可抵御节点恶意行为的锚节点型IP坐标系统

黄 琼[1]，王万新[2]，阳小龙[3]，隆克平[3]

(1. 重庆邮电大学移动通信技术重点实验室 重庆 南岸区 400065; 2. 电子科技大学通信与信息工程学院 成都 631711;
3. 北京科技大学计算机与通信工程学院 北京 海淀区 100083)

【摘要】锚节点型IP坐标系统的性能受锚节点选择与布局情况以及节点恶意行为的影响较大，由此提出了一种新的可抵御节点恶意行为的锚节点型IP坐标系统(LCSD)，锚节点按聚类最优化选择与布局，并采用协作推荐信任评估机制限制恶意节点对其他节点坐标更新的影响。从相对误差、邻居度和最近邻居可信度等方面分析了LCSD。结果表明与ICS相比，LCSD相对误差更小；不论恶意节点比例大小，LCSD邻居度和最近邻居可信度都较优越。

关 键 词 时延; IP坐标系统; IP网络; 锚节点
中图分类号 TP393 文献标识码 A doi:10.3969/j.issn.1001-0548.2012.02.022

Landmark-Based IP Coordinate System with Defend-Capable Malicious Behaviors

HUANG Qiong[1], WANG Wan-xin[2], YANG Xiao-long[3], and LONG Ke-ping[3]

(1. Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications Nan'an Chongqing 400065;
2. School of Communication and Information Engineering, University of Electronic Science and Technology of China Chengdu 631711;
3. School of Computer and Communication Engineering, University of Science and Technology Beijing Haidian Beijing 100083)

Abstract The distance prediction performances of landmark-based IP coordinate system are sensitive to the selection and placement of landmarks and the malicious behaviors of some hostile nodes, which have greatly impact on the accuracy and trustiness of the predicted distances for most of applications. This paper proposes a new landmark-based IP coordinate system with defend-capable malicious behaviors (for short LCSD), in which the selection and placement of landmarks are optimized through the distance matrix clustering scheme, the malicious behaviors of hostile nodes are prohibited to disturb the coordinate update of the normal nodes through the cooperative recommending trust-evaluation mechanism. Finally by some simulations, its performances are analyzed in terms of the relative error (RE), the neighbor approximation degree. The closest neighbor trust degree, and the results show that LCSD has much smaller RE on the whole, and outperforms ICS in the neighborhood in despite of the proportion of hostile nodes to the all nodes.

Key words delay; IP coordinate system; IP networks; landmark

随着IP网络规模增长、网络结构日益异构和复杂化，如何快速、及时地获取反映网络运行性能和行为特征的第一手资料，准确掌握IP网络性能及状态参数，成为当前网络应用性能优化的关键过程。在实际IP网络中所涉及的性能及状态参数很多，如带宽、时延、吞吐量等，而节点间时延是其中关键参数之一，在许多基于Overlay的大规模网络服务的设计和部署中发挥着重要作用，如内容分发网络(CDN)[1]、Overlay路由构造[2]等。

对于IP网络中节点间的时延，在网络性能测量中称为网络距离。在实际网络中，虽然网络距离可以采用Ping、Traceroute等方式按需精确测量，但是其测量开销随网络规模的扩大而激增。一些研究者提出，依据空间嵌入理论，利用少量节点间的实测时延构建一个虚拟空间，即网络坐标系统(network coordinate system，NCS)。在时延测度意义下，网络中各节点可以一一嵌入到该虚拟空间，即可用一组坐标唯一地标识网络中的节点，由该坐标系统可以

收稿日期：2010－03－16； 修回日期：2011－09－16
基金项目：国家973计划(2007CB310706，2012CB315905)；国家自然科学基金(60932005，61172048，61100184)；国家科技重大专项(2011ZX03005-004-02)；教育部新世纪优秀人才计划(NCET-09-0268)；四川省青年基金(09ZQ026-032)；重庆市教委科研项目(KJ100514)
作者简介：黄琼(1971－)，女，副教授，主要从事计算机网络方面的研究.

