。本文利用 nfv 和 sdn，提出了大规模灾害管理中动态分布式网关资源调配

的体系结构。在所提出的体系结构中，网关功能被设置为虚拟网络函数 (vnf)，这些功能使用 sdn 在**物联网**域中进行实时链接。建立了样机，并给出了性能结果。少

2018 年 8 月 21 日提交;最初宣布 2018 年 8 月。

123. 第: 1808. 06 120[pdf] Cs。镍

物联网中的节能服务分配

作者:barzan yosuf, mohamed musa, taisir elgorashi, ahmed q.lawey, j. m. h. elmirghani

摘要: 物联网 (**iot**) 网络预计将涉及无数设备，从简单的传感器到功能强大的单板计算机和智能手机。嵌入式技术计算能力的巨大进步使这些设备能够集成到**物联网**网络中，从而使云功能能够扩展到更接近数据源的地方。本文研究了一种以雾和云为支撑的多层分布式**物联网**体系结构。我们优化**了物联网**服务在此体系结构中的位置，从而最大限度地降低了总功耗。结果表明，与中央云中的通用服务器相比，在**物联网**层引入本地计算可节省高达 90% 的电力。少

2018 年 8 月 18 日提交;最初宣布 2018 年 8 月。

124. 第: 1808. 06 119[pdf] Cs。镍

雾计算健康监测应用的能源效率

作者:ida syafiza m.isa , mohamed o.i. musa, taisir e.h. el-gorashi, ahmed q. lawey, jaafar m. h. elmirghani

摘要: 雾计算提供了一个可扩展和有效的解决方案，以克服不断增长的处理和网络需求的东西 (**物联网**) 设备的互联网。本文研究了雾计算在健康监测应用中的应用。我们考虑一种心脏监测应用程序，即患者在美国心脏建议的时间限制范围内，发送 30 分钟的心电图 (ecg) 信号记录，用于雾处理单元的处理、分析和决策当检测到心电图信号异常时，协会 (aha) 来挽救心脏病患者。对处理服务器的位置进行了优化，从而最大限度地降低了处理和网络设备的能耗。结果表明，与在中央云处理相比，在雾处理单元处理心电图信号可实现高达 68% 的总能耗。少

2018 年 8 月 18 日提交;最初宣布 2018 年 8 月。

125. 第 1808. 05283[pdf,其他] Cs。镍

所有一个人需要了解雾计算和相关的边缘计算范式: 一个完整的调查

作者:ashkan yousefpour, caleb fung, tam nguyen , krishna kadiyala, Fatemeh jalali, amureza niakanlahiji, jian kong, jason p. ju

摘要: 随着物**联网** (**iot**) 成为我们日常生活和环境的一部分，我们预计连接设备的数量将迅速增长。**物联网**预计将连接数十亿设备和人类，为我们带来有希望的优势。随着这一增长，雾计算及其相关的边缘计算范式，如多址边缘计算 (mec) 和云，被视为处理大量安全关键和时间敏感数据的有希望的解决方案。**物联网**生产的产品。在本文中，我们首先提供了一个关于雾计算及其相关计算范式的教程，包括它们的异同。接下来，我们提供了雾计算研究主题的分类，并通过全面的调查，对雾计算及其相关计算范式的工作进行了总结和分类。最后，为雾计算的研究提供了挑战和未来的方向。少

2018 年 9 月 6 日提交;v1 于 2018 年 8 月 15 日提交;最初宣布 2018 年 8 月。

评论:开放访问. 47 页, 7 张桌子, 11 个数字, 450 个参考。[更新: 添加新论文。这项调查的数据 (类别和特点) 现在可以公开查阅]

126. 第 xiv: 1808. 04967[pdf, ps,其他] Cs。镍

flynetsim: 一种基于 ns-3 和 ardupilot 的开源同步无人机网络模拟器

作者:sabur baidya, zoheb shaik, marco levorato

摘要: 无人飞行器系统正越来越多地用于需要广泛通信的广泛应用，要么将无人机相互连接，要么与地面资源互联。无论是专注于无人机操作的建模，还是通信和网络动力学，可用的仿真工具都无法捕获问题的这两个方面之间的复杂相互依存关系。本文的主要贡献是一个灵活和可扩展的开源模拟器--flynetsim--将这两个领域联系在一起。总体目标是能够模拟和评估在铰接式多层技术生态系统 (如城市物**联网 (iot)**) 内运行的无人机群。为此, flynetsim 接口了两个开源工具 ardupilot 和 ns-3，它们使用发布和基于订阅的中间件在系统中运行的设备之间创建单独的数据路径。flynetsim 的功能通过几个案例研究场景得到了说明，包括无人机与多技术通信基础设施的互联和群内临时通信。少

2018 年 8 月 15 日提交;最初宣布 2018 年 8 月。

评论:本文已被接受于 2018 年 10 月 28 日至 11 月 2 日在加拿大蒙特利尔举行的无线和移动系统建模、分析和仿真第 21 届国际会议 (mswiim ' 18)上发表。

127. **第 xiv:1808. 04616[pdf,其他] cs. it**

通过无线功能计算实现物联网的无线供电数据聚合: 波束形成和功率控制

作者:李晓阳,朱光旭,易功,黄开斌

摘要: 作为网络的革命，物**联网 (iot)** 旨在通过连接和利用大量分布式设备 (如传感器和执行器) 来实现我们社会运营的自动化。一个设计挑战是在巨大的**物联网**设备上实现高效的无线数据聚合 (wda)。这可以实现一系列**物联网**应用，从对延迟敏感的高移动性传感到数据密集型分布式机器学习。无线 (功能) 计算 (aircomp) 已成为一个很有前途的解决方案，通过利用模拟波在空气中的添加，将计算和通信结合起来。另一个**物联网**设计挑战是密集传感器的电池充电，可通过无线功率传输 (wpt) 进行解决。**aircomp** 和 wpt 在物联网系统中的共存要求它们进行集成，以提高 wda 的性能和效率。这推动了目前开发无线供电 aircomp (wp-aircomp) 框架的工作，通过共同优化无线功率控制、能源和 (数据) 聚合波束形成，最大限度地减少 aircomp 错误。为了得到一个实用的解决方案，我们将非凸关节优化问题重铸为等效的外部和内部子问题 (内部) 无线电功率控制和能量波束形成，以及 (外部) 高效的聚合波束形成。前者以闭合形式求解，后者则使用半定松弛技术有效地求解。结果表明，最优能量束指向 wpt 通道的显性本征方向，最优功率分配倾向于均衡不同传感器的闭环 (下行链路 wpt 和上链 aircomp) 有效通道。仿真结果表明，控制 wpt 为大幅减少 aircomp 误差提供了额外的设计尺寸。少

2018 年 8 月 14 日提交;最初宣布 2018 年 8 月。

128. **第: 1808. 04581[pdf,其他] Cs。铬**

多伊 10.1109/CNS.2018.8433209

物联网安全游戏中的黑桃 ace: 用于访问控制的灵活 ipsec 安全配置文件

作者:santiago aragon, marco tiloca, max maass, matthias hollick, shahid raza

摘要: 受约束环境的身份验证和授权 (ace) 框架在物联网中提供了细粒度的访问控制，在这些 internet 中，设备资源有限且连接有限。ace 框架定义了单独的配置文件，以指定实体的确切交互方式以及要使用的安全和通信协议。本文介绍了新的 ace ipsec 配置文件，其中指定了客户端如何使用资源服务器建立安全的 ipsec 通道，并在上下文中使用 ace 框架强制对远程资源进行授权访问。通过该配置文件，可以通过 ipsec

安全关联的直接配置或标准的 ikev2 协议建立 ipsec 安全关联。我们为 contiki os 提供 ace ipsec 配置文件的第一个开源实现，并在资源受限的 zolertia 萤火虫平台上对其进行测试。我们的实验性能评估证实，ipsec 配置文件及其操作模式经济实惠，也可在受限**的物联网**平台上部署。少

2018 年 8 月 14 日提交;最初宣布 2018 年 8 月。

杂志编号：2018 ieee 通信和网络安全会议 (cns)，北京，中国，2018，第 1-9 页

129. 第 1808. 04517[pdf] Cs。镍

5g 毫米波通信在互联车辆中的可行性

作者:sakib mahud khan, mashrur chowdhury, mizanur rahman, mhafuzul isam

摘要：物联网 (**iot**) 环境将不同的智能组件联网连接在一起，并将实现连接组件之间的无缝数据通信。互联自主车辆或 cav 是**物联网**的主要组成部分，cav 的平稳、可靠和安全运行需要可靠的无线通信系统，这可以确保高连接性、高吞吐量和低通信延迟。5g 毫米波或毫米波通信网络提供了这样的优势，这可以成为 cav 的助推器，特别是对于密集的拥堵地区。在这项研究中，我们评估了 5g 毫米波和专用短距离通信 (dsrc) 为不同的 cav 应用在网络模拟器 3 (ns-3)。对于 cav 应用，我们评估了 5g mm 波的端到端延迟、数据包丢失和数据速率 (适用于 cav 接收器和发射器)。我们发现，5g 毫米波可以支持 cav 安全应用，确保较低的延迟，而不是所需的最小延迟 200 毫秒的正向碰撞警告应用程序。对于移动应用，我们发现 5g mm 波可以支持多个具有高数据接收速率的 cav，这足以实现车载信息娱乐的实时高清视频流，平均数据包延迟为 13 毫秒。这项研究的结果表明，5g 毫米波可以成为未来在拥堵地区的 cav 的推动者。利用本文开发的评价框架，公共机构可以对 5g 毫米波进行评估，以支持其管辖范围内的交通拥堵区、商业区等拥堵地区的 cav。少

2018 年 8 月 13 日提交;最初宣布 2018 年 8 月。

评论:16 页，3 张表格，6 个数字

130. 第 1808. 03826[pdf,其他] Cs。Sy

保护网格免受高功率设备物联网僵尸网络的影响

作者:萨利赫·索尔坦, prateek mittal, h. vincent poor ' s

摘要：我们提供的方法是通过高功率设备**的物联网**僵尸网络，防止新发现的需求 manip0p (mad) 攻击导致电网线路故障。特别是，我们开发了两种算法，分别是 "在经济调度 (safe) 算法中为发电机获取附加余距" 算法和迭代微型经济调度 (immune) 算法，用于在生成器中查找可靠的操作点。经济调度，使没有线路超载后自动主控制响应任何 mad 攻击。在电网在可靠状态下的运行成本很高 (或者没有强大的操作点) 的情况下，我们提供了有效的方法来验证内置--如果可能的话，在任何 mad 攻击后的二次控制期间都可以清除线路过载。然后，我们定义αα d-鲁棒性概念的网格，表明任何线路故障可以清除在二次控制期间，如果对手可以增加/减少的需求αα分数。我们证明了实际的上限和下限的最大值αα网格是αα d-在多项式时间内可以有效地找到鲁棒性。最后，对所开发的算法和方法在现实电网测试用例中的性能进行了评价。我们的工作提供了保护网格免受 mad 攻击导致的潜在线路故障的第一种方法。少

2018 年 8 月 11 日提交;最初宣布 2018 年 8 月。

131. 第 xiv:1808. 03778[pdf,其他] Cs。铬

通过同地办公应用程序对 ble 设备的攻击

作者:paralavi Sivakumaran,豪尔赫·布拉斯科

摘要: 蓝牙低功耗 (ble) 是一种快速增长的无线技术，具有大量潜在的使用案例，尤其是在**物联网**领域。在许多使用案例中，ble 设备存储敏感的用户数据或关键设备控件，这些数据或控件可以通过增强式 android 或 ios 应用程序进行访问。不受控制地访问此类数据可能会侵犯用户的隐私，导致设备出现故障，甚至危及生命。ble 规范旨在解决这一问题，并采用网络层安全机制 (如配对和绑定)。遗憾的是，这没有考虑到许多应用程序可能位于同一移动设备上的位置，这就带来了未经授权的应用程序访问和修改存储在 ble 设备上的敏感数据的可能性。在本文中，我们提出了一种攻击，在这种攻击中，未经授权的 android 应用程序可以利用以前由授权应用程序触发的绑定关系，从 ble 设备访问配对保护的数据。我们讨论了可能的缓解策略，并对 13500 + 支持 ble 的 android 应用程序进行了分析，以确定其中有多少应用程序实施了此类策略以避免此攻击。我们的结果表明，这些应用程序中有 60% 以上没有应用层安全性形式的缓解策略，并且加密有时在实现的应用程序中实现不正确。这意味着相应的 ble 设备可能容易受到恶意应用程序未经授权的数据访问的影响。少

2018 年 8 月 11 日提交;最初宣布 2018 年 8 月。

评论:14 页, 10 个数字, 3 个表

132. 建议: 1808. 03557[pdf] Cs。铬

多伊10.5121/ijcnc.2018.10406

物联网加密的安全性分析: Simeck32/64 上的侧通道立方体攻击

作者:alya geogiana buja, shekh faisal Abdul-Latip,rabiah ahmad

摘要: simeck，一个轻量级的块密码已被提出成为可用于物联网 (**iot**) 应用的加密之一。因此，本文介绍了 simeck32/64 块密码对侧通道立方体攻击的安全性。我们展示了我们对 simeck32/64 的攻击，它使用 hamming 称重泄漏假设来提取关键位中的线性独立方程。我们只考虑了在第四轮密码中来自哈明内部状态的汉明重量泄漏的 lsb 的第二个位，就能在 32 个关键变量中找到 32 个线性独立方程。这使我们的攻击能够改进以前对 simeck32/64 的侧通道攻击模型的攻击，其时间和数据复杂度分别为 2 ^ 35 和 2 ^ 11.29。少

2018 年 8 月 10 日提交;最初宣布 2018 年 8 月。

评论:12 页, 6 个数字, 4 个表，国际计算机网络和通信杂志

日记本参考:国际计算机网络与通信杂志 (ijcnc) 第 10 卷，第 4 期, 2018 年 7 月

133. 第 xiv:1808. 03071[pdf,其他] Cs。铬

用于安全和控制商品物联网设备和域控制设备生命周期管理的基准功能

作者:markus miettinen, paul c. van oorschot , ah 发 reza sadeghi

摘要: 新兴的物联网 (**iot**) 极大地增加了家庭、工作场所和智慧城市基础设施中的连接设备数量。这就需要有办法不仅确保设备相关通信的保密性，而且确保设备配置和管理的保密性--确保只有合法设备才被授予本地域的特权，只有经过授权的代理才具有访问设备和它所持有的数据，并且软件更新是真实的。由于需要支持设备的入职、正在进行的设备管理和控制以及安全的停用，因此需要提供一套关键管理服务，用于对设备的访问控制以及设备对无线基础设施和网络资源的访问。我们确定了这一核心功能，并主张承认高效可靠的密钥管理支持 (包括**物联网**设备内的支持，以及通过统一的外部管理平台)，将其作为**物联网**世界的基准要求。我们提供了一个框架体系结构，以促进商品**物联网**方案中安全、灵活和方便的设备管理，并提供了一组说明性的协议作为基本

解决方案----不是为了促进特定的解决方案细节，而是为了突出显示基准功能，以帮助域所有者监督大量独立多供应商**物联网**设备的部署。少

2018 年 8 月 9 日提交;最初宣布 2018 年 8 月。

134. 第 xiv:1808.02741[pdf, ps,其他] Cs。铬

偷看：我看到你的智能家居活动，甚至加密了！

作者:abbasacar , hossein fereidooni, tigist ab 板, amit kumar sikder, markus miettinen, hidayetaksu, mauro conti, ahad-reza sadeghi , a. selcuk Uluagac

摘要: 智能家居环境中的各种**物联网**设备（如灯泡、开关、扬声器）使用户能够轻松控制周围的物理世界，并促进他们的生活方式。但是，智能家居环境内或附近的攻击者可能会利用这些设备使用的固有无线媒体来泄露有关用户及其活动的敏感信息，从而侵犯用户隐私。考虑到这一点，在这项工作中，我们介绍了一个新的多阶段隐私攻击的用户隐私在智能环境中。它是利用最先进的机器学习方法，通过被动地观察无线**技术,**以级联方式检测和识别特定类型的物联网设备、它们的行为、状态和正在进行的用户活动来实现的来自智能家居设备的流量。攻击有效地适用于加密和未加密的通信。我们利用一系列不同的网络协议（如 wifi、zigbee 和 ble），从一系列流行的现成智能家居**物**联网设备中进行实际测量，从而评估攻击的效率。我们的研究结果表明，对手被动嗅到网络流量可以在识别目标智能家居设备及其用户的状态和行为方面达到非常高的精度（超过 90%）。与早期的简单方法不同，我们的多级隐私攻击可以在没有大量背景知识或分析协议规范的情况下自动执行活动检测和识别。这使得对手能够有效地聚合目标用户的广泛行为配置文件。为了防止这种隐私泄漏，我们还提出了一种基于生成欺骗网络流量的对策，以隐藏设备的真实活动。我们还证明，所提供的解决方案比现有解决方案提供了更好的保护。少

2018 年 8 月 8 日提交;最初宣布 2018 年 8 月。

评论:14 页, 6 个数字

135. 第 xiv:1808.02131[pdf,其他] Cs。铬

管道僵尸网络-将绿色技术转化为水灾难

作者:ben nassi, moshe sror, ido lavi, yair meidan, asaf shabtai, yuval elovici

摘要: 目前一代的**物联网**设备正被客户和消费者用来调节从关键基础设施（如城市供水服务和智能电网）获得的资源（如水电），从而创造了一种新的攻击矢量对关键的基础设施。本研究表明，智能灌溉系统是一种新型的绿色技术和**物联网**设备，旨在节约用水和金钱，攻击者可以将其作为攻击城市供水服务的手段。我们提出了一个分布式攻击模型，攻击者可以利用商业智能灌溉系统的僵尸网络来攻击城市供水服务。然后，我们展示了在 lan can:(1) 中在受损设备上运行的机器人如何在 15 分钟内通过使用专用分类模型分析 lan 的行为来检测连接的商业智能灌溉系统（rainmachine、bluemapay 和 greeniq），并 (2) 启动通过商业智能灌溉系统浇水，根据攻击者的意愿使用欺骗和重播攻击。此外，我们还对进行这种攻击可能造成的损害进行了建模，并表明标准的水塔可以在一个小时内使用 1 355 个洒水车的僵尸网络清空，洪水水库可以使用 23, 866 洒水车的僵尸网络连夜清空。最后，我们讨论了对策方法，并假设下一代管道工是否会使用卡利 linux 而不是猴子扳手。少

2018 年 8 月 6 日提交;最初宣布 2018 年 8 月。

评论:https://www.youtube.com/watch? v=Yy8tOEhH6T0

136. 第 xiv:1808.02125[pdf,其他] Cs。铬

智能家居中的跨应用干扰威胁：分类、检测和处理

作者:迟浩田,曾强，杜晓江,于嘉萍

摘要: 出现了许多物联网（**iot**）平台，使第三方开发人员开发的各种 **iot** 应用能够实现智能家居的自动化。此前的研究主要涉及许可模型中的过度特权问题。然而，我们的工作表明，即使是遵循最小特权原则的**物联网**应用，当它们相互作用时，也会导致独特类型的威胁，称为跨应用干扰（cai）威胁。我们描述和分类新的威胁，显示意外的自动化、安全和隐私问题可能是由此类威胁造成的，而这些威胁无法由现有**的物联网**安全机制处理。为了解决这个问题，我们提出了 homeganguard，这是一个用于存储物**联网**平台的系统，用于检测和应对 cai 威胁。构建了一个符号执行器模块，以便从**物联网**应用中精确提取自动化语义。然后，将综合考虑不同**物联网**应用的语义，以评估它们之间的相互作用并系统地发现 cai 威胁。在 **iot 应用安装**过程中，会向用户提供用户界面，解释发现的威胁，以帮助他们做出决策。我们通过三星智能产品的概念验证实施来评估 homeguard，并在智能事物公共存储库中的应用程序中发现许多威胁实例。评价表明，该方法准确、有效、高效。少

2018 年 10 月 10 日提交;v1 于 2018 年 8 月 6 日提交;最初宣布 2018 年 8 月。

评论:本文件的早期版本于 2018 年 5 月 9 日提交给了 ccs18。此版本包含基于该提交的一些小修改

137. 第 1808.01895[pdf] cs.cy

地理空间分析与环境信息学中的物联网

作者:andreas kamilaris, frank stermann

摘要: 地理空间分析为更好地理解、建模和可视化我们的自然和人工生态系统提供了巨大的潜力，利用物联网作为一种普遍的传感基础设施。本文对基于**物联网**的研究工作进行了综述，在环境信息学中应用了地理空间分析。确定了六种不同的地理空间分析方法，并介绍了采用其中一些技术**的 26 项相关物联网**举措。对使用的**物联网**设备的类型、其部署状态和数据传输标准、使用的数据类型以及测量的可靠性进行分析。本文触及了这种技术和工艺组合的表面，说明**了物联网**以及地理空间分析目前在环境研究领域的应用。少

2018 年 8 月 1 日提交;最初宣布 2018 年 8 月。

评论:物联网技术在环境研究研讨会中的应用，环境信息项目 2018

138. 第 xiv:1808.01761[pdf,其他] cs.it

不完全正交条件下 lora 网络的可扩展性分析

作者:aamir mahood, emiliano sisinni, lakshmikanth Guntupalli 陆军, raúl rondón, syed ali hassan , mikael gidlund

摘要: 低功耗广域网（lpwan）技术在物联网（**iot**）应用方面的势头越来越大，因为它们有望使用无赠款的介质接入覆盖大量电池供电的设备。lorawan 凭借其物理（phy）层的设计和监管工作，已成为广泛采用的 lpwan 解决方案。通过使用带有 qausi--同安正交扩散因子（sf）的轻快扩频调制，lora phy 为广域应用提供覆盖，同时支持高密度器件。然而，到目前为止，它的可伸缩性性能还没有被充分建模，并且没有考虑到 sf 不完全正交性所产生的干扰效应。在本文中，我们提出了一个单细胞 lora 系统的分析模型，该模型解释了在同一 sf（共同 sf）和不同 sf（间 sf）上传输之间的干扰的影响。通过将干涉场建模为责任循环的 loha 下的泊松点过程，推导出了几种干扰条件下的信噪比（sir）分布。结果表明，在占空比低至 0.33 的情况下，仅在共同 sf 干扰下的网

络性能就相当乐观，因为包括 sf 之间的干扰会进一步降低成功概率和覆盖概率。约 10% 和 15%，分别适用于 lora 通道中的 1500 台设备。最后，我们说明了我们的分析如何能够根据给定的可靠性目标的单元大小来表征关键器件密度。少

2018 年 8 月 6 日提交;最初宣布 2018 年 8 月。

139. 第 xiv:1808.01412[pdf,其他] Cs。铬

用于无线物联网入侵检测的主动学习

作者:杨凯,任杰,朱燕桥，张伟义

摘要: 物联网 (iot) 在我们的日常生活中变得非常普遍，但它也面临着独特的安全挑战。入侵检测对于无线**物联网**网络的安全性和安全性至关重要。本文讨论了无线入侵检测中的人与环主动学习方法。我们首先提出了针对成功的无线**物联网**网络入侵检测系统 (ids) 的设计所面临的根本挑战。然后，我们简要回顾了主动学习的基本概念，并提出了它在无线入侵检测的各种应用中的应用。并通过实验实例说明了主动学习方法比传统监督学习方法有显著的性能改进。虽然机器学习技术在入侵检测中得到了广泛的应用，但利用机器和人的智能进行物联网入侵检测的人在**环机**学习中的应用仍处于起步阶段。希望本文能帮助读者理解主动学习的关键概念，促进这一领域的进一步研究。少

2018 年 8 月 3 日提交;最初宣布 2018 年 8 月。

评论:7 页，4 位数字，接受 ieee 无线通信

140. 第 xiv:1808.01356[pdf,其他] Cs。简历

基于深度学习的物联网和移动边缘计算嵌入式系统的多目标视觉跟踪

作者:beatriz blanco-filgueira, daniel garcía-lesta, mauro fernández-sanjurjo, víctor m. brea, paula lópez

摘要: 最先进的深度学习方法的计算和内存需求仍然是一个缺点，必须加以解决，使它们在**物联网**终端节点上有用。特别是，最近的结果表明了使用卷积神经 netwoks (cnn) 进行图像处理的前景，但对于**物联网**和移动边缘计算应用来说，软件和硬件实现之间的差距已经相当大由于其高功耗。该方案执行在 nvidia jetson tx2 开发套件上实现的低功耗和实时基于深度学习的多目标视觉跟踪。它包括摄像头和无线连接功能，并为移动和户外应用提供电池供电。使用机载摄像机 detrusc 视频数据集捕获的具有代表性序列的集合用于举例说明所提出的算法的性能，并便于基准测试。在功耗和帧速率方面的研究结果表明了在嵌入式平台上进行深度学习算法的可行性，但还需要对 cnn 的联合算法和硬件设计进行更多的努力。少

2018 年 7 月 31 日提交;最初宣布 2018 年 8 月。

评论:这项工作已提交 ieee，以便可能出版。版权可以在不通知的情况下转让，之后这个版本可能不再可以访问

141. 第 xiv:1808.002[pdf,其他] Cs。铬

多伊 10.1109/JIOT.2017.2764384

车辆自组织社交物联网网络中的密钥生成非互惠补偿与涡轮码的结合

作者:gregory epipaniou, petros karadimas, dhouha kbaier ben ismail, haider al-khateeb, ali dehghantanha, kim-kwang raymond choo

摘要: 动态车辆对车辆 (v2v) 传播通道的物理属性可用于生成高度随机和对称的加密密钥。然而，在物理层密钥协议方案中，由于固有的信道噪声和硬件损伤而产生的非互惠性会传播位分歧。这必须在对称密钥生成之前解决，这在社交物联网 (iot) 网络中(包

括在战场环境中) 是非常重要的。本文将时间可变性属性 (如三维散射和散射器的移动性) 参数化地结合在一起。因此，这是将非互惠补偿与涡轮代码结合起来，将这些功能纳入关键生成过程的首次工作。初步结果表明，与样本索引技术相比，在位不匹配率 (bmr) 和密钥生成率 (kgr) 中使用 turbo 码有了显著改善。少

2018 年 8 月 3 日提交;最初宣布 2018 年 8 月。

评论:10 页

142. 第 xiv:1808.01039[pdf,其他] Cs。镍

一种适用于无线物联网传感器网络的节能路由协议

作者:anshuman chhabra, vidushi vashishth, anirudh khanna , deepak kumar sharma, jyotsna singh

摘要: 物联网 (**iot**) 正越来越多地被应用到安全系统、智能基础设施、交通管理、天气系统等实际应用中。虽然这些应用的规模是巨大的，但设备能力有限，特别是在电池寿命和能源效率方面。尽管正在进行研究以改善这些缺陷，无线**物联网**网络仍然不能保证令人满意的网络寿命和更长的传感覆盖。此外，文献中提出的方案是复杂的，在现实世界中不容易实施。这就需要为无线**物联网**传感器网络开发一种简单而节能的路由方案。本文将物**联网**应用中设备的能量约束问题作为一个优化问题进行了建模。为了节省设备节点的能量，路由协议首先根据多个不同的功能 (如与基站的距离、数据消息长度和当前时代从环境中检测到的数据) 将设备聚合为集群。然后，为每个群集选择一个群集头，并生成一个定向无环图 (dag)，所有群集头都作为节点。边缘表示从发射器到接收机的通信意图，边缘权重是使用一个公式化的方程计算的。计算到基站的最低成本路径，以便实现高效的实时路由。睡眠调度也可选择用于进一步提高网络能效。在活动节点数量、能量动态和网络覆盖等指标方面，对所提出的路由协议进行了仿真，并优于现有的路由协议。少

2018 年 8 月 2 日提交;最初宣布 2018 年 8 月。

143. 第 xiv:1808.00664[pdf,其他] Cs。铬

多伊 10.114/3218603.3218646

利用多级互联 puf 对物联网进行高效、安全的群密钥管理

作者:顾红祥，苗拉波孔恰克

摘要: 面向群的安全通信对于物联网 (**iot**) 中的广泛应用至关重要。随着技术的发展，放置在隐私敏感环境中的基于物**联网**的应用程序中与面向群体的通信相关的安全问题已成为一个主要问题。不幸的是，许多**物联网**设备的设计是便携式和重量轻的;因此，它们的功能，包括安全模块，受到有限的能源资源 (例如电池容量) 的严重限制。为了解决这些问题，我们提出了一个基于新的物理不可压缩函数 (puf) 设计的群密钥管理方案: 多级互联 puf (mipuf)，以确保在能源受限的环境中进行群通信。我们的设计能够执行关键管理任务，如密钥分发、密钥存储和安全高效地重新加密。我们证明了我们的设计是安全的，反对多种攻击方法，我们的实验结果表明，与最先进的基于椭圆曲线加密 (ecc) 的密钥管理方案相比，我们的设计在全球节省了 47.33 的能源。少

2018 年 8 月 2 日提交;最初宣布 2018 年 8 月。

评论:6 页, 4 位数字，低功耗电子与设计国际研讨会

日记本参考:低功耗电子与设计国际研讨会论文集。含该委员会, 2018

144. 第 xiv:1808.00386[pdf] Cs。直流

多伊10.1109/MCOM.2016.1600460CM

基于标准的物联网的全球语义互操作性

作者:erno kovacs, martin bauer, jaeho kim, Jaeseokyun, franck le gall, mémxuan zhao

摘要: 全球**物联网**服务 (giots) 正在将本地可用**的物联网**资源与基于云的服务相结合。他们的目标是全球服务。giots 需要本地安装的异构**物联网**系统之间的互操作性。语义处理是实现数据中介和基于知识的处理的一项重要技术。本文介绍了使用国际标准 (如 onem2m 和 oma ngsi-910 上下文接口) 实现全球语义互操作性的系统体系结构 (在欧洲未来互联网平台 fiware 中使用)。语义还支持使用基于知识的语义处理代理。此外, 我们还解释了语义验证如何能够对这种复杂的系统进行测试。少

2018 年 8 月 1 日提交;最初宣布 2018 年 8 月。

评论:欧洲联盟 (欧盟), fp7 fi-core, 赠款协议 no 632893, 地平线 2020 fiesta 赠款协议 no 643943, 欧盟-韩国, 地平线 2020 wi-iot 授权协议 723156, 韩国, iitp, 韩国政府 mssip no.b0184-15-1003

日记本参考:e. kovacs, m. bauer, j. kim, j. yun, f. le gall and m. zhao, "物联网的基于标准的全球语义互操作性", 载于 ieee 通信杂志, 第 54 卷, 第 12-46 页, 2016 年 12 月

145. 第 1808. 00277 [pdf, ps,其他] cs. it

5g 及以后的非正交多址

作者:刘元伟,秦志金, maged elkashlan, zhiguo ding, arumugam nallanathan, lajos hanzo

摘要: 在先进多媒体应用程序 (如超高清视频、虚拟现实等) 对无线容量要求迅速升级的推动下, 以及互联网对用户访问的需求急剧增加的推动下第五代 (**5g**) 网络在支持大规模异构数据通信方面面临挑战。最近为第三代伙伴关系项目提出的非正交多重接入 (noma) 是一项很有前途的技术, 可以通过以下方式应对 5g 网络中的上述挑战:在同一正交资源块中容纳多个用户。通过这样做, 可以通过传统的正交多址 (oma) 技术显著提高带宽效率。这促使许多研究人员在这一领域投入了大量的研究贡献。在此背景下, 我们全面概述了功率域多路复用辅助 noma 的最新技术, 重点介绍了 noma 的理论原理、多天线辅助 noma 设计、noma 与协同传输之间的相互作用, 关于 noma 的资源控制, 关于 noma 与其他新兴的潜在 5g 技术的共存, 以及与其他 noma 变种的比较。与其他现有的 noma 技术相比, 我们强调了功率域多路复用 numa 的主要优势。我们总结了 noma 现有研究贡献的挑战, 并提供了潜在的解决方案。最后, 我们为 noma 系统提供了一些设计指南, 并为未来确定了有希望的研究机会。少

2018 年 8 月 1 日提交;最初宣布 2018 年 8 月。

评论:本文被《 ieee 学报》所接受

146. 第 1807. 11850 [pdf] Cs。铬

低功耗物联网设备的网络攻击缓解和影响分析

作者:asutosh bandekar, ahmad y. javaid

摘要: 近年来, 无线传感器设备及其作为**物联网**的重生出现了指数级发展, 在灯泡、风扇和微波等无线家庭设备中也越来越受欢迎。由于它们可用于医疗设备、环境研究、消防部门或军事应用等各个领域, 因此这些低功耗设备的安全性始终是所有用户和安

全专家关注的问题。如今，用户希望通过智能手机通过互联网连接控制所有这些 "智能 " 无线家庭设备。对这些设备的分布式攻击等攻击将使整个系统变得脆弱，因为这些攻击可以记录和提取机密信息，并增加整个网络的资源 (能源) 消耗。本文提出了一种网络攻击检测算法，并将易于启动的网络攻击作为**物联网**器件模型，对低功耗 mote (z1 zolertia) 进行了影响分析。我们还给出了具有和不攻击的功耗分析的详细结果，以及在实现入侵检测缓解算法时的结果。少

2018 年 7 月 31 日提交;最初宣布 2018 年 7 月。

147. **第 1807. 11023[pdf] Cs。铬**

物联网 (iot) 安全的机器和深度学习方法综述

作者:mohammed ali al-garadi, amr mohamed, abdulla al-ali, xi 晓江 du , mohsen guizani

摘要: 物联网 (**iot**) 集成了数十亿智能设备，这些设备可以在最少的人为干预下相互通信。它是计算史上发展最快的领域之一，到 2020 年底估计有 500 亿台设备。一方面，**物联网**在增强可提高生活质量的多个现实生活智能应用方面发挥着至关重要的作用。另一方面,**物联网**系统的跨领域性质以及部署此类系统所涉及的多学科组成部分带来了新的安全挑战。对**物联网**设备及其固有漏洞实施加密、身份验证、访问控制、网络安全和应用程序安全等安全措施是无效的。因此，应加强现有的安全方法，以有效地保护**物联网**系统的安全。在过去的几年里，机器学习和深度学习 (ml/dl) 有了相当大的进步，机器智能已经从实验室的好奇心过渡到了几个重要应用中的实际机械。因此, ml/dl 方法对于将**物联网**系统的安全性从仅仅促进设备之间的安全通信转变为基于安全的智能系统非常重要。这项工作的目的是提供一个关于 ml/dl 方法的全面调查，这些方法可用于开发**物联网**系统的增强安全方法。介绍了与固有或新引入的威胁相关的**物联网**安全威胁，并讨论了各种潜在**的物联网**系统攻击面以及与每个表面相关的可能威胁。然后，我们深入回顾了用于**物联网**安全的 ml/dl 方法，并介绍了每种方法的机会、优势和缺点。我们讨论了将 ml/dl 应用于**物联网**安全所涉及的机遇和挑战。这些机遇和挑战可以作为未来潜在的研究方向。少

2018 年 7 月 29 日提交;最初宣布 2018 年 7 月。

148. **第 xiv:1807. 10884[pdf,其他] Cs。铬**

基于物理不可克隆功能的物联网安全密钥共享

作者:张继良

摘要: 在许多物联网 (**iot**) 应用中, cpu、内存和电池电源等资源有限，无法负担传统的加密安全解决方案。硅物理不克隆函数 (puf) 是一种轻量级的安全基元，它利用芯片制造过程中的制造变化进行密钥生成和设备认证。环形振荡器 (ro) puf 作为最流行的硅弱 puf 之一，可以通过比较任何两个 ro 之间的频率差产生秘密位。以前的 ro puf 通过添加冗余的 ro 来提高灵活性和可靠性，这会产生不可接受的硬件开销。此外，传统的弱 puf (如 ro puf) 会为每个设备生成芯片唯一密钥，这限制了它们在安全协议中的应用，在这些协议中需要在资源受限的设备中共享相同的密钥。为了解决这些缺点，我们提出了一个交叉 ro puf (cro puf)，以提高灵活性和可靠性，并减少硬件开销。它是第一个能够在物理上生成共享密钥的 puf。其基本思想是在每个级别的逆变器中使用基于查阅表 (lut) 的跨阶段交叉结构实现一对一的输入输出映射。跨阶段交叉结构的配置位和不同的 ro 选择带来的挑战带来了很高的灵活性。因此，借助跨阶段交叉结构的灵活配置和挑战, cro puf 可以为资源受限的设备生成相同的共享密钥，从而实现轻量级

密钥共享协议的新应用。实验结果表明，与以往可配置的 ro puf 相比，我们提出的 puf 结构具有更低的硬件开销、更好的唯一性和可靠性。少

2018 年 10 月 29 日提交;v1 于 2018 年 7 月 27 日提交;最初宣布 2018 年 7 月。

评论:12 页, 13 位数字

149. **第 xiv:1807. 10438[pdf] Cs。铬**

多伊 10.1016/j.future.2017.07.060

物联网安全与取证：挑战与机遇

作者:mauro conti, ali dehghantanha, k 不安 in franke, steve watson

摘要: 物联网 (**iot**) 设想普及、互联和智能节点自主交互，同时提供各种服务。**物联网**对象分布广泛、开放性强，处理能力相对较高，使其成为网络攻击的理想目标。此外，由于许多**物联网**节点正在收集和处理私人信息，它们正在成为恶意行为者的数据宝库。因此，在成功部署**物**联网网络时，安全性，特别是检测受损节点的能力，以及收集和保存攻击或恶意活动的证据，将成为优先事项。在本文中，我们首先介绍**了物联网**领域中现有的主要安全和取证挑战，然后简要讨论了在这一特殊问题中发表的针对已确定挑战的论文。少

2018 年 7 月 27 日提交;最初宣布 2018 年 7 月。

150. **第 1807. 10234[pdf,其他] Cs。铬**

radis：分布式物联网服务的远程认证

作者:mauro conti, edlira dushku, luigi v. mancini

摘要: 远程认证是一种安全技术，通过这种技术，名为 prover 的可能不受信任的设备可以向称为验证程序的外部受信任方证明其当前状态。远程认证协议的主要目的是保证证据的可靠性，以便验证程序能够远程验证证明程序的可信度。在物联网 (**iot**) 系统中，现有的远程认证协议旨在通过检测每个 iot 设备来检查每个**设备的**完整性。修改后的软件和物理篡改攻击。然而，在互联的**物联网**系统中,**物联网**设备之间进行独立交互，受到损害的**物联网**服务可以影响其他调用服务的真正操作，而无需更改软件。在本文中，我们展示了分布式**物联网**服务中的受损服务如何在真正的服务上诱发恶意行为，并强调了分布式服务认证的必要性。我们提出了分布式**物联网**服务 (radis) 远程认证协议，该协议为分布式**物联网**服务的可信度提供了完整的证据。radis 依靠控制流认证技术来检测由于与恶意远程服务的**交互而执行意外操作的物联网**服务。此外, radis 还跟踪**物联网**分布式服务之间的交互，允许验证程序检查活动是否遵循合法的交互模型。我们讨论了我们的协议在验证分布式**物联网**服务的完整性状态方面的有效性。少

2018 年 7 月 26 日提交;最初宣布 2018 年 7 月。

评论:10 页, 8 个数字, 1 个表

151. **建议: 1807. 09333[pdf,其他] Cs。镍**

自组织低功耗物联网网络：一种分布式学习方法

作者:amin azari, cicek cavdar

摘要: 实现大规模节能物联网 (**iot**) 连接是实现网络化社会的重要一步。虽然传统的广域无线系统高度依赖于网络端协调，但信令消耗的能量水平以及**物联网**设备数量的预期增加，使得这种集中式方法在未来。在这里，我们通过从过去的通信**中**学习物联网网络的自我协调来解决这个问题。为此，我们首先研究了适用于**物联网**通信的低复杂性分布式学习方法。然后，我们提出了一个学习解决方案，使设备的通信参数适应环境，以

最大限度地提高数据传输的能源效率和可靠性。此外，利用随机几何的工具，我们根据集中协调来评估所提出的分布式学习解决方案的性能。最后，我们分析了能效、通信在噪声和数据通道干扰下的可靠性以及对数据和反馈通道上的对抗干扰的可靠性之间的相互作用。仿真结果表明，与目前的先进方法相比，采用该学习方法可以显著提高**物联网**通信的能效和可靠性。这些通过轻量级学习实现的有希望的结果，使我们的解决方案在许多低成本**低功耗物联网**应用中处于有利地位。少

2018 年 7 月 15 日提交;最初宣布 2018 年 7 月。

评论:ieee 环球公司 2018

152. 第 1807. 08461 [pdf] Cs。Db

一种基于缓存的查询增强知识库的优化器

作者:wei emma zhang, quan z.sheng , scahram dustdar

摘要: 随着物联网 (**iot**) 等新兴技术的出现，我们物理世界和环境的信息收集可以以更高的粒度实现，这些详细的知识将在改善生产力、运营效率、决策和确定经济增长的新商业模式。有效地发现和查询此类知识仍然是一项关键挑战，因为与知识库接口 (例如 sparql 终结点) 的连接能力有限，而且延迟很高。在本文中，我们在 sparql 终结点上为知识库提供了一个查询系统，该知识库比最先进的系统执行查询的速度更快。我们的系统采用了基于缓存的优化方案，通过预先提取和缓存预测的潜在查询结果来提高查询性能。对来自 dbpedia 和链接地理数据的 sparql 端点的查询集的评估展示了我们方法的有效性。少

2018 年 7 月 23 日提交;最初宣布 2018 年 7 月。

评论:9 页, 3 个数字

153. 第: 1807. 07737 [pdf,其他] Cs。铬

基于电压过标的轻量级认证中的机器学习攻击与防御

作者:张继良,苏海汉

摘要: 在资源受限**的物联网**应用程序中部署轻量级安全协议是一项具有挑战性的任务。为了解决这个问题，最近提出了一种基于电压过标 (vos) 过程中生成的设备签名的面向硬件的轻量级身份验证协议。基于 vos 的身份验证使用加载项等计算单元生成与密钥组合的进程变化相关错误，以创建双因素身份验证协议。本文提出了基于机器学习 (ml) 的建模攻击来破坏这种身份验证。我们还提出了一种基于密钥 (domk) 的动态模糊机制，用于基于 vos 的身份验证，以抵御 ml 攻击。实验结果表明，在部署所建议的 ml 弹性值后, ann、mn 和 cma-es 可以克隆基于 vos 的身份验证的质询响应行为，预测精度高达 99.65，而预测精度低于 51。2 技术。少

2018 年 10 月 18 日提交;v1 于 2018 年 7 月 20 日提交;最初宣布 2018 年 7 月。

评论:7 页, 10 个数字

154. 第 xiv: 1807. 07711 [pdf,其他] cs. it

物联网网络中非正交多址的盲信号分类

作者:崔民秀,大中云,金俊勋

摘要: 对于基于非正交多址 (noma) 的下行多用户 (mu) 传输，需要先进的接收器策略来消除用户间的干扰，例如连续干扰消除 (sic)。只有在用户终端 (ut) 一侧知道有关共计划信号的信息时, sic 过程才可适用。特别是, ut 在对信号进行解码之前，应知道接收到的信号是 oma 还是 noma，是否需要 sic，以及对叠加 ut 使用了哪些调制顺

序和功率比。一个高效的网络（**如物联网（iot）**）要求 ut 盲目地对接收到的信号进行分类，并应用匹配的接收策略来减少高层信令开销并提高资源效率。本文首先分析了 noma 信号分类中的错误对性能的影响，并解决了实际**基于物联网**的 mu 使用案例中随之而来的接收器挑战。为了减少盲信号分类误差，我们提出了根据传输信号格式将数据符号或飞行员旋转到特定相位的传输方案。在飞行员旋转的情况下，还提出了一种新的信号分类算法。通过密集的仿真结果验证了该方法的性能改进。少

2018 年 7 月 20 日提交;最初宣布 2018 年 7 月。

评论:11 页，15 个数字，提交给物联网杂志

155. 建议: 1807. 0787[pdf,其他] Cs。直流

基于区块链技术的基于微服务的智能监控架构

作者:deeraj n 久, roghuu, seyed yahya nikouei, yu chen

摘要: 虽然物联网（**iot**）技术增强的智能监控系统已成为智能城市的重要组成部分，但它也带来了数据安全的新问题。与采用整体架构进行监测和记录等较低级别操作的传统监控系统相比，现代监控系统有望支持更具可扩展性和分散性在大容量分布式边缘设备上进行高级视频流分析的解决方案。此外，由于缺乏对监控源的保护，传统监控系统的集中架构容易受到单点故障和隐私侵犯的影响。本文介绍了一种基于微业务架构和区块链技术的新型安全智能监控系统。将视频分析算法封装为各种独立的微服务，不仅可以隔离来自不同扇区的视频馈送，还可以通过分散操作来提高系统的可用性和鲁棒性。区块链技术可安全地在跨监视域的微服务之间同步视频分析数据库，并在无信任的网络环境中提供数据篡改。支持智能合同的访问授权策略可防止任何未经授权的用户访问微服务，并为智能监控系统提供可扩展、分散和细粒度的访问控制解决方案。少

2018 年 7 月 19 日提交;最初宣布 2018 年 7 月。

评论:作为立场文件提交给第一届 block 连锁可持续智能城市国际研讨会（bless 2018）

156. 第: 1807.07460[pdf, ps,其他] cse

基于模型的 iot 智能城市应用监控

作者:matteo oru, marco mobilio , anas shatnawi, oliviero riganelli, alessandro tundo, leonardomariani

摘要: 智能城市是未来的城市聚合，在这里，众多异构系统和**物联网**设备进行交互，以提供更安全、更高效和更环保的环境。智能城市的愿景正相应地适应软件和**基于物联网**的服务的演变。目前的趋势不是要有一个大的综合系统，而是有大量的小型、综合的系统相互作用。由于多种原因，监测这类系统具有挑战性。少

2018 年 7 月 19 日提交;最初宣布 2018 年 7 月。

157. 特别报告: 1807. 07422[pdf,其他] Cs。直流

具有轻量级物联网客户端的区块链系统的延迟和通信权衡

作者:pietro danzi, anders e. kalör, Čedomir stefanović, petar popovski

摘要: 新兴的区块链协议提供了一种分散的体系结构，适用于支持物联网（**iot**）交互。但是，对于低功耗和内存受限的设备来说，保留区块链分类帐的本地副本是不可行的。因此，它们配备了轻量级软件实现，仅在更新时从区块链网络下载有用的数据结构，例如帐户状态。本文考虑和分析了一种由区块链网络节点实现的新方案，该方案定期对区块链数据进行聚合，进一步降低了互联**物**联网设备的通信成本。我们表明，聚合周期

应该根据通道质量、提供的速率和有用数据结构更新的统计来选择。这些结果为 ethereum 协议提供了一些好处，说明了聚合方案在降低设备占空比方面的好处，特别是在信噪比较低的情况下，以及在下行链路（例如，从无线基站到**物联网**设备）。该方案的一个潜在应用是让 **i o t** 设备要求比实际需要更多的信息，从而增加其隐私，同时保持通信成本不变。总之，我们的工作是首次为具有无线连接的轻量级区块链协议的设计提供严格的指导。少

2018 年 10 月 17 日提交;v1 于 2018 年 7 月 19 日提交;最初宣布 2018 年 7 月。

评论:本文件已提交出版

158. **建议: 1807. 07363[pdf] cse**

网络物理微服务和基于 iot 的框架: 可进化装配系统的案例

作者:kléanthamaboulidis, danai c. vachtsevanou , ioanna kontou

摘要: 制造业正面临着满足客户个性化需求的挑战，这些需求导致产品种类的增加和体积的减少。可进化装配系统 (as) 是在过去几年中定义的，目的是使制造资产能够快速适应不断变化的市场需求。与此同时，由于第四次工业革命，即工业 4.0，制造业时代正在发生变化，这将使传统的制造业环境转变为以**物联网**为基础的环境。在此背景下，本文提出了一个基于网络物理微服务和**物联网**的 as 框架，目的是利用微服务和**物联网**技术的优势，同时也利用现有的巨额投资。基于这一领域的传统技术。该框架为建立装配系统专家和**物联网**专家的通用词汇提供了坚实的基础，并为获取由模型驱动的工程方法所利用的领域知识提供了坚实的基础。as 的开发和运营。采用了组装日常生活产品的案例研究，以证明即使是这一领域的非专家也采用了这种方法。少

2018 年 7 月 19 日提交;最初宣布 2018 年 7 月。

评论:12 页, 16 位数字

159. **建议: 1807. 06724[pdf,其他] Cs。铬**

应对物联网中的安全和隐私挑战

作者:arsalan mosenia

摘要: 物联网 (**iot**) 也被称为 "对象互联网"，被认为是一种整体和变革性的方法，可提供众多服务。各种通信协议的迅速发展和收发器的小型化，以及传感技术的最新发展，为将孤立的设备转化为智能通信提供了机会。智能的东西，可以感知，存储，甚至处理电气，热，光学，化学和其他信号，以提取用户/环境相关的信息，使服务只受到人类想象力的限制。尽管**支持物联网**的系统承诺如画如画，但智能设备集成到标准 internet 中带来了一些安全挑战，因为大多数互联网技术、通信协议和传感器都没有旨在支持**物联网**。最近的几项研究表明，针对**支持物联网**的系统，特别是基于可穿戴医疗传感器 (wms) 的系统，发动安全隐私攻击可能会导致灾难性的情况和危及生命的情况。条件。因此，需要积极研究**和积极解决物联网**领域中的安全威胁和隐私问题。在本文中，我们解决了与**支持物联网**的系统相关的几个特定领域的安全/隐私挑战。少

2018 年 7 月 17 日提交;最初宣布 2018 年 7 月。

评论:博士论文 (短版)

160. **建议: 1807. 06463[pdf, ps,其他] cs. it**

lpwa 物联网网络的性能评价与优化: 一种随机几何方法

作者:amin azari, cicek cavdar

摘要: 近年来，利用无赠款无线电接入实现低功耗广域 (lpwa) 物联网 (**iot**) 连接已引起广泛关注。针对 lpwa **物联网**网络研究不足的问题，本文致力于此类网络的可靠性建模、电池寿命分析和操作控制。我们推导了接入点密度、通信带宽、异构源通信量和通信服务质量 (qos) 之间的相互作用。所提出的分析框架包括具有相关部署位置和时频异步无线电资源使用模式的异构源干扰建模。推导出的表达式分别表示设备的操作区域和速率、设备的能源和成本资源以及接入网络，以达到通信中的一定数量。例如，我们的表达式通过增加传输副本的数量、传输功率、接入点的密度和通信带宽来指示 qos 的预期增加。我们的结果进一步揭示了此类网络的可扩展性，并找出了扩展资源可以补偿流量和 qos 需求增长的界限。最后，我们提出了**物联网**设备的能源优化操作控制策略。仿真结果证实了所导出的分析表达式的紧密性，并表明它们在**物联网**网络的规划和操作控制中的有效性。少

2018 年 7 月 15 日提交;最初宣布 2018 年 7 月。

评论:ieee globecom 2018. arxiv 管理说明: 文本与 arxiv:1804. 09464 重叠

161. xiv:180. 7.06462[pdf,其他] Cs。铬

spoc: 外包计算的安全付款

作者:michaèról , ioannis psaras

摘要: **物联网**网络中的受限设备通常需要外包资源密集型计算或数据处理任务。目前，这些工作大多是在集中云中完成的。然而，随着设备数量的迅速增加和生成数据的数量的增加，边缘计算代表了一种效率更高的解决方案，可降低成本、延迟并提高用户的隐私。为了能够在边缘广泛部署执行节点，请求设备需要一种支付提交任务的方法。我们提出 spoc-一个安全的支付系统的网络，其中节点彼此不信任。spoc 允许任何节点执行任务，包括结果验证和强制用户的适当行为，而无需第三方、复制或昂贵的计算证明。我们使用以太智能合同和英特尔 sgx 实施我们的系统，并提供首次评估，证明其安全性和较低的使用成本。少

2018 年 7 月 17 日提交;最初宣布 2018 年 7 月。

162. 第: 1807. 06193[pdf,其他] Cs。直流

基于容器的群集业务流程系统: 分类和未来方向

作者:maria a. rodriguez , rajkumar buyya

摘要: 容器、支持轻量级环境和性能隔离、快速灵活的部署以及细粒度的资源共享，除了硬件虚拟化外，在更好的应用程序管理和部署中也越来越受欢迎。它们正被组织广泛用于在专有集群或私有云数据中心部署来自现代应用程序 (如 web 服务、大数据和**物联网**) 的日益多样化的工作负载。这导致了容器编排平台的出现，这些平台旨在管理大型集群中容器化应用程序的部署。这些系统能够在数千台机器上运行几十万个作业。要有效地做到这一点，他们必须解决几个重要的挑战，包括可伸缩性、容错能力和可用性、有效的资源利用率以及请求吞吐量最大化等。本文研究了这些管理系统，并提出了一种分类方法，确定了可用于应对上述挑战的不同机制。然后，拟议的分类被应用于各种最先进的系统，从而确定文献中的开放研究挑战和差距，作为从事这一专题工作的研究人员的未来方向。少

2018 年 7 月 16 日提交;最初宣布 2018 年 7 月。

163. 第 1807. 05805[pdf,其他] Cs。镍

比特冲浪: 外包符号生成的无线通信

作者:ageliki tsioliaridou, christos liaskos, sotiris ioannidis

摘要: 纳米**物联网**实现了广泛的突破性技术，但由于规模的极端，在实施方面面临挑战。空间限制造成了严重的电源考虑，以至于仅仅几个数据包传输就足以耗尽最先进的电源。反过来，这也意味着即使是基本操作 (如寻址和路由) 也很难开发高效的协议。目前的工作提出了一个新的网络适配器体系结构，可以解决这些挑战。bit 面连接适配器不会生成数据包，因此消除了对相应传输电路和功耗的需求。相反，它依赖于外部符号生成器。bit 面讯适配器读取传入符号，等待预期的消息出现在符号流中。然后发出一个短的 (1 位)、低能脉冲来通知相邻节点。bit 面适配器表现出永久 (甚至无电池) 操作，能够在没有介质访问控制的情况下运行，同时对应用程序完全透明。此外，它们的操作是事件驱动的，允许无时钟的实现。新的适配器在模拟的多跳纳米物联网网络中进行评估，并在任何拥塞级别下提供近乎完美的数据包传输速率，几乎没有冲突。少

2018 年 7 月 16 日提交;最初宣布 2018 年 7 月。

评论:论文被接受在 ieee camad 2018 主轨道上发表。由欧盟通过 "地平线 2020: 未来的新兴主题" 提供资金 (f 异 open)，授予欧盟 736876, visorsurf 项目 (http://www.visorsurf.eu)

164. **第: 1807. 0761[pdf,其他] cs. cy**

"隐私是无聊的点": 用户对物联网的感知和行为

作者:meredydd williams, jason r. c. 护士, sadie creese

摘要: 在民意调查中，公众经常声称重视自己的隐私。然而，个人似乎常常忽视这一原则，造成了一种被称为 "隐私悖论" 的差异。物联网 (**iot**) 的发展经常被认为会危及隐私。然而，在**物联网**中，悖论仍未得到充分探索。在解决这个问题时，我们首先进行了一次在线调查 (n = 170)，以比较 iot 和不那么新颖的设备的公众意见。尽管我们发现用户感知隐私风险，但许多用户仍决定购买智能设备。由于**物联网**的使用量较低，我们断言它限制了保护行为。为了探索这一假设，我们与公众进行了情境化访谈 (n = 40)。在这些对话中，业主用个人设备讨论自己的意见和行为。我们发现，悖论在**物联网**中更为普遍，通常是由于缺乏意识而造成的。最后，我们强调用户的定性评论，并为他们的问题提出切实可行的解决方案。据我们所知，这是在广泛的技术上评估隐私悖论的第一项工作。少

2018 年 7 月 16 日提交;最初宣布 2018 年 7 月。

评论:10 页, 2 个数字，第十五届隐私、安全和信任国际会议 (pst2017) 会议记录 (2017)

165. **第: 1807. 0554[pdf,其他] cs. cy**

多伊 10.1109/ARES.2016.25

完美风暴: 隐私悖论与物联网

作者:meredydd williams, jason r. c. 护士, sadie creese

摘要: 隐私是整个人类历史上的一个概念，民意调查表明，公众重视这一原则。然而，虽然许多人声称关心隐私，但他们往往被认为表达了相反的行为。这种现象被称为隐私悖论，它的存在已经通过大量的心理学、经济学和计算机科学研究得到了证实。提出了几个促成因素，包括用户界面设计、风险显著性、社会规范和默认配置。我们认为，物联网 (**iot**) 的进一步普及将加剧其中许多因素，对个人隐私构成更大的风险。本文探讨了这一悖论和**物联网**的演变，讨论了未来几年隐私风险可能发生的变化，并提出了解决合理平衡问题所需的进一步研究建议。我们认为，在一个无处不在的技术世界中，技术和社会技术措施都是必要的，以确保隐私得到保护。少

2018 年 7 月 16 日提交;最初宣布 2018 年 7 月。

评论:9 页, 1 个图, 第十一届可用性、可靠性和安全性国际会议论文集 (2016 年)

166. 第: 1807. 0731[pdf] Cs。直流

物联网中增强生活环境的 qos 管理机制

作者:yassine banouar, clovis anicet ouedraogo, christophe chassot, abdellah zyane

摘要: 物联网 (**iot**) 模式有望通过新的应用程序带来无处不在的智能, 以增强生活和其他环境。目前, 一些研究和标准化研究主要集中在底层通信系统的中间件级别。对于这一水平, 需要考虑若干挑战, 其中包括服务质量问题。自主计算范式现在被认为是一种很有希望的方法, 可以帮助通信和其他系统在环境变化时自我适应。为了促进基于**物联网**的系统自主中间件级 qos 管理的愿景, 本文提出了一套面向 qos 的机制, 可以在中间件级别动态执行, 以纠正 qos 的退化。还说明了拟议机制对加强生活环境的具体案例的好处。少

2018 年 7 月 16 日提交;最初宣布 2018 年 7 月。

评论:2017 iipieee 集成网络和服务管理研讨会 (im), 2017 年 5 月, 葡萄牙里斯本。ieee, 2017

报告编号:rapport laas n {\textdegree} 17625

167. 第: 1807. 0729[pdf] Cs。直流

通过运行时可插拔 qos 管理机制增强基于中间件的物联网应用程序。应用于符合 onem2m 标准的物联网中间件

作者:clovis anicet ouedraogo, samir medjiah, christophe chassot, khalil drira

摘要: 近年来, 电信和计算机网络通过网络功能虚拟化 (nfv) 和软件定义网络 (sdn) 见证了新的概念和技术。sdn 允许应用程序对网络进行控制, 而允许在虚拟化环境中部署网络功能的 nfv 是越来越多地用于物联网 (**iot**) 的两种模式。这种互联网 (**iot**) 带来了在未来几年内互连数十亿设备的希望, 提出了几个科学挑战, 特别是**物联网**应用所需的服务质量 (qos) 满意度。为了解决此问题, 我们确定了 qos 方面的两个瓶颈: 遍历网络和允许应用程序与**物联网**设备交互的中间实体。在本文中, 我们首先提出了一个关于 "网络功能" 的创新愿景, 即它们的部署和运行时环境。然后, 我们描述了我们的解决方案的一般方法, 该解决方案包括 qos 管理机制的动态、自主和无缝部署。我们还描述了实施这种方法的要求。最后, 我们提出了一个重定向机制, 作为一个网络函数实现, 允许无缝控制给定中间件流量的数据路径。这一机制是通过一个与车辆运输有关的使用案例进行评估的。少

2018 年 7 月 16 日提交;最初宣布 2018 年 7 月。

报告编号:rapport laas n {\textdegree} 18131

日记本参考:第九届环境系统、网络和技术国际会议 (反 2018 年), 第八届可持续能源信息技术国际会议 (seit-2018), 2018 年 5 月, 葡萄牙波尔图。130, pp.619, 2018

168. 第 1807. 05602[pdf,其他] cs. it

基于神经网络物联网系统中的信道调度和重复的后期能源交易

作者:amin azari, guowang miao, cedomir stefanovic, petar popovski

文摘: 窄带**物联网**(nb-iot) 是 3gpp 提供的最新**物联网**连接解决方案.**nb-iot** 引入了覆盖类, 并通过允许经历高路径丢失的节点重复传输, 引入了显著的链接预算改进。然而, 这些重复必然会增加整个 **nb-iot** 系统的能耗和延迟。整个系统的受影响程度取决于上

行和下行通道的调度。我们通过开发 **nb-iot** 访问协议操作的可跟踪模型来解决这个问题，该模型包括上行链路和下行链路中随机访问、控制和数据通道中的消息交换。然后，该模型通过推导每个覆盖类的预期延迟和电池寿命，分析通道调度的影响以及共存覆盖类的交互。这些结果随后被应用于 **nb-iot** 信道调度中的延迟能量权衡的研究以及优化操作点的确定。仿真结果表明了分析的有效性，证实了信道调度对 nb 物联网设备的延迟和寿命性能有显著影响。少

2018 年 7 月 15 日提交;最初宣布 2018 年 7 月。

评论:ieee 环球公司 2018

169. **特别报告: 1807.05002[pdf,其他] Cs。铬**

多伊 10.1109/TCAD.2018.2858422

assured: 用于安全更新现实嵌入式设备的软件的体系结构

作者:n. askan, thomas nyman, norrathep rattanavipanon, ahad-reza sadeghi, gene tusdik

摘要: 安全固件更新是**物联网**设备生命周期中的一个重要阶段。以前的技术专为其他计算设置而设计，并不容易适用于**物联网**设备，因为它们不考虑现实**的大规模物联网**部署的特性。这推动了我们对 assured 的设计，这是一个安全且可扩展的物**联网**更新框架。assured 包括典型**物联网**更新生态系统中的所有利益相关者，同时在制造商和设备之间提供端到端安全性。为了验证其可行性和实用性，在两个商品硬件平台上对 assured 进行了实例化和实验评价。结果表明, assured 比现实设置中的当前更新机制要快得多。少

2018 年 10 月 18 日提交;v1 于 2018 年 7 月 13 日提交;最初宣布 2018 年 7 月。

评论:作者的作品版本，出现在国际嵌入式软件会议 (emsoft' 18), 2018 年 10 月，图林，意大利。《关于集成电路和系统计算机辅助设计的 ieee 交易》 (ieee) 出版了《最终记录》，第 37 卷，第 11 号, 2018 年 11 月 11 日

日记本参考:ieee 集成电路与系统计算机辅助设计的交易，第 37 卷，第 11 期, 2018 年 11 月

170. **建议: 1807. 04356[pdf, ps,其他] cs. it**

联合状态采样和更新，以最大限度地减少物联网中的信息时代

作者:周波,瓦利德·萨阿德

摘要: 时间紧迫的物联网 (**iot**) 应用程序的有效运行需要实时报告底层物理进程的最新状态信息。本文考虑了一个实时**物联网**监控系统，其中**物联网**设备以采样成本采样物理过程，并以更新成本将状态数据包发送到给定的目标。这种联合状态采样和更新过程旨在在每个设备的平均能源成本约束下，最大限度地降低目标节点上的平均信息年龄 (aoi)。这被表述为无限视界平均成本约束马尔可夫决策过程 (cmdp)，并利用拉格朗日方法转化为无约束 mdp。对于单个 **iot** 设备情况, cmdp 的最优策略被证明是不受约束的 mdp 的两个确定性策略的随机混合，该 mdp 是阈值类型。然后，提出了一种结构感知优化算法来获得 cmdp 的最优策略，并研究了无线信道动力学的影响，证明了平均信道增益较大、散射较小的信道可以获得更好的 aoi 性能。针对多**物联网**设备，提出了一种低复杂度分布式次优策略，在目标位置进行了更新控制，并在每个设备上进行了采样控制。然后，开发了一种在线学习算法来获取此策略，该算法可以在每个 **iot** 设备上实现，只需要来自目的地的本地知识和小信号。所提出的学习算法几乎肯定收敛

到次优策略。仿真结果表明了单个**物联网**器件的最优策略的结构特性;并表明，针对多个**物联网**设备的拟议策略优于零等待基准策略，平均 aoi 减排幅度高达 33%。少

2018 年 7 月 11 日提交;最初宣布 2018 年 7 月。

评论:30 页, 6 个数字

171. **建议: 1807. 04343[pdf,其他] Cs。Hc**

利用主题模型通过连接的物联网传感器挖掘日常对象使用常规

作者:张燕霞,洪海丽

摘要: 随着传感和**物联网**基础设施的巨大进步，可以预见,**物联网**系统很快就会出现在商业市场，比如人们的家中。在本文中，我们提出了一个部署研究使用传感器附加到家用物品，以捕捉三个人的足智多谋。足智多谋的概念突出了人类自发地将物体重新定位为与最初预期不同的用例的能力。它是人类健康和福祉的关键因素，对 hci 和设计研究的各个方面都非常感兴趣。传统上，足智多谋是通过人种学实践捕捉。人种学只能提供对人类经验的稀疏的、往往是短暂的观察，往往依赖于参与者意识到并记住他们需要报告的行为或想法。我们的假设是，足智多谋也可以通过持续监控日常生活中使用的对象来捕捉。我们开发了一个系统，可以连续记录物体运动，并将其部署在 3 名老人家中两周多。我们探讨了使用概率主题模型来分析收集的数据和识别常见模式。少

2018 年 7 月 11 日提交;最初宣布 2018 年 7 月。

172. **第 1807. 04114[pdf,其他] Cs。镍**

theingpot: 一个交互式的物联网蜜罐

作者:王蒙,哈维尔·桑蒂兰,费尔南多·奎伯斯

摘要: mirai 分布式拒绝服务 (ddos) 攻击利用了物联网 (**iot**) 设备的安全漏洞，从而清楚地表明攻击者的雷达上有**物联网**。因此，保护**物联网**是必不可少的，但要做到这一点，了解此类攻击者的策略至关重要。为此，本文提出并部署了一种名为 "廷锅" 的**新型物联网**蜜罐。蜜罐技术模仿攻击者可能利用的设备，并记录他们的行为，以检测和分析使用的攻击媒介。theingbot 是同类中的第一个，因为它不仅专注于**物联网**应用协议本身，而且专注于整个**物联网**平台。使用 xmpp 和 rest api 实现了概念验证，以模拟飞利浦 hue 智能照明系统。thingbot 已经部署了 1.5 个月，通过捕获的数据，我们发现了针对智能设备的五种类型的攻击和攻击媒介。廷锅源代码作为开源提供。少

2018 年 7 月 11 日提交;最初宣布 2018 年 7 月。

173. **特别报告: 1807.0 04087[pdf] cs. cy**

物联网: 基础架构、体系结构、安全和隐私

作者:zainab alansari, nor badrul anuar, amirrudin kamsin, mohammad riyaz belgaum, jawdatalshaer, safeeullah soomro, mahdi h. miraz

摘要: 物联网 (**iot**) 是本世纪的新兴技术之一，其各个方面，如基础设施、安全、架构和隐私，在塑造数字化世界的未来方面发挥着重要作用。物联网设备通过传感器连接，这些传感器对数据及其安全性有重大影响。在这项研究中，我们使用**了物联网**的五层架构来解决**支持物联网**的服务和应用程序的安全性和私有问题。此外，还对物联网的基础结构、体系结构、安全性和异构对象的隐私进行了详细的调查。本文确定**了物联网**领域的主要挑战;其中之一是在通过传感机器访问物体时保护数据。这项研究倡导在每一层保护物联网生态系统的重要性，从而增强了连接设备和生成的数据的整体安全性。因此,

本文提出了**一种供物联网**设备、应用和服务的研究人员、制造商和开发者使用的安全模型。少

2018 年 7 月 11 日提交;最初宣布 2018 年 7 月。

期刊参考: ieee 计算、电子和通信工程国际会议 (ieee icece ' 18) 的记录, 2018 年 8 月 16 日至 17 日, 英国, 在线国际标准书号: 978-1-5386-4904-6, e-isbn:978-1-5386-4903-9, 由 ieee 出版

174. 第 xiv:1807. 03954[pdf, ps,其他] cs. ne

多伊 10.1109/SMC.2017.8122711

从重复深信仰网络中提取的实时确定性控制知识

作者:shinkamada, takumi ichimura

文摘: 近年来, 包括软件在内的深度学习市场也在快速发展。大数据是通过**物联网**设备收集的, 行业世界将对其进行分析, 以改进其制造工艺。深度学习具有分层的网络体系结构, 可以表示输入模式的复杂特征。虽然深度学习可以显示出很高的分类、预测等能力, 但需要在 gpu 设备上实现。我们可以通过深度学习来满足更高的精度和 gpu 设备更高的成本之间的权衡。我们可以成功地从受过训练的深度学习中提取出具有较高分类能力的知识。从给定输入数据的网络信号流中提取了能够实现预训练深网络快速推理的知识。通过时间序列数据集基准测试的实验结果表明, 我们提出的方法与计算速度有关。少

2018 年 7 月 11 日提交;最初宣布 2018 年 7 月。

评论:6 页, 10 个数字. arxiv 管理说明: 文本与 arxiv:1807. 03953 重叠

日记本参考:2017 年 ieee 系统、人和控制论国际会议 (ieee smc2017) 的项目

175. 第: 1807. 03755[pdf,其他] Cs。直流

物联网环境中无服务器函数的动态分配

作者:duarte pinto , jao pedro dias, hugo sereno ferreira

摘要: **物联网**领域在过去几年中显著增长, 预计到 2020 年将达到 500 亿台。无服务器体系结构的出现, 特别是突出了 faas, 这就提出了在**物联网**环境中使用此类体系结构的问题。当尝试**利用物联网**设备本地网络中存在的本地处理能力并创建一个利用计算能力的雾层时, 将物联网与无**服务器**架构设计相结合是有效的。更接近最终用户。在这种方法中, 放置在设备和无服务器函数之间, 当设备请求执行无服务器函数时, 将根据以前的执行指标在雾中决定是否应在本地执行无服务器函数**物联网**设备的本地网络层, 或者如果应在其中一台可用的云服务器中远程执行。因此, 此方法允许将函数动态地分配到最合适的图层。少

