软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(Suppl.(11)):71−81

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于边缘计算与信任值的可信数据收集方法*

邱 磊[1], 蒋文贤[1], 李玉泽[1], 於志勇[2,3], 马 樱[4], 王 田[1,4]

[1](华侨大学 计算机科学与技术学院,福建 厦门 361021)

[2](福州大学 数学与计算机科学学院,福建 福州 350108)

[3](福建省网络计算与智能信息处理重点实验室(福州大学),福建 福州 350108)

[4](数据挖掘与智能推荐福建省高校重点实验室(厦门理工学院),福建 厦门 361024)

通讯作者: 王田, E-mail: wangtian@hqu.edu.cn

摘 要: 物联网应用中,底层传感网所采集的数据是上层决策的基础和一切应用的根本.如果收集的数据本身就是有问题、不可信的,这将使得上层的数据保护和应用成为空中楼阁.为了解决数据不可信的问题,提出了基于移动边缘节点的可信数据收集方案.通过对节点的评估,将节点的信任值用于路径选择,采用移动边缘节点来充当移动元素,访问可信的簇头节点,从而实现高效的可信数据收集.对所提出的基于效用值的可信数据收集算法(UTDC)进行了理论分析和广泛的模拟实验.实验结果表明,所提出的基于效用值的可信数据收集算法可以很好地避开不可信的节点,有效降低了网络延迟,延长了网络的生命周期.

关键词: 信任值;可信数据收集;边缘计算;物联网;移动路径

中文引用格式: 邱磊,蒋文贤,李玉泽,於志勇,马樱,王田.基于边缘计算与信任值的可信数据收集方法.软件学报,2019,30(Suppl.(11)):71−81. http://www.jos.org.cn/1000-9825/19008.htm

英文引用格式: Qiu L, Jiang WX, Li YZ, Yu ZY, Ma Y, Wang T. Trustworthy data collection method based on edge computing and trust value. Ruan Jian Xue Bao/Journal of Software, 2019,30(Suppl.(11)):71−81 (in Chinese). http://www.jos.org.cn/1000-9825/19008.htm

Trustworthy Data Collection Method Based on Edge Computing and Trust Value

QIU Lei[1], JIANG Wen-Xian[1], LI Yu-Ze[1], YU Zhi-Yong[2,3], MA Ying[4], WANG Tian[1,4]

[1](College of Computer Science and Technology, Huaqiao University, Xiamen 361021, China)

[2](College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China)

[3](Fujian Provincial Key Laboratory of Networking Computing and Intelligent Information Processing (Fuzhou University), Fuzhou 350108, China)

[4](Key Laboratory of Data Mining and Intelligent Recommendation (Xiamen University of Technology), Xiamen 361024, China)

Abstract. In the internet of things application, the data collected by the underlying sensor network is the basis of the upper decision and the foundation of all applications. If the collected data itself is problematic and untrustworthy, this will make the upper level of data protection and application a castle in the air. In order to solve the problem of untrustworthy data, a trustworthy data collection scheme based on mobile edge nodes is proposed. Through the evaluation of the node, the trust value of the node is used for path selection, and the mobile edge node is used as a mobile element to access the trustworthy cluster head node, thereby achieving efficient and reliable data

* 基金项目: 数据挖掘与智能推荐福建省高校重点实验室开放基金(DM201902);福建省网络计算与智能信息处理重点实验室开放课题;福建省社会科学规划基金(FJ2018B038);福建省自然科学基金(2018J01092);华侨大学研究生科研创新基金(17014083012)

Foundation item: Open Fund of Key Laboratory of Data Mining and Intelligent Recommendation, Fujian Province University (DM201902); Open Foundation of Fujian Provincial Key Laboratory of Network Computing and Intelligent Information Processing; General Projects of Social Sciences in Fujian Province (FJ2018B038); Natural Science Foundation of Fujian Province of China (2018J01092); Subsidized Project for Postgraduates' Innovative Fund in Scientific Research of Huaqiao University (17014083012)

收稿时间: 2019-09-15; 采用时间: 2019-10-24

collection. Theoretical analysis and extensive simulation experiments are carried out on the proposed trustworthy data collection algorithm based on utility value (UTDC). The experimental results show that the proposed trustworthy data collection algorithm based on utility value can avoid untrustworthy nodes, effectively reduce network delay and prolong the life cycle of the network.

Key words. trust value; trustworthy data collection; edge computing; Internet of Things; movement path

随着大数据、云计算和物联网的广泛应用,作为继计算机、互联网和移动通信网络之后的第 3 波信息产业,物联网(IoT)已成为国家层面技术和产业创新的重点,而雾/边缘计算在物联网和云系统中发挥着不可替代的作用[1,2].物联网使用云处理边缘传感器网络生成的数据,并为上层用户提供服务.用户可以按需收集、处理、分析和存储数据,因此其应用领域多种多样[3].最常见的应用包括森林风险监测、入侵检测和车辆跟踪.在这些应用中,物联网边缘设备(如传感器)的基本工作是数据采集.边缘物联网设备收集传感数据并将其转发到基站(或发送到汇聚节点),数据最终被移交给上层物联网应用以进行决策[4,5].

