Gnutella对等网中抵御DDoS攻击的评估算法

蒲荣富[1]，马新新[2]，秦志光[2]

(1. 绵阳师范学院网络中心 四川 绵阳 621000; 2. 电子科技大学计算机学院与工程学院 成都 610054)

【摘要】为了有效降低恶意节点利用泛洪查找机制对网络造成的破坏，提高对等网抵御DDoS攻击的自适应力，提出了基于马尔科夫的评估(ME)算法。运用可信和信誉机制对节点的历史行为进行评估，确保节点所获取的信息来源节点的可信；通过节点邻居信息的交互将恶意节点尽早识别、隔离，并将恶意消息的传播控制在局部范围，增强抵御DDoS攻击的效能。仿真实验结果表明，该算法能有效地隔离恶意节点，阻止恶意消息的传输，增强Gnutella对等网对基于泛洪DDoS攻击的容忍度。

关 键 词 分布式拒绝服务攻击; 对等网; 信誉; 可信

中图分类号 TP393.08 **文献标识码** A

An Evaluation Algorithm Improving Resilience Against DDoS Attack in Gnutella Peer-to-Peer

PU Rong-fu[1], MA Xin-xin[2], and QIN Zhi-guang[2]

(1. Network Center, Mianyang Normal University Mianyang Sichuan 621000;

2. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract In unstructured Peer-to-Peer (P2P) systems such as Gnutella, the general routing search mechanism used is to blindly flood a query to the network among peers. However, the blindly flooding search mechanism makes the whole network subjected to distributed denial of service (DDoS) attacks. In order to alleviate or minimize the bad effect due to behavior of malicious nodes making use of the flooding search mechanism, we propose the Markov-based evaluation (ME) mechanism in which reputation is applied as incentive pattern called a trusted based incentive scheme. Trust based incentive is enabled by evaluating the transaction history of the peer and changing the peer's significance or capacity within the P2P network based on this evaluation. Our simulation study shows that this approach can effectively isolate the malicious peer and its message transmitting and improve resilience against DDoS attack.

Key words DDoS; P2P; reputation; trust

近年来对等(P2P)技术在文件信息交换领域的应用普及受到广泛关注。根据定位查找机制和逻辑拓朴结构，P2P系统主要被划分为集中式、分布式且非结构化和分布式但结构化三类不同的体系结构。在集中式P2P模式(如Napster)中，所有节点自身的共享文件信息索引项目存储于中央索引服务器，中央索引服务器以<文件对象键值，节点地址>的映射方式将节点和共享文件信息进行关联，并以目录的形式进行维护管理。节点查找文件信息，只需在索引服务器上进行查询就可以得到拥有在该文件信息的节点信息。这种集中式的P2P体系结构简单，易于部署和维护，但该结构存在单点失效性的问题。在分布式且非结构化P2P模式如Gnutella中，泛洪(flooding)是最主要的搜索查找技术，该技术为控制查找的范围而引进了生存时间(TTL)参数。与集中式P2P不同，该结构没有单点失效性的不足，节点之间进行直接的信息交换和服务，具有更大的灵活性和自由度。但是，泛洪的盲目查找机制的查询开销很大，且易于被系统中的恶意节点利用，发起分布式拒绝服务攻击(DDoS)。在分布式但结构化P2P模式(典型的如Chord、Pastry、Tapestry和CAN)中，查询是分布式的，而拓朴结构是结构化且采用分布式哈希表(DHT)技术进行精确查询控制的。在理想情况下查询具有确定性的跳数。

本文针对基于Gnutella协议的对等网进行研究，该体系结构通常采用盲目泛洪的路由查找协议在对

收稿日期：2006 – 08 – 02；修回日期：2006 – 12 – 23

作者简介：蒲荣富(1968 –)，男，副教授，主要从事网络安全技术与应用方面的研究.

