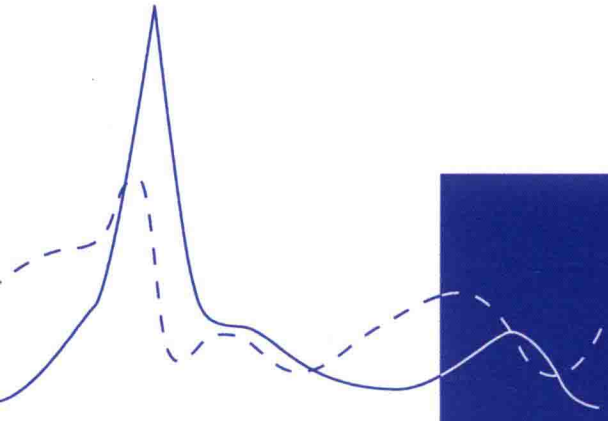


移动智能体及其主动保护技术

吴杰宏 著

北京航空航天大学出版社
BEIHANG UNIVERSITY PRESS

移动智能体及其主动保护技术

吴志宏　著

北京航空航天大学出版社

内 容 简 介

本书从实际需要出发，从主动保护和同步检测两方面对移动代理的保护技术进行了深入分析和研究，从代码数据迷乱、控制结构迷乱、组合函数和同态理论、时间核查等角度展开了研究；从改进蜂拥算法和满足安全通信距离要求两方面对多无人机的安全通信进行了分析和研究；从引入变速虚拟领导者、虚拟通信圆环、改进目标位置移动函数等角度展开了研究。

全书共分2篇，包括10章。上篇是移动代理篇，包括6章，介绍移动代理的主动保护策略和方法及在IDC分布式网络管理系统中的实际应用；下篇是无人机篇，包括4章，介绍多无人机安全通信距离的协同控制方法。

本书内容严谨，结构清晰，例证合理，既可作为高等院校计算机相关专业研究生的参考教材，也可作为对信息安全、移动代理技术、多无人机安全通信技术感兴趣的读者和相关专业科研人员的参考用书。

图书在版编目(CIP)数据

移动智能体及其主动保护技术 / 吴杰宏著. -- 北京 : 北京航空航天大学出版社，2017.3

ISBN 978-7-5124-2334-3

Ⅰ. ①移… Ⅱ. ①吴… Ⅲ. ①移动通信－安全技术 Ⅳ. ①TN929.5

中国版本图书馆CIP数据核字(2017)第030790号

移动智能体及其主动保护技术

吴杰宏 著

责任编辑 杨 昕

*

北京航空航天大学出版社出版发行

北京市海淀区学院路37号(邮编100191) http://www.buaapress.com.cn

发行部电话：(010)82317024 传真：(010)82328026

读者信箱：goodtextbook@126.com 邮购电话：(010)82316936

北京九州迅驰传媒文化有限公司印装 各地书店经销

*

开本：710×1 000 1/16 印张：9.5 字数：202千字

2017年3月第1版 2017年3月第1次印刷

ISBN 978-7-5124-2334-3 定价：40.00元

前　言

移动代理(MA)是能够在异构网络中自主迁移的软件实体，它的迁移性和自治性很好地弥补了分布式技术的不足，具有广阔的应用前景。目前对移动代理的研究已经取得一些成果，但尚不完善的移动代理安全技术正逐渐成为移动代理发展的障碍。与主机保护技术相比，对移动代理主动保护技术的研究还处于起步阶段。

无人机(UAV)已被广泛应用于生活中的各个领域。相对于单个无人机，多无人机在执行任务过程中的高效性优势越来越明显。无人机间的通信性能，严重影响了信息交换的实时性。因此，基于无人机间安全可靠通信的无人机协同控制方法就成为当今比较重要的研究课题。

