



基于私有云信任度量的对等网络节点安全互联模型

林 伟,郑相涵

(福州大学数学与计算机科学学院 福州 350108)

摘 要:在缺乏必要信任关系的对等网络环境中,节点的安全互联对系统的稳定运行具有重要意义。针对对等网络存在的信任缺陷,借助私有云平台在计算与存储过程中的高效性、安全性等特点,提出一种私有云协助的对等网络信任度量模型。该模型基于主观逻辑理论对连接过程中的节点可信度进行度量,针对网络环境中存在的低质量服务、节点虚假推荐及策略性欺骗等问题开展研究,提出了应对机制。实验仿真结果表明,提出的模型具有较好的可行性、有效性和动态适应性。

关键词:对等网络;私有云;信任度量;主观逻辑

doi: 10.11959/j.issn.1000-0801.2015015

Private Cloud Assistant Trust Model for P2P Secure Transactions

Lin Wei, Zheng Xianghan

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

Abstract: Secure transactions among P2P peers are critical for system stability. Considering existing security breaches, a private cloud assistant trust model for P2P session negotiation and connection was proposed. With a few characteristics during computing and storage process (e.g. high efficiency, security, neutrality), private cloud platform is capable to provide trustworthiness calculation, storage and evaluation for each peer in P2P network. Some coping mechanisms were proposed to curb malicious behaviors, such as low quality services, false recommendation and strategic fraud attaches. Simulation result shows that the proposed model has feasibility, efficiency and dynamic adaptability.

Key words: P2P, private cloud, trust evaluation, subjective logic

1 引言

对等网络环境特有的去中心化网络结构、协同计算服务模式、动态波动网络特性带来了新的安全挑战。如图1所示,首先由于中心化认证机制的缺失,在对等网络节点互联过程中,消息发送方无法判断其邻居节点是否安全可靠,同时消息接收方也很难对接收到的数据进行安全性分析;其次,节点间的交互依赖于一系列参与节点的协同计算,在源节点(节点A)与目的节点(节点B)连接过程中,

恶意中间节点能够对收到的消息进行增加、删除、修改、复制、恶意转发等操作,破坏数据的机密性、完整性,降低系统可用性,也能够通过解析获取到的消息窃取消息路径中的节点隐私^[1],如标识符、IP、端口、数据内容等;最后,对等网络是动态波动的自组织网络,任何节点都可以随时、自由地加入与退出,给消息的可靠传递与网络的稳定运行带来了不确定因素。因此,开展对等网络节点安全互联的研究,确保消息的可靠传递和系统的稳定运行,具有重要的现实意义。

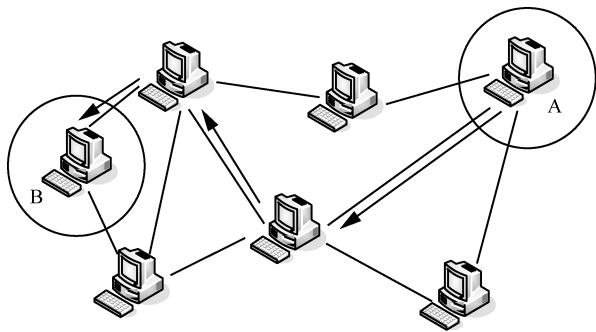


图 1 对等网络节点互联

针对以上问题,本文构建了一个私有云协助的对等网络信任度量模型,借助私有云平台在存储与计算过程中的高效性、安全性等特点,引入主观逻辑理论对节点进行信任评估,信任评估依赖节点自身经验以及其他节点的推荐信息,引入迭代推荐过滤算法筛选推荐信息,并充分考虑信任的时间衰减特性。

2 相关工作

现有网络信任模型为 P2P 网络节点安全互联提供了可参考的理论依据,主要分为两个类别:集中式信任度量和分布式信任度量。在集中式信任度量方案中,中心化的信任服务器收集各个节点在每次交易完成后的相互信任评价,并对各个节点进行信任度统一计算与存储。如 eBay^[2]采用简单的加权平均法对节点信任值进行计算;Spora 系统^[3]在 eBay 算法的基础上,引入时间加权因子,对近期的信任评价赋予更高的权值。集中式信任度量方案具有结构简单、易于实现等优点,目前广泛应用于各大电子商务交易中。但是该方案在 P2P 系统中的应用可能带来如下几个方面的限制。

