一种面向移动 Agent 网络管理的安全模型

陈 志[1] 王汝传[1,2]
(南京邮电大学计算机学院 南京 210003)[1]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[2]

摘 要 基于移动 Agent 的网络管理模型利用移动 Agent 对网络进行灵活的管理,但该模型中网络管理站、被管理节点和移动 Agent 存在的安全问题阻碍了其进一步的发展和应用。研究这些安全问题,利用 Java 卡和加密技术构建一个综合的安全模型,给出安全管理过程。实例分析表明该模型能够对网络管理过程有效地实施硬件和软件的安全保护。

关键词 移动 Agent,网络管理,安全,Java 卡
中图法分类号 TP393.07 **文献标识码** A

Security Model for Mobile Agent-based Network Management

CHEN Zhi[1] WANG Ru-chuan[1,2]
(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[1]
(State Key Lab. for Novel Software Technology, Nanjing University, Nanjing 210093, China)[2]

Abstract Mobile agent-based network management model can have a flexible management on network based on mobile agents, but the security problems that exist in network manger, managed nodes and mobile agents of this model have hindered its further development and application. This paper studied these security problems, built an integrated security model based on Java card and encryption technology, and gave the secure management process. The case analysis shows that the proposed model can carry on security protection of hardware and software in the network management process.

Keywords Mobile agent, Network management, Security, Java card

1 引言

移动 Agent[1,2]是一个程序实体,拥有一定的智能和判断能力,可以在异构的网络上寻找合适的资源,代表用户完成特定的任务。利用移动 Agent 进行网络管理,得到了广泛的研究[3,4],但移动 Agent 本身的安全性以及在网络管理中出现的安全隐患阻碍了其进一步的发展和应用[5,6]。在移动 Agent 网络管理过程中,接纳移动 Agent 的每一个被管理节点可以对 Agent 的代码和数据拥有完全的控制权,它们很有可能滥用职权而破坏网络管理;另一方面,移动 Agent 离开网络管理站后具有相对的独立性,当遇到被伪装、篡改和重发等安全问题时,它将对管理站和被管理节点造成破坏,从而影响网络管理的安全运行。因此,利用移动 Agent 进行网络管理必须同时考虑到管理站和被管理节点以及执行网络管理任务的移动 Agent 所受到的威胁。本文就利用移动 Agent 进行网络管理所出现的安全问题提出一个综合的安全模型,来保障网络管理站、被管理节点和移动 Agent 的安全。

2 移动 Agent 网络管理安全模型

在移动 Agent 网络管理过程中,恶意攻击节点可能截获移动 Agent 程序代码和数据进行流量分析,破坏被管理网络的资源或者使其变得不可用,利用假冒的移动 Agent 进行非授权的网络管理活动。解决这些安全问题的方法包括基于检测的安全性措施、加密函数、黑匣子安全法和为每个节点配置可信赖且能抵御攻击的硬件[7,8]。网络管理站面临的安全问题是返回的移动 Agent 含有恶意的代码、移动 Agent 所带回的数据被篡改或伪造过,其可行的保护方案是通过可信度分析、与历史纪录比较等机制对返回的移动 Agent 进行检测,监控和禁止移动 Agent 执行程序代码。被管理节点面临各种恶意移动 Agent 带来的可能的攻击,其可行的保护方案包括移动 Agent 自带证明代码、数字签名、沙箱技术、核查记录等。

针对基于移动 Agent 的网络管理存在的上述安全问题及相应解决方案,提出了一个面向移动 Agent 网络管理的安全模型 MANMSM(Mobile Agent based Network Management

到稿日期:2009-01-22 返修日期:2009-04-03 本文受国家自然科学基金(60573141,60773041 和 60905040),国家高科技 863 项目(2007AA01Z404,2007AA01Z478),江苏省高校自然科学研究计划(08KJB520006),南京邮电大学科研基金项目(NY207020)资助。
陈 志(1978—),男,博士,讲师,主要研究方向为无线传感器网络、Agent 和多 Agent 系统、普适计算等,E-mail:chenz@njupt.edu.cn;王汝传(1943—),男,教授,博士生导师,主要研究方向为计算机软件、计算机网络、信息安全、移动 Agent 和虚拟现实技术等。

