传感云中的信任评价机制研究进展

王田[1]，张广学[1]，蔡绍滨[1]，贾维嘉[2,3]，王国军[4]

（1. 华侨大学计算机科学与技术学院，福建 厦门 361021；2. 澳门大学数据科学中心，澳门 999078；
3. 上海交通大学电子信息与电气工程学院，上海 200240；4. 广州大学计算机科学与教育软件学院，广东 广州 510006）

摘 要：传感云系统逐渐发展为一个研究热点。好的信任评价机制能够解决这种新结构中存在的内部攻击等一些安全问题，并且能更好地保障该结构中信息的安全、高效传输。通过对传感云和信任评价机制进行广泛的调研，归纳出传感云的信任评价机制可分为实体间和实体内 2 类，对比现有信任评价机制的优点与不足，设计了基于雾计算模式的新型信任评价模型，探讨了未来的研究方向。

关键词：传感云；内部攻击；信任评价机制；雾计算

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018098

Survey on trust evaluation mechanism in sensor-cloud

WANG Tian[1], ZHANG Guangxue[1], CAI Shaobin[1], JIA Weijia[2,3], WANG Guojun[4]

1. College of Computer Science and Technology, Huaqiao University, Xiamen 361021, China
2. Data Science Center, University of Macau, Macao 999078, China
3. School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai 200240, China
4. School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China

Abstract: Sensor-cloud has gradually developed into a research hotspot. A good trust evaluation mechanism can better address some security issues in this new structure, such as internal attacks. A good trust evaluation mechanism can also ensure the security and efficient transmission of information in this structure. After an extensive research on sensor-cloud and trust evaluation mechanisms, it was found that trust evaluation mechanisms in sensor-cloud can be divided into two categories, among entities and in entity. After comparing the advantages and shortcomings of existing trust evaluation mechanisms, a new fog-based trust evaluation mechanism was designed and future research directions of trust evaluation mechanisms were discussed in sensor-cloud.

Key words: sensor-cloud, internal attack, trust evaluation mechanism, fog computing

1 引言

传感云系统是目前学术界的一个研究热点，它将无线传感器网络（WSN, wireless sensor network）和云计算无缝地连接起来[1-3]。传感云的提出，可以使各种应用服务不再单独地占用物理传感器，从而提高传感器节点的利用率并能为用户提供定制化服务[4-5]。WSN 被誉为 21 世纪最重要的科技，主要分为陆地监控、地下监控、水下监控、多媒体、移动网络等几种形式[6-7]。云计算拥有大规模的硬件和

收稿日期：2017-09-12；**修回日期**：2018-03-15

通信作者：王田，cs_tianwang@163.com

基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（No.2015CB352401）；国家自然科学基金资助项目（No.61532013, No.61632009, No.61571150, No.61772148, No.61672441）；上海交通大学 985 千人计划启动基金资助项目（No.WF220103001）

Foundation Items: The National Basic Research Program of China (973 Program) (No.2015CB352401), The National Natural Science Foundation of China (No.61532013, No.61632009, No.61571150, No.61772148, No.61672441), 985 Project of Shanghai Jiaotong University (No.WF220103001)

软件，而且具有强大的并行批量处理能力，这为传感数据的存储、处理以及分析提供了有力保障[8-9]。然而，许多WSN的建立并未执行统一的标准，使WSN的利用率和数据共享率较低，例如，单个WSN中的传感器只应用于特定应用、不同WSN的数据存在格式转换问题等[10]。针对WSN资源利用率低以及数据共享差等缺点，一些研究者结合云计算的经济优势和技术优势，提出传感云的概念，并逐渐发展成为一个研究热点[11-12]。传感云可应用于军事探测、工业控制、医疗协助、环境监测等领域，为人们的工作和生活带来了很大便利[13-16]。

随着传感云系统的快速发展和广泛应用，其安全问题也逐渐显现[17-18]。传感云所面临的安全威胁有外部攻击、内部攻击以及针对信任评价机制的攻击[19-21]。传统的加密、授权和认证等安全方式能够有效地应对外部攻击，但却不能准确地处理内部攻击问题[22-23]。此外，传感器节点存在能量少、存储能力和计算能力有限等缺陷，传统的安全措施由于计算量较大并不太适用于WSN[24-26]。信任评价机制能够有效应对内部攻击，提高网络的安全性能[27-28]，并且更适用于资源受限的WSN。

信任评价机制是传感云安全的重要补充策略，广泛存在于WSN、云计算、物联网（IoT, Internet of things）、移动自组织网络（MANET, mobile ad-hoc network）等领域，并且在应用上取得了较好的成果[29-31]。信任评价机制来源于人类社会生活经验，虽然学术界并没有对其做出统一的定义，但一个共识是：信任评价机制相比于传统安全机制更加轻量，能较好地解决网络中的内部攻击问题，并具有保证网络性能和提高网络通信量等优势，是传统安全机制的有益补充[32-33]。传感云是一个新型结构，其信任评价机制正在逐步完善[34]。本文对传感云系统中的信任评价机制进行了广泛研究和对比，并设计了一些方案来填补传感云系统在信任评价机制方面的一些不足之处。其中，基于雾计算的信任评价机制可以更好地管理传感云底层结构之间的信任关系。最后，本文也对传感云信任评价机制的未来发展和研究方向进行了探讨。

2 传感云中信任评价机制的研究

传感云的基本结构可分为3个部分：WSN层、云层、用户层。这3个基本部分对应于3个决策实体，分别是：WSN层中的传感网服务提供商（SNSP, sensor network service provider）、云层中的云服务提供商（CSP, cloud service provider）、用户层中的用户。其中，SNSP主要提供传感数据服务，将其所拥有的传感数据（交通监测数据、环境监测数据、工业监测数据等）发送给CSP；CSP主要提供存储服务和处理服务，存储服务将来自SNSP的数据存储在云端，处理服务对传感数据做进一步处理来满足一些应用需求；用户主要是使用CSP提供的数据处理服务。传感云的信任评价机制研究总体上可分为2类：实体间信任和实体内信任。实体间信任为3个决策实体间的信任关系，而实体内信任多为WSN中节点间的信任关系。实体间的信任更多地涉及人与人之间信任关系的建立问题，而实体内的信任则更多地关注于如何通过节点间的行为信息来构建节点间的信任关系。其中，实体内信任关系的建立需要考虑底层网络性能稳定、能耗较少、负载较低等一些急需解决的问题。

2.1 实体间的信任

实体间的关系可以定义为服务使用者与服务提供者之间的信任关系。

实体间的信任关系又可以细分为3类：用户和SNSP对CSP的信任、CSP对用户的信任、CSP对SNSP的信任。就目前的研究状况来说，根据实体间信任评价机制建立方式的不同，一般分为以下几类[35]，如表1所示。

2.1.1 用户和SNSP对CSP的信任

在云中，CSP提供大量相似云服务，并且其所提供的服务具有动态性，服务质量也会变化，这给服务使用者选择合适的云服务造成了困扰[36]。就服务使用者来说，对云服务的信任是建立在其可靠性、安全性、友好性、可控性、私有性、稳定性等特征的基础上[37]。其中，用户和SNSP对云服务的要求有些区别。用户主要考虑其可靠性、稳定性、友好性等一些特征。SNSP将更多的数据存储在云中，对数据安全性、私密性和完整性的要求更加严格。

文献[38]提出了一种基于服务水平协议/隐私水平协议（SLA/PLA, service level agreement/privacy level agreement）的信任和声誉管理系统。首先，信任中心（TCE, trust center entity）根据一些服务参数对CSP进行信任计算以及声誉管理。然后，用户根据自身需求快速准确地选择合适的CSP。

文献[39]提出了基于服务质量（QoS, quality

表 1　　**实体间的信任评价机制分类**

信任分类	说明	特征	优点	缺点
基于政策信任	对一些参数进行监测，并通过约定的规则进行信任计算	SLA/PLA、监控、审计、QoS	完整性高、安全性高	灵活性低、速度慢
基于推荐信任	综合多个服务使用者对服务提供者的认知，建立对服务提供者的信任	直接推荐、传递推荐	速度快、灵活性高	安全性低、完整性低
基于声誉信任	声誉是服务使用者对服务提供者长期行为的一个评价，将声誉用于服务提供者信任值的计算	推荐、信任反馈、声誉积聚	速度较快、灵活性较高	安全性一般、完整性一般
基于预测信任	服务使用者与陌生服务提供者之间信任关系的建立是基于预测信任的	相似实体、信任决策、信任预测	速度快、灵活性高	安全性一般、完整性低

of service）的信任评价模型，该模型关注 CSP 所提供服务的可用性、可依赖性、周转效率和数据完整性。然后，采用基于权重的方式综合考虑 CSP 的信任状况。

文献[40]基于用户的反馈评级提出了一种轻量型的声誉测量方式，利用反馈评级为每一个云服务建立信任向量，并通过模糊集理论对信任向量中的期望值、熵值和超熵值进行计算，最后得出其声誉值。

文献[41]采用了混合的粒子群优化—神经网络算法对云服务进行信任预测，使用粒子群优化算法优化神经网络的初始参数设定，然后进行全局最优适应值的计算并进行信任预测。

2.1.2　CSP 对用户的信任

云服务具有开放性，任何用户都可以连接到云服务平台获取服务。但是，也存在一些恶意用户不合理地使用云服务、恶意占用资源、诽谤或提供虚假反馈信息等行为。解决这些问题的有效方式是对用户进行接入控制或将用户权限进行等级操作[42]。

