针对无线网络的入侵检测系统设计方法研究

林海涛

(海军工程大学 电子工程学院,湖北 武汉 430033)

摘 要：从实际应用出发,提出了一种针对无线网络的入侵检测方法,给出了入侵检测系统的设计方案,扩展了系统管理员的安全管理能力(包括安全审计、监视、攻击识别和响应),具有较强的经济效益和借鉴意义。

关键词：无线网络;入侵检测;传输协议;体系结构

中图分类号：TN911.32 **文献标识码**：A **文章编号**：1674-7720(2010)19-0047-04

An approach to design intrusion detection system applied in wireless network

LIN Hai Tao

(College of Electronic Engineering, Naval University of Engineering, Wuhan 430033, China)

Abstract: This paper puts forward a new scheme about how to design intrusion detection system objected to wireless network. The results show that this system is advantageous and guidable, which can greatly help enterprise and government to guard against network attach, extend the ability of network administrator in audit, surveillance, recognition.

Key words: wireless network; IDS; transfer protocol; architecture

随着笔记本电脑、个人数字代理(PDA)以及3G通信等技术的发展,人们使用信息技术进行通信联系和交流的空间、灵活性得到不断拓展。无线网络尤其是3G网络成为技术发展和社会应用的新宠。各种类型的移动数据终端以及多媒体终端得到广泛应用,促使传统网络由有线向无线、由固定向移动、由单一业务向多媒体的发展。然而,这种扩展给用户带来了更大的自由度的同时,也带来了安全上的挑战。由于无线信道的开放性和移动设备在存储能力、计算能力和供电方面的局限性,无线网络面临着更复杂的安全威胁和隐患[1]。如何构造一个安全可靠的无线局域网已经成为一个迫切需要解决的问题。

1 IDS基本原理

入侵检测系统(IDS)是一种主动保护自己免受攻击的网络安全系统。入侵检测系统对网络行为进行实时检测,可以记录和阻止某些网络行为,被认为是防火墙之后的第二道安全闸门,可与防火墙配合工作[2]。

IDS扫描当前网络的活动,监视和记录网络的流量,根据定义好的规则来过滤经主机网卡的流量,并提供实时报警。入侵检测系统至少应包括3个功能模块:提供事件记录流的信息源、发现入侵迹象的分析引擎和基于分析引擎的响应部件。公共入侵检测框架CIDF阐述了一个入侵检测系统的通用模型,即入侵检测系统的四个组件:事件产生器、事件分析器、响应单元和事件数据库,共通用模型如图1所示。CIDF将需要分析的数据统称为事件。

2 无线网络入侵检测系统架构

2.1 入侵检测体系结构

目前比较成熟的入侵检测方法是异常检测和误用检测两种类型[3]。异常检测是根据使用者的行为或资源使用状况的正常程度来判断是否入侵。异常检测与系统相对无关,通用性较强,其主要缺陷是误检率较高。误用检测有时也称为特征分析或基于知识的检测,根据已定义的入侵模式,判断在实际的安全审计数据中是否出现这些入侵模式,这种检测准确度较高,检测结果有明确的参照性,便于决策响应,缺陷是无法检测未知的攻击类型。无线网络的IDS系统,必须考虑两者的互补性结合使用,如图2所示。