本书是作者多年研究所得，其目的是给对移动代理和多无人机安全通信感兴趣的研究人员提供安全保护及安全通信技术的一些见解，希望能够起到抛砖引玉的作用。全书分上、下两篇共10章，涉及数据迷乱、混合加密、时间核查等方面的移动代理主动保护策略，以及如何改进相关参数和技术条件，使无人机之间满足安全通信的范围要求。本书主要内容如下：

(1) 根据迷乱的原则和目标，提出基于数据迷乱的移动代理保护策略，设计数据抽象、过程抽象以及内嵌数据类型的具体迷乱方案。对迷乱的代价和开销进行了讨论，并对已有方案进行改进，不仅能够成功地抵御反向解析代码，还能在一定程度上缩短执行时间，并减小存储空间。

(2) 针对程序的不同控制结构，提出移动代理的控制流迷乱策略。基本块分裂迷乱、交叉循环迷乱以及替换goto迷乱，是本书所采用的三种控制流迷乱的主要方法。在迷乱转换的同时，详细分析了解码程序中采用的模式匹配原则，并以此作为依据改进算法，增强抗回弹能力，减小时空开销。实验结果表明，该迷乱算法不仅能够抵御各种解码器的攻击，而且比单级退出迷乱和多级退出迷乱更具优越性。

(3) 提出基于组合函数(FnC)和混合乘法同态加密(S－MMHE)技术的移动代理保护策略。研究策略起源于由Sander和Tschudin提出的移动密码学思想，书中用FnC和S－MMHE方案来加密移动代理，是对

移动密码学思想的扩展。加密的移动代理能够在任何主机上运行而不需解密，加密产生的结果数据最终由移动代理生成者解密，真正达到了代理的保护目的。同时对S-MMHE方案的安全性进行了验证，证明了方案的可行性和有效性。

(4) 基于时间核查协议的移动代理保护方案是本书提出的又一个移动代理保护策略。时间核查协议的设计思想是基于限制移动代理在目标主机上的执行时间，按照协议，移动路线中的每一台主机都要记录代理的到达和完成任务时间，并让时间记录和移动代理一起迁移到路线中的下一台主机，最后路线中所有主机的时间记录和代理产生的结果数据都被送回到派发代理的初始主机。初始主机通过三个时间核查不等式来查验在代理执行期间，路线中主机的安全行为；如果有一个不等式不满足，则前后两台主机都是可疑的。通过这个时间核查协议可以侦测出全部有恶意行为的个体主机，虽然不能侦测出所有的串通攻击，但提供了避免串通的方法。

(5) 合并前面提出的数据迷乱和控制流迷乱方案，设计了适合IDC (Internet Data Center)分布式网络管理应用的移动代理迷乱器。迷乱程序通过对执行任务的移动代理进行派发前迷乱，可有效地保护移动代理的安全。

(6) 提出基于移动代理迷乱器和时间核查协议合并的具体方案，并在基于移动代理的IDC网络管理环境中进行实施。移动代理代码和数据的迷乱过程在移动代理迷乱器中进行，迷乱后的移动代理遵照时间核查协议执行任务，既可以保护代理的安全，又可以检测恶意主机。通过对比移动代理在不同方案中的抗攻击能力，验证了方案的优势。

(7) 提出基于FnC和S-MMHE的加密技术与时间核查协议的合并MA保护方案，与单一的S-MMHE方案或时间核查方案相比，本方案可以保护MA安全，并有效侦测出恶意行为主机，增加了系统的安全性。

(8) 加入对于变速虚拟领导者的导航输入跟踪项，改进学者Olfati-Saber提出的采用固定速度虚拟领导者的蜂拥算法，并给出改进算法的稳定性分析。经过实验对比，改进的算法能够使各无人机节点更准确地追踪变速虚拟领导者的速度。

(9) 基于上述改进的蜂拥算法，结合虚拟通信圆环和改进的目标位置移动函数，通过研究多无人机的群组通信范围和无人机间距离的关系，提出一种解决多无人机间安全通信问题的分布式协同控制方法，最终使各

