支持入侵容忍的网络距离选举计算模型

王 聪* 张凤荔 杨晓翔 李 敏 王瑞锦
(电子科技大学计算机科学与工程学院 成都 611731)

摘 要：为了增强非可信环境下网络坐标系统生存能力，该文重新解释了经典模型中锚节点作用力的物理意义，以锚节点信誉代替距离预测误差作为权值，提出了网络距离选举计算模型，并将其归结为 l_1 损失函数优化问题求解。针对目标函数的不可微特性，基于增量次梯度算法搜索目标函数极优值，并利用比例控制器实现了迭代步长的负反馈控制。实验证明，在计算代价可接受的前提下，模型不仅实现了可信环境下更高的计算精度，而且体现了远较基准算法为优的入侵容忍能力，在严重非可信环境下仍能提供质量尚可的网络距离计算服务。

关键词：入侵容忍；网络坐标系统；网络测量；最优化
中图分类号：TP393.1 **文献标识码**：A **文章编号**：1009-5896(2013)11-2637-07
DOI: 10.3724/SP.J.1146.2012.01402

A Voter Model Supporting Intrusion-tolerance for Network Distance Estimation

Wang Cong Zhang Feng-li Yang Xiao-xiang Li Min Wang Rui-jin
(*School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu* 611731, *China*)

Abstract: To enhance the survivability of Network Coordinate System (NCS) in un-trusted environment, the physical meaning of anchor nodes' spring force in classic model is re-explained, weight vector is taken for anchor nodes' reputations instead of their prediction errors. Thus a voter model is proposed for network distance prediction and this model is categorized as a kind of method to solve a l_1-loss function minimizing problem. By taking the objective function's non-differentiability into consideration, the incremental sub-gradient descending algorithm is used to minimize this function, and a proportional regulator is used to control the iterative step factor with negative feedback. The experiments show that the proposed model is more accurate than classic model in trusted environment with acceptable computing cost. Furthermore, it can also estimate network distance with moderate accuracy in serious un-trusted environment, and shows a stronger intrusion-tolerance capability than classic model.

Key words: Intrusion-tolerance; Network Coordinate System (NCS); Network measurement; Optimization

1 引言

网络坐标系统(Network Coordinate System, NCS)将网络节点嵌入到度量空间中，并以空间距离拟合真实距离。作为一种低成本且高效的网络距离预测机制，已被广泛应用于云计算[1]、内容分发网络[2]、深海探测[3]、资源聚合[4]乃至社交图嵌入[5,6]等领域。

NCS 在设计之初并未考虑安全性问题，交互信息校验机制的缺失使得恶意节点可以扭曲交互信息来实施对 NCS 的攻击[7]。安全性问题的一个解决思路是引入可信第三方进行信息校验[8,9]，但此类方法削弱了 NCS 的分布式特性，不利于系统广泛部署；另一个思路是利用恶意节点与正常节点的动力学差异来实现恶意节点识别[10,11]。然而受样本集完备性的局限，节点在行为特征空间中的几何距离并不能保证精确拟合真实环境，而任何一种攻击模型的假阴性误报都有可能被恶意节点捕捉并学习。更进一步地，如 Frog-boiling 攻击给定攻击节点较小的行为特征偏移以避免触发入侵告警，通过偏移量的累加，以“提线木偶”的方式操控受害节点落入告警区间，使得入侵检测算法本身也成为攻击对象[12]。为了防范新攻击模型，文献[13]基于时域差分特征实现了宏观安全态势的感知和预警，然而该文并未给出个体行为识别算法，因而对恶意节点的检测和预

2012-10-31 收到，2013-05-23 改回
国家科技重大专项课题(2011ZX03002-002-03)，国家 863 计划项目(2011AA010706)和国家自然科学基金(61133016)资助课题
*通信作者：王聪 wangcong@gmail.com

防仍须依赖前两类机制; 而文献[14]虽提出了一种基于物理定律的信息清洗算法，但它忽略了对邻居节点可信性的验证，也没有给出安全的节点漂移重心生成与更新策略。

本文试图提出一种 NCS 生存能力确保的新思路：在承认恶意攻击不可避免和不可完全检出的前提之下，尽可能地抑制恶意攻击行为造成的性能损失，在系统容忍限度内保证一定质量的服务能力，避免攻击行为对系统服务造成灾难性影响。本文算法既可作为假阴性误报的修复手段部署于入侵检测或信任模型等信息清洗策略的后端，也可作为一种强化鲁棒性的 NCS 构建算法单独实施。

