Research of Distributed Network Intrusion Detection System Based on Rough Set

Zhong Zufeng
zhanjiang normal university, Zhanjiang, china
e-maili: zhongzufeng@163.com

Abstract: With the great development of computer network, the single IDS can not meet the needs of network security, so the DIDS comes forth .This paper was with the technology of intelligent agent an architecture and Rough Set were put forward and formal analysis of the distributed network monitoring system made. The experimental result shows that the network intrusion detection developed by this paper can work very stably under the Ethernet, find intrusion activities in time, enhance the detective ability of intrusion detection, and possess a favorable performance of intrusion detection.

Keywords: intrusion detection system; distribution; rough set; JXTA

基于粗糙集的分布式网络入侵检测系统的研究

钟足峰
湛江师范学院商学院，湛江，中国，524048
e-maili: zhongzufeng@163.com

【摘　要】随着计算机网络的迅猛发展，单一的集中式的入侵检测系统已不能满足网络安全发展的需要，分布式入侵检测系统应运而生。文中应用智能代理技术和粗糙集算法,提出一种分布式网络监控系统结构,并进行了形式化分析和实现。系统实验结果表明,所开发的网络入侵检测系统可以稳定地工作在网络环境下,能够及时发现入侵行为,增强了入侵检测系统的检测能力,具备了良好的网络入侵检测性能。

【关键词】入侵检测系统；分布式；粗糙集；JXTA

1 引言

自从计算机网络的兴起，网络安全一直是一个无法回避的重要问题。传统上，一般采用防火墙作为安全的第一道防线。但随着攻击者知识的日趋成熟，攻击工具与手法的复杂多样化，单纯的防火墙策略已经无法满足那些对安全高度敏感的部门之需要，网络的防卫必须采用一种纵深的、多样的手段[1]。

分布式的入侵检测架构就是适应此种需求而迅速发展起来的。分布式入侵检测系统一般指的是部署于大规模网络环境下的入侵检测系统，任务是用来监视整个环境中的安全状态，包括网络设施本身和其中包含的主机系统。分布式入侵检测是目前网络安全领域的研究热点之一。国外的研究机构已经提出并实现了多种原型系统。分布式入侵检测系统相对于传统的入侵检测系统具有明显的优势：能够检测大范围的攻击行为；提高了检测的准确率；提高了检测的效率；各检测组件之间能够通过协调来进行响应[2] [3]。

国内外在将数据挖掘用于入侵检测方面已取得了良好的进展,提出了一些基于数据挖掘的入侵检测模型。特别是粗糙集算法在运用属性约简对入侵的分类和判断上效果较好。本文提出基于粗糙集的分布式网络入侵检测系统结构模型,对算法进行讨论,并运用 JXTA 进行了实现。

2 系统结构

如图 1 所示，分布式网络入侵检测系统，其总体结构可以分成两个部分，即部署在网络内部的分布式节点，部署在网络外的控制服务器、数据挖掘规则库及日志数据库服务器。每个分布式节点都保存不一样的入侵检测类型，能对不同类型的入侵类型进行检测。分布式节点的任务主要是通过各节点之间的协作对进出该

湛江市科技攻关项目（项目号：2008C09024）
湛江师范学院资助科研项目（项目号：W0721）

Figure 1. System frame
图 1. 系统结构图

子网的流量进行捕包，通过实时检测分析，发现入侵行为。分析器还需要定时的从数据挖掘规则库服务器更新本地的规则库，并及时地将检测的结果反馈给日志服务器。此外，分布式节点还会对该子网的入侵行为进行分析，如果发现异常，会将异常作为日志的一部分，发送给日志服务器，当情况较为严重时，分布式节点端起用报警器进行报警、告知管理员发生了入侵，从而阻止入侵的继续。数据挖掘规则服务器中保存着通过粗糙集挖掘出来的评定规则。控制服务器则控制着整个分布式网络的运行。

3 基于粗糙集的入侵检测技术

粗糙集理论近年来在数据挖掘中得到广泛应用，主要被用来发现数据库中隐含着的确定性规则，粗糙集(Rough Set, RS)理论是一种刻画不完整性和不确定性的数学工具，能有效地分析和处理不精确、不一致、不完整等各种不完备信息，并从中发现隐含的知识，揭示潜在的规律[4] [5]。

在 RS 理论中，一个信息系统 SI 可用一个四元组表示：[6]

$$IS = (U, A, V, f)$$

假设 $X \subseteq U$ ，R 是 U 上的等价关系，$A = (U, R)$ 是一个近似空间，则有：[7]

$$R_*(X) = \cup\{Y \in U/R : Y \subseteq X\}$$

$$R^*(X) = \cup\{Y \in U/R : Y \cap X \neq \Phi\}$$

分别称它们为 X 的 R 的下近似和 R 的上近似。

假设 P 和 S 为 U 中的等价关系，S 的 P 正域，记为 $POS_p(S)$：

$$POS_p(S) = \cup P_*(X) \qquad X \in U/S$$

设 Q 是 P 的 S 的独立的子集，且 $POS_Q(S) = POS_P(S)$，则称子集 Q 为 P 的 S 约简，P 中所有 S 不可约去的属性称为 P 的 S 核。记为 CORE(R)：

$$CORE(R) = \cap RED(R)$$

其中 RED(R)是 R 的所有约简集。

本系统中，通过粗糙集找出入侵数据的约简集，步骤如下：属性约简得到入侵判定的最小条件属性集；对属性值的进行约简，删除该入侵决策规则的多余属性值后，该入侵决策规则的一致性保持不变；算法约简得到的最小入侵决策规则集便是所求的最小算法。

