第35卷 第23期 计 算 机 工 程 2009年12月
Vol.35 No.23 Computer Engineering December 2009
·博士论文· 文章编号：1000—3428(2009)23—0001—03 文献标识码：A 中图分类号：TP393

基于IPv6的接收者匿名Crowds系统

徐 静，王振兴
(解放军信息工程大学信息工程学院，郑州 450002)

摘 要：基于下一跳重路由方式的Crowds匿名通信系统存在较多缺点。提出基于IPv6协议的Crowds系统，解决发送者与最后一跳的秘密共享问题。理论分析和实验结果表明，该系统的抗攻击能力与源路由方式相等，实现了接收者匿名，减少了通信延迟。
关键词：匿名通信；IPv6协议；接收者匿名

Receiver Anonymous Crowds System Based on IPv6

XU Jing, WANG Zhen-xing
(College of Information Engineering, PLA Information Engineering University, Zhengzhou 450002)

【Abstract】Crowds anonymous communication system based on next hop rerouting mode has a lot of the drawback. This paper proposes a Crowds system based on IPv6 protocol, which solves the problem of secret sharing between sender and the last hop. Theoretical analysis and experimental results demonstrate that this system has the same ability of attack againsting as source rerouting mode, achieves receiver anonymity and reduces the communication delay.
【Key words】anonymous communication; IPv6 protocol; receiver anonymity

1 概述

在互联网上传输数据时，通信协议需要的包头信息很难被隐藏，匿名通信通过隐藏收发双方的身份或通信关系，为网络用户个人隐私和涉密通信提供良好保护。匿名通信系统通过重路由和填充等机制实现3种形式的匿名保护，即发送者匿名、接收者匿名和通信关系匿名。

目前匿名通信研究主要集中在匿名的有效性上，匿名通信系统借助多个代理的重路由技术、填充包技术和加密技术实现匿名发送或接收的目的。重路由在应用层对数据进行存储转发，发送的数据经过一条由多个中继节点组成的重路由路径到达接收者，通过隐藏发送者的识别信息达到匿名目的。现有重路由匿名通信系统包括Onion Routing[1], Crowds[2], Hordes[3], Tarzan[4]和MorphMix[5]等。重路由路径的建立方式主要有2种，即源路由方式和下一跳方式。源路由方式由发送者确定中继节点形成的路由，并采用嵌套加密机制封装各节点的地址和数据。对于前驱攻击，该方式具有较强的抵御能力，其缺点是发送者必须拥有匿名网络的完全拓扑知识。在下一跳路由方式中，成员只要维护邻居的信息，建立路径时，顺次由中继节点从邻居中随机选取一个作为下一跳的中继节点，发送者无需获取匿名网络的完全拓扑知识。其不足在于对前驱攻击的抵御能力较弱，无法实现接收者匿名。Crowds系统使用下一跳路由方式。

2 Crowds匿名通信系统

美国电话电报公司的Crowds为Web浏览用户提供发送者匿名形式的保护。Crowds协议用一系列互相合作的代理维持用户组中的匿名性。需要匿名保护的主机必须加入系统成为成员，在被保护的同时提供匿名服务。当成员需要发起一次匿名通信时，将请求转发给其他成员，其他成员将该请求转发或直接递交给Web服务器。

2.1 Crowds实现机制

Crowds系统中每个成员上运行一个名为jondo的代理程序，用于转发来自本地浏览器或其他成员上jondo的HTTP请求。初始时，jondo向系统中行使管理功能的成员(称为blender)注册，并获得系统中的活动jondo表和相应的共享密钥。当收到来自本地浏览器的HTTP请求时，jondo从jondo列表中随机选取一个作为后继(可能是它自己)，并将请求转发给该后继jondo。若后继jondo接收到请求，则以概率$p_f(1/2<p_f<1)$将该请求继续转发，否则以概率$1-p_f$将请求直接提交给接收者，即发送给系统中任何一个jondo的可能性是p_f，而发送给服务器的概率是$1-p_f$。每一步跳都决定是否将HTTP请求直接交给目的服务器或根据转发可能性将它转发给下一个随机选择的成员，重路由路径中允许存在循环。选择了一条重路由路径后，在24 h的时段内，所有从该发送者到该接收者的匿名通信都将使用该路径。新成员可以在一些特定时段加入Crowds并形成新路径。图1给出了在Crowds系统中构造的路径，其中包括：1->5->server；2->6->2->server, 3->1->6->server, 4->4->server, 5->4->6->server和6->3->server 6条重路由路径。

