一种基于混合加密的移动代理安全传输模型 [1]

陈志贤 * 王汝传 * ** 王绍棣 * 孙知信 *

*(南京邮电学院计算机系 南京 210003)
**(中国科学院研究生院信息安全国家重点实验室 北京 100039)

摘 要: 该文分析了目前移动代理系统存在的主要安全问题及现有的解决方案，随后提出了一种基于混合加密的移动代理安全传输模型 (HESTM) . 该模型主要分成两部分: (1) 利用混合加密算法加密移动代理; (2) 利用 TLS 加密通信信道. 仿真与性能分析表明, HESTM 模型的确能有效地保护移动代理的传输安全，从而有效地提高了整个系统的安全性和稳健性. 该算法已成功地应用在作者开发的原型系统——基于移动代理的入侵检测系统中.

关键词: 移动代理，传输层安全，混合加密
中图分类号: TP393, TN918 **文献标识码:** A **文章编号:** 1009-5896(2004)09-1407-06

A Secure Transport Model of Mobile Agent Based on Hybrid Encryption

Chen Zhi-xian* Wang Ru-chuan** Wang Shao-di* Sun Zhi-xin*

*(*Computer Science & Technology Dept., Nanjing Univ. of P&T, Nanjing* 210003, *China*)

**(*State Key Lab of Info. Security, Graduate School of CAS, Beijing* 100039, *China*)

Abstract This article analyzes the main security problems that current mobile agent systems face with and existing solving methods, then a secure transport model of mobile agent based on hybrid encryption HESTM is brought forward. The model comprises two parts: (1) Using hybrid encryption encrypt mobile agent; (2) Using TLS encrypts communication channel. The simulation and performance analysis show that HESTM can efficiently protect the transport security of mobile agent indeed, thus enhance the security and robustness of the whole system. This algorithm has been successfully applied in authors developed prototype—mobile agent based intrusion detection system.

Key words Mobile agent, Transport Layer Security(TLS), Hybrid encryption

1 引言

移动代理 (Mobile agent) 是一可确认的、具有跨地址空间运行机制的 agent，是一种以自治的方式来完成任务并具有一定程度的预动性、反应性、合作性和交互性的程序代码; 它可以转移到不同的地址空间执行，转移过程中可以保持自身的状态; 它必须是可以验证确认的 [1] .

由于移动代理能够在异构的网络节点间移动，并且可通过与服务设施和其它的 agent 协商获取、提供服务来完成全局目标，因此我们认为移动代理需要具有以下技术特征: 中小规模，跨平台语义一致性、持久性和安全机制。

移动代理的应用要求分布式系统中相互协作的主机提供移动代理的执行环境，因而这些主机可能会受到恶意代理的攻击。与此类似，移动代理系统也要保证在主机上运行的移动代理的安全，以防止恶意主机的攻击。特别是移动代理在网络间迁移时，也可能遭到恶意攻击或者窃听

[1] 2003-05-04 收到, 2003-08-22 改回
国家自然科学基金 (60173037 和 70271050) 、江苏省自然科学基金 (BK2003105) 、国家高科技项目 863 (2002AA776032) 、江苏省计算机信息处理技术重点实验室基金 (kjs03061 和 kjs04) 资助课题

等。所以，设计移动代理系统时，其安全性是主要考虑的问题之一。下面我们先分析目前移动代理系统普遍存在的安全问题及现有的保护方案，接着就移动代理在网间迁移的安全问题提出一种基于混合加密的移动代理安全传输模型 (Hybrid Encryption based Secure Transport Model, HESTM)，最后对它进行仿真和性能分析。

2 移动代理的安全问题及现有的保护方案

2.1 移动代理的安全问题

移动代理在目标机器中可能遭受以下两种攻击：来自恶意服务器 (或运行环境) 的攻击和来自其它代理和实体的攻击。而移动代理在网络中迁移时，其代码和数据也有可能成为攻击的对象。因此，移动代理的安全问题可以归纳为以下 3 个方面： (1) 主机或代理执行环境受恶意代理攻击问题。 (2) 移动代理受恶意主机或代理执行环境攻击问题。 (3) 移动代理在传输过程中受攻击问题。