- 单点故障问题。由于系统的运行过度依赖少数中心化的信任服务器,容易造成单点故障问题,影响系统的可靠性与可扩展性。
- 高复杂度信任度量算法难以实施。在规模大、连接频率高的 P2P 系统中,高复杂度的信任度量算法与更新机制可能给信任服务器带来较大负担,直接影响系统的实际运行效率。
- 接入与响应的高时延。节点的网络异构性(如移动接入)、连接频率等因素可能会大大增加信任服务器的接入与响应时延,降低终端用户的体验度。

分布式信任度量是从主观角度出发,结合信任概念对节点的行为属性、行为交互及结果进行判断,一定程度上

实现节点行为的主观可信度量。EigenTrust^[4]利用信任的传递特性,提出了一种由邻居节点间的直接信任计算全局信任的方法。在算法描述中,直接信任值高的邻居节点推荐的信任值被赋予更大的权重。PowerTrust^[5]在 EigenTrust 的基础上提出了向前看随机游走(look-ahead random walk)策略,将邻居节点的直接信任与间接邻居的推荐信任综合考虑到算法中,进一步提高了信任值计算的准确性。PeerTrust^[6]给出了类似 EigenTrust 的信任计算方法,但认为节点的直接信任值是由反馈评价、交易数量、反馈评价节点的可信度、交易属性、交易环境 5 个要素决定的。DRS^[7]考虑到节点的信任评价随时间而衰减,引入了时间衰减因子,提出了一种基于 Dirichlet 概率分布的信任计算方法,有效抑制了恶意节点在累积一定信任度后对网络或其他节点施加的恶意行为。相比于集中式信任度量机制,分布式信任度量方案不存在单点故障问题,具有更高的可靠性与可扩展性,而且将信任算法的计算分配给所有的网络节点,因此在系统实际应用中不受信任算法复杂度的影响。但是,该方案在 P2P 系统的扩展应用中,也普遍存在以下两方面的局限。

- 间接信任度采集过程繁琐。由于缺乏中心化的管理模式,节点间接信任度的获取需要依靠大量的数据发送与采集工作,这在增加节点负担的同时也可能造成较高的时延。
- 分布式数据存储的安全性不高。虽然上述方案采用各种算法对信任数据进行分布式存储,但却很难保障数据在异地存储过程中的机要性、完整性以及访问过程的便利性,可能直接影响系统的安全性与实际应用性能。

近年来,云计算技术的发展及其在安全领域的广泛应用为 P2P 信任机制的建立提供了一条新思路。一方面,云计算平台融合了分布式计算、负载均衡等概念与技术特点^[8,9],克服了集中式信任模型方案无法解决的单点故障难题,并能够为大规模终端用户提供高性能计算、随时随地的网络异构接入等服务;另一方面,在公有云安全技术尚未成熟的当前阶段,作为面向客户个性化定制的私有云平台^[10],能提供对数据、安全性和服务质量的有效控制,可以有效解决分布式信任模型方案在数据存储与安全领域的局限性。

本文提出了一种私有云协助的 P2P 信任模型,它具有如下特点。

- 信任度量基于主观逻辑理论,算法复杂度低。



- 私有云协助扩展信任模型,借助私有云平台在存储与计算过程中的高效性、安全性等优势,保证历史交易记录数据存储与信任计算过程的安全、可靠。
- 信任数据采用本地与云平台双端存储,信任计算时优先采用本地存储信任数据,本地数据信息不足以进行信任计算时,将计算转移至云平台进行,提高信任度量准确性的同时兼顾运行效率。
- 信任计算依赖自身经验与其他节点的推荐,动态赋予权重,并提出一种推荐过滤算法,遏制节点的虚假推荐恶意攻击行为。
- 考虑信任随时间而衰减的特性,引入时间权重因子,提升信任度量的准确性和模型的动态适应能力。

