# 簇技术在移动 Ad hoc 网络入侵检测中的应用研究

黄烟波,胡 波,周忠华
(中南大学 信息科学与工程学院,湖南 长沙 410083)

**摘 要**:由于移动 Ad hoc 网络的独特网络特性,其安全性特别脆弱。为其提供高安全的入侵检测系统势在必行,然而入侵检测审计数据的准确性、及时性、可靠性等是其获得高效的前提。在此将簇技术应用于 Ad hoc 网络入侵检测中,有效地提高了 Ad hoc 网络的安全性和对分布式攻击的协同检测能力,并降低了网络的通信负荷。

**关键词**:簇;入侵检测;数据挖掘;移动 Ad hoc 网络
**中图分类号**:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2007)04-0113-04

# Application and Research of Cluster Technology in Intrusion Detection of Mobile Ad hoc Networks

HUANG Yan-bo, HU Bo, ZHOU Zhong-hua
(College of Information Science and Engineering, Central South University, Changsha 410083, China)

**Abstract**: There are inherent vulnerabilities that are not easily preventable in the mobile Ad hoc networks. To build a highly secure wireless Ad hoc networks intrusion detection techniques need to be deployed, but accuracy, timeliness and reliability of the audit data is the premise. In this paper, application of cluster technology in intrusion detection of mobile Ad hoc networks has been shown, which can enhance the security and collaborative detection capability of intrusion detection, and the communication load is reduced effectively.

**Key words**: cluster; intrusion detection; data mining; Ad hoc networks

## 0 引 言

移动 Ad hoc 网络(以下简称 Ad hoc 网络)是由一组带有无线收发装置的移动主机组成的一个多跳的临时性自治系统[1]。与传统的无线网络不同,它不依赖于任何固定的基础设施和管理中心。在这种网络环境下,由于终端无线通信覆盖范围有限,两个无法直接通信的终端需要借助其它终端进行通信,终端之间通过无线信道相互协作和自我组织连接形成一个任意网状拓扑结构,而且主机可以任意移动,因而网络拓扑结构高度动态[2]。

由于 Ad hoc 网络的独特结构,产生了一些突出的特点:脆弱的无线通道、缺乏集中监控机制、拓扑结构高度动态、移动节点本身的安全性等[3,4],从而使得 Ad hoc 网络安全更加脆弱,因此,现在常采用入侵检测技术作为其安全防范的第二道防护墙。然而对于入侵检测技术,其审计数据是相当重要的,如何保障数据的准确性、及时性、可靠性等成为首要应解决的问题。

**收稿日期**:2006-07-08
**作者简介**:黄烟波(1959-),男,湖南邵阳人,教授,主要研究方向为计算机网络、现代教育技术。

## 1 入侵检测与 Ad hoc 网络

无线信道、动态拓扑、合作的路由算法、缺乏集中的监控等安全缺陷都使得 Ad hoc 网络安全更加脆弱,特别是移动节点缺乏物理保护,容易被偷窃、捕获,落入敌手后重新加入网络,导致攻击从内部产生,而采用密码学理论的网络安全方案无法对抗此类攻击。安全问题成为 Ad hoc 网络面临的一个主要挑战,比如受到窃听、伪造、重放、篡改报文以及拒绝服务等攻击,已成为 Ad hoc 网络能否健康发展的一个关键问题。

### 1.1 当前 Ad hoc 网络入侵检测模型

(1)现在 Ad hoc 网络通用的入侵检测模型是由 Yongguang Zhang 和 Weeke Lee 提出的一个基于 agent 的分布式协作入侵检测方案。该方案的优势是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,适合于移动自组网自组织的特点。如果每个节点的 IDS agent 具有同等的检测能力,那么其全局的入侵检测则可以保证。

(2)Oleg Kachirski 和 Ratan Guha 提出了基于移动 agent 的入侵检测方案。他们认为 Yongguang 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。

(3) Chin - YangTseng 等提出了基于规范(specification - based)入侵检测方案。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警。检测过程为:监听节点对查询报文的处理过程,记录下来形成转发表和操作树,然后用规范形成的有限状态机进行检查,输出为正常状态、怀疑状态、入侵状态三种结果,再分别进行不同的处理。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:占用节点较多的计算资源,未用实验进行验证。

(4) 易平(复旦大学)等人提出一种基于时间自动机的入侵检测算法。其算法为,将整个网络划分为一个个区域,每个区域随机选出一个节点作为监视节点。然后,按照路由协议构筑节点正常行为和入侵行为的时间自动机,监视节点收集其邻居节点的行为信息,利用时间自动机分析节点的行为,确定入侵者。本算法不需要事先进行数据训练并能够实时检测入侵行为。