Security Model)，它利用 Java 卡[9]和加密技术对网络管理过程实施安全保护。MANMSM 分为两个部分(如图 1 所示)：一个部分在网络管理站，另一部分在被管理节点。

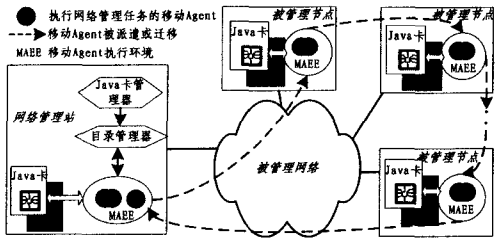

图 1　面向移动 Agent 的网络管理安全模型

2.1　MANMSM 管理站模型组成

MANMSM 网络管理站是实施网络管理安全保护的中心，负责协调整个管理模型的安全运行；根据不同的网络管理任务，产生相应的移动 Agent，并将其派遣到被管理节点在本地执行具体的管理任务。在网络管理站中，MANMSM 主要由 4 个部分组成。

(1)Java 卡管理器

Java 卡管理器为各个节点的 Java 卡加载各项必要的功能和数据，提供相应的 Java 卡证书，该证书包含 Java 卡的制造商、类型、所提供的安全策略以及有关密钥等信息。当一个 Java 卡分配给被管理节点，它的 Java 卡证书要提供给目录管理器。

(2)目录管理器

目录管理器提供一种目录服务。网络管理站和各个被管理节点需要在目录服务器处登记下列参考信息：所在节点的标识符(例如机器名或其他唯一的标识符)和物理网络地址、提供何种安全策略；Java 卡管理器为目录管理器提供各个节点的 Java 卡证书。这些信息用于为网络管理站定位被管理节点，对移动 Agent 进行加密服务，以保护其安全。

(3) 移动 Agent 执行环境 MAEE(Mobile Agent Execution Environment)

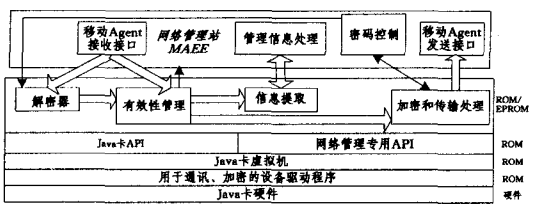

图 2　MANMSM 管理站模型

在 MANMSM 网络管理过程中，移动 Agent 通过与各个被管理节点交互，完成管理任务，返回管理结果。MANMSM 的 MAEE 对移动 Agent 提供各种功能支持。这里只考虑 MAEE 的安全管理方面，它一方面利用 Java 卡为移动 Agent 进行有效性管理和加密，另一方面解密返回管理站的移动 Agent，提取管理结果信息。如图 2 所示，MANMSM 管理站主要由 4 部分组成：①移动 Agent 接收接口，负责将移动 Agent 输入到 Java 卡；②管理信息处理模块，进一步处理 Java 卡提取的管理结果信息(如统计、过滤和综合等)；③密码控制模块，与目录管理器交互，为 Java 卡中的加密解密程序提供必要的密码(在管理站中，移动 Agent 加密和解密所涉及的密码很多，考虑到 Java 卡的存储容量限制和管理站的安全可靠性，这些密码都由目录管理器通过 MAEE 提供给管理站的 Java 卡；而在被管理节点中，加密和解密的密码保存在该节点的 Java 卡中)；④移动 Agent 发送接口，负责发送从 Java 卡中所获取的经过加密处理过的移动 Agent。