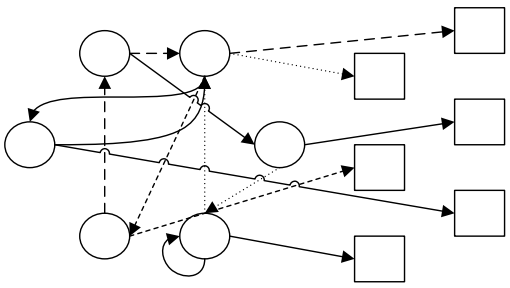

图1 Crowds匿名浏览系统

基金项目：国家“863”计划基金资助项目(2006AA01Z449)
作者简介：徐 静(1973－)，女，工程师、博士研究生，主研方向：网络与信息安全，P2P通信技术；王振兴，教授、博士生导师
收稿日期：2009-05-08 **E-mail：**xujingcwz@126.com

2.2 Crowds系统存在的问题

Crowds 系统存在如下问题:

(1)无法实现接收者匿名

根据 Crowds 的实现机制，由于没有解决发送方与重路由路径上的最后一个中继之间的密钥分配问题，因此在重路由路径中，消息内容和接收方地址以明文传输，路径上的中继节点均能获知传输数据的内容和接收者地址，因此，Crowds 系统不能实现接收者匿名。

(2)加解解密方案导致通信性能低

为防止窃听泄漏和篡改隐私内容，Crowds 系统中传送的消息使用 2 个相邻 jondo 的共享密钥进行加密。假设路径为 I->j1->j2->j3->R，则消息传送描述如下(其中，k_{ij} 是代理 i 与代理 j 之间的共享密钥，p_i 为路径号):

I->j1:$K_{Ij1}(p_0, R, message)$

j1->j2:$K_{j1j2}(p_1, R, message)$

j2->j3:$K_{j2j3}(p_2, R, message)$

j3->R:p_3, data

消息返回采用原路径返回，用路径标识符寻找发起者。所以，任意 2 个 jondo 之间进行通信时，都要用它们的共享密钥进行加密和解密操作，导致 Crowds 系统的通信延迟较大。因此，其加密解密方案是制约 Crowds 性能的一个瓶颈。

3 基于IPv6 的Crowds6 系统

3.1 实现机制

通过上述分析可以看出，Crowds 系统没有解决发送方与路径上最后一个中继的密钥共享问题[6]，导致路径上的所有成员都可以看到消息内容和接收方的地址。因此，在一条重路由路径上，发送方和路径上的最后一个中继的身份识别信息很重要，是 2 个关键节点。本文基于 IPv6 提出 Crowds6 匿名通信系统，其基本思想是由消息发送方在所有 jondo 中随机确定重路由路径上的最后一个中继，采用对称加密算法将消息内容和接收者地址加密，并使用选出的最后一个中继的公钥加密用于解密消息内容的对称密钥。路径上其他中继只负责将消息转发给最后一个中继。最后一个中继接收到数据包后，使用自己的私钥解密得到能解密消息内容的对称密钥，并使用该密钥解密消息内容，获得接收者地址，最终将消息传送给接收者。Crowds6 系统的加密解密算法借鉴了数字信封的思想。为便于描述，在 Crowds6 系统中将重路由路径上的最后一个中继称为 keynode。

Crowds6 系统在消息传送方面要解决的一个问题是，发送方在不能确定重路由路径上其他中继的情况下，如何使其他中继获得 keynode 的地址。由于 IPv6 定义了目的地选项扩展报头，用于为数据包经过的中间节点或最终目的地指定转发参数，并允许用户自定义 IPv6 选项，因此 Crowds6 系统通过在发送的消息数据包中添加目的地选项头，并在其中自定义一个被称为 Crowds 的选项来解决上述问题。IPv6 选项采用 TLV 编码格式，由选项类型、选项长度和选项内容组成，Crowds 选项的主要作用是存放 keynode 的 IPv6 地址和使用 keynode 的公钥加密后的密钥密文。Crowds 选项结构见图 2。

