基于雾计算的可信传感云研究进展

王田[1,2]，沈雪微[1]，罗皓[1]，陈柏生[1]，王国军[3]，贾维嘉[2,4]

（1. 华侨大学计算机科学与技术学院，福建 厦门 361021；2. 澳门大学智能城市物联网国家重点实验室，澳门 999078；
3. 广州大学计算机科学与教育软件学院，广东 广州 510006；4. 上海交通大学电子信息与电气工程学院，上海 220240）

摘 要：云计算技术与无线传感器网络结合所产生的传感云（sensor-cloud）系统已经逐渐成为研究的热点。传感云在云计算平台的支撑下扩展了传统传感网的服务能力。对目前主流传感云系统进行了充分调研，总结了传感云系统的特点和发展规律，发现系统中存在的可信问题将直接影响到上层数据保护和应用；揭示了已有方案难以提供可信传感云服务是因为底层无线传感网能量不足、计算能力弱、易故障等，以及云计算模式缺乏对底层传感器节点和数据的直接管理等；构建了基于雾计算模式的可信传感云实现框架，设计了可信评估、可信数据收集、可信存储等关键技术，也为后续研究提出可供借鉴的新思路。

关键词：传感云；无线传感网；可信云计算；雾计算

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019068

Research progress of trusted sensor-cloud based on fog computing

WANG Tian[1,2], SHEN Xuewei[1], LUO Hao[1], CHEN Baisheng[1], WANG Guojun[3], JIA Weijia[2,4]

1. College of Computer Science and Technology, Huaqiao University, Xiamen 361021, China
2. The State Key Laboratory of Internet of Things for Smart City, University of Macau, Macao 999078, China
3. School of Computer Science and Educational Software, Guangzhou 510006, China
4. School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Abstract: The sensor-cloud is combined with cloud computing and wireless sensor networks, which extends the service ability of WSN by the support of cloud computing. It is one of the hot topics among the current researches. After comparing and surveying the mainstream system adequately, the characteristics and development of sensor-Cloud were summed up. Then, the direct influence of existing trust issues in the system for data protection and application on upper layer were found. The announced reasons explained that existing schemes were difficult to provide trusted sensor-cloud services. This was because that the capabilities of the underlying WSN nodes were too weak, and cloud computing model lacked the direct management of underlying nodes and data and so on. The trusted structures based on fog computing were given, and the key technologies of trusted evaluation, trusted data collection, and trusted storage were designed. Finally, the discussion pointed out new views for the researches in trusted sensor-cloud.

Key words: sensor-cloud, WSN, trusted cloud computing, fog computing

1 引言

近年来，由于政府及商业市场对大数据、云计算、物联网等技术的广泛推力，云计算技术被更多地考虑与传感网络协同合作，一方面，无线传感网扩展了人们收集信息的能力，并将物理世界与信息

收稿日期：2018−08−08；**修回日期**：2019−01−21

基金项目：福建省社会科学规划基金资助项目（No.FJ2018B038）；福建省自然科学基金资助项目（No.2018J01092）；福建省教育厅中青年教师教育科研基金资助项目（No.JAT170040）

Foundation Items: The General Projects of Social Sciences of Fujian Province (No.FJ2018B038), The Natural Science Foundation of Fujian Province (No. 2018J01092), The Fujian Education and Research Project for Junior Teachers (No.JAT170040)

世界结合起来；另一方面，随着智能城市和智能空间应用规模的扩大，传感器数据和服务将被考虑转移到云计算和雾计算中[1]。众所周知，云计算延伸了无线传感网的应用领域，也构建了许多解决现存限制条件的变化结构，如为传感网提供可信数据与后续可信存储奠定了坚实基础等。

传感云系统的出现为云计算提供了一种新的数据管理机制，可以说其扩展了市场空间。以传感云技术为背景，信息产业能够更加自动化、降低能耗成本和提高决策效率。随着云计算、物联网、大数据等技术的不断发展，与之密切相关的传感云平台一直是效率和可靠应用的有前途的候选者。然而，传感云在提供扩展服务的同时，也存在着新的挑战。其一，底层传感节点资源有限，在复杂苛刻的部署环境中发生故障和错误的概率普遍偏高且可能产生较大时延。其二，云端服务器作为下层的管理平台又与传感网络相隔过远，传统的远程管理无法满足用户对数据直接掌控的需求。综上，底层传感网所采集的数据可信与否、上层数据保护可靠与否都将成为传感云系统一切应用实现的基础和根本。

传感云技术响应了人们在网络中的关键需求，但不能为了追求应用性能而牺牲可信性的保障。传感云系统应用的关键在于应用性能（如服务质量等）和制约因素（如可信度、可靠度等）之间进行权衡。通过对现阶段传感云解决方案的广泛研究发现，传感云系统的可信问题并未得到很好的解决，依然存在几个方面的漏洞，例如数据收集、数据处理、可信通信与信任机制内在性能等。同时，应充分考虑传感云系统在云端也无法保证完全可信，除本身易受攻击的性质外，它的管理漏洞也都成为系统运行的风险。

综上所述，需要一种新的思路和模式去探索这些可信问题的解决方案。雾计算作为云计算的延伸，是当前新兴的热点技术，主要特点是比云计算更加靠近底层网络，支持移动性且具备较强的计算能力。人们可以贴切地形容雾计算是介于云端与个人主机之间的一种中间态，可以将雾计算看作一种“微型云（micro-cloud）”，移动于传感云体系架构的中层范围，实现安全可靠的数据处理与存储[2]。当前，雾计算所采用的分布式架构更多地应用于物联网等相关领域内。在新技术时代，除了基本的通信业务外，基于云雾层的数据采集、数据存储、移动计算等方面也都发挥着积极和重要的作用[3-5]。本文期望通过对现有传感云系统进行总结与讨论，发现该系统中存在的可信问题对上层数据的保护和应用的直接影响[6]，使研究结果能够对推动可信传感云系统的融合性与应用性的提升有所启发。此外，本文结合雾计算模式设计新的框架结构也是对传感云系统的重要补充和探索实践。

2　传感云系统

传感云应该能够通过无线传感网互连数十亿或数万亿个传感器对象，因此需要了解传感云灵活的分层结构。传感云系统的运作需要以数据流的形式和特定功能的结果来交换数据[7]。

单一中心多终端类型的系统可以提供海量数据存储、统计接口、分层管理等功能，一般来说，应用最多的是私有云[8]。其可划分为五层管理结构：第一层为数据平面，目的是收集和处理信息；第二层为控制层，通过安全通道将基础设施层产生的数据传输到服务管理层；第三层为服务管理层或中间件层，根据地址和名称将服务与其请求进行配对，使应用程序程序员能够在不考虑特定硬件平台的情况下处理异构对象；第四层为应用层，用于客户的响应要求；第五层为业务层，管理整个系统的活动和业务，还可以支持基于雾计算、大数据分析或其他技术的决策过程。对于许多跨区域的企业和公司来说，业务管理层更适合作为多中心、多终端的模式[9]，使用这个模型的前提是云计算中心必须包含公共云和私有云，并且它们之间的互联没有障碍[10]。