文献[43]提出，在用户和云平台之间建立彼此信任的关系来实现云平台的接入控制。通过用户身份证明（ID, identification）和物理地址（MAC, medium access control）来确定用户身份，并在 CSP 之间共享这些用户信息。

然而，一些攻击者会通过一些恶意外部攻击获取用户 ID 等信息并控制用户设备，并通过这些俘获的用户设备实施内部攻击。一般检测机制检测到的是已发生的攻击事件，而事后的弥补措施并不能减少已有损失。文献[44]根据入侵事件发生前会出现一些特殊信号这一特征，提出了一种基于用户行为识别的概要管理系统来监测可疑行为，并通过动态触发反映模块来监控可疑节点并收集必要的证据。

文献[45]通过用户行为风险值、用户信任等级和其他因素构建了新的基于角色的接入控制模型，通过风险值和用户信任水平的衡量，对不同用户进行动态灵活的授权。

2.1.3　CSP 对 SNSP 的信任

从 CSP 的角度来说，SNSP 的数据必须是真实的，不能存在人为的编撰或篡改。传感数据应该具有时效性、完整性、精确性等一些特征，否则会对 CSP 的声誉造成严重影响。就目前的研究状况来看，科研人员对这方面的研究处于初步阶段。

文献[38]提出通过一些基本信任计算（数据收集信任、网络寿命信任、网络响应时间信任、数据传输信任）得出 CSP 对 SNSP 的信任值，并且根据历史记录计算 SNSP 的声誉值。基于 SNSP 的信任值和声誉值，CSP 可根据自身需求快速准确地选择合适的 SNSP。

2.2　实体内的信任

实体内的信任主要发生在传感数据产生时和中间节点对数据处理时 2 个方面。数据产生过程中导致数据有误的原因有 2 类，一类是由节点故障产生的，另一类是由被俘获节点产生的[46]。对于内部恶意节点攻击或节点故障，信任评价机制可以很快检测到并做出及时反应来改善网络环境。实体内的信任评价机制已经得到了广泛的研究，一般信任评价机制的基本步骤如图 1 所示。

2.2.1　数据收集

在信任评价机制中，很重要的一个环节就是有效、及时的信任数据收集。收集到的信任数据可用于一般信任公式计算，如直接信任、推荐信任、间接信任等，也可以应用到一些综合信任策略中，如仿生信任计算等。在网络中可收集的信任数据很多，如节点剩余能量、网络拥堵情况、接收数据的正确性、节点能量效率、节点之间的交互状态、节点接收信号的能力等。

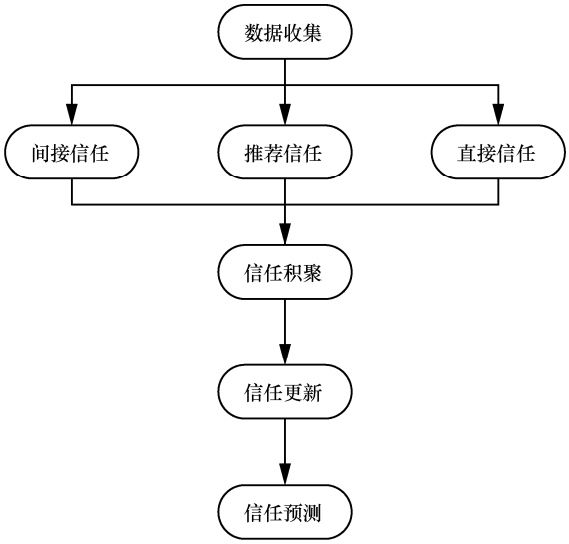


图 1 实体内信任评价机制框架

表 2 为一些英文表达简化成大写首字母后的形式，并给出了其所对应的中文含义。

表 2 计算公式中英文缩写对照

原始表示	缩略词	意义
trust	T	信任
direct	D	直接信任
recommendation	R	推荐信任
indirect	I	间接信任
positive	P	积极行为
negative	N	消极行为
energy	E	能量
communication	C	通信

2.2.2 基本信任计算

1) 直接信任

直接信任的一般定义为：在 2 个相邻节点的直接交互过程中，一个节点通过所获取的直接交互信息来评价另一个节点的行为。直接信任的简单模式如图 2 所示。

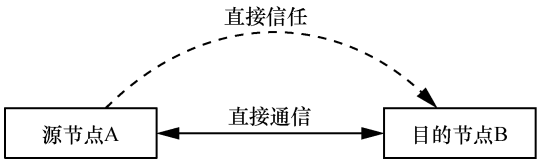


图 2 直接信任

在节点间的直接交互过程中，很多观测值可以用来检测恶意节点。

文献[47]提出节点信任水平的衡量基于以下 2 个方面，一个是对目的节点行为的观测，另一个是目的节点的剩余能量。在直接信任计算中，该文献设定行为信任和能量信任占据相同的比重，并综合考虑了历史行为和现有行为因素，如式(1)所示。

$$T_{\mathrm{D}(x,y)^l}=\frac{1}{2}w_1T_{\mathrm{P}(x,y)^{l-1}}+\frac{1}{2}w_2T_{\mathrm{N}(x,y)^{l-1}}+\frac{1}{2}T_{\mathrm{Now}(x,y)^l}+\frac{1}{2}T_{\mathrm{E}} \tag{1}$$

其中，$T_{\mathrm{P}(x,y)}$为 y 节点对 x 节点过去良好行为的信任值，$T_{\mathrm{N}(x,y)}$为 y 节点对 x 节点过去不良行为的信任值，$T_{\mathrm{Now}(x,y)}$为 y 节点对 x 节点现有行为的信任值，T_{E}为 y 节点对 x 节点的能量信任值。

文献[48]提出基于权重的方式来计算目的节点的信任值，综合考虑了能量信任 T_{E}、通信信任 T_{C} 和数据信任 T_{data} 这 3 个因素，其计算式如式(2)所示。

$$T_{\mathrm{D}}=w_1T_{\mathrm{E}}+w_2T_{\mathrm{C}}+w_3T_{\mathrm{data}} \tag{2}$$

文献[49]基于多个网络活动，综合历史信任信息、积极行为、消极行为 3 个因素来计算目的节点的直接信任值，如式(3)所示。

$$T_{\mathrm{D}}(i,j)^l=\sum_{a\in A}f_d\left(T_{\mathrm{D}}(i,j)^{l-1},P_j(a)^l\right)P_w(a)-\sum_{a\in A}f_d\left(T_{\mathrm{D}}(i,j)^{l-1},N_j(a)^l\right)N_w(a) \tag{3}$$

其中，直接信任是通过积极行为信任和消极行为的信任差值形式得出，并且对每一个不同的网络活动 a，通过 $P_w(a)$和 $N_w(a)$赋予不同的权重。其中，$T_{\mathrm{D}}(i,j)^{l-1}$为上一轮 i 节点对 j 节点的信任值，$\frac{P_j(a)^l}{N_j(a)^l}$ 为对 j 节点现在积极/消极行为记录。

但是，考虑到 WSN 的用途、性能、所处环境、安全级别等实际情况，实体内的直接信任通常仅仅考虑一些重要的观测值，如数据分组丢失率、路由失败率、能量消耗、数据分组错误率、传输速率等。在系统设计时，较少的观测值可以达到减少节点能耗、降低计算和设计复杂度、保证网络性能、增加系统可实现性等设计要求。

在这里，本文列举了一些经常使用观测值的信任计算，如下所示。

①通信因素

在节点交互过程中，最容易观测的是一段时间内成功通信的次数。其信任计算一般采用 Beta 分布[50]，如式(4)所示。

$$T_{\mathrm{C}}=\frac{\alpha+1}{\alpha+\beta+2} \tag{4}$$

其中，α 为节点通信成功次数、β 为节点通信失败次数。在通信成功率的信任计算中，通常采用时间窗方式来综合考虑节点的长期行为变化[51]。

然而，存在一些针对信任评价机制的攻击方式，如 On-Off 攻击等。为应对这些攻击，多数研究者在信任计算中加入了惩罚机制，如文献[52]中加入惩罚因子 $\frac{1}{\sqrt{\beta}}$、文献[53]中加入惩罚因子 $\left(1-\frac{1}{\alpha+1}\right)$、文献[54]中针对节点行为波动情况加入余弦函数 $\cos\left(\left(\frac{\pi}{2}\right)\times Behavior_{\text{fluctuation}}\right)$ 等，当节点表现出友好行为时，信任会缓慢增加；反之，信任值则会急剧减少。

②能量因素

通信过程中，正常节点的能量消耗总是有规律的，而恶意节点在进行恶意攻击时会产生不正常的能量消耗。如果环境变化较小，正常节点能量消耗率将维持在一个稳定的区间。文献[48]提出了一个能量预测模型来获取节点在不同时期的能量消耗，然后依据能量预测模型来计算节点能量信任，如式(5)所示。

$$T_{\text{E}}=\begin{cases}1-P_{\text{E}} & ,E_{\text{remain}}\geqslant\theta\\ 0 & ,\text{其他}\end{cases} \tag{5}$$

其中，P_{E} 为能量消耗率，E_{remain} 为剩余能量，θ 为阈值。其中，P_{E} 是通过能量预测模型计算得出的。当剩余能量大于阈值时，通过计算能量消耗率来得到关于能量的信任值；反之，信任值为 0。

