文章编号:1001 - 9081(2005)02 - 0377 - 04

移动因特网中安全组播通信的密钥管理研究

王国军,廖 麟,马 好
(中南大学 信息科学与工程学院,湖南 长沙 410083)
(csgjwang@csu.edu.cn)

摘 要:比较了各种确保安全组播通信的密钥管理算法和方案,针对移动环境下移动频繁、可靠性差的特点,讨论了在 RingNet 结构下移动因特网的组播密钥管理问题。

关键词:IP 组播;密钥管理;移动因特网;RingNet 结构
中图分类号: TP393.08 **文献标识码**:A

Survey on key management for secure multicast communications in mobile Internet

WANG Guo-jun, LIAO Lin, MA Hao
(School of Information Science and Engineering, Central South University, Hunan Changsha 410083, China)

Abstract: A survey of many kinds of schemes was present about secure multicast key management. In the meanwhile, in view of mobile environment, frequent handoff and poor reliability are the key properties and differences. Thus the secure multicast key management strategy in mobile Internet was discussed deeply in the survey.

Key words: IP multicast; key management; mobile Internet; RingNet hierarchy

0 引言

随着无线技术的成熟,人们开始随时随地利用各种无线设备对网络进行访问。支持移动性已经成为通信发展的必然要求。在移动环境中,由于移动节点使用无线链路,因而明显的特征就是链路带宽受限、错误率高,同时由于移动节点体积较小导致它的处理器能力和存储能力都比较低。IP 组播高效利用资源的特点可以有效地弥补上述不足。将组播技术和移动技术结合,在移动网络中确保组播通信的安全性成为了一个重要的研究领域。移动因特网组播不仅要考虑移动主机的特点(如资源能源受限),无线通信的特点(如带宽窄、延时大、可靠性差),还要考虑因主机的移动性带来的突出特点:1) 成员关系的动态性和位置的动态性;2) 成员数量相当巨大并且相当分散。

1 基本概念

1.1 IP 组播

1989 年,IETF 通过 RFC1112,定义了因特网上的组播方式。组播技术依靠 IGMP 协议,中间经过具有组播能力的路由器的多次复制和转发,将数据包从一个发送方同时向一组任意数目的接收方发送。在固定的因特网上,一般使用两级的组播传输模型。在局域网级,主机必须连接到本地局域网的组播路由器上,通过组管理协议 IGMP 和组播侦听发现协议 MLD,申请加入或退出某个应用组。本地组播路由器记录本地局域网组成员,通过 IGMP 和 MLD 协议查询消息以维持组成员关系。在广域网级,组播路由器采用组播路由协议交换组信息,建立和管理组播传输树,通过组播传输树发送组播分组到叶节点组播路由器。

1.2 移动 IP

移动 IP 是一个对 IP 移动性的网络层的解决方案。移动 IP 的移动性是指,移动节点可以改变物理位置而且保持当前的连接不被中断,使移动节点能够以一个永久的 IP 地址连接到任何链路上。移动 IP 通过在合适的节点上设立路由表,最终将 IP 包发送到不在家乡链路上的移动节点。移动 IP 定义了 3 种功能实体:家乡代理(Home Agent, HA)、外地代理(Foreign Agent, FA)和移动节点(Mobile Node, MN)。家乡代理 HA 是移动节点的本地网络上的服务器,负责维护移动节点的当前位置信息,截获送往移动节点家乡地址的数据包,通过隧道送往移动主机的转交地址处。FA 提供移动节点的转交地址,维护当前漫游到本子网的主机信息,并为其提供存储转发服务。

2 移动网络中组播通信面临的问题

随着组播通信开始走向实际应用,组播通信中的安全问题越来越突出。在移动环境中,组播不仅要管理动态组成员,建立和维护组播树,还需要解决组成员位置动态变化的问题。由于组成员的动态性,组播通信为了达到较高的安全性,组密钥以及用于方便组密钥管理而引入的有关辅助密钥在成员的

收稿日期:2004 - 07 - 13;**修订日期**:2004 - 11 - 02
基金项目:国家自然科学基金资助项目(90104028);中国博士后科学基金资助项目(2003033472)

作者简介:王国军(1970 -),男,湖南长沙人,副教授,博士,主要研究方向:计算机网络、容错计算、移动计算、分布式计算; 廖麟(1981 -),女,湖南岳阳人,硕士研究生,主要研究方向:移动因特网中的安全组播通信; 马好(1980 -),男,湖南益阳人,硕士研究生,主要研究方向:Petri 网、移动自组网、故障诊断.