(4)Java 卡

Java 卡通过明确的接口与 MAEE 进行交互。一方面，它对即将执行网络管理任务的移动 Agent 进行有效性管理(如加上唯一标识、有效时间戳等)和各项加密；另一方面，Java 卡还对返回管理站的移动 Agent 进行解密，然后检查其有效性(如通过唯一标识检查是否重发，通过有效时间戳检查其是否过期)，最后 Java 卡为网络管理站提取管理结果信息。Java 卡提供一个平台，加密、解密、有效性管理和提取信息的活动都能在其中安全地运行。Java 卡的体系结构如图 2 所示。Java 卡 ROM 中最底层代码是访问存储器(包括 RAM，ROM 和 EEPROM)和 I/O 的设备驱动程序，根据需要也可能包括访问加密处理器的驱动程序。在这之上，就是 Java 卡虚拟机，它是传统的 Java 虚拟机的简化版本，将负责控制上层应用程序对 Java 卡硬件驱动程序的访问。Java 卡虚拟机之上就是实现了各种 API(基本的 Java 卡 API 和网络管理专用的 API)的 Java 中间字节码。最后，实现了 Java 卡专用功能的应用程序位于最上层。在 MANMSM 管理站中，这些应用程序包括解密器、有效性管理程序、信息提取程序以及加密和传输处理程序等。

2.2　MANMSM 被管理节点模型的组成

在被管理节点中，MAEE 为执行网络管理任务的移动 Agent 提供了落脚点，但它不需要处理管理结果信息，也不需要密码控制模块(被管理节点涉及到的密码都封装在该节点的 Java 卡中)。在安全管理方面，它包含 3 个部分(如图 3 所示)：①移动 Agent 接收接口；②移动 Agent 发送接口；③本地资源控制模块，这个模块是被管理节点 MAEE 的特有模块，它控制对被管理节点的资源访问、读写被管理对象、协助 Java 卡完成管理任务，同时保护被管理节点的资源。

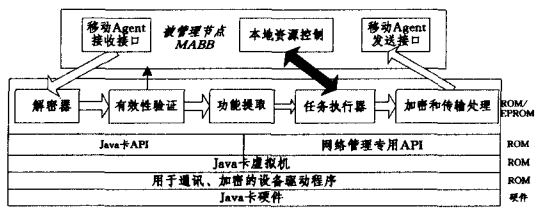

图 3　MANMSM 被管理节点模型

在被管理节点中，Java 卡所实现的功能不同于管理站的 Java 卡，它主要实施本地的网络管理。如图 3 所示，被管理节点的 Java 卡应用程序包括：①解密器，用于解密在本节点执行管理任务的移动 Agent。②有效性验证程序，验证移动 Agent 的合法身份和唯一标识，验证本节点私有代码和数据的唯一标识，通过有效时间戳检查其是否过期。如果验证通过，记录下该 Agent 的标识及本节点执行代码和数据的标识并将该 Agent 提交给功能提取程序处理，否则向 MAEE 报告错误信息。③功能提取程序，从验证通过的移动 Agent 中提取在本节点执行的代码和数据。④任务执行器，在 MAEE 的协助下执行网络管理任务。⑤加密和传输处理程序，卸解废弃的代码和数据(如只在本节点执行的代码、一些不再用的公共代码和数据)，重新组合移动 Agent，对变化部分和执行结果重新加密，并为 MAEE 传输该 Agent 提供信息。

2.3 模型的安全实现

2.3.1 硬件保护

在MANMSM中，Java卡不受节点及其MAEE的控制，但可以执行移动Agent，通过消息与不可信赖环境（如节点及其提供的服务）的交互来完成管理任务，从而为移动Agent提供一个安全的运行环境，其完成的功能有：①加密和解密移动Agent；②验证移动Agent的合法身份、唯一性和时间有效性；③执行网络管理任务；④提取管理结果信息（在网络管理站中）等。不论在网络管理站还是在被管理节点，Java卡都不受本地节点控制，而通过与MAEE交互完成网络管理任务。另外，被管理节点不可更改移动Agent的代码和数据，移动Agent也只能根据自己的权限获取节点的资源，进行合法的网络管理。因而，Java卡使得MANMSM的网络管理站、被管理节点和移动Agent都得到了保护。