2.2 现有的保护方案

2.2.1 主机或代理执行环境保护方案 由于移动代理系统中的服务器允许不同的代理程序在其上运行，这使得它不得不面临恶意代理可能带来的攻击，如偷窃敏感资料、破坏服务器系统资源、扰乱性攻击、拒绝服务攻击等等。

对此，研究人员提出了沙盒模型，签名、认证、授权和资源分配， Proof-carrying code，代码检验，限制技术，核查记录等保护方案。

2.2.2 现有移动代理保护方案 移动代理程序必须在服务器上运行，因此，其代码和数据对于服务器主机来说都是暴露的。当一个服务器是恶意的，或是被攻击者侵占或伪装的时候，它可能对代理程序进行如下几种攻击：破坏代理使其无法完成任务，从代理中窃取有用信息，修改代理携带的数据，修改代理的执行代码，使其在其它的宿主和代理的所有者中运行时做恶意操作等等。

对此，相关的研究人员提出了加入状态评价函数 [2]，加密跟踪法 [3]，有限的黑匣子安全法 [4]，配置可信赖且能抵御攻击的硬件 [5] 等保护方案。

2.2.3 移动代理传输保护方案 当在开放型网络中 (如 Internet) 中传递信息时，固有的一个缺点就是不安全。因而当代理程序在网络中漫游时，它的程序码和数据都是不安全的。在数据传递和通信链接中都存在着不安全威胁。

主动攻击：攻击者截获并修改网络层的数据报，甚至将原数据报删除，而用伪造的数据取代。另外，身份伪装也可看作一种主动攻击，攻击者伪装成系统的一个合法参与者 A，截取并处理发给 A 的数据。

被动攻击：在这种攻击模式下，攻击者并不干预通信流量，只是尝试从中提取有用的信息。最简单的例子就是窃听，以获取代理程序中存储并传递的敏感信息。另一种情况是，攻击者可能无法得到具体的数据 (如数据采用加密传输)，但可以通过对相关数据进行流量分析 (如分析通信频度、交换的数据长度、通信双方的身份) 获取所需的敏感信息。

3 HESTM 模型的实现

由于目前很多移动代理平台更多考虑的是服务器和移动代理在平台中的安全问题，而没有考虑到移动代理在网络上安全传输和加密方面的问题，所以我们提出一种基 HESTM 算法就是在这两个方面对移动代理系统的安全性进行扩展，增强它的安全性和稳健性。

如图 1 所示， HESTM 算法主要分成两部分，即利用混合加密算法加密移动代理和利用传输层安全 (Transport Layer Security, TLS)[6] 加密通信信道。经过混合加密的移动代理在经过 TLS 加密通信信道中传输。

