第33卷 第18期 计 算 机 工 程 2007年9月
Vol.33 No.18 Computer Engineering September 2007
·安全技术· 文章编号：1000—3428(2007)18—0159—03 文献标识码：A 中图分类号：TP393.08

JXTA下P2P点组认证协议的设计和实现

李海宝[1,2]，张玉清[2]，韩 臻[1]
（1. 北京交通大学软件学院，北京 100044；2. 中国科学院研究生院国家计算机网络入侵防范中心，北京 100039）

摘 要：JXTA是由SUN公司推出的一项旨在为P2P应用而建立的一个通用开发平台。虽然JXTA平台提供了成员协议来验证Peer加入点组，但它没有提供认证要求的修改，在申请过程中也没有组内成员的参与。该文扩展了一种基于投票的、灵活的点组认证协议，通过实例对点组认证协议的可行性、正确性进行了验证。

关键词：对等网；JXTA；认证协议；点组

Design and Implementation of Peer Group Authentication Protocol in JXTA

LI Hai-bao[1,2], ZHANG Yu-qing[2], HAN Zhen[1]
(1. School of Software, Beijing Jiaotong University, Beijing 100044;
2. National Computer Network Intrusion Protection Center, Graduate School of Chinese Academy of Sciences, Beijing 100039)

【Abstract】JXTA proposed by SUN Corporation is designed to provide a uniform development platform for P2P application. Although there is a peer membership protocol used to validate Peer during joining Peer Group in JXTA, it does not support to modify the demand of authentication and other peers do not participate in the application. This paper proposes a novel peer group authentication protocol which is based on voting and very flexible. The validity and feasibility of peer group authentication protocol is validated by an experiment.

【Key words】P2P network; JXTA; authentication protocol; peer group

Sun公司推出了主要用于提供P2P程序所需的基础服务的JXTA[4,5]基础平台，由于JXTA具有互操作性、平台无关性、安全支持和开放性等特点，JXTA的应用越来越广，更加突出了JXTA的优势所在。也许P2P网络中的点最有趣的特性就在于它们能够动态地加入到被称为点组的协作的联盟中。点组在企业和协作计算应用程序中特别重要。在点组方面，虽然JXTA专门有Peer成员协议(peer membership protocol, PMP)来确保Peer的成员资格，它只是提供了一个“实体级”的策略，如果申请者满足加入组的要求，即可以加入该组，但是如果该对等组需要调整加入组的要求或者需要组内成员来共同参与决定时，那成员资格服务就不能实现了；节点加入组后其在组内的行为也不再受成员资格服务控制。

本文在原有的成员协议上进行扩展，给出了更灵活、更安全的、基于投票机制的点组认证协议，根据组内成员的投票结果来决定节点是否加入点组。

1 JXTA下的点组认证

1.1 JXTA协议结构

JXTA是位于操作系统或虚拟机之上、P2P网络应用或服务之下的一个P2P堆栈，它提供了P2P应用所需的核心功能。JXTA体系结构(如图1)分为3层：(1)JXTA核心层(JXTA core)，它包含了服务所需要的核心功能；(2)服务层(JXTA services)，它提供了访问JXTA协议的接口；(3)应用层(JXTA applications)，它使用服务来访问JXTA网络和JXTA提供的功能。

JXTA的服务层主要提供了一系列代表核心协议的标准服务，这些核心服务分别包括发现服务、成员资格服务、访问服务、节点认证服务、管道服务、分析服务和监测服务。

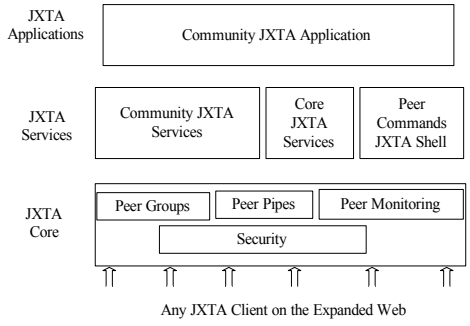

图1 JXTA系统结构

1.2 JXTA下的点组认证

为了认证一个Peer是否属于某个对等组，在JXTA中专门有Peer成员协议来确保Peer的成员资格。成员资格有两点关键特性——认证和信任状。认证是对等组的看门人，而信任状是确保认证发生的令牌，认证和信任书都可以复杂或简单，这依赖对等组的严格性。