在物联网服务计算系统的基础数据采集应用中,采用移动数据采集器(MDC)能够节省能量并延长网络生命周期[6].然而,在这个过程中,大多数研究只考虑能量和延迟问题[7].但是,由于物联网服务计算系统中的大多数传感器节点部署在恶劣的自然环境中,又极为有限,所以受噪声及恶意攻击等影响,导致传感器采集到无效甚至是误导性的数据,只有不到 49%的数据是有效的、可信的[8,9].一些常见的方法,如数据加密,只能应用于传感器节点的外部攻击,不适用于节点内部的攻击[10].

我们提出了一种基于效用的贪心启发式可信数据收集算法来进行可信数据的收集.采用了一系列的信任评估标准来评价物联网服务计算系统中的传感器节点,以此分别恶意节点.同时将信任值用于数据收集路径规划之中,通过综合考虑移动路径上的能量消耗和节点的数据信任度来生成一条可信度最高且能量消耗最少的移动路径.而针对普通移动数据收集器的限制问题,我们提出了采用边缘计算中的边缘节点来解决这个问题.最后给出仿真结果和对比分析.

本文第 1 节总结了现有的可信评估和数据收集的相关研究.第 2 节对所研究问题进行了具体描述.第 3 节给出方法的详细设计过程和算法分析.第 4 节在模拟环境下进行了实验,并与同类方法进行了对比.最后对全文进行了总结.

1 相关工作

物联网服务的快速发展和广泛应用产生了许多节点信任评估和新型移动元素收集数据的研究.Fan 等人提出了一个基于特定因子(CF)的直接信任模型和模糊的 C-means 方法的间接信任模型,通过信任信息收集和信任值计算两个过程来对节点进行信任评估[11].但是,此方案将直接信任和间接信任平均计算,在某些情况下的信任值并不可靠,同时增加了额外计算开销.Osama 等人提出了一种基于激活函数的可信邻居选择(AF-TNS)方法,利用具有能量约束的信任评估和基于附加度量的节点信任评估[12].但是,在信任评估方法中只包含直接信任,避开间接信任和推荐信任,同时节点评估指标仅有数据包和能量,这将导致可信评估的片面性和最终信任值的不可靠性.Gao 等人提出了一种 MADG(运动辅助数据收集)数据收集方案.在移动区域中设置缓冲器,数据沿着最短路径传输到缓冲器,然后由移动基站收集,以此解决基站周围节点或数据汇聚点能耗过大的问题[4].但是,移动元素的数据收集是无选择性的,没有考虑节点的可信性和恶意节点问题带来的能量和延迟问题.文献[13]在网络簇头和路由机制中引入了信任机制,通过评估节点的信任值,避免了低信任值节点参与网络数据转发.但是,数据只通过节点转发传输导致过多的能量消耗,也增加数据接收的延迟.Kumar 等人研究发现,传感器节点的能量不仅决定了网络的寿命,还对网络的连通性和覆盖范围产生不利影响,使用通用移动数据收集器收集数据延迟很高.因此作者提出了一种新的移动数据收集模型,该模型结合了基于聚类的巡回策略和基于无线通信的数据收集机制[14].但是,该模型的移动数据收集器需要访问所有节点,没有考虑节点面临的恶意攻击问题.

上述的相关研究是使用移动节点在物联网服务计算系统中收集传感数据的不同方面的改进.一些研究使用不同的移动收集方法来考虑能量空洞问题,一些方法通过在模型或路由中引入信任评估机制来抵抗数据转发中的攻击[15].但是,这些方法只考虑能量、延迟和攻击的一个或两个方面,同时数据的收集必须要访问所有的

节点.大多数物联网服务应用方法都没有在应对恶意攻击中全面考虑节点的信任评估问题,忽略了边缘节点最终获得数据的可用性问题.因此,我们提出一种基于节点信任值效用的可信数据收集方法.构建一个信任评估模型来评估节点的可信度,并使用可信度来生成可信的簇头节点,然后使用基于效用的启发式路径算法来为移动边缘节点生成最短路径,同时可以有效减少能量消耗和延迟,提高收集数据的可信度,从而延长网络的生命周期.

2 问题描述

节点的可信值指无线传感器网络中的节点对其周围节点的信任程度,而主体(评估节点)是否信任客体(被评估节点)主要取决于主体对客体的评估,且评估的信任值会随着网络的运行而不断更新[16].评估节点,获得节点的信任值.基于信任值构造可信簇头节点的最小生成树(MST),通过求解最小生成树问题,构造由可信簇头节点组成的最短路径,移动边缘节点通过该路径收集可信节点的数据.

为了简化计算,认为评估的节点是可信节点,则移动边缘从该节点收集的数据即为可信赖的数据.如图 1 所示,基于节点信任值的评价,生成可信的簇头节点[17].将移动边缘节点在簇头节点间的移动轨迹抽象为一个简单带权连通无向图 $G(V,E)$,顶点集 V 代表簇头节点集,边集 E 代表簇头节点间的移动路径,同时在每个簇内构建以簇头节点为根节点,簇内非簇头节点为子节点的子树.对于一个给定的带权连通无向图 G,图 G 的生成树是一棵连接所有簇头节点子图的树.