等网络进行文件信息的查询。使用盲目泛洪查找机制目的是尽可能提高查询的命中率。但盲目泛洪查找机制设计的前提是构成P2P重叠网的所有节点是彼此信任的善意节点。所有节点因共同的兴趣进行无私的协作，并自愿提供自身的资源或服务共同维护整个网络。但是，实际上，对等网中每一节点对其行为不负任何责任，利己、以自我为中心、尽最大可能地使用网络资源等现实情况，都对基于Gnutella的P2P对等网的可靠性、鲁棒性和安全性提出了挑战。更为严重的是，恶意节点可以利用该协议查询机制的漏洞，轻意地在对等网中发动DDoS攻击，通过恶意更改转发的消息包，传播不正确或破坏性的文件信息甚至病毒。与传统的针对单一节点的DoS攻击不同，对等网中的DDoS的攻击是针对整个网络，而基于Gnutella的对等网本身对利用该协议漏洞的攻击没有任何防范措施，因此具有更大的危害性和破坏力。

为有效降低恶意节点利用泛洪查找机制对网络造成的破坏，提高对等网抵御DDoS攻击的自适应力，本文提出了基于马尔科夫的评估(ME)算法，运用可信和信誉机制对节点的历史行为进行评估，确保节点所获取的信息来源节点的可信，通过节点邻居信息的交互将恶意节点尽早识别、隔离，并将恶意消息的传播控制在局部范围，增强抵御DDoS攻击的效能。仿真实验结果表明，该算法能有效地隔离恶意节点的消息数，提高对DDoS攻击的容忍度。

1　基于马尔科夫的评估算法

马尔科夫过程是涉及将来可能的事件行为由现在的行为得出的随机过程，即将来可能的取值只与现在的取值有关，与过去的取值无关，系统在每一时刻的状态仅仅取决于前一时刻的状态，而与过去的历史无关。这种性质称为无后效性。若已知系统现在的状态，则系统未来状态的规律就可确定，而不管过去的状态如何，数学函数表示为$x(t)$。根据N种可能的状态和序列时间$t_1<t_2<\cdots<t_n$得出如下公式：

$$P(x(t_n)\leqslant x_n \mid x(t_{n-1}),\cdots,x(t_1))=P(x(t_n)\leqslant x_n \mid x(t_{n-1})) \quad (1)$$

或者：

$$P(x(t_n)\leqslant x_n \mid x(t) \text{ for all } t\leqslant t_{n-1})=P(x(t_n)\leqslant x_n \mid x(t_{n-1})) \quad (2)$$

基于马尔科夫过程预测将来概率事件行为的特性，本文提出了基于马尔科夫可信和信誉评估算法。通过将可信值和推荐值进行关联计算得出节点的评估值，对节点的信任等级进行划分以识别恶意节点。描述基于马尔科夫评估计算模型的如下。

设T表示所有可信节点的信誉值集合，R表示这些可信节点对某一节点推荐值的集合。集合T和R的笛卡尔集体构成一个可信评估矩阵。该矩阵值为某一被评估节点未来行为可信的概率值，根据上述设定得出基于马尔科夫可信计算公式如下：

$$E=T\times R=[T_{i1},T_{i2},\cdots,T_{ik},\cdots,T_{in}]^{\mathrm{T}}\times[R_{1j},R_{2j},\cdots,R_{kj},\cdots,R_{nj}] \quad (3)$$

式中　i表示提出对某一节点进行评估的节点；j表示待评估的节点；而整数集合$\{1,2,3,\cdots,n\}$表示网络中除去节点i和j的节点；T_{ik}表示节点k的可信值；R_{kj}表示节点k对节点j的推荐值。接下来本文详细讨论如何计算集合T和集合R中的元素。由于可信值和推荐值分别侧重于可信评估的某一方面，但可信评估的结果是基于一个具体的数值。为此，可信或推荐集合的计算过程用集合X表示，即$X=[x_0,x_1,\cdots x_k,\cdots,x_n]$，其中$x_k$表示第$k$步评估过程，且计算结果值构成评估集合$P$，即$P=[p_1,p_2,\cdots,p_k,\cdots,p_n]$。本文假设前$N$次的评估结果已得出，基于前$N$步的评估，可以预测计算第$N$+1步的评估值。在具体的计算过程前，本文将评估准则划分为四种。