近几年来，许多新的研究方向均在利用云计算对传统的无线传感网服务进行完善和性能提升方面，如为传感网的数据处理和存储提供了强有力的支撑和可信度。传感云结构的研究现状如表 1 所示，不同领域的传感网可以与云计算相结合，其应用领域可遍及能源、安全、异构等方面，而最突出的表现则在于利用云平台强大的计算和管理能力进行分析，传感云系统能及时做出反应。

3　可信传感云研究现状

在商业化市场存在着许多传感云用例，它们有一定的可信性能需求。通过第 2 节的汇总可以发现，现有的传感云系统设计中关于可信的制约因素需要深入考虑。此处探讨了几个细化领域的研究问题，以可信传感云系统为出发点，列出其

表 1 传感器网络与云的结合

网络	与云的结合	服务	主要贡献
WSN	CC-WSN [11]CoS④[12]	XaaS⑤应用	数据源实时处理是做出决策的关键，传感云可提供分析、监控、存储、计算等多种类型的数据服务
WBAN①	WBAN-cloud [13]	移动传感应用/多途径数据传递	医疗领域的传感云应用着重考虑安全与隐私问题，提供隐私与可信兼容的方式实现远程服务是必要的
WSAN②	sensor-cloud[14]	SaaS 应用	传感云并不会将传感器数据作为一种服务来提供，而是专注于通过云来管理传感器
IOT③	CloudIoT [15]CoT [16]	IoTaaS⑥应用	用户能够在不关心传感器的物理位置和访问规则的情况下，从不同的传感器所有者处获得服务

注：① WBAN (wireless body area network)；② WSAN (wireless sensor and actor network)；③ IoT (Internet of things)；④ CoS (cloud of sensor)；⑤ XaaS (everything as a service)；⑥ IoTaaS (IoT as a service)。

体系结构及用例，并包含可信传感云系统的关键需求和实现概念。

3.1 实时性能

就当前需求来看，许多应用都必须是实时的，才能确保其方案有意义，且得到的最终结果可信[17]。为了实现传感器云系统的快速响应，即为了达到实时性的目的，更多的应用集中在数据处理和通信处理这 2 个方面，在此基础上，将传感器云系统中的实时性应用划分为 3 类：可信数据收集、可信数据处理和可信实时通信。

3.1.1 可信数据收集

数据采集是传感云系统中的底层操作，采集的响应速度直接影响整个系统的实时性，甚至于影响所收集数据的可信程度。文献[18]给出了一种信息融合、分散无线传感器和执行器网络虚拟化模型。在该模型中，数据约简的一种可能方法是使用信息融合，并利用数据抽象技术对数据进行分类。文献[13]提出了一种基于云的实时远程健康监测系统（CHMS, cloud-based real-time remote health monitoring system），目的是关注患者与全球云之间的连通性问题，将云划分为局部云（包括受监控用户和本地医务人员）及包含外部世界的全球云。该系统可以最大限度地减少整个网络中的业务流，实现对拥塞和干扰的管理。

除了通过数据聚合来缩短传感云系统的响应时间外，通过信任辅助传感云（TASC, trust-assisted sensor-cloud）也可以提高传感云服务质量，以满足实时性的要求。文献[14]是将信任结合到无线传感网和云计算中，以提高传感云的服务质量。TASC 可以大大提高用户从云中获取传感器数据的吞吐量和响应时间。

3.1.2 可信数据处理

数据的集中分析和处理也是传感云中大量实时性应用的重要组成部分。传感云因其可伸缩、低成本的特性提供了大量计算、存储和软件服务。在文献[17]提出了一种新的数据错误检测方法，该方法充分利用云平台的计算潜力和 WSN 的网络特性，实现了数据错误的快速检测。在数据错误分类的基础上，该方法引入并分析了集群 WSN 的网络特征，支持快速地检测和定位传感云上的大数据集中的错误。文献[19]结合雾计算，对无线网络中的传输与处理时延问题进行了研究。该文献中引入了一些边缘节点作为雾节点，例如基站，这些基站与云服务器相连，拥有一定的缓存能力。这些基站中存储一定量的前摄信息可以大大减少内容交互的时延。此外，文献[20]提出了一种新型的无线传感器网络——移动云计算（WSN-MCC, wireless sensor network mobile cloud computing）集成方案，以解决影响传感器数据有用性和可靠性的关键问题。考虑到移动用户所要求的数据时间和优先级特性，方案选择性地传输对云端更有用的传感数据。

3.1.3 可信实时通信

3.1.1 节和 3.1.2 节中讨论了面向数据的实时可信问题，而传感云的实时性还有一个非常重要的问题，即传输通信中的实时性问题[21]。在文献[22]中，为了响应传感云中同时向多用户传输相同的数据的请求，提出了一种面向传感云用户的多方法数据传递方案，该方案使用了 4 种传递方式，更好地满足传感云用户关于传输成本或传输时间的要求。当谈到传感云的即时性时，必须讨论传感云在车载自组织网络（VANET, vehicular ad hoc network）中的应用，在 VANET 中，有效的信息传播对道路安全和交通效率至关重要。在文献[23]中指出，现有的研究在选择合适的网关将安全消息从远程服务器到目标区域的快速安全消息传播尚未得到很好的解决。因此，文献[23]提出了一种结合多种通信

和云计算技术优点的快速消息传播框架。云服务器中的安全消息首先借助云计算传送到相关道路上经由参数选择的合适移动网关，然后通过车辆对车辆（V2V, vehicle to vehicle）通信在相邻车辆之间传播。

由上述分析可知，实时性的实现与否总是对产生的数据质量有巨大的影响[24]，这些方法中主要利用的也是数据分类和聚合的思想，以减少数据冗余，确保数据的可信度。此外，确保通信过程实现实时性也是关键，如表 2 所示，列举了现有传感云实时性方案，其中的可信方式所覆盖的类别仍有完善空间，为后续研究提供参考和借鉴。

表 2　　实时性方案分析

方案	应用类别			可信方式
	数据收集	数据处理	通信	
CHMS[13]	√	×	√	信息聚合
TASC[14]	×	×	√	快速误差检测与定位
网络虚拟[18]	×	√	×	云内与云间调度
基于雾计算的数据传输[19]	√	√	×	多方式数据传递
WSN-MCC[20]	×	×	√	WSN-MCC 集成方案
多通信信息传播[23]	×	√	√	数据聚合与卸载

3.2　可信机制

自从传感云被提出以来，可信机制的研究一直备受关注。传统意义上的传感云设计已有不少解决方案和针对此类问题的分析，值得借鉴与学习。

文献[25]提出了一种新的实用方法，以防止内部攻击中的数据泄露。新方案支持无限数量的参与者，只要对手不能破坏一半或更多的计算玩家，就会安全。入侵检测是传感云系统中的主要问题之一，文献[26]介绍了无线传感器网络中的选择性转发问题。该模型利用雾计算的基础结构来实现这一目的，利用雾计算的基础设施及其与传感器层的接近，提供全局跟踪和监视。

