基于流量优化的包标记 IP 追踪策略研究*)

周 曜[1] 徐长江[2] 徐 佳[1] 刘凤玉[1]

(南京理工大学计算机科学与技术学院 南京 210094)[1] (海军兵种指挥学院 广州 510430)[2]

摘 要 传统的攻击源追踪方案在面对大规模 DDoS 攻击时,重构路径的收敛速度往往过慢。文中提出一种根据 DDoS 流量分布优化的随机包标记策略 OMS(Optimized Marking Scheme),该策略通过在 IP 报头中插入控制信息,使标记包采样概率在攻击路径上随终点的距离递增,从而更远处的标记包能够以更高的概率到达终点。仿真试验的结果表明,OMS 收敛速度较以往的方案有了明显的提高。

关键词 DDoS,攻击源追踪,流量分布

Traffic-based Optimized Marking Scheme for IP Traceback

ZHOU Yao[1] XU Chang-jiang[2] XU Jia[1] LIU Feng-yu[1]

(Department of Computer, Nanjing University of Science and Technology, Nanjing 210094, China)[1]

(Naval Arms Command Academy, Guangzhou 510430, China)[2]

Abstract Traditional IP traceback schemes can not trace the attacking sources quickly enough when facing large-scale DDoS attack. This paper presents an Optimized Marking Scheme(OMS) based on the characteristic of DDoS traffic distribution. This sheme inserts some controlling informaton into the marked packets' headers, which makes the sampling probability of such packets keep increasing along with the marking router's distance to the destination. Thus, the packets from farer routers where the DDoS traffic is lower can reach the destination with larger probability, which improves the speed of tracing. Simulation results show that OMS is much more efficient than other traditional schemes.

Keywords DDoS, IPtraceback, Traffic distribution

1 引言

寻找匿名分布式拒绝服务攻击(DDoS)的源点是网络安全领域中的研究难点和热点,我们称之为攻击源追踪问题。

研究人员提出了多种方案,如进入诊断[1](input debugging)、受控洪流[2](controlled flooding)、日志挖掘[3](data mining based on logging)、ICMP 跟踪[4](ICMP traceback messages)、代数方法[5](algebraic approach)、随机包标记法[6,7](probabilistic packet marking),等等。以上方法从不同方面指出了对攻击源追踪问题的解决方案,但均有局限性。进入诊断和受控洪流方法只能用在 DDoS 攻击的发生阶段,如果攻击结束,这两类方法将失去作用。日志挖掘虽然在攻击发生后也能构造攻击路径,但需要在攻击路径上的各路由器端存储大量的数据包信息,增加路由器的处理负担。ICMP 跟踪法与包标记法相似,存在的最大问题是不能判别 ICMP 跟踪消息包是路由器发送的还是由攻击者发送的。文献[6,7]中提出的随机包标记法较好地解决了以上问题,使之既能在攻击发生阶段起作用,又能在攻击停止后用于发现攻击路径。但该方法也存在当 DDoS 攻击源数目众多时收敛速度较慢和误报率较高的缺陷。

本文在 FMS[6] 和 AMS[7] 的基础上,提出了适应 DDOS 流量分布的优化包标记策略(Optimized Marking Scheme, OMS),该策略在标记时加入控制信息,使标记包到达终点的概率随距离递增,在流量较小处有较大的采样概率,从而能够更好地适应实际环境中的 DDoS 流量分布,提高整个追踪系统的性能。

2 现有包标记法的缺陷

FMS 在攻击包的传输路径上的每个路由器处按固定的概率随机标记经过的数据包,当被攻击者收集到足够多的数据包后,它可以根据里面的标记信息重构出攻击的路径。AMS 采用了 FMS 的思想,所不同之处在于标记的内容。

