网络入侵行为表示的分类研究*)

孙美凤[1,2]　龚　俭[1]

(东南大学计算机系网络中心　南京 210096)　(扬州大学信息工程学院　扬州 225009)

摘　要　在计算机安全领域,特别是网络安全领域,对入侵行为进行研究十分重要,它是入侵的预防、检测、预警和响应等多项技术的基础。本文从本体论的角度对入侵行为进行分类,介绍了每种表示观的实质及其表示方法。最后讨论了入侵行为研究存在的问题及今后的方向。

关键词　入侵行为,本体,表示,检测语言

A Survey of Research on Intrusion Behavior and its Representation

SUN Mei-Feng[1,2]　GONG Jian[1]

(Department of Computer Science and Technology , SouthEast University, Nanjing 210096)[1]

(Information and Engineering College, Yangzhou University, Yangzhou 225009)[2]

Abstract　A theory of intrusion behavior is a highlighted topic of network security research in recent years, it is the base of many security techniques such as intrusion prevention, intrusion detection, pre-alarming and auto-response. In this paper, the researches of intrusion behavior and its representation are summarized in terms of ontological commitments. The spirit of each view is introduced, and many intrusion representation techniques are described. Last the existing problems and the future directions in this field are discussed.

Keywords　Intrusion behavior, Ontological commitments, Representatio, Detection language

1　引言

近年来随着互连网的迅速发展,入侵行为明显地表现出两个特性:入侵出现的频率越来越高,入侵的手段越来越复杂。根据美国权威安全应急响应小组 CERT/CC 最新发布的统计报告[1],2003 年有据可查的安全事件报告达到 137,529 起,比 2002 年增加了一半以上。同时入侵行为已经从手工入侵发展到自动入侵、从零碎的小规模的入侵发展成为大规模的、分布式的入侵。近年爆发的 Sadmind/IIS 蠕虫、CodeRed 蠕虫、Nimda 蠕虫等入侵与早期的简单入侵存在明显区别,它们综合运用了多种技术,入侵过程需要多个步骤的协同合作才能完成,并且大部分该类型的入侵由程序实现。互连网规模及其应用范围的不断扩大、入侵工具的普遍存在、入侵手段的不断复杂化使得入侵具备了巨大的危害性。

与入侵技术相比,计算机安全保障技术特别是入侵检测技术在市场上的失败致使互连网上的机器面对入侵显得脆弱无力。20 世纪 90 年代中后期,DARPA 资助了大量的入侵检测项目,目标是开发一组入侵检测系统(IDS),其检测率大于 99%误报率小于 1%,并且对已知和未知入侵同样有效,评估表明没有项目达到预期的目标。

John McHugh[2]认为建立在直觉之上的入侵检测技术的进一步发展将有赖于合适的入侵行为理论的开发,这样的一个理论应能够指导入侵行为关键属性的提取以及抽象的通用的检测规则的设计,从而显著地提高 IDS 的性能。围绕入侵检测技术和入侵检测系统的综述文献有很多,文[3]是其中的经典研究之一,但还未见关于入侵行为表示的研究综述,而入侵行为表示是入侵预防、检测、修复以及安全产品的测试等研究的基础。围绕表达能力和表示形式系统地分析入侵行为研究的现状,实践上指导特定应用环境的入侵表示技术的选择,理论上揭示行为研究存在的问题,指明未来方向,为入侵行为理论的全面建立提供基础是本文的目标。

由于客观世界的复杂性,任何表示都只是表示对象的不完美的近似,不可避免地"聚焦"某些属性,忽略另外的属性[4],因此表示首先是一组看待客观对象的约定,即表示的本体论。本体论是表示技术的"精神"实质,无论表示的形式如何变化,只要本体论是相同的,它们必然具有本质上的一致性,因此本体论非常适合于表示技术的综述和分类研究。

在给出了本文所使用的一些概念定义之后,文章首先介绍了入侵行为的各种表示观,随后对行为模式观点下的入侵表示技术从表达能力和表示形式两方面讨论,文章最后讨论了入侵行为研究存在的问题以及今后的方向。

