基于时空约束的IDS系统能力评估方法[1]

杨望 [1,2] 龚俭 [1,2]

（[1] 东南大学计算机科学与工程学院，江苏 南京 210096）

（[2] 江苏省计算机网络技术重点实验室 江苏 南京 210096）

摘要：传统的评估方法在尽管在评估 IDS 具体攻击的检测效果上有重要作用，但由于其在评估对象、评估测试案例生成和评估测度上的缺陷，无法完备地对 IDS 进行测试，获得公平、合理和准确的评估结果。本文提出了基于时空约束的评估方法，把承载攻击的报文序列作为描述 IDS 检测能力的基础，通过时空约束及其对应的内容约束对 IDS 的检测能力空间进行等价划分，完善基于分辨率方法提出的系统能力测度体系，提高了入侵检测系统评估结果的公平性、合理性和准确性。

关键字：网络入侵检测系统 评估 系统能力 等价划分

中图分类号: TP393. 2 文献标识码: A

Spatial-Temporal Restrain based IDS System Capacity Evaluation Method

Yang Wang[1,2], Gong Jian[1,2]

([1]. School of Computer Science and Technology, Southeast University, Nanjing 210096, China;)

([2]. Key Laboratory of Computer Network Technology of Jiangsu Provincial, Nanjing 210096, China)

Abstract: Although the conventional IDS evaluation method is important for IDS in the assessment of specific attack detection effect, It can't fulfill the request of fair,reasonable and accurate IDS evaluation because of its Deficiency in evaluation object, test case generation and evaluation metric. This paper propose a t Spatial-Temporal Restrain based IDS System Capacity Evaluation Method, which use the packets sequence carrying the attack as the base of describing the ability of the IDS detection. The method use Spatial-Temporal restrain and content restrain to equivalent partition the IDS detection capacity, and improve the intrusion detection system evaluation results's fairness, reasonableness and accuracy.

Keyword: NIDS, Evaluation, system capacity, Equivalence partition

随着入侵检测技术的不断发展，IDS(Intrusion Detection System)已经成为网络安全防御体系中必备的一环，而对IDS评估的需求也不断增长。在IDS评估过程中，研究者对IDS基于各类测度进行测试，发现影响IDS检测精度的原因，提高IDS系统的检测率，降低误报率。

现有评估方法分为两类。一类以IDS及其规则为评估对象，以真实攻击为测试案例。这类评估方法可以评估IDS及其配置规则对当前部分攻击的检测能力，另一类仅以IDS本身为评估对象，根据软件等价测试原则对IDS的系统能力生成测试案例。本文分析了现有两类评估方法在测试方法、测度选择上的不足，对基于系统能力的评估方法【1】进行了改进，使用时空约束定义系统能力评估的测度，并在新测度的基础上提出系统能力覆盖率和系统能力正确性两种等级的评估方法。新方法的评估测度对IDS具有更好的描述能力，并有更广泛的适用范围。

本文的结构如下，第 1 节介绍目前评估方法的工作，指出目前各类评估方法中的不足；第 2 节讨论了系统能力的测度所需要具有的性质，并基于系统能力讨论了评估测度，提出了基于时空约束的测度描述方法；第 3 节介绍了基于时空约束的 IDS 系统能力评估方法；第 4 节对 Snort【2】、Bro【3】、Rishi【4】三种不同的入侵检测系统应用不同的评估方法进行评估，通过对比评估结果说明新的基于时空约束的评估方法相对于传统评估方法的优点，第 5 节是结论和未来的工作。

基金项目：1本文受国家十一五科技支撑计划课题（2008BAH37B04）资助。

作者简介：杨望（联系人），男，讲师，wyang@njnet.edu.cn；龚俭(1957-)，男，教授，博士生导师。

1 目前评估方法的问题

目前的评估方法可以分为两类，一类是传统方法，一类是基于系统能力的方法。传统方法的特点是将IDS 的实现和规则作为一个整体进行评估，并且尽量使用真实攻击作为测试案例。基于系统能力的方法则将 IDS 自身作为评估对象，不追求使用真实攻击，而使用能达到分区测试(partition testing)效果的案例作为测试案例。