3 信任管理模型

本文提出的信任模型如图2所示,主要包含4个模块,具体介绍如下。

(1)本地信任维护模块

该模块负责本地交易记录的存储、更新,并将本地记录周期上传至私有云平台。假设节点A为服务请求者,节点B为服务提供者,A与B的交互记录可以表示为 $H_A(B) = \{H_1, \dots, H_n\}$,每个分量 H_i 代表A与B的单次交易记录。 H_i 可以表示为一个三元组 $\langle e_i, s_i, d_i \rangle$,其中 e_i 为交互的评价,1表示满意,0表示不满意, s_i 为交易的类型, d_i 为交易发生的时间。随着时间的推移,同一个节点提供服务的质量可能发生变化,而越是最近发生的交互在信任计算中所占的权重越大。

(2)云端信任维护模块

该模块存储网络所有节点上传的交互记录,这些记录

在云端信任计算时作为推荐数据使用。

(3)本地可信度量模块

该模块利用本地历史交互记录进行直接信任计算,模块首先对本地已有交互记录进行评估,只有本地记录足够充分时才进行本地信任计算。

(4)云端可信度量模块

一旦本地交互记录不够充分,信任计算需借助私有云平台中存储的大量推荐数据,为防止虚假推荐对信任计算的影响,推荐数据需进行相应过滤。

4 信任计算

参考文献[11]中,Jøsang等人在 β 分布的基础上,引入证据空间(evidence space)和观念空间(opinion space),提出了基于主观逻辑(subjective logic)的信任度量模型。本文的信任计算便是在主观逻辑理论基础上的相应扩展。

4.1 本地信任计算

当节点A试图与节点B交互时,它要基于本地记录进行信任计算,以判断节点B是否可信。

根据主观逻辑理论,节点A对节点B的主观信念可以用四元组 $\omega_b^a = (b, d, u, a)$ 表示。其中 b, d, u 分别表示节点A对节点B的信任度、不信任度和不确定度,且满足 $b + d + u = 1$; a 为基率且 $a \in [0, 1]$,用于计算一个信念的概率期望值。信念的概率期望值计算如式(1)所示。

$$E(\omega_b^a) = b + au \quad (1)$$

因此,基率 a 直接决定了不确定度 u 对概率期望值计算所起的作用。

节点A对节点B的本地信任值用 $T_A^L(B)$ 表示,它代表节点B能够为节点A提供满意服务的概率。主管信念四

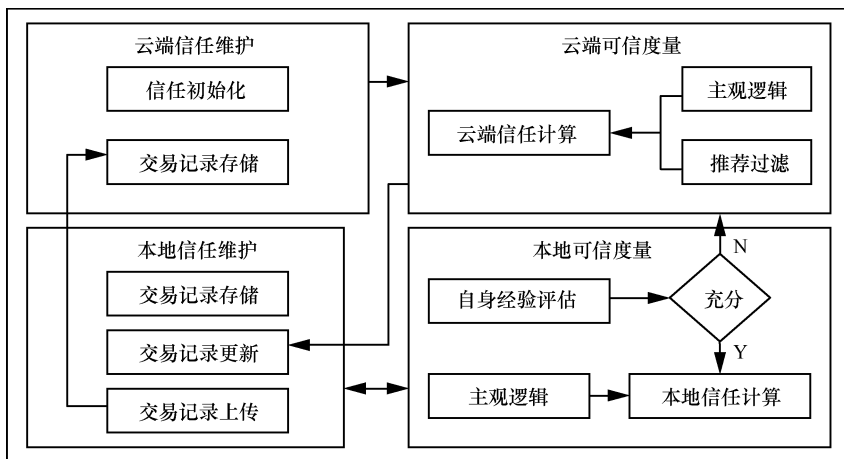


图2 信任模型体系

元组中, a 为变量, b 、 d 、 u 的取值分别为:

$$b = \frac{n_s}{n_s + n_u + C} \quad (2)$$

$$d = \frac{n_u}{n_s + n_u + C} \quad (3)$$

$$u = \frac{C}{n_s + n_u + C} \quad (4)$$

其中, C 为常量, n_s 和 n_u 分别表示节点 A 与节点 B 的交互记录中满意和不满意交互的次数。因此, 信任度计算可根据式(5)进行。

$$T_A^d(B) = E(\omega_b^A) = b + a_u = \frac{n_s + aC}{n_s + n_u + C} \quad (5)$$