2018 年 7 月 17 日提交;v1 于 2018 年 7 月 10 日提交;最初宣布 2018 年 7 月。

176. 建议: 1807. 03590[pdf, ps,其他] Cs。镍

面向智能物联网社区的设备间支持社会功能的通信

作者:杜清河,宋厚兵,朱学杰

摘要: 未来的**物联网**有望在全球范围内获得无处不在的连接和访问。与此同时, 随着**物联网**设备的通信能力的增强,**物联网**即使在基础设施的帮助下, 也将发展成为高度自主的企业, 从而逐步建立智能**物联网**社区。智能**物联网**社区面临的主要挑战之一是**物联网**通信的社会化, 因为大规模**的物联网**访问使集中控制变得非常困难, 并且还面临频谱资源的短缺。针对这些问题, 我们在本文中首先介绍了影响设备之间连接的社会特征的

概述和讨论。然后，我们推动研究智能**物**联网设备之间连接的社会特征的统计特征。进一步提出了统一渐近分析框架下的排队模型，以描述统计社会特征，重点分析信用、声誉、中心地位等典型社会指标。进一步提出了如何将这些功能应用于网络优化的建议。最后，我们分享了我们对未来智能**物联网**的社会意识设计的公开问题的看法。少

2018 年 7 月 10 日提交;最初宣布 2018 年 7 月。

177. **建议: 1807. 03542[pdf] cs. cy**

识别伊朗国际共和国 4g 技术传播关键因素的战略框架----一种模糊 de 安全部方法

作者:侯赛因·萨齐安、侯赛因·加里布、塞耶德 mostafa seyyed hashemi、 ali maleki

摘要: 长期演进 (lte) 技术作为 4g 最突出的代表，已成为全球移动网络运营商关注的焦点。然而，尽管 mci 和 irancell 等伊朗主要运营商在部署这一技术方面投入了大量资金，但其传播速度非常缓慢, 2017 年春季结束时的渗透率为 0.06。然而，如果这一比率不提高，将给电信运营商带来一些负面的意外后果，如 (i) 未能提供大量高质量的服务 (ii) 无法与 ott 技术竞争 (iii) 许多收入的损失机会 (四) 延长回收期和 (五) 第五代网络缺乏技术可及**性，许多物联网**机会丧失。通过讨论技术采用和传播的文献，一般和具体地，确定这些研究的主要局限性，并建立一个全面的因素集的基础上，四个主要群体 (i) 手机和与操作相关的因素 (ii) 订阅者相关的生物因素, (iii) 订阅者相关的感知因子和 (iv) 订阅相关的上下文因子，开发了一种新的模糊 demedel 模型，通过该模型，所有 ict 决策者不仅可以通过该模型清楚地了解影响技术采用的因素，但也要了解影响伊朗人对 lte 采用的心态的关键成功因素 (csf)。因此，它们可以制定有效和可操作的政策，在全社会推广 lte 传播或其他与信通技术有关的技术。少

2018 年 7 月 10 日提交;最初宣布 2018 年 7 月。

评论:20 页, 5 个数字, 7 个表, 14 个方程式

178. **建议: 18007. 05110[pdf,其他] Cs。直流**

三位一体: 基于区块链的不可变性的分布式 publish/订阅经纪商

作者:gowri sankar ramachandran, kwame-lante wright, bhaskar krishnamachari

摘要: 物联网 (**iot**) 和供应链监控应用程序依赖于消息传递协议来交换数据。由于发布-订阅消息传递模型的资源效率，当代物联网部署被广泛使用。但是，具有发布-订阅消息传递模型的系统采用集中式体系结构，其中来自应用程序网络中所有设备的数据通过中央代理流向订阅者。这种集中式体系结构使发布-订阅消息传递模型容易受到故障的中心点的影响。此外，它还为拥有代理的组织提供了篡改数据的机会。在这部作品中，我们贡献了三一重工，这是一家新型的分布式发布-订阅经纪商，具有基于区块链的不可变性。trinity 将发布的数据分发给网络中的某个经纪商，并将其分发给网络中的所有经纪商。通过使用区块链技术，分布式数据存储在不可变的分类帐中。此外, trinity 在将数据保存到区块链上之前，会执行智能合同来验证数据。通过使用区块链网络, trinity 可以保证跨信任边界的持久性、排序和不变性。我们的评估结果表明, trinity 消耗的资源最少，使用智能合同使利益相关者能够自动化数据管理过程。据我们所知, trinity 是第一个将区块链技术的组件与发布-订阅消息传递模型结合在一起的框架。少

2018 年 6 月 12 日提交;最初宣布 2018 年 7 月。

179. **第: 1807. 03065[pdf] Cs。镍**

基于 5g-物联网和下一代技术的新型物联网体系结构

作者:hamed rahimi, ali zibaeenejad, ali akbar safavi

摘要: 物联网 (**iot**) 是工业 4.0 的重要组成部分。由于客户的需求不断增长，目前的**物联网**架构对于下一代**物**联网应用和即将推出的服务将无法可靠和响应。本文提出了一种基于新技术的下一代**物联网**体系结构，其中解决了未来应用、服务和生成数据的要求。特别是，此体系结构包括纳米芯片、毫米波 (毫米波 (mmwave)、异构网络 (hetnet)、设备**到**设备 (d2d) 通信、5g-物联网、机器类型通信 (mmWave)、无线网络功能虚拟化 (wnfv)、无线软件定义网络 (wsdn)、高级频谱共享和干扰管理 (高级 ssim)、移动边缘计算 (mec)、移动云计算 (mcc)、数据分析和大数据。这种技术组合能够满足新应用的要求。提出的新体系结构是模块化的、高效的、敏捷的、可扩展的、简单的，能够满足大量的数据和应用程序需求。少

2018 年 7 月 9 日提交;最初宣布 2018 年 7 月。

评论:向 ieee 2018 年全球通信会议提交 7 页, 1 个图, 1 个表格

180. **第 xiv:1807.02846[pdf,其他] Cs。直流**

"思想我的价值": 一个分散的基础架构，用于公平和值得信赖的物联网数据交易

作者:paolo missier, shaimaa bajoudah, angelo capossele, andrea gaglione, miche nati

摘要: 物联网 (**iot**) 数据日益被视为一种大规模分布式和大规模数字资产的新形式，这些资产由数百万连接设备不断生成。只有允许**物联网**数据交易在一个非常精细的水平上奖励每一个生产者和消费者的市场上，才能实现这些资产的真正价值。至关重要的是，我们认为，这样的市场不应该为任何人拥有，而应该公平和透明地自我执行一套明确界定的治理规则。在本文中，我们讨论了实现这样一个市场所涉及的一些技术挑战。除了广泛采用的物联网代理数据基础架构外，我们还利用新兴的**区块链**技术，为**物联网**流量计量和合同合规性构建分散、可信、透明和开放的架构。我们讨论了基于 etheres 的原型实现，并对与智能合同事务相关的开销成本进行了实验评估，得出的结论是，一个可行的业务模型确实可以与我们的技术方法相关联。少

2018 年 7 月 8 日提交;最初宣布 2018 年 7 月。

181. **第 xiv:1807.02558[pdf,其他] Cs。镍**

物联网支持 eh 的 cr 网络中的节能资源分配

作者:ali shahini, abbas kiani, nirwan ansari

摘要: 随着物联网 (**iot**) 设备的快速增长，下一代移动网络对更多的操作频段提出了更高的需求。通过利用未充分利用的无线电频谱，认知无线电 (cr) 技术被认为是**解决物联网**应用频谱稀缺问题的一个很有前途的解决方案。在 cr 技术发展的同时，无线能量收集 (weh) 被认为是消除**物联网**和 cr 网络充电或更换电池需求的新兴技术之一。为此，我们建议将 weh 用于 cr 网络，在这些网络中, cr 器件不仅能够以协作的方式检测可用的无线电频率，而且能够获取接入点 (ap) 传输的无线能量。更重要的是，我们设计了一个优化框架，该框架抓住了网络的能效 (ee) 和频谱效率 (se) 之间的根本权衡。特别是，我们提出了一个混合整数非线性规划 (minlp) 问题，最大限度地提高 ee，同时考虑到用户的缓冲区占用率，数据速率公平性，能源因果关系约束和干扰约束。进一步证明了所提出的优化框架是一个 np-hard 问题。因此，我们提出了一个低复杂启发式算法，称为即时综合算法，以解决资源分配和能量采集优化问题。该算法在多项式复杂度的同时，具有较高的精度，能够实现接近最优的解。通过精心设计的仿真验证了我们的建议的有效性。少

2018 年 7 月 6 日提交;最初宣布 2018 年 7 月。

182. 第 xiv:180. 7.02173[pdf] Cs。镍

浅谈物联网中的解决方法

作者:mehdi imani, abolfazl haasi moghadam, nasrin zarif, omekolsoom Noshiri, k 米亚 faramarzi, hamid arabnia, majid joudaki

摘要: 在过去的 10 年里，物联网得到了极大的关注，在这一领域撰写了许多论文。**物联网**的目标是将我们周围的所有事物连接到互联网，并为我们提供更智能的城市、更智能的家园和更智能的生活。连接到互联网的设备数量正在不断增加，支持所有这些设备给**物联网**带来了一些挑战。**物联网**面临的挑战之一是解决全球数十亿的问题，包括计算机、平板电脑、智能手机、可穿戴设备、传感器等。在本文中，我们对解决方法进行了全面的调查，并试图仔细研究这一领域所有提出的方法。此外，我们还在 "备注" 节中的每个讨论结束时提供了每种方法的优缺点。我们还提供了一些用于评估所有讨论的方法的指标，并根据我们的指标对这些方法进行比较。少

2018 年 7 月 5 日提交;最初宣布 2018 年 7 月。

183. 第: 1807. 01147[pdf,其他] Cs。镍

快速跟踪: 最大限度地减少基于 cdn 的顶级视频流系统的支架

作者:Abubakr alabbasi, vaneet Aggarwal, tian lan, yu 钩香, Moo-Ryong ra, yih-farn r. chen

摘要: 互联网视频流的流量一直在迅速增加，预计随着更高的清晰度视频和**物联网**应用 (如 360 度视频和增强虚拟现实应用) 的增加，流量还将进一步增加。虽然高效管理异构云资源以优化体验质量很重要，但这一问题空间中的现有工作往往忽略了重要因素。在本文中，我们提出了一个描述当今具有代表性的视频流应用程序系统体系结构的模型，该模型通常由一个集中的源服务器和几个 cdn 站点组成。我们的模型全面考虑了以下因素: cdn 站点的缓存空间有限、视频请求的 cdn 分配、cdn 不同端口的选择以及中央存储和带宽分配。利用该模型，重点研究了性能指标、失速持续时间尾概率 (sdtp)，提出了一种新的、有效的算法来解决所提出的优化问题。并对 sdtp 度量的理论边界进行了分析和提出。我们广泛的仿真结果表明，与基线策略相比，所提出的算法可以显著提高 sdtp 指标。在实际的云环境中实现小规模的视频流系统，进一步验证了我们的结果。少

2018 年 6 月 30 日提交;最初宣布 2018 年 7 月。

评论:18 页. arxiv 管理说明: 文本与 arxiv:1806. 09466、arxiv:1703.08348 重叠

184. 第 xiv:1807. 00976[pdf,其他] Cs。直流

雾计算: 趋势、体系结构、要求和研究方向的概述

作者:ranesh kumar naha, Saurabh garg, Dimitrios ge 支配 kopoulos , prem prakash jiaraman, long 民儿 gao, yong 角 , rajiv ranjan

摘要: 物联网 (**iot**) 等新兴技术需要实时应用程序处理的延迟感知计算。在**物联网**环境中，连接的东西会生成大量数据，这些数据通常被称为大数据。由于云计算范式的按需服务和可扩展性功能，从**物联网**设备生成的数据通常在云基础架构中进行处理。但是，对于某些**物联网**应用程序 (尤其是对时间敏感的应用程序) 来说，专门在云上处理物联网应用程序请求并不是一个有效的解决方案。为了解决这个问题，提出了驻留在云和**物联网**设备之间的雾计算。通常，在雾计算环境中,**物联网**设备连接到雾设备。这些雾设备位于靠近用户的位置，负责中间计算和存储。雾计算研究仍处于起步阶段，仍然需要对与当前研究映射的雾基础设施、平台和应用程序的需求进行分类调查。本文首先

对雾计算进行了综述，回顾了雾计算的定义、研究趋势以及雾与云之间的技术差异。然后，我们研究了许多提出的 fog 计算体系结构，并详细描述了这些体系结构的组件。由此，将定义每个组件的角色，这将有助于将雾计算部署。其次，通过考虑雾计算范式的要求，提出了雾计算的分类方法。我们还讨论了现有的研究工作以及在资源分配和调度、容错、仿真工具和基于 f 因为 f 因为微服务方面的差距。最后，通过解决当前研究工作的局限性，提出了一些悬而未决的问题，将决定未来的研究方向。少

2018 年 7 月 3 日提交;最初宣布 2018 年 7 月。

185. 第: 1807. 00971[pdf,其他] Cs。Db

物联网分析: 一项调查

作者:eugene siow, thanassis tiropanis, wendy hall

摘要: 物联网 (**iot**) 设想了一个全球范围内相互关联的智能物理实体网络。这些物理实体生成大量运行中的数据，随着**物联网**在部署方面获得的势头，这些数据的综合规模似乎注定会继续增长。**物联网**的应用程序越来越多地涉及分析。数据分析是从数据中获取知识的过程，从数据中产生可操作的洞察等价值。本文从**物联网**和大数据分析在为广泛的领域创建高效、有效和创新的应用程序和服务方面的效用的角度回顾了它们的工作。我们回顾了**物联网**在不同社区形成的广阔愿景，审查了数据分析在物**联网**领域的应用，提供了分析方法的分类，并提出了物**联网**的分层分类数据到分析。此分类为我们提供了有关分析技术的适宜性的见解，这反过来又形成**了对物联网**分析的使能技术和基础架构的调查。最后，我们将研究**物联网**分析的一些权衡因素，这些权衡可以影响未来的研究。少

2018 年 7 月 3 日提交;最初宣布 2018 年 7 月。

186. 第: 1807. 00649[pdf,其他] Cs。Sy

分布式分类帐技术、网络物理系统和社会合规性

作者:pietro ferraro, christopher king, robert shorten

摘要: 本文介绍了如何使用分布式分类器技术来设计一类网络物理系统，以及执行社会契约和协调试图访问共享资源的代理的行为。本文第一部分分析了使用分布式分类帐技术体系结构在物联网 (**iot**) 设置中实现某些控制系统的优缺点，然后重点介绍了基于定向无环图。在此设置中，我们提出了一组延迟微分方程来描述 tgle 的动力学行为，这是一种为加密货币 iota 设计的物联网启发的定向无环图。第二部分提出了分布式分类帐技术作为动态存款定价机制的应用，其中数字货币的存款用于协调对共享资源网络的访问。定价信号被用作一种机制，根据一组预定的规则强制执行所需的合规性级别。在给出一个示例后，对控制系统进行了分析，为网络的稳定性提供了充分的条件。少

2018 年 10 月 20 日提交;v1 于 2018 年 7 月 2 日提交;最初宣布 2018 年 7 月。

评论:本论文已被接受在 ieee access 杂志上发表，其标题为 "智能城市分布式分类帐技术、共享经济和社会合规性" 。

187. 第 xiv:1807. 00491[pdf, ps,其他] Cs。镍

物联网网络中的多武装强盗学习: 即使在非平稳环境中学习也有帮助

作者:rémi bonnefoi, lilian besson , christophe moy, emilie kufmann, jacques palicot

摘要: 建立未来的物联网 (**iot**) 网络将需要支持越来越多的通信设备。我们证明，在无牌频段的智能设备可以使用多武装强盗 (mab) 学习算法来改善资源开发。我们评估了

两种经典的 mab 学习算法 ucb1 和 thompson 采样的性能，以处理**应用于物联网**网络的频谱访问的分散决策;以及越来越多的智能终端设备的学习性能。我们表明，使用学习算法确实有助于在这样的网络中安装更多的设备，即使所有终端设备都是智能的，都在动态变化通道。在所研究的场景中，随机 mab 学习在成功的传输概率方面提供了高达 16% 的增益，即使在大多数智能设备的非平稳和非 i. d. 设置中，也具有近乎最佳的性能。少

2018 年 7 月 2 日提交;最初宣布 2018 年 7 月。

日记本参考:conwncom 2017-12 eai 面向认知无线电的无线网络国际会议, 2017 年 9 月，葡萄牙里斯本。http://crowncom.org/2017/

188. **建议: 180.00035[pdf] cs. cy**

一种高效的作物产量预测数据仓库

作者:vuong m. ngo , nhien-an le-khac , m-tahar kechadi

摘要: 如今，精确农业与现代信息和通信技术相结合，在自动化灌溉系统、精确种植、营养物质的可变率应用和现代信息和通信技术等农业活动中越来越普遍。农药和农业决策支持系统。在后者中，基于机器学习和数据挖掘的作物管理数据分析主要侧重于如何有效预测和提高作物产量。近年来，原始和半加工农业数据通常是使用传感器、机器人、卫星、气象站、农业设备、农民和农业企业收集的，而物联网 (**iot**) 应兑现以下承诺:以无线方式连接农业生态系统中的对象和设备。农业数据通常捕获有关农业实体和经营的信息。每个农业实体都包含了一个单独的农业概念，如农田、作物、种子、土壤、温度、湿度、害虫和杂草。农业数据集是空间的、时间的、复杂的、异构的、不标准化的，而且非常大。特别是，农业数据在数量、品种、速度和准确性方面被认为是大数据。设计和开发精准农业数据仓库是建立作物智能平台的关键基础，这将使资源高效的农学决策和建议成为可能。此类农业数据仓库的一些要求是利益攸关方 (如农民、农业设备制造商、农业企业、合作社、客户以及可能的政府) 之间的隐私、安全和实时访问机构)。然而，目前文献中很少有报告侧重于设计高效的数据仓库，以便能够进行农业大数据分析和数据挖掘。在本文中.. 。少

2018 年 6 月 26 日提交;最初宣布 2018 年 7 月。

评论:12 页。关键 字。数据仓库、星座模式、作物产量预测、精准农业

日记本参考:第十四届国际精准农业大会论文集。2018 年 6 月 24 日至 27 日，加拿大魁北克蒙特利尔

189. **第 1806. 1191399[pdf] Cs。铬**

智能城市中动态无线网络的滚动式链

作者:sergii kushch, francisco prieto-castrillo

摘要: 区块链是目前讨论的最热门的话题之一。然而，大多数专家仍然认为这种技术只是比特币、其他加密货币或汇款系统的一部分。通常情况下，年轻研究人员提出的新解决方案被评审人员阻止，只是因为这些解决方案不能用于比特币。然而，区块链技术更加普遍，也可用于其他领域，例如**物联网**、无线传感器网络和移动设备。本文认为区块链技术作为**物联网**的一个组成部分在传感器网络中的实现。提出了 "滚动条链" 的概念，可用于智能汽车参与下的无线传感器网络建设，作为网络的节点。提出了链中块形成和结构的顺序，并为其建立了数学模型。我们估计了 wsn 节点的最佳数量，节点之间的连接数，对于指定的网络可靠性值，执行了。少

2018 年 6 月 29 日提交;最初宣布 2018 年 6 月。

190. 第 xiv:866.11386[pdf] cs. cy

伊斯兰视角下的物联网伦理问题

作者:wazir zada khan, mohammed zahid, mohammed y aalsalem, hussein mohammed zangoti, quratulain arshad

摘要: 物联网 (**iot**) 是一项不断发展的新技术面貌，它使用无处不在的连接智能对象提供最先进的服务。这些智能对象能够感知、处理、协作、传达事件并提供服务。**物联网**是传感器、rfid、通信和纳米技术等异构技术的集合。这些技术使智能对象能够识别对象、收集有关其状态的信息、传达收集到的信息以执行一些所需的操作。基于**物联网**的设备和服务的广泛适应为用户带来了道德挑战。在本文中，我们强调了**物联网**带来的伦理挑战，并讨论了鼓励人们根据伊斯兰教义正确使用这些技术的解决方案和方法。少

2018 年 6 月 29 日提交;最初宣布 2018 年 6 月。

评论:4 页, 3 位数字，第九届 ieee-gcc 大会暨展览-2017

191. 第 xiv:1906.10906[pdf,其他] Cs。铬

多伊 10.1049/cp.2018.0001

如果你不能理解它，你就不能正确地评估它!物联网系统中安全风险评估的现实

作者:jason r. c.护士, petar radanliev, sadie creese, david de roure

摘要: 在过去 20 年里，安全风险评估方法对我们很有帮助。随着技术系统的复杂性、普遍性和自动化程度的提高，特别是物联网 (**iot**) 的复杂性、普遍性和自动化程度的提高，有令人信服的论据表明，我们将需要新的方法来评估风险和建立系统信任。在本文中，我们报告了一系列范围界定研讨会和与行业专业人士 (企业系统、**物联网**和风险方面的专家) 进行的访谈，以调查这一论点的有效性。此外，我们的研究旨在与这些专业人员协商，以了解两个关键方面。首先，我们力求确定将**物联网**系统应用于企业环境中的更广泛问题，无论是智能制造车间还是智能办公场所。其次，我们研究了工业中试图有效和高效地评估**物联网**中的网络风险的方法所面临的主要挑战。少

2018 年 6 月 28 日提交;最初宣布 2018 年 6 月。

评论:9 页, 1 个图

日记本参考:生活在物联网中: 2018 年物联网会议的网络安全

192. 第 xiv:1806. 10638[pdf] Cs。铬

可持续的链功能服务: 智能合同

作者:craig wright, antoaneta serguieva

摘要: 本章通过扩展区块链强制执行的智能合同的功能，有助于不断发展支持区块链的服务的多功能性和复杂性。贡献包括: (i) 通过智能代理的层次结构和使用分层加密密钥对自动管理具有分层条件结构的合同的方法;(ii) 在不同的智能合约/分包合约之间，有效及有保障地匹配及转让智能合约 (实体) 的方法;(iii) 一种产生共同秘密层次结构的方法，以便在智能合同/分合同的情况下促进加强安全的分层沟通渠道;(iv) 在合同/分包/底页的情况下，通过分布式哈希表建立安全和优化存储库的方法。这些方法有助于提供服务，使资源能够在全世界范围内范围内得到利用和分配。区块链技术的寿命是通过不断创新实现的。支持区块链的服务有可能是一系列领域 (法律、医疗、财务、政府、**物联网**) 中当前服务基础架构的高效、安全、自动化和经济高效的替代或补充。少

2018 年 6 月 18 日提交;最初宣布 2018 年 6 月。

评论:10 页, 3 个数字, 1 个表, 2017 年 ieee 大数据国际会议

193. 特别报告: 1806. 10521[pdf,其他] Cs。镍

具有分散插槽管理的可靠无线多跳网络: ieee 802.15.4 dsme 的分析

作者:florian kauer, maximian köstler, volker turau

摘要: 无线通信是实现工业物联网的关键要素，可灵活且经济高效地监控工业过程。使用 ieee 802.15.4 的无线网状网络具有很高的执行监视和控制任务的潜力，能耗低，部署和维护成本低。然而，基于载波传感的传统介质接入技术不能为工业应用提供所需的可靠性。因此，该标准扩展了在多个通道上的时隙介质访问技术。本文提出了一种开放的开放式多通道扩展 (dsme) 的综合实现，并提出了一种交通感知和分散插槽调度的方法，以实现可扩展的无线工业网络。omnet ++ 模拟器和 fit/iot 实验室中实际部署的无线网络展示了 dsme 的性能和我们的实施.结果表明，在给定的方案中，使用 dsme 而不是 csmama/ca 可以可靠地传输两倍的流量，从而显著降低了能耗。本文最后提出了参数选择的重要权衡，并揭示了当前规范中需要进一步努力研究和标准化的未决问题。少

2018 年 6 月 27 日提交;最初宣布 2018 年 6 月。

评论:27 页, 18 位数字

194. 建议: 1806.10463[pdf, ps,其他] lo c

建立网络物理攻击影响指标的正式概念 (完整版)

作者:ruggero lanotte, masimo mero, simone tini

摘要: 工业设施和关键基础设施正在转变为动态适应外部事件的 "智能" 环境。其结果是，网络物理系统中整合了异构物理和网络组件的生态系统，越来越多地受到网络物理攻击，即网络空间的安全漏洞，对网络系统的物理过程产生不利影响。系统的核心。我们提供了一个正式的组合指标来估计针对**物联网**系统传感器设备的网络物理攻击的影响，这些攻击是在 hennessy 和 regan 的定时过程语言的简单扩展中正式确定的。我们的影响度量依赖于 des 特殊性等人对并发系统的弱二混量度量的离散时间概括。我们展示了我们对简单监控系统的两种不同攻击的定义是否充分。少

2018 年 6 月 27 日提交;最初宣布 2018 年 6 月。

195. 第 xiv: 1806. 10200[pdf,其他] cs. it

具有聚合器的随机接入物联网网络中的网络级协作

作者:nisipaos pappas, ioannis Dimitriou,郑晨

摘要: 在这项工作中，我们考虑了由两个聚合器辅助的**随机访问物联网**无线网络。节点和聚合器在开槽时间内以随机访问的方式进行传输，聚合器使用网络级的协作。我们假设所有节点共享相同的无线通道，将其数据传输到一个共同的目标。具有带外全双工功能的聚合器配备了队列，用于存储由网络节点传输的数据包，并将其中继到目标节点。我们描述**了物联网**网络的吞吐量性能。此外，我们还得到了聚合器上队列的稳定性条件和数据包的平均延迟。少

2018 年 6 月 26 日提交;最初宣布 2018 年 6 月。

评论:国际电信交通大会 (itc30)

196. 第 xiv: 1806. 09846[pdf,其他] Cs。Sy

多伊 10.4204/EPTCS.272。1

物联网时代的系统设计---迎接自主挑战

作者:约瑟夫·西法基斯

摘要: **物联网**的出现是一个很好的机会，通过专注于自主系统设计来重振计算。这当然提出了技术问题，但更重要的是，这需要建立新的基础，系统地整合面对日益增加的环境和任务复杂性所需的创新成果。一个关键的想法是通过自适应控制来弥补人类干预的不足。这有助于提高系统的恢复能力：它既可以应对不确定性，也可以管理混合关键度服务。我们提出的以知识为基础的设计方案寻求一种妥协：尽管在设计时无法保证基本属性，但仍保持严谨性。它使知识生成和应用成为首要关注的问题，旨在将自适应控制范式完全无缝地纳入系统架构。少

2018 年 6 月 26 日提交;最初宣布 2018 年 6 月。

评论:《诉讼》 metrid 2018, arxiv:1806. 09

日记本参考:eptcs 272, 2018, 第 1-22 页

197. 第 xiv:1806. 09814[pdf,其他] cs. it

下行 swipt 部分无线供电传感器网络的最佳波束形成和时间分配

作者:龚世奇,马少丹,程文兴,杨光华

摘要: 无线供电传感器网络 (wpsn) 已成为面向未来可自我维持的物联网 (**iot**) 网络的关键发展。为了在自我可持续性和可靠性之间实现良好的平衡，在实际应用中需要部分具有混合电源解决方案的 wpsn。具体来说，大多数传感器节点都是无线供电的，但关键传感器节点采用传统的无线电池电源来保证可靠性。因此，本文主要研究了在下行链路中同时采用无线信息和功率传输 (swipt) 的部分无线 psn 的优化设计。考虑了上行链路中空间划分多重访问 (sdma) 和时间划分多重访问 (tdma) 的两种情况。对于支持 sdma 和 tdma 启用的部分 wpsn，研究下行波束形成、上行波束形成和时间分配的联合设计，以最大限度地提高上行和速度，同时保证服务质量 (即满足下行链路)率约束)。在分析上行和速率最大化问题的可行性和下行速率约束的影响后，提出了支持 sdma 和 tdma 启用的 wpsn 的半闭式最优解，保证了全局最优性。还提供了复杂性分析，以证明在低复杂性下提出的解决方案的优势是合理的。最后通过仿真验证了所提出的最优解的有效性和最优性。少

2018 年 6 月 26 日提交;最初宣布 2018 年 6 月。

评论:14 页

198. 第 xiv:1806. 09612[pdf] Cs。艾

基于层次修正模糊支持向量机的汽车车队工业物联网预测维护

作者:arindam chaudhuri

摘要: 互联车队部署在全球**多个工业物联网**方案中。随着通过联网智能设备控制和管理的机器逐渐增多，预测性维护潜力迅速增长。预测性维护具有优化正常运行时间和性能的潜力，从而减少与检查和预防性维护相关的时间和人工。为了了解车辆故障的发展趋势，包括车辆行驶里程、车龄、车辆类型等，通过分层修正模糊支持向量机 (hmfsvm) 解决了这一问题。将该方法与其他常用的方法 (如逻辑回归、随机林和支持向量机) 进行了比较。这有助于更好地实现远程信息处理数据，以确保作为所需解决方案的一部分进行预防性管理。通过几个实验结果，突出了该方法的优越性。少

2018 年 6 月 24 日提交;最初宣布 2018 年 6 月。

评论:在印度德里三星研发研究所完成的研究工作

199. 第 1806. 09381 [pdf,其他] Cs。镍

多伊 10.1016/j.adhoc.2018.04.010

一种基于 d2d 卸载的无线网络中可靠的集群形成的主动可扩展方法

作者:sanaa sharafeddine, omar farhat

摘要: 随着当前流量和服务需求的指数级增长，设备对设备 (d2d) 合作被确定为使 5g 网络能够有效和高效地增加网络资源的主要机制。d2d 合作的有效性取决于广泛的决策过程，其中包括集群形成、资源分配以及连接和移动管理。无论 d2d 合作场景如何，无论是在传感器、临时网络还是蜂窝网络中，文献通常都假定选择为继电器或数据源的设备是可靠的;这意味着他们将保持连接，直到通信会话结束。然而，这一假设在实践中受到挑战，因为设备的电池可能会耗尽 (例如，**物联网**网络中的传感器)，而设备可能会移动导致连接终止 (例如, wifi 网络中的移动用户或车辆临时网络中的汽车)。为此，我们通过提出一种新的方法来解决无线网络中可靠的 d2d 协作问题，这种方法在决策过程中利用可靠性指标是主动的，并且具有适用于以下环境的低实现复杂性即可扩展。密集的网络。与标准技术相比，这些差异因素提高了网络的整体可靠性，并促进了动态运行，这对实际实施至关重要。除了试验台实验演示外，还使用大量模拟对性能进行评估，以便量化收益并提取对一系列现有设计权衡的见解。少

2018 年 6 月 25 日提交;最初宣布 2018 年 6 月。

评论： --

日记本参考:ad hoc networks, 77, 42-53, 2018

200. 第 xiv:1806.09199[pdf,其他] Cs。直流

多伊 10.1109/MSP.2018.2842097

物联网：安全的分布式推理

作者:yuan chen, soummya kar, josém. f. moura

摘要: 连接到物联网 (**iot**) 的设备数量的增长对安全性提出了重大挑战。数据和数据分析的完整性和可信度是**物联网**应用中日益重要的问题。**物联网**设备的高度分布式特性加剧了这些问题，因此无法防止对所有数据源的攻击和入侵。对手可能会劫持设备并危及其数据。因此，响应性对策 (如入侵检测和弹性分析) 成为安全的重要组成部分。本文综述**了物联网**中安全分布式推理的算法。少

2018 年 6 月 24 日提交;最初宣布 2018 年 6 月。

201. 第 xiv:1806.09099[pdf,其他] Cs。铬

物联网的区块链技术：研究问题与挑战

作者:mohamed amine ferrag, Makhlouf derdour, mithun mukherjee, abdelouahid derhab, leandros maglaras, helge janicke

文摘: 本文对现有的物联网 (**iot**) 网络区块链协议进行了全面的综述。我们首先描述区块链，并总结现有的调查，处理区块链技术。然后，我们概述了区块链技术在**物联网**中的应用领域，如车辆互联网、能源互联网、云互联网、雾计算等。此外，我们还将威胁**模型分为五个主要类别，即基于身份的攻击、基于操纵的**攻击、密码分析攻击、基于信誉的攻击和基于服务的攻击。此外，我们还提供了分类和最先进的方法的并行比较，以实现安全和隐私保护的区块链技术，包括区块链模型、特定安全目标、性能、限制、计算复杂性和通信开销。在目前调查的基础上，我们强调了开放的研究挑战，并讨论了**物联网**区块链技术未来可能的研究方向。少

2018 年 6 月 24 日提交;最初宣布 2018 年 6 月。

评论:14 页, 5 个数字

202. 第 xiv:1806.09081[pdf] cs.cy

多伊 10.1109/JIOT.2018.2841969

车辆系统社交互联网的伦理意蕴

作者:ricardo silva, razi iqbal

摘要: **物联网**的核心理念是为现实世界中的对象配备计算、处理和通信功能，使它们之间能够进行社会化。车辆互联网 (iov) 是**物联网**的追随者，它利用通信技术实现了重大进步。通过互联网连接的车辆能够分享信息，从而大大提高道路交通质量。社交物联网 (soot) 是**物联网**的一个例子，专门处理连接对象的社会化。物联网支持车辆社交互联网 (siov) 的概念，即车辆是它们与基础设施 (通常称为路边单元 (rsus)) 之间共享信息的关键实体。siov 的车辆通过交换数据进行社交，如交通拥堵、天气状况、信息娱乐、空置停车位、备用路线和餐馆折扣券等。在 siov 中，车辆可以通过传统通信技术 (如 wi-fi、蜂窝网络或专用短距离通信 (dsrc) 等) 与其他车辆和基础设施进行通信。siov 将面临道德困境，并有望以道德上负责任的方式运作。本文重点介绍了 siov 系统的伦理含义。车辆对车辆 (v2v) 和车辆到基础设施 (V2V) 涉及自主决策，需要在作出判决之前制定道德和道德规则。本文讨论了在设计和部署非常重要的 siov 系统时缺乏道德准则的问题。最后，提出了对 siov 体系结构的补充，以纳入伦理和道德原则，用于规划 siov 系统。少

2018 年 6 月 24 日提交;最初宣布 2018 年 6 月。

日记本参考:ieee 物联网杂志 2018

203. 第 1806.08953[pdf] cs.cy

物联网与大数据集成面临的挑战

作者:zainab alansari, nor badrul anuar, amirrudin kamsin, safeeullah soomro, mohammad riyaz belgaum, mahdi h.miraz, jawdat alshaer

摘要: 物联网预计物理小工具与内网的结合和它们对无线传感器数据的访问，这使得它是权宜之计，以限制物理世界。大数据融合使众多的新机会在企业进入新市场或加强其在当前市场上的运营。考虑到现有的技术和工艺，可以肯定地说，最好的解决方案是使用大数据工具为物联网提供分析解决方案。根据当前的技术部署和采用趋势，设想物联网是未来的技术，而今天的现实世界中的设备可以提供真实而有价值的分析，现实世界中的人们使用许多**物联网**设备。尽管公司提供了所有与物联网有关的广告，但作为一个负责任的消费者，你有权对**物联网**广告持怀疑态度。主要问题是: 互联网对现实的承诺是什么，未来的前景是什么。少

2018 年 6 月 23 日提交;最初宣布 2018 年 6 月。

评论:2018 年在英国伦敦伦敦都市大学举行的 2018 年新兴计算技术国际会议 (icetic '18) 会议论文集，由 springer-verlag 出版

204. 第 xiv:1806.08893[pdf,其他] Cs。铬

安卓恶意软件网络基础设施的自动调查框架

作者:elmouatez billah karbab, mouarad debbabi

摘要: android 系统的普及，不仅在手机设备中如此，在**物联网**设备中也是如此，这使得它成为恶意软件非常有吸引力的目的地。事实上，恶意软件正在以类似的速度扩展，这些设备的目标在大多数情况下依赖于互联网才能正常工作。最先进的恶意软件缓解

解决方案主要侧重于检测实际的恶意 android 应用，使用动态和静态分析功能来区分恶意应用和良性应用。但是，android 恶意应用程序的 internet®网络维度的覆盖率很小。在本文中，我们提出 to 聚集，一个自动调查框架，将 android 恶意软件样本作为输入，并产生有关这些样本家族的恶意网络基础结构的情况感知。tog 表扬利用最先进的图论技术生成可操作的细粒度智能，以减轻 android 恶意软件应用程序的恶意 internet 活动所带来的威胁。我们实验 to 绝大多数从各种 android 家族的真正的恶意软件样本，并获得的结果是有趣的，很有希望少

2018 年 6 月 22 日提交;最初宣布 2018 年 6 月。

评论:12 页

205. 第 1806.08616[pdf,其他] Cs。简历

在嵌入式空间中部署深神经网络

作者:stylianos i. venieris,亚历山大·库里斯 , christos-savvas bouganis

文摘: 近年来，深神经网络 (dnn) 已成为各种人工智能应用中的主要模型。在**物联网**和移动系统时代，在嵌入式平台上高效部署 dnn 对于实现智能应用的开发至关重要。本文总结了我们最近在嵌入式设置上优化 dnn 映射的工作。通过涵盖 dnn 到加速器工具流、高吞吐量级联分类器和域特定模型设计等不同主题，本文的工作旨在在尖端移动设备上部署复杂的深度学习模型。嵌入式系统。少

2018 年 6 月 22 日提交;最初宣布 2018 年 6 月。

评论:参加 mobisys18: 2018 年第二届嵌入式和移动深度学习国际研讨会 (emdl)

206. 第 xiv:1806.08337[pdf] cse

多伊 10.528 半碘. 1296528

检查物联网的关键功能和平台

作者:rena bakhshi, mary hester, jeroen schot, lode kulik

摘要:为了帮助促进**物联网**技术方面的专业知识, nlesc 和 surf 合作中心合作开展了一个项目，重点是...

2018 年 6 月 22 日提交;v1 于 2018 年 6 月 21 日提交;最初宣布 2018 年 6 月。

评论:11 页, 7 个数字，技术报告

类:a.1;D.2.11;D.2.12

207. 第 xiv:1806.08252[pdf] Cs。镍

通过深度数据包检测实现约束节点动态状态的透明恢复

作者:girum ketema teklemariam, floris van den abeele, ingrid moerman, jeroen hoebeke

摘要: 许多**物联网**应用广泛使用受约束的设备，其特点是意外故障。此外，节点可以暂时脱机进行维护 (例如更换电池)。这些事件会导致由于节点之间的交互而生成的动态数据丢失。例如，通过向传感器发送 put 请求调整的配置设置将在节点重新启动时丢失。丢失的数据 (我们称之为动态状态) 会导致**物联网**应用程序的错误结果或故障。本文介绍了一种通过深度数据包检测实现智能动态恢复的智能动态恢复机制。放置在网关上的状态目录可拦截外部设备与受约束设备和存储 (或更新) 对恢复动态状态非常重要的信息之间的每个通信。当节点报告重新启动时，状态目录将重播生成动态状态的数据包，以便还原所有动态状态。我们在一个不受约束的设备上实现了该解决方案，该设备充当受限网络的网关，并使用 cooja 模拟器测试了结果。少

2018 年 6 月 21 日提交;最初宣布 2018 年 6 月。

208. 第 xiv:1806.07057[pdf] Cs。Lg

超参数优化对物联网环境下分布式攻击检测的深度学习模型的影响

作者:md mohaimenuzzaman, zahraa said abdallah, joarder kamruzzaman, bala srinivasan

摘要: 本文研究了各种超参数的作用及其对 [1] 中提出的物联网 (**iot**) 分布式攻击检测深度学习模型最佳性能的选择。结果表明，有三个超参数对模型实现的最佳性能有较大影响。因此，这项研究表明，根据参数的最佳选择，该模型的准确性是无法实现的，最近的另一份出版物也支持了这一点 [2]。少

2018 年 6 月 19 日提交;最初宣布 2018 年 6 月。

评论:6 页、2 个数字和 2 个表

209. 第 xiv:1806.07055[pdf,其他] Cs。Hc

基于电容的动能可穿戴设备的活动传感

作者:郭豪兰,马东,徐伟涛,马布·哈桑,文虎

文摘: 我们提出了一种新的使用传统的储能组件，即电容器，在动力学动力可穿戴 **iot** 作为传感器，以检测人类的活动。由于不同的活动以不同的速率在电容器中积累能量，因此可以通过观察电容器的充电速率直接检测到这些活动。拟议的基于电容器的活动传感机制 (capsense) 的主要优点是，它无需在活动检测期间对运动信号进行采样，从而显著节省了可穿戴设备的功耗。我们面临的一个挑战是，电容器本质上是非线性能量蓄能器，即使对于相同的活动，这也会导致不同时间的充电速率发生显著变化，具体取决于电容器的当前充电水平。我们通过联合配置电容器和相关能量收集电路的参数来解决这个问题，这使得我们能够在近似线性的充电周期上运行。我们设计并实施了一个动能鞋底，并对 10 个对象进行了实验。结果表明，与传统的基于运动信号的活动检测相比，capsense 可以对五种不同的日常活动进行分类，准确率达到 95%，同时消耗 73% 的系统功率。少

2018 年 6 月 19 日提交;最初宣布 2018 年 6 月。

210. 第 xiv:1806.06620[pdf,其他] Cs。镍

基于机器学习的基于机器学习的 lte 和即将到来的 5g 网络的在线在线传输功率预测中使用的无源下行链路指示器

作者:robert falkenberg, benjamin sliwa, nico piatkowski, christian wietfeld

摘要: 能量感知系统设计是基于静态和移动物联网 (**iot**) 传感器节点的一项重要优化任务，尤其是对于移动机器人系统等资源高度有限的车辆而言。对于基于 g 的蜂窝通信系统，上行数据传输的有效传输功率对于整个系统的功耗至关重要。遗憾的是，这些信息通常隐藏在现成的调制解调器和移动手机中，因此无法用于实现绿色通信。此外，在大多数已建立的仿真框架中，移动设备的动态传输功率控制行为甚至没有显式建模。本文提出了一种基于机器学习的基于机器学习的基于现有无源网络质量指标和应用级信息的数据传输传输所产生的上行传输功率预测方法。该模型来自在公共蜂窝网络中执行的驱动测试的综合现场测量，可以参数化，以便将给定目标平台能够提供的所有测量集成到预测过程中。在三种不同机器学习方法的比较中，随机林模型表现非常好，平均误差为 3.166 db。由于误差的绝对总和收敛到零，在平均 28 个预测后，下降到 1 db 以下，该方法非常适合长期功率估计。少

2018 年 6 月 18 日提交;最初宣布 2018 年 6 月。

211. 第 xiv:1806. 06580[pdf, ps,其他] Cs。Ds

非结构化 p2p 网络中频繁项目的挖掘

作者:Pulimeno cafaro, italo Epicoco, marco pulimeno

摘要: 大规模分散系统 (如 p2p、传感器或**物联网**设备网络) 正变得越来越普遍，需要强大的协议来应对数据分布和属于网络。本文讨论了非结构化 p2p 网络中频繁项目的挖掘问题。这个问题具有实际重要性，有许多有用的应用。我们利用节省空间的算法，设计了 p2pss，这是一种完全分散的、基于闲谈的频繁项目发现协议。我们正式证明了理论误差的正确性和正确性约束。大量的实验结果清楚地表明, p2pss 提供了非常好的准确性和可扩展性，也存在具有高度动态的 p2p 网络和搅动。据我们所知，这是第一个基于八卦的分布式算法，为非结构化 p2p 网络中的近似频繁项问题和发现的频繁频率估计提供了强有力的理论保证项目。少

2018 年 10 月 16 日提交;v1 于 2018 年 6 月 18 日提交;最初宣布 2018 年 6 月。

212. 第 1806. 06191[pdf,其他] Cs。镍

边缘云卸载算法: 问题、方法和视角

作者:王建宇,潘建利,弗拉维奥·埃斯波西托,普拉萨德·卡利亚姆,杨志成, 普拉桑特·莫哈特拉

摘要: 支持 "物联网" (**iot**) 的移动设备在计算、电池能量和存储空间方面的能力通常有限，特别是在支持涉及虚拟现实 (vr) 的资源密集型应用方面,现实 (ar)、多媒体传输和人工智能 (ai)，这可能需要宽带宽、低响应延迟和大计算能力。边缘云或边缘计算是一个新兴的主题和技术，它可以解决当前仅集中的云计算模型的不足，并将计算和存储资源移动到更接近支持上述功能的设备的位置应用。要做到这一点，需要有效的协调机制和 "卸载" 算法，使移动设备和边缘云能够顺利地协同工作。在本调查论文中，我们研究了与卸载问题有关的关键问题、方法和各种最先进的工作。我们采用了一个新的特征模型来研究从移动设备卸载到边缘云的整个过程。通过全面的讨论，我们的目标是在现有的努力和研究方向上全面了解 "大局"。我们的研究还表明，边缘云中的卸载算法在未来的技术和应用开发中具有巨大的潜力。少

2018 年 6 月 16 日提交;最初宣布 2018 年 6 月。

评论:23 页、9 个数字和 2 个表

213. 第 1806.06188[pdf,其他] Cs。镍

安全和可扩展的未来 fot-物联网架构的关键使能技术: 综述

作者:潘建利,刘元妮,王建宇,奥斯丁·赫斯特

摘要: 雾或边缘计算最近引起了业界和学术界的广泛关注。它被认为是从目前的集中式云计算模型的范式转变，并有可能带来一个 "**fot-iot**" 架构，这将大大有利于未来无处不在的物联网 (**iot**) 系统和应用。然而，实现这一愿景需要一系列关键的使能技术，包括新兴技术。在本文中，我们将特别关注这些关键的使能技术，这些技术是未来大规模部署的两个非常重要和急需的特征。我们的目标是为这些领域的研究和开发描绘一个全面的未来。少

2018 年 6 月 16 日提交;最初宣布 2018 年 6 月。

评论:7 页、5 个数字和 1 个表

214. 第 06:1806. 06 185[pdf,其他] Cs。直流

边缘链：基于区块链和智能合同的边缘-物联网框架和原型

作者:潘建利,王建宇,奥斯丁·海丝特, ismail alqerm, yuanni liu, ying zhao

摘要: 新兴的物联网（**iot**）正面临着巨大的可扩展性和安全性挑战。一方面,**物联网**设备"薄弱"，需要外部帮助。边缘计算为解决集中式云计算在扩展大量设备方面的不足提供了一个很有希望的方向。另一方面，由于资源限制,**物联网**设备也相对"脆弱"地面临着恶意黑客。新兴的区块链和智能合同技术为**物联网**和边缘计算带来了一系列新的安全功能。为了应对这些挑战，我们设计并原型设计了一个基于区块链和智能合同**的边缘-物联网**框架，名为"edge-"。其核心理念是整合一个允许的区块链和内部货币或"硬币"系统，将边缘云资源池与每个**物联网**设备的帐户和资源使用情况联系起来，从而将物**联网**设备的行为联系起来。EdgeChain 使用基于信用的资源管理系统，根据关于优先级、应用程序类型和过去行为的预定义规则，控制**物联网**设备可以从边缘服务器获得的资源数量。智能合同用于执行规则和策略，以不可否认和自动化**的方式规范物联网**设备的行为。所有**物联网**活动和交易都记录到区块链中，以便安全地进行数据记录和审核。我们实现了 EdgeChain 原型，并进行了广泛的实验来评估这些想法。结果表明，在获得区块链和智能合同的安全优势的同时，将它们集成到 EdgeChain 的成本在一个合理和可接受的范围内。少

2018 年 6 月 16 日提交;最初宣布 2018 年 6 月。

评论:14 页、13 位数字和 5 张表格

215. 第 6.6: 1806 06151 [pdf,其他] Cs。Db

多伊 10.1016/j.pmcj.2018.05.003

高效的数据摄动，实现隐私保护和准确的数据流挖掘

作者:m. a. p.chamikara, p. bertok, d.liu, s. camtepe, i.khalil

摘要: 物联网（**iot**）的广泛使用引起了许多关注，包括保护私人信息。现有的隐私保护方法不能在数据实用程序和隐私之间提供很好的平衡，而且在效率和可扩展性方面也存在问题。本文提出了一种有效的数据流摄动方法（称为 $p ^ 2rocal $）。$p ^ 2rocal $ 提供了更好的数据实用程序比类似的方法：分类精度 $p ^ 2rocal $ 扰动数据流是非常接近那些原始数据流。$p ^ 2rocal $ 还提供了更高的抵御数据重建攻击的能力。少

2018 年 6 月 19 日提交;v1 于 2018 年 6 月 15 日提交;最初宣布 2018 年 6 月。

评论:2018 年普适和移动计算

216. 第 xiv: 1806. 0606032 [pdf,其他] Cs。直流

vollet：物联网的大型虚拟环境

作者:shreyas badiger, shrey baheti , yogesh simmhan

摘要: **物联网**部署不断发展，包括传感器、网络、边缘、雾和云资源。尽管研究人员和从业者非常感兴趣，但大多数人无法使用大规模**的物联网**测试台进行验证。允许进行分析建模的仿真环境对于在实际计算环境中评估软件平台或应用程序工作负载来说是一个糟糕的替代方法。在这里，我们提出了一个虚拟环境，用于在云虚拟机中定义和启动大规模**物联网**部署。它提供了一个声明性模型，用于指定与使用 docker 的本机边缘、雾和云设备的性能相匹配的基于容器的计算资源。这些可以通过复杂的拓扑相互关联，在这些拓扑上强制执行私有网络以及带宽和延迟规则。用户还可以为这些设备上的数据生成配置合成传感器。我们对 vollet 使用 & gt; 400 台设备和 & gt; 1500 个设备内核进行部署进行验证，并显示虚拟**物联网**环境以低廉的成本与预期的计算和网络性能紧密匹配。这填补**了物联网**模拟器和实际部署之间的一个重要空白。少

2018 年 6 月 15 日提交;最初宣布 2018 年 6 月。

评论:将于 2018 年 8 月 27 日至 31 日在意大利都灵举行的第 24 届欧洲并行和分布式计算国际会议 (euro-par) 会议上发表，欧洲参与 20188 年。被选定为将提交会议全体会议的杰出文件

217. 第 xiv:1806.05766[pdf,其他] Cs。铬

pads: 高动态群拓扑的实用认证

作者:moreno ambrosin, mauro conti , riccardo lazzeretti , md masoom rabbani , silvio ranise

摘要: 远程认证协议广泛用于检测物联网 (iot) 方案中的设备配置 (例如，软件和/或数据) 的危害。不幸的是，在处理数千台智能设备时，此类协议的性能并不令人满意。最近，研究人员正专注于解决这一限制。方法是以集体的方式进行认证，目的是减少计算和通信。尽管取得了这些进展，但目前的认证解决方案仍然不能令人满意，因为它们复杂的管理和对拓扑的严格假设 (例如，是时间不变的或保持固定的拓扑)。在本文中，我们提出了一个安全、高效和实用的协议，用于证明具有非结构化或动态拓扑结构的潜在大型智能设备网络。港口及艾滋病方案以最近的非互动证明概念为基础，将集体证明问题简化为最低限度的共识问题。我们将 pads 与最先进的集体认证协议进行了比较，并通过使用显示实用性和效率的逼真仿真对其进行了验证。研究结果证实了 pads 适用于低端设备和高度非结构化网络的适用性。少

2018 年 6 月 14 日提交;最初宣布 2018 年 6 月。

评论:提交给 2018 年电子教育

218. 第 xiv:1806.05583[pdf,其他] Cs。直流

面向智能城市的物联网 (iot) 信息交易

作者:张泽辉,都喜尼亚托,王平，朱汉

摘要: 物联网 (**iot**) 技术是智能城市实施中信息传输和集成的基础设施，可实现高效的细粒度城市管理、高效运营并提高公民。智慧城市**物联网**系统通常涉及大量和多样的信息流通。信息生命周期还涉及许多各方、利益攸关方和实体，如个人、企业和政府机构，其目标本身的目标需要适当加以激励。因此，最近的研究将智慧城市**物联网**系统建模为一个市场，市场参与者将信息视为商品。在本文中，我们首先介绍了一个通用的以信息为中心的系统体系结构，用于分析智能城市**物联网**系统。然后讨论**物联网**中面向市场的方法的特点，包括市场激励、**物联网**服务模式、信息新鲜度和社会影响。并对系统设计的变化和相关工作进行了综述。最后，我们在智能城市**物联网**系统中优化信息交易，考虑到社会领域的直接和间接网络外部性。少

2018 年 6 月 14 日提交;最初宣布 2018 年 6 月。

219. 第 xiv:1806.05332[pdf,其他] Cs。铬

为资源受限的物联网设备实现强大且低成本的安全基础

作者:费泰梅· Tehranipoor

摘要: 近年来，由于全球化的趋势，系统集成商不得不比以往任何时候都更需要处理集成电路 (ic)/知识产权 (ip) 的假冒问题。这些假冒硬件会产生假冒硬件，从而满足对更安全的芯片身份验证的需求。来自物理源的高熵随机数是安全系统中身份验证和加密过程中的一个关键组件 [6] 。安全加密依赖于生成密钥的真正随机数的来源，并且需要一个芯片上的随机数生成器来实现足够的安全性。此外，物联网 (**iot**) 采用了大量基于

硬件的安全和预防解决方案，以便以高效的资源方式安全地交换数据。在这项工作中，我们开发了几种基于硬件的随机函数的方法，以解决这些问题，并增强 ic 的安全性和信任度：一种新的基于 dram 的固有物理不克隆函数 (puf) [13] 用于系统级安全性和同时分析各种环境条件的影响，特别是硅老化;基于 dram 的真实随机数生成 (trng) 生成开销非常低的随机序列;dram trng 模型使用其启动值行为创建随机位流;一种基于电源噪声的高效 trng 模型，用于生成无限数量的随机位，并被评估为一种具有成本效益的技术;物联网 (**iot**) 环境的架构和硬件安全解决方案。由于**物联网**设备的资源受到严重限制，我们提出的设计可以缓解以高效、低成本的方式建立值得信赖和安全性的担忧。少

2018 年 6 月 13 日提交;最初宣布 2018 年 6 月。

评论:7 页, 6 个数字, 1 个表

220. 第 xiv:1806.05242[pdf] Cs。铬

支持的区块链增强的物联网生态系统安全

作者:mahdi h. miraz , maaruf ali

摘要: 区块链 (bc) 是比特币加密货币系统背后的技术，它已开始被采用，以确保物联网 (**iot**) 生态系统中增强安全性和隐私性。目前，热研究正集中在学术界和产业界这一领域。工作证明 (pow) 是一个加密难题，通过维护被认为是廉洁的数字交易记录，在确保 bc 安全方面发挥着至关重要的作用。此外, bc 使用可变公钥 (pk) 来记录用户的身份，从而提供了额外的隐私层。不仅在加密货币方面成功地采用了 bc，而且在多方面的非货币体系中也得到了成功的实施，例如：分布式存储系统、位置证明和医疗保健。对最近的研究文章和项目或应用进行了调查，以评估物**联网安全 bc** 的实施情况，确定相关的挑战，并为有助于增强**物联网**生态系统的 bc 安全提出解决方案。少

2018 年 6 月 12 日提交;最初宣布 2018 年 6 月。

日记本参考:2018年计算机新兴技术国际会议 (icetic ' 18), 2018年8月23日至24日，英国伦敦都市大学，由 springer-verlag 出版

221. 第 xiv:1806.05165[pdf,其他] cs. it

学习在无人机辅助无线网络中进行通信：基于地图的方法

作者:omid esrafilian, ragiev gangula, david gesbert

摘要: 我们考虑的情况是，安装在无人机上的飞行基站向分布在地面上的一些无线电节点提供数据通信服务。重点研究了以 (i) 最优参数学习和 (二) 最优数据吞吐量为关键目标的资源约束无人机轨迹设计问题。虽然通过优化轨迹的问题已经在以前的工作中得到了解决，但有效地发现传播参数的优化路径的制定尚未得到解决。在数据通信阶段，这项工作的优势来自于三维城市地图的开发。虽然直接基于原始地图数据的飞行路径优化导致了一个棘手的不可微分成本最小化问题，但我们引入了一种新的地图压缩方法，使我们能够用标准工具来解决这个问题。然后将路径优化与节点调度算法结合起来。在城市**物联网**环境中阐述了学习路径优化和地图压缩方法在数据通信轨迹设计中的优势。少

2018 年 6 月 13 日提交;最初宣布 2018 年 6 月。

评论:12 页, 6 个数字，提交可能公布

222. 第 xiv:1806.04796[pdf] cs. cy

开放低功耗物联网技术生态系统的整体框架

作者:胡鹏

摘要: 由于最近的技术进步和生态系统满足了垂直应用的要求和市场需求，低功耗物联网 (**iot**) 蓬勃发展。低功耗**物联网**的**开放物联网**技术生态系统对所有参与者和利益相关者以及研究界来说变得越来越重要。然而，有几个主流的低功耗**物联网生态系统**可从行业联盟或研究项目中获得，其中隐含着不同的模式。我们需要确定幕后的工作框架，找出推动行业和研究界未来趋势的原则。通过仔细研究这些**物联网**技术生态系统，确定了四个主要业务模式，这些模式可以导致拟议的生态系统框架。该框架考虑了技术构成块、市场需求和业务垂直部分，这些部分正在使**物联网**在未来几年作为一个整体不断发展。少

2018 年 6 月 12 日提交;最初宣布 2018 年 6 月。

223. 第 xiv:1806.04582[pdf] Cs。镍

基于强化学习的各种物联网环境下的无线接入网资源分配

作者:almuthanna t. nassar , yasin yilmaz

文摘: 雾无线电接入网 (f-ran) 最近被提出来，以满足物联网 (**iot**) 应用的低延迟通信要求。我们考虑了将雾节点的有限资源按顺序分配给具有不同延迟要求的异构物**联网**应用程序的问题。具体来说，对于及时接收到的每个服务请求，雾节点需要决定是在本地为该用户提供低延迟通信服务，还是将其提交到云控制中心，以保持有价值的雾资源可供将来使用对系统具有更高利用率的用户 (即更低的延迟要求)。我们将问题表述为马尔可夫决策过程 (mdp)，采用两种替代公式：无限视距 mdp (ih mdp) 和有限视界 mdp (fh mdp)。在 ih 和 fh 配方中，我们通过强化学习 (rl) 提出了最佳解决方案，称为最优策略。使用不同的 rl 方法从 **iot 环境中**学习这两种情况下的最佳策略。与基于固定的实用程序阈值进行决策的简单方法相比，建议的 rl 方法的显著优势在于 rl 方法可以快速地从 **iot 环境中**学习最佳决策阈值，从而始终无论在何种环境下，都能实现最佳性能。它们在两个相互冲突的目标之间取得了适当的平衡，最大限度地提高了平均总服务效用与最小化雾节点的空闲时间。针对各种**物联网**环境的大量仿真结果证实了所提出的 rl 方法的理论基础。少

2018 年 5 月 27 日提交;最初宣布 2018 年 6 月。

224. 第 1806.03157[pdf,其他] Cs。镍

多伊 10.528 至素. 1098298

大规模物联网流量业务流程的一个公开/订阅 qos 感知框架

作者:pedro moraes, rafael reale , joberto martins

摘要: 物联网 (**iot**) 应用程序部署需要资源分配，如虚拟机、存储和网络元素，这些资源必须部署在不同的基础架构上，如云计算、物联网 (cot)、数据中心和骨干网。对于大规模**的物联网**数据采集，通常使用基于网关的数据聚合方法，其特点是传感器/执行器无缝访问，并提供缓存/缓冲和预处理功能。从这个角度来看，作为生产者的网关需要分配网络资源，以便向消费者发送**物联网**数据。本文提出了一种公共订阅 (pos) 服务质量感知 (psiot-orch) 框架 (psiot-orch)，该框架协调**物**联网流量，并在大规模**物联网**流量的聚合和使用者之间分配网络资源。psiot-orch 根据其配置的 qos 要求来规划**物联网**数据流。此外，该框架还通过受控制的主干网络分配网络资源 (lsp/零)，这些主干网络在**物联网**数据用户和使用者之间的资源有限且受限。网络资源使用带宽分配模型 (bam) 进行分配，以实现计划**物联网**数据流的高效网络资源分配。psiot-orch 采用 icn (以信息为中心的网络) pubsub 体系结构方法来处理框架组件之间的**物联网**数

据传输请求。拟议的框架旨在收集基于 icn 的方法的固有优势，使用 pubsub 消息方案，同时有效地分配资源，保持 qos 感知，并处理大量物联网的受限网络资源 (带宽) 交通状况。少

2018 年 6 月 8 日提交;最初宣布 2018 年 6 月。

评论:https://lrsm.ibisc.univ-evry.fr/Advance2018/

225. 第 xiv:1806.02975[pdf, ps,其他] cs. it

用于大规模物联网连接的新型稀疏编码环境反向散射通信

作者:tae yeong kim, dong in kim

摘要: 低功耗环境反向散射通信 (ambc) 依赖射频 (rf) 能量采集，是一种节能的无电池互联网 (**iot**) 解决方案。然而，环境反向散射信号被二进背散射通道 (dbc) 严重褪色，限制了传统的正交时间划分的 ambc (td-ambc) 中的连通性。为了支持 ambc 中的大规模连接，我们提出了基于非正交信令的稀疏编码 ambc (sc-ambc)。稀疏代码利用 ambc 固有的稀疏性，其中 rf 标签的电源依赖于环境射频能量采集。因此，稀疏编码的后向散射调制算法 (sc-bma) 可以实现非正交多重访问 (noma) 以及 m-ary 调制并发反向散射传输，从而提供额外的多样性增益。利用迭代消息传递算法 (mpa)，可以在接入点 (ap) 有效地检测到来自多个标记的稀疏码字。为了克服 dbc 和符号间干扰 (isi)，我们提出了二进信道估计算法 (d-cea) 和二进 mpa (d-mpa) 利用 isi 的加权和进行因子图中的信息交换。仿真结果验证了 sc-ambc 在连接性、检测性能和总和吞吐量方面的潜力。少

2018 年 6 月 8 日提交;最初宣布 2018 年 6 月。

评论:15 页, 10 个数字

226. 第 xiv:1806.02566[pdf, ps,其他] Cs。铬

基于 ai 的软件定义物联网网络两级入侵检测

作者:李嘉奇,赵志峰,李荣鹏,张洪刚

摘要: 软件定义的物联网 (**sdot**) 网络从集中式管理和交互式资源共享中获益，从而提高**了物联网**应用的效率和可扩展性。但随着服务和应用程序的快速增长，它很容易受到可能的攻击，并面临严峻的安全挑战。入侵检测已被广泛用于确保网络安全，但经典的检测手段通常是基于签名或基于明确行为的，无法智能地检测到未知攻击，难以满足 sd 的**要求。物联网**网络。本文提出了一种基于 ais 的两阶段入侵检测方法，该检测是由软件定义技术授权的。它通过全局视图灵活地捕获网络流，并通过应用 ai 算法智能地检测攻击。首先利用具有群分裂和微分突变的蝙蝠算法来选择典型特征。然后，利用加权投票机制自适应地改变样本的权重来对流量进行分类，从而开发随机林。评价结果表明，改进后的智能算法选择了更重要的特征，在流量分类方面取得了较好的性能。并验证了智能入侵检测具有较好的精度，与现有的解决方案相比具有较低的开销。少

2018 年 6 月 7 日提交;最初宣布 2018 年 6 月。

227. 第 xiv:1806.02474[pdf, ps,其他] Cs。镍

物联网中的时钟同步系统

作者:sathiya komaran mani, ramakrishnan durairajan, paul barford, joel sommers

摘要: 在物联网 (**iot**) 设备上同步时钟对于监控和实时控制等应用非常重要。在本文中，我们描述了**物联网**设备中的时钟同步系统，该系统设计为可扩展、灵活地适应各种硬件，并在一系列工作条件下保持紧密同步。我们首先研究两个标准**物联网**原型平台上的时

钟漂移。我们观察时钟漂移在相对较短的时间内的秒漂移，以及时钟速率稳定性差，每一个都使标准同步协议无效。为了解决这个问题，我们开发了一个同步系统，其中包括一个轻量级客户端、一个名为 sapt 的新数据包交换协议和一个可扩展的参考服务器。我们评估我们的系统在一系列配置、操作条件和目标平台上的有效性。我们发现，spt 在高噪声水平下分别比 mqtt 和 sntp 更准确地执行同步 22 x 和 17x，并在不同噪声水平下保持在 ~ 15 毫秒内的时钟精度。最后，通过微基准和广域实验报告了服务器实现的可扩展性，表明我们的系统能够扩展到有效地支持大量客户端。少

2018 年 6 月 6 日提交;最初宣布 2018 年 6 月。

228. 第 xiv:1806.02374[pdf,其他] cse

不同类型 web 服务描述的快速上下文注释分类

作者:serguei a. mokhov, joey paquet, arash khodadadi

摘要: 在最近 web 服务、**物联网**和云计算的快速增长中，许多 web 服务和 api 出现在 web 上。随着全球 uddi 注册表的失败，开始出现不同的服务存储库，试图列出和分类各种类型的 web 服务，以供客户端应用程序发现和使用。为了在执行服务组合或建议 web 服务的请求时，提高在经纪公司中查找兼容 web 服务的有效性并加快其任务，需要确定服务的高级功能。由于缺乏指定此类功能的结构化支持，因此有必要将服务分类为一组抽象类别。我们采用了广泛的机器学习和信号处理算法和技术，以便在本文的范围内找到可实现的最高精度，从而快速分类三种类型的服务描述: wsdl 、rest 和 wadl。此外，我们还通过展示上下文信息对服务描述分类的重要性和效果来补充我们的方法，并表明它提高了 5 个不同类别服务的准确性。少

2018 年 5 月 31 日提交;最初宣布 2018 年 6 月。

评论:扩大了 20 页;icprai 2018 年会议记录，第 562-570 页, concordia 大学, concordia, 蒙特利尔

229. 第 xiv:1806.02088[pdf,其他] Cs。镍

结合卫星的 5g 系统的体系结构和关键技术挑战

作者:a. guidotti, a. vanelli-corali, m. conti , s. andrenacci, s. chatzinotas, n. maturo, b. evans, a . awoseyila, a. ugolini, t. ffiggi, l. gaudio, n. alagha, s. cioni

摘要: 卫星通信系统是在未得到服务或服务不足的地区扩大和补充地面网络的一个有希望的解决办法。这一方面反映在最近的商业和标准化努力中。特别是, 3gpp 最近启动了一个新的无线电网络研究项目，即 5g 非陆地网络，目的是将卫星系统作为一种独立的解决方案或作为与移动宽带和机器类型的地面网络的整合通信方案。然而，典型的卫星信道损伤，如路径损失、延迟和多普勒变化，对实现基于卫星的 nr 网络构成了严峻挑战。本文根据目前在标准化中讨论的体系结构选项，讨论并评估了卫星信道特性对物理和中访问控制层的影响，包括传输增强的移动宽带 (embb) 和窄带物联网 (nb-iot) 应用的波形和程序.拟议的分析表明，主要的技术挑战与 phy\ mac 过程有关，特别是随机访问 (ra)、定时高级 (ta) 和混合自动重复重新查询 (harq)，并根据考虑到的服务和体系结构,提出了不同的解决方案。少

2018 年 6 月 6 日提交;最初宣布 2018 年 6 月。

评论:2018 年 4 月提交车辆技术交易

230. 第 xiv:1806 2008[pdf, ps,其他] Cs。铬

iot 链: 基于三层块链的物联网安全体系结构

作者:朴子健,石文波,何德标,金光雷蒙德·乔德

摘要: 人们对区块链在加强设备和系统 (**如物联网 (iot)**) 的安全性方面的潜力越来越感兴趣。在本文中，我们提出了一个基于区块链的**物联网**安全体系结构 iotchink。三层体系结构包括身份验证层、区块链层和应用层，旨在实现身份认证、访问控制、隐私保护、轻量级功能、区域节点容错、拒绝服务恢复能力和存储完整性。我们还评估 iotchink 的性能，以展示其在**物联网**部署中的实用性。少

2018 年 6 月 14 日提交;v1 于 2018 年 6 月 6 日提交;最初宣布 2018 年 6 月。

评论:23 页----11 位数字

231. 第 xiv:1806.019006[pdf,其他] Cs。铬

使用 fiware 和英特尔软件保护扩展 (sgx) 实现安全数据传播

作者:dalton cézane gomes valadares, matteus sthefano leite da silva, and 列 y elísio Matteus brito, ewerton Matteus salvador

摘要: 物联网 (**iot**) 领域受到业界和学术界的广泛关注，成为众多研发项目的主要课题。通常情况下，来自**物联网**应用程序生成的大量数据被发送到负责处理和存储的云服务。其中许多应用程序由于其敏感性质，需要其数据的安全性和隐私性。当此类数据必须在公共云中承载的实体中进行处理时尤其如此，在这些实体中，运行应用程序的环境可能不受信任。然后提出一些问题，因为为这些敏感数据提供所需的保护并非微不足道。我们提供了一个考虑 fiware 安全组件和英特尔 sgx 功能的解决方案。fiware 是一个平台，旨在支持包括**物联网**系统在内的智能应用程序的开发, sgx 是适用于可信执行环境 (tee) 的英特尔解决方案。我们为密钥管理提出了一个新组件，该组件与其他 fiware 组件一起可用于**为物联网**数据提供隐私、保密性和完整性保证。一个案例研究说明了如何在现实的场景中使用这一拟议的解决方案，这样可以通过公共云传播敏感数据，而不会有隐私问题的风险。实验结果证明，我们的方法不会损害系统的可伸缩性或可用性。此外，在考虑所实现的隐私保障的好处时，它还带来了可接受的内存成本。少

2018 年 6 月 5 日提交;最初宣布 2018 年 6 月。

评论:将在 ieee 2018 年计算机与通信研讨会上发表的论文 (iscc 2018)

