一种基于分组的 P2P网络安全路由算法

徐 鹤[1], 王汝传[1, 2], 韩志杰[1]

(1. 南京邮电大学 计算机学院, 江苏 南京 210003; 2 南京大学 计算机软件新技术国家重点实验室, 江苏 南京 210093)

[摘要] 当前, 对等计算 (Peer to Peer)引起了广泛的关注, 其典型应用有文件共享、即时通信等. 为了保证 P2P网络的有效运行和部署, 在现有的混合式 P2P网络中, 以现有的 P2P网络路由协议为基础, 针对路由攻击和安全隐患, 结合分组密钥管理机制, 提出了一种过滤虚假路由信息和提供消息认证的机制. 与传统的 PKI密钥管理机制不同, 该混合式 P2P网络分组密钥管理机制提供了一种基于分组密钥的 P2P安全路由机制, 能够有效过滤虚假路由信息, 为路由机制提供可靠消息认证算法.

[关键词] P2P; 路由; 分组密钥

[中图分类号] TP 393 [文献标识码] A [文章编号] 1672-1292(2008)04-0017-04

A Novel Peer to Peer Network Security Route Algorithm Based on Group

Xu He[1], Wang Ruchuan[1, 2], Han Zhijie[1]

(1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. State Key Lab of Novel Software Technology, Nanjing University, Nanjing 210093, China)

Abstract Recently, there has been a growing interest in the potential use of Peer to Peer computing (P2P) in many applications such as file sharing, instant communication. Therefore, to realize their potential, there is a need of a P2P security route algorithm that facilities the deployment of a network. Based on present P2P network route protocol, aiming at route attacks and potential security defects, combined with Block Cipher management mechanism, this paper analyzes the current hybrid P2P network and presents a algorithm which can filter false routing message and provide a message authentication protocol. The paper puts forward a novel P2P security routing mechanism using group by using the Block Cipher in the P2P network, which is different from the traditional PKI key management mechanism, and the present algorithm can filter false routing message effectively and provide a reliable message authentication protocol for routing mechanism.

Key words Peer to Peer; route; Block Cipher

目前对等计算技术(Peer to Peer Computing, P2P)已受到学术界和产业界的双重关注, 财富杂志更将 P2P列为影响 Internet未来的 4项科技之一[1]. 在对等网络中, 每台主机既是客户机又是服务器, 称之为 Peer节点. P2P网络是一个 瞬态网络[2], 网络中的节点可以随意地加入和退出, 用户可以任意地登陆到一个网络中, 共享其中的资源. 节点间相对自由的行为给网络带来了安全隐患, 因此有必要提供一种 P2P网络的安全模型. P2P网络路由协议为 P2P网络提供节点定位、资源搜索、节点的加入、退出、更新以及失效管理机制, 是 P2P网络安全的关键技术和核心机制. 但 P2P网络路由机制也面临如下安全威胁: 恶意节点编造篡改路由信息、Hello洪泛攻击、ACK 攻击、选择传递攻击、Sinkhole攻击、Sybil攻击和 Wormhole攻击等[3-7].

鉴于以上原因, 研究和分析 P2P安全路由机制具有十分重要的理论意义和现实价值. 本文在现有的混合式 P2P网络中, 以现有的 P2P网络路由协议为基础, 针对路由攻击和安全隐患, 结合分组密钥管理机

收稿日期: 2008-06-18
基金项目: 国家自然科学基金(60573141和 60773041)、国家 863 计划(2006AA01Z201, 2006AA01Z439, 2007AA01Z404和 2007AA01Z478)和江苏省高技术研究计划(BG2006001和 2007软资 127)资助项目.
通讯联系人: 王汝传, 教授, 博士生导师, 研究方向: 计算机软件、计算机网络和网格及信息安全等. E-mail: wangrc@njupt.edu.cn

制, 提出一种过滤虚假路由信息和提供消息认证的机制, 主要思想基于每个节点的 ID 产生 RSA 公钥私钥对, 节点 ID 与公私钥对是一一对应关系, 发送节点通过私钥对发布的路由信息进行加密, 接受节点通过公钥进行解密, 从而完成路由信息的认证, 过滤虚假路由信息.

1 P2P混合网络架构

本文所采用的 P2P网络架构为混合式网络架构, 是基于半分布式结构, 该结构吸取了中心化结构和全分布式非结构化拓扑的优点, 选择性能较高 (处理、存储、带宽等方面性能)的节点作为超级节点 (Super Peer), 在各个超级节点上存储了系统中其他部分节点的信息, 发现算法仅在超级节点之间转发, 超级节点再将查询请求转发给适当的叶子节点. 半分布式结构也是一个层次式结构, 超级节点之间构成一个高速转发层, 超级节点和所负责的普通节点构成若干层次. 可以进一步将半分布式结构规划为三层网状逻辑结构, 如图 1所示.