2　基本概念

入侵:一个用户恶意地违背系统安全政策的行为。定义中突出强调了安全政策,说明是否入侵在很大程度上取决于系统的所有者。在信息安全领域,安全政策的研究和实现仍属于薄弱环节,人们通常仅在一个行为发生之后才能确定其合法性。参考计算机安全 CIA.[5],总的来说,入侵是指破坏了信息或资源的机密性、完整性以及可用性的行为。

简单入侵:能够构成入侵的最小行为序列。从技术的角度看,简单入侵指的是针对一个漏洞、采取一种手段完成的入侵。例如一次栈溢出入侵、一次基于 Web 的 cgi 漏洞入侵等。

多阶段入侵:利用了多个漏洞的交互关系、采用多种技术手段、通过多个步骤的相互合作间接完成的入侵。

事件:系统或用户行为可观察的内容,形式上可表示为一组(name,value)对。如果不考虑审计的具体实现,行为和事

*)本课题得到国家自然科学基金(90104031)资助。孙美凤　博士研究生,主要研究方向为网络安全监测。龚　俭　博士生导师,主要研究方向为网络安全、网络管理和网络体系结构。

件具有对应关系，事件的观点不局限于审计记录，而是主机或网络中任何可抽象、可观察的内容。

入侵特征/场景：入侵过程在一个可观察的系统中留下的痕迹。一个入侵可能呈现出多维的特征，从理论上说，入侵特征越多检测准确率就越好，因此从测准率的角度考虑，入侵特征搜集得越全面越有利于检测结论的生成；但是，从算法可行性和性能考虑，入侵特征越多检测算法的时间和空间复杂度就越大，为了保证算法能够顺利运行，入侵特征必须尽可能少。一个实际的滥用系统总是在特定的应用环境下对测准率和检测效率的均衡。

检测语言：特指行为模式观点下的入侵特征的描述规范。检测语言的提出需要综合多方面的因素：描述入侵的能力、算法支持的有效性、使用的方便性等。

3 入侵行为的本体论

3.1 行为模式

这种观点看待入侵为特定的行为模式，致力于揭示每个入侵区别于背景噪声以及其它入侵的特征行为以及行为之间的关系，因此如果入侵者的行为逃脱了审计或者其不表现为异常或者其异常分布于一个较长的时间区间，则采用行为模式表示观的 IDS 不能表示和检测此类入侵，例如检测慢扫描是所有此类 IDS 的困难问题。

该观点对简单入侵和多阶段入侵同样有效。行为在系统中的痕迹(事件)是主机审计记录或网络报文，具有瞬时的特点。由于入侵者可能对入侵行为以及行为的顺序尝试各种变化，因此定义的模板应当能够描述可能的变形。这种观点下的入侵形式化表示技术统称为检测语言。总的来说，检测语言都包括如下几部分：(1)过滤器—入侵特征的基本单元，它用于描述单事件特征(行为在系统中的痕迹)，通常由多个关于事件域的约束条件组成；(2)事件组合方式，用于描述事件间的时序和等价关系；(3)其它类型的约束，如否定条件和时间约束，用于撤销不可能推进的部分匹配实例，提高 IDS 的运行效率。

"刻画攻击现象"、"计算可接受"以及使用方便性是三个可能相互冲突的条件，在入侵检测发展的二十年中出现的大量检测语言[6~18]对这些条件有不同侧重，本文第 4 节详细介绍了该领域的研究成果。

3.2 行为模型

当考虑多阶段入侵时，模式和模式匹配的观点遇到难以克服的困难，这种困难主要来自于多阶段入侵模式的获取方面。由于变异、重排序、替换、分布、循环等技术的运用，多阶段入侵场景的变形可能是无穷的，显式给出所有的变形可能不可行。基于模型的观点试图捕捉并描述大量变形背后隐藏的规律，它认为入侵由意图驱动逐步实现，前面阶段为后阶段提供条件，从而将多阶段入侵纳入因果关系框架中。

与行为模式观点事件的结构关系不同，因果关系是语义层的，因此模型是比模式更深层次的知识。模式反映了安全专家的经验，经验可能是不准确、不完备的，也难以对其质量进行验证；而模型反映了对入侵世界的深刻认识，它具有系统性、抽象性的特点。总之基于模型的观点的优点在于模型的建立比模式的提取简单，利用模型可获得所有可能的入侵序列，发现未知的入侵模式。