4 系统关键技术实现

本系统采用 JXTA 结构。JXTA 是 SUN 公司提出的一个 P2P 的网络底层支撑平台[8] ,包括 JXTA 核心层、业务层和应用层。支持协同工作系统的开发。基于 JXTA 平台开发的 P2P 应用程序具有三个特征：(1)互操作性，即 JXTA 能使对等点很容易的进行相互定位，相互通信，加入基于团体的活动，提供无缝跨越不同 P2P 系统和不同团体的服务。(2)平台无关性，即 JXTA 独立于开发语言(如 C、Java)、独立于平台(如 Unix，Windows)以及独立于网络传输协议(如 TCP/IP，Bluetooth)。(3)广泛性，即 JXTA 能运行在任何数字处理的装置(如传感器、消费电子、路由器、桌面计算机、数据中心等) [9,10]。系统关键技术实现如下：

捕包器实现：

```
//通过调用 WinPcap 来进行
  CallWinPcap();
```

分析器实现：

```
//生成代表描绘捕获包的 CreatePackage 类的对象
  CreatePackage CreatePackage1=
  new CreatePackage(s. package)
//生成代表描绘入侵规则库的 CreateRules 类的对象
  CreateRules CreateRules1=
  new CreateRules (s. Rules)
//根据捕获包和入侵规则库调用分析函数
AnalysisPackage（CreatePackage1，
CreateRules1）；
```

报警器实现：

```
//生成代表报警信息产生时间的 CreatTime 类的对象
  CreateTime CreateTime1=
  new CreateTime(s.timestamp)
```


978-1-935068-06-8 © 2009 SciRes.

```
//生成描述入侵行为的 Classification 类的对象
    Classifieation Classification1=
    new Classifieation (s.sig_name);
//根据入侵类型调用报警函数
    InvasionAlarm（Classification1）；
交互器的实现：
    While(true){ //持续进行监听
    java.net.Socket inRequest=_
    serverSocket.accept();//建立连接
    //启动 InPeeiConnectionThread 对象的运行，以处理具体交互过程
    inConnecrionThread.start();
    }
```

4 总结

将数据挖掘技术应用到入侵检测系统是目前入侵检测研究的重要方向,本文设计的分布式网络入侵检测系统采用了粗糙集算法和 JXTA 的网络入侵检测技术,有效地解决了入侵检测的速度问题,本系统能够提高系统检测的准确率、降低误报率,同时能够对未标记的数据进行日志分析,提高了系统的自适应性和可扩展性。

致谢

本文的完成感谢商学院各位同事的帮助和协助。没有这些支持，本文很难继续，无限感激。

References (参考文献)

[1] Tang Zheng-jun, Li Jian-hua. Intrusion detection [M]. Beijing: Tsinghua University Press, 2004.27-28.
唐正军，李建华.入侵检测技术[M].北京:清华大学出版社，2004.27~28.

[2] Sun Yuan-cheng. Key Problems in Technical Research of Agent-Based Distributed Intrusion Detection System[D]. Xian: Xian University of Technology,2008.
孙元成，基于 Agent 的分布式入侵检测系统关键技术研究[D].西安:西安理工大学,2008.

[3] HUANG Xian-Ying, WANG Ke-Ke, FAN Wei. Study of Star-based Distributed Association Rules Mining Algorithm[J]. computer science. 2007，34(12): 180-182.
黄贤英，王柯柯，范伟. 基于星型网络的分布式关联规则挖掘算法研究[J] .计算机科学，2007，34(12): 180-182.

[4] Z. Pawlak , Rough sets[J] .Internal Journal of Computer and Information Science, 1982,11:341-356.

[5] Mohamed Q. A-RST:A generalization of rough set theory[J]. Information Sciences,2000,12(124):301-316.

[6] YANG Wu,HUANG Zhi-Zhen,LI Li-Xin. An Inference Quantized Analysis Scheme of MLS DBMS Using Rough Set [J]. computer science. 2005，32(8): 75-76.
杨武，黄志真，李立新. 一种基于粗糙集的多级安全数据库推理问题的量化方法[J] .计算机科学，2005，32(8): 75-76.

[7] Pawlak Z， Rough Set Approach to multi-attribute Decision Analysis[J]. European journal of operational Researeh.1994，72: 443-459.

[8] Xu Bing. JXTA-Java P2P network programming[M]. Beijing: Tsinghua University Press,2003.
许斌. JXTA-Java P2P 网络编程技术[M].北京：清华大学出版社，2003.

[9] JXTA[EB],http://www.jxta.org,2007. Ji Qiao.jxta in a nutsbell[M]. Beijing: Tsinghua University Press,2004,1.
技桥.JXTA 技术手册[M]. 北京：清华大学出版社，2004 年 1 月.