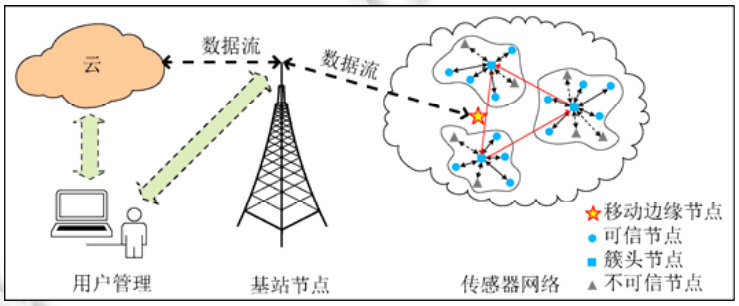

Fig.1 Edge-based IoT computing system data collection architecture

图 1 基于边缘节点的物联网计算系统数据收集架构

一棵最小带权生成树是一棵生成树 T 使得 $\sum_{(u,v)\in T} C(u,v)$ 最小.此处 $C(u,v)$是边(u,v)的移动代价(收益),定义为 u 和 v 两点之间的欧氏距离与将到达的下一个点(此处为 u 到 v,则下一个到达的顶点为 v)的信任值的比值,即文中的效用值.移动边缘通过一条确定的路径逐次访问每个簇头节点来遍历整个网络,在移动距离受限的条件下(如限制访问距离只为 500m),移动边缘节点通过规划的最短路径移动,按照效用值降序原则的顺序(从起点出发后,先访问效用值最大的节点,之后访问除了这两节点之外的效用值最大的节点,以此类推)访问效用最大的部分簇头节点来收集数据.最后,移动边缘节点将数据进行聚合,直接发往最近的基站节点.

3 算法步骤与分析

3.1 信任评估模型

在网络初始化阶段,我们设置节点的初始可信值(设置为 T_i)和节点的可信度阈值Δ.节点的信任值规则如下:

定义. 使用区间来表示节点的信任值范围.区间限制为(0,1),设置节点的初始信任值为 0.5.某一时刻的信任值表示为 T_c,当 T_c=0 时,表示节点完全不可信; T_c=1 表示该节点完全受信任.

对节点信任的度量从两个方面来计算:直接信任和间接信任.直接信任包括 3 个细粒度参数:节点的历史通信交互、节点能量剩余和丢包率.间接信任在直接信任的基础上,通过节点间的关系确定信任传递的路径计算信任值.

3.1.1 直接信任模型

(1) 节点通信交互

节点与邻居节点进行通信,用 S 表示成功交互的次数,C 表示交付的总次数.节点间的通信信任值 T_i 表示为

$$T_i = \omega_{oldi} \times T_{oldi} + \omega_{newi} \times T_{newi} \tag{1}$$

$$T_{newi} = S/C \tag{2}$$

$$\omega_{oldi}+\omega_{newi}=1,\text{且 } \omega_{oldi},\omega_{newi}\in[0,1] \tag{3}$$

ω_{oldi} 与 ω_{newi} 分别表示节点旧的通信信任权值和新通信权值,T_{newi} 和 T_{oldi} 分别表示新旧信任值,初始化阶段 $T_{oldi}=0$,ω_{oldi} 和 ω_{newi} 可根据应用环境调节.

(2) 能量剩余

在节点的信任评估中,节点的能量也是重要的评估指标,设节点初始能量为 E_i,剩余能量为 E_c.同时为每个物理节点设置一个阈值 E_m,当节点的剩余能量小于阈值时,能量信任值 T_e 为 0,否则节点的能量信任值 T_e 计算表示为

$$T_e = E_c/E_i \tag{4}$$

(3) 丢包率

发送的数据包数目为 P_S,接收到的数据包数目为 P_r,同时为物理节点设置数据包传送阈值 P_m,当节点接收的数据包数量小于阈值时,直接采用推荐来计算节点的信任值,同时丢包率信任值 T_P 置为初始值 0.5.丢包率相关的信任值 T_P 为

$$T_p = \frac{P_s - P_r}{P_s} \tag{5}$$

在可以得到直接信任的情况下,根据上述分量计算节点的直接信任值:

$$T_c = \omega_i \times T_i + \omega_e \times T_e + \omega_p \times T_p \tag{6}$$

T_C 表示为总的信任值,$\omega_i,\omega_e,\omega_p$ 分别表示通信交互信任、能量信任和丢包率的权重.

3.1.2 间接信任

节点不能与所有节点直接通信,部分节点要依靠其他节点与其交互的历史记录而得到间接信任值.同时由于恶意攻击问题和可能出现的节点间通信数据包数量过小的问题,只采用直接信任评价节点并不准确[12].因此,通过间接的推荐信任可以很好的提高传感器节点信任评价的准确度.由于每个节点的可信程度不同,如推荐节点可能为恶意节点,故需要对推荐节点赋予权值,权值定义为 $\partial\in(0,1)$.在间接信任评估前,需要统计评估节点和被评估节点间的公共邻居节点集.同时被评估节点也应对公共节点集中的节点的信任值进行判定,只有满足可信阈值的节点才能作为信息的传递节点.如图 2,要在节点 Y 处计算节点 X 的信任,则先要判定传递节点 A、B、C、D 的信任值,信任值小于阈值的节点(如节点 B)则不作为传递节点.