为了控制对网络的安全访问，对应答设备的认证是必不可少的，现有的认证方案大多不能很好地适应传感器网络和云计算的结合。文献[27]认为云可能在收集敏感数据方面存在一定的缺陷，因此，认证方案被要求集成到云环境中。由于传感云系统由大量的传感器节点组成，它们通过多跳无线链路相互通信，故而对于信息源的保护尤为重要，特别是源节点的位置信息不应被暴露。文献[28]提出了一种基于冗余雾端环路的无线传感器网络方案，保护源节点位置隐私，并通过 2 种重要的机制实现能量效率优化。该方案通过在非热点区域充分利用额外的能量构造多个雾层来提供本地源位置隐私。与此同时，动态构造与撤销雾层的设计提高网络的安全性。

另外，还有研究考虑到雾和云之间脆弱的连接，以此说明雾计算中的身份验证和授权问题，并讨论了该方案的潜在解决方案[29]。此方案引入了一种未与云服务器连接的情况下实现用户身份验证的新机制，称为独立身份验证。在服务器端，系统对用户进行身份验证可能需要的信息进行采集，也可将数据加密成密文，通过预定的方式进行解密并获取数据。通过使用这种身份验证方法，即使雾和云之间的连接是脆弱的，用户也能够被认证和授权来使用雾设备。

文献[30]将基于雾计算的安全控制引入了车载自组织网络中，考虑了如何抵抗恶意车辆攻击及避免单点失效问题。方案中设计了交通灯作为雾计算设备，并利用其设计产生指定难度 CDH（cloudera's distribution, including apache hadoop）谜题散布给附近车辆，从而实现有效性及安全性验证。由于车载自组织网络中无线通信模型被划分为路边单元通信及车辆通信，所涉及的道路信息及交通管理信息容易受到伪造身份的误导攻击，这阻碍了系统网络运行以及人们对其的信任程度，严重时则威胁生命财产安全。隐私信息不被追踪或受威胁、交互通信满足保密、交互双方互为可信，都是方案中能够设计的需求。然而，此种方案更多的是从认证机制的角度对于雾设备加以利用，未能够全面地考虑到云端及相关环境下的信任程度。

上述各方法具体对照比较如表 3 所示。通过上述分析，目前仍有许多威胁亟待解决，而系统的安全性能与隐私保护也是实现可信传感云系统的关键。现如今，物联网系统已完全连接到公共互联网和云。它们的执行会直接由更加集成、更高性能的系统控制，如车联网络系统、医疗保健系统等隐私性关键系统。如果这些网络的安全受到破坏，系统无法维持其可信性能，结果造成的代价高昂甚至直接且立即对物理世界造成影响。

4　基于雾计算的可信传感云系统

综合第 3 节对现有传感云系统的分析，其解决方案虽有对系统可信的考虑和设计，但是不够全面

表 3 当前传感云可信性能研究比较

方案	信任机制	传输安全	存储安全	攻击类别	对象
多用户泄露预防[25]	√	×	×	内部	云计算/传感网
基于雾计算的入侵检测[26]	×	×	√	外部	云计算/传感网/雾计算
传感云系统信息流保护[27]	×	√	√	内部	云计算
基于冗余雾端环路的无线传感器网络[28]	×	×	×	外部	云计算
基于雾计算的身份验证[29]	√	√	×	内部	云计算/传感网/雾计算
基于雾计算的车载网安全控制[30]	√	√	√	内部/外部	云计算/传感网/雾计算

和完善，无法保障应用服务可靠可信。这可能会阻碍可信传感云的进一步发展，因此仍需要更加充分地考虑传统可信问题及其衍生的可信威胁等一系列解决方案。

4.1 基于雾计算的可信传感云框架

为实现更好的系统性能，可信传感云系统将引入雾计算模式作为云计算的补充。在雾计算概念提出之后，许多机构和企业对雾计算展开了研究，也产生了许多应用模型，如 OpenFog[31]、Multi-Cloud[2]、Prismtech Votex[32]等。雾计算技术已在不知不觉中融入了社会，如车联网、无线传感器网络、智能建筑控制、物联网、现实增强、移动通信、软件定义网络等[33]。雾计算的架构符合分布式系统的部署要求，它能够更加贴近网络边缘，进行一些数据操作，但对于用户而言又是透明化的，并且这样将应用汇集在边界范围更加凸显其内聚性和高度自治的特征[34]。如图 1 所示，与传统云计算相结合，雾节点层贴近边缘网络，易于管理，可信程度高。

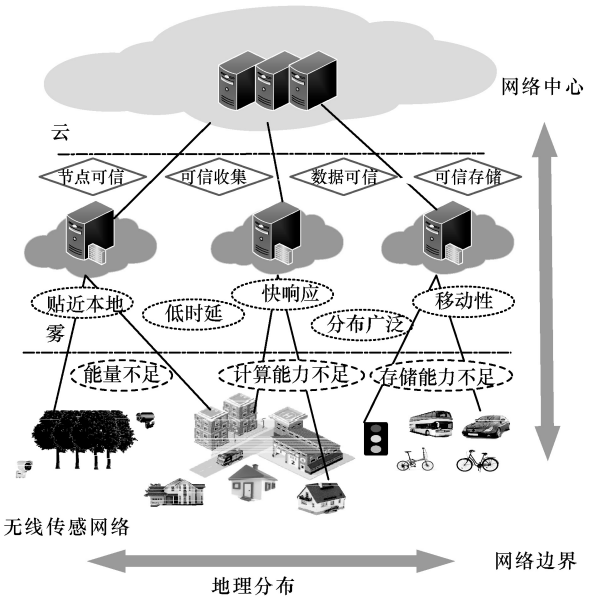


图 1 基于雾计算的可信传感云框架

即使现有传感云具备充足优势，云计算模式缺乏对底层传感节点及数据的直接管理，导致数据的可信性和可靠性无法得到保证[35]。

这些问题成为传感器网络采集的数据不可信以及云端不可靠等的瓶颈之处，而雾层能够构建起桥梁与纽带。

1) 雾层计算与存储能力弥补传感网缺陷。传感器网络自身的不可信主要是因为能力太弱，无法运行复杂的准确评价及信任评价。雾层节点作为可移动单元，便可突破能力限制，成功应用于拓扑控制、移动监测等领域。

2) 雾层在地理位置上贴近网络边缘，易于管理。较之云端服务器的“遥不可及”，雾层以其位置优势能够获取更为全面的底层网络信息，可信度更高。在特定情况下，本地雾端服务器可以进行简单的数据统计和处理分析，以达到高效快速的应用要求。

这种基于本地计算的模式，由于贴近网络末端，获取底层网络信息比较全面，相对基础云计算模式更为可信可靠。传感器节点因其自身能量弱、易故障等缺陷导致传感器网络采集的数据并不可信。反观云端也并不是完全可信的，一是因为云服务器本身容易遭受各种恶意攻击，二则是云服务器提供商可能留有后门，因此传感网交付来的数据可能面临隐私泄露的风险。

