移动代理恶意主机问题研究综述

Survey of the Problem of Malicious Host

周 冲 戴晓明 邵惠鹤 孙永强

(上海交通大学计算机系 上海200030)

Abstract What the Problem of Malicious Hosts means is: When there are malicious hosts, how to protect mobile agents. In this paper, the possible attacks by malicious hosts are listed, and the methods to protect mobile agents from malicious hosts are analyzed and discussed. In the end, the perspective of research in this field is given.

Keywords Mobile Agents, Mobile Agents Security, The Problem of Malicious Hosts

1 引言

移动代理技术在1994年一经提出,因其开放性、灵活性、健壮性、扩缩性、经济性和支持移动客户等特点,作为一个提供网络服务开发和个性化的统一框架,作为一种分布计算和移动计算的支撑技术,得到广泛的研究。

移动代理在远程实时控制、移动客户支持、信息查询、电子商务、网络管理和控制、远程信息处理、个性化网络服务、分布科学计算等方面都有很好的应用背景。学术界和工业界对移动代理都呈现出浓厚的兴趣,纷纷进行研究。国际上至今已涌现出70多个移动代理系统。但是我们也要看到,移动代理作为一种非常灵活的新型计算模型,存在一些亟待解决的问题[1],如:移动代理安全问题、强迁移问题、移动代理的 exactly once 容错问题,等。

特别是由于移动代理系统支持移动代理的迁移执行,从而引起了一个全新的安全问题:当存在试图攻击移动代理的主机时,如何保护移动代理?这就是恶意主机问题,(即 The Problem of Malicious Hosts)。这个问题如果不解决,移动代理运行的完整性和正确性就难以得到保证。

本文将阐述恶意主机可能的攻击手段,详细讨论当前防范恶意主机攻击的方法及其优缺点,最后给出对恶意主机问题研究的展望。

2 恶意主机攻击方法及其防范

移动代理只是一个程序,它必须依赖于主机运行。主机可以对移动代理进行如下攻击:①窥探移动代理的代码、数据或通讯(Spying);②篡改移动代理的代码、数据或通讯(Manipulation);③复制移动代理进行黑箱测试(Blackbox Testing);④伪装其他主机获益(Masquerading);⑤拒绝服务(Denial Of Service)。

对移动代理的代码,数据或通讯进行窥探,会损害移动代理的私密性要求;并且在此基础上恶意主机获得对移动代理行为的理解,从而使得恶意主机对移动代理代码、数据或通讯的篡改更有目的性,以便为其获取不正当的利益。复制移动代理进行黑箱测试则是另一种理解移动代理行为的手段,特别是当移动代理的行为与输入有直接关联时,黑箱测试能准确测出这种关系,以便恶意主机进行下一步的攻击。伪装和拒绝服务容易理解,这里不再作解释。恶意主机攻击的例子可参见文[2,3]等。

根据现有的文献资料,我们将防范恶意主机攻击的研究分为以下三种:①保护移动代理部分内容或功能;②检测恶意主机的攻击;③防止恶意主机的攻击。

这里要指出的是这三种方法并不互相排斥,只是在功能强弱方面有所区分而已。

3 保护移动代理的部分内容或功能

本节将阐述目前在保护移动代理部分内容或功能方面的进展。主要有:保护移动代理的路由[4];移动代理和路由 ID 的匿名性[2];保护移动代理不被主机恶意复制运行[5],移动代理运行结果保护[3]等。

3.1 保护移动代理的路由

文[4]作者 Westhoff 提出了应用类洋葱结构加密的方法,使得当前主机只知道移动代理的前一到达主机和下一目的主机。经过类洋葱结构加密的移动代理路由信息如下:

