第 33 卷 第 4 期 计 算 机 工 程 2007 年 2 月
Vol.33 No.4 Computer Engineering February 2007
·安全技术· 文章编号：1000—3428(2007)04—0118—03 文献标识码：A 中图分类号：TP390

移动 Ad Hoc 网络入侵检测研究

杨 清[1,2]，李方敏[2]
(1. 武汉理工大学信息工程学院，武汉 430072；2. 湖南科技大学计算机科学与工程学院，湘潭 411201)

摘 要：介绍了移动 Ad Hoc 网络入侵检测技术的最新研究进展。提出了移动 Ad Hoc 网络的特点、安全目标及其脆弱性等，分析了 Ad Hoc 网络中存在的主要安全威胁和 Ad Hoc 网络中入侵检测系统结构，并对现有的几种典型 Ad Hoc 网络入侵检测方案进行了的分类论述，从决策方式、通信机制、检测模式和优缺点几个方面进行综合比较。对移动 Ad Hoc 中入侵检测技术的选择提出了建设性的建议，并指出了下一步的研究方向。

关键词：移动 Ad Hoc 网；入侵检测系统；自治系统；通信机制

Study on Intrusion Detection for Mobile Ad Hoc Network

YANG Qing[1,2], LI Fangmin[2]
(1. School of Information Engineering, Wuhan University of Technology, Wuhan 430072;
2. School of Computer Science & Engineering, Hunan University of Science and Technology, Xiangtan 411201)

【Abstract】 This paper introduces the developments of techniques for mobile Ad Hoc network. it introduces characteristics of mobile Ad Hoc network, objects of security and vulnerabilities and so on. It analyzes the primary threats in mobile Ad Hoc network and the structure of the intrusion detection system for mobile Ad Hoc network, also discusses present representative solutions for mobile ad hoc network, and makes a comparison on aspects of decision method, communication machine, detection model, merits and faults. It makes some constructive suggestions on selection of intrusion detection techniques in the mobile Ad Hoc network, also presents the area of the further research in the future.

【Key words】 Mobile Ad Hoc network; Intrusion detection system (IDS); Autonomy system; Communication mechanism

1 概述

随着移动 Ad Hoc 网络的广泛应用，由于 MANET 的自组织性和移动性，安全问题正成为人们普遍关注的问题，也成为了它应用的瓶颈，因此入侵检测方法的研究显得尤为重要，但是它的研究还刚刚起步。

1.1 移动 Ad Hoc 网络

MANET 是一种新型的无线移动通信网络，它是由一组带有无线收发装置的动态节点组成的一个多跳的临时性自治系统，节点不依赖于任何固定的基础设施和管理中心，节点同时具备主机和路由器两种功能。MANET 的独特结构产生了一些突出的特点：自组织性，动态的拓扑结构，有限的资源，多跳的通信，脆弱的网络安全和存在单向的无线信道等。节点的无线通信范围是有限的，在此范围内的节点可以直接通信，对在无线通信范围外的节点，则需要中间节点充当路由器对数据包进行转发。其主要用于军事战术通信、应急通信、协同移动通信、无线接入系统和传感器。

1.2 MANET 安全目标

安全的自组网应该具有如下的特点：

(1)可用性：保证在拒绝服务攻击下，网络依然可用；(2)机密性：保证特定的信息不会泄漏给未授权的节点；(3)完整性：保证传输中的消息没有被破坏过；(4)有鉴别能力：保证一个节点能够识别正在与它通信的节点的身份；(5)不可抵赖性：保证发送源不能否认它所发出的消息。

1.3 MANET 脆弱性

信道的弱点：由于使用的是无线连接，因此自组网络容易受到从被动监听到主动扮演、消息重放、消息扭曲等各种攻击。监听使得敌人可以接触到机密的信息，有悖于机密性原则。主动攻击使得敌人能够删除消息、注入错误消息、修改消息、甚至伪装成一个合法的节点。

节点的弱点：因为移动节点是自主移动的，特别是漫游在敌对环境中的节点，缺乏相应的物理保护，其被敌人俘获的机率是不可忽略的。所以，不仅要考虑网络外部的恶意攻击，还需要考虑由网络内部被俘获节点发起的攻击。

动态变化的拓扑结构：由于拓扑结构和成员的不断变化，因此成员间的信任关系也是在不断变化的。任何静态配置的安全方案都是不适用的，自组网的安全机制必须能够适应这种动态的变化。