2.3.2 加密和数字签名

在基于移动Agent的网络管理过程中，移动Agent迁移到各个被管理节点，完成管理任务，其所执行的代码和数据（在本文中，数据指除执行代码以外的信息）可能是相同的（称其为公共代码和数据），也可能是不同的（称其为被管理节点的私有代码和数据）。其中，公共数据也包含移动Agent的所要访问节点目录、路由信息和有关安全的数据等。

在MANMSM中，采用常规密钥密码体制的加密解密算法和公开密钥密码体制的加密解密算法对移动Agent不同代码和数据部分进行加密，可以实现数字签名。公共代码和数据要被所有的被管理节点执行，因此只需用常规密钥密码体制的加密解密算法进行处理；而私有数据和代码属于各个被管理节点，从安全角度考虑，必须用公开密钥密码体制的加密解密算法对其进行处理。被管理节点的私有代码和数据用加密密钥PK加密后，只能由所属的合法被管理节点或网络管理站用解密密钥SK进行解密。在被管理节点中，私有代码和数据以及一些公共代码和数据不再用时，需要从移动Agent卸解掉，而产生的私有数据要用该节点的加密密钥PK进行加密；另外，新产生的公共管理结果数据以及剩下的公共代码和数码组合后要用常规加密解密算法的密钥重新加密。在MANMSM中，常规加密解密算法的密钥和公开密钥密码体制的加密解密算法涉及的两个密钥都得到了保护。这些密钥都是由网络管理站及其Java卡管理器自动生成和加载的（存入Java卡证书或保存到Java卡），不需要人为地分配。另外，这些密钥只能由功能模块读取，例如被管理节点Java卡中保存的密钥只能由Java卡专用功能的应用程序（如解密器、加密和传输处理程序）访问。因为Java卡不受被管理节点的控制，所以这些密钥对节点是保密的。

MANMSM中采用密码技术，实现了对移动Agent信息的数字签名。移动Agent的公共代码和数据只能由网络管理站和各被管理节点的Java卡进行加密和解密，而私有代码和数据只能由所属的合法被管理节点或网络管理站进行加密和解密。在MANMSM网络管理过程中，因为Java卡不受被管理节点控制，其输入必须是加密之后的移动Agent，被管理节点因不知道移动Agent代码和数据加密的密钥而不能对移动Agent进行加密，所以执行网络管理任务的移动Agent只能最先由网络管理站发出。移动Agent的数字签名使网络管理站和被管理节点可通过核实移动Agent的合法身份来防止伪造，从而保证网络管理的准确性、真实性和安全性。

2.3.3 其他安全保护

在网络管理中，不同管理任务对时间的要求是不一样的。一些紧急的任务需要在有限的时间内完成，当然其他的管理任务对于不断变化的网络来说也是有一定的时间上限的。因此，在MANMSM中，在移动Agent的公共数据中放入了一个时戳数据，网络管理站和各被管理节点据此可以验证收到的移动Agent是否过期，这也有助于确定移动Agent是否为重发的或已被篡改。在MANMSM中，还为每一个执行网络管理任务的移动Agent和每一个私有代码分别分配了一个唯一标识符，前一个标识符放入公共数据中，后一个标识符放入私有数据中。为移动Agent及其私有代码分配唯一标识符的主要目的是避免移动Agent的修改或重发。在被管理节点中，Java卡记录访问过的移动Agent的唯一标识符和执行过的私有代码的唯一标识符，通过验证这两个标识符，便可以确定移动Agent及其私有代码的合法性和不重复性。

