第 34 卷 第 8 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.8 Computer Engineering April 2008
·安全技术· 文章编号：1000—3428(2008)08—0182—02 文献标识码：A 中图分类号：TP309

基于重路由匿名通信系统中的攻击模型

陈智俐
(湖南大学湖南财经高等专科学校，长沙 410205)

摘 要：基于重路由技术的匿名通信系统模型，提出一种攻击算法，假定发送者采用固定路长变化重路由路径的发送策略，攻击者在有多个同伴的情况下对系统进行多次观测。理论分析和计算数据表明，攻击者能正确找到发送者的概率与路径长度成反比，与观测次数和同伴数量成正比。实验结果表明，该算法能有效地破坏发送者的匿名度。

关键词：重路由；匿名通信系统；模型；攻击

Attack Model Based on Rerouting in Anonymous Communication System

CHEN Zhi-li
(Hunan Financial and Economic College, Hunan University, Changsha 410205)

【Abstract】This paper presents a model of anonymous communication system based on rerouting. Based on the system model, a attack algorithm is proposed, which adopts a transmission strategy with the fixed length and changeable rerouting path. Attackers can observe the system multitudinously with many companions. Computation and analysis indicate that probability of the attacker's finding out the sender is inversely proportional to path length, proportional to observation frequencies and the number of companion. It is proved that the attack model can effectively destroy the anonymity degree of the senders.

【Key words】rerouting; anonymous communication system; model; attack

匿名通信的一个重要目的就是隐藏通信双方的身份或通信关系，从而实现网络用户的个人通信隐私，更好地保护涉密通信[1]。目前，有关网络匿名通信技术的研究已成为网络安全研究领域的一个重要分支。而所有的安全防御技术又都是针对具体的攻击而提出的，匿名通信技术也不例外，对匿名通信技术的研究也可以转化为对匿名通信中攻击的研究。目前，国内对攻击模型的研究还较少，本文提出一种基于重路由技术匿名系统的攻击模型，并对该攻击模型进行了理论分析和模拟计算。

1 系统模型

当前的匿名通信系统按其底层的路由机制可分为两类：基于广播的匿名通信系统，基于重路由的匿名通信系统[2]。大部分匿名系统都是基于重路由机制的。按重路由部件的不同，又可把它分为基于单代理、基于串行代理和基于P2P结构3 种。笔者提出一个基于P2P结构的重路由匿名通信系统模型，该模型由N个节点组成，节点集合表示为$V=\{v_j \mid 0 \leqslant j \leqslant n-1\}$，这$N$个节点相互合作，以实现发送者和接收者的不可关联性。为了隐藏真正发送者的特征，信息从源节点发出去，经过一个或多个中间节点，达到目的节点。信息传输过程中所经历的路径称为重路由路径，可以描述为$<S, I_1, I_2, \cdots, I_L, R>$，其中，$S$是信息的发送者；$L$是路径长度；$R$是信息的接收者。图 1 是一个包含 16 个节点的匿名通信系统，表示了从源主机到目标主机的路径。

在该图中，节点 0 和节点 5 为信息发送者，在发送信息前选定要经过的中间节点和目的节点 $R1$,$R2$。节点 0 的重路由路径为<0, 5, 2, 7, 11, 8, $R1$>，中间节点有 5 个，重路由长度为 5；节点 5 的重路由路径为<5, 10, 3, 9, $R2$>，中间节点有 3 个，重路由长度为 3。