安全机制：在传统的公钥密码体制中，用户采用加密、数字签名、报文鉴别码等技术来实现信息的机密性、完整性、不可抵赖性等安全服务。然而它需要认证中心来提供密钥管理服务。但在移动 Ad Hoc 网络中不存在单一的认证中心。

路由协议[2]：路由协议的实现也是一个安全的弱点，路由算法都假定网络中所有节点是相互合作的，共同去完成网络信息的传递。如果某些节点为节省本身的资源而停止转发数据，这就会影响整个网络性能。更可怕的是参与到网络中的攻击者专门广播假的路由信息，或故意散布大量的无用数据包，从而导致整个网络的崩溃。

基金项目：湖南省自然科学基金资助项目(06JJ50132)
作者简介：杨 清(1969－)，男，副教授、博士，主研方向：计算机网络和机器学习；李方敏，教授、博导
收稿日期：2006-03-09 **E-mail**：gyang081@163.com

2 MANET 入侵检测系统

2.1 攻击类型

由于MANET本身特点和特殊的工作模式，MANET网络的安全威胁是复杂、多样的，因此对攻击行为的分析显得至关重要。攻击行为可以按多种方式进行分类[3]。

按攻击性质可分为：被动攻击。共享的开放信道易被窃听，攻击者不发送任何消息，不破坏协议的操作，仅企图发现有价值的信息；主动攻击。入侵者主动破坏网络协议、违反安全策略。按攻击来源可分为：外部攻击，指没有获得 CA 认证的网络外节点对网络的攻击；内部攻击，指来自于内部节点的攻击，其威胁远大于外部攻击。

按所攻击对象可分为：对主机的攻击，类似于有线网络对主机的攻击；对网络的攻击，路由协议是 MANET 的核心协议，安全的路由要求消息的可用性、完整性、保密性、不可否认性。

按不同协议层次分为：MAC 层，传输层，网络层和应用层攻击。对数据链路层、物理层协议的攻击手法比较简单。但对路由层协议的攻击却是异常复杂，攻击者常使用下述手法进行多种多样的攻击：(1)修改，攻击者修改经过它的路由控制消息或数据分组；(2)模仿，攻击者使用其他节点的ＭＡＣ地址或 IP 地址向网络发射消息；(3)伪造，攻击者生成假的路由消息并向网络发送。对网络层协议的攻击是对 MANET 网络安全的最大威胁。攻击类型如图 1 所示。

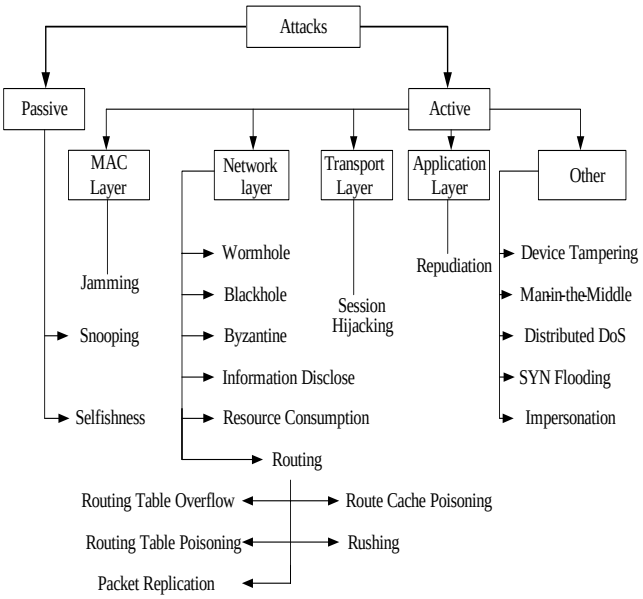

图 1 入侵攻击类型

2.2 IDS 体系结构

(1)孤立IDS。在这种体系结构中，每个主机都有IDS，且它们独立检测攻击，节点之间不通过相互协作，所有的决定都是依靠本地节点。这种体系结构虽然不是很有效，但它能应用在不是所有节点都能运行IDS的环境中[1]。

(2)分布式协作 IDS。在这种体系结构中，每个节点有一个 IDS Agent 并作本地检测。同时，所有节点参与全局的入侵检测，这种结构更适合于平面的 MANET 网络。

(3)层次 IDS。该结构适合于多层 MANET 系统。在多层 MANET 系统中，族头节点为该族所有节点集中提供路由和支持安全措施，包括 IDS。另外，CH 节点也检测来自拜占庭节点对虚拟骨干网络的攻击，这在 MANET 中尤为重要。