利用空间中几何距离计算方式，不需直接测量也能近似地获得节点间的网络距离。与Ping直接测量相比，该方法开销小、测量简便且预测准确度较高，现已被运用到很多实际网络中解决拓扑优化设计以及网络应用性能优化的一些实际问题[3-4]。

一般而言，NCS大致可分为锚节点型和非锚节点型两类。前者的坐标空间由锚节点间的距离矩阵建立，普通节点的坐标则利用自身到锚节点间的距离和锚节点的坐标得到，如PIC[5]、ICS[6]等；节点采用物理学上弹簧伸缩效应等类似机理计算坐标，如Vivaldi[7]。非锚节点型NCS虽然定位准确度高，但其开销大、稳定性差。相反，锚节点型NCS的计算简单、定位准确度高，因此本文主要考虑锚节点型IP网络坐标系统。

在锚节点型NCS的构建中，锚节点的选择通常是最重要的环节之一，因为所选择的节点充当锚节点以及锚节点所分布的网络区域等，这些因素对坐标系统的网络距离预测性能的影响很大。此外，NCS系统通常默认节点间相互信任，且探测节点所报告的距离信息不虚假。然而现实中这些假设不一定成立，虚假的距离信息或者错误的坐标信息都导致其他节点无法准确地预测网络距离。因此在实际IP网络中，锚节点型NCS的稳健性差。PIC[8]试图利用三角不等式违例(常简称TIV)检测恶意节点，然而在实际网络中，TIV现象很普遍且发生频繁，而且TIV也并非都是因节点恶意行为引发，还可能是因为网络路由策略等因素造成，因此这类恶意行为检测方法不可行。文献[9]深入分析了网络坐标系统里存在的各种攻击方式及其对系统距离预测性能的影响程度，并进一步在文献[10]中提出了基于卡曼滤波器的恶意节点鉴别方法，以消除节点恶意行为。此外，文献[11]提出了基于社交关系的恶意节点屏蔽方法，文献[12-13]则针对非锚节点型NCS分别提出了基于坐标更新受限和节点坐标可信度评测方法，以提高系统在非可信环境的距离预测性能。

针对当前非可信的IP网络环境，结合上述文献的思路，本文提出了一种新的可抵御节点恶意行为的锚节点型IP网络坐标系统(landmark-based coordinate system with defend-capable malicious behaviors，LCSD)。首先LCSD采用与ICS[6]类似的主元分析法PCA对锚节点时延矩阵简化分析处理，将其距离空间映射到一个新的低维测度空间，然后在锚节点数目的约束下，采用聚类算法最优化锚节点的选取和布局，以实现锚节点分布能与网络拓扑特征与时延分布最大限度地匹配。其次，LCSD采用基于锚节点和邻居节点协作推荐的信任评估机制维护节点的RTT和坐标信息的可信度。依据节点的可信度信息，坐标系统可以限制低可信节点的坐标更新、减少它与其他节点的信息交互，从而达到有效地抵御该节点的恶意行为对整个坐标系统性能的影响。最后，本文从相对误差、邻居度和最近邻居可信度等方面对LCSD的性能进行了深入的评测，仿真结果表明，与ICS相比，LCSD距离预测准确度更高，即使系统中存在较多恶意节点时，其距离预测性能仍很好，而且从邻居节点的选择角度上看，预测值与实际值接近。

1 锚节点型网络坐标系统的脆弱性分析

1.1 锚节点型坐标系统的主要实现环节

锚节点型坐标系统的距离预测过程通常包括基准坐标系统构建、普通节点空间嵌入(网络节点在基准坐标系统中坐标计算)两个环节。首先收集锚节点间的距离信息，然后采用单纯形等最优化方法构建一个基准坐标系统。其次实测普通节点到各锚节点而得到一组距离向量，然后再采用单纯形等最优化方法将该距离向量转化为该节点空间嵌入到基准坐标系统下的一组多维坐标。最后依据嵌入空间距离定义，可用任意两点间的空间距离近似估计相应网络节点间的时延距离。