232. 第 xiv:1806.01885[pdf, ps,其他] Cs。镍

多伊 10.1109/ICC.2018.8423017

通过软件定义的网络 (sdn) 实现协同物联网安全

作者:garegin Grigoryan, yaoeingliu, laurent njilla, charles kamhoua, kevin kwiat

摘要: 物联网 (**iot**) 正在成为网络犯罪分子日益具有吸引力的目标。我们观察到，对 **iot** 的许多攻击都是以串通的方式发起的，比如暴力攻击用户名和密码，以针对特定的受害者。然而，在大多数情况下，我们对此类攻击的防御机制是单独和独立地进行的，这导致防御无效和薄弱。为此，我们建议利用软件定义的网络 (sdn)，为传统的**基于 ip 的物联网**设备提供协作安全性。sdn 解耦控制平面和数据平面，可以帮助连接应用程序和网络层之间的知识。在本文中，我们讨论了**物联网**安全问题和挑战，并提出了一个基于 sdn 的体系结构，以协作的方式实现**物联网**安全。此外，我们还实现了一个平台，可以快速与同行控制器共享攻击信息，阻止攻击。我们使用 openflow 开关在虚拟和物理 sdn 环境中进行了实验。我们的评估结果表明，这两种环境都可以很好地扩展以处理攻击，但硬件实现比虚拟环境高效得多。少

2018 年 6 月 5 日提交;最初宣布 2018 年 6 月。

评论:ieee icc 2018

期刊参考: 2018 ieee 国际通信会议 (icc)

233. 第 xiv:1806.01444[pdf,其他] Cs。镍

多伊 10.115/326795.326267967

ndn、coap 和 mqtt: 物联网的比较测量研究

作者:cenk gündoan, peter kietzmann, martine lenders, hauke petersen, thomas c. schmidt, matthias wählisch

文摘: 本文对未来物联网 (**iot**) 的协议栈进行了全面的研究。它解决了哪种解决方案对常见**物联网**用例有益的整体问题。我们在单跳和多跳场景中的大型物联网测试台上部署 ndn 和两种流行的基于 ip 的应用程序协议 (coap 和 mqtt) 的不同变体。我们分析了不同负载下的定期和计划外流量的用例。我们的研究结果表明: (a) ndn 承认节点上最环保的部署, (b) 在多跳场景中表现出卓越的鲁棒性和恢复能力, 而 (c) ip 协议在单跳部署中以更低的开销和更高的速度运行。最引人注目的是, 我们发现基于 ndn 的协议比基于 udp 的 ip 协议具有更好的流量平衡, 并且需要较少的纠正措施。少

2018 年 9 月 27 日提交;v1 于 2018 年 6 月 4 日提交;最初宣布 2018 年 6 月。

日记本参考:2018 年含法律组织 icn 会议记录

234. 第 xiv:1806.01430[pdf] Cs。直流

面向开放物联网的 gpu 自动卸载技术研究

作者:yoki yamato, tatsuya demizu, hiumi noguchi, misao kataoka

摘要: **物联网**技术取得了进展。现在, 开放**物联网**的概念已经吸引了人们的关注, 通过集成水平分离的设备和服务来实现各种**物联网**服务。对于开放**物联网**时代, 我们提出了隐性计算技术, 以发现具有必要数据的设备, 供用户按需使用, 并动态使用它们。但是, 现有的 tacit 计算并不关心性能和运营成本。因此, 本文提出了一种基于遗传算法提取适当的卸载环路语句的战术计算的通用 gpu 卸载技术, 以提高其性能。我们评估 c/c ++ 矩阵操作, 以验证 gpu 卸载的有效性, 并在 1 小时的调整时间内确认超过 35 倍的性能。少

2018 年 6 月 4 日提交;最初宣布 2018 年 6 月。

评论:6 页, 日文, 5 个数字, ieice 技术报告, sc2018-10, 2018 年 6 月

日记本参考:ieice 技术报告, sc2018-10, 2018 年 6 月。(c) 2018 年 ieice

235. 第 xiv:1806.001 198[pdf] cs. cy

网络安全劳动力发展的新途径: 安全设计课程

作者:fil 提 o sharevski, adam trowbridge, jessica westbrook

摘要: 培训未来的网络安全劳动力以应对新出现的威胁, 需要在网络安全课程中引入新的教育干预措施。为了有效, 这些干预措施必须纳入网络安全和其他相关领域的趋势知识, 同时允许通过动手实验进行体验式学习。迄今为止, 传统的网络安全培训跨学科方法已将政治学、法律、经济学或语言学知识纳入网络安全课程, 允许进行有限的实验。网络安全学生几乎没有机会在这些领域以外的领域获得知识、技能和能力。另外, 外部专业的学生也没有进入网络安全的选择。考虑到这一点, 我们开发了网络安全和互动设计领域的体验式学习跨学科课程。开设本课程教授来自网络安全、用户交互设计和视觉设计的学生安全使用或安全设计的原则, 并允许他们将其应用于物联网 (**iot**) 产品

的原型设计。智能家居。本文阐述了安全设计的概念，以及我们的方法如何加强对未来网络安全员工的培训。少

2018 年 6 月 4 日提交;最初宣布 2018 年 6 月。

评论:2018 年第八届 ieee 综合 stem 教育大会 (isec)

236. 第 xiv:1806.01035[pdf, ps,其他] cs. it

无线网络中多天线多播的延迟性能

作者:marios kountouris, Apostolos avranas

摘要: 由于关键任务物联网 (**iot**) 应用程序和以内容为中心的服务的出现，低延迟通信目前正受到极大关注。深入了解延迟性能对于高效无线系统设计和端到端延迟保证至关重要。本文研究了物理层多天线多播的网络层性能，即当相同的数据同时传输给多个用户时。我们提供了服务过程的统计描述，根据其 mellin 变换，并推导出概率延迟边界使用工具从随机网络演算。此外，利用极值理论，我们将大量用户的服务过程描述出来，并推导出标度定律，将天线和用户的数量带到无穷大。我们的结果可用于系统尺寸测量，以保证无线多播网络中的延迟要求。少

2018 年 6 月 4 日提交;最初宣布 2018 年 6 月。

237. 第 xiv:1806.00951[pdf,其他] Cs。铬

基于区块链的物联网系统的双键隐身地址更快

作者:范新新

摘要: 隐身地址可防止区块链交易的输出与收件人的钱包地址的公共关联，并隐藏交易的实际目标地址。虽然隐身地址为加密货币网络提供了有效的隐私增强技术，但它需要区块链节点来主动监视所有事务并计算所谓的目标地址，这限制了其在资源受限的环境，如物**联网 (iot)**。在本文中，我们提出了 dksap-iot，这是一种更快的基于区块链**的物联网**系统的双键隐身地址协议.dksap-**物联网采用**了类似于 tls 会话恢复的技术，以提高性能并同时减少两个通信对等方之间的事务大小。我们的理论分析以及在嵌入式计算平台上进行的广泛实验表明，与最先进的方案相比，dksap-**物联网**能够将计算开销至少降低 50%，从而为它在基于区块链的**物联网**系统中的应用方式。少

2018 年 6 月 4 日提交;最初宣布 2018 年 6 月。

评论:将于 2018 年中国工商银行出版

238. 第 xiv:006.00882[pdf,其他] Cs。Lg

使用非 iid 数据的联合学习

作者:岳赵,孟丽,赖良珍,纳文·苏达,达蒙·奇辛,维卡斯·钱德拉

摘要: 联合学习使资源受限的边缘计算设备 (如移动电话和**物联网**设备) 能够学习用于预测的共享模型，同时保持培训数据的本地化。这种分散的模型培训方法提供了隐私、安全、监管和经济效益。在这项工作中，我们关注的是当本地数据是非 iid 时联合学习的统计挑战。我们首先表明，对于针对高度倾斜的非 iid 数据进行训练的神经网络，联合学习的准确性显著降低了 55%，其中每个客户端设备仅在单个类数据上进行训练。我们进一步表明，这种精度的降低可以用重量发散来解释，这可以用地球搬运工在每个设备上的类分布和种群分布之间的距离 (emd) 来量化。作为一种解决方案，我们提出了一种策略，通过创建在所有边缘设备之间全局共享的一小部分数据来改进有关非 iid 数据的培训。实验表明，只有 5% 的全局共享数据，cifar-10 数据集的精度可以提高 30%。少

2018 年 6 月 2 日提交;最初宣布 2018 年 6 月。

239. 第 xiv:806.00555[pdf,其他] cs. cy

机器对机器通信的智能合同: 可能性和局限性

作者:yuichi hanada, luke xiao, phillip levis

摘要: 区块链技术 (如智能合同) 为机器对机器的通信提供了一个独特的接口, 它提供了一个安全的、仅限附录的记录, 无需信任, 也无需中央管理员即可共享。我们通过设计、实施和评估 agasp (用于自动购买汽油的简单应用) 来研究使用机器对机器通信的智能合同的可能性和局限性。我们发现, 使用智能合同使我们能够直接应对**物联网**应用的透明度、寿命和信任方面的挑战。但是, 使用智能合同的实际应用程序必须解决其重要的权衡问题, 例如性能、隐私以及确保正确编写这些应用程序的挑战。少

2018 年 6 月 1 日提交;最初宣布 2018 年 6 月。

240. 第 1805 5.12272[pdf, ps,其他] Cs。镍

硬期限的预测边缘计算

作者:xing yuxuan , hh 利亚·seferoglu

摘要: 边缘计算是许多边缘应用和系统 (包括物联网 (**iot**)) 的本地化数据处理的一种很有前途的方法, 在这些应用和系统中,**物联网**设备中的计算密集型任务可分为子任务和子任务。卸载到其他**物联网**设备、移动设备和/或服务器的边缘。然而, 现有的边缘计算解决方案并不能解决所有的挑战, 特别是异质性;边缘设备本质上是高度异构和动态的。在本文中, 我们开发了一个具有硬期限的预测边缘计算框架。我们的算法;prcomp (i) 预测边缘设备资源的不确定动态, 包括能源、计算能力和移动性, (ii) 在考虑到预测的可用资源以及硬性期限的情况下, 做出子任务卸载决策任务的约束。我们在由真正的基于 android 的智能手机组成的测试台上对 prcomp 进行评估, 并表明与基线相比, 它显著提高了边缘设备的能耗和任务完成延迟。少

2018 年 5 月 30 日提交;最初宣布 2018 年 5 月。

评论:兰曼纸业的技术报告

241. 第 1805. 12263[pdf,其他] Cs。镍

在 lora 网络模拟器上使用 p-csma

作者:nikos kuvelas, vijay rao, r. r. venkatesha prasad

摘要: 低功耗广域网络 (lpwan) 的出现是为了满足物联网 (**iot**) 设备的需求, 从而实现了长寿命和长时间的运行。在 lpwan 中, 远程 (lora) 广域网是最有希望的;即将推出的**物联网**协议, 已被 kpn 和 ttn 等大型移动运营商采用。借助 lorwan,**物联网**设备可以在一个跃点内将数据传输到其相应的网关, 长达数公里, 占空比为 1%。但是, 在 lora 网络中, 任何设备都可以在不执行通道传感或与其他设备同步的情况下声明用于数据传输的通道。当每个网关连接的**物联网**设备数量增加时, 这将大大增加信息数据包的冲突次数。为了提高信道利用率, 我们提出了在 lorwan mac 层上应用持久载波感知多址 (p-csma) 协议的方法。在本手稿中, 我们报告了用于在 ns3 中模拟 lora 网络的 p-csma 组件的初始设计。特别是, 给出**了向物联网**设备添加 p-csma 功能的类。此外, 还详细介绍了这些类与它们所应用的现有 lorwan 模块之间的依赖关系和关系。此外, 我们还通过模拟 lora 网络, 从数据包接收比 (prr) 的角度对这个新的 p-csma lorawan 模块进行了评估。本报告是创建一个整体 p-csma 模块的第一步, 旨在支持网络研究人员和鉴赏家模拟 ns3 中 lora 网络的所有方面。少

2018 年 5 月 30 日提交;最初宣布 2018 年 5 月。

评论:ns3、lorawan、p-csma、信道感知、持久性、隐藏终端、可扩展性

242. 第 1805 5.11725[pdf, ps,其他] cs. it

绿色物联网无线传输能效的表征: 一种面向数据的方法

作者:杨红川,穆罕默德-斯利姆·阿卢伊尼

摘要: 物联网 (**iot**) 应用的日益普及给无线通信社区带来了新的挑战。**物联网**中的众多智能设备和传感器将生成大量的短数据包。未来的无线传输系统需要以极高的能效支持此类小数据的可靠传输。本文介绍了一种面向数据的新方法, 用于描述**物联网**应用中无线传输策略的能效。具体来说, 我们针对单个数据传输会话提出了新的能效性能限制。通过对两种通道自适应传输策略的初步分析, 提出了几种重要的小数据绿色传输设计指南。我们还提出了拟议的面向数据的能效特性的几个有希望的未来应用。少

2018 年 5 月 29 日提交;最初宣布 2018 年 5 月。

评论:2018 年 5 月向 ieee 通信杂志绿色通信系列提交了 14 页, 4 位数字

243. 第 1805 5.11482[pdf,其他] cs. it

通过机器学习实现 lte rach 碰撞多重检测

作者:davedmagrin, chiara pielli, cedomir stefanovic, miche zorzi

摘要: 在机器类型的流量情况下, 已知长期演化 (lte) 标准的随机访问通道 (rach) 过程中的碰撞解析机制是一个严重的瓶颈。它的主要缺点是, 基站 (eNBs) 通常无法推断碰撞用户设备 (ue) 的数量, 而碰撞的 ue 由于缺乏在 rach 后期阶段的反馈, 才含蓄地了解碰撞程序。然后, 碰撞的 ue 重新启动过程, 从而增加 rach 负载, 使系统更容易发生碰撞。在本文中, 我们利用机器学习技术设计了一个系统, 该系统在 lte rach 过程的前导检测方面优于最先进的方案。最重要的是, 我们的方案还可以估计碰撞多样性, 从而收集有关有多少设备选择相同的序言的信息。此数据可由 enb 用于解决冲突、增加支持的系统负载并减少传输延迟。该方法适用于针对大规模**物联网**(如 lte-m 和 nb-iot) 的新型 3gpp 标准。少

2018 年 5 月 29 日提交;最初宣布 2018 年 5 月。

评论:提交给 ieee globeicom 2018

244. 第 1805 5.11011[pdf] cs. cy

多伊 10.1109/MC.2017.195

用于安全和智能医疗保健的物联网基础架构的软件化

作者:mohammad a. salahuddin , ala al-fuqaha, mohsen guizani, khaled shuaib, farag sallabi

摘要: 我们提出了一个灵活的软件基础架构, 为智能医疗应用和服务提供灵活、经济、安全和隐私保护的物联网 (**iot**) 部署。它集成了**跨物联网**、雾和云领域的最先进的网络和虚拟化技术, 采用区块链、tor 和消息代理为患者和医疗保健提供商提供安全和隐私。我们提出了一个新的平台, 使用机器到机器 (m2m) 消息传递和基于规则的信标进行无缝数据管理, 并分别讨论了数据和决策融合在云中的作用和雾, 分别用于智能医疗保健应用和服务。少

2018 年 5 月 28 日提交;最初宣布 2018 年 5 月。

评论:9 页, 3 个数字

日记本参考:ieee 计算机杂志，第 50 卷，第 7 期，第 74-79 页，2017

245. 第 1805 5.987[pdf] cse

启用受信任的应用开发 @ 边缘

作者:托马斯·洛奇,安东尼·布朗,安迪·克拉布赖

摘要: 我们将数据库应用程序开发环境或 sdk 作为在网络边缘支持受信任**的物联网**应用开发的一种手段。databox 平台是一个专门的国内平台，可存储**物联网**、移动和云数据，并由第三方应用执行本地数据处理，以提供最终用户对数据流的控制并实现数据最小化。在边缘环境中构建应用的主要挑战涉及**物联网**设备的复杂性和用户要求，以及 ii。支持符合新数据保护法规的隐私保护功能。我们展示了数据库 sdk 如何减轻法规遵从性的负担，并在构建应用程序的过程中使用该 sdsd 来提高开发人员对隐私相关问题的认识。我们向超过 3000 人提供有关 sdk 的反馈，包括一系列开发人员和行业活动。少

2018 年 4 月 26 日提交;最初宣布 2018 年 5 月。

246. 第 1805 5.815[pdf,其他] Cs。铬

netra: 利用基于 nfv 的边缘流量分析增强物联网安全

作者:rishi sairam, suan sankar bhunia, vijayanand thangavelu, mohan gurusamy

摘要: 这是一个智能设备或东西的时代，它们正在推动物联网 (**iot**) 的发展。它正在影响我们周围的每一个领域，使我们的生活依赖于这一技术壮举。令人高度关切的是，这些智能事物正成为网络犯罪分子利用这些设备内的异质性、微小的安全功能和漏洞的目标。传统的集中式 it 安全措施在可扩展性和成本方面存在局限性。因此，需要对这些智能设备进行更靠近其位置的监控，理想情况下，要在**物联网**网络的边缘进行监控。在本文中，我们探讨了如何在网络边缘实现一些安全功能，以保护这些智能设备。为了在网络边缘部署安全功能，我们解释了网络功能虚拟化 (nfv) 的重要性。为了实现这一目标，我们引入了 netra-一种基于鸽子的新型轻量级体系结构，用于虚拟化网络功能，以提供**物联网**安全性。此外，我们还强调了与标准化 nfv 体系结构相比，拟议体系结构在存储、内存使用、延迟、吞吐量、负载平均值、可扩展性方面的优势，并解释了标准化体系结构不适合**物联网的原因**.我们研究了基于 nfv 的物**联网**安全边缘分析的性能，表明在不到一秒的时间内可以检测到精度超过 95% 的攻击。少

2018 年 5 月 28 日提交;最初宣布 2018 年 5 月。

247. 第 1805 5.783[pdf, ps,其他] Cs。镍

ecd: 移动边缘计算中的边缘内容交付和更新框架

作者:王尚光,丁春涛,张宁，程南，黄杰, 刘英

文摘: 本文提出了物联网时代基于移动边缘计算的边缘内容交付框架，以减轻核心网络的负载，提高移动用户的体验质量。考虑到移动设备既是内容消费者又是提供商，并且大部分内容没有必要上载到云数据中心，在网络边缘，我们部署内容服务器来存储从移动用户生成的原始内容,和缓存池，用于存储移动用户在 ecd 中经常请求的内容。缓存池是排名的，排名较高的缓存池将以更高的受欢迎程度存储内容。此外，我们还根据内容受欢迎程度和缓存池排名，提出了边缘内容交付方案和边缘内容更新方案。内容传递方案是为了有效地向移动用户传递内容，而边缘内容更新方案则是根据用户的请求频繁减少用户生成的内容到适当的缓存池，并缓存排名不佳。边缘内容交付与内容交付网络完全不同，可以进一步减少核心网络上的负载。此外，由于排名靠前的缓存池优先考虑优先级较高的内容，并且缓存池优先考虑优先级较高的内容，并且缓存池靠近

移动用户，因此移动用户和缓存池可以实现。提供了一个具有代表性的幼儿发展案例研究，并讨论了开放的研究问题。少

2018 年 5 月 28 日提交;最初宣布 2018 年 5 月。

248. 第 xiv:1805 5.10635[pdf, ps,其他] Cs。哦

用于绿色建筑管理的物联网

作者:wayes tushar, nipun wijerathne, wen-taili, chou yuen, h.vincent poor ' s poor ' s, kristin l. wood

摘要: 建筑物消耗了全球 60% 的电力。然而，目前的建筑管理系统非常昂贵，中小型建筑很难证明是合理的。因此，物联网 (**iot**) 可以监控和收集建筑物不同上下文上的大量数据，并将数据提供给 bms 的处理器，它提供了一个新的机会，可以将智能集成到 bms 中，以监控和收集以具有成本效益的方式管理建筑物的能耗。尽管有大量关于**基于物联网**的 bms 的文献，以及信号处理技术在建筑能源管理某些方面的应用，但对它们的集成进行详细研究以解决整个 bms 问题的研究相当有限.因此，拟议的文件将通过利用信号处理和机器学习技术概述基于**物联网**的 bms 来解决这一差距。研究了如何通过简单、低成本**的物联网**传感器提取高层建筑占用信息，研究了人类活动对建筑物能源利用的影响，可利用这些措施设计节能措施以减少建筑物的能耗。少

2018 年 5 月 27 日提交;最初宣布 2018 年 5 月。

评论:20 页, 7 个数字, 1 个表，接受的期刊论文

249. 第 1805 5.0401 [pdf,其他] Cs。铬

可信任物联网的无监督学习

作者:nikhil banerjee, than 下 il giannetsos, emmanouil panaousis, clive cheong 计

摘要: 物联网 (**iot**) 边缘设备与各种类型的传感器的进步使我们能够利用移动人群传感应用 (mcs) 利用各种信息。这种高度动态的设置需要收集无处不在的数据跟踪，这些数据跟踪来自于人们携带的传感器，带来了新的信息安全挑战;其中之一就是保持数据可信度。在这些设置中需要的是及时分析这些大型数据集，以准确洞察用户报告的正确性。现有的数据挖掘和其他人工智能方法是从**物联网**数据中获得隐藏见解的最常用方法，尽管存在许多挑战。本文首先在智能和合谋对手面前对 mcs 报告的网络可信度进行建模。然后，我们使用真实**的物联网**数据集，严格评估已知数据挖掘算法在**应用于物联网**安全和隐私时的有效性和准确性。通过考虑到潜在现象的时空变化，我们展示了概念漂移如何伪装攻击者的存在及其对聚类和分类过程准确性的影响。我们最初的研究结果清楚地表明，这些无人监督的学习算法容易受到对抗性感染，从而通过利用先进的机器学习模型和数学相结合，放大了在这一领域进行进一步研究的必要性优化技术。少

2018 年 5 月 25 日提交;最初宣布 2018 年 5 月。

评论:9 页, 9 个数字, 2018 年 ieee 模糊系统国际会议

250. 第 1805 5.0190 [pdf,其他] Cs。CI

剪辑语音平台：用于私人设计语音接口的嵌入式口语理解系统

作者:alice coucke, alaa saade, adreen ball, théodore bluche,亚历山大·考利耶, davidleroy, clément doumouro , thibault gisselbrecht,francescocaltagirone, thibaut lavril, maël primet, joseph dureau

文摘: 本文介绍了限听语音平台的机器学习架构，该平台是一种在**物联网**设备典型的微处理器上执行口语理解的软件解决方案。由于不收集个人用户数据，嵌入式推理在执行隐私的同时，在执行隐私的同时是快速和准确的。我们专注于自动语音识别和自然语言理解，详细介绍了我们培训高性能机器学习模型的方法，这些模型足够小，可以在小型设备上实时运行。此外，我们还介绍了在不影响用户隐私的情况下提供充足、高质量培训数据的数据生成过程。少

2018 年 5 月 25 日提交;最初宣布 2018 年 5 月。

251. 第 1805 5.09561[pdf,其他] cs. cy

基于 iot 的学校建筑绩效大数据分析

作者:ioannis chatzigiannakis, geargeos Mylonas, irene mavrommati , Dimitrios amaxilatis

文摘: 到目前为止,**物联网**在教育领域的应用已经落后于其他更多的商业应用领域。在本章中，我们将研究基于部署在欧洲教育建筑车队内的大型基础设施所产生的海量数据的许多方面。我们讨论了此基础架构如何基本实现一组不同的应用程序，并对此 **iot** 平台实施的性能方面进行了详细讨论，以及提供了对以下方面的见解:它在现实生活中的实际应用，无论是从教育和商业的角度来看。少

2018 年 5 月 24 日提交;最初宣布 2018 年 5 月。

252. 第 1805 5.09473[pdf] Cs。Lg

在具有局部量化区域的资源受限物联网设备中部署大型深神经网络

作者:杨毅,陈国荣,陈晓明,姜吉,陈振阳,戴燕

摘要: 在低成本**物联网**设备上实现计算复杂度较高的大型深部神经网络可能不可避免地受到有限计算资源的限制，使这些设备难以实时响应。这种分离使得最先进的深度学习算法，即 cnn (cnn) 与**物联网**世界不兼容。我们提出了一个低比特 (范围从 8 位到 1 位) 方案与我们的局部量化区域算法。我们使用 caffe 模型动物园中的模型作为示例任务，以评估我们的低精度数据表示方案的效果。利用局部量化区域的可用性，我们发现，在这些方案的基础上实现，除了降低计算复杂度外，还可以极大地保持模型的准确性。例如，我们的 8 位方案在英特尔 edison **物联网**平台上没有下降到前 1 名和前 5 名的精度，速度提高了 2 倍。基于我们的 4 位、2 位或 1 位方案的实现也适用于计算复杂度较低的**物联网**设备。例如，当使用 2 位方案时，我们任务的下降幅度只有 0.7%，这种方案可以在很大程度上节省晶体管。在这里使用低比特方案为商品**物联网**控制器的进一步优化打开了新的大门，即通过将多重累积操作替换为建议的表查找操作可以实现额外的加速。整个研究为解决将先进的深度学习算法引入资源有限的低成本**物**联网设备的挑战提供了一种新的途径。少

2018 年 5 月 23 日提交;最初宣布 2018 年 5 月。

253. 第 1805. 09254[pdf] Cs。镍

用于智能网格架构的雾辅助云模型--比较研究与优化部署

作者:md. muzakkir hussain, mohammad saad alam,m. m. sufyan beg

摘要: 云计算 (cc) 是满足现代智能电网 (sg) 存储和计算需求的关键驱动力。但是，由于数据中心部署在集中和遥远的地区，因此无法保证 sg 服务的体验 (qoe) 属性的质量，即延迟、带宽、能耗和网络成本。雾计算 (fc) 将处理能力扩展到网络边缘，为 sg 的关键任务需求提供位置感知、低延迟和延迟敏感分析。在本工作中，我们首先研究基

于云的 sg 体系结构的当前状态，并强调采用 fc 作为可持续和实时 sg 分析的技术促进因素的动机。然后，我们提出了一个分层 fc 体系结构，用于支持将大量**物联网**设备集成到未来的 sg 中。在此体系结构下，我们提出了一个成本优化框架，该框架共同研究数据使用者关联、工作负载分布、虚拟机放置和 qos 约束，以便通过 sg 网络实现 fc 模型的可行部署。然后使用改进的微分演化 (mde) 算法求解所提出的 minlp 问题。对拟议的真实世界参数框架的综合评估显示，对于具有近 50% 应用程序请求实时服务的基础架构，雾计算的总体服务延迟将减少到通用云的近一半范式。研究还表明，雾辅助云框架将纯云计算范式的总用电量降低了 40% 以上。少

2018 年 5 月 14 日提交;最初宣布 2018 年 5 月。

评论:8 个数字, 1 张桌子

254. **第: 1805.08898[pdf, ps,其他] cs. it**

通过 miso swipt 多播实现具有单独 qos 约束的能源可持续物联网

作者:deepak mishra, george c. 亚历山大·亚历山罗普洛斯, swades de

摘要: 能源可持续物联网 (**iot**) 的支持技术至关重要，因为低功耗网络设备的高数据通信需求激增。本文考虑了由多天线发射机 (tx) 组成的多输入单输出(miso) 多播物联网系统，该系统同时将信息和功耗传输到低功耗和数据匮乏的**物联网**接收器 (rx)。每个 **iot 设备都**假定配备了电源拆分 (ps) 硬件，可实现能量收集 (eh)，并对下行通信施加单独的服务质量 (qos) 约束。我们研究了 tx 预编码和物联网 ps 比率的联合设计，用于被考虑的 miso 同步无线信息和**功率传输**(swipt) 多播物**联网**系统，目的是最大限度地提高其中的最小采集能量**物联网**，同时满足其个人的 qos 要求。在我们新的 eh 公平最大化公式中，我们采用了通用射频 (rf) eh 模型，捕获实际整流操作，并产生了一个非凸优化问题。对于这个问题，我们首先提出了一个等效的半确定松弛公式，然后证明它具有独特的全局最优性。我们还在全局最优解决方案上推导出严格的上限和下限，该解决方案被用于获得目标关节设计的低复杂性算法实现。给出了最优 tx 波束形成方向、功率分配和**物联网** ps 比的解析表达式。我们具有代表性的数字结果，包括与基准设计的比较，证实了拟议框架的有用性，并就关键系统参数的相互作用提供了有用的见解。少

2018 年 5 月 22 日提交;最初宣布 2018 年 5 月。

评论:12 页, 13 位数字，可在《 2018 年 ieee 物联网杂志》上发表

255. **第: 1805.08876[pdf,其他] Cs。铬**

soteria: 物联网安全和安保自动化分析

作者:z. berkay celik, patrick mcdaniel, gang tan

摘要: 广义地定义为物联网 (**iot**)，将物理流程与数字系统集成在一起的商品设备的增长改变了我们的生活、游戏和工作方式。然而，现有**的物联网**平台无法评估**物联网**应用或环境是否安全、安全且运行正常。在本文中，我们介绍了 soteria，这是一个静态分析系统，用于验证**物联网**应用或**物联网**环境 (协同工作的应用程序集合) 是否符合已识别的安全、安保和功能属性。soteria 分三个阶段运作;(a) 将特定于平台的**物联网**源代码转换为中间表示 (ir), (b) 从 ir 中提取状态模型, (c) 应用模型检查来验证所需的属性。我们通过 35 个楼盘在 65 个智能物品市场应用上对 soteria 进行评估，发现 9 个 (14%) 的个人应用违反了 10 个 (29%) 属性。此外，我们对组合应用环境的研究发现了 11 起未在独立应用中显示的财产侵犯。最后，我们在 mal 联网上演示 soteria，这是一个新颖的开源测试套件，包含 17 个应用程序，其中有 20 个独特的违规行为。少

2018 年 5 月 22 日提交;最初宣布 2018 年 5 月。

评论:2018 年参加 usenix 年度技术会议 (usenix atc)

256. 第 09iv:1805 5.07907[pdf] Cs。Hc

iot2vec: 通过活动足迹识别类似的物联网设备

作者:kushal singla, joy bose

摘要: 我们考虑智能家居或智能办公环境，其中包括连接和相互传递数据的许多**物**联网设备。传输的数据的足迹可以提供有关设备的有价值的信息，这些信息可用于 (a) 识别**物联网**设备和 (b) 发生故障时，为这些设备确定正确的替代品。在本文中，我们使用 word2vec 生成智能家居中的**物联网**设备的嵌入，并探讨了对**物联网**设备 (又名 iot2vec) 有类似概念的可能性。这些嵌入可通过多种方式使用，例如在**物联网**设备存储区中查找类似设备，或作为每种类型**的物联网**设备的签名。我们展示**了对物联网**设备活动日志的 casas 数据集的可行性研究结果，使用我们的方法来识别家庭**中各类物联网**设备的嵌入模式。少

2018 年 5 月 21 日提交;最初宣布 2018 年 5 月。

评论:5 页, 4 个数字

类:I.2。6

257. 第: 1805.07738[pdf,其他] cs et

存储器对全差分跨频放大器性能的影响

作者:berik argimbayev, olga krestinskaya, alex pappachen james

摘要: 物联网 (**iot**) 技术和应用的进步需要高效的低功耗电路和架构来维护和提高日益增长的数据处理系统的性能。记忆电路和用记忆电阻器替代耗能器件是降低芯片上面积和功耗的一个很有前途的解决方案。本文提出了一种 cmos-mem-memichaty 全微分晶体管放大器，并评估了记忆电阻器对放大器性能的影响。采用 180nm cmos 技术对全差分放大器进行了仿真，具有 5.3-23mhz 带宽和 2.3-5.7kω当一个 1 pf 负载的时间增加。我们将基于记忆电阻器的放大器与传统的体系结构进行了比较。报道了增益、频率响应、线性范围、功耗、面积、总谐波失真和性能随温度的变化。少

2018 年 5 月 20 日提交;最初宣布 2018 年 5 月。

258. 第: 1805 5.07487[pdf,其他] Cs。铬

具有多个参考 puf 响应的轻量级 (反向) 模糊提取器

作者:高燕松,杨素,徐磊,达米思 c. 拉纳辛哈

摘要: 物理不克隆函数 (puf) 与人类的指纹相似，利用制造随机性将每个物理项与唯一标识符绑定在一起。一个主要的 puf 应用是通过模糊提取器进行安全加密密钥派生，其中包括两个顺序过程: 纠错和熵提取器。尽管熵提取器可以是非常轻量级的，错误修正逻辑负责协调自然模糊 puf 响应的开销是非常昂贵的，但仍然是非常昂贵的。当 puf 的目标是保护资源约束物联网 (**iot**) 对象 (例如，计算能力和电池寿命有限) 时，这就会遇到硬度。在这项工作中，我们认识到，响应不可靠与 puf 工作的工作条件 (例如电压和温度) 之间存在近似的线性关系。我们第一次利用这样一个 {"重要}", 但 {"它无意中}" 事实。在 puf 密钥配置阶段，我们建议在不同的挑战下，在标称操作条件下只允许单个响应，而不是只注册一个响应，而不是在多个离散操作下生成多个参考响应 (mrr)条件。作为一个直接的应用，我们结合 mrr 与反向模糊萃取器 (rfe)，以实现基于 mrr 的 rfe (mr)3 个 fe)，很好地适应了轻量级的相互身份验证，这是因为开销大

大降低。为了检验 mrr 的泛化，它被采用在 fe 的情况下，称为 mr2 铁。两个 mr 的软件实现 3 个 fe 和 mr2 对无电池、资源限制的计算射频识别 (crfid) 装置进行了综合实验。少

2018 年 5 月 18 日提交;最初宣布 2018 年 5 月。

评论:11 页, 6 个数字

259. 第 1805 5.07013[pdf,其他] cs. it

用于自主无赠款高超载多址的盲接收波束形成

作者:袁志峰,李伟民, 胡玉洲, 杨迅, 唐红, 戴建强

摘要: 大量的物联网 (**iot**) 设备有望同时连接到 mmtc 和未来几代无线网络之外，这对 rach 程序、用户设备检测和通道等方面构成了严峻挑战估计。尽管空间组合在传统的基于赠款的传输中取得了显著的进步，但在为**物联网**用例量身定制的自主无赠款传输方面，这种技术陷入了两难的境地。为了解决这一问题，本文阐述了盲空间结合及其在数据专用 mud 中的结合，以回应学术界和业界对自主无农传输 (agf) 超载潜力的关注。盲空间组合可以解释为盲接收波束形成启发式。仿真结果表明，对于 agf 传输，盲空间结合增强的仅数据无 mud 性能是相当令人印象深刻的。少

2018 年 5 月 17 日提交;最初宣布 2018 年 5 月。

260. 第: 1805 5.06980[pdf,其他] Cs。铬

一种基于元状态 reram 的物理不可克隆函数的物联网密钥生成方案

作者:ashwija reddy korenda, fatemeh afghah, bertrand ambou

摘要: 在物联网 (**iot**) 中使用传统加密技术的一些主要挑战包括需要为这样一个大型网络生成密钥，将生成的密钥分发到所有设备，密钥存储，以及当对手获得对设备的物理访问权限时容易受到安全攻击的可能性。本文提出了一种新的 **iot** 秘密密钥生成方法，该方法利用了制造过程中引入的器件存储器中固有的随机性。提出了一种使用串行串联 BCH-Polar 码的模糊提取器结构，用于从基于 reram 的 \ 萃取 {个状态} 物理不可克隆函数 (puf) 中生成可重现的密钥，用于设备认证和密钥生成。基于 reram 的 puf 是**物联网**中身份验证和密钥生成的最实用的选择，因为它们的操作速度与系统的噪声水平或以下相同，因此与替代内存相比，它们更不容易受到侧通道攻击技术。但是，当前基于 reram 的 puf 呈现较高的假负身份验证速率，因为这些设备的行为在不同的物理条件下可能会有所不同，从而导致在不同的尝试中重新生成相同响应的可能性较低。本文提出了一种三元状态 puf 的秘密密钥生成方案，该方案可以利用串行连接的 BCH-Polar 模糊提取器对所需的密钥进行可靠的重构。实验结果表明，所提出的模型可以显著降低原始密钥和再生密钥之间不匹配的概率，而使用的具有 \ textiten {帮助器数据} 的位数量较少，而与以前提出的模糊提取技术。少

2018 年 5 月 17 日提交;最初宣布 2018 年 5 月。

评论:6 页, 8 位数字，国际无线通信和移动计算会议, 2018 年

261. 第 09iv:1805.06695[pdf,其他] Cs。镍

物联网实现的多址边缘计算综述

作者:pawani porambage, jude okwuibe, madhusanka liyanage, mika ylianttila, tarik taleb

摘要: 物联网 (**iot**) 最近已从一项实验技术发展成为产品和服务部门企业未来客户价值的支柱。这凸显了**物联网**在迈向第五代 (5g) 无线通信系统的过程中的重要作用。**物**

联网技术与智能和大数据分析相结合，有望迅速改变从医疗保健到智慧城市和工业自动化等多个应用领域的格局。多址边缘计算（mec）技术的出现旨在将云计算能力扩展到无线接入网络的边缘，从而提供对无线网络资源的实时、高带宽、低延迟访问。鉴于mec 能够在网络边缘提供云平台和网关服务,**物联网**被确定为 mec 的一个关键用例。mec 将以其密集的地域分布和对移动性的广泛支持，激发对超低延迟和高质量服务（qos）需求的众多应用和服务的发展。因此，mec 是物联网应用和服务**的重要**推动因素，需要实时操作。在本次调查中，我们全面概述了利用 mec 技术实现**物联网**应用及其协同效应的情况。我们进一步讨论了在**物联网**中启用 mec 的技术方面，并对其中的各种其他集成技术提供了一些见解。少

2018 年 5 月 17 日提交;最初宣布 2018 年 5 月。

评论:提交给 ieee 通信调查和教程

262. 第: 1805 5.06661[pdf,其他] Cs。镍

多伊 10.1007/978-3-030-00247-3 _ 28

在密集无线网络测试台中构建定制的多跳拓扑结构

作者:florian kauer, volker turau

文摘: 测试台是无线多跳网络评估的关键要素。为了使研究人员摆脱部署自己的试验台的麻烦，构建了远程可控测试台，如 fit/iot 实验室.然而，虽然**物联网**-lab 有大量的节点，但它们被部署在约束区域中。这一点，再加上无线电传播的复杂性，使得具有大量跃点的多跳拓扑的临时构造变得困难。本文提出了解决这一问题的策略方法，并提出了生成具有所需属性的拓扑的算法。对**物联网**实验室测试台的实现进行了评估，并将其作为开源软件提供。结果表明，即使在密集的无线试验台中，也能建立各种类型的预置拓扑结构。少

2018 年 5 月 17 日提交;最初宣布 2018 年 5 月。

评论:12 页, 11 位数字

日记本参考:临时、移动和无线网络。adhoc-now 2018。《计算机科学讲座笔记》，第 114 卷。springer, cham

263. 第 1805.06583[pdf,其他] cs. it

基于 fdd 的多用户 mimo 通信有限反馈设计--利用物联网网络中的用户合作

作者:宋继浩,李炳菊,李钟浩

摘要: 多用户多输入多输出（mimo）系统是支持物联网（**iot**）网络中大规模连接密度的主要候选系统。在**物联网**网络中促进多用户信令的主要挑战之一是在发射机上获得准确的信道状态信息（csi），以便通过启用增强的 mimo 技术来提高频谱效率。但是，由于速率受限的反馈体系结构和耗时的调度框架，目前依赖频分复用（fdd）的通信机制可能无法完全支持大量设备。本文提出了一种用户合作算法，以开发适用于高密度**物联网**网络中通信系统的有限反馈策略。在该算法中，两个相邻用户形成一个单一的合作单元，通过相互共享一定程度的信道信息，最大限度地减少信道量化误差（通过反馈链路）。合作过程设计为在没有任何发射机干预的情况下运行，以满足**物联网**网络中的低延迟要求。此外，我们还利用所提出的协同反馈算法，分析了多用户 mimo 系统的估计速率吞吐量，研究了一个主动的用户协作决策框架。在分析研究的基础上，我们开发了一种自适应协作算法，根据渠道和网络条件打开和关闭用户协作模式。少

2018 年 7 月 13 日提交;v1 于 2018 年 5 月 16 日提交;最初宣布 2018 年 5 月。

评论:12 页, 4 位数字

264. 第 1805.06031 [pdf,其他] cs. cy

多伊 10.114/32262

利用上下文完整性发现智能家庭物联网隐私规范

作者:noah apthorpe, yan shvartzshnaider, arunesh mathur, dillon reisman, nick feamster

摘要: 面向消费者 "智能" 家居的物联网 (**iot**) 设备的激增引发了人们对用户隐私的担忧。我们提出了一种基于上下文完整性 (ci) 隐私框架的调查方法，该方法可以快速、高效地发现大规模的隐私规范。我们应用该方法在智能家居环境中发现隐私规范，在亚马逊机械土耳其人身上调查了 1731 美国成年人。在不到 6 小时的时间内，我们以 2, 800 美元和不到 6 小时的时间内测量了 3, 840 个信息流的可接受性，这些信息流代表了智能家居设备在各种条件下向第一和第三方收件人发送消费者信息的组合空间。我们的研究结果为**物联网**设备制造商提供了可操作的建议，包括设计最佳实践和采用我们的方法进行进一步研究的说明。少

2018 年 5 月 15 日提交;最初宣布 2018 年 5 月。

评论:23 页, 5 个数字, 3 个表

日记本参考:《交互式、移动、可穿戴和无处不在的技术论文集》，第 2 卷，第 2 期，第 59 条。2018 年 6 月

265. 第: 1805.05887 [pdf,其他] Cs。铬

lucon: 基于消息的物联网系统的数据流控制

作者:julian schütte , gerd stefan brost

摘要: 当今新兴的工业物联网 (iiot) 方案的特点是企业之间的服务之间的数据交换。传统的访问和使用控制机制只能确定一个主体是否可以使用数据，但对如何使用数据缺乏了解。然而，控制数据处理方式的能力对于企业保证 (并提供证据) 关键数据的合规处理以及需要控制其私人数据是否可能被分析或与附加数据链接的用户至关重要。信息-**物联网**应用处理个人信息的主要问题。在本文中，我们介绍了 lucon，这是一个以数据为中心的分布式系统安全策略框架，它通过控制消息在服务之间的路由方式以及如何组合和处理数据流来考虑数据流。lucon 策略可防止信息泄露，将数据使用与义务绑定，并在服务之间强制实施数据流。策略实施基于运行时的动态污点分析和针对策略的消息路由的前期静态验证。我们讨论了这两个补充实施模型的语义，并说明了如何将 lucon 策略从简单的策略语言编译为一阶逻辑表示形式。我们演示了 lucon 在实际物**联网**中间件中的实际应用，并讨论了它与 apachaccamel 的集成。最后，我们评估了 lucon 的运行时影响，并讨论了性能和可伸缩性方面。少

2018 年 5 月 14 日提交;最初宣布 2018 年 5 月。

评论:数据流控制，信息流控制，信任, 11 页

266. 第 1805.05853 [pdf,其他] Cs。铬

物联网安全: 端到端视图和案例研究

作者:郑玲,刘开正，徐一玲，高超，金一岳，邹克里夫，傅新文，赵伟

文摘: 在本文中，我们提出了**物联网**安全和隐私的端到端视图和一个案例研究。我们的贡献有三个方面。首先，我们展示了**物联网**系统的端到端视图，此视图可以指导**物联网**系统的风险评估和设计。我们确定了 10 个与安全和隐私相关的**基本物联网**功能。基于

此观点，我们系统地介绍了**云中物联网**系统、软件、网络和大数据分析方面的安全和隐私要求。其次，利用**物联网**安全和隐私的端到端视图，对 edmax ip 摄像系统进行了漏洞分析。我们是第一个利用这个系统的人，已经确定了各种攻击，可以完全控制制造商的所有相机。我们在现实世界中的实验证明了所发现攻击的有效性，并再次为**物联网**制造商发出警报。第三，在利用 edemax 摄像机和我们以前利用 edmax 智能插头时发现的此类漏洞可能会导致另一波米拉伊攻击，这可能是僵尸网络或蠕虫攻击。为了系统地了解米拉伊恶意软件的危害，我们对米拉伊的传播进行建模，并使用模拟来验证建模。本文的工作再次为**物联网**设备制造商敲响了警钟，以更好地保护他们的产品，从而防止像米拉伊这样的恶意软件攻击。少

2018 年 5 月 15 日提交;最初宣布 2018 年 5 月。

267. **第 09iv:18005.05674[pdf,其他] Cs。直流**

物联网生态系统的近似边缘分析

作者:文振宇, do le quoc, pramod bhatotia, ruicchan chen, myungjin lee

摘要: 支持**物联网**的设备继续生成大量数据。将不断获得的原始数据转化为及时的洞察对于许多现代在线服务至关重要。对于此类设置，对整个数据集的传统数据分析形式将受到令人望而却步的限制，并且对于支持实时流分析而言成本高昂。在本工作中，我们为**物联网**设置中的数据分析提供了近似计算的理由。近似计算的目的是在近似输出而不是精确输出的情况下高效执行工作流。近似计算背后的思想是在具有代表性的样本而不是整个输入数据集上进行计算。因此，基于所选择的样本量的近似计算可以在输出精度和计算效率之间进行系统的权衡。这推动了对于**物联网**中的近似计算的数据分析系统的设计。为了实现这一思想，我们设计了一种在线分层储层采样算法，该算法利用边缘计算资源产生具有严格误差边界的近似输出。为了展示我们算法的有效性，我们实施了基于 apache 卡夫卡的 approxiot，并使用一组微观基准和实际案例研究对其有效性进行了评估。结果表明，与简单的随机抽样相比, approxiot 实现了 1.3x-9.9x 的加速，采样分数变化为 80% 至 10%。少

2018 年 5 月 15 日提交;最初宣布 2018 年 5 月。

268. **第 xiv:1805 5.04880[pdf, ps,其他] Cs。铬**

照亮通往智能世界的道路: 基于网格的物联网加密技术

作者:徐瑞,志成,秦岳,姜涛

摘要: 乌克兰电网网络攻击提醒我们，智能物联网 (**iot**) 可以帮助我们控制灯泡，但如果受到攻击，也可能把我们带入黑暗。如今，许多文献都试图解决**有关物联网**安全的问题，但很少有文献考虑量子计算的进步对**物联网**造成的严重威胁。基于网格的密码学作为未来后量子密码学标准的一个有前途的候选技术，具有强大的安全保证和高效率的优点，使其非常适用于**物联网**应用。本文总结了基于网格的加密技术的优点及其在**物联网**设备上的实现现状。少

2018 年 5 月 13 日提交;最初宣布 2018 年 5 月。

269. **第 1805.04837[pdf, ps,其他] Cs。毫米**

多媒体物联网系统的边缘视频处理

作者:曹强,徐泽宇,秦鹏, 姜涛

摘要: 在本文中，我们首先调查了在三种典型情况下 (即**智能城市**、**卫星网络**和车辆互联网) 的边缘视频处理的现状。通过总结边缘视频处理的一般模型，突出了开发边缘计

算平台的重要性。然后，给出了一种基于轻加权虚拟化技术在边缘计算平台上实现协同视频处理的方法。进行绩效评估，并可获得一些有见地的意见。此外，我们还总结了为 m-iot 系统实现有效边缘视频处理所面临的挑战和机遇。少

2018 年 5 月 13 日提交;最初宣布 2018 年 5 月。

评论:7 页, 5 个数字, 1 个表

270. **第 1805.0 4747[pdf,其他] Cs。铬**

以消费者为中心的数据控制、跟踪和透明度----立场文件

作者:james tapsell, raja naeem akram, konstantinos markantonakis

摘要: 与用户的活动、偏好和服务相关的个人数据不仅被认为是谷歌、亚马逊和苹果等各种以技术为导向的公司的宝贵商品，也被认为是旅行运输等更传统的公司的宝贵商品银行、娱乐和营销行业。这导致了更有针对性的个人个性化服务----在大多数情况下，他们的财务费用最低。用户授权公司收集其个人数据以接收更多的个性化/目标/上下文感知服务和无忧活动 (针对用户) 的操作现实得到了广泛的部署。显然，所收集数据的安全性、完整性和可访问性至关重要。在物联网 (**iot**)、自主车辆和无缝旅行的时代，这些特征变得越来越根深蒂固。在本立场文件中，我们将探讨用户和组织在处理个人身份信息 (pii) 方面所面临的挑战。此外，我们还进一步阐述了《一般数据保护条例》(gdpr) 对 pii 管理的具体影响。随后，我们将讨论扩展到未来的技术，特别是**物联网**和集成运输系统，以获得更好的客户体验，以及它们在数据治理和 pii 管理方面的扩展。最后，我们提出了一个平衡用户隐私和数据控制的框架，以及一个组织的目标，即使用 "收集的用户数据" 向客户提供高质量、有针对性和高效的服务。此框架被称为 "面向消费者的数据控制 \ & amp; 审核性" (codca)，并定义了适合隐私问题和法律监管框架的技术。少

2018 年 5 月 12 日提交;最初宣布 2018 年 5 月。

评论:10 页, 2 图，会议

271. **第 xiv:1805 5.04282[pdf,其他] Cs。铬**

基于无信配送验证的物联网软件更新激励交付网络

作者:obd leiba, yechiav yitzchak, ron bitton, asaf nadler, asaf shabtai

摘要: **物联网**设备的普及使其成为攻击者的理想目标。为了降低攻击风险，供应商会定期为其设备提供安全更新 (修补程序)。由于可伸缩性问题，安全更新的交付变得很有挑战性，因为设备数量的增长可能比供应商的分发系统快得多。以前的研究表明，在一个基于权限和分散的基于区块链的网络中，节点可以承载和提供安全更新，从而增加了新的节点，从而扩展了网络。但是，这些研究并不鼓励节点加入网络，因此节点不太可能自由贡献其托管空间、带宽和计算资源。在本文中，我们提出了一种新型的分散**的物联网**软件更新交付网络，其中被称为分销商的参与节点由具有数字货币的供应商进行补偿，以便向设备提供更新。在发布新的安全更新后，供应商将承诺向提供更新的分销商提供数字货币;承诺将通过使用智能合同来作出，因此将是公开的、有约束力的和不可逆转的。智能合同承诺向提供分发证明的任何分销商提供补偿，这是一个更新交付到单个设备的不可预见的证据。分发服务器通过使用零知识或装付 (zkcp) 无信任数据交换协议交换设备签名的安全更新来获取分发证明。通过提供公平的补偿，消除了安全更新分发服务器和安全使用者 (**iot** 设备) 之间的信任需求，可以显著增加分销商的数量，从而促进快速扩展。少

2018 年 5 月 11 日提交;最初宣布 2018 年 5 月。

评论:ieee 区块链安全与隐私研讨会, 2018 年

272. 第 1805 5.04215[pdf,其他] Cs。pf

procal: 适用于物联网器件的低成本可编程校准工具

作者:李嘉志,贝南德兹富里

摘要: 校准是构建可靠的**物联网**系统的重要一步。例如, 精确的传感器读数需要 adc 校准, 在用于测量**物联网**设备的能耗之前, 必须校准功率监测芯片。在本文中, 我们介绍了一种低成本、准确且可扩展的功率校准工具 procal。procal 是一个可编程平台, 为校准提供动态电压和电流输出。其基本思想是使用数字电位器连接到通过数字交换机控制的并行电阻网络。procal 的电阻和输出频率由通过 spi 接口与主板通信的软件控制。我们的设计提供了一个简单的同步机制, 防止了精确的时间同步的需要。我们提出了数学建模和验证的工具结合了斐波那契序列的概念。我们广泛的实验研究表明, 该工具可以显著提高测量精度。例如, 对于 atmega2560, adc 误差从 0.2% 减少到 0.01%。procal 不仅成本低于当前商业解决方案的 2%, 而且能够提供广泛的电流和电压值, 因此具有高度的精度。少

2018 年 5 月 10 日提交;最初宣布 2018 年 5 月。

报告编号:tr-siotlab-april2018-procal

273. 第 1805 5.04101[pdf,其他] Cs。铬

多伊 10.114/3230383.3232807

在胡椒中添加盐: 一种基于人形机器人的结构化安全评估

作者:alberto giaretta, mic 其莱 e de donno, nicola dragoni

摘要: 互联互通、数字化、机器人技术和人工智能 (ai) 的兴起正在迅速改变我们的社会, 并塑造其未来的发展。在这场技术和社会革命中, 安全一直被忽视, 然而被黑客攻击的机器人可以在组织、行业、公共空间和私人住宅中充当内部威胁。在本文中, 我们对商业人形机器人辣椒进行了结构化的安全评估。我们的分析由自动化和手动部分组成, 指出了一些相关的安全缺陷, 可以用来接管和指挥机器人。此外, 我们建议如何解决这些问题, 从而避免今后的解决。这项工作的最终目的是**在物联网**产品在公开市场上销售之前推动其安全级别的提高。少

2018 年 7 月 4 日提交;v1 于 2018 年 5 月 10 日提交;最初宣布 2018 年 5 月。

评论:8 页, 3 个数字, 4 个表

274. 第 1805.04007 Cs。直流

物联网中的统一知识表示与上下文感知推荐系统

作者:yinhaoli, awa alqahtani, ellis solaiman, charith perera, prem prakash jayaraman, boualem benatallah, rajiv ranjan

摘要: 在快速发展的物联网 (**iot**) 中, 众多多样的物理设备、边缘设备、云基础架构及其服务质量要求 (qos) 需要在统一的规范中得到体现, 以便实现快速**的物联网**应用程序开发、监控和动态重新配置。但是, 不同配置知识表示模型之间的非均匀性**对协调物联网**应用的配置知识的获取、发现和管理构成了限制。本文提出了一种统一的数据模型来表示**物联网**资源配置知识的工件。它还提出了**物联网**-can (上下文感知建议系统), 以促进增量知识获取和声明性上下文驱动的知识推荐。少

2018 年 5 月 24 日提交;v1 于 2018 年 5 月 10 日提交;最初宣布 2018 年 5 月。

评论:本文是一篇不完整的草案。因此, 我想撤回它

275. 第 1805.03591 [pdf,其他] Cs。Lg

通过协作式在线学习实现物联网中的安全移动边缘计算

作者:李炳聪,陈天一,乔治奥斯 b. 吉安纳基斯

摘要: 为了适应物联网 (**iot**) 中的异构任务，出现了一种名为移动边缘计算的新通信和计算范式，它将计算服务从云扩展到边缘，但同时也带来了新的挑战。安全。本文研究了干扰攻击下的在线安全感知边缘计算。利用在线学习工具，分别开发了缩写为 save-s 和 save-a 的新算法，以应对干扰的随机形式和对抗形式。在不利用频谱和传输功率等额外资源来逃避干扰攻击的情况下，save-s 和 save-a 可以选择最可靠的服务器，以最小的隐私和安全考虑下卸载计算任务。通过分析，确定在没有任何关于未来干扰和服务器安全风险的信息的情况下，所提出的方案可以实现 o(t----√)后悔。设备之间的信息共享可以加快安全感知计算任务。save-s 和 save-a 结合了其他设备共享的信息，为转耳遗憾提供了令人印象深刻的改进，这被称为 "合作价值"。在合成数据集和实际数据集上测试了所提出方案的有效性。少

2018 年 5 月 9 日提交;最初宣布 2018 年 5 月。

276. 建议: 1805.039:1805 5.0409 [pdf,其他] Cs。铬

多伊 10.1109/MPRV.2018.03367731

n-baiot: 基于网络的使用深度自动编码器检测物联网机器人攻击

作者:yair meidan, michael bohadana, yael ma 特征 ov, yisroel mirsky, dominik breitenbacher, asaf shabtai , yuval elovici

摘要: **物联网**设备的普及比台式计算机更容易受到危害，导致基于**物联网**的僵尸网络攻击的发生增加。为了缓解这一新的威胁，有必要开发新的方法来检测从受损**的物联网**设备发起的攻击，并区分小时和毫秒长的基于物联网的攻击。本文提出了一种新的基于网络的异常检测方法，该方法提取网络行为快照，并利用深度自动编码器检测来自受损**物联网**设备的异常网络流量，并对其进行了实证评价。为了评估我们的方法，我们在实验室中感染了 9 个商业**物**联网设备，其中两个最著名的**基于物联网的**僵尸网络米拉伊和 bashlite。我们的评估结果证明了我们建议的方法能够准确和即时地检测攻击，因为这些攻击是从作为僵尸网络一部分的受损**物联网**设备发起的。少

2018 年 5 月 9 日提交;最初宣布 2018 年 5 月。

评论:接受于 7 月号出版 ieee 普适计算

msc 类: 68u35

277. 第 xiv:180 5.02982 [pdf, ps,其他] Cs。燃气轮机

基于方法的边缘计算资源分配: 一种市场均衡方法

作者:duong tong nguyen, long baole , vijay bhargava

摘要: 新兴的边缘计算模式有望提供卓越的用户体验，并实现广泛的物联网 (**iot**) 应用。在这项工作中，我们提出了一个新的基于市场的框架，以有效地分配资源的异构能力有限的边缘节点 (en) 到多个竞争服务的网络边缘。通过适当定价地理位置分散的 ens，建议的框架生成了一个市场均衡 (me) 解决方案，该解决方案不仅最大限度地提高了计算资源的边缘利用率，而且还分配了最佳 (即效用最大化) 资源由于其预算限制，服务的捆绑。当服务的效用被定义为服务可以从其资源分配中获得的最大收入时，可以通过求解艾森伯格-盖尔 (eg) 凸程序来集中计算均衡。取材于经济学文献。进一步表明，均衡分配是最优的，满足了所期望的公平属性，包括共享激励、相称性和无能力。此外，还介绍了两种可有效收敛到 me 的分布式算法。当每个服务的目标是最大限度地提高

其净利润 (即收入减去成本) 而不是收入时，我们推导出一个新的凸优化问题，并严格地证明其解决方案正是一个 me。为了验证所提出的技术的有效性，给出了大量的数值结果。少

2018 年 5 月 8 日提交;最初宣布 2018 年 5 月。

278. 第 1805.02818[pdf,其他] Cs。直流

物联网的区块链：机遇与挑战

作者:gowri sankar ramachandran, bhaskar krishnamachari

摘要: 区块链技术一直在改变金融业，并在过去十年中创造了一种新的加密经济。分散信任和分布式分类帐等基本概念对于分布式和大型物联网 (**iot**) 应用具有广阔的前景。然而，由于缺乏理解和固有的体系结构挑战，区块链在加密货币之外的应用在这一领域的应用很少。在本文中，我们描述**了物联网**区块链应用的机遇，并研究了构建基于区块链的**物联网**应用程序所涉及的挑战。少

2018 年 5 月 7 日提交;最初宣布 2018 年 5 月。

279. 第 1805 5.02797[pdf,其他] Cs。镍

基于电子双值 pc 的内容和计算感知通信，用于实时边缘计算

作者:sabur baidya, yanchen, marco levorato

摘要: 通过将计算资源放在单跳无线拓扑中，最近的边缘计算范式是实时物联网 (**iot**) 应用的关键推动因素。在**物联网**方案中，来自传感器的相同信息由位于不同位置的多个应用程序使用，因此需要复制数据流。但是，由于传输数据的网络容量有限，并行流的传输可能不可行。针对这一问题，提出了一种基于软件定义网络 (sdn) 范式的内容和感知计算的通信控制框架。该框架支持使用扩展的 berkeley 分组筛选器 (ebpf) 进行多流传输，在该筛选器中，每个特定计算过程的流量和数据包复制由内核内虚拟 ma-chine (vm) 内运行的程序控制。该框架被实例化，以解决来自多个摄像机的视频流传输到边缘处理器进行实时分析的案例研究场景。数值结果表明了该框架在可编程性、网络带宽和系统资源节约方面的优势。少

2018 年 5 月 7 日提交;最初宣布 2018 年 5 月。

评论:本文已被接受在 2018 年 ieee 国际计算机通信会议 (infocom 研讨会) 上发表

280. 第 1805 5.02751[pdf,其他] Cs。铬

多伊 10.1109/JIOT.2018.2866423

物联网儿童玩具的安全性和隐私性分析

作者:gordonchu, noah apthorpe, nick feamster

摘要: 本文通过对三种商业产品的案例研究，对连接互联网的儿童智能玩具的安全性和隐私进行了调查。我们使用静态和动态分析技术对每个玩具进行网络和应用程序漏洞分析，包括应用程序二进制反编译和网络监控。我们发现了一些公开未公开的漏洞，这些漏洞违反了儿童在线隐私保护规则 (coppa) 以及玩具的个人隐私政策。这些漏洞，尤其是与第一方服务器的网络通信中的安全缺陷，表明许多**物联网**玩具开发人员与安全和隐私最佳实践之间存在脱节，尽管人们对这些漏洞的关注越来越多。互联网连接的玩具黑客攻击风险。少

2018 年 8 月 28 日提交;v1 于 2018 年 5 月 7 日提交;最初宣布 2018 年 5 月。

评论:8 页, 8 位数字; 出版版

日记本参考:ieee 物联网杂志 (iot-j), 2018

281. 第 1805.02305[pdf, ps,其他] Cs。直流

边缘云物联网应用的统一管理和优化

作者:shadi a. noghabi, jack k 首府, peter bodik, eduardo cuervo

摘要: 物**联网 (iot**) 应用实现了惊人的增长，预计到2020年将发展到250亿美元的行业。随着**物联网**应用的规模不断扩大，对延迟的要求也越来越严格，边缘计算引起了人们对此类环境的兴趣。然而，业界仍处于起步阶段，无法适当支持在整个边缘云环境中运行的应用程序，也没有一系列手动繁琐的每个应用程序优化。在这项工作中，我们提出了 steel，这是一个统一的框架，用于在边缘云中开发、部署和监视应用程序。钢支持动态调整，并在边缘和云之间轻松地来回移动服务。在常见优化 (但对边缘至关重要) 可以作为可插拔和可配置模块构建的情况下，钢是可扩展的。我们增加了两个非常常见的优化: 放置和自适应通信，以应对工作负载和环境的短期和长期变化。少

2018 年 5 月 6 日提交;最初宣布 2018 年 5 月。

评论:被接受为 nsdi 2018 海报

282. 第 1805.01831[pdf,其他] 反渗透委员会

超低功耗深度学习动力自主纳米无人机

作者:daniele palossi, antonio loquercio, francesco conti, eric flamand, davel scaramuzza, luca benini

摘要: 在动态、城市、人口密集的环境中飞行是机器人技术中一个悬而未决的问题。最先进的无人机 (soa) 自主无人驾驶 (uav) 采用基于计算昂贵算法的先进计算机视觉技术，如同时本地化和映射 (slam) 或卷积神经网络 (cnn)在这样的环境中导航。在物联网 (**iot**) 时代，能够自主导航的纳米无人机作为自我意识**的移动物**联网节点将是非常理想的。然而，在纳米无人机的背景下，自主飞行被认为是负担不起的，在这种情况下，微小转子-工艺的超约束电源包将机载计算能力限制在低功耗微控制器上。在这项工作中，我们提出了第一个垂直集成系统，完全自主深度神经网络导航纳米大小的无人机。我们的系统基于 gap8，一个新的并行超低功耗计算平台，并部署在一个 27 克的商业，开源的裂纹和 flie 2.0 纳米四旋翼。我们讨论了一种方法和软件映射工具，使 soa cnn 在 [1] 中提出的完全执行在严格的 12 fps 实时约束内，在飞行结果方面没有妥协，而所有处理都是在平均只有 94 mw-1 部署的纳米飞机的功率包络的%。少

2018 年 5 月 4 日提交;最初宣布 2018 年 5 月。

评论:ieee 物联网杂志 (ieee iotj) 正在审查 12 页、10 个数字、6 个表格

283. 第 1805.01525[pdf,其他] Cs。铬

了解和减轻亚马逊亚历克莎和谷歌首页语音控制的第三方技能的安全风险

作者:张楠,米香航, 玄峰, 王晓峰,袁天, 钱峰

摘要: 虚拟个人助理 (vpa) (如 amazon 亚历克莎和 google 助手) 今天主要依靠语音通道与用户沟通，但众所周知，用户是脆弱的，缺乏适当的身份验证。vpa 技能市场的快速增长开辟了一条新的攻击途径，有可能允许远程对手发布攻击技能，通过热门**的物联网**设备 (如 amazon echo 和 google home) 攻击大量 vpa 用户。在本文中，我们报告了一项研究，得出这种远程、大规模攻击确实是现实的。更具体地说，我们实施了两种新的攻击: 语音蹲，其中对手利用技能的调用方式 (例如, "开放资本一")，使用具有类似发音的名称 (例如, "资本赢得") 或转述名称 (例如, "资本一请 ") 劫持语音命令，意味着不同的技能，和语音伪装，其中恶意技能模拟 vpa 服务或合法技能窃取

用户的数据或窃听她的对话。这些攻击针对的是 vpa 的工作方式或用户对其功能的误解，并被我们在 amazon echo 和 google home 上的实验 (包括用户研究和实际部署) 发现构成了现实的威胁。我们的发现的重要性已经得到了亚马逊和谷歌的认可，我们构建的新检测系统在亚历克莎和谷歌市场上发现的高风险技能进一步证明了这一点。我们进一步开发了自动检测这些攻击的技术，这些技术已经抓住了可能构成此类威胁的现实世界技能。少

2018 年 6 月 29 日提交;v1 于 2018 年 5 月 3 日提交;最初宣布 2018 年 5 月。

284. 第 1805 5.01374[pdf] Cs。铬

rf-puf: 通过使用原位机器学习对无线节点进行身份验证来增强物联网安全

作者:baibhab chatterjee, debayan das, shovan maity,shreyas sen

摘要: 射频 (rf) 系统中的传统身份验证通过数字签名和基于哈希的消息身份验证代码 (hmac) 等技术在网络中实现安全数据通信，这些技术会受到密钥恢复攻击。最先进的**物联网**网络 (如 neest) 还使用易于跨站点恢复伪造 (csrf) 的开放身份验证 (oauth 2.0) 协议，这表明这些技术可能不会阻止对手复制或建模使用侵入性、侧通道、学习或软件攻击的机密 id 或加密密钥。另一方面，物理不克隆函数 (puf) 可以利用制造过程的变化来唯一地识别硅芯片，这使得基于 puf 的系统以低成本实现极其强大和安全，因为实际上不可能复制相同的芯片模具上的硅特性。从人类通信中汲取灵感，利用语音签名中固有的变体来识别某个扬声器，我们提出了 rf-puf: 一个基于深度神经网络的框架，允许对无线节点进行实时身份验证，使用通过接收机端的原位机器学习检测到固有过程变化对无线发射机 (tx) 射频特性的影响。该方法利用了现有的非对称射频通信框架，不需要任何额外的电路来生成 puf 或进行特征提取。涉及标准 65 nm 技术节点的过程变化的仿真结果，以及在隐藏层中具有 50 个神经元的神经网络检测到的 lo 偏移和 i-q 不平衡等特征表明，该框架最多可以区分 4800 在不同的信道条件下，精度为 99.9% (10, 000 个发射机约 99%) 的变送器，无需传统的序言。少

2018 年 6 月 18 日提交;v1 于 2018 年 5 月 3 日提交;最初宣布 2018 年 5 月。

评论:接受: ieee 物联网杂志 (jiot), 2018 年

285. 第 1805.01332[pdf, ps,其他] cs. it

超可靠低延迟通信中的能量延迟权衡

作者:Apostolos avranas, marios kountouris, philippe ciblat

摘要: 通过超可靠的低延迟通信 (urllc)，物联网 (**iot**) 和触觉互联网的出现，可以实现高保真、实时的交互式应用。利用时间多样性以节能的方式满足 urllc 的要求是一项具有挑战性的任务，因为数据包大小、重传轮和延迟以及传输功率之间的相互作用非常重要。本文研究了采用增量冗余 (ir) 混合自动重复请求 (harq) 的 urllc 系统中的基本能量延迟权衡。我们用有限的块长度 (延迟) 约束和反馈延迟来推导平均能量最小化问题，这是非凸的。针对每轮再传输次数、堵塞长度和功率等方面，提出了一种高效节能 ir-harq 优化的动态规划算法。数值结果表明，与一次性变速器 (无 harq) 相比，我们的 ir-harq 方法可提供约 25 至 25% 的节能效果。少

2018 年 5 月 3 日提交;最初宣布 2018 年 5 月。

评论:期刊提交

286. 第 1805.01241 [pdf] cse

物联网: 质量保证和测试方法当前面临的挑战

作者:miroslav bures, tomas cerny, bestoun s. ahmed

摘要: 物联网 (**iot**) 技术的当代发展给质量保证领域带来了诸多挑战。讨论了当前与安全性、用户隐私、服务的可靠性、互操作性和集成有关的问题。所有这些都对**物联网**解决方案的特定质量保证方法产生了需求。本文介绍了这一领域的最新情况，并讨论了系统测试学科的具体领域，到目前为止，相关工作还没有涵盖这些领域。我们最近在 10 个**物联网**解决方案提供商中进行的一项调查的结果支持了这一分析，该调查涵盖**了物联网**应用的各个领域。少

2018 年 5 月 3 日提交;最初宣布 2018 年 5 月。

评论:10 页物联网 (iot)

杂志简介: 2018 年国际信息科学与应用研讨会

287. 第 09iv:1805 5.0162[pdf,其他] Cs。Lg

多伊 10.1109/CCNC.2017.7983123

安全网络: 车辆互联网和移动人群传感时代的安全运输路径

作者:刘群,苏曼·库马尔,维贾伊·马戈

摘要: 世界范围内的道路交通死亡率和事故率都很高，即使在美国这样的技术先进的国家也是如此。尽管智能交通系统取得了进展，但安全的运输路线，即寻找最安全的路线在很大程度上是一个被忽视的模式。近年来，人们、车辆互联网和物联网 (**iot**) 产生了大量的流量数据。此外，由于云计算的进步和移动通信技术的普及，现在可以对大量生成的数据 (人群来源) 进行分析，并将结果实时传递给用户。本文提出了一种安全的路径计算框架 safimet，利用这些技术分析流媒体流量数据和历史数据，有效地推断安全路径并将其实时传递给用户。safrnet 利用贝叶斯网络建立了安全的路由模型。此外，还提出了一个案例研究，以证明我们的方法使用实际流量数据的有效性。safrnet 打算在现代技术丰富的交通系统中提高驾驶员的安全性。少