随着云计算模式与移动传感网络的深度融合，引入雾计算思想来完善传感云系统就显得尤为重要，究其原因，一旦数据掌握于云服务商手中，用户完全无法掌控所有权，无法达到安全可信的要求。如表 4 所示，首先对现有雾计算应用进行了汇总，以明确在雾计算背景下的研究方向。雾计算模式的许多优势为其应用构建了研究前景，本文以其服务的开发为起点，介绍传感云的相关示例，以解决传感云背景下的可信场景。

表 4　　现有雾计算设计方案

方案	可信	特征	优势	缺陷	说明
分级存储方案[36]	√	存储技术	编码速度快，完整性高	涉及传递机制，灵活性相对弱	完善传统云存储技术，对抗网络威胁，实现系统可信
大数据环境下健康检测[37]	×	大数据	准确性高	时间性能相对弱	针对基础设施实现健康监测
传感云系统数据监控[38]	×	结构化	灵活性高	响应速度不足	与传感云相结合的健康监测
基于雾计算的节点信任评价[39]	√	信任评价	安全性高	间接完整度不足	雾端设定信任评价层次结构，完善数据可信度
基于雾计算模式的数据收集[40]	√	数据收集	安全可靠	灵活性相对弱	利用雾端的计算能力辅助传感云进行可靠的数据收集

4.2　雾计算与云服务信任推荐

随着云计算技术的发展和数据的全球增长，传感云服务的应用与实践范围越来越广泛，吸引了大量的用户。但是，正如文献[41-42]所述，传统的安全策略无法有效应对传感云服务中内部攻击等安全隐患，这将严重影响系统的服务质量。更为重要的是，系统效率一旦受到干扰，用户将面临数据缺失或泄露的风险，也使得云服务系统不再是可信可靠的数据托管方。因此，为解决传感云服务功能的可信性能，可以设计一种信任推荐机制及基于云计算和雾计算的平衡动态结合体系，这种基于雾计算的层次结构降低了资源消耗，同时也确保了信任评价机制的可扩展性。

4.2.1　环境设置

在公共云中，雾层结构将很大一部分的信任评估机制从传感网络中转移，传感网络中的设备执行直接信任计算，而后向雾服务器发送异常信息。雾服务器进一步从设备中收集信任信息，并评估传感网络的整体可信状态。与之对应的服务参数模板由云端数据中心进行匹配和存储，雾服务器会根据模板提供解析策略。其中所涉及的 3 层结构如图 2 所示，具体介绍如下：第一层为节点间的直接信任推荐，主要任务是信任证据的收集和异常因素监测；第二层为节点间的综合信任推荐，若第一层的检测结果显示异常就会触发二级评估，并执行推荐信任与综合计算；第三层为雾服务器的数据分析与决策，它包含了对于全局信任的分析、对隐藏数据攻击的检测和一般异常处理。

4.2.2　工作机制

具体举例说明，在一个应用环境中，当存在物理设备需要被多个应用服务共享时，首先需要做的就是对物理设备进行虚拟化。这些虚拟设备可以作为细化的应用资源进行存储，因而当解析模板有调用物理设备的需求时，雾服务器会为这些模板分配相应的虚拟接口。

$$\text{device}_{\text{phy}} \overset{\text{virtualization}}{\Rightarrow} \text{device}_{\text{vir}} \overset{\text{interface}}{\Rightarrow} \begin{cases} \text{service}_1 \\ \vdots \\ \text{service}_n \end{cases} \tag{1}$$

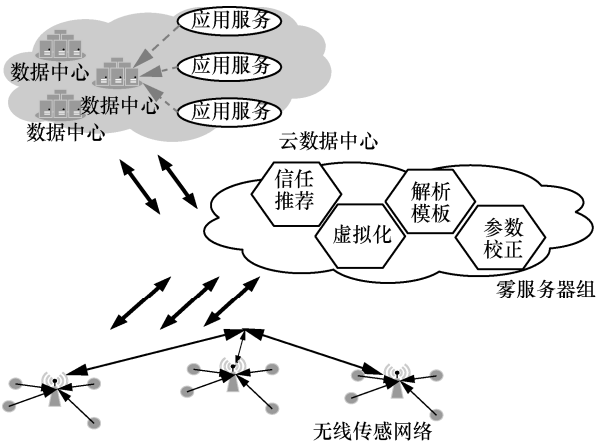


图 2　基于雾计算的信任推荐用例

在无线传感网中，直接推荐算法根据相邻设备之间的交互通信依据来计算，这些依据可能是设备路由故障率、设备通信成功率、设备信号强度及设备转发时延等。它们被划分为一般依据、网络状态依据和确认信任依据，然后用于计算信任推荐值。

$$T_{\text{dir}}(x_i)=\begin{cases} \dfrac{E_{\text{norm}}}{E_{\text{total}}}, & \left|T_{\text{old}}^{E}-\dfrac{E_{\text{norm}}}{E_{\text{total}}}\right|<T_{d_1} \\ w_1\dfrac{E_{\text{norm}}}{E_{\text{total}}}+w_2T_{\text{old}}^{E}, & T_{d_1}<\left|T_{\text{old}}^{E}-\dfrac{E_{\text{norm}}}{E_{\text{total}}}\right|<T_{d_2} \\ 0 \end{cases} \tag{2}$$

其中，T_{d_1} 和 T_{d_2} 代表了新旧信任推荐值的差异值，w_1 和 w_2 则分别对应着新旧值的权重。

而在雾端的服务器实质上与底层传感器网络并行，且会保存设备推荐状态，以确保整个传感云系统是可信的。这里的推荐状态会受到 3 个方面的影响：底层传感网络中的直接推荐值、传感网络的异常积累量和雾端的异常积累量。

云服务中心将不同的应用区域进行连接，故而云中的服务大致可划分为本地服务和远程服务 2 种。本地服务能够直接有雾服务器提供并在本地完成，远程服务将会根据用户需求由云或云端与雾服务器协同完成。2 种不同服务的选择取决于资源消耗和总时间消耗。

$$\begin{aligned}\mathrm{con}_{\mathrm{res}} &= \mathrm{con}_{\mathrm{res}}^{\mathrm{storage}} \bigcap \mathrm{con}_{\mathrm{res}}^{\mathrm{process}} \bigcap \mathrm{con}_{\mathrm{res}}^{\mathrm{bandwidth}} \\ \mathrm{con}_{\mathrm{time}} &= \mathrm{con}_{\mathrm{time}}^{\mathrm{transm}} \bigcap \mathrm{con}_{\mathrm{time}}^{\mathrm{transfer}} \bigcap \mathrm{con}_{\mathrm{time}}^{\mathrm{process}}\end{aligned} \tag{3}$$