1.1 传统评估方法

自 1995 年 PUKETZA[5]等人开始 IDS 评估的研究工作，目前的大多数评估方法，不论是麻省理工学院的林肯实验室(Massachusetts Institute of technology/Lincoln Lab, 后文简称为MIT/LL)进行的通用目的IDS 评估[6]，还是 Massicotte[7]、Sommer[8]等人进行的专门目标的 IDS 评估，都是传统评估方法。传统方法的第一个特点是将 IDS 的实现和规则作为一个整体进行评估，孙美凤在文献[1]中指出由于 IDS 各自定义所使用的检测规则，并且在定义之后，规则及其数量还可能变化，所以 IDS 在评估时表现出的检测能力与实际运行中表现出的能力可能不同，这就失去了评估的意义。传统的评估方法的第二个特点是着重于真实攻击的模拟。不论是以 MIT/LL 为代表的研究性评估还是以 NSS 实验室[9]为代表的商业评估，尽管攻击分类和生成方法不同，其目标都是模拟出更多类型真实的攻击，这种强调使用真实攻击的方法类似于软件测试中的随机测试，其测试结果不能应用在 IDS 对其他已知攻击以及未知攻击的检测能力评估上，是一种测试效率低且测试范围极其有限的测试评估方法。尽管传统 IDS 评估方法有其局限性，但仍有它存在的必要性，特别是对于商用 IDS。

1.2 基于系统能力的评估方法

因为传统 IDS 评估方法的局限，研究者又提出了基于系统能力的评估方法。Alessandri 首先给出的基于攻击分类的比较分析方法[10][11]。这种方法利用统一的 IDS 描述框架(Scheme)分别描述攻击类型和 IDS。攻击的分类基于攻击可被观察的属性，并且要满足等价划分的要求，因此分析结果对某一类的所有攻击有效。但是 Alessandri 分类的目标是用于 IDS 设计，并未考虑该方法在 IDS 评估上的可操作性。

文献[1]正式提出了系统能力的概念，提出检测能力由2个因素决定：入侵特征的描述能力和IDS的系统能力，并指出描述能力取决于规则开发者和IDS的管理员，而系统能力才是IDS本身所固有的属性。同时文献[1]中还提出了基于分辨率的系统能力评估方法，以区分了IDS的本身的质量和规则的质量，反映出IDS表现出的以及潜在的检测能力，让研究者可以获得更准确的IDS的能力描述。但是该评估方法仍存在一些不足。首先基于分辨率的系统能力评估方法虽然提出了用户行为分辨率的概念，但没有给出用户行为分辨率的测度评估实现方法。其次，文献[1]提出的入侵特征分辨率模型过于粗疏，无法体现IDS之间的差异。最后，基于分辨率的方法不规定任何特定的实现技术，以IDS抽象模型为讨论基础。这样虽然不失一般性，并降低了评估的复杂度，但忽视了一个问题：由于系统实现的不同，即使是同样的功能在不同的IDS实现会有不同的效率和效果。

综上所述，基于分辨率的系统能力评估方法尽管已经选取了合适的评估对象，但现有的评估方法的测度体系不够完整，在特征分辨率和行为分辨率下不足以区分不同 IDS 的能力；同时评估方法只注重了 IDS 对不同功能的覆盖率，忽视了不同 IDS 在同一能力下的实现正确度的不同。本文将在基于分辨率的系统能力评估方法基础上加入新的测度体系和评估方法来弥补原有方法的不足。

2 基于时空约束的系统能力测度

本节将首先讨论 IDS 评估中的测度需要具有的基本性质，再从报文序列的时空约束角度上定义新的测度体系来完善原有的分辨率体系，最后说明新测度具有 2.1 节所列出的各类性质。

2.1 评估测度的性质

IDS 的评估测度应该具备以下性质：

1） 可测性。测度必须是可以通过测试过程获得的，不可测的测度是无意义的。文献[10]中的评估方法未考虑其测度的可测性使其无法应用于 IDS 评估过程，文献[1]中的用户行为分辨率测度不具备可

测性也削弱了基于分辨率的评估方法的可用性。

2） 可扩展性。攻击是一个开放的体系，新的攻击形式和方法不断的出现，测度体系必须在攻击发展的情况下能够通过自我修订过程继续有效地评估 IDS 的检测能力。如果存在测度无法描述的检测能力，则在评估该检测能力时评估方法就会失效。