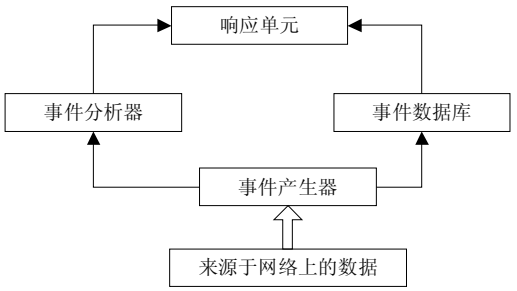

图 1 入侵检测通用模型 CIDF

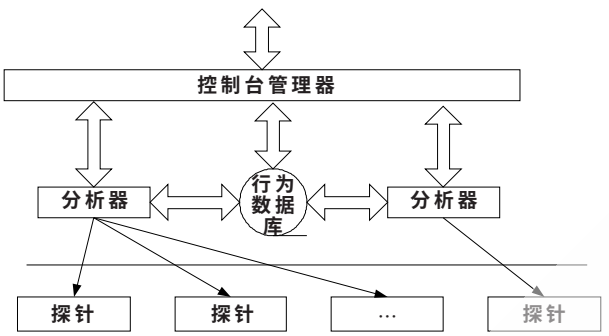

图 2 无线局域网入侵检测架构

信息获取和预处理层主要由主机探头(HSensor)和网络探头(NSensor)组成。综合分析决策层包含分析器(AnalysisSvr)和数据库(DB),在获取数据进行预处理后,进一步详细分析和最后的决策融合,从而制订响应策略和方式。控制管理层则是进行人机交互、控制管理、报警融合以及态势分析。

2.2 入侵单元检测模型

为满足无线网络的需要,入侵检测与响应系统应采用分布式结构,且协同工作。网络中的每个节点都参与入侵检测与响应,每个节点检测本地入侵,邻近节点进行协作检测[4]。在系统的每个节点都有独立的入侵检测单元,每个单元能够独立运行,监测本地行为(包括用户和系统的行为、节点间的通信行为),检测来自本地的入侵,并发起响应。这些入侵检测单元共同组成无线网络的入侵检测系统,如图 3 所示。

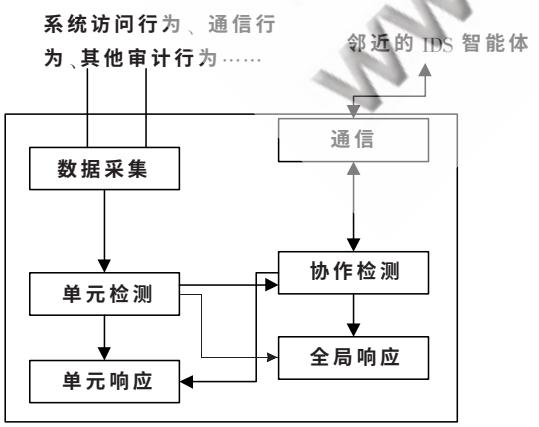

图 3 入侵检测单元模型

数据采集模块采集实时审计数据,这些数据包含系统和用户在节点内部的操作行为、通过该节点的通信行为以及在通信范围内、通过该节点可观察到的其他通信行为。协作检测模块的作用是传送邻近节点之间的入侵检测状态信息,利用最近接收到的其他节点的状态信息,计算出本节点的入侵检测状态[5]。协作检测的步骤如图 4 所示。

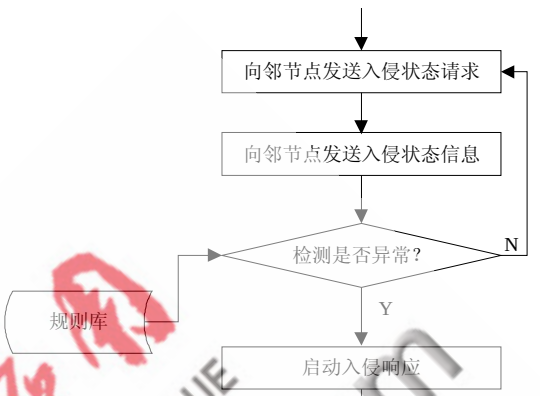

图 4 入侵检测流程图

2.3 分析器概念模型与系统部署

分析器概念模型如图 5 所示。首先获取来自主机探头和网络探头的数据信息,然后采用特征检测、异常检测、统计分析、拒绝服务检测等多种方法进行并行分析,把分析的结果采用特定的融合算法进行融合,从而得出分析结果。分析结果一方面通知控制管理层,另一方面通知响应决策部分,驱动响应决策,并进行物理定位。