③数据因素

数据信任是指经过中继节点转发的数据或从中继节点接收的数据是否正确可信。文献[55]提出了一种数据信任计算方式：通信过程中正确数据分组占整体数据分组的比率，如式 (6)所示。

$$T_{\text{data}}=\left(1-\frac{N_{\text{error}}}{N_{\text{total}}}\right)\times 100\% \tag{6}$$

其中，N_{error} 为错误数据分组数量，N_{total} 为所传输的数据分组总数。

数据分组具有一定的空间关联性，即在相同的区域，节点向相邻节点传送的数据分组总是相似的。文献[48]将这一特性抽象为正态分布，用一组数据的平均值来衡量数据的相似性。如果数据接近平均值，则其信任值越高，反之，信任值越低，如式(7)所示。

$$T_{\text{data}}=2\left(0.5-\int_{\text{mean}}^{\text{variance}}f(x)\,\text{d}x\right) \tag{7}$$

其中，$f(x)$为正态分布的密度函数，积分区间为从平均值 mean 到数据的方差 variance。

另外，在一定的空间内，不同节点的监测值存在相似性。也就是说，在同一段时间内，一定区域内的节点对环境的监测值差距不大或具有一定的关联性。文献[56]评估比较节点自身的监测值与目的节点的监测值，以此来预防恶意节点对数据的伪造，其计算如式(8)所示。

$$T_{\text{data}}(t)=\frac{Consist_{\text{number}}(t)}{Consist_{\text{number}}(t)+Inconsist_{\text{number}}(t)} \tag{8}$$

其中，$Consist_{\text{number}}$ 为 t 时间内，2 个节点具有相同/相似数据分组的数量；$Inconsist_{\text{number}}$ 为 t 时间内，2 个节点不具有相同/相似数据分组的数量。

④传输速率因素

信任评价机制中，可以通过监控节点的传输速率来监测一些恶意行为，如当节点传输速率低于最低阈值时，很可能是自私节点；当节点的传输速率高于最高阈值时，很可能是拒绝服务（DoS, denial of service）攻击等。针对上述情况，文献[56]提出当节点传输速率和期望速率接近时，节点拥有更高的信任值，如式(9)所示。

$$T_{\text{transmission}}(t)=\begin{cases}\dfrac{Sending_{\text{quantity}}(t)-Threshold_{\text{low}}}{Expecting_{\text{quantity}}(t)-Threshold_{\text{low}}}, & Sending_{\text{quantity}}(t)\leqslant Expecting_{\text{quantity}}(t)\\ \dfrac{Threshold_{\text{high}}-Sending_{\text{quantity}}(t)}{Threshold_{\text{high}}-Expecting_{\text{quantity}}(t)}, & Sending_{\text{quantity}}(t)>Expecting_{\text{quantity}}(t)\end{cases} \tag{9}$$

其中，$Expecting_{\text{quantity}}$ 为 t 时刻的期望传输速率，$Sending_{\text{quantity}}$ 为 t 时刻的真是传输速率，$\frac{Threshold_{\text{high}}}{Threshold_{\text{low}}}$ 为最高/最低传输速率。

2) 推荐信任

推荐信任的一般定义为：当源节点对目的节点的观测值不足时，源节点通过评估与其两者互为邻节点的节点推荐值得到对目的节点的信任值。推荐信任的简单模型如图 3 所示。

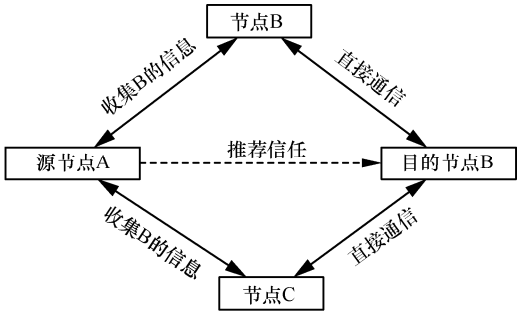


图 3 推荐信任

推荐信任的基本计算如式(10)所示[57]。在多数研究工作中，一般选择信任值超过一定阈值的节点参与推荐信任计算。

$$T_{\mathrm{R}}=\sum_{k\in N,k\neq i}T_{\mathrm{D}(i,k)}T_{\mathrm{D}(k,j)} \tag{10}$$

其中，$T_{\mathrm{D}(i,k)}$为 i 节点对 k 节点的直接信任值，$T_{\mathrm{D}(k,j)}$为 k 节点对 j 节点的直接信任值，k 为信任推荐节点。

在推荐信任的计算中，来自邻接节点的推荐值可能是不准确的或恶意的。为了减少这些情况所造成的影响，文献[53]使用基于权重的方式综合考虑其不同邻接节点的推荐值，如式(11)所示。权重值的计算与推荐节点 m 及剩余推荐信任列表中的信任节点相关，即考虑推荐节点的信任值与其他节点信任值的偏离程度，如式(12)所示。

$$T_{\mathrm{R}(i,j)}=\frac{\sum_{m\in Set(j)}\left(1-Diff_{(i,m)}\right)T_{\mathrm{D}(m,j)}}{\left|Set(j)\right|} \tag{11}$$

$$Diff_{(i,m)}=\frac{\sum_{k\in Set(j)}\left|T_{\mathrm{D}(k,j)}-T_{\mathrm{D}(m,j)}\right|}{\left|Set(j)\right|} \tag{12}$$

其中，集合 $Set(j)$中的节点与 i 节点和 j 节点都相邻，并且是 i 节点的信任节点；m 为推荐节点；$Diff_{(i,m)}$为推荐节点 m 的推荐信任值与其他信任节点推荐信任值的偏离程度；$T_{\mathrm{D}(m,j)}$为 m 节点对 j 节点的直接信任，其他符号与此类似。

在推荐信任计算过程中，对于推荐节点选择和恶意节点推荐值排除这些问题，可以使用一些现有的检测系统来解决。但是这些检测系统不太适合一些资源有限的 WSN。因此，文献[48]提出了一种基于推荐可靠性和推荐熟悉度的检测理论。推荐可靠性是 B 节点将接收到 C 节点的信任推荐值 $T_{\mathrm{C}}^{\mathrm{B}}$ 与接收到其他节点的平均推荐值 $T_{\mathrm{average}}^{\mathrm{B}}$ 进行比较，然后通过差值进行推荐可靠性计算，计算式为 $T_{\mathrm{reliable}}=1-\left|T_{\mathrm{C}}^{\mathrm{B}}-T_{\mathrm{average}}^{\mathrm{B}}\right|$。推荐熟悉度是指长期交互节点比短期交互节点拥有更高的权重值，推荐熟悉度计算式与节点之间成功通信次数相关，其计算式为 $T_{\mathrm{familiar}}=\left(\frac{number_{\mathrm{C}}^{\mathrm{B}}}{number_{\mathrm{C}}}\right)\times\alpha_{\mathrm{times}}^{\frac{1}{number_{\mathrm{C}}^{\mathrm{B}}}}$，其中，$number_{\mathrm{C}}^{\mathrm{B}}$ 为推荐节点 C 与目的节点 B 成功通信的次数；$number_{\mathrm{C}}$ 为推荐节点 C 总的成功推荐次数；$\alpha\in(0,1)$为与通信次数相关的调节因子。综合两者的作用，文中给出推荐信任的计算式为

$$T_{n-\mathrm{recommendation}}=\frac{\sum_{i=1}^{n}0.5+\left(T_{\mathrm{C}}^{\mathrm{B}}-0.5\right)T_{\mathrm{reliable}}T_{\mathrm{familiar}}}{n} \tag{13}$$

3) 间接信任

间接信任的一般定义为：源节点和目的节点不是相邻节点，源节点在向目的节点传送数据之前，需要通过其他节点建立与目的节点的信任关系，间接信任的简单模型如图 4 所示。

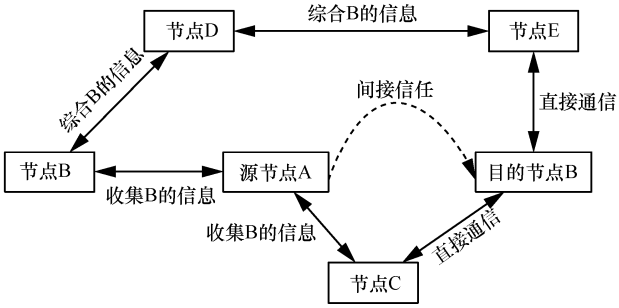


图 4 间接信任

源节点和目的节点之间没有直接通信路径，需要通过其他节点来建立节点间的信任关系。文献[48]提出间接信任的建立分为 2 个步骤：选择源节点和目的节点之间可能存在的推荐节点；以信任链的方式建立间接信任。从源节点到目的节点之间的路径由信任推荐节点组成，这条路径被称为信任链。信任链的建立需要遵循 3 个机制：① 推荐节点应尽可能接近目的节点；② 推荐节点的选择应是信任值最高的，以保证信任链的可靠性；③ 最优的信任链应该兼顾距离和信任值这 2 个因素。间接信任中信任链越长，其所面临的环境因素越复杂。所以，间接信任更容易受到一些针对性攻击，如 slander 攻击、self-promoting 攻击、collusion 攻击等，这些攻击都是基于信任链中源节点对中间节点信任的不确定性导致的。

