文章编号:1001 - 9081(2009)02 - 0503 - 04

DrTrust:一种非结构化 P2P 网络信任模型

张云昌,陈建新,陈珊珊
(南京邮电大学 计算机学院,南京 210003)
(zhangyunchang@163.com)

摘 要:P2P 网络的动态性、匿名性和自治性带来许多安全问题,传统的结构化的 P2P 信任模型并不能很好的适应对等网络环境。提出了一种应用于非结构化 P2P 网络中的信任模型——DrTrust。该模型充分利用直接信任值和推荐信任值相结合方式的优点,实现了精确计算信任值,并采用分布式存储方式和激励、惩罚机制分别存储和更新信任值。仿真结果表明,DrTrust 在准确计算节点信任值和抑制恶意节点行为等问题上较已有的信任模型有一定的改进。

关键词:非结构化;P2P 网络;信任模型;激励机制;惩罚机制
中图分类号: TP393 **文献标志码**:A

DrTrust: A trust model in unstructured P2P network

ZHANG Yun-chang, CHEN Jian-xin, CHEN Shan-shan
(*College of Computer, Nanjing University of Posts and Telecommunications, Nanjing Jiangsu* 210003, *China*)

Abstract: The dynamics, autonomy and anonymity of the P2P network cause many security problems. The traditional trust model in structured P2P network can not satisfy the P2P environment commendably. In this paper, a trust model named DrTrust in unstructured P2P network was proposed, which was based on direct and recommended trust scheme. It takes advantage of the combination of the direct trust and recommended trust to calculate the trust accurately, using distributed way to store trust value and incentive and punishment mechanism to update trust value. The experimental results prove that DrTrust outperforms the current trust models in accurate trust computation and the inhibition to the malicious peers.

Key words: unstructured; P2P network; trust model; incentive mechanism; punishment mechanism

0 引言

随着 P2P 技术的迅速发展,P2P 网络提供服务的安全性和可靠性成为重要问题。一些传统的安全技术并不能很好解决 P2P 网络认证、授权和保密通信等问题。可信计算,作为这种分布式网络安全问题解决方案应运而生。

在可信计算中,信任[1]是指在不断的交互过程中,某一实体逐渐动态地形成对另一实体的评价,这个评价用来指导该实体下一步的行为。在 P2P 网络中,信任指一个节点对另一节点所提供服务的相信程度,并以此作为选择服务的依据。近几年出现了许多 P2P 可信计算模型,可分为结构化的和非结构化的信任模型。由于结构化的信任模型在节点定位和信任存储方面有很高的效率,所以得到长足的发展,典型的如基于能量迭代的 EigenTrust[2]、基于声望的 PeerTrust[3]和基于幂率分布的 PowerTrust[4]模型。

EigenTrust 模型建立了一个类似于 Gnutella 的纯分布式的文件共享信任网络,它建立信任矩阵,通过给每个节点设置一个节点管理者计算信任矩阵的特征向量获得节点信任值,是一种基于交易记录的信任模型。PeerTrust 将信任值的计算建立在五个因素之上,通过收集其他节点的信任反馈来进行加权,并计算信任值。PowerTrust 根据幂率分布的特性,通过贝叶斯方法获得节点的本地信任值,然后通过分布式的排队机制产生超级节点,用超级节点来管理整个网络,获得全局信任值。

在非结构化的 P2P 信任模型中,网络拓扑没有严格定义,信任值的存储同拓扑结构没有任何联系。非结构化 P2P 的信任模型[5]是一个二进制信任模型,节点只存储与之交易过的不信任节点的信息,通过查询节点过去行为获得节点的不信任度,这种方法很容易造成节点惰性。Credence 系统[6]采用基于对象信誉的方法,节点通过 gossip 过程收集其他节点的推荐,使用 Pearson 相似系数作为节点推荐的衡量标准,赋予其他节点的推荐以权重,并对所收集的推荐进行两次抽样,由于采用 gossip 过程,需要对推荐信息进行加密和解密验证,带来了很大开销,而且没有解决“搭便车”问题,也没有考虑到邻居节点的选取。

本文提出用于非结构化 P2P 网络中的信任模型 DrTrust,通过直接信任值和向友元节点发起推荐请求获得推荐信任值,全面搜集信任信息,计算信任值,采用激励机制有效地解决了节点惰性问题,惩罚机制抑制了恶意节点的行为,分布式的存储方式更适合非结构化的 P2P 网络,也进一步提高了信任的存储安全。