4.2 云端信任计算

一旦本地记录不充分, 可能导致信任计算结果不准确, 此时应将计算转移至拥有大量交互记录的私有云平台。

4.2.1 节点自身经验置信度计算

使用式(5)计算信任度将导致不同的交互记录获得相同信任度的问题。受参考文献[12]的启发, 本文引入“Confidence”变量来描述本地信任计算的置信度, 记为 $Conf$, 通过 β 分布的方差计算得到:

$$Conf = 1 - Var(X) \quad (6)$$

$$Var(X) = \frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)} = \frac{(n_s + aC)(n_u + aC)}{(n_s + n_u + 2aC)^2(n_s + n_u + 2aC + 1)} \quad (7)$$

其中, α 和 β 为满足 β 分布的两个参数。表 1 比较了当 $a=0.5$, $C=2$ 时不同交互次数的置信度, 虽然不同的交互记录数将可能计算出相同的信任度, 然而随着交易次数的增多, $Conf$ 值将越来越大, 即信任计算结果将更加准确。

表 1 不同交互次数置信度比较

n_s	n_u	$T_A^d(B)$	$Var(X)$	$Conf$
4	1	0.714 3	0.123 4	0.987 6
9	3	0.714 3	0.009 2	0.990 8
14	5	0.714 3	0.007 1	0.992 9
19	7	0.714 3	0.005 7	0.994 3
24	9	0.714 3	0.004 8	0.995 2

本文提出的方案首先对节点自身信任数据进行 $Conf$ 值计算, 如果 $Conf$ 值过低, 则认为当前本地数据不充分, 此时将计算转移至拥有更多交互记录的私有云平台。

4.2.2 云端信任计算

一旦本地记录不充分, 信任计算将需要借助云端存储的大量推荐数据。云端计算信任值用 $T_A(B)$ 表示, 可采用

式(8)计算得出。

$$T_A(B) = \gamma T_A^d(B) + (1-\gamma) T_P^r(B) \quad (8)$$

其中, $\gamma=1-\rho^n$ 表示信任权重, $\rho \in [0,1]$ 为信任权重因子, n 为节点 A 与节点 B 的直接交互次数。因此节点 A 与节点 B 的直接交互经验越多, 节点 A 对节点 B 的直接信任度占比越大。 $T_P^r(B)$ 为推荐信任度, P 为推荐者集合。假设 i 为推荐者数量, n_s^m 和 n_u^m 分别表示第 m 个推荐者 D_m 的推荐信息中满意与不满意交互记录的数量, 则 $T_P^r(B)$ 可表示为:

$$T_P^r(B) = \frac{\sum_{m=1}^i n_s^m + aC}{\sum_{m=1}^i n_s^m + \sum_{m=1}^i n_u^m + C} \quad (9)$$

4.2.3 推荐信息过滤

在 P2P 中, 推荐者提供信息的准确性和诚实性无法保证, 恶意节点可能提供虚假的推荐信息执行恶意攻击^[13], 因此云端信任计算过程中的推荐信息过滤是必要的。受参考文献[14]和参考文献[15]的启发, 本文推荐过滤过程主要包括以下两个步骤。

(1) 推荐者过滤

对每个推荐者 D_m 计算 $T_A^d(D_m)$, 如果 $T_A^d(D_m)$ 大于预设阈值, 则该推荐者提供的信息是诚实的; 否则, 过滤掉该推荐者所提供的信息。

(2) 推荐信息过滤

过滤推荐者后, 为进一步保证信任计算的准确性, 推荐信息也需做相应过滤。推荐信息依据推荐者分组。假设有 i 组, 计算每一组信任值 $T_{D_m}^d(B)$, 获得平均值 $T_{ave}^d(B)$ 。比较信任值 $T_{D_m}^d(B)$ 与平均值 $T_{ave}^d(B)$, 如果 $T_{D_m}^d(B)$ 偏离平均值, 则第 m 组推荐不准确, 将其过滤。