结合考虑网络资源消耗等因素的信任推荐使得这一方案能够使系统拥有更高的数据处理效率，对于数据层的检测也能够延长推荐信任的更新周期，从而优化服务质量。

4.3 基于雾端的传感云信任评估

数据来源于节点，因此有效、全面地对底层物理节点进行信任评估十分必要，用以辨别出错的、恶意的节点。传统方法过分依赖于可信云中心，难以对底层网络状况进行全面掌握，只能进行粗粒度的评估。考虑到雾节点层的优势，集中于网络边缘地设备能够较为全面和及时地获取传感网数据收集过程中的各种状态信息。文献[43-44]均有提及基于雾的传感云底层结构的层次信任机制易于建立和实现。结合以上观点，将粗粒度和细粒度的数据分析任务转移到雾层，能够获取底层网络的整个信任状态。在这种层级信任结构下查找隐藏的“脏数据”攻击节点，恢复误判节点，才能够确保系统可信运作。

4.3.1 环境设置

根据雾计算的特性，将分析的重点放在细粒度、强直接信任评估方案研究中，对传感节点进行信任评估。移动雾节点分布广泛，所获取到的信息也更加全面、丰富，因此能够对底层网络中的节点、数据进行客观的评估。考虑到多簇节点的构建和管理能够满足协同操作的需要，本文认为将移动雾节点设计成多簇结构是可行的。此外，传感网中的信任评估可分为 2 类：直接信任评估与间接信任评估。直接信任来源于有直接交互的节点，而对没有直接交互的节点则需要通过其他相邻节点的推荐信任间接得来。可以看出，这种经过第三者的间接信任（例如来自恶意节点的推荐）的可信度显然不如直接信任。

4.3.2 工作机制

传感器节点的数据处理能力有限，而本文参阅大量文献总结出，底层网络的信任机制可以由 3 个层次联合设计完成：物理传感器节点之间的直接信任层；针对路由失败频繁、数据转发时间较长、新信任值与旧信任值差异较大等异常事件评估层；位于数据处理中心全局信任层。另外，节点移动性的优势不容忽视，而雾节点与传感节点有直接交互的机会增强，故本文认为可以加强直接信任评估。基于云平台的评估方案一般只能关注传感网的网络覆盖率、网络生存时间等粗粒度的参数。而在雾计算模式下，移动雾节点可以移动到被评估节点的附近，进而获取更为详实的、细粒度的评估参数，如数据传输成功率（假设其可信度表示为 T_{s1}）、节点剩余能量（T_{s2}）、传输时延（T_{s3}）、数据正确率（T_{s4}）等与传感网质量密切相关，而云端难以触及的数据。对直接信任评价来说，以节点的数据传输可信度为例，可以由计算式(4)描述。

$$T_{s1} = \frac{F_{s1}}{U_{k1} + F_{s1}} \tag{4}$$

其中，F_{s1} 表示传输的历史数据中无差错的数据量大小，U_{k1} 则表示传输的历史数据中有差错的数据量大小。类似式(4)可以分别计算出 T_{s2}，T_{s3}，T_{s4}，$\cdots$，T_{sn}（假设有 n 个细粒度的评估参数）。然后赋予不同参数以不同的权重，依次表示为 W_1，W_2，W_3，W_4，$\cdots$，W_n 等，则节点的直接可信度可以表示为

$$T_s = W_1T_{s1} + W_2T_{s2} + W_3T_{s3} + W_4T_{s4} + \cdots + W_nT_{sn} \tag{5}$$

其中，$\sum_{1}^{n} W_i = 1$。

这种方法还可以提高直接信任评价的机会。图 3 给出了一个基于雾节点的信任评估的例子。移动雾节点在节点 A 附近，节点 B 和节点 C 是节点 A 的直接邻居，则移动雾节点可以得到节点 A、B 和 C 的直接信任评价。但是对于节点 D 而言，由于移动雾节点和节点 D 没有直接交互，因此在传统方法下，无法得到其直接信任评价，只能通过其他中间节点的信任传递间接得到。然而，通过雾节点的移动，假设其从图 3 的节点 A 处移动到了节点 D 附近，在此过程中，雾节点会与很多传感节点建立直接的通信关系，从而对它们进行直接信任评价。如图 3 所示，最终只有节点 E、F、G 和 H 不能进行直接信任评价。这是不同于已有方法的新方法，根据本研究团队的初步实验结果，通过移动雾节点的引入，对节点进行直接可信评估的机会可增加 40%以上。

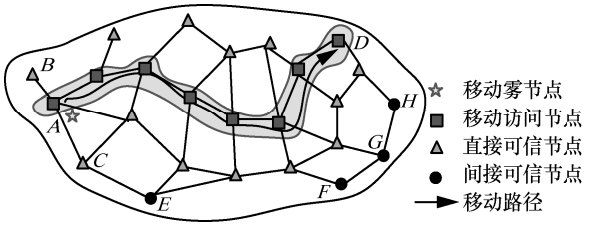


图 3　基于雾节点的信任评估

而对节点的间接信任评价而言，传统的方法是首先找出一条通信路径，然后计算出这条路径上的链式信任传递。然而，这种推荐式、传递型的信任计算非常不精确，多跳信任传递容易产生信任评估失真、不准确。而在本文设计的后续研究中，移动雾节点模式下，这种信任传递的链条可以尽量缩短，构建设计方案的完整性，保证可信评估性能的合理性与稳定性，在下文中提出讨论。

4.4　可信数据收集

基于云计算强大的计算和存储能力，无线传感网中的时延敏感应用得到更有活力的发展。无线传感网自身通信能力差，数据收集问题成为其发展的瓶颈。基于前文所述的节点信任评估，可信收集的设计中可以认为移动雾节点具备避开不可信节点的条件。正如文献[5]、文献[11]和文献[45]由多个移动 sink 节点组成的移动雾结构，用以连接无线传感器网络和云端的数据传输。综合分析后发现，实际设定应考虑到移动节点速度较慢的特性，所提出的路径规划也应全面考虑一片区域的总体的信任情况，而非单一节点，这样在数据收集的时候能够最大化效率，从而满足数据时效性的要求。故本文认为方案设计中应贴合移动节点设计详细的路由算法，如跳数限制及能耗要求等。

4.4.1　环境设置

雾节点通常由一些功能强大的节点组成，它们比普通传感器具有更强的存储和处理能力。以之前的理论为依据，可以使用移动接收器充当雾节点，使雾节点间相互协作，其目的是提高吞吐量、最大限度地减少传输时延。网络拓扑由底层 sink 节点的移动性改变，并利用数学上图像原理实现规划，如 Voronoi (VA)。这一层中的每个接收器用作发生器，而每个 VA 只有一个接收器。雾层就能够将一个 VA 区域认定为一个完整的区域和一个基本的调度单元。然后，传感器编号高于平均值的 VA 将传感器数据分配给传感器编号低于平均值的其他 VA。为简单说明方案设计思路，这里假设单跳时延为 1 s，每个传感器产生数据为 1 000 B，每个 sink 节点的吞吐量为 2 000 bit/s，如图 4(a)所示，传统无调度机制中传感器只能按照预先设置的方向转发数据，再由 sink 节点上传云端。而图 4(b)为网络设置高效调度过程后的转变。