另外，在MANMSM中，可以在移动Agent的公有数据和私有数据中放入更多的安全策略（如复制限制等），这样公有代码和私有代码的执行能够得到更多的保护。

3 模型的安全管理过程

在MANMSM中，假设执行管理任务的移动Agent要访问n个被管理节点，每一个被管理节点的Java卡都保存有常规加密解密算法的密钥和公开密钥密码体制的加密解密算法涉及的两个密钥。这里假设常规加密解密算法的密钥为K，第$i(1\leqslant i\leqslant n)$被管理节点的Java卡保存的公开密钥密码体制的加密解密算法的加密密钥为PK_i，解密密钥为SK_i。网络管理站的Java卡先从MAEE可以获得K，$PK_1\sim PK_n$，$SK_1\sim SK_n$。在管理过程中，网络管理站的MAEE创建移动Agent（装配有公共代码和数据、所访问的各节点的私有代码和数据），管理站和各个被管理节点的MAEE负责移动Agent的传送和接收。具体的安全网络管理过程如下：

(1)网络管理站的Java卡先对移动Agent进行有效性管理，为移动Agent和各个私有代码加上唯一标识、时戳数据等，然后用常规加密算法加密移动Agent的公共代码和数据，再分别用公开密钥密码体制的加密算法对各个节点的私有代码和数据进行加密，最后交给MAEE，传送给第一个被管理节点。

(2)移动Agent到达第$i(1\leqslant i\leqslant n)$被管理节点后，MAEE将其上载到该节点的Java卡中。

(3)第i被管理节点的Java卡用常规解密算法解密移动Agent的公共代码和数据，再用公开密钥密码体制的解密算法对本节点的私有代码和数据进行解密，然后从解密后的数据中提取移动Agent的唯一标识、私有代码和数据的唯一标识、时戳数据等，对移动Agent进行有效性验证（验证移动Agent以及本节点的私有代码是否重发、有没有过期等）。

(4)第i被管理节点Java卡的功能提取程序从通过有效性验证的移动Agent中提取需在本节点执行的公共代码和数据以及私有代码和数据，交给Java卡任务执行器。任务执行器通过与第i被管理节点MAEE的本地资源控制模块进行交互，完成网络管理任务。

(5)第i被管理节点完成网络管理任务后，Java卡卸解掉

移动 Agent 中不再需要的私有代码和数据以及一些公有代码和数据，重新组合移动 Agent，对公有代码和数据（可能包含新的数据）用常规加密算法重新加密，而对新的私有数据（可能不存在）用公开密钥密码体制的加密算法重新加密。最后，Java 卡将重新组合后的移动 Agent 和下一个节点的传输信息交给第 i 被管理节点的 MAEE。第 i 被管理节点的 MAEE 将移动 Agent 传送到下一个节点。移动 Agent 在剩下的被管理节点继续进行网络管理。

(6)移动 Agent 完成所有管理任务后，返回管理站。网络管理站的 MAEE 将其交给管理站的 Java 卡。

网络管理站的 Java 卡先用常规解密算法解密移动 Agent 的公共数据，再用公开密钥密码体制的解密算法对所有节点的私有数据进行解密，然后对解密后的移动 Agent 进行有效性验证。通过验证后，Java 卡的信息提取程序就从这些解密后的数据中提取管理结果信息，交给管理站 MAEE 的管理信息处理模块做进一步的处理。网络管理站可根据这些信息做最后的统计分析等工作。