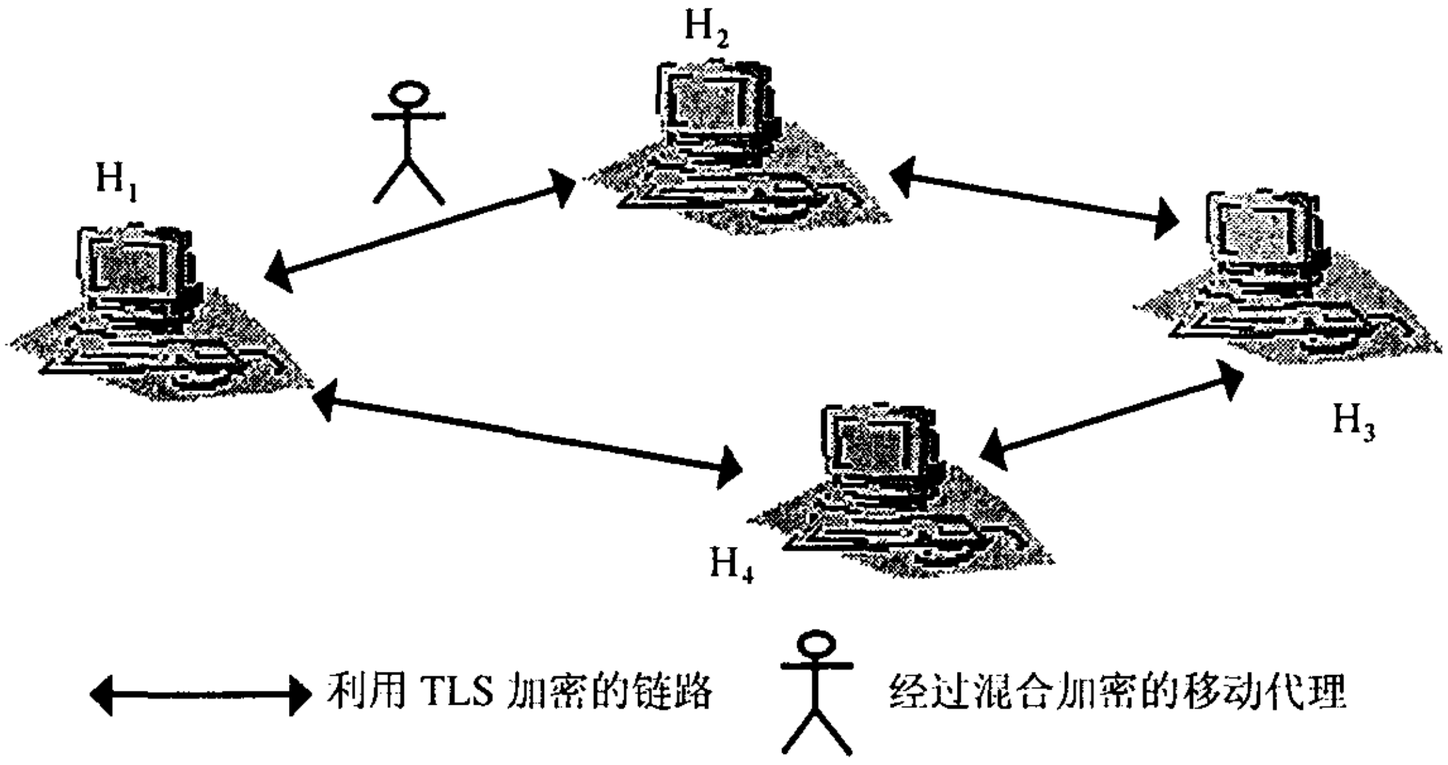

图 1　HESTM 模型的总体架构图

3.1 利用混合加密算法加密移动代理

将移动代理要完成的任务以及所涉及到的所有数据封装成一个类 (Object)，这样一来加密这个类的实例与加密整个移动代理是等效的，但是在编程的效率上前者显然更简单并且容易实现，同时也减少了执行加解密算法所需要的时间开销。