$$\begin{aligned} r=&E_{e1}\{h,ip(c_2),S_h(h,ip(c_1),ip(c_2),t,E_{e2}\{\cdots\}),\\ &E_{e2}\{ip(c_1),ip(c_3),S_h(ip(c_1),ip(c_2),ip(c_3),t,E_{e3}\{\cdots\}),\\ &\cdots\\ &E_{en-1}\{ip(c_{n-2}),ip(c_n),S_h(ip(c_{n-2}),ip(c_{n-1}),ip(c_n),t,E_{en}\{\cdots\}),\\ &E_{en}\{ip(c_{n-1}),EOR,S_h(ip(c_{n-1}),ip(c_n),EOR,t)\}\cdots\} \end{aligned}$$

r:移动代理路由信息;E:非对称加密算法;ei:第 i 个主机的公钥;h:发出移动代理的源主机;$ip(c_i)$:第 i 个主机的 ip 地址;t:路由唯一性标志代码;EOR:路由结束;S_h:源主机的数字签名算法。

对于移动代理路由中的第 i 个主机 c_i,拥有对应于 ei 的私钥,可以解密用 ei 加密的部分。从而得到前一主机和下一主机的 ip 地址 $ip(c_{i-1})$和 $ip(c_{i+1})$,数字签名 $S_h(ip(c_{i-1}),ip(c_i),ip(c_{i+1}),t,E_{ei+1}\{\cdots\})$,以及用下一主机公钥 e_{i+1}加密的信息 $E_{ei+1}\{\cdots\}$。数字签名信息被 ci 用来验证路由信息的完整性。

在解密后主机删除它用到的所有信息(包括 $ip(c_{i-1})$,$ip(c_{i+1})$和 $S_h(ip(c_{i-1}),ip(c_i),ip(c_{i+1}),t,E_{ei+1}\{\cdots\})$),将余下的信息(即 $E_{ei+1}\{\cdots\}$)发送到 c_{i+1};c_{i+1}再进行类似于 c_i 的处理,获得前一主机和下一主机的 ip 地址,当前路由信息的数字签名,和待发到下一主机的加密路由信息。

·c_i 要得到 c_{i-1}之前的路由信息是不可能的,因为从 c_1到 c_{i-2}的路由信息都已被此前的主机逐一删除;

·而 c_i 要得到 c_{i+1}之后的路由信息也是不可能的,因为相关信息被 e_{i+1}所加密。

周 冲 博士生,主要研究领域为移动代理,并行与分布计算。孙永强 教授,博士生导师,主要研究领域为程序语言,并行与分布处理,等。

这整个的结构就象一个洋葱，第 i 层的洋葱皮只知道第 i −1层和第 i+1层的洋葱皮的信息；而整个的路由信息的逐步获得，就象洋葱皮被逐层剥离。显而易见，在非对称加密算法是安全的前提下，这种方法是安全的。这种方法的问题在于：如果下一主机无法到达，移动代理无法跳过这个出问题的主机而继续迁移。

3.2 移动代理和路由 ID 的匿名性

文[2]通过引入 MIX 路由器和组签名技术，发展了前一种保护移动代理路由的方法[4]，使得当前主机连前一主机和后一主机也不知道。这种方法的问题在于：首先必须广泛应用 MIX 路由器，其次是 MIX 路由器也有可能是恶意主机。

3.3 保护移动代理不被主机恶意复制运行

为防止移动代理被主机恶意复制运行[5]，该文作者通过引入移动代理运行、迁移和自解等的执行许可令牌，保证在源主机的控制下，能够防止恶意复制运行的发生。这种方法的问题在于：如果主机只复制得到运行令牌后的可执行的部分，或者切断移动代理和源主机的通讯然后伪造令牌，那么恶意复制还是可以进行。

3.4 移动代理运行结果保护

Yee 等人提出部分结果验证码的方法(Partial Results Authentication Code)[3]，用于保护当前主机的运行结果不被此后的主机所篡改。其主要思想是移动代理在某主机运行后的结果由与该主机对应的给定密钥计算 MAC(即消息鉴别码)，该主机将移动代理迁移到下一主机前删除此给定密钥；由于密钥不可知，此后的目的主机不可能伪造该 MAC，从而根据该 MAC 源主机可以检测对运行结果的篡改。密钥系列可以由源主机直接给定，也可以由源主机给定的初始密钥和单向函数所产生。这种方法的问题在于只能验证主机给出的运行结果有否被其他主机篡改，而不能检测或者防止恶意主机篡改移动代理在该恶意主机的运行结果。