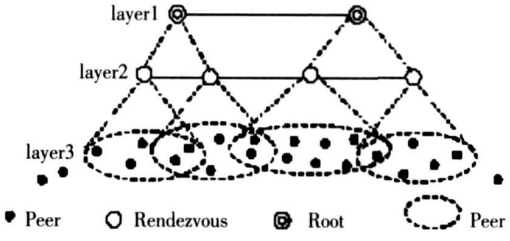

图 1 P2P 三层网状逻辑结构

Fig.1 Three layered logical structure of P2P

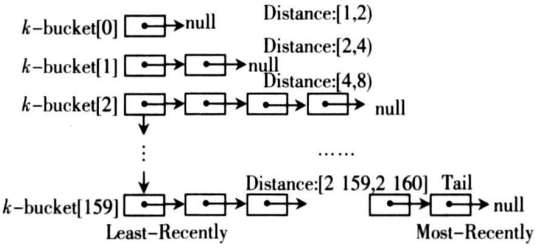

图 2 普通节点密钥的管理

Fig.2 Key management of normal nodes

2 P2P密钥管理机制

2 1 传统的 RSA 公钥密码体制[8]

随机选取两个大素数 p、q(约为 10进制 100位或更大), 且 p、q保密, 计算 $n = pq$ 和 n的欧拉函数 $(n) = (p - 1)(q - 1)$, n称为模数, 是公开的, 而 (n)是保密的, 随机选取一个 d, 且 d是与 (n)互素的正整数, 然后用欧几里德扩展算法从 $ed \equiv 1 \bmod (n)$ 中计算出 e, 即 e和 d以 (n)欧拉函数为模互为乘法逆元, (e, n)为公钥, (d, n)为私钥. 信息的加密和解密过程如下: 对于某个明文 $M = (0 < M < n - 1)$, 通过关系式 $C = M^e \bmod n$将明文 M 转化为密文 $C(0 < C < n - 1)$; 接收方收到密文 C后, 再通过关系式 $M = C^d \bmod n$ 将密文 C 还原为明文 M.

RSA 公钥密码体制实现了用一把密钥加密, 另一把密钥解密的非对称机制.

2 2 密钥的发布

考虑到 P2P网络的节点数目庞大, 而且无法采用 PKI机制[9], 使用认证中心为每一个节点来生成 RSA 公钥私钥对, 且认证中心的存在违背了 P2P网络的非中心化特征. 在本方案中采用节点自己随机生成公私钥对, 与节点 ID一一对应, 为一个三元组 (P_{id}, C_e, C_d), 其中 P_{id}表示节点 ID, C_e 表示公钥, C_d 表示私钥. 在本方案中, 超级节点和普通节点角色和作用有所不同, 超级节点除了自己生成公钥私钥对以外, 还负责收集所对应区域所有节点的公钥和私钥信息, 并对所有节点提供公开认证服务. 普通节点负责生成密钥对, 负责将密钥对发布到两个位置: (1)本区域的超级节点, 此时发 (P_{id}, C_e, C_d)三元组. (2)单项哈希节点, 并且向单项哈希节点异或距离最近的几个节点备份节点, 此时发布 (P_{id}, C_e, C_d). 为了防止恶意节点伪造和篡改其他节点的密钥信息, (P_{id}, C_e, C_d)三元组以加密文件隐藏存放到节点文件中, 防止恶意节点伪造和篡改密钥信息.

2 3 密钥管理

在超级节点中, 存在以下类型的三元组表格 (P_{id}, C_e, C_d), 具体如表 1所示. 其中为了提高查询速度, 根据节点的 ID利用二叉树组织起来, 整体查找效率为 $O(\log_2 n)$, 其中 n表示整个区域中节点的数量.

表 1 密钥结构表

Table 1 Key structure information

P_{id}	C_e	C_d
11000011	11110000	1111001

2.4　密钥存储机制

在普通节点中, 每一个节点均维护了 160个链表 (list), 其中的每个 list均被称之为一个 *K*-桶 (*K*-bucket), 如图 2所示. 在第 *i*个 list中, 记录了当前节点已知的与自身异或距离为 $2^i \sim 2^{i+1}$的一些其它对等节点的认证信息 (P_{id}, C_e, C_d), 每一个 list(*K*-桶)中最多存放 *K* 个对等节点信息.

K-桶中节点信息的更新基本遵循 Least-recently Seen Eviction原则: 当 list容量未满 (*K*-桶中节点个数未满 *K* 个), 且最新访问的对端节点信息不在当前 list中时, 其信息将直接添入 list队尾, 如果其信息已经在当前 list中, 则其将被移动至队尾; 在 *K*-桶容量已满的情况下, 添加新节点它将首先检查最早访问的队首节点是否仍有响应, 如果有, 则队首节点被移至队尾, 新访问节点信息被抛弃, 如果没有, 这才抛弃队首节点, 将最新访问的节点信息插入队尾. 尽可能重用已有节点信息、并且按时间排序是 *K*-桶节点更新方式的主要特点. 依据是在线时间长一点的节点更值得信任, 因为它已经在线了若干小时, 它在下一个小时以内保持在线的可能性将比最新访问的节点更大.