$$(T_{X,Y})_A = T_{X,A} \times T_{A,Y} \tag{7}$$

即为经节点 A 推荐后的节点 X 在节点 Y 处的信任值.推荐节点的权值与相邻节点的直接信任值成正比,则推荐节点 A 的权值定义为

$$\partial_A = \frac{T_{A,Y}}{\sum_{n=1}^{m} T_{A,n}} \tag{8}$$

其中 m 表示邻居节点的个数,$T_{A,Y}$ 表示节点 A 与节点 Y 的直接信任值,$\sum_{n=1}^{m} T_{(A,n)}$ 表示推荐节点的直接信任值的和.节点 Y 处得到的节点 X 的间接信任即为各推荐路径信任值的均值,公式为

$$T_{X,Y} = \frac{\sum_{n=1}^{m} \partial_k * (T_{X,Y})_k}{m} \tag{9}$$

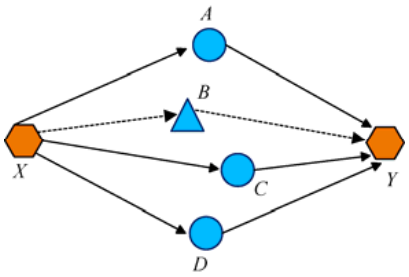

Fig.2 Indirect trust relationship

图 2 间接信任关系

3.1.3 节点的能量效率

在设计数据收集算法时,传感器的能量消耗是首要考虑的问题,而网络的生命周期定义为传感器中第 1 个节点能量耗尽失效所用的时间[18].在本研究中,我们对节点加入了信任的考察,所以用能量的效率来衡量节点的数据收集效用:

$$\beta=\frac{D\times T}{E_l-E_n} \tag{10}$$

其中 D 表示节点单次收集的数据量,T 表示节点当前的信任值,E_l 表示节点上次的能量,E_n 表示节点当前的能量,β 表示节点单位能量的数据可用效率.从公式(10)可以看出,通过提高节点的可信数据量 $D\times T$,就能提高节点的单位能量效率,从而降低节点的能量消耗.在路径规划中,将节点分成多个簇,在每个簇中选择簇头节点为收集节点.建立最短路径优化模型,求解最可信路径问题,使移动边缘节点在限定的移动距离内遍历最多的收集节点,收集效用最大的可信数据,同时能最大化网络的生命周期.

3.2 算法步骤

3.2.1 节点信任值评估算法

当节点 i 想要获取节点 j 的信任值时,节点 i 首先检查它记录邻居节点的列表,如果节点 j 在邻居节点列表中,则采用直接信任评价,否则采用间接信任评价.节点的信任值评估算法通过计算节点直接信任值得到节点的信任评估值.

首先,对于任意给定的稳定网络,我们的目标是计算出每个节点的信任值(包括簇头节点).主要方法是对节点的通信交互、能量剩余和丢包率等参数进行计算,同时结合权重获得区域节点的直接信任值.在计算中要先进行判断,看节点是否是自己的邻居节点,同时节点此次接收的数据包是否满足要求.满足上述条件的节点,计算直接信任值,否则计算间接信任值.

算法 1 主要分为两步:首先是计算直接信任值 $T_{X,Y}$(节点 X 与邻居节点 Y 间的信任值),其次是在 $T_{X,Y}$ 的基础上根据路由表中节点的关系,决定是采用直接信任值或利用间接信任关系求解间接信任值,最终得出节点信任值 T_c.对于不在自己邻居节点列表内的节点,或者是邻居节点但此次接收到的数据包数量 P_r 不满足要求,即 $P_r<P_m$ 时,我们需要通过间接信任来计算节点的可信度.

算法 1. 节点信任值计算

输入:节点成功交互次数 S;节点交互总次数 C;节点初始能量 E_i;节点剩余能量为 E_c;发送数据包数目 P_S;接收数据包数目 P_r;通信交互信任权重 ω_i;间接信任权重 $\omega_{X,Y}$;能量信任权重 ω_e;丢包率权重 ω_P

输出:节点的信任值 $\boldsymbol{T_c}$

1: **for** each node in cluster **do**

2: **if** 邻居节点可以通信

3: 计算 $T_{newi}=S/C$;且 $\omega_{oldi}+\omega_{newi}=1$;

4: 计算 $T_i=\omega_{oldi}\times T_{oldi}+\omega_{newi}\times T_{newi}$;

5: 计算 $T_p=\frac{P_s-\mathrm{P_r}}{P_s}$;

6: 计算 $T_e=E_c/E_i$;

7: 计算 $T_c=\omega_i\times T_{i+}\omega_e\times T_e+\omega_p\times T_p$//直接信任值

8: **else**

9: 获取节点邻居节点个数 m

10: 计算 $\partial_A=\frac{T_{A,Y}}{\sum_{n=1}^{m}T_{A,n}}$, $\partial\in(0,1)$//推荐权值

11: 计算 $T_{X,Y}=\frac{\sum_{n=1}^{m}\partial_k*(T_{X,Y})_k}{m}$

12: $T_c=\omega_i\times T_{i+}\omega_e\times T_e+\omega_p\times T_p$//加入间接信任的节点信任值

13: **end if**

14: **end for**

3.2.2 基于效用值的路径选择算法

本节基于前面对节点的信任评价,对移动路径的选择提出基于效用的路径选择算法(UTDC).目标是找到一段时间中网络中信任效用较大的簇头节点集,由此节点集连线构成移动边缘节点的数据收集路径,如图 3 所示.