1 相关工作

在基于信任的 P2P 网络中应该建立两种机制,一个对信任值进行计算,另一个对信任值进行管理。但是,很多模型在

收稿日期:2008 - 08 - 19;**修回日期**:2008 - 10 - 06。 **基金项目**:国家自然科学基金资助项目(60873231);江苏省自然科学基金资助项目(08KJB520006);江苏省研究生培养创新工程项目(CX07B_109z);南京邮电大学青蓝计划项目(XK0070906052)。

作者简介:张云昌(1984 -),男,陕西咸阳人,硕士研究生,主要研究方向:可信计算、计算机通信与网间互连; 陈建新(1973 -),男,江苏南通人,博士,主要研究方向:通信网络协议、传感器网络; 陈珊珊(1980 -),女,安徽安庆人,博士,主要研究方向:分布式计算、网络安全。

上述两个问题上是相互独立的，一个完整的解决方案应该同时解决这两个问题。本文提出的信任模型 DrTrust 包括：

可信计算模型(Trust Computing Model，TCM) 解决如何准确地表述、度量和计算信任值的问题。现有的计算模型基本可以分为两类：一是基于直接交易的信任值，另一种是基于推荐的信任值。我们采用的是将两者结合的方式。

可信管理模型(Trust Management Model，TMM) 解决如何存储和更新信任值的问题。现有的大部分的信任模型都需要一个中心服务器来存储和处理信任信息，这样虽然能够有效抑制恶意节点的行为，但是容易造成单点失效和增加中心服务器的负担。我们采用分布式的存储和更新机制。

2 P2P 可信计算模型 TCM

下面是 DrTrust 中的一些记号。

1) $DT(p_i,p_j)$：直接信任值，表示节点节 p_i 对节点 p_j 的直接信任值，是节点 p_i 与节点 p_j 直接交易的历史记录计算的结果。

2) $RT(p_i,p_j)$：推荐信任值，p_i 的友元节点推荐的 p_j 的信任值。

3) $T(p_i,p_j)$：信任值，p_i 对 p_j 的最终信任值，依此判断节点服务的优劣。

节点 p_i 对节点 p_j 的信任值 $T(p_i,p_j)$ 由两部分组成：一个是 p_i 和 p_j 直接交易信任值 $DT(p_i,p_j)$；另一个是 p_i 的友元节点的推荐信任值 $RT(p_i,p_j)$。

2.1 DrTrust 系统架构

图1是有 n 个节点的 DrTrust 的系统架构，每个节点维护一张交易列表(Transaction List，TL)[6]，存储与该节点有过直接交易的节点每次交易的评价值。为了计算目标节点的信任值，请求节点先查询自己的交易列表，获得目标节点的直接信任值，然后通过过滤交易列表，构建友元列表(Friend List，FL)，并向友元列表中的节点发送推荐请求，这些节点响应推荐请求，反馈推荐信任值，由信任计算模块进行计算，最终得到目标节点的信任值。安全接口保证节点之间的安全通信，发送方可以将发送的消息进行加密和签名，接收方通过认证和解密消息，从而保证信任信息的安全交互。

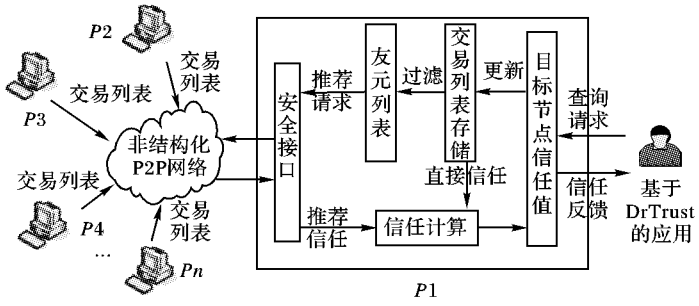

图1 DrTrust 系统架构

2.2 $DT(p_i,p_j)$ 的计算

假如 p_i 有与 p_j 最近 n 次的交易信任评价，用一个向量记为 $S_{ij}=\{S_{ij}^1,S_{ij}^2,S_{ij}^3,\cdots,S_{ij}^n\}$，$S_{ij}^k$ 代表最近的第 k 次交易的评价值，S_{ij}^1 是最近的一次交易的评价值。根据这些交易记录可以计算目标节点 p_j 的直接信任值 DT：

$$DT(p_i,p_j)=\begin{cases}\dfrac{\lambda S_{ij}^1+\lambda^2 S_{ij}^2+\lambda^3 S_{ij}^3+\cdots+\lambda^n S_{ij}^n}{\lambda(1-\lambda^n)/(1-\lambda)}, & n\neq 0\\ 0, & n=0\end{cases} \tag{1}$$