设计采用这种多 *K*-bucket数据结构的初衷主要有二: (1)维护最近、最新见到的节点信息更新; (2)实现快速的节点信息筛选操作, 只要知道某个需要查找和认证的节点 *N* 的 ID, 便可从当前节点的 *K*-buckets结构中迅速地查出距离 *N* 最近的若干已知节点, 查找节点密钥信息速度为 $O(\log N)$, 其中 *N* 为网络中节点的数量.

3　P2P安全路由机制

在 P2P网络中, 路由信息主要包括如下几种类型信息: (1) PING: 测试是否节点存在, 在 P2P路由机制中, 这种消息极易导致拒绝服务攻击 (Deny of Service, DoS攻击); (2) STORE: 存储通知的资料, 主要是把关键词和文件的哈希值存放到特定节点; (3) FIND_NODE: 通知其它节点帮助寻找节点; (4) FIND_VALUE: 通知其他节点帮助寻找值. 这些路由消息面临着各种伪造和篡改的威胁, 本文基于 RSA对路由消息进行认证和过滤, 防止虚假路由信息在 P2P网络上进行传输和散播. 具体过程分为两种方式:

(1)需要认证的节点在同一个区域内, 发送节点采用私钥对要发布的路由信息进行加密, 接受节点通过和同一区域内的超级节点进行连接, 采用 RSA认证方式对路由信息的发布者进行认证, 如果认证通过, 则接收并发布路由信息; 如果认证没有通过, 则放弃该条路由信息, 并把发布该条信息的节点列入黑名单, 拒绝该节点再次连接.

(2)需要认证的节点不在同一个区域, 分为如下步骤进行认证:　根据路由信息的发布节点 ID, 进行哈希运算, 得到一个目标 ID, 目标 ID节点或者附近节点存放有发布节点的认证密钥信息;　由查询发起者从自己的 *K*-桶中筛选出若干距离目标 ID最近的节点, 并向这些节点同时发送异步查询请求;　被查询节点收到请求之后, 将从自己的 *K*-桶中找出自己所知道的距离查询目标 ID最近的若干个节点, 并返回给发起者;　发起者在收到这些返回信息之后, 再次从自己目前所有已知的距离目标较近的节点中挑选出若干没有请求过的, 并重复步骤 2;　上述步骤不断重复, 直至无法获得比查询者当前已知的 *K* 个节点更接近目标的活动节点为止;　在查询过程中, 没有及时响应的节点将立即被排除; 查询者必须保证最终获得的 k个最近节点都是活动的;　通过步骤 1~步骤 6, 最终获得发布路由信息节点的认证信息, 采用 RSA认证方式对路由信息的发布者进行认证, 如果认证通过, 则接收并发布路由信息; 如果认证没有通过, 则放弃该条路由信息, 并把发布该条信息的节点列入黑名单, 拒绝该节点再次连接.

4　结语

与传统的 PKI密钥管理机制不同, 本文提出一个混合网络架构下密钥管理机制, 节点自己产生 RSA公钥私钥对, 在同一个区域内基于信誉值和积分以及其它信息选出一个节点作为认证中心, 负责一个区域内的节点公钥私钥认证信息, 同时为了防止超级节点不在线或者被攻击的情况, 采用基于异或距离的分布式节点认证机制.

[参考文献] (References)

[1] M R, Foster I. Mapping the Gnutella network[J]. IEEE Internet Computing, 2002, 6: 50-57.

[2] Petar Maymounkov, David Mazi res. Kademlia: a Peer-to-Peer information system based on the XOR metric[C]// Peer-to-Peer Systems: The 1st International Workshop, IPTPS 2002. Cambridge, USA, 2002: 7-8.

[3] Saroiu S, Gummadi P K, Gribble S D. A measurement study of peer-to-peer file sharing systems[C]// Multimedia Computing and Networking 2002 (MMCN2002). California, USA, 2002: 156-170.

[4] Karlo Berket, Abdelilah Essiari, Artur Muratas. PKI-based security for p2p information sharing[C]// Proceedings of the 4th International Conference on Peer-to-Peer Computing. Washington, 2004: 45-52.

[5] Paillier P. Trapdooring discrete logarithms on elliptic curves over rings[C]// Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advance in Cryptology. Singapore, 2000: 573-584.

[6] Rita Chen, William Yeager. Poblano: a distributed trust model for peer-to-peer networks[EB/OL]. (2005-03-01)[2007-04-11]. http://www.jxta.org/docs/trust.pdf.

[7] Cornelli F. Choosing reputable servants in a P2P network[C]// Proceedings of the Int'l World Wide Web Conference. Hawaii: ACM Press, 2002: 441-449.

[8] 冯登国. 密码学原理与实践[M]. 2版. 北京: 电子工业出版社, 2003: 245-257.
Feng Dengguo. Cryptography and Network Security: Principles and Practice[M]. 2nd ed. Beijing: Electronics Industry Press, 2003: 245-257. (in Chinese)

[9] 关振胜. 公钥基础设施 PKI与认证机构 CA[M]. 北京: 电子工业出版社, 2002.
Guan Zhensheng. Pulic Key Infrastructure-PKI and Certificate Authority-CA[M]. Beijing: Electronics Industry Press, 2002. (in Chinese)

[责任编辑: 严海琳]