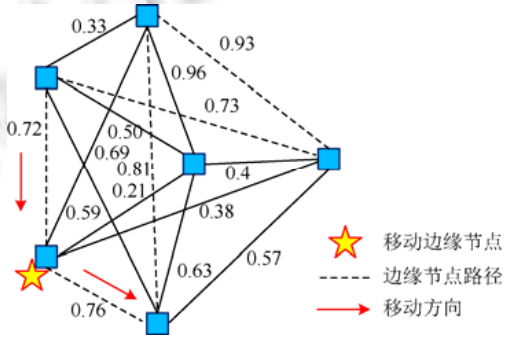

Fig.3 Moving edge node maximum utility value path

图 3 移动边缘节点最大效用值路径

簇头节点间的信任效用值定义为 u 和 v 两点之间的欧氏距离与到达的下一个点(此处为 u 到 v,则下一个到达的顶点为 v)的信任值的比值,在数据收集的有限移动距离内,可以经过可信度最高的节点区域,达到一次移动收集最多可信数据的目标.算法选择效用值最大的节点作为下一个移动目标节点,并要求移动边缘节点的移动路径长度不超过 L_m.在延迟要求(即距离限制)下,移动边缘节点访问具有最高效用值的部分簇头节点.基于信任值效用的启发式贪婪算法进行比较和选择,最后,输出满足数据收集时间限制要求和信任值效用值的路径.

在有限的移动距离 L_m 内,访问最多的可信簇头节点,同时收集可信数据,即移动边缘节点移动效用的最大化.对于给定的树结构 $G(V,E)$,由根节点 B,簇头节点集 $V=\{v_i\}\subseteq S$ 构成.寻找一条路径 P,从某一源节点 A 出发,访问所有簇头节点,最后回到源节点.使得移动边缘节点的移动路径 P 的长度不超过限定的移动距离L_m,同时应该有 $P=\arg\min\sum_{S_j\in S}N(v_i,s_j)$;其中 $N(v_i,s_j)$为簇内非簇头节点 s_i 到其所属的簇头节点 v_i 的跳数.见算法 2.

算法 2. 基于效用的贪心启发式可信数据收集算法

输入:起始节点 B;关联节点集$\{A_1,A_2,\cdots,A_i,\cdots,A_{k-1},A_k\}$;初始路径长度 sum;限制路径长度 L_m;簇头节点集

$\{C_1,C_2,\cdots,C_i,\cdots,C_m\}$.
输出:路径队列中的簇头节点 *ID*;总的路径长度 *sum*
1: **for** 关联节点集$\{A_1,A_2,\ldots,A_i,\ldots,A_{k-1},A_k\}$中节点 **do**
2: 计算与起始节点 *B* 的欧氏距离 ρ 和信任值 T_C
3: Case1 计算 $U=\rho/T_c$;
4: 对两节点的信任效用 U_i 降序排列为 $S=\{S_n,S_{n-1},\ldots,S_i,\ldots,S_2,S_1\}$
5: Case2 **while** $i<1$ **do**
6: H = max$\{S_n,S_{n-1},\ldots,S_i,\ldots,S_2,S_1\}$
7: **if** $ID(H)=ID(B)$ **then**;
8: 移除集合 *S* 中最大的节点,定义为新的 *S* 集合 goto Case2;
9: **else**
10: 将节点 *H* 加入路径队列;
11: 计算 $sum=sum+l_h$;
12: **end if**
13: **end while**
14: **while** $sum<L_m$ **do**
15: **goto** Case1
16: **end while**
17: **end for**

定理. 设计一个移动节点在最短的移动距离内去访问所有的节点是 NP-hard 问题.

证明:在我们的场景中,节点集为 $S=\{S_1,S_2,\cdots,S_n\}$,移动节点的移动距离为 L_m,簇头节点集为 $V=\{V_1,V_2,\cdots,V_i\}$,有 $i<n$ 且 $V\subseteq S$.我们需要找到最多的簇头节点 $V_{s1},V_{s2},\ldots,V_{si}$ 使得 $V_c=(V_{s1}\cup V_{s2}\cup\ldots\cup V_{si})$同时 $L_{sum}\leqslant L_m$.如果有 $n=i$.则有 $V=V_c=S$.因此,所有节点都是簇头节点.移动边缘节点访问指定距离内的所有节点以收集数据并最终返回到起始点,这是一个旅行商问题(TSP).TSP 问题是组合优化问题,已被证明具有 NPC 计算复杂性.因此,这个最短路径问题也是 NP 难问题.证毕. □

算法时间复杂度分析:考虑所有节点都通过直接信任方法(算法 1)来计算节点的信任值,在最差的情况下,网络中的节点两两间可以通信,计算两两节点的信任值,时间复杂度为 $O(n^2)$.如果网络中所有的节点除了评估节点和被评估节点外,其他所有节点都在信任传递节点中,则此时算法 2 的时间复杂度为 $O(n^3)$.在计算出节点的信任值后,我们采用快速且稳定的归并排序算法,最坏情况下的时间复杂度为 $O(n\log n)$.所以,综合上面我们可以得到,我们整体算法的时间复杂度为 $O(n^3)$.