其中 $\lambda(0<\lambda<1)$ 是一个常数，大小可以根据最近的若干次交易的观察值确定。由于 λ 是界于0和1之间的数，所以随着指数的增长，它的指数次幂越来越小，从而保证了近期的交易在计算过程中占有较大的比重，交易记录时间越远，比重越小。由于分子的最大值趋于 $\lambda(1-\lambda^n)/(1-\lambda)$，保证信任值界于0和1之间。

2.3 $RT(p_i,p_j)$ 的计算

当节点 p_i 要计算节点 p_j 推荐信任值时，我们假设 $\{w_1,w_2,w_3,\cdots,w_k\}$ 代表推荐 p_j 的所有推荐节点，w_i 将自己对节点 p_j 的信任值作为推荐值反馈给节点 p_i。那么 RT 的计算公式为：

$$RT(p_i,p_j)=\begin{cases}\sum_{m=1}^{k} DT(p_i,w_m)\cdot T(w_m,p_j)/k, & k\neq 0\\ 0, & k=0\end{cases} \tag{2}$$

其中，$k(0<k<n)$ 代表推荐节点的个数，为了降低网络负载，只选取 p_i 的所有友元节点作为推荐节点，也就是友元列表 FL 中的节点。事实上，如果选择网络中的所有节点作为推荐节点，不但会增加网络负载，更重要的是很多节点的推荐值根本没有被采纳，p_i 只相信自己信任的节点推荐的信息。

2.4 $T(p_i,p_j)$ 的计算

有了 DT 和 RT 的值，就可以通过加权求和的方式计算节点 p_i 对节点 p_j 的信任值 $T(p_i,p_j)$，其计算公式为：

$$T(p_i,p_j)=\begin{cases}\delta DT(p_i,p_j)+(1-\delta)RT(p_i,p_j), & k\neq 0\\ 0.5, & k=0\end{cases} \tag{3}$$

其中 $\delta(0\leqslant\delta\leqslant 1)$ 是节点 p_i 对其推荐节点的信任参数，δ 越大，说明 p_i 对推荐节点信任度越低；反之，越高。当 $\delta=1$ 时，表明 p_i 只相信与自己直接交易的信任值，而不接受其他节点的推荐。当 $\delta=0$ 时，表明 p_i 只接受其他节点的推荐值，而不参考自己以往与目标节点的交易记录。对于一个新加入的节点，由于我们没有任何信任记录，也就没有办法判断该节点的好坏，由于的信任值都是界于0和1之间的，所以取它们的信任值为0.5。

2.5 激励与惩罚机制

前面计算假设各个节点比较积极、善意，但在实际网络中，一些节点不愿意反馈其他节点的推荐信息，还有些恶意节点通过诋毁[7]其他节点获得相对高的信任值。解决这两个问题的主要办法是采用激励机制[8-9]和惩罚机制[10]。奖励推荐合理的节点，惩罚推荐不合理的节点。

因此，我们设置一个评价标准，当推荐节点的数目比较多时，它们的推荐值近似满足二维正态分布[10]，假设 FL 中有 k 个友元节点，它们的推荐值的平均值为 μ，均方差为 σ，计算公式为：

$$\begin{cases}\mu = \dfrac{1}{k}\sum_{m=1}^{k} T(w_m, p_j) \\ \sigma^2 = \dfrac{1}{k}\sum_{m=1}^{k} T(w_m, p_j)^2 - \mu^2 \end{cases} \tag{4}$$

如式(4),对于二维正态分布函数,我们作如下的分类:

A: $[\mu - d_1 \cdot \sigma, \mu + d_1 \cdot \sigma]$

B: $[\mu - d_2 \cdot \sigma, \mu - d_1 \cdot \sigma] \cup [\mu + d_1 \cdot \sigma, \mu + d_2 \cdot \sigma]$