2018 年 5 月 3 日提交;最初宣布 2018 年 5 月。

评论:论文在第十四届 ieee 消费者交流与网络大会 (ccnc 2017) 上被接受

288. 第 09iv:1805. 00969[pdf,其他] Cs。铬

物联网中一切事物的认证: 学习与环境影响

作者:yan sharaf dabbagh, walid saad

文摘: 要从物联网 (**iot**) 系统中获益，就必须开发特定于物**联网**的安全解决方案。由于**物联网**对象的计算有限和可移植性，传统的安全和身份验证解决方案通常无法满足**物联网**安全要求。本文提出了**一种物联网**对象认证框架。该框架使用特定于设备的信息 (称为指纹) 以及传输学习工具**来对物联网**中的对象进行身份验证。该框架跟踪物理环境变化对指纹的影响，并使用独特的**物联网**环境效应功能来检测网络和网络物理仿真攻击。提出的环境影响估计框架在不增加误报率的情况下提高了攻击者的检出率。该框架还证明能够检测到能够复制传统方法无法检测到的目标物体指纹的网络物理攻击者。提出了一种转移学习方法，允许在环境影响估算过程中使用具有不同类型和功能的对象，以提高框架的性能，同时捕获具有不同功能**的实际物联网**部署对象类型。实际**物联网**设备数据的仿真结果表明，该方法可以使网络仿真攻击检测提高 40%，能够检测出传统方法无法检测到的网络物理仿真攻击。结果表明，该框架提高了认证精度，而转移学习方法可获得高达 70% 的额外性能提升。少

2018 年 4 月 24 日提交;最初宣布 2018 年 5 月。

289. 第 09iv:805.00825[pdf,其他] Cs。镍

基于联合能力的物联网访问控制机制 (iot)

作者:徐荣华,陈宇,埃里克·布拉希,陈根舍

摘要: 物联网 (**iot**) 的普及使异构嵌入式智能设备能够协作提供智能服务，无论是否有人为干预。在利用基于智能电网和智能城市等大规模**物联网**应用的同时,**物联网**也会带来更多的隐私和安全问题。**iot** 面临的主要安全挑战之一是访问**授权对于 iot** 的资源和信息保护至关重要。传统的访问控制方法，如访问控制列表 (acl)、基于角色的访问控制 (rbac) 和基于属性的访问控制 (abac)，无法提供可扩展、可管理和高效的机制来满足**物联网**的要求系统。数量众多的节点、异质性和动态性，需要为**物联网**设备提供更精细、更轻量级的机制。本文提出了一个基于功能的联合访问控制 (fedcac) 框架，以便能够对大型**物联网**系统中的设备、服务和信息进行有效的访问控制。提出了一种基于身份的功能令牌管理策略，涉及访问授权的注册、传播和撤销。通过将集中授权决策策略委托给本地域委派者，访问授权过程在本地对服务提供商进行，该过程集成了态势感知 (saw) 和自定义上下文条件。我们的实验结果证明了拟议的 fedcac 方法的可行性，包括智能传感器和 raspberry pi 等资源受限的设备以及非资源受限的设备。为连接到系统网络的**物联网**系统提供可扩展、轻量级和细粒度的访问控制解决方案。少

2018 年 5 月 1 日提交;最初宣布 2018 年 5 月。

评论:spie 国防和商业传感 2018 (dcs)，空间应用传感器和系统会议，美国佛罗里达州奥兰多, 2018 年 4 月 15 日. arxiv 管理说明: 文本与 arxiv:1804.09 267

290. 第 09iv:18005.00789[pdf,其他] Cs。Hc

物联网与脑机接口的关系: 实现人的事物认知互动的统一深度学习框架

作者:张翔,姚丽娜,张帅，萨利尔·坎奈，全.. 盛军，刘云豪

摘要: 大脑-计算机接口 (bci) 获取大脑信号，分析这些信号并将其转换为命令，这些命令被中继到驱动设备，以执行所需的操作。随着物联网 (**iot**) 的出现实现了日常设备的广泛连接, bci 可以使个人能够直接控制智能家电或辅助机器人等对象，直接通过他们的想法。然而，实现这一愿景面临着一些挑战，最重要的是准确解释个人从原始大脑信号中的意图的问题，这些信号往往是低保真的，容易受到噪音的影响。此外，预处理大脑信号和随后的特征工程既耗时又高度依赖人类领域的专业知识。为了解决上述问题，本文提出了一个统一的基于深度学习的框架，该框架能够实现有效的人与事的认知交互性，从而将个人和**物联网**对象联系起来。我们设计了一种基于增强学习的选择性注意机制 (sam)，以发现输入大脑信号的显著特征。此外，我们还提出了一个改进的长期短期内存 (lstm)，以区分从 sam 转发的跨次元空间信息。为了评估建议框架的效率，我们进行了广泛的实际实验，并证明我们的模型优于一些具有竞争力的最先进的基线。提出了两个实用的实时人与事认知交互应用，验证了该方法的可行性。少

2018 年 10 月 22 日提交;v1 于 2018 年 5 月 1 日提交;最初宣布 2018 年 5 月。

评论:接受 ieee 物联网杂志 (http://ieee-iotj.org/). arxiv 管理说明: 实质性文本重叠与存档: 1804.0-05493

291. 第 09iv:1805 5.00428[pdf,其他] Cs。镍

在实际 crn 模型中用于 pue 攻击检测的递归神经网络研究

作者:齐东,陈宇,李晓华，曾凯

摘要: 物联网 (**iot**) 的普及和许多不同类型移动计算设备的广泛使用使无线通信频谱成为一种宝贵的资源。为了适应仍在快速增长的请求无线连接的设备数量，迫切需要更高效、更细粒度的频谱分配和共享方案。认知无线电网络 (cm) 已被广泛认为是一个有希望的解决方案，在这种解决方案中，允许二级用户 (sus) 与有执照的主要用户 (pu) 共享频道，只要不给 pu 的正常运行带来干扰。但是，恶意攻击者或自私的 sus 可能会模仿 pu 的行为来非法占用通道。准确、及时地检测此类主要用户仿真 (pue) 攻击是一件不平凡的事情。本文介绍了一种利用递归神经网络 (rnn) 进行有效的 pue 攻击检测方法。在采用基本 mn 的基本算法后，提出了一种利用长短时内存 (lstm) 的高级算法，该算法在处理具有长期记忆的时间序列方面更为有效。实验研究对 mn 取得的不同性能提供了更深入的见解，并验证了所提出的探测器的有效性。少

2018 年 5 月 1 日提交;最初宣布 2018 年 5 月。

292. 第 xiv:1804.11239[pdf,其他] Cs。直流

基于结构化重量矩阵的深部神经网络中的硬件加速器: fpga 和 asic

作者:丁彩文,阿仁,耿远, 马晓龙 , 李嘉宇,刘宁, 刘波元,王延志

摘要: 业界和学术界都广泛地研究了硬件加速。在本工作中，为了满足计算能力和内存需求的不断增加的需求，我们为 \ 强调 (领域可编程门阵列) 和 \ 强调 {提出了基于结构化权重矩阵 (swm) 的压缩技术。特定应用的集成电路} (asic) 实现。在算法部分，基于 swm 的框架采用块循环矩阵，实现精度和压缩比之间的细粒度权衡。基于 swm 的技术可以降低计算复杂度，从 o (n2) 到 o (n 日志 n) 和 o (n2) 到 o (n)，适用于每一层以及训练和推理阶段。对于深卷积神经网络 (dcnn) 上的 fpga 实现，我们分别使用基于 swm 的框架在性能和能效方面实现了至少 152x 和 72 倍的改进，而 ibm truenorth 处理器的基线则在使用 mnist、svhn 和 cifar-10 的数据集的精度约束相同。对于长期内存 (lstm) 网络上的 fpga 实现，与基线加速器相比，基于 swm 的 lstm 可以实现高达 21X 的性能增强和 33.5 倍的能效提升。对于 asic 的实现，基于 swm 的 asic 设计在功率、吞吐量和能源效率方面具有令人印象深刻的优势。实验结果表明，该方法非常适用于将 dnn 应用于 fpga 和移动/**物联网**设备。少

2018 年 3 月 28 日提交;最初宣布 2018 年 4 月。

评论:6 页, 7 个数字, glsvlsi2018

293. 第 1804 4.1135[pdf,其他] cs. it

物联网网络中认知频谱访问的非参数多阶段学习框架

作者:thulasi tholeti, vishnu raj, sheetal kalyani

摘要: 随着物联网的出现，越来越多的设备将连接到无线网络，频谱稀缺将是一个重大挑战。在**物联网**网络中应用机会主义频谱访问机制将变得越来越重要。本文提出了一种利用多级在线学习技术对设备进行频谱分配的认知无线网络体系结构，旨在提高**物联网**设备的吞吐量和能效。在第一阶段，我们使用 ai 技术来了解用户通道配对的质量。下一阶段利用非参数贝叶斯学习算法来估计每个通道中的主用户关闭时间。第三阶段通过内隐探索增强贝叶斯学习者，加快学习过程。该方法显著提高**了物联网**器件的吞吐量和能效，同时将对主要用户的干扰保持在最低限度。我们使用其他基于学习的方法对该方法进行全面的经验验证。少

2018 年 4 月 30 日提交;最初宣布 2018 年 4 月。

294. 第 1804.11118[pdf,其他] Cs。镍

窄带物联网覆盖增强方法的分析分析

作者:pilar andray-maldonado, pablo amegeiras, jonathan prados-garzon, juan j.ramos-munoz,豪尔赫·纳瓦罗-ortiz, juan m. Lopez-Soler

文摘 窄带物联网 (**nb-iot**) 作为蜂窝 **iot** 技术的引入旨在支持大规模的机器类型通信应用。这些应用的特点是来自大量低复杂性和低功耗设备的大量连接。**nb-iot** 的目标之一是在现有蜂窝技术之外改进覆盖范围的扩展。为了做到这一点,**nb-iot** 在上行链路中引入了传输重复和不同的带宽分配配置。这些新的传输方法在上行链路中产生了许多传输选项。在本文中，我们提出了分析表达式，描述了这些新方法在传输中的影响。我们的分析是基于香农定理。从所需的信噪比、带宽利用率和每个传输位的能量等方面对传输进行了研究。此外，我们还提出了一种上行链路自适应算法，该算法考虑了这些新的传输方法。所进行的评估总结了这些方法的影响。此外，我们还从我们提出的扫描设备覆盖范围的算法中提出了产生的上行链路适应。少

2018 年 4 月 30 日提交;最初宣布 2018 年 4 月。

评论:2018 年全球物联网峰会 (gots) 会议接受

295. 第 1804. 1070707[pdf,其他] Cs。铬

通过对具有 tee 的约束传感平台的相互认证，实现远程凭据管理的安全

作者:carlton sheperd, raja n. akram, konstantinos markantonakis

摘要: 受信任的执行环境 (tee) 正在迅速成为信任的主到根，它使用硬件支持的独立执行世界来保护敏感的应用程序和数据--超越相关的计划，如安全元素，以实现受约束的设备。tee 旨在通过远程认证提供敏感的**物联网**部署，并就关键算法执行、防篡改凭据存储和平台完整性提供可靠的保证。然而，在现有文献中，远程管理 tee 之间的凭据的挑战在很大程度上仍未得到解决。在这里，凭据必须保持受不受信任的系统元素的保护，并通过安全通道传输，并对其真实性和运行状态进行双向信任保证。在本文中，我们提出了使用相互证明远程 tee 凭据管理的四个关键领域的新协议：备份、更新、迁移和吊销。所提出的协议与 tee 实现和网络体系结构无关，符合**物联网**技术的要求和威胁模型，并使用 "scyther" 进行正式的符号验证，没有发现任何攻击。少

2018 年 4 月 27 日提交;最初宣布 2018 年 4 月。

评论:正在进行的工作, 20 页, 5 个数字, 6 个协议

296. 第 xiv:1804.09689[pdf,其他] cs. it

空间聚类 rf 供电物联网网络中的联合能量和 sinr 覆盖

作者:mohamed a. Abd-Elmagid, mustafa a.kishk , harpreet s. dhillon

摘要: 由于射频 (rf) 信号无处不在，射频能量采集正在成为**为物联网**设备供电的一个吸引人的解决方案。本文对一个利用射频能量并接收同一无线网络信息的**物联网**网络进行了建模和分析。为了启用此操作，每个时隙都被划分为充电和信息接收阶段。对于此设置，我们描述了两个性能指标: (i) 能量覆盖率和 (ii) 联合信号到干扰噪声 (snr) 和能量覆盖率。分析是使用逼真的空间模型进行的，该模型捕获**物**联网设备的位置与无线网络节点 (下称**物联网**网关) 之间的空间耦合，而无线网络节点在的文学。特别是，我们使用泊松群集进程 (pcp) 对**物联网**设备的位置进行建模，并假定某些群集的中心部署了**物联网**网关 (gw)，而其他 gw 的部署则独立于**物联网**设备。耦合级别可以通过调整部署在群集中心的 gws 总数的分数来控制。由于计算该设置的镜头噪声过程分布的内在可棘手性，我们提出了两种精确的近似方法，利用这两种近似方法对上述指标进行了表征。从我们的结果中得出多个系统设计见解。例如，我们演示了可最大限度

地提高系统吞吐量的最佳插槽分区的存在。此外，我们还探讨了物联网设备位置与 gws 之间的耦合级别对这一最佳插槽分区的影响。特别是，我们的结果表明，随着耦合水平的降低，充电阶段的最佳时间长度值也会增加。少

2018 年 4 月 25 日提交;最初宣布 2018 年 4 月。

297. 第 1804.09464[pdf, ps,其他] cs.it

低功耗广域物联网网络的优化资源调配和操作控制

作者:amin azari, meysam masoudi, cicek cavdar

文摘: 从通信的可靠性和耐久性方面研究了接入网成本与物联网设备提供服务质量之间的权衡。我们首先开发了面向上行的大规模物联网网络中的可靠性评估分析工具。这些工具包括利用时频异步无线电资源使用模式对异构干扰源的干扰进行建模，并受益于用于建模通道衰落和位置的现实分发过程。干扰源。我们进一步提出了接入网的成本模型，作为配置资源的函数，如接入点密度 (ap)，以及物联网设备的电池寿命模型，作为内部参数的函数，例如存储能量水平和网络参数，例如通信的可靠性。派生模型表示通过牺牲电池寿命 (耐久性) (例如，增加副本传输次数) 或牺牲网络成本和增加配置来实现所需可靠性水平的方式资源，例如 ap 的密度。然后，研究了最优资源配置和运营控制策略，前者旨在根据每个资源的成本寻找接入网的优化投资;后者的目的是优化物联网设备的数据传输策略。仿真结果验证了导出的分析表达式的紧密性，并说明了如何利用导出的表达式来寻找物联网网络的最佳操作点。少

2018 年 4 月 25 日提交;最初宣布 2018 年 4 月。

298. 第 1804.09336[pdf,其他] Cs。镍

无线量化指数调制: 通过现有信号实现通信

作者:zerina kaketanovic, vamsi talla, aaron parks, jing qian, joshua r. smith

摘要: 随着物联网设备数量继续呈指数级增长并使无线频谱饱和，迫切需要额外的频谱来支持大型无线设备网络。在过去几年里，提出了许多有希望的解决方案，但它们都受到新的基础设施成本、设置和维护的缺陷，或者由于 fcc 法规而难以实施。本文提出了一种新的无线量化指数调制 (qim) 技术，该技术利用现有的基础设施将信息嵌入到现有的无线信号中，与物联网设备进行通信，对原始信号的影响微乎其微。信号和零频谱开销。探讨了无线 qim 的设计空间，并对不同条件下电视、调频和调幅广播信号中嵌入信息的性能进行了评价。我们证明，我们可以嵌入多达 8-200~kbps 的消息，对原始 fm、am 和电视信号的音频和视频质量的影响可以忽略不计。少

2018 年 4 月 24 日提交;最初宣布 2018 年 4 月。

评论:8 页, ieee rfid

299. 第 1804.09307[pdf,其他] cs.it

环境反向散射系统: 淡入淡出通道下的精确平均误码率

作者:j. kartheek devineni, harpreet s. dhillon

摘要: 物联网 (iot) 范式的成功，除其他外，取决于开发节能通信技术，从而实现数十亿电池供电的物联网设备之间的信息交流。凭借其同时提供信息和能量传输的技术能力，环境反向散射正在迅速成为这种通信范式的一个吸引人的解决方案，特别是对于低数据速率要求的链接而言。本文研究了环境后向散射系统的信号检测和精确误码率的特征。特别是，我们在接收机上建立了一个二元假设测试问题，并在三种检测技术下分析了系统性能: a) 平均阈值 (mt)、b) 最大似然阈值 (mlt) 和 c) 近似 mlt。在物联

网设备的能量限制特性的推动下，我们对两种接收器类型进行了上述分析: (一) 能够准确跟踪信道状态信息 (csi) 的类型; ii) 不能准确跟踪通道状态信息的类型。分析的两个主要特点是对这项工作与现有技术的描述，即平均接收信号能量的精确条件密度函数的表征，以及对此设置的精确平均误码率 (ber) 的表征。关键的挑战在于处理两个假设的信道增益之间的相关性，以推导出误码率分析所需的震级平方通道增益的联合概率分布。少

2018 年 4 月 24 日提交;最初宣布 2018 年 4 月。

300. 建议: 1804. 09267[pdf,其他] Cs。镍

blendcac:block 基于分布式功能的 iot 访问控制

作者:徐荣华,陈宇,埃里克·布拉希,陈根舍

摘要: 物联网 (**iot**) 的普及使异构嵌入式智能设备能够协作提供智能服务，无论是否有人为干预。在利用基于大规模**物联网**的应用程序 (如智能电网或智能城市) 的同时, **iot** 还会对隐私和安全性产生更多关注。在 **iot** 面临的主要安全挑战中，访问授权对于资源共享和信息保护至关重要。当今访问控制 (ac) 的弱点之一是集中式授权服务器，它可能是性能瓶颈或单点故障。本文提出了一种基于交流的基于分散能力的区块链 --blendcac，用于 **iot** 的安全。blendcac 旨在对大型**物联网**系统中的设备、服务和信息建立有效的访问控制流程。在区块链网络的基础上，提出了一种访问权限传播的能力委派机制。提出了一种基于身份的强容量令牌管理策略，该策略利用智能契约对访问授权进行注册、传播和撤销。在拟议的 blendcac 方案中,**物联网**设备是自己的主人来控制其资源，而不是由一个中央机构监督。我们的实验结果在 raspberry pi 设备和本地专用区块链网络上实施和测试，证明了拟议的 blendcac 方法提供分散、可扩展、轻量级和细粒度交流解决方案的可行性. **物联网**系统。少

2018 年 4 月 24 日提交;最初宣布 2018 年 4 月。

301. 决议: 1804. 09266[pdf,其他] Cs。镍

认知无线电网络的一种自适应初级用户仿真攻击检测机制

作者:齐东,陈宇,李晓华，曾凯

摘要: 先进信息技术的普及，特别是物联网 (**iot**) 的广泛普及，使无线频谱成为宝贵的资源。认知无线电网络 (crn) 已被公认为实现通信频段高效利用的关键。由于动态频谱访问 (dsa) 的难度、高度复杂性和法规，保护 crn 免受恶意攻击者或自私的攻击者的攻击是非常具有挑战性的。主要用户仿真 (pue) 攻击是 crn 中一种易于启动但难以检测到的攻击，即恶意实体模仿 pu 信号，以便自私地占用频谱资源或进行拒绝服务 (dos) 攻击。本文以各种电子器件的物理特征为研究手段，提出了一种自适应、逼真的 pue 攻击检测技术。它利用了攻击者无法模仿的 pu 传输功能。在这项工作中，由于 pu 和攻击者之间的内在差异，传输功率被选定为难以模仿的功能之一，同时在实际实现中考虑约束。实验结果验证了该机构的有效性和正确性。少

2018 年 4 月 24 日提交;最初宣布 2018 年 4 月。

评论:将出席 2018 年 8 月 8 日在新加坡举行的第十四届通信网络安全与隐私国际会议 (安全通信 2018)

302. 第 1804.08 273[pdf, ps,其他] Cs。镍

模块化生产设施的无线通信

作者:christian schellenberger, marc zimmermann, hans d. schotten

摘要: 对个性化产品的需求不断增长，导致需要更灵活的产品生产。本文介绍了构成模块化生产设施的使用实例，并对其要求进行了阐述。对蓝牙（经典和 le）、zigbee、ieee 802.11（n 和 ah）和 4g 蜂窝技术（3gpp 版本 8、emtc 和 **nb-iot**）等现有技术进行了评估。此外，还讨论了未来可能的技术，如 5g nr 和专用蜂窝网络。少

2018 年 4 月 23 日提交;最初宣布 2018 年 4 月。

评论:7 页, 1 张表格

303. **第: 1804. 07474[pdf,其他] Cs。铬**

d 物联网: 一种用于检测受影响的物联网设备的自学习系统

作者:thien duc nguyen, samuel marchal , markus miettinen, n.asokan, ahad-reza sadeghi

摘要: **物联网**设备正在被广泛部署。由于不安全的实现和配置，他们中的许多人很容易受到攻击。因此，许多网络已经有了容易破坏的易受攻击的设备。这导致了一个新的类别的恶意软件，专门针对**物联网**设备。现有的入侵检测技术在检测受威胁的物联网设备方面并不有效，因为在涉及不同类型的设备和制造商的数量方面，问题的规模巨大。本文介绍了一种有效检测受损**物**联网设备的系统--diot。与以前的工作不同，d 联网使用一种新的自学习方法将设备分类为设备类型，并为每个设备构建正常的通信配置文件，这些配置文件随后可用于检测通信模式中的异常偏差。d 联网是完全自主的，可以以分布式众包的方式进行培训，而无需人工干预或标记培训数据。因此，物联网可以应对新设备类型的出现以及新的攻击。通过使用 30 多台**现成物联网**设备进行的系统实验，我们证明了 dot 在检测受到臭名昭著的米拉伊恶意软件危害的设备方面是有效的（94% 的检测率）和快速（2 秒）。在实际部署环境中评估时，物联网不会报告任何错误警报。少

2018 年 5 月 11 日提交;v1 于 2018 年 4 月 20 日提交;最初宣布 2018 年 4 月。

评论:18 页, 7 个数字, 9 个表

304. **第 1804. 07376[pdf,其他] Cs。镍**

多伊10.1109/JIOT.2017.2788802

通过雾卸载减少物联网服务延迟的探讨

作者:ashkan yousefpour, genya ishigaki, riti gour,jason p. jue

摘要: 随着物联网（**iot**）成为我们日常生活的重要组成部分，了解如何通过雾**计算提高物联网**应用的服务质量（qos）正成为一个重要问题。在本文中，我们介绍了**物联网**云应用程序的一般框架，并针对支持雾的设备提出了一种延迟最小化协作和卸载策略，旨在减少**物联网**应用的服务延迟。然后，我们开发一个分析模型来评估我们的策略，并展示拟议的框架如何帮助减少**物联网**服务延迟。少

2018 年 4 月 19 日提交;最初宣布 2018 年 4 月。

日记本参考:ieee 物联网杂志，第 5 卷，第 2 期, 998-1010 页, 2018 年 4 月

305. **特别报告: 1804.07190[pdf,其他] Cs。镍**

可靠的物联网存储: 在没有新节点的情况下最大限度地减少存储中的带宽使用

作者:赵晓波,丹尼尔 e. 卢卡尼,沈晓红,王海燕

摘要: 这封信描述了在物联网（**iot**）方案中的分布式存储问题的带宽使用和存储的最佳策略，在这些情况下，丢失的节点无法被新节点所取代，这通常是在数据中心和云中所假设的场景。我们开发了一个信息流模型，该模型捕获物联网设备之间数据传输的

整个过程，从最初的准备阶段（从原始数据生成冗余）到不同的修复阶段，越来越少设备。数值结果表明，在一个具有 10 个节点的系统中，所提出的优化方案可以节省多达 10.3 的带宽利用率，与最接近的次优方法相比，存储利用率可节省多达 44%。少

2018 年 4 月 19 日提交;最初宣布 2018 年 4 月。

评论:4 页, 3 位数字，可在 ieee 通信信函中发布

306. 第 1804.07141 [pdf] cs.cy

多伊 10.5220/0005915429043

智能城市政策分析的起源框架

作者:barkha javed, richard mcclatchey, zaheer khan, jetendr shamdasani

摘要: 基于物联网（**iot**）技术的可持续城市环境需要适当的策略管理。然而，这些政策是由于潜在的、复杂的和长期的决策过程而制定的。因此，更好的政策需要改进和可核查的规划进程。为了评估和评价规划过程，系统的透明度至关重要，可以通过跟踪决策过程的来源来实现。然而，目前还没有能够跟踪城市规划和决策整个周期的系统。我们建议捕获整个决策过程，并调查**物**联网来源的作用，以支持策略分析和实施的设计。这项研究将在其中得到展示的环境是智能城市的环境，其要求将推动研究进程。少

2018 年 3 月 19 日提交;最初宣布 2018 年 4 月。

评论:7 页, 1 个图, 1 个表

日记本参考:物联网和大数据国际会议的提案（iotbd 2016），第 499-434 页

307. 第 1804.06543 [pdf,其他] cs.it

uav 辅助物联网网络中的平均信息影响最小化

作者:mohamed a.abdelmagid , harpreet s. dhillon

摘要: 出于确保在物联网（**iot**）范式中及时提供信息（例如状态更新）的需要，本文研究了无人驾驶飞行器（uav）作为移动中继的作用，以最大限度地减少平均峰值源目标对的信息信息（paoi）。在此设置中，我们制定了一个优化问题，以共同优化无人机的飞行轨迹以及数据包传输的能量和服务时间分配。为了解决这个非凸问题，我们提出了一种有效的迭代算法，并对其收敛性进行了分析。还为一些子问题提供了闭式解决方案。我们在这个过程中解决的子问题之一是共同优化无人机给定轨迹的能量和服务时间分配。这个问题本身就引起了人们的兴趣，因为在某些情况下，我们可能无法根据**物联网**设备的位置改变无人机的轨迹（特别是当它的主要任务是别的时候）。我们的数值结果量化了通过额外优化无人机的轨迹可以获得的收益。少

2018 年 4 月 18 日提交;最初宣布 2018 年 4 月。

308. 第 1804.06404 [pdf, ps,其他] Cs。直流

fpga 是否适用于边缘计算?

作者:saman biookaghazadeh, fimboren, ming zhao

摘要: 物联网（**iot**）和人工智能应用的迅速发展提出了一种新的计算范式--边缘计算。本文从吞吐量敏感性、对算法特性的体系结构适应性和能效等方面研究了部署 fpga 进行边缘计算的适用性。这一目标是通过在英特尔 arria 10 gx1150 fpga 和 nvidia tesla k40m gpu 上进行比较实验来实现的。实验结果表明，采用 fpga 进行 gpu 边缘计算的主要优点是三倍: 1) fpga 可以提供一致的吞吐量不变的应用程序工作负载的大小，这对于聚合单个服务至关重要来自各种**物联网**传感器的请求;(2) fpga 以精细粒度和大规模提供空间和时间并行性，保证了加速高并发和高度依赖算法的一贯高性能;(3)

fpga 的功耗低 3-4 倍，能效高达 30.7 倍，提供更好的热稳定性和更低的每个功能的能源成本。少

2018 年 4 月 17 日提交;最初宣布 2018 年 4 月。

评论:6 页，热门 2018

309. 第 1804. 05501[pdf] Cs。铬

主动交通管理系统中的网络安全问题研究

作者:zulqarnain h. khattak, hyungjun park, seongah hong, richard atta boateng, brian l. smith

摘要: 运输机构已引入主动交通管理系统，以管理经常和非经常的挤塞情况。atm 系统依赖于有线和无线网络使组件的互连。不幸的是，这种支持 atm 系统的连接还提供了潜在的系统接入点，从而容易受到网络攻击。随着 atm 系统开始集成物联网 (**iot**) 设备，这种情况变得越来越明显。因此，有必要严格评估 atm 系统的网络攻击漏洞，并探索在网络攻击面前提供稳定性和优雅退化的设计概念。在这项研究中，开发了一个原型 atm 系统和一个实时网络攻击监测系统，用于北维吉尼亚州 i-66 1.5 英里的路段。监测系统通过将 atm 系统生成的车道控制状态与监测系统认为最有可能的车道控制状态进行比较，检测出 atm 系统的预期运行偏差。在两组状态之间出现任何偏差的情况下，监控系统将显示由备份数据源生成的车道控制状态。在仿真实验中, atm 原型系统和网络攻击监控系统受到了仿真网络攻击。评价结果表明，在受到网络攻击时，平均速度比 atm 系统下降了 1 5%，与基线情况相似。这说明 atm 系统的有效性被网络攻击所否定。然而，监测系统使自动取款机系统恢复到预期的安全状态，并减少了网络攻击的负面影响。这些结果表明，除了传统的系统入侵防护方法外，还需要重新审视 atm 系统设计概念，以此作为防范网络攻击的一种手段。少

2018 年 4 月 16 日提交;最初宣布 2018 年 4 月。

评论:25 页 7 位数字，可用于《运输研究记录》出版，《2018 年运输研究委员会杂志》

报告编号:trr 纸号: 18-03501

310. 第 1804. 05549[pdf, ps,其他] Cs。镍

缓解物联网中零日攻击的框架

作者:vishal sharma, jiyoon kim, soonhyun kwon, ilsun you, kyungroul lee, kkkbin yim

摘要: 物联网 (**iot**) 旨在为每个计算实体之间提供连接。然而，这种便利也导致更多的网络威胁，这些威胁可能会利用一段时间内脆弱性的存在。其中一个漏洞是零日威胁，它可能导致零日攻击，这对企业和网络安全都是有害的。本文介绍了**对物联网**网络的零日威胁的研究，并提出了一个基于上下文图形的框架，以提供缓解这些攻击的策略。该方法使用分布式诊断系统对中央服务提供者以及当地用户站点的上下文进行分类。一旦确定了潜在的零日攻击，就会使用关键的数据共享协议来传输警报消息，并重新建立网络实体和**物联网**设备之间的信任。结果表明，与集中诊断系统相比，分布式方法能够有效地缓解零日威胁，在运营成本和通信间接费用方面分别提高 33% 和 21%。少

2018 年 4 月 16 日提交;最初宣布 2018 年 4 月。

评论:6 页, 6 图，信息安全和密码学会议 (cisc-s17)

日记本参考:2017 年 6 月 22-23 日，韩国新昌-阿山，第 1-6 页

311. 第 xiv: 1804. 05533[pdf,其他] Cs。镍

基于上下文感知通信的车辆传感器数据资源高效传输

作者:benjamin sliwa, thomas liebig, robert falenberg, jones pillmann, christian wietfeld

摘要: 即将推出的智能交通控制系统 (itsc) 将根据为用作移动传感器节点的汽车获得的人群传感数据进行优化。总之，公共蜂窝网络将面临机器类型通信 (mtc) 的大幅增加，并将需要高效的通信方案，以最大限度地减少物联网 (**iot**) 数据流量对人类的干扰通信。在本演示中，我们提出了一个开源框架，用于车辆传感器数据的上下文感知传输，该框架利用有关传输通道特征的知识，以利用数据传输热点 (其中数据传输)可以执行一个较高的品位，如果资源效率。在会议上，我们将介绍用于获取和实时可视化所需网络质量指标的测量应用程序，并根据获得的测量数据展示传输方案在实际车辆场景中的性能从现场实验。少

2018 年 4 月 16 日提交;最初宣布 2018 年 4 月。

312. 决议: 1804. 05[pdf,其他] Cs。直流

资源约束边缘计算系统中的自适应联合学习

作者:王世强,蒂芙尼·图尔,西奥多罗斯·萨洛尼迪斯, kin k. leung, christianmakaya, tinghe, chevin chan

摘要: 新兴技术和应用，包括物联网 (**iot**)、社交网络和众包，在网络边缘产生大量数据。机器学习模型通常是根据收集到的数据构建的，以便能够检测、分类和预测未来的事件。由于带宽、存储和隐私问题，将所有数据发送到集中位置通常不切实际。本文考虑了从分布在多个边缘节点上的数据中学习模型参数的问题，而不将原始数据发送到集中位置。我们的重点是使用基于梯度下降的方法训练的通用机器学习模型。从理论上分析了分布式梯度下降的收敛性，在此基础上，我们提出了一种控制算法，确定局部更新和全局参数聚合之间的最佳权衡，以最大限度地减少损失函数在给定的资源预算下。通过对实际数据集的大量实验，对该算法的性能进行了评价，既可以在网络原型系统上进行，也可以在更大规模的模拟环境中进行实验。实验结果表明，在各种机器学习模型和不同的数据分布下，我们提出的方法表现得接近最优。少

2018 年 8 月 2 日提交;v1 于 2018 年 4 月 14 日提交;最初宣布 2018 年 4 月。

评论:当前版本包含一个新的收敛绑定，它比以前版本中的绑定更通用。当前版本中的控制算法和实验结果是新的。随着资源预算的无限，新的控制算法可以保证收敛到零最优性差距。实验是在较大的数据集上进行的，其中包括更多的结果

313. 第 xiv:1804. 04798[pdf,其他] Cs。铬

使用分布式分类器对网络设备进行值得信赖的配置管理

作者:holger kinkelin, valentin hauner, heiko niemerayer, georg carle

摘要: 如今，许多**物联网**应用，如楼宇自动化或工业场所的过程控制。这些应用程序本质上与物理世界有着密切的联系。因此, it 安全威胁不仅会导致数据泄露等问题，还会导致可能危害他人的安全问题。对 it 系统的攻击不仅由外部攻击者执行，还由管理员等内部人员执行。因此，我们介绍了正在进行的配置管理系统 (cms) 的工作，该系统提供对管理员的控制、限制其权限并强制分离关注点。我们通过执行配置管理过程来实现这一目标，该过程要求关键配置的多方授权，以实现拜占庭对管理员攻击和故障的容错能力。只有在配置得到多个专家的授权后，它才会应用于目标设备。对于整个配置管理过程，我们的 cms 保证问责制和可追溯性。最后，我们的系统是防篡改的，因为我们利用超分类帐结构，它为我们的 cms 提供了一个分布式执行环境，并提供了一个基于区块链的分布式分类帐，用于存储配置。这种方法的一个有益的副作用是，我

们的 cms 还适合管理不同组织之间共享的基础结构配置，这些组织不需要彼此信任。少

2018 年 5 月 8 日提交;v1 于 2018 年 4 月 13 日提交;最初宣布 2018 年 4 月。

评论:作者的版本----将在与网络操作和管理合用同一地点的分布式异构事物的分散编排和管理国际讲习班的会议上发表的最后论文研讨会 (noms)

314. 第 xiv:1804.04794[pdf,其他] Cs。镍

empiot：一种用于无线物联网设备的能量测量平台

作者:behnam dezfouli, immanuel amirtharaj, chia-chi li

摘要: 分析物联网设备并最大限度地降低**其**能耗是在各种应用领域应用**物联网**的重要步骤。本文提出了一种精确、低成本、易于构建、灵活、功率测量平台的 empiot。介绍了该平台的硬件和软件组件，研究了各种设计参数对精度的影响。重点分析了驱动器、总线速度、输入电压和缓冲机构对采样率、测量精度和处理需求的影响。这些广泛的实验研究使我们能够配置系统，以实现其最高性能。我们还提出了一种新的校准技术，并在各种设置下报告校准参数。我们使用五种不同的**物联网**设备执行四种类型的工作负载，根据从高精度设备获得的地面事实评估 empiot 的性能。结果表明，对于采用 802.15.4 无线标准的低功耗器件，测量误差小于 4%。此外，对于生成短、高功率峰值的基于 802.11 的设备，误差小于 3%。少

2018 年 4 月 13 日提交;最初宣布 2018 年 4 月。

报告编号:tr-siotlab-march2018-empiot

315. 第 xiv:18004.0461[pdf] cs. cy

通过物联网网络设备创建外向的机器人助手

作者:panagiotis Doxopoulos, konstantinos l. panayiotou , emmanouil g.tsardoulias, and 列 as l. symeonidis

摘要: 网络物理系统，包括机器和机器人，在它们之间以及与人类之间的沟通和协作，有望在未来几年吸引研究人员的兴趣。新革命的一个关键要素是物联网 (**iot**)。**物联网**基础架构支持使用互联网协议在不同连接的设备之间进行通信。机器人在**物联网**平台中的集成可以通过提供对其他设备和资源的访问来提高机器人的能力。本文介绍了一个**支持物联网**的应用，包括一个 nao 机器人，它可以通过**一个具有**反射测量系统的物联网平台进行通信，并提供以 restful web 形式提供面向机器人的服务的硬件节点。服务。还包括一个活动提醒应用程序，说明了系统的扩展功能。少

2018 年 4 月 12 日提交;最初宣布 2018 年 4 月。

评论:接受 iccr17

316. 第 xiv:18004.04358[pdf,其他] Cs。铬

清除为 mud：生成、验证和应用物联网行为配置文件 (技术报告)

作者:ayyoob hamza, dinesha ranathunga, h. habibi gharakheili, matthew roughan, vijay sivaraman

摘要: **物联网**设备越来越多地卷入网络攻击，这引发了社区对其给关键基础设施、企业和公民带来的风险的担忧。为了降低这种风险, ietf 正在推动**物联网**供应商以制造商使用说明 (mud) 的形式，为其**物联网**设备的预期用途制定正式规范，以便他们在任何运营中的网络行为环境可以被锁定和严格验证。本文旨在帮助**物联网**制造商开发和验证 mud 配置文件，同时还帮助这些设备的采用者确保它们与他们的组织策略兼容。我们

的第一个贡献是开发一种工具，该工具将任意 **iot** 设备的流量轨迹作为输入，并自动为其生成 mud 配置文件。我们将我们的工具作为开源提供捐助，将其应用于 28 台消费**物联网**设备，并突出介绍在此过程中遇到的见解和挑战。我们的第二个贡献是应用一个正式的语义框架，该框架不仅验证给定的 mud 配置文件的一致性，而且检查其与给定组织策略的兼容性。最后，我们将我们的框架应用于具有代表性的组织和选定的设备，以演示 mud 如何减少**物联网**验收测试所需的工作量。少

2018 年 4 月 12 日提交;最初宣布 2018 年 4 月。

317. 第 1804.04300[pdf,其他] Cs。铬

基于算术编码的轻量级联合压缩-加密-身份认证完整性框架

作者:alaa eldin rohiem shehata, hassan yakout el-arsh

摘要: 算术编码是一种高效的无损压缩方案，适用于许多多媒体标准，如 jpeg、jpeg 2000、h.263、h.264 和 h.265。由于非线性、高误差传播和算法编码器的高误差敏感性，已经开发了许多技术来扩大算术编码器作为轻量级联合压缩和加密解决方案的使用，作为一个轻量级的联合压缩和加密解决方案的系统有限的资源。通过本文，我们将介绍如何升级这些技术，以实现具有算术编码器的额外低成本身份验证和完整性功能。因此，新的技术可以为有限的资源环境 (**如物联网 (iot)** 和嵌入式系统) 生成一个安全且轻量级的压缩、加密、身份验证和完整性框架。尽管所提出的技术可以与任何基于算术编码器的系统一起使用，但我们将重点介绍 jpeg 和 jpeg2000 标准的实现。少

2018 年 4 月 11 日提交;最初宣布 2018 年 4 月。

318. 第 xiv:1804.04250[pdf] cs.cy

多伊 10.1109/MIC.2018.112102519

面向物联网和基于云的医疗保健系统的实用的优先级分析

作者:sagar sharma, keke chen, amit sheth

摘要: 现代医疗系统现在依靠先进的计算方法和技术，如物联网 (**iot**) 设备和云，以前所未有的规模和深度收集和分析个人健康数据。患者、医生、医疗服务提供者和研究人员依靠从这些数据来源获得的分析模型远程监控患者，早期诊断疾病，并找到个性化的治疗和药物。然而，如果没有适当的隐私保护，进行数据分析就会成为隐私噩梦的根源。在本文中，我们提出了在医疗保健信息系统中开发实用隐私保护分析的研究挑战。这项研究是基于 khealths----一个个性化的数字医疗信息系统，正在开发和测试疾病监测。我们分析相关方的数据和分析要求，识别隐私资产，分析现有的隐私基础，并讨论隐私、效率和模型质量之间的潜在权衡。少

2018 年 4 月 11 日提交;最初宣布 2018 年 4 月。

评论:2018 年 4 月

319. 第 1804.04159[pdf,其他] Cs。铬

面向消费类物联网设备的机器学习 ddos 检测

作者:rohan doshi, noah apthorpe, nick feamster

摘要: 越来越多的物联网 (**iot**) 设备正在连接到互联网，但其中许多设备从根本上是不安全的，使 internet 面临各种攻击。mi 莱等僵尸网络使用不安全的消费**物联网**设备对关键的 internet 基础结构进行分布式拒绝服务 (ddos) 攻击。这推动了自动检测消费者物联网攻击流量的新技术的发展。在本文中，我们证明，使用**特定于物联网**的网络行为 (例如有限的端点数量和数据包之间的定期时间间隔) 来通知功能选择，可以在**物**

联网网络中实现高精度的 ddos 检测流量与各种机器学习算法，包括神经网络。这些结果表明，家庭网关路由器或其他网络中间框可以使用低成本的机器学习算法和基于流和协议无关的流量数据自动检测本地**物**联网设备源的 ddos 攻击。少

2018 年 4 月 11 日提交;最初宣布 2018 年 4 月。

评论:2018 年深度学习和安全讲习班 (dls ' 18) 共 7 页、3 个数字、3 个表格

320. 第 xiv:1804. 03903[pdf,其他] Cs。直流

混合物联网：物联网的混合区块链体系结构-pow 子区块链

作者:gokhan sagirlar, barbara carminati, elena ferrari, john d.sheehan, Emanuele ragnoli

摘要: 物联网 (**iot**) 从早期就已发展成为一个分散的智能对象合作系统，除其他外，需要实现分布式共识。然而，当前**的物联网**平台解决方案是基于云的集中式计算基础架构，体现了许多重大缺陷，例如，云服务器维护成本高，支持时间紧迫的弱点**物联网**应用程序、安全和信任问题。将区块链技术启用到**物联网**有助于实现基于分布式共识的适当分布式物**联网**系统，从而克服这些缺点。虽然这是一个理想的匹配，但仍然是一个具有挑战性的努力。在本文中，我们通过设计**面向物联网**的混合区块链架构--**hyviri-iot**，朝着这一目标迈出了第一步。在 hych 进来-**物联网**中,**物联网**设备的子群形成了 pow 区块链，称为 pow 子区块链。然后, pow 子区块链之间的连接采用了 bft 连接器间框架，如 polkadot 或 cosmos。本文重点介绍了 pow 子区块链的形成，并以一组基于维度、度量和边界的准则为指导。为了证明该方法的有效性，我们进行了性能和安全性评估。少

2018 年 7 月 5 日提交;v1 于 2018 年 4 月 11 日提交;最初宣布 2018 年 4 月。

321. 第 1804. 03852[pdf,其他] Cs。铬

物联网设备的行为指纹识别

作者:bruhadeshwar bezawada, maalvika bachani, jordan peterson, hossein shirazi, indrakshi ray, Indrajit ray

摘要: 物联网 (**iot**) 带来了新的挑战，设备识别--设备是什么，认证--是它声称的设备。传统上，身份验证问题是通过加密协议解决的。然而，由于加密协议的计算复杂性和与密钥管理相关的可伸缩性问题，几乎所有基于加密的身份验证协议对**物联网**来说都是不切实际的。另一方面，设备识别问题不幸被忽视。我们相信，设备指纹识别可以有效地解决这两个问题。在本工作中，我们提出了一种方法来执行设备行为指纹，可用于进行设备类型识别。使用从设备的网络流量中提取的要素近似设备行为。这些功能用于训练可用于检测类似设备类型的机器学习模型。我们使用 5 倍交叉验证来验证我们的方法;我们报告的识别率为 86-99，平均准确率为 99%，在我们所有的实验中。即使设备使用加密通信，我们的方法也是成功的。此外，我们还展示了指纹设备类别的初步结果，即识别具有类似功能的不同设备类型。少

2018 年 4 月 11 日提交;最初宣布 2018 年 4 月。

评论:11 页, 7 个表, 7 个数字关键词: 物联网设备，物联网网络安全，设备行为，设备类型指纹，机器学习，网络流量功能

322. 第 1804. 03475[pdf,其他] cs. it

多伊 10.1109/MSP.2018.2844952

无源大规模连接的稀疏信号处理：物联网中随机访问协议的未来范式

作者:刘亮, erik g. larsson, wei yu, petar popovski, cedomir stefanovic, elisabeth de carvalho

摘要: 下一波无线技术将在连接传感器、机器和机器人以实现无数新应用方面激增，从而为物联网 (**iot**) 创造结构。**物联网**连接的通用方案涉及大量的机器类型连接。但在典型的应用程序中，在任何给定的时刻只有一个小 (未知) 设备子集处于活动状态，因此，提供大规模**物联网**连接的关键挑战之一是首先检测活动设备，然后用低延迟对其数据进行解码.本文概述了几种适用于大规模**物联网**接入问题的关键信号处理技术，主要侧重于先进的压缩传感技术及其在有效检测有源器件中的应用。我们证明，大规模的多输入多输出 (mimo) 特别适合于大规模**的物联网**连接，因为设备检测错误可以在有限的范围内作为基座上的天线数量连续驱动到零通过使用多测量矢量 (mmv) 压缩传感技术，站的速度达到无穷大。本文还对海量访问的几种相关的重要技术进行了展望，如将短消息嵌入到设备活动检测过程中和编码随机访问。少

2018 年 7 月 18 日提交;v1 于 2018 年 4 月 10 日提交;最初宣布 2018 年 4 月。

评论:出现在 ieee 信号处理杂志上，关于物联网信号处理的特刊

323. xiv:1804. 02904[pdf] Cs。铬

侧向: 一种基于侧通道的隐式安全随机导引头的启发式和原型，设计为平台和架构-不可知性

作者:jv roig

摘要: 生成安全随机数对于我们今天所依赖的安全和隐私基础架构至关重要。由于计算机系统的确定性，让计算机系统生成一个安全的随机数并不是一个微不足道的问题。服务器通常通过基于硬件的随机数生成器来处理此问题，这些随机数生成器可以以扩展卡、加密狗的形式出现，也可以集成到 cpu 本身中。然而，随着网络和互联网连接设备的爆炸，加密问题不再是一个以服务器为中心的问题;即使是小型设备也需要可靠的加密操作随机性来源--例如，网络设备和设备 (如路由器、交换机和接入点)，以及用于安全和远程的各种物联网 (**iot**) 设备管理。本文提出了一种基于侧通道测量的软件解决方案，作为高质量熵的来源 (绰号 "siderand")，理论上可以应用于大多数平台 (大型服务器、设备，甚至像 raspberrypi 或 arduino 这样的制造商板)，并为常规 ccprng 生成种子，以实现适当的加密操作，从而实现安全和隐私。本文还提出了两个标准--开放性和可审计性--作为对任何随机生成器进行加密使用的信心的基本要求，并讨论了 sidesand 如何满足这两个标准 (以及大多数硬件设备如何不满足这两个标准)。少

2018 年 4 月 9 日提交;最初宣布 2018 年 4 月。

324. 第 xiv:1804. 02834[pdf,其他] Cs。铬

基于 f 因为 f 因为的工业应用中的有限粒度访问控制，确保数据删除

作者:yong yu, liang xue, yannan li, den xias 江 du, mohsen guizani, bo yang

摘要: 云计算、雾计算和物联网 (**iot**) 的进步使行业比以往任何时候都更加繁荣。通过成功地集成云计算、雾计算和**物联网**，开发了广泛的工业系统，如运输系统和制造系统。安全和隐私问题是阻碍广泛采用这些新技术的主要问题。本文重点研究了有保证的数据删除问题，这个问题很重要，但在学术界和产业界受到的关注较少。我们首先提出了一个框架，将云、雾和事物结合在一起，以管理来自行业或个人的存储数据。然后，我们将重点放在此框架中的安全数据删除上，提出了一个有保证的数据删除方案，该方案实现了对敏感数据的细粒度访问控制和可验证的数据删除。删除数据密钥和验证数据删除时只涉及数据所有者和雾设备，这使得协议具有低延迟和雾计算实时交互的特

点而切实可行。该协议利用了基于属性的加密，在标准模型下可以证明是安全的。理论分析表明了良好的性能和功能要求，而实施结果则证明了我们的建议的可行性。少

2018 年 4 月 9 日提交;最初宣布 2018 年 4 月。

评论:9 页, 4 个数字

325. 第 1804. 02781 [pdf] Cs。铬

一种基于 iot 的智能电网中一种有效的基于随机响应的预置算法

作者:曹辉,刘树波,关志涛,吴龙飞,邓浩南,杜晓江

摘要: 在现有的隐私保护方法中，差异隐私 (dp) 是一种强大的工具，可以在统计数据库上提供隐私保护的噪声查询答案，并已被广泛应用于许多实际领域。特别是，作为 dp 的隐私机器，随机聚合可聚合的顺序级响应 (rappor) 为数据众包中的每个客户端字符串提供了强大的隐私、高效和高实用性的保证。然而，对于物联网 (**iot**) (如智能网格)，数据通常是分批处理的。因此，开发一种新的支持批处理的随机响应算法，往往比现有的随机响应算法更高效，更适合**物联网**应用。本文提出了一种新的随机响应算法，该算法可以实现消费者行为的差异化隐私和效用保护，并在每次处理一批数据。首先，在该算法中应用稀疏编码，从雾中的聚合能耗数据中创建了行为签名字典。然后，利用经典的随机响应技术将噪声添加到行为签名字典中，实现数据重新聚合后的差分隐私。通过对差分隐私原理的安全分析和实验结果验证，发现该算法可以在包含效用的情况下保护消费者的隐私。少

2018 年 4 月 8 日提交;最初宣布 2018 年 4 月。

326. 第 1804.02161 [pdf,其他] Cs。铬

分散物联网智能对象的隐私执法

作者:gokhan sagirlar, barbara carminati , elena ferrari

摘要: 物联网 (**iot**) 现在正在发展成为一个松散耦合、分散的协作智能对象系统，在这里，高速数据处理、分析和更短的响应时间变得比以往任何时候都更加必要。这种权力下放对保护智能对象生成和消费的个人信息的方式产生了很大影响，因为如果没有集中的数据管理，就更难控制智能对象如何组合和使用数据。为了解决这个问题，在本文中，我们提出了一个智能对象的用户可以指定其隐私首选项的框架。用户个人隐私首选项的合规性检查由智能对象直接执行。此外，认识到将强制机制嵌入到智能对象中意味着一些开销，我们在不同的场景中对建议的框架进行了广泛的测试，得到的结果表明了我们的方法的可行性。少

2018 年 4 月 6 日提交;最初宣布 2018 年 4 月。

327. 第 xiv:1804. 02139 [pdf, ps,其他] Cs。镍

适用于智能手机的轻量级移动自组网络路由协议

作者:md shahzamal

摘要: 移动自组织网络 (manet) 是一种很有前途的无线网络方法，在这种方法中，一组无线设备可以在没有任何基础结构的情况下在它们之间建立通信。manet 已成功地在应急通信、战场和车辆自组网 (vanet) 等领域得到了成功实施。最近, manet 也进行了研究，以建立村级离网电话系统使用移动电话 (智能手机)。随着移动电话和其他现代电子设备越来越多地配备高效的无线 wi-fi 设备，基于手机的 manet 实施将为手机的非自助服务以及**物联网**实施开辟新的视野。然而，由于对高内存、换相功率和高能耗的要求，目前的 manet 路由协议在移动电话中实现 manet 的性能较差。当网络中的

手机数量增加时，性能会严重下降。因此，轻量级路由协议是使用手机成功实施 manet 的关键要求。本文介绍了相关的路由协议设计及其在开发手机轻量级 manet 路由协议方面的适用性。总之，我们提出了这一领域的挑战和研究方向.

2018 年 4 月 6 日提交;最初宣布 2018 年 4 月。

评论:研究前沿报告 2015，计算系，麦格理大学，澳大利亚

328. 第 xiv:1804.02060[pdf，ps,其他] Cs。铬

lptd：在物联网中实现轻量级和优先的真理发现

作者:张川,朱立黄,张旭，沙里夫,杜晓江，莫赫森桂扎尼

摘要: 近年来，认知物联网 (c 联网) 由于能够从各种物联网 (**iot**) 设备中提取有价值的信息而受到了广泛的关注。在物联网中，真相发现在从大规模数据中识别真实价值以帮助 cot 从收集到的信息中提供更深入的洞察和价值方面发挥着重要作用。然而,**物联网**设备的隐私问题在设计真相发现方法时带来了重大挑战。尽管现有的真相发现方案可以在强大的隐私保证下执行，但它们效率不高，或者不能应用于实际的 cot 应用程序。本文提出了一个新的轻量级和隐私保护真相发现框架，称为 lptd-i，它是通过结合雾和云平台，并采用同态 paillier 加密和单向哈希链技术来实现的。该方案不仅保护了设备的隐私，而且实现了高效率。此外，我们还引入了一个容错 (lptd-ii) 框架，可以有效地克服 cot 设备故障。详细的安全分析表明，在全面设计的威胁模型下，所提出的方案是安全的。还进行了实验模拟，验证了所提出方案的有效性。少

2018 年 4 月 5 日提交;最初宣布 2018 年 4 月。

329. 第 1804.01822[pdf，ps,其他] Cs。铬

一种用于移动医疗人群传感的大型并发数据匿名批量验证方案

作者:刘景伟,曹惠娟,李庆清,蔡方辉，杜晓江,莫赫森·吉扎尼

摘要: 近年来，随着大数据的快速发展，物联网 (**iot**) 为人们的日常生活带来了越来越多的智能化、便捷的服务。移动医疗人群传感 (mhcs) 作为**物联网**的典型应用，正在成为为个人或组织提供各种医疗卫生服务的有效途径。然而，mhcs 在实践中仍然要面对不同的安全挑战。例如，如何在不泄露所有者敏感信息的情况下，快速有效地对**物联网**终端上传的大量生物信息进行身份验证。因此，我们提出了一种基于改进的无证书聚合签名的 mhcs 大规模并发数据匿名批处理验证方案。该方案可以通过隐私保护的方式同时对所有传感生物信息进行认证。不同用户生成的单个数据可以批量验证，而参与者的实际身份是隐藏的。此外，假设 cdhp 的难解性，我们的方案被证明是安全的。最后，性能评价表明，该方案由于效率较高，适合 mhcs。少

2018 年 4 月 5 日提交;最初宣布 2018 年 4 月。

330. 第 xiv:1804.01754[pdf,其他] Cs。哦

基于天气状况的数据中心能耗预测：遥感与机器学习方法

作者:geiranos smpokos，mohamed a. elshatshat，Athanasios lioumpas，lias liiopoulos

摘要: 数据中心 (dc) 的能耗不仅在成本方面，而且在运营可靠性方面，都是电信运营商非常重要的数字。能源消耗与天气状况之间的关系表明，天气预报模型可用于预测发展中国家的能源消耗。可靠的预测将使现有能源得到更有效的管理，并将更容易地利用以可再生能源为基础的现代电网。本文利用 fieta-iot 平台提供的功能，研究了 dc 的天气状况与能耗之间的相关性。然后，利用多变量线性回归过程，对能耗与优势天气条

件参数之间的相关性进行建模，以便根据天气预报对能耗进行有效预测。我们已经通过realdc 试验台的现场测量验证了我们的结果。我们提出的方法结果表明，根据天气条件预测能耗不仅有助于 dc 运营商管理其冷却系统和电力使用，而且有助于电力公司优化电力配电系统。少

2018 年 5 月 30 日提交;v1 于 2018 年 4 月 5 日提交;最初宣布 2018 年 4 月。

评论:6 页，数据中心的能源效率, dc-iot, fiesta-iot

331. 第 xiv:1804.01747[pdf,其他] Cs。镍

物联网与云计算集成的相关挑战的通信协议综述

作者:jesenka Dizdarevic, francisco carpio , admela jukan, xavi masaip-bruin

摘要: **物联网**(iot) 设备数量的快速增加正在加速对新解决方案的研究，以使云服务具有可扩展性。在此背景下，雾计算的新概念以及雾到云的组合计算模式对于分散云，同时使服务更接近终端系统变得至关重要。本文研究了满足**物联网**通信需求的应用层通信协议及其在雾与云**信息物**联网系统中的实施潜力。为此，本文首先对**物联网**通信协议的主要特点进行了比较分析，包括请求-回复和发布-订阅协议。之后，本文对系统每个部分 (**物联网**、雾、云) 中广泛采用和实现的协议进行了调查，从而开启了对其互操作性和更广泛的系统集成的讨论。最后，本文回顾了主要的性能问题，包括延迟、能耗和网络吞吐量。在集成**的物联网**到模糊系统体系结构中选择通信协议时，该调查有望对系统架构师和协议设计人员有所帮助。少

2018 年 4 月 5 日提交;最初宣布 2018 年 4 月。

332. 第 xiv:1804.01242[pdf,其他] Cs。镍

用于数据采集和感知的智能家庭网关平台

作者:潘旺,叶峰,陈学娇

摘要: 随着物联网 (**iot**) 和智能设备的扩展，智能家居备受关注。本文提出了一个智能家居网络数据采集和感知的智能网关平台。智能网关将取代连接家庭网络和互联网的传统网络网关。智能家庭网络支持不同类型的智能设备，如家庭**物联网**设备、智能手机、智能电器等。传统的网络网关无法提供服务质量测量、用户行为分析或网络优化。传统上，此类任务由部署在核心网络中的测量代理 (如光分流器或网络探头) 执行。我们建议的平台是一个轻量级插件，用于智能网关完成数据收集、感知和报告。虽然智能网关能够在本地调整数据收集和感知的控制策略，但也包括基于云的控制器，以实现更精细的控制策略更新。此外，我们还提出了一个多维感知框架，以实现智能网关的准确数据感知。通过对大量智能家居用户实际数据流量的测试，证明了该平台的数据收集效率和数据感知的准确性。少

2018 年 4 月 4 日提交;最初宣布 2018 年 4 月。

333. 第 xiv:1804.01239[pdf,其他] Cs。镍

基于模糊的智能电网物联网应用体系结构与编程模型

作者:潘王,刘世东, 叶峰,陈学娇

摘要: 智能电网利用多种物联网 (**iot**) 应用来支持其智能电网监控和控制。由于智能电网中的任务不同,**物联网**应用的要求也会有所不同。本文提出了一种新的计算范式，为智能电网中的**物联网**应用提供位置感知、延迟敏感监控和智能控制。特别是设计了一种新的基于雾的体系结构和编程模型。雾计算将计算扩展到网络的边缘，它与**物联网**应用完美匹配。然而，现有的方案很难满足智能电网雾计算节点内的分布式协调。在该模

型中，我们引入了一个新的分布式雾计算协调器，它定期收集雾计算节点的信息，如剩余资源、任务等。此外，雾计算协调器还管理作业，以便所有计算节点都可以在复杂的任务上进行协作。此外，我们还构建了智能电动汽车服务的工作原型，对该模型进行了评价。实验结果表明，我们提出的模型超过了传统**的智能电网**物联网应用雾计算方案。少

2018 年 4 月 4 日提交;最初宣布 2018 年 4 月。

334. **第鲁斯: 1804. 00706[pdf,其他] Cs。直流**

协同作用: 嵌入式异构 soc 上高通量 cnn 的 hwsw 框架

作者:郭文,阿克沙特·杜贝,谭城, tulika mitra

摘要: 卷积神经网络 (cnn) 已广泛应用于不同的应用领域。在使用高性能 gpu、fpga 和自定义 asic 进行数据中心规模环境的培训和推理方面取得了重大进展。最近移动和**物联网**设备的普及使得有必要在嵌入式级、资源受限的平台上进行实时、节能的深度神经网络推理。在此背景下，我们介绍了 {\em synergy}，这是一个自动化的、硬件软件共同设计的、流水线化的、高通量的基于嵌入式异构片上系统 (soc) 架构 (xilinx zynq) 的 cnn 推理框架。{\em synergy} 通过多线程利用所有可用的片上资源，其中包括双核 arm 处理器以及 fpga 和 neon simd 引擎作为加速器。此外, {\em synergy} 提供了异构加速器 (fpga 和 neon) 的统一抽象，并且可以在运行时适应不同的网络配置，而无需通过平衡工作负载更改底层硬件加速器体系结构通过工作盗窃跨越加速器。{\em synergy} 实现了 7.3 倍的加速，平均在 7 个 cnn 模型之间，超过了一个经过优化的纯软件解决方案。{\ em synergy} 与当代美国有线电视新闻网在同一 soc 架构上的实现相比，展示了更好的吞吐量和能效。少

2018 年 3 月 28 日提交;最初宣布 2018 年 4 月。

评论:34 页，提交给嵌入式计算系统 (tecs) 上的交易

类:C.1 。3

335. **第 xiv:1804. 0004[pdf] Cs。直流**

动态设备协调服务的协调逻辑描述与执行研究

作者:yoki yamato, naoto hoshikawa, hirofumi noguchi, tatsuya demizu, misao kataoka

摘要: 最近,**物联网**技术取得了进展，许多设备都连接到了网络。此前,**物联网**服务是通过垂直集成风格开发的。但现在开放**物联网**的概念已经引起了人们的关注，通过集成水平分离的设备和服务来实现各种**物联网**服务。对于开放**物联网**时代，我们提出了隐性计算技术，以发现具有必要数据的设备，供用户按需使用，并动态使用它们。尽管隐性计算可以根据情况发现和使用该设备，但在协调多个设备时，对协调逻辑描述的研究是不够的。本文研究了协调逻辑描述和执行对多台设备的动态协调。我们将抽象描述转换为执行时的特定接口访问手段的方法与思想进行了比较，研究了优缺点，并提出了相应的方法。少

2018 年 3 月 23 日提交;最初宣布 2018 年 4 月。

评论:2 页，日文, 2018 年 ieice 大会, bs-4-1, 2018 年 3 月

日记本参考:2018 年 ieice 大会, bs-4-1, 2018 年 3 月。(c) 2018 年 ieice

336. **第 xiv:18004.0023[pdf,其他] Cs。直流**

超驱动器: 用于 mw 物联网端节点的系统可扩展的双重 cnn 推理引擎

作者:renzo andri, lukas cavigelli, davde rossi, luca benini

摘要: 深部神经网络在计算机视觉和机器学习方面取得了令人印象深刻的成果。不幸的是，最先进的网络是非常计算和内存密集型的，这使得它们不适合于 mw 设备，如物联网终端节点。这些网络的积极量化极大地减少了计算和内存占用。二值神经网络 (bwn) 遵循这一趋势，将权重量化推向极限。到目前为止介绍的 bwn 硬件加速器专注于核心效率，而忽略了 ito 带宽和系统级效率，而这些对于在超低功耗设备中部署加速器至关重要。我们提出了 hyperdrive: bwn 加速器极大地减少了 ito 带宽，利用了一种新的二值流媒体方法，并能够通过其系统可扩展的体系结构处理高分辨率图像。我们实现了 5.9 tops/w 系统级效率 (即包括 ito)----比最先进的 bnn 加速器高 2.2 倍，即使我们的核心使用资源密集型 fp16 算法来提高鲁棒性。少

2018 年 6 月 13 日提交;v1 于 2018 年 3 月 5 日提交;最初宣布 2018 年 4 月。

337. 第 xiv:18004.00524[pdf, ps,其他] Cs。镍

上下文中的位置数据质量: 方向和挑战

作者:maria luisa damiani

摘要: 在过去的十年里，随着移动应用领域的出现，位置信息的意义发生了根本的变化。如今，位置数据不仅是地理空间数据库的关键组成部分，也是广泛应用 (包括基于位置的服务和物联网解决方案) 的关键资源。由于本地化技术的可用性，可以实时提供关于移动实体的准确可靠的位置信息，从而实现了这一视角的转变。我们将实时定位称为定位数据。定位数据具有独特的特点，如本地化技术和环境环境的强烈依赖性，使标准质量指标和质量评估程序的规范成为一项复杂的任务。本文阐述了这一方面，特别侧重于室内定位数据。少

2018 年 3 月 27 日提交;最初宣布 2018 年 4 月。

338. 第 xiv:18004.00503[pdf, ps,其他] Cs。镍

解码叠加的 lora 信号

作者:nancy el rachkidy,亚历山大 guitton, megumi kaneko

摘要: 远程低功耗无线通信 (如 lora) 可用于许多物联网和环境监测应用。它们通常会将通信范围增加到几公里，代价是将比特率降低到每秒几位。冲突进一步降低了这些通信的性能。本文提出了两种对碰撞信号进行解码的算法: 一种算法要求发射机稍微去同步，另一种算法要求发射机同步。为此，我们使用计时信息将正确的符号与正确的发射器匹配。我们表明，我们的算法能够显著提高 lora 的整体吞吐量。少

2018 年 3 月 21 日提交;最初宣布 2018 年 4 月。

339. 第 xiv:18004.0002[pdf] Cs。镍

商用航空应用物联网的高效透明空气湍流避免算法

作者:amlan chatterjee, hugo flores, bin tang, ashish mani, khondker s. hasan

摘要: 随着过去几十年商业航空的发展，有许多应用旨在提高飞行作业的效率以及安全和安保。其中一些应用是根据从航班上收集的数据提出的;数据通常是从飞机上可用的各种传感器获得的。飞机上的电气和电子设备中有许多传感器，其中大多数对飞机的正常运行至关重要。由于传感器在飞机移动的整个过程中都在运行，每次飞行都会收集大量数据。通常情况下，收集到的大部分数据都存储在飞机上的存储设备上，并在以后进行现场分析和研究，以便进行研究，重点是改善航空公司的运营和有效地维护相同的数据。在某些情况下，当飞行过程中有数据传输时，是在飞机和作为基站的空中交通

管制 (atc) 塔之间。配备了所有这些传感器的飞机，可以收集和交换数据，形成了物联网 (**iot**) 的框架。探测和避免飞机任何形式的湍流至关重要;它增加了乘客和飞机的安全，同时降低了航空公司的运营成本。因此，本文在飞机**物联网**框架的基础上，研究了探测和避免透明空气湍流 (cat) 的技术，这是一种特殊类型的湍流。我们提出的算法考虑到飞机之间在特定区域内的直接和间接通信。通过仿真结果，我们发现，我们提出的利用**物联网**框架进行直接通信的技术比传统的通过单 atc 塔和多个 atc 塔进行无线通信的技术要快。少

2018 年 3 月 18 日提交;最初宣布 2018 年 4 月。

340. **决议: 1804. 00229[pdf,其他] Cs。Hc**

vr 中的多传感器提示能否帮助公民科学家训练模式识别?

