一种基于 JXTA 的协同工作 P2P 系统*)

孟 波[1] 马 勇[1,2] 张玉清[2]

(武汉大学计算机科学与技术学院 武汉 430072)[1]

(中科院研究生院国家计算机网络入侵防范中心 北京 100039)[2]

摘 要 针对目前分布式协同设计软件的特点,本文提出了一种基于 JXTA 协同设计 P2P 模型。介绍了该模型的总体结构和节点结构、群组通信的算法和相应的通信协议的设计、用户和系统的双向认证机制。该系统具有高效、分散、安全和健壮等特点。最后以协同绘图作为实例验证了系统的正确性和实用性。

关键词 CSCW,P2P,JXTA,群组通信,安全

Research on Collaborative P2P System in JXTA

MENG Bo[1] MA Yong[1,2] ZHANG Yu-Qing[2]

(School of Computer Science& Technology, Wuhan University, Wuhan 430072)[1]

(National Computer Network Intrusion Protection Center, GSCAS, Beijing 100039)[2]

Abstract A collaboration development P2P system in JXTA is put forward in accord with the current distributed collaboration design software in this paper. Key issues, including system and peer structure, group communication, communication protocols, two-side authentication between the system and peer, are discussed. The system features on high performance, decentralization, security and robustness. Collaboration picture, as an example, verifies the validity and practicability of the mode.

Keywords CSCW,P2P,JXTA,Group communication,Security

1 引言

自从 1984 年 MIT 的教授首次提出了协同工作的概念以来,先后出现了协同编辑系统、协同绘画和更为复杂的协同设计软件。协同方式从交换数据文件的粗粒度松散耦合的协同工作,发展到集成多种 CAD 软件传递用户操作和设计意图的细粒度的紧密耦合的在线集成。但是前者是异步协同设计,不可能快速从其他协作者那里得到反馈信息;后者是同步协同任何一个协作者,可以从其他协作者那里得到反馈信息。网络结构有传统的客户机服务器模型、采用分布式对象的或者基于 Agent 的客户浏览器模型。采用分布式对象的典型系统有 SDRC 公司开发的 Open I-DEAS、MIT 的 Pahng 等研究开发的 DOME[1]和陆薇等改进的 CAD 支撑系统构件/软总线模型[2]。采用 Agent 代理封装技术的典型系统有美国 NASA Ames 研发中心的 Gee 开发的自治 Agent[3]、林守勋等研究的多 Agent 协同工作环境[4]和何发智等研制的 CoCaD-ToolAgent 等[5]。

无论采用客户机/服务器模型(C/S),还是采用客户浏览器模型(B/S),其差异主要是对业务划分的不同配置。系统或多或少都要受到服务器的限制,服务器成了系统运行和安全的瓶颈。C/S 和 B/S 这两种结构都是一个以站点为中心的物理网络,同时由于 NAT、DHCP 和防火墙的存在限制了不同物理网络之间的通信。而 P2P 网络是建立在现有网络之上的更强调功能应用的逻辑网络,以反集中和实现多个节点的并行工作为主要特点,强调节点的自由工作,更能体现协同工作的特点。

SUN 公司开发的 JXTA[6]协议簇为 P2P 的应用提供了一个很好的开发平台,适合计算机支持的协同工作。其主要特点有:①单个节点同时完成了客户机和服务器的功能,节点之间功能相对独立,便于角色的划分;②有共同兴趣的用户组成了一个小组,以组为单位对资源进行管理;③实现了资源标识的唯一性,不同的资源具有不同的标识;④提供了多种组服务机制,允许用户自己扩展组服务,把扩展的组服务作为组广告的一部分在点组内广播;⑤节点之间的消息以 XML 形式进行传递,便于设计针对具体应用的通信协议。

JXTA 协议所具有的特点十分符合计算机支持的协同工作的要求。本文采用 JXTA 来开发 FP2PCD(Framework for the Peer-to-Peer Collaborative Design)。FP2PCD 主要具有如下特性:①各个协同者组成一个动态的协同网络;②以组为单位对协同者进行管理;③高效:多个协调者可以同时工作;④安全:实现协同者和组之间的双向认证和协调者之间的安全通信。同时,FP2PCD 采用 JXTA 天生具有的如下特点:独立于具体的编程语言、通信协议、操作系统和硬件平台;可以集成多种设备,如智能手机、PDA、计算机等设备;可以不受 NAT、DHCP 和防火墙的限制,使网络更好地联通。