文献[48]给出了间接信任的计算式，间接信任计算基于信任链，如式(14)所示。

$$T_{\mathrm{I}}\left(\begin{matrix}\mathrm{B}\\ \mathrm{C}_{i+1}\end{matrix}\right)=\begin{cases}T_{\mathrm{C}_{i+1}}\times T_{\mathrm{I}}\left(\begin{matrix}\mathrm{B}\\ \mathrm{C}_{i}\end{matrix}\right) & ,T_{I}\left(\begin{matrix}\mathrm{B}\\ \mathrm{C}_{i}\end{matrix}\right)<0.5\\ 0.5+\left(T_{\mathrm{C}_{i+1}}-0.5\right)\times T_{I}\left(\begin{matrix}\mathrm{B}\\ \mathrm{C}_{i}\end{matrix}\right) & ,\text{其他}\end{cases} \tag{14}$$

其中，$T_{\mathrm{C}_{i+1}}$ 为对信任链上第 i+1 个节点的信任值；$T_{\mathrm{I}}\left(\begin{matrix}\mathrm{B}\\ \mathrm{C}_{i}\end{matrix}\right)$ 为对信任链上前 i 个节点的信任值。

2.2.3 信任积聚和更新

1) 信任积聚

信任积聚是指将节点自我观测值或同级节点反馈的信任值进行聚合[58]，将聚合后的数据作为最终信任值或进行信任预测等。

目前，主要的信任积聚方式有基于权重、基于仿生、基于 D-S 证据理论等。在信任积聚的研究中，使用最多的是基于权重的信任积聚方式。

基于权重的积聚方式具有计算量小、轻便等特点，其计算式如式(15)所示[52,59]。

$$T_{\mathrm{total}}=w_{1}T_{\mathrm{D}}+w_{2}T_{\mathrm{I}} \tag{15}$$

信任积聚的计算式综合考虑了直接信任 T_{D} 和间接信任 T_{I}（包括推荐信任），w_1+w_2=1，其中，直接信任占有更大权重。

文献[60]提出通过数据分组正确转发信任、数据分组转发时间信任、正确推荐信任和公平推荐信任 4 个指标可以预防数据篡改和针对信任评价模型的攻击。文中也使用基于权重的方式进行信任值的积聚。

直接信任和间接信任的简单加权计算收敛较慢，对突发事件不敏感，不能及时检测出突然变坏的节点。为预防 On-Off 这一类型的攻击，文献[53]在信任积聚中加入了基于熵理论的风险预测机制，这种方式能够帮助模型及早地检测出恶意节点。

文献[61]提出了改进的仿生信任评价机制，在算法中设置一些人工蚂蚁来寻找从源节点到目的节点的路径，路径中节点信息素的多少表示节点的信任值大小。其中，同级信任系统（PTS, peer trust system）是一个动态的点对点信任评价机制模型，它权衡的因素有通信满意度、邻接节点的可信度、传输环境因素和社会环境因素。

D-S 理论是解决不确定问题的一类重要理论。文献[62]使用 D-S 理论来解决信任评价机制中的随机性和主观不确定性问题，通过修正 D-S 理论来动态计算推荐信任的权重。

2) 信任更新

在网络中，信任关系不是一成不变的。在一些异常状态下，交互节点的行为可能出现快速或不可预料的改变，如环境变化、节点被俘获、节点故障、节点被移除、节点被更新等，这是信任关系具有动态性的本质。当节点处于异常状态时，其信任值需要及时更新以维持网络的信任环境。信任的更新包括部分信任更新，如直接信任、推荐信任和间接信任的更新，也包括整体信任值的更新。一般信任的更新采用值累积的方式进行[57]，如式(16)所示。

$$T_{(i,j)}^{\mathrm{update}}\left(t+\Delta t\right)=T_{(i,j)}+T_{(i,j)}\left(t+\Delta t\right) \tag{16}$$

其中，$T_{(i,j)}$为 i 节点对 j 节点的历史信任值，$T_{(i,j)}(t+\Delta t)$为 i 节点对 j 节点在 $t+\Delta t$ 时刻的信任值。

另一种信任更新方式是基于权重的[63]，如式(17)所示。

$$T_{\mathrm{final}}\left(x,y\right)=w_{\mathrm{old}}T_{\mathrm{old}}\left(x,y\right)+w_{\mathrm{new}}T_{\mathrm{new}}\left(x,y\right) \tag{17}$$

其中，$T_{\mathrm{old}}(x,y)$为旧的信任值；$T_{\mathrm{new}}(x,y)$为新的信任值；$\frac{w_{\mathrm{old}}}{w_{\mathrm{new}}}$ 为新/旧信任值的权重，w_{old}+w_{new}=1。

考虑到一些休眠节点和不频繁交互节点，文献[60]对新的信任值增加了与时间相关的指数因子Δt，Δt 值越大，历史信任值的权重越小。文献[38]在更新信任值的过程中采用了忘记因子的方式来减少历史信任对整体信任的影响。

对于部分更新，节点在观察过程中可直接更新直接信任值；推荐信任和间接信任则通过收集其他节点的推荐值来更新信任值。太过于频繁的更新会占用太多的网络资源，然而周期太长的信任更新不能有效地反映节点的行为。

针对此类问题，多数研究工作中采用滑动时间窗机制[64]。更新方式为每过一个通信周期，时间窗向前滑动一个时间槽，然后对时间窗内的每一个时间槽赋予一定的权值并进行信任更新。

2.2.4 信任决策/预测

信任决策/预测是根据历史信任值和现有观测值或单独的现有观测值对节点未来行为进行决策/预测，并确定是否与其建立合作关系。一般信任决策/预测方式如表 3 所示。

文献[65]提出进化博弈论，通过将节点的信任度与激励机制相结合的方式来高效地促使节点选择具有信任行为的节点。在进化过程中，该策略存在一定稳定性。

表 3 信任决策/预测方式

方式	作用域	计算复杂度	准确性	内存消耗
基于博弈论	普通节点	复杂	一般	小
基于模糊理论	普通节点	简单	一般	大
基于贝塔分布	普通节点	简单	一般	小
基于相似性	特殊节点	复杂	准确	大
基于主观逻辑	普通节点	一般	准确	小

文献[52]提出了基于模糊理论的信任预测模型。在模型中，输入变量为直接信任值、邻接节点信任值的变动数量、推荐不一致性 3 个变量，通过模糊理论规则输出对节点的预测信任水平。

Beta 分布是二项分布的先验分布，具有计算灵活简单的优点，可以用来预测节点的行为。文献[66]中的信任计算考虑通信信任和数据信任 2 种情况，通过 Beta 分布来进行节点行为的预测。

节点间的交互通道存在不稳定性和噪声因素。文献[67]提出使用轻量型的主观逻辑来解决信任评价过程中存在的不确定性问题。

3 基于雾计算的信任评价机制模型

在传感云系统中，信任评价机制的研究已有很大进展。但是，对传感云底层结构的信任评价机制研究仍存在一些不足之处。

1) 在底层无线传感器网络中，信任评价机制的建立需要消耗一些必要资源（能量、计算能力、通信资源等），这造成了 WSN 性能降低、寿命减少以及一些其他方面的问题。因此，信任评价机制的设计目标应为：尽量减少不必要的观测值；尽量降低信任推荐次数；尽量降低数据运算量等。

2) 有一些恶意节点表现出正常节点的行为，并且不影响网络的性能，但会产生错误数据来误导用户做出错误决策。本文定义这类攻击为隐藏数据攻击。WSN 不具备针对这种类型攻击的分析和辨别能力。

3) 传统方法采用云端可信中心作为 CSP 和 SNSP 的信任第三方。但是，云端远离传感网端，这就造成可信中心对 WSN 端的监测实时性不强，缺乏一定指标（数据缺失率、检测周期、底层网络异常信息等）来建立 CSP 与 SNSP 的信任关系。从已有的研究内容来看，涉及 CSP 和 SNSP 之间信任关系的研究不多。

只有 CSP 和 SNSP 之间相互信任，才能从源头上保证为用户提供真实、安全、高效的数据服务。CSP 与 SNSP 之间是一种多对多的关系，并且他们之间的信任关系动态变化。为解决这种复杂关系下的信任问题，可采用一种机制实时监测双方的信任变化情况，并提供及时可信的数据监测指标。

针对这些问题，本文研究团队提出了基于雾计算（fog computing）的传感云信任评价机制。在传感云系统中，还没有基于雾计算的信任评价模型，现在的研究更多的是在无线传感器网络层和云层。雾计算对于解决这类问题有独特的优势，并且能减轻双方的计算和存储负担。

3.1 雾计算

雾计算由思科公司首次提出，它将云计算延伸到了网络边缘，应用在 IoT，如车联网、智能电网、智慧城市、无线传感网络[68-70]。雾计算位于云计算和边缘设备之间，具有低延时、位置感知、移动性、实时性、支持异构设备等特点。雾计算的定义[71]如下：“雾计算场景中，大量存在和分散的异构（无线或自治）设备在没有第三方介入的情况下，通过通信和相互协作方式来完成存储和处理任务。这些任务能支持基本的网络功能或运行在沙盒环境下的新服务和应用。用户通过租用一些设备来获取这些服务。”将雾计算作为宿主环境，可以普遍改善网络性能以及更好地支持设备之间的合作。

3.2 基于雾计算的信任评价机制

雾计算具有一定的数据存储和处理能力，与云计算相比，雾计算具有更强的实时性。雾计算能够较为全面、充分地获取底层网络的状况，作为连接传感网端和云端的桥梁和纽带，充当云 CSP 和 SNSP 的服务管理中心。此外，雾计算还有一个好处是：大量底层的数据处理任务不用提交到云端，可直接在雾层进行处理，然后将处理结果传送至云端，从而降低数据传送量，节约能量。这种新的信任评价模型如图 5 所示。