ICS[6]为锚节点型IP网络坐标系统中的典型代表。除包含上述主要环节，它还对锚节点距离矩阵采用主元分析处理，最大程度地提取出主要拓扑信息，以使基准坐标系统的维度尽可能降低，减少坐标系统的计算复杂度。

1.2 潜在的脆弱性及其分析

锚节点型坐标系统能较好地将IP网络距离嵌入到几何测度空间。在多数情形下，该系统的距离预测性能够满足CDN、P2P等网络应用的性能优化需要。但是当锚节点选择不恰当或布局不合理时，该类系统的距离预测准确度将很差。另外，因网络拓扑的动态变化，各节点的坐标也需相应更新，此时该类系统可能因一些节点恶意发布不真实的RTT或虚假的坐标更新等行为而误导其他节点的坐标更新，严重影响其预测距离的可信度。

在传统锚节点型坐标系统中，通常假设锚节点是可信的，而普通节点常通过以下两种恶意行为影响系统的距离预测性能：1) 发布虚假的距离向量。

如某节点可能故意延迟一段时间后，再响应Ping请求，而致使得到的RTT不真实。2) 发布虚假的更新坐标信息。如某恶意节点可能发起中间人攻击，篡改其转发报文中的其他节点的坐标信息。

相对误差(relative error，RE)是评估网络坐标系统距离预测性能的一个重要典型参数，其定义为：

$$\mathrm{RE}=\frac{|\tilde{D}-D|}{\min(\tilde{D},D)} \tag{1}$$

式中，D表示实测时延；$\tilde{D}$表示由坐标系统预测而得到的时延。若相对误差RE越小，表明坐标系统预测距离的准确度越高。本文以ICS系统为例，给出了节点恶意行为对其距离预测相对误差的影响程度，具体如图1所示。当30%的恶意节点散布虚假距离向量时，系统中半数以上的节点其相对误差大于0.8；系统30%的恶意节点散布虚假坐标信息时，50%以上的节点其相对误差大于1。随着恶意节点数目的增多，系统预测距离的准确度也随着大大降低。

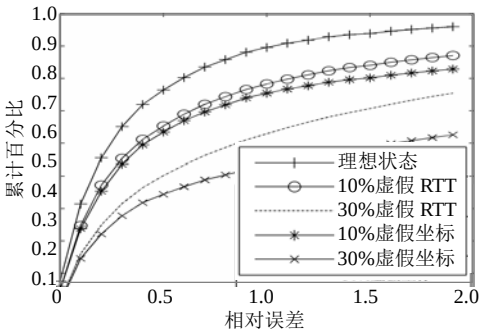


图1　节点恶意行为对系统相对误差的影响

2　可抵御恶意行为的锚节点型网络坐标系统(LCSD)

为了使锚节点的选择与布局更能与实际网络的拓扑结构和节点间时延分布相匹配，LCSD系统拟采用聚类算法对其锚节点进行最优化选择和布局。同时为了抵御节点的恶意行为，LCSD拟采用基于多节点协作推荐的信任评估机制计算普通节点的可信度。当且仅当信誉值超过预设可信门限时，系统允许某节点更新坐标或者与其他节点进行交互。

2.1　锚节点最优化选择与布局策略

为了降低计算复杂度，锚节点坐标系统通常仅需少量的锚节点。在锚节点数约束下，如何实现锚节点的最优化选择与布局，成为提高坐标系统距离预测准确度的关键之一。目前常用锚节点选择与布局策略，主要有随机选择、最大距离选择和聚类选择等。由于随机选择策略不能完全排除最坏选择，如选择的锚节点分布过于集中。另外，文献[14]的研究表明与最大距离选择相比，聚类选择能使系统预测误差更小。因此LCSD系统采用基于聚类算法的锚节点最优化选择与布局策略。