本文第 2 节描述了 FP2PCD 总体结构和单个对等体的结构,对单个对等体的构成模块进行了详细的描述。在第 3 节给出了 JXTA 下如何实现节点之间的安全可靠的群组通信和通信协议的设计。第 4 节给出节点和群组之间的双向认证,实现系统的安全性。第 5 节给出了与以前的基于 SOCKET 和 CORBA 集中协同模型的对比及其应用实例。

*)由国家 863 计划资助项目(2003AA142150)和自然基金项目(60373040)支持。

2 FP2PCD 系统设计

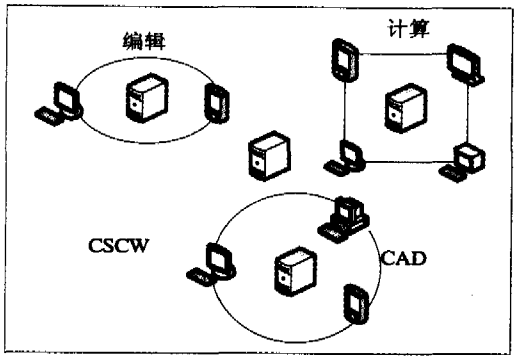


图 1 FP2PCD 的总体结构

2.1 总体结构

JXTA 以组为单位对资源和节点进行管理，每一个组的成员既可以是另外的一个点组，也可以是一个对等点。图 1 给出了 FP2PCD 总体结构的一个简单示意图，其中点组 CSCW 由编辑、绘画和 CAD3 个点组和一个任务注册服务器组成。同样，CAD 点组是由共同完成 CAD 设计的协作者和一个提供全局唯一逻辑操作序列的序列服务器所组成。节点从序列服务器获得全局唯一的逻辑操作序列号后，向其他节点传递操作命令。正是由于序列服务器保证了全局操作的一致性。

有相同兴趣的协作者组成了一个组，点组内的协作者才能执行相应的操作。只有 CAD 点组的成员才能发送和接收到 CAD 操作命令。如果一个协作者也拥有同样的爱好，可以申请加入这个点组，经过点组的认证后才能加入点组。任务的创建者可以成为点组的管理者，其他协作者承担工程师的角色。FP2PCD 是以点组为单位对协同者进行管理（第 2 点）。协作者可以根据自己的爱好选择加入编辑点组或绘画点组，可以在任何时候申请加入和离开点组。各个协同者组成了一个动态的网络（第 1 点）。

2.2 节点结构

FP2PCD 的各个协作者同时扮演了客户机和服务器的角色，既要负责捕获用户的输入，将用户的输入转换成命令，发送给所有的协作者，又要将别的协作者传递来的命令，按序输出。FP2PCD 的节点由打包器、JXTA 协议层和互联网络组成。图 2 给出了 JXTA 单个节点的 3 层结构，图 3 给出了打包器的具体结构。外打包器位置上靠近 JXTA 协议层，通过内打包器访问数据和请求操作。外打包器将内打包器传递来的命令转换成中性协议调用，通过 JXTA 管道服务传递给其他协同者；把 JXTA 层传递来的其他协同者的操作转换成 CAD 软件 API 调用，传递给内打包器的协同控制器。“命令↔中性协议”模块实现客户端 API 和中性协议之间的互相转换。

当客户通过 GUI 进行操作，感应器将会感知事件的发生，自动地将事件传递给其他对象，例如用户拷贝、删除或者修改对象，或者当用户执行 UNDO 和 REDO 命令，内打包器中的监控器将会根据事件产生相应的命令。另外，内打包器也会按照全局唯一顺序执行的命令，在终端输出结果。打包器可使不同的 CAD 软件协同工作。