2 NCS 安全性问题

NCS 通过维护映射 $f:i\to R^N$ 将节点 i 嵌入到 N 维度量空间 R^N 中。对应地，任意两个节点 i 和 j 间的真实距离 $\hat{d}_{i,j}$ 可用空间距离 $d_{i,j}$ 来拟合，即满足 $d_{i,j}=\|\boldsymbol{i}-\boldsymbol{j}\|\approx\hat{d}_{i,j}$。其中 $\|\cdot\|$ 运算求 R^N 上定义的范数，N 维列向量 $\boldsymbol{i}$ 和 $\boldsymbol{j}$ 是节点在度量空间中的坐标。NCS 测量节点到少量锚节点的往返时延，并利用时延与度量距离的差值定义误差损失函数 e_i，进而极小化 e_i 为节点分配较优坐标。绝大多数情况下 e_i 定义为 l_2 损失函数。不失一般性地，当 R^N 定义为欧氏空间，有

$$e_i=\sum_{j\in\Omega(i)}\left(\|\boldsymbol{i}-\boldsymbol{j}\|_2-\hat{d}_{i,j}\right)^2 \tag{1}$$

其中 $\Omega(i)=\{j_1,j_2,\cdots,j_\omega\}$ 为节点 i 的锚节点集合，$\|\cdot\|_2$ 运算求向量 l_2 范数作为节点的度量距离。令 $\boldsymbol{w}_i[\delta_{j_1}(\|\boldsymbol{i}-\boldsymbol{j}_1\|_2-\hat{d}_{i,j_1})\cdots\delta_{j_\omega}(\|\boldsymbol{i}-\boldsymbol{j}_\omega\|_2-\hat{d}_{i,j_\omega})]$，则 e_i 的 Jacobian 矩阵 $\boldsymbol{J}_i$ 可分解为 $\boldsymbol{w}_i$ 与一组单位向量的乘积。当 e_i 取极小值时，满足：

$$\boldsymbol{J}_i=\boldsymbol{w}_i\times\left[\left(\boldsymbol{i}-\boldsymbol{j}_1\right)\Big/\left\|\boldsymbol{i}-\boldsymbol{j}_1\right\|_2\cdots\left(\boldsymbol{i}-\boldsymbol{j}_\omega\right)\Big/\left\|\boldsymbol{i}-\boldsymbol{j}_\omega\right\|_2\right]^{\mathrm{T}}=\boldsymbol{0} \tag{2}$$

不同的 NCS 赋予 $\boldsymbol{w}_i$ 不同的物理意义，如应用最广泛的弹簧模型将 $\boldsymbol{w}_i$ 视为弹簧作用力，根据锚节点反馈的网络距离、锚节点坐标和误差信息计算弹簧的作用力，并求取弹簧系统达到平衡时的坐标[15]。

显然，无论坐标 $\boldsymbol{j}$，误差 δ_j 抑或两点间的距离 $\hat{d}_{i,j}$ 的真实性都依赖于锚节点的诚实性假设。针对 NCS 的多种攻击模型效能已得到广泛证实[7]，如 Inflation 攻击可推拉目标节点远离正确位置，Deflation 攻击可将目标节点“锁定”在特定的位置无法移动，而 Oscillation 攻击则向目标节点随机发送任意虚假信息造成其剧烈抖动[11]。所有的攻击序列都仅包含 3 种原子操作：延迟应答时延测量请求，发布虚假坐标信息以及发布虚假误差信息[16]，即对 $\boldsymbol{j}$，δ_j 和 $\hat{d}_{i,j}$ 3 个参数的扭曲。

3 网络距离选举计算模型

3.1 模型的基本思想

目前针对 NCS 中的恶意攻击行为尚不存在完美的解决方案。因此本文提出了支持入侵容忍的选举模型，力图在尚未部署防御策略，或防御策略失效时，仍能将恶意攻击行为的影响力抑制在尽可能低的水平。当考虑安全性问题时，相对于锚节点投送的距离和误差信息，一个更合理的计算依据应该是锚节点的可信度。如果将 $\boldsymbol{w}_i$ 视为锚节点的信誉向量，可以引出选举模型的基本思路：假定目标节点 i 的选取的每个锚节点 j 都拥有一张选票 $\boldsymbol{t}_j=(\boldsymbol{i}-\boldsymbol{j})/\|\boldsymbol{i}-\boldsymbol{j}\|_2$，并可以对 i 在度量空间 R^N 中的位移方向进行投票。通过计票，也就是计算投票向量的加权和得到节点的位移方向，并沿该方向移动一段距离，然后开展下一轮投票。这个“投票-微调”的过程往复循环直至投票方“势均力敌”，即可得到节点的坐标。

选举模型的物理意义如图 1(a)所示。与经典的弹簧模型相比，选举模型截断了 e_i 分量函数的误差，仅保留锚节点的作用力方向与信誉，从而可以利用善意锚节点的数量和信誉优势对冲攻击行为的负面影响。