作者:阿丽娜·斯特林纳

摘要: 随着物**联网 (iot**) 集成了物理和数字技术，多感官媒体 (mulsemedia) 的设计变得更加容易实现。多感官设计技术具有提高虚拟真实感、扩展处理信息能力以及更轻松地在物理和数字环境之间传输知识的能力。hci 研究人员开始探索将多媒体集成到虚拟体验中的可行性，但研究尚未考虑多媒体是否真正增强了现实主义、沉浸性和知识转移。我开发了 streambed，这是一个 vr 培训平台，用于培训公民科学水监测员，计划考虑多人在浸入和学习目标中的作用。关于多人在学习环境中的作用的未来发现将有可能使学习者能够体验、连接、学习那些不可能亲身体验的空间。少

2018 年 3 月 31 日提交;最初宣布 2018 年 4 月。

341. **第 1804. 00086[pdf,其他] Cs。铬**

hcap: 基于历史的物联网设备能力体系

作者:llakshya tandon, phillip w. l. fong, reihaneh Safavi-Naini

摘要: 在物联网 (**iot**) 应用中，权限非常敏感，因为**物联网**设备会收集我们的个人数据并控制我们环境的安全。为了实现最小权限原则，应对权限使用施加进一步的限制，而不是简单地授予权限。由于**物联网**设备是物理嵌入的，因此通常会根据它们的相对物理位置按特定的顺序访问它们。通过监视**在访问物联网**设备时是否遵守了此类排序约束，可以避免恶意访问。本文提出了一种基于历史的能力系统 hcap，用于在分布式授权环境中强制实施权限排序约束。我们正式建立 hcap 的安全保障，并对其性能进行实证评估。少

2018 年 3 月 30 日提交;最初宣布 2018 年 4 月。

342. **第 1803.1157[pdf] cs. cy**

了解信息体系结构和业务模型之间的关系

作者:张楠,赵学娇,何晓培

摘要:基于 k 局和 janssen (2011 年) 对信息体系结构和商业模式的二元论，提出了理解**物联网**与智能社区之间关系的理论框架。作为一个配置集的智能社区开发，包括信息体系结构因素和业务模型模式。

2018 年 3 月 21 日提交;最初宣布 2018 年 3 月。

343. **第 1803. 10930[pdf,其他] Cs。简历**

b-dcgan: fpga 二值 dcgan 的评价

作者:hido terada, hayaru shouno

摘要: 我们正在尝试在边缘计算环境中为物**联网**(iot)、fintech 等实际应用实施深度神经网络，以利用深度学习在最近取得的重大成就年。特别是，我们现在把算法的实现集中在 fpga 上，因为 fpga 是低成本、低功耗计算机实现的有前途的设备之一。在这项工作中，我们介绍了二进制 dcgan (b-dcgan)-深卷甘模型与二元权重和激活，并使用整数值操作的正向传递 (培训时间和运行时)。并展示了如何在 fpga (xilinx zynq) 上实现 b-dcgan。利用 b-dcgan，对 fpga 的特性和深度学习性能进行了可行性研究。由于二值化和使用整数值运算降低了内存容量和电路门的数量，对 fpga 的实现是非常有效的。另一方面，这些减少将降低模型生成数据的质量。因此，我们调查这些削减的影响。少

2018 年 3 月 29 日提交;最初宣布 2018 年 3 月。

评论:10 页

msc 类: 00a99

344. **第 xiv:1803.10147[pdf,其他] Cs。铬**

多伊 10.114/3139937.3139939

消费类物联网医疗设备中的数据传输

作者:daniel wood, noah apthorpe, nick feamster

文摘: 本文介绍了一种从医疗**物联网**设备中捕获网络流量并自动检测可揭示敏感医疗条件和行为的明文信息的方法。这项研究遵循的是包括交通收集、明文检测和元数据分析的三步方法。我们分析了四种流行的消费**医疗物联网**设备，包括一台智能医疗设备，该设备以明文形式泄漏敏感的健康信息。我们还提供了一个流量捕获和分析系统，该系统与家庭网络无缝集成，并为消费者提供了一个用户友好的界面，以监控和可视化**其**家中物联网设备的数据传输。少

2018 年 3 月 27 日提交;最初宣布 2018 年 3 月。

评论:6 页, 5 个数字

日记本参考:2017 年物联网安全与隐私研讨会论文集 (iots & amp; p ' 17)

345. **第 xiv:1803. 09710[pdf,其他] Cs。铬**

针对资源受限的系统和物联网的安全、可靠的生物识别访问控制

作者:nima karimian, Karimian guo, Fatemeh Tehranipoor, damon woodard, mark Tehranipoor, Domenic forte

摘要: 随着物联网 (**iot**) 的出现，对低功耗、普及设备的访问控制和数据保护的需求日益增加。基于生物特征的身份验证由于其方便的性质和较低的攻击易感性，在物**联网**上很有前途。但是，与生物识别处理和模板保护相关的成本对于智能卡、密钥 fobs 等来说是不重要的。本文讨论了生物识别系统的安全性、成本和实用性，并开发了两个主要的改进框架。首先，我们引入了一个新的框架，用于实现基于物理不克隆函数 (puf) 和硬件混淆的生物识别系统，与传统的软件方法不同，该框架不需要生物特征的非易失性存储。除了降低影响生物识别的风险外，模糊处理的性质还提供保护，防止通过恶意软件和故障注入规避访问控制。puf 提供非可逆性和不可链接性。其次，提出的 puf/模糊处理方法的一个主要要求是从用户输入生物识别生成可靠 (可靠) 的密钥。我们提出了一个噪声感知生物识别量化框架，能够生成独特的，可靠的关键与减少注册时间和去噪成本。最后，我们进行了几个案例研究。在第一种方法中，将拟议的噪声感知方法与我们以前的多种生物识别方法进行了比较，包括流行的生物识别方法 (指纹和虹膜) 和新兴的心血管方法 (心电图和 ppg)。结果表明，心电图在可靠性、密钥长度、熵

和成本之间提供了最佳的权衡。在第二个和第三个案例研究中，我们演示了如何通过对心电图的主题内部变化进行建模来提高可靠性、去噪成本和注册时间。少

2018 年 3 月 26 日提交;最初宣布 2018 年 3 月。

评论:11 页, 9 个数字

346. 第 xiv:1803.09156[pdf, ps,其他] Cs。铬

语音控制系统的漏洞概述

作者:袁公,克里斯蒂安·波拉鲍尔

摘要: 在过去几年中，越来越多的物联网 (**iot**) 系统采用语音作为主要用户输入。事实证明，这些系统容易受到各种类型的语音欺骗攻击。然而，这些技术究竟是如何相互区分或相互关联的，目前还没有得到广泛的研究。本文对语音控制系统的最新攻击和防御技术进行了综述，并对这些技术进行了分类。我们还讨论了普遍防御战略的必要性，以保护一个系统免受各种类型的攻击。少

2018 年 3 月 24 日提交;最初宣布 2018 年 3 月。

评论:第一届物联网安全和隐私国际讲习班 (iotsec)

347. 第 1803.086007[pdf,其他] Cs。简历

一种面向移动网的多量无关可分离卷积

作者:陶生,陈峰,卓兆，张小鹏,梁申,米奇·阿列克西奇

摘要: 随着深度学习 (dl) 被迅速推向边缘计算，研究人员发明了各种方法，以便在移动/**物联网**设备上更有效地进行推理计算，如网络修剪、参数压缩等。量化作为关键的方法之一，可以有效地卸载 gpu，使 dl 在定点管道上的部署成为可能。不幸的是，并非所有现有的网络设计都对量化友好。例如，流行的轻量级 mobiletenv1 虽然通过可分离卷积成功地减小了参数大小和计算延迟，但实验表明，它的量子化模型与浮点模型相比具有较大的精度差距。为了解决这个问题，我们分析了量化损失的根本原因，并提出了一个量子友好的可分离卷积体系结构。通过评估 imagenet2012 数据集上的图像分类任务，我们改进的 mobiletev1 模型可以将 8 位推理前 1 名精度存档到 68.03%，几乎缩小了与浮点管道的差距。少

2018 年 3 月 22 日提交;最初宣布 2018 年 3 月。

评论:在第 1 届能源效率机械学习和嵌入式应用的识别计算机工作室接受 (emc2)

348. 第 xiv:1803.08179[pdf] Cs。镍

物联网域的协议体系结构

作者:jelena misic, m. zulfiker ali, vojislav b. misic

摘要: 在本文中，我们讨论了将运行 coap 的 **iot** 域与其他 internet (包括微数据中心) 和构建可扩展层次结构的其他域互连的代理体系结构。我们假设 coap 域是由带有缓存的 **iot** 代理终止的，我们研究了与成功数据传输、往返延迟和能耗有关的几个设计问题。当代理自主维护数据新鲜度时，我们会为这种情况提供性能数据，这清楚地表明了高效的设计选择。少

2018 年 3 月 21 日提交;最初宣布 2018 年 3 月。

349. 第 1803.08104[pdf, ps,其他] Cs。镍

随机通道增益下 rf-收集传感器节点采样时间最大化的研究

作者:杨长林,陈光武,刘英

摘要: 将来，传感器节点或物联网 (**iot**) 将负责对环境进行采样。这些 nodes/设备可能由混合接入点 (hap) 无线供电，并且可能由 hap 编程，并有 {\em 采样时间}，以收集感官数据、进行计算并将感知数据传输到 hap。然而，一个关键的挑战是随机信道增益，这导致传感器节点接收不同数量的射频 (rf) 能量。为此，我们制定了一个随机程序，以确定 hap 的充电时间和传感器节点的采样时间。我们的目标是最大限度地减少传感器节点出现能量不足时的预期罚款。我们考虑两种情况: {\em 单} 和 {\em 多} 时隙。在前者中，我们在逐槽的基础上确定合适的 hap 充电时间和节点采样时间，而后者则考虑下一个插槽中使用的最佳充电和采样时间 t 插槽。我们对从高斯、瑞利或瑞斯分布中提取的信道增益进行实验。数值结果证实，我们的随机程序可用于计算良好的充电和采样时间，从而在上述分布上产生最小的惩罚。少

2018 年 3 月 21 日提交;最初宣布 2018 年 3 月。

评论:2018 年加入 ieee 国际商会

350. **第: 1803. 07842[pdf,其他] Cs。镍**

关键任务 unb-iot 系统频谱预留的最佳动态契约

作者:muhammad junaid farooq, quanyan zhu

摘要: 频谱保留正在成为一种潜在的解决方案，以满足大量具有可靠性限制的无线物联网 (**iot**) 设备的通信需求，尤其是在关键任务方案中。在大多数关键任务系统中，保留的真正效用可能不会提前完全知道，因为不可预见的事件可能无法完全预测。本文提出了一种动态合同方法，即在预订时根据有关频谱预订效用的部分信息进行预付款。一旦获得完整的信息，如果预订被释放，将对付款进行回扣。本文提出了一种合同理论方法，用于设计一种激励机制，该机制强制应用程序揭示其真实的应用类型，从而提高**物联网**网络运营商的盈利能力。运营商在不了解应用程序类型的情况下，提供了一系列合同，这些合同向**物联网**应用程序提供了高级付款和回扣。申请选择合同的决定，导致其真实类型向经营者披露，使其能够产生比传统频谱拍卖机制更高的利润。在对应用效用分布的一些假设下，给出了最优动态频谱保留契约的闭合形式解，并分析了对系统参数的敏感性。少

2018 年 3 月 21 日提交;最初宣布 2018 年 3 月。

期刊参考:第十六届移动、特设和无线网络建模与优化国际研讨会 (wiopt 2018)

351. **第 xiv: 1803.07760[pdf,其他] Cs。铬**

物联网的一种负责任的匿名数据聚合方案

作者:吴龙飞,杜晓江,吴杰,刘景伟,爱德华·德拉古特

摘要: 物联网 (**iot**) 在人们的日常生活中越来越流行。为了更好地为用户服务，我们鼓励普及的物联网设备相互共享数据。但是，出于隐私考虑，用户不愿意共享敏感数据。本文研究**了物联网**系统的匿名数据聚合问题，其中**物联网**公司服务器虽然不完全可信，但却被用来辅助聚合。我们提出了一个高效和负责任的聚合方案，可以保持数据的匿名性。分析了该方案的通信和计算开销，并通过大量仿真对总执行时间和每个用户的通信开销进行了评估。结果表明，我们的方案比以前的对等洗牌协议更有效，特别是对于来自多个提供程序的数据聚合。少

2018 年 6 月 30 日提交;v1 于 2018 年 3 月 21 日提交;最初宣布 2018 年 3 月。

352. **建议: 1803. 07310[pdf,其他] Cs。镍**

多伊 10.1109/MVT.2015.2508320

cttc 5g 端到端实验平台: 集成异构有线网络、分布式云和物联网设备

作者:raul muñz, josep mangues, ricard vilalta, christos verikoukis , jesús alonso-zaratt, nikolaos bartzoudis , Apostolos gearadis, miquel payaró, anapérez-neira, ramon casellas, ricardo martínez , josénúñez-martínez, manuelrequena-esteso, david pubill , oriol Font-Bach, pol henarejos, jordi serra, francisco vazquez-gallgoo

摘要: 物联网 (**iot**) 将促进不同领域的各种应用，如智能城市、智能电网、工业自动化 (工业 4.0)、智能驾驶、老年人援助和家庭自动化。具有不同应用程序要求的数十亿异构智能设备将连接到网络，并将生成将在分布式云基础架构中处理的大量数据。另一方面，在云基础架构中 (例如，网络功能虚拟化 (nfv) 或移动边缘计算 (mec)] 中将功能部署为软件 (sw) 实例也有普遍趋势。因此，下一代移动网络，第五代 (5g)，不仅需要开发新的无线电接口或波形，以应对预期的流量增长，而且还需要将异构网络从端到端 (e2e) 与分布式集成云资源，以提供 e2e **物联网**和移动服务。本文介绍了由加泰罗尼亚电信中心 (cttc) 开发的 e2e 5g 平台，该平台是第一个能够重现这种雄心勃勃的场景的已知平台。少

2018 年 3 月 20 日提交;最初宣布 2018 年 3 月。

353. **修订: 18006854[pdf, ps,其他] Cs。镍**

汉堡的 monica: 在智慧城市中实现大规模物联网部署

作者:sebastian me 玲, dorothea purnomo , ji 怀 a-ann shiraishi, michael fischer, thomas c. schmidt

摘要: 21 世纪，世界各地的现代城市和大都市地区面临着新的管理挑战，主要原因是城市人口对生活水平的要求不断增加。这些挑战包括气候变化、污染、交通和公民参与，以及城市规划和安全威胁。智慧城市的首要目标是通过现代信息和通信技术来抵消这些问题并减轻其影响，以改善城市管理和基础设施。关键的想法是利用网络通信与相互联系的公共当局;同时还可以在整个城市基础设施中部署和集成众多传感器和执行器--这也被广泛称为物联网 (**iot**)。因此,**物联网**技术将成为实现智慧城市愿景的许多目标的重要组成部分和关键推动因素。本文的贡献如下。我们首先研究了许多有助于营造智慧城市环境的**物联网**平台、技术和网络标准。其次，我们介绍了欧盟项目 monica，该项目旨在在公共、城市内部活动中演示大规模**物联网**部署，并概述其**物联网**平台架构。第三，我们提供了汉堡市有关 smartcity 活动的案例研究报告，并就最近 (正在进行的) 垂直集成的端到端物**联网**传感器应用的现场测试提供见解。少

2018 年 5 月 15 日提交;v1 于 2018 年 3 月 19 日提交;最初宣布 2018 年 3 月。

评论:6 页

日记本参考:欧洲网络与通信会议论文集, eucnc, 2018

354. **第 xiv: 18006534[pdf, ps,其他] Cs。镍**

不完全扩散因子正交性的环压吞吐量分析

作者:antoine waret, megumi kaneko,亚历山大 guitton, nancy el rachkidy

摘要: lora 是为未来的物联网 (**iot**) 设备启用低功耗广域网 (lpwan) 的技术之一。尽管 lora 允许灵活地调整覆盖范围和数据速率，但它受固有类型的干扰的影响: 在具有相同传播因子 (sf) 的终端设备发生碰撞的情况下，共同 sf 干扰发生冲突，而 sf 间干扰在具有不同 sf 的终端设备会发生碰撞。目前的大多数作品都认为不同的 sf 之间是完美的正交性。在这项工作中，我们提供了上行链路中可实现的 lora 吞吐量的理论分析，其中包括特定于 lora 的捕获条件。结果表明，在不同的 sf 分配下，我们的分析是

准确的，而在不同的 sf 分配下，sf 正交性不完全的影响下，我们的吞吐量损失是准确的。我们的分析将能够设计特定的 sf 分配机制，以进一步增强吞吐量。少

2018 年 3 月 17 日提交;最初宣布 2018 年 3 月。

355. xiv:1803 06494[pdf,其他] Cs。铬

伊莎贝尔的攻击树

作者:florian kammüller

摘要: 本文提出了攻击树的证明理论。攻击树是构建对系统的攻击的一个成熟且有用的模型，因为它们允许在应用程序方案中逐步探索高级攻击。利用 isabelle 高阶逻辑的表现力，我们成功地开发了一种基于 kripke 结构和 ctl 的基于状态的基于状态的攻击树的通用理论。由此产生的框架允许机械支持的逻辑分析的元理论的攻击树的证明演算，同时开发的证明理论使应用到案例研究。在 isabelle 中证明了一个中心正确性和完整性结果，它在攻击树有效性的概念和 ctl 之间建立了联系。通过医疗保健**物联网**系统和 gdpr 合规性验证的实例说明了该应用。少

2018 年 5 月 15 日提交;v1 于 2018 年 3 月 17 日提交;最初宣布 2018 年 3 月。

356. 第 xiv:180006059[pdf, ps,其他] Cs。镍

分布式缓存支持 v2x 网络：建议、研究趋势和挑战问题

作者:张迪

摘要: 如今，车辆互联网 (iov) 已经发展成为车辆到一切 (v2x) 的舞台。然而，现有的大部分工作都集中在机动车上。相反，共享自行车系统被大大和快速地部署为一个可行的物联网 (**iot**) 应用场景的最后英里的问题 (例如，从车站到家庭办公室)。此外，目前 v2x 的互联网接入还依赖于回调到路边单元 (rsu) 的连接。本文除前期工作外，还提出了一种具有分布式框架和异构缓存方法的多功能 v2x 系统。所有道路上的车辆和装置 (机动车、非机动车、行人等) 都被全面纳入拟议的网络。进一步介绍了一种利用海量连接设备实现有效无线传输的异构缓存方法。重点介绍了实现高速传输、深度编程专用网络切片的潜在研究趋势以及大数据、机器学习 (ml)、基于雾计算的图像识别和重建，为实现实现高速传输、深度编程专用网络切片提供了一些见解。未来的研究。最后讨论了城市街道峡谷路径丢失和信道模型、超可靠通信和低延迟要求等具有挑战性的问题。少

2018 年 7 月 16 日提交;v1 于 2018 年 3 月 15 日提交;最初宣布 2018 年 3 月。

357. 第 xiv:18005788[pdf,其他] Cs。简历

深 n-jpg：一种基于 jpeg 的深度神经网络支持的图像压缩框架

作者:刘子浩,刘涛,文武杰,江磊,徐杰, 王燕志, 刚全

摘要: 深度神经网络 (dnn) 作为最引人入胜的机器学习技术之一，在图像分类等各种智能任务中表现出了优异的性能。dnn 在很大程度上通过对大量培训数据执行昂贵的培训来实现此类性能。为了减少智能资源有限的 internet (**iot**) 系统中的数据存储和传输开销，在传输实时生成的数据集进行培训或分类之前，有效的数据压缩是 "必备条件" 功能。虽然有许多众所周知的图像压缩方法 (如 jpeg)，但我们首次发现，基于人工视觉的图像压缩方法 (如 jpeg 压缩) 并不是 dnn 系统的优化解决方案，尤其是在高压缩比。为此，我们开发了一个为 dnn 应用程序量身定制的图像压缩框架，名为 "deepn-jpg"，以包含 dnn 体系结构的深层级联信息处理机制的本质。基于具有各种最先进 dnn 的 "imagenet" 数据集的广泛实验表明，"deepn-jpeg" 可以比流行的

jpeg 解决方案实现 ~ 3.5 倍的压缩率，同时保持相同的图像识别精度水平,在基于 dnn 的智能**物联网**系统设计中展示了其巨大的存储和能效潜力。少

2018 年 3 月 13 日提交;最初宣布 2018 年 3 月。

评论:第 55 届设计自动化大会 (dac2018)

358. 第 xiv:18005368[pdf,其他] Cs。镍

家庭物联网网络流量与行为分析

作者:yousef amar, hamed haddadi, richard mortier, anthony brown, james colley, andy crabtree

摘要: 互联网连接设备越来越多地存在于我们的家中，侵犯隐私、数据泄露和安全威胁正变得越来越普遍。为了避免这些，我们必须首先了解这些设备的行为。在这项工作中，我们分析了来自常见**物联网**设备测试平台的网络跟踪，并描述了对其行为进行指纹识别的一般方法。然后，我们使用从这些数据中获得的信息和见解来评估隐私和安全风险在哪里表现出来，以及设备行为如何影响带宽。我们演示了一些简单的措施，以规避保护设备和保护隐私的尝试。少

2018 年 3 月 14 日提交;最初宣布 2018 年 3 月。

评论:提交给 2018 年 tma

359. 第 1803. 05109[pdf,其他] cs. ne

pt-spike: 一种具有高效监督学习的精确时间依赖的单尖刺神经形态体系结构

作者:刘涛,江磊,金一儿,刚泉,温武杰

摘要: 在过去十年中，人工智能最令人兴奋的进步之一是在许多现实世界的应用中广泛采用了事实上的起，例如 dnn 和 cnn。然而，潜在的大量计算和存储需求极大地挑战了它们在无人机、移动电话和**物联网**设备等资源有限平台上的适用性。第三代神经网络模型--尖峰神经网络 (snn)，受人脑工作机制和效率的启发，已成为在轻量化范围内实现更令人印象深刻的计算和能效的一个有希望的解决方案设备 (如单芯片)。然而，为了完成实际认知任务，低估了 snn 的能源效率、吞吐量和系统灵活性，对传统的基于速率的尖峰系统设计进行了严格的相关研究活动。尽管基于时间的 snn 在概念上更有吸引力，但由于缺乏高效的编码和实际学习方案，其潜力并没有在实际应用中发挥出来。在这项工作中，开发了一个精确时间相关的单尖点神经形态结构，即 "pt-sppike"，以弥补这一差距。相应地提出了三种易于使用的硬件技术: 精确的单尖峰时间编码、高效的监督时间学习和快速的非对称解码，以提高其能源效率和数据处理能力。在执行实际认知任务时，以更紧凑的神经网络模型大小建立基于时间的 snn。仿真结果表明，与基于速率的 snn 和 ann 相比，"pt-sprake" 在网络尺寸、处理效率和功耗方面有显著改善，并在类似情况下的基于速率的 snn 和 ann 进行了边际分类精度的降低。网络配置。少

2018 年 3 月 13 日提交;最初宣布 2018 年 3 月。

评论:第二十三届亚洲及南太平洋设计自动化大会 (asp-dac 2018)

360. 第 xiv:18005022[pdf,其他] Cs。铬

多伊 10.1109/JIOT.2018.2846040

在机器学习和软件定义的网络时代保护物联网

作者:francesco restuccia, salvatore d ' oro, tommaso melodia

摘要: 物联网 (**iot**) 实现了一个愿景，即从我们的身体内部到全球最偏远的地区，几乎到处都有数十亿的互联设备。由于**物联网**很快就会渗透到我们生活的方方面面，并且可以从任何地方访问，因此，解决关键**的物联网**安全威胁现在比以往任何时候都更加重要。将安全性作为事后考虑和针对已知攻击的 "修补程序" 应用的传统方法是不够的。事实上，下一代**物联网**挑战将需要一个新的逐个设计的安全愿景，在这个愿景中，我们可以主动应对威胁,**并让物联网**设备学会动态地适应不同的威胁。为此，机器学习和软件定义的网络将是**为物联网**设备提供可重构性和智能化的关键。在本文中，我们首先提供了一个分类**和**调查物联网安全研究的最新技术，并提供了一个与机器学习和软件定义网络的应用有关的具体研究挑战的路线图，以解决现有的和下一代**物联网**安全威胁。少

2018 年 6 月 11 日提交;v1 于 2018 年 3 月 13 日提交;最初宣布 2018 年 3 月。

评论:ieee 物联网杂志, 2018

361. 第 xiv:18004780[pdf,其他] Cs。直流

多伊 10.4204/EPTCS.264。1

物联网架构框架: 物联网系统的连接和集成框架

作者:onoriode uviase, gerald kotonya

摘要: 此后，物**联网 (iot**) 的普及使人们对建筑设计和自适应框架产生了越来越大的兴趣，以促进异构**物联网**设备和**物联网**系统之间的连接。**物联网**中最受欢迎的软件体系结构是面向服务的体系结构 (soa)，其目的是提供一个松散耦合的系统，以利用中间件层物联网服务的使用和重用,最大限度地减少系统集成问题。然而，尽管 soa 提供了灵活性,**但在物联网**系统中集成、扩展和确保恢复能力的挑战依然存在。**物联网**系统集成不良的主要原因之一是缺乏智能、易于连接的框架来支持**物联网**系统中的交互。本文回顾了用于集成**物联网**设备的现有体系结构框架，并确定了需要进一步研究改进的关键领域。最后，本文提出了一种基于微服务的可能解决方案。拟议的**物联网**集成框架受益于智能 api 层，该层采用外部服务汇编程序、服务审核员、服务监视器和服务路由器组件来协调服务发布、订阅、解耦体系结构中的服务组合。少

2018 年 2 月 5 日提交;最初宣布 2018 年 3 月。

评论:2017 年 ALP4IoT 联网, arxiv:1802. 00976

类:物联网

日记本参考:eptcs 264, 2018, 第 1-17 页

362. 第 xiv:18004453[pdf] Cs。镍

多伊 10.10077/978-3-319-7495-8 _ 22

物联网中设备监控的隐私方案

作者:zygmunt j. haas , ashkan yousefpour

摘要: 足够强大的安全和隐私机制是积累物联网技术的良好优势并将其融入**我们**日常生活的先决条件。本文介绍了一种新的网络隐理方法 ，该方法特别符合**物联网**的特点。我们的一般方法是基于不断更改**物联网**节点的识别属性。特别是，本文中提出的方案是基于更改**物联网**节点的 ip 地址，而且由于非预期观察者认为 ip 地址的变化模式看起来是随机的，因此对手无法识别源或目的地一个特定的传输。因此，承载由特定节点生成的信息的数据包不能链接在一起。该方案提供了额外的安全优势，包括 dos 缓解，相对容易实现，并且不需要对现有的网络基础结构进行任何更改。我们讨论了该方案实施的细节，并对其性能进行了评价。少

2018 年 3 月 12 日提交;最初宣布 2018 年 3 月。

评论:出现在 2016 年 fallouus 会议 (第二届 eai 关于无处不在和智能基础设施的未来接入能力国际会议上)

日记本参考:《普适计算心理健康范式》, 153-165 页。斯普伦格, 查姆, 2016

363. 第 18003807[pdf,其他] cs. cy

ciota: 通过区块链进行协同物联网异常检测

作者:tomer golomb, yisroel mirsky, yuval elovici

摘要: 由于物联网 (**iot**) 设备的快速增长和部署, 已成为我们日常生活的一个核心方面。但是, 它们往往有许多漏洞, 攻击者可以利用这些漏洞。无监督技术 (如异常检测) 可以帮助我们保护**物联网**设备的安全。但是, 必须对异常检测模型进行长时间的训练, 才能捕获所有良性行为。这种方法容易受到对抗攻击, 因为所有观测都被认为是良性的, 同时训练异常检测模型。本文提出了 ciota, 它是一个轻量级的框架, 它利用区块链概念对资源有限的设备执行分布式和协作异常检测。ciota 使用区块链, 通过自**认证和物联网**设备之间的共识, 逐步更新受信任的异常检测模型。我们在自己的分布式**物联网**仿真平台上对 ciota 进行评估, 该平台由 48 个树莓派组成, 以展示 ciota 增强每个设备的安全性和整个网络的安全性。少

2018 年 4 月 9 日提交;v1 于 2018 年 3 月 10 日提交;最初宣布 2018 年 3 月。

评论:参加 2018 年网络和分布式系统安全研讨会 (ndss) 的分散物联网安全与标准 (diss) 研讨会

364. 第 18003525[pdf,其他] cse

使用链接数据和基于 mqtt 的数据仓库改进集成工具链中的生命周期查询

作者:andrii berezovskyi, jad El-khoury, omar kacimi, frédéric loiret

摘要: 日益复杂的**物联网**系统的开发需要庞大的工程环境。这些环境通常由来自不同供应商的工具组成, 并且不一定彼此很好地集成。为了自动执行各种分析, 来自多个工具的跨资源的查询必须与工程活动并行执行。在本文中, 我们确定了对这种查询功能的必要要求, 并根据这些要求对不同的体系结构进行了评估。我们提出了一个改进的生命周期查询体系结构, 该体系结构建立在现有的跟踪资源集 (trs) 协议的基础上, 并与 mqtt 消息传递协议相结合, 以便使仓库中的数据能够实时更新。作为以开发**物联网**自动化仓库为重点的案例研究的一部分, 此体系结构是为使用 restful 微服务和链接数据集成的工具链实现的。少

2018 年 3 月 9 日提交;最初宣布 2018 年 3 月。

评论:12 页, 研讨会

365. 第 18003444[pdf,其他] Cs。直流

一种适应性自然启发的雾建筑

作者:dragi kimovski, humaira ijaz, nisant surabh, radu prodan

摘要: 在过去十年中, 云计算通过在互联网上提供低成本的计算和存储资源, 有效地利用了规模经济, 最终将计算资源整合到大型数据中心。然而, 高度分散的物联网 (**iot**) 技术的起步, 无法有效地利用集中式云基础架构, 将计算推向了资源分散。雾计算通过在网络边缘的计算和存储资源分散到数据生成的位置附近, 扩展了云范式。从本质上讲, 雾计算促进了物理上靠近边缘设备的有限计算、存储和网络资源的运行。然而, 由于 fog 的共同复杂性以及最近的**物联网**趋势对部署和连接非常大的无处不在的设备和传

感器的影响，需要探索自适应的 fog 体系结构方法能够适应和扩展，以应对分布式**物联网**应用程序不可预知的负载模式。本文介绍了一种具有前景的新的自然启发的雾体系结构，名为 smartogh，能够提供低决策延迟和自适应资源管理。利用多标准决策、图论和机器学习等领域的新算法和技术，将雾作为分布式智能处理系统，从而模拟人脑的功能。少

2018 年 3 月 9 日提交;最初宣布 2018 年 3 月。

366. **xiv:1803.03190[pdf] Cs。直流**

动态物联网编排--管理发现、分发、失败和重新配置

作者:jan seeger, rohit a. deshmukh, arne bröring

摘要: ..... 事物正在以惊人的速度增长，并扩展到各种应用领域。我们使用**物联网**概念设计、实施和评估了一个弹性和分散的系统。我们将其应用于维护楼宇自动化系统的功能，使新设备能够实时出现和消失。

2018 年 3 月 22 日提交;v1 于 2018 年 3 月 8 日提交;最初宣布 2018 年 3 月。

评论:提交给 ieee 普适计算的特刊 "物联网通信". v2: 修正了一些拼写错误 v2: 扩展评估部分、改进的图表、小文本改进

367. **第 xiv:18003058[pdf,其他] cse**

多伊 10.10077/978-3-319-77243-1 _ 2

物联网开发公司如何处理用户体验要求的探索性研究

作者:johnna bergman, thomas olsson, isabelle johansson , kirsten Rassmus-Gröhn

摘要: [背景和动机]物联网 (**iot**) 在日常生活中越来越普遍。但是，交互通常不同于使用计算机和其他智能设备时。此外,**物联网**设备通常依赖于其他几个系统，严重影响用户体验 (ux)。最后，该领域正在迅速变化，并受到技术创新的推动。[问题/问题]在本定性研究中，我们探讨了企业如何在**物联网**环境中获得用户体验需求。数据驱动方法也是现代**物联网**发展的一个关键部分。因此，研究中也考虑到了这些问题。[主要理念/结果]围绕数据驱动的方法存在知识差距，有一些公司收集大量数据，但并不总是知道如何利用这些数据的例子。此外，许多公司难以处理更大的系统环境，他们的产品和他们控制的 ux 只是完整**的物联网**生态系统的一部分。[捐款额]我们提供**物联网**发展中公司的定性经验数据。根据我们的发现，我们确定了公司面临的挑战和未来工作的领域。少

2018 年 3 月 8 日提交;最初宣布 2018 年 3 月。

期刊参考:第 24 次国际工作会议，需求工程: 软件质量基金会，荷兰乌得勒支, 2018 年 3 月 19-22 日

368. **第 xiv:180002890[pdf] cse**

挑战: 云与物联网之间的桥梁

作者:mohammad riyaz belgaum, safeeullah soomro, zainab alansari, muhammad alam, shahrulniza musa, mazliham mohd suud

摘要: 在实时处理中，一种新兴的技术提高了通过互联网将智能设备与云连接的需求。**经过处理的物联网**设备将在任何需要的地方存储和访问，并支持强大的计算性能、高效的异构系统存储基础架构和软件，这些系统和软件可配置和控制这些不同的设备。这项新兴技术列出了许多需要应对的挑战，因为它也需要与即将推出的 5g 无线设备兼容。本文展示了这一创新范式的好处和挑战，以及开放进行研究的领域。少

2018 年 2 月 5 日提交;最初宣布 2018 年 3 月。

评论:2017 年电子商务论文集

369. 第 xiv:18002889[pdf] cse

建立基于 mdd 的自适应物联网应用开发框架

作者:yousef abuseta

摘要: 随着技术和通信技术的进步，更多的设备 (和事物) 能够连接到互联网并相互交谈，以实现一个共同的目标，从而导致物联网 (**iot**) 时代的出现。相信**物联网**将带来无限数量的应用和商机，几乎影响我们生活的方方面面。已经进行了研究，以调查阻碍**物联网**实现的挑战，以及为**物联网**的接受和启用铺平道路的有希望的解决方案。对于使**物联网**范式成为可能，非常重要的研究领域之一是存在一个统一的编程框架，该框架掩盖了物联网平台所涉及**设备的**异质性。这样的框架指导系统开发人员**在整个物联网**应用程序开发过程中。本文总体上研究**了物联网**概念及其高级体系结构，并对应用开发方面进行了更多的研究。我们相信，**物联网**应用本质上是高度动态的，因此需要在设计时考虑到自适应和自主的概念。因此，我们提出的**物联网**软件开发生命周期基于 ibm 自主系统的架构蓝图。为了满足**物联网**应用的运行时动态和异质性方面，我们在建议的开发框架中采用了 mdd 范式。我们强调弹性开发框架的核心要求，该框架能够满足成功**的物联网**应用所需的概念和流程。少

2018 年 2 月 11 日提交;最初宣布 2018 年 3 月。

评论:11 页. arxiv 管理说明: 文本与 arxiv:150 8.01330 重叠

日记本参考:国际计算机科学与软件工程杂志 (ijcsse)，第 6 卷，第 11 期, 2017 年 11 月。issn (在线): 2409-4285

370. 第 180002500[pdf,其他] Cs。直流

面向智慧城市实用程序的数据驱动物联网软件体系结构

作者:yogesh simmhan, pushkara ravindra , shilpa chaturvedi, malatihegde , rashmi ballamajalu

摘要: 物联网 (**iot**) 正在成为互联网上数十亿设备的下一个数字存在浪潮。智能城市是**物联网**的实际体现，其目标是通过智能管理，高效、可靠、安全地向居民提供水、电力和交通等城市公用事业。数据驱动**的物联网**软件平台对于实现可管理和可持续的智能实用程序以及在此基础上开发新的应用程序至关重要。在这里，我们提出了这样一个面向服务的软件体系结构，以解决智能实用程序中的两个关键操作活动--用于资源管理的**物联网**结构，以及用于决策的数据和应用程序平台。我们的设计使用开放的 web 标准和不断发展的网络协议、云和边缘资源，以及流式传输的大数据平台。我们使用智能水管理领域来激励我们的设计要求;其中一些要求是发展中国家所独有的。我们还在班加罗尔印度科学学院 (iisc) 的校园规模物联网测试台中验证了该架构，并介绍了我们的经验. 我们的建筑可扩展到乡镇或城市，同时也可推广到其他智能实用程序领域。我们的经验为其他类似工作提供了模板，尤其是在新兴市场，并突出了智能城市数据驱动的**物联网**软件架构的差距和机遇。少

2018 年 3 月 6 日提交;最初宣布 2018 年 3 月。

评论:文章的预打印显示在软件: 实践与经验，威利, 2018

371. 第 xiv:18002288[pdf,其他] cs. it

一种新的大规模 mimo 系统活动检测标度法

作者:saeid hhagaatshoar, peter jung , giuseppe caire

抽象: 在本文中，我们研究了在一个庞大的 mimo 设置中的 \ text 标题 {活动检测} (ad) 问题，在这个设置中，基站 (bs) 具有 m 该 1 天线。我们考虑块衰落通道模型，其中 m-每个用户的暗淡通道向量在包含 Dc 信号尺寸。我们研究的是一个潜在用户的数量 Kc 分配给特定 cb 的规模远远大于 cb 的尺寸。Dc (Kc 该 Dc)，但仅在每个时间段 a 个 c 联合国 Kc 他们都是活跃的。以前的大多数结果，基于压缩传感，要求 a 个 c≤Dc，这是大规模部署方案 (**如物联网 (iot)** 和设备到设备 (d2d) 通信) 中的瓶颈。在本文中，我们证明，当 bs 天线的数量时，我们可以克服这一基本限制。m 是足够大的。更具体地说，我们在参数上推导出一个 \ textin{缩放定律}(m,Dc,Kc,a 个 c)还有具有信噪比的 \ texi{信噪比} (snr)，根据该值，我们的 ad 方案将成功。我们的分析表明，有了尺寸的 cbDc，和足够数量的 bs 天线 m 与 a 个 c/m=不，不，不(1)，可以识别 a 个 c=o(D2c/日志 2(Kca 个 c))活动用户，比以前的绑定大得多 a 个 c=o(Dc)通过传统的压缩传感技术获得。特别是，在我们提出的计划中，只需支付多对数罚款 o(日志 2(Kca 个 c))用于增加潜在用户的数量 Kc，这使得它非常适合**物联网**设置中的 ad。我们提出了 ad 的低复杂度算法，并提供了数值模拟来说明我们的结果。我们还比较了我们提出的 ad 算法与文献中其他竞争算法的性能。少

2018 年 6 月 19 日提交;v1 于 2018 年 3 月 6 日提交;最初宣布 2018 年 3 月。

评论:11 页, 3 图

372. 第 xiv:18002123[pdf,其他] Cs。Sy

在边缘和 5g 以上实现关键任务控制

作者:per skarin, william tärneberg, karl-erik orzen, maria kihl

摘要: 随着工业**物联网**和云计算的出现，以及 5g 和边缘云的出现，人们对下一代 ict 网络中要求苛刻的用例的弹性、规模经济和快速上市时间抱有雄心勃勃的期望。随着边缘云的概念越来越普遍，云中无线通信链路和服务的响应性和可靠性将显著提高。为了实现工业吸收，我们必须在网络中提供云容量，但也必须在软件平台中提供足够的简单性和自我可持续性。本文提出了一个研究试验台，用于研究分布式边缘云的关键任务控制。我们使用传统的控制应用程序以模型预测控制器的形式评估系统属性。我们的云平台提供了持续运行我们的关键任务应用程序的手段，同时在地理位置分散的计算节点之间无缝地重新定位计算。通过使用 5g 无线无线电，我们允许移动性，并可靠地提供低延迟的计算资源，在边缘。本文的主要贡献是最先进的、全面运行的测试台，该测试台展示了融合**物联网**、5g 和云的潜力。我们还在运行关键任务应用程序的同时对该系统进行评估，并提供了新的研究方向展望。少

2018 年 6 月 18 日提交;v1 于 2018 年 3 月 6 日提交;最初宣布 2018 年 3 月。

评论:6 月 18 日: 将提交给 ieee 服务 [edge] 2018 年 5 月 16 日的最终版本 (更新摘要和一些措辞，结果不变)

373. 第 xiv:18002023[pdf, ps,其他] cs. it

累积然后传输: 全双工无线功率物联网系统中的多用户调度

作者:di zhai, hechen, Zihuailin, yonghuili , branka vucetic

摘要: 本文开发并评估了一个用于全双工 (fd) 无线物联网系统中的多用户调度的累积传输框架, 该系统由多个能量采集 (eh)物联网设备 (iod) 和一个 fd 组成。混合接入点 (hap)。所有的 iod 都没有嵌入式能源供应, 因此在将其数据传输到 hap 之前需要执行 eh。由于其 fd 功能, hap 可以同时接收数据上行和广播能量轴承信号下行链路充电 iod。本文整篇认为瞬时信道信息不可用。为了最大限度地提高系统的平均吞吐量, 我们设计了一种新的面向吞吐量的调度方案, 在该方案中, 选择一个具有最大加权剩余能量的单一 iod 将信息传输到 hap, 而另一个 iod 则从 hap 广播的信号。不过, 与现时大部分以渠道为导向的计划一样, 建议的以渠道为导向的计划, 亦会导致不公平的用户间吞吐量, 因为通道性能较好的 i o d 会获得更多的传送机会。为了在系统吞吐量和用户公平性之间取得平衡, 我们提出了一种基于归一化累积能量的面向公平的调度方案。为了评价系统性能, 我们将每个 iod 的动态充电放电过程建模为一个有限状态马尔可夫链。对于这两种方案, 通过 r 之所以导出系统中断概率和平均吞吐量的分析表达式。仿真结果验证了性能分析, 证明了两种方案比现有方案的性能优势。少

2018 年 3 月 6 日提交;最初宣布 2018 年 3 月。

评论:同意在 ieee 物联网杂志上发表

374. 第 xiv:1803. 00989[pdf,其他] Cs。直流

多伊10.114/31472 13. 3147230

基于云的应用程序的安全和优先感知数据发布

作者:lilia sampaio, fábio silva, amanda souza, and 输给 brito , pascal felber

摘要: 在本文中, 我们提出了一个数据传播平台, 支持数据安全和不同的隐私级别, 即使该平台和数据由不受信任的基础设施托管。拟议的系统旨在启用使用现成的受信任平台 (在本例中为英特尔 sgx) 的应用程序生态系统, 以便用户可以允许或不允许第三方访问具有特定敏感级别的实时数据流。此外, 此方法不要求用户直接管理加密密钥。我们的实验表明, 这种方法对于中型系统确实是可行的, 在这些系统中, 参与者一次传播少量数据, 例如在智能电网和**物联网环境中**。少

2018 年 3 月 2 日提交;最初宣布 2018 年 3 月。

375. 第 xiv:1803. 00916[pdf,其他] Cs。铬

大规模物联网系统中信号认证与安全的深度学习

作者:aidin ferdowsi, walid saad

摘要: 安全信号身份验证可以说是物联网 (**iot**) 环境中最具挑战性的问题之一, 因为该系统具有巨大的性质, 而且容易受到中间人和窃听攻击。本文提出了一种新的**物联网**信号动态认证的深度学习方法, 以检测网络攻击。基于长时间短期存储器 (lstm) 结构的拟议学习框架使**物联网**设备 (iotd) 能够从其生成的信号中提取一组随机特征, 并动态地将这些特征水印到信号中。这种方法使从**物联网**设备收集信号的云能够有效地验证信号的可靠性。此外, 在大规模**的物联网**场景中, 由于计算限制, 云无法同时对所有 iotd 进行身份验证, 因此提出了一个博弈论框架, 通过预测易受攻击的环境来改进云的决策过程。物联网。推导了该博弈的混合策略纳什均衡 (msne), 并证明了该模型在平衡条件下期望效用的唯一性。在庞大的**物联网**系统中, 由于云的大量可用操作, 它表明, 在分析性上推导 msne 具有挑战性, 因此, 提出了一个收敛到 msne 的学习算法。

此外，为了应对云无法访问未经身份验证的 iotd 状态的不完整信息情况，提出了一种深度强化学习算法，用于动态预测未经身份验证的 iotd 的状态，并允许云，以决定要对哪些 iotd 进行身份验证。仿真结果表明，在攻击检测延迟不到 1 秒的情况下，可以从**物联网**设备传输消息，可靠性几乎达到 100%。少

2018 年 2 月 28 日提交;最初宣布 2018 年 3 月。

评论:30 页, 11 位数字. arxiv 管理说明: 文本与 arxiv:1711.01306 重叠

376. 第 xiv:1803. 00899[pdf,其他] Cs。镍

不需要重定向 dns 的基于服务的雾体系结构

作者:mays al-naday, martin j.reed, janne riihijärvi, dirk trossen, nikolaos tomos, mohammed q. s. al-khalidi

摘要: 物联网 (**iot**) 的异构性和分布式特性推动了 5/5+G 架构和其他架构中对极其快速和细粒度的服务调配的需求。为了满足这些需求，实现高效、灵活的计算和网络结构至关重要，可以快速重新配置这些结构，以满足当前的计算和通信任务。在本文中，我们提出了一种新的忘记计算体系结构，该体系结构可将 **iot** 通信转换为服务事务，通过快速高效的网络结构进行配置。服务匹配是由使用以信息为中心的网络 (icn) 研究原则设计的网络功能提供的，将边缘请求直接路由到最近的服务点，而不会产生昂贵而缓慢的 dns 重定向。提出的雾基板在架构简单的同时，降低了网络的复杂性和开销。我们通过与如何在现有网络结构上建立忘记来评估体系结构，并量化性能优势。评价结果表明，该体系结构在降低所需的回程容量和路径长度方面具有优越性。少

2018 年 3 月 2 日提交;最初宣布 2018 年 3 月。

377. 第 xiv:1803.0 466[pdf] cs. cy

智能虚拟助手了解您的生活

作者:钟贤基,李桑金

摘要: 在**物联网**世界中，智能虚拟助理 (iva) 是一种流行的基于语音命令与用户交互的服务。为了获得最佳性能和高效的数据管理，著名的 iva (如 amazon 亚历克莎和 google 助手) 通常基于云计算架构进行操作。在此过程中，可以将大量包含用户语音活动历史记录以及详细说明的行为跟踪存储在 iva 生态系统中的远程服务器中。如果这些数据 (也称为 iva 云原生数据) 被攻击泄露，恶意用户不仅可以收集 iva 服务的详细使用历史记录，还可以通过各种数据分析技术揭示其他与用户相关的信息。在本文中，我们首先显示和分类类型的 iva 相关的数据，可以收集从流行的 iva，亚马逊亚历克莎。然后，我们分析了一个实验数据集，涵盖三个月的亚历克莎服务，并描述了用户的生活方式和生活模式的属性。我们的研究结果表明，有可能发现关于个人信息的新见解，如用户兴趣、iva 使用模式和睡眠、唤醒模式。本文给出的结果对 iva 供应商和用户的隐私威胁也有重要影响和威胁。少

2018 年 2 月 27 日提交;最初宣布 2018 年 3 月。

评论:6 页, 7 个数字

378. 第 xiv:1803. 00087[pdf,其他] Cs。直流

智能环境下不同计算平台本体论的文献综述

作者:souvik sengupta, jordi garcia, xavi masip-bruin

摘要: 智能环境集成了各种类型的技术，包括云计算、雾计算和**物联网**范式。在这样的环境中，必须高效地组织和管理广泛而复杂的异构资源集。因此，资源分类和分类成为

控制系统中的一个重要问题。本文对定义智能环境背景下任何类型的本体的各种计算系统和体系结构进行了详尽的文献综述，同时考虑到了明确提出资源分类和资源分类的作者。作者含蓄地提出了一些资源分类作为其系统体系结构的一部分。作为这项研究调查的一部分，我们建立了一个表格，总结了所有考虑到的研究工作，并提供了当前分类趋势的紧凑和图形快照。本文献调查的目标和主要动机是了解当前的最新技术，并确定智能环境场景中涉及的不同计算范式之间的差距。因此，我们发现，必须共同考虑几种计算范式和技术，而且还没有任何研究工作能够集成此类异构所需的合并资源分类、分类或本体场景。少

2018 年 2 月 28 日提交;最初宣布 2018 年 3 月。

评论:15 页, 1 个图

379. 建议: 1802. 10011[pdf,其他] cs. it

随机控制计算卸载到具有动态负载 cpu 的帮助器

作者:陶云正,你, 张平,黄开斌

文摘: 由于无线网络的致密化，边缘器件存在大量的闲置计算资源。通过从邻近**的小型物联网**设备中卸载繁重的计算任务，可以清除这些资源，从而克服其限制并延长电池寿命。但是，与专用服务器不同的是，边缘帮助程序提供的备用资源是随机的和间歇性的。因此，用户必须智能地控制卸载和本地计算的数据量，以确保计算任务能够在耗时的最小能量范围内完成。本文设计了具有随机通道和动态加载 cpu 的辅助器的计算卸载系统中的节能控制策略。具体而言，帮助程序采用的策略旨在确定不同插槽中给定任务的卸载和本地计算数据的大小，以便在任务期限内最大限度地减少传输和本地 cpu 的总能耗约束。因此，除了平衡卸载和局部计算外，这些策略还赋予卸载用户对通道和帮助者随机性的鲁棒性。通过将信道和地狱 cpu 建模为马尔可夫链，将卸载控制问题转化为马尔可夫决策过程。尽管用于数值解决问题的动态规划 (dp) 并不能以封闭的形式产生最优策略，但我们利用该过程对最优策略结构进行量化，并将结果应用于设计最优或次优策略。对于从零到大缓冲区的不同情况，策略的低复杂性克服了由于联合考虑通道、辅助器 cpu 和缓冲区状态而产生的 dp 中的 "维度曲线"。少

2018 年 2 月 27 日提交;最初宣布 2018 年 2 月。

评论:这项正在进行的工作已提交 ieee，以便可能出版

380. 第 1802.09949[pdf,其他] Cs。铬

工具演示: 用于设计安全的 e 据此智能合同的 fsolidm

作者:anastasia mavridou, aron laszka

摘要: 基于区块链的分布式计算平台支持在没有受信任代理的情况下执行以智能协定形式定义的可信计算。智能合同预计将有各种应用，从金融到**物联网**资产跟踪。不幸的是，智能合同的开发已被证明极容易出错。实际上，合同中充满了安全漏洞，其中包含一个关键问题，因为由于设计上存在错误是不可修复的，合同可能会处理具有重大价值的金融资产。为了促进安全智能合同的开发，我们创建了 fsolidm 框架，该框架允许开发人员使用严格而清晰的语义将合同定义为有限状态机 (fsm)。fsolidm 提供了一个易于使用的图形编辑器，用于指定 fsm、用于创建 ethereum 智能合同的代码生成器，以及开发人员可以添加到其 fsm 以增强安全性和功能的一组插件。少

2018 年 2 月 26 日提交;最初宣布 2018 年 2 月。

评论:arxiv 管理说明: 与 arxiv:1711.9327 有实质性文本重叠

381. 建议: 1802. 09207[pdf,其他] Cs。直流

利用大规模仿真技术评价物联网的突发行为

作者:stig bosmans, siegfried mercelis peter helrinckx, joachim denil

摘要: 随着物联网设备和更分散架构的增加，我们看到一种新型的应用程序变得越来越重要，在这种类型中，单个实体之间的本地交互会导致全局紧急行为，基于紧急情况的**物联网**(ebi) 系统。在本位置本文中，我们探讨了**评估物联网**应用中这种紧急行为的技术。由于所需的规模和多样性，这不是一项容易的任务。因此，我们主要关注分布式仿真方法，并概述了可优化整体仿真性能的可能技术。我们的工作重点是建模和仿真技术。少

2018 年 2 月 26 日提交;最初宣布 2018 年 2 月。

382. 建议: 1802 09052[pdf,其他] Cs。Lg

宽压缩: 张紧环网

作者:王文奇,孙一凡,布赖恩·埃里克森,王文林,瓦内特·阿加瓦尔

摘要: 深度神经网络在各种实际应用中展示了最先进的性能。为了获得性能提升，这些网络变得越来越大，越来越深，包含数百万甚至数十亿的参数和一千多层。需要权衡的是，这些大型体系结构需要大量的内存、存储和计算，从而限制了它们的可用性。在最近张量环分解的启发下，我们引入了张量环网络 (tr-net)，它显著压缩了深度神经网络的完全连接层和卷积层。我们的结果表明，我们的 tr-net 方法 {能够通过压缩 lenet-511x 在不丢失准确性的情况下}，并可以压缩最先进的广域 resnet243x{Cifar10 图像分类} 中的下降幅度为 2.3%。总体而言，这种压缩方案在科学计算和深度学习方面显示出希望，特别是对于智能手机、可穿戴设备和**物联网**设备等新兴资源受限的设备。少

2018 年 2 月 25 日提交;最初宣布 2018 年 2 月。

评论:2018 年接受 cvpr

383. 建议: 1802.08307[pdf,其他] Cs。铬

商品物联网中的敏感信息跟踪

作者:z. berkay celik, leonardo babun, amit k.Berkay, hidayet aksu, gang tan, patrick mcdaniel, a. selcuk Uluagac

摘要: 广义地定义为物联网 (**iot**)，将物理过程与数字连接相结合的商品设备的增长对社会产生了深远的影响--智能家居、个人监控设备、增强的制造和其他**物联网**应用改变了我们的生活、娱乐和工作方式。然而，现有**的物联网**平台几乎没有提供评估敏感信息的使用 (以及滥用的潜在途径) 的方法。因此，消费者和组织几乎没有信息来评估这些设备所存在的安全和隐私风险。在本文中，我们提出了**一种用于物联网**应用的静态污点分析工具 s 这儿，这是一种静态的污染分析工具。圣特分三个阶段运作:(a) 将特定于平台的**物联网**源代码转换为中间表示 (ir)，(b) 识别敏感源和汇，(c) 执行静态分析以识别敏感数据流。我们在 230 个智能产品市场应用上对 s1987 年 t 进行了评估，发现 138 (60%) 包括敏感数据流。此外，我们还演示了 itb 台上的 s 鲜明，这是一个新颖的开源测试套件，其中包含 19 个应用程序，其中有 27 个独特的数据泄漏。通过这项工作，我们引入了一个严格的框架来评估**物联网**应用中敏感信息的使用情况，其中为开发人员、市场和消费者提供了识别安全和隐私潜在威胁的方法。少

2018 年 2 月 22 日提交;最初宣布 2018 年 2 月。

评论:首次提交

384. **建议: 1802.08182[pdf, ps,其他] Cs。Hc**

多伊 10.114/3274469

用户对智能家居物联网隐私的看法

作者:serena zheng, noah apthorpe, marshini chetty,nick feamster

摘要: 智能家居物联网 (**iot**) 设备的普及程度正在迅速提高，包括持续监控用户活动的互联网连接设备在内的家庭越来越多。在这项研究中，我们与智能家居业主进行了 11 次半结构化访谈，调查了他们购买**物联网**设备的原因、对智能家居隐私风险的看法，以及为保护他们的隐私免受外部用户的影响而采取的行动。创建、管理、跟踪或监管**物联网**设备和/或其数据的家庭。我们注意到几个反复出现的主题。首先，用户对便利性和连接性的渴望决定了他们与外部实体 (如设备制造商、互联网服务提供商、政府和广告商) 打交道时与隐私相关的行为。其次，用户对收集智能家居数据的外部实体的意见取决于从这些实体中获得的明显利益。第三，用户信任**物联网**设备制造商来保护他们的隐私，但不验证这些保护是否到位。第四，用户不知道在非视觉设备上操作数据的推理算法会带来隐私风险。这些发现激发了对设备设计人员、研究人员和行业标准的若干建议，以便更好地将设备隐私功能与智能家居所有者的期望和偏好相匹配。少

2018 年 10 月 16 日提交;v1 于 2018 年 2 月 22 日提交;最初宣布 2018 年 2 月。

评论:20 页, 1 张

日记本参考:《人机交互论文集》，计算机支持的合作工作和社会计算会议，第 2 卷，第 200 条。2018 年 11 月

385. **建议: 1802.07855[pdf,其他] Cs。镍**

rt-dap: 用于大型工业过程监控的实时数据分析平台

作者:宋汉,陶公,马克·尼克松,埃里克·罗特沃尔德,林锦耀,克里蒂拉玛姆里瑟姆

摘要: 在当今大多数过程控制系统中，过程测量是定期收集并存档在历史学家。分析应用程序处理数据，并在脱机或在与制造过程的性能相比相当缓慢的时间段内提供结果。随着物联网 (**iot**) 的普及和过程工业中 "普及传感器" 技术的引入，越来越多的传感器和执行器安装在用于普适传感和控制的过程工厂中,而产生的过程数据量呈指数级增长。为了消化这些数据，满足不断增长的提高生产效率和提高产品质量的要求，需要有一种方法来提高分析系统的性能，并扩展系统，以密切监测更大的设备集资源。在本文中，我们提出了一个名为 rt-dap 的实时数据分析平台，以支持过程行业中的大规模连续数据分析。rt-dap 旨在能够以实时的方式对从异构工厂资源收集的大量实时数据流进行流式传输、存储、处理和可视化，并将数据流反馈给控制系统和操作员。该平台的原型在 microsoft azure 上实现。我们广泛的实验验证了 rt-dap 的设计方法，并在组件和系统级别上验证了其效率。少

2018 年 2 月 21 日提交;最初宣布 2018 年 2 月。

386. **建议: 1802.07476[pdf,其他] Cs。镍**

多伊 10.1109/VNC.2017.8275635

资源高效的车载到云通信预测信道感知传输的实证评价

作者:约翰内斯·皮尔曼,本杰明·斯利瓦,克里斯蒂安·卡斯廷,克里斯蒂安·维特费尔德

摘要: 现在的车辆默认配备了通信硬件。这就为互联服务提供了新的可能性，例如在物联网 (**iot**) 环境中作为高度移动传感器平台的车辆。因此，汽车需要通过移动通信网络

将数据上传到云中，以便进一步评估。由于无线资源有限，所有用户都能共享，因此需要有效地进行数据传输。在本工作的范围内，在经验设置中对三种车载到云数据传输算法、通道感知传输 (cat)、预测 cat (pcat) 和周期方案进行了评估。cat 利用通道质量测量来启动数据上传，最好是在通道质量良好的情况下。cat 的扩展 pcat 除了使用过去的测量值来估计未来的通道条件外，还使用过去的测量值。在实证评价中，为研究车配备了一个测量平台。在沿参考路线的测试驱动器上，收集了车辆传感器数据，并随后通过长期演进 (lte) 网络将其上传到云服务器。少

2018 年 2 月 21 日提交;最初宣布 2018 年 2 月。

日记本参考:车辆网络会议 (vnc), 2017 ieee

387. 建议: 1802.07475[pdf,其他] Cs。镍

多伊 10.1109/VTCSpring.2017.8108664

基于通用车辆信息模型的车载通信流量分析

作者:约翰内斯·皮尔曼, benjamin sliwa, jens schmutzler, christoph ide, christian wietfeld

摘要: 尽管连接服务在许多最新的汽车车型中已经引入，但在物联网 (**iot**) 中作为高度移动传感器平台的车辆的潜力尚未得到充分挖掘。因此，欧洲 aut 马项目结合跨行业、基于云的大数据市场，定义了一个开放的通用车辆信息模型 (cvim)。因此，即使在交通相关应用 (如局部天气预报) 之外，车辆传感器数据也可以用于设计全新的服务。本文利用基于经验测量的分析模型，对可实现的数据速率进行预测。为了进行深入分析，cvim 已集成到车辆交通模拟器中，以产生 cvim 投诉数据流，这是每辆车的个人行为 (速度、制动活动、转向活动等) 的结果。下一步，在一个现实的模型，大面积街道网络中的车辆流量模拟已使用结合蜂窝长期进化 (lte) 网络，以确定在每个网络单元内产生的累计数据量。因此，建立了一种新的车载到云通信流量模型，根据当前的交通情况 (自由流和交通堵塞)，量化车辆到云汇总数据的数据速率。研究结果为智能城市背景下汽车到云型服务的网络规划和资源调度提供了参考。少

2018 年 2 月 21 日提交;最初宣布 2018 年 2 月。

日记本参考:2017 年车辆技术会议 (vtc spring), ieee 第 85 届

388. 建议: 1802. 06902[pdf,其他] Cs。镍

用于工业物联网预测数据发布的缓存辅助 d2d 操作

作者:antonimino orsino, roman kovalchukov, andrey samuylov, dmitri moltchanov, sergey andreev, yevgenikoucheryavy, Valkama valkama

摘要: 工业自动化部署构成了具有挑战性的环境，在这些环境中，移动**的物联网**机器可能会在测量和检测操作过程中产生高清视频和其他重传感器数据。将大量内容传输到边缘网络基础设施，然后最终传输到远程人工运营商，需要由智能数据缓存和交付机制支持的可靠和高速无线电链路。在这项工作中，我们通过建议将移动的工业机器作为设备到设备 (d2d) 缓存帮助程序来解决典型工厂自动化方案中内容传播的挑战。为了提高高速毫米波 (mmwave) 数据连接的可靠性，我们引入了替代内容传播模式，然后构建了一种新的行动感知方法，帮助开发预测模式的选择基于预期的无线电连接条件的策略。我们还对具有代表性的数据传播策略进行了全面的系统级评估，以确认在无线边缘使用支持 d2d 的协作缓存的预测解决方案的优势，从而降低内容交付延迟和提高数据采集的可靠性。少

2018 年 2 月 19 日提交;最初宣布 2018 年 2 月。

389. 建议: 1802.06691[pdf,其他] Cs。铬

面向物联网设备的基于海绵的控制流保护

作者:mario werner, thomas unterluggauer, david scanfenrath, stefan mangard

摘要: 物联网 (**iot**) 中的嵌入式设备面临着各种各样的安全挑战。例如，软件攻击者在其远程接口上执行代码注入和代码重用攻击，对**物联网**设备的物理访问允许篡改内存中的代码、窃取机密知识产权 (ip) 或发起故障攻击以操作 cpu 的控制流。在这项工作中，我们提出了基于海绵的控制流量保护 (scfp)。scfp 是一种有状态的、基于海绵的方案，旨在确保软件 ip 及其在**物联网**设备上的真实执行的保密性。在编译时，scfp 使用指令级粒度对软件进行加密和身份验证。在执行过程中，cpu 的提取和解码阶段之间的 scfp 硬件扩展连续解密和验证指令。scfp 中基于海绵的身份验证加密可产生细粒度的控制流完整性，从而防止代码重用、代码注入以及对代码和控制流的故障攻击。此外，scfp 还能承受内存中对软件的任何修改。为了进行评估，我们使用 scfp 扩展了 risc-v 内核，并在芯片上构建了一个真正的系统 (soc)。scfp 在这种设计上的平均开销分别为 19.8% 和 9.1%，从而满足嵌入式**物联网**设备的要求。少

2018 年 2 月 19 日提交;最初宣布 2018 年 2 月。

评论:接受 ieee 欧洲标准普尔 2018 年会议

390. 建议: 1802. 06305[pdf,其他] Cs。Lg

多伊 10.1016/j.dcan.2017.10.002

物联网数据分析的机器学习: 一项调查

作者:mohammad saeid mahdavinejad, mohammad m 不过是 za rezvan , mohammadamin barekatain, peyman adibi, payam barnaghi, amit p. shth

摘要: 硬件、软件和通信技术的迅速发展使互联网连接的感官设备得以出现，这些设备提供来自物理世界的观测和数据测量。到 2020 年，估计正在使用的互联网连接设备总数将在 250 亿至 500 亿之间。随着数字的增长和技术的成熟，公布的数据量将增加。互联网连接设备技术，被称为物联网 (**iot**)，通过提供物理世界和网络世界之间的连接和交互，继续扩展当前的互联网。除了增加体积外,**物联网**还生成大数据，其特点是在时间和位置依赖方面具有速度，具有多种模式和不同的数据质量。对这些大数据进行智能处理和分析是开发智能**物联网**应用的关键。本文以智慧城市为主要用例，评估**了应对物联网**数据挑战的不同机器学习方法。本研究的主要贡献是介绍了机器学习算法的分类，解释了如何将不同的技术应用于数据，以提取更高级别的信息。还将讨论**机器学习在物联网**数据分析方面的潜力和挑战。本文给出了一种将支持向量机 (svm) 应用于奥胡斯智慧城市交通数据的用例，以进行更详细的探索。少

2018 年 2 月 17 日提交;最初宣布 2018 年 2 月。

评论:数字通信与网络 (2017)

391. 建议: 1802. 06195[pdf] 中心

智能嵌入式系统的高速 srt 分频器

作者:bhavana mehta, janti talukdar , sachin gajjar

摘要: 嵌入式系统、vlsi 和处理器设计的不断发展，在功率、速度、面积、吞吐量等方面都对系统提出了越来越高的要求。大多数复杂的嵌入式系统应用程序由处理器组成，处理器现在需要一个算术单元，能够以最高的效率执行复杂的除法操作。因此，算术单元的速度在很大程度上取决于除法运算。大多数分隔符都使用 srt 除法进行除法。在

物联网和其他嵌入式应用程序中，通常使用基数 2 和 radix 4 除法。该算法在于并行执行各种步骤，以减少时间临界路径，利用模糊逻辑解决商选择中的重叠问题，从而减少最大延迟，提高精度。每个逻辑电路都有一个最大延迟，电路的时间取决于该电路和路径，从而导致最大延迟被称为关键路径。我们的方法使用以前的 srt 算法方法进行高度并行的流水线设计，并使用 mamdani 模型来确定重叠问题的解决方案，以减少 64 位双精度浮动上的 radix 4 srt 除法的整体执行时间点数到 281ns。该设计采用 bluesec 系统 verilog，利用 vivado v.2016.1 进行合成和仿真，并在 xilinx virtex 超微 fpga 板上实现。少

2018 年 2 月 17 日提交;最初宣布 2018 年 2 月。

评论:ieee 国际连接 17 (5 页)

392. **建议: 1802.0 5832[pdf,其他] cs. it**

一种基于报复性的 stackelberg 游戏模型，用于提高自私物联网设备频谱租赁中的保密率

作者:fatemeh afghah, alireza shamsoshoara, laurent njilla, charles kamhoua

文摘: 研究了将合作频谱租赁到无证物联网 (**iot**) 设备的问题，以解释这些设备潜在的自私行为。提出了一个分布式频谱租赁游戏理论框架，即许可用户可以心甘情愿地将部分频谱访问权限租赁到未授权的**物联网**设备，并作为回报，**物联网**设备提供合作服务，首先是通过增加故意干扰来加强持牌用户的信息保密，以保护他们免受潜在窃听者的攻击；其次是通过合作中继提高沟通质量。使用基于信誉的机制监视潜在自私的**物联网**设备的合作行为，使主要用户只能与可靠的**物联网**设备交互。仿真结果表明，采用基于信誉的方法可以降低来自自私**物联网**设备的攻击可能性，从而提高了主要用户的保密率。因此，该模型可以为移动**物联网**设备的频谱租赁提供实用的解决方案，从而确保频谱所有者所需的通信质量和信息保密。少

2018 年 2 月 15 日提交;最初宣布 2018 年 2 月。

评论:6 页, ieee infocom 软件定义和上下文感知认知网络进展研讨会

393. **建议: 1802. 0597[pdf,其他] Cs。铬**

混合现实中的安全与隐私方法: 一门文献综述

作者:jaybie a. deguzman , kanchana thilakarathna, aruna seneviratne

摘要: 由于计算机视觉、传感器融合和现实显示技术的进步，混合现实 (mr) 技术的发展正在获得动力。由于大部分的研究和开发都集中在实现 mr 的承诺上，因此只有少数研究这项技术对隐私和安全的影响。本调查文件旨在揭示这些风险，并研究 mr 的最新安全和隐私工作. 具体而言，我们列出并审查了为确保 mr 中的用户和数据安全和隐私而提出的不同保护方法。包括关于增强现实 (ar)、虚拟现实 (vr) 和人机交互 (hci) 等相关技术的工作的范围，将其作为 mr 的关键组成部分，如果不是其起源的话，以及来自更大移动设备领域的许多相关工作,可穿戴设备和物联网 (**iot**)。我们强调，在 mr 中缺乏对数据保护方法的调查、实施和评价，还讨论了 mr 安全和隐私方面的进一步挑战和方向。少

2018 年 6 月 25 日提交;v1 于 2018 年 2 月 15 日提交;最初宣布 2018 年 2 月。

评论:40 页、11 个数字、2 个表格 (附录中的 3 个表格)

394. **第 1802. 05198[pdf,其他] Cs。镍**

多伊 10.114/31·32105

icn 支持基于 ip 的物联网设备的 coap 扩展

作者:nikos fotiou, george xylomenos, george c. polyzos, h 山伊斯兰, demrij lagutin, teemu hakala, eero hakala

摘要: 约束应用程序协议 (coap) 及其扩展 (如观察和群通信) 为开发新型**物联网**应用程序提供了潜力。但是，一个成熟的基于 coap 的应用程序需要对多播进行延迟容错通信和支持: 由于现有 ip 网络不容易提供这些属性，开发人员无法充分利用 coap，而更愿意使用 http 相反。在本演示中，我们展示了如何通过 icn 网络代理 coap 流量释放 coap 的全部潜力，同时将开销和复杂性从 (受约束的) 端点转移到网络。少

2018 年 2 月 14 日提交;最初宣布 2018 年 2 月。

日记本参考:2017 年 9 月 26 日至 28 日在德国柏林举行的第四届以信息为中心的网络会议论文集, 218-219 页

395. 建议: 18004410[pdf, ps,其他] Cs。铬

基于智能契约的物联网访问控制

作者:张元宇,卡萨哈拉 shoji,沈玉龙,姜晓红,万建雄

文摘: 本文研究了物联网 (**iot**) 中的一个关键访问控制问题。特别是，我们提出了一个基于智能合同的框架，它由多个访问控制合同 (acc)、一个法官合同 (jc) 和一个注册合同 (rc) 组成，以实现**物联网**系统的分布式和可信的访问控制。每个 acc 为主题对象对提供了一种访问控制方法，并通过检查主题的行为来实现基于预定义策略的静态访问权限验证和动态访问权限验证。jc 通过接收 acc 的不当行为报告、判断不当行为并返回相应的惩罚，实现了一种错误判断方法，以方便对 a c 的动态验证。驻地协调员登记访问控制和错误判断方法的信息及其智能合同，并提供管理这些方法的功能 (例如，注册、更新和删除)。为了演示该框架的应用，我们在**物联网**系统中提供了一个案例研究，该系统有一台台式计算机、一台笔记本电脑和两台树莓派单板计算机，其中的 acc、jc 和 rc 是基于 ethereum 智能合同实现的平台，实现访问控制。少

2018 年 2 月 12 日提交;最初宣布 2018 年 2 月。

396. 建议: 1802.04345[pdf,其他] Cs。Sy

移动代理内部的本地化: 一种线性方法

作者:sam safavi, usman a. khan, soummya kar, josém . f. moura

摘要: 第五 generation~(5G) 网络提供更高的带宽和更快的数据速率，将允许连接大量静态和移动设备、传感器、代理、用户、机器和车辆，支持物联网 (**iot**)，实时移动设备的动态网络。定位和位置意识将变得越来越重要，从而能够部署新的服务，并有助于大大提高 5G~system 的总体业绩。目前讨论的许多定位 in~5G 解决方案都是集中式的，主要需要直接查看 (los) 到部署的访问节点或锚点，这反过来又需要高密度的锚点部署。但随着用户和设备数量的不断增长，这些 los 和集中定位解决方案可能会变得难以操作。作为集中式解决方案的替代方案，本文讨论了启用 5g 的**物联网**环境中的分布式本地化，在这种环境中，许多低功耗设备、用户或代理都要在没有全局或 los 访问锚点的情况下定位自己。尽管定位本质上是一个非线性问题 (通过三进法或三角法求解圆方程)，我们讨论了一个只有局部测量、通信和计算的协同的结状 {00 分布式迭代解需要在每个代理。通过基于局部邻域几何的重心坐标表示对代理位置进行再分析，得到了线性度，这些坐标表示可以根据涉及相对局部互剂的某些 cayley-menger 决定因素来计算距离测量。少

2018 年 2 月 12 日提交;最初宣布 2018 年 2 月。

评论:技术报告

397. 特别报告: 1802. 0422[pdf,其他] Cs。镍

lpwa 网络的比较研究

作者:joseph finnegan, stephen brown

摘要: 由于所建议的物联网 (**iot**) 应用的差异越来越大，以及当前无线技术在可扩展的远程部署中缺乏适用性，一些不同的低功耗广域 (lpwa) 技术已开发。这些技术有望在廉价的低功耗设备上实现可扩展的高范围网络，从而促进无处不在**的物联网**的开发。本文提供了这种新的 lpwa 范式的定义，提出了定义合适用例的系统方法，并对当前的 lpwa 标准进行了详细比较，包括主要技术、即将推出的蜂窝选项和剩余的专有解决方案。少