针对第三方可信评估缺失的情况，雾计算提供了可选方案。雾层充当云层和 WSN 层信任关系的缓冲地带。在模型中，SNSP 和 CSP 协商服务内容以及一些服务参数，这些内容都由雾层进行保存。在服务过程中，雾层接收来自 WSN 层的传感数据以及安全状态信息，并进行服务参数的监测以及异常情况的分析和处理。雾层将在正常监测范围内的数据以及异常报告传送给 CSP。另外，为了实时监测 CSP 的信任状况，雾层会定期收集来

自声誉较好 SNSP 的推荐信任信息。雾层记录收集到的推荐信任信息和对 CSP 服务的实时监测信息，并综合这 2 个方面的因素对 CSP 的信任值进行实时更新。

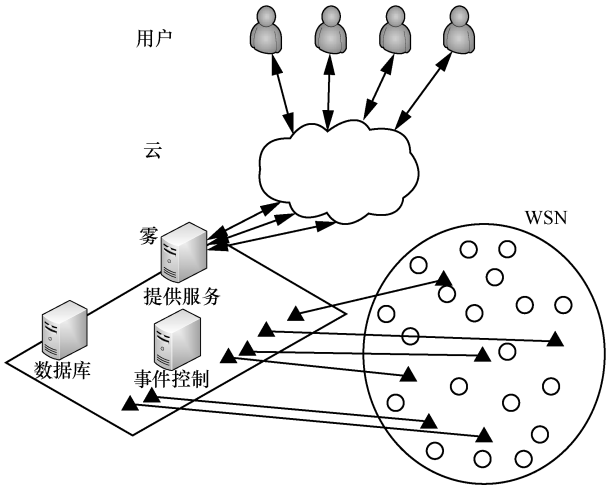


图 5　基于雾计算的传感云信任评价模型

3.3　实验设计

雾层可以很好地进行通信和服务参数的监测。这里，本文主要设计雾层对 WSN 网络信任状态的监测，实现降低不必要的资源消耗、延长网络寿命、保证网络通行能力、检测隐藏数据攻击、发现针对信任评价机制的攻击、恢复误判节点等目标。

雾层是云层和 WSN 层的中间层，其组成为一些功能较普通传感节点强的分布式设备（如移动式节点），这些设备形成独有的雾层网络结构。这些设备主要完成传感数据的暂时性备份、WSN 的网络信任状态监测、向云端提供服务等功能。具体来说，一部分监测类型的设备 $Device_{\text{monitor}}^{\text{collection}}$ 分散在监测区域的不同地方，直接从节点获取信任列表、路由表、推荐信任列表、网络拓扑等信息或执行雾层下达的恶意节点隔离等一些命令操作，减少信息在 WSN 中传播所造成的资源消耗。另一部分监测类型设备 $Device_{\text{monitor}}^{\text{collection}}$ 则安放在某一区域，通过从 $Device_{\text{monitor}}^{\text{collection}}$ 获取的信息建立 WSN 的全局信任状态。另外，用于传感数据暂时性备份的存储设备则位于传统汇聚节点的位置，这些设备可以向云端传送传感数据 $Device_{\text{storage}}^{\text{upload}}$、进行短时间内传感数据的存储 $Device_{\text{storage}}^{\text{temporal}}$、对这些传感数据进行分析处理 $Device_{\text{storage}}^{\text{analysis}}$ 等任务。

实验环境及相关参数设置如表 4 所示。

表 4　　实验环境及相关参数设置

参数	值
实验环境	Matlab R2016B
网络协议	阶梯扩散算法
WSN	3 层（外层节点数增大）
簇内节点	60 个
簇数量	6 个
雾层分布式设备	（30+24）个

针对 WSN 层，本文采用了分层信任评价机制。3 层机制分别为节点间基本信任层、节点间异常情况处理层和网络整体安全层。

3 层机制具体的设计方案如下所示。

1) 在节点间基本信任层，节点在通信或周期检测过程中进行相邻节点间信任值的更新。在实验中，本文设定 3 个观测值，分别为数据分组丢失率、路由失败率和转发时延。式(18)为直接信任更新。

$$T_{\text{D}} = \left(w_1 T_{\text{packet}} + w_2 T_{\text{history}}\right) \times Delay_{\text{forwarding}} \quad (18)$$

其中，T_{packet} 为数据分组信任值；T_{history} 为历史信任值；$Delay_{\text{forwarding}}$ 为转发时延，值为 0 或 1；w_1 和 w_2 为权重因子，且 $w_1+w_2=1$。

另外，w_2 是与时间相关的权重因子，如式(19)所示。

$$w_2 = real_1 \times Period \times \exp(-real_2 \times Period) \quad (19)$$

其中，$real_1$ 和 $real_2$ 为 2 个可变实数；$Period$ 为距离上一次节点信任更新的周期数。

在一个检测周期内，节点计算开销为对其他节点的信任更新 C_{update} 和权重值的计算 C_{weight}；节点的通信开销为与相邻节点的周期检测开销；节点的存储开销为信任值列表、监测数据、权重值和其他参数。若节点间 1 跳线路数为 n，邻节点数为 L，则其在一个周期检测内的通信开销小于 n（节点正常通信过程进行观测值监测和信任更新），计算开销小于 $C_{\text{indirect}}=n(C_{\text{update}}+C_{\text{weight}})$，存储开销为常数级 $O(L)$。

2)在节点异常情况处理层，当节点对其某一相邻节点的观测值（数据分组丢失率、路由失败率、转发时延、新旧信任值差值等）处于异常范围时，节点会将这一信息通过 AC（异常情况）数据分组传递给其他相邻节点，这些相邻节点将自身对异常节点的信任值回复给发送者。同时，节点也将这些推荐信息告知 $Device_{\text{monitor}}^{\text{collection}}$。$Device_{\text{monitor}}^{\text{collection}}$ 将信息发送给 $Device_{\text{monitor}}^{\text{compute}}$ 并请求异常情况判断。当

$Device_{\text{monitor}}^{\text{compute}}$ 确定异常节点确实是恶意节点时，$Device_{\text{monitor}}^{\text{collection}}$ 会在该区域内进行异常节点的隔离。当该异常为误判时，$Device_{\text{monitor}}^{\text{compute}}$ 会通知 $Device_{\text{monitor}}^{\text{collection}}$ 进行异常状态解除，保证网络性能不变。推荐信任计算如式(20)所示。

$$T_{\mathrm{R}(j,k)}=\sum_{i\in set(neighbor)} w_i \times T_{\mathrm{D}(i,k)} \tag{20}$$

其中，*set*(*neighbor*)中的节点与 *j* 节点和 *k* 节点均相邻且为 *j* 节点的信任节点；$T_{\mathrm{D}(i,k)}$为 *i* 节点对 *k* 节点的直接信任值；w_i 为 *i* 节点的权重值。

权重值的计算如式(21)所示。

$$w_i=\frac{i}{\sum_{i=1}^{n} i}=2\frac{i}{n(n+1)} \tag{21}$$

其中，*n* 为对 *set*(*neighbor*)中所有节点信任值排序后 *i* 节点所处队列的位置。

综合信任计算如式(22)所示。

$$T_{\text{synthesis}}=w_3\times T_D+\mathrm{w}_4\times T_R \tag{22}$$

其中，w_3 和 w_4 为权重值，且 $w_3+w_4=1$。

若没有异常情况发生，则没有计算和通信方面的开销。若出现异常情况，其计算开销为 $C_{\text{abnormal}}=C_{\text{recommend}}+C_{\text{weight}}+C_{\text{synthesis}}$；通信开销为获取推荐信任值和向雾层发送异常状态信息，为常数级 $O(L)$；存储开销为权重值的存储、排序的信任列表和其他参数。

3) 在网络整体安全层，$Device_{\text{monitor}}^{\text{compute}}$ 根据节点信任列表、拓扑结构和历史传感数据进行网络全局信任信息更新。当 $Device_{\text{monitor}}^{\text{compute}}$ 接收到 AC 数据分组时，也会根据网络拓扑状态、信任表、推荐信任表和历史传感数据进行节点异常状态的判定。另外，一些节点处于同一区域，执行相同或相似的功能，那么这些节点的传感数据存在一定的相关性。$Device_{\text{monitor}}^{\text{compute}}$ 会根据这些传感数据对节点进行周期性检测，查看网络是否存在隐藏恶意节点攻击。其中，针对同一区域同一观测值这类数据相关，其恶意节点检测如式(23)所示。

$$Array_i=\begin{cases} Count_{\text{crest}}\cup degree & \dfrac{(X_{2i}-X_{1i})}{(Y_{2i}-Y_{1i})}>0 \\ Count_{\text{trough}}\cup degree & \dfrac{(X_{2i}-X_{1i})}{(Y_{2i}-Y_{1i})}<0 \end{cases} \tag{23}$$

其中，$Array_i$ 记录某一时刻是否存在波峰/波谷；$\dfrac{Count_{\text{crest}}}{Count_{\text{trough}}}$ 保存数值的增减度 *degree*；$\dfrac{Y}{X}$ 为 $\dfrac{\text{数据}}{\text{时间}}$。