离开和加入时应该更新,这使得离开的成员无法访问目前的通信量即向前安全性(Forward Confidentiality),同时一个新加入的成员也无法访问以前的通信量即向后安全性(Backward Confidentiality),因而,组密钥更新问题是整个组播安全问题的核心问题。对于一个节点从一个蜂窝移动到另一个蜂窝,或是移动中出错,或是移动到不存在组播传播树的网络区域等情况,都是移动网络中的组播通信必须解决的问题,因此已有的群组通信系统不能简单地移植到移动因特网中来。

由于组播用户处于不同的地理位置,不同的网络结构和特性,以及无线网络的局限性等因素,构建组播密钥管理系统有如下的标准和原则:密钥的数量和结构不应该随着用户数目的增加而大量增加,即可扩展性;系统支持现有的网络结构和网络组成,即独立性、可靠性;更新密钥时发送的更新消息尽可能少;系统鲁棒性即避免单点故障等。

3 密钥管理研究现状

所有基于组播的应用程序都需要提供组播内容的访问控制机制。典型的访问控制是通过加密来完成的,而这个过程与密钥信息的分发紧密相连。针对组通信密钥管理问题,现在学术界提出了很多解决方案,如基于核心基本树路由算法CBT的可伸缩多播密钥分配方案SMKD、HCD、MKMP、IOLUS方案和密钥树(图)方案[1]。其中IOLOUS和密钥树(图)方案成为了后来越来越多改进方案的基本思想。

在IOLUS方案中,一个群组被划分为多个子组,子组被组织成一个树型层次结构。由于每个子组相对独立,因而成功地解决了可扩展性的问题。分发树上的每一个子组具有单独的子组地址,可以使用任意组播协议。每一个子组拥有自己的子组密钥KSGRP,因而不存在所谓的全局会话密钥。子组内部有成员加入或退出时,密钥更新只在此子组内进行,不会影响其他子组。因而只有子组的KSGRP需要更新,可扩展性问题得到了很大程度上的缓和。在IOLUS的框架中,提供了两类实体用于管理和联系各个子组,分别是GSC(Group Security Controller)和GSI(Group Security Intermediaries)[2]。GSC管理最顶层的子组,即在分发树的根部层;GSI类似于GSC的代理服务,负责各个子组。GSI在加入时都有各自的层次位置,它成为了各个子组之间通信的桥梁。GSI可以从它的父节点或是孩子节点接收组播数据,又可以分别组播数据给父亲节点和孩子节点。GSC和GSI统一称为GSA(Group Security Agent)。该方案的一个问题是GSIs解密和加密每一个数据包所引入的延迟开销是影响系统性能的重要因素。由于各个子组通信密钥由各GSI自行产生,因此GSI的信任问题也会变得很复杂[3]。

在密钥树(图)方案中,所有的密钥由一个集中的密钥服务器生成,并且使用一个逻辑树层次结构来维护三种类型的密钥:1)所有成员共享的会话密钥(Session Key);2)每一个成员拥有的各自的成员密钥;3)为从密钥服务器沿着树路径传递密钥信息给叶子节点所使用的辅助密钥。由于成员变化时必须更新群组密钥并影响到部分成员,因而可扩展性不够好。因此基于密钥树的思想,学术界又提出了很多密钥管理策略。如借鉴Huffman编码思想,采用用户离开概率模型构造密钥树,使得平均密钥更新代价和用户密钥存储量最小。下面简单介绍两种基于树的密钥管理。

3.1 移动网络中的匹配密钥管理树

3.1.1 TMKM树的安全策略

组播应用的访问控制大部分都是使用加密密钥树来更新和维护。在普通的组播密钥管理树中,大部分的更新密钥消息仅仅适用于一个用户子集,而这些用户子集也仅仅是在密钥管理树上是邻居节点。与网络拓扑相匹配的密钥管理树,即拓扑匹配密钥管理(Topology-Matching Key Management,TMKM)树,被认为是一种有效的密钥管理树。它减少了密钥更新的数量,提高了管理效率。在这种密钥管理树中相邻的节点在网络物理结构上也是相邻的。利用这种密钥树的优势,将更新密钥消息的分发定位到网络上每个小的区域。TMKM树减少了网络中的交叉通信量,这对于网络的部分成员不需要更新密钥时十分有效。