在面对大规模的 DDoS 攻击时,它们都面临着重构攻击路径过慢的问题,其原因是由于当 DDoS 的规模很大时,在攻击发起端往往不需要太多的数据包就可以在被攻击处达到拒绝服务所需的流量,而上述几种方案为了降低路由器的计算成本,标记概率往往取得很小,这样为了达到重构路径所需的标记包数量,在靠近攻击源的地方就需要很长的时间来收集数据包,当数量不够时,甚至会产生误报的现象。

定理 1 数据包在传输路径上所经过的路由器个数为路径长度,若长度为 d 的路径上每个路由器都按概率 p 随机地在报文中标记自己的地址,则重构出攻击路径所需包的数目 X 的期望值 $E[X]$ 满足以下条件

$$\frac{1}{p(1-p)^{d-1}}\leqslant E[X]<\frac{\ln(d)+\gamma}{p(1-p)^{d-1}}$$

其中 γ 是欧拉常数,$\gamma\approx 0.577$。

证明:设 $L=(A\rightarrow R_1\rightarrow R_2\rightarrow\cdots\rightarrow R_{d-1}\rightarrow R_d\rightarrow V)$ 为长度为 d 的攻击路径,A 和 V 分别为源点和终点,R_i 为路径上的中间路由器,易见某个包被 R_i 采样(被标记且在到达 V 前未被重新标记,下同)的概率 $P_i=p(1-p)^{d-i}$。

由于 $1-p$ 小于 1,故 P_i 与 i 成正比关系,即在 R_1 处 P_i 最小,为 $p(1-p)^{d-1}$,所以

$$E[X]\geqslant\frac{1}{p(1-p)^{d-1}} \tag{1}$$

设 $p_s=\sum P_i/d$ 为整个路径上的平均采样概率,由于 P_i 随 i 递增,因此 $p_s>P_1=p(1-p)^{d-1}$。设 F_i 为被 R_i 采样的包,若 F_i 未被之前的 $i-1$ 个路由器采样,则定义 F_i 采样成功。记 X_i 为从 F_i 采样成功到 F_{i+1} 采样成功后所需要的包数,

*)国家自然科学基金资助项目(60273035)。周 曜 博士生,主要研究方向为信息安全与移动自组织网络;徐长江 博士生,主要研究方向为计算机仿真;徐 佳 博士生,主要研究方向为拥塞控制与网络管理;刘凤玉 教授,博士生导师,主要研究领域为网络安全、软件性能保持和多媒体。

易见

$$X=\sum_{i=0}^{d-1}X_i$$

在 F_i 采样成功后之后每个包采样成功的概率 $p_i=\frac{d-i}{d}$

$\sum P_i=(d-i)p_s$，并且 X_i 符合 p_i 上几何分布，故 $E[X_i]=\frac{1}{p_i}=\frac{1}{(d-i)p_s}$，且

$$E[X]=\sum_{i=0}^{d-1}E[X_i]=\frac{1}{p_s}\sum_{i=0}^{d-1}\frac{1}{d-i}=\frac{1}{p_s}\sum_{i=1}^{d}\frac{1}{i}<\frac{H_d}{p(1-p)^{d-1}}$$

其中 H_d 为 d 阶调和级数，因为

$$\lim_{d\to\infty}H_d=\lim_{d\to\infty}\sum_{i=1}^{d}\frac{1}{i}=\ln(d)+\gamma$$

所以

$$E[X]<\frac{\ln(d)+\gamma}{p(1-p)^{d-1}} \quad (2)$$

由式(1)，(2)可得

$$\frac{1}{p(1-p)^{d-1}}\leqslant E[X]<\frac{\ln(d)+\gamma}{p(1-p)^{d-1}}$$

证毕。

从定理 1 可以看出整个系统的收敛时间主要取决于采样概率最小的路由器标记包到达终点的时间，在 FMS 和 AMS 中，采样概率随距终点的跳数递减，最远处的路由器具有最小采样概率 $p(1-p)^{d-1}$。由于 DDoS 的攻击流量与采样概率具有同样的分布特性，因此越远处的标记包越难到达终点，造成整个系统的效率低下。与之相比，本文中提出的 OMS 可以使采样概率随距终点的跳数递增，从而具有更快的收敛速度。