C: 除 A、B 之外

其中 d_1、d_2 可由系统的具体情况确定,必须满足条件: $0 < d_1 < d_2$。当节点 w_m 对节点 p_j 的推荐信任值属于集合 A 时,说明节点 w_m 非常公正地评价了节点 p_j,那么对节点 w_m 进行奖励,即在节点 p_i 的交易列表 TL 中对节点 w_m 的直接信任值乘以奖励因子 η,η 是一个稍大于1的数;当推荐信任值属于集合 B 时,说明节点 w_m 比较公正地评价了节点 p_j,不奖励也不惩罚;当推荐信任值属于集合 C 的时,说明节点 w_m 给节点 p_j 不公正的评价,作为惩罚,给节点 p_i 的交易列表 TL 中的关于 w_m 的直接信任值乘以惩罚因子 θ,$\theta \in [0,1]$。由于以上的操作都是对交易列表 TL 的更新,等价于对直接信任值的更新,如式(5):

$$DT(w_m, p_j) = \begin{cases} \eta \cdot DT(p_i, w_m), & T(w_m, p_j) \in A \\ DT(p_i, w_m), & T(w_m, p_j) \in B \\ \theta \cdot DT(p_i, w_m), & T(w_m, p_j) \in C \end{cases} \tag{5}$$

这个公式必须满足的条件是: $\eta * \theta < 1$, 因为良好的信任值需要逐渐积累,但一次不好的行为就会导致信任值大幅度下降,即信任难得易失。

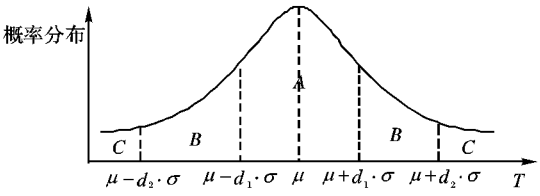

图2　推荐信任值分布图

3　P2P 可信管理模型

P2P 可信管理模型就是对信任值进行管理,具体体现在信任值的安全存储和有效更新。

3.1　直接信任值 DT

在 P2P 网络中,每一个节点维护一张交易列表 TL,它记录与该节点有过交易的节点的标识和每次交易的评价值。定义 p_i 的友元列表 FL 为:节点 p_i 交易列表 TL 中前 k 个直接信任值高的节点构成的列表。k 是 FL 的容量,其大小可以根据网络中节点的规模确定,最大值取与交易列表中的节点数相同,这时友元列表 FL 就是交易列表 TL。我们创建 FL 是出于以下考虑的:1)对于不属于友元列表中的节点其推荐值缺乏准确性;2)过滤无效推荐,提高模型的效率。

3.2　推荐信任值 RT

如图 3 所示信任计算拓扑结构,假设节点 p_i 的友元列表 $FL = \{w_1, w_3, w_n, \cdots, w_m\}$ $(0 \leqslant m \leqslant k)$。$p_i$ 发起推荐请求,请求推荐目标节点 p_j, 友元列表 FL 中的节点收到推荐请求之后,计算目标节点 p_j 的信任值,推荐节点再向它的友元节点发送请求,这样逐级推荐下去,最后逐级反馈,然后将最终信任值反馈给节点 p_i。设置一个 TTL 作为迭代的次数。

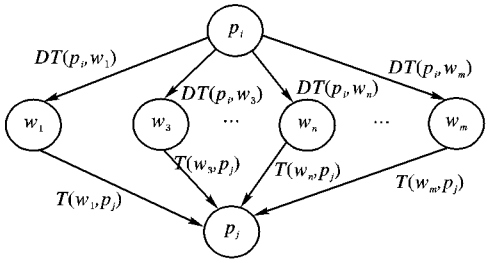

图3　P2P 信任计算拓扑结构

3.3　信任值的更新

当计算完毕目标节点的信任值后,请求节点一方面选择信任值高的节点进行服务,另一方面计算推荐值的均值和方差,确定是善意节点、一般节点或恶意节点,然后运行激励和惩罚机制,对交易列表进行更新。

当服务完毕之后,请求节点对目标节点的服务进行评价,并将结果写入本地 TL 中。如果交易列表 TL 中的数据项没有达到列表容量,则直接将此结果添加到 TL 中,如果交易列表已满,则替换最早的记录。