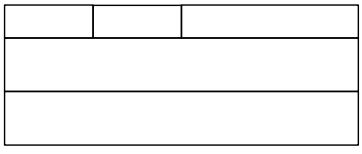

图 2 Crowds 选项结构

重路由路径上的中继 jondo 接收到消息数据包后，通过查看目的地选项头中 Crowds 选项的内容确定自己是否是此次匿名浏览路径上的 keynode。如果不是，则以概率 p_f ($1/2<p_f<1$)将该请求继续转发，否则以概率 $1-p_f$ 将请求直接提交给 keynode。如果是 keynode，则使用自己的私有密钥解密 Crowds 选项中的密钥密文，使用该密钥解密消息内容，获得真正的接收者地址，并直接将请求转发给接收者。数据返回过程与 Crowds 系统实现相同。为防止合谋成员利用多次构建重路由进行前驱攻击，发送方访问同一个 Web 服务器时，如果需要重新构建路由，则将选择一个新的中继作为 keynode，即在匿名访问时发送方选择的 keynode 不与特定 Web 服务器绑定，并选择不同密钥用于加密消息内容。jondo 处理算法的伪代码描述如下:

```
client.request = receive_request()
if (client == local browser)
keynode = R (Jondos \ {client})//在所有活动 jondo 中随机选择一
//个 keynode，自己除外
'Crowds' option1 = keynode.address//数据包目的地选项报头，其
//中“Crowds”填入 keynode 的地址
'Crowds' option2 = encrypt1(K) //随机产生对称密钥 K，用
//keynode 公钥加密填入“Crowds”
packet request = encrypt2(client.request, request.receiver, K)
//将消息内容和接收者地址用 K 加密
my_path_id = new_path_id()
next[my_path_id] = R (Jondos \ {keynode})//在所有活动 jondo 中
//随机选择下一跳，keynode 除外
forward_request(my_path_id)
else
prior jondo = client.id //记录返回时的路径
coin = coin flip(pf) //取得发送概率
if (coin == heads) //如果概率为 1- pf
submit_request(keynode) //将请求传给 keynode
else
next[my_path_id] = R (Jondos \ {keynode})
forward_request(my_path_id)
subroutine forward_request(out_path_id)
  send out_path_id || request to next[out_path_id]
  reply = await_reply()
  if (reply == 'jondo failed') //移除该 jondo
        Jondos = Jondos \ {next[out_path_id]}
        next[out_path_id] = R Jondos
        forward_request(out_path_id)
  else
        send reply to client
subroutine submit_request(keynode)
  K = decrypt1('Crowds' option2) //解密得到 K
client.request = decrypt2(request, K)
send request to destination(client.request)
  reply = await_reply(timeout)
  send reply to client
```

3.2 接收者匿名

Crowds6 系统可以在一定程度上实现接收者匿名。消息内容在传送过程中由发送方加密，加密密钥再使用 keynode 的公钥加密，路径上的其他中继无法得知接收者地址。keynode 使用自己的私钥解密出加密密钥，并使用该密钥解密消息内容获得接收方地址。在 Crowds6 系统的重路由路径上，只有发送方和 keynode 2 个节点能获得接收者信息，合

谋成员只有占据 keynode 才能获得接收者地址，增加了合谋成员的攻击成本，在一定程度上达到了接收者匿名的效果。

3.3 加解密方案

Crowds6 系统相对原有 Crowds 系统简化了加密解密方案，消息内容的加密仍然采用对称加密算法，但对称密钥使用公开密钥加密方法加密传递。加密与解密操作仅发生在消息从发送者发出和消息到达 keynode 时，其他中继只负责转发消息。加解密方案的改变使系统中的管理成员 blender 必须存储每个成员的公开密钥以便成员查询。

4 系统性能分析

4.1 前驱攻击抵御

前趋攻击是指在系统中加入一定数目的合谋成员，当有成员需要发起建立一条重路由路径时，根据随机的成员选择策略，合谋成员将以一定概率被选中作为重路由路径上的转发节点，通过共享窃听到的通信内容以及接收到请求的时序关系，合谋成员能确定位于该重路由路径上的第 1 个合谋成员，假设攻击者认定第 1 个合谋成员的前趋为通信发起者，则攻击者将以一定概率猜对发起者的地址。用户的兴趣、爱好等特点局限了用户经常浏览的站点范围，根据用户浏览的内容，可以将同一个用户在不同周期内发起建立的重路由路径关联起来，通过记录不同周期内第 1 个合谋成员的前趋，可以用统计方法以较高概率找出发起者。

假设匿名系统中成员总数为 n，其中，合谋成员数为 c。根据 Matthew Wright 的分析，对基于下一跳路由方式的 Crowds 系统，在单轮情况下，攻击成功的概率为 c/n，重路由路径重构轮数的复杂度是 $O((n/c)\ln n)$。对基于源路由方式的 Onion Routing 系统，在单轮情况下，攻击成功概率为 $(c/n)^2$，重路由路径重构轮数的复杂度是 $O((n/c)^2\ln n)$。

在 Crowds6 系统中，根据其实现算法，在一次会话中除 keynode 外的其他中继无法查看到消息内容。如果需要重新构建路由，则发送方将选择一个新的 jondo 作为 keynode。在单轮情况下，只有当路径上第 1 个中继与 keynode 同为合谋成员时，攻击者才能确定会话内容并观测到发起者，因此，攻击成功概率为 $\frac{c}{n-1}\cdot\frac{c-1}{n-1}$。由于合谋成员无法通过消息内容将不同周期内建立的重路由路径关联起来，极大增加了攻击难度，因此重路由路径重构轮数的复杂度为 $O((n/c)^2\ln n)$，达到了与基于源路由方式的 Onion Routing 系统的同等水平。因此，Crowds6 系统抵御前驱攻击的能力远高于原有 Crowds 系统。