3.2 求解算法

令信誉向量 $\boldsymbol{w}_i^{'}=[r_{j_1}\ \cdots\ r_{j_\omega}]$，选举模型实质是求解方程组：

$$\boldsymbol{J}_i^{'}=\boldsymbol{w}_i^{'}\times\left[\boldsymbol{t}_{j_1}\cdots\boldsymbol{t}_{j_\Omega}\right]^{\mathrm{T}}=\boldsymbol{0} \tag{3}$$

我们知道 l_1 损失函数定义为

$$e_i^{'}=\sum_{j\in\boldsymbol{\Omega}(i)}r_j\times abs\left(\|\boldsymbol{i}-\boldsymbol{j}\|_2-\hat{d}_{i,j}\right) \tag{4}$$

从而得出 $\boldsymbol{J}_i^{'}$ 明确的数学意义，即 l_1 损失函数的 Clarke 次梯度(以下简称次梯度)。因此选举模型可被归结为 l_1 损失函数优化问题。最大熵原理指出，零知识前提下锚节点信誉值应服从均匀分布以极小化决策风险。因此在未引入信任模型时[8]，不妨假定所有的锚节点具备相同的信誉，即 $\boldsymbol{w}_i^{'}=\boldsymbol{1}$。从优化的角度看，$l_1$ 比 l_2 损失问题复杂之处在于，其非光滑性直接导致高阶梯度算法的失效。增量次梯度下降

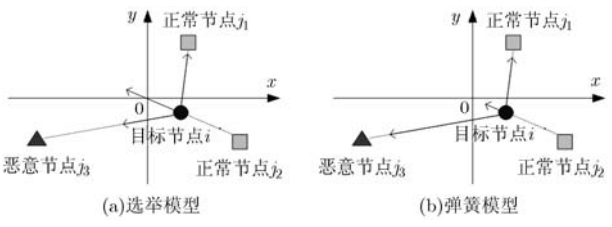


图1 选举模型的物理意义比较

算法 (Incremental Sub-Gradient Descending algorithm, ISGD)被广泛认为是求解此类可分极值不可微最优化问题的较好方法[17]。其主要思想是：在每步迭代中抽取优化函数的 m 个分量，并令因变量沿各分量函数的次梯度方向下降。当迭代初值远离点列极限时，ISGD 拥有较直接次梯度法更快的收敛速度。ISGD 的一个重要问题在于易受分量函数迭代顺序的影响，从而在收敛极优值的某个邻域内抖动。为了抑制迭代次序对准确性的负面影响，本文随机抽取损失函数的分量进行迭代。本文优化选举模型使用的 ISGD 算法细节如下：

步骤 1　监听网络端口。当收到锚节点 k 的信息，更新锚节点的传输时延 $\hat{d}_{i,k}$、坐标 $\boldsymbol{k}$ 以及锚节点集合 $\Omega(i)$，并转步骤 2；

步骤 2　从当前锚节点集合 $\Omega(i)$ 中随机抽取非空子集 $\Psi(i)$，满足 $|\Psi(i)|=\min(|\Omega(i)|,\psi)$。其中 $|\cdot|$ 运算取集合的势；ψ 是一个预定义的整数常量，且满足 $\psi\geq 1$；

步骤 3　计算本轮迭代的单位化误差[18] $e_i'(t)/|\Omega(i)|$，其中的分母项是去尺度因子，用于消除网络拓扑结构对误差的影响。如果单位化误差较上一轮迭代有所下降，则令 $\delta(t)=\min(\delta_{\max},\delta(t-1)\times h)$，否则令 $\delta(t)=\max(\delta_{\min},\delta(t-1)\times l)$。其中 $\delta_{\max}$ 与 $\delta_{\min}$ 是预定义的步长上界和下界，h 和 l 是步长增长和衰减因子；

步骤 4　从 $\Psi(i)$ 中随机抽取元素 j，令 $\boldsymbol{i}=\boldsymbol{i}+\delta(t)\times\boldsymbol{t}_j$，$\Psi(i)=\Psi(i)-\{j\}$；

步骤 5　如果 $\Psi(i)=\psi$，则输出坐标值 $\boldsymbol{i}$，否则转步骤 4。

从算法细节可以看出，选举模型的系统资源占用率极低：相较于传统算法仅需多维护一个包含少量锚节点信息的列表，并不带来任何额外的测量负载。

3.3 算法理论分析

首先讨论算法涉及的步长比例因子 h 和 l 取值的可行域。步骤 4 在计算迭代步长时引入了一个简单的误差函数负反馈比例控制器，其目的是确保算法以较大的步长快速收敛到极优值附近，并以较小的步长逐步求精。设第 t 轮迭代时单位化误差增大和减小的概率分别为 $p^+(t)$ 和 $p^-(t)$，则迭代步长 $\delta(t)$ 的数学期望：

$$\begin{aligned}E(\delta(t))=&\,p\left(\delta(t-1)<\delta_{\min}/l\right)\\&\times\left(p^-(t)h\delta(t-1)+p^+(t)\delta_{\min}\right)\\&+p\left(\delta(t-1)>\delta_{\max}/h\right)\times\left(p^-(t)\delta_{\max}\right.\\&\left.+p^+(t)l\delta(t-1)\right)\\&+p\left(\delta(t-1)\in\left[\delta_{\min}/l,\delta_{\max}/h\right]\right)\\&\times\delta(t-1)\left(hp^-(t)+lp^+(t)\right)\end{aligned}\tag{5}$$