### 1.2 现有模型的局限性

因为没有统一的监测点,任何节点收集的信息是不完全的,所以上述方法都采用分布式邻居监测、协同检测的方法。现行的入侵检测的架构为使用 agent 作为入侵检测的执行者,agent 驻留并运行于网络中每一个节点内,分布式地监视网络状况,信息共享,合作检测入侵行为。这种架构对于入侵检测本身来说是较为有效的,但未充分考虑到移动自组网自身的局限性,存在以下一些缺陷:

(1) 让每个节点都驻留 agent,而且都处于对等的地位,这没有考虑到移动自组网网络带宽和节点计算资源有限的特点,也许会占用过多节点资源。

(2) 如果采用 Oleg Kachirski 和 Ratan Guha 的方案,只是在某些节点上驻留有监视网络的 agent,虽然可以节省节点资源,但势必会对入侵检测的效果产生一定的影响。

笔者认为在设计上应充分考虑到网络资源有限的特点,降低其对资源的要求,不必让每一个节点都处于对等的地位,但又要考虑能够进行有效的入侵检测。

## 2 簇技术

簇(也称集群)技术是一种通过网络将多台同构或异构的计算机连接起来并协同完成特定任务的计算机的技术[5],此技术能够使网络客户连接到一个由多个节点组成的服务器系统上,这样,数据的可靠性就能得到保证。而且簇技术以其高可用性、高可扩展性、高性能、高性价比和易管理性等优越性[5,6],随着因特网的迅猛发展,日益受到高性能计算和高性能服务两大领域的关注。

由于移动自组网络没有像路由器等这种可以将入侵检测系统置于其中,收集全部网络审计数据的设备,因此,在任意时刻,审计数据只能局限于无线通信覆盖范围之内传输,入侵检测算法也只能够对部分或者局部地区的信息进行分析,加上局部地区的信息收集局限于某层,信息量大打折扣,从而导致误报率增加,检测性能大大下降。

为了克服移动自组网络的安全脆弱性,以及现有移动自组网络入侵检测模型的局限性,解决 Ad hoc 网络入侵检测中输入数据的问题,针对其审计数据局限于无线通信覆盖范围之内传输,而现有的入侵检测算法也只能够对部分或局部地区的信息进行分析,信息量大打折扣,误报率增加,检测性能大大下降的情况,在此将成熟的簇技术运用于移动自组网的入侵检测系统中,把节点分成多个区域,每个区域里的每一个节点都参与检测,但使用一个 cluster head 负责管理区域中的成员。这样既考虑到网络带宽和节点计算资源有限的特点,又能够有效地进行入侵检测。

## 3 簇技术在 Ad hoc 网入侵检测中的应用

在此入侵检测系统中,IDS agent 驻留于每个节点上,整个网络拓扑结构分割成一系列称为簇的区域,每个簇选举出一个簇头节点(cluster head)管理该区域。而且 IDS agent 的本地数据源来源于该主机系统的多个层次,不局限于网络层。这样可以有效地分布管理站的管理任务,增强系统的容错性,提高通信效率。

### 3.1 基于簇的 Ad hoc 网络

簇结构化分得合理与否对系统的性能有直接的影响,目前人们已经提出了一系列基于簇的控制结构和相应的算法,各结构和算法也各有千秋。在此采用是文献[7]中提到的 The Near - term Digital Radio(NTDR)簇控制结构和算法,充分考虑了网络节点的处理级别、能量、移动频率等因素。

在 NTDR 中,节点间通过周期性接受一种称为熏肉的消息来确定是否属于同一个簇,从而实现它们之间的通信。每个簇选举出一个簇头节点管理该区域。而且为了弥补原簇头失效的情况,新簇头选出的过程很迅速。每个簇头使用两种不同的频率进行通信,一种用于和其它簇头之间的通信,一种用于和簇内的节点通信。簇的内部结构如图 1 所示,在一个簇范围内,

各节点可和一跳范围内的其它节点直接通信。如果某节点要和超过一跳范围的其它同一簇范围内的节点通信,则必须通过簇头节点才能完成。而不在同一簇范围内的节点,即使在一跳范围内也不能直接通信。如图 1 中所示,节点 A 和节点 B 在一跳范围之内,可直接通信。而节点 C 超出节点 A 和 B 的一跳范围,但属于同一簇,所以可通过簇头来完成节点 A,B 和节点 C 之间的通信。节点 D 在节点 A 的一跳范围之内,但它们不属于同一簇,故不能直接通信[7],它们之间的通信同样也要通过各个簇头来完成。簇间的通信方式如图 2 所示。图中两个不在同一簇内的节点必须通过各个簇头才能通信。