在聚类算法中，任意两个节点间的距离仍采取欧氏距离定义，即某聚类C中节点n_i与节点n_j之间的距离定义为：

$$D_{i,j}=\sqrt{\sum_{l}(\mathrm{RTT}(n_i,n_l)-\mathrm{RTT}(n_j,n_l))^2} \tag{2}$$

式中，$n_i\in C$；l为集合中节点的总数；RTT(n_i, n_j)为节点n_i与节点n_j之间的时延距离。各节点间的欧式距离构成一个欧氏距离矩阵$\boldsymbol{M}_{nn}$，其中第i行j列元素D_{ij}即表示n_i与n_j之间的距离。

聚类开始时将网络中各节点单独设置为一个聚类；然后由各节点之间的时延得到欧氏距离矩阵$\boldsymbol{M}_{nn}$，对该矩阵$\boldsymbol{M}_{nn}$按如下方式聚类：先计算$\boldsymbol{M}_{nn}$各行向量之间的相关系数，将最相似的两个行向量聚类为一类，然后重复该过程，即每次都将相似度最大的两类聚为一类，直至系统中有S类，其中$S<|C|$；最后从各聚类中选取其中心节点为锚节点。

2.2　抵御节点恶意行为的坐标更新机制

为了抵御恶意节点散布虚假信息对坐标系统性能带来的影响，LCSD采用基准信任节点和参考节点协作推荐的信任评估机制。普通节点只有在其信誉值高时，才允许其更新本地坐标。

2.2.1　信誉定义与基于协作推荐的信任评估机制

某一实体A的信誉是其他所有实体对A的信任的综合评价，信任是指某一实体基于一定经验对另一个实体的未来行为的主观期望。信任强调的是主观、局部的信赖程度，信誉强调的是集体对某实体的综合评价，它是全局和客观的评价；经验是其他实体对该实体A的行为观察。

传统锚节点型坐标系统中节点坐标的更新不受任何限制，而在LCSD中，某一节点进行坐标更新前首先向信任信息库查询关联对等节点的信誉值。当且仅当该关联对等节点可信时，它们之间的实测距离才可用于该节点的坐标更新中，或者该节点可选为可信邻居进行交互。信任信息库中的信任信息来自系统中基准信任节点和参考节点的协作推荐，其中基准信任节点从锚节点中随机选取，周期性地测量它们到普通节点的距离向量，并根据距离向量的经验做出信任评估；参考节点从与普通节点有交互行为的节点中选择，计算它们到该普通节点预测距离的误差，并做出信任评估。因此，LCSD中某一普

通节点的信誉值R是基准信任节点和参考节点协作推荐信任的综合评估值。

假定在k时刻，基准信任节点L_i与普通节点N_j的经验为：

$$\mathrm{EL}_{N_j}^{L_i}=1-\frac{\langle \mathrm{RTT}^k,\sum_{i=k-h+1}^{k}\frac{1}{h}\mathrm{RTT}_{N_j}^{L_i}\rangle}{\sum_{i=k-h+1}^{k}\frac{1}{h}\mathrm{RTT}_{N_j}^{L_i}} \tag{3}$$

式中，h为距离向量经验的长度；$\langle\cdot\rangle$为标准方差运算。基于该经验，基准信任节点L_i对节点N_j的信任为：

$$\mathrm{TL}_{N_j}^{L_i}=\begin{cases}1 & \mathrm{EL}_{N_j}^{L_i}>\alpha\\ 0 & \mathrm{EL}_{N_j}^{L_i}<\alpha\end{cases} \tag{4}$$

