

基于结构化 P2P 的可控匿名通信系统的研究

孙 黎 王小刚¹

(江苏科技大学计算机工程与科学学院, 镇江 212003; 常州信息职业技术学院软件学院, 常州 213164)

摘 要 为防止匿名系统被滥用,在 PGACS 匿名通信系统模型的基础上,提出了分层架构的结构化 P2P 匿名通信系统(CACSBSP)。通过采用基于数据包的加密机制实现匿名的可撤销,结合节点的信誉机制实现对节点自私行为的惩罚机制,使系统具有对匿名的可控性。理论分析表明本系统的匿名性等于 Crowds 和 PGACS 系统;经实验模拟发现,本系统在提供较高匿名性的同时,可使系统中自私节点和恶意节点数目的变化对系统的负载影响较小。

关键词 匿名通信 可控匿名 惩罚机制 结构化 P2P

中图分类号 TP393.08; **文献标志码** A

与传统 C/S 模式相对的是 P2P 匿名通信技术。如 Crowds^[1]、Tarzan、MorphMix、P5 协议、PGACS^[2]等。其中,Crowds 随着节点数的增加,存在可扩展性低的问题;MorphMix 与 Tarzan 的结构类似,但没有节点的加入控制机制,P5 通过广播方式来隐匿接收者,信道利用率较低;PGACS 中通过引入接入点的方式,能对新成员的加入进行有效控制,缺少对转发路径长度的控制,可能会使转发路径无限长^[3]。另外,现有 P2P 匿名系统普遍缺乏对匿名滥用行为的可控性及对节点自私行为的惩罚机制,从而存在突出的匿名滥用问题。目前,撤销匿名的方法主要包括群签名、标记报文等。其中,群签名虽然适用性广,但计算复杂。标记报文主要用于定位 DDos 攻击者,当系统规模增大时,其误判率较高。

基于以上分析,我们在 PGACS 模型的基础上,构建基于结构化 P2P 的可控匿名通信系统(CACSBSP)。通过为每个新加入组的成员分配初始的信誉度值,并动态调整。使具有不同信誉度值的成员,获得的匿名通信服务的级别也不同。通过在数据包中内嵌经发送源所在组管理员加密的发送源地址信

息,可实现对发送源的匿名撤销。

1 支持可控匿名的结构化 P2P 匿名系统体系结构

1.1 系统的基本功能描述

CACSBSP 系统的成员结构如图 1 所示,系统由入口介绍点和多个系统成员组所组成,每个成员组又由组管理员和一般成员构成。

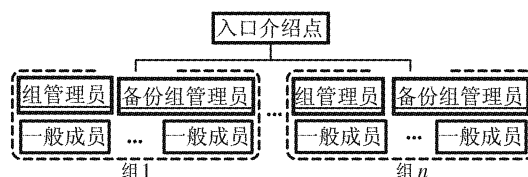


图 1 CACSBSP 系统基本成员构成示意图

入口介绍点负责系统成员的加入和控制成员组的分裂。入口介绍点接收到新成员的加入申请后,根据新成员 IP 地址的哈希映射,查找具有相同后缀,并且成员数未达设定上限的组,由该组管理员负责将其加入;如果该组的成员数已达上限,则入口介绍点通知该组的组管理员要进行小组分裂。

组管理员负责新节点的加入、组成员信誉度值的管理、小组分裂、匿名节点的选择及匿名撤销。新

2009 年 9 月 25 日收到

第一作者简介:孙 黎(1981—),安徽省马鞍山人,研究方向:计算机网络。E-mail:sunli1891@sina.com。

节点的初始信誉度值为 0,根据在线时间的长短以及其为其其他节点提供转发服务的行为动态调整信誉度值。自私成员的信誉度值为 -1,最高信誉度值为 10。当组内成员申请匿名转发节点时,管理员根据该成员的信誉度值,为其提供从其他组管理员处获得的重路由节点。当需要进行匿名撤销时,由管理员解密发送源的 IP 地址,并通知发现匿名滥用行为的节点实现匿名撤销。当管理员得到来自自入口介绍点的组分裂信息后,由管理员负责从本组成员中随机选取一半成员划分给新的小组。