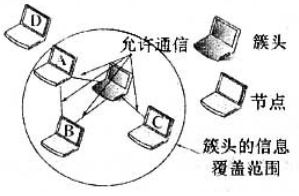


图 1　簇的内部结构

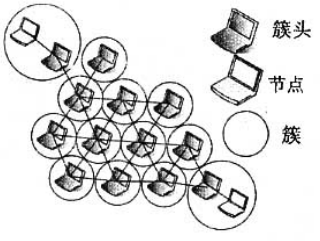


图 2　基于簇的移动 Ad hoc 网络结构

### 3.2　基于簇技术的入侵检测系统架构

如图 3 所示,每个节点都配置一个自治的 IDS agent,负责独立地对本地进行入侵检测,而簇头作为主要的入侵检测节点能够控制和管理簇中的其它节点监控本地的各种行为,这些 agent 共同完成入侵检测和响应。在簇内,IDS agent 驻留在各个节点上,各 IDS agent 独立运行监控本地(即 IDS agent 的控制范围内)的各种行为,包括用户、系统行为及无线通信范围内的通信活动等,并根据监控结果检测入侵和发起响应。当某个节点如果只是怀疑有入侵行为,则激发多节点的协作检测。驻留于簇头上的 IDS agent 将管理和控制各节点间的相互协作,并和它们共同完成全局入侵检测,如果确定有入侵则激发全网的入侵响应。

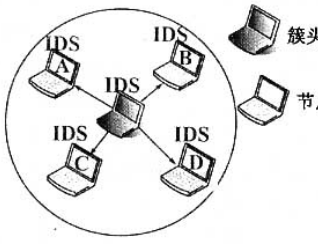


图 3　IDS 中单个簇的内部结构

IDS agent 的内部结构非常复杂,但从概念上讲,可以分为 6 个模块,如图 4 所示:本地数据收集模块、本地分析引擎、本地入侵响应模块、全局入侵响应模块、安全通信模块、协作检测模块。本地数据收集模块负责收集本地各种审计跟踪数据,而本地分析引擎则使用这些数据进行本地异常检测,其检测结果将被送达协作检测模块。本地入侵响应模块和全局入侵响应模块共同提供入侵响应行为。本地响应模块将行为传达给本地移动节点;而全局响应模块负责调整相邻节点之间的行为。最后,安全通信模块在各个 IDS agent 之间提供高可靠性的通信通道。

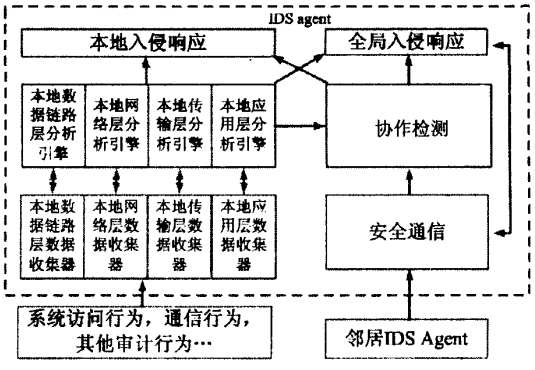


图 4　IDS 节点中的 IDS agent 结构

#### 3.2.1　基于簇的入侵检测运用数据挖掘技术

整个入侵检测框架使用数据挖掘技术,并且除了传感器外都驻留在簇头的 IDS agent 上,由簇头负责指挥簇中各节点如何计算行为特征。关于如何计算、哪里计算以及传输行为特征值,有两种方案来处理。一种是在每个特征值取样周期,簇头从成员节点中随机选择一个节点,要求其传输整个特征值集给簇头;另一种是为减轻各节点的负担和流量,簇头帮助计算一些特征值,包括与流量有关的特征值。通常簇头通过传感器收集簇内各节点的输入和输出流,整个簇就像个特大节点,共同完成与流量有关的特征值以及内部传输的数据包数量的计算,并通过簇大小平均值进行规格化。

另外成员节点还要将与路由和位置有关的特征值传输给簇头。簇头根据修订过的特征值集,使用数据挖掘技术来评估入侵检测模型。因为获得与流量有关的特征值将花费主要的计算时间,而特征值集中大部分是与流量有关的特征值,因此采用这种计算特征值的方案,将会大大地降低整个簇计算特征值的代价。