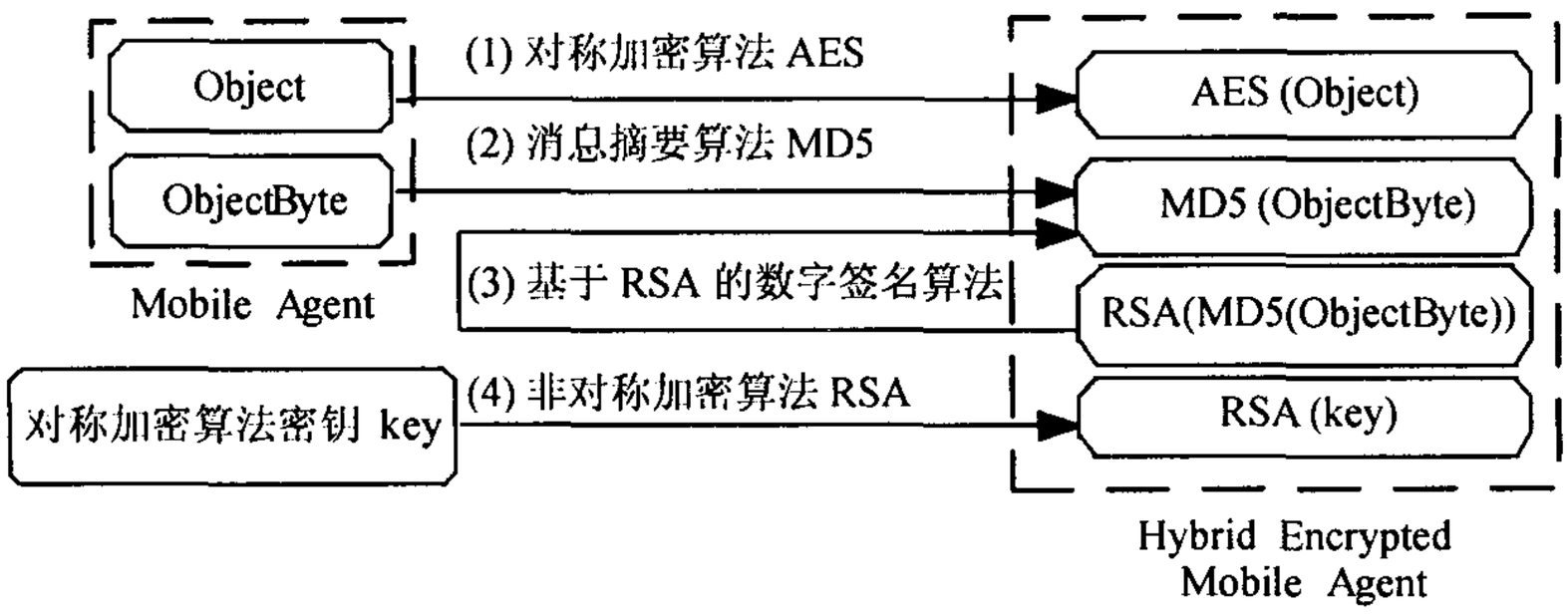

图 2　发送方的混合加密算法原理图

图 2 中，Object 是一个经过抽象、封装而成的类的实例，ObjectByte 是一个表征该实例的字节数组，对称加密算法为 AES(高级数据加密标准)[7]，其密钥为 key，非对称加密算法为 RSA[8]，其公钥为 publickey，私钥为 privatekey。

发送方的混合加密算法实现步骤：

(1) $\text{Object}\xrightarrow{\text{AES}}\text{AES(Object)}$，即利用 AES 算法加密类实例；

(2) $\text{ObjectBytes}\xrightarrow{\text{MD5}}\text{MD5(ObjectByte)}$，即利用 MD5 算法产生消息摘要；

(3) $\text{MD5(ObjectBytes)}\xrightarrow{\text{RSA+ 发送方的私钥}}\text{RSA (MD5(ObjectByte))}$，即利用 RSA 算法对消息摘要进行数字签名；

(4) $\text{key}\xrightarrow{\text{RSA+ 接收方的公钥}}\text{RSA(key))}$，即利用 RSA 算法对 AES 算法的密钥进行非对称加密。