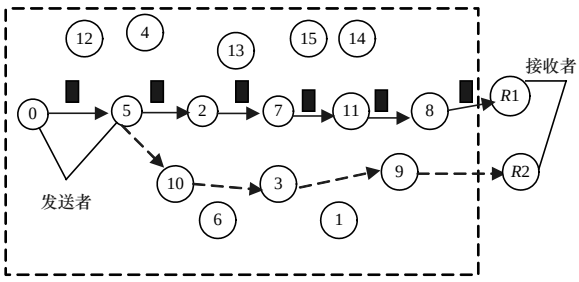

图 1 基于重路由匿名通信系统模型

2 攻击模型

事先假设攻击者采用被动攻击方式，并且假定攻击者具有如下能力：

(1)假定攻击者知道重路由方式，能窃取数据流并能分析出当前通信双方的身份。

(2)路径可变但路径长 L 为固定值。

(3)为了加大攻击者的攻击能力，假定攻击者有 m-1 个同伴，也就是说攻击者能同时监控系统内任意 m 个节点。

攻击算法如下：

Step1 假设观测次数为 k，k 的初值为 1；观测总次数为 n(n 值由攻击者确定)。

作者简介：陈智俐(1973－)，女，讲师、硕士研究生，主研方向：网络与信息安全

收稿日期：2007-12-25 **E-mail：**czl6144@163.com

Step2 如果 k 的值小于 n，随机选取 m 个节点进行观测，如果其中有一节点处于数据通信状态，则标记为活动节点，转 Step3；否则过一段时间后，另外选取 m 个节点进行观测，直至找到活动节点；如果 k 的值等于 n，转 Step6；

Step3 若活动节点处于接收状态，则记录其前一节点为原始节点，且置步长S_k初值为 1，继续监视此节点，直至有数据发送；否则记录当前节点为原始节点，且置步长Sk初值为 0，追踪监视下一节点。

Step4 当发现被监视节点有数据流传输时，截获数据流并分析它的下一节点是否在本系统内，如是，转Step5。否则记录步长S_k值，观测次数k加 1，转Step2。

Step5 监视节点，直到节点有数据发送时，则步长 Sk 值加 1，转 Step4。

Step6 计算出步长值L，$L=\max(S_1, S_2,\cdots, S_n)$。

Step7 重复Step1~Step5，在执行Step4 时，如果记录到的S_k值为L，则本次观测所记录的第 1 个节点为发送者，输出发送节点。算法结束。

$$L=\max(S_1,\ S_2,\ \cdots,\ S_n) \tag{1}$$

其中，$S_1, S_2,\cdots, S_n$为每次观测所记录下的步长值。

那么，当 $S=L$ 时，则 step1 所记录下的原始节点为真正的发送者。

定义 1 设匿名系统采用变化路径固定路长来发送信息，攻击者在系统中任选一个节点对目标流进行观测，观测 n 次后，能正确求得路径长的概率 P 由式(2)定义。

$$P(n)=1-(1-1/L)^n \tag{2}$$

证明 设L_k为第k次观测数据流得出的路径长，$Y_k=\mathrm{MAX}(L_1, L_2,\cdots, L_k)$，不难看出$L_k\leqslant Y_k\leqslant L$。

n=1 时，因为最开始跟踪的发送数据的结点只是L个结点中任意一个，而只有当最开始跟踪的结点是发送者时，才有$L_k=L$，所以，求得正确路径长的概率为

$$P=1/L=1-(1-1/L)^1$$

同理，每一次单独观测求得正确路径长的概率为 $1/L$。

设当$n=k$时，前面k次共能正确求得路径长的概率(即$L=Y_k$)为$P(k)=1-(1-1/L)^k$。不能求得正确路径长的概率为$(1-1/L)^k$。

又因为第 k+1 时，正确求得路径长的概率为 $1/L$，即不正确求得路径长的概率为$(1-1/L)$。

根据Y_k+1 =MAX(Y_k,L_k), $L_k\leqslant Y_k\leqslant L$，因此，所有$k$+1 次时，不能求得正确路径长的概率为$(1-1/L)^k\cdot(1-1/L)$，即：所有$k$+1 次时，能求得正确路径长的概率为$P=1-(1-1/L)^{k+1}$。