3 优化包标记策略 OMS

3.1 标记算法

OMS 标记策略采用两种方式来提高性能：第一，在 IP 报头重载时加入了控制位 MF，设置该位的作用是使采样概率呈随距终点跳数递增的趋势；第二，使用一组相互独立的 HASH 函数来降低地址冲突率。

OMS 重载后的报头格式如图 1 所示，图中阴影部分为重载的部分，各个域的含义分别是：

fID：HASH 函数族索引，用于确定所使用的函数。

Edge：边，表示标记路由器和它的下一跳所构成的攻击路径上一条边的信息。

Distance：距离，表示标记路由器距离终点的跳数。

以上三个域通过重载报文头部的识别号域(Identification)得到

MF：标记控制位，为“0”时允许标记，为“1”时禁止标记。

MF 域通过重载报文头部中三位分片控制符(Flags)的最高一位得到，该位在 IP 报文头部中作为保留位不被使用，且初始值为 0，因此该选择是合理的。在算法中，我们增加了对 MF 的检验，由于仅需检验其为“0”还是为“1”，因此增加的成本相当有限。

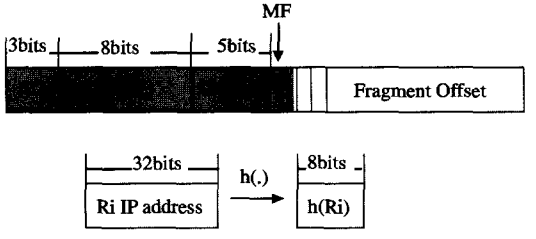

图 1 OMS 报头重载格式

下面是在路由器 R_i 处的标记算法。其中 p 为标记概率，Pt 为 R_i 转发的某个数据包。

算法 3.1 Marking(p,Pt)

```
for each packet Pt transmitted by Ri
    let u be a random number from [0,1]
    if (u ≤ p) and (MF = = 0) then
    //按概率 p 选择是否标记
        let k be a random integer from [0,7]
        //HASH 函数族的大小为 8
        MF ← 1
        P. fID ← k
        P. Distance ← 0
        P. Edge ← g(k,Ri)
        // g(k,Ri):由索引 k 决定的 HASH 函数
    else
        if (P. Distance = = 0) then
            P. Edge ← P. Edge ⊕ g(P. fID,Ri)
        P. Distance ← P. Distance + 1
```

在算法 3.1 中，攻击路径上的路由器按概率 p 随机抽取数据包，对抽中的包检查其 MF 标志，若为“0”，则在 Edge 域中写入自己地址的 HASH 值，同时置 Distance 为 0，置 MF 为“1”。对未抽中或者虽然抽中但 MF 值为“1”的包，若 Distance 为 0，则把自己的地址的 HASH 值与 Edge 做一次异或(⊕)运算，结果赋给 Edge，同时 Distance 加 1；若不为 0，则仅 Distance 加 1。

算法 3.1 中的 HASH 函数按如下原则确定：取 $g(x)$ 为理想的 HASH 函数，则$\{H_i(x)\mid H_i(x)=g(\langle i,x\rangle)(0\leqslant i\leqslant 7)\}$构成数量为 8 的 HASH 函数族，其中$\langle_,_\rangle$代表串联关系。以随机数 i 为索引在该函数族选择一个 HASH 函数。可以看出，由于 Edge 域的长度为 8，$g(x)$的冲突率为 $1/2^8$，因此整个 HASH 函数族具有$(1/2^8)^8=1/2^{64}$的冲突率。

算法保证了如下结果：若 R_d 为距离被攻击者跳数 d 的路由器，则当 $d>0$ 时，来自它的标记包中三元组$\langle$fID,Edge,Distance$\rangle$的内容为$\langle k,H_k(R_d)\oplus H_k(R_{d-1}),d\rangle$；当 $d=0$ 时，该三元组的内容为$\langle k,H_k(R_0),0\rangle$。被攻击者可以根据这些信息逐跳地、回溯地重构出整个攻击路径。