假定在k时刻，参考节点N_i关于节点N_j的经验为$\mathrm{EN}_j^i=\mathrm{Err}_j^i$，Err表示参考节点$N_i$与节点$N_j$距离的相对误差。基于该经验，参考节点$N_i$对节点$N_j$的信任为：

$$\mathrm{TN}_{N_j}^{N_i}=\begin{cases}1 & \mathrm{EN}_{N_j}^{N_i}<\beta\\ 0 & \mathrm{EN}_{N_j}^{N_i}>\beta\end{cases} \tag{5}$$

在式(4)和式(5)，α 和 β 是与实际网络背景相关的阈值。

信任信息库收到所有来自基准信任节点和参考节点对目标节点的推荐信任后，由信任的传递运算 $\otimes$ 和合并运算 $\oplus$ 得出目标节点A的信誉评价。$\otimes$ 可看作是信任的传递，即节点B在没有直接交互的情况下，对目标节点A的信任值为实体B对推荐实体x的信任度和推荐实体对目标实体A的信任值的乘积；$\oplus$ 运算则为多源信任的平均。因此目标节点A的信誉值为：

$$R_A=\mathrm{TL}_A\oplus\mathrm{TN}_A \tag{6}$$

式中，TL_A、TN_A 分别为基准信任节点和参考节点对节点A的协作推荐信任，即有：

$$\mathrm{TL}_A=\mathop{\oplus}_{L_i\in\mathrm{LA}}(\mathrm{DL}_i\otimes\mathrm{EL}_A^{L_i}) \tag{7}$$

$$\mathrm{TN}_A=\mathop{\oplus}_{N_i\in\mathrm{NA}}(\mathrm{DN}_i\otimes\mathrm{EN}_A^{N_i}) \tag{8}$$

式中，LA为节点A的基准信任节点集合；DL_i为基准信任节点i的推荐信任强度；$\mathrm{DL}_i\otimes\mathrm{EL}_A^{L_i}$为管理员得到来自基准信任节点$i$的关于节点$A$的推荐信任。所有对节点$A$的推荐信任平均即是该节点的综合信任。同理，式(8)为信任信息库得到的来自参考节点对目标节点A的综合信任。

在式(7)和式(8)中，DL_i和DN_i分别是基准信任节点和参考节点对信任信息库各自的推荐信任度。推荐信任度体现了推荐者推荐行为的可靠度，应当“因人而异”。本文中基准信任节点视为可靠的实体，因此有$\mathrm{DL}_i=1$。而参考节点的推荐信任度则根据其是否与节点A有交互行为而不同，即有：

$$\mathrm{DN}_i=\begin{cases}\mathrm{EL}_i^A & i\text{与}A\text{有交互}\\ \theta & i\text{与}A\text{无交互}\end{cases} \tag{9}$$

式中，θ为信誉值区间中值。

2.2.2 坐标更新机制及实现

节点i与节点j进行交互前，计算节点j的综合信任按以下步骤进行：

1) 从信任信息库查询基准信任节点对节点j的直接信任，i根据推荐信任度和基准信任节点对节点j的直接信任，合议来自基准信任节点推荐信息。

2) 从信任信息库查询参考节点对节点j的直接信任。若参考节点与节点i无交互经验，则返回θ；反之，返回参考节点对节点j的直接信任。节点i根据推荐信任度和参考节点对节点j的直接信任，合议来自参考节点的推荐信息。

3) 节点i将基准信任节点和参考节点的推荐信息进行合议，即得出对节点j的综合信任值。根据网络的状态，确定节点j的信誉值，若信誉值高于阈值，则进行更新或者与节点j进行交易；反之，舍弃节点j。

4) 当节点i与节点j在基于信任机制的基础上成功交互后，节点i记录本次与节点j的交易结果，包括节点i与节点j的相对误差，并将其反馈给信任信息库。

3 仿真与性能分析

本文以美国NLANR研究中心在AMP项目中分布在全球的实验节点间的RTT数据为例[15]，从中选取1 000个有效的节点间的RTT形成一个时延矩阵，从相对误差、邻居度和最近邻居可信度等3个方面分析评估本文构建的坐标系统LCSD的距离预测性能。