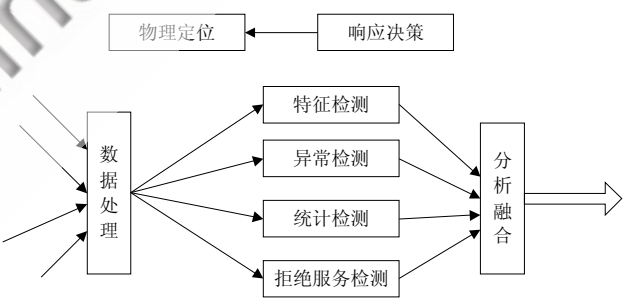

图 5 分析器概念模型

IDS 系统部署时,主机探头安装在客户端操作系统上,而网络探头则根据其地理环境情况适当布置,分析机尽可能地放在用户内部网络,降低分析机的风险,系统应该部署在电磁波干扰小的地方,避免由于辐射信号不稳定而带来的影响。

3 无线网络入侵检测系统核心模块实现

分布式入侵检测系统分为 3 个部件,(1)探测器。对应信息采集和预警层,下设探头和数据采集模块;(2)分析器对应综合分析决策层,下设协议解码模块、预处理模块和检测分析模块;(3)控制管理器。对应控制管理层,下设规则解析模块、日志模块和响应报警模块。本文

将重点介绍数据预处理、数据检测与分析和规则解析三个模块。

3.1 数据预处理模块

预处理模块对得到的数据包进行预处理，一方面可发现入侵信息，另一方面为检测分析模块做最后的准备。预处理模块采用了插件技术，可以很方便地增加功能，使系统具有可扩展性。与预处理相关的函数以链表的形式存在于动态链接库中，如图 6 所示。

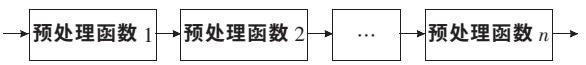

图 6 数据预处理模块处理过程

预处理函数是由控制管理器来配置的。控制中心将配置规则和预处理函数一起传送到各检测引擎，检测引擎在进行规则解析时，自行识别预处理指令，并作相应的处理。在 IP 报文的首部包含了分片和重组的信息，如图 7 所示。

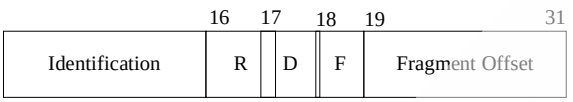

图 7 IP 包(32 位)格式

(1)Identification：唯一标识发送端的一个 IP 报文，如果需要分片，则所有分片具有相同的标识，这样目标主机便能够根据源主机的 IP 地址以及该标识来组合报文；(2)R：保留未用；(3)D："不分片"位，置为 1，则 IP 层不将数据报分片，只有为 0 时才允许分片；(4)F："更多分片"位，为 1 表示后面还有数据报的更多分片，为 0 则表示这是数据报的最后一个分片；(5)Fragment Offset：分片偏移，指出该分片数据在原始数据报文(未分片前)相对于起点的位置，实际位置为偏移值乘以 8，如为 0 则表示这是分片后的第一个信息包，放在组合后分组的最前面。

IP 重组的函数中定义了每一个分片的结构为：

```
Struct IpFrag
{
  dint offset;  //IP 分片的偏移值
  int end;      //分片的最后字节
  int len;      //分片的长度
  u char mff;   //更多的分片标志
  unsigned char *ptr;  //指向分片包中的数据
  struct IpFrag *ipf next;  //链接的下一个分片
};
```

这些分片形成一个单向链表，表示一个尚未组装完的分片队列，它属于一个 IP 报文，而分片链表的头指针放在 IpHeader 结构中：

```
struct IpHeader
{
  struct IpFrag;                    //第一个 IP 分片
  int len;                          //报文长度
  struct timer list timer;          //定时器
  u_char Proto;                     //协议类型
  u_short Ip_ttl;                   //生存时间
  u_short id;                       //IP 标识
  struct in addr Ip-Src, Ip_Dst;    //IP 报文的源，目的 IP 地址
  struct IpHeader *next;            //下一个 IP 报文
};
```