移动无线网络如图1所示,它由移动主机MH、基站BS、高级主机SH组成。假设一个BS下所有的用户是均匀分布而且数量很大时,可以将它看作是一个子群,而且BS知道子群是否需要更新密钥。根据这个假设,一个密钥更新消息首先由SH通过有线连接组播给每个BS,然后BS根据自身的子群是否需要此消息决定是否广播给子群的所有用户,这样处理的好处是,密钥更新消息不需要发送给所有用户,而是通过子群的方式发送。

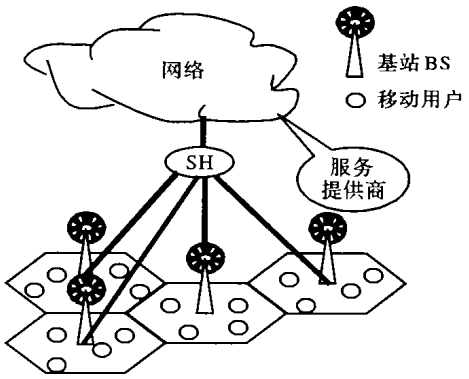

图1 蜂窝网络模型

传统的密钥管理树是与网络结构独立、不相干的,称之为独立拓扑密钥管理(Topology-Independent Key Management,TIKM)树。若使用TIKM树,更新密钥消息将会发送给每个用户;若使用TMKM树,这些消息则只会被部分BS发送。假定用 S_1 表示组播发送给BS的消息数目;S_2 表示被BS广播的消息数目。用 C_{wire} 表示有线的代价;$C_{wireless}$ 表示无线的代价;总的代价为 C_T。

$C_{wire} = E[S_1]$, $C_{wireless} = E[S_2]$

$C_T = \gamma \times C_{wireless} + (1-\gamma) \times C_{wire}$($\gamma$ 表示无线权值,即表示考虑无线代价的比重)

3.1.2 结论

不管是TIKM树还是TMKM树,目标都是尽可能地减少总通信代价 C_T。文献[4]中,通过一个模拟过程,分析了TMKM、TIKM的性能。假设在一个同机种蜂窝网络中,由12个蜂窝组成,用户的到达过程类似泊松分布,用户的服务时间呈指数分布,R 表示蜂窝的半径,V_{max} 表示移动用户的最大速

度,无线权值假定大于 0.5。TMKM、TIKM 性能的模拟分析结果表明,对于不同的无线权值,TMKM 的总通信代价总是少于 TIKM 的 40%,无线权值 γ 越大则 TMKM 与 TIKM 的性能比例越小,TMKM 的优势更加明显。通过对不同的用户加入比例和用户移动速度进行模拟,结果表明 TMKM 树的通信代价只有 TIKM 树的 33% ~45%。

由于 TMKM 树依赖于网络拓扑结构,因而当一个用户在物理上从一个蜂窝移动到另一个蜂窝时,它同时也要在逻辑上从 TMKM 树的一个分支移动到另一个分支。这必然造成额外的通信代价,也是 TMKM 树的主要不足之处。

3.2 大规模动态组播密钥批量更新算法

3.2.1 批量研究的背景

在大规模组播系统中,密钥更新、数据传输、加密所引起的额外开销不应与组的规模呈线性增长,而且某个主机加入或离开组播组不应该影响组的其他成员,因此组播安全中密钥更新问题的可扩展性以及批量处理需求显得尤为重要。

3.2.2 密钥图独立更新

基于密钥图的密钥更新方案集中讨论了独立更新的问题,即每次处理一个用户加入或离开所需要的密钥更新。密钥图的独立更新过程,如图 2 所示,方框代表用户节点,圆圈代表密钥节点,与用户节点直接相连的密钥节点为用户的专用密钥,密钥更新时专用密钥不需要更新。