3.1 锚节点最优化选择与布局策略对系统性能的影响

本文首先以无恶意节点情形为例，对比分析锚节点最优化选择与布局前后坐标系统预测距离准确度的变化。如果设定系统中锚节点的数目为10，则余下的90个节点作为普通节点。以文献[6]的ICS系统为比较对象，它采取随机锚节点选择与布局策略。不同锚节点选择与布局策略对系统性能的影响如图2所示。由图2可知，与采取锚节点随机选择的ICS系统相比，LCSD因采取了最优化选择与布局策略，其全局相对误差更小。如在LCSD系统中有更多节点

间的距离预测相对误差小于0.4，比ICS高出近7%。

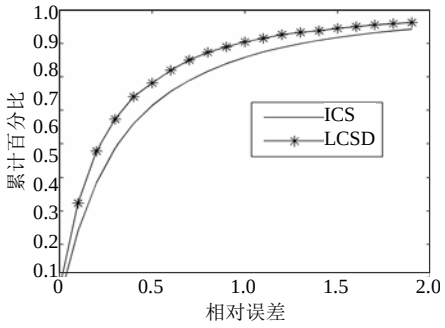


图2　锚节点选择与布局策略对系统性能的影响

3.2　坐标更新机制性能仿真

除了相对误差，邻居选择的优劣性也是衡量坐标系统性能的一个重要性能指标。在无恶意节点时，LCSD邻居度分布如图3所示。由图3可知，邻居度为1的节点比例高达36%，而邻居度为2和3的节点比例分别为8%和9%。

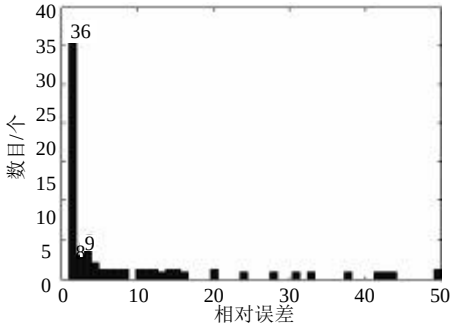


图3　无恶意节点情形下LCSD邻居度分布情况

为了抵御恶意节点行为，LCSD为每个普通节点分配3个基准信任节点和3个参考节点，经验观察的长度h为4。假定节点间时延相对稳定，因此α可设为0.95，$\beta = \mathrm{Co}\cdot\mathrm{Average(error)}$，Average(error)为整个系统相对误差的平均值，Co设为1.5。恶意节点在90个普通节点中随机分布，它们散布虚假RTT和虚假坐标信息的概率相同。为了简单起见，假定系统在整个运行过程中，恶意节点的行为方式固定不变。LCSD和ICS各自运行100次，取系统邻居度的平均值进行比较。

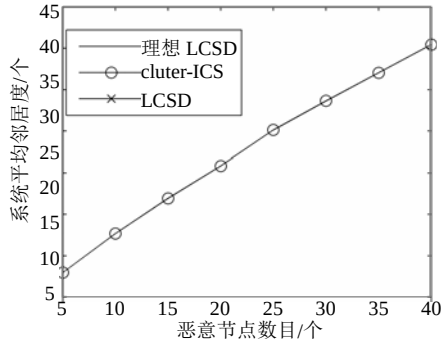
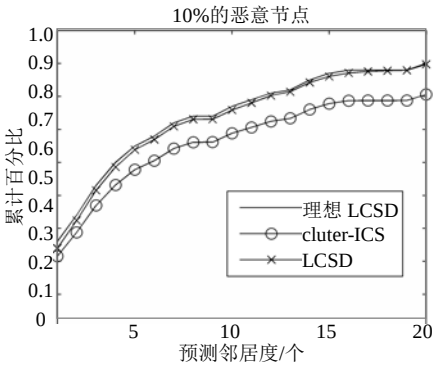
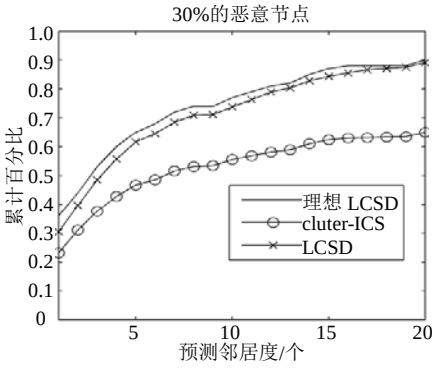