IpHeader 描述还未收到全部分片报文结构，多个 IpHeader 构成的链表形成一个重装链表，等待其他分片到达后重装。

3.2 数据检测分析模块

检测分析模块对预处理模块提交的数据，运用匹配算法和规则库中的规则进行比较分析，从而判断是否有入侵行为。检测分析模块是检测引擎的核心，它将从数据采集模块传来的数据顺着规则链表与入侵规则进行比较，如果匹配成功，则说明检测到了入侵，同时产生报警。其流程如图 8 所示。

3.3 规则解析模块

规则解析模块将从控制中心传送过来的规则按照一定的数据结构存储在规则库中，作为对入侵行为进行判断分析的知识库。在该模块的设计中，本文采用动态

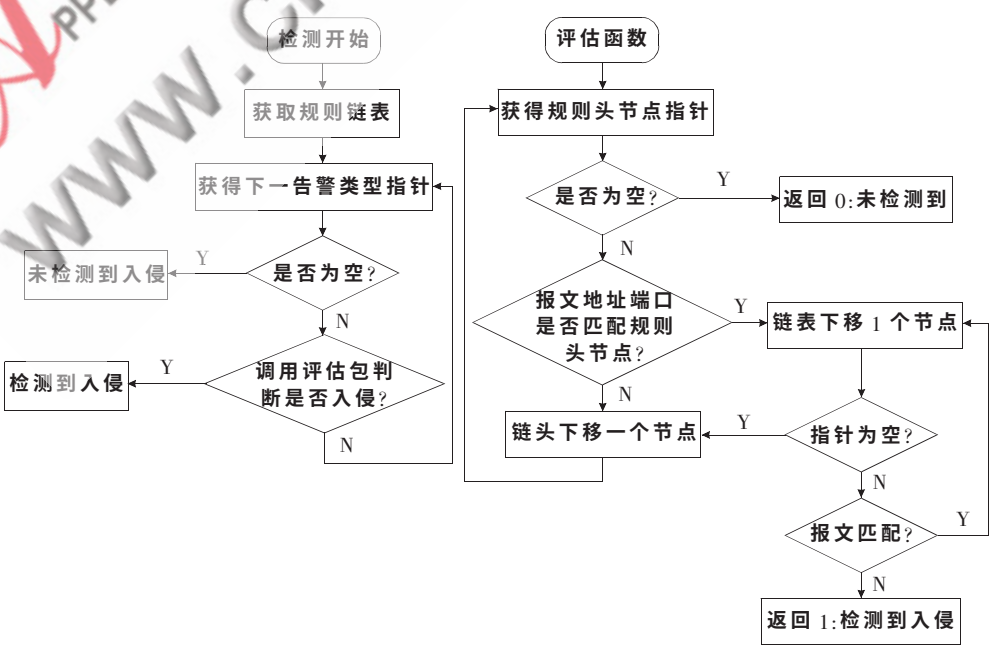

图 8 数据检测分析模块流程图

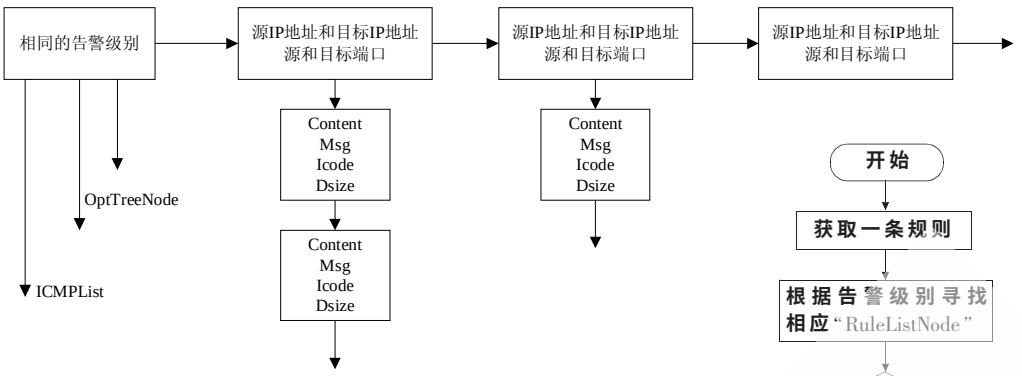

图 9 规则解表的结构

生成链表的方式构建规则的语法树，把所选择的规则存储在数据检测器所在的主机内存中，规则链表的结构如图 9 所示。

第一层是具有相同处理动作（Alert（警告），Log（记录），Pass(忽略)）的节点，以 RuleListNode 结构表示。其次，是在具有相同处理动作的基础上，按照不同的协议类型（IP，TCP，ICMP 和 UDP）再分成几条链表。而在每条链表中，具有相同源 IP 地址、目的 IP 地址、源端口和目的端口的规则头节点 RuleTreeNode 构成了结构图的第二层。以下的几层由具有相同源 IP 地址、目的 IP 地址、源端口和目的端口所对应的规则选项节点即 tTreeNode 组成。例如在一组规则中有 45 条检测 CGI-BIN 探测活动的规则，而它们都具有相同的源/目的 IP 地址及端口号，则它们在链表中可以将这些共同属性压缩到一个单独的 RuleTreeNode 节点中，而每个不同的属性（规则选项）保存在与 RuleTreeNode 节点相连的 OptTreeNode 节点中。这样的结构方式，将大大有助于提高检测速度。