3） 公平性。测度不可对被测系统产生偏好性。

4） 等价划分性。测度能够达到对攻击空间等价划分的效果。如果测度描述的检测能力没有等价划分的效果，则评估仍会是随机测试的效果。在等价划分的性质下，即使出现的新的攻击，只要攻击所对应的检测能力仍是原有的，评估结果就可以继续使用，使评估不会因为攻击的更新而失效。

2.2 基于时空约束的评估测度

尽管攻击的技术手段在不断变化，攻击的种类根据攻击的目的、方式有众多的种类，但攻击在网络中的时空表现形式是有限的，文献[1]中也指出攻击是发生在特定时间和空间范围内的行为序列。无论针对什么样的漏洞，攻击总包含在一定时间和空间内的报文序列,攻击的逃逸技术也可以看成对原有攻击报文序列在时间和空间上的改变。报文序列最基本的组成元素是单报文，单报文可以看作没有时间约束和空间约束的报文序列，即 0 阶时空约束报文序列 。对单报文施加不同的时间约束和空间约束，则可以得到各种不同类型的流，即 1 阶时空约束报文序列。如果对流进行进一步的时间和空间约束就可以得到聚合流，即 2 阶时空约束报文序列 ，依此类推可以得到 n 阶时空约束报文序列。

下面给出**时空约束报文序列的形式化定义**：

RS 和 RT 是作用于报文序列 S 上的空间和时间关系约束。

0 阶报文序列 s^0 是单报文。

1 阶报文序列 s^1 是 0 阶报文序列 s^0 的集合且该集合中的每一个元素 s_i^0 满足空间关系约束 r_s 和时间关系约束 r_t，即 $s^1=\{s_i^0 \mid RS(s_1^0,\cdots,s_n^0)=r_s, RT(s_1^0,\cdots,s_n^0)=r_t, 1\le i\le n\}$

n 阶报文序列 S^n 是 *n-1* 阶报文序列 s^{n-1} 的集合且该集合中的每一个元素 s_i^{n-1} 满足空间约束 r_s 和时间约束 r_t，即 $s^n=\{s_i^{n-1} \mid RS(s_1^{n-1},\cdots,s_n^{n-1})=r_s, RT(s_1^{n-1},\cdots,s_n^{n-1})=r_t, 1\le i\le n\}$

在时空约束报文序列的描述空间下，IDS 对攻击的检测能力具有以下两条性质：

性质 1：如果 IDS 具有检测某种 *n* 阶时空约束报文序列的能力，则该 IDS 一定能够检测该 *n* 阶时空约束报文序列所需要的 *n-1* 阶直到 0 阶时空约束报文序列的能力。

性质 2：如果 IDS 只具备检测 *n-1* 阶时空约束报文序列的能力，则 IDS 无法准确检测需要 *n* 阶时空约束下才能表达的攻击。

文献[12]中定义的基于对象的多阶段入侵特征表示框架 OBDL （Object-Based Detection Language）支持完备时间和空间关系约束运算。本文中的具体时间和空间约束将使用 OBDL 语言来描述。表 1 和表 2 列出了使用了 OBDL 描述的常用 1 阶时空约束和 2 阶时空约束报文序列类型。

表 1 常用 1 阶时空约束报文序列类型

常用 1 阶时空约束	时间关系约束 r_t	空间关系约束 r_s
分片报文序列约束	{(S^0_i.time – S^0_{i-1}.time) < timeout, 1<i<=n}	{(S^0_i.ip.src=S^0_{i-1}.ip.src， S^0_i.ip.dst=S^0_{i-1}.ip.dst), (S^0_i.ip.id=S^0_{i-1}.ip.id), 1<i<=n}
IP 单向流报文序列约束	{(S^0_i.time – S^0_{i-1}.time) < timeout, 1<i<=n}	{(S^0_i.ip.src=S^0_{i-1}.ip.src, S^0_i.ip.dst=S^0_{i-1}.ip.dst), 1<i<=n}