备份组管理员作为组管理员的备用人选,在组管理员失效时,为本组成员提供服务。

一般成员只属于一个组,可以向本组管理员申请匿名服务,也为其他用户提供匿名转发服务。

1.2 基于节点的信誉机制实现自私行为的惩罚机制

现有的匿名惩罚机制主要采用区分服务的思想。由于自私节点充当重路由节点时,可能会拒绝为其他节点服务,造成转发路径的不断重试,由此引起的延迟,会为攻击者的攻击提供便利。

CACSBSP 系统为了避免转发过程中不断重试而造成的安全威胁,在选择重路由节点时,并未将自私节点考虑在内。同时,如果发送源的信誉度值较低,则只能得到来自少量组的部分成员信息。这些节点所在组分布范围的大小,将直接影响发送源所获得的匿名性。

参数的含义:

Data 表示源数据;

IP_s 表示含有组管理员加密标志的发送源地址;

IP_{GMR} 表示由重路由路径上的节点 K 所在组管理员加密的发送源所在组管理员的地址;

IP_K 表示节点 K 的 IP 地址;

Key_n 表示节点 n 与发送源之间的共享密钥;

S_n 表示节点 n 所在组管理员的签名标志;

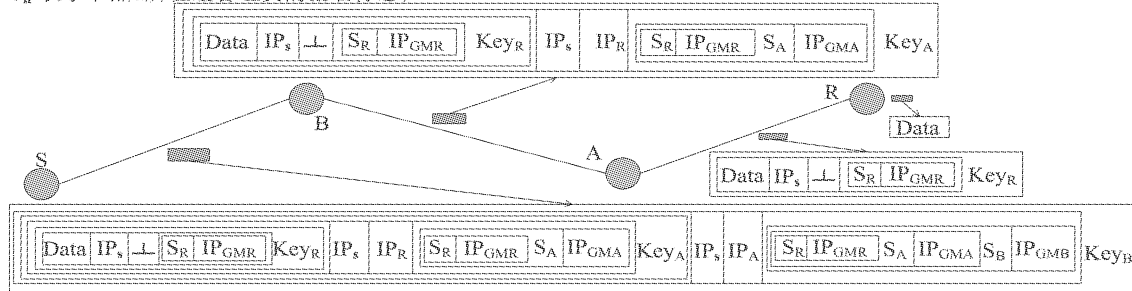


图3 节点 S 与节点 R 通信过程示意图

1.3 基于数据包的加密机制实现匿名的可撤销

CACABSP 使用的数据包如图 2 所示。

数据	组管理员加密的发送源地址	下一跳地址	类洋葱包
----	--------------	-------	------

图 (a) 洋葱包结构图

重路由路径上组管理员的签名	由重路由路径上的组管理员加密的发送源所在组管理员地址
---------------	----------------------------

图 (b) 洋葱包结构图

图 2 洋葱包及类洋葱包结构图

假设节点 S 要发送消息给节点 R,并已选择节点 B、节点 A 为重路由节点。图 3 为节点 S 与节点 R 通信过程的示意图。

首先,S 要与 B、A、R 协商获得与他们通信时使用的对称密钥。然后,S 利用此对称密钥逐层加密数据。

转发节点 B 收到数据包后,首先使用与 S 协商的对称密钥解密洋葱包,然后验证类洋葱包中本组管理员的签名标识,以决定是否转发该数据包。如果验证签名通过,则可以转发给下一节点 A。如果验证签名出错,则此段可能存在匿名滥用行为,节点 B 将数据包内包含的发送源地址信息 IP_s 、由节点 B 所在组管理员加密的发送源所在组管理员的地址 IP_{GMB} 一并传给本组管理员,由本组管理员委托发送