4 检测恶意主机攻击

从检测恶意主机攻击的角度出发：人们提出了基于 reference states 即参考状态的方法[6~8]，基于模仿生物学中细胞保护性自解即 Apoptotic function 的方法[9]；基于移动代理复制(Mobile Agent Replication)的方法[3]和基于全息证据校验(Holographic Proof Verification)的方法[3]；等。

4.1 基于参考状态的方法

Farmer 首先提出在移动代理系统安全问题中应用移动代理的状态评估[6]，但是真正将状态应用于防范恶意主机并提出具体机制的是 Vigna。Vigna 在文[6]中提出了应用参考状态的方法，利用第三方可信主机记录移动代理运行前后状态和运行记录的信息摘要，当源主机检测某主机是否对移动代理进行了攻击时，源主机要求该主机提供移动代理运行前后状态和运行记录，并从第三方可信主机获取相应的信息摘要，进行验证。

设：A 为前一主机；B 为当前主机；D 为下一主机；A' 为第三方可信主机；X_p 表示用 X 主机的公钥加密；X_s 表示用 X 主机的私钥加密；C 为移动代理代码；S^i 为从第 i 主机迁移到第 i+1主机前移动代理的状态；H 表示消息摘要；t_A 表示时间戳，i_A 表示唯一标识码。T_c^i 表示移动代理在第 i 个主机的运行记录。那么，这一机制规定移动代理从 A 迁移到 B 并运行的过程是这样的：

·B 从 A 得到消息 $m_0(A,B_p(C,S^0),A_s(H(C),H(S^0),B,A',t_A,i_A))$。B 解密得到代码 C 和状态 S^0，并用 $A_s(H(C),H(S^0),B,A',t_A,i_A)$验证 C 和 S^0。

·B 向 A' 发送消息 $m_1(B,B_s(A,A_s(H(C),H(S^0),B,A',t_A,i_A)))$。证实它收到消息 m_0。

·B 以状态 S^0为当前状态运行代码 C，直到移动代理迁移，此时运行状态为 S^1，并产生运行记录 T_c^i。

·B 向 A' 发送消息 $m_2(B,B_s(D,H(S^1),H(T_c^i),i_A))$。数字签名以下消息：移动代理的下一目的主机，移动代理在本机的最终运行状态和运行记录的消息摘要，以及移动代理的唯一标识码。

·最后 B 向 D 发送消息 $m_3(B,A,D_p(C,S^1),B_s(H(S^1),D),A_s(H(C),H(S^0),B,A',t_A,i_A))$。完成移动代理的迁移。

当源主机检测主机 i 是否对移动代理进行了攻击时，源主机要求该主机提供移动代理运行前后状态 S^{i-1}，S^i 和运行记录 T_c^i，然后从第三方可信主机获取相应的信息摘要 $H(S^{i-1})$，$H(S^i)$，和 $H(T_c^i)$，进行验证；并可以将移动代理从状态 S^0开始运行，对状态序列($S^1\cdots S^n$)进行逐步验证。

这种方法可以检测出对移动代理的篡改攻击，但是无法检测出对移动代理的窥探攻击。在非对称加密算法和数字签名算法是安全的前提下，恶意主机伪装其他主机或拒绝服务都可以直接检测出来。这种方法的问题在于：首先它需要一个可信主机；其次这种机制在运行记录的计算、存储和传送方面的开销是很大的。

Hohl 针对参考状态方法需要可信主机的缺陷，提出利用当前主机来检测前一主机的篡改攻击[7]，这样上述机制就变成将前一主机和当前主机迁移移动代理前的状态，当前主机移动代理运行时的输入发送到下一主机，由下一主机对移动代理在当前主机的运行进行检查。这种方法避免使用可信主机，并且只需要将运行前后状态和输入传送到下一主机即可，降低了开销。但是这一方法引起了一个新问题：无法防止当前主机和下一主机的联合攻击；并且检查变成必须进行的步骤，增加了运行开销。