4 实例分析

4.1 实例分析一

攻击者截获了被管理网络传输中的移动 Agent，就有可能篡改、伪造和重发该移动 Agent。在 MANMSM 中，攻击者必须获取常规加密解密算法的密钥或者公开密钥密码体制的加密解密算法的加密密钥 PK 和解密密钥 SK，才能够篡改和伪造该移动 Agent。在 MANMSM 中，这些密钥都是由网络管理站及其 Java 卡管理器自动生成和加载（存入 Java 卡证书或保存到 Java 卡）的，对任何人（包括管理员）都是保密的；同时，各个被管理节点的 Java 卡都不受节点的控制，因此攻击者一般来说是不可能获取这些密钥的。当然还是有可能，我们将在实例分析二和实例分析三中进一步讨论密钥泄密后引起的安全问题。攻击者截获传输中的移动 Agent 后，对网络管理的另一个攻击就是重发。但在 MANMSM 管理过程中，通过 Java 卡的有效性验证（管理站 Java 卡的有效性管理），检查移动 Agent 唯一的标识及移动 Agent 中被管理节点私有代码唯一的标识和时戳数据，能够验证该 Agent 是否访问过当前节点，该 Agent 中被管理节点私有代码是否曾经执行过，该 Agent 是否过期。因此，MANMSM 能够在一定程度上抵御传输中移动 Agent 被篡改和伪装，也能够有效地抵御重发攻击。

4.2 实例分析二

攻击者获取了公开密钥密码体制的加密解密算法的加密密钥 PK 和（或）解密密钥 SK。在 MANMSM 中，因为公开密钥密码体制的加密解密算法是用来加密或解密移动 Agent 的各个被管理节点的私有代码和数据的，所以当攻击者只获得某个被管理节点公开密钥密码体制的加密解密算法的解密密钥 SK 时，可以解密移动 Agent 中属于该节点的私有代码或数据。但当他没有获得加密密钥 PK 时，就不能篡改和伪造私有代码或数据。因为 Java 卡输入的必须是加密后的私有代码和数据，而攻击者因不知道加密密钥 PK 而无法对篡改和伪造后的私有代码或数据进行加密，所以攻击者对私有代码或数据的篡改和伪造对于 Java 卡执行管理任务来说是无效的。因此，当攻击者同时知道加密密钥 PK 和解密密钥 SK 时，就可以在 MAEE 将移动 Agent 输入 Java 卡之前，解密属于该节点的私有代码或数据，然后进行篡改和伪造，并重新加密后放回移动 Agent，输入到 Java 卡中，从而欺骗了本节点的 Java 卡执行非法的网络管理任务。另外，攻击者在移动 Agent 完成任务输入到 MAEE 后，可以解密本节点的私有数据，进行篡改和伪造，然后重新加密后放回移动 Agent，从而欺骗网络管理站。当然，如果攻击者在当前节点还知道其他被管理节点公开密钥密码体制的加密解密算法的加密密钥 PK 和解密密钥 SK，他就可以篡改和伪造其他被管理节点的私有代码或数据。但我们看到公开密钥密码体制的加密解密算法的加密密钥 PK 和解密密钥 SK 的泄密只影响局部节点的安全网络管理，不影响其它部分安全的网络管理。因此，MANMSM 对各个被管理节点私有代码和数据的分开加密保护，能够将网络管理过程的安全隐患限制在局部节点，从而减少了安全威胁的影响在整个被管理网络中的扩散。

4.3 实例分析三

攻击者获取了常规加密解密算法的密钥。因为常规加密解密算法是用来加密或解密移动 Agent 的公共代码和数据的，所以攻击者获得常规加密解密算法的密钥，便可以解密所有移动 Agent 的公共代码或数据，并篡改和伪造它们（比如移动 Agent 路由信息、时戳数据、管理结果数据等），然后加密，欺骗网络管理站或被管理节点。另外，攻击者获得常规加密解密算法的密钥后，可以伪装成网络管理站发送非法的移动 Agent，从而可以获取非法权益。当然，在 MANMSM 中，可以取消常规加密解密算法对移动 Agent 公共代码和数据的加密和解密，而将公共代码和数据放入各个被管理节点的私有代码和数据中，然后一起用公开密钥密码体制的加密解密算法进行加密和解密。这种改进的优点使 MANMSM 网络管理的安全性得到提高，这是因为个别被管理节点公开密钥密码体制的加密解密算法密钥的泄密只影响本节点的安全管理，而不能破坏其他被管理节点的安全管理。这种改进的缺点是移动 Agent 的体积变大，被管理网络的通信量增加。常规加密解密算法的密钥的泄密对移动 Agent 本身和网络管理过程所造成的破坏是很大的。但我们看到，在 MANMSM 中，网络管理站只是获取移动 Agent 带回的信息，禁止移动 Agent 执行程序代码，同时各个被管理节点 MAEE 中的本地资源控制模块控制对被管理节点的资源访问，保护被管理节点的资源。因而 MANMSM 能够有效地保护网络管理站和各个被管理节点。