易知当算法处于收敛过程中时单位化误差总体呈下降趋势，此时有 $p^+(t)<p^-(t)$。由式(5)可知 h 和 l 应满足 $hp^-(t)+lp^+(t)>1$，即 $(h-1)/(1-l)>p^+(t)/p^-(t)$，才能保证迭代步长概率递增；而当节点坐标收敛到极优值的某个邻域内时 $e_i'(t)$ 将往复振荡，此时有 $p^+(t)=p^-(t)$。要使得迭代步长概率递减，则应满足 $(h-1)/(1-l)<p^+(t)/p^-(t)=1$。综合节点生命周期不同阶段的需求，可估算一个实数 $\eta\in(p^+/p^-,1)$，其中 p^+/p^- 是收敛阶段单位化误差增大和减小的概率比值，并令 $h=1+\eta(1-l)$ 以兼顾收敛过程中的收敛速度和稳定状态下的计算精度。式(5)同样显示在稳定状态下距离预测精度将主要取决于 $\delta_{\min}$ 和 h，因此一般可将这两个参数适当取小以提高计算精度，而收敛速度可通过取较大的迭代步长初值来补偿。

算法的另一个重要参数是每轮迭代选取的锚节点数量 ψ，该参数决定了算法的计算复杂度。事实上在每步迭代中节点坐标都会逐次改变 ψ 次，因此 ISGD 的计算复杂度为 $O(\psi\times n)$。文献[15,19]令 $\psi=1$，即选择随机(次)梯度下降法(Stochastic (Sub)-Gradient Descending Algorithm)作为 NCS 优化算法，此时算法具有最低的计算复杂度 $O(n)$。然而在非可信环境下随机(次)梯度法存在两个不容忽视的问题：一是恶意节点可以通过增加更新信息发送频率来实施对系统的攻击；二是 l_1 损失函数的误差截断特性限制了每一步迭代中节点位移的距离，降低了算法的收敛速度。因此选取一个恰当的 ψ 值仍是十分必要的。考虑到 ISGD 更新单个分量函数的计算量极小，而其计算复杂度也仅仅随着每轮迭代选取的锚节点数量增加而线性增长，所以 ISGD 的计算代价无疑是可以接受的。

4　仿真实验

为了检验模型的速度、精度与鲁棒性，本文以经典的 Vivaldi 算法及利用 Huber 损失函数增强鲁棒性的 Robust-Vivaldi 算法[20]为基准算法进行性能对比。所有的算法均假定邻居节点数为 60 个。实验以 Planetlab 数据集[21]为仿真基础，该数据集测量了 226 个 PlanetLab 节点之间 4 h 内的传输时延。将度量空间定义为 2 维 Euclid 空间，使其能够与节点在地理上的经纬度大致重合，从而具备更加直观的物理意义[22]。信任模型或入侵检测算法的优劣并非本文分析重点，因此假定所有的交互信息均已经过前端清洗。此外，由于误差截断后 Frog-boiling 攻击表现出与传统攻击模型完全相同的特性，为了简化讨论，本文未单独分析 Frog-boiling 攻击下的系统

效能。

首先定义距离计算相对误差(Relative Error, RE)以评价系统性能[23]：

$$\mathrm{RE}_{i,j} = abs\left(d_{i,j} - \hat{d}_{i,j}\right)\Big/\hat{d}_{i,j} \times 100\% \qquad (6)$$

与之相关地，引入相对误差的 90%分位数(Ninetieth Percentile Relative Error, NPRE)作为算法整体性能评价指标[24]，以及 50%分位数(Fiftieth Percentile Relative Error, FPRE)以评价非可信环境下系统残存服务能力。

4.1 算法参数确定

选取恰当的参数是实现性能优化的重要前提。前期工作证实[18]，亚毫秒级的抖动对距离预测精度的影响极小，本文经验地取 $\delta_{\min} = 0.2$ ms；此外考虑到网络直径通常在1000 ms左右，如 PlanetLab 数据集的网络直径就仅为1450 ms，因此可以认为 $\delta_{\max} = 10$ ms能够满足收敛速度的要求。据 3.3 节对参数与性能相关性的理论分析所给出的参数选取原则，本节重点讨论 h，l 和 ψ 的选取。