图4　LCSD与ICS系统的平均邻居度比较

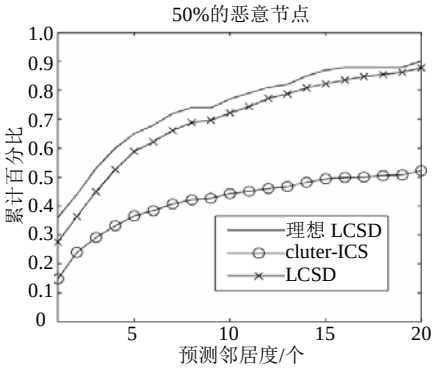
LCSD与ICS系统的平均邻居度比较如图4所示。由图4可知，ICS的平均邻居度随着恶意节点的增多而近似呈线性增大，LCSD的平均邻居度则接近于理想状态下的邻居度。由此表明从最近邻居选择的可信性角度，LCSD系统的距离预测性能比ICS更优越。这主要因为LCSD采取了基于协作推荐的信任评估机制，对恶意节点行为进行有效的抑制，避免它们的恶意行为误导其他节点的坐标更新。



a. 恶意节点占10%时的邻居度比较



b. 恶意节点占30%时的邻居度比较



c. 恶意节点占50%时的邻居度比较

图5　恶意节点不同比例下LCSD与ICS系统的邻居度比较

系统中恶意节点比例为10%、30%和50%情形下，坐标系统邻居度的累积百分比曲线如图5所示。在实际IP网络应用性能优化中，更关注较小邻居度的分布情况，因此本文着重分析了邻居度从1～20

的分布。在系统恶意节点比例为10%时，ICS中目标邻居和实际邻居的吻合度大约为31%；在LCSD中其吻合度增大至34%。在恶意节点比例为50%时，LCSD目标邻居和实际邻居的吻合度比ICS高出约12%。因此，不管系统中存在多高比例的恶意节点，与ICS相比，LCSD在最近邻居选择方面总能有较好的表现。

本文分析比较了LCSD的最近邻居可信度，如图6所示，横坐标表示恶意节点数，纵坐标表示系统的最近邻居可信度总值。由图6可知，系统最近邻居可信度总和随着恶意节点数目的增多不断下降。在恶意节点达到25时，LCSD的系统最近邻居可信度为82，比ICS高近5%；在恶意节点达到50时，系统最近邻居可信度提高了近10%，由此表明LCSD在提供可信邻居选择方面可信度更高。