这样，就可以把经过安全措施保护的移动代理发送到目的机器。

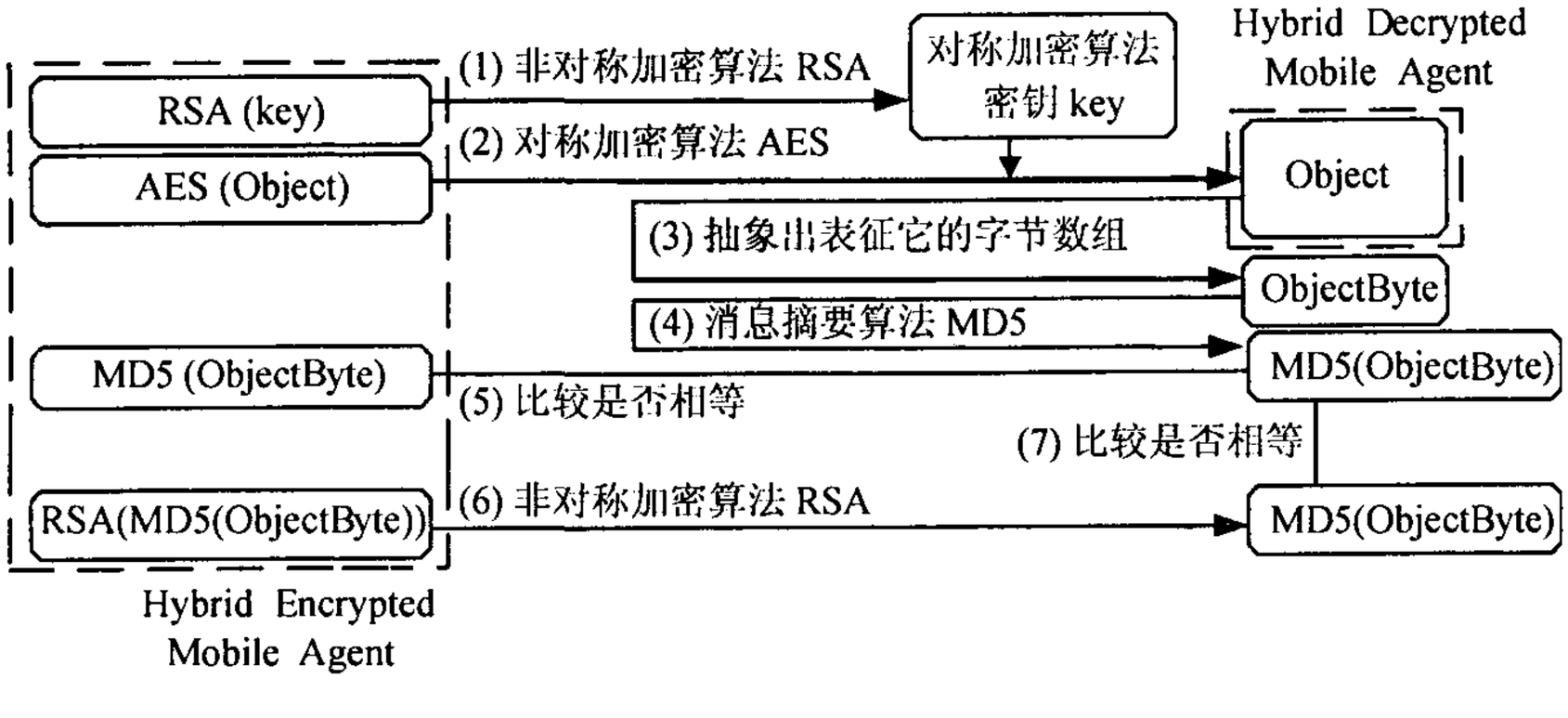

图 3 接收方的混合解密算法原理图

接收方的混合解密算法实现步骤：

(1) RSAkey$\xrightarrow{\text{RSA+ 接收方的私钥}}$key，即利用 RSA 算法得到 AES 算法的密钥；

(2) EncryptedObject$\xrightarrow{\text{AES}}$Object，即利用 AES 算法解密得到类实例 Object；

(3) 对于步骤 2 得到的 Object，得到表征它的字节数组 ObjectByte；

(4) ObjectBytes$\xrightarrow{\text{MD5}}$MD5(ObjectByte)，即利用 MD5 算法产生消息摘要；

(5) 把步骤 (4) 得到的消息摘要与传送过来的 MD5(ObjecByte) 进行比较，如果相同，则说明此移动代理在传输过程中没有被篡改；否则就是已经被篡改过的移动代理，应予以丢弃，这是为了保证移动代理的数据完整性。

(6) RSA(MD5(ObjectByte))$\xrightarrow{\text{RSA+ 发送方的私钥}}$ MD5(ObjectByte)，即利用 RSA 算法解密得到数字签名；

(7) 类似步骤 (5) 来验证数字签名，如果验证成功，则认为此移动代理的确是发送方发送过来的；否则就是非法主机发送过来的移动代理，应予以丢弃，这是为了保证移动代理来源的可靠性。

3.2 利用 TLS 加密通信信道

如图 4 所示，我们在移动代理平台与 TCP 层之间集成了 TLS，采取结合 TLS 的通信协议来保障通信信息的安全。TLS 建立在 SSL(Secure Socket Layer) 的基础上，它大量采用对称加密和非对称加密技术，提供客户机、服务器之间相互身份验证和保密性、完整性。