首先讨论迭代步长更新策略与收敛速度的关系。3.3 节虽给出了 h 和 l 理论上的可行域，但由于 p^-/p^+ 的值是未知的，参数的较优取值仍须通过实验测算和验证。将 h 和 l 可能的取值各自分为低和高两个子区间，令 $h = 1.1$,1.5 和 $l = 0.2$,0.5 作为子区间的代表取值交叉配对进行实验，并取 $\psi = 10$，可得收敛曲线如图 2(a)所示。可以看出，实验结果与理论推导较为吻合：无论是较大的 h 亦或 l 都能够显著提升收敛速度。然而较大 h 会导致精度的下降。可以看出当 l 取相同值的条件下，h 值越小，距离预测就越精确。并且，选举模型的收敛速度并不逊色于基准算法。如当 $h = 1.5$，$\eta = 0.5$ 时，本文算法和 Vivaldi 拥有几乎相同下降速度的收敛曲线，而计算精度上则优于 Vivaldi；相比之下，Robust-Vivaldi 算法由于采用 Huber 损失函数截断了 l_2 误差，而又缺乏相应的补偿机制，导致其收敛速度相对最慢。综合考虑，我们认为 $h = 1.5$，$\eta = 0.5$ 应是较好的一组取值。

ψ 对算法性能的影响体现在图 2(b)中。可以看出，得益于每一步迭代计算量的增加，收敛速度也会随着 ψ 的增长而加快。然而值得注意的是，当 ψ 取值过小时不仅会降低收敛速度，也会带来一定的精度损失。并且，在非可信环境下过小的 ψ 也难以保证每次迭代均能抽取足够数量的正常节点对冲风险。结合计算代价的考量，我们认为 ψ 取 10 到 20 较为合理。本文后续实验均取 $\psi = 10$。

4.2 可信环境下的性能

图 3 是收敛状态下的相对误差累积分布，从图中可以分析算法距离预测的精确性。可以看出，在可信环境下选举模型的距离计算与预测性能明显优于 Vivaldi 算法，较 Robust-Vivaldi 算法也略好。例如，选举模型的 FPRE 为 7.1%，比 Vivaldi 的 9.4%和 Robust-Vivaldi 的 7.4%更低；同样地，选举模型的 NPRE 为 41.1%，远低于 Vivaldi 算法的 50.4%，也比 Robust-Vivaldi 算法的 43.5%更低。这说明，当网络趋于稳定时，选举模型的对网络距离的计算与预测精度优于基准算法。由于 Huber 损失函数实质上是 l_1 和 l_2 损失函数的拼接，可以认为 l_1 损失函数的误差截断特性是选举模型和 Robust-Vivaldi 性能较好的内在原因。

4.3 入侵容忍能力评价

非可信环境下算法的入侵容忍能力是评价系统效能的关键。本节通过构建 Inflation, Deflation 与 Oscillation 攻击来检验算法在非可信环境下的效能。

4.3.1 Inflation 攻击实验 首先通过延迟发布应答信息，并向目标节点投放一个距其极近的虚假坐标发动 Inflation 攻击。图 4 是算法在少量 Inflation 攻击(10%恶意节点)和大量 Inflation 攻击(30%恶意节点)情况下的相对误差累积分布。

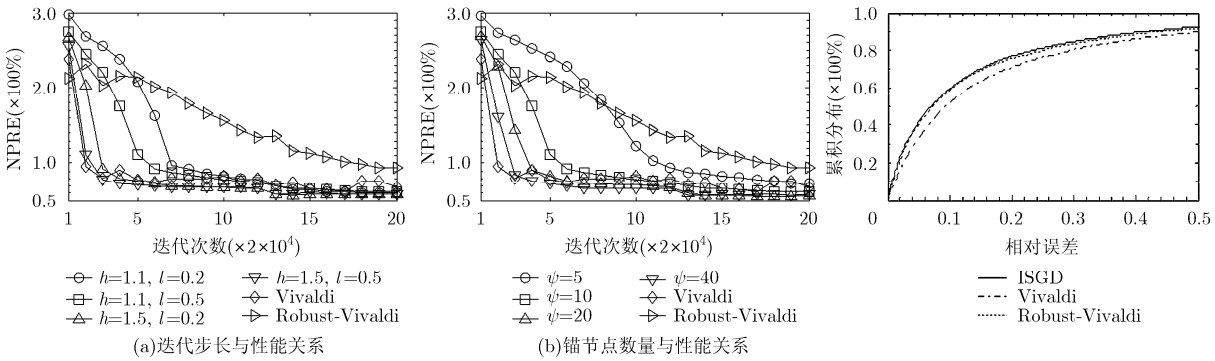
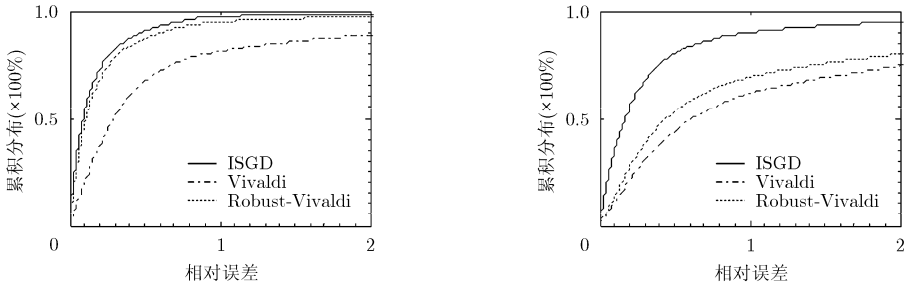