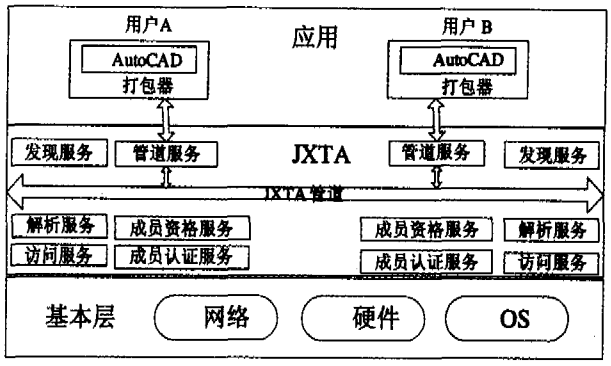


图 2 FP2PCD 节点的三层结构

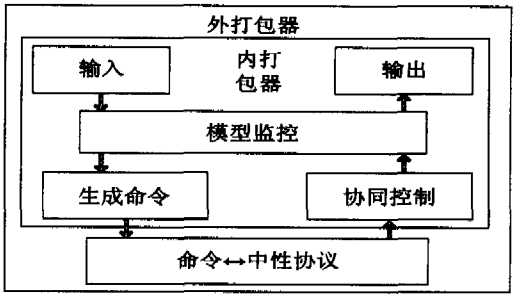


图 3 打包器的结构

JXTA 协议层主要为协作者提供基本的服务。发现服务让协作者在对等组内搜索资源（Peer、对等组、管道），解析任务可以把查询任务分发到同一组的其他实体上。我们利用点组和对等点之间双向认证的点组资格成员服务替换了默认的成员资格服务，确保了双方身份的合法性。通过向加入点组的节点颁发我们项目小组开发的 ExSPKI 证书来作为通信期间的成员资格证明[7]。ExSPKI 证书实现了授权和认证的统一，可以同时兼容目前流行的多种证书（Kerboros 票据和 X.509 证书等），摆脱传统 CA 的限制，更加符合 P2P 的特点。认证服务使用成员资格服务颁发的证书来确认点组成员的消息正确性。访问服务要求发出请求的协作者提供证书以及访问服务所要求的信息来确定是否允许访问。我们利用公密钥提供安全的管道服务、管理和创建点组中协作者之间的管道连接。

3 FP2PCD 群组通信设计

3.1 群组通信的建立

点组成员之间通过管道进行通信。管道通信是一种异步和无方向性的消息传输机制。我们使用 JXTA 进行通信，单播管道类似于用户数据报协议（UDP），并不是十分可靠。如果需要在两个确定的节点之间建立管道连接，通信节点的双方必须知道用来建立通信的管道 ID。因此，我们创建管道并且使用 JXTA 的参考实现里提供的单向散列函数的哈希值来生成管道 ID。图 4 给出了当一个协作者加入点组后如何建立双向安全的群组通信的方法，协作者可以直接向其他节点发送消息而不用经过中心节点的转发，有效实现了多个协同者的并行同步工作（第 4 点）。建立双向安全的群组通信，可以分为得到组内节点、建立双向管道和建立会话密钥 3 个阶段，具体步骤如下（见图 4）：

（1）得到组内节点。

①～②新加入的节点 Loc 向组成员资格服务查询组内的

节点。

(2) 建立双向管道。

③~⑤建立了节点之间的双向连接。首先根据 RemWaitID(单向散列函数(点组 ID+节点 Rem 的 ID))建立节点 Loc 到节点 Rem 的联系,节点 Rem 根据 Rem2LocID(单向散列函数(节点 Rem 的 ID+节点 Loc 的 ID))建立到节点 Loc 的连接,节点 Loc 根据 Loc2RemID(单向散列函数(节点 Loc 的 ID+节点 Rem 的 ID))建立到节点 Loc 的连接。⑥断开自己的等待管道和节点 Loc 的连接。⑦节点 Loc 建立自己的等待管道,等待以后加入节点的连接。

(3) 建立会话密钥。

⑧~⑨利用双方的公钥对一随机数进行加密,确定节点之间进行信息传输的会话密钥。EKrem(会话密钥) 表示用节点 Rem 的公钥对会话密钥进行加密,EKLoc(会话密钥) 表示用节点 Loc 的公钥对会话密钥进行加密。