在JXTA原有提供的点组认证协议中，某Peer是否能加入点组，要根据该节点提供的消息或证书是否满足点组的要求来决定。但是随着各种因素的改变，其加入点组的要求可能需要改变，这时就需要重新设计程序来满足新的要求；在

基金项目：国家自然科学基金资助项目(60373040，60573048)；中国科学院研究生院科研启动基金资助项目
作者简介：李海宝(1982－)，男，硕士研究生，主研方向：网络安全；张玉清，研究员；韩 臻，博士生导师
收稿日期：2006-10-13 **E-mail：**lihb@nipc.org.cn

某些对等组中，可能存在需要组内多个或者全部节点共同参与决定申请节点是否能够加入点组。对于这些需求，JXTA 原来的点组认证就不能满足。为了使 JXTA 点组认证更加灵活、更具适应性，在原有的基础上给出了扩展 JXTA 下 P2P 点组认证协议。

2 扩展的点组认证

符号说明如下：

A：申请节点。

M：组内的某个节点，作为代理节点。

PG：点组。

β：组内的所有非代理节点集合$\{\beta_1,\beta_2,\ldots,\beta_n\}$。

$SK_x\{m\}$：主体x对消息m签名。

$PK_x\{m\}$：主体x对消息m加密。

Req_{PG}：满足加入点组PG要求的相关消息。

N_x：主体x发送消息中的随机值。

T_{xy}：主体x对主体y的信任值的评估$(0\le T_{xy}\le 100)$。

TR ：加入点组的门限，当投票结果大于等于 TR 时才能加入点组。

$Cert_x$：节点x的证书。

扩展的点组认证协议大致可以分为 4 个阶段，其工作过程如图 2 所示。

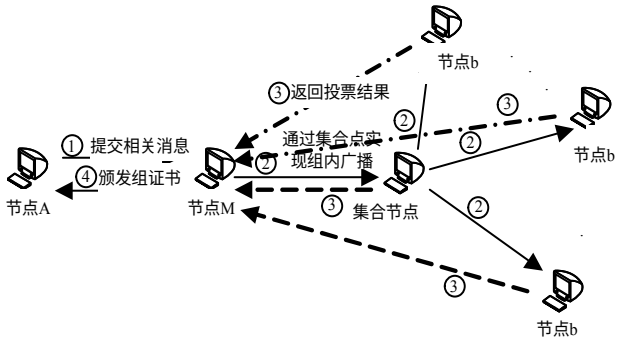

图 2 点组认证的工作过程

(1)申请加入点组

申请者和代理节点的信息交换。申请节点A根据查询组广告来知道加入该组所要的要求，并把满足要求的相关消息Req_{pg}发送给代理节点M。

m1:A → M: $PK_M\{A, N_A, \mathrm{Re}\,q_{PG}\}$

(2)代理节点转发

代理节点把消息转发给组内多个或全部节点。

m2:M → β :$SK_M\{N_M, \mathrm{Re}\,q_{PG}\}$

M 广播消息给组内其他节点β。

(3)联合投票

根据各个节点投票结果决定颁发给申请者证书。

m3: β_i → M: $PK_M\{\beta_i, SK_{\beta i}\{N_M, T_{\beta iA}\}\}$

for $i = 1,\ldots,n$

(4)颁发成员资格证书

M 根据下式计算信任值

$$T = \sum_{i=1}^{n} T_{\beta_i A} / n \qquad (1)$$

其中，$T_{\beta_i A}$表示节点 i 给申请者信任值的评估，当 T≥TR 时，节点 M 才给节点 A 颁发证书。

m4:M → A: $PK_A\{N_A, Cert_A\}$

扩展的点组认证协议主要有 2 个特点：(1)可以修改加入组的要求；(2)通过投票来决定申请者是否加入点组。对于加入组的认证要求，根据组内成员的讨论来决定，最后通过组内投票来决定加入组的要求是否更改。

3 扩展点组认证协议的实现

3.1 总体设计

基于 JXTA 平台实现的点组认证协议。认证协议的实现由 4 个模块组成：申请者处理模块，代理者处理模块，其他节点的联合投票模块和加入组要求修改模块，如图 3 所示。本文主要介绍 2 个核心模块：申请者处理过程和代理者处理过程。修改组要求模块的实现过程类似代理节点处理模块，而联合投票模块主要是接受消息和发送投票结果，相对比较简单。

