计算机工程与应用 2010 46 (7): 110-114 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

一种可控路长的P2P匿名通信协议

邓 琳，谢 鲲，李仁发，练 琪

湖南大学 计算机与通信学院，长沙 410082

收稿日期 2008-9-17 修回日期 2008-11-17 网络版发布日期 2010-3-2 接受日期

摘要 P2P匿名通信系统带来了良好的可扩展性，然而要兼顾匿名和效率仍然是个难题。匿名技术在使用户获得良好匿名性能的同时，往往增加了通信延时及成员负载，牺牲了效率。在分析现有匿名通信技术的基础上，提出了一种新的可控路长的P2P匿名通信协议LCPACP（Length Controllable Protocol for P2P Anonymous Communication）。LCPACP采用嵌套加密来保证强匿名性，利用转发概率递减的策略来有效控制重路由路径长度，以取得高效率。理论分析与计算结果表明，新的协议能显著缩短路长，保证良好的传输性能，同时能提供良好的匿名保护。

关键词 匿名通信 P2P 嵌套加密

分类号 TP393.08

Length controllable protocol for P2P anonymous communication

DENG Lin，XIE Kun，LI Ren-fa，LIAN Qi

School of Computer and Communication，Hunan University，Changsha 410082，China

Abstract

P2P anonymous communication system brings well scalability；however，it is still a difficult problem to trade off anonymity and efficiency.Anonymous technology makes users obtain anonymous performance but contemporary often increases communication delay and member payload，sacrifices efficiency.Based on analyzing existing anonymous communication technology，this paper proposes LCPACP，a new length controllable protocol for P2P anonymous communication.It uses nested encryption to guarantee strong anonymity and adopts forwarding probability decreasing strategy to control path length to obtain high efficiency.The theory analysis and calculation results show that this protocol can not only shorten path，ensure well transmission performance，but also can provide good anonymous protection.

Key words anonymous communication P2P nested encryption

DOI: 10.3778/j.issn.1002-8331.2010.07.033

通讯作者 邓 琳 denglin0820@126.com