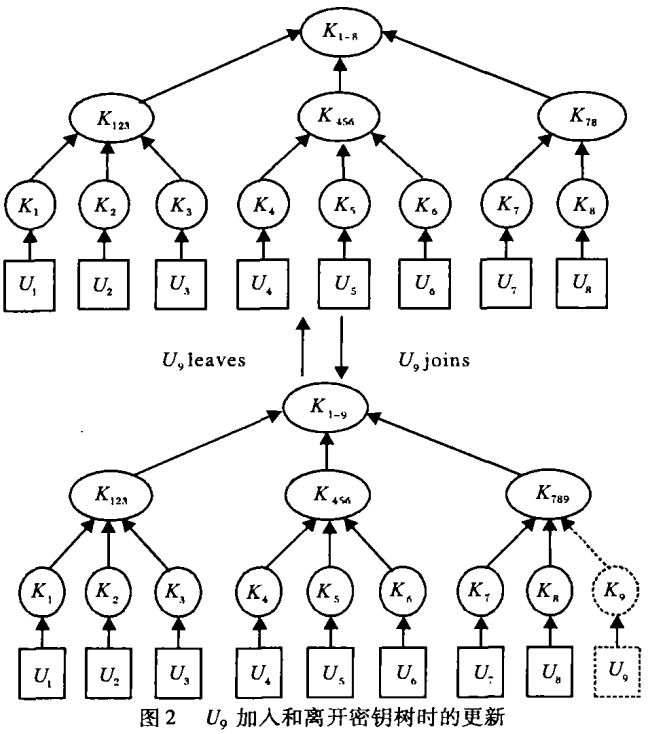

图 2　U_9 加入和离开密钥树时的更新

1) 加入组播组。当新成员加入组播组时,利用新成员的专用密钥加密新产生的组密钥,单播传送给新成员;利用原来的组密钥加密新产生的组密钥组播传送给原来组的成员,即可实现密钥更新。图 2 中假定用户 U_9 想加入组播组,密钥服务器找到 U_9 的加入节点 K_{78},此时需要将密钥 K_{1-8} 更新为 K_{1-9},将 K_{78} 更新为 K_{789}。密钥服务器产生如下的密钥更新消息,组播到整个组,单播 U_9 所需要的密钥给 U_9:

$$s \rightarrow u_1, \cdots, u_9 : \{K_{1-9}\}_{K_{1-8}}, \{K_{789}\}_{K_{78}},$$

$$s \rightarrow u_9 : \{K_{1-9}, K_{789}\}_{K_9},$$

其中 $\{K'\}_K$ 表示密钥 K' 用密钥 K 加密[5]。

2) 离开组播组。由于原来的组密钥已经不能使用,一个简单的密钥更新方案就是利用每个组成员的专用密钥对新产生的组密钥加密进行单播传送。如用户 U_9 想离开组播组,此时密钥服务器需要更新 U_9 所拥有的密钥,即将密钥 K_{1-9} 更新为 K_{1-8},将 K_{789} 更新为 K_{78}。密钥服务器产生如下的密钥更新消息,组播到整个组:

$$s \rightarrow u_1, \cdots, u_8 : \{K_{78}\}_{K_7}, \{K_{78}\}_{K_8}, \{K_{1-8}\}_{K_{123}}, \{K_{1-8}\}_{K_{456}}, \{K_{1-8}\}_{K_{78}},$$

值得注意的是,接收到密钥更新消息后,用户只提取它所需的密钥更新消息,例如 u_8 只需要 $\{K_{1-8}\}_{K_{78}}, \{K_{78}\}_{K_8}$ 即可。

3) 离开后且未加入。有时一个移动节点从一个组播组中离开后,并没有加入到另外的组播组中,或是移动到没有组播传播树的网络,这样的节点若要重新加入到组播服务,通过 IGMP 可以通知组播路由器它所加入的组播组,。组播路由器也利用 IGMP 来获知此网络子网中的组播组的信息。

3.2.3 批量密钥更新算法

在移动网络中,由于节点的频繁切换和网络的错误率,节点的频繁加入和退出必然导致大量的密钥更新和服务器的多余开销。在批量密钥更新方案中,密钥服务器收到用户的加入请求或离开请求时,不是立即更新密钥而是要等待一定的时间间隔。在这个时间间隔内,由于网络的并发性以及组成员变化的频繁性,会有一批成员请求加入或离开组播组,此时密钥服务器进行批量密钥更新,以降低服务器的开销。

