Ad Hoc 网络与有线网络互连中的入侵检测①

刘尧华　刘卫国 (中南大学 信息科学与工程学院 湖南 长沙 410083)

摘　要： 针对 Ad Hoc 网络与有线网络互连中面临的安全问题，致力于建立一个适合两网互连的入侵检测系统，构建了 Ad Hoc 网络与有线网络的互连模型，并提出了适用于该互连模型的入侵检测实施方案。该方案采用基于统计的异常检测技术和基于模式匹配的误用检测技术相结合的入侵检测技术，减少了单纯使用某种入侵检测技术时的漏报率和误报率，从而提高系统的安全性。

关键词： Ad Hoc 网络；网络安全；入侵检测

Intrusion Detection For the Interlinkage Between Ad Hoc Networks and Lineate Networks

LIU Yao-Hua, LIU Wei-Guo

(School of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: In this paper, the security issues in the interlinkage between Ad Hoc networks and lineate networks are investigated. An intrusion detection system for the interlinkage between two networks is established and a model which can realize the interlinkage between Ad Hoc and lineate networks is presented. This scheme is based on combination of misuse detection and anomaly detection. It combines the two technologies to reduce the false positive rate and the false negative rate in only one detection technology, and then security of intrusion detection system is improved.

Keywords: Ad Hoc network; network security; intrusion detection

Ad Hoc 网络既可以作为一个独立的自组织网络，又可以作为一个子网接入到有线网络中，并且 Ad Hoc 网络只有与其他网络实现互连互通才能真正发挥网络的潜能。随着 Ad Hoc 网络的应用范围不断扩大，这种需求将越来越多。但是，由于两类网络的互连增加了网络的复杂性，对系统的安全也提出了更高的要求，别有用心的攻击者除了可以通过无线方式入侵外，还可通过有线网络来实现对 Ad Hoc 网络的攻击。因此，入侵检测在这样复杂的网络环境中显得尤为必要。同时，在两网互连的应用中，IDS(Intrusion Detection System)要面对来自于有线和无线两方面的分组数据，数据源的复杂性对检测系统的能力也有了更高的要求，需要采用更为完善的检测方案来保证系统的准确高效[1]。

本文首先介绍了一种利用互联网关构建 Ad Hoc 网络与有线网络互连互通的实验模型，然后针对该互连模型，提出采用混合检测技术的入侵检测方案，以确保两网互连的安全可靠。

1　互连模型的建立

1.1 互联网关

Ad Hoc 网络与有线网络的互连可以通过一个特定网关来实现[2]。作为两类网络互连的枢纽，网关的作用十分重要，具有三个方面的功能：一是地址映射。当 Ad Hoc 网络节点需要访问有线网络中的节点或者有线网络的节点试图访问 Ad Hoc 网络内部节点时，需要将 Ad Hoc 网络的内部地址映射为标准的 IP 地址，便于有线网络中路由器进行路由寻址和返回数据分组。二是协议转换。当一个 Ad Hoc 网络节点想要发送数据到有线网络节点时，它首先必须将数据发送

① 基金项目:国家自然科学基金(60773013);湖南省自然科学基金(07JJ5078)
收稿时间:2009-09-18;收到修改稿时间:2009-10-19

到网关。由于 Ad Hoc 网络路由协议不同于有线网络路由协议，且所采用的分组格式不同于标准的 IP 分组，因此在跨网通信时，网关必须对通过的分组进行分析，根据要到达网络的协议类型进行分组的重组，实现协议转换功能。三是分组转发。当通过网关的分组经过地址映射和协议转换以后，网关必须将该分组在相应端口中转发出去，最终实现两类网络的互联互通。

1.2 构建实验模型

为了便于入侵检测系统的设计，有必要模拟 Ad Hoc 网络和有线网络互联的应用环境，建立一个演示实验系统，该系统的拓扑结构如图 1 所示。

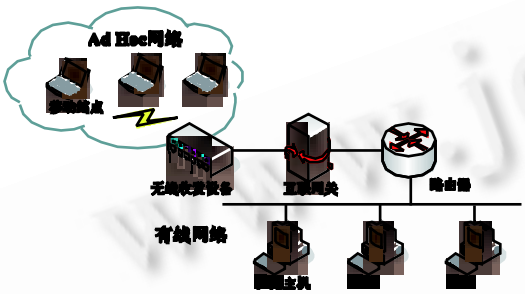

图 1 Ad hoc 网络与有线网络互联演示拓扑图

实验环境中的互联网关采用一台具有 RS232 接口和以太网接口的固定主机，而 Ad Hoc 节点均为移动 PC，有线网络部分则由实验室内部的一个连接到路由器上的小型的局域网模拟。