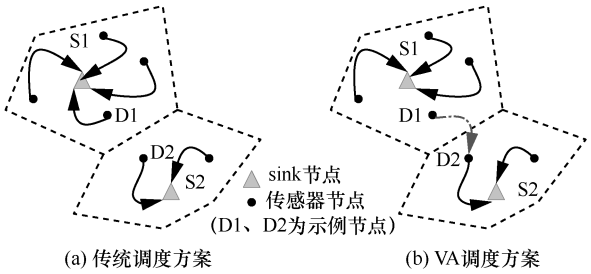


图 4　调度方案简单示例

4.4.2　工作机制

根据本研究团队的前期工作，最优化的数据收集问题是 NP-hard 问题，因此本文按照此理论进一步的思路拓展。如图 5 所示，为了方便阐述思路，将网络节点划分为可信节点和不可信节点，如根据节点可信度值的大小划分不同程度的可信，节点可以根据所属地理区域或者成簇的方式划分为不同的区。在这种思路下，可信节点以吸引力，而赋予不可信节点以排斥力，力的大小与可信程度相关。此处把移动路径看作一条具有磁性的软绳，通过引力与斥力相互作用的合力来把移动路径“推向”可信的区域，而非排斥不可信区域，从而达到高效收集可信数据的目的。由于在设计中必然要考虑移动路径长度的限制因素，该过程的设计可由初始路径不断根据引力与斥力的改变进行迭代产生，直至符合限定条件在输出路径（即规定时间内的满足移动距离限制的收集路径）。路径规划生成后，大多数可信节点可以通过单跳传输把数据送到移动雾节点，少数可信节点则通过多跳传输的方式把数据送到最近的移动雾节点。此外，该方案使用与 LEACH（low energy adaptive clustering hierarchy）相同的能量消耗模型，当传感器以 d 的距离传输 k 位数据时，发送的能耗为

$$E_{\mathrm{tx}}(k,d)=\begin{cases}E_{\mathrm{elec}}k+\varepsilon_{\mathrm{fs}}kd^2, d\leqslant d_0\\ E_{\mathrm{elec}}k+\varepsilon_{\mathrm{fs}}kd^4, d>d_0\end{cases} \tag{6}$$

其中，$d_0=\sqrt{\dfrac{\varepsilon_{\mathrm{fs}}}{\varepsilon_{\mathrm{mp}}}}$。

由此，在雾层中，雾节点之间相互合作，形成一个“小型世界”。而上层路由层负责每个传感器的最终路径，在这一层中，方案设计了一种能量有效的路由算法。

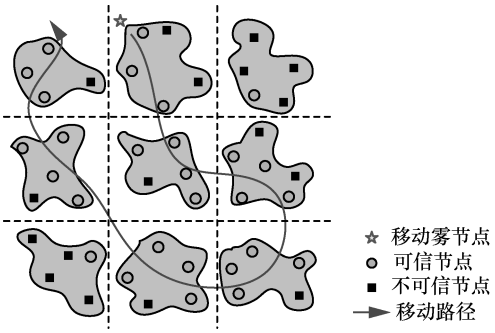


图 5 基于可信度虚拟力的移动路径规划

5 未来研究方向

前文对影响传感云系统可信性的关键制约因素进行了大量总结，并且针对云计算技术中数据收集、数据存储等方面深入讨论了解决方案与结论，但传感云系统仍然存在许多复杂场景下的可信应用问题，由此分析了雾计算模式在该领域内的应用优势。在本文的工作基础上，对于未来基于雾和云的相互作用的数据密集型服务的计算与存储有一些展望。未来工作将在可信评估、数据的收集与检测、移动性能以及跨平台优势方面更加深入，使得传感云与雾设备的工作机制更加融合[39]。在这种情况下，独立的雾设备可以直接与云协同合作，而相互连接的雾设备也可以相互协作商议，进一步完善为具有更高可信度的联合。

5.1 基于雾计算模式的可信节点信任评估

如前所述，云端远离传感网络，对传感网络的信息掌控不全面、不及时，因此无法对底层传感网提供可信的评估。信任传递这种推荐式、传递型的信任计算非常不可靠，多跳信任传递容易产生信任评估失真、不准确[46-48]。而在移动雾节点模式下，这种信任传递的链条可以尽量缩短。如图 6 所示，若雾节点固定在节点 *A* 处不动，则其对节点 *I* 的信任评价链条为 *A*—*B*—*C*—*D*—*E*—*H*—*I* 或者 *A*—*B*—*C*—*D*—*F*—*G*—*I*。而在移动的情况下，假设沿着图 6 实线箭头移动到了节点 *E*，而节点 *E* 又恰好是一个不可信的节点，则可以避免选择该不可信的中间节点，而是回退一个节点从节点 *D* 开始构建信任传递链条。最后其对节点 *I* 的信任评价链条为 *D*—*F*—*G*—*I*。这种方法较传统方法大大缩减了信任传递链条的长度，从而提高了信任评价的可信度。通过选取关键性的可信评估参数，可以建立一套细粒度的节点信任评估方法，提高信任评估的准确度，从而甄别、标识不可信的节点，为后续的可信数据收集提供依据。

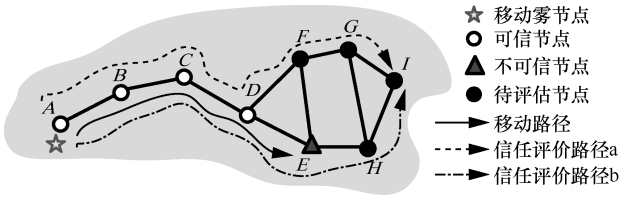


图 6 利用移动雾节点的信任传递链条

5.2 基于可信度的移动式数据收集

对于可信系统而言，准确高效的数据收集是管理决策的基础。一旦无法认定收集到的数据可以信任，后续的数据保护便无从谈起[49]。因此，云端有必要对底层传感器网络的数据可信性进行管理，综合 4.3 节的信任评估，在移动雾节点规划移动路径的过程中加入节点的可信性因素的考虑。移动雾节点可以绕开不可信的传感节点，这是设计时延敏感型数据收集方法时需要参考的重要特性，从而避免不必要的移动时延。进行路径规划应该综合考虑设定区域范围内的总体信任情况，而非单一节点。将总体与局部信任的不同情况结合处理，能够最大化效率，满足数据时效性的要求，有助于提升传感云系统的可信级别。在不影响网络部署与应用平台的同时，应考虑在有限的移动距离内，节点尽可能地向可信度高的区域移动，以达到一次收集更多的可信数据的需求。

5.3 可信数据筛选与检测

即便系统可以通过移动节点访问可信数据源进行数据收集，依然无法确保这些数据完全可信。在数据的生命周期中，由于数据传输过程存在若干不可靠因素，如被恶意节点故意干扰破坏等，系统还需要对数据进行广泛筛选[50]。因此，将数据进行实时评估和筛选，对于保证系统可信性具有重要意义。在后续研究中，如何深度挖掘雾计算与传感云结合后的计算能力与存储能力，利用雾端靠近本地的优势进行研究设计也是研究关键。基于离群点检测的可信数据筛选是一种有效的方法，如图 7 所示，运用雾层动态维护一个空间数据集（其中的数据可以是单个数据值，也可以是向量数据值），大圆点代表数据值的空间位置，小圆点表示 3 个平面上的