4.2 基于 Apoptotic Function 的方法

Tschudin 提出了模仿生物学中细胞保护性自解功能(即 Apoptotic Function)的方法[9]。当移动代理检测到攻击时，实行自我解构，终止运行。这是一个新思路。但是由于移动代理在主机中运行，如何进行有效的攻击检测和自我解构？作者没有提供具体实施的有效方法。

4.3 基于移动代理复制的方法

Yee 提出应用移动代理复制可以检测甚至防止恶意主机攻击的一类特殊问题[3]：即最优服务寻求问题。文中的例子是寻求一个提供最低价格飞机票的航空公司，Yee 采用的方法是运行两个移动代理，它们的路由完全反向，但是功能相同；在两个移动代理运行完毕返回源主机时，将两个结果相比较，如果相同，说明没有受到篡改攻击；如果不同，说明发生了恶意主机攻击，但是由于恶意主机不能篡改移动代理迁移到它之后的主机的运行结果，而两个移动代理的路由是反向的，那么将两个移动代理的结果相比较，其中更低的那个价格就是实际最低的价格。这种方法的问题是：首先只适用于特定的应用场合；其次这种方法的前提是路由中只存在一个恶意主机的情况。

4.4 基于全息证据校验的方法

在文[3]中，Yee 还提出应用全息证据校验的方法进行移动代理运行检测。全息证据校验的基本思想如下：设程序为

x,x 的运行记录为 y;P(x,y)=1如果运行 x 得到的结果确实是 y,否则 P(x,y)= 0。为了校验 x 在迁移到的主机上是否运行正确,无需将 y 送回源主机;而只需要计算 y 的全息证据 y^1,将 y^1送回源主机即可。而且为了校验 P(x,y)是否为1,源主机只需检查 y^1中的某些位即可。这种方法的优点在于减少了需要回送的信息和加快了校验的速度。但是目前构建全息证据的方法是不实用的,因为它是个 NP 完全问题。

5 防止恶意主机攻击

防止恶意主机攻击目前主要有以下四种方法:基于防篡改硬件的方法[3,12,13];基于防篡改软件的方法[14~16];基于可信主机的方法[10];基于移动代理服务器复制[11]的方法;等。

5.1 基于防篡改硬件的方法

目前主要有 TPE[12],Secure CoProcessor[3],Smartcard[13]等研究。Wilhelm 提出了应用一个防篡改的硬件环境(Tamper-Proof Environment)的方法[12]。这种环境具有防篡改功能,安装它的主机不能窥探和篡改在该环境中运行的移动代理;这种环境拥有自己的公钥、私钥和数字证书中心,用于加密通讯,将移动代理在各主机的防篡改硬件之间迁移。而由有声望的第三方生产这种防篡改的硬件环境。但这种方法的问题在于:首先 Wilhelm 没有提出实际的构建防篡改硬件环境的方案;其次是防篡改硬件制造的成本;第三是第三方生产商的监督和控制;第四是防篡改硬件的功能无法扩缩。

Yee 提出了具体的防篡改硬件环境的构建方案[3]。他的方案是一块防篡改的板卡,板卡整体被一物理材料层所包裹,该层中含有密集的感应电路以检测对该物理层的破坏和侵入,一旦发现有此类行为发生,感应电路立刻启动相应动作擦除甚至销毁存储体的所有内容;板卡装配有 CPU,启动 ROM,永久性存储体,DES 加密芯片和长命电池。板卡拥有一对公钥/私钥,利用非对称加密方法传送加密通讯的对称密钥,然后用该密钥对称加密通讯。

Funfrocken 提出了应用一种现成的防篡改硬件即智能卡的方法[13]。文中具体采用的是支持 sun 公司 Javacard 技术的智能卡。这种方法解决了防篡改硬件的构建问题,并且生产成本很低;但是引入了一个新的问题:由于智能卡的系统资源很少,例如内存是64K,如何实现一个在如此少的资源之上的移动代理系统?