此方案将新加入的成员放入 Join 队列中,离开的成员加入 Leave 队列,两队列数目分别是 J 和 L。依次考虑 J 和 L 的大小关系,若 J 和 L 相同,则简单的一一替代,若 J 小于 L,则找到 Leave 中的成员的位置,按叶子节点优先的原则选择 Leave 中的节点替代。假设替换后,剩余 $J-A$ 个加入节点,则余下的节点替换离开的 $L-A$ 个,剩下的 $L-J$ 个则单独调用离开过程[6]。在组播安全密钥更新方案的具体实现时,必须考虑密钥树的平衡性。然而,当组成员数量特别多时,树中每个节点的存储开销仍很大,密钥服务器的计算任务相当繁重,会成为系统的性能瓶颈。

4 RingNet 结构下的组播密钥管理

4.1 引入 RingNet 结构

基于现已提出的各种移动因特网体系结构,本文提出了适合于移动因特网群组成员管理的通信模型,称之为 RingNet 模型[7]。首先介绍该模型的结构,如图 3 所示理。RingNet 基于四层结构:最底层为移动主机(MH)层,其上层为访问代理(AP)层,再上层为访问网关(AG)层,最上层为边界路由器(BR)层。AP 直接与移动主机通信;AG 负责不同的无线网络之间或无线网络和有线网络之间的通信,AG 的覆盖范围称为微移动性管理域;BR 负责更大范围的多个微移动性管理域之间的通信,BR 的覆盖范围称为宏移动性管理域。AP、AG 和 BR 统称为网络实体(NE)。上面两层的 NE 根据位置相邻性分别组织成一个或多个 AG 逻辑环和 BR 逻辑环。每个逻

辑环有一个领导节点负责与上层的逻辑环中的某个节点联系,构成父子关系。如果将 RingNet 的每个逻辑环看作一个节点,则该结构变成一棵树,具有树的一些特点如通信效率高等;如果单就考虑每个逻辑环,则该模型具有环的一些特点如简单和可靠性高等。在文献[7]的 RingNet 成员管理协议中,模拟实验表明这些优点都保留下来了。结合树和环结构,通过自组织性可以克服因为 NE 和通信链路的出错导致网络分区带来的问题。直观上看,基于 RingNet 模型的组播协议是在不同层次上对组播移动性管理的简化。越往上层走组播移动性越弱,相应的拓扑结构变化越慢。

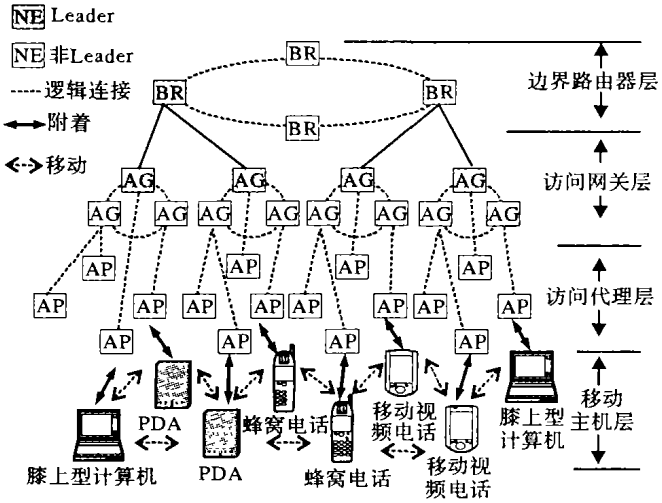

图 3 RingNet 结构

4.2 RingNet 结构的密钥管理

在 RingNet 结构中,为了实现大型超动态的安全组播通信,对安全方案的可扩展性有较高要求。在组播通信中,组播源首先将组播数据包发送到最顶层环的 BR 节点上,然后 BR 同时将数据包沿着环和孩子节点向底层发送。下一层的领导节点收到数据包后也同时发送到 Next 节点和 Children 节点,最终数据包到达各个组成员。

为了实现可扩展性,将 RingNet 层次结构的 AG 层的每一个 AG 节点下的移动节点看作是一个子群[8]。这样,RingNet 结构的密钥管理就变成了对多个子群的密钥管理,而不是庞大的移动节点群。每个 AG 节点作为其子群的控制服务器,负责其子群内成员的加入和离开管理以及密钥的更新。由于每个子群是相对独立的,其内部节点的变化可以使用类似于密钥图的独立更新过程,因而不会影响到其他子群。通过将 RingNet 结构分成多个子群的方式,组通信可以很容易地满足可扩展性需求而不会降低组播通信性能。