源所在组管理员解密,发送源地址。由发送源所在组管理员删除匿名滥用节点,并告知 B,本次匿名服务被撤销。

2 系统性能分析

2.1 匿名性分析

2.1.1 系统的匿名性分析

假设系统成员数为 n ,其中包括 m 个预设的入口介绍点($m < n$),系统中共有 g 个组, c 个泄密节点和 z 个自私节点。

为了便于分析,我们采用文献[3]中的定义。令 I 表示重路由路径上第 1 个泄密者的前驱节点恰是发送源的事件; $H_k(k \geq 1)$ 表示路径上的第 1 个泄密者占据第 k 个位置的事件; $H_{k+} = H_k \vee H_{k+1} \vee \dots$ 表示路径上的第 1 个泄密者位于第 k 个位置之后(包括第 k 个位置)的事件; $P(I|H_{1+})$ 表示路径上有泄密者的情况下,攻击者正确猜测发送源的概率。

系统中可以作为重路由的节点数为 $n - m - z$ 个,发送源的信誉度值为 e 。设路径长度为 $k + 1$,令 $n - m - z = t$, $\frac{n - m - c - z}{n - m - z} = q$ 。按照 $e = 10$,即最高信誉度值计算系统的匿名度。

第 1 个泄密者位于路径上的第 i 个位置的概率:

$$P(H_1) = \frac{c}{n - m - z} \left(\frac{n - m - c - z}{n - m - z} \right)^{i-1} = (1 - q)q^{i-1} \quad (1)$$

第 1 个泄密者位于路径上第 1 个位置或之后的概率为:

$$P(H_{1+}) = \sum_{i=1}^k P(H_i) = 1 - q^k \quad (2)$$

第 1 个泄密者位于路径上第 2 个位置或之后的概率:

$$P(H_{2+}) = \sum_{i=2}^k P(H_i) = q(1 - q^{k-1}) \quad (3)$$

当第 1 个泄密者位于路径上第 1 个位置时,它的前者肯定是发送源,事件 I 成立,所以 $P(I|H_1) = 1$ 。但当第 1 个泄密者位于路径上第 2 个位置或之

后时,它的前者是发送源的概率是 $\frac{1}{t - c}$,因为出现任何非泄密成员的概率是相等的,即 $P(I|H_{2+}) = \frac{1}{t - c}$ 。

$$P(I) = P(H_1)P(I|H_1) + P(H_{2+})P(I|H_{2+}) = (1 - q) + q(1 - q^{k-1}) \frac{1}{t - c} \quad (4)$$

$$P(I|H_{1+}) = \frac{P(I \wedge H_{1+})}{P(H_{1+})} = \frac{1}{\sum_{i=0}^{k-1} q^i} + \frac{q(1 - q^{k-1})}{(t - c)(1 - q^k)} \quad (5)$$

又因为 $q \leq 1$,所以 $1 - q^{k-1} < 1 - q^k$,所以:当 $\sum_{i=0}^{k-1} q^i \geq 2 + \frac{4}{t - 2}$ 时, $P(I|H_{1+}) \leq \frac{1}{2}$,即发起者的匿名度可达到 probable innocence。

2.1.2 CACSBSP 与 Crowds、PGACS 系统匿名性比较

文献[3]给出了 Crowds 系统中存在泄密者情况下,系统被攻击者猜中的概率。

文献[2]给出了 PGACS 系统的匿名性公式,PGACS 系统采取与 Crowds 相同的转发机制。在成员加入组数为 1 时,系统可看成 Crowds 系统。所以,与成员加入组数为 1 的 PGACS 系统的比较可以等同于与 Crowds 系统的比较。