无人机节点移动到满足其安全通信距离要求的期望位置上。利用工具MATLAB和基于AODV/OLSR无线自组织网络协议的NS2工具对多无人机的运动过程进行仿真，并对比分析实验结果，验证了算法的有效性和收敛性。本方法是解决多无人机间安全通信的一种有效方式。

本书由吴杰宏统稿编写，曹玉琪参与了第9、10章的编写工作。

MA及多UAV安全通信技术发展迅速，涉猎分支领域广泛。作者学识有限，兼时间和精力有限，书中难免存在不妥之处，若蒙读者诸君不吝告知，将不胜感激。

吴杰宏

2016年11月

目　　录

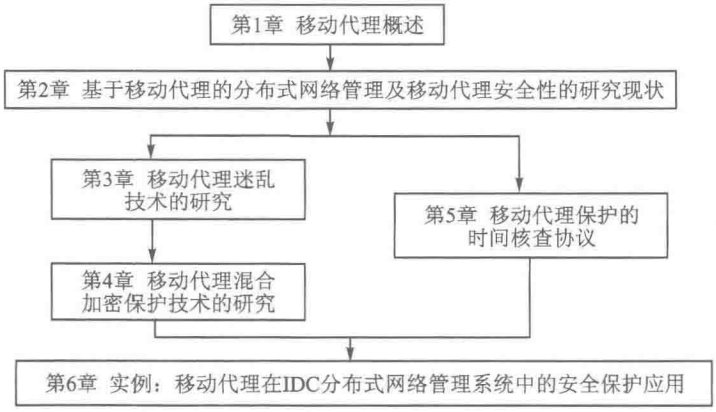
上篇　移动代理

下篇　无人机

上篇　移动代理

移动代理篇的结构及章节安排

移动代理篇的结构和章节安排如下：



第 1 章：阐述了课题的研究背景，针对当前分布式计算发展的特点及移动代理技术所存在的安全性问题，给出了课题的研究目标和研究思路，概述了研究内容和主要研究工作。

第 2 章：对所涉及的研究领域——基于移动代理的分布式网络管理及移动代理安全性的研究现状，首先，从网络管理的基本概念出发，对两种典型的体系结构进行了描述，并介绍了基于移动代理的分布式网络管理技术；其次，系统地介绍了移动代理技术的特点及其发展优势；最后，就影响移动代理应用的安全性问题进行了具体分析，说明移动代理保护的重要性。

第 3 章：提出了基于控制结构和数据迷乱的移动代理保护方案，给出了具体实现方案，并对其可行性进行了验证。

第 4 章：提出了基于组合函数和混合乘法同态加密的移动代理保护方案，该方案改进了移动加密技术的思想，给出了方案的具体算法，并对其正确性和安全性进行了验证。

第 5 章：提出了基于检测的时间核查协议，该协议通过限制主机的执行时间，可以检测出对移动代理进行攻击或窃听的有恶意行为的主机。在改进措施中指出，该协议通过与第 3 章提出的迷乱代码的移动代理保护方案合并，既可以保护移动代理代码避免被窃听或篡改，还可以准确侦测出有恶意行为的主机；通过与第 4 章提出的基于组合函数和混合乘法同态加密的移动代理保护方案合并，使其保护移动代理和检测恶意主机的能力增强。

第 6 章：首先以第 3 章所提出的技术为核心，设计了一个代码迷乱器，用来对网络管理中派发前的移动代理进行迷乱；接着给出 IDC 基于移动代理的分布式网络管理模型，描述了网络管理系统中管理域的动态划分方法，在给出的 Aglet 安全模型的基础上，对第 5 章改进措施中所提出的基于代码迷乱和时间核查的移动代理保护方案进行了验证，证实了该方案的可行性和有效性。