该观点主要面向多阶段入侵，事件是来自底层 IDS 的报警，攻击树[19~21]和供求模型[22~24]是因果关系的两种表示技术。利用因果关系进行报警关联可以消除误报、综合报警结论和意图识别等[23~28]，是当前研究的热点问题。

(1)*攻击树*　典型的攻击树[19]是一种策略模型，它描述了入侵者权力逐步提升的过程。攻击树由结点和连接两个结点的有向边组成，根结点表示入侵意图，叶结点代表最小条件，中间结点是子目标，边表示子目标与上层目标之间的因果关系，多个结点能够通过"与"、"顺序与"和"或"三种构造算子组合。

扩展攻击树[20,21]的边可以存在于任意结点之间，因此扩展的攻击树已经失去了树的特性，而是由入侵事件结点以及状态结点组成的因果关系图。

(2)*供求模型*　供求模型[22]将入侵视为"概念"的可能组合，"概念"是入侵子任务的抽象表示，"能力"是"概念"出现的前提或结果条件，多个"概念"通过"能力"的蕴涵被组合在一起。通过规定入侵出现的需求能力，模型能够捕捉满足要求的所有可能手段，却不需要明显的给出这些手段；通过规定一个入侵提供的能力，模型能够捕捉所有使用该能力的对象却不需要显式的给出这些对象。

可以将供求模型看作攻击树中入侵事件结点的数据库，每个入侵事件结点包括下层结点(条件)和上层结点(结果)属性，存在的问题是攻击树中状态结点的连接特别是间接连接很难准确翻译成"能力"的蕴涵，因此供求模型实现简单，但可能不及攻击树的表达能力。

3.3 行为图

GrIDS[29]观察到蠕虫独特的扩散性特征，并将其作为检测的重要依据判定大规模入侵出现的可能性，因此该表示观只对蠕虫有效。GrIDS 实现简单，它将一定时间范围内的 TCP 连接首尾相接进行关联，形成 TCP 连接的扩散图，一定形状和规模的扩散图代表蠕虫的出现。GrIDS 的缺点是模型太弱，缺乏对入侵过程的具体分析，因此安全结论比较粗糙；另外 GrIDS 的关联条件是两个同类型事件发生在一定时间范围内，选择一个合适的时间窗口比较困难，窗口过小会产生漏关联，窗口过大导致关联正常的 TCP 连接，产生误报。

3.4 陷阱

文[30]观察到扫描和蠕虫行为通常是无目的和机械的，例如当攻击者发起扫描时，网络中的一个连续的 IP 地址区间都会遭到扫描；蠕虫在扩散时只要探测到相邻主机存在可用漏洞就尽力感染对方。IP 陷阱是受保护网络中的一些专门用于捕捉异常流量的 IP 地址，在正常使用时，陷阱 IP 不会有任何流量，如果发现某个陷阱 IP 产生了流量，那么一定有异常情况，或者是正常用户访问了错误地址，或者是攻击者将其选为目标，并且通过捕捉到的异常流量模式可以进一步判定入侵类型。IP 陷阱对扫描和蠕虫十分简单有效，但其不能应用于针对特定对象的入侵。

3.5 趋势模板

MAITA[31]是美国西点军校(United States Military Academy, West Point)信息保障和安全工作组开发的入侵防范系统，它使用的趋势模板语言(TTL)基于对 FTP 劫取入侵的观察扩展了传统的事件和事件关系的观点。FTP 劫取是一类常见的入侵，该入侵的典型特征不在于入侵发生的具体步骤(其中的大部分 FTP 事务是正常的)，而是入侵使得 FTP 流量行为呈现出特定的异常模式：FTP 流量从正常开始攀升，经过一定的时间间隔，到达并维持在饱和状态。显然标准的滥用和异常方法都无法准确识别该入侵。TTL 最初用于医学上对儿童的生长发育模式的刻画，允许事件是抽象的统计属性，允许事件的起始和结束时间的不确定性，从而可描述入侵在阶段性统计上的抽象特征，形式上表现为统计量在时间轴上分阶段的曲线图。TTL 不适合作为统一的检测语言，