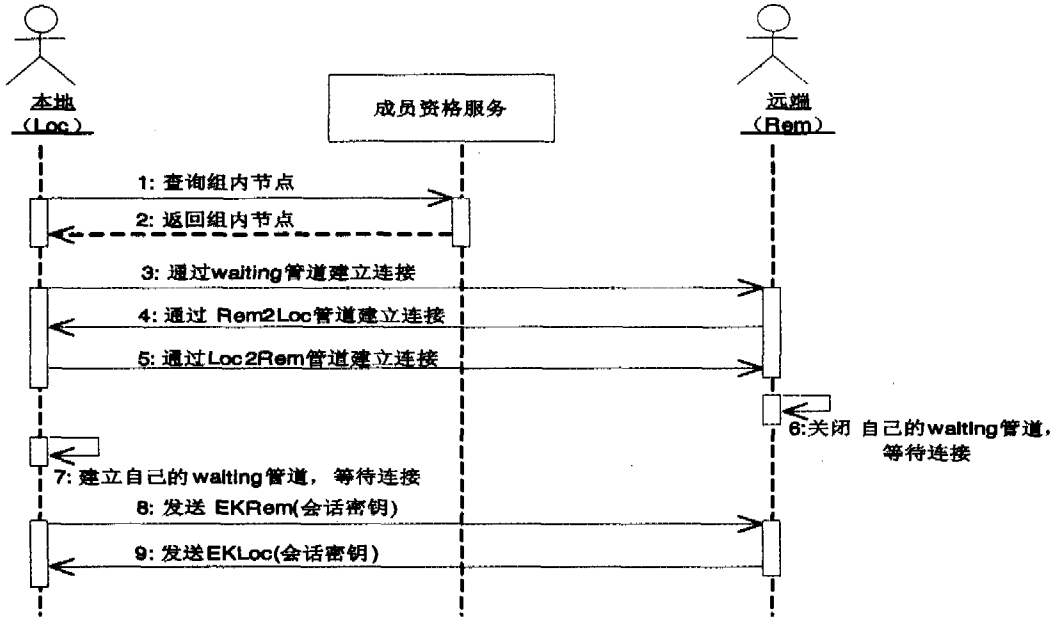


图 4 建立双向安全的群组通信

3.2 群组通信协议

为了支持不同 P2P 协同设计,FP2PCD 采用了变长的通信协议包格式。对于新的不同的 P2P 协同设计,仅需调用对应的基本属性的积累协议单元,而不必重新刷新通信包的全部属性。协议包编码格式描述如下:

〈MessagePacket〉::=〈Prefix〉,〈Style〉,〈State〉,〈SerialNo〉^{0,1},〈Parameters〉^{0,1}

〈Prefix〉::=〈String〉

〈Style〉::=〈EDIT〉 | 〈PICTURE〉 | 〈CAD〉| …

〈State〉::=〈APPLY〉 | 〈SUBTASK〉 | 〈CONFLICT〉 | 〈SERIALNO〉

〈SerialNo〉::=〈Integer〉

〈Parameters〉::=〈Operations〉 | 〈Others〉

〈Operations〉::=〈ADD〉 | 〈DELETE〉

〈Others〉::=〈String〉 | 〈Integer〉 | 〈Double〉| 〈Array〉 | …

协议包的编码格式中,'0,1'该项可以省略,如果出现也只能出现一次;'|'子项之间进行逻辑运算里'或运算'。下面以二维协同绘图作为实例说明通信协议在实际中的应用,示例如下:

(1)申请序列号

协作者和序列服务器之间以流的形式进行传输。协作者把最近执行的全局序列号和本地生成的命令打包后发送给序列服务器,申请分配全局序列号。其消息格式如下:

"CSCW|CAD |APPLY|SerialNo|Parameters"

(2)分配任务

序列服务器判断该命令是不是该协作者未执行的,而序列服务器已经接收的命令是否冲突? 如果不冲突,序列服务器把全局序列号返回给协作者。返回的消息格式如下:

"CSCW|CAD |SERIALNO |SerialNo"