2018 年 2 月 12 日提交;最初宣布 2018 年 2 月。

评论:10 页

398. 特别报告: 1802. 04102[pdf,其他] cs. cy

物联网时代的广告: 愿景与挑战

作者:hidayet aksu, leonardo babun, mauro conti , gabriele tolomei, a. selcuk Uluagac

摘要: 物联网 (**iot**) 将计算机连接到众多不同设备 (统称为智能设备) 的想法扩展。这些都是物理项目----即 "事物"----例如可穿戴设备、家用电器和车辆，这些设备富含计算和网络功能。由于涉及大量的设备，因此也因此也涉及其普遍性，物联网是一个很好的平台，可以利用它来构建新的应用程序和服务或扩展现有的应用程序和服务。在这方面，将网络广告扩展到**物联网**领域是一个调查不足但前景广阔的研究方向，特别是考虑到传统的互联网广告市场已经价值数千亿美元。本文首先提出了一个以传统网络广告为基础的著名商业生态系统启发的**物联网**广告平台的体系结构。此外，我们还讨论了实现此类平台的主要挑战，特别关注与体系结构、广告内容交付、安全性和用户隐私相关的问题。少

2018 年 1 月 31 日提交;最初宣布 2018 年 2 月。

评论:可在 ieee 通信杂志上发表

类:h。3

399. 建议: 180003898[pdf,其他] Cs。镍

无线传感器网络和物联网驱动的可扩展下行路由

作者:钟晓阳,姚亮

文摘: 本文研究了大规模异构无线传感器网络 (wsn) 和物联网 (**iot**) 中网络控制驱动的下行路由。我们提出了一个可扩展和可靠的向下路由协议的机会源路由 (osr) wsnss/iot.osr 基于节点向上路由的父集合引入传统的源路由，显著解决了低功耗和有损 wsn 中的剧烈链接动态问题。我们设计了一种新的自适应 bloom 滤波器机制，有效地编码 osr 中的向下源路由，从而显著缩短了数据包头中源路由字段的长度。osr 可扩展到非常大的 wsn/iot 部署，因为网络中的每个资源受限节点只存储其直接子节点集.布鲁姆滤波器的概率性质被动地探索机会主义路径。在沿着下行路径的任何跃点发生传递失败时, osr 都会主动执行机会路由，以绕过过时的/坏的链接。我们展示了 osr 相对于标准 rpl 向下路由的理想可扩展性。我们通过模拟和实际测试实验来评估 osr 的性能，并与标准的 rpl (存储模式和非存储模式)、orpl 和具有代表性的传播协议

drip 进行比较。结果表明, osr 在可扩展性和可靠性方面明显优于 rpl 和 orpl。与基于与 osr 实现相同的 tinyos 平台的 tinyrpl 和 drip 相比, osr 还实现了显著提高的能效。少

2018 年 2 月 12 日提交;最初宣布 2018 年 2 月。

评论:10 页

400. **建议: 180003858[pdf,其他] Cs。马**

物联网代理中基于机器学习的可变性处理

作者:nathalia nascimento, paulo alencar, carlos lucena, donald cowan

摘要: 基于代理的**物联网**应用最近在医疗保健、智慧城市和农业等多个领域得到了应用。在特定设置中部署这些应用程序非常具有挑战性, 原因有很多, 包括传感器和执行器等物理设备的复杂静态和动态变化、软件应用程序行为和环境。应用程序嵌入的。本文提出了一种基于反馈评估机器学习的可自构**物**联网代理方法。该方法涉及: i) 物**联网**代理的可变性模型;(ii) 定制代理的生成;(三) 反馈评价机器学习;iv) 一组**物联网**代理的建模和组成;和 v) 基于手动和自动反馈的功能选择方法。少

2018 年 2 月 11 日提交;最初宣布 2018 年 2 月。

评论:提交 8 页, 6 个数字

401. **建议: 180003835[pdf,其他] Cs。简历**

基于特征空间编码的深部神经网络对资源受限物联网平台的边缘-主机划分

作者:jong hwan ko, taesik na , mohammad faisal amir, saibal mukhopadhyay

文摘: 本文介绍了**在物联网**环境中, 在边缘和主机平台之间划分深度神经网络的推理任务。我们提出了一个 dnn 作为编码管道, 并建议将中间层的输出特征空间传输到主机。提出了特征空间的无损或有损编码, 以提高边缘平台支持的最大输入率, 或降低边缘平台的能量。仿真结果表明, 在卷积 (特征提取) 层的末尾对 dnn 进行分区, 再加上特征空间编码, 可以显著提高比执行的基线配置的能效和吞吐量更高在边缘或主机上的整个推断。少

2018 年 2 月 11 日提交;最初宣布 2018 年 2 月。

402. **建议: 1802.03714[pdf,其他] Cs。铬**

基于图像识别的物联网恶意软件轻量级分类

作者:su jalwei, danilo vasconcellos vargas, sanjiva prasad, daniele sgandurra, yaokai feng, kouichi sakurai

摘要: 物联网 (**iot**) 是传统互联网的延伸, 它允许大量的智能设备, 如家用电器、网络摄像机、传感器和控制器相互连接, 以共享信息和提高用户水平经验。当前**的物联网**设备通常是用于特定于域的计算的微型计算机, 而不是传统的特定于功能的嵌入式设备。因此, 针对连接到互联网的传统计算机的许多现有攻击也可能针对**物联网**设备。例如, ddos 攻击在**物联网**环境中变得非常普遍, 因为这些环境目前缺乏基本的安全监视和保护机制, 最近的 mirai 和 brickerbot 物联网僵尸**网络**就表明了这一点。本文提出了一种检测**物联网**环境中 ddos 恶意软件的新的轻量级方法。首先提取从二进制文件转换的单通道灰度图像, 然后利用轻量级卷积神经网络对**物联网**恶意软件家族进行分类。实验结果表明, 该系统对好软件和 ddos 恶意软件的分类可以达到 94.0% 的准确率, 对好软件和两个主要恶意软件家族的分类可以达到 81.8 的准确率。少

2018 年 2 月 11 日提交;最初宣布 2018 年 2 月。

403. 建议: 1802. 03462[pdf,其他] Cs。铬

oei: 嵌入式设备的操作执行完整性

作者:孙志庄,博峰 , 龙路,索姆梅, 贾沙子

摘要: 我们制定了一个新的安全属性, 称为 "操作执行完整性" 或 oei, 专为嵌入式设备量身定制。在面向操作的嵌入式程序设计的启发下, 考虑到嵌入式设备的硬件功能有限, oei 认证可对控制流完整性和关键变量进行选择性和实际验证正在执行的操作的完整性。此认证允许远程验证程序在保护 **iot** 所需的嵌入式设备能力上检测控制流劫持以及仅数据攻击 (包括面向数据的编程), 但使用现有方法无法实现。我们设计并构建了一个名为 oat 的系统, 以实现和评估基于 arm 的裸机设备上的 oei 认证的想法。oat 具有高效的测量收集机制、为确定可验证性而设计的控制流测量方案以及轻量级可变完整性检查方法。在开发板上针对实际嵌入程序进行测试时, oat 只产生了轻微的运行时开销 (2.7%)。少

2018 年 2 月 9 日提交;最初宣布 2018 年 2 月。

评论:16 页, 4 个数字

404. 建议: 1802.0159[pdf, ps,其他] Cs。直流

运行分布式和动态物联网编排

作者:jan seeger, rohit a. deshmukh, arne bröring

摘要: **物联网**系统越来越大, 越来越适合基本的自动化任务。**物联网**自动化系统可以提供的功能之一是处理动态系统--设备在运行过程中离开和加入系统。此外,**物联网**自动化系统以分散的方式运行。目前的商业自动化系统很难提供这些功能。将新设备集成到自动化系统需要手动干预。此外, 自动化系统还需要中央实体来协调参与者的操作。借助更智能的传感器和参与者, 我们可以将控制操作移动到分散的设备网络上部署的软件中, 并为动态系统提供支持。在本文中, 我们提出了一个自动化系统的框架, 它演示了这两个属性 (分布式和动态)。我们将应用程序表示为语义上描述的数据流, 这些数据流在参与设备上分散运行, 并在运行时通过规则进行连接。这样就可以在不进行手动交互的情况下将新设备集成到应用程序中, 并将中央控制器从公式中删除。此方法提供了与当前自动化系统 (中央工程、应用程序的多个实例化) 类似的功能, 但支持分布式和动态操作。通过定量评价, 我们展示了该系统令人满意的性能。少

2018 年 2 月 9 日提交;最初宣布 2018 年 2 月。

评论:提交给 gots 2018

405. 建议: 1802.03 110[pdf] Cs。铬

物联网新功能对安全性和隐私的影响: 新的威胁、现有的解决方案和有待解决的挑战

作者:周伟,张玉清,刘鹏

摘要: 物联网 (**iot**) 的未来已经摆在我们的脑后。**物联网**应用已广泛应用于社会生产和社会生活的许多领域, 如医疗保健、能源和工业自动化。在**享受物联网**给我们带来的便利和效率的同时,**物联网**也出现了新的威胁。为缓解这些威胁, 越来越多的研究工作, 但许多问题仍然悬而未决。为了更好地了解新威胁的根本原因和当前研究中的挑战, 本次调查首先提出了 "**物联网**功能" 的概念。然后讨论了八个**物联网**新功能的安全和隐私影响, 包括它们造成的威胁、现有的解决方案和有待解决的挑战。为了帮助研究人员跟踪这一领域的最新工作, 本文最后阐述了**物联网**安全研究的发展趋势, 并通过对现

有的大多数领域的研究，揭示了物联网特征对现有安全研究的影响 2013 年至 2017 年与物联网安全相关的研究工作。少

2018 年 2 月 8 日提交;最初宣布 2018 年 2 月。

406. 建议: 18003033[pdf,其他] Cs。镍

多伊 10.1109/SYSCON.2018.8369572

大型基于 iot 的仓库系统中高效通信的环路设计空间探索

作者:robert falkenberg, jens Drenhaus, benjaminsliwa, christian wietfeld

摘要: 未来的智能仓库将超越容器，进入积极自主参与优化物流流程的网络物理系统 (cps)，而不是将库存物品视为静态资源。因此，必须解决大规模物联网 (iot) 上下文的系统内在新挑战，例如共享通信媒体中的通道访问。本文提出了一种多方法系统模型，该模型汇集了用于测量真实硬件特性的试验台实验和大规模考虑的仿真评价。作为一个示例案例研究，我们将特别关注基于 802.15.4 的无线通信系统的参数化，由于收获的能量很少，该系统必须具有能源效率，但避免延迟以维护覆盖仓库系统。结果表明，与标准相比，修改初始回退时间可同时节省 50% 的能量和时间。少

2018 年 6 月 12 日提交;v1 于 2018 年 2 月 8 日提交;最初宣布 2018 年 2 月。

期刊参考: 2018 年 ieee 国际系统年会 (syscon)

407. 建议: 1802.0 2986[pdf,其他] cse

多伊 10.1007/978-3-319-74030-0 _ 33

自适应网络物理过程的认知业务流程管理

作者:andrea marrella , masimo m 中 ella

摘要: 在大数据和物联网 (iot) 时代，随着互联设备和嵌入式 ict 的存在，所有真实世界的环境都逐渐成为网络物理环境 (如应急管理、医疗保健、智能制造等)产生大量数据和事件的系统 (如智能手机、传感器、执行器) 会影响在此类环境中颁布的网络物理进程 (cpp) 的颁布。需要用于执行 cpp 的过程管理系统 (pms)，通过在运行时最大限度地减少任何人为干预，自动调整其运行过程以适应异常情况和外源事件。在本文中，我们通过引入一种方法和自适应认知 pms 来解决这个问题，该方法和方法结合了流程执行监视、意外异常检测和自动解决策略，利用了基于既定操作的基础人工智能中的形式主义，它允许解释不断变化的网络物理环境知识，并通过保留其基础结构来适应 cpp。少

2018 年 2 月 8 日提交;最初宣布 2018 年 2 月。

评论:第一届认知商业流程管理国际研讨会论文集 (cbpm 2017) 预印

408. 建议: 1802.02186[pdf] Cs。简历

fastnet

作者:john olafenwa, moses olafenwa

摘要: 卷积神经网络结构的初始和重网家族在过去几年中打破了记录，但最近的最先进模型在训练、推理和模型尺寸方面也产生了很高的计算成本。使这些模型在边缘设备上的部署不切实际。鉴于此，我们提出了一种新的新型体系结构，旨在提高 gpu 和 cpu 的计算效率，非常适合在移动应用程序、智能相机、 iot 设备和控制器上部署，并且成本较低。无人 机。我们的架构在标准数据集上具有竞争力的精度，甚至超过了原来的 resnet。下面是这项研究的动机、网络的体系结构、cifar 10 和 cifar 100 上的单一测试精度、与其他知名体系结构的详细比较以及与 keras 实现的链接。少

2018 年 1 月 17 日提交;最初宣布 2018 年 2 月。

409. xiv:1802. 02138[pdf,其他] Cs。简历

音乐椅: 使用协同物联网设备实现高效的实时识别

作者:ramyad hadidi, cao. Jiashen , matthew woodward, michael s.ryoo, hyesoon kim

摘要: 物联网 (**iot**) 设备的普及和传感器数据的丰富，增加了语音、图像和视频识别等实时数据处理。虽然目前此类进程已卸载到计算功能强大的云系统，但本地化和分布式方法是可取的，因为 (i) 它保留了用户的隐私, (ii) 它忽略了对云服务的依赖。但是,**物联网**网络通常由资源受限的设备组成，单个设备的功能不足以处理实时数据。为了克服这一挑战，我们在深度神经网络的背景下检查此类设备的数据和模型并行性。我们建议音乐椅通过从与输入传感器相同的**物联网**网络中的资源受限设备中获取聚合计算能力，实现高效、本地化和动态的实时识别。音乐椅可适应计算设备在运行时的可用性，并可根据**物联网**网络的继承动态进行调整。为了演示音乐椅，在每个连接到摄像机的树莓 pi (最多 12个) 网络上，我们为视频实现了最先进的动作识别模型，并为图像实施了两个识别模型。与具有六核 cpu 和 gpu 的嵌入式低功耗平台 tegra tx2 相比，我们的分布式动作识别系统不仅实现了类似的能耗，而且还实现了 tx2 性能的两倍。此外，在图像识别中，音乐椅实现了相似的性能，节省了动态能量。少

2018 年 3 月 21 日提交;v1 于 2018 年 2 月 5 日提交;最初宣布 2018 年 2 月。

410. 建议: 180002041[pdf,其他] Cs。铬

基于传感器的物联网 (iot) 设备和应用威胁调查

作者:amit kumar sikder, giuseppe petraca, hidayet aksu, trent jaeger , a. selcuk ululuagac

摘要: 物联网 (**iot**) 的概念在现代技术时代比以往任何时候都更加流行。从小型家用设备到大型工业机器,**物联网**的愿景使设备能够与周围的物理世界连接。这种日益普及的情况也使**物联网**设备和应用成为攻击者关注的焦点。已经存在多种类型的恶意活动，这些活动试图破坏**物联网**设备的安全和隐私。一个有趣的新出现的威胁媒介是滥用物联网设备上使用传感器的攻击。由于缺乏适当的安全测量可用于控制应用对传感器的使用,**物联网**设备容易受到基于传感器的威胁。通过**利用物联网**设备上的传感器 (例如，加速度计、陀螺仪、麦克风、光传感器等)，攻击者可以从设备中提取信息、将恶意软件传输到设备或触发恶意活动以危害设备。在本次调查中，我们探讨了针对**物联网**设备的各种威胁，并讨论了如何将其传感器滥用于恶意目的。具体而言，我们提供了一份详细调查,介绍了现有的基于传感器的物联网设备威胁以及专门为**保护物联网**设备传感器而制定的对策。此外，我们还结合基于传感器的威胁讨论**了物联网**设备的安全和隐私问题，并总结了未来的研究方向。少

2018 年 2 月 6 日提交;最初宣布 2018 年 2 月。

评论:基于传感器的威胁、物联网、智能设备、侧信道攻击

411. 建议: 180001818[pdf] Cs。直流

物联网辅助智能电网转型中的雾计算-要求、前景、现状与挑战

作者:md. muzakkir hussain, mohammad saad alam,m. m. sufyan beg

摘要: 由于 it 领域的发展，即智能交通和信息技术的现代智能电网 (sg) 系统被智能设备和实体所利用。当被赋予物联网 (**iot**) 和传感器网络时，这样的基础设施会使大量

的对象活跃且在线。传统的云部署可以满足分散的、动态的、动态的和资源时间关键的 sg 生态系统的分析和计算紧急情况。本文对云计算实用程序在多大程度上能够满足 sg 生态系统的关键任务要求以及哪些子域和服务需要基于雾的计算原型进行了综合考察。这项工作的目的是理解雾计算算法的适用性，以相互作用的核心为中心的云计算支持，从而能够提出一个新的类型的实时和延迟无延迟 sg 服务。这项工作还突出了基于雾的 sg 部署所带来的机会。相应地，我们也强调了挑战和研究的重点，阐明了为成功的 sg 转换的雾计算的可行性。少

2018 年 2 月 6 日提交;最初宣布 2018 年 2 月。

评论:13 页, 1 张, 1 图

412. **xiv:1802 01790[pdf,其他] cs.PL**

多伊 10.4204/EPTCS.264。4

节点的运行时监测及其在物联网中的应用

作者:davde ancona, luca franceschini, giorgio delzanno, maurizio leotta, marina ribaudo, Filippo ricca

摘要: 在过去的几年里, node. js 已经成为一个特别适合于实现轻量级**物联网**应用程序的框架，这得益于其底层的异步事件驱动、非阻塞 ito 模型。但是，使用异步嵌套回调验证程序的正确性是相当困难的，因此，运行时监视可以成为解决此类复杂任务的宝贵支持。运行时监控是一种有用的软件验证技术，它补充了静态分析和测试，但尚未在物联网 (**iot**) 系统中进行充分的探索。跟踪表达式已成功地用于广泛使用的多智能体系统平台中的运行时监视。最近，它们的表现力得到了扩展，允许对数据进行参数化规范，这些数据只能在运行时捕获和监视。此外，它们可以是语言和系统的不可知论者，通过事件域和类型的概念。本文研究了参数跟踪表达式的使用，作为对 node. js 和 node-red 开发的程序进行运行时监视的第一步，这是一种基于流的**物联网**编程工具，构建在 node. js 之上。这类系统的运行时验证是一项迄今在文献中似乎大多被忽视的任务。为了用跟踪表达式动态地检查 api 函数的正确使用，提出了一个实现 node. js 系统的原型。该工具利用动态分析框架 jalangi 来监视 node. js 程序，并允许检测使用其他技术难以捕获的错误。此外，它还提供了一个简单的 rest 接口，可用于节点 -red 组件的运行时验证，更广泛地说，还可以利用 **iot** 设备。少

2018 年 2 月 5 日提交;最初宣布 2018 年 2 月。

评论:2017 年 ALP4IoT 联网, arxiv:1802. 00976

日记本参考:eptcs 264, 2018, 第 27-42 页

413. **建议: 180001789[pdf,其他] Cs。直流**

多伊 10.4204/EPTCS.264。3

用于汇总分布式数据的弹性块

作者:giorgio audrito, sergio bergamini

摘要: 汇总分布式数据是并行编程的核心常规，位于 map/缩减范式等广泛使用的框架的核心。在**物联网**环境中，它更加关键，因为它是允许远程交互的特权手段: 事实上，需要进行总结，以避免每个计算单元中的数据爆炸。介绍了一种新的分布式数据动态总结算法，加权多径，改进了最先进的多路径算法。我们在原型场景中验证了新算法，同时考虑到多种波动源，并将其与其他现有实现进行了比较。因此，我们表明，即使在其他算法与正确值有显著差异的高变异性情况下，加权多路径也能保持足够的准确性。少

2018 年 2 月 5 日提交;最初宣布 2018 年 2 月。

评论:2017 年 ALP4IoT 联网, arxiv:1802. 00976

类:C.2.4;D.1.3;D.3。2

日记本参考:eptcs 264, 2018, 第 23-26 页

414. xiv:1802 01788[pdf,其他] Cs。直流

多伊10.4204/EPTCS.264。2

聚合图形统计信息

作者:giorgio audito, fer 鲁乔? 达米亚尼, mirko viroli

摘要: 从基于图形的数据中收集统计数据是数据挖掘界日益研究的课题。我们认为，这些统计数据在动态**物联网**环境中也有很大的价值: 它们可以支持复杂的计算活动，包括分布式协调和提供情况识别。我们证明，利用对场微积分的映射，即为集体提出的分布模型，计算图形顶点顶点邻域函数的 hyperanf 算法自然允许完全分布式和异步实现自适应系统。此映射证明，字段微积分框架非常适合在图形上容纳大规模并行计算。此外，它还提供了一个新的 "自我稳定" 构建块，可用于在多个上下文中的聚合计算，其中包括改进的领导者选举或网络漏洞检测。少

2018 年 2 月 5 日提交;最初宣布 2018 年 2 月。

评论:2017 年 ALP4IoT 联网, arxiv:1802. 00976

类:C.2.4;D.1.3;D.3。2

日记本参考:eptcs 264, 2018, 第 18-22 页

415. 建议: 1802.01016[pdf,其他] cs. ne

基于域墙记忆的深部构想神经网络的随机计算区域与节能设计

作者:马晓龙 ,张一鹏,耿元,奥仁, 李哲, 韩杰,胡景通, 王延志

摘要: 随着可穿戴设备和物联网 (**iot**) 的最新发展趋势，为嵌入式应用开发基于硬件的深卷积神经网络 (dcn) 变得很有吸引力，因为嵌入式应用需要低功耗和小的功耗。硬件足迹。最近的研究表明，随机计算 (sc) 技术可以从根本上简化算术单元的硬件实现，并有可能满足嵌入式设备中严格的功率要求。然而，在这些工作中，对重量存储来说，内存设计优化被忽略了，这必然会导致较大的硬件成本。此外，如果使用传统的挥发性 sram 或 dram 单元进行重量存储，则每当重新启动 dcnn 平台时，都需要重新初始化权重。为了克服这些限制，在这项工作中，我们采用了一种新兴的非易失性域-壁内存 (dwm)，它可以实现超高密度，以取代 sram 在基于 scn 的 dnn 中用于重量存储。提出了基于 dwm 的重量存储方法的第一个综合设计优化框架--dw-nnn。我们推导出最佳的内存类型、精度和组织，以及是存储二进制数字还是随机数字。提出了基于 dwm 的权重存储在基于 scn 的卷积层和完全连接层的有效资源共享方案，以实现面积、功耗 (能源) 消耗和应用级精度之间的理想平衡。少

2018 年 2 月 3 日提交;最初宣布 2018 年 2 月。

416. 建议: 1802. 00976 Cs。直流

多伊10.420n/eptcs. 264

关于物联网的体系结构、语言和范式的第一次研讨会

作者:danilo pianini, guido salvaneschi

摘要: 关于**物联网**的架构、语言和范式的第一届研讨会 (alp4iot 2017) 于 2017 年 9 月 19 日在都灵举行。alp4iot 是第十三届综合正式方法国际会议 (ifm 2017) 的卫星活动。该研讨会旨在严格审查**物联网**的正式技术和软件方法的最新技术和最新实践，提出了

悬而未决的问题和挑战，并引发了与会者之间的讨论。不同的观点和背景。物联网带来了互联和智能对象数量和种类的急剧增加。通信能力和计算能力日益嵌入到日常设备中，包括个人智能设备、公共显示器、汽车、无人机和电子标签。事物的这种状态打开了前所未有的一系列研究机会：这类装置的内在分布、流动性、情境性和异质性要求对这些系统的基础有适当的科学认识，也需要新颖软件方法。研讨会就架构、语言、范例和技术等方面提供了原创文章，对面向**物联网**的软件系统具有潜在的实际和理论影响，欢迎采取跨学科的方法。少

2018 年 2 月 3 日提交;最初宣布 2018 年 2 月。

日记本参考:ettcs 264, 2018

417. **建议: 1802. 00917[pdf, ps,其他] cs. it**

小细胞网络中随机调度和循环的延迟分析

作者:杨晓明,王英, tony q. s. quek

摘要: 分析了在随机调度 (rs) 和循环 (rr) 协议下运行的小型蜂窝网络的延迟性能。基于随机几何和排队理论，我们推导出准确而可追溯的平均延迟分布表达式，这解释了随机流量到达、排队交互和数据包重传失败的影响。我们的分析断言，无论流量统计情况如何，rr 在平均延迟方面都优于 rs。此外，在交通拥挤的情况下，rr 的收益更加明显，这证实了会计公平在调度策略设计中的重要性。我们还发现，在相同的延迟中断概率的限制下，rr 能够支持比 rs 更多的用户设备 (ue)，证明它是物联网 (**iot**) 网络流量调度策略的合适候选设备。少

2018 年 5 月 30 日提交;v1 于 2018 年 2 月 3 日提交;最初宣布 2018 年 2 月。

418. **建议: 1802: 0000[pdf,其他] Cs。镍**

qos 感知动态雾服务资源调配

作者:ashkan yousefpour, ashish patil, genya ishigaki, inwoongkim , xiwang, haki c. cankaya, 序言 zhang, weishengxie, jason p. jue

摘要: 物联网 (**iot**)、云计算和大数据领域的最新进展归因于越来越多的复杂和有用的应用程序的兴起。随着**物联网**在我们的日常生活中变得更加普遍，预计将出现更多的数据密集型、延迟敏感和实时应用程序。确保这些应用程序在带宽和低延迟方面的服务质量 (qos) 至关重要，雾计算已被视为满足这些 qos 要求的主要使能因素之一。雾使计算、存储和网络资源更贴近用户。本文首先介绍了动态雾服务配置问题，即在雾节点上动态部署新的雾类服务 (应用程序) 或释放已部署在雾节点上的服务，以满足 qos 要求。约束。将该问题表述为 inlp 任务，并提出了两个启发式方法来有效地解决该问题。最后，利用基于现实世界流量轨迹的仿真和作为**物联网**应用的移动增强现实对启发式进行了评价。少

2018 年 2 月 2 日提交;最初宣布 2018 年 2 月。

评论:10 页，技术报告，工作进行中

419. **建议: 1802. 00152[pdf,其他] Cs。铬**

控制: 利用 cpsbot 设计和实现网络物理攻击僵尸网络

作者:daniele Antonioli, giuseppe bernieri, nils ole tippenhauer

摘要: 最近，米拉伊和波斯雷等僵尸网络大规模地瞄准**了物联网**设备。我们考虑僵尸网络对网络物理系统 (cps) 的攻击，这些攻击需要先进的功能，如实时控制物理过程。传统僵尸网络不适合实现此目标，主要是因为它们缺乏过程控制能力，没有针对低延迟

通信进行优化，并且机器人通常不利用本地资源。我们认为，这类攻击将需要网络物理僵尸网络。网络物理僵尸网络需要协调和异构的机器人，能够执行对抗性控制策略，同时受目标 cps 的约束。在这项工作中，我们提出了 cpsbot，一个框架，以建立网络物理僵尸网络。我们提供了一个针对集中控制系统的集中 cpsbot 和针对系统分布式控制的分散 cpsbot 的示例。我们将 mqtt 用于 c & amp; c 信道，并将 mobustctctcp 作为目标网络协议，实现了以前的 cpsbot，并利用它对真实和模拟的水分配发起了几次攻击。我们通过对 cps 的分布式答复和分布式模拟攻击来评估我们的实现，并表明具有可忽略不计的延迟的恶意控制是可能的。少

2018 年 1 月 31 日提交;最初宣布 2018 年 2 月。

420. 建议: 1801 1.10391[pdf] Cs。铬

物联网取证: 挑战与案例研究

作者:saad alabdulsalam, kevin schaefer, tahar kechadi , nhien-an le-khac

摘要: 今天是物联网 (**iot**) 的时代，数以百万计的机器，如汽车、烟雾探测器、手表、眼镜、网络摄像头等，都正在连接到互联网上。具有远程访问能力的机器数量不断增加，以监控和收集数据。这种发展一方面使人类生活更舒适、更方便，另一方面也提出了安全和隐私问题。然而，当**物联网**设备涉及犯罪场景时，这一发展也给数字调查员带来了挑战。事实上，目前文献中的研究重点是**物联网环境的**安全和隐私，而不是**物联网**设备的取证获取和分析方法或技术。因此，本文首先讨论了**与物联网**取证有关的不同方面，然后重点讨论了当前的风险。我们还将物**联网**设备智能设备的法医方法描述为一个案例研究。我们分析从智能设备中检索到的法医文物，并讨论与**物联网**取证中的挑战相一致的证据.

2018 年 1 月 31 日提交;最初宣布 2018 年 1 月。

421. 建议: 1801 1.10340[pdf] cse

网络物理微服务: 基于 iot 的制造系统框架

作者:kl 一切 anthamboulidis, danai c. vachtsevanou,亚历山大 Kleanthis

摘要: 最近在信息和通信技术方面的进步使制造业的发展能够满足社会的新要求。网络物理系统、物**联网** (**iot**) 和云计算在第四次工业革命 (工业 4.0) 中发挥着关键作用。微服务体系结构已发展成为 soa 的替代方案，并有望解决软件开发中的许多挑战。本文采用了微服务的概念，描述了以网络物理微服务为关键结构的制造系统框架。制造工厂的工艺被定义为采用编排或编排模式的原始网络物理服务的组合。**物联网**技术用于系统集成，模型驱动工程用于工业工程师的半自动化开发过程，因为他们不熟悉微服务和**物联网**。两个案例研究证明了该方法的可行性。少

2018 年 4 月 1 日提交;v1 于 2018 年 1 月 31 日提交;最初宣布 2018 年 1 月。

评论:8 页, 7 个数字, 1 个表

422. 建议: 1801. 10207[pdf,其他] Cs。Db

a 树: 一个有界近似索引结构

作者:alex galakatos, michael markovitch, carsten binnig, rodgo fonseca, tim kraska

摘要: 索引结构是 dba 利用的最重要的工具之一，以提高分析和事务性工作负载的性能。然而，随着在包括自主车辆、物**联网** (**iot**) 设备和电子商务网站在内的各种领域不断生成的数据的激增，构建多个索引通常会变得令人望而却步,消耗宝贵的系统资源。事实上，最近的一项研究表明，作为 tpc-c 基准的一部分创建的索引可以占最先进的

内存 dbms 中可用总内存的 55%。此开销会消耗有价值且昂贵的主内存，并限制数据库可用于存储新数据或处理现有数据的空间量。本文提出了一种新的近似指数结构--a 树。我们索引的核心是一个可调整的错误参数，它允许 dba 平衡查找性能和空间消耗。为了在这一权衡中导航，我们提供了一个成本模型，可帮助 dba 在 (1) 查找延迟要求 (例如, 500ns) 或 (2) 存储预算 (例如, 100mb) 的情况下选择适当的错误参数。使用各种实际数据集，我们表明我们的索引结构能够提供与完整索引结构相比较的性能，同时将存储占用空间减少数量级。少

2018 年 1 月 30 日提交;最初宣布 2018 年 1 月。

评论:12 页

423. **xiv:1801. 09224[pdf,其他] Cs。镍**

利用蠕变波传播保护身体上的物联网设备

作者:王伟,杨琳,张谦,姜涛

摘要: 机上设备是物联网 (**iot**) 愿景的固有组成部分，可提供以人为本的服务。这些主体**性物联网**设备主要是嵌入式设备，缺乏复杂的用户界面，以方便传统的基于预共享密钥的安全协议。在这种真实世界安全漏洞的推动下，本文提出了 securetag，该系统旨在通过将物理层 (phy) 信息与上层协议集成，从而为攻击提供深度防御。安全标签的基础是一种信号处理技术，它提取蠕动波特有的传播特性，以识别人体上的设备。在无意中听到可疑传输后, securetag 启动了基于 phy 的质询者响应协议，以减轻攻击。我们在不同的商用现成 (cots) 可穿戴设备和智能手机上实施我们的系统。在实验室、公寓、商场和室外区域进行了广泛的实验，涉及 12 个不同年龄段的志愿者，以证明我们系统的稳健性。结果表明，我们的系统可以减轻 99.13% 的主动攻击尝试，同时仅在 5.64 的合法流量上触发错误警报。少

2018 年 1 月 28 日提交;最初宣布 2018 年 1 月。

424. **建议: 1801. 09109[pdf, ps,其他] cs. it**

光谱和节能无线动力物联网网络: noma 还是 tdma?

作者:吴庆清,陈文,德瑞克·永权,罗伯特·肖伯

摘要: 无线供电通信网络 (wpcns) 被设想为未来物联网 (iot) 的一个有希望的解决方案，在这种网络中，多个能源有限的设备首先在下行链路中采集能量，然后在上行链路传输信息).同时，提出了非正交多址访问 (noma)，通过允许在同一频谱下多个用户的并发传输，提高了第五代 (5g) 网络的系统频谱效率 (se)。因此, nova 最近被考虑用于基于 wpcn 的**物联网**网络的上行链路，并配备了大量的设备。然而, noma 中的同步传输也可能在实际应用中产生更多的传输能耗以及电路能耗，这对于受能源限制**的物联网设备**至关重要。因此，与正交多重接入方案 (如时分多重访问 (tdma)) 相比，在这种情况下, se 是否可以改进和/或使用 noma 可以降低总能耗仍是未知数。为了回答这个问题，我们首先推导出最佳时间分配，以最大限度地提高基于 tdma 的 wpcn (t-wpcn) 和基于 nma 的 wpcn (n-wpc 子) 的 se。随后，我们分析了这两个网络的总能耗以及最大 se。令人惊讶的是，人们发现, n-wpcn 不仅消耗更多的能量，而且比 t-wpc 子更低的光谱效率。仿真结果验证了我们的理论发现，揭示了多用户 noma 系统中的基本性能瓶颈，即 "最严重的用户瓶颈问题"。少

2018 年 1 月 27 日提交;最初宣布 2018 年 1 月。

评论:被 ieee tvt 接受

425. **建议: 1801. 08648[pdf,其他] Cs。直流**

引导流：用于高性能计算的流处理框架

作者:andre luckow, george chantzialexiou, shantenu jha

摘要: 越来越多的科学应用依赖于流处理，以便从科学仪器、模拟和物联网 (**iot**) 传感器的数据馈送中生成及时的见解。流应用程序的开发是一项复杂的任务，需要集成异构、分布式基础架构、框架、中间件和应用程序组件。不同的应用程序组件通常使用不同的抽象和框架用不同的语言编写。通常，需要额外的组件 (如消息代理 (如卡夫卡)) 来分离数据的生成和使用，并避免背压等问题。由于数据源引起的可变数据速率、自适应采样技术或网络拥塞、使用不同机器学习算法导致的可变处理负载等因素，流应用程序可能具有极强的动态性。因此，能够响应其中一个因素的变化的应用程序级资源管理至关重要。我们提出了一种 pilot-流式传输，它是一个支持 hpc 基础架构上的流媒体框架、应用程序及其资源管理需求的框架。引导流基于 "试点作业" 概念，使开发人员能够管理复杂流应用程序的分布式计算和数据资源。它使应用程序能够通过在运行时添加删除资源来动态响应资源需求。此功能对于平衡复杂的流管道至关重要。为了解决流应用程序开发和表征的复杂性，我们提出了流式传输微型应用程序框架，该框架支持用于数据生成和处理的不同可插入算法，例如用于重构光源的算法使用不同技术的图像。我们利用微型应用程序框架对上流社会进行评估。少

2018 年 1 月 25 日提交;最初宣布 2018 年 1 月。

评论:12 页

426. xiv:1801. 08206[pdf,其他] cs. it

多伊 10.1109/MSP.2018.2789521

无线通信中的稀疏表示：一种压缩方法

作者:秦志金,范建春,刘元伟, 高悦,杰弗里·叶丽

摘要: 稀疏表示可以有效地在不同的应用中建模信号，以方便处理。在本文中，我们将讨论稀疏表示在无线通信中的各种应用，重点介绍最新的压缩传感 (cs) 启用方法。借助稀疏特性, cs 能够提高第五代 (5g) 网络和物联网 (**iot**) 网络的频谱效率和能源效率。本文从全面概述 cs 原理以及 5g 和**物联网**网络中可能使用的不同稀疏域开始。然后介绍了应用 cs 应对 5g 和**物联网**网络的主要机遇和挑战的最新研究进展，包括认知无线电网络中的宽带频谱传感、**物联网**网络中的数据采集以及大型 mimo 系统中的信道估计和反馈。此外，还确定了 5g 和**物联网**网络稀疏表示的其他潜在应用和研究挑战。本文将为读者提供一个清晰的图片，说明如何利用稀疏特性在不同的应用中处理无线信号。少

2018 年 6 月 24 日提交;v1 于 2018 年 1 月 24 日提交;最初宣布 2018 年 1 月。

评论:本文已被 ieee 信号处理杂志所接受。请引用本文的格式版本，可 https://ieeexplore.ieee.org/document/8350399/

日记本参考:z. qin, j. fan, y. liu, y. g. g. li, "无线通信的稀疏表示：一种压缩传感方法", 载于 ieee 信号处理杂志，第 35 卷，第 3 期, 40-58 页, 2018 年 5 月

427. 建议: 1801. 08024[pdf,其他] Cs。Hc

用于多目标自动自动和机器学习技术合作研究的集体知识工作流

作者:grori fursin, anton lokhmotov, dmitry savenko, eben upton

摘要: 无论是小型**物联网**设备还是 exascale 超级计算机，开发高效的软件和硬件都从未像现在这样困难。除了不断增长的设计和优化复杂性外，还存在着更根本的问题，如

缺乏有效的软件硬件协同设计所需的跨学科知识，以及学术界之间的技术转让差距越来越大和工业。我们介绍我们的新的教育计划，以解决这些问题，开发集体知识 (ck)，一个统一的实验框架，计算机系统的研究和开发。我们使用 ck 向社区传授如何使他们的研究工件和实验工作流程便携、可复制、可定制和可重复使用，同时实现可持续的研发并促进技术转让。我们还演示了如何重新设计多目标自动调整和机器学习，作为一个可移植和可扩展的 ck 工作流。这样的工作流使研究人员能够试验不同的应用程序、数据集和工具;跨不同平台的多方联动源实验;分享实验结果、模型、可视化;使用简单的 json api 逐渐公开更多的设计和优化选择;并最终建立在彼此的发现之上。作为第一个实用步骤，我们在树莓 pi 3 设备上实现了可自定义的编译器自动调整、众包优化，将执行时间和代码大小缩短了 40%，并应用机器学习来预测优化。我们希望这种方法将帮助教学生如何在彼此工作的基础上，为新出现的工作负载启用高效和自我优化的软件/硬件/模型堆栈。少

2018 年 1 月 19 日提交;最初宣布 2018 年 1 月。

评论:交互式 ck 报告: http://cKnowledge.org/rpi-crowd-tuning;包含工件的 ck 存储库: https://github.com/ctuning/ck-rpi-optimization-results;图共享数据存档: https://doi.org/10.6084/m9.figshare.5789007.v2

428. 建议: 1801 1.07947[pdf,其他] Cs。Db

tritandb:time 系列快速物联网分析

作者:尤金·肖德东瑞斯·蒂罗帕尼斯、新王、温迪厅

摘要: 数据的有效管理是实现物联网 (**iot**) 潜力的重要前提。考虑到结构化时间序列 **iot** 数据的数量众多，有两个问题是解决异构事物之间数据集成的困难，以及在资源受限的情况下提高数据库之间的接收和查询性能事物和在云中。本文研究了公共**物联网**数据的结构，发现大多数数据具有独特的扁平、宽和数值特性，混合了均匀和不均匀间隔的时间序列。我们研究遥测数据时间序列数据库的进展，并将这些发现与微观基准相结合，以确定最佳压缩技术和存储数据结构，从而为**设计针对物联网优化的新解决方案提供信息**数据。即使在资源受限的事物上，低开销的查询转换方法也允许我们利用丰富的数据模型 (如资源描述框架 (rdf)) 在优化的存储之上实现互操作性和数据集成。我们的解决方案 tritandb 展示了**物联网**方案中许多最先进的数据库上的物和云硬件性能的数量级改进。最后，我们描述了 tritandb 如何支持**对物联网**时间序列数据的各种分析，如预测。少

2018 年 1 月 24 日提交;最初宣布 2018 年 1 月。

429. 建议: 1801 1.07379[pdf, ps,其他] Cs。铬

通过深度学习实现移动人群传感的安全

作者:梁晓,姜东华,徐东进,安宁安

摘要: 为了刺激物联网 (**iot**) 应用 (如医疗保健和交通监控) 的安全传感，移动人群传感 (mcs) 系统必须在以下期间应对安全威胁，如干扰、欺骗和伪造传感攻击。大规模动态和异构网络中的传感和信息交换过程。本文研究了安全移动人群传感，介绍了如何使用深度学习 (dl) 方法，如堆叠自动编码器 (sae)、深神经网络 (dnn) 和卷积神经网络 (cnn) 来改进 mcs 安全方法，包括 mcs 中的认证、隐私保护、假传感对策、入侵检测和抗干扰传输。我们讨论了与传统安全方案相比，这些基于 dl 的方法的性能提升，并确定了在实际 mcs 系统中实现这些方法所需应对的挑战。少

2018 年 1 月 22 日提交;最初宣布 2018 年 1 月。

评论:7 页, 5 个数字

430. 建议: 1801 1.07[pdf] Cs。Hc

多伊 10.1016/j.clsr.2017.12.004

避免不安全的工业事物的互联网

作者:lachlan urquhart, derek m 甘利

文摘: 安全事件，如有针对性的分布式拒绝服务 (ddos) 攻击电网和黑客攻击工厂工业控制系统 (ics) 正在增加。本文从技术和监管两个角度出发，揭示了工业物联网面临的新出现的安全风险所在。2016 年欧洲联盟 (欧盟) 网络和信息安全指令 (nis) 和 2016 年一般数据保护条例 (gdpr) (均将于 2018 年 5 月实施) 正在带来法律变革。我们利用新兴智能能源供应链的案例研究，对所发挥的安全问题的广度以及监管对策进行了构建、界定和整合。我们认为，工业**物联网**带来了四个安全问题，即: 欣赏从离线基础设施向在线基础设施的转变;管理安全的时间维度;解决执行方面的差距，以促进最佳做法;并参与基础设施的复杂性。我们的目标是暴露风险，促进对话，避免出现不安全的工业物互联网少

2018 年 1 月 22 日提交;最初宣布 2018 年 1 月。

日记本参考:计算机法律和安全审查, 2018 年

431. 建议: 1801 1.07189[pdf] Cs。Hc

多伊 10.1007/00779-017-1069-2

实现国内物联网的数据可移植性

作者:lachlan urquhart, neelima Sailaja, derek mauley

摘要: it 设计界在监管新兴信息技术方面发挥着越来越大的作用。2016 年欧盟一般数据保护条例 (gdpr) 第 25 条规定，这是一个严格的法律依据，规定了个人数据驱动技术在设计和默认 (pbd) 方面对信息隐私的需求。在此背景下，我们围绕 gdpr 中新设立的数据可移植性法律权利 (rtdp)，研究法律、商业和技术方面的观点。我们的动机是迫切需要解决物联网 (**iot**) 带来的监管挑战。我们需要找到渠道，在实践中支持对用户的这些新法律权利的保护。在第一部分中，我们将更详细地介绍物联网和信息 pbd。我们简要回顾**了物联网**带来的监管挑战，以及围绕设计信息隐私监管响应的性质和实际挑战。在第二部分中，我们深入了解 rtdp 的法律性质，确定它在实践中对 it 设计人员的要求，但也确定了对权利的限制以及它与**物联网**的关系。在第三部分中，我们重点介绍了能够支持实现这项权利的技术方法。我们考虑了数据管理架构、工具和平台的最新情况，这些架构、工具和平台可以提供可移植性、提高透明度和用户对数据流的控制。在第四部分中，我们将我们的观点汇集在一起，反思将影响 rtdp 实践实施的技术、法律和商业障碍和机遇，以及这些关系如何影响新兴**的物联网**创新和业务模式。最后，我们简要总结了**物联网**中 rtdp 和 pbd 的未来。少

2018 年 1 月 22 日提交;最初宣布 2018 年 1 月。

日记本参考:个人和无处不在的计算，斯普林格, 2017

432. 建议: 1801 1.07 185[pdf] Cs。Hc

白色物品发出的白噪音? 国内环境计算的概念与实证分析

作者:拉奇兰·厄克特

摘要: 在本章中，我们从概念和经验两方面考虑了环境国内计算系统的出现。我们严格评估后桌面计算的愿景，特别关注一个当代趋势: 物联网 (**iot**)。我们研究了这一术语的

争议性质，审视了类似技术的历史轨迹，以及它们可能带来的监管问题，特别是在家庭中。我们还希望通过设计来解决新出现的隐私监管解决方案，拆包它所面临的实际挑战。我们贡献的新颖性源于通过一套经验观点转向实践。我们提出的研究结果，记录了实践经验和领先的专家在技术法律和设计。少

2018 年 1 月 22 日提交;最初宣布 2018 年 1 月。

评论:25 页

433. 建议: 1801 1.07 168[pdf] Cs。Hc

在物联网中表现出明显的责任

作者:lachlan urquhart, tom lodge, andy crabtree

文摘: 本文探讨了对数据保护负责的重要性，以及如何将其构建到物联网 (**iot**) 中。需要将问责**制纳入物联网**的动机是分布式数据流的不透明性质、同意机制不足以及缺乏接口，无法最终用户控制支持互联网的设备的行为。由于缺乏问责制，最终用户无法对其个人数据进行有意义的接触，并对建立用户对**物联网**的信任和数字经济的互惠发展构成了关键挑战。欧盟《2016 年一般数据保护条例》 (gdpr) 旨在通过强制要求迅速发展的技术生态系统承担责任来解决这一特殊问题。在这样做的过程中，它为数据控制器规定了新的责任，包括设计和默认数据保护，以及新的数据主体权利，如数据可移植性。虽然 gdpr 在技术上是中立的，但预计实现这一愿景将转向有效的技术发展。因此，本文探讨了问责制的概念、如何将其转化为**物联网**的系统设计建议，以及**物联网**数据库如何将关键数据保护原则付诸实施。少

2018 年 1 月 22 日提交;最初宣布 2018 年 1 月。

评论:31 页

434. 建议: 1801.07090[pdf,其他] Cs。铬

多伊 10.1109/CTTE.2017.8260940

智能家居领域中的无线物联网协议安全性综述

作者:stefan marksteiner, víctor juan expósito jiménez, heribert valant, herwig zeiner

摘要: 随着**物联网**在智能技术中的应用越来越广泛，其协议的混乱也越来越令人困惑。更严重的是，这些协议的严重安全缺陷变得很明显，因为上市时间是一个关键因素，满意是以不太彻底的安全设计和测试为代价的。这尤其适用于智能家居领域，在智能家居领域，消费者驱动的市场需要快速而廉价的解决方案。本文概述了**物联网**应用领域，讨论了智能家居最重要的无线**物联网**协议，即 knx-rf、enocean、zigbee、z-wave 和线程。最后，它描述了上述协议的安全功能，并将它们相互比较，就谁的协议更适合安全的智能家居提出了建议。少

2018 年 1 月 22 日提交;最初宣布 2018 年 1 月。

评论:8 页, 4 个数字

日记本参考:2017 年第十三届 ctte 和第十届 cmi 物联网商业模式、用户和网络联合会议论文集

435. 建议: 1801. 06964[pdf,其他] cs. it

5g 动态频谱访问中的机会主义: 一种概念及其在双工中的应用

作者:Jeemin kim, so-minkim, han cha, jinhochoi, Seung-Wooko, chan-byoung chae, seong-lyun kim

摘要: 随着设想中的大规模物联网 (**iot**) 时代, 5g 无线系统面临的挑战之一将是应对前所未有的频谱紧缩。一个潜在的解决方案已经出现在频谱共享的形式, 这偏离了垄断频谱使用系统。本文研究了媒体访问控制 (mac) 作为提高频谱共享技术可行性的一种手段。我们首先以概率的方式量化频谱访问的机会, 这种方法称为机会概率 (op)。在 op 框架的基础上, 我们提出了一种随机 mac 算法, 其中节点的访问是用自己的 op 值随机确定的。作为基于 op 的随机 mac 的一种可能应用, 我们提出了一种混合半双工 (hd)/全双工 (fd) 通信, 其中每一对根据两个对节点的 op 值决定双工模式。这种方法很适合频谱共享系统, 因为它能够根据频谱使用水平灵活地操作频谱访问。通过数值分析, 我们通过实现基于 fpga 的实时样机, 验证了性能增强的可行性。测量和数值结果证实, 该体系结构的系统吞吐量比传统的 lte-tdd (时分双工) 系统高 4 倍。少

2018 年 1 月 22 日提交;最初宣布 2018 年 1 月。

评论:2017 年 12 月在新加坡 ieee 环球公司进行了 9 页、6 位数字的实时演示, 并在 http://www.cbchae.org/提供完整的演示视频

436. 建议: 1801.06679[pdf, ps,其他] cs. it

主要骑行: 一种新的无线电源物联网设备频谱共享模式

作者:康欣,梁英昌,杨静

文摘: 针对具有环境反向散射通信功能的无线功率**物**联网设备, 提出了一种新的频谱共享模型--"骑在主电源 (rop) 上"。rop 的关键思想是, 二次发射机从主信号中获取能量, 然后将其信息位调制到主信号, 并在不违反主系统的情况下将调制信号反射到辅助接收机。干扰要求。与传统的频谱共享模型相比, 提出的 rop 中的二次系统不仅利用了主系统的频谱, 而且利用了主信号来获取能量并传输其信息。本文研究了这种频谱共享系统在衰落信道下的性能。具体而言, 我们通过联合优化主信号的发射功率和二次环境后向散射的反射系数, 最大限度地提高了二次系统的遍历能力。不同的 (实际) 能耗模型、不同的 (峰值) 传输功率约束、不同类型的 (固定可调) 反射系数、不同的主系统的干扰要求 (速率/停机)被考虑。得到了每种情况下的最佳功率分配和反射系数。少

2018 年 1 月 20 日提交;最初宣布 2018 年 1 月。

评论:提交给 ieee trans. 无线通信

437. 建议: 1801. 06623[pdf, ps,其他] Cs。镍

上位机物联网超密集网络的承诺与注意事项

作者:ming ding, david lopez perez

文摘: 本文通过仿真, 从覆盖概率和可靠工作的用户设备 (ue) 的密度等方面对支持物联网 (**iot**) 的上行链路 (ul) 性能进行了评估。通过我们的研究, 我们展示**了 ul iot**udn 将在未来带来的好处和挑战。更详细地说, 对于低可靠性标准, 例如实现 0 db 以上的 ul 信噪比 (snr), 可靠工作的 ue 的密度随着网络致密化而快速增长, 显示了 ul **iot** udn 的潜力。相反, 对于高可靠性标准 (如实现 10 db 以上的 ul snr), 由于单元间干扰过多, 在 udn **中**可靠工作的 ui 密度仍然较低, 在操作 ul iot udn 时应考虑到这一点。此外, 考虑到基站 (bs) 和 ue 之间存在非零天线高度差, 随着部署更多基站的部署, 可靠工作的 ue 密度甚至可能降低。这就需要在 ul **物**联网 udn 中使用复杂的干扰管理方案和梁式操纵技术。少

2018 年 1 月 20 日提交;最初宣布 2018 年 1 月。

评论:将出现在 ieee wcnc2018 中

438. 成果: 1801.06601[pdf,其他] cs. ne

cmis-nn: 用于臂 cortex-m cpu 的高效神经网络内核

作者:赖良珍,苏达,维卡斯·钱德拉

摘要: 深度神经网络在始终在线的**物联网**边缘设备中越来越流行，这些设备可直接从源头上执行数据分析，从而减少了数据通信的延迟和能耗。本文介绍了针对智能物联网边缘设备的 CMSIS-NN，它是为最大限度地提高性能和最大限度地减少针对智能**物联网**边缘设备的臂 cortex-m 处理器上的神经网络 (nn) 应用的内存占用而开发的高效内核。基于 cmis-nn 内核的神经网络推理在运行时/吞吐量方面实现了 4.6 倍的改进，在能源效率方面实现了 4.6X 的改进。少

2018 年 1 月 19 日提交;最初宣布 2018 年 1 月。

439. 建议: 1801. 06552[pdf] Cs。DI

信息与环境的文献遥测: iot 动力推荐系统的评价

作者:吉姆·哈恩

摘要: 物理库环境中的物联网 (**iot**) 基础架构是对数字资源推荐人采取集成、混合方法的基础。**物联网**基础架构为集合中的项目提供移动、动态寻路支持，其中包括基于位置的建议功能。此处的模块化评价和分析澄清了用户根据其位置提出建议的性质，并说明了用户要求提供建议的图书馆主题领域。模块化的移动设计允许在整个全球模块系统中深入探索用户的书目标识符，为作为本研究重点的浏览数据提供背景。介绍了文献学作为图书馆馆藏中**物联网**中间件的一种评价方法。少

2018 年 3 月 29 日提交;v1 于 2018 年 1 月 19 日提交;最初宣布 2018 年 1 月。

评论:10 页, 8 个数字, 6 个表

440. 建议: 1801 1.06 374[pdf, ps,其他] cs. it

物联网分布式天线系统中的节能 swipt

作者:黄玉文,刘梦宇,刘元

摘要: 物联网 (**iot**) 的快速增长极大地增加了无线设备的功耗。同时无线信息和功率传输 (swipt) 是**物联网**设备可持续运行的一个很有前途的解决方案。本文研究了基于 swipt 的分布式天线系统 (das) 中的能效 (ee)，在这种系统中，功率分裂 (ps) 应用于物**联网**器件，通过改变传输来协调能量采集 (eh) 和信息解码 (id) 过程。分布式天线 (da) 端口的功率和**物联网**器件的 ps 比。在单个**物联网**器件的情况下，我们根据 karush-kuhn-tucker (kkt) 条件推导出一些有用的特性，找到了最优的闭式解，该解不需要数值迭代。针对多**物联网**器件，提出了一种有效的次优算法来解决 ee 最大化问题。仿真结果表明，与其他基准方案相比，该方案在单**物联网和多物联网**器件的情况下都能获得更好的 ee 性能。少

2018 年 1 月 19 日提交;最初宣布 2018 年 1 月。

评论:被 ieee 物联网杂志所接受

441. 建议: 1801. 06326[pdf,其他] Cs。镍

普适计算中物理原型的几个方面

作者:stepan sigg

文摘: 本文件总结了过去七年来开展的几次研究活动的成果。连接的主题是普适计算领域中广泛部署的传感器的物理层。特别是，我们关注的是 rf 通道或环境音频。我们开

始这项工作的最初问题是分布式自适应传输波束形成问题。我们一直在寻找一种简单的方法来协调联合传输节点的阶段 (例如传感器或**物联网**节点)。解决这一问题的算法是在参与节点上实现分布式随机优化方法，在该节点上，发射机和接收机遵循迭代问答方案。我们已经能够得到一个进化随机优化器的预期优化时间的尖锐渐近边界，并提出了一个渐近优化的方法。我们从这些物理层算法的工作中学到的一点是，我们所研究的信号是脆弱的，对物理环境变化有感知能力。这些可能是家具、打开或关闭的窗户或门以及个人移动等障碍。这一观察促使我们将无线接口视为普适计算环境中环境变化的传感器。物理层 rf 信号的另一个用途是用于安全应用。我们目前正在努力进一步推动这些提到的方向和新的物理原型领域。特别是，传输时无线信道上的数学运算计算似乎包含了在普适计算领域提高通信和计算效率的良好潜力。少

2018 年 1 月 19 日提交;最初宣布 2018 年 1 月。

442. **建议: 1801 1.06[pdf, ps,其他] Cs。铬**

基于机器学习的物联网安全技术

作者:梁晓,万晓月，陆晓珍,张延勇，吴迪

摘要: 将各种设备集成到网络中以提供高级智能服务的物联网 (**iot**) 必须保护用户隐私，并解决欺骗攻击、拒绝服务攻击、干扰和窃听等攻击。本文研究**了物联网**系统的攻击模型，并回顾了基于机器学习技术的**物联网**安全解决方案，包括监督学习、无监督学习和强化学习。我们专注于基于机器学习的**物联网**认证、访问控制、安全卸载和恶意软件检测方案，以保护数据隐私。在本文中，我们讨论了在实际**物联网**系统中实现这些基于机器学习的安全方案所需解决的挑战。少

2018 年 1 月 18 日提交;最初宣布 2018 年 1 月。

443. **建议: 1801. 05394[pdf, ps,其他] Cs。Lg**

通过自动功能学习进行时间序列分割

作者:李伟汉,豪尔赫·奥尔蒂斯，高本军,李鲁比

摘要: 近年来，物**联网** **(iot)** 应用越来越流行，应用范围从建筑能源监控到个人健康跟踪和活动识别。为了利用这些数据，必须大规模地进行自动知识提取----我们将观测到可解释的状态和转换进行映射。因此，我们看到许多最近的**物联网**数据集包含注释，其中包含指定状态的人工专家，在数据序列中记录为一组边界和关联标签。这些数据可用于构建自动标记算法，从而像专家那样生成标签。在这里，我们将人类指定的边界称为断点。传统的更改点检测方法只查找统计可检测的边界，这些边界被定义为数据序列生成参数的突然变化。然而，我们观察到，断点发生在更微妙的边界上，这些边界是不平凡的，可以用这些统计方法来检测。在这项工作中，我们提出了一种新的无监督方法，基于深度学习，它优于现有技术，并以更高的精度学习更微妙的断点边界。通过对各种现实数据集的广泛实验--包括人类活动传感数据、语音信号和脑电图 (eeg) 活动轨迹--我们展示了我们的算法在实际应用中的有效性。此外，我们还表明，与以前的方法相比，我们的方法实现了更好的性能。少

2018 年 1 月 26 日提交;v1 于 2018 年 1 月 16 日提交;最初宣布 2018 年 1 月。

444. **建议: 180004964[pdf,其他] Cs。镍**

未来是无证的: 5g 的无证频谱中的共存

作者:suzan bayhan, gürkan gür, anatolij zubow

摘要: 5g 必须满足超密集、可扩展和可定制网络 (如**物联网**) 的要求，同时提高频谱和能源效率。考虑到所设想的应用程序和场景的多样性, 5g 新无线电 (nr) 的一个关键属性是灵活性: 灵活的 ul/dl 分配、带宽或可扩展的传输时间间隔，最重要的是在不同频段上运行。特别是, 5g 应利用无证频谱中的频谱机会，在需要时随时随地扩展网络容量。然而，无证团伙构成了 "共存网络" 的挑战，这些网络大多缺乏谈判和协调的通信手段。**物联网**系统和应用程序的异质性、巨大的连通性和无处不在性进一步加剧了这一缺陷。因此, 5g 需要提供共存甚至在无证频段中趋同的机制。在这方面, wifi 作为无证频段中最突出的无线技术，既是提高 5g 容量的关键使能因素，也是共享无证频谱 5g 蜂窝网络的竞争对手。在本工作中，我们描述了 5g 中的频谱共享，并提出了关键共存解决方案，主要是在 wifi 的上下文中。我们还强调机器学习的作用，认为机器学习通过提供必要的情报和适应机制，对于实现共存和趋同目标至关重要。少

2018 年 1 月 15 日提交;最初宣布 2018 年 1 月。

评论:7 页, 4 个数字

445. **建议: 180.1. 04416[pdf,其他] Cs。铬**

mof-bc: 一种适用于大型网络的内存优化和灵活的区块链

作者:ali dorri, salil s. kanhere, raa jurdak

摘要: 区块链 (bc) 的不可变性可确保 bc 对存储数据的修改或删除具有弹性。然而，在物联网 (**iot**) 等大型网络中，此功能显著增加了 bc 存储大小，并带来了隐私挑战。在本文中，我们提出了一个内存优化和灵活 bc (mof-bc)，使**物联网**用户和服务提供商能够删除或汇总他们的事务和老化他们的数据，并行使 "被遗忘的权利"。为了增加隐私，用户可以为不同的事务使用多个密钥。为了允许删除存储的事务，需要存储所有密钥，这会使密钥管理和存储复杂化。mof-bc 引入了发电机验证程序 (gv) 的概念，它是生成器验证程序秘密 (gvs) 的签名哈希。gv 更改每个事务，以提供隐私，但由一个唯一的密钥签名，从而最大限度地减少需要存储的信息。提出了一种灵活的交易费用模型和奖励机制，以激励用户参与优化内存消耗。定性安全和隐私分析表明, mof-bc 能够抵御多次安全攻击。评价结果表明，与传统的 bc 实例化相比, mof-bc 可将 bc 内存消耗降低 25%，用户成本降低两个数量级以上。少

2018 年 1 月 13 日提交;最初宣布 2018 年 1 月。

446. **建议: 1801.0 4357[pdf, ps,其他] Cs。直流**

边缘动态异质遗传感知编码协同计算

作者:yaaman keshtkarjahromi, yuxuan xing, hulya seferoglu

摘要 协同计算是一种很有前途的边缘本地化数据处理方法，例如物联网 (**iot**)。合作计算提倡将设备中计算密集型任务划分为子任务，并卸载到邻近的其他设备或服务器。然而，利用协同计算的潜力具有挑战性，主要是由于边缘器件的异构性和时变性。编码计算提倡通过使用擦除代码将数据混合在子任务中，并将这些子任务卸载到其他设备进行计算，由于其更高的可靠性、更小的延迟和更低的通信成本，它最近越来越受到人们的兴趣.本文考虑到边缘器件的异构资源，开发了一个编码协同计算框架，并将其命名为编码协同计算协议 (c3p)。c3p 动态地将编码的子任务卸载到帮助程序中，并且能够适应时变资源。我们表明: (一) c3p 的任务完成延迟非常接近于最优编码的协同计算解决方案, (二) c3p 在资源利用率方面的效率高于 99%与通过模拟和由真正基于 andrid 的智能手机组成的测试台相比, c3p 显著提高了任务完成延迟。少

2018 年 10 月 22 日提交;v1 于 2018 年 1 月 12 日提交;最初宣布 2018 年 1 月。

447. 建议: 1801.04345[pdf,其他] Cs。艾

多伊10.1109/AHS.2017.8046366

基于体现认知的工程协同智能事物

作者:nathalia moraes do nascimento, carlos jose pereira de lucena

摘要: 物**联网** (**iot**) 的目标是将我们周围的任何东西 (如垃圾桶或路灯) 转变为智能的东西。聪明的东西具有传感、处理、交流和驱动的能力。为了实现智能**物联网**应用的目标，如最大限度地降低废物运输成本或降低能耗，应用程序方案中的智能产品必须在没有集中控制的情况下相互合作。在已知的合作自主机器人群设计方法的启发下，我们根据所体现的认知概念对我们的智能事物进行了建模。每一个智能的东西都是一个物理代理，它的主体由微控制器、传感器和执行器组成，大脑由人工神经网络表示。这种类型的代理通常被称为体现剂。这些体现的代理的行为是通过根据应用程序性能触发的进化算法自主配置的。为了说明这一点，我们设计了三个基于进化网络的智能路灯均匀原型。该应用表明，该方法以一种可行的方法对分散智能事物进行建模，具有自主开发和协作的能力。少

2018 年 1 月 12 日提交;最初宣布 2018 年 1 月。

评论:ieee 2017 nasa™自适应硬件和系统会议 (ahs)

448. 新建: 1801 1.04185[pdf,其他] cse

交互语义的参考模型

作者:约翰内斯·里奇,蒂齐安·施罗德

摘要: 了解语义互操作性问题将是未来**物联网**设备和网络物理系统设计的关键。在本文中，我们引入了网络系统交互语义的参考模型，为这种理解提供了基础。系统、功能、信息、行动、事件、互动、过程和意义的概念是以一种很好的方式定义的，以弥合物理学、信息和意义世界之间的差距。应用参考模型对交互接口和组件进行分类，并定义软件层和角色概念。这为更轻松地设计可互操作**的物联网**设备和网络物理系统提供了参考体系结构的重要元素。少

2017 年 12 月 23 日提交;最初宣布 2018 年 1 月。

449. 建议: 1801. 04001[pdf,其他] cs. it

物联网设备的高效 c-ran 随机访问: 通过推荐系统学习链接

作者:奥兹贡·burslioglu, zhidali, chevwei wang, haralabos papadopoulos

文摘: 我们重点研究的**是面向物联网**设备的 c-ran 随机访问协议，这些协议可在大阵列远程无线电头密集网络中产生低延迟的高速有源设备检测。在此背景下，我们研究了了解检测到的设备和网络站点之间链接的优势的问题。特别是，我们开发了推荐系统启发的算法，这些算法利用通过网络收集的随机访问观测来对网络上活动设备和网络站点之间的链接进行分类。我们的模拟和分析揭示了数据驱动方案在广域网上的这种动态链接分类和后续资源分配的潜在优点。少

2018 年 1 月 11 日提交;最初宣布 2018 年 1 月。

评论:本手稿已提交给 2018 年 ieee 国际交流研讨会 (icc 研讨会): 通信网络中机器学习的承诺和挑战

450. 建议: 180003984[pdf,其他] Cs。铬

多伊10.100/2559-018-9543-3

一种基于云的神经科学应用物联网框架中的脑灵感信任管理模型，以确保安全性

作者:mufti mahud, m. shamim kaiser, m. mostafizur rahman, m. arifur rahman, antesar shabut, shamim al-mamun, amir hussain

摘要: 物联网 (**iot**) 和云计算的迅速普及使神经科学家能够收集多级和多渠道的大脑数据，以更好地了解大脑功能、诊断疾病和设计治疗方法。为了确保当前**物联网**和云基础架构支持的端到端 (e2e) 设备之间的安全和可靠数据通信，需要**在物联网**和用户端进行信任管理。本文介绍了一种基于神经模糊的脑激励信任管理模型 (tmm)，以保护**物联网**设备和中继节点的安全，并保证数据的可靠性。提出的 tmm 分别利用自适应神经模糊推理系统和加权加法对节点行为信任和数据信任进行估计，以评估节点的可信度。与现有的基于模糊的 tmm 相比，ns2 仿真结果证实了所提出的 tmm 在识别通信网络中的恶意节点方面的鲁棒性和准确性。随着基于云的**物联网**框架在神经科学研究中的使用日益增多，将拟议的 tmm 集成到现有基础架构中，将确保 e2e 设备之间安全可靠的数据通信。少

2018 年 1 月 11 日提交;最初宣布 2018 年 1 月。

评论:17 页，10 个数字，2 个表

类:K.6.5;i.2;c.3;h.4;j 。3

日记本参考:认知计算，2018

451. **建议: 1801. 03975[pdf,其他] cs. it**

大规模物联网系统中的及时状态更新: 无线上行的分散调度

作者:江志远,巴斯卡·克里希纳卡查,西正,周生，牛志生

摘要: 在典型的物联网 (**iot**) 应用中，中央控制器通过无线多址上行链路从多个终端 (如传感器和显示器) 收集状态更新，一个重要的问题是如何获得及时的状态自主更新。在本文中，状态的及时性是用最近提出的信息年龄指标来衡量的;对该问题的理论和实践两个方面进行了研究: 我们的目标是获得一个最小 aoi 的调度策略，同时，由于信号交换开销，仍然适合分散实现。为此，我们首先考虑了一套独立于到达的更新 (air) 策略;将时间平均 aoi 最小化的最佳策略被证明是具有单数据包 (仅限最新数据包，而其他数据包被丢弃) 缓冲区 (rr-one) 的循环策略。在广义泊松-到达-时间平均 (pasta) 定理的基础上建立了最优性。进一步证明了 rr-one 在大规模**物联网**系统中的所有政策中是渐近最优的。推导了 rr-one 下 aoi 稳态平稳分布。提出了一种完全分散的 rr-one 实现方法，该方法能够适应动态终端的外观。此外，考虑到数据包无法丢弃的情况，还可以使用凸问题的解决方案给出的参数找到数据包的最佳 air 策略。少

2018 年 1 月 11 日提交;最初宣布 2018 年 1 月。

评论:提交给 2018 年 isit 的手稿的扩展版本

452. **xiv:1801. 03890[pdf,其他] Cs。镍**

hopp: 以信息为中心的物联网的强大而有弹性的公开订阅

作者:cenk gündoan, peter kietzmann, thomas c.schmidt, matthias wählisch

文摘: 本文对**物联网**中的 ndn 部署进行了重新审视，重点介绍了传感器和执行器之间的相互作用。此类方案需要高响应能力和受约束节点上的有限控制状态。我们认为，防止数据推送的 ndn 请求-响应模式对于**物联网**网络至关重要。我们为典型的物联网场景提供 hop--lutrit (hopp) ，这是一种强大的发布-订阅方案，针对的是由数百台资源受限设备组成的**间歇性**连接设备的物联网网络。我们的方法将 fib 表限制在最低限度，并且自然支持移动性、临时网络分区、数据聚合和近乎实时的反应性。我们在实际部

署中使用**物联网**实验室测试台对协议进行实验评估，测试台中有不同数量的受限设备，每个设备都通过 ieee 802.15.4 lowpans 进行无线互连。实现是建立在 CCN-lite 与 riot 和支持实验使用各种单跳和多跳方案。少

2018 年 1 月 11 日提交;最初宣布 2018 年 1 月。

453. **建议: 1801. 03648[pdf] cs. cy**

制造业中的无线技术格局: 一个现实的检验

作者:xavier vilajosana, cristina cano , borja martíez, pere tuset, joan melia , ferran adelantado

摘要: 即将到来的工业**物联网**革命，据称是由在工业过程中引入嵌入式传感和计算、无缝通信和海量数据分析所引领的 [1]，在今天似乎是毋庸置疑的。多项技术正在开发中，并正在做出巨大的营销努力，以便在这一工业格局中定位解决方案。然而，我们注意到，制造业几乎没有采用工业无线技术。在本文中，我们试图通过访问制造业和采访这些行业的维护和工程团队来了解目前无线技术使用不足的原因。制造业是非常多样化和专业化的，因此我们试图涵盖一些最具代表性的案例: 汽车行业、制药行业 (起泡)、机床行业 (包括消费和航空航天部门) 和机器人。我们分析了它们的机械技术、应用要求和限制，并确定了采用无线技术的障碍列表。我们发现的最直接的障碍是需要严格遵守标准和认证流程，以及这些程序的谨慎性。但不太明显甚至更有限的障碍是，他们显然不关心低能耗或成本，相比之下，无线研究人员和从业人员认为这些因素至关重要。在这篇现实检查文章中，我们分析了这种不同感知的原因，我们找出了这些障碍，并设计了互补的路径，使工业制造业在未来几年的无线采用成为现实。少