迭代过滤算法的简要步骤如下。

步骤 1 用二元对 (n_s^m, n_u^m) 表示每组推荐信息。

步骤 2 对每组推荐信息计算信任值 $T_{D_m}^d(B)$ 。

步骤 3 根据式(10)计算平均值。

$$T_{ave}^d(B) = \frac{1}{i} \sum_{m=1}^i (T_{D_m}^d(B)) \quad (10)$$

步骤 4 判断不等式 $|T_{D_m}^d(B) - T_{ave}^d(B)| > S$ 是否成立, 其中 $S \in [0,1]$ 为预定阈值。如果不等式成立, 则第 m 组推荐是虚假的, 将之过滤; 否则, 该组推荐暂时保留。

步骤 5 重复步骤 2 到步骤 4, 直至过滤完毕。

4.2.4 交互记录时间加权

通常情况下, 近期发生的交易记录更能反映节点的当



前状态,对信任计算具有更高的价值^[6]。本文引入时间权重,对近期发生的交互记录赋予更高的权重。假设当前时间为 t_{cur} ,则时间权重为 $W_k=\omega^{t_{cur}-d_k}$, $\omega \in [0,1]$ 为时间权重因子, d_k 是第 k 条交互发生的时间。因此,信任加权计算式为:

$$T_A^d(B) = \frac{\sum_{k=1}^{n_i} W_k + aC}{\sum_{k=1}^{n_i} W_k + \sum_{k=1}^{n_i} W_k + C} \quad (11)$$

$$T_P^r(B) = \frac{\sum_{m=1}^i \sum_{k=1}^{n_i^m} W_k + aC}{\sum_{m=1}^i \sum_{k=1}^{n_i^m} W_k + \sum_{m=1}^i \sum_{k=1}^{n_i^m} W_k + C} \quad (12)$$

5 仿真实验与结果分析

5.1 仿真环境与性能指标

实验以 P2P 环境下的资源共享为应用背景,使用开源项目 openChord 模拟 P2P 环境,每个节点试图从其他节点上下载自身没有的资源,选用 Hadoop+Hbase 搭建私有云平台。实验仿真环境为 3 台 Intel Core i5 (3.2 GHz, 8 GB 内存),实验中使用了以下性能指标。

- 交互成功率:交互成功次数与总交互次数的比值。
- 识别准确率:准确识别节点的次数与总识别次数的比值。

5.2 仿真实验

实验中设置了 4 种节点,具体介绍如下。

- 好节点:提供的资源和推荐信息都是真实可靠的。
- 简单恶意节点:固定以 70% 的概率提供不可靠的资源。
- 虚假推荐节点:提供虚假推荐信息。
- 策略恶意节点:先提供可靠的资源服务积攒信任度,随后提供不可靠服务。

实验基本参数见表 2。

表 2 实验基本参数

实验参数	默认值
节点总数	10 000
信任阈值	0.6
置信度阈值	0.92
信任权重因子 ρ	0.6
推荐过滤阈值 s	0.2
时间权重因子 ω	0.3
基率 a	0.5
常数 C	2

5.2.1 信任阈值的影响

本文首先研究信任阈值对交互成功率的影响,给出 4 个信任阈值,分别为 0.4、0.5、0.6 和 0.7,并假设恶意节点所占比例为 30%,实验结果如图 3 和图 4 所示。