如果冲突,序列服务器就会拒绝该协作者的申请。返回的消息格式如下:

"CSCW|CAD |CONFLICT"

(3)向其他协作者传送命令

协作者把要发送的命令和全局序列号打包后,将消息发送给组内的其他协作者。如果协作者新绘制了一个圆,发送的消息如下:

"CSCW | CAD | SUBTASK | SerialNo | ADD | Starting-point | End-Point"。

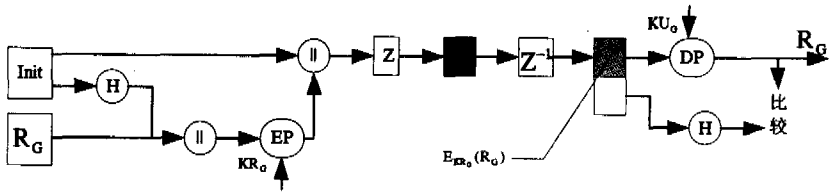
4 安全设计

我们采用点组和协作者之间双向认证的组成员资格服务和采用会话密钥对传输内容进行加密的管道服务替换了 JXTA 默认的成员资格服务和管道服务,从而确保了加入用户的合法性和通信的安全,很大程度上避免了用户的恶意行为,提高了系统的安全性(第 4 点)。图 5 说明了节点和组之间双向认证的过程,我们用节点和组之间双向认证的组成员资格服务来替换 JXTA 默认的组成员资格服务。

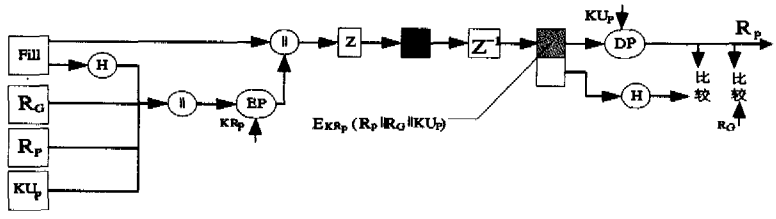
(1)用户 P 申请加入点组 G,点组 G 传递给用户 P 一个随机数 R_G,用来完成组对用户 P 的认证。这个过程如图 5(A)所示。

(2)用户把自己的公钥 KU_P 和随机数 R_G、R_P 用自己的私钥加密后返回给组 G,组 G 通过验证 R_G 是否一致来完成对用户 P 的认证。这个过程如图 5(B)所示。

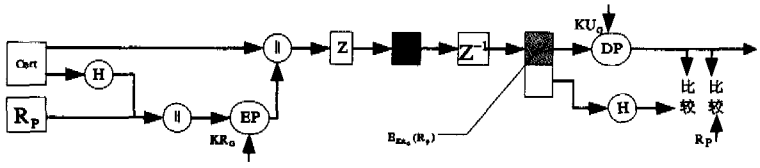
(3)组用自己的公钥 KU_G 对随机数 R_P 加密后返回给用户 P,用户 P 通过验证 R_P 是否一致来完成对用户组的认证。这个过程如图 5(C)所示。



(a) 用户 P 申请加入组



(b) 组对用户 P 的认证



(c) 用户 P 对组的认证

图 5 节点和组双向的认证

经过以上 3 步的操作,将会建立一个参与者和点组之间的双向认证。点组向用户颁发 ExSPKI 作为其身份凭证,参与者在点组内广播包含有点 ID 及其公钥的点广告。点组内的任何两个协作者进行通信时,可以采用双方的会话密钥对传输的内容进行加密。这样可以通过管道进行密文传输,对方接受到信息后使用会话密钥进行解密。从而可以大大提高通信的安全性,防止别人对信息的恶意篡改。因为采用对称加密体制,信息加密的速度很快,并不会因为对数据进行加密和解密而造成时间上的延迟。

5 比较和实例

表 1 FP2PCD 和集中式结构对比

	FP2PCD	WebSPIFF	WebCosMos
操作系统	Windows Linux	Windows	Windows
通信协议	JXTA	SOCKET	JAVA3D CORBA
结构	P2P	集中	集中
效率	点到点直接通信(高)	集中转发(低)	集中转发(低)
安全	授权 认证	操作系统安全性	操作系统安全性
粒度	支持细粒度	细粒度	细粒度
异步	同步	同步	同步
鲁棒性	强	单点失败	单点失败