#### 3.2.2　本地数据的收集和检测

本地数据收集模块收集来自各种信息源的跟踪数

据并进行处理,处理的结果被用作本地分析引擎的输入。根据入侵检测算法,这些数据流包括本节点的系统、用户和通信行为,以及和通信范围内的其它节点的通信行为。

本地检测引擎分析来自于本地数据收集模块收集来的异常行为信息,该模块采用基于统计学方法的异常检测技术,其检测结果将被送达协作检测模块。

3.2.3 入侵响应

本地入侵响应模块和全局入侵响应模块共同提供入侵响应行为。入侵响应类型因入侵的类型、网络协议和应用的类型以及入侵证据的确凿程度不同而不同。入侵响应应该通知网络中的其它节点。它可能是识别出被俘节点,并将这个节点排除在外重新组织网络,直到该节点重新得到认证为止;也可能只是简单给出告警指示。用户可以根据它选择拒绝和可疑节点连接,当进行合作时可以将这个节点排除在外。本地响应模块将行为传达给本地移动节点;而全局响应模块负责调整相邻节点之间的行为。

## 4 小 结

Ad hoc 网络由于其动态拓扑、无线信道以及各种资源有限等脆弱性特点,其安全性对安全防范提出了更高的要求。入侵检测技术作为其安全防范的第二道防线,是 Ad hoc 网络获得高抗毁性的必要手段,然而其审计数据的准确性、及时性、可靠性是入侵检测获得高效的前提。针对现有 Ad hoc 网络入侵检测模型的不足,将簇技术应用于 Ad hoc 网入侵检测中,该技术增强了入侵检测系统自身的安全性和对分布式攻击的协同检测能力,有效降低了网络的通信负荷。

**参考文献:**


[1] 冯建新,王光兴. MAIDS—Ad Hoc 网络的多层分布式入侵检测系统[J]. 小型微型计算机系统,2004(12):2195-2198.

[2] 易 平,蒋嶷川,张世永,等. 移动 ad hoc 网络安全综述[J]. 电子学报,2005(5):893-899.

[3] 王 松,王卫红,张 繁. 一种新的移动 ad-hoc 网络异常入侵检测技术[J]. 浙江工业大学学报,2004(12):696-699.

[4] Zhang Y, Lee W. Intrusion Detection in Wireless Ad-Hoc Networks[C]//Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking. New York, USA: ACM Press, 2000:275-283.

[5] 徐有明,曹元大. 集群技术在消息中间件中的应用[J]. 微机发展,2005,15(10):109-111.

[6] 程 洪,钱乐秋,洪 圆. 基于 Linux 集群的 Web 服务的研究和构建[J]. 计算机工程与应用,2004(34):158-161.

[7] Zavgren J. NTDR mobility management protocols and procedures[C]//In: Proceedings of the IEEE Military Communications Conference. Boston, USA: IEEE Press, 1997.


(上接第 99 页)

的 TANC 结构学习算法是有效的和准确的。

## 4 结束语

现有的 TANC 结构学习算法是基于相关性分析的或搜索打分机制的,相关性分析中采用互信息测度和条件互信息测度,基于搜索和打分的 TANC 结构学习中采用 BIC 测度。文中提出了一种新的结构学习方法,用 BIC 测度作评价函数,引入遗传算法学习 TANC 结构。在 MBNC 实验平台上实现了 GA-TANC 算法。实验结果表明,用这种结构学习算法得到的 TANC 是有效的,在某些数据集中的分类准确率要优于 TANC-MI, TANC-CMI 和 TANC-BIC。

**参考文献:**


[1] Cooper G, Herskovits E. A Bayesian method for the induction of probabilistic networks from data[J]. Machine Learning, 1992,9:309-347.

[2] 林士敏,田凤占,陆玉昌. 用于数据采掘的贝叶斯分类器研究[J]. 计算机科学,2000,27(10):73-76.

[3] Duda R O, Hart P E. Pattern Classification and Scene Analysis [M]. New York: John Wiley & Sons, 1973.

[4] Friedman N, Goldszmidt M. Building classifiers using Bayesian network[C]//In proc. Nation Conference on Artificial Intelligence. Menlo park, CA: AAAI Press, 1996:1227-1284.

[5] Chow C K, Liu C N. Approximating discrete probability distributions with dependence trees[J]. IEEE Trans. on Info. Theory, 1968, 14:462-467.

[6] 程泽凯. 贝叶斯网络结构学习及 MBNC 实验平台的构建[D]. 南宁:广西师范大学,2004.

[7] 程泽凯,林士敏. TANC-BIC 结构学习算法[J]. 微机发展,2004,14(11):10-12.

[8] Larranaga P, Poza M, Yurramendi Y, et al. Structure Learning of Bayesian networks by genetic algorithms: A performance analysis of control parameters[J]. IEEE Trans on Pattern Analysis and Machine Intelligence, 1996, 18(9):912-925.

[9] 刘大有,王 飞,卢奕南,等. 基于遗传算法的 Bayesian 网结构学习研究[J]. 计算机研究与发展,2001,38(8):916-922.

[10] 程泽凯,林士敏,陆玉昌,等. 基于 Matlab 的贝叶斯分类器实验平台 MBNC[J]. 复旦学报,2004(5):729-732.