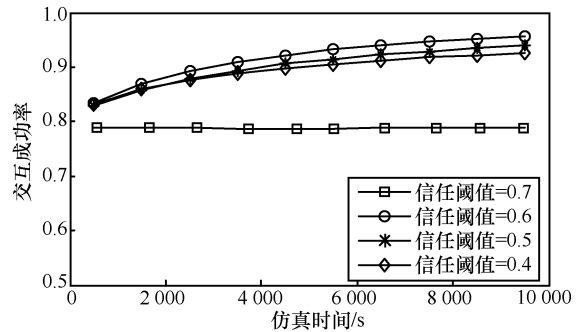


图 3 交互成功率随时间变化

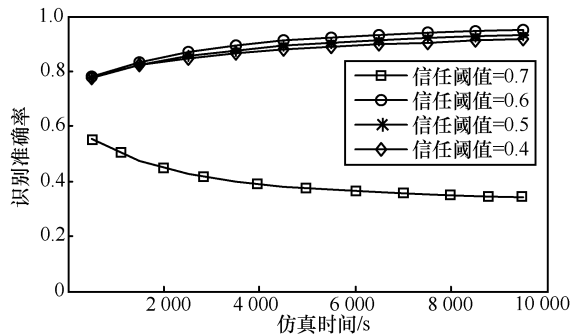


图 4 识别准确率随时间变化

从图 3 和图 4 可以看出,除了信任阈值为 0.7 的情况,交互成功率和识别准确率都随着时间以及信任阈值的增加而增加。这是因为交互记录的累积以及合适信任阈值的选取,使得模型可以有效识别恶意节点。而当信任阈值设置过大时(如 0.7),模型无法识别恶意节点。在后续实验中,将信任阈值设定为 0.6。

5.2.2 简单恶意节点比例的影响

研究简单恶意节点比例对模型的影响,仿真时间分别取 500 s、4 500 s 和 9 500 s。从图 5 可以看出,仿真时间越

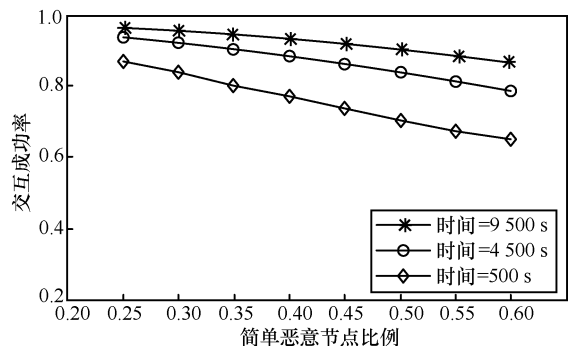


图 5 简单恶意节点比例的影响

长,交互成功率越高。此外,随着恶意节点比例的增加,交互成功率下降,而仿真时间为 9 500 s 的曲线下降幅度最小,这是因为时间越长,模型拥有足够多的记录来识别恶意节点。

5.2.3 网络大小的影响

通过设定不同的节点数量研究网络大小对模型的影响,简单恶意节点的比例为 30%。从图 6 可以看出,只要模型积累足够多的交互记录,交互成功率就始终保持在很高的水平,节点数量的改变不会对模型造成太大影响。

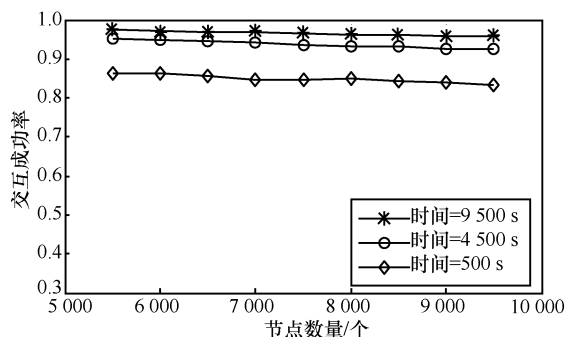


图 6 网络大小的影响

5.2.4 虚假推荐攻击抵抗

研究模型是否能够有效抵抗虚假推荐攻击。实验中给定不同的虚假推荐者比例,并对比使用迭代推荐过滤算法与不使用迭代推荐过滤算法的性能,仿真时间为 10 000 s。从图 7 可以看出,随着虚假推荐者比例的增加,两种情况的交互成功率都明显下降,但是前者的交互成功率大大高于后者的交互成功率。因此推荐过滤算法可有效抵抗虚假推荐攻击。此外,当虚假推荐节点比例不超过 35%时,模型的有效性最佳。