(1) 若第N步被评估节点的结果是诚实行为，且令评估节点满意，则$p_{n+1}=p_n+A$；

(2) 若第N步被评估节点的结果是诚实行为，但评估节点不完全满意，则$p_{n+1}=p_n+B(A>B)$；

(3) 若第N步被评估节点的结果是不诚实行为，但评估节点对该结果可以容忍，则$p_{n+1}=p_n-C$；

(4) 若第N步被评估节点的结果是不诚实行为，且评估节点对该结果不可容忍，则$p_{n+1}=p_n-D(C<D)$。

上面四种划分类中，A、B、C、D被定义为权重系数，且均为非负整数。第N+1步评估结果值$x_{n+1}=i_n+1$的产生依赖于前一步即$x_n=i_n$，而与$x_0=i_0,x_1=i_1,\cdots,x_{n-1}=i_{n-1}$无关，此时集合$\{x_n,\ n\geqslant 0\}$构成一离散状态的齐次马尔科夫链。

在模型的初始化过程中，本文假设任一节点在第一次进行交互前其评估值为零，即$x_0=i_0=0$。对于权重系数A和B的取值，根据评估节点的满意程度分别取值为10和5；而对于C则定义为评估节点对被评估节点不诚实行为的惩罚，其取值为10。若$i_n-r_c\geqslant 0$，$r\geqslant 1$且$r\in Z$，同时被评估节点连续发生上述第(3)类情况，则i_{n+1}的值连续减少，直至$i_{n+1}\leqslant 0$的情况时，该被评估节点被认为是不可靠的节点，且被剔除或者说被P2P网络隔离。当连续发生上述第(1)或(2)类情况，则i_{n+1}将持续增加，但该值的上限为90，即$i_{n+1}\geqslant 90$时，$i_{n+1}=90$。当被评估节点处于第(4)种情况

时，权重值D被指定为30。选择D为30是基于当i_n=90的情况下，若被评估节点连续发生3次第(4)类行为，通过计算就可以得出该节点为不可信任节点而被隔离。

基于上述A、B、C和D的不同设定值，i_n的取值范围[0，90]及有限集合$X\{x_i \mid x_i = 5n$，$0 \leqslant n \leqslant 18$，且$n \in Z\}$中的元素代表$x_n$的可能取值，可以构造出马尔科夫链的转移概率矩阵$\boldsymbol{P}=\{p_{ij}\}$，其中$\boldsymbol{P}$满足如下条件：

$$\boldsymbol{P}_{ij}=0 \qquad i,j \in X \tag{4}$$

$$\sum_i \boldsymbol{P}_{ij}=1 \qquad i \in X \tag{5}$$

而转移概率矩阵的元素根据上述评估标准划分为四类。

(1) 0→5，0→10 and 5→10，5→15。在该类评估条件下，一旦被评估节点发生评估准则的第(3)类或第(4)类行为，则会立即被隔离，即被评估节点只能产生评估准则第(1)或(2)类行为，且都为等概率事件，则：

$$p_{0,5}=p_{0,10}=p_{5,10}=p_{5,15}=\frac{1}{2} \tag{6}$$

(2) 当$i \in \{10,15,20,25\}$时，由于被评估节点有条件产生评估的第(3)类行为，且与评估准则的第(1)、(2)类行为的产生为等概率事件，则：

$$p_{i,i-5}=p_{i,i+5}=p_{i,i+10}=\frac{1}{2} \tag{7}$$

(3) 当$i \in \{30,35,40,45,\cdots,80\}$时，由于被评估节点有条件产生评估的第(4)类行为，且与评估准则第(1)、(2)和(3)类为等概率事件，则：

