 移动Agent有很多优点适合于分布式入侵检测系统。 本文提出一种基于移动Agent的分布式入侵检测系统方法，讨论了系统结构及其Agent机制；详细讨论了移动Agent技术在分布式入侵检测系统中的应用特点和存在的问题；最后给出了未来的入侵检测系统的发展趋势。 1、入侵检测系统综述 1.1 入侵检测系统 随着信息技术的发展，计算机成为社会活动中的必不可少的工具，大量重要的信息存储在系统中，同时，连入网络中的计算机数量也在成倍增加，这些都使得信息安全问题日益严重。入侵检测已经成为网络安全的一个重要的研究领域。 入侵(Intrusion)是指系统的未经授权用户试图或已经窃取了系统的访问权限，以及系统的被授权用户超越或滥用了系统所授予的访问权限，而威胁或危害了网络系统资源的完整性、机密性或有效性的行为集合[1]。其中，完整性是指防止网络系统资源被非法删改或破坏；机密性是指防止网络系统内部信息的非法泄露；有效性是指网络资源可以被授权用户随时正常访问和程序资源能够按期望的方式正常地运行。入侵检测就是检测入侵活动，并采取对抗措施。入侵检测主要有两种：滥用检测和异常检测。 滥用检测（Misuse Detection）是假定所有入侵行为和手段（及其变种）都能够表达为一种模式或特征，那么所有已知的入侵方法都可以用匹配的方法发现。滥用检测的关键是如何表达入侵的模式，把真正的入侵和正常行为区分开来。滥用检测的优点是可以有针对性地建立高效的入侵检测系统，

其主要缺陷是不能检测未知的入侵，也不能检测已知入侵的变种，因此可能发生漏报。 异常检测(Anomaly Detection)[2]是假定所有入侵行为都是与正常行为不同的。异常检测需要建立目标系统及其用户的正常活动模型，然后基于这个模型对系统和用户的实际活动进行审计，以判定用户的行为是否对系统构成威胁。常用的异常检测方法有：专家系统、神经网络、机器学习、和人工免疫等。异常检测的关键问题是：① 特征量的选择。异常检测首先是要建立系统或用户的“ 正常 ”行为特征轮廓，这就要求在建立正常模型时，选取的特征量既要能准确地体现系统或用户的行为特征，又能使模型最优化，即以最少的特征量就能涵盖系统或用户的行为特征。②参考阈值的选定。因为在实际的网络环境下，入侵行为和异常行为往往不是一对一的等价关系，这样的情况是经常会有的：某一行为是异常行为，而它并不是入侵行为。同样存在某一行为是入侵行为，而它却并不是异常行为的情况。这样就会导致检测结果的虚警和漏警的产生。由于异常检测是先建立正常的特征轮廓作为比较的参考基准，这个参考基准即参考阈值的选定是非常关键的，阈值定的过大，那漏警率会很高；阈值定的过小，则虚警率就会提高。合适的参考阈值的选定是影响这一检测方法准确率的至关重要的因素。入侵检测系统（Intusion Detection System，IDS）可以定义为识别针对计算机或网络资源的恶意企图和行为并对此做出反映的系统。 1.2 当前分布式入侵检测系统特点及存在的问题[3] 当前分布式系统的整体结构多为分级的多层次结构，见图1。 这是一种自顶向下的树状结构，由控制节点、数据聚合节点和数据搜集节点组成。位于树顶层的是控制节点，负

责控制整个系统以及提供接口与外界通信；处在中间层的是数据聚合节点，它接受来自上层的命令后对下层进行控制，分析来自下层的数据流并进行缩减后递交到上层；而底层的叶节点负责数据搜集功能，它既可以是网络中的某台主机，也可以是网络中的某个数据采集器。 这种系统架构的优点是显而易见的：它能很好的处理基于滥用和基于异常的入侵检测模型，从而保护网络的安全；并且能适应网络通信大小的需要，很方便地随时进行扩充和缩减从而达到它所监控的网络环境的最优化。 但是正因为它的分层结构也导致了它自身的不安全性。表现在两个方面：（1）在这种系统中，网络中有大量的数据传送将造成网络拥塞。（2）由于分层结构使得IDS极易受到攻击。攻击者通过攻击内部节点有可能切断某一控制分支，甚至破坏整个IDS。图1 层次架构的分布式入侵检测系统模型 