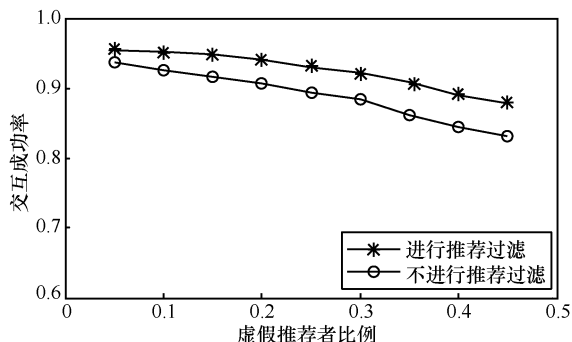


图 7 虚假推荐节点比例的影响

5.2.5 动态行为攻击抵抗

研究模型能否有效抵抗动态行为攻击。实验假设恶意

节点在 3 500 s 前以 95% 的概率提供可靠服务,而后以 95% 的概率提供不可靠服务。本文还对比了引入时间权重与不引入时间权重的情况,策略恶意节点比例为 30%。从图 8 可以看出,策略恶意节点在积攒足够信任度后开始提供不可靠服务,交互成功率急剧下降。随着时间的增加,交互成功率也逐渐缓慢上升,这说明模型已初步具有抵抗动态行为攻击的能力。而时间权重因子的引入进一步增强了模型的动态适应性,节点的当前状态得以有效反映,因此交互成功率依旧可以维持很高的水平。

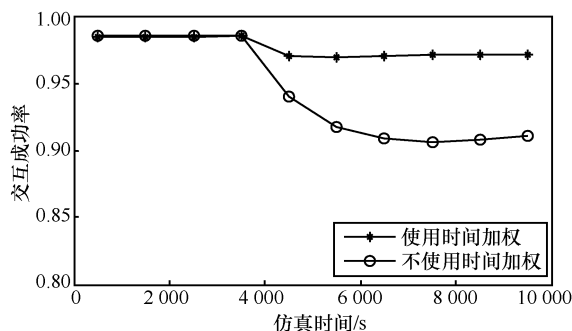


图 8 时间权重的影响

6 结束语

本文提出了一种私有云协助的对等网络信任度量模型,模型中信任度量依靠节点自身经验以及其他节点的推荐信息,合理赋予权重,使用过滤算法对推荐信息进行筛选,充分利用了网络动态性及时间相关性。模型还借助私有云平台为大规模终端节点提供了高性能计算及安全数据存储,从而有效解决了传统方案存在的单点故障问题及在数据存储与安全领域的局限性。仿真结果表明,模型能有效遏制低质量交互攻击、虚假推荐攻击、动态行为攻击等恶意攻击行为。最后,对对等网络存在的节点隔离问题进行了分析与研究。

本文的研究并未考虑 P2P 环境中存在的其他行为和因素,如数据消息在传输过程中的安全性以及更为复杂的恶意行为攻击,这些都是下一步需要完善的工作。

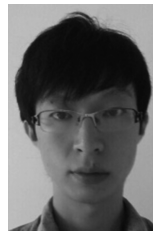
参考文献

- 1 Tomas I, Michael P, Arvind K, *et al.* A privacy-preserving P2P data sharing with one swarm. *ACM SIGCOMM Computer Communication Review*, 2010, 40(4): 111~122
- 2 eBay. <http://www.ebay.com>, 2013
- 3 Spora. <http://www.spora.ws/en>, 2013