$$p_{i,i-10}=p_{i,i-30}=p_{i,i+5}=p_{i,i+10}=\frac{1}{4} \tag{8}$$

(4) 当$i \in \{85,90\}$时，因为i_n+1上限值等于90，则：

$$p_{85,55}=p_{85,75}=p_{90,60}=p_{90,80}=\frac{1}{4}$$

且$p_{85,90}=p_{90,90}=\frac{1}{2}$，根据Kolmogorov-Chapman方程有：

$$p_{ij}^{(m+n)}=\sum_k P_{ik}^{(n)} P_{kj}^{(m)} \tag{9}$$

因为$\forall i \in X$，$\sum_{j \in X} P_{ij}=1$，并且集合X是一闭集，利用以上四类条件(即对应的公式)可计算得到：

$$\boldsymbol{P}_{ij}^{(n)}=\sum_k p_{ik} p_{kj}^{(-1)} \sum_{k \in X} p_{ik} p_{kj}^{(-1)} \tag{10}$$

式中　初始条件为：

$$\boldsymbol{P}_{ij}^{(0)}=\delta_{ij}=\begin{cases}1 & i=j\\ 0 & i \neq j\end{cases}$$

且$\boldsymbol{P}_{ij}^{(n)}$的结果在[0,1]范围内。

2　仿真实验及分析

2.1　仿真实验环境

仿真实验基于PeerSim平台，并采用Gnutella0.4网络协议。查询消息是以泛洪方式传递的，且每一个节点都连接一定数量的邻居节点，由节点发出的查询消息通过邻居节点向网络扩散。消息的跳数由TTL指定。在仿真实验中，人为指定所有节点都共享一定数量的文件，并以一定的时间间隔选择本地不存在的文件向网络发出查询消息。在收到文件查询消息时，如果本地发现了所查询的文件则返回一个响应消息。对于恶意节点在收到文件查询消息时，恶意节点会对文件查询消息进行篡改，使查询的消息在网络中不停地转发直至超时。在仿真测试实验中，仿真了20 000个节点，每个节点的邻居节点定为3，TTL等于3。每个节点在一个循环时间内能处理的最大消息数为300，则整个网络的消息总数为600万。每个节点侦测其邻居节点的可信度，并建立邻居节点可信评估表。为得到恶意节点攻击网络产生的破坏力及评估本文提出的ME抵御面向整个对等网的DDoS攻击。本文假设仿真实验中的节点一旦加入系统则始终不会动态地加入、离开，即构成的网络是相对静态的。

2.2　仿真实验结果分析

网络中恶意节点合谋对网络资源的消耗示意图如图1所示。

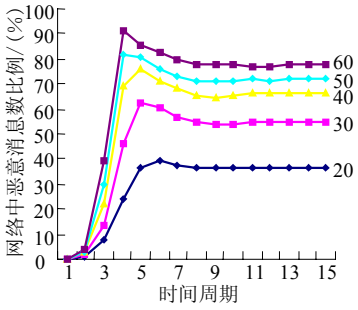

图1　未使用ME网络中恶意节点消息数

图中，横坐标为一个循环周期时间内的恶意消息数；纵坐标为不同的循环周期时间网络中恶意节点产生的恶意消息数占整个网络资源的百分比数。图中共有5条曲线，分别代表恶意节点数占整个网络节点的比例从20%～60%时对网络资源的消耗。从图中可以看出，恶意节点产生的恶意消息数曲线呈幂函数分布，并且随着恶意节点的增加，网络资源的

消耗也呈急剧增大的趋势。恶意节点的增加会在极短的循环周期时间内使网络处于资源消耗殆尽的边缘，如图中当恶意节数的比例为50%时，在不到4个循环周期的时间内，其合谋产生的恶意消息数占整个网络可容纳的消息数的80%以上。这说明利用泛洪的查询机制恶意节可以轻意地对网络发起攻击，破坏力极大。网络本身对此类攻击没有任何作为。