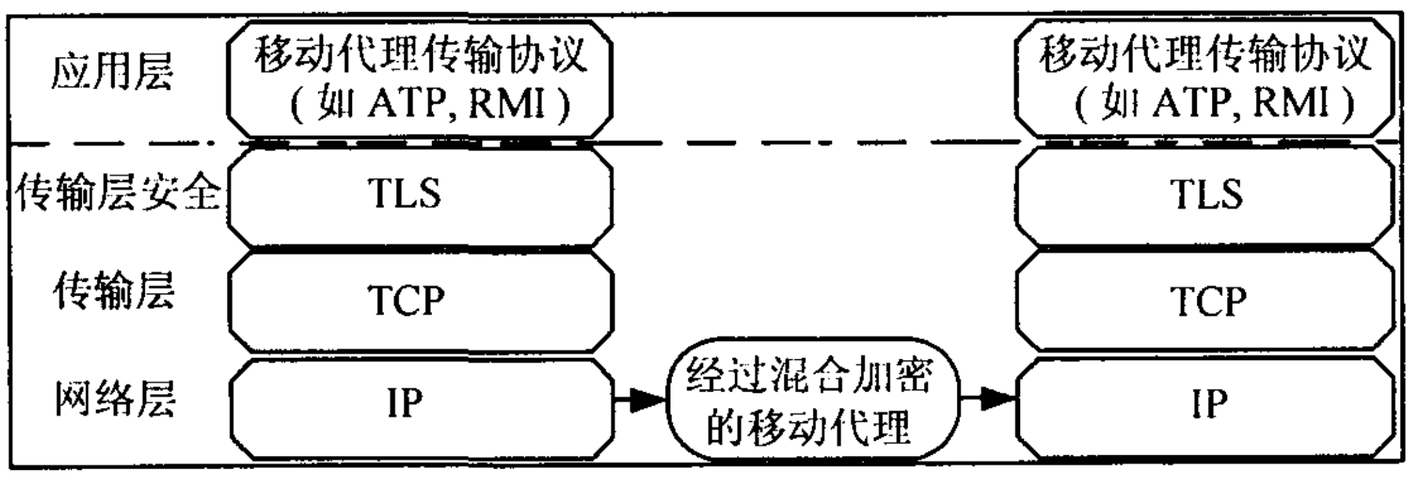

图 4 利用 TLS 加密通信链路

(1) 身份验证：身份验证的目的是让通信双方确认对方的身份。可以使用不对称的或公用的密钥或加密系统对连接进行验证。TLS 支持基于 RSA 和带有 X.509v3 证书的 Diffie-Hellman/DSS 的身份认证。

(2) 保密性：连接是保密的。所有的通信内容都经过安全套接字的处理，即用一组对称密钥和一个在真正的 TLS 会话开始之前就协商好了的加密算法进行加密。虽然 IP 数据包仍有被

截取的可能，但加密后的数据对于截取者来说毫无用处。它支持不同的加密程度，其中包括 40 位、 56 位、 128 位和 168 位加密。

(3) 完整性：连接是可靠的。消息传输中包括了使用键控消息身份认证代码 (MAC) 进行的消息完整性检查。消息在传输过程中被修改，不管是传输错误还是有人蓄意破坏，消息验证码 (MACs) 都能验证出来。可以采用安全哈希函数 (例如， SHA1 、 MD5) 来进行 MAC 计算。

移动代理平台服务器所用的协议一般都是建立在 TCP/IP 协议的基础之上，如在 Java2 中 TCP 传输协议由 java.net.Socket 和 java.net.ServerSocket 类所提供，所以我们有必要对它进行改造，创建并安装一个定制的 TLSSocketFactory—HETLSSocketFactory 将允许移动代理传输协议层使用一个非标准 TCP 的传输协议。其实现步骤如下：

(1) 开发自己的 Socket 类型。

(2) 通过提供新的实现，扩展 TLSSocketFactory 类，参见步骤 (3) 和步骤 (4) 。

(3) 替换 TLSSocketFactory 类的 createSocket 方法。

(4) 替换 TLSSocketFactory 类的 createServerSocket 方法。

使用 TLSSocketFactory 类提供的 setSocketFactory 方法将 SocketFactory 设为定制的 HETLSSocketFactory ，这样移动代理平台使用的协议层就可以与 TLS 无缝结合使用，从而达到保护传输中移动代理的目的。