2018 年 1 月 11 日提交;最初宣布 2018 年 1 月。

评论:5 页

报告编号: 01-a

日记本参考:mmtc 通信-行业中的多种无线技术和物联网的前沿，专题: 应用与挑战，第 12 卷，第 6 期, 2017 年 11 月

454. **建议: 1801. 03528[pdf] Cs。铬**

区块链技术在加密货币之外的应用

作者:mahdi h. miraz , maaruf ali

摘要: 区块链 (bc) 是比特币加密货币系统背后的技术，被认为对确保增强安全性和 (在某些实现中，不可追溯) 许多其他领域的不同应用程序的隐私都具有吸引力和关键作用包括物联网 (**iot**) 生态系统。目前，学术界和工业界正在进行密集的研究，将区块链技术应用于多种应用。工作证明 (pow) 是一个加密难题，通过维护被认为是廉洁的数字交易记录表，在确保 bc 安全方面发挥着至关重要的作用。此外, bc 使用可变公钥 (pk) 来记录用户的身份，从而提供了额外的隐私层。不仅在加密货币中成功地采用了 bc，而且在多方面的非货币系统中也得到了成功的实施，例如: 分布式存储系统、位置验证、医疗保健、分散投票等。对最近的研究文章和项目应用进行了调查，以评估 bc 在加强安全性方面的实施情况，确定相关的挑战，并为不列颠哥伦比亚省启用的增强安全系统提出解决方案。少

2018 年 1 月 3 日提交;最初宣布 2018 年 1 月。

日记本参考:计算机新兴技术年鉴 (aetic), 印刷 issn:2516-0281, 在线 issn:2516-029x, 第 1-6 页, 第 2 卷, 第 1 期, 2018 年 1 月 1 日, 可用: http://aetic.theiaer.org/archive/v2n1/p1.pdf

455. **建议: 1801.03290[pdf,其他] Cs。镍**

多伊 10.1109/VTCSpring.2018.8417753

在即将到来的 5g 网络中, 使用多指标上下文感知的汽车高效机器式通信

作者:benjamin sliwa, thomas liebig, robert falenberg, jones pillmann, christian wietfeld

摘要: 即将推出的基于 5g 的通信网络将面临与静态和移动物联网 (**iot**) 系统的大规模部署相关的传输传感器数据量的大幅增加。作为移动传感器的汽车将成为基于云的应用程序 (如预测维护和动态流量预测) 的重要数据源。由于现有通信资源的限制, 预计机器类型通信 (mtc) 的增长将对人与人 (h2h) 通信造成严重干扰。因此, 非常需要更有效的传输方法。本文提出了一种有效传输车辆传感器数据的概率方案, 该方案利用了良好的信道条件, 避免了在预计具有高度资源消耗的情况下传输。在综合现实世界实验中, 对该方案的多个变种进行了评价。通过基于机器学习的多个上下文指标组合, 该方案能够实现比定期传输更高的传感器应用的平均数据速率值, 比定期传输高出 164%。少

2018 年 7 月 31 日提交;v1 于 2018 年 1 月 10 日提交;最初宣布 2018 年 1 月。

评论:最佳学生论文奖

期刊参考: 2018 ieee 第 87 届汽车技术会议 (职业训练局春季)

456. **建议: 1801. 02833[pdf,其他] Cs。镍**

连接嵌入式移动的世界: riot 方法到无处不在的网络的物联网

作者:martine lenders, peter kietzmann, oliver hahm, hauke petersen, cenk gündoan, emmanuel bacelli, kaspar schleiser, thomas c.schmidt, matthiaswählisch

摘要: 物联网 (**iot**) 基于低功耗兼容协议标准, 将互联网扩展到嵌入式世界, 正在迅速发展。创先争优的实现已经证明, 跨网络非常受限的设备是可行的, 但必须依赖于特殊的跨层设计并提供一组简约的功能。然而, 从长远来看,**物联网**设备的专业使用和大规模部署需要功能齐全、简洁、灵活的网络堆栈。本文介绍了将 riot 转变为功能强大的**物联网**系统的网络体系结构, 以实现低功耗无线方案。riot 网络提供了 (i) 具有通用接口的模块化体系结构, 用于插入驱动程序、协议或整个堆栈, (ii) 支持可同时操作的多个异构接口和堆栈, 以及 (iii) gnrc, 其干净的分层,递归组合默认网络堆栈。我们通过在微观基准级别以及通过比较不同平台的物**联网**通信, 对 riot 的通信性能和资源效率进行深入分析。我们的研究结果表明, 尽管 riot 的网络子系统基于明显不同的设计权衡, 但它的性能与 contiki 和 tinyos 相当, 这两个操作系统是首创物联网软件的始作让系统 。平台。少

2018 年 1 月 9 日提交;最初宣布 2018 年 1 月。

457. **建议: 1801. 02811[pdf,其他] Cs。镍**

wi-fi 电话: 物联网的超频 ofdm

作者:王伟,何世月, 杨琳,张谦,姜涛

摘要: 传统的高速 wi-fi 最近成为低功耗物联网 (**iot**) 通信的竞争者。ofdm 继续采用新的**物联网** wi-fi 标准, 因为它的频谱效率可以支持大规模**物联网**连接的需求。虽然

iot wi-fi 标准提供了许多新功能来提高电源和频谱效率，但收发器设计的基本物理层(phy)结构仍然符合其传统的设计原理，即接入点(ap)和客户端使用相同的 ofdm phy。本文认为，目前的 wi-fi phy 设计并没有充分利用 ap 和**物联网**之间固有的不对称。为了填补这一空白，我们提出了一种非对称设计，其中**物联网**设备使用最低功率传输上行数据包，同时将所有解码负担推送到 ap 端。这种设计利用 ap 的足够的功率和计算资源**来交易物联网**设备的传输(tx)功率。实现这种非对称设计的核心技术是 ap 充分利用其高时钟速率来提高解码能力。我们提供了我们的设计实现，并表明它可以通过提高接收器的解码能力来降低**物联网的** tx 功率。少

2018 年 1 月 9 日提交;最初宣布 2018 年 1 月。

458. 建议: 1801. 02351[pdf, ps,其他] cs. it

noma-loha 的博弈论方法

作者:崔金浩

摘要: 非正交多重访问(noma)可以通过利用功率域和连续干扰消除(sic)来提高频谱效率，并可应用于各种传输方案，包括随机访问，这些方案在物联网(**iot**)，以支持许多活动稀少的设备的连接。本文提出了一个将 noma 应用于 aloha 的博弈来确定传输概率。我们考虑了基于能效度量的收益函数，并驱动混合策略纳什均衡(ne)。少

2018 年 1 月 8 日提交;最初宣布 2018 年 1 月。

评论:5 页，提交给 eucnc2018

459. 特别报告: 1801.02154[pdf] Cs。镍

基于 iot 的应用程序中的事件管理的发布订阅框架

作者:truc d. t.nguyen , quan m. b.nguyen, hoang-anh pham

摘要: 传感器和微控制器单元的惊人增长使基于物联网(**iot**)的应用程序中的实时事件监控任务变得更轻松、更实用。为了有效地支持**基于物联网**的应用程序中的事件管理，我们提出了一个基于发布-订阅模型的框架，用于检测**来自物联网**传感器节点的事件并向订阅者发送通知(最终用户)通过互联网、短信和通话。除了从发布-订阅模型继承的优势外，拟议框架的进一步优势是在用户配置方面易于使用，而不需要任何技术技能，还需要安全机制来防止网络入侵，以及最低的硬件资源需求。此外，该框架适用于各种平台，因为它是使用 boost c++ 库和 cmake 开发的。为了对所提出的框架进行评估，我们开发了一个实时事件监控系统的原型，本文也给出了该模型。少

2018 年 1 月 7 日提交;最初宣布 2018 年 1 月。

评论:第十一届东南亚技术大学联合会研讨会，胡志明市, 2017

460. xiv:1801. 02077[pdf, ps,其他] Cs。镍

基于异步多用户深度强化学习的无线系统切换控制

作者:王志,李丽华,徐悦，惠田, 崔树光

文摘: 在本文中，我们提出了一个两层框架，以学习最佳切换(ho)控制器在可能的大规模无线系统支持移动物联网(**iot**)用户或传统的蜂窝用户，其中用户的移动性模式可能是异构的。特别是，我们提出的框架首先将具有不同移动模式的用户设备(ue)划分为集群，其中移动模式在同一个集群中是相似的。然后，在每个集群中，开发一个异步多用户深度强化学习方案，以控制每个集群中的统一 ui 中的 ho 进程，目的是降低 ho 速率，同时确保一定的系统吞吐量。在该方案中，我们使用深度神经网络(dnn)作为每个 ue 通过协作学习学习学习的 ho 控制器。此外，我们使用监督学习在执行

增强学习之前初始化 dnn 控制器，以利用我们已经知道的传统 ho 方案，并减轻随机探索在初始阶段的负面影响。此外，我们还表明，所采用的基于全局参数的异步框架使我们能够使用更多的 ue 更快地进行训练，从而很好地解决可伸缩性问题，从而支持大型系统。最后，仿真结果表明，该框架在 ho 速率方面比最先进的在线方案具有更好的性能。少

2018 年 5 月 8 日提交;v1 于 2018 年 1 月 6 日提交;最初宣布 2018 年 1 月。

评论:12 页、10 个数字和 1 个表

461. 建议: 1801. 01444[pdf,其他] Cs。简历

深度预期: 递归结构在物联网中的轻量化智能移动传感

作者:广陈、舒柳、克嘉仁、中南区、傅长虹、热永欣兹、阿洛斯·克诺勒

摘要: **物联网**时代的快速发展正在塑造移动服务的未来。先进的通信技术实现了异构连接，移动设备将信息广播到所有内容。机器人和车辆连接到云和周围的移动应用将短板载传感器感知系统转移到远程移动传感感知系统。然而，移动传感感知给如何有效地分析和智能地解释 **iot** 数据在任务关键型服务中的泛滥带来了新的挑战。在本文中，我们将这些挑战建模为延迟、数据包丢失和测量噪声，严重降低**了物联网**数据的可靠性和质量。我们将人工智能集成到**物联网**中，以应对这些挑战。我们提出了一种新的架构，利用反复神经网络 (mn) 和卡尔曼滤波来预测对象之间的运动和相互作用。其基本思想是通过经常性网络学习环境动力学。为了提高**物联网**通信的鲁棒性，我们采用卡尔曼滤波的思想，并部署了预测和校正步骤。通过这种方式，架构学会了在不同情况下在预测和测量之间形成一种有偏见的信念。我们通过模拟物联网通信挑战的噪音，通过合成数据集和真实**世界**数据集展示了我们的方法。我们的方法带来了物**联网**智能的新水平。与其他最先进的卷积经常性架构相比，它也非常轻巧，非常适合资源有限的移动应用。少

2018 年 10 月 15 日提交;v1 于 2017 年 12 月 5 日提交;最初宣布 2018 年 1 月。

评论:7 页, 6 个数字, 1 个表

462. 建议: 1801. 01249[pdf, ps,其他] cs. it

绿色物联网的协同环境反向散射通信

作者:杨刚,张乾谦,梁英昌

摘要: 环境反向散射通信 (ambc) 使被动反向散射设备能够使用环境射频信号将信息传输给读者，并已成为绿色物联网 (**iot**) 的一个有前途的解决方案。传统的 ambc 接收器仅对从环境反向散射设备 (a-bd) 中恢复信息感兴趣。在本文中，我们提出了一个合作 ambc (cabc) 系统，其中读者不仅从 a-bd，而且从 rf 源回收信息。首先从扩频和频谱共享的角度建立了 cacb 系统的系统模型。然后，对于平面衰落通道，我们推导出最优最大似然 (ml) 检测器、次优线性检测器以及基于连续干扰抵消 (sic) 的检测器。针对频率选择性衰落信道，提出了基于环境正交频分复用 (ofdm) 载波的 cabc 系统系统模型，并在此基础上导出了低复杂度最优 ml 检测器。对于这两种通道，所提出的检测器的误码率 (ber) 表达式都是以封闭的形式推导出来的。最后，大量的数值结果表明，当 a-bd 信号和 rf 源信号具有相等的符号周期时，提出的基于 sic 的检测器可以在典型的应用场景中实现近 ml 检测性能，而当 a-bd 符号时, a-bd 信号周期比 rf 源符号周期长, cabc 系统中存在的背散射信号可以提高 rf 源信号的 ml 检测性能，这得益于在 a-bd 传输时背散射链路的有益效果比射频源的速率。少

2018 年 1 月 4 日提交;最初宣布 2018 年 1 月。

评论:本期刊论文有 16 页的双栏和 6 个数字，将出现在 ieee 物联网杂志上。题为 "用于具有多个天线的环境反向散射通信的协同接收器" 的会议版本已在 ieee 会议通信 (icc, 2017) 上公布

463. 建议: 1801. 01087[pdf,其他] Cs。直流

跨边缘和云资源的动态事件分析的自适应能量感知调度

作者:rajrup ghosh, siva prakash reddy Simmhan,yogesh simmhan

摘要: 作为物联网 (**iot**) 一部分的传感器的部署日益增多，正在产生数千个事件流。复杂事件处理 (cep) 查询为快速对此类数据源进行决策提供了有用的范例。虽然通常集中在云中，但在现场部署有能力的边缘设备激发了对跨越边缘和云计算的合作事件分析的需求。在这里，我们确定了一个新的问题，即在边缘资源上放置查询和云资源，以动态到达和离开分析数据流。我们将此定义为一个优化问题，以最大限度地减少所有事件分析的总临时，同时满足资源的能量和计算约束。我们针对此类动态数据流提出了 4 个自适应启发式和 3 个重新平衡策略，并使用 100-1000 边缘设备和虚拟机的详细模拟对其进行验证。结果表明，我们的启发式方法提供了 o (秒) 规划时间，在所有情况下都能提供有效、高质量的解决方案，并减少了查询迁移的次数。此外，在这些启发式方法中应用的再平衡策略使制造量显著降低了约 20-25% 。少

2018 年 1 月 3 日提交;最初宣布 2018 年 1 月。

评论:11 页, 7 个数字

464. xiv:1801. 00356[pdf] cs. cy

物联网将如何实现增强个性化的健康?

作者:amit shth, utkarshani jaimini, hong yung yip

摘要: 物联网 (**iot**) 正在深刻地重新定义我们创建、使用和共享信息的方式。健康爱好者和市民越来越多地使用**物联网**技术来跟踪他们的睡眠、食物摄入、活动、重要的身体信号和其他生理观察。此外,**物联网**系统还可持续收集环境和生活区内部与健康相关的数据。这些共同为新一代医疗解决方案创造了机会。然而，解释数据以了解个人的健康状况是具有挑战性的。通常有必要查看该人的临床记录和行为信息，以及影响该个人的社会和环境信息。解释病人的表现也需要了解他对各自健康目标的坚持程度、相关临床知识的应用以及预期的结果。我们采用增强个性化医疗 (aph) 的愿景，利用人工智能 (ai) 技术利用广泛的相关数据和医学知识，以扩展和增强人类健康，呈现不同的增强阶段健康管理策略: 自我监控、自我评价、自我管理、干预、疾病进展跟踪和预测。khealths 技术是 aph 的一个具体体现，它在哮喘和其他疾病中的应用被用来提供插图和讨论技术辅助健康管理的替代方案。还确定了涉及**物联网**和患者生成的健康数据 (pghd) 的若干突出努力，将多式联运数据转换为可操作的信息 (大数据转换为智能数据)。讨论了基于证据的语义感知方法中三个组成部分的作用--语境化、抽象化和个性化。少

2017 年 12 月 31 日提交;最初宣布 2018 年 1 月。

465. 第 (xiv:1712.10210) [pdf, ps,其他] Cs。镍

大型软件定义的物联网的动态负载平衡垂直控制

作者:张连明,钟晓勋,魏业华,杨坤

摘要: 随着全球物联网越来越受到消费者和商业环境的欢迎，网络流管理已成为优化物联网性能的重要课题。僵化的现有物联网 (**iot**) 架构阻碍了当前的流量管理技术，为

大规模**物联网**提供了真正的差异化服务。软件定义的物联网 (**sd-iot**) 是一种将控制平面和数据平面分开的新计算范式，可实现集中式逻辑控制。在本文中，我们首先介绍了 **sdot** 的总体框架，它由两个主要组件组成: sd-**物联网**控制器和 **sdot** 交换机。**sdot** 的控制器使用资源池技术，该池负责对整个网络进行集中控制。**sdad** 的交换机与网关功能集成，网关功能负责数据访问和转发。**sd-物联网**控制器池设计为垂直控制体系结构，包括主控制层和基本控制层。主控制层的控制器 (主控制器) 向上与应用层交互，与基础控制层向下交互，基本控制层的控制器 (基本控制器) 与数据转发层交互。提出了一种基于选择机制的主控制器动平衡算法和基于平衡延迟的基本控制器的动负载平衡算法。实验结果表明，基于选择机制的动平衡算法可以保证主控制器之间消息的一致性，而基于平衡延迟的动态负载平衡算法可以在主控制器之间进行平衡。这些不同的工作负载在基本的控制器。少

2017 年 12 月 29 日提交;最初宣布 2017 年 12 月。

评论:25 页, 10 个数字

466. 第 xiv:1712.09916[pdf,其他] Cs。铬

一种基于神经不可克隆函数 (reram puf) 的软件定义无线网络认证安全性的方法

作者:fatemeh afghah, bertrand ambou, masih abedini, sherali Zeadally

摘要: 物联网 (**iot**) 网络中与互联网连接的无处不在的无线设备数量呈指数级增长，这突出表明在软件定义的大型网络中，需要一种新的数据流管理模式无线网络 (sdwn)。**物联网**设备的有限功耗和计算能力以及 sdwn 的集中管理和决策方法给网络带来了一整套全新的安全威胁。特别是, sdwn 中的控制器和转发设备之间的身份验证机制是保密和完整性两个方面的关键挑战。考虑到网络的大规模和异质性以及部署成本以及由此产生的安全漏洞，基于公钥基础结构 (pki) 的传统身份验证协议对于这些网络来说已经不够了密钥分发和存储。我们提出了一种新的基于物理不克隆函数 (puf) 的安全协议，称为硬件安全原语，以增强 sdwn 中的身份验证安全性。在这种方法中，数字 puf 是使用嵌入在大多数**物联网**设备中的电阻式随机存取存储器 (reram) 纳米材料的固有随机性进行开发的，以便在这些网络中实现安全的身份验证和访问控制。这些 puf 是基于一种新的多状态方法开发的，在这种方法中，由于环境中的物理变化而产生的自然漂移预计将减少在不同情况下测试的压力-响应对的 pof 的潜在误差。我们还提出了一种基于 puf 的 pki 协议，以确保 sdwn 中控制器的安全。实验结果对所开发的基于 reram 的 puf 的性能进行了评价。少

2017 年 12 月 21 日提交;最初宣布 2017 年 12 月。

评论:16 页, 10 个数字，提交给斯普林格国际无线信息网络杂志

467. 第 1712.0958[pdf,其他] Cs。简历

基于网格化超级像素的内存高效深显著对象分割网络

作者:caglar aytekin, x 兴阳 ni, francesco cricri, lixinfan, emre aksu

摘要: 采用像素化标记任务的计算机视觉算法，如语义分割和突出目标检测，随着深度学习的结合，精度显著提高。深度分割方法稍微修改和微调了具有数亿参数的预先训练的网络。在这项工作中，我们质疑是否需要有这样的内存要求网络的突出对象分割的具体任务。为此，我们提出了一种从零开始学习内存效率网络的方法，只在突出的对象检测数据集上对其进行培训。我们的方法对图像进行编码，使其成为覆盖的超级像素，从而同时保留对象边界和常规像素的连接规则。这种表示使我们能够使用在常规网格上运行的卷积神经网络。通过使用这些编码的图像，我们只使用其他深突出对象检测网络

所具有的参数数量的 0.048%--来训练一个内存高效的网络。我们的方法显示了与最先进的深突出物体检测方法的可比准确性，并为其提供了更快、更高效的内存替代方法。由于其易于部署，这样的网络更适合于内存有限设备 (如移动电话和**物联网**设备) 中的应用程序。少

2018 年 5 月 22 日提交;v1 于 2017 年 12 月 27 日提交;最初宣布 2017 年 12 月。

评论:6 页，提交给 2018 年 mmsp

468. 第 1712.09347[pdf,其他] cs. cy

智能雾：可穿戴物联网中无监督群集分析的雾计算框架

作者:debanjan borthakur, harishchandra dubey, nicolasconstant, leslie mahler, kunal mankodiya

摘要: 在智能远程保健中越来越多地使用可穿戴设备，从而产生异质医疗大数据。云和雾服务处理这些数据，以协助临床程序。基于**物联网**的电子医疗服务从高效的数据处理中获益匪浅。本文提出并评价了低资源机器学习在保持在可穿戴设备附近的低资源机器学习的应用，以促进智能医疗。在最先进的电信系统中，信号处理和机器学习模块部署在云中处理生理数据。我们开发了一个基于 f 因为 f 开始的无监督机器学习大数据分析的原型，用于发现生理数据中的模式。我们使用英特尔爱迪生和树莓派作为雾计算机在建议的架构。我们对帕金森病 (pd) 患者家庭监测中的真实病理语音数据进行了验证研究。提出的体系结构采用机器学习来分析从 pd 患者佩戴的智能手机中获得的病理语音数据，结果表明，所提出的体系结构对于低资源临床机器学习具有广阔的应用前景。通过将机器学习方法从云后端转换为早期计算设备 (如忘记)，它可用于可穿戴物联网中的其他应用程序,以满足智能远程健康方案的需要。少

2017 年 12 月 24 日提交;最初宣布 2017 年 12 月。

评论:5 页, 3 个数字. 第五届 ieee 全球信号和信息处理会议

469. 第: 1712.09052[pdf] cs.PL

pwct：物联网和云计算应用与系统的视觉语言

作者:mahmoud s. fayed, muhammad al-qurishi, atif alamri, ahmad a. al-daraseeh

摘要: 开发**物联网**、数据计算和云计算软件需要不同的编程技能和不同的编程语言。这给许多需要雇用许多程序员来开发完整解决方案的公司和研究人员带来了问题。这个问题直接关系到财务成本和开发时间，是许多研究项目非常重要的因素。本文提出了一种无需直接编写文本代码即可开发**物联网**、数据计算和云计算应用与系统的 pwct 可视化编程工具。使用 pwct 可提高工作效率，并为研究人员提供一个可视化编程工具来开发不同的解决方案。少

2017 年 12 月 25 日提交;最初宣布 2017 年 12 月。

470. 第: 1712.08996[pdf,其他] Cs。铬

基于 api 方法序列的深度学习的 android 恶意软件检测

作者:elmouatez billah karbab, mourad debbabi , abdelouahid derhab, djedjiga mouheb

摘要: .. 。自过去几年以来，操作系统经历了极高的人气。这一占主导地位的平台不仅在移动世界中站稳脚跟，而且在物联网 (**iot**) 设备中也确立了自己的地位。然而，这种人气是以牺牲安全性为代价的，因为它已经成为恶意应用的诱人目标。因此，越来越需要复杂的.. 。更多

2017 年 12 月 24 日提交;最初宣布 2017 年 12 月。

评论:17 页，提交给 elsevier 数字调查杂志

471. 第 1712.08768[pdf, ps,其他] Cs。镍

基于学习的能量收集物联网设备的计算卸载

作者:明辉敏,徐东进,梁晓，唐玉良,吴迪

摘要: 物联网 (**iot**) 设备可以应用移动边缘计算 (mec) 和能量采集 (eh)，为计算密集型应用提供令人满意的体验质量，并延长电池寿命。本文研究了具有多个 mec 设备 (如基站和接入点) 的无线网络中具有能量采集的**物联网**设备的计算卸载问题，这些设备的计算资源和接入点各不相同，每个网络的计算资源和无线电都不同。通信能力。我们提出了一个强化学习计算卸载框架，为**物联网**设备选择 mec 设备，并根据当前的电池电量、以前对每个 mec 设备的无线电带宽和预计的收获能量的数量。针对**物联网**器件，提出了一种基于 "热启动" q 学习的计算卸载方案，以实现最佳的卸载性能，而不了解 mec 模型、能耗和计算延迟模型。提出了一种基于快速深度 q 网络 (dqn) 的卸载方案，该方案结合深度学习和热启动技术，加快了 q 学习的学习速度。结果表明，该方案在经过足够长的学习时间后，可以实现最优的卸载策略，并在两种典型的 mec 方案下提供其性能边界。对于使用无线功率传输捕获环境射频信号以为**物联网**电池充电的**物**联网设备，将进行模拟。仿真结果表明，与基准相比，基于 dqn 的快速卸载方案降低了能耗，降低了计算延迟和任务降比，提高**了物联网**器件在动态 mec 中的利用率。基于 q 学习的卸载。少

2017 年 12 月 23 日提交;最初宣布 2017 年 12 月。

472. 第: 1712.08583[pdf,其他] Cs。铬

不同状态下认证的 ppg 生物识别技术评价

作者:umang yadav, sherif n abbas, Dimitrios hatzinakos

摘要: 在所有医学生物特征中，光导运动仪 (ppg) 是最容易获得的。ppg 记录血量的变化，只需结合光发射二极管和光电二极管从身体的任何部分。借助**物联网**和智能家居的渗透, ppg 录制可以轻松地与其他重要的可穿戴设备集成。ppg 代表了每个人的血流动力学和心血管系统的特殊性。本文提出了一种基于 ppg 的生物识别非基准方法。ppg 信号是一种生理信号，随着身体压力和时间的推移而改变。为了鲁棒性，不能忽视这些变化。虽然以前的大部分作品只集中在单期会议上，但本文展示了利用连续小波变换对 ppg 生物识别技术进行的广泛的性能评价。cwt) 和直接线性判别分析 (ddda)。

在不同的状态和数据集中进行评估时,0。5%-6%实现了 45-60 它的平均训练时间。

我们基于 cwt/ddda 的技术优于所有其他降维技术和以往的工作。少
2017 年 12 月 22 日提交;最初宣布 2017 年 12 月。

评论:2018 年在第 11 届 iaprieee 生物鉴别技术国际会议上接受.

473. 第 (xiv:1712.08 296)[pdf,其他] Cs。艾

物联网中的智能设备发现-实现机器人社会

作者:james sunthonlap, phuoc nguyen, zilong ye

摘要: 物联网 (**iot**) 不断发展，可随时随地以类似互联网的结构连接数十亿智能设备，从而实现各种应用程序、服务以及人与对象之间的交互。在未来，智能设备应该能够自主地发现具有所需功能的目标设备，并生成一组不受人类监督甚至想象的全新服务和

应用程序。智能设备的普及及其设计和功能的异质性引起了一个主要问题：智能设备如何有效地发现所需的目标设备？在本文中，我们提出了一种社会感知和分布式（sand）方案，该方案可在**物联网**中实现快速、可扩展和高效的设备发现。提出的 sand 方案采用了一种新的器件排序标准，测量器件的程度、社会关系多样性、聚类系数和相互关系。根据设备排名标准，可以引导发现请求通过位于网络主要路口的关键设备，从而通过只接触数量有限的中间体来快速到达所需的目标设备设备。借助伴随着 sand 这样的智能设备发现，物**联网**设备以及互联网上的其他计算设施、软件和数据可以像人类一样自主地建立新的社会关系。他们可以制定自组织计算组来执行所需的计算任务，促进各种计算服务、网络服务和数据的融合，以生成新颖的应用程序和服务，从个人的情况演变而来智能的协作情报，并最终使机器人社会的诞生。少

2018 年 1 月 8 日提交;v1 于 2017 年 12 月 21 日提交;最初宣布 2017 年 12 月。

474. 第 1712.08221 [pdf,其他] Cs。镍

flip：联盟支持远程低功耗物联网协议

作者:stphane delbruel, nicolas 小, danny hughes

摘要：人们对物联网（**iot**），特别是低功耗广域网（lpwan）的兴趣越来越大，这些网络正在全球范围内迅速推出。在 lpwan 市场内，lorawan 被认为是一个领先的解决方案，并取得了显著的成功。尽管 lorwan 的应用很快，但由于干扰和争用而产生的可伸缩性问题也在不断增加。虽然目前的 lorawan 协议包括处理这些问题的基本技术，但最近的研究表明，这些机制在大规模上是无效的。本文提出了一种面向 lorawan 的新颖、完全分布式和开放的体系结构 flip 来解决这一问题，该体系结构将标准 lora 网关转换为联合网络，同时保留原始 lorawan 的隐私和安全属性建筑。flip 使用网关之间的共识驱动和本地化资源共享来解决 lorawan 的可伸缩性限制，同时还为 lora 设备在整个联盟中的漫游提供固有的支持。关键的是，flip 体系结构与所有现有的 lora 网关完全向后兼容，无需修改 lora 终端设备的固件，从而促进了其快速采用。少

2018 年 4 月 22 日提交;v1 于 2017 年 12 月 21 日提交;最初宣布 2017 年 12 月。

评论:从科技报告到预打印版本

475. 第: 1712.07740 [pdf,其他] Cs。铬

使用安全箱保护边缘网络

作者:ibbad hafeez, aaron yiding, sasu tarkoma

摘要：连接到家庭和企业网络的移动和**物联网**设备的数量正在快速增长。这些设备为用户提供了新的服务和体验;但是，它们还提供了与数据和设备安全以及用户隐私相关的新类别的安全威胁。在本文中，我们首先分析了这些连接到边缘网络的设备所带来的潜在威胁。然后，我们提出了安全箱：一种新的云驱动、低成本的安全即服务解决方案，该解决方案应用软件定义的网络（sdn）来改进网络监控、安全和管理。安全箱支持通过云安全服务（css）远程管理网络，只需最少的用户干预。为了降低成本和提高可扩展性，securebox 基于 css 提供的虚拟化中链。我们的建议不同于现有的解决方案，将 sdn 和云集成到统一的边缘安全解决方案中，并提供协作保护机制，以便在所有连接的网络中快速传播安全策略。减少系统检测到的新威胁或攻击。我们已经实现了两个安全盒原型，使用低成本的 raspberry-pi 和现成的无风扇 pc。我们的系统评估表明，securebox 可以实现自动网络安全，并以较低的管理开销逐步部署到基础架构中。少

2017 年 12 月 20 日提交;最初宣布 2017 年 12 月。

476. 第: 1712.06878[pdf,其他] Cs。镍

lpwan 中分组碎片化的影响分析

作者:ioana suciu, xavier vilajosana, feran adelantado

摘要: 在文献中，当提到不适合框架的拆分数据时，主要是在文献中讨论了数据包碎片。ietf 的 6lwpan 工作组开始研究碎片标头，允许通过 ieee 802.15.4 支持 127 b mtu 的网络发送 ipv6 1280 b mtu，此后，它在**iot**社区受到了关注。本文根据 ietf lpwan 工作组最近采取的一些方向，对 lpwan 中的数据包碎片进行了分析。考虑到工业义务循环网络的限制，我们的目标是确定以较小的碎片发送数据的影响。分析的参数为破碎引起的能耗、吞吐量、良好的加工和端端延迟。分析结果表明，在占空比受限网络中，数据包碎片可以提高通信的可靠性。这在对网络进行致密化时具有特殊的相关性。我们观察到了能耗和额外延迟的相关影响，并确定需要网关/接收器的确认，以利用碎片化带来的一些好处。少

2018 年 4 月 19 日提交;v1 于 2017 年 12 月 19 日提交;最初宣布 2017 年 12 月。

评论:4 月 15 日至 18 日在西班牙巴塞罗那举行的 ieee 无线通信和网络会议上接受和提交的论文

477. 决议: 1712.06 272[pdf,其他] 中心

用于压缩卷积神经网络的自动流，用于 fpga 的高效边缘计算

作者:farhan shafiq, takato yamada, antonio t.vilchez , sakyasingha dasgupta

摘要: 基于深层卷积神经网络 (cnn) 的解决方案是目前计算机视觉任务的最先进技术。由于这些型号的尺寸很大，它们通常在 cpu 或 gpu 集群上运行。然而，电力需求和成本预算可能是采用美国有线电视新闻网用于**物联网**应用的主要障碍。最近的研究表明, cnn 在其结构中包含显著的冗余，并且可以量化到较低的位宽度参数和激活，同时保持可接受的准确性。由于双相化 cnn 所涉及的按位逻辑运算，低位宽，特别是单位宽 (二进制) cnn 特别适用于基于 fpga 实现的移动应用。此外，向较低比特宽的过渡为性能优化和模型改进开辟了新的途径。本文提出了一种从训练的滕索流模型到 fpga 系统二进制 cnn 芯片实现的自动流程。这种流程涉及模型参数和激活的量化、嵌入 c 中网络和模型的生成，以及用于二元卷积的 fpga 加速器的自动生成。通过在低成本、低功耗的环氧-v fpga 器件上实现双值化 "youlov2"，证明了该自动化流程。使用二值化 youv2 进行的目标检测实验表明，与 cpu 和移动 cpu 平台相比, fpga 在模型大小和推理速度方面具有显著的性能优势。此外，从训练有素的模型到 fpga 合成的整个自动化流程可以在一小时内完成。少

2017 年 12 月 18 日提交;最初宣布 2017 年 12 月。

评论:7 页, 9 个数字。接受并在 2017 年 NIPS mlpcd 研讨会上提交 (加利福尼亚州龙滩)

478. 第 1712-06 250[pdf, ps,其他] cs. it

基于无线能量收集的物联网激励机制设计

作者:侯占伟,何晨,李永辉,布兰卡·武切蒂

摘要: 射频能量采集 (rfeh) 是一种很有前途的技术，可远程为无人值守的物联网 (**iot**) 低功耗设备供电。为了实现这一点，在未来**的物联网**系统中，除了传统的数据接入点 (dap) 用于收集数据外，还应部署能源接入点 (eap) 对**物联网**设备进行充电，以保持其可持续运营。实际上, dap 和 eap 可能由不同的运营商操作，因此 dap 需要提供

有效的激励措施，以激励周围的 eap 为其相关**的 iap** 充电。与现有的激励方案不同，我们考虑的是信息不对称的实际情况，即 dap 不了解 eap 的通道条件和能源成本。我们首先将现有的 stackelberg 基于游戏的方法扩展到非对称信息场景，在这种情况下，dap 的预期效用得到了定义和最大化。为了更有效地处理不对称信息，我们开发了一个基于契约理论的框架，在这个框架中，我们推导出最优契约，以最大限度地提高 dap 的预期效用和社会福利。仿真结果表明，信息不对称导致基于 stackelberg 游戏的框架的性能严重下降，而使用非对称信息的基于契约理论的方法优于 stackelberg 基于游戏的方法提供完整的信息。这表明，所考虑的系统的性能在很大程度上取决于市场结构（即是否允许 eap 在**物联网**设备上完全自由地优化其接收功率），而不是信息可用性（即完整或不对称的信息）。少

2017 年 12 月 18 日提交;最初宣布 2017 年 12 月。

评论:论文全文：1703.0 05902 接受出现在 ieee 物联网杂志上

479. 第 xiv:171205990[pdf] Cs。马

利用机器学习提高 atn (prt) 系统中的车辆流量

作者:bogdan czejdo, wiktor b. daszczuk , mikovaj baszun

摘要：本文讨论了基于人工智能工具增强自动公交网络（atn，以前称为个人快速交通-prt）的新技术。主要方向是按照 **iot** 范式改进使用协商协议的自治模块的合作。目标之一是通过调整自主车辆的合作来提高 atn 系统的吞吐量。机器学习（ml）被用来改进人类程序员设计的算法。我们使用了与近乎最优的解决方案相对应的 "现有控件"，并构建了优化模型，以便更准确地将系统的动态与其性能联系起来。一种主要影响 atn 性能的机制是空车管理（evm）。使用了人类程序员设计的算法：为等候的乘客空车，在重新分配空车的基础上进行平衡，以实现更好的结算规律性。在本文中，我们讨论了如何通过使用 ml 来定制个人行为策略来改进这些算法（并根据当前条件对其进行调整）。使用 ml 技术是可能的，因为我们的算法基于一组参数。可以调整一些重量和门槛，以便更好地决定在赛道上移动空车。少

2017 年 12 月 16 日提交;最初宣布 2017 年 12 月。

评论:6 页，3 个数字

msc 类：68t05 类：I.2。6

日记本参考:autususy-test 第 18 卷（2017），第 12 号，1484-1489 页

480. 第：1712.05958[pdf，ps，其他] Cs。铬

物联网中安全边缘网络对设备（d2d）通信的研究

作者:ibbad hafeez, aaron yiding, markku antikainen,sasu tarkoma

摘要：物联网（**iot**）的日益普及，使得人们需要基于网络的流量异常检测系统，这些系统可以识别行为不当的设备。在本工作中，我们提出了一种轻量级技术**--物联网**保护，用于识别恶意流量。**物联网**保护使用半监督学习来区分使用设备生成的网络流量的恶意和良性设备行为。为了实现这一目标，我们从网络日志中提取了 39 个要素，并放弃了任何包含冗余信息的要素。在特征选择的基础上，训练模糊 c-p 指（fcm）算法，以获得识别良性流量与恶意流量的聚类。我们研究了这些集群中的特征得分，并利用这些信息预测新流量的类型。**使用**包含 30 多台设备的真实世界测试台对物联网防护进行了评估。结果表明，iotguard 在区分各类恶意良性流量时，具有较高的准确性（98％），误检率较低。此外，它的资源占用空间较低，可以在启用 openwrt 的接入点和 cots 计算板上运行。少

2018 年 10 月 16 日提交;v1 于 2017 年 12 月 16 日提交;最初宣布 2017 年 12 月。

评论:在第 12 届网络与系统安全国际会议上亮相, nss, 2018 年 8 月 (http://www4.comp.polyu.edu.hk/~nss2018/program.html)

481. **第 xiv:1712.05133[pdf, ps,其他] cs. it**

多伊 10.1109/LCOMM.2017.2720585

一种具有部分序言传输机制的 nb-iot 系统增强访问保留协议

作者:taehoon kim, dong min kim , nuno pratas, petar popovski, dan keun sung

文摘: 在本文中，我们提出了一个增强的访问保留协议 (arp)，它具有窄带物联网 (nb-iot) 系统的部分前导传输(ppt) 机制。提出的 arp 可以通过减少前导冲突的发生来提高 arp 性能，同时与传统的 **nb-iot** arp 兼容。我们提供了一个分析模型，从虚警、误检和碰撞概率的角度来捕捉拟议的 arp 的性能。此外，我们还研究了误射与碰撞概率之间的权衡，并根据系统负载对提出的 arp 进行了优化。结果表明，所提出的 arp 优于传统的 **nb-iot**arp，特别是在较重的系统负载下。少

2017 年 12 月 14 日提交;最初宣布 2017 年 12 月。

日记本参考:ieee 通信信函, 21 (10), 2270-2273 页, 2017 年 10 月

482. **第: 1712.04980[pdf,其他] Cs。镍**

多伊 10.1109/JIOT.2018.2796542

5g 网络的边缘计算感知 nma

作者:abbas kiani, nirwan ansari

摘要: 随着物**联网 (iot**）的快速发展，第五代 (5g) 无线网络需要提供**物联网**设备的大规模连接，并满足低延迟的需求。为了满足这些要求，非正交多址 (noma) 已被认为是 5g 网络显著提高网络容量的一种有前途的解决方案。随着 noma 技术的发展，移动边缘计算 (mec) 正在成为降低 5g 网络延迟和提高服务质量 (qos) 的关键新兴技术之一。为了在 mec 的背景下捕捉 noma 的潜在优势，本文提出了一种边缘计算感知 noma 技术，该技术可以享受上行链路 noma 在降低 mec 用户上行能耗方面的优势。为此，我们制定了一个基于 noma 的优化框架，通过优化用户集群、计算和通信资源分配以及传输能力，最大限度地减少了 mec 用户的能耗。特别是，类似于频率资源块 (rb)，我们将云上可用的计算能力划分为计算 rb. 因此，我们探讨将频率和计算 rb 联合分配给分配给不同顺序的用户在 noma 集群中的指数。我们还设计了一种有效的用户聚类和 rb 分配启发式算法，并提出了每个 noma 聚类独立求解功率控制的凸优化问题。通过仿真对所提出的 noma 方案的性能进行了评价。少

2017 年 12 月 13 日提交;最初宣布 2017 年 12 月。

报告编号:tr-anl-2017-007

日记本参考:ieee 物联网杂志, 2018

483. **第 xiv:1712. 04902[pdf] 中心**

面向物联网终端节点的多线程 risc-v 兼容处理核心系列的微观架构

作者:abdallah Cheikh, gianmarco cerutti, antonio mastrandrea, francesco menichelli, mauro olivieri

摘要: 物联网终端节点需要低功耗处理平台，其特点是异构专用单元，由运行并发控制线程的处理器核心控制。这种体系结构方案符合 risc-v 指令集的主要目标应用领域之一。我们在软件方面推出了符合 risc-v 的开源处理核心，在硬件方面提供了流行的

pulpino 处理器平台，同时支持**物联网**应用的交错多线程处理。后一个特点是在这一应用领域中的一个新的贡献。我们报告有关微体系结构设计的详细信息以及性能数据。少

2017 年 12 月 13 日提交;最初宣布 2017 年 12 月。

评论:8 页

484. **第 1712.04804[pdf,其他] Cs。镍**

环境背散射通信：当代调查

作者:nguyen van huynh, dinh thaihoang , xiah lu, dusit niyato, pingwang, dong in kim

摘要: 最近，环境反向散射通信已被引入作为一种尖端技术，使智能设备能够通过使用环境射频 (rf) 信号进行通信，而无需主动 rf 传输。该技术在解决传感器网络等低功耗通信系统的通信和能效问题方面特别有效。预计它将实现众多物联网 (**iot**) 应用。因此，本文旨在对环境后向散射通信的基本原理、应用、挑战和研究进展提供当代、全面的文献综述。特别是，我们首先介绍了反向散射通信的基本原理，并简要回顾了双基地后向散射通信系统。然后讨论了解决环境后向散射通信系统存在的问题和局限性的一般体系结构、优点和解决方案。此外，还突出显示了环境反向散射通信的新应用。最后，我们概述了一些悬而未决的问题和未来的研究方向。少

2017 年 12 月 13 日提交;最初宣布 2017 年 12 月。

评论:32 页，18 个数字，期刊

485. **第 xiv:1712.04301[pdf,其他] Cs。镍**

对物联网大数据和流分析的深度学习：一项调查

作者:Mohsen mohamadi, ala al-fuqaha, sameh sorour, mohsen guizani

摘要: 在物联网 (**iot**) 时代，大量传感设备会随着时间的推移收集和生成各种感官数据，用于广泛的领域和应用。根据应用程序的性质，这些设备将产生大的或快速的实时数据流。对此类数据流进行分析以发现新信息、预测未来洞察并做出控制决策是一个至关重要的过程，可**使物联网**成为企业的一个有价值的范例和提高生活质量的技术。在本文中，我们提供了有关使用一类高级机器学习技术 (即深度学习 (dl)) 的全面概述，以促进**物联网**领域的分析和学习。我们首先阐明**物联网**数据特征，并从机器学习的角度**确定物联网**数据的两种主要处理方法，即**物联网**大数据分析和**物联网**流数据分析。我们还讨论了为什么 dl 是在这些类型的数据和应用程序中实现所需分析的一种有希望的方法。然后讨论了将新兴 dl 技术用于**物联网**数据分析的潜力，并介绍了其承诺和挑战。我们对不同的 dl 体系结构和算法提供了一个全面的背景。我们还分析和总结**了在物联网**领域利用 dl 的主要报告研究尝试。还讨论了在智能背景中集成了 dl 的智能**物联网**设备。还研究了支持**物联网**应用的雾和云中心的 dl 实现方法。最后，我们为今后的研究提供了一些挑战和潜在的方向。在每一节的最后，我们强调根据我们的实验和对最近文献的回顾所吸取的经验教训。少

2018 年 6 月 4 日提交;v1 于 2017 年 12 月 9 日提交;最初宣布 2017 年 12 月。

评论:40 页，接受 ieee 通信调查和教程杂志

486. **第: 1712.03623[pdf,其他] Cs。铬**

idiot：保护物联网，就像 1994 年一样

作者:david barrera, ian molloy, he 庆 huang

摘要: 到 2020 年，超过 200 亿台物联网设备将上线。保护如此大量的动力不足、无 ui、网络连接的设备需要一个新的安全模式。我们认为，依赖于供应商合作的解决方案 (如安全编码和平台更改) 不可能为大多数设备提供足够的防御。同样，监管办法在执行方面也面临一些挑战，限制了其有效性。作为新范式的一部分，我们提出了 idot，这是**物联网**设备的网络安全策略实施框架。idiot 将 iot 设备限制为其必要的网络行为，从而防止广泛的网络攻击。idiot 简单而有效，基于数十年久经考验的网络安全原则，无需更改设备或云基础架构。少

2017 年 12 月 10 日提交;最初宣布 2017 年 12 月。

487. **第 1712.03314[pdf,其他] cs. it**

通过多址无线传感器网络实现高效的数据采集

作者:alejandro cohen, asaf cohen, omer gurewitz

摘要: 无线传感器网络 (wsn) 中的数据采集引起了人们的极大关注，因为人们对从物联网 (**iot**) 网络到简单的 "状态" 应用程序的技术产生了浓厚的兴趣，这些应用程序可以识别设备的状态 (活动或非活动)。多年来，人们提出了许多无线传感器网络的媒体访问控制 (mac) 协议，这些协议可以解决密集网络中数据收集的挑战。这些协议大多使用传统的分层方法，在这种方法中，mac 层不知道封装的数据包有效负载，因此收集的数据、物理层和信令机制之间没有连接。尽管如此，在许多打算使用此类协议的应用程序中，节点可能只需要很少交换信息，而且只是零星地这样做，也就是说，虽然网络中的设备数量可能非常大，但只有一个子集希望在任何给定的时间。因此，需要一个定制的协议，将信令、物理层和访问控制与流量模式相匹配。本文设计并分析了一种基于信息理论原理的数据采集协议。在建议的协议中，接收器从大量传感器中同时收集多达 k 传感器的消息，而不事先知道哪些传感器将传输，也不需要任何同步、协调或管理开销。换句话说，接收器和其他传感器都不需要知道谁是主动传输的传感器，这些数据直接从通道输出中解码。我们提供了一个简单的码本结构，具有非常简单的编码和解码过程。我们进一步设计了协议的安全版本。少

2018 年 10 月 15 日提交;v1 于 2017 年 12 月 8 日提交;最初宣布 2017 年 12 月。

488. **第: 1712.02969[pdf,其他] Cs。铬**

lsb: 适用于物联网安全和隐私的轻量级可扩展区块链

作者:ali dorri, salil s. kanhere, raga jurdak , praven gauravaram

摘要: 区块链 (bc) 由于其不可改变的性质以及相关的安全和隐私好处，引起了极大的关注。bc 有潜力克服物联网 (**iot**) 的安全和隐私挑战。但是，bc 的计算成本很高，可扩展性有限，并且会产生大量的带宽开销和延迟，而这些开销和延迟并不适合**物联网**环境。我们提出了一个分层轻量级可扩展 bc (lsb)，该 bc 针对**物联网**要求进行了优化。我们在智能家居环境中探索 lsb，将其作为更广泛的**物联网**应用的一个具有代表性的范例。智能家居中的低资源设备受益于集中式管理器，该管理器为通信建立共享密钥并处理所有传入和传出请求。lsb 通过形成覆盖网络来实现权力下放，高资源设备在该网络中共同管理公共 bc，以确保端到端隐私和安全。覆盖被组织为不同的集群，以减少间接费用，并且集群头负责管理公共 bc。lsb 包含了几个优化，其中包括轻量级共识、分布式信任和吞吐量管理的算法。定性参数表明 lsb 能够抵御多种安全攻击。大量的仿真结果表明，与相关基线相比，lsb 减少了数据包开销和延迟，并提高了 bc 的可扩展性。少

2017 年 12 月 8 日提交;最初宣布 2017 年 12 月。

489. 第 1712.0999[pdf] Cs。直流

可持续云计算的分类与未来发展方向: 360 度视图

作者:sukhpal singh gill, Rajkumar buyya

摘要: 云计算模式通过互联网提供按需服务，并支持各种应用程序。随着最近基于物联网 (**iot**) 的应用程序的增长，云服务的使用呈指数级增长。下一代云计算必须具有高能效和可持续性，以满足正在动态变化的最终用户要求。目前，云提供商在确保其服务的能源效率和可持续性方面面临挑战。大量云数据中心的使用增加了成本和碳足迹，进一步影响了云服务的可持续性。在本文中，我们提出了一个可持续云计算的综合分类。分类用于调查现有的可持续性技术，需要认真关注和调查，正如几个学术和行业团体所建议的那样。此外，目前对可持续云计算的研究分为几个类别: 应用程序设计、可持续发展指标、容量规划、能源管理、虚拟化、热感知调度、冷却管理、可再生能源和余热利用。根据现有技术的共同特点和特点，对现有技术进行了比较和分类。提出了可持续云计算的概念模型，并对未来的研究方向进行了讨论。少

2018 年 7 月 9 日提交;v1 于 2017 年 12 月 7 日提交;最初宣布 2017 年 12 月。

评论:68 页, 38 个数字, 2018 年中、区域中心计算调查

类:D.4。1

490. 第 1712.02141[pdf,其他] Cs。镍

多伊 10.114/3144477.3144478

利用商品硬件对环环的选择性干扰

作者:emekcan aras, nicolas 小额, gowri sankar ramachandran, stphane delbruel, wouter joosen, danny hughes

摘要: 远程、低功耗网络由于能够经济地支持远程传感和控制应用，同时提供多年电池寿命，因此正在迅速获得物联网 (**iot**) 的认可。lora 是这一新网络类的一个关键示例，正在全球多个国家大规模部署。当这些网络走出实验室进入现实世界时，它们暴露了一个巨大的网络物理攻击表面。因此，确保这些网络的安全既重要又紧迫。本文重点介绍了由于在协议中选择了鲁棒但缓慢的调制类型而产生的 lora 和 lorwan 中的安全问题。我们利用这些问题来开发一套基于选择性干扰的实际攻击。这些攻击是使用商品硬件进行和评估的。最后，本文提出了一系列可用于减轻攻击的对策。少

2017 年 12 月 6 日提交;最初宣布 2017 年 12 月。

评论:2017 年 11 月 7-10 日，澳大利亚维也纳国际中心墨尔本

491. 第 1712.01611[pdf,其他] Cs。铬

基于内存的嵌入式系统中设备认证组合 puf

作者:soubhagya sutar, arab raa, vijay rahunathan

摘要: 嵌入式系统在推动物联网 (**iot**) 在医疗保健、家庭自动化、交通等应用领域的增长方面发挥着至关重要的作用。然而，它们日益与网络相连的性质，加上它们获取潜在敏感机密信息的能力，引起了许多安全和隐私问题。另一个挑战是这些设备中假冒部件的数量不断增加，造成了严重的可靠性和所涉经费问题。物理上不可克隆函数 (puf) 是一个很有前途的安全原语，可以帮助解决这些问题。基于内存的 puf 特别有吸引力，因为它们的操作需要最少或不需要额外的硬件。但是，当前基于内存的 puf 仅使用一种内存技术来构建 puf，它有几个缺点，包括使它们容易受到安全攻击。在本文中，我们提出了一个新的基于内存的组合 puf，智能地结合了两种内存技术, sram 和 dram,

以克服这些缺点。所提出的组合 puf 具有较高的熵，支持大量的质询响应对，并且本质上是可重构的。我们使用 terasic tr4-230 fpga 板和几个现成的 sram 和 dram 实现了拟议的组合 puf。实验结果表明，与当前基于内存的 puf 相比，包括抵御各种攻击的能力有了很大的改进。在宽温度范围 (20-60 度摄氏度) 和加速老化 (12 个月) 范围内进行广泛的身份验证测试，证明了所建议设计的稳健性，实现了 100% 的真实阳性率和 0% 的假阳性率在这些参数范围内。少

2017 年 12 月 5 日提交;最初宣布 2017 年 12 月。

评论:7 页, 10 个数字

492. 第 1712.01214[pdf] Cs。铬

tri 投 ta: 无线物联网设备的安全性、能效和通信容量比较

作者:shreyas sen, jinkyu koo, Saurabh bagchi

摘要: 在物联网 (**iot**) 时代，传感器节点的广泛普及，加上传感器保真度和数据采集方式的增加，预计到 2018 年，每天将产生 3 + tb 的数据。由于这些**物联网**设备大多将在最后几英尺内进行无线连接，因此无线通信是未来**物联网**方案不可或缺的一部分。单元计算 (摩尔定律) 的规模不断缩小，高效通信 (香农定律) 的持续改进有望利用**物联网**革命的真正潜力并产生巨大的社会影响。然而，减少**物联网**节点的大小和缺乏显著的储能密度改进会导致能源利用率下降。此外，更小的尺寸和能源意味着用于保护**物联网**节点的资源较少，使网络中能源稀少的低成本叶节点成为攻击者的主要目标。本文从安全、能源效率、通信能力三个维度方面对六大主要无线技术进行了综述。我们指出了最先进的、开放的问题，以及未来有希望的研究方向。少

2017 年 11 月 22 日提交;最初宣布 2017 年 12 月。

评论:等待在 ieee 互联网计算杂志上发表

类:B.2.3;c.3;K.6。5

493. 第 1712.01084[pdf,其他] Cs。Lg

基于矩阵旋转的结构深部神经网络修剪

作者:ranko sredojevic, shaoyi cheng, lazar supic, raan naous, vladimir stojanovic

摘要: 深神经网络 (dnn) 是最先进的机器视觉、传感器融合和音频视频信号处理的关键。不幸的是，它们的计算复杂性和边缘上的资源约束很严格，因此很难在移动、嵌入式和**物联网**设备上加以利用。由于边缘设备的多样性，dnn 设计人员在网络培训期间必须考虑硬件平台和应用程序要求。在本工作中，我们引入了通过矩阵旋转修剪，以此来改善网络修剪，在架构忽略的设计灵活性和架构感知修剪的性能效率之间产生损害，这两种主要技术是获得资源节约型的 dnn。我们还描述了本地和全局网络优化技术，以便有效地实现生成的修剪网络。结合实践，随着修剪过程中网络系数的降低，所提出的修剪和实现速度接近线性。少

2017 年 11 月 30 日提交;最初宣布 2017 年 12 月。

评论:16 页, 3 个数字, 2 个表, 1 个列表

494. 第 1712. 00537[pdf,其他] cs. it

车辆网络的高可靠性和低延迟: 挑战与解决方案

作者:杨浩军,简正,赵龙, 张权, periklis chatzimisios, yong teng

摘要: 近年来，无线网络正经历着从高速数据速率到连接一切的范式转型，提升了物联网 (**iot**) 的发展。作为**物联网**的典型场景，车载网络引起了汽车和电信行业的广泛关注，

尤其是在超可靠和低延迟通信 (urllc) 应用中。然而，传统的无线网络主要是为了提高频谱效率而设计的，而没有充分关注 urllc 的要求。为此，本文旨在研究车载网络中的延迟和可靠性问题。具体来说，我们首先介绍有前途的 urllc 应用程序和要求。随后从物理和媒体访问控制层的角度讨论了几种性能评价方法。利用这些方法，可以有效、准确地评估底层传输技术和调度算法。最后，提出了一些有希望的解决办法，以应对潜在的挑战。少

2017 年 12 月 1 日提交;最初宣布 2017 年 12 月。

495. **第: 1712.00100[pdf, ps,其他] cs. it**

雾的虚拟化控制: 可靠性和延迟之间的交互

作者:hazer inaltekin, maria gorlatova, mung chiang

摘要: 本文介绍了一个分析框架，研究了沿云到物连续体放置虚拟控制器的最佳设计选择。主要的应用场景包括低延迟网络物理系统，在这些系统中，需要实时控制操作来响应物**联网**节点状态的变化。在这种情况下，由于从网络边缘到云的延迟，通常无法在云服务器上部署控制器软件。因此，最好通过将控制器逻辑移动到更靠近网络边缘的地方来计算具有延迟的可靠性。**将物联网**节点建模为一个动态系统，该系统在时间上线性演变，对状态偏差有二次惩罚，通过虚拟迷雾得到最优控制策略的递归表达式和产生的最小成本值控制器的可靠性和响应时间延迟。我们的结果表明，在针对雾端点的虚拟化控制服务中，延迟比可靠性更重要，因为它决定了雾控制系统的快速性以及状态测量的及时性。在现实无人机轨迹跟踪模型的基础上，进行了广泛的仿真研究，说明了可靠性和延迟对自主车辆控制雾的影响。少

2018 年 2 月 13 日提交;v1 于 2017 年 11 月 30 日提交;最初宣布 2017 年 12 月。

496. **第: 1711.11390[pdf] Cs。锞**

多伊 10.1007/98-991-10-1741-4 _ 12

智能家居的半分布式需求响应解决方案

作者:rim kaddah, daniel kofman, fabien mathieu , mical pioro

摘要: 物联网 (**iot**) 范式为高级需求响应 (dr) 解决方案带来了机遇。它可以在可能消耗、储存或在家庭中产生能量的各种设备上实现可见性和控制。事实表明，对一组家庭的电器进行集中控制，就会产生有效的恢复机制;不幸的是，这样的解决方案会引发隐私和可伸缩性问题。在本章中，我们提出了处理这些问题的方法。具体来说，我们引入了一个可扩展的两级控制系统，其中一个集中式控制器将电源分配给一侧的每栋房子，并且每个家庭在另一侧实现 dr 本地解决方案。对集中式控制器的有限反馈可以提高性能，而不会对隐私产生影响。提出了能力市场总体框架的解决方案。少

2017 年 11 月 30 日提交;最初宣布 2017 年 11 月。

日记本参考:智能城市信息创新技术，第 17 页 (163-179), 2017

497. **第: 1711.111210[pdf,其他] lo c**

多伊 10.4204/EPTCS.261 。6

物联网工具支持的分析

作者:chiara bodei, pipipaolo degano, letteriogalletta , emilio tuosto

文摘: **物联网**系统的设计可以从两种不同分析的结合中受益。我们执行第一次分析来近似系统组件之间的数据流，而第二分析检查它们的通信健全性。我们展示了这两种分析的结合如何通过单独使用每项分析来产生难以实现的进一步好处。我们利用两个独立

开发的工具进行分析。首先，我们在**物联网**-lysa 中指定**物联网**系统，这是一种简单的规范语言，具有元组的异步多播通信功能。元组携带的值来自通过参数签名获得的术语代数。chorgram 支持对通信健全性的分析，该工具是为验证通信有限状态机的兼容性而开发的。为了将分析结合起来，我们将**物联网**-lysa 进程编码到通信机器中。这种编码并不完全简单，因为**物联网**-lysa 具有与数据的多播通信，而通信计算机基于点对点通信，在点对点通信中只能交换有限的多个符号。为了突出我们方法的好处，我们呼吁举一个简单而又说明问题的例子。少

2017 年 11 月 29 日提交;最初宣布 2017 年 11 月。

评论:2017 年会议记录，第 7xiv:1711. 10708

日记本参考:eptcs 261, 2017, 37-56 页

498. 决议: 1711.11133[pdf,其他] Cs。镍

多伊 10.14569/IJACSA.2016.071254

软件定义的物联网安全服务设置框架

作者:faraz idris khan, sufian hameed

摘要: 可编程管理框架为网络中的设备管理铺平了道路。最近，新兴的软件定义网络 (sdn) 范式使可编程网络发生了革命性的变化。网络应用 (**即物联网**) 的设计人员已经开始研究 sdn 范式在改善网络管理方面的潜力。**物联网**设想将环境中的各种嵌入式设备与 ip 连接起来，实现互联网连接。与传统的网络架构不同,**物联网**的特点是资源约束和无线和有线媒体的异构互连性。因此，本文提出了管理**物联网**的独特挑战。**物联网**的普及在**物联网**领域提出了独特的安全挑战，而**物联网是物联网**管理框架的一个方面。本文从调查**物联网**安全挑战的**最新工作中**提取的物联网中总结了安全威胁和要求。提出了基于 sdn 的物**联网**安全服务提供框架。少

2017 年 11 月 29 日提交;最初宣布 2017 年 11 月。

评论:15 页, 18 位数字

日记本参考:国际高级计算机科学与应用杂志 (ijacsa), 7 (12), 2016。
http://dx.doi.org/10.14569/IJACSA.2016.071254

499. 第: 1711. 10941[pdf,其他] Cs。Sy

基于分布式多代理 q 学习的智能交通灯控制

作者:刘英,刘磊,陈伟鹏

摘要: 人工智能 (ai) 和物联网 (**iot**) 的结合 (称为 ai 驱动的物联网 (aiot)) 能够处理从大量设备生成的海量数据并处理复杂的内容社会基础设施中的问题。随着人工智能和**物联网**技术的日益成熟，本文提出将 aiot 技术应用于交通灯控制，这是智能交通系统的重要组成部分，以提高智能城市道路系统的效率。.具体而言，监控摄像头等各种传感器为智能红绿灯控制系统提供实时信息，以观察机动车交通和非机动车交通的状态。本文提出了一种利用分布式多代理 q 学习的智能交通灯控制解决方案，同时考虑到邻近路口的交通信息以及当地的机动和非机动交通，以改进整个控制系统的整体性能。利用所提出的多智能体 q 学习算法，我们的解决方案是针对机动和非机动车交通的优化。此外，我们还考虑了现实世界中交通灯控制的许多约束规则，并将这些约束集成到学习算法中，这有助于在实际操作场景中部署所提出的解决方案。我们对包含真实世界交通数据的真实世界地图进行了数值模拟。仿真结果表明，我们提出的解决方案在车辆和行人队列长度、交叉口等待时间以及许多其他关键性能指标方面优于现有解决方案。少

2017 年 11 月 29 日提交;最初宣布 2017 年 11 月。

期刊参考: 2017 ieee 第 20 届智能交通系统国际会议

500. 第: 1711.10685[pdf,其他] Cs。直流

基于物联网的平台即提供并行应用程序的服务

作者:deepak kumar Aggarwal, rahni aron

摘要: 在现代, 物联网 (**iot**) 迅速发展。根据 2020 年的统计数据, 将有 200 亿台设备连接到互联网。互联网连接设备的大量增加将导致大量工作, 以有效地执行关键的并发应用, 如火灾检测、基于医疗保健的系统、灾难管理、高能物理、汽车和医疗成像。为了加快新应用程序的出现, 这一庞大的基础架构需要 "平台即服务 (paas)" 模型来利用**物联网**。由于所有设备类型和**基于物联网**的应用域的单一全球标准是不可行的, 本文提出了一种基于物联网的云, 以利用 **paas** 模型。该模型可以承载无线传感器网络 (wsn) 的并发应用。该模型通过将网络接口唯一地分配给特定容器, 提供了进程之间的通信接口。少

2017 年 11 月 29 日提交;最初宣布 2017 年 11 月。

501. 第: 1711. 10304[pdf,其他] Cs。镍

多伊 10.114/3102304.332345

面向以信息为中心的网络 (icn) 物联网 (iot) 命名: 智能校园的案例

作者:sobia arshad, muhammad awais azam, syed hassan ahmed, jonathan loo 教授

摘要: 以信息为中心的网络 (icn) 特别是命名数据网络 (ndn) 是名称库 (内容基) 网络, 并将命名内容作为 "一流公民", 被认为是形成未来互联网基础的理想候选对象。ndn 显著的功能, 如命名数据自保护内容、名称基转发、网络内缓存和移动支持, 适用于物联网 (**iot**) 环境, 其目的是实现智能设备之间的通信, 并将所有设备结合在一起基于互联网的智能应用程序在一个屋檐下。有了这些目标,**物联网**对其网络架构提出了许多研究挑战, 因为它应该支持异构设备并提供可扩展性。**物联网**可能取决于数十亿个设备的名称和地址, 并且应该巧妙地管理每一秒钟产生的大量数据。物联网应用智能校园由于诸多原因,**受到**了业界和学术界的广泛关注。因此, 要设计**物联网**的 ndn, 需要探索一个复杂的命名方案, 这也是这项工作的主要动机。本文从连接设备和内容**的**角度对 ndn-iot 智能校园进行了研究, 发现它缺乏合理的命名和寻址机制;因此, 我们为基于**物联网**的智能校园 (iotsc) 提出了基于 ndn 的混合命名方案 (ndn-hns)。少

2017 年 11 月 28 日提交;最初宣布 2017 年 11 月。

评论:6 页 3 无花果

502. 第 (xiv:1711. 10190)[pdf,其他] Cs。铬

一种有效的无隐私性的故障辅助传感器检测方案

作者:陈硕,陆荣兴,张杰

文摘: 物联网 (**iot**) 一直是研究界和业界的热门话题。预计在未来**的物联网**中, 大量传感器每时每刻都将收集物理信息, 使控制中心能够做出更好的决策, 以提高服务质量 (qos)。然而, 传感器可能有故障, 从而产生不准确的数据, 这将危及决策。为了保证 qos, 系统应该能够检测到有故障的传感器, 以消除不准确数据的损害。在无线传感器网络 (wsn) 的背景下, 开发了各种故障传感器检测机制。其中一些只适合 wsn, 而另一些则会给控制中心带来通信负担。为了检测一般**物联网**应用中的故障传感器, 同时节

省通信资源，提出了一种有效的故障传感器检测方案。该方案利用雾化计算的优势，节省了控制中心的计算和通信资源。为了保护传感器数据的隐私，在雾计算中采用了 paillier 密码系统。采用批量验证技术实现了高效的认证。通过性能分析，证明了所提出的检测方案能够在保持可接受的假阳性比的情况下，保护控制中心的通信资源，实现较高的真阳性率。该计划还可以抵御各种安全攻击并保护数据隐私。少

2017 年 11 月 28 日提交;最初宣布 2017 年 11 月。

评论:11 页, 5 个数字

503. 第: 1711.10182[pdf,其他] Cs。铬

物联网中安全态势感知的一种新方法

作者:何凡夫,张玉清,刘慧珍

摘要: 物联网 (**iot**) 的特点是各种异构设备，面临着众多的威胁。**物联网**安全性建模仍然是一个挑战。本文定义了基于**物联网**的智能环境的随机彩色 petri 网 (scpn)，并在定义的 scpn 中提出了一个用于安全态势感知 (ssa) 的马尔可夫博弈模型。所有可能的攻击路径都由 scpn 计算，并根据博弈论动态地考虑攻击者和防御者的对抗行为。考虑了智能家居环境中的两种攻击场景，以证明该模型的有效性。该模型可以形成安全态势的宏观趋势曲线。对结果的分析显示了该模型在查找易受攻击设备和潜在攻击路径，甚至减轻攻击影响方面的能力。据我们所知，这是首次尝试为复杂**的基于物联网**的智能环境建立动态 ssa 模型。少

2017 年 11 月 28 日提交;最初宣布 2017 年 11 月。

504. 建议: 1711. 09157[pdf, ps,其他] Cs。直流

面向开放物联网的异构资源优化研究

作者:yoki yamato, naoto hoshikawa, hirofumi noguchi, tatsuya demizu, misao kataoka

摘要: 最近,**物联网**技术取得了进展，许多传感器和执行器都连接到了网络。此前,**物联网**服务是通过垂直集成风格开发的。但现在开放**物联网**的概念已经引起了人们的关注，通过集成水平分离的设备和服务来实现各种**物联网**服务。对于开放**物联网**时代，我们提出了隐性计算技术，以发现具有必要数据的设备，供用户按需使用，并动态使用它们。我们还实施了隐性计算的基本技术。本文提出了三层优化，以降低 tacit 计算服务的运行成本，提高其性能，从而使其成为已发现设备的连续服务。在优化过程中，在全面运行之前，在设备、网络和云层上计算适当的函数分配或卸载特定功能。少

2017 年 11 月 24 日提交;最初宣布 2017 年 11 月。

评论:3 页, 1 个图, 2017 年第五届计算机与网络国际研讨会 (ccandar2017), 2017 年 11 月

期刊参考: 2017 年第五届计算机与网络国际研讨会 (ccandar2017)，第 6609-611 页，2017 年 11 月。(c) 2017 年 ccandar2017

505. 第: 1711. 0818[pdf,其他] Cs。镍

多伊 10.1016/j.comcom.2017.11.002

一种基于 jxta 的用于实现异构物联网的新型体系结构

作者:菲利波·巴塔利亚, lucia lo bello

摘要: 本文介绍了 embjxtacord，这是一种新颖的点对点 (p2p) 体系结构，它集成了不同来源 (如 jxta、exi、coap) 的良好功能，并对其进行了组合和增强，以提供**专门为**

开发物联网而设计的框架。在异构网络上的应用程序。embjxtacord 提供了几个有趣的属性，例如分布式和容错资源发现、子网上的透明路由、应用程序协议独立于窄带 wsn 中的传输协议，从而消除了需要使用专用软件或配置自定义网关来实现这些功能。此外，embjxtacord 不仅为 tcp/http 提供本机支持，还为蓝牙 rfcomm 和 6lwpan 提供本机支持，从而向使用不同互连技术的网络组成的超级**网络中的各种物联网**设备开放，而不是必要的 ip 为基础。此外，embjxtacord 还通过异构网络提供安全性，为安全的轮组（甚至嵌套）和组加密提供支持，从而允许共享相同资源的对象组之间进行单播和多播通信。最后，embjxtapard 提供了 jxCOAP-E，这是一种新的 coap 实现，利用了 embjxtacord 提供的异构网络的传输机制。jxCOAP-E 支持实现对等窄带或宽带网络的 restful 服务体系结构，该网络由通过以太网、wi-fi、蓝牙、ble 或 ieee 802.15.4 连接的设备组成。与 coap 不同，jxCOAP-E 提供了分布式容错服务发现机制，并支持安全的多播通信。本文介绍了 embjxtacord，讨论了所有相关的设计挑战，并介绍了与商用现成设备上最先进的解决方案进行的比较实验性能评估。少