对于 Crowds6 系统，合谋成员虽然无法通过消息内容将重路由路径关联起来，但在一条重路由路径上，由于所有中继都可以获得 keynode 的地址，且在一次匿名访问过程中 keynode 是固定不变的，因此合谋成员可以根据 keynode 地址关联信息猜测第 1 个合谋成员的前驱为发送者。所以，Crowds6 系统抵御前驱攻击的能力略低于基于源路由方式的 Onion Routing 系统。

4.2 接收者的匿名性

下文将定量证明 Crowds6 系统接收者匿名性优于原 Crowds 系统。假设系统共有 n 个成员，在成员中有 c 个合谋成员，路径长度为 L。由于重路由路径上每个成员都可以看到接收者的地址，因此合谋成员发现接收者的概率为

$$p_r = 1-\underbrace{\frac{n-c}{n}\cdot\frac{n-c}{n}\cdots\cdots\frac{n-c}{n}}_{L} = 1-\left(\frac{n-c}{n}\right)^L$$

对于 Crowds6 系统，由于重路由路径上只有 keynode 节点能获得接收者的地址信息，因此合谋成员发现接收者的概率是 $p_r=\frac{c}{n}$，当 L=1 时，有 $1-\left(\frac{n-c}{n}\right)^L=\frac{c}{n}$，利用数学归纳法可得

$$1-\frac{(n-c)^{L-1}}{n^{L-1}}>\frac{c}{n}\Rightarrow 1-\frac{(n-c)^L}{n^L}>\frac{2nc-c^2}{n^2}$$

又因为 $\frac{2nc-c^2}{n^2}-\frac{c}{n}=\frac{c(n-c)}{n^2}>0$，所以 $1-\frac{(n-c)^L}{n^L}>\frac{c}{n}$。因此，Crowds6 系统中接收者暴露的可能性小于 Crowds 系统。

4.3 系统通信延迟

由于 Crowds6 系统的加解密操作只发生在消息从发送者发出和消息到达 keynode 时，因此减小了通信延迟，提高了系统通信性能。图 3 给出了访问一个大小为 4 KB 的 HTTP 页面时，Crowds 系统和 Crowds6 系统的响应时间。实验中主机配置为：Intel Pentium 4 CPU 3.00 GHz，1 GB 内存，运行 Windows XP SP2 操作系统。模拟程序运行环境如下：CPU 平均使用率为 0~1%，物理内存占用 471 MB~480 MB。

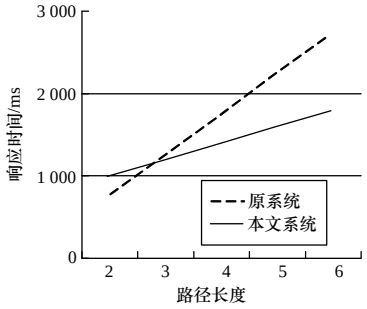

图 3 本文系统和原系统的响应时间

5 结束语

本文系统采用由发送者自主选择 keynode 节点的机制，与原有 Crowds 系统相比，其抵御前驱攻击的能力更强。下一步工作将在增强匿名性和抗攻击性的基础上，提高通信效率。

参考文献

[1] Goldschlag D, Reed M, Syverson P. Onion Routing for Anonymous and Private Internet Connections[J]. Communications of the ACM, 1999, 42(2): 39-41.

[2] Reiter M K, Rubin A D. Anonymous Web Transactions with Crowds[J]. Communications of the ACM, 1999, 42(2): 32-38.

[3] Shields C, Levine B N. A Protocol for Anonymous Communication over the Internet[C]//Proc. of the 7th ACM Conf. on Computer and Communication Security. New York, USA: ACM Press, 2000: 33-42.

[4] Freedman M J, Morris R. Tarzan: A Peer-to-Peer Anonymizing Network Layer[C]//Proc. of the 9th ACM Conf. on Computer and Communications Security. Washington D. C., USA: [s. n.], 2002: 193-206.

[5] Rennhard M, Plattner B. Introducing MorphMix: Peer-to-Peer Based Anonymous Internet Usage with Collusion Detection[C]//Proc. of the Workshop on Privacy in the Electronic Society. Washington D. C., USA: [s. n.], 2002: 91-102.

[6] 眭鸿飞, 陈建二. 重路由匿名通信系统中基于秘密共享的重路由算法[J]. 计算机研究与发展, 2005, 42(10): 1660-1666.

编辑 陈 晖