- 4 Kamvar S D, Schlosser M T, Garcia-Molina H. The eigentrust algorithm for reputation management in p2p networks. Proceedings of the 12th International Conference on World Wide Web, Budapest, Hungary, 2003: 640~651
- 5 Zhou R F, Hwang K. Powertrust: a robust and scalable reputation system for trusted peer-to-peer computing. IEEE Transactions on Parallel and Distributed Systems, 2007, 18(4):460~473
- 6 Li X, Ling L. Peertrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transaction on Knowledge Data Engineering, 2004, 16(7):843~857
- 7 Jøsang A, Haller J. Dirichlet reputation systems. Proceedings of International Conference on Availability, Reliability and Security, Vienna, Austria, 2007:112~119
- 8 Armbrust M, Fox A, Griffith R. A view of cloud computing. Communications of the ACM, 2010, 53(4):50~58
- 9 罗军舟, 金嘉晖, 宋爱波. 云计算: 体系架构与关键技术. 通信学报, 2011, 32(7): 3~17
Luo J Z, Jin J H, Song A B. Cloud computing: architecture and key technologies. Journal of Communications, 2011, 32(7): 3~17
- 10 Basmadjian R, De Meer H, Lent R, *et al.* Cloud computing and its interest in saving energy: the use case of a private cloud. Journal of Cloud Computing, 2012, 1(1): 1~25
- 11 Jøsang A, Hayward R, Pope S. Trust network analysis with subjective logic. Proceedings of the 29th Australasian Computer Science Conference, Hobart, Australian, 2006: 85~94
- 12 Denko M K, Sun T, Woungang I. Trust management in ubiquitous computing: a bayesian approach. Computer Communications, 2011, 34(3):398~406
- 13 Quercia D, Hailes S, Capra L. B-trust: bayesian trust framework for pervasive computing. Proceedings of 4th International Conference, iTrust, Pisa, Italy, 2006: 298~312
- 14 Teacy W T, Patel J, Jennings N R, *et al.* Coping with inaccurate reputation sources: experimental analysis of a probabilistic trust model. Proceedings of the 4th International Conference on Autonomous Agents and Multiagent Systems, Utrecht, Netherlands, 2005: 997~1004
- 15 Whitby A, Jøsang A, Indulska J. Filtering out unfair ratings in bayesian reputation systems. Journal of Management Research, 2005, 4(2): 48~64
- 16 Sun Y L, Han Z, Yu W, *et al.* A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks. Proceedings of the 25th IEEE International Conference on Computer Communications, Barcelona, Spain, 2006: 1~13

[作者简介]



林伟,男,福州大学数学与计算机科学学院硕士生,主要研究方向为云计算应用。

郑相涵,男,博士,福州大学数学与计算机科学学院副研究员,主要研究方向为云计算、大数据挖掘及新一代网络技术。

2015015-7

(上接 2015031-5)

- Zhang P, Wu L N, Miao P. Realization method for EBPSK multi-carrier based on time-division. Journal of Southeast University (Natural Science Edition), 2014, 44(2): 227~231
- 9 陈志敏, 吴乐南, 陈贤卿. 用于多路 MCP-EBPSK 信号解调的冲击滤波器组设计. 信号处理, 2012, 28(8): 1063~1068
Chen Z M, Wu L N, Chen X Q. The impacting filter bank design for MCP-EBPSK multicarrier demodulation. Signal Processing, 2012, 28(8): 1063~1068
- 10 黄铭波. 基于软件无线电的 EBPSK 调制抗干扰研究 (硕士学位论文). 东南大学, 2014
Huang M B. Anti-interference studies of EBPSK modem based on software defined radio (master dissertation). Southeast University, 2014
- 11 Soroushnejad M, Geraniotis E. Performance comparison of different spread-spectrum signaling schemes for cellular mobile radio networks. IEEE Transactions on Communications, 1992, 40(5): 947~956
- 12 Mimura K, Okada M. Generating functional analysis for iterative CDMA multiuser detectors. IEEE Transactions on Information Theory, 2014, 60(6): 3645~3670
- 13 苗圃, 吴乐南, 张鹏. 扩展二元相移键控调制信号的多路传

输. 电波科学学报, 2013, 28(6):1033~1040

Miao P, Wu L N, Zhang P. On multi-carrier transmission of extended binary phase shift keying modulated signals. Chinese Journal of Radio Science, 2013, 28(6): 1033~1040

[作者简介]



张鹏,男,东南大学信息科学与工程学院博士生,主要研究方向为通信信号处理。

吴乐南,男,东南大学信息科学与工程学院教授、博士生导师,东南大学多媒体技术研究所所长,江苏省数码技术工程研究中心主任,主要研究方向为通信信号处理和多媒体信息处理。

2015031-6