5.2 基于防篡改软件的方法

目前主要有以下两种方法:Time Limited Blackbox[14],Computing with Encrypted Function[15~17]。Hohl 提出应用 mess-up 方法使得移动代理的代码在规定的时限内不能被理解的方法[14],就是将移动代理代码转变成所谓的时限黑箱代码,在超过时限后移动代理不再有效。这种方法避免了移动代理代码被恶意主机所理解,使得恶意主机无法发起有效的篡改攻击,但是 Hoho 所提出的 mess-up 方法还不能定量地给出计算时限的方法;另外这种方法不能防范黑箱测试,(恶意主机恶意复制移动代理并在向移动代理提供不同输入的情况下进行运行,监视移动代理运行的结果)。

Sander 等人提出应用加密函数计算(Computing with Encrypted Function)的方法[15]。加密函数计算中有一个基本问题:是否存在公钥加密函数 E,使得从 E(x)和 E(y)可以很方便地计算 E(x+y) 和 E(xy)(前者称为加法同态函数,后者称为乘法同态函数)[17]? 如果存在这样的函数,那么就可以构建一个多项式计算的加密函数。Sander 等人的贡献是提出可以只用 E(x+y) 和 E^1(xy)来构建多项式计算的加密函数;E^1(xy)称为混合乘法同态函数,是从 E(x)和 y 计算得到,但它的构建可以应用 E(x+y)来完成[15]。Lipton 和 Sander 在文[18]中提出了一个基于光滑整数 N(仅有小质因子的正整数)的环 Z/NZ 上的加法同态函数,使得这一思想变为现实。但是这种方法目前只适用于多项式计算;另外应用这种方法的移动代理也无法防范黑箱测试。

Loureiro 等人提出应用纠错编码的方法来加密布尔电路计算[16]。纠错编码最早应用于密码学是在 McEliece 公钥密码系统中。Loureiro 等人提出如下应用方法:

设 F 为基于 Z_2的 k×k 阶矩阵,表示计算的目标函数 f。z 为任意 k×n 阶矩阵,其中至少有 n−t 列为0向量。

·Alice 计算 F^1=FGP+z 并将 F^1送给 Bob。

·Bob 给出输入 x,计算 $y^1=xF^1$并将结果返回给 Alice;($y^1=xF^1=xFGP+xz$)。

·Alice 解密 y^1,得到 $y=xF$。($y^1P^{-1}=xFG+xzP^{-1}$,再用 Goppa 码的解码算法可求得 xF)。

这种方法能够实现布尔电路的加密计算,而理论研究表明任何一个图灵机程序都可以用布尔电路来模拟[17];但是这种方法要有效地应用到移动代理系统中还必须解决两个问题:一是算法的密钥至少为19位,加密会导致目标函数矩阵的成倍扩大,增加计算开销;二是还缺乏有效的机制实现任意计算程序向布尔电路的转换。

5.3 基于可信主机的方法

这种方法利用第三方可信主机运行移动代理的关键代码甚至整个移动代理。管旭东等人提出了 POM(Police Office Model)模型[10],用警察局来比拟第三方可信主机,并提出将移动代理分为关键代码和非关键代码两部分,关键的部分在可信主机上运行,非关键部分则直接到目的主机上运行,一般要求可信主机和目的主机之间有可靠的能保证带宽的联接。这个方法的问题是:首先如何提供并验证大量的可信主机,其次是如何高效地划分移动代理代码并实现两部分代码的协调运行。

5.4 基于移动代理服务器复制的方法

Minsky 在文[11]中提出利用移动代理服务器复制,然后从这些复制的服务器上分别运行的结果中经选举产生认可的结果,从而可以允许这些复制的服务器中有一定数量的恶意服务器存在。其实,如果在这些由同一个服务供应商提供的服务器中存在恶意服务器,那么就不能保证它不会使所有的服务器都进行恶意攻击。所以这种方法更适用于服务器容错,而不是恶意主机防范。