为了能与 Crowds 进行比较,对 Crowds 系统采用上文的条件进行修改,则 Crowds 系统的匿名性能为:

$$P(I|H_{1+}) = \frac{(1 - p) + (1 - p^{k-1}) \frac{1}{t}}{(1 - p^k)}。$$

本系统被攻击者猜中发送源的概率为:

$$P'(I|H_{1+}) = \frac{1 - q + q(1 - q^{k-1}) \frac{1}{t - c}}{(1 - q^k)}。$$
 因为, $q < 1$,所以:

$$P'(I|H_{1+}) \leq \frac{1}{\sum_{i=0}^{k-1} q^i} + \frac{q}{t - c} = \frac{1}{\sum_{i=0}^{k-1} q^i} + \frac{q}{t(1 - \frac{c}{t})} \leq \frac{1}{\sum_{i=0}^{k-1} q^i} + \frac{1}{t}。$$

通过比较可知,本系统匿名性等于 Crowds 系统,也等于成员加入组数为 1 的 PGACS 系统。

2.1.3 系统的匿名可控性与匿名性之间的关系分析

CACSBPS 系统采用源路由方式建立重路由路径。攻击者只能获得被攻破节点前后的转发节点地址,而无法获得发送源的真实 IP 地址,因此,不会影响系统的匿名性能。而且,自私节点不参与匿名转发,有效地避免了转发路径的重试及通信失败的可能,保证了系统的匿名性。

2.2 系统传输性能的分析

洋葱路由系统利用洋葱路由器的公钥逐层进行封装。本系统中洋葱包的封装采用仅由重路由节点与发送源协商的对称密钥加密,其所需的加解密时间明显少于采用公钥机制的加解密时间。从传输效率上来说,本系统要优于洋葱路由系统。

3 仿真实验

3.1 模拟环境及测试内容

我们主要采用匿名性和匿名系统的成员负载两个指标来评估系统的性能。为了便于描述,设定如下参数: n 为系统中节点的总数, m 为系统预设的入口介绍点的数目($n > m$), z 为系统中的自私节点数, c 为系统中的泄密节点数, $\frac{n-m-c-z}{n-m-z} = q$ 。根据所设参数随机产生 p 个通信请求,即有 p 条重路由路径,设请求通信的节点为非泄密节点,路径长度和转发节点由发送源决定。规定路径长度大于 2 的为有效路径长度。自私节点和入口介绍点不参与通信。其中, p 条重路由路径中,至少存在一个泄密者的传输路径有 w_1 条,在 w_1 条传输路径中第一个泄密者之前为发送源的传输路径为 w_2 条。路径中存在泄密者的条件下,发送源被发现的概率为 $P(I|H_{1+}) = \frac{w_2}{w_1}$ 。

负载测试的基本过程与匿名性测试相同,记录每个充当重路由节点的次数,并对总负载取平均值。

3.2 模拟测试结果与分析

图 4 给出了参与重路由的节点数 $n-m$ 为 1 000, c 为 50、100, z 为 100、200,信誉度值 e 为 -1、0、1、10, $P(I|H_{1+})$ 随 e 的增加而递减。当 e 一定时, $P(I|H_{1+})$ 随 z 的增加而递增。

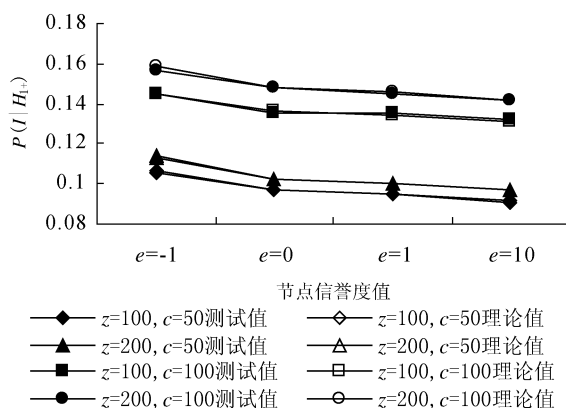


图 4 系统匿名性随节点信誉度值的变化图

图 5 给出了系统中参加重路由的成员为 1 000, c 为 50、100,信誉度值 e 为 -1、0、1、10, z 为 100、200 时,系统中节点的平均负载的变化。