4 模型分析

4.1 HESTM 的仿真和测试

为了证明上述理论的可行性，我们对 HESTM 模型进行了局域网内粗略的仿真和测试，随后对该模型的性能进行分析。

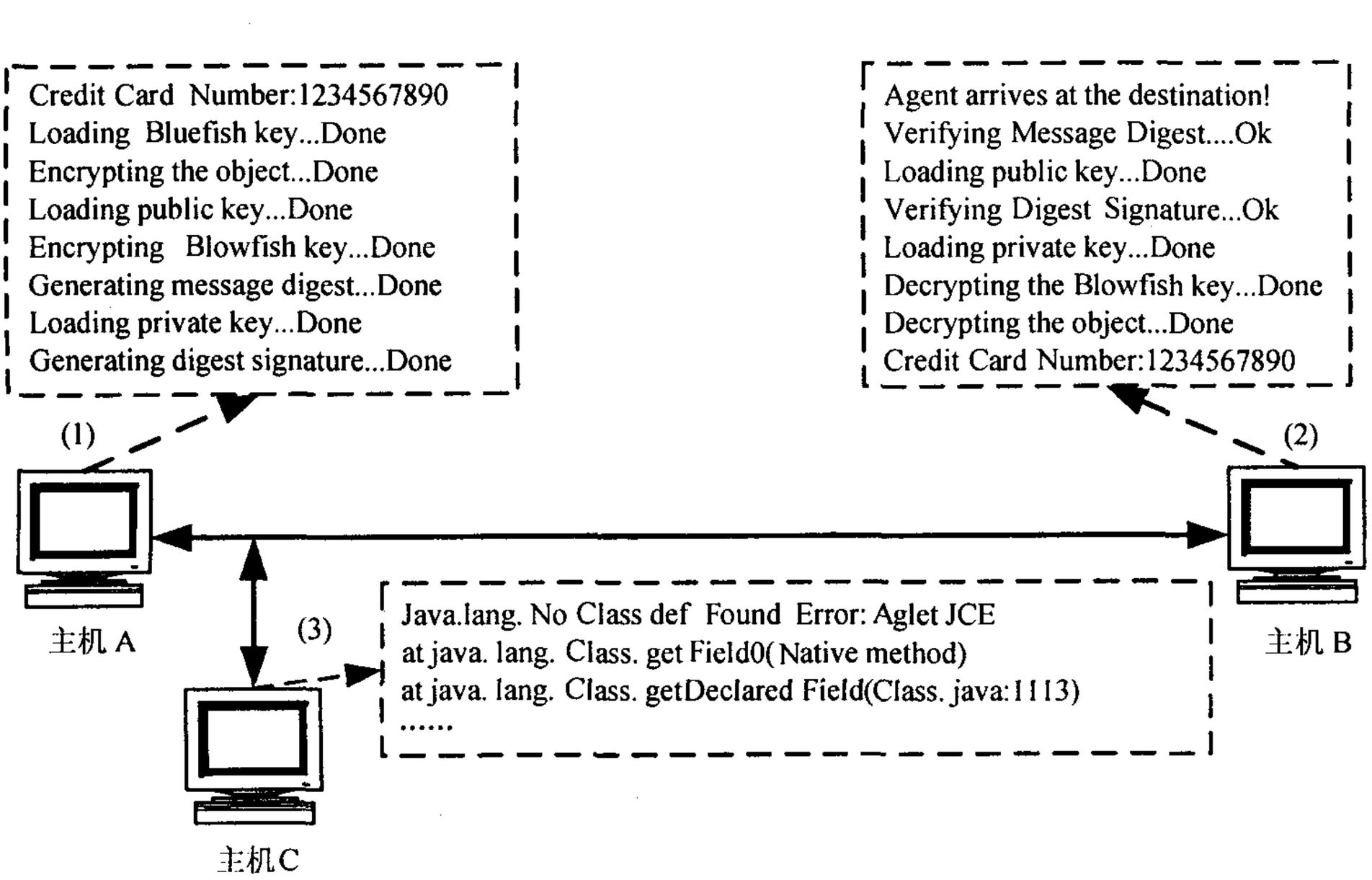

图 5　实验仿真原理图

仿真平台：一个包含三台主机的小局域网。主机上的操作系统为 Red hat Linux 7.0.2 ，移动代理平台为 IBM Aglets2.0.1 ，开发平台为 J2SE1.4.0 ， JCE 的实现包为 Bouncy Castle Cryptography API 1.04 版 [9] 。其中主机 A 、 B 上配置有自定义的混合加密算法的实现类 AgletJCE 和信用卡类 CreditCard 。而主机 C 扮演的是黑客角色，它对主机 A 、 B 之间的通信链路进行监听。