它表示瞬时事件及其关系过于复杂，可用作对传统语言的完备性的补充。

4 检测语言分类

检测语言由于对“刻画攻击现象”、“计算可接受”以及使用方便性三个可能相互冲突的条件的不同侧重，表现出不同的表达能力、语法形式、执行语义以及其它操作特性。表示是检测的前提，因此表达能力可能是检测语言最重要的特性，它既遵从完备性的追求又受到处理效率的制约；表示形式服务于内容又最大限度地追求使用的方便。本文提出一种综合分类方法，由表达能力和表示形式两个属性组成，能够准确地分类检测语言。

4.1 表示形式

检测语言的表示形式可被分成三种，如图 1。其中规则语言明显的具有过程性的特点，表示“什么是入侵”是通过表示“如何检测入侵”实现的，因而要求入侵场景的规则编写者了解检测的算法。陈述性高级语言是针对过程性使用不便的缺点提出的，它带来了表示内容和处理方法的分离，具有使用方便、便于共享以及系统实现灵活的特点。自动机语言可视为中间语言，它具有直观的图形表示，因此检测语言的三种表示形式也代表了不同的抽象层次和方便程度。下面介绍每种形式下下的主要研究成果。

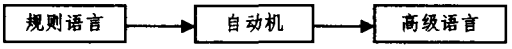

图 1 检测语言的在种形式

4.1.1 *规则语言* 规则语言的代表是专家系统语言 P-BEST。专家系统提供处理特定环境下的事实并推导出结论的策略和机制，通过将审计事件映射为专家系统的事实，滥用检测可以方便地映射到专家系统的推理框架中。P-BEST 由 SRI 开发，最初被应用在 MIDAS 中，增强后的 P-BEST 被应用在 IDES 和 NIDES 中，面向大规模分布式网络环境的入侵检测系统 EMERALD 也利用了 P-BEST 工具集[6]。

RUSSEL 语言[7] 和 Bro[8] 语言是一种专用的规则语言，两者都用类似于 C 函数的结构体作为规则，支持表达式评估、if 语句、报警触发和新规则调用。

总的来说，规则语言描述入侵特征是通过描述入侵特征的检测过程实现的。由于 what 和 how 纠缠在一起，使得特征的编写困难，并且特征不能在不同系统间共享，但具有较高的效率，通常作为系统的低级语言。

4.1.2 *自动机语言* Kemmerer 最早提出状态转移图的概念，它图形化表示入侵的过程，将入侵过程看作一个行为序列，这个行为序列的变迁导致系统从初始状态进入被入侵状态。这种技术首先在 STAT 系统中研究实现，尔后扩展到 UNIX 环境中形成了 USTAT 系统[9] 和面向网络环境的 NetSTAT 系统[10]，这两个系统都是由美国的加州大学圣巴巴拉分校(university of califorlia santa barbara)研究完成的，最后 Steven T. Eckmann 、Kemmerer 等在这三个系统的开发经验基础上总结出 STATL[11] 语言。

图 2 是一个状态转移图的例子。结点表示系统的状态，边是状态的变迁，结点和边都可以附加断言。所有的入侵过程都可以看作是从有限的特权开始，利用系统存在的漏洞，逐步提升自己的权限，正是这种特性使得入侵过程可以利用系统状态转移的形式来表示，在每个步骤中，入侵者获得的权限或入侵的结果都可以表示为系统状态。

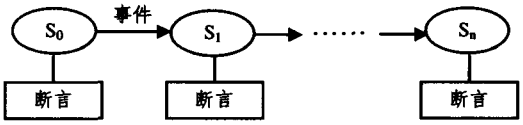

图 2 状态变迁图

有色 Petri 网(CPN)[12] 是另一个著名的基于自动机的语言，它由 Kumar 设计并被应用在美国普度大学(purde university)的入侵检测系统 IDIOT。在这个模型中，入侵被表示为一个 CPN，整个特征匹配的过程由标记(Token)完成，标志在审计记录的驱动下由初始状态向最终状态(标识入侵完成的状态)逐步前进，标记的颜色代表了事件序列及其发生的环境即标记的上下文。图 3 是一个 CPN 的例子。