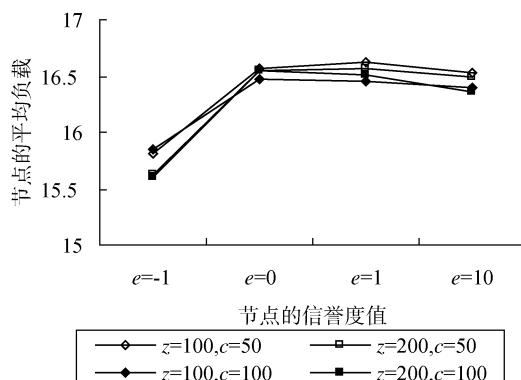


图 5 系统负载均值图

从图 5 中可以看出发送源的信誉度值从 -1 变化到 0 时,系统中节点的负载均值的变化呈上升趋势;节点信誉度值从 0 变化到 10 时,系统中节点的负载均值的变化趋势接近于直线。当 z 一定时,系统中自私节点的增加,系统中节点的负载均值变化不大。当 e 一定时,恶意节点的增加,对系统的负载影响不大。

意节点数的变化对系统的负载影响小。

4 结论

本文针对现有 P2P 匿名系统存在匿名滥用等问题,在 PGACS 模型的基础上提出了一种新的可控匿名的结构化 P2P 匿名系统(CACSBSP),通过引入对自私行为的匿名惩罚机制,具有运行高效、匿名性高、系统可扩展强的特点。通过对 CACSBSP 系统的理论分析和仿真测试,结果表明本系统的匿名性与 PGACS 系统的匿名性相同,系统中自私节点数和恶

参 考 文 献

- 1 Reiter M K, Rubin A D. Crowds: anonymity for Web transactions. ACM Transactions on Information and System Security, 1998,1(1):66—92
- 2 Wang Weiping, Luo Xi, Wang Jianxin. PGACS: a P2P grouped anonymous communication system model. Gaojishu Tongxin/Chinese High Technology Letters, 2007;17(9):912—918
- 3 王伟平,陈建二,王建新,等. 基于组群的有限路长匿名通信协议. 计算机研究与发展, 2003;4(40):609—614

Research on Controllable Anonymous Communication System Based on Structured P2P

SUN Li, WANG Xiao-gang¹

(Dept. of Computer Engineering and Science, Jiangsu University of Science and Technology, Zhenjiang 212003, P. R. China;

Dept. of Software, Changzhou Vocational College of Information Technology¹, Changzhou 213164, P. R. China)

[Abstract] The anonymous communication technology based on P2P has been playing an important role for protecting the privacy of clients, and has received a rapid development recently. In order to prevent anonymous system from abusing. A new controllable anonymous communication system based on structured P2P(CACSBSP) is presented. Based on PGACS anonymous system model, CACSBSP with two layers architecture achieves revocable anonymity by exploiting package cryptography and penalty mechanism against selfish behaviors by logging nodes credits. These mechanisms let CACSBSP have the capability of controllable anonymous. Both theoretical analysis and simulation results show that the system could provide the same anonymity as Crowds and PGACS, and the number of selfish nodes and malicious nodes has little effect on the performance of the system.

[Key words] anonymous communication revocable anonymity penalty mechanism structured P2P

(上接第 293 页)

Import Data to Excel Based on Text Formatting

LIU Yu-min, SONG Ji-bo, ZHAO Yu-feng

(College of Electricity and Information Engineering, Daqing Petroleum Institute, Daqing 163318, P. R. China)

[Abstract] A method that write data to Excel with text formatting was introduced, the development software is Visual c#. Before, Excel COM is adopt and used cell property to write data, but because of the different versions of components, there will be not compatible. If directly write with text formatting, it would not involve the issue of versions. This method is used in a natural gas production decision system, results show that this method has good compatibility.

[Key word] Visual c# Excel COM text formatting