第 1 章　移动代理概述

近年来，随着 Internet 的迅速发展，网络技术和分布式人工智能领域不断取得新的突破，传统的分布式计算模式（如客户/服务器模式）已经不能满足当前异构网络上的复杂分布式计算的要求。WWW（World Wide Web）已被广泛用作实现信息发布、电子商务以及各种娱乐等的业务平台。移动代理（Mobile Agent，MA）技术就是在这种情况下诞生的一种新的网络计算技术。

代理（Agent）的研究起源于人工智能领域。代理是指模拟人类行为与关系，具有一定智能并能够自主提供相应服务的程序。与现在流行的软件实体相比，代理的粒度更大，智能化更高。随着网络技术的发展，可以让代理在网络中移动并执行，完成某些功能，这就是移动代理的思想。

移动代理是一种能在异构网络中从一台主机自主迁移到另一台主机，并可与其他代理或资源进行交互的程序。它实际上是代理技术与分布式计算技术的结合体。移动代理代表用户完成特定的任务，具有自主性、移动性、协作性。它能有效地减少分布式计算的网络负载，提高通信效率，支持异步及自主交互，支持非连接互操作，为移动计算提供了一种灵活的模式，在电子商务、信息的收集与发布、网络及时监控、科学并行计算等领域具有广阔的应用前景。

1.1　研究背景

移动代理技术的移动特性适用于多种 Internet 应用，如移动计算、智能网络、电子商务等，应用范围广泛。因此，移动代理技术能否具有足够的安全性和稳健性就成为人们关心的首要问题。在移动代理系统中，代理的运行需要分布式系统中的远程主机为其提供执行环境。远程主机的所有者、代理所代表的用户以及移动代理软件的开发者都是不同的实体，这样就必然会存在安全隐患。

移动代理系统的安全问题主要涉及以下三方面。

1. 网络中数据传输的安全性

当移动代理在开放网络中漫游时，它所携带的程序代码和数据都有可能受到如下的安全威胁：

① 被动攻击。这种攻击模式有两种情形：一种情形是攻击者并不干预移动代理

通信流量，只是试图从中获取代理程序中存储并传递的敏感信息；另一种情形是由于数据已经采用传输加密，攻击者无法得到具体的数据，但可以通过对相关数据进行流量分析，比如分析通信频度、交换的数据长度、通信双方的身份等来获取所需的信息。

② 主动攻击。主动攻击是指攻击者能够任意截获并修改网络中的数据，甚至将传输的数据删除，并用伪造的数据取代；另外，攻击者也可以进行身份伪装，如伪装成系统的一个合法参与者，截取并处理发送给它的相应信息。

2. 恶意代理攻击执行环境

代理程序将在远程主机上运行，这使得主机有可能面临各种恶意代理程序所带来的攻击。这些攻击可归纳为如下几种：

① 偷窃敏感资料：当恶意代理访问某公司服务器时，它有可能试图打开包括该公司商业机密的敏感文件，并将这些信息发送给指定用户，从而使这些用户利用这些信息在商业竞争中获利。

② 破坏服务器系统资源：恶意代理访问远程主机时，它有可能删除该主机的某些重要文件甚至格式化整个硬盘。

③ 拒绝服务攻击(DoS)：恶意代理可以故意大量消耗服务器的系统资源，如硬盘空间、内存、网络端口等，从而使该服务器无法完成与其他代理的交互以及相应的正常业务。

④ 扰乱性攻击：如不断地在服务器上打开各种应用程序的窗口或使机器不断地重启等。

3. 恶意主机攻击移动代理

因为移动代理必须在远程主机上运行，所以移动代理的代码以及所携带的数据对于远程主机来说都是暴露的。若一个主机是恶意的，则它可以对代理进行如下的几种攻击：

① 恶意主机可以破坏或终止代理，从而阻止该代理继续执行相应的用户任务。

② 恶意主机可以偷窃代理所携带的有用信息，如代理携带的用户信息、电子货币以及其漫游过程中所搜集的中间信息等。

③ 恶意主机可以修改代理携带的数据，以满足自己的利益，如当一个代理负责为用户收集某种商品的最佳报价时，该主机可以通过篡改代理之前所收集的报价，使用户误以为它提供的报价为最佳价格。