3 入侵检测技术及比较

3.1 典型 IDS 技术方案

方案 1 Yongguan Zhang等提出了基于Agent的适合MANET分布式特性的检测方案[2,4]。

在该方案中 IDS Agent 运行于网络中每一个节点上，拥有 6 大功能模块，如图 2 所示。

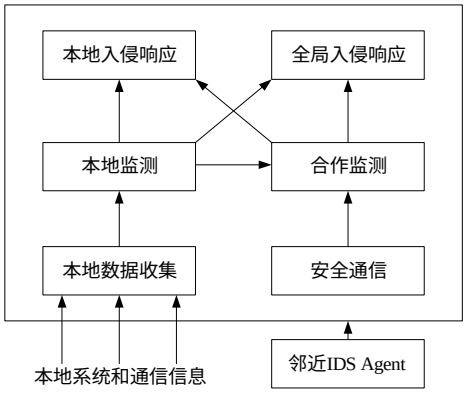

图 2 IDS Agent 的组成

其过程为首先执行本地数据收集和检测，然后本地节点能够激发多节点的协作检测，进一步判断是否发生了入侵。

这种适合于 MANET 分布式特性的 IDS 体系结构更适合平面 MANET 的网络，但在较大的多层 MANET 中也可分步运行。同时，该方案运行在多审计日志环境中，如果入侵检测系统需要新的审计数据，它只需在 IDS Agent 中加入更多的数据收集模块。

该方案的优势有两点：(1)提出了分布式协作入侵检测的架构，利用分布在每个节点的 IDS Agent 独立完成本地检测，合作完成全局检测，适合于移动 Ad Hoc 网络自组织的特点，(2)采用多层综合入侵检测，提高了检测效率。

缺点也有两点：(1)采用异常检测模式，要事先采样数据进行训练，不适合于移动 Ad Hoc 网络多变的应用场合。(2)每个节点都运行于 Agent，占用过多的资源。

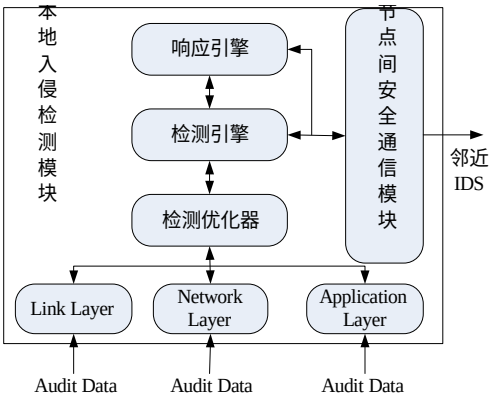

图 3 混合入侵检测系统

方案 2 Oleg Kachirski和Ratan Guha提出了基于移动Agent的入侵检测方案[1,5]。他们认为Yongguan Zhang的方案每个节点都有Agent，过于占用网络资源，为了节省资源，只是在某些节点上驻留有监视网络的Agent，并且Agent的数量可按要求进行增减。提出了一个在多种审计数据下运行的IDS结构。这种结构具有较好的扩展性，如果IDS需要在新的审计日志下工作，只要合并另外的监控新的审计日志Agent。但是，这种结构IDS的性能还没有人通过实验来证实。

方案 3 由Huang and Lee+ 2003 年提出[6]。该方式将入侵检测限定在某一些节点来使IDS有限地使用资源，从而提高MANET IDS的有效性。它的实现证明了该方法能达到较为满意的检测率。这种结构也被应用于安全需求中等而有效性要求高的网络环境中。同样，这种方法也很容易被扩展到多层MANET系统中。

方案 4 Chin Yang Tseng等提出了基于规范入侵检测方案[1,7]。该方案利用分布在网络中的监测点，合作监视在AODV路由查询过程中，被监视节点是否按路由规范进行操作，如果发现不一致则报。该方案优点在于采用了基于规范入侵检测，既不需要事先提取入侵行为特征，也不需要数据进行训练，有较高的检测率和较低的误报率。缺点为，由于

该方案中没有通常的本地检测机制，但由于数据包在每一跳都要检测，占用节点较多的计算资源，它的效率较低。并且它的有效性也未用实验进行验证。

方案 5 Sun, Wu and Pooch 于 2003 年建议[8]，在仿真测试显示该方法极大地提高了检测率，降低了误检率，这是MANET中IDS的主要性能指示器。但是在该系统运行时，实验没有给出该方法所需要的各项数据指标 :如需要多少资源，CPU的运行时间，网络带宽等。因为该系统中用于入侵检测的节点间的通信协议和区域建立算法都较为复杂，所以该方法需要较大数量的资源。该结构中没有用移动Agent，有像族头一样的网关节点。能被用于IDS性能要求和安全要求较高的MANET中，且MANET中的资源普遍能用。