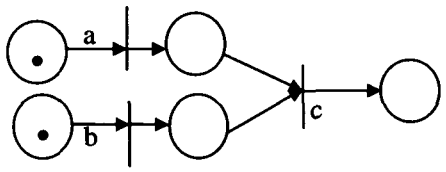

图 3 CPN

使用自动机形式化入侵场景是最自然的方法，并且有较成熟的理论基础。自动机语言具有直观的表示，在一定程度上实现了 what 和 how 的分离。

4.1.3 *高级语言* 陈述性语言的实现有两种技术路线。第一种是入侵特征是直接可执行的，逻辑语言、关系代数和文法等形式化工具因为有研究得较为充分的算法成为该路线下陈述性语言的理想选择。例如：Musigs 语言[13] 使用代数演算，文[14]使用了逻辑表示和模型检查算法，Parsing Schema[15] 使用文法表示入侵特征并将检测置于分析方案(Parsing Schema)的通用框架中。这类通用表示技术的缺点是高的计算复杂性，例如谓词公式的模型检查是 NP 完全的，入侵检测的巨大数据量以及实时性能的要求限制了陈述性语言的表达能力。第二种思路采用了编译的思想，高级语言特征被翻译成可执行特征，这个特征的编译过程允许对入侵自然而且简洁的刻画，如 Sutekh 语言[16]。

4.2 表达能力

不能仅从形式上决定检测语言的表达能力。例如 Russel 语言和 Bro 系统使用的语言语法非常相似，两者都用类似于 C 函数的结构体作为规则，支持表达式评估、if 语句、报警触发和新规则调用，但是由于执行语义的不同，Bro 语言描述单事件特征的检测，而 Russel 则具有近似于属性语法的表达能力。

通过分析比较，我们发现检测语言都具有两类语法元素：事件内容约束和组合方式。与形式语言理论的研究对象不同，检测语言不存在预定义的有穷过滤器表，甚至过滤器在描述时可能不确定。例如：Snort 将端口扫描攻击的场景描述为“时间 T 内某个主机访问目的主机 TCP 端口数超过 N”，该场景可形式化描述为“$X_1 X_2 \cdots X_n$”，其中的 X_i 代表 IP 报文，任意两个 X_i 要求同源同宿。Kumar 将这种需要统一不确定事件的场景称为 Unified。

Unified 场景的存在极大地增加了场景的复杂度，进而也增加了表示和检测实现的难度。但在另一方面，所有的多事件语言都使用变量支持 Unified 场景的表示。能否直接表示攻击场景的组合方式是检测语言本身的一个重要性质，也是

不同检测语言的最根本的区别，这种区别导致不同形式的特征库和不同的检测能力，因此本文将检测语言包含的组合方式作为分类标准。

定义 1 令 S1，S2，S 为任意的场景，其中 S 由 S1 和 S2 组合而成：

顺序与(S = S1 then S2)：S = {ω1ω2：ω1∈S1，ω2∈S2}；

或(S = S1 or S2)：S = S1∪S2；

与(S = S1 and S2)：S = {ω1 · ω2 ： ω1∈S1，ω2∈S2}。

·操作表示两个 F 序列任意位置连接，ω1 · ω2 ={"ABCD","ACBD","ACDB","CABD","CADB","CDBA"}。·操作是可交换的：ω1 · ω2 = ω2 · ω1；·操作可结合：ω1 · ω2 · ω3 = (ω1 · ω2) · ω3。·操作具有非常强的表示和生成序列的能力。

定义 2(γ关系) 令 M' 是检测语言的集合，γ= {($M1$，$M2$)：$M1$，$M2 \in M'$ 且 $\forall x$：$x \in$ {then，and，or}，$M1$ 支持 x 等价于 $M2$ 支持 x}。

显然 γ 关系自反、对称和传递。

定义 3(分类 μ) μ 是检测语言集合 M' 上的按照 γ 关系构造的划分。

μ = {[{}]，[{then}][{and}]，[{or}]，[{then，and}]，[{then，or}]，[{and，or}]，[{then，and，or}]}，其中，对 $\forall x$：$x \subseteq$ {then，and，or}，

