基于 OpenFlow 的入侵检测评估模型①

廖大强, 郑海清

(南华工商学院, 广州 510507)

摘 要: 针对传统测评方法依赖模拟环境来仿真真实网络流量的现状, 提出一种基于 OpenFlow 的入侵检测评估系统. 该系统基于软件定义网络技术(OpenFlow)的入侵检测评估模型,随后对该模型的框架、设置方法、具体工作过程等进行详细阐述, 设计了基于该模型的测评系统, 该系统利用 OpenFlow 灵活的网络控制能力为 IDS 测评搭建真实可控的网络环境, 提供入侵检测所需的真实网络流量和攻击数据. 最后利用该测评系统对该模型进行试验仿真,实验结果表明传统方法相比, 本文提出的基于OpenFlow的入侵检测评估模型在测评效果和准确性上有较好的性能.

关键词: IDS 评估; OpenFlow; 入侵检测; 评估模型

Evaluation Model of Intrusion Detection Based on OpenFlow

LIAO Da-Qiang, ZHENG Hai-Qing

(Nanhua College of Industry and Commerce, Guangzhou 510507, China)

Abstract: The traditional evaluation methods rely on simulation environment to simulate real network traffic status quo, the proposed intrusion detection system is based on OpenFlow's assessment. The system is software-defined networking technology (OpenFlow) evaluation model based on the intrusion detection.We discussed the framework, setting methods, and specific work of this model in details. Our work designed an evaluation system based on this model, which uses a flexible network OpenFlow control structures for the evaluation of the true IDS controlled network environment, and provides the necessary intrusion detection and attack the real network traffic data. Finally, the evaluation system was used to test the simulation model. The experimental results show that compared to the traditional methods, the proposed OpenFlow intrusion detection model based on the evaluation can assess the effectiveness and accuracy of better performance.

Key words: IDS; OpenFlow; software defined network technology; evaluation model of intrusion detection based on OpenFlow

1 引言

入侵检测系统(Intrusion Detection Systems, 简写IDS)是网络安全中的一种重要防御系统, 是计算机安全体系重要组成部分,它可以对网络和计算机系统中的各种信息收集和分析, 找出计算机系统或者网络中不符合安全策略的行为, 记录下这种行为, 并及时报告给安全管理人员[1]. 因此,配置一个好的入侵检测系统对网络管理人员和网络安全运行都具有非常重要的意义, 目前, IDS 在网络安全中使用非常广泛.

入侵检测评估值的是对现有 IDS 的评价, 这些评价能为用户和 IDS 开发者提供一些理论依据, 是 IDS 发展不可或缺的部分, 但目前的市场甚至研究机构都比较少关注这个问题, 很难从市场或者专业机构获得某一IDS产品的专业评价[2]. 即使有, 也是很早之前开展的评价, 评价方法、技术手段都相对比较落后, 近几年的研究也很少. 主要原因是在目前的网络环境下, 因为网络的不可控致使 IDS 测评工作只能在仿真环境下进行, 而仿真环境下的研究工作早在 90 年代就已经

① 基金项目:广东省教育科学"十二五"规划 2013 年度教育信息技术研究项目(13JXN044)
收稿时间:2014-05-07;收到修改稿时间:2014-06-06

比较成熟, 以后就一直没有重大突破[3]. 另外仿真环境下的评估工作存在很多的问题, 也一直没有解决. 主要问题是: 网络流量仿真、用户行为仿真、攻击特征库的构建、评估环境的仿真实现以及测评结果的分析[4]. 仿真环境与实际环境相比具有很大的不同, 这些巨大的差异会导致入侵检测系统的评估在准确性、权威性、系统性方面存在不足, 说服力不大[5]. 因此, 要打破这一不足, 必须从另外角度出发, 单纯靠改进模拟环境, 健全模拟数据, 改进测评算法等方面着手是不行的, 必须另辟蹊径, 找到新的解决方法. 其中仿真环境是核心, 如果能打破传统的基于仿真环境的测评技术, 而建立基于真实网络环境的测评技术, 很多关键问题都可以迎刃而解[6].