表 2 常用 2 阶时空约束报文序列类型

常用 2 阶约束类别	时间关系约束 r_t	空间关系约束 r_s
源 IP 聚合 TCP	{(S^1_i.time –S^1_{i-1}.time) < timeout, 1<i<=n}	{(S^1_i.sip= S^1_{i-1}.sip， 1<i<=n}

单向流		
宿端口 TCP 单向聚合流	{(S^1_i.time –S^1_{i-1}.time) < timeout, 1<i<=n}	{(S^1_i.dport= S^1_{i-1}.dport，1<i<=n}

2.3 内容约束的定义

内容约束和每一种类型的时空约束报文序列类型相关，不同阶或者同阶不同约束参数的时空约束报文序列的内容约束测度都可能不同。例如 0 阶时空约束报文序列的内容约束测度包括对各种类型报文头部、原始负载以及各种类型应用负载的约束能力，1 阶时空约束报文序列则会产生各种流相关的测度，如流报文数、流字节数、流持续时间等等，高阶测度在产生新测度的同时也会失去部分低阶测度，例如 2 阶时空约束报文序列不再拥有应用负载相关的测度。

表 3 内容约束测度

时空约束类别	内容约束测度
0 阶时空约束报文序列	IP 头部 IPv6 头部 TCP 头部 UDP 头部 ICMP 头部 ICMPv6 头部…
	原始负载
	HTTP 负载 FTP 负载 IRC 负载…HTTP 编码负载…
1 阶时空约束报文序列	HTTP 负载 FTP 负载 IRC 负载…HTTP 编码负载…
	IP 流头部 TCP 流头部 UDP 流头部

3 基于时空约束的 IDS 系统能力评估方法

与传统评估不同，系统能力评估必须根据评估目标选定时空约束和对应的内容约束组合测度的集合，在完成测度的选择后，再为组合测度的集合生成测试案例集合进行测试。完全准确的评估 IDS 检测能力是一项耗费资源的工作。为了更有效的利用测试资源，在不同的测试需求和条件下，可以放宽或严格测试约束，获得不同粒度的评估结果。本文提出基于时空约束的系统能力评估方法，以完成对系统能力覆盖性的评估要求为目标，如果要求更严格的评估能力，则可以在覆盖率评估的基础上进行进一步的评估。

系统能力的覆盖率评估假定：对于某一类型时空约束报文序列的检测能力，一个 IDS 要么没有实现，要么正确实现。系统能力覆盖率评估的目的是获得 IDS 的实现功能在环境需要的系统能力的各个测度上的覆盖情况，以解释 IDS 对环境需求能力的满足度。如果需要横向对比不同 IDS 的检测能力，则可以通过对测度集合的评估结果进行加权计算 IDS 综合覆盖率进行比较。在覆盖率评估中：如果一个 IDS 的实现缺陷导致评估过程中 IDS 的系统能力被视为未实现，将和 IDS 未实现该系统能力等同处理。覆盖率评估给出一个 IDS 系统能力的粗粒度视图，每个组合测度的结果都用布尔型表示，可以用于对 IDS 设计效果的评估。

和传统评估方法不同，系统能力评估中必须告知被测 IDS 必要的检测知识，让被测 IDS 根据测试信息对系统进行配置，因此存在被测 IDS 使用作弊技术来完成评估目标的可能性。为了防止 IDS 使用作弊技术通过评估，需要引入证伪测试案例。证伪案例的作用是证明 IDS 没有实现某种功能，证伪案例有优先于普通案例的判定标准。

系统能力覆盖率评估测试方法的伪算法如下：

设评估的时空约束和内容约束组合测度集合为$\{(r_i, c_i) \mid 1 \le i \le n\}$，$a_i$ 是(r_i, c_i)对应的检测能力的评估结果。