3.2 重构算法

下面给出被攻击者 V 处的路径重构算法，算法中的符号含义如下：

max$d$：所有标记包中 Distance 最大值。

Ωx：x 的上游邻居路由器集合。

S_i：攻击路径上距离 V 跳数为 i 的路由器集合。

$\Phi_{d,j}$：来自 S_d 中路由器且 fID$=j$ 的所有标记包中 Edge 值的集合

算法 3.2 Reconstruction(max d)

```
for each router R in ΩV
    for i := 0 to 7 //检查所有的 HASH 函数
        for e in Φ0,i
            if (g(i,R) = = e) then
                insert R into S0
for d := 0 to maxd−1 //由 S0 出发逐跳回溯
    for each router T in Sd
        for each router R in ΩT
            for i := 0 to 7
                for e in Φd+1,i
                    if g(i,T) = e ⊕ g(i,R) then
                        insert R into Sd+1
output Sd for 0≤d≤maxd
```

算法 3.2 中，V 首先对 Ω_V 中的每个路由器 R，计算出所有的 $H_i(R)(0\leqslant i\leqslant 7)$，若 $H_i(R)\in\Phi_{0,i}$，则认为 R 是攻击路径上距离最近的路由器，放入集合 S_0 中；对 $\forall T\in S_0$，$\forall R\in\Omega_T$，$\forall e\in\Phi_{1,i}$若 $H_i(R)=H_i(T)\oplus e$，则置 R 于 S_1 中；……。如此循环，直到到达最大距离 max$d$ 处，即可重构出整条攻击路径。重构路径时在每个 d 处要进行$|S_d|\times|\Omega_{d+1}|$次异或运算，因此重构算法的计算复杂度为 $O(\sum_{0\leqslant d<\max d}|S_d|\times|\Omega_{d+1}|)$。

4 OMS的性能分析

4.1 重构路径所需包数量

设 A_i 为DDoS中某个攻击者，V为被攻击者，R_i 为传输路径上距V的跳数i的路由器，$L_i=(A_i\rightarrow R_{d-1}\rightarrow R_{d-2}\rightarrow\cdots\rightarrow R_1\rightarrow R_0\rightarrow V)$ 为一条由 A_i 到V跳数为 d 的攻击路径。在OMS中，L_i 上的所有路由器以概率 p 进行包标记，定义 P_0，$P_1,\cdots,P_{d-2},P_{d-1}$ 分别为来自 $R_0,R_1,\cdots,R_{d-2},R_{d-1}$ 的标记包采样概率(采样的概念见第2节)。

一旦某个包被 R_{d-1} 所标记，它的MF即被设为"1"，其他路由器不能重新标记，所以 $P_{d-1}=p$；对于 R_{d-2}，它对某个包的标记只能发生在 R_{d-1} 未对该包标记时，所以 $P_{d-2}=(1-p)p$，同理有

$$P_{d-3}=(1-p)^2p,$$

$$\cdots$$

$$P_i=(1-p)^{d-i-1}p,$$

$$\cdots$$

$$P_0=(1-p)^{d-1}p。$$

由于 $1-P<0$，$P_i=(1-p)^{d-i-1}p$ 随 i 递增，也就是说，距离终点越远，P_i 的值越大。另一方面，DDoS的攻击流量是从源点由许多路径逐渐汇聚到终点的，距终点越远流量越小，因此OMS可以更快地收集到来自远端的标记包，减少重构路径的所需的数据包数量。