4 实 验

4.1 实验环境设置

实验采用 MATLAB R2018a 构建仿真平台,对所提出的可信数据收集算法进行性能评估和分析.仿真环境设定为在 300m×300m 的区域内随机部署 400 个节点,并且选取 100 个节点为簇头节点,假设移动边缘节点从选定的出发点开始匀速移动,并且移动速度和通信半径可调节.节点的最小能量阈值被设置为节点的初始能量的千分之一,并且最小分组接收阈值是节点数据生成的阈值的千分之二.

4.2 实验结果分析

为了更直观地展示能耗,使用不同的策略比较系统的总能耗,如图 4 所示.随着恶意节点数量的增加,仅考虑节点的可信值和考虑可信值与距离策略的能耗都增加了,然而后者增长更慢,比例远小于前者.仅考虑距离的策略的能耗基本稳定,仅考虑信任值并忽略移动边缘节点的下一个访问节点的距离,则将导致相当大的能量消耗.只考虑移动距离虽然能量消耗少,但最终收集的数据的可信度根本得不到保证.结合我们之前的实验,可以看出,在移动数据采集中,同时考虑节点的信任值和下一节点的移动距离,可以获得更可靠的数据,同时确保更少的能量消耗.

为了更清楚地显示不同数据采集模式的节能效果,我们比较了不同模式下的网络生命周期.如图 5 所示,我们比较了移动边缘节点的随机移动、通用方法(LEACH 方法)生成的簇头节点及 UTDC 方法访问节点的网络生命周期.从结果可以看出,在随机接入收集模式中生命周期最短,而普通簇头节点的访问模式次之,UTDC 模式的网络生命周期最长.同时,当节点数量从 100 增加到 400 时,可以看出 UTDC 方法可以更有效地延长网络生命周期.

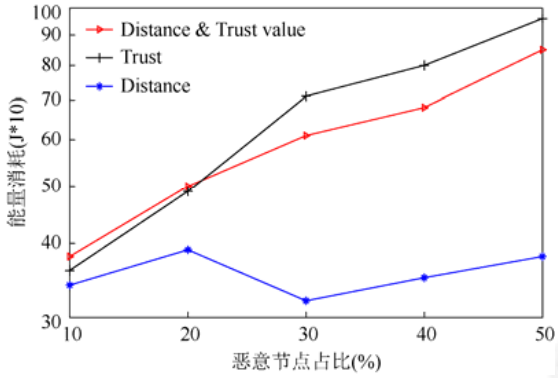

Fig.4 Energy consumption in the case of different malicious nodes

图 4 不同恶意节点占比情况下的能量消耗

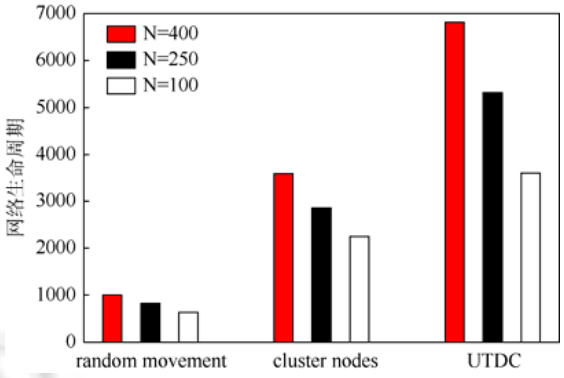

Fig.5 Comparison of the advantages of the algorithm under different number of nodes

图 5 UTDC 算法在不同数量节点下的优势比较

如图 6 所示,在实验中,我们比较了移动基站辅助数据收集(MADG)和 UTDC 方法.可以看出,随着移动速度的增加,MADG 方法与 UTDC 方法消耗的能量都降低.但是随着速率移动增加,UTDC 方法能量消耗降低更快,同时可信评估避免访问远距离的不可信节点,有效降低移动节点的能量消耗.与多跳协议方法相比,UTDC 方法下移动边缘节点收集数据可以节省 35%~60%的能量,与使用 MADG 的方法相比,在移动速度为 2m/s 以下时,能耗消耗基本接近.但是结合图 9,MADG 方法的延迟却远远高于 UTDC 方法,这在低延迟要求较高的数据收集应用中显得十分重要.

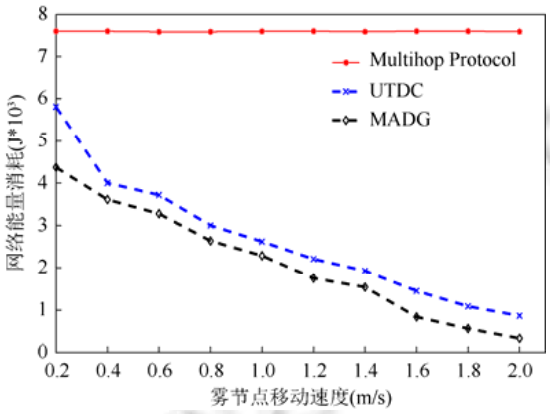

Fig.6 Network energy consumption of mobile edge nodes at different rates

图 6 移动边缘节点在不同速率下的网络能耗

路径距离和节点的信任值是我们基于效用值的 UTDC 算法的关键.因此,我们评估了不同恶意节点占比下单位能量的数据信任率,如图 7 所示.由图 7 可以知道,当路径中只考虑距离时,随着恶意节点比例的增加,消耗单位能量获得的可信数据的比例急剧下降,因为收集的大部分数据都来自不受信任的恶意节点的数据.同时考虑距离和信任值,下降速度较慢;这说明,相比较只有距离因素的情况,当消耗相同的能量时,基于效用值

的可信数据收集方法可以获得更可靠的数据,结果更加有效.因此,该结果还表明信任值在数据收集中是必不可少的.