2017 年 11 月 22 日提交;最初宣布 2017 年 11 月。

评论:54 页，16 位

506. **第: 1711.07 277[pdf, ps,其他] cs. it**

物联网的反向散射通信: 一种随机几何方法

作者:mudasar bacha, bruno clerckx

摘要: 在物联网（**iot**）和无线功率传输（wpt）的最新进展的推动下，我们研究了一种由功率信标（pbs）和被动后向散射节点（bn）组成的网络体系结构。pbs 传输正弦连续波（cw），而 bn 在采集剩余部分时反射该信号的一部分。bn 从附近的多个 pbs 中获取能量，并通过反向散射调制在复合 cw 上调制其信息位。由于双衰落通道及其对 bn 和 pbs 公私伙伴关系的依赖，分析带来了真正的挑战。然而，在随机几何的帮助下，我们推导出了网络的覆盖概率和容量，并根据不同的系统参数，以可跟踪和容易计算的表达式。我们观察到，随着 bn 密度的增加，覆盖概率降低，而网络容量的提高。我们进一步将该网络的性能与一个常规供电网络进行了比较，在该网络中，bn 具有可靠的电源，并表明，对于非常高密度的 pbs，前一个网络的覆盖概率接近常规供电网络的覆盖概率.少

2018 年 4 月 17 日提交;v1 于 2017 年 11 月 20 日提交;最初宣布 2017 年 11 月。

评论:这项工作已提交一份可能的期刊出版物

507. **决议: 1711.07268[pdf,其他] cs. it**

评估面向智慧城市应用的 emtc 和 nb-iot 的性能

作者:mohieddine el soussi, pouria zand, frank pasveer, guido dolmans

摘要: 低功耗广域网（lpwan）是为低比特率互连设备而设计的无线通信网络，专注于远距离和功率效率。本文研究了由现有的长期进化（lte）功能构建的两种最新技术：增强型机器类型通信（emtc）和窄带物联网（nb-iot）。这些技术旨在与现有的 lte 基础结构、频谱和设备共存。我们首先简要介绍这两个系统，然后比较它们在能耗、延迟和可伸缩性方面的性能。介绍了一种计算能耗的模型，研究了时钟漂移的影响，并提出了克服时钟漂移的方法。我们还提出了一个模型，用于分析评估网络中的延迟和设备的最大数量。此外，我们实现了这两种技术的主要功能，并在离散事件网络模拟器 ns-3 中模拟了端到端延迟和设备的最大数量。数值结果表明，在覆盖较差的情况下，两种技术都可以实现 8 年的电池寿命，根据覆盖条件和数据长度，一种技术消耗的能量比另一种

技术少。结果还表明，与 nb-物联网相比，emtc 可以为网络中更多的设备提供服务，同时提供的延迟是 nb-物联网的 10 倍。少

2017 年 11 月 20 日提交;最初宣布 2017 年 11 月。

508. 第: 1711. 06469[pdf] Cs。镍

非常绿色、灵活和盈利的 5g m2m 无处不在的通信基础知识，适用于远程电子医疗保健和其他社交应用

作者:亚历山大·马尔哈辛

摘要: 最新医学的革命趋向可以公式化作为广泛介绍到电子 (电子健康) 和移动 (m 健康) 保健服务和信息应用的基本医学领域。不幸的是，所有合格的医疗保健服务清单只能在城市地区提供具有成本效益的服务，这些服务都覆盖了宽带 4g 5g 无线通信。需要对光学核心基础设施的部署进行高得令人无法接受的投资，以便利用最近 (4g) 和即将推出的 (5g) 宽带接入 (5g)，对人口稀少的农村、偏远和难以进入 (rrd) 地区进行无处不在的广泛覆盖，投资高得令人无法接受 ran) 集中的技术，以短的细胞范围为特征，因为他们的盈利边界超过几百居民每平方公里。此外，即将推出的物联网 (**iot**)、机器对机器 (m2m) 和许多其他机器类型的 it 系统的前所未有的要求和新功能，在设计极其绿色、灵活和为未来 5g 无线系统提供经济高效的技术，能够实时达到性能极值、权衡优化和基本极限。本文考察了 5g phy-mac 的基本原理和创造有利可图的无处不在的远程医疗服务和远程医疗的极端方法，作为 rrd 大众医疗保健和其他社会电子应用的主要创新技术界。建议的方法依赖于总结和发展我们以前的工作成果, rrd 适应盈利无处不在的绿色 4g ng 无线多功能技术。少

2017 年 11 月 17 日提交;最初宣布 2017 年 11 月。

评论:6 页, 8 位数字, 2017 年 ieee 工程、计算机和信息科学国际多会议 (sibiircon)

509. 建议: 1711.06 315[pdf,其他] Cs。直流

sparce: 生物意识通用核心扩展加速深神经网络

作者:sanchari sen, shubham jain, swagath venkataramani, anand raghunathan

摘要: 深神经网络 (dnn) 已成为解决各种机器学习任务的首选方法。dnn 带来的巨大计算需求通常通过自定义加速器的设计得到解决。然而，由于严格的区域成本限制，这些加速器在许多设计方案 (例如可穿戴设备和**物联网**传感器) 中令人望而却步。加速这些低功耗系统 (主要由通用处理器 (gpp) 内核组成) 上的 dnn 需要新的方法。我们通过利用 dnn 的一个关键属性 (即稀疏性) 来提高 dnn 在 gpp 上的性能。我们提出了稀疏感知核心扩展 (sparsity)-一组微体系结构和 isa 扩展，利用稀疏性，是最小的侵入性和低开销。我们动态检测零操作数，并跳过使用它的一组未来指令。我们的设计可确保无法将要跳过的指令提取，因为挤压指令会受到惩罚。sparce 由 2 个关键的微体系结构增强文件组成-一个跟踪零寄存器的稀疏级集文件 (sprf) 和一个显示要跳过的指令的稀疏感知跳过地址 (sasa) 表。提取指令时, sparce 动态地预先识别是否可以跳过以下指令并适当修改程序计数器，从而跳过冗余指令并提高性能。我们使用 gem5 架构模拟器对 sparce 进行建模，并在训练和推理的背景下，使用 caffe 框架对 6 个图像识别 dnn 进行了评估。在标量微处理器上, sparce 的应用级别降低了 19%-31%。我们还使用 openblas 库在 4 路 simd armv8 处理器上评估 sparce，并证明 sparce 在应用程序级执行时间上减少了 8%-15%。少

2017 年 11 月 29 日提交;v1 于 2017 年 11 月 6 日提交;最初宣布 2017 年 11 月。

510. 第: 1711.06041[pdf,其他] Cs。镍

通过智能 ddos 攻击行为学习保护异构物联网

作者:nhu-ngoc dao, trung v.phan, umar sa ad, joongheon kim, thomas bauschert, sungrae cho

摘要: 多样化的物联网 (**iot**) 服务和设备的迅速增加在连接、计算和安全性方面带来了诸多挑战，而网络必须面对这些挑战才能提供令人满意的支持。这导致网络演变为以多种接入技术和移动边缘计算 (mec) 功能为特征**的异构物联网**网络基础架构。网络、设备和服务的异质性给安全攻击带来了严重的漏洞，尤其是分布式拒绝服务 (ddos) 攻击，这些攻击利用大量**物联网**设备耗尽网络和受害者资源。因此，本研究建议利用 mec 电源在相关攻击源/目标网络的边缘部署多个智能滤波器，这是一个本地化的 ddos 预防框架。智能滤波器之间的合作由一个中央控制器监督。中央控制器根据攻击行为，通过将适当的训练参数输入自组织映射 (som) 组件来定位每个智能滤波器。利用三种典型**的物联网**流量方案验证了 mec 屏蔽框架的性能。数值结果表明，mec 屏蔽优于现有解。少

2017 年 11 月 16 日提交;最初宣布 2017 年 11 月。

评论:提交给 ieee 通信杂志

511. 第: 1711.05036[pdf] Cs。镍

多伊 10.1109/MCOM.2015.7263372

支持公开/软件定义的网络，实现高效和可扩展的物联网通信

作者:akram hakiri, pascal bersuu, aniruddha gokhale, slim abdellatif

摘要: -物联网 (**iot**) 是许多不同的使能技术的结果，如嵌入式系统、无线传感器网络、云计算、大数据等，用于收集、处理、推断和传输数据。整合所有这些技术需要开展全面和整体的研究工作，以应对这些技术带来的所有挑战，特别是在从物理世界向云托管服务的传感和信息传递方面。在本文中，我们概述了与标准化工作、对象移动性、网络和网关访问以及 qos 支持相关的最重要问题。特别是，我们描述了一种新型的**物联网**网络体系结构，它集成了软件定义的网络 (sdn) 和对象管理组的数据分发服务 (dds) 中间件。拟议的架构将改善**物联网**系统的服务交付，并为网络带来灵活性。少

2017 年 11 月 14 日提交;最初宣布 2017 年 11 月。

日记本参考:ieee 通信杂志，电气和电子工程师协会, 2015, 53 (9)，第 48-54 页。\&\ #x3008; 10.1109/MCOM.2015.7263372\& #x3009

512. 第: 1711. 03966[pdf] Cs。马

基于多智能体的物联网智能废物监控和收集架构

作者:eunice david Likotiko, devotha nyambo, joseph mwangoka

摘要: 固体废物管理是城市地区现有的挑战之一，由于人口的迅速增加，固体废物管理正成为一个关键问题。适当的固体废物管理系统对于改善环境和居民福祉十分重要。本文提出了一种用于实时废物监测和收集的物联网 (**iot**) 体系结构;能够改善和优化城市固体废物的收集工作。netlogo 多智能体平台已被用于模拟废物管理方面的实时监测和明智决策。垃圾箱和卡车收集过程中的废物灌装水平被抽象为多代理模式，公民通过支付垃圾收集服务的价格参与其中。此外，废物水平数据不断更新和记录，并提供给决策算法，以确定向城市分布式垃圾桶收集废物的最佳路线。执行了几个模拟案例并验证了结果。所提出的解决方案使废物收集过程更加有效，从而为所有废物利益攸关方带来了巨大的好处。少

2017 年 11 月 10 日提交;最初宣布 2017 年 11 月。

513. **第: 1711.03906[pdf,其他] Cs。Lg**

多伊 10.114/30840441. 3084049

d-slats: 分布式同时本地化和时间同步

作者:amr alanwar, henrique ferraz, kevin xeh, rohit Thazhath, paul martin, joao hespanha, mani srivastava, mani srivastava

摘要: 在过去的十年里，我们目睹了物联网 (**iot**) 设备的激增，随之而来的是，更需要在时间和空间上编排它们的行动。尽管这两个问题，即时间同步和本地化，有许多共同点，但它们传统上是单独处理或结合在集中式方法上处理的，这些方法会导致资源的难以言表的使用，或者是在不使用非可扩展的**物联网**设备数量。因此，我们提出了 d-sats，它由三种不同的独立算法组成，以分布式的方式共同解决时间同步和本地化问题。前两种算法主要基于分布式扩展卡尔曼滤波 (ekf)，而第三种算法则采用优化技术。不需要融合中心，设备只与邻居通信。在自定义超宽带通信试验台和表示静态和移动节点网络的四旋翼上对所提出的方法进行了评估。我们的算法可实现高达 3 微秒的时间同步精度和 30 厘米的定位误差。少

2017 年 11 月 10 日提交;最初宣布 2017 年 11 月。

514. **第: 1711.03832[pdf,其他] cs. it**

nb-iot 系统中的到达时间估计

作者:沙虎,李旭红,弗雷德里克·鲁塞克

摘要: 我们考虑到达时间 (toa) 估计在窄带物联网 (nb-iot) 系统中工作的设备的第一个到达路径.由于 **nb-iot** 中使用的 180 khz 带宽有限，传输的 nb 定位参考信号 (nprs) 的时域自相关函数 (acf) 具有宽的主瓣。如果不考虑这一点, toa 估计的性能可能会降低，原因有二。首先，在多径信道环境下，对应于不同接收路径的 nprs 相互叠加，对应的交叉相关关系也相互叠加。其次，用于检测 nprs 存在的测量峰值与平均功率比 (papr) 是不准确的。因此，本文提出了一种基于空间交替广义期望最大化 (sage) 的方法，用于联合估计 **nb-iot** 系统中的通道水龙头数量、信道系数和相应的延迟。考虑到 nprs 的不完善 acf。该方法仅使用接收信号与传输的 nprs 之间的时域交叉相关性，具有较低的复杂度。我们通过仿真表明，对该方法的 toa 估计对单通道的估计接近于最大似然 (ml) 估计，并且明显优于传统的使用信噪比 (snr) 或功率的 toa 估计器基于阈值的估计。少

2017 年 11 月 10 日提交;最初宣布 2017 年 11 月。

评论:6 页, 8 个数字

515. **建议: 1711. 03204[pdf,其他] Cs。直流**

elascale: 自动缩放和监视即服务

作者:hamzeh khazaei, rajsimman Ravichandiran , byungchul park, hadi bannazadeh, ali tizghadam, alberto leon-garcia

摘要: 自动可扩展性已成为云软件系统的一个明显功能，包括但不限于大数据和**物联网**应用。云应用程序提供商现在完全控制其应用程序的微服务和宏观服务;虚拟机和容器可以在运行时根据需要进行配置或取消配置。elascale 努力根据工作负载和整个应用程序堆栈的内部状态的变化来调整微观宏资源。elascale 利用弹性搜索堆栈来收集、分析和存储性能指标。然后, elascale 使用其默认缩放引擎弹性地调整托管应用程序。

elascale 中的提供程序、模式、插件和策略元素保证了可扩展性，通过这些元素，可以针对各种技术设计和实现灵活的可扩展性算法，包括被动和主动技术,基础设施和软件堆栈。在本文中，我们提出了 elascale 的结构和初步实现;将利用一个实例向通用**物联网**应用程序添加自动可伸缩性。由于对目标软件系统的依赖性为零，因此可以利用 elascale 为任何类型的云软件系统提供自动可扩展性和监控即服务。少

2017 年 11 月 8 日提交;最初宣布 2017 年 11 月。

516. **第: 1711. 02844[pdf,其他] Cs。燃气轮机**

移动区块链网络边缘计算资源管理的最优拍卖: 一种深度学习方法

作者:阮聪联,熊泽辉,王平, 都喜尼亚托

摘要: 区块链最近被应用于许多应用中，如比特币、智能电网和物联网 (**iot**)，作为交易的公共分类帐。然而，由于挖掘过程消耗了太多的移动设备上的计算和能源资源，在移动环境中使用区块链的情况仍然有限。边缘计算服务提供商提供的边缘计算可作为一种可行的解决方案，用于在移动区块链环境中从移动设备 (即矿工) 卸载挖掘任务。但是，需要设计一种边缘资源分配机制，以最大限度地提高边缘计算服务提供商的收入，并确保激励兼容性和个人理性仍然开放。本文在深度学习的基础上，为边缘资源配置开发了最优拍卖。具体而言，我们构建了一个基于最优拍卖解析解的多层神经网络体系结构。神经网络首先对矿工的投标进行单调的转换。然后，他们计算矿工的分配和有条件的支付规则。我们利用矿工的估值作为数据训练，调整神经网络的参数，以优化损失函数，这是边缘计算服务提供商的预期，否定的收入。实验结果表明，利用深度学习得出高收入移动区块链的最优拍卖效果，效果显著.

2017 年 11 月 16 日提交;v1 于 2017 年 11 月 8 日提交;最初宣布 2017 年 11 月。

517. **第: 1711.02825[pdf] Cs。铬**

基于机器学习技术的物联网机器人活动网络取证机制的构建

作者:nickolaos koroniotis, nour moustafa , elena sitnikova, jill slay

摘要: **物联网**是一个由相互连接的日常对象组成的网络，称为 "通过少量计算能力" 来增强的东西。最近,**物联网**受到各种不同僵尸网络活动的影响。由于多年来僵尸网络一直是造成严重安全风险和财务损失的原因，现有的网络取证技术无法识别和跟踪当前复杂的僵尸网络方法。这是因为商业工具主要依赖于基于签名的方法，而这些方法无法发现新形式的僵尸网络。在文献中，一些研究已经使用机器学习 ml 技术，以培训和验证定义此类攻击的模型，但它们仍然产生高误报率，挑战调查僵尸网络的轨迹。本文研究了 ml 技术在开发基于网络流标识符的网络取证机制中的作用，该机制可以跟踪僵尸网络的可疑活动。使用 unsw-nb15 数据集的实验结果表明，带有流标识符的 ml 技术可以有效地检测僵尸网络攻击及其轨迹。少

2017 年 11 月 7 日提交;最初宣布 2017 年 11 月。

518. **第: 1711.01454[pdf,其他] Cs。直流**

针对安全间歇性物联网设备的最佳检查

作者:zahra ghodsi, Siddharth garg, ramesh karri

摘要: 能量收集是为物联网 (**iot**) 设备供电的一个有前途的解决方案。由于这些能源的间歇性，不能保证程序执行的前进。以前的工作主张将中间状态检查为片外非易失性存储器 (nvm)。加密检查点解决了安全问题，但大大增加了检查点开销。在本文中，我们提出了一个新的在线检查点策略，它明智地确定何时到检查点，以便在保证安全性的

同时最大限度地缩短申请完成时间。与不考虑加密检查点开销的最先进的检查点方案相比，我们将执行时间提高到 1.4 倍。少

2017 年 11 月 4 日提交;最初宣布 2017 年 11 月。

评论:iccad 2017

519. 第: 1711.01336[pdf] Cs。直流

开放物联网异构资源的优化研究

作者:yoki yamato, naoto hoshikawa, hirofumi noguchi, tatsyua demizu, misao kataoka

摘要: 最近,**物联网**技术取得了进展，许多传感器和执行器都连接到了网络。此前,**物联网**服务是通过垂直集成风格开发的。但现在开放**物联网**的概念已经引起了人们的关注，通过集成水平分离的设备和服务来实现各种**物联网**服务。对于开放**物联网**时代，我们提出了隐性计算技术，以发现具有必要数据的设备，供用户按需使用，并动态使用它们。我们还实施了隐性计算的基本技术。本文提出了三层优化，以降低 tacit 计算服务的运行成本，提高其性能，从而使其成为已发现设备的连续服务。在优化过程中，在全面运行之前，为设备、网络和云层计算适当的功能分配。少

2017 年 11 月 3 日提交;最初宣布 2017 年 11 月。

评论:6 页，日本 2 个数字

报告编号:ieice 技术报告, sc2017-26, 2017 年 11 月

日记本参考:ieice 技术报告, sc2017-26, 2017 年 11 月。(c) 2017 年 ieice

520. 第: 1711.01320[pdf,其他] cs. it

射频无线功率传输: 重建未来网络

作者:ha-vu tran, georges kaddoum

摘要: 绿色无线电通信是一个新出现的议题，因为预计 2007 年至 2020 年期间，信息和通信技术 (信通技术) 服务的总体足迹将增加两倍。在这一研究领域，能量采集 (eh) 和无线功率传输 (wpt) 网络可以被评估为有希望的方法。本文综述了 eh 和 wpt 平台上未来绿色网络的最新发展趋势。通过重新思考射频 (rf)-wpt 的应用，引入了一个新的概念，即绿色 rf-wtp。因此，详细讨论了当前技术 (如小单元、毫米 (mm) 波和物联网 (**iot**) 网络) 之间的开放挑战和有希望的组合，以寻求解决问题的方法，以及如何重新绿化未来的网络? 少

2018 年 3 月 8 日提交;v1 于 2017 年 11 月 3 日提交;最初宣布 2017 年 11 月。

评论:6 页, 5 个数字

521. 第: 1711. 01306[pdf,其他] cs. it

基于深度学习的动态水印在物联网安全信号认证中的应用

作者:aidin ferdowsi, walid saad

摘要: 保护物联网 (**iot**) 是加快其应用程序和服务部署的必要里程碑。特别是,**物联网**设备的功能非常依赖于其消息传输的可靠性。网络攻击 (如数据注入、窃听和中间人威胁) 可能会导致安全挑战。保护**物联网**设备免受此类攻击需要考虑其严格的计算能力和低延迟操作的需求。本文提出了一种新的**物联网**信号动态水印检测网络攻击的深度学习方法。基于长短期存储器 (lstm) 结构的拟议学习框架使**物联网**设备能够从其生成的信号中提取一组随机特征，并动态地将这些特征水印到信号中。这种方法使 **iot** 的云中心

(从**物联网**设备收集信号) 能够有效地验证信号的可靠性。此外，该方法还可以防止网络攻击者从**物联网**设备中收集数据并旨在破坏水印算法的复杂攻击场景，如窃听。仿真结果表明，在攻击检测延迟不到 1 秒的情况下，可以从**物联网**设备传输消息，可靠性几乎达到 100%。少

2017 年 11 月 3 日提交;最初宣布 2017 年 11 月。

评论:6 页, 9 个数字

522. 第: 1711.0081[pdf, ps,其他] cs. it

无级无线接入物联网网络: 共存场景中的可扩展性分析

作者:meysam masoudi, amin azari, emre altug yavuz, cicek cavdar

摘要: 具有无赠款无线电接入的**物联网**网络 (如 sigfox 和 lora) 通过无证频段提供低成本的持久通信。由于对超耐用、电池寿命、**物联网**网络的需求日益增加，这些网络越来越受欢迎。大多数研究在进行单次无线接入技术部署的情况下对系统性能进行评估。本文研究了共存的竞争无线接入技术对系统性能的影响。考虑$\ mathpzc k $由时间和频率活动因素、带宽和功率定义的技术，共享一组无线电资源，我们推导出成功的传输概率、预期电池寿命和经验延迟作为到服务接入点的距离功能。我们的分析模型通过仿真结果验证，为评估共存场景和分析引入新的共存技术如何降低系统在成功概率和电池方面的性能提供了一个工具。一生。我们进一步研究了这种破坏性影响可以得到补偿的解决方案，例如，通过在一定程度上对网络进行致密化和利用联合接收。少

2017 年 11 月 1 日提交;最初宣布 2017 年 11 月。

523. 建议: 1711.00540[pdf, ps,其他] cs. it

物联网器件区块链同步的通信流量分析

作者:pietro danzi, anders ellersgaard kalör, Čedomir stefanović, petar popovski

摘要: 由于分散的会计机制，区块链是一种独特的技术，适用于在物联网 (**iot**) 生态系统中支持大量交易和智能合同。在区块链网络中，帐户的状态由验证器节点存储和更新，并以对等方式相互连接。**物联网**设备的特点是计算能力相对较低，功耗较低，以及零星和低带宽的无线连接。**物联网**设备连接到一个或多个验证器节点，以观察或修改帐户的状态。为了与帐户的最新状态交互，设备需要与验证器节点存储的区块链副本同步。在本文的工作中，我们介绍了**一般的**体系结构和同步协议，这些体系结构和协议能够将物联网端点同步到区块链，具有不同的通信成本和安全级别。我们对同步协议产生的流量进行了建模和分析描述，并通过数值模拟研究了功耗和同步的权衡。据我们所知，这是首次严格模拟无线连接在区块链驱动的**物联网**系统中的作用的研究。少

2018 年 2 月 12 日提交;v1 于 2017 年 11 月 1 日提交;最初宣布 2017 年 11 月。

评论:2018 年 ieee 国际通信大会 (icc) 接受论文

524. 第: 1711.0025[pdf,其他] Cs。铬

云互联网: 安全和隐私问题

作者:allan cook, michael robinson, mohamed amine ferrag, leandros a. maglaras, ying he,kevin jones, helge janicke

摘要: 云和**物联网**之间的协同作用在很大程度上是由于云具有直接惠及**物联网**并使其能够持续增长的属性。**iot** 采用云服务带来了新的安全挑战。在本书一章中，我们追求两个主要目标: 1) 分析云计算和**物联网**的不同组件, 2) 介绍这些系统面临的安全和隐

私问题。我们彻底研究了当前在这一领域存在的安全和隐私保护解决方案，着眼于工业物联网，讨论悬而未决的问题，并提出未来的方向少

2017 年 11 月 1 日提交;最初宣布 2017 年 11 月。

评论:27 页, 4 个数字

525. 第 17.11: 0057[pdf, ps,其他] Cs。镍

蓝牙 5: 迈向物联网的具体一步

作者:mario collotta, giovanni pau, timothy t 还好 , ozan k. tonguz

文摘 在标准 4.0 通过六年后，一个非营利协会----蓝牙特殊兴趣小组 (sig)----负责研究和开发技术标准，包括蓝牙标准，正式发布了蓝牙 5.0。它是短距离无线通信技术的重要发展之一。正如 sig 所指出的，新标准将永远改变人们对待物联网 (iot) 的方式，将其变成以近乎自然和透明的方式围绕物联网 (**iot**) 发生的事情。在本文中，介绍了未来的**物联网**方案和用例，这些方案和用例证明了对蓝牙 5 的推动是合理的。介绍了蓝牙 5 中包含的一组新技术功能，并介绍了它们的优缺点。少

2017 年 11 月 1 日提交;最初宣布 2017 年 11 月。

评论:17 页, 3 个数字, 3 个表, 15 个参考, ieee 通信杂志杂志

526. 第 xiv:1711. 0044[pdf,其他] Cs。直流

压缩深神经网络的高效推理

作者:dharma teja vooturi, Saurabh goyal, anamitra r.choudhury, yogish sabharwal, ashish verma

摘要: 深度神经网络中的大量权重使得模型难以部署在低内存环境中，如移动电话、**物联网**边缘设备以及云上的 "作为服务的推理" 环境。以前的工作已经考虑到减少模型的大小，通过压缩技术，如修剪，量化，赫夫曼编码等。然而，使用压缩模型的有效推理却很少受到关注，特别是在赫夫曼编码到位的情况下。本文提出了在各种内存约束下，单图像和批处理推理的有效并行算法。我们的实验结果表明，我们使用可变批处理大小进行推理的方法在保持内存和延迟约束的同时，在 alex net 的推理吞吐量方面实现了 15-25 的性能改进。少

2017 年 11 月 1 日提交;最初宣布 2017 年 11 月。

527. 建议: 1710.06564[pdf,其他] Cs。Lg

多伊 10.1109/IoTDI.2018.00025

替换自动编码器: 一种用于感官数据分析的预置算法

作者:mohammad malekzadeh, richard g. cleg, hamed haddadi

摘要: 移动、物联网 (**iot**) 和可穿戴设备上越来越多的传感器生成物理活动的时间序列测量。尽管获得感官数据对于许多有益应用的成功至关重要，如健康监测或活动识别，但也可以通过获得感官发现有关个人的各种潜在敏感信息数据，这不能很容易地使用传统的隐私方法来保护。本文提出了一个隐私保护传感框架，用于管理对时间序列数据的访问，以便在保护个人隐私的同时提供效用。我们引入了替换自动编码器，这是一种新的算法，它学习如何将与敏感推理相对应的数据的判别特征转换为一些在非敏感推理中观察到的特征，以保护用户 "隐私。通过为深度自动编码器定义用户自定义的目标函数，实现了这一效率。我们的替换方法不仅可以消除识别敏感推断的可能性，还可以消除检测这些推断发生的可能性。这是其他方法 (如过滤或随机化) 的主要弱点。我们利用对三个基准数据集的大量实验，在多传感环境中通过活动识别任务来评估该算法

的有效性。我们证明，它可以保留最先进技术的识别精度，同时保护敏感信息的隐私。最后，我们利用 gans 检测数据发布后发生的替换情况，并表明只有在对用户的原始数据进行对抗网络培训的情况下才能做到这一点。少

2018 年 2 月 27 日提交;v1 于 2017 年 10 月 17 日提交;最初宣布 2017 年 10 月。

评论:12 页, 11 位数字

msc 类: 68t05 类: I.2。6

528. 第: 1710.04919[pdf] Cs。直流

云计算中的机器人即服务: 大型灾害中的搜救案例研究

作者:carla mouradian, sami yangui, roch h. g 物洛

摘要: 物联网 (**iot**) 有望通过互联网连接传感器和机器人等对象，实现无数的应用。**物联网**应用范围从医疗保健到自主车辆，包括灾难管理。要在云环境中实现这些应用程序，需要设计适当的**物联网**基础架构即服务 (iaas)，以简化**物联网**对象作为云服务的配置。本文讨论了大规模灾害场景中搜索救援物**联网**应用的案例研究。它提出了一个**物联网** iaas 架构，该架构虚拟化机器人 (机器人的 iaas)，并将其提供给上游应用程序即服务。支持节点和网络级机器人虚拟化。该体系结构满足了一组已确定的要求，例如需要为异构机器人建立统一的描述模型、发布/发现机制，以及在需要时与其他 iaas 机器人联合起来。建立了概念验证的验证方法，并对其性能进行了实验研究。讨论了吸取的经验教训和未来的研究方向。少

2017 年 11 月 3 日提交;v1 于 2017 年 10 月 13 日提交;最初宣布 2017 年 10 月。

529. 第 1710.04[pdf, ps,其他] cs. cy

多伊 10.100/cp.4370

物联网和智能领域的分布式混合仿真

作者:gabriele d ' angelo, Stefano ferretti, vittorio ghini

摘要: 本文介绍了利用混合仿真构建和组合异构仿真场景的方法，这些场景可以熟练地用于建模和表示物联网 (**iot**)。混合仿真是一种结合模型/模拟多种模式的方法。复杂场景被分解为更简单的场景，每个场景都通过特定的模拟策略进行模拟。然后对所有这些模拟构建块进行同步和协调。这种模拟方法是代表**物联网**设置的理想方法，由于大量部署传感器和设备所产生的可能场景的异质性，这些设置通常要求很高。我们提出了一个与智能区域的分布式模拟有关的用例，这是一种分散地理空间的新视图，由于使用**了物联网**，构建了 ict 服务，以可持续且无害的方式管理资源。对环境的影响。将三种不同的仿真模型组合在一起，即基于自适应代理的并行分布式模拟器、基于 omnet + 的离散事件模拟器和基于 matlab 的脚本语言模拟器。性能分析的结果证实了使用混合模拟对复杂**的物联网**方案进行建模的可行性。少

2018 年 4 月 10 日提交;v1 于 2017 年 10 月 6 日提交;最初宣布 2017 年 10 月。

评论:arxiv 管理说明: 实质性文本重叠与 arxiv:1605 5.04876

日记本参考:并发与计算: 实践与经验, wiley, 第 30 卷, 第 9 期 (2018 年 5 月)。issn:1532-0634

530. 建议: 1710.03473[pdf,其他] Cs。镍

基于信息的网络 (icn-iot) 的最新进展

作者:sobia arshad, muhammad awais azam,mubashir husain rehmani, jonathan loo

摘要: 以信息为中心的网络 (icn) 正在被实现为实现当前基于 ip 地址的网络的缺点的一种有希望的方法。icn 模型基于命名内容以消除地址空间稀缺，通过基于名称的路由访问内容，在中间节点缓存内容以提供可靠、高效的数据传递和自我认证内容，以确保更好地实现安全。icn 在快速、高效的数据交付和更高的可靠性方面的显著优势使 icn 成为物联网 (**iot**) 环境中非常有前途的网络模型。**物联网**的目标是在任何地方的任何路径上随时连接任何人或任何东西。从过去十年开始，**iot** 吸引了业界和研究界。**iot** 是一个新兴的研究领域，目前仍处于起步阶段。因此，本文通过提供最先进的文献调查，介绍了 icn 对 **iot** 的潜力。我们简要讨论了 icn 特性及其模型 (和体系结构) 在**物联网**环境中的可行性。随后，我们对基于 icn 的 **iot** 缓存、命名、安全性和移动性方法进行了全面的调查，并进行了适当的分类。此外，我们还介绍了 icnot 的操作系统 (os) 和仿真工具。最后，我们为 **iot** 提供了重要的研究挑战和 icn 面临的问题。少

2018 年 10 月 12 日提交;v1 于 2017 年 10 月 10 日提交;最初宣布 2017 年 10 月。

评论:物联网杂志

531. **决议: 1710.02282[pdf, ps,其他] Cs。pf**

多伊 10.1109/DISTRA.2017.8167672

物联网仿真中的可扩展性和准确性探索: 一种基于多层次仿真的方法

作者:Stefano ferretti, gabriele d ' angelo, vittorioghini, moreno marzolla

文摘: 本文提出了一种利用多层次仿真模型模拟物联网 (**iot**) 的方法。对于传统的模拟器，这种方法使我们能够在不影响模拟可伸缩性的情况下调整模型不同部分的详细级别。作为一个用例，我们开发了一个两级模拟器，以研究在农村地区部署智能服务的情况。较高的层次是基于粗粒度的、基于代理的自适应并行和分布式模拟器。在需要时，此模拟器生成 omnet ++ 模型实例，以便更详细地评估模拟世界中限制区域的无线通信相关问题。性能评估证实了**物联网**环境的多层次模拟的可行性。少

2018 年 8 月 7 日提交;v1 于 2017 年 10 月 6 日提交;最初宣布 2017 年 10 月。

评论:分布式仿真和实时应用国际研讨会论文集 (ds-rt 2017)

532. **第 xiv:1710.00560[pdf, ps,其他] Cs。Db**

kv 匹配: 支持归一化和时间扭曲的子序列匹配方法 [扩展版本]

作者:吴嘉业,王鹏,潘宁亭, 王晨, 王伟,王建民

摘要: 由于数据中心管理和**物联网**等新应用程序的普及，时间序列数据量激增。子序列匹配是挖掘时间序列数据的一项基本任务。所有基于索引的方法只考虑原始子序列匹配 (rsm)，不支持子序列归一化。ucr 套件可以处理归一化子序列匹配问题 (nsm)，但需要扫描全时序列。本文提出了一个新的问题，即约束归一化子序列匹配问题 (cNSM)，为 nsm 问题增加了一些约束。cNSM 问题为灵活控制偏移偏移和振幅缩放的程度提供了一个旋钮，使用户能够构建索引来处理查询。提出了一种新的指标结构、kv 指数和匹配算法 kv 匹配。通过单一索引，我们的方法可以在 ed 或 dtw 距离下同时支持 rsm 和 cNSM 问题。kv 索引是一种键值结构，可以很容易地在本地文件或 hbase 表上实现。为了支持任意长度的查询，我们将 kv 匹配扩展到 kv 匹配 DP，它使用多个可变长度索引来处理查询。我们在合成数据集和真实世界数据集上进行了广泛的实验。结果验证了我们方法的有效性和效率。少

2018 年 9 月 9 日提交;v1 于 2017 年 10 月 2 日提交;最初宣布 2017 年 10 月。

评论:13 页

533. **第: 1709.01015[pdf,其他] Cs。镍**

室内本地化系统与技术综述

作者:faheem zafari, Athanasios gkelias, kin leung

摘要: 由于室内本地化可以通过利用物联网 (**iot**) 和无处不在的连接提供潜在的广泛服务，室内本地化的兴趣最近有所增加。文献中提出了不同的技术、无线技术和机制，以提供室内本地化服务，从而改善为用户提供的服务。然而，缺乏纳入最近提出的一些准确和可靠的本地化系统的最新调查文件。本文旨在详细介绍不同的室内定位技术，如到达角 (aoa)、飞行时间 (tof)、飞行回程时间 (rtof)、接收信号强度 (rss);基于 wifi、射频识别设备 (rfid)、超宽带 (uwb)、蓝牙和文献中提出的系统等技术。本文主要讨论了人类用户及其设备的本地化和定位。我们强调文献中提出的现有制度的优势。与现有调查相比，我们还从能源效率、可用性、成本、接收范围、延迟、可扩展性和跟踪准确性的角度对不同的系统进行评估。我们没有比较技术或工艺，而是比较本地化系统，总结它们的工作原理。我们还讨论了准确的室内定位仍然存在的挑战。少

2018 年 3 月 14 日提交;v1 于 2017 年 9 月 4 日提交;最初宣布 2017 年 9 月。

评论:这项工作已提交 ieee，以便可能出版

534. 第 (xiv:170 9.000999)[pdf] Cs。镍

多伊10.1109/MNET.2017.1700081

大容量机器类型通信的窄带物联网数据传输程序

作者:pilar andlear-maldonado, pablo amigeiras, jonathan pradoss-garzon,豪尔赫·纳瓦罗- ortiz, juan m. Lopez-Soler

摘要: 大规模部署大型机器类型通信 (mmtc) 涉及蜂窝网络上的几个挑战。为了应对 mmtc (更广泛地说，物联网 (**iot**)) 的挑战，第三代合作伙伴项目开发了窄带**物联网** (nb-iot)，作为第 13 版的一部分。**nb-iot** 旨在提供更好的室内覆盖范围，支持大量低吞吐量设备，具有宽松的延迟要求和更低的能耗。**nb-iot** 通过简化和优化重用长期演进功能。特别是对于小型数据传输,**nb-iot** 指定了两个减少所需信令的过程：一个基于控制平面 (cp)，另一个基于用户平面 (up)。在这项工作中，我们概述了这些程序，并对其业绩进行了评价。能耗结果表明，在考虑的情况下，两种优化均可在较大范围内延长电池寿命 2 年以上，cp 可达到 8 年，覆盖范围良好。就细胞容量而言，cp 从 26% 提高到 224%，up 范围从 36% 提高到 165%。除了某些特定配置外，cp 和 up 优化的比较会产生类似的结果。少

2018 年 3 月 13 日提交;v1 于 2017 年 9 月 4 日提交;最初宣布 2017 年 9 月。

评论:接受 ieee 网络杂志. 17 页，5 个数字，1 个表

日记本参考:ieee 网络 (卷:31，发行: 6，2017 年 11 月至 12 月)

535. 第: 1709. 00462[pdf,其他] Cs。直流

移动边缘计算增强物联网

作者:nirwan ansari,香孙河

摘要: 在本文中，我们提出了一个移动边缘物联网 (meiot) 架构，利用光纤无线接入技术，云发展概念，和软件定义的网络框架。meiot 架构将计算和存储资源与物联网 (**iot**) 设备紧密结合，以加快**物联网**数据共享和分析。具体来说,**物联网**设备 (属于同一用户) 与附近云中的特定代理虚拟机 (vm) 相关联。代理虚拟机实时存储和分析**物联网**数据 (由其**物联网**设备生成)。此外，我们还在 meiot 环境中引入了语义**和社交物联网技术,** 以解决**物联网**系统中的互操作性和低效访问控制问题。此外，我们还提出了两种动态代

理虚拟机迁移方法，以最大限度地减少代理虚拟机与其**物联网**设备之间的端到端延迟，并分别最大限度地降低云的网格能耗总量。通过大量的仿真验证了所提出方法的性能。少

2017 年 11 月 1 日提交;v1 于 2017 年 9 月 1 日提交;最初宣布 2017 年 9 月。

536. **第 (xiv:1709 9.00105)[pdf, ps,其他] Cs。直流**

酒店业的技术：前景与挑战

作者:prasanna kansakar, arslan munir , neda shabani

摘要: 休闲和接待行业是全球经济的推动力之一。近年来，这一行业广泛采用新技术，从根本上改变了提供和接受服务的方式。在本文中，我们探讨了目前在酒店业使用的一些最先进的技术，以及它们是如何改善客人体验和改变酒店服务平台的。我们还设想了一些潜在的未来酒店服务，随着物**联网** **(iot)** 技术的不断发展，我们可以期待这些服务。我们认识到，许多接待机构的技术骨干需要改革，以促进现代世界不断变化的技术格局。我们讨论了一些需要克服的基本挑战，以便为酒店业建立一个持久的面向未来的解决方案。我们还讨论了这些挑战给客人和酒店服务提供商 (hsp) 带来的问题。少

2018 年 2 月 6 日提交;v1 于 2017 年 8 月 31 日提交;最初宣布 2017 年 9 月。

评论:可在 ieee 消费电子杂志上发布, 2018 年

537. **第 xiv:1708.05905[pdf,其他] Cs。Hc**

为实用主义者和原教旨主义者设计：物联网上的隐私问题和态度

作者:lesandro ponciano, pedro barbosa, francisco brasileiro, andrey brito, nzareno andrade

摘要: 物联网 (**iot**) 系统引起了人们的热情和关注。热情来自于人们日常生活中的公用事业，人们的担忧可能与隐私问题有关。通过使用两个**物联网**系统作为案例研究，我们检查用户的隐私信念、担忧和态度。我们关注四个主要方面：个人数据的收集、新信息的推断、与第三方的信息交流以及系统功能带来的风险效用权衡。总共有 113 名巴西人回答了关于这些层面的调查。虽然他们的看法似乎取决于背景，但也有反复出现的模式。我们的研究结果表明,**物联网**用户可以分为不关心、原教旨主义者和实用主义者。他们中的大多数人表现出实用主义的形象，并相信隐私是法律保障的一项权利。最隐私的方面之一是向第三方交换个人信息。个人感知到的风险与他们在系统特征中感知到的效用呈负相关。我们讨论了这些结果的实际含义，并建议在设计**物联网**系统时考虑隐私问题的启发式方法。少

2018 年 1 月 19 日提交;v1 于 2017 年 8 月 19 日提交;最初宣布 2017 年 8 月。

评论:巴西计算系统中的人为因素专题讨论会 (hc' 17), 2017 年 10 月 23 日至 27 日，巴西 sc joinville, 5 个数字

类:K.4.1;H.1。2

538. **第: 1708. 00052[pdf,其他] Cs。简历**

基于 fpga 的数据流平台上的大型量化神经网络流体系结构

作者:chaim baskin, natan liss , evgenii zheltonozhskii, alex m. bronshtein, avi mendelson

摘要: 深度神经网络 (dnn) 由在一系列计算机体系结构上执行的不同应用程序使用，从**物联网**设备到超级计算机。这些网络的占地面积是巨大的，它们的计算和通信需求也是巨大的。为了减轻对资源的压力，研究表明，在许多情况下，权重和其他参数的低精

度表示 (每个参数 1-2 位) 可以在所需资源较少的情况下实现类似的精度。使用量化值可以使用 fpga 来运行 nn，因为 fpga 很适合这些基元;例如，fpga 为按位操作提供了高效的支持，并且可以使用任意精确的数字表示。本文提出了一种在 fpga 上运行 qnn 的新的流体系结构。拟议的体系结构比替代架构扩展得更好，使我们能够利用具有多个 fpga 的系统。我们还包括对跳过连接的支持，这些连接在最先进的 nn 中使用，并表明我们的架构几乎可以免费添加这些连接。所有这些都使我们能够实现一个 18 层 resnet 的 224x224 图像分类，实现了 57.5 的前一的准确性。此外，我们还实现了一个全尺寸的量化亚历克网。与以前的作品不同的是，我们使用 2 位激活而不是 1 位激活，这将 alesnet 的前 1 名准确性从 41.8 提高到 51.03 的 imagenet 分类。alresnet 和 resnet 都可以在 fpga 上处理 1000 类实时分类。与最新 nvidia gpu 上的相同 nn 相比，我们实施的 renet-18 功耗降低了 5 倍，而且 imagenet 的功耗降低了 4 倍。较小的 nn 适合单个 fpga，在小型 (32x32) 输入上的运行速度快于 gpu，同时消耗的能量和功率减少了 20x。少

2018 年 3 月 13 日提交;v1 于 2017 年 7 月 31 日提交;最初宣布 2017 年 8 月。

评论:将出现在 raw 2018 中

539. 特别报告: 1707.05425[pdf] Cs。简历

快速准确的图像超分辨率由深 cnn 与跳过连接和网络在网络

作者:金山中县, shigesumi kuwashima, takio k 鲁 ita

摘要: 我们提出了一种高效、快速的具有深卷神经网络 (深 cnn) 的单图像超分辨率 (sisr) 模型。深美国有线电视新闻网最近表明，他们在单图像超分辨率上有显著的重建表现。目前的趋势是使用更深层次的 cnn 层，以提高性能。然而，深模型需要更大的计算资源，并不适合移动、平板电脑和**物联网**设备等网络边缘设备。我们的模型实现了最先进的重建性能与至少 10 倍的计算成本较低的深有线电视新闻网与残余网络，跳过连接和网络在网络 (dcscn)。深度 cnn 和跳过连接图层的组合用作本地和全局区域上图像要素的特征提取器。并行 1x1 cnn，就像一个称为网络中的网络，也用于图像重建。该结构减少了前一层输出的尺寸，以加快计算速度，减少信息丢失，并使直接处理原始图像成为可能。此外，我们还优化了每个 cnn 的层数和过滤器，以显著降低计算成本。因此，该算法不仅达到了最先进的性能，而且实现了更快、更高效的计算。代码可 https://github.com/jiny2001/dcscn-super-resolution

2018 年 9 月 29 日提交;v1 于 2017 年 7 月 17 日提交;最初宣布 2017 年 7 月。

评论:9 页，4 个数字。本论文在第 24 届国际神经信息处理大会 (iconip 2017) 上被接受

期刊参考:第 24 届神经信息处理国际会议，iconip 2017，会议记录，第二部分 (第 217-225 页)

540. 第 07.008005[pdf,其他] Cs。镍

以知识为中心的网络的愿景与挑战

作者:吴大鹏、李振江、王建平、郑元庆、莫丽、黄秋远

摘要: 在创建智能未来信息社会的过程中，物联网 (**iot**) 和内容中心网络 (ccn) 为前端传感和后端网络打破了两个关键障碍。然而，我们仍然观察到目前网络流量控制和系统管理的缺失部分，例如，缺乏渗透到传感和网络的知识，以整体地粘合它们。在本文中，我们设想利用新兴的机器学习或深度学习技术来创造知识的各个方面来促进设计。特别是，我们可以从收集的数据中提取知识，以减少数据量，增强系统智能和交互性，提高服务质量，提高通信，提高可控性和成本。我们将这样一个面向知识的流量控制和网

络管理范式命名为以知识为中心的网络 (kcn)。本文介绍了 kcn 的基本原理、kcn 的好处、相关工作和研究机会。少

2018 年 6 月 23 日提交;v1 于 2017 年 7 月 3 日提交;最初宣布 2017 年 7 月。

541. 第 07h:170 6.09711[pdf] Cs。哦

电力公用事业的智能资产管理: 大数据与未来

作者:swasti r. khuntia, jose l.rueda , mart a. m. van der Meijden

摘要: 本文从大数据和新技术的角度讨论了未来的挑战。公用事业公司一直在收集大量数据，但由于数量巨大，而且存在不确定性，因此几乎没有加以利用。资产的状态监测在日常操作中收集大量数据。问题产生于 "如何从大量数据中提取信息？"随着机器学习技术的出现，大数据分析正对 "富数据和糟糕的信息" 的概念提出挑战。随着物联网 (**iot**) 等技术的进步，大数据分析将在电力企业中发挥重要作用。在本文中，通过途径和指南来应对挑战，使当前的资产管理实践在未来更加明智。少

2018 年 2 月 17 日提交;v1 于 2017 年 6 月 18 日提交;最初宣布 2017 年 6 月。

评论:13 页, 3 个数字，《2017 年第十二届世界工程资产管理大会 (wceam) 论文集》

542. 第 1705.0230[pdf,其他] Cs。直流

实现基于区块链的物联网数据的可审计存储和共享

作者:hossein shafagh, lukas burkhalter, anwar hithnawi, simon duquennoy

摘要: 如今，云在存储、处理和分发数据方面发挥着核心作用。尽管为**物联网**应用的快速发展做出了贡献，但目前的**物联网**以云为中心的架构已形成无数孤立的数据孤岛，阻碍了整体**数据驱动分析在物联网**。本文提出了一种基于块**链**的物联网设计，它带来了分布式访问控制和数据管理。我们背离了目前的信任模型，该模型将对数据的访问控制委托给一个集中的受信任机构，而是赋予用户数据所有权。我们的设计是为**物联网**数据流量身定制的，可实现安全的数据共享。我们通过将区块链作为存储层的可审核和分布式访问控制层，实现安全且有弹性的访问控制管理。我们通过使用区块链技术管理的具有本地化意识的分散存储系统，促进在网络边缘存储时间序列**物**联网数据。我们的系统是物理存储节点的不可知性，支持云存储资源作为存储节点的利用。少

2017 年 11 月 14 日提交;v1 于 2017 年 5 月 22 日提交;最初宣布 2017 年 5 月。

543. xiv:1705.03288[pdf,其他] Cs。镍

多伊 10.1109/MCOM.2017.1600617

物联网的不协调访问方案: 方法、法规和性能

作者:daniel zucchetto, andrea zanella

摘要: 物联网 (**iot**) 设备使用各种协议进行通信，在许多方面有所不同，而通道访问方法是最重要的方法之一。大多数明确为**物联网**和机器对机器 (m2m) 通信设计的传输技术要么使用基于 al 董建华的信道访问，要么使用基于载波传感的某种类型的 "通话前听" (lbt) 策略。本文结合 etsi 和 fcc 监管框架，对**物联网**技术 (即基于 al 董建华和 lbt 计划) 的不协调信道访问方法进行了比较综述。此外，我们还在典型**的物联网**部署中提供了这些接入方案的性能比较，包括成功传输和能源效率方面的性能比较。结果表明, lbt 即使在远距离传输中也能有效地减少节点间干扰，但其能效可以低于 aloha 方法提供的能量效率。速率适应方案的采用进一步降低了能耗，同时提高了与接收机不同距离的节点之间的公平性。还对共存问题进行了调查，这表明在大规模部署中, lbt 受到同一地区有 aloha 设备的严重影响。少

2017 年 12 月 6 日提交;v1 于 2017 年 5 月 9 日提交;最初宣布 2017 年 5 月。

日记本参考:ieee 通信杂志，第 55 卷，第 9 号，48-54 页，2017

544. 第 1704.08688[pdf,其他] Cs。铬

多伊 10.14569/IJACSA.2017.080151

sit: 一种安全物联网的轻量级加密算法

作者:muhammad usman, irfan ahmed, m. imran aslam, shujaat khan, usman ali shah

摘要: 物联网 (**iot**) 是未来一项很有前途的技术，预计将连接数十亿台设备。通信数量的增加预计将产生堆积如山的数据，数据的安全性可能是一个威胁。体系结构中的设备基本上更小，功耗较低。传统的加密算法由于其复杂性，通常计算成本很高，需要多次加密，这实质上是浪费了小工具的受限能量。但是，较不复杂的算法可能会损害所需的完整性。本文提出了一种称为安全**物联网**(sit) 的轻量级加密算法。它是 64 位块密码，需要 64 位密钥来加密数据。该算法的体系结构是一个混合的狂热和一个统一的替代置换网络。仿真结果表明，该算法仅在五轮加密中提供了实质性的安全性。该算法在低成本的 8 位微控制器上实现了硬件，并与基准加密算法进行了代码大小、内存利用率和加密解密执行周期的比较。相关模拟的 matlab 代码可在 https://goo.gl/Uw7E0W 在线查阅。少

2018 年 3 月 22 日提交;v1 于 2017 年 4 月 27 日提交;最初宣布 2017 年 4 月。

评论:原始文章可在 sai ijacsa 第 8 卷第 1 期 2007 年

日记本参考:(ijacsa) 国际高级计算机科学与应用杂志，第 8 卷，第 1 期，2017 年

545. 第 xiv:1704. 04174[pdf,其他] Cs。镍

在基于 lrawan 的 lpwa 网络中，双向流量的危害是否大于好处?

作者:亚历山大·伊安普普, usman raza, parag kulkarni, mahesh sooriyabandara

摘要: 由于需要低功耗、远距离和低成本的连接来满足**物联网**应用的要求，因此出现了低功耗广域 (lpwa) 网络技术。这些技术承诺以低成本无线连接大量分散在不同地理位置的设备，这继续吸引学术界和企业界的极大关注。尽管这些技术的性能尚未完全了解，但目前已经在进行几次推出。鉴于这些发展，需要使用工具进行 "假设分析" 和部署前研究，以了解在设计时做出的选择的含义。虽然 lpwa 空间中有几种很有前途的技术，但本文特别关注的是 lora/lorawan 技术。特别是，我们介绍了 lorawansim，这是一个模拟器，它扩展了 lorasim 工具，以添加对 lrawan mac 协议的支持，该协议采用双向通信。这是任何其他 lora 模拟器中都不可用的突出功能。随后，我们通过大量的模拟提供了有关基于 lorwan 的网络性能的重要见解。特别是，我们表明，早期研究报告的可实现的网络容量相当乐观。下行流量的引入会对上行吞吐量产生重大影响。在 lorawan 规范中建议的传输尝试次数可能并不总是最佳选择。我们还强调了与选择重传输尝试次数相关的能耗与可靠性权衡。少

2017 年 12 月 14 日提交;v1 于 2017 年 4 月 13 日提交;最初宣布 2017 年 4 月。

评论:包括应用原始 lorasim 中的错误修复后更新的图形，从该版本中对 lorawansim 进行了调试-6 页、6 个数字、1 个表

546. 第 1704. 008 1988[pdf,其他] cs. it

一种新的时空模型下的大规模物联网网络随机访问分析: 一种随机几何方法

作者:南江,邓燕莎,新康 , arumugam nallanathan

摘要: 大规模的物联网 (miot) 为构建强大且无处不在的连接提供了一个良好的机会，这些连接面临着大量新的挑战，蜂窝网络由于具有较高的可扩展性、可靠性和效率。随机存取链 (rach) 过程是基于蜂窝**的 mIoT** 网络中物联网设备和基站 (bs) 之间建立连接的第一步，在该网络中，对物理层静态属性之间的相互作用进行建模在每个**物联网**设备中不断发展的队列的网络和动态特性具有挑战性。为了解决这一问题，我们提供了一个新的流量感知时空模型来分析基于蜂窝的 miot 网络中的 rach，在这种模型中，基于空间域中的随机几何对物理层网络进行建模和分析，队列演化是基于时域概率论进行了分析。对于性能评估，我们推导出随机选择的每个插槽中具有不同例来述的**物联网**设备的前导传输成功概率的确切表达式，从而深入了解每个例期间的有效性。.我们获得的分析结果通过真实的模拟来验证，这些模拟捕捉了每个**物联网**设备中数据包的演变。该数学模型和分析框架可简单地结合基于蜂窝的网络的前导传输原理，用于评价其他类型的 rach 方案在其性能上的表现。少

2018 年 7 月 4 日提交;v1 于 2017 年 4 月 6 日提交;最初宣布 2017 年 4 月。

547. 第 07:17003892[pdf,其他] cse

设计注意原始的物联网应用

作者:charith perera, mahmoud barhamgi, ar 间 sha k.bandara, Barhamgi ajmal, blaine price, bashar nausebeh

摘要: 物联网 (**iot**) 应用程序通常收集和分析可用于获取有关个人的敏感信息的个人数据。然而，到目前为止，在设计**物联网**应用程序时，软件工程过程中还没有明确考虑隐私问题。在本文中，我们探讨了作为一组准则而制定的基于设计的设计框架如何能够帮助软件工程师设计隐私感知的**物联网**应用程序。我们通过研究软件工程师如何使用 pbd 框架来设计**物**联网应用，从而研究了我们提出的 pbd 框架的效用。我们还探讨了使用一套准则来影响**物联网**应用设计过程的挑战。本文还重点介绍了提供一个框架的好处，该框架可帮助软件工程师明确考虑**物联网**应用的隐私问题，并揭示了与我们的方法相关的一些挑战。我们的研究表明, pbd 框架显著提高了新手和专业软件工程师设计隐私**感知物联网**应用的能力。少

2018 年 4 月 26 日提交;v1 于 2017 年 3 月 10 日提交;最初宣布 2017 年 3 月。

评论:技术报告

548. 第 07:170000541[pdf,其他] Cs。镍

当物联网将人挡在循环中时: 迈向新的全球实用程序的路径

作者:vitaly petrov, konstantin mikhaylov, dmitri moltchanov, sergey andreev, gbor fodor, joh torsner, halim yanikomeroglu, markku juntti , yevgeni 库切里亚维

摘要: 虽然物联网 (**iot**) 在支持单个机器类型应用程序方面取得了重大进展，但直到最近，人们作为整个**物联网**不可或缺的组成部分的重要性才被视为基础设施已开始得到充分承认。为了促进这一愿景，出现了几个强有力的概念，无论是在需要的时候涉及人类环境，还是直接影响用户行为和决定。由于这些成为将**物联网**发展成为一个新型以人为本的公用事业的垫脚石，本文概述了实现这一决定性转变的途径。我们首先回顾了人类感知无线网络的最新进展，然后对有吸引力的人机应用进行分类，并总结了启用**物联网的无线电**技术。我们继续对具有代表性的城市**物联网**方案进行独特的系统级性能定性，并量化将人们留在各个级别的循环中的好处。我们全面的数字结果证实了在更严格的用户参与下所取得的重大进展，也证实了有效激励机制的发展，从而为未来的商品化打开了大门。以人为中心的全球物**联网实用程序**。少

2018 年 9 月 18 日提交;v1 于 2017 年 3 月 1 日提交;最初宣布 2017 年 3 月。

评论:8 页, 5 个数字。这项工作已被 ieee 通信杂志所接受, 2019 年

549. 建议: 170008817[pdf,其他] Cs。直流

多伊 10.1016/j.scs.2018.02.013

通过传感器分组汇总物联网数据

作者:Stefano bennati, evangelos pournaras

摘要: 使用物联网 (**iot**) 普及技术的大数据收集做法往往带有隐私侵入性, 并导致对公民的监视、特征分析和歧视行为, 进而损害公民的参与可持续发展的智慧城市。然而, 来自**物联网**设备的实时数据分析和汇总信息为管理智慧城市基础架构提供了巨大的机遇。分布式传感器数据的隐私增强聚合, 如住宅能耗或交通信息, 是本文的研究重点。公民可以选择自己的隐私级别, 降低共享数据的质量, 而牺牲数据分析服务的准确性。考虑了一种基线方案, 即**与**不可信的中央聚合器直接共享物联网传感器数据。引入了一种分组机制, 通过首先在组级别共享聚合的数据来提高隐私, 而不是直接将数据共享到中央聚合器。分组级聚合模糊了个人的传感器数据, 其方式类似于差分隐私和同态加密方案, 因此, 与基线方案。拟议的系统使用两个智慧城市试点项目的真实数据进行评估。分组下的隐私增加, 同时保持基线方案的准确性。衡量了一个群体成员对另一个群体成员的群体内隐私的影响, 发现具有类似隐私选择的群体成员之间对隐私的公平性得到了最大化。比较了几种分组策略。通过邻近的隐私选择进行分组, 可获得最高的隐私收益。讨论了该战略对激励机制设计的影响。少

2018 年 3 月 1 日提交;v1 于 2017 年 2 月 28 日提交;最初宣布 2017 年 2 月。

550. 建议: 170004054[pdf, ps,其他] cs. it

物联网网络中基于矩阵完成的本地化

作者:luong trung nguyen, junhankim, sangtae kim, byonghyo shim

摘要: 为了对从物**联网** (**iot**) 设备收集到的信息做出正确的反应, 数据中心应该提供事物的位置信息。大规模**物联网**网络面临的一个挑战是从部分观测到的距离信息中识别整个传感器节点的位置图。本文提出了一种基于矩阵完成的定位算法, 利用部分观测距离信息重建传感器的位置图。通过数值实验表明, 基于修正共轭梯度的方法能有效地恢复欧几里得距离矩阵。少

2018 年 8 月 3 日提交;v1 于 2017 年 2 月 13 日提交;最初宣布 2017 年 2 月。

551. 特别报告: 1702. 00606[pdf, ps,其他] cs. it

无线动力移动边缘计算系统中的联合卸载与计算优化

作者:王峰,徐杰,王欣,崔树光

摘要: 移动边缘计算 (mec) 和无线功率传输 (wpt) 已被公认为物联网 (**iot**) 时代的有前途的技术, 可提供具有增强的计算能力和可持续性的大规模低功耗无线设备能源供应。在本文中, 我们提出了一个统一的 mec-wpt 设计, 考虑无线供电多用户 mec 系统, 其中一个多天线接入点 (ap) (集成到一个 mec 服务器) 广播无线电功率, 为多个用户充电, 每个用户节点依赖于收集的能量来执行计算任务。使用 mec, 这些用户可以自己在本地执行各自的任务, 也可以根据时分多重访问 (tdma) 协议将其全部或部分卸载到 ap。在该模型的基础上, 我们开发了一个创新的框架, 以提高 mec 性能, 通过联合优化能量传输波束在 ap, 中央处理单元 (cpu) 频率和卸载位的用户, 以及用户之间的时间分配。在此框架下, 我们将解决需要延迟限制计算的实际方案。在这种

情况下，我们开发了一个最佳的资源分配方案，最大限度地减少 ap 的总能耗，受用户的个人计算延迟限制。利用最先进的优化技术，我们以半封闭的形式获得最佳解决方案。数值结果表明，与其它基准方案相比，该设计具有较好的优点。少

2017 年 12 月 17 日提交;v1 于 2017 年 2 月 2 日提交;最初宣布 2017 年 2 月。

评论:接受 ieee 无线通信交易，本文的一部分已在 ieee icc 2017 中介绍

552. 建议: 1702. 00131[pdf, ps,其他] cs. it

如何在移动混合物联网网络中缓存?

作者:trung-anh do, sang-won jeon, won-yong shin

摘要: 研究了以内容为中心的移动混合物联网 (iot) 网络，该网络由移动设备和静态飞向接入点 (fap) 组成，每个设备根据随机游动移动模型移动并从根据 zipf 的受欢迎程度分布，图书馆是独立随机的。我们不允许通过提供与核心网络连接的昂贵回程来访问宏基站中的内容对象，而是考虑了一个更实际的场景，即移动设备和静态 fap (每个设备都有有限大小的缓存空间) 能够缓存内容对象的子集，以便每个请求由其他移动设备或静态 fap 提供服务。在一般的基于多跳的内容传递协议下，我们通过提出一种新的缓存分配策略来分析订单最优吞吐量-延迟权衡。特别是，在给定的缓存策略下，我们首先从扩展规律以及一般内容传递多跳路由协议的角度来描述吞吐量-延迟权衡。然后，通过提出顺序最优缓存分配策略，通过一种新的变量解耦方法，在移动设备和静态 fap 上共同找到复制集，从而实现了订单最优吞吐量-延迟权衡。在我们的移动**物联网**网络中，一个有趣的观察是，非常流行的内容对象主要由移动设备提供服务，而其余内容对象则由静态 fap 提供服务。我们进行数值评估以验证我们的分析结果。我们还表明，订单优化策略严格优于基线方法，即分别优化移动设备和静态 fap 上的复制集。少

2018 年 10 月 29 日提交;v1 于 2017 年 1 月 31 日提交;最初宣布 2017 年 2 月。

评论:18 页, 7 个数字，本论文将发表在 ieee 访问，并提出了部分 ieee 信息理论国际研讨会,巴塞罗那，西班牙, 2016 年 7 月

553. 建议: 1701. 06783[pdf] cse

许可证制度的自治结构

作者:基兰·格里尔

摘要: licas (用于自主服务的轻量级基于互联网的通信) 是用于构建基于服务的系统的分布式框架。该框架通过其人工智能算法提供了 p2p 服务器和更智能的信息处理。分布式通信包括 xml-rpc、rest、http 和 web 服务。它现在可以为构建不同类型的系统提供一个强大的平台，在这个平台上，微服务或 soa 是可能的。但是，该系统可能同样适用于**物联网**，因为它提供了与外部源连接的类，并具有可选的自治管理器，并集成了 mape 控制环。该系统还与 android 兼容。本文特别关注自主设置以及如何使用。以前已经描述了一种新的链接机制 [5]，它可用于动态链接源，这也被认为是自治框架的一部分。少

2018 年 4 月 19 日提交;v1 于 2017 年 1 月 24 日提交;最初宣布 2017 年 1 月。

554. 建议: 1610.07273[pdf,其他] Cs。Lg

在图中编码时间马尔可夫动力学，用于可视化和挖掘时间序列

作者:刘祖光,王志光

摘要: 时间序列和信号在统计、机器学习和模式识别领域引起了越来越多的关注，因为它在行业中广泛存在，特别是在传感器和**物联网**相关的研究和应用中，但几乎没有取得什么进展在有效的时间序列中，视觉分析和交互由于其时间维数和复杂的动态。在最近使用网络度量来描述时间序列进行分类的工作的启发下，我们提出了一种基于时间排序中的一阶马尔可夫过程将时间序列可视化为复杂网络的方法。与经典条形图、折线图和其他基于统计的图相比，我们的方法提供了更直观的可视化，从而更好地保留了时间依赖性和频率结构。它提供了一个自然的逆操作，将图形映射回原始信号，从而可以使用图形统计来描述时间序列，以便更好地进行视觉探索和统计分析。我们的实验结果表明，在各种任务的有效性，如模式发现和分类的合成和实时序列和传感器数据。少

2018 年 8 月 14 日提交;v1 于 2016 年 10 月 23 日提交;最初宣布 2016 年 10 月。

评论:aaai 2018 研讨会

555. 第 1608. 01537[pdf,其他] Cs。直流

跨边缘和云的事件分析的分布式调度

作者:rajrup ghosh, yogesh simmhan

摘要: 物联网 (**iot**) 域从传感器生成大量高速事件流，需要以低延迟对其进行分析，以推动决策。复杂事件处理 (cep) 是一种大数据技术，可用于实现此类分析，传统上在云虚拟机 (vm) 上执行。利用专属**的物联网**边缘资源与云虚拟机相结合，可以为 cep 提供更好的性能、灵活性和货币成本。在这里，我们针对 cep 查询的能量感知位置制定了一个优化问题，该问题由其组成为分析数据流，跨越边缘和云资源的集合，目的是最大限度地减少数据流的端到端延迟。针对这一问题，提出了一种遗传算法元启发式算法，并将其与蛮力优化算法 (bf) 进行了比较。我们对边缘和云资源的计算、网络和能源容量执行详细的实际基准。这些结果用于定义一个真实而全面的模拟研究，用于验证 45 种不同的 cep 数据流、lan 和 wan 设置以及不同边缘资源可用性的 bf 和 ga 解决方案。我们将 ga 和 bf 解决方案与不同配置的随机基线和仅限云的基线进行比较，总共进行了 1764 模拟运行。我们的研究表明, ga 是在最佳 bf 解决方案的 97%，需要数小时，映射数据流与 4-50 查询在 1-26 秒，只有未能提供一个可行的解决方案 < = 20% 的时间。少

2017 年 12 月 9 日提交;v1 于 2016 年 8 月 4 日提交;最初宣布 2016 年 8 月。

评论:29 页, 6 个数字，期刊

556. 第 16002393[pdf,其他] Cs。哦

多伊 10.1109/TCAD.2017.2717782

物联网的微处理器优化：综述

作者:tosiron Adegbija, anita rogacs, chandrakant patel, ann godon-ross

摘要: 物联网 (**iot**) 是指互联和唯一可识别的物理设备的普遍存在。这些设备的目标是收集数据并推动行动，以提高生产率，并最终减少或消除对人工干预数据获取、解释和使用的依赖。这些连接的低功耗设备的扩散将导致数据爆炸，从而大大增加数据的消耗和延迟方面的数据传输成本。边缘计算通过在数据传输之前在边缘节点上执行计算来解释和/利用数据来降低这些成本。虽然很多研究都集中在**物联网的**互联性质和通信挑战上,**但物联网**嵌入式计算在设备微处理器方面的挑战却得到了较少的关注。本文从微体系结构的角度探讨**了物联网**应用的执行特性，以及能够实现高效和有效边缘计算的微体系结构特征。为了可追溯地代表各种**下一代物联网**应用，我们推出了基于应用程序

功能的**广泛的物联网**应用分类方法，以实现**物联网的更快工作负载特征**微处理器。然后，我们调查和讨论潜在的微体系结构优化和计算范式，这些优化和计算范式将支持高效、可配置、可扩展和可扩展的正确配置的微处理器的设计。本文为分析和设计下一代**物联网**设备的各种微处理器架构提供了基础。少

2018 年 2 月 20 日提交;v1 于 2016 年 3 月 8 日提交;最初宣布 2016 年 3 月。

评论:在 ieee 集成电路与系统计算机辅助设计 (tcad) 上发表;物联网电路与系统设计专题

557. 第 1511. 09120[pdf,其他] 反渗透委员会

运动数据的核心集：从定理到实时系统

作者:soliman nasser, ibrahim Jubran, dan feldman

摘要: 数据集的核心集 (或核心集) 是它相对于一组查询的语义压缩，这样 (小) 核心集就可以得到查询原始 (完整) 数据集的近似答案。在过去的十年里，coresets 为近似算法提供了理论计算机科学方面的突破，最近，在机器学习社区为学习 "大数据" 提供了突破。然而，我们不知道实时系统以每秒几十个帧的速率计算核心集。在本文中，我们提出了一个框架，将定理转换为这样的系统使用核心集。我们开始与独立利益的证明，任何一套 n 中的矩阵 $R^{D\times D}$ 其总和为 s，具有正加权子集，其总和具有与之相同的质量中心 (均值) 和方向 (左 + 右奇异向量)s，并包括 o(DR)矩阵 (独立于 n)、其中 $r\le D$ 是排名 s.我们提供了一种算法，它在一次传递中计算出这个 (核心) 集，在 $D_{o(1)}$ 每个矩阵插入的时间。通过维护这样一个线器的运动学 (移动) 集 n 点，我们可以在小核心集上运行后估计算法，如 kabsch 或 pnp，而不是 n 点，实时使用弱设备，同时获得相同的结果。这使我们能够实施低成本 (<$100 元) **物联网**无线系统，跟踪玩具 (和无害) 四轮车，引导客人到所需的房间 (在医院，商场，酒店，博物馆等) 没有额外的人力或遥控器的帮助。我们希望我们的框架将鼓励理论社区以外的研究人员在未来的系统和论文中设计和使用核心集。为此，我们提供了关于合成数据和真实数据的广泛实验结果，以及指向我们系统和算法的开放代码的链接。少

2017 年 12 月 18 日提交;v1 于 2015 年 11 月 29 日提交;最初宣布 2015 年 11 月。