对所有(r_i, c_i)属于$\{(r_i, c_i) \mid 1 \le i \le n\}$，执行

{

（1）从样本集中随机选取对应的测试样本 $case_i$

（2）对 $case_i$ 根据时空测度类型选取对应算法生成证伪案例 $tfcase_i$

（3）对被测系统测试 $tfcase_i$：

（4）如果 $tfcase_i$ 测试结果为 IDS 有报警，说明 IDS 有作弊行为，IDS 对(r_i, c_i)测度无检测能力，$a_i = 0$。

（5）如果 $tfcase_i$ 测试结果为 IDS 无报警，则对被测系统测试 $case_i$。

（6）如果 $case_i$ 测试结果为 IDS 有报警，说明 IDS 对 (r_i, c_i) 测度有检测能力，$a_i = 1$；如果 $case_i$ 测试结果为 IDS 没有报警，则 IDS 对 (r_i, c_i) 测度无检测能力，$a_i = 0$。

}

评估过程结束。

如果需要计算综合覆盖率，则需要对 $\{(r_i, c_i) | 1 \le i \le n\}$ 的测试结果进行加权规格化计算。设 f_i 是 (r_i, c_i) 对应的检测能力相对于评估目标的权重值。则 IDS 的综合覆盖率 C_{cov} 的计算公式为：$C_{\text{cov}} = \dfrac{\sum_{i=1}^{n} f_i a_i}{\sum_{i=1}^{n} f_i}$。当 C_{cov} 为 1，表示 IDS 实现了对所有测度的检测能力；当 C_{cov} 为 0，表示 IDS 对所有测度的检测能力都没有实现。如果 IDS 实现了部分测度的检测能力，则 C_{cov} 在 0 和 1 之间。当 IDS 实现了相同数量的测度时，实现测度权重高的 IDS 的 C_{cov} 更高。

4 实验

4.1 传统评估方法

MIT/LL 在 98/99 年进行的两次离线评估数据是目前传统评估方法唯一公认的测试数据集，本节实验从 MIT/LL 99 年离线评估的测试数据中选取第 4 周 1 日的测试流量作为测试数据。被测试三种 IDS 均是基于滥用检测的 IDS，所以 MIT/LL 中的训练过程被省略。Snort 的非报文规则使用 2.6.14 安装后的缺省配置，报文规则使用 2007 年 3 月 22 日的版本；Bro 的非报文特征规则使用 1.2.1 版安装后的缺省规则，报文特征规则使用 Bro 提供的 Snort2Bro 程序从 Snort 的规则进行翻译；Rishi 的所有规则使用 0.96 版安装后的缺省配置。传统评估方法中 IDS 事先无法得知被测试的攻击类型，所以各 IDS 的缺省规则均不进行裁剪，使用完整的规则集。下图是根据检测率和误报率得出的评估结果：

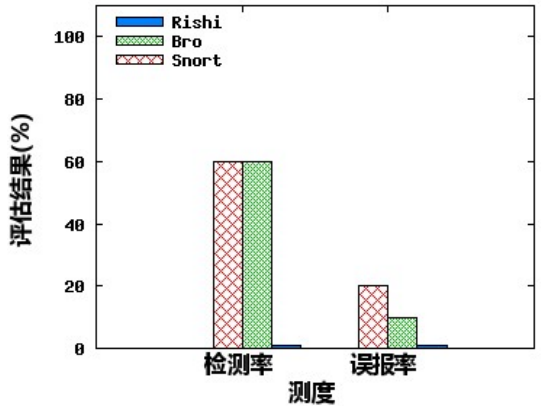

图 1 传统评估方法的评估结果

从图 1 中可以看出 Snort 和 Bro 有相似的检测率，而 Bro 的误报率要好于 Snort，Rishi 的检测率为 0 而误报率也为 0。但传统方法无法说明导致该测试结论的原因是来源于 IDS 的设计、实现还是配置，除了实验中的攻击外，该评估结论也无法说明 IDS 对其他实验中未出现的攻击的检测能力。因此传统评估方法只能给出 IDS 及其缺省规则对 MIT/LL 99 测试案例中攻击的检测效果。

4.2 基于分辨率的系统能力评估方法

基于分辨率的系统能力评估方法的测试案例按照文献[1]和[15]中提出的算法进行构造。基于分辨率的方法会告知被测系统检测测试集必备的知识，所以 Snort、Bro 和 Rishi 系统分别根据测试集提供的知识配置相应的规则，其中 Bro 报文特征规则使用 Bro 提供的 Snort2Bro 程序从 Snort 的报文规则进行翻译。Snort、Bro 和 Rishi 的测试结果如表 4 所示：