4　实验仿真

基于上文的信任模型,构造了多个实验场景来检测该模型的性能。应用场景是 P2P 文件共享系统。以在善意节点和恶意节点上下载文件的次数作为衡量系统好坏的标准。

设置以下节点类:

善意节点(best nodes)　提供良好和真实的文件下载服务,并给其他节点合理的评价,初始默认信任值为 1。

一般节点(common nodes)　提供较好的、相对真实的文件下载服务,初始默认信任值为 0.5。

恶意节点(malicious nodes)　总是提供恶意或伪造文件,并且一旦有下载请求,就立即响应,初始默认信任值为 0。

资源定位方式选择非结构化 P2P 网络 Gnutella 采用的泛洪法[11]。假设网络包含 1 000 个节点,随机设置 200 个节点为善意节点,600 个节点为一般节点,200 个节点为恶意节点,每个节点随机分配 10 个不同的资源。模拟进行 100 次下载实验,并记录每一次实验中分别与善意节点和恶意节点进行交易的次数,TTL 设置为 6。

4.1　DrTrust 和没有信任模型 NoTrust 的比较

初始条件:取 $\lambda = 0.1$, 奖励因子 $\eta = 1.1$, 惩罚因子 $\theta = 0.8$, $\delta = 0.5$, $d_1 = 0.5$, $d_2 = 1$。我们随机选择一个节点发起下载请求,请求一个随机文件,将 DrTrust 和没有采用任何信任模型的 NoTrust 进行比较,仿真结果如图 4 所示。

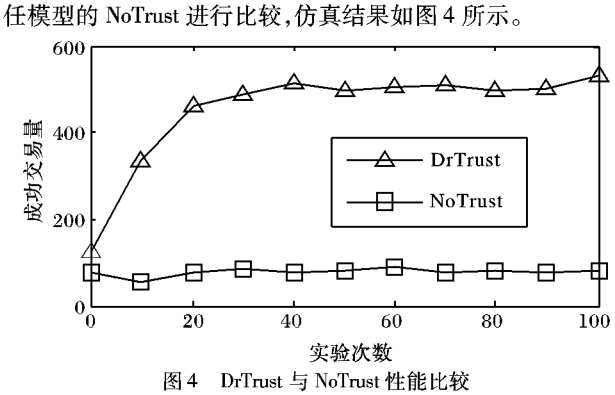

图4　DrTrust 与 NoTrust 性能比较

从图 4 中可以看出,随着交易的进行,NoTrust 的成功交易量没有明显变化,并一直保持较低的水平,而 DrTrust 的成

功交易量逐步上升,在实验次数达到40次后逐渐保持平稳。表明DrTrust能准确反映节点信任值,有效提高交易的成功率。

4.2 DrTrust和EigenTrust的比较

初始条件与4.1节设置相同。两种信任模型分别模拟从善意点和恶意节点上的进行文件下载。仿真结果如图5所示。

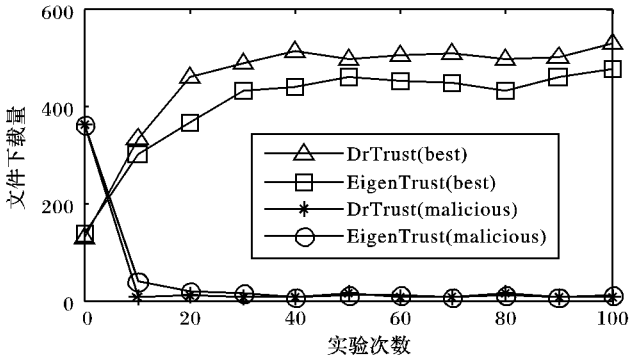

图5 DrTrust与EigenTrust性能比较

从图5可以看出,随着交易的进行,对于善意节点上文件的下载数量,DrTrust相对于EigenTrust有明显上升。而对于恶意节点上的文件下载数量,DrTrust比EigenTrust下降速度更快,并最终趋向于0。说明该模型相对于EigenTrust能更有效识别恶意节点,抑制恶意节点的行为,并能激励善意节点,提高成功交易率。

5 结语

本文从信任的定义、量化、存储和更新等方面出发,提出了一个应用于非结构化P2P网络中的信任模型DrTrust,强调了模型的可行性和合理性。仿真结果表明,该模型较好地实现了准确计算信任值和抑制恶意节点行为的功能。由于我们只采用了一个信任值衡量节点信任值,后续研究可以考虑将服务质量和节点信任结合起来衡量一个节点,并可以将DrTrust的思想用在结构化的P2P网络中。

参考文献:

[1] KALLATH, DINESH. Trust in trusted computing-the end of security as we know it[J]. Computer Fraud and Security, 2005(12): 4-7.