4.4 实例分析四

在网络管理过程中，根据不同的管理任务，移动 Agent 的代码和数据变化情况是不一样的。MANMSM 在一些情况下能够为网络管理提供更加安全的保护。将移动 Agent 公有代码和私有代码、公有数据和私有数据分别合在一起对典型管理实例做进一步的分析。

(1)移动 Agent 只含有私有代码和公共数据，主要用于收集管理信息。如图 4(a)所示，这时代码逐渐减少，数据逐渐增多；

(2)移动 Agent 只含有私有代码和数据以及公共数据，主要用于设置管理参数。如图 4(b)所示，这时代码逐渐减少，数据也逐渐减少；

（下转第 107 页）

受，且不会对网络性能产生明显影响。

结束语 本文针对干扰环境中武器协同数据链网络骨干节点的路由问题，提出了一种面向延迟的路由方法，并给出了实现模型。该方法通过信息反馈、跨层手段感知、充分利用了链路端到端时延信息以及干扰状况，来为当前节点选择路由，实现了信息的最小端到端时延，满足了武器协同数据链网络中低时延业务的需求。仿真表明，同传统的 DSDV，OLSR 协议相比，I-DOBR 路由方法除开销稍大以外，其他主要性能指标均好于两者。

参 考 文 献

[1] Belding-Royer E M. Multi-level Hierarchies for Scalable Ad hoc Routing[C]// Santa Barbara. Wireless Networking (WINET). California: Department of Computer Science. University of California, 2003: 461-478

[2] Saha A K, Johnson D B. Self - Organizing Hierarchical Routing for Scalable Ad hoc Networking[R]. Houston, Texas: Rice University Department of Computer Science, 2000

[3] Xu K, Hong X, Gerla M. Landmark Routing in Ad hoc Networks with Mobile Backbones[M]. Orlando: Academic Press, INC., *2003: 110-122*

[4] Chiang C C, Wu H K, Liu W, et al. Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel[C]// IEEE Singapore International Conference on Networks. Guangzhou, *1997: 197-211*

[5] Westcott J, Lauer G. Hierarchical routing for very large net - works[C]// IEEE MILCOM'84. Los Angeles, 1984: 214-218

[6] Shiang Hsien-po, van der Schaar M. Multi - User Video Streaming over Multi-Hop Wireless Networks: a Distributed, Cross-Layer Approach Based on Priority Queuing[J]. IEEE Journal Selected Areas in Communications, 2007, 25(4): 770-785

[7] Krishnaswamy D. Network-Assisted Link Adaptation with Power Control and Channel Reassignment in Wireless Networks[C]// 3G Wireless Conf. New York, 2002: 165-170

[8] Kleinrock L. Queuing Systems Volume I: Theory [M]. New York: Wiley-Interscience Publication, 1975: 320-322

[9] Srivastava V, Motani M. Cross-Layer Design: A Survey and the Road Ahead[J]. IEEE Comm. Magazine, 2005, 43(12): 112-119

[10] van der Schaar M, Turaga D S. Cross-Layer Packetization and Retransmission Strategies for Delay-Sensitive Wireless Multimedia Transmission[J]. IEEE Trans. Multimedia, 2007, 9(1): 185-197