$[x]$ = { $M \mid M \in M'$ 且 M 支持且仅支持集合 x 中的组合方式}

为了书写的简便，本文去掉了 $[x]$ 中 x 的集合符号，即将[{then，or}]直接缩写为[then，or]。分类 μ 是利用检测语言的语法元素进行的分类，这一点保证了分类的无歧义和可重复。同时，分类 μ 是建立在等价关系上的划分，因此互斥而完备。这里的完备性是基于定义 3.1 给出的三种组合方式，而非语义的完备。

陈述性高级语言支持的组合方式是显然的，而图形化表示(有色 Petri 网、STATL)的组合方式也容易直观看出。确定规则语言如 P-Best 和 Russel 的表达能力需要仔细分析其执行语义。Russel 规则具有 IF…THEN…的形式，IF 评估到达事件，THEN 决定激活规则和发送报警，激活规则行为规定了后续过滤器(then)，IF 是 or 的典型语法，因此 Russel 语言支持 then 和 or 的直接表达。P-Best 语言有些区别，它评估事实，事实既可以是到达事件，也可以是匹配过程的中间状态，因此当 IF 表达式是多个事实的与时，P-Best 表达了 and 关系。表 1 给出典型检测语言的分类，如语言没有独立命名，本文用项目和系统名称代替。

表 1 典型检测语言的分类

表达能力 / 表示形式	[]	[then]	[then，or]	[then，and]	[then，and，or]
规则语言	Bro		Russel		P-BEST
自动机语言		Ustat	NetSTAT，Statl		Colored Petri-Net
高级语言	Snort		REE[17]	Musigs，Parsing Schema	Sutekh

结论 如何看待入侵或者说"聚焦"入侵哪些属性即入侵的本体论是入侵表示的最基本问题，本文研究看到目前还不存在一种对所有入侵有效的本体论。行为模型适合描述多阶段入侵，但对于简单入侵，人们只能依据安全专家的经验获取行为模式；检测慢扫描一类的入侵一直是传统 IDS(行为模式)的困难问题，但 IP 陷阱技术可以轻松地发现异常并且准确度高，问题是 IP 陷阱对有针对性的入侵无能为力。同样 TTL 语言适合描述时间区间特征，但它表示瞬时事件及其关系过于复杂，不适合作为入侵检测应用的统一语言。因此我们可能不应该期望一种表示技术刻画所有的攻击现象，而是应该探讨如何将入侵分类以及为每类入侵寻找最合适的表示技术，探讨分布和集成多种表示技术的方法。

从表 1 我们还看出，面向入侵行为模式表示的检测语言在二十多年的发展中实践上已经趋于成熟，但理论上还非常欠缺，表 1 中没有一种语言充分地说明其完备性和有效性。在目前成果的基础上，人们有可能并且也很需要一种评估方法，该方法不仅有助于为不同的应用环境寻找最好的检测语言；而且其研究可揭示现有检测语言的不足，促进新的检测语言的出现，这对于标准化工作的需求分析是十分有益的。

参 考 文 献

1 CERT Coordination Center. CERT/CC Statistics. http://www.cert.org/stats，2004

2 McHugh J. Intrusion and intrusion detection. International Journal of Information security，July 2001

3 Axelsson S. Intrusion detection systems：a survey and taxonomy. http://citeseer.nj.nec.com/axelsson00intrusion.html，2000

4 Davis R，Shrobe H，Szolovits P. What is a knowledge representation? . AI Magazine，1993，14(1)：17～33

5 Commision of the European Communities. Information Technology Security Evaluation Criteria，Version 1.2 . June 1991

6 Ulf Lindqvist，Porras P A. Detecting computer and network misuse through the production-based expert system toolset (P-BEST). In：Proc. of the 1999 IEEE Symposium on Security and Privacy，1999. http://www.sdl.sri.com/emerald/pbest-sp99-cr.pdf

7 Habra B，Charlier L，Mounji A，Mathieu I. ASAX：software architecture and rule-based language for universal audit trail analysis. In：Proc of (ESORRICS) '92. Springer-Verlag，1992. 435～450