表 4 基于分辨率方法的评估结果

测度	Snort	Bro	Rishi
操作分辨率	1 （支持对入侵过程的单个正向事件）	3 （支持入侵过程的正向和反向事件）	1 （支持对入侵过程的单个正向事件）
时间分辨率	0 （不支持时间维的特征）	2 （支持多事件的时间区间长度约束）	0 （不支持时间维的特征）
空间分辨率	0 （不支持空间维的特征）	1 （支持多事件的空间关系约束）	0 （不支持空间维的特征）

从表 4 的评估结果可以看出，在各维分辨率测度上 Bro 的检测能力要强于 Snort 和 Rishi，而 Snort 和 Rishi 的检测能力相同。相对于传统方法，评估结果中不仅说明 Bro 的检测能力强于 Snort 和 Rishi 系统，而且说明 Bro 在哪些检测能力上强于 Snort 和 Rishi 系统。但是基于分辨率的评估方法的结论仍然粗疏，表 4 给出的评估结果中 Snort 和 Rishi 的检测能力相同，而实际 Snort 和 Rishi 的检测能力有很大差异，而分辨率测度无法描述出这种差别。

4.3 基于时空约束的系统能力评估方法

3.2 节中指出主要的攻击形式可以用 0 阶到 2 阶之间的时空约束来描述。本文的实验采用 0 阶到 2 阶的中最重要的部分时空约束能力来进行实验。表 5 给出了用于测试的 0 阶到 2 阶的时空约束及其对应的内容约束组合测度。在进行各 IDS 检测能力规格化计算时分两种情况：1）各测度的权重都为 1，此种情况下各测度对安全目标的贡献相同；2）负载相关的测度的权重高于其他测度，即负载测度相关的检测能力对安全目标更重要。

表 5 实验所用各阶时空约束报文序列组合测度列表

时空约束	时空约束测度	内容约束测度
0 阶时空约束报文序列	单报文	IP 头部 IPv6 头部 TCP 头部 UDP 头部 ICMP 头部 ICMPv6 头部
		原始负载
		HTTP 负载 IRC 负载
1 阶时空约束报文序列	IP 单向流 TCP 单向流 TCP 单向乱序流	HTTP 负载 HTTP 编码负载 IRC 负载
		流 IP 统计信息
2 阶时空约束报文序列	源 IP 聚合 TCP 单向流 宿 IP 聚合 TCP 单向流 宿端口聚 TCP 单向合流	流 IP 统计信息

根据第 3 节的算法对测度集合生成测试案例和证伪案例，对 Snort、Bro 以及 Rishi 系统根据测试案例集配置相应的规则，Bro 报文特征规则使用 Bro 提供的 Snort2Bro 程序从 Snort 的规则进行翻译。因篇幅所限只给出 0 阶测度评估结果的细节，Snort、Bro 和 Rishi 的测试结果如图 2 所示：(下表中 S 代表 Snort,B 代表 Bro，R 代表 Rishi)：

表 6 0 阶时空约束及其内容约束组合测度

内容约束	IPv4 头部	IPv6 头部	TCP 头部	UDP 头部	ICMP 头部	ICMPv6 头部	原始负载	HTTP 负载	IRC 负载
单报文	S：1 B：1 R：1	S：1 B：1 R：0	S：1 B：1 R：1	S：1 B：1 R：0	S：1 B：1 R：0	S：1 B：1 R：0	S：1 B：1 R：1	S：1 B：1 R：1	S：1 B：1 R：1

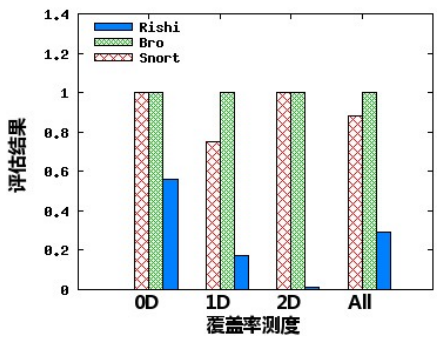

图 2 综合覆盖率测度比较结果(权重相同)