[11] Xiao Wendong, Boon Hee Soong, Choi Look Law. QoS Routing Protocol for Ad hoc Networks with Mobile Backbones[C]// IEEE ICNSC. Singapore, 2004: 1212-1217

(上接第 92 页)

(3)移动 Agent 只含有私有代码和公共数据，不产生结果数据。如图 4(c)所示，这时代码逐渐减少，数据不变；

(4)移动 Agent 只含有公共代码和数据以及私有数据，主要用于收集管理信息。如图 4(d)所示，这时代码不变，数据逐渐增多；

(5)移动 Agent 只含有公共代码和公共数据以及私有数据，主要用于设置管理参数。如图 4(e)所示，这时代码不变，数据逐渐减少；

(6)移动 Agent 只含有公共代码和公共数据，不产生结果数据。如图 4(f)所示，这时代码不变，数据也不变。

(1)－(3)含有私有代码而不含有公共代码，而(4)－(6)含有公共代码而不含有私有代码，因为移动 Agent 中属于某个被管理节点的私有代码被篡改和伪造只影响这个节点安全的网络管理，而移动 Agent 中公共代码被篡改和伪造将影响要访问的所有被管理节点安全的网络管理，所以在(4)－(6)网络管理过程中，MANMSM 能够提供比(1)－(3)更加安全的保护。可见，在 MANMSM 中，我们能够基于不同的安全要求，灵活地选择和装配不同的移动 Agent 进行具体的网络管理。

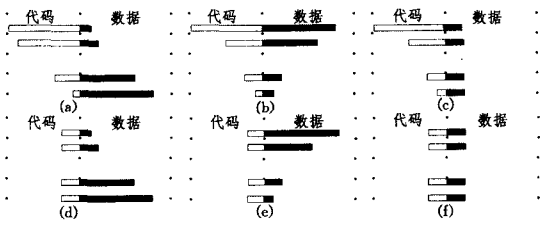

图 4 安全管理过程移动 Agent 典型的代码和数据变化实例

结束语 面向移动 Agent 网络管理的安全模型 MANMSM 利用 Java 卡和加密技术对基于移动 Agent 的网络管理过程实施硬件和软件的保护，较好地解决了网络管理站、被管理节点和移动 Agent 的安全保护问题。但该模型并不能保证网络管理过程绝对安全，因为 MANMSM 安全性的高低还要取决于安全保护措施(例如网络管理站、Java 卡)自身的保护程度，所以在 MANMSM 中，安全的网络管理站和 Java 卡能够给 MANMSM 网络管理过程带来高度的安全性。

参 考 文 献

[1] 张云勇，刘锦德. 移动 agent 技术[M]. 北京：清华大学出版，2003

[2] Braun P, Rossak W. Mobile Agents : Basic Concepts , Mobility Models, and the Tracy Toolkit[M]. Morgan Kaufmann Publishers, 2004

[3] 王汝传，徐小龙，黄海平. 智能 Agent 及其在信息网络中的应用[M]. 北京：北京邮电大学出版社，2006

[4] Autran G, Li Xining. Large Scale Deployment a Mobile Agent Approach to Network Management[C]// Proceedings of 2008 Seventh International Conference on Networking (ICN 2008). April 2008: 614-619

[5] Nilchi A R N, Vafaei A, Hamidi H. Evaluation of security and fault tolerance in mobile agents[C]// Proceedings of 2008 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN'08). May 2008: 1-5

[6] Ketel M. Applications of mobile agents and related security issues[C] // Proceedings of IEEE SoutheastCon 2007. March 2007: 23-28

[7] 陈志，王汝传. 移动代理网络管理模型的安全性研究[J]. 南京邮电学院学报，2004, 24(2): 70-75

[8] Koliousis A, Sventek J. A Trustworthy Mobile Agent Infrastructure for Network Management[C]// Proceedings of 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (IM'07). 2007: 383-390

[9] Mayes K, Markantonakis K. Smart Cards, Tokens, Security and Applications[M]. Berlin: Springer, 2008