在传统的包标记追踪策略中，$P_i=p(1-p)^i$，P_i 随 i 递减，这就使得DDoS攻击中，来自远端的包很难被采样。以AMS为例，在面对有 n 个攻击源的DDoS时，假设所有攻击源与被攻击者距离相等都为 d(若不等，取最短距离)，则根据定理1，为了得到一条攻击路径，AMS至少需要收集约 $\frac{1}{p(1-P)^{d-1}}$ 个包，n 条路径需要至少 $\frac{n}{p(1-P)^{d-1}}$ 个包。而在OMS中，由于最远处的包采样概率为 $\frac{1}{p}$，则只需要 $\frac{n}{p}$ 个包。若取 $p=0.04$，$d=10$，在AMS和OMS中分别需要 $36n$ 和 $25n$ 的包来重构路径，后者比前者的收敛速度提高约50%。实际上，随着 d 的增加，OMS的优势将更加明显，例如在 $d=20$ 时，AMS约需 $54n$ 的包来重构，OMS同样是 $25n$，所需包数量减少一倍以上。

4.2 误报率

OMS的误报主要是由于HASH函数冲突所引起的。为了降低冲突率，OMS采用了一组相互独立的HASH函数来取代单个函数，正如在3.1节中所分析的，若单个函数的输出长度为 m，则按OMS策略所选取的一组数量为 k 的函数族将具有 $1/2^{mk}$ 的冲突率。假设网络上距离被攻击者 d 处存在 $|M_d|$ 个攻击者，若采用 2^w 个相互独立的HASH函数，则对于 $d-1$ 处某个有 t_y 个子孙(上游的邻居路由器)的节点 y 来说，其子孙中的误报数为 $t_y\times\prod_{1\leqslant l\leqslant 2^w}\frac{|\Phi_{d,l}|}{2^{11-w}}$，其中 $\Phi_{d,l}$ 的定义见3.2节。若HASH函数是理想的，则 $E(|\Phi_{d,l}|)=(1-(1-\frac{1}{2^{11-w}})^{|M_d|})\times 2^{11-w}$。

例如取 $w=3$，$t_y=32$，$|M_d|=128$，则 y 的子孙中预计的误报数将不大于1。文献[8]中的研究表明，采用此种策略可以对抗来自约1500个节点的DDoS攻击。

5 仿真试验结果

为了检验OMS在真实环境下的性能，引进朗讯-贝尔实验室的因特网拓扑数据库[9]作为仿真数据来源，该数据库包含从单个源节点65.198.68.56到342243个目标主机的真实路径，试验中以源节点V作为被攻击者，以所有路径中的路由器作为上游节点构成追踪拓扑树。每次仿真试验随机选取 s 个目标主机作为攻击者，路径上的路由器按上述标记算法进行标记，V按重构算法从标记包中得到攻击路径，每次试验独立重复做50次，以平均值作为试验结果。

5.1 重构路径所需包的数目

为了检验OMS的收敛速度，选取数据库中距离分别为特定值 d 的目标主机作为攻击者，统计出重构出路径所需的标记包数目。取 $p=0.04$，$d=1,2,\cdots,30$，$m=5$，发送包的数量每次按100递增，直到能重构出攻击路径为止，每个数据点都是从50次独立重复试验中取的平均值。图2显示了FMS，AMS和OMS的各自仿真结果，可以看出，OMS的收敛速度与FMS，AMS相比较有明显的提高，其优势随距离的增加而愈加明显，这是与前面的理论分析结果相一致的。

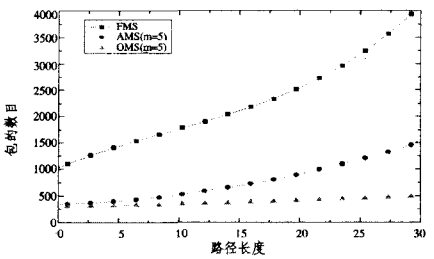

图2 重构路径所需包的数目

5.2 误报数

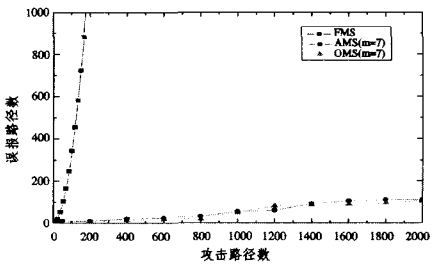

图3 误报路径数

从数据库中分别选取100，200，…，2000个目标主机作为不同的攻击者，取 $p=0.04$，$m=7$(AMS，OMS)，统计在存在不同数目的攻击者时的路径误报数，每个数据点取独立重复50次试验的平均值。