图 2 参数选取与性能的关系

图 3 可信环境下算法性能



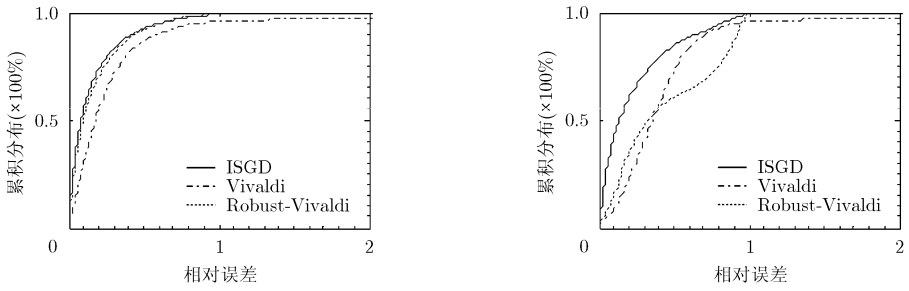
(a) 10% Inflation节点　　(b) 30% Inflation节点

图 4 抵御 Inflation 攻击效果

可以看出，选举模型的抗 Inflation 攻击能力明显优于基准算法。如图 4(a)所示，当系统存在 10%的 Inflation 节点时，选举模型的 NPRE 仍低至 9.1%，仅比可信环境下增加 2%；相应地，选举模型的 NPRE 值为 47%，仅较可信环境下升高 7.6%，算法的表现甚至比可信环境下的 Vivaldi 算法更好。反观两种基准算法，Vivaldi 算法此时的 FPRE 则高达 35.4%，而 NPRE 则大幅上升到 323%，已丧失相当程度的服务能力；而 Robust-Vivaldi 算法也有较好表现，其 FPRE 和 NPRE 分别为 11.2%和 62.2%，均稍弱于选举模型。究其原因，是因为 Inflation 攻击基本落入到 Huber 损失函数的误差截断区间，降低了 Inflation 节点的伪造信息所带来的精度损失。而由于选举模型比 Robust-Vivaldi 的误差截断区间更大，因此拥有更好的性能表现。图 4(b)是 Inflation 节点的比例增加到 30%时的相对误差累积分布。此时选举模型的 FPRE 上升到了 12.3%，而 NPRE 则上升为 100%。这意味着此时绝大部分节点距离预测误差仍在一倍以内，而一半以上的节点距离预测误差仍控制在 13%以内，算法仍能提供质量尚可的服务；而此时 Vivaldi 算法的 FPRE 达到了 93.7%，NPRE 更是高达 591%，表明其节点已完全失序，无法进行距离预测。Robust-Vivaldi 算法的性能也严重恶化：其 FPRE 为 44.9%而 NPRE 为 443%，同样不具备任何服务能力。Robust-Vivaldi 算法性能急剧下降的原因在于，虽然 Robust-Vivaldi 对大部分 Inflation 节点投送的误差进行了截断，但恶意节点数量过多且具有不小于正常节点的权值，足以冲抵正常节点的数量优势。