[2] KAMVAR S D, SCHLOSSER M T, GARCIA-MOLINA H. The Eigentrust algorithm for reputation management in P2P networks [C]// Proceedings of the 12th international World Wide Web conference. New York: ACM Press, 2003: 640-651.

[3] LI XIONG, LING LIU. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857.

[4] ZHOU RUNFANG, KAI H. PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2007, 18(4): 460-473.

[5] ABERER K, DESPOTOVIC Z. Managing trust in a peer-2-peer information system[C]// Proceedings of the 10th International Conference on Information and Knowledge Management. New York: ACM Press, 2001: 310-317.

[6] WALSH K, SIRER E G. Experience with an object reputation system for peer-to-peer file-sharing[C]// Proceedings of Symposium on Networked System Design and Implementation. Berkeley: USENIX Association, 2006: 1.

[7] ALMENAREZ F, MARIN A, DIAZ D, *et al*. Developing a model for trust management in pervasive devices[C]// Proceedings of Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops. Washington, DC: IEEE Computer Society, 2006: 267-271.

[8] GE LIANG, LUO JUNZHOU, XU YAOBIN. Developing and managing trust in peer-to-peer systems[C]// Proceedings of the 17th International Conference on Database and Expert Systems Applications. Washington, DC: IEEE Computer Society, 2006: 687-691.

[9] 孙知信, 唐益慰. 基于全局信任度的多层分组p2p信任模型[J]. 通信学报, 2007, 28(9): 133-140.

[10] SUN TAO, DENKO M K. A distributed trust management scheme in the pervasive computing environment[C]// Canadian Conference on Electrical and Computer Engineering. New York: IEEE, 2007: 1219-1222.

[11] JOSANG A, ISMAIL R, BOYD C. A survey of trust and reputation systems for online service provision[J]. Decision Support Systems. 2007, 43(2): 618-644.

[12] LIU YU-MEI, YANG SHOU-BAO, GUO LEI-TAO, *et al*. A distributed trust-based reputation model in p2p system[C]// Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. Washington, DC: IEEE Computer Society, 2007: 294-299.

[13] 陈贵海, 李振华. 对等网络: 结构、应用与设计[M]. 北京: 清华大学出版社, 2007.

(上接第502页)

3 结语

本文通过深入理解BSOL算法的核心思想,分析了该算法的优缺点,并提出了一种带布鲁姆过滤器的折半层次搜索包分类算法,即BSOLBF算法。BSOLBF算法继承了BSOL算法的原有特性,并能在hash冲突较大或者hash装载因子过大的情况下,提升算法的性能。经过仿真测试,设定hash装载因子为0.75和0.69,在规则集为30万条时,BSOLBF算法在搜索时间上要优于BSOL算法,数据包在规则库中的命中率越低优势越明显。

参考文献:

[1] 王永纲, 石江涛, 戴雪龙, 等. 网络包分类算法仿真测试与比较研究[J]. 中国科学技术大学学报, 2004, 34(4): 400-409.

[2] BABOESCU F, SINGH S, VARGHESE G. Packet classification for core routers: is there an alternative to CAMs[EB/OL]. [2008-06-23]. http://www.ieee-infocom.org/2003/papers/02_02.PDF.

[3] LU HAIBIN, SAHNI S. O(logW) multidimensional packet classification[C]// IEEE/ACM Transactions on Networking. New York: ACM, 2007: 462-472.

[4] DHARMAPURIKAR S, KRISHNAMURTHY P. Longest prefix matching using bloom filters[C]// IEEE/ACM Transactions on Networking. New York: ACM, 2006, (2): 201-212.

[5] ERGUN F, MITTRA V. A dynamic lookup scheme for bursty access patterns[C]// Proceedings of the IEEE INFOCOM. San Francisco: IEEE Computer Socity Press, 2001: 1444.

[6] 谢鲲, 张大方, 文吉刚, 等. 布鲁姆过滤器代数运算探讨[J]. 电子学报, 2008(5): 869.