从图3的仿真结果可以看出，OMS与AMS具有相似的误报率，但是同FMS相比，误报率有很大的提高，这是由于同FMS相比，OMS采用了由相互独立的HASH函数组成的函数族，使得地址冲突率呈指数级降低，从而在追踪精度方面有更好的表现。

结束语 传统的攻击源追踪技术在整条路径上使用同样的概率进行标记，路由器所标记的包到达终点的概率随距离呈递减趋势，在现实环境中，DDoS的流量分布是从远处逐渐汇聚到终点的，这就使得越远处的路由器标记包越难到达终点。本文中提出的OMS策略在报文重载时加入了控制信息，使标记包到达终点的概率随距离递增，提高了整个追踪系统的性能。

参 考 文 献

[1] Stone R. CenterTrack: An IP overlay network for tracking DoS

floods // Proceedings of 2000 USENIX Security Symposium. Denver, Colorado, USA, 2000: 199-212
[2] Burch H, Cheswick B. Tracing anonymous packets to their approximatesource // Proceedings of 2000 USENIX LISA Conference. Seattle. Washington, USA, 2000: 319-327
[3] Jing Y N, Li J T, Wang X P, et al. Distributed-log-based IP traceback scheme to defeat DDoS attacks // Proceedings of 20th International Conference on Advanced Information Networking and Applications (AINA 2006). Vienna, Austria. April 2006, 2: 25-32
[4] Thing V L L, Lee H C J, et al. Enhanced ICMP traceback with cumulative path. IEEE VTC2005 'Spring. Stockholm, Sweden, June, 2005, 4: 2415-2419
[5] Dean D, Franklin M, Stubblefield A. An algebraic approach to IP traceback // Proceedings of 2001 Network and Distributed System Security Symposium. Sand Diego, California, USA, 2001: 3-12
[6] Savage S, Wetherall D. Network support for IP traceback. IEEE/ ACM Transactions on Networking, 2001, 9(3): 226-237
[7] Song D, Perrig A. Advanced and authenticated marking schemes for IP traceback // Proceedings of the IEEE INFOCOM. Anchorage, Alaska USA, 2001, 2: 878-886
[8] Li Dequan, Su Purui, Feng Dengguo. Notes on packet marking for IP traceback[J]. Journal of Software, 2004, 15(2): 250-258
[9] Internet Mapping Project. http://cm. bell-labs. com/who/ches/ map/ dbs/index. html, 2006

(上接第 83 页)

务成功率的关系，以此分析该信任模型的有效性，实验结果如图 1 所示，在有信任机制和无信任机制下，随着网络中恶意节点比例的增加，服务成功率都相应地减小，但是有信任机制情况下服务成功率下降得慢，甚至当网络中存在 90% 的恶意节点时，服务成功率还为 47%。

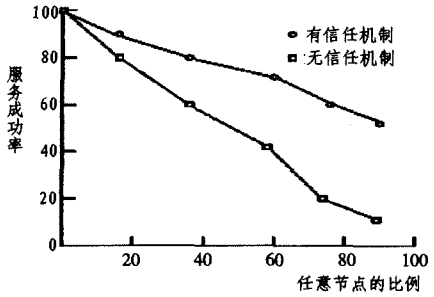

图 1 普通恶意行为模拟图

模拟实验 2：诋毁行为模拟

本实验模拟在有诋毁攻击时善意节点和恶意节点的服务成功率，以检验信任模型对诋毁攻击的抵御能力。假设网络中存在 20% 的恶意节点，实验结果如图 2 所示，随模拟周期的增加，善意节点的服务成功率的有所下降，但恶意节点的服务成功率远低于善意节点，这些现象表明诋毁攻击对善意节点的影响并不大，系统有良好的抵御诋毁攻击的能力。