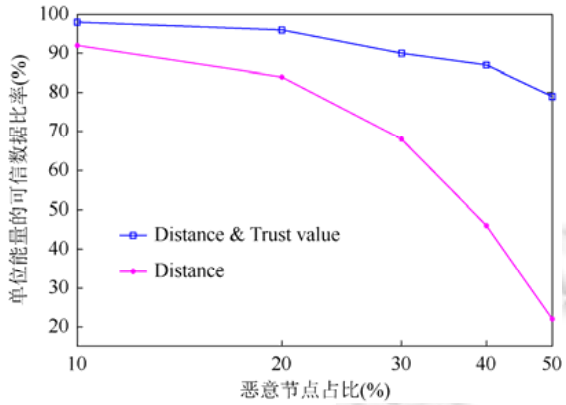

Fig.7 Trustworthy data ratio of unit energy for different malicious nodes

图 7 不同恶意节点占比下单位能量的可信数据比率

在信任值的计算中,我们使用 3 个权重来测量直接信任值的结果,即通信交互、能量剩余和丢包率,分别表示为 ω_i,ω_e 和 ω_p.在不同的权重比下连续进行多次(轮)实验,如图 8 所示.我们将 3 组权重分为 6 组,每次保持一个权重不变,另外两个权重改变.从图中我们可以看出,具有相同权重的通信交互的两条线具有相同的转换趋势,并且信任值最小.最大的信任值是具有相同能量权重的最上面折线和第二位折线,另外两个是居中的,信任值发生变化的是因为不同的权重分配的结果.

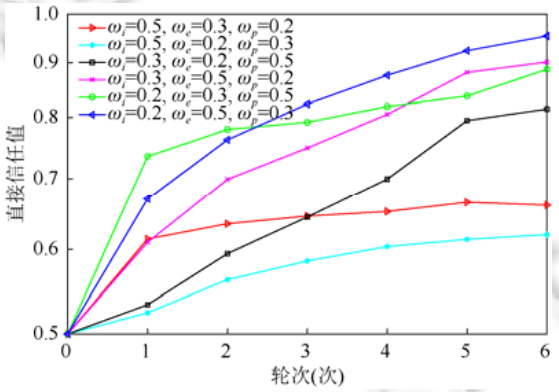

Fig.8 The effect of different weight distribution on direct trust value

图 8 不同权重分配对直接信任值的影响

为了更好的显示 UTDC 方法在网络延迟方面的性能,我们将 UTDC 方法与类似的 RCC 方法和文献中的 MADG 方法进行了比较,结果如图 9 所示.由图 9 可以看出,采用 MADG 方法的延迟最高,RCC 方法的网络延迟与我们的 UTDC 方法接近,但我们的 UTDC 方法优于 RCC.与现有的同类型的 RCC 方法相比,我们的方法可以将总的网络延迟降低约 16.2%.延迟降低的原因在于我们的数据收集是访问分区的可信的簇头节点,而不是 RCC 方法中的访问整个网络的节点,与必须传输数据的 MADG 方法相比,也节省了数据传输的时间.

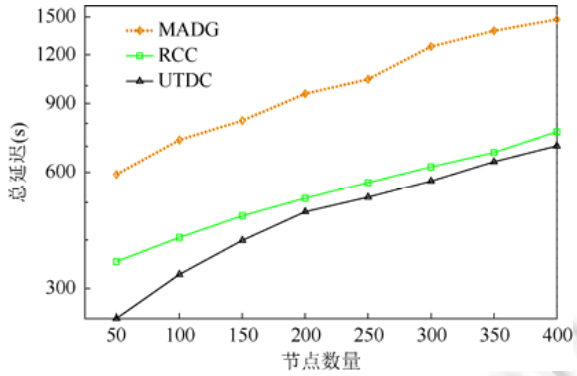

Fig.9 Comparison of network delays in different methods

图 9 不同方法下的网络延迟比较

5 结 论

物联网服务的快速发展正在不断改变世界,然而,由于诸如环境噪声和恶意攻击之类的问题,物联网系统当前收集的数据是不可信的.为了确保数据收集的可信度,我们提出了一种基于效用的可信数据收集算法.通过建立信任模型获得节点的信任值,根据信任值选择可信的簇头节点,并且作为可信的数据收集节点.此外,为了实现最小能量消耗和局部最大信任,在规划移动边缘节点的路径时兼顾下一节点的信任值和距离.最后,实验结果表明,该方法可以充分评估节点的可信度,数据采集方法的设计可以节省网络能量,有效延长网络的生命周期.

References:

[1] Bi R, Li JZ, Gao H. Approximate monitoring algorithm for minimizing communication cost in wireless sensor networks. Chinese Journal of Computers, 2015,38(10):2092–2105 (in Chinese with English abstract).