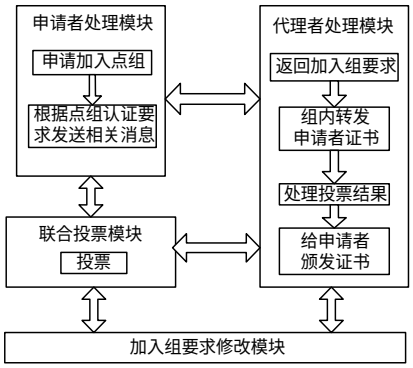

图 3 协议实现的基本框架

3.2 申请者的处理过程

当节点 A 想要参加某个点组 PG 时，首先通过查询 PG 的组广告得知加入该组所需要满足的条件，然后向社区中的某个节点 M 提出申请请求。在给 M 发申请请求消息之前，A 应该首先确定节点 M 是否活动。基于 JXTA 平台，实现了一个类似传统 ping 命令的 JXTA 下的 ping。JXTA 下的 ping 可以指定某个节点，也可以指定多个节点或者广播。其他节点为了能够响应 ping，在启动的时候可以运行监听 ping 请求。此 JXTA 下 ping 设计的框架见图 4。

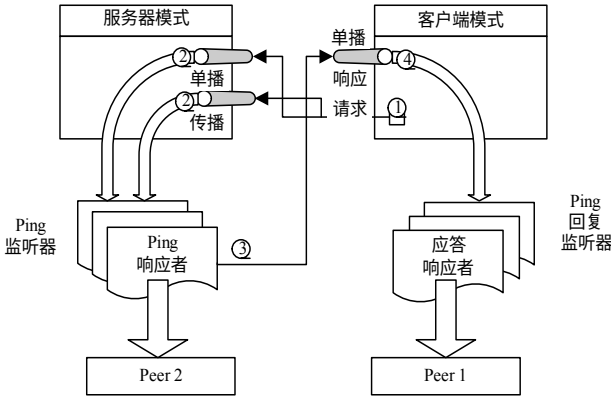

图 4 JXTA 下 Ping 的设计框架

服务器发布两个可以被客户端 pinger 发现和使用的管道。其中一个表示对创建它的点惟一的单播管道。在实现的过程中，管道是由继承自点名的名称来标识。例如，如果点名为 pier，那么管道就被命名为 ping.pierserver。另一个管道是一个传播管道。这个管道的名称为 ping.pinggroup，它能被所有在接听的点发现和发布。

服务器在发布管道通告之前，ping 命令会创建 PingHandler 类的两个对象。因为 ping 请求可能在任何一个管道上到达，所以每个 PingHandler 对应一个管道。Ping 请求将在点管道(单播)或匿名管道(传播)上到达。每个 PingHandler 都启动一个线程等待输入管道上的消息。除了在

线程中处理接收到的 ping 请求之外，ping 框架还必须通知感兴趣的监听器 PingListener 发生一个 ping 事件，并为它们提供工具来检查事件中的数据。

客户端的设计是服务器设计的镜像，但有些地方又对服务器设计进行了扩展。当客户端显示或匿名地 ping 另一个点时，ping 会创建一个管道通告和一个处理程序，这个处理程序监听到达该管道的 ping 应答。在客户端模式中使用 PingReplayHandler 来处理入站 ping 请求消息。

根据上面ping的实现，节点A首先通过ping 节点M来确定M是否活动。如果ping收到应答，那么节点A可根据ping建立的管道给节点M发消息。即节点A生成一个新鲜随机数N_A，满足加入组要求的消息和自己的身份标识用M的公钥加密后发送给节点M。其过程如图 5。

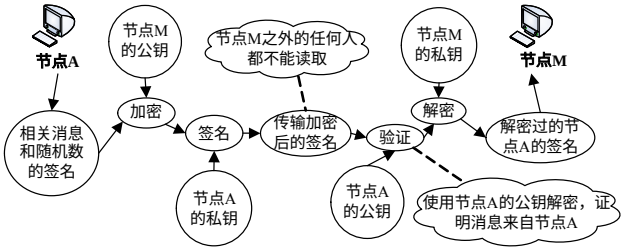

图 5　加密通信

3.3　代理节点的处理过程

当节点M受到节点A的申请请求后，节点M首先生成一个新随机数N_M，然后把随机数和申请节点提交的消息用自己的私钥加密后广播给组内其它所有节点β或某些指定的节点(根据具体的应用)。在节点M向其它节点广播消息的时候，利用广播消息的方式，如果在指定的时间没有受到足够的节点发回相应的消息，那么节点A将隔某个时间片之后再次广播此消息，直到受到足够的返回消息。在实现组内广播时，利用JXTA提供的集合点协议(rendezvous protocol, RVP)。RVP协议利用集合点来代表自己向其他的节点传播消息，图 6 显示了消息顺序。