方案 6 Guha and Schwartz于 2002 年自动地构造异常检测模型[9]，但它具有较高的计算开销。

方案 7 Huang, Lee and Yu [10]提出了一种基于丢包和路由表异常变化的入侵检测方案，具有较低的费用，但该设计只适合于一种路由协议，但应用于其他的路由协议时，必须进行修改。

方案 8 Albers and Camp 于 2003 年利用 Agent 提供了一种可伸缩的体系结构，如果 IDS 需要更多的功能，它只需合并更多的新任务移动 Agent。同时它也能减少 IDS 网络流量。但是该结构很大程度上是依赖 Agent 的使用，Agent 的创建和管理以及 Agent 之间通信和协作大大地增加了网络的开销，也加大了计算的复杂性。该结构的有效性有待进一步证实。

方案 9 Rajavar和Shah建议的基于网络信息的入侵检测系统。由于在每一跳都要检测数据包，因此检测的效率较低，且造成资源浪费[12]。

方案 10 Pttini和Percher提出的基于MIB的一种有效的、高可伸缩性的分布式结构，能在多级检测攻击，但存在与Agent相关的安全、计算开销和管理问题[13]。

3.2 方案比较

表 1 为不同入侵检测方案的比较。

表 1 不同入侵检测方案的比较

比较内容 / 协议名称	系统输入数据	检测模式	决策方式	通信机制	优　点	缺　点
方案 1 (Zhang and Lee, 2003)	Audit Data on Local Nodes	异常检测	协作	Network message	各 Agent 合作响应，能适应不同审计日志	对拜占庭节点脆弱，占用资源较多
方案 2 (Kachirski and Guhua,2002)	Network Packet, Program level Audit Data	异常检测	独立	Mobile Agent	具有较好的扩展性和灵活性；大多数节点保存资源	MA 的安全是最大的难题，协议复杂
方案 3 (Huang and Lee, 2003)	Numbers of the Packets and Route Control Message	异常检测	独立	Network message	能动态调整 Agent 的数量，提高网络资源和 CPU 的效率	需组织被泄露的节点作为族头，没提及误警率
方案 4 (Tseng and Balasubra, 2003)		基于规范的检测		Network message	不需要训练数据，较低的管理费用	基于一种路由协议设计，通用性差
方案 5 (Sun, Wu and Pooch 2003)	Data of the Routing Table	异常检测	分布协作	Network message	较低的误警率，能合并多检测技术	复杂结构需要多协议合并，建区计算复杂，
方案 6 (Guha and Schwartz 2002)	Packet Information	误用检测	分布协作	Mobile Agent	考虑了 MANET 的分布式特性，较好的带宽意识	MA 的安全性问题，丢包率较高
方案 7 (Huang, Lee and Yu, 2003)	Packet Statistics(Packet Dropped and Change in Routing Tables)	异常检测			能自动地构造异常检测模型	较高的计算开销
方案 8 (Albers and Camp, 2003)	Audit Data in MIB		独立	Mobile Agent	伸缩性强，较小的网络流量	创建和管理 MA 较为复杂
方案 9 (Rajavar and Shah, 2003)			分布协作	Network message	不同于传统的本地入侵检测机制	Packet 需在每一跳检测，效率较低
方案 10 (Pttini and Percher, 2003)	MIB		分布协作	Mobile Agent	分布性和伸缩性，能检测多级入侵	只适合于 MA，存在安全、计算花费和管理问题

4 结论及研究展望

本文从分析 Ad Hoc 网络的特点着手，介绍了移动 Ad Hoc 网络入侵检测的几种体系结构和协议，并对目前提出的几种入侵检测方案进行详细的综合和讨论，总结出了它们的应用条件和各自的特点。同时也对它们存在的问题进行了分析，为 Ad Hoc 网络中入侵检测技术的进一步研究提供较好的依据。

总的来说，移动 Ad Hoc 网络入侵检测技术的研究包括以下几个方面：

(1)根据移动 Ad Hoc 网络独自的特点，设计一个更适合具有自组织和移动特性的无线网络的 IDS 体系结构是 MANET IDS 研究的一个重要方向。

(2)由于 MANET 中审记日志的部分性和局部性的特点，

(下转第 124 页)