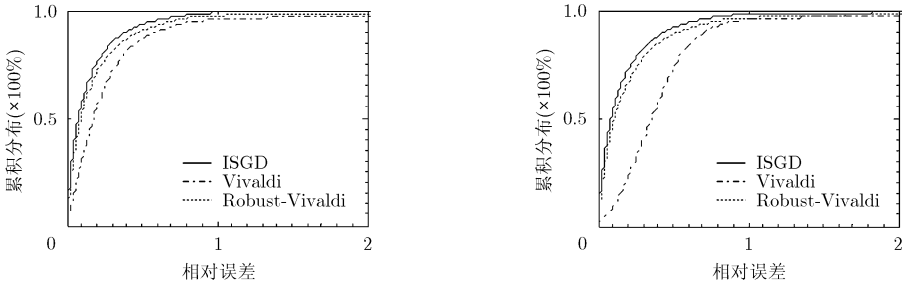
4.3.2 Deflation 攻击实验　实验采用的 Deflation 攻击试图将目标节点锁定在坐标原点位置，因此相对误差通常不超过 100%。图 5(a)显示，当存在 10%的 Deflation 攻击节点时选举模型的 FPRE 仍有 8.4%，远优于 Vivaldi 算法的 28.9%，较 Robust-Vivaldi 算法的 9.9%也略优；同时，选举模型的 NPRE 为 43.5%，同样比 Vivaldi 算法的 61.5%和 Robust-Vivaldi 算法的 44.1%更优。可以看出，面对少量 Deflation 攻击时选举模型的性能明显优于 Vivaldi 算法，略优于 Robust-Vivaldi 算法。当 Deflation 节点增加到 30%时的累积分布如图 5(b)所示。直观上两种基准算法的累积分布曲线都出现了明显的畸形，表明节点失序现象已极为严重。具体而言，选举模型的 FPRE 上升到了 13.6%, NPRE 也上升到了 65.4%；对应地，Vivaldi 算法的 FPRE 和 NPRE 则分别为 35.9%和 91.9%, Robust-Vivaldi 算法也高达 33.2%和 71.9%。考虑到 Deflation 攻击的相对误差上界为 100%，可知此时两种基准算法的节点都被压缩在原点附近，节点的区分度已十分不明显，而选举模型则仍保持着一定的节点区分能力。

4.3.3 Oscillation 攻击实验　通过向目标节点随机发送坐标和随机延迟应答的方式发动 Oscillation 攻击，相对误差累积分布如图 6 所示。实验发现选举模型抵御 Oscillation 攻击效果同样十分明显。举例而言，如图 6(a)所示，选举模型在 10%的恶意节点环境下的的 FPRE 仅为 7.8%，相较于 Vivaldi 算法的 18.1%具备明显优势，也略低于 Robust-Vivaldi 算法的 9.5%；从 NPRE 的表现来看，选举模型也只有 39.8%，比 Vivaldi 算法的 60.1%和 Robust-Vivaldi 算法的 49.1%有了明显的性能改善。当 Oscillation 攻击节点增加到 30%时的相对误差累积分布曲线如图 6(b)所示。此时选举模型的 TPRE 仅为 9.1%，而 Vivaldi 和 Robust-Vivaldi 算法则分别上升到了 35.9%和 11.2%；而选举模型的 NPRE 仅为 42.2%，同样明显低于 Vivaldi 和 Robust-Vivaldi 算法的 72.1%和 55.3%。实验表明 Oscillation 攻击几乎不能对选举模型产生影响：即使 Oscillation 节点增加到 30%，算法的 FPRE 和 NPRE 仅较可信环境下分别上升 2%和 1.1%，并不具备明显的统计学意义。究其原因，在于 Oscillation 攻击随机发送伪造数据的特点恰恰使得恶意节点的投票相互抵消。



(a) 10% Inflation节点 (b) 30% Inflation节点

图 5 抵御 Deflation 攻击效果



(a) 10% Inflation节点 (b) 30% Inflation节点

图 6 抵御 Oscillation 攻击效果

5 结论

本文在承认网络坐标系统安全问题不可避免的前提下提出了一种复杂环境中服务质量确保的新思路：首先赋予 NCS 权值向量新的物理意义，并利用投票的方式限制恶意攻击行为的影响，提出了一种具备较强入侵容忍能力的网络距离选举计算模型，将票选平衡点作为最优解，并将其归结为一类 l_1 损失函数极小化问题。针对目标函数的非光滑性，以增量次梯度算法为基本计算框架，基于误差函数负反馈比例控制器调节迭代步长，以可接受的计算代价显著提高了 NCS 的入侵容忍能力。实验结果显示，在可信与非可信环境下选举模型对网络距离的计算和预测能力均显著优于基准算法，能够有效抑制各类 NCS 攻击行为。

参 考 文 献

[1] Agarwal S, Dunagan J, Jain N, *et al*.. Volley: automated data placement for geo-distributed cloud services[C]. 7th USENIX Symposium on Networked Systems Design & Implementation, San Jose, CA, USA, Apr. 28–30, 2010: 1–16.

[2] Szymaniak M, Presotto D, Pierre G, *et al*.. Practical large-scale latency estimation[J]. *Computer Networks*, 2008, 52(7): 1343–1364.

[3] Noh Y, Lee U, Wang P, *et al*.. VAPR: void aware pressure routing for underwater sensor networks[J]. *IEEE Transactions on Mobile Computing*, 2012, 12(5): 895–908.

[4] Beaumont O, Bonichon N, Duchon P, *et al*.. Use of Internet embedding tools for heterogeneous resources aggregation[C]. 2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and PhD Forum, Anchorage, AK, USA, May 16–20, 2011: 114–124.

[5] Chen Z, Chen Y, Ding C, *et al*.. Pomelo: accurate and decentralized shortest-path distance estimation in social graphs[C]. ACM SIGCOMM, Toronto, Canada, Aug. 15–19, 2011: 406–407.