2 互连模型中的入侵检测系统设计

在设计入侵检测系统时，不能完全照搬有线网络通用 IDS 模型，必须考虑到两网互联环境与单纯的有线网络的区别。一是 Ad Hoc 网络与有线网络互联，增加了网络结构的复杂性和数据来源的多样性，使得攻击样式难以预测，这就要求所设计的 IDS 能够较好地检测未知的攻击行为；二是在构建的实验模型中，互连网关不仅担负协议转换、地址映射等工作，而且是整个互联网络的关键位置。基于互连网关的重要性，需要 IDS 具有高度的可靠性，较低的误报率和漏报率，确保互联网关的安全可靠；三是在两网互联的环境中，攻击者既可利用有线网络对 Ad Hoc 网络发起攻击，也可利用 Ad Hoc 网络对有线网络的主机进行攻击，并且 Ad Hoc 网络具有动态的拓扑结构，各节点可以灵活游走，发现、定位、追踪攻击行为比较困难[3]，对检测系统的性能要求比较高；四是移动 Ad Hoc 网络缺乏足够的物理保护、节点采用分布式协作、节点的带宽和计算能力有限等特征[4]，使得这种网络非常脆弱，节点自身检测能力比较差，对互联网关的检测能力的依赖比较大。

基于以上考虑，本文提出了一个同时采用误用检测技术和异常检测技术的混合入侵检测系统。该入侵检测系统主要由数据获取模块、检测分析模块、入侵响应模块三个部分组成。其结构图如图 2 所示。

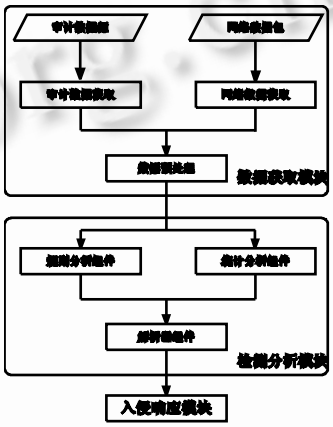

图 2 IDS 的系统结构

2.1 数据获取模块

在互连网络中，需要收集的数据源包括主机审计数据和网络数据包，它们获取的方法各不相同。

(1) 主机审计数据的获取

不同的系统环境下所收集到的审计数据类型有所区别，主要分为以下 4 个典型类型：文件访问、系统访问、资源消耗、进程调用。

(2) 网络数据包的获取

网络数据包既包括有线网络的数据包，也包括 Ad Hoc 节点与有线网络节点之间通信的数据包。一般主机的网卡只接收属于本机 MAC 地址的数据，为截获流经网卡的不属于自己主机的数据，必须绕过系统正常工作的处理机制，直接访问网络底层，首先将网卡工作模式设置为混杂模式，使之可以接收目标 MAC 地址不属于本机 MAC 地址的数据包，然后直接访问数据链路层，获取相关数据，这样便能截获到流经网卡的所有数据。

(3) 数据的预处理

在收集到数据后，为确保检测系统的有效识别及

正确检测，需要对数据进行预处理，通过过滤、映射、格式转换等操作，使所获取的数据符合检测系统的要求。

2.2 检测分析模块

在 Ad Hoc 网络与有线网络互连的模型中，由于网络结构复杂，同时具有多种数据源，应采用基于规则分析和统计分析相结合的混合型入侵检测技术。检测分析模块安装具有规则分析组件和统计分析组件的混合检测系统，这两类组件独立并行工作，共享相同的数据源，生成不同的分析报告，然后由解析器组件合并分析这两个组件的输出结果。

(1) 规则分析组件

每一个基于规则分析的入检测方法都需要一个既定的入侵模式。这就需要一种对入侵行为的描述方法。现在的各种入侵检测系统中的描述方法各不相同，每个厂商定义自己的描述方法，每种方法各有长短。在网关处的检测系统中，可以采用 Snort 的入侵行为描述方法。这种描述方法简单、易于实现，能够描述绝大多数的入侵行为，并且具有较快的检测速度[5]。

(2) 统计分析组件

统计分析组件主要采用行为建模分析算法，这个算法属于异常入侵检测算法的派生算法。其基本思想为：把正常的用户行为分为很多类，例如 CPU 的使用情况、I/O 使用情况、文件操作、一段时间内登录失败次数等，统计各种行为的发生概率，根据最近的行为分布得出正常行为的标准，当所观测的行为如果与所期望该主体的行为偏离显著时，就被标识为潜在的入侵行为[6]。

检测算法评价整个使用行为模式，而不是仅考虑主体行为的单个测量值的情况。系统实现时首先定义用户行为，然后对它进行记录。一般采用统计值 T^2 对多个测量值异常度进行综合评价。

假设 IDS 有 n 个代表用户行为是否正常的评估值，这些单个评估值表示为 S_i，$1 \leqslant i \leqslant n$。$A_i$ 为权重，其值可根据以往经验预先设定。

统计值 T^2 定义为：

$$T^2 = A_1S_1^2 + A_2S_2^2 + \cdots + A_nS_n^2$$

T^2 代表对某个用户最近时间内所有行为的评估值。

通过计算 T^2 值的大小来确定是否有异常行为发生，当 T^2 偏离系统设定的正常值较多时，将指示有异常行为，输出报警信号。

(3) 解析器组件

解析器组件负责综合由基于规则分析组件和统计分析组件所各自发出的警报信号，并报告取出冗余后的警报信号。根据预先设定的误报率及漏报率阈值，启动数据更新模块，使检测模块能够及时适应网络环境的变化。