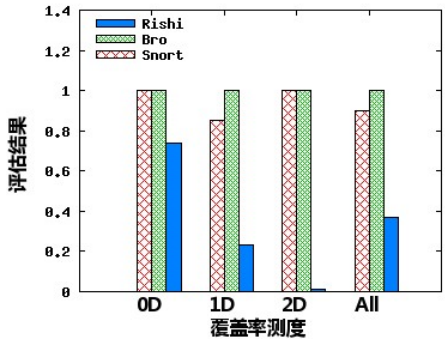

图 2 综合覆盖率测度比较结果(权重不同)

在基于时空约束的系统能力覆盖率评估中，可以看出 Bro 对表 5 给出的测度集合有最强的检测能力，Snort 次之，Rishi 的检测能力最弱。基于时空约束的系统能力评估不仅给出了各个 IDS 检测能力的强弱，并且根据 IDS 所能检测时空约束测度范围说明了这种强弱的原因，并且能更准确地说明 IDS 的实际检测能力。从表 6 中可以看出 Rishi 只具备对 0 阶和 1 阶时空约束报文序列下部分负载类内容约束的检测能力，Snort 和 Bro 具有相近的 0 阶和 2 阶时空约束报文序列下的各种内容约束对应的检测能力，但 Snort 的 1 阶时空报文序列下检测能力弱于 Bro

5 结论

传统的评估方法在尽管在评估 IDS 对具体攻击的检测效果上有重要的作用，但由于其在评估对象、评估测试案例生成以及评估测度上的缺陷无法满足 IDS 研究者的需要；基于分辨率的系统能力评估方法考虑 IDS 的系统能力，能够有效的区分 IDS 实现和配置的不同，但其测度体系尚不完善，评估结果失之粗疏。基于时空约束的评估方法把承载攻击的报文序列作为描述 IDS 检测能力的基础，通过时空约束及其对应的内容约束对 IDS 的检测能力空间进行等价划分，完善了基于分辨率方法提出的系统能力测度体系。公平性、准确性。

参考文献(Refserences)

[1] 孙美凤, 龚俭, 杨望. 基于特征的入侵检测系统的评估新方法[J]. 通信学报, 2008, 28 (11):6-14
Sun meifeng, Gong Jian, Yang Wang. New approach to evaluate the capacity of signature-based intrusion detection systems[J] Journal of Communicatios, 2008 28(11):6-14

[2] Snort 2.6.14[EB/OL] http://www.snort.org/. 2008

[3] Bro 1.3.0[EB/OL] http://www.bro-ids.org/ 2008

[4] Jan Goebel, Thorsten Holz. Rishi: identify bot contaminated hosts by IRC nickname evaluation[C]. Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, p.8-8, April 10, 2007, Cambridge, MA

[5] PUKETZA N J. A methodology for testing intrusion detection system[J]. IEEE Trans on Software Engineering,1996,22(10):719-729.

[6] Haines, J, Lippmann, R, Fried, D. Design and Procedures of the 1999 DARPA Intrusion Detection Evaluation: Design and Procedures[R], MIT Lincoln Laboratory, 2001.

[7] Frederic Massicotte; Francois Gagnon; Yvan Labiche; Lionel Briand; Mathieu Couture, "Automatic Evaluation of Intrusion Detection Systems"[C], Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual , pp.361-370, Dec. 2006, Florida, USA

[8] Sommers J, Yegneswaran V, Barford P. Toward Comprehensive Traffic Generation for Online IDS Evaluation[R]. UW Technical Report, August, 2005.

[9] NSS Group. Intrusion Prevention Systems Group Test (Edition 5)[R]. NSS Group, 2008.

[10] Dominique Alessandri. Attack-Class-Based Analysis of Intrusion Detection Systems[D] University of Newcastle. May 2004

[11] ALESSANDRI, D. 2000. Using rule-based activity descriptions to evaluate intrusion-detection systems.[C] In RAID2000, H. Debar, L. Me, and S. F. Wu, Eds. Springer-Verlag, New York, NY, 183–196.

[12] 孙美凤. 滥用入侵检测系统中入侵表示的研究[D] 东南大学. 2007
Sun Meifeng. INTRUSION REPRESENTATION IN MISUSE-BASED INTRUSION DETECTION SYSTEM[D] Southeast University. 2007