投影。基于这样的数据集，采用离群点检测算法检测、甄别异常及不可信数据。

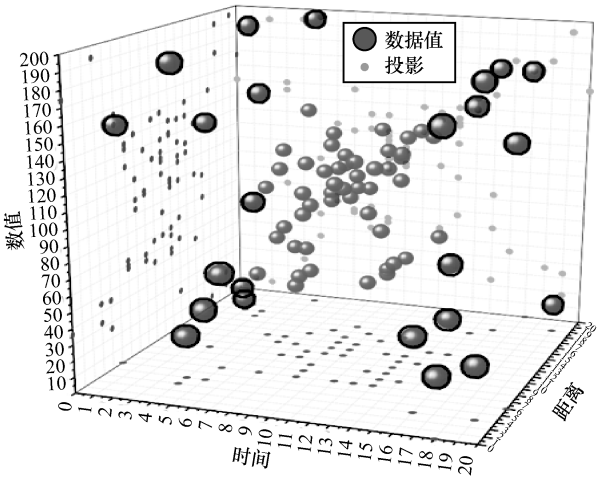


图 7　离群点检测示例（颜色越深、球越大且有边缘表示异常）

6　结束语

随着云计算技术的发展，可信传感云系统面临着越来越多的挑战，它们主要集中于数据收集、数据处理、节点信任评估及数据存储与隐私保护等层面。本文首先讨论了传感云在无线传感器网络环境中成为一个强大系统的原因，并系统地总结与分析了传感云系统在可信方面的制约因素。通过大量调研发现，传感云系统应满足更高的可信要求，这是因为不可信的信息会导致云端执行错误的决策与操作。通过分析和归纳发现，传感云与雾计算模式结合的新型应用模式可能成为未来的重点发展方向。特别是数据存储、节点可信评估及可信数据收集等问题在雾计算背景下实现场景的复杂性与实践性。最后，对基于可信节点信任评估、可信数据收集以及可信数据筛选等问题进行了展望，也希望能够为后续研究提供可参考的研究思路。

参考文献：

[1] GUPTA A, MUKHERJEE N. Implementation of virtual sensors for building a sensor-cloud environment[C]// International Conference on Communication Systems and Networks. IEEE, 2016: 1-8.

[2] SELIMI M, CERDAALABERN L, WANG L, et al. Bandwidth-aware service placement in community network micro-clouds[C]// Conference on Local Computer Networks. IEEE, 2017: 220-223.

[3] MISRA S, CHATTERJEE S, OBAIDAT M S. On theoretical modeling of sensor cloud: a paradigm shift from wireless sensor network[J]. IEEE Systems Journal, 2017, 11(2): 1084-1093.

[4] ZHOU P, ZUO D H, HOU K, et al. A decentralized compositional framework for dependable decision process in self-managed cyber physical systems[J]. Sensors, 2017, 17(11): 2580-.

[5] 林晖, 于孟洋, 田有亮,等. 移动云计算中基于动态博弈和可靠推荐的传递信誉机制[J]. 通信学报, 2018, 39(5): 85-93.
LIN H, YU M Y, TIAN Y L, et al. Dynamic game and reliable recommendation based transferring reputation mechanism for mobile cloud computing[J]. Journal on Communications, 2018, 39(5): 85-93.

[6] TAK B C, KWON Y, URGAONKAR B. Resource accounting of shared it resources in multi-tenant clouds[J]. IEEE Transactions on Services Computing, 2015, 10(2): 302-314.

[7] ZHU C, LI X, LEUNG V C M, et al. Job scheduling for cloud computing integrated with wireless sensor network[C]// International Conference on Cloud Computing Technology and Science. IEEE, 2014: 62-69.

[8] 王田, 李洋, 贾维嘉, 等. 传感云安全研究进展[J]. 通信学报, 2018, 39(3):35-52.
WANG T, LI Y, JIA W J, et al. Research progress of sen-sor-cloud security[J]. Journal on Communications, 2018, 39(3):35-52.

[9] SANTOS, IGOR L, et al. Olympus: the cloud of sensors[J]. IEEE Cloud Computing, 2015, 2(2): 48-56.

[10] 孟倩, 马建峰, 陈克非,等. 基于云计算平台的物联网加密数据比较方案[J]. 通信学报, 2018, 39(4): 167-175.
MENG Q, MA J F, CHEN K F, et al. Data comparable encryption scheme based on cloud computing in Internet of things[J]. Journal on Communications, 2018, 39(4): 167-175.

[11] BOTTA A, DE D W, PERSICO V, et al. Integration of cloud computing and internet of things: a survey[J]. Future Generation Computer Systems, 2016, 56: 684-700.

[12] WANG T, ZENG J D, BHUIYAN M Z A, et al. Trajectory privacy preservation based on a fog structure for cloud location services[J]. IEEE Access, 2017, 5: 7692-7701.

[13] DIVI K, LIU H. Modeling of WBAN and cloud integration for secure and reliable healthcare[C]//International Conference on Body Area Networks. ICST, 2013: 128-131.

[14] ALMASHAQBEH G, HAYAJNEH T, VASILAKOS A, et al. Qos-aware health monitoring system using cloud-based WBANS[J]. Journal of Medical Systems, 2014, 38(10): 121.

[15] 王文华, 王田, 吴群, 等. 传感网中时延受限的移动式数据收集方法综述[J], 计算机研究与发展, 2017, 54 (3): 474-492.
WANG W H, WANG T, WU Q, et al. Survey of delay-constrained data collection with mobile elements in WSNs[J]. Journal of Computer Research and Development, 2017, 54 (3): 474-492.

[16] ZHU C, LEUNG V C M, YANG L T, et al. Trust assistance in sensor-cloud[C]// Conference on Computer Communications Workshops. IEEE, 2015: 342-347.

[17] YANG C, LIU C, ZHANG X, et al. A time efficient approach for detecting errors in big sensor data on cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(2): 329-339.

[18] ZHU C, SHENG Z, LEUNG V C M, et al. Toward offering more

useful data reliably to mobile cloud from wireless sensor network[J]. IEEE Transactions on Emerging Topics in Computing, 2015, 3(1): 84-94.

[19] SENGUPTA, AVIK, RAVI T, et al. Fog-aided wireless networks for content delivery: fundamental latency tradeoffs[J]. IEEE Transactions on Information Theory, 2017, 63(10): 6650-6678.

[20] ZHU C S, LEUNG V C M, WANG K, et al. Multi-method data delivery for green sensor-cloud[J]. IEEE Communications Magazine, 2017, 55(5): 176-182.

[21] 王田, 梁玉珠, 彭臻, 等. 无线传感器网络中移动目标探测跟踪研究进展[J], 软件学报, 2017, 28(s1): 115-128.
WANG T, LIANG Y Z, PENG Z, et al. Research advance of detection-centric target tracking with mobile elements in wireless sensor networks[J]. Journal of Software, 2017, 28(s1): 115-128.