结束语 本文阐述了恶意主机可能的攻击手段,并详细讨论了当前防范恶意主机攻击的方法及其优缺点。从中可以看出:在移动代理路由和移动代理运行结果方面的研究已经可以实际应用。对移动代理防恶意复制方面的研究还有待突破。基于参考状态的方法已经有较成熟的应用机制,但是目前的方法开销太大。而基于 Apoptotic Function 的方法和基于全息证据校验的方法目前还只是一个概念,缺乏具体的实现方法。基于移动代理复制的方法目前仅应用于一类特殊问题。基于防篡改硬件的方法是至今为止最有效的防范恶意主机攻击的方法,但成本很高。在基于防篡改软件的方法中,时限黑箱还缺乏实际可行的构建方法,而加密函数计算还停留在理论方法研究的阶段。基于可信主机缺乏实现的硬件条件。基于移动代理服务器的方法则基本上无法应用于防止恶意主机攻

击。

在这一领域的下一步研究中，以下方向是值得注意的：移动代理防恶意复制，基于参考状态的恶意主机攻击检测，基于移动代理复制的一般化攻击检测方法，基于智能卡的防恶意主机攻击系统的研究，基于加密函数计算的防恶意主机攻击方法研究，时限黑箱有效构建方法，等。

参 考 文 献

1 Farmer W M, Guttman J D, et al. Security for mobile agents: Issues and requirements. In: Proc. of the 19th National Information Systems Security Conf. Baltimore, Md., October 1996. 591～597. http://csrc. nist. gov/nissc/1996/papers/NISSC96/paper033/SWARUP96. PDF

2 Ng S K. Protecting Mobile Agents against Malicious Hosts. Master Thesis. Division of Information Engineering, The Chinese University of Hong Kong, June 2000. http://mole. informatik. uni-stuttgart. de/security/ngthesis. pdf

3 Yee B S. A Sanctuary for Mobile Agents. DARPA Workshop on Foundations for Secure Mobile Code, Feb. 1997. http://www. cs. ucsd. edu/～bsy/pub/sanctuary. ps

4 Westhoff D, Schneider M, et al. Protecting a Mobile Agent's Route against Collusions. In: Proc. of SAC'99, Springer LNCS 1758, 1999. http://www. informatik. fernuni-hagen. de/import/pi2/agents/Papers/ontario99-env. ps

5 Baek J. A design of a protocol for detecting a mobile agent clone and its correctness proof using Coloured Petri Nets: [Technical Report TR-DIC-CSL － 1998-002]. Info. &Comm., K-JIST, 1998. http://atom. kjist. ac. kr/～jsbaek/pub/tr-dic－1998-02. ps

6 Vigna G. Protecting Mobile Agents through Tracing. Mobile Object Systems ECOOP Workshop'97. http://arthur. cs. ucdavis. edu/～barnes/seminar/papers/vigna97. ps

7 Hohl F. A Protocol to Detect Malicious Hosts Attacks by Using Reference States. Universitat Stuttgart, Fakultat Informatik, Bericht Nr. 1999. ftp://ftp. informatik. uni-stuttgart. de/pub/library/ncstrl. ustuttgart_fi/TR－1999-09/TR－1999-09. ps. gz

8 Farmer W, Guttman J, et al. Security for Mobile Agents: Authentification and State Appraisal. Fourth European Symposium on Research in Computer Security (ESORICS 96), P. 118－130. http://imps. mcmaster. ca/doc/esorics96. ps

9 Tschudin C. Environmental Security: Apoptotic Functions and a Way to Protect Them. 4th WORKSHOP ON MOBILE OBJECT SYSTEMS: Secure Internet Mobile Computations. In association with the 12th European Conference on Object-Oriented Programming (ECOOP'98), 21 July 1998, Brussels, Belgium. http://cuiwww. unige. ch/～ecoopws/ws98/slides/tschudin. ps

10 Guan Xudong, Yang Yiling, et al. POM - A Mobile Agent Security Model Against Malicious Hosts. In: Proc. HPC-Asia 2000, pp. 1165～1166, Beijing, China, May. 15～18, 2000. http://202. 120. 7. 27/member/～gxd/pom(hpcasia2000_2_pages). zip