在云层，本文从 3 个方面建立 CSP 对 SNSP 的信任关系，分别为 WSN 网络状态信息信任、服务监测信任和推荐信任。根据一些 CSP 在雾层的历史信息来获得 CSP 的可信度，然后通过 CSP 可信度对其推荐信任进行计算。就 SNSP 对 CSP 的信任关系建立，也需要通过雾层进行。一方面是对 CSP 服务参数的监测，另一方面是可信 SNSP 的信任推荐。在可信 SNSP 的寻找方面，也需要通过雾层的 SNSP 服务记录来分析获取。

3.4 实验分析

3.4.1 WSN 层信任状态的监测

在信任评价机制的建立过程中，通信开销是一个重要的方面。因此，本文将增强的多属性信任协议（EMATP, enhanced multi-attribute trust protocol）[60]、轻量可靠的信任系统（LDTS, lightweight and dependable trust system）[52]、分层信任管理协议（HTMP, hierarchical trust management protocol）[72]和基于雾计算的分层信任机制（FHTM, fog-based hierarchical trust mechanism）几种方案的通信开销做了对比实验，记录一个簇内节点进行信任更新所需要的网络通信开销。在簇内，节点彼此邻接，在不同节点数目情况下，各个方案的通信开销如图 6 所示。EMATP 的通信开销在直接信任、推荐信任检测和簇头信任更新 3 个方面。随着邻接节点数量的增加，其在推荐信任检测方面的开销很大。HTMP 的通信开销在直接信任、推荐信任、簇头信任更新和簇头之间信任更新 4 个方面。在实验中，本文没有计算簇头之间信任计算的开销。LDTS 的通信开销为直接信任、簇头信任更新、簇头之间直接信任和基站信任更新 4 个方面。在实验中，本文没有计算基站的通信开销和多簇头情况。FHTM 的通信开销为直接信任、异常触发的推荐信任和雾层信任更新 3 个方面。

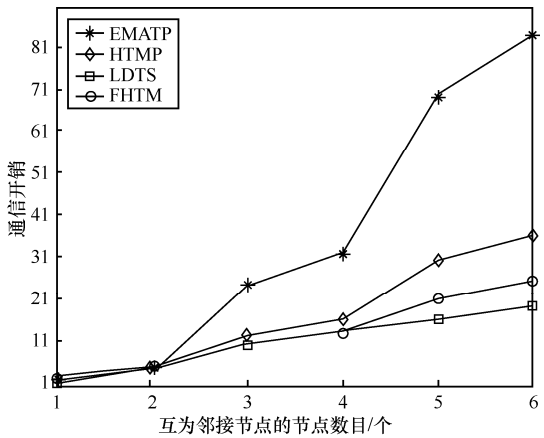


图 6 不同数目邻接节点的通信开销

由图 6 可知，本文方案比 EMATP 和 HTMP 的通信开销要少。由于 LDTS 没有节点推荐信任这一环节，节点通过簇头获取推荐信任信息，所以其通信开销较其他方案更少。由于其没有节点间的推荐信任，因此在应对异常情况方面，LDTS 比其他方案稍弱而且其簇头节点在存储、计算、通信方面的开销相对较大。

本文在3种不同攻击类型场景下测试了几种方案的恶意节点检测速度，如图 7 所示。对于共谋攻击，HTMP 和 LDTS 在这方面做得不太好，EMATP 将这种攻击的检测放在了节点之间（基于恶意节点推荐不一致性），本文方案 FHTM 则将其放在了雾层（基于拓扑结构、节点信任列表和历史传感数据），这 2 种方案所花费的时间差别不大。同样地，HTMP 和 LDTS 对伪造数据攻击的检测和确认也不太擅长，EMATP 的检测和确认所花时间较少（簇内完成），本文方案 FHTM 应对伪造数据攻击所花费时间较多（需要雾层的确认）。对于可以通过节点行为来进行检测的攻击类型，HTMP 花费的时间最少，EMATP 和 FHTM 需要进行多种攻击类型的检测和确认，花费的时间较长，但在可容忍范围之内。

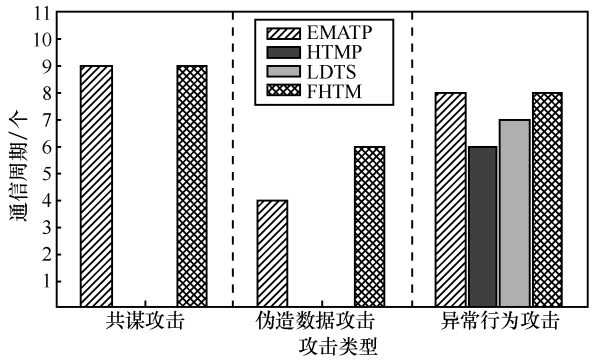


图 7　恶意节点的检测和确认

针对隐藏数据攻击检测和误判节点恢复问题，本文也做了一些仿真实验，如图 8 所示。图中的#符号表示节点所处环境发生了较大变化，节点的行为出现了较大异动；&符号表示此处出现了隐藏数据攻击节点，但是节点的行为表现正常；%符号表示一般内部攻击方式产生，节点出现了异常行为。每隔 20 个周期，设定对网络恶意节点进行一次清理。对于隐藏数据攻击节点检测和误判节点恢复问题，会存在一定的时延问题。这个时延的产生原因是：需要对节点最近一段时间内的传感数据进行特征的提取、对比和分析。

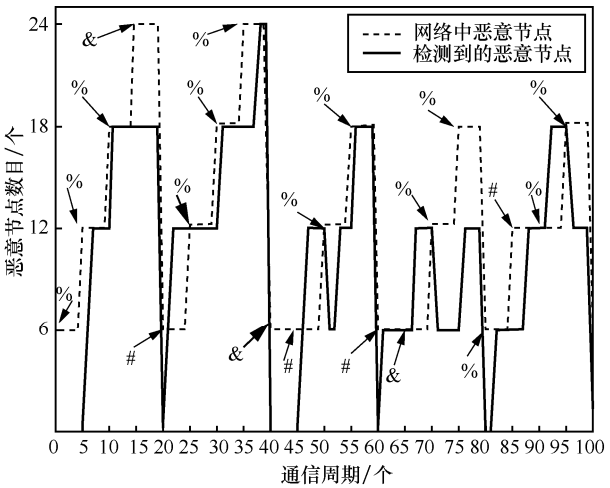


图 8　隐藏数据攻击和误判节点恢复

3.4.2　CSP 和 SNSP 之间信任的建立

就 SNSP 对 CSP 的信任问题，对服务参数的监测在雾层进行。在这里，本文主要设计如何通过服务记录获得可信的 SNSP。表 5 是 SNSP 的一些服务记录信息。

表 5 中有 7 个指标，其中，SNSP 服务记录是指 SNSP 在使用服务过程中所出现异常情况的次

表 5　雾层 SNSP 的信息记录

大雾层	SNSP 服务记录	SNSP 需求服务种类	交往过的 CSP	交往过的 SNSP	突变风险	认可次数/推荐次数	入驻时间/月
$SNSP_1$	1 异常 8 正常	可靠性、安全性	CSP_1/CSP_2/CSP_3	$SNSP_1$/$SNSP_2$/$SNSP_3$/$SNSP_4$	0.1	56/58	10
$SNSP_2$	0 异常 8 正常	可靠性、安全性、带宽	CSP_2/CSP_3	$SNSP_1$/$SNSP_3$/$SNSP_5$	0.5	46/60	8
$SNSP_3$	0 异常 10 正常	可靠性、安全性、兼容性	CSP_1/CSP_4/CSP_5	$SNSP_1$/$SNSP_2$/$SNSP_3$/$SNSP_4$/$SNSP_5$	0.1	88/52	15
$SNSP_4$	1 异常 1 正常	可靠性、安全性、高性能	CSP_2	$SNSP_1$/$SNSP_2$/$SNSP_4$/$SNSP_5$	0.2	26/29	4
$SNSP_5$	0 异常 1 正常	可靠性、安全性、平台资源	CSP_1	$SNSP_3$/$SNSP_4$/$SNSP_5$	0.1	32/33	1

数；SNSP需求服务种类指的是SNSP对CSP的一些具体性能要求；交往过的CSP是指它接收过哪些CSP的服务；交往过的SNSP是指它为哪些SNSP提供过推荐信任服务；突变风险指的是选择该SNSP的推荐信任值可能承担的风险；认可次数/推荐次数是指该SNSP的推荐信任值是否对需求者有用；入驻时间是指该SNSP使用雾服务平台的时间。

推荐信任的计算分为2个部分，其一是一般推荐信任计算（通过权值综合考虑所有使用过该CSP服务的SNSP评价），其二是专项推荐信任计算（查找所有与需求服务相似或相同的SNSP，然后对这些SNSP的评价进行综合考虑）。CSP的排除原则是一般推荐信任计算值与专项信任推荐计算值差值较大的、风险代价较大的、入驻时间较短的、不良记录高的。

就CSP选择SNSP来说，其信任评价分为3类：WSN网络状态信息信任、服务监测信任和推荐信任。在雾层，可以进行WSN网络状态信息和服务信息的监测，推荐信任的计算类似于前面所提到的推荐信任方式。

4 未来研究方向

4.1 不同传感云平台之间的信任

就目前的研究进展来看，传感云信任评价机制的研究还处于初级阶段。从传感云的发展模式来说，有2种趋势。1) 数据与服务是分开的，即CSP可接收多个SNSP提供的传感数据服务，然后对这些传感数据进行处理、分析和加工，最后为用户提供服务，这种模式下只需考虑传感云平台内的信任评价机制。2) 数据与服务一体，即SNSP拥有数据的绝对控制权，其兼顾CSP的职责，SNSP可以从其他SNSP处获取数据，然后为用户提供服务，这种情况下就需要考虑平台间的信任关系。第二种情况的是未来的一个研究方向。