8 Paxson V. Bro：a system for detecting network intruders in real-time. Computer Networks，1999，31(23-24)：2435～2463

9 Ilgun K. USTAT：a real-time intrusion detection system for UNIX：[Master's thesis]. Computer Science Dept.，University of California，Santa Barbara，USA，1992

10 Vigna G，Kemmerer R A. NetSTAT：a network-based intrusion detection system. Journal of Computer Security，1999，7(1)：37～71

11 Vigna G，Echmann S T，Kemmerer R A. STATL：an attack language for state-based intrusion detection. Dept. of Computer Science University of California Santa Barbara，2000

12 Kumar S. Classification and detection of computer intrusions：[PhD thesis]. Dept. of Computer Science，Purdue University，USA，1995

13 Lin J-L，Wang X S，Jajodia S. Abstraction-based misuse detection：high-level specifications and adaptable strategies. In：Proc. of the 11th Computer Security Foundations Workshop，Rockport，MA，1998. 190～201

14 Roger M，Goubault-Larrecq J. Log auditing through model checking. In：Proc. of the 14th IEEE Computer Security Foundations Workshop (CSFW'01)，2001. 220～236

15 Pouzol，Mireille Ducass'e pouzol. Formal specification of intrusion signatures and detection rules. In：Proc. of the 15th IEEE Computer Security Foundations Workshop(CSFW)，2002

16 Pouzol J-P，Ducasse M. From declarative signatures to misuse IDS. In：Proc. of the RAID Intl. Symposium，Davis，CA，2001，2212：1～21

17 Sekar R，Uppuluri P. Synthesizing fast intrusion prevention/detection systems from high-level specifications. In：Proc. of 8th USENIX Security Symposium，1999

18 Cuppens F. Ortalo R. Lambda：a language to model a database for detection of attacks. In：Proc. of the third Intl. Workshop on the Recent Advances in Intrusion Detection(RAID'2000)，Oct. 2000

19 Schneier B. Attack Trees. Secrets and Lies. John Wiley and Sons，New York，2000. 318～333

20 Tidwell T，Larson R，Fitch K，Hale J. Modeling internet attacks. In：Proc. of the 2001 IEEE Workshop on Information Assurance and Security，United States Military Academy，West point，NY，

June 2001
21 Daley K, Larson R, Dawkins J. A structural framework for modeling multi-stage network attacks. In: Proc. of the intl. Conf. on Parallel Processing Workshops, 2002
22 Templeton S J, Levit K. A requires/provides model for computer attacks. In: Proc of New Security Paradigms Workshop, Sept. 2000. 31～38
23 Cuppens F. Managing alerts in a multi-intrusion detection environment. In: 17th Annual computer security applications conf. (ACSAC), New-Orleans, Dec. 2001
24 Cuppens F. Alert correlatin in a cooperative intrusion detection framework. In: Proc. of IEEE Symposium on Security and Privacy, 2002. 187～200
25 Debar H, Wespi A. Aggregation and correlation of intrusion-detection alerts. In Recent Advances in Intrusion Detection, number 2212 in Lecture Notes in Computer Science, 2001. 85～103
26 Ning P, Reeves D, Cui Y. Correlating alerts using prerequisites of intrusions: [Technical Report TR-2001－13]. North Carolina State University, Department of Computer Science, Dece. 2001
27 Ning P, Cui Y, Reeves D S. Constructing attack scenarios through correlation of intrusion alerts. In: Proc. of the 9th ACM Conf. on Computer and Communications Security (to appear), Washington, D. C., Nov. 2002
28 Ning P, Cui Y. An intrusion alert correlator based on prerequisites of intrusions. Submitted for publication: [Technical Report TR-2002-01]. Department of Computer Science, North Carolina State University, Jan. 2002
29 Staniford-Chen S, Crawford C R, Dilger M, et al. GrIDS－a graph based intrusion detection system for large networks. In: Proc. of the 20th National Information Systems Security Conf. 1996, 1: 361～370
30 Chen Shuo, An Chang-Qing, Li Xue-Nong. A Distributed Intrusion Detection System and Its Apperception ability. China Journal of Software, 2001, 12(2): 225～232
31 Doyle J, Kohane I, Long W, Shrobe H, Szolovits P. Event recognition beyond signature and anomaly. In: Proc. of the 2001 IEEE. Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, June 2001