我们以 Windows 2000、JXTA 2.0(C 语言版)、FP2PCD 1.1 (C 语言版)和 AutoCAD2002 作为软件平台,利用 FP2PCD 对 AutoCAD2002 进行了封装,使多个单机版 AutoCAD 2002 可以协同设计。图 6 显示了 FP2PCD 在 AutoCAD 上的二维协同绘图的实例。FP2PCD 采用 JXTA 平台协议簇可以很好地屏蔽不同操作系统和硬件的差异;由于采用点到点的工作模型节点,具有更大的灵活性;节点之间直接通信不需要某个中间节点的转发,确保了通信效率的提高;不存在中央服务器,避免了单点失败导致系统的失败,具有较强的鲁棒性;通过点组和用户的双向认证确保了用户身份的合法性;实现了安全可靠的群组通信,确保系统消息传递的可靠性。表 1(WebSPIEF 和 WebCosMos)在操作系统、通信协议、结构、效率、安全、粒度、异步和鲁棒性等方面对 FP2PCD 和集中式结构进行了对比。

图 6 FP2PCD 利用 AutoCAD 进行协同绘图

结束语 本文结合现有的分布式协同工作系统的特点,设计了一种基于 JXTA 的协同开发 P2P 系统(FP2PCD),为分布式协同工作系统的设计提供了一种新的手段和方法。采用点到点的网络拓扑结构和以组为单位进行管理,更能符合

(下转第 116 页)

SASL 安全配置文件获得 SASL 协议的支持，提供联动实体间的认证。

因此，根据上面给出的定义和证明，在此基础上组合而成的 SIPF 的安全性质是可以保持的，且安全联动模型 SIM 的安全性得到保证。

6 模型的应用

根据上述的安全联动模型，我们在 Linux 环境下实现了 SIM 应用程序库 Libsim，它的核心是一个无限的循环，它等待联动事件的出现并处理它们。联动事件由 SIM 的通信模块 Beepcore 来处理，然后再调用用户定义的其他函数做进一步的处理。SIM 应用程序库 Libsim 的结构如图 2 所示。

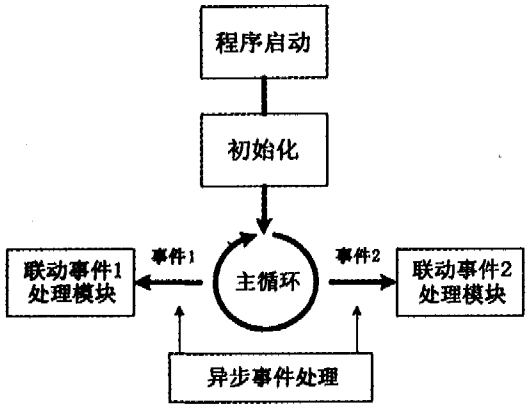


图 2 SIM 应用程序库的结构

以 SIM 为框架，可以实现防火墙和 IDS、Honeypot、安全审计系统等之间的联动，从整体上构建一个安全联动系统。在 Linux 环境下，我们使用 Netfilter/Iptables、Snort 和 Libsim 构建了一个由防火墙与 IDS 组成的安全联动系统，结构如图 3 所示。

在这里，入侵检测系统中集成了一个安全联动 Client，即前面所说的 SIM Client；而防火墙系统中集成了一个安全联动管理 Console，即 SIM Server。入侵检测系统中的传感器/分析器和管理器，对网络数据流进行监视，一旦发现入侵行为发生，立即生成报警、阻断信息。安全联动 Client 将事件信息发送给安全联动管理 Console，实现它们之间的通信。其中的联动事件转换模块主要完成对联动事件信息格式的转换和加密。在 SIM 模型中，联动信息都采用 SIMEF 格式描述，XML 负责数据的表示。安全联动管理 Console 通过事件引擎完成对联动事件信息的收集和分类，再由事件分析模块结合联动策略库，分析匹配接收的联动事件，对分类的联动事件采取不同的响应策略，达到阻断攻击、主动防御的目的。