4.2 基于雾计算的信任评价模型

雾计算具有几个明显的特征：低时延、位置感知、广泛的地理分布、适应移动性的应用、支持更多的边缘节点[73-74]。将雾计算引入信任评价机制，能更好地应对WSN拓扑结构的改变。当节点被俘获或失效时，雾计算能够及时发现并做出适当决策，防止恶意节点对网络的破坏或降低失效节点所造成的不必要的网络能耗。在未来，雾层可以建立成一个具有公信力的第三方平台，保证数据来源的安全可靠，在管理无线传感器网络、桥接云计算、成为可信第三方等方面都具有一定的优势。

4.3 传感云中信任评价机制的未来研究

在传感云模型方面，信任评价机制未来研究内容应该更多地基于全局数据分析挖掘。传感云模型的提出是为了提高WSN资源、数据的利用率和共享率，那么我们需要将复杂的信任评价数据运算、消耗更多网络资源的信任评价机制移出WSN，在WSN之外进行。在传感器网络等底层结构中，应关注恶意节点行为的监测，而在底层结构之外则应更多地关注恶意节点的检测、确认、处理、挖掘和预防。在未来研究中，信任评价机制应该是基于可信平台的。在平台上，可以获取更多的信息，拥有更好的计算、存储等资源。特别地，随着传感云日益壮大，不可避免地要考虑跨域（不同传感云或第三方雾计算平台）信任评价机制。跨域信任评价机制更多地基于推荐信任，更关注推荐者的可信程度。一般来说，推荐者评价具有随意性、夸大性、局限性、以偏概全等问题。这些问题的解决方案可分为2个阶段：第一阶段为可信第三方收集用户使用服务的记录，排除不良用户的推荐资格，针对不同的服务需求提供专项的信任推荐；第二阶段为用户评价行为的规范化、具体化，各个平台服务情况差异对比标准化。

4.4 对不可信事件的处理措施

传统的信任机制对不可信事件的处理措施是隔离或放弃。如在WSN层中，某些节点可能因为一些自身原因产生了异常数据，有些信任评价机制会将该节点直接抛弃，这势必会造成资源的浪费。在选择CSP时，也不能因为仅仅一次的不信任事件导致对该CSP的永久性不信任。当然一些研究者也提出了信任恢复措施，但同时也为恶意节点的信任恢复提供了机会。在处理不可信源方面的研究还很少，需要一种机制进行信任分类以及信任恢复。

4.5 传统安全机制与信任评价机制的权衡

在安全领域，信任评价机制与传统安全机制相辅相成。攻击者可以通过外部攻击获取权限，以合法的身份对网络进行破坏。信任评价机制可以检测恶意实体，对恶意实体进行信任评价，并联结其他可信实体抵制信任值低的实体。但是信任评价机制并不能有效防止外部攻击。在某些方面，需要统筹部署传统安全机制和信任评价机制以达到合理应用的目的。

4.6　信任存储

在信任评价机制中，信任值的存储是一个重要的部分。在很多信任评价机制中，研究重点在于信任评价机制算法的设计，而对信任值的安全保护和存储方面并未给予太多的研究。如在 WSN 中，信任值直接存储在节点的存储区域并没有进行加密等处理措施，信息容易被篡改；CSP、SNSP 和用户之间的信任数据库更容易受到恶意攻击等。在很多情况下，我们需要强化信任数据的安全存储措施。

4.7　信任评价机制标准的建立

在对信任评价机制的研究过程中，本文发现信任评价机制的种类繁多，缺乏一种统一的标准来促进该机制的长久发展。另外，在用户选择或自己设计符合自身情况的信任评价机制时，缺少相应的参考标准来辅助设计，这也是信任评价机制发展道路上的一个障碍。因此，在信任评价机制的研究中，需要设定一定的门类来区别不同的机制，并设定一些衡量参数来显示该机制的适用范围、能耗、性能、配置需求等。

5　结束语

WSN 的广泛应用和云计算的快速发展促进了传感云技术的产生。传感云继承了 WSN 和云计算的很多优点，但也面临着更多的安全问题。在安全领域的研究方法中，信任评价机制已是一个热点领域。信任评价机制可以很好地应对内部攻击，在提高服务质量和辅助决策方面也有很大的优势，可以应用在安全定位、高效传输、数据保护等领域。在传感云中，WSN 和云计算中信任评价机制的研究已有一定规模，但是在用户、CSP 和 SNSP 实体间的信任评价机制还有待提高。本文总结了传感云信任评价机制在最近几年的发展状况，详细介绍了传感云结构中实体间以及实体内的信任评价机制，并对现有的信任评价机制进行了分类和对比，探讨了其未来的研究方向。基于对传感云信任评价机制的研究，提出了一种基于雾计算模式的信任评价模型。通过仿真实验，证明该模式可以保证传感云底层结构的安全、可信。而且，雾计算可以设计成可信第三方平台，作为 SNSP 和 CSP 之间信任的桥梁。

参考文献：

[1] CHATTERJEE S, LADIA R, MISRA S. Dynamic optimal pricing for heterogeneous service-oriented architecture of sensor-cloud infrastructure[J]. IEEE Transactions on Services Computing, 2017, 10(2): 203-216.

[2] 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.

[3] 曾建电, 王田, 贾维嘉,等. 传感云研究综述[J]. 计算机研究与发展, 2017, 54(5):925-939.
ZENG J D, WANG T, JIA W J, et al. A survey on sensor-cloud[J]. Journal of Computer Research and Development, 2017, 54(5): 925-939.

[4] MADRIA S K. Sensor cloud: a cloud of sensor networks[C]//2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). 2017: 2660-2661.

[5] ALAMRI A, ANSARI W S, HASSAN M M, et al. A survey on sensor-cloud: architecture, applications, and approaches[J]. International Journal of Distributed Sensor Networks, 2013(6):18.

[6] RASHID B, REHMANI M H. Applications of wireless sensor networks for urban areas: a survey[J]. Journal of Network and Computer Applications, 2016, 60: 192-219.

[7] RAWAT P, SINGH K D, CHAOUCHI H, et al. Wireless sensor networks: a survey on recent developments and potential synergies[J]. The Journal of Supercomputing, 2014, 68(1):1-48.

[8] RITTINGHOUSE J W, RANSOME J F. Cloud computing: implementation, management, and security[M]. CRC Press, 2016.

[9] COUTINHO E F, SOUSA F R D C, REGO P A L, et al. Elasticity in cloud computing: a survey[J]. Annals of Telecommunications - Annales Des Télécommunications, 2015, 70(7-8):289-309.

[10] YURIYAMA M, KUSHIDA T. Sensor-cloud infrastructure - physical sensor management with virtualized sensors on cloud computing[C]// International Conference on Network-Based Information Systems. 2010:1-8.

[11] BOSE S, GUPTA A, ADHIKARY S, et al. Towards a sensor-cloud infrastructure with sensor virtualization[C]//IEEE International Conference on Cyber Security and Cloud Computing. 2015:25-30.

[12] HUH E N, ABAWAJY J. Emerging sensor-cloud technology for pervasive services and applications[J]. International Journal of Distributed Sensor Networks, 2016, 2014(1):1-3.

[13] MEHVAR R, ZHANG X. Optimal gateway selection in sensor-cloud framework for health monitoring[J]. IET Wireless Sensor Systems, 2013, 4(2):61-68.

[14] CHATTERJEE S, MISRA S. Target tracking using sensor-cloud: Sensor-target mapping in presence of overlapping coverage[J]. IEEE Communications Letters, 2014, 18(8): 1435-1438.

[15] MISRA S, SINGH A, CHATTERJEE S, et al. Mils-cloud: a sensor-cloud-based architecture for the integration of military tri-services operations and decision making[J]. IEEE Systems Journal, 2016, 10(2): 628-636.

[16] BHUIYAN M Z A, WANG G, 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.

[17] TSO R, ALELAIWI A, RAHMAN S M M, et al. Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud[J]. Journal of Signal Processing Systems, 2016:1-9.

[18] LIU J, SHEN S, YUE G, et al. A stochastic evolutionary coalition game model of secure and dependable virtual service in Sen-

sor-Cloud[J]. Applied Soft Computing Journal, 2015, 30(C):123-135.

[19] SEN A, MADRIA S. A risk assessment framework for wireless sensor networks in a sensor cloud[C]//2015 16th IEEE International Conference on Mobile Data Management (MDM). 2015: 38-41.

[20] GRANJAL J, MONTEIRO E, SILVA J S. Security in the integration of low-power wireless sensor networks with the internet: a survey[J]. Ad Hoc Networks, 2015, 24:264-287.

[21] JIANG J, HAN G, ZHU C, et al. A trust cloud model for underwater wireless sensor networks[J]. IEEE Communications Magazine, 2017, 55(3):110-116.

[22] HAN G, JIANG J, SHU L, et al. Management and applications of trust in wireless sensor networks: a survey[J]. Journal of Computer & System Sciences, 2014, 80(3):602-617.

[23] HU Y, WU Y, WANG H. Detection of insider selective forwarding attack based on monitor node and trust mechanism in WSN[J]. Wireless Sensor Network, 2014, 06(11):237-248.