[6] Kermarrec A M, Leroy V, and Trédan G. Distributed social graph embedding[C]. The 20th ACM International Conference on Information and Knowledge Management, Glasgow, UK, Oct. 24–28, 2011: 1209–1214.

[7] Kaafar M A, Mathy L, Turletti T, *et al*.. Virtual networks under attack: disrupting Internet coordinate systems[C]. The Second ACM CoNEXT Conference, Lisbon, Portugal, Dec. 4–7, 2006: 12:1–12:12.

[8] Sherr M, Blaze M , and Loo B T. Veracity: practical secure network coordinates via vote-based agreements[C]. The 2009 Conference on USENIX Annual Technical Conference, San Diego, CA, USA, June 14–19, 2009: 13–13.

[9] Chan-Tin E and Hopper N. Accurate and provably secure latency estimation with treeple[C]. The 18th Annual Network & Distributed System Security Symposium, San Diego, CA, USA, Feb. 6–9, 2011.

[10] Kaafar M A, Mathy L, Barbkat C, *et al*.. Securing Internet coordinate embedding systems[C]. ACM

SIGCOMM, Kyoto, Japan, Aug. 27–29, 2007:61–72.

[11] Zage J and Nita-Rotaru C. On the accuracy of decentralized virtual coordinate systems in adversarial networks[C]. The 14th ACM conference on Computer and Communications Security, Alexandria, VA, USA, Oct. 29–Nov. 2, 2007: 214–224.

[12] Chan-Tin E, Heorhiadi V, Hopper N, *et al.*. The Frog-Boiling attack: limitations of secure network coordinate systems[J]. *ACM Transactions on Information and System Security*, 2011, 14(3): 27:1–27:23.

[13] Becker S, Seibert J, and Nita-Rotaru C. Securing application-level topology estimation networks: facing the frog-boiling attack[C]. Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, 2011: 201–221.

[14] Seibert J, Becker S, and Nita-Rotaru C. Securing Virtual Coordinates by Enforcing Physical Laws[C]. 2012 IEEE 32nd International Conference on Distributed Computing Systems, Macau, China, June 16–18, 2012: 315–324.

[15] Dabek F, Cox R, Kaashoek F, *et al.*. Vivaldi: a decentralized network coordinate system[C]. ACM SIGCOMM, Portland, OR, USA, Aug. 30–Sep. 3, 2004: 15–26.

[16] Donnet B, Gueye B, and Kaafar M A. A survey on network coordinates systems, design, and security[J]. *IEEE Communications Surveys & Tutorials*, 2010, 12(4): 488, 503.

[17] Nedic A and Bertsekas D. Incremental subgradient methods for nondifferentiable optimization[J]. *SIAM Journal on Optimization*, 2001, 12(1): 109–138.

[18] 王聪, 张凤荔, 刘梦娟, 等. IP 网络坐标抖动感知与慢启动抑制[J]. 电子科技大学学报, 2012, 41(6): 921–926.
Wang C, Zhang F, Liu M, *et al.*. IP-based network coordinate oscillation awareness and sow-start mitigation[J]. *Journal of the University of Electronic Science and Technology of China*, 2012, 41(6): 921–926.

[19] Liao Y, Du W, Geurts P, *et al.*. Decentralized prediction of end-to-end network performance classes[C]. The 7th ACM CoNEXT Conference, Tokyo, Japan, Dec. 6–9, 2011: 14:1–14:12.

[20] Tang L, Shen Z, Lin Q, *et al.*. Towards a Robust Framework of Network Coordinate Systems[M]. NETWORKING 2012, Springer Berlin Heidelberg, 2012: 331–343.

[21] PlanetLab dataset[OL]. http://www.eecs.harvard.edu/~syrah/nc/sim/pings.4hr.stamp.gz. 2012.5.

[22] Wang Y, Burgener D, Flores M, *et al.*. Towards street-level client-independent IP geolocation[C]. The 8th USENIX Conference on Networked Systems Design and Implementation, San Jose, CA, USA, Apr. 25–27, 2011: 27–36.

[23] Lua K, Griffin T, Pias M, *et al.*. On the accuracy of embeddings for Internet coordinate systems[C]. The 5th ACM SIGCOMM Conference on Internet Measurement. Philadelphia, PA, USA , Nov. 30–Dec. 3, 2005: 125–138.

[24] Wu S, Chen Y, Fu X, *et al.*. NCShield: securing decentralized, matrix factorization-based network coordinate systems[C]. The 20th International Workshop on Quality of Service, Coimbra, Portugal, June 4–5, 2012: 1–9.

王　聪：　男，1981 年生，博士生，研究方向为网络空间嵌入模型.

张凤荔：　女, 1963 年生，博士，教授，博士生导师，研究方向为信息安全.

杨晓翔：　男, 1978 年生，博士生，研究方向为分布式安全协议.