[22] PARICHEHREH A, SPAGNOLINI U. Inter-and intra-cloud resource allocation for delay sensitive industrial networks[C]// Conference on Networks and Communications. IEEE, 2014: 1-5.

[23] LIU B, JIA D, WANG J, et al. Cloud-assisted safety message dissemination in VANET–cellular heterogeneous wireless network[J]. IEEE Systems Journal, 2017, 11(1): 128-139.

[24] KUMARI R. An efficient data offloading to cloud mechanism for smart healthcare sensors[C]// International Conference on Next Generation Computing Technologies. IEEE, 2015: 90-95.

[25] TSO R, ALELAIWI A, RAHMAN S, et al. Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud[J]. Journal of Signal Processing Systems, 2017, 89(1): 51-59.

[26] LAI Y, YANG F, SU J, et al. Fog-based two-phase event monitoring and data gathering in vehicular sensor networks[J]. Sensors, 2017, 18(1): 82.

[27] BUTUN I, EROL-KANTARCI M, KANTARCI B, et al. Cloud-centric multi-level authentication as a service for secure public safety device networks[J]. IEEE Communications Magazine, 2016, 54(4): 47-53.

[28] DONG M, OTA K, LIU A. Preserving source-location privacy through redundant fog loop for wireless sensor networks[C]// International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. IEEE, 2015: 1835-1842.

[29] HUANG X, XIANG Y, BERTINO E, et al. Robust multi-factor authentication for fragile communications[J]. IEEE Transactions on Dependable and Secure Computing, 2014, 11(6): 568-581.

[30] 刘健. 智能交通灯系统中雾计算适用的车辆信息安全采集协议研究[D]. 上海: 华东师范大学.2017.
LIU J. Research on vehicle information security acquisition protocol in intelligent traffic light system for fog computing[D]. Shanghai: East China Normal University. 2017.

[31] WANG T, PENG Z, WEN S, et al. Reliable wireless connections for fast-moving rail users based on a chained fog structure[J]. Information Sciences, 2017, 379: 160-176.

[32] CORCORAN P, DATTA S K. Mobile-edge computing and the internet of things for consumers: extending cloud computing and services to the edge of the network[J]. IEEE Consumer Electronics Magazine, 2016, 5(4): 73-74.

[33] WANG T, ZENG J D, LAI Y, et al. Data collection from WSNs to the cloud based on mobile fog elements[J]. Future Generation Computer Systems, 2017, Doi: 10. 1016/ j. future. 2017.07.031.

[34] 贾维嘉, 周小杰. 雾计算的概念、相关研究与应用[J]. 通信学报, 2018, 39(5): 153-165.
JIA W J, ZHOU Xi J. Concepts, issues, and applications of fog computing[J]. Journal on Communications, 2018, 39(5): 153-165.

[35] LIU Q, WANG G J, LIU X H, et al. Achieving reliable and secure services in cloud computing environments[J]. Computers and Electrical Engineering, 2017, 59: 153-164.

[36] WANG T, ZHOU J Y, HUANG M Z, et al. Fog-based storage technology to fight with cyber threat[J]. Future Generation Computer Systems, 2018, 83: 208-218.

[37] WANG T, MD ZAKIRUL A B, WANG G J, et al. Big data reduction for smart city's critical infrastructural health monitoring[J]. IEEE Communications Magazine, 2018, 56(3): 128-133.

[38] MD ZAKIRUL A B, WANG G J, WU J, et al. Dependable structural health monitoring using wireless sensor networks[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(4): 363-376.

[39] WANG T, ZHANG G X, MD ZAKIRUL A B, et al. A novel trust mechanism based on fog computing in sensor-cloud system[J]. Future Generation Computer Systems, 2018, DOI: 10.1016/j. future. 2018 .05. 049.

[40] WANG T, LI Y, FANG W, et al. A comprehensive trustworthy data collection approach in sensor-cloud systems[J]. IEEE Transactions on Big Data, 2018, DOI: 10.1109/TBDATA.2018.2811501.

[41] GONG W, QI L, XU Y. Privacy-aware multidimensional mobile service quality prediction and recommendation in distributed fog environment[J].Wireless Communications and Mobile Computing, 2018, 2018(4): 1-8.

[42] HAMID H, RAHMAN M, HOSSAIN S, et al. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography[J]. IEEE Access, 2017, 5: 22313-22328.

[43] QI L, ZHANG X, DOU W, et al. A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment[J]. Future Generation Computer Systems, 2018, 88: 636-643.

[44] ZHU L, ZHANG C, XU C, et al. RTSense: providing reliable trust-based crowd sensing services in CVCC[J]. IEEE Network, 2018, 32(3): 20-26.

[45] WANG T, LI Y, WANG G J, et al. Sustainable and efficient data collection from WSNs to cloud[J]. IEEE Transactions on Sustainable Computing, 2017, DOI: 10. 1109/ TSUSC.2017.2690301.

[46] WANG T, ZHOU J Y, CHEN X L, et al, A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2(1): 3-12.

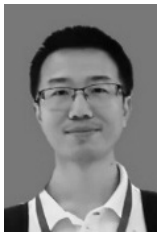
[47] ZHANG G X, WANG T, MD Z A B, et al. A fog-based hierarchical trust mechanism for sensor-cloud underlying structure[C]// International Symposium on Parallel and Distributed Processing with Applications. IEEE, 2017: 481-485.

[48] 王田, 张广学, 蔡绍滨, 等. 传感云中的信任评价机制研究进展[J], 通信学报, 2018, 39(6): 37-51.
WANG T, ZHANG G X, CAI S B, et al. Survey on trust evaluation mechanism in sensor-cloud[J]. Journal on Communications, 2018, 39(6): 37-51.

[49] GAO C Z, CHENG Q, LI X, et al. Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network[J]. Cluster Computing, 2018, DOI: 10.1007/s10586-017-1649-y.

[50] PENG T, LIU Q, MENG D C, et al. Collaborative trajectory privacy preserving scheme in location-based services[J]. Information Sciences, 2017, 387: 165-179.

[作者简介]



王田（1982− ），男，湖南汨罗人，博士，华侨大学教授，主要研究方向为物联网及其安全问题、云计算技术、社交网络、软件安全、大数据处理等。

沈雪微（1994− ），女，河南新乡人，华侨大学硕士生，主要研究方向为雾计算、传感云、物联网及其安全问题等。

罗皓（1994− ），男，广东惠州人，华侨大学硕士生，主要研究方向为雾计算、传感云、物联网及其安全问题等。

陈柏生（1980− ），男，湖南蓝山人，华侨大学讲师，主要研究方向为云计算技术。

王国军（1970− ），男，湖南长沙人，博士，广州大学教授、博士生导师，主要研究方向为网络和信息安全、物联网、云计算等。

贾维嘉（1957− ），男，中国香港人，博士，上海交通大学教授、博士生导师，主要研究方向为下一代无线通信、协议、异构网络等。