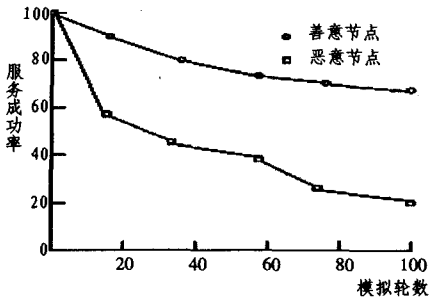

图 2 诋毁行为模拟图

模拟实验 3：串谋行为模拟

本实验模拟在有串谋攻击时善意节点和恶意节点的服务成功率，以检验信任模型对串谋攻击的抵御能力。假设网络中存在 20% 的恶意节点，实验结果如图 3 所示，实验结果与诋毁行为结果相似，只不过结果变化平稳些，一般来说，这两类攻击联系在一起，形成串谋诋毁攻击。

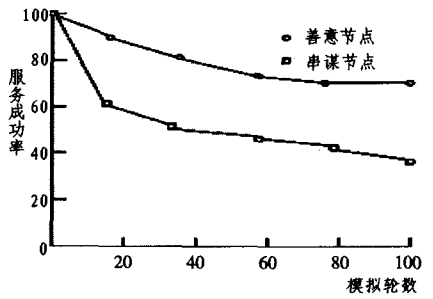

图 3 串谋行为模拟图

结束语 本文提出基于 Vague 集的信任模型，Vague 集的隶属度能够很好地表示和处理不确定信息，信任度具有主观性，包含不确定信息，用隶属度度量信任度是一种理想的度量方法。信任机制常受到 4 类行为的攻击，本文深入分析这些攻击行为的本质，引入信任时间敏感系数和惩罚系数，对资源提供者的反馈信息做出了合理的处理，使信任值正确反映资源的价值，有效地克服了背叛和策略摇摆攻击。Vague 集的相似度量理论较为成熟，本文采用 Vague 集相似度量理论评价推荐节点的回馈信息，判断推荐节点是否存在诋毁攻击和串谋攻击的趋势。本文给出该信任模型的实现方案，并进行了仿真实验，实验表明该信任模型是科学、合理和可行的。

参 考 文 献

[1] Shneidman J, Parkes D. Rationality and self-interest in peer to peer networks [C] // the 2nd Int'l Workshop on Peer-to-Peer Systems(IPTPS2003). Berkeley, CA, USA, 2003
[2] Duma C, Shahmehri N. Dynamic trust metrics for peer-to-peer systems// Proc. of 2nd IEEE workshop on P2P Data Management. security and trust, 2005
[3] 窦文，王怀民，贾焰，等. 构建基于推荐的 peer-to-peer 环境下的 Trust 模型[J]. 软件学报，2004, 15(4): 571-583
[4] Xiong L, Lin L. A reputation-based trust model for peer-to-peer E-commerce communities [C] // IEEE Conf. on E-commerce. Newport Beach, California, USA, 2003
[5] Kamvar S. EigenRep: Reputation management in P2P networks [R]. Tech Rep: SCCM-02-16. Stanford University, 2002
[6] Song S, Hwang K, Zhou R, et al. Trusted P2P transactions with fuzzy reputation aggregation, Internet Computing, IEEE, 2005 (9): 24-34
[7] Gau, Wenlung, Buehrer D J. Vague sets IEEE Transactions on systems. Man and Cybernetics, 1993, 23(2): 610-614
[8] 李凡，徐章艳. Vague 集之间的相似度量[J]. 软件学报，2001, 12 (06): 922-926
[9] Jϕsang A, Knapskog S J. A metric for trusted systems. Global IT Security. Wien: Austrian Computer Society, 1998: 541-549