11 Minsky Y, van Renesse R, et al. Cryptographic Support for Fault-Tolerant Distributed Computing. In: Proc. of the Seventh ACM SIGOPS European Workshop. Connemara, Ireland, September 1996. 109～114. http://www. tacoma. cs. uit. no/papers/SIGOPS. ft-agents. ps

12 Wilhelm U G. A Technical Approach to Privacy based on Mobile Agents Protected by Tamper-resistant Hardware. PH. D. dissertation. 1999. http://lsewww. epfl. ch/～ wilhelm/Papers/thesis. pdf

13 Funfrocken S. Protecting Mobile Web-Commerce Agents with Smartcards. In: Proc. of the First International Symp. on Agent Systems and App. s / 3rd International Symp. on Mobile Agents (ASA/MA'99), IEEE Computer Society, 1999. 92～102. http://www. informatik. th-darmstadt. de/VS/Publikationen/papers/ma99/secure-webagents. pdf

14 Hohl F. Time Limited Blackbox Security: Protecting Mobile Agents From Malicious Hosts. In: Vigna G, ed. Mobile Agents and Security. Springer-Verlag, 1998. 92～113. http://www. informatik. uni-stuttgart. de/ipvr/vs/projekte/mole/vignabuch. ps. gz

15 Sander T, Tschudin C. Towards Mobile Cryptography. IEEE Symposium on Security and Privacy, 1998. 215～224. ftp://ftp. icsi. berkeley. edu/pub/techreports/1997/tr-97-049. ps. gz

16 Loureiro S, Molva R. Function Hiding Based on Error Correcting Codes. In: Blum M, Lee C H, eds. Cryptographic Techniques and E-Commerce. Proc. of the 1999 Intl. Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99), City University of Hong Kong Press. ftp://ftp. eurecom. fr/pub/loureiro/cryptec99. ps. gz

17 Feigenbaum J, Merritt M. Open questions, talk abstracts, and summary of discussions. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 1991, 2: 1～45,

18 Lipton R, Sander T. An additively homomorphic encryption scheme or how to introduce a partial trapdoor in the discrete log. Nov. 1997

（上接第58页）

分组管理节点 —协议 P0→ 分组成员节点

协议 GRRMP 具有这样一些特点：(1)采用分组和差错恢复组思想，实现差错恢复本地化，减少骨干网上报文流量。(2)已经正确接收报文的节点不会接收到重传报文，能避少不必要的处理开销及网络资源浪费。(3)支持“点对多”和“多对多”可靠报文传输服务。

结论 作者采用 B. N. Levine 和 J. J Garcia-Luna-Aceves 在文[3]中提出的模型，对协议 GRRMP 的吞吐性能、骨干网上的报文流量、传输延迟等进行了分析，并在校园网环境下，利用该协议实现了远程教学中的共享白板应用。分析和实验表明，该协议具有良好的吞吐性能、较小的传输延迟，能有效减少骨干网上的通信负荷。由于使用了分组和差错恢复多点广播组策略，使差错恢复局部化，同时均衡了主机的处理负担，克服了集中处理的性能瓶颈问题，因此协议 GRRMP 能适合大规模分布式实时协同应用环境。

参 考 文 献

1 龙晓苑，吴良芝. 多媒体通信协议与应用. 清华大学出版社，1998

2 郑庆华. CSCW 的理论、实现方法与应用. 计算机科学，1996，23(5)：18～25

3 Towsley D. A Comparison of Sender-Initiated and Receiver-Initiated Reliable Multicast Protocol. Proceeding of ACM Multimedia，1996，11(2)：282～291

4 Holbrook H W. Log-based Reliable Multicast for DIS. Proceeding of SIGCOMM'95，1995，25(4)：328～341

5 Levine B. The Case for Concurrent Multicast Using Shared ACK Trees. Proceeding of ACM Multimedia，1996，11(2)：365～376

6 Yavatkar R. A Reliable Dissemination Protocol for Interactive Collaborative Application. University of Kentucky，1995(10)：36～47