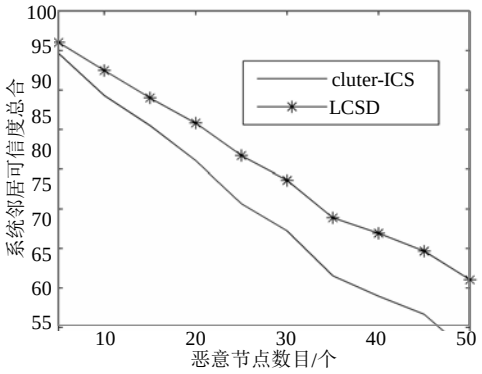


图6 LCSD与ICS系统的最近邻居可信度比较

4 结 论

由于锚节点型IP坐标系统的距离预测准确度易受锚节点选择的影响，且任何节点的恶意行为将降低系统预测距离的可信度，本文针对性地提出了一种新的可抵御节点恶意行为的锚节点型IP坐标系统LCSD。LCSD采用了基于聚类的最优化锚节点选择与布局策略，同时引入基于协作推荐的信任评估机制维护每个节点的信誉度。信誉值有效地反映该节点距离向量的稳定性以及坐标信息的准确度。普通节点只有在其信誉值高时才允许更新本地坐标；低信誉值的节点被限制与其他节点进行交互。在信誉模型里，每个节点的信任由信任信息库基于基准信任节点和参考节点的推荐信任来评估。节点同时依据距离的远近和信誉值的高低选择最优邻居节点。

仿真结果表明，LCSD由于采取了基于聚类算法的锚节点选择与布局策略，其全局相对误差更小。无论系统中存在多高比例的恶意节点，与ICS相比，LCSD在最近邻居选择方面总能有较好的表现。

参 考 文 献

[1] JOHNSON K, CARR J, DAY M, et al. The measured performance of content distribution networks[J]. Computer Communications, 2001, 24(2): 202-206.

[2] ANDERSEN D G, BALAKRISHNAN H, KAASHOEK M F, et al. Resilient overlay networks[C]//Proc 18th ACM SOSP. Banff, Canada: ACM, 2001.

[3] HUANG A C, STEENKISTE P. Network-sensitive service discovery[J]. Journal of Grid Computing, 2003, 1(3): 309-326.

[4] XU Z, TANG C, BANERJEE S, et al. RITA: receiver initiated just-in-time tree adaptation for rich media distribution[C]//Proc of NOSSDAV'2003. Monterey, USA: [s.n.], 2003.

[5] COSTA M, CASTRO M, ROWSTRON A, et al. PIC: practical Internet coordinates for distance estimation[C]//Proc of ICDCS'2004. Tokyo, Japan: [s.n.], 2004.

[6] LIM H, HOU J, CHOI C H. Constructing Internet coordinate system based on delay measurement[C]//Proc of ACM SIGCOMM IMC'2003. Miami, Florida, USA: ACM, 2003.

[7] DABEK F, COX R, KAASHOEK K, et al. Vivaldi: a decentralized network coordinated system[C]//Proc of ACM SIGCOMM'2004. Portland, Oregon, USA: ACM, 2004.

[8] ZHENG H, LUA E, P M, GRIFFIN T. Internet routing policies and round-trip times[C]//Proc of ACM PAM2005. Boston, MA, USA: ACM, 2005.

[9] KAAFAR M, MATHY L, TURLETTI T, et al. Virtual networks under attack: disrupting Internet coordinate systems[C]//Proc of ACM CoNEXT'2006. Lisboa, Portugal: ACM, 2006.

[10] KAAFAR M, MATHY L, BARAKAT C, et al. Securing Internet coordinate embedding systems[C]//Proc of ACM SIGCOMM2007. Kyoto, Japan: ACM, 2007.

[11] SONG X X, ZHAO X H, LUA E K, et al. SLINCS: a social link based evaluation system for network coordinate systems[C]//Proc of IEEE CCNC 2009. Las Vegas, Nevada, USA: IEEE, 2009.

[12] SAUCEZ D, DONNET B, BONAVENTURE O. A reputation-based approach for securing vivaldi embedding system[J]. Lecture Notes in Computer Science, 2007, 4606: 78-85.

[13] SHERR M, LOO B T, BLAZE M. Veracity: a fully decentralized service for securing network coordinate systems[C]//Proc of IPTPS'2008. [S.l.]: [s.n.], 2008.

[14] MAO Y, SAUL L K, SMITH J M. IDES: an Internet distance estimation service for large networks[J]. IEEE Journal of Selected Areas in Communication, 2006, 24(11): 2273-2284.

[15] National Laboratory for Applied Network Research. Active measurement project (AMP)[EB/OL]. [2009-08-15] http://watt.nlanr.net.

编 辑 黄 莘