在组播通信过程中,BR 节点作为总的服务控制器,在配置 RingNet 服务时分发给每个子群服务器,即 AG 节点各自的子群密钥 K_{LG} (Local Group Key)。BRT(Border Router Tier)中的每个 BR 节点为各自的宏移动性管理域的服务控制器。由于每个 BR 节点完成的过程一样,这里只考虑一个 BR 节点。BR 节点管理所有子群的组密钥,但并不可以改变子群的组密钥,当然子群加入的初始化过程除外,而每个 AG 节点则管理子群内部的局部成员信息。当子群内部成员变化时,子群内部进行独立密钥更新过程,AG 节点产生新的子群密钥 K'_{LG},新的子群密钥用原有密钥加密后单播传递给相应的 BR 节点,同时 BR 更新子群信息。由于移动网络节点的频繁移动性,若是某个 AG 内部成员均离开且全部移动到另一个 BR 区域,这种情形下则不需要对每个成员一一进行更新,可以由子群控制器 AG 节点直接和新的 BR 节点进行相互认证,而子群内部成员的密钥并不需要改变。这样,通过将 RingNet 结构的组成员分成若干子群进行局部管理的方式,掩盖了子群内部繁杂的密钥更新过程,使整个安全组播通信过程得到简化。这种密钥管理方案与 IOLUS 的不同之处在于,本方案是基于 RingNet 结构的,而 IOLUS 的各个子组则是由加入的层次形成一种树形结构。由于 RingNet 具有很好的可扩展性、可靠性、分区运行性和自组织性,这些特性对于将 IOLUS 的思想扩展到移动因特网环境十分关键。

5 结语

各种密钥管理策略与环境和需求是紧密联系的。在大型动态群的组播通信中,批量处理显著地提高了服务器处理的效率。在这种情况下,独立更新则会导致服务器很多无谓的开销。但是,批量更新也存在自己的问题,如延时以及对以前的组播组的可访问性等问题。而与网络拓扑结构匹配的密钥树对于蜂窝较小和移动频繁的较小动态群则是一个较好的选择。它有效地减少了网络的交叉数据流量和密钥消息流量。由于树结构的单点出错率较高并且系统修复不太容易,RingNet 层次结构很好地弥补了这一缺陷,理论分析也表明在此模型基础上的密钥管理将会更加安全和有效。

参考文献:

[1] ZHANG XB, LAM S, LEE DY, *et al*. Protocol Design for Scalable and Reliable Group Rekeying[J]. IEEE/ACM Transactions on Networking, 2003, 11(6): 908 - 922.

[2] MITTRA S. Iolus: A Framework for Scalable Secure Multicasting [A]. Proceedings of the ACM SIGCOMM '97 Conference on Applications, Technologies, Architectures and Protocols for Computer Communication[C], 1997. 277 - 288.

[3] 刘璟,周明天. 大型动态多播群组的密钥管理和访问控制[J]. 软件学报, 2002, 13(2): 291 - 296.

[4] YAN S, TRAPPE W, LIU KJR. An Efficient Key Management Scheme for Secure Wireless Multicast[J]. Proceedings of the IEEE International Conference on Communications (ICC2002), 2002, 2: 1236 - 1240.

[5] WONG CK, GOUDA M, LAM SS. Secure Group Communications Using Key Graphs[J]. IEEE/ACM Transactions on Networking, 2000, 8(1): 16 - 30.

[6] 陆正福,李亚东,于光德. 多播安全中批量密钥更新问题研究[J]. 云南大学学报, 2002, 24(5): 335 - 340.

[7] WANG GJ, CAO JN, CHEN ZD. A Reliable Totally - Ordered Group Multicast Protocol for Mobile Internet[A]. Proceedings of the 33rd International Conference on Parallel Processing Workshops (ICPPW 2004)[C]. Montreal, Quebec, Canada, 2004. 108 - 115.

[8] WANG GD, CAO JN, CHEN ZD. RGB: A Scalable and Reliable Group Membership Protocol in Mobile Internet[A]. Proceedings of the 33rd International Conference on Parallel Processing (ICPP 2004)[C]. Montreal, Quebec, Canada, 2004. 326 - 333.