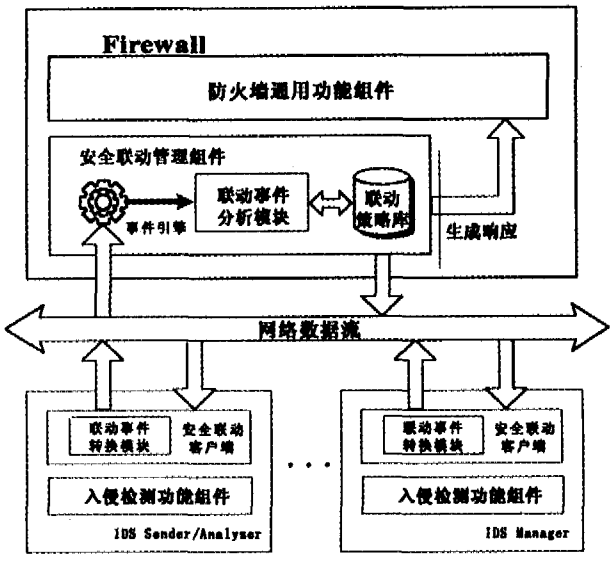


图 3 防火墙与 IDS 联动的实现过程

结束语 本文构建的安全联动模型 SIM 采用标准化协议，保证了各个安全系统间联动信息的安全通信，并对数据格式进行统一描述，具有通用性、可扩展性好的特点，方便实现。采用 SIM 模型实现的防火墙系统可以具备安全联动管理的能力，能够实现对其他安全系统的联动管理、协同控制，及时遏制网络不安全事态的发展。

参 考 文 献

1 Rose M T. The Blocks Extensible Exchange Protocol Core [S]. RFC3080, 2001
2 Rose M T. BEEP: The Definitive Guide[M]. O'Reilly Press, 2002
3 Dierks T. The TLS protocol version 1.0[S]. RFC2246, 1999
4 Myers J. Simple Authentication and Security Layer (SASL)[S]. RFC2222, 1997
5 Curry D. Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language Document Type Definition [EB/OL]. http://www.ietf.org/proceedings/03nov/I-D/draft-ietf-idwg-idmef-xml-10.txt, 2003
6 Menga J. CCSA NG: Check Point Certified Security Administrator Study Guide[M]. Sybex Press, 2003

(上接第 87 页)

人们进行协同工作的模式，突破了服务器的瓶颈，使系统更加高效和具有良好的鲁棒性。同时，由于 JXTA 是一个开源项目，我们可以根据自己的需要进行修改。在 FP2PCD 系统里，节点和点组之间双向认证的组成员资格服务和使用会话密钥对传输的内容加密的管道服务替换了 JXTA 默认的服务，使系统更加安全。但是，我们还需要进一步研究具体的 CAD 软件实体结构、API 命令，充实和完善中间协议，使 FP2PCD 更好地集成不同的 CAD 软件。

参 考 文 献

1 Pahng F, Senin N, Wallace D R. Distributed modeling and evaluation of product design[J]. Computer-Aided Design, 1998, 30(5): 411～423
2 陆薇，孙家广. CAD 支撑系统构件-软总线模型[J]. 计算机辅助设计与图形学学报，2001，13(1)：1～7
3 Gree K. Vehicle analysis using an agent based analysis tools frameworks[A]. In: Proc. of 2001 ASME Design Engineering Technical Conference[CD], Pittsburgh, Pennsylvania, 2001, DETC2001/CIE-21290
4 林守勋，林宗楷，郭玉钗，等. 多 Agent 系统工作环境 MACE [J]. 计算机学报，1998，21(2)：188～193
5 高曙明，何发智. 分布式协同设计技术综述[J]. 计算机辅助设计与图形学学报，2004. 849～855
6 Project JXTA. http://www.jxta.org/
7 Zhang Dehua, Zhang Yuqing. SAP2P: A P2P Network Security Architecture based on Trust Management System. In: The 2004 International Conference on Parallel and Distributed Processing Techniques and Applications, PDPTA'04, Las Vegas, Nevada, USA, 2004. 849～855