[24] AHMED A, BAKAR K A, CHANNA M I, et al. A trust aware routing protocol for energy constrained wireless sensor network[J]. Telecommunication Systems, 2016, 61(1): 123-140.

[25] XIANG M, LIU W, BAI Q, et al. The double-edged sword: revealing the critical role of structural hole in forming trust for securing Wireless sensor networks[C]//2015 International Telecommunication Networks and Applications Conference (ITNAC). 2015: 286-291.

[26] 王国军, 王田, 贾维嘉. 无线传感器网络中一种基于行进启发的地理位置路由[J]. 传感技术学报, 2007, 20(2):382-386.
WANG G J, WANG T, JIA W J. March inspired geographic routing protocol in wireless sensor networks[J]. Chinese Journal of Sensors and Actuators, 2007, 20(2):382-386.

[27] AHMED A, BAKAR K A, CHANNA M I, et al. A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks[J]. Frontiers of Computer Science, 2015, 9(2):280-296.

[28] MACHHI S, JETHAVA G B. Feedback based trust management for cloud environment[C]// International Conference on Information and Communication Technology for Competitive Strategies. 2016:114.

[29] YAN Z, ZHANG P, VASILAKOS A V. A survey on trust management for Internet of things[J]. Journal of Network & Computer Applications, 2014, 42(3):120-134.

[30] ISHMANOV F, MALIK A S, KIM S W, et al. Trust management system in wireless sensor networks: design considerations and research challenges[J]. Transactions on Emerging Telecommunications Technologies, 2015, 26(2): 107-130.

[31] MANUEL P. A trust model of cloud computing based on quality of Service[J]. Annals of Operations Research, 2015, 233(1): 281-292.

[32] GOVINDAN K, MOHAPATRA P. Trust computations and trust dynamics in mobile adhoc networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2012, 14(2):279-298.

[33] WU J, CHEN L, YU Q, et al. Trust-aware media recommendation in heterogeneous social networks[J]. World Wide Web, 2015, 18(1): 139-157.

[34] WANG T, LI Y, CHEN Y, et al. Fog-based evaluation approach for trustworthy communication in sensor-cloud system[J]. IEEE Communications Letters, 2017, 21(11): 2532-2535.

[35] NOOR T H, SHENG Q Z, ZEADALLY S, et al. Trust management of services in cloud environments: obstacles and solutions[J]. ACM Computing Surveys, 2013, 46(1):1-30.

[36] SIDHU J, SINGH S. Improved TOPSIS method based trust evaluation framework for determining trustworthiness of cloud service providers[J]. Journal of Grid Computing, 2016:1-25.

[37] PEARSON S. Privacy, security and trust in cloud computing[M]// Privacy and Security for Cloud Computing. Springer London, 2013: 3-42.

[38] ZHU C, NICANFAR H, LEUNG V C M, et al. An authenticated trust and reputation calculation and management system for cloud and sensor networks integration[J]. IEEE Transactions on Information Forensics & Security, 2014, 10(1):118-131.

[39] MANUEL P. A trust model of cloud computing based on quality of service[J]. Annals of Operations Research, 2015, 233(1):281-292.

[40] WANG S, SUN L, SUN Q, et al. Reputation measurement of cloud services based on unstable feedback ratings[J]. International Journal of Web & Grid Services, 2015, 11(4):362-376.

[41] MAO C, LIN R, XU C, et al. Towards a trust prediction framework for cloud services based on PSO-driven neural network[J]. IEEE Access, 2017, 5: 2187-2199.

[42] LIN G, WANG D, BIE Y, et al. MTBAC: a mutual trust based access control model in cloud computing[J]. China Communications, 2014, 11(4): 154-162.

[43] HOSSEINI S B, SHOJAEE A, AGHELI N. A new method for evaluating cloud computing user behavior trust[C]// Information and Knowledge Technology. 2015:1-6.

[44] LIU Z, PENG D. User behavior identification for trust management in pervasive computing systems[C]//IEEE International Workshop on Future Trends of Distributed Computing Systems. 2007:65-72.

[45] JING X, LIU Z, LI S, et al. A cloud-user behavior assessment based dynamic access control model[J]. International Journal of System Assurance Engineering & Management, 2015:1-10.

[46] SAVAS O, JIN G, DENG J. Trust management in cloud-integrated wireless sensor networks[C]//International Conference on Collaboration Technologies and Systems. 2013:334-341.

[47] QIN D, YANG S, JIA S, et al. Research on trust sensing based secure routing mechanism for wireless sensor network[J]. IEEE Access, 2017.

[48] JIANG J, HAN G, WANG F, et al. An efficient distributed trust model for wireless sensor networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(5): 1228-1237.

[49] DUAN J, GAO D, YANG D, et al. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications[J]. IEEE Internet of Things Journal, 2014, 1(1): 58-69.

[50] FANG W, ZHANG W, YANG Y, et al. A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution[J]. Science China, 2017, 60(4):040305.

[51] LIU Y, DONG M, OTA K, et al. ActiveTrust: secure and trustable routing in wireless sensor networks[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(9): 2013-2027.

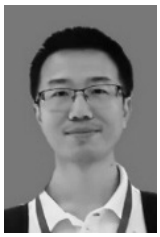
[52] LI X, ZHOU F, DU J. LDTS: a lightweight and dependable trust system for clustered wireless sensor networks[J]. IEEE Transactions on Information Forensics & Security, 2013, 8(6):924-935.

[53] LABRAOUI N, GUEROUI M, SEKHRI L. A risk-aware reputation-based trust management in wireless sensor networks[J]. Wireless Personal Communications, 2016, 87(3): 1037-1055.

[54] REDDY V B, VENKATARAMAN S, NEGI A. Communication and data trust for wireless sensor networks using D-S theory[J]. IEEE Sensors Journal, 2017, 17(12): 3921-3929.

[55] CHATURVEDI P, DANIEL A K. Trust based node scheduling protocol for target coverage in wireless sensor networks[M]// Emerging Research in Computing, Information, Communication and Applications. 2015:197-205.
[56] CHEN Z, HE M, LIANG W, et al. Trust-aware and low energy consumption security topology protocol of wireless sensor network[J]. Journal of Sensors, 2015, 2015(1):1-10.
[57] AHMED A, BAKAR K A, CHANNA M I, et al. Energy-aware and secure routing with trust for disaster response wireless sensor network[J]. Peer-to-Peer Networking and Applications, 2017, 10(1): 216-237.
[58] GUO J, CHEN I R, TSAI J J P. A survey of trust computation models for service management in internet of things systems[J]. Computer Communications, 2016, 97:1-14.
[59] ANITA X, BHAGYAVENI M A, MANICKAM J M. Fuzzy-based trust prediction model for routing in WSN[J]. The Scientific World Journal, 2014, 2014(2):1-11.
[60] PRABHA V R, LATHA P. Enhanced multi-attribute trust protocol for malicious node detection in wireless sensor networks[J]. Sādhanā, 2017:1-9.
[61] MARZI H, LI M. An enhanced bio-inspired trust and reputation model for wireless sensor network[J]. Procedia Computer Science, 2013, 19:1159-1166.
[62] FENG R, CHE S, WANG X, et al. Trust management scheme based on D-S evidence theory for wireless sensor networks[J]. International Journal of Distributed Sensor Networks, 2013, 2013(4):130-142.
[63] GUPTA G P, MISRA M, GARG K. Energy and trust aware mobile agent migration protocol for data aggregation in wireless sensor networks[J]. Journal of Network & Computer Applications, 2014, 41(1):300-311.
[64] CHAE Y, DIPIPPO L C, SUN Y L. Trust management for defending on-off attacks[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(4): 1178-1191.
[65] SHEN S, HUANG L, FAN E, et al. Trust dynamics in WSN: an evolutionary game-theoretic approach[J]. Journal of Sensors, 2016, 2016:1-10.
[66] FANG W, ZHANG C, SHI Z, et al. BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks[J]. Journal of Network & Computer Applications, 2016, 59:88-94.
[67] REN Y, ZADOROZHNY V I, OLESHCHUK V A, et al. A novel approach to trust management in unattended wireless sensor networks[J]. IEEE Transactions on Mobile Computing, 2014, 13(7): 1409-1423.
[68] BONOMI F, MILITO R, ZHU J, et al. Fog computing and its role in the internet of things[C]// Edition of the Mcc Workshop on Mobile Cloud Computing. 2012:13-16.
[69] 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.
[70] WANG T, ZENG J, 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.
[71] VAQUERO L M, RODERO M L. Finding your way in the fog: towards a comprehensive definition of fog computing[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(5): 27-32.
[72] BAO F, CHEN R, CHANG M J, et al. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection[J]. IEEE transactions on network and service management, 2012, 9(2): 169-183.
[73] HONG K, LILLETHUN D, RAMACHANDRAN U, et al. Mobile fog: a programming model for large-scale applications on the internet of things[C]//ACM SIGCOMM Workshop on Mobile Cloud Computing. 2013:15-20.
[74] BONOMI F, MILITO R, NATARAJAN P, et al. Fog computing: a platform for internet of things and analytics[M]// Big Data and Internet of Things: A Roadmap for Smart Environments. Springer International Publishing, 2014:169-186.

[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。

张广学（1992-），男，河南开封人，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。

蔡绍滨（1973-），男，辽宁辽中人，博士，华侨大学教授、博士生导师，主要研究方向为物联网、海洋监测网络、网络计算、信息安全等。

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。

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、物联网和云计算等。