如定义规则分析组件的漏报率阈值为 u，统计分析组件的误报率阈值为 v，规则分析组件的漏报事件数为 i，统计分析组件的误报事件数 j，总的报警事件数为 m，则算法处理过程可表述为：

① 系统初始化。构建常见入侵行为的特征数据库；将系统处于安全环境，建立正常的行为模板。

② 令 i，j，m 均为 0。

③ 令 m=m+1。如规则分析组件检测到攻击行为，则启动自动响应策略；如规则分析组件未检测到攻击行为，但统计分析组件检测到攻击行为，则将报警信号输出到控制台，交由管理员判断。如为误报则 j=j+1，否则 i=i+1。

④ 如 j/m>v，则行为建模引擎将重新进入学习阶段，重新建立与当前网络环境相适应的正常的行为模板，转②；如 i/m>u，则解析器将未检测到的攻击场景总结成攻击模式插入规则分析引擎的特征数据库中，转②。

⑤ 启动入侵响应,并转③。

2.3 入侵响应模块

响应是一个入侵检测系统必须的一部分，如果没有它，入侵检测就失去了存在的价值。入侵响应根据攻击的类型、网络协议的类型以及证据的可信度的不同而不同，最简单的响应是自动通知。当检测到入侵发生时，入侵检测系统可以给管理员发 E-mail 或发告警信息。根据攻击情况还可以采用撤销 TCP 连接、攻击回避、隔离保护、复位连接、反击攻击者等自动响应策略。另外，在两网互联的环境中，考虑 Ad Hoc 网络的特殊性，入侵响应策略还包括将可疑节点列入“黑名单”、隔离可疑节点、停止与之通讯等操作[7]。

3 实验及结果

实验模型采用本文前面介绍的互联模型，网络仿真平台是 NS2。仿真中，Ad Hoc 网络的 MAC 层使用 802.11 协议，节点运动范围 200m×200m，节点传

输半径为 200m, 链路带宽为 2Mbps。运动方式采用随机运动模型，即每个节点在该区域内从一点向另一点运动，运动速度在零到最大速度之间随机选取，到达目标点后，停留一段时间，然后随机选择一个新的目标点和一个新的速度，向新的目标点运动，依此类推，直至仿真结束。检测过程中使用了 5 组数据，每组数据包含 1000~8000 个预处理过的记录。在评估入侵检测模型时，统计被正确检测到的攻击行为数量和被错误判定为攻击行为的正常行为的数量，然后计算出检测率和误报率。经过实验，该检测模型的检测率可以达 90%，误报率始终低于 5.9%，属于可以容忍的范围。由于系统能够根据网络运行状态进行自我调节，随着测试数据增加，检测的准确性也越来越高。

表 1 各次仿真实验检测结果

测试记录数	检测率(%)	误报率(%)
1000	90.90	5.90
2000	90.00	5.81
3500	90.62	5.68
5000	91.12	5.54
8000	91.41	5.52

4 结语

随着 Ad Hoc 网络与有线网络互联的广泛应用，其安全性问题将受到越来越多的关注。本文在总结前人研究成果的基础上，设计了一种混合异常检测和误用检测技术的入侵检测方案。由于两种检测技术各有优缺点：基于统计分析的异常检测技术可以检测未知的攻击但误报率高，而基于规则分析的误用检测技术检测准确性高，但不够灵活，不能检测到未知的攻击模式。所以将这两种方法结合起来可以互补，能够提高系统的检测性能。另外，本文提出的入侵检测方案可以利用入侵数据以及审计数据自动更新检测模块，进一步提高了系统的可靠性，能够适应 Ad Hoc 网络与有线网络互联的复杂环境。

参考文献

1 林亚卓,唐陈峰. Ad Hoc 网络的入侵检测技术研究. 通信技术, 2008,41(1):99－101.

2 董慧,柴乔林.具备 Internet 接入功能 Ad Hoc 互联网关设计.华中科技大学学报(自然科学版), 2003,31(10):92－94.

3 Zhou LD, Hass ZJ. Securing Ad Hoc networks.IEEE Nerworks Special Issue on Network Security, 1999, 7(6):24－30.

4 杨黎斌,慕德俊,蔡晓妍.无线传感器网络入侵检测研究.计算机应用研究, 2008,25(11):3204－3208.

5 高平利,任金昌.基于 Snort 入侵检测系统的分析与实现.计算机应用与软件, 2006,23(8):134－138.

6 蒋盛益,姜灵敏.一种高效异常检测方法.计算机工程, 2007,33(7):166－168.

7 顾春媛,易平,蒋兴浩,等.移动 Ad Hoc 网络的入侵响应模型.微计算机信息, 2008,24(6):25－27.