采用本文提出的ME评估方法后，网络中恶意节点合谋对网络资源的消耗如图2所示。

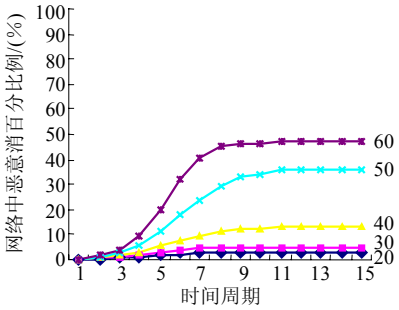

图2　使用ME后网络中恶意节点消息数

与图1类似，图2中的5条曲线分别代表恶意节点数占整个网络节点的比例从20%～60%时对网络资源的消耗。曲线同样呈幂函数分布。与图1相比，图2中出恶意节点合谋对网络资源的消耗明显降低，当在恶意节点数比例为20%～40%范围时，恶意节点消息数占整个网络消息数在10%之内，恶意消息数降低了4～8倍，即使恶意节点数比例为50%～60%时，恶意消息数也降低1倍。实验仿真数据说明，本文提出的ME方法能有效抵抗基于泛洪的DDoS攻击。

3　结　论

本文提出了基于可信和信誉的马尔科夫评估算法来防范基于Gnutella协议对等网的DDoS攻击。仿真实验数据表明，在基于Gnutella的P2P对等网中，该评估算法可以从盲目泛洪的邻居节点中识别恶意节点，并告知其他邻居节点，从而将该节点隔离，并可有效地降低恶意消息数达50%。

参　考　文　献

[1]DESPOTOVIC Z, ABERER K. P2P reputation management: Probabilistic estimation vs social networks[J]. Computer Networks, 2006, 50: 485-500.

[2] MA Xin-xin, LIU Yong, ZHANG Feng-li, et al. The Markov-based evaluation on trust and reputation in peer-to-peer[C]//In: Proceeding of International Conference on Control, Automation and Systems. [S. l.]: IEEE Computing, 2006.

[3] PAPAIOANNOU T G. STAMOULIS G D. Effective use of reputation in peer-to-peer environments[C]//Cluster Computing and the Grid of IEEE International Symposium. [S. l.]: IEEE Computing, 2004.

[4] XU Ping, GUO Hang. Rating reputaion: a necessary consideration in reputation mechanism[C]//In: Proceeding of International Conference on Machine Learning and Cybernetics. Guangzhou: Springer-Verlag, 2005.

[5] CZENKO M, TRAN H, DOUMEN J, et al. Nonmonotonic trust management for P2P applications[J]. Electronic Notes in Theoretical Computer Science, 2006, 157: 113-130.

[6]RAHMAN A A, HAILES S. A distributed trust model[C]//In: Proceeding of New Security Paradigms Workshop. Langdale Cumbria: ACM Press, 1997.

[7] YAO W. Bayesian network-based trust model in peer-to-peer networks[C]//In: Proceeding of Agents and peer-to-peer Computing of Second International Workshop. Melbourne: Springer-Verlag, 2003: 23-34.

[8] KHAMBATTI M, DASGUPTA P, RYU K D. A role-based trust model for peer-to-peer communities and dynamic coalitions[C]//In: Proceeding of IEEE International Information Assurance Workshop. Charlotte: ACM Press, 2004.

[9] IGUCHI M, TERADA M, FUJIMURA K. Managing resource and servent reputation in P2P networks[C]//In: Proceeding of International Conference on System Sciences. Hawaii: Springe-Verlag, 2004.

[10] DEWAN P. Peer-to-Peer reputations[C]//In: Proceeding of International Paralleland Distributed Processing Symposium. Santa Fe: Sprenger-Verlag, 2004.

[11] CORNELLI F, DAMIANI E, VIMERCATI S, et al. Choosing reputable servents in a P2P network[C]//In: Proceeding of World Wide Web Conference. Hawaii: ACM Press, 2002: 441-449.

编　辑　熊思亮