(上接第 45 页)

其它站没有机会接入进行通信。为了避免这种不足而提出了一个概念——最大占用周期。每次连接只允许传输最多 M 个数据分组，如果已经交换了 M 个数据分组，则不管还有多少个分组要送都必须要终止连接。除了能避免这种不足之外，这种策略还能提供 DCH 信道预留周期的计算，而信道预留周期在决定忙 DCH 变成空闲的时间是很关键的。M 的取值由具体的网络性能决定。

4 初步仿真

我们先对 IEEE 802.11b 单信道协议进行仿真研究，仿真参数如表 1 所示，所有站都产生数据流，为仿出不同网络负载，平均间隔时间是变化的而分组长度保持不变，吞吐量也可通过信道容量刻画出来。

表 1 802.11b 仿真参数

参数	值
分组长度(字节)	常量(500)
分组间隔到达时间	指数的
目的站地址	随机
RTS/CTS	永远
信道容量	1Mbps
物理层特性	PHSS

其仿真结果如图 3 所示，当网络大小从 2 站增加到 20 站时，可看出网络的吞吐量逐渐降低直到网络满负荷。

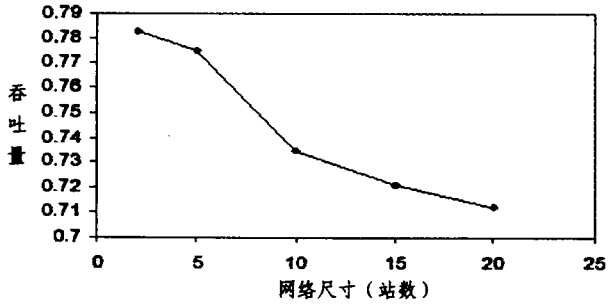

图 3 802.11b 的性能仿真结果图

接下来是对本文提出的协议进行仿真，其仿真参数如表 2 所示。其仿真结果如图 4 所示。

结论 与单信道 MAC 协议相比较而言，使用多信道的负载均衡 MAC 协议能提供同时多个信道的交叉连接从而提高了信道的利用率，并能通过负载平衡来更好地利用资源。在本文提出来基于信道均衡的动态多信道 MAC 协议中，在网络中使用了多信道技术，且信道的预约使用是动态的，在需要传数据时动态地选择空闲信道来传数据，选择信道是基于信道接收功率最大原则从而解决了信道均衡问题，初步仿真结果表明在网络负荷增加时比单信道 MAC 协议有更高的吞吐量，性能更好。

表 2 协议仿真参数

参数	值
网络大小	20 个站
分组长度(字节)	常量(500)
分组间隔到达时间	指数的
目的站地址	随机
最大允许连接大小	5 个分组
每个子信道容量	1Mbps
每个站的数据端口数	1
物理层特性	PHSS

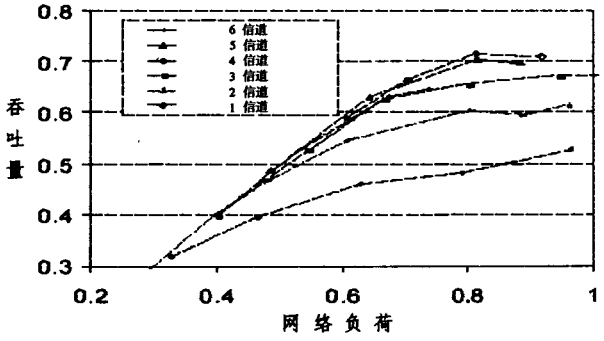

图 4 协议性能仿真图

参考文献

1 IETF. Mobile ad hoc networks charter. http://www.ietf.org/html.charters/manet-charter.html
2 Li Jiandong, Haas Z J, Sheng Min. Capacity evaluation of multi-channel multi-hop ad hoc networks. In: 2002 IEEE Intl. Conf. on Personal Wireless Communications, Dec. 2002. 211～214
3 何一，李伟光，陈迎春. 软件无线电在自组网动态物理层中的应用. 现代电子技术，2002(8): 36～39
4 IEEE Standard 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications[S]. 1999