正常通信仿真：主机 A 欲向主机 B 派遣一个携带有信用卡卡号 (敏感信息) 的移动代理 MA 。为此主机 A 首先产生类 CreditCard 的一个对象，并且把信用卡的卡号置入该对象。接着利用混合加密算法的实现类 AgletJCE 对该对象进行加密，然后由 MA 携带此经过混合加密的对象发送出去，混合加密过程如图 5 中的 (1) 所示。在目的主机 B ，由于主机 B 拥有 AgletJCE 类及信用卡类，所以它可以对移动代理 MA 携带的信息进行正确的混合解密，重新构造出被加密封装的 CreditCard 对象，然后它可以访问该对象而获得信用卡卡号，混合解密过程如图 5 中的 (2) 所示。

异常窃听仿真：主机 C 一直在监听通信链路，当主机 A 向主机 B 派遣移动代理的时候它截获了该移动代理，并且试图在自己的移动代理平台上对其进行解密以获取敏感信息，如图 5 中的 (3) 所示，但是由于它无法获取正确的 AgletJCE 类以及 CreditCard 类，所以无法进行正常的混合解密，导致失败。

4.2 HESTM 模型的性能分析

HESTM 模型主要利用 TLS 协议来保证通信信道的安全性和可靠性，同时利用公钥和私钥加密方法对移动代理的关键类实例进行混合加密，在移动代理接收端进行混合解密，充分保证了移动代理的数据保密性、完整性和来源的可靠性。

相对于没有采用任何保密措施，或者仅仅采取其中一种措施的安全机制，这种双重保护的方法显然能起到更好的作用，与此同时混合加密方法的应用也大大缩短了程序的时间开销。因为私钥加密方法既安全速度又快；公钥加密比私钥加密速度要慢，但是对于认证和钥匙交换又是必不可少的。而 HESTM 模型利用这两类加密方法各自的优点，取长补短，从上面的平台仿真可以看出，这种方法在保护传输中的移动代理方面能起到很好的效果。

5 结束语

移动代理安全问题的解决是决定其能否广泛应用的关键问题。本文分析了目前移动代理系统面临的主要安全问题及现有的保护方案，并在其基础上提出了一种基于混合加密的移动代理安全传输模型 HESTM 。实验表明，此模型能有效地保护移动代理的安全，从而有效地提高了整个系统的安全性和稳健性。该算法已成功地应用在我们开发的原形系统——基于移动代理的入侵检测系统中，下一步的工作是在此基础上开发实用的、产品化的入侵检测系统。

参 考 文 献

[1] 王汝传，郑晓燕. 移动代理技术及其在电子商务中的应用研究. 南京邮电学院学报， 2001, 21(2): 80–81.

[2] Fritz Hohl. A protocol to detect malicious hosts attacks by using reference states. Technical Report Nr.09/99, Faculty of Informatics, University of Stuttgart, Germany, 1999.

[3] Giovanni Vigna. Cryptographic Traces for Mobile Agents, Mobile Agents and Security, Berlin: Springer-Verlag, 1998, LNCS 1419: 137–153.

[4] Fritz Hohl. Time Limited Blackbox Security: Protecting mobile agents from malicious hosts, Mobile Agents and Security, Berlin: Springer-Verlag, 1998, LNCS 1419: 92–113.

[5] UWE G. Wilhelm, Sebastian M. Staamann, Levente Buttyan. A pessimistic approach to trust in mobile agent platforms. *IEEE Internet Computing*, 2000, 4(5): 40–48.

[6] Dierks T, Allen C. The TLS Protocol. IETF, January 1999.

[7] 陈鲁生，沈世镒. 现代密码学. 北京：科学出版社， 2002: 53–66.

[8] 赖溪松，韩亮，张真诚. 计算机密码学及其应用. 北京：国防工业出版社， 2001: 84–106.

[9] Garms J, Somerfield D. Java 安全性编程指南. 北京：电子工业出版社， 2002: 48–272.

[10] Sander T, Tschudin C F. Towards mobile cryptography. Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 1998: 215–224.

[11] 张云勇. 移动 agent 及其应用. 北京：清华大学出版社， 2002: 46–53.

陈志贤： 男， 1979 年生，博士生，主要研究方向为计算机在通信中的应用.

王汝传： 男， 1943 年生，教授，博士生导师，主要研究方向是计算机软件理论、计算机网络、信息安全及移动代理技术等.

王绍棣： 男， 1942 年生，教授、博士生导师，主要研究方向是计算机网络和信息安全.

孙知信： 男， 1964 年生，副教授，博士，主要研究方向为计算机网络技术.