定义 2 已知系统内节点总个数为N，攻击者有m-1 个同伴，在此次攻击之前，攻击者已经进行了k次观察，重路由路径长为L(攻击者并不知道L的具体值是多少)。系统可能有多个节点发送数据，但在同一时间段系统内只有一个数据发送者。经过k次观测后，不能找到发送者的概率为P_f，P_f由式(3)确定。

$$P_f=1-(1-(1-1/L)^k)\left(\frac{C_2^1C_N^{m-1}+C_{N-2}^{m-2}C_2^2}{C_N^m}\cdot\frac{L-1}{L}+\frac{C_{N-1}^{m-1}}{C_N^m}\cdot\frac{1}{L}\right) \tag{3}$$

证明 由定义 2 可知，经过 k 次观察后，攻击者能正确求得路径长的概率为

$$P_L=1-(1-1/L)^k$$

如果某个节点在与其他节点进行通信，就称之为活动节点。对于本次攻击，攻击者及其同伴能同时监视 m 个节点。

因为在同一时间段内，系统只有一个数据发送者，也就是说同一时刻只能有一个活动节点在发送数据，如果接收者在系统内，则系统内还有一个活动节点在接收数据，否则系统内只有一个活动节点。系统内最多只有两个活动节点。

因此，攻击者能找到活动节点的概率由式(4)定义。

$$P_N=\frac{C_2^1C_N^{m-1}+C_{N-2}^{m-2}C_2^2}{C_N^m}\cdot\frac{L-1}{L}+\frac{C_{N-1}^{m-1}}{C_N^m}\cdot\frac{1}{L} \tag{4}$$

因为重路由路径长为 L，所以找到的第 1 个节点是真正的数据发送者的概率为 $1/L$。

由正确求得路径长的概率P_L与找到活动节点的概率P_N可知，攻击者能找到发送者的概率为

$$P_S=P_L\cdot P_N=$$

$$(1-(1-1/L)^k)\left(\frac{C_2^1C_N^{m-1}+C_{N-2}^{m-2}C_2^2}{C_N^m}\cdot\frac{L-1}{L}+\frac{C_{N-1}^{m-1}}{C_N^m}\cdot\frac{1}{L}\right)$$

则不能找到发送者的概率为

$$P_f=1-P_s=$$

$$1-(1-(1-1/L)^k)\left(\frac{C_2^1C_N^{m-1}+C_{N-2}^{m-2}C_2^2}{C_N^m}\cdot\frac{L-1}{L}+\frac{C_{N-1}^{m-1}}{C_N^m}\cdot\frac{1}{L}\right)$$

3 理论分析

攻击者采用上述攻击算法时，正确求出路径长的概率 P 与路长 L 和观测次数的关系见表 1。

表 1 P,L,n 的关系

L	n	P
1	1	1.00
5	1	0.20
10	1	0.10
1	5	1.00
5	5	0.67
10	5	0.41
1	10	1.00
5	10	0.89
10	10	0.65

L 固定时，观测次数越多，能正确求得路径长的概率越大；例如，L=5 时，观测 1 次、2 次、20 次、25 次时，能正确求得路长的概率为 0.20, 0.36, 0.99, 1.00。在一定的观测次数下，L 值越大，能正确求得路长的概率越小。

对于同一个匿名系统，N,L 一定时，能找到活动节点的概率随攻击者同伴数 m 的值增大而增大，能正确找到发送者的机会也就越大。

表 2 给出了系统节点数N=16，攻击者同伴数为 3 时，能正确找到发送者的概率P_s与观测次数k及重路由长度L之间的关系。

表 2 攻击者找到发送者的概率P_s的变化情况

k	L	P_s
1	1	0.214
3	1	0.214
5	1	0.214
1	3	0.142
3	3	0.300
5	3	0.371
1	5	0.094
3	5	0.229
5	5	0.315

从表中可以看出，对于同一系统，重路由长度 L 值越大，能找到发送者的概率越小，即攻击的成功率越低，匿名性越好。例如，当 L=5 时，在第 1 次观测中找到发送者的概率为 0.094，即不能找到发送者的概率为 0.906。而随着观测次数的增多，能找到发送者的概率越高。 (下转第 186 页)