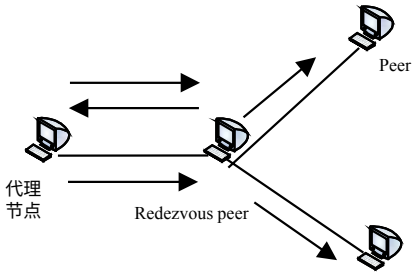

图 6　消息顺序

当节点β受到 M 广播的消息后，为了确保投票的结果到达节点 M，节点β首先 ping 节点 M，如果节点 M 活动，那么节点β就把加密的消息通过 ping 过程中建立的 pipe 传给节点 M。节点β把自己的投票结果先利用随机数进行加密，再把加密的结果利用的自己的私钥进行签名，最后把签名的结果发送给代理节点 M。上面提到当节点 M 在指定的时间的内没有受到足够的返回消息时，它将再次广播消息，这时如果节点β已经收到并把结果返回给了节点 M，那它将忽略此消息。

因为很难收集到社区内所有节点的投票，所以代理节点M在指定的时间内受到一定数量的投票的结果后即进行计算信任值。在程序实现过程中，把这个数值定为指定成员的90%，也就是如果节点M在某个时间段内收到了投票节点大于等于指定节点的 90%后，节点M即根据式(1)计算信任值。当节点的初始信任度T≥TR，点组才会给节点A颁发成员资格证书$Cert_A$。

根据组内要求得出门限 TR 为 65，而投票结果为 70，则代理节点给申请节点颁发证书(证书如图 7 所示)。在节点 M 给节点 A 颁发证书时，节点 M 首先 ping 节点 A，确定节点 A 是否活动，如果活动，即利用 ping 时建立的 pipe 把证书传给节点 A。

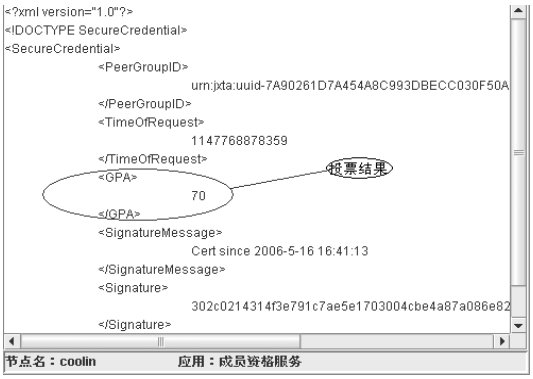

图 7　颁发的证书

4　总结

本文分析了 JXTA 下 P2P 点组认证上存在的不足，并在其基础上进行了扩展。当对等组随着时间或其他因素的变化时，可以通过组内投票来改变加入组的要求；在申请节点的加入点组的过程中，组内的其他节点也参与评审，这样更加体现了对等网络的对等性，也使点组认证更加灵活。需要指出的是，对于点组加入对等组后根据其在组内的行为、表现来相应地更改其评审值(即投票结果)。更新组内成员关系等问题须进一步地研究与探讨。

参考文献

1 Fox G. Peer-to-Peer Networks[J]. Computing in Science and Engineering, 2001, 3(3): 75-77.

2 Singh M P. Peering at Peer-to-Peer Computing[J]. IEEE Internet Computing, 2001, 5(1): 4-5.

3 Parameswaran M, Susarla A. P2P Networking: An Information Sharing Alternativ[J]. IEEE Computing, 2001, 34(7): 31-38.

4 Project JXTA: A Technology Review[Z]. (2006-05). http://www.jxta.org/project/www/docs/TechOverview.pdf .

5 Li Gong. Get connected with Jxta[C]//Proc. of Conference on Sun Microsystems JavaOne. 2001-06.

6 常晓波. Java P2P 程序设计[M]. 北京: 中国电力出版社, 2003.

7 Oaks S, Traversat B, Li Gong. JXTA 技术手册[M]. 北京: 清华大学出版社, 2004.

8 朱　岱. 深入Java™ 2 平台安全[M]. 北京: 电子工业出版社, 2004.