建立规则链表的流程如下：首先读取规则文件，检查规则文件是否存在并可读，然后依次读取每一条规则，同时进行多行规则的整理；对规则进行解析，按类型进行分支处理，并用相应的规则语法表示，建立规则语法树；最后进行一些完善操作，如连接所有的动态规则，进行规则树的完整性检查。其中解释规则并将其添加到规则链表的流程如图 10 所示。

作为个人通信的一个重要的组成部分，无线局域网在现实及未来的社会生活中将得到广泛的应用。无线入侵检测技术也将必然随着计算机技术的发展而发展，随着无线网络的普及和移动设备的性能的提高而得到进一步的发展。下一步将在本文研究的基础上，重点解决入侵检测系统的应用瓶颈问题，以大幅度提升检测准确性以及大量应用网络环境下的系统性能。

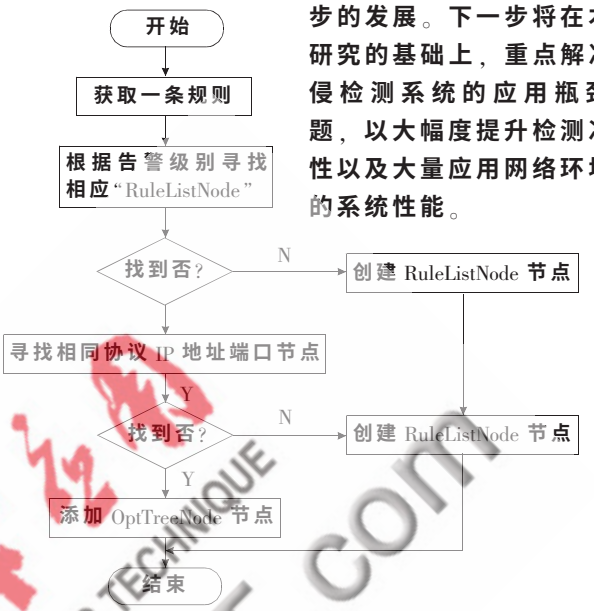

图 10 规则解析模块流程

参考文献

[1] 张丙凡，李永忠，宛智勇.多元化入侵检测技术[J].计算机仿真，2009，26(11):141-144.

[2] 张耀辉.入侵检测在高速网络环境下的技术研究[J].长沙通信职业技术学院学报，2009，8(4):27-30.

[3] 李旺，吴礼发，胡谷雨.分布式网络入侵检测系统 NetNumen 的设计与实现[J].软件学报，2002，13(8):1723-1728.

[4] 伍爱平，施月玲.分布式入侵检测中的数据融合模型[J].计算机与数字工程，2007，35(4):97-99.

[5] 程玉青，梅登华，陈龙飞.基于数据挖掘的入侵检测系统模型[J].计算机技术与发展，2009，19(12):123-166.

（收稿日期：2010-05-11）

作者简介：

林海涛，男，1974 年生，讲师，主要研究方向：通信网络管理。