④ 恶意主机可以通过改写部分代理的代码，使其在返回用户或漫游到其他主机后执行一些恶意操作。

1.2　恶意主机问题目前的解决方案

保护移动代理本身的安全对策在某些方面与传统的安全机制有着本质的区别。这是因为传统的安全机制不是用来防止执行环境对应用程序的攻击威胁，而移动代理系统却存在着如何在不完全可信的移动代理平台上安全地执行移动代理的问题。移动代理保护问题也称为恶意主机问题，它曾一度被认为是不可解决的。

目前，对于保护移动代理免遭恶意主机攻击的研究已经有了一些解决方案。但与保护主机技术相比，移动代理的保护技术仍处于起步阶段。下面对一些方案进行简单介绍。

1. 两个代理之间相互保护

Roth 利用两个代理之间的合作提出了相互保护的思想。该思想是假设在开放的系统中，主机相互间的信任关系是很有限的，恶意主机间的联合很困难，因此提出将代理的运行结果存储在具有不同路由的合作代理上来进行保护。其缺点如下：

① 合作代理的丢失就意味着相应代理运行结果的丢失。

② 恶意主机间进行联合的可能性依然存在，协议不能很好地解决该问题。

2. “避难所”

利用封闭的抗破坏硬件子系统，Yee 提出了给移动代理提供一个“避难所”(Sanctuary)的思想。在“避难所”内，代理可以安全地运行。其缺点是：要求每一主机都要购买相应的硬件装置，也要求硬件供应者完全可信。

3. 环境密钥

学者 Riordan 和 Schneier 提出的生成环境密钥的思想使代理的代码只有在具备一定的环境条件下才能解密。其主要缺点是：恶意主机可以不断模拟环境条件，对代理代码进行试解；且协议要求主机对环境进行连续监控。

4. 轨迹追踪

Vigna 引入了轨迹追踪的思想来保护移动代理。代理运行时追踪改变代理状态的指令，主机将代理在其上运行轨迹的 Hash 值连同运行结果传送给代理起始者。当代理起始者怀疑主机的行为时，可以再次执行代理，并向主机索要相关的运行轨迹进行证实。若执行过程与所提供的相关运行轨迹不符，则说明主机说谎。该协议不仅可以发现攻击，而且可以对主机的恶意行为提供证据。其缺点如下：

① 如何确定代理执行结果可疑。因为只有在代理主人对代理执行结果产生怀疑时才会对运行轨迹进行相应的证实。

② 由于随时可能受到询问，故主机必须对代理运行轨迹保存很长时间。

③ 需要由一个可信的第三方来对主机的恶意行为进行惩罚。

5. 黑　盒

基于时间受限的黑盒在一定时间内可以提供很好的安全性质，但这段时间以后，代理的运行代码、状态等不再受到保护。它主要采用迷乱对代理的代码、数据等进行隐藏。协议的主要困难是安全时间的估计，同时由于迷乱后的代码长度远大于迷乱前，故系统也要具有一定的运算资源。

6. 加密程序

从理论上看，加密程序的思想对于保护移动代理代码的保密性和完整性应该是非常有效的。主机直接执行加密后的代理代码。代理返回起始主机后，通过解密函数，起始主机可以恢复出相应的运行结果。但是它的困难是找到适合于此的加密函数。

因此，如何以最小的代价解决移动代理系统的安全问题，尤其是如何保护移动代理免受恶意主机攻击，已经成为当前网络信息安全研究的主要目标，并受到国内外的广泛关注。这个难题的解决是移动代理技术得到更广泛应用的关键前提，具有重要的现实意义。