[2] Li WX, Fu XW. Survey on invulnerability of wireless sensor networks. Chinese Journal of Computers, 2015,38(3):625–647 (in Chinese with English abstract).

[3] Bhuiyan MZA, Wang G, Wu J, Cao JN, Liu XF, Wang T. Dependable structural health monitoring using wireless sensor networks. IEEE Trans. on Dependable and Secure Computing, 2017,14(4):363–376.

[4] Gao S, Zhang H, Das S. K. Efficient data collection in wireless sensor networks with path-constrained mobile sinks. IEEE Trans. on Mobile Computing, 2011,10(4):592–608.

[5] Wang T, Zhang GX, Liu AF, Bhuiyan MZA, Jin Q. A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing. IEEE Internet of Things Journal, 2019,6(3):4831–4843.

[6] Wang T, Zhou JY, Chen XL, Wang GJ, Liu AF, Liu Y. A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing. IEEE Trans. on Emerging Topics in Computational Intelligence, 2018,2(1):3–12.

[7] Shi GT, Liao MH. Movement-assisted data gathering scheme with load-balancing for sensor networks. Ruan Jian Xue Bao/Journal of Software, 2007,18(9):2235–2244 (in Chinese with English abstract).

[8] Kaswan A, Nitesh K, Jana PK. Energy efficient path selection for mobile sink and data gathering in wireless sensor networks. AEU Int'l Journal of Electronics and Communications, 2017,73:110–118.

[9] Awan KA, Din IU, Almogren A, Guizani M, Altameem A, Jadoon SU. Robust trust—A pro-privacy robust distributed trust management mechanism for Internet of Things. IEEE Access, 2019,7:62095–62106.

[10] Wang T, Zhou JY, Liu AF, Bhuiyan MZA, Wang GJ, Jia WJ. Fog-based computing and storage offloading for data synchronization in IoT. IEEE Internet of Things Journal, 2019,6(3):4272–4282.

[11] Wen W, Zhao S, Shang C, Chang CY. Eapc: Energy-aware path construction for data collection using mobile sink in wireless sensor networks. IEEE Sensors Journal, 2018,18(2):890–901.

[12] Wang T, Zhang GX, Cai SB, Jia WJ, Wang GJ. Survey on trust evaluation mechanism in sensor-cloud. Journal on Communications, 2018,39(6):37–51 (in Chinese with English abstract).

[13] Wu YK, Huang HY, Wu Q, Liu AF, Wang T. A risk defense method based on microscopic state prediction with partial information observations in social networks. Journal of Parallel and Distributed Computing, 2019,131:189–199.

[14] Wang T, Liang Y, Jia W, Arif M, Xie MD. Coupling resource management based on fog computing in smart city systems. Journal of Network and Computer Applications, 2019,135:11–19.

[15] Bhuiyan MZA, Wu J, Wang GJ, Wang T, Hassan MM. E-sampling: event-sensitive autonomous adaptive sensing and low-cost monitoring in networked sensing systems. ACM Trans. on Autonomous and Adaptive Systems, 2017,12(1):1–29.

[16] Zeng JD, Wang T, Jia WJ，Peng SL, Wang GJ. A survey on sensor-cloud. Journal of Computer Research and Development, 2017,54(5):925–939 (in Chinese with English abstract).

[17] Wang T, Bhuiyan MZA, Wang GJ, Rahman AM, Wu J, Cao JN. Big data reduction for a smart city's critical infrastructural health monitoring. IEEE Communications Magazine, 2018,56(3):128–133.

[18] Xing GL, Li M, Wang T, Jia WJ, Huang J. Efficient rendezvous algorithms for mobility-enabled wireless sensor networks. IEEE Trans. on Mobile Computing, 2011,11(1):47–60.

附中文参考文献:

[1] 毕冉,李建中,高宏.无线传感器网络中最小化通信开销的近似监测算法.计算机学报,2015,38(10):2092–2105.

[2] 李文锋,符修文.无线传感器网络抗毁性.计算机学报,2015,38(3):625–647.

[7] 石高涛,廖明宏.传感器网络中具有负载平衡的移动协助数据收集模式.软件学报,2007,18(9):2235–2244.

[12] 王田,张广学,蔡绍滨,贾维嘉,王国军.传感云中的信任评价机制研究进展.通信学报,2018,39(6):37–51.

[16] 曾建电,王田,贾维嘉,彭绍亮,王国军.传感云研究综述.计算机研究与发展,2017,54(5):925–939.

邱磊(1994－),男,湖北十堰人,硕士生,主要研究领域为边缘计算,无线传感器网络.

於志勇(1982－),男,博士,副教授,博士生导师,CCF 专业会员,主要研究领域为普适计算,移动社交网络,群智感知.

蒋文贤(1974－),男,副教授,CCF 专业会员,主要研究领域为物联网,网络安全,区块链.

马樱(1982－),男,博士,副教授,CCF 专业会员,主要研究领域为数据挖掘,物联网,人工智能.

李玉泽(1994－),男,主要研究领域为边缘计算,无线传感器网络.

王田(1982－),男,博士,教授,CCF 高级会员,主要研究领域为物联网,云计算,雾计算/边缘计算,网络信息安全,软件安全,社交网络.