为此, 本文提出一种基于软件定义网络技术的入侵检测评估系统, 该系统利用 OpenFlow 灵活的网络控制能力为 IDS 测评搭建真实可控的网络环境, 提供入侵检测所需的真实网络流量和攻击数据. 近几年兴起的新技术 OpenFlow 具有强大的网络控制能力, 可以实现网络数据与实验数据的分析, 这为 IDS 评估提供真实的网络流量提供了可能, 从而改变了 IDS 评估的设计思路, 这将带动 IDS 评估方面更为广泛的学术探讨和新技术的实际应用, 具有重要的理论意义和实践应用价值.

2 传统入侵检测评估环境模型

2.1 研究现状

入侵检测系统对计算机系统和网络在安全方面的保障越来越受到从业人员的重视, 参差不齐的 IDS 被计算机安全爱好者以及厂商开发出来, 有的厂商甚至不具备入侵检测的功能也声称自己的产品如何先进. 面对种类繁多的入侵检测系统, 广大的非专业使用者却无从辨别. 所以, 迫切需要对 IDS 进行科学、公正和可信的测试和评估[7]. 入侵检测技术出现的时间不长, 相应的评估工作更是少见, 因此, 针对评估工作的研究会有各种各样的问题需要解决[8]: 评估数据的来源问题.

首先说网络中的正常流量, 看起来是最容易实现的, 但在测评的过程中, 正常的网络流量反而不容易获得, 原因有三, 第一, 正常的流量有的涉及商业或者敏感数据可能通过加密, 不可能拿给做研究; 第二, 不同网络流量大小不一, 有的很大很拥堵, 有的很小, 不同的流量对测评结果影响很大, NASS 集团的评估就是典型例子; 第三, 正常的网络流量不可控, 即使与企业愿意公布数据给用, 也能从技术上解决流量大小的影响, 也不能从网络中分析的实验数据和正常网络流量.

再来看攻击流量, 虽然网络中的攻击无处不在, 但是要把这部分攻击完全识别出来, 并作为评价标准显然是不行的, 有点贼喊捉贼的味道.

最后是用户行为, 用户行为是最让人捉摸不透的部分, 可以知道大部分人的绝大部分行为, 但是不可能知道小部分人的偶然性行为, 但这些小部分人的、偶然性的行为对测评却能产生很大的影响.

因此从上面分析可以看出测评中需要的数据如何得到是一个关键问题, 也是难点. 本文主要针对评估数据的来源问题展开研究, 解决评估中的数据来源问题, 并在此基础上提出的评估模型.

2.2 传统 IDS 评估方法和步骤

大部分的评估工作都要围绕着模型进行, 其具体步骤也相对比较固定. 主要过程如下[9]:

(1)准备好背景流量和攻击流量, 模拟正常使用网络过程中的各种行为, 一般以脚本或者工具的形式存放.

(2)确定 IDS 类型和安全级别, 比如基于主机的 IDS 还是基于网络的 IDS, 以及被测试网络或者主机的安全等级.

(3)在适当位置配置好 IDS.

(4)运行工具或者脚本, 产生网络行为.

(5)运行 IDS 平开始测评.

(6)产生评估报告.

2.3 传统 IDS 评估的数据源

理论情况下, 可以考虑使用下面三种方法生成评估数据[10]:

(1)抓取网络中的正常通信数据;

(2)抓取正常通讯数据并清除秘密信息后人为加入攻击;

(3)不使用网络中的正常通讯数据而是在测评网络中模拟重建正常通信和攻击数据.

在这三种方法中, 目前比较常用的是第三种, 主要是前两种方法在已有的评估环境中很难实现, 将网络中的正常流量作为评估数据的可行性很低, 没有企

业或机构愿意开发自己的数据，即使开放也需要先清除一些秘密信息，而这一工作几乎是不可能完成的[11]. 而第三种方法比较容易在实验室环境中就可以实现，所以是目前所有的 IDS 评估工作所采用评估数据.

2.4 传统 IDS 评估的环境配置与框架

评估 IDS 需要使用模拟的网络流量和攻击流量，把 IDS 放在实验环境下进行，而不是真实网络中进行，为此，需要专门构架一个测评用的网络. 这个网络的基本配置包括: IDS、IDS 保护系统、攻击模拟、网络流量生成器. IDS 保护系统模拟正常运行中的一个内部网络或者一台主机；网络流量生成器模拟网络之间的通信；攻击模拟用来模拟入侵行为，入侵检测系统就是需要评估的系统. 另外在评估中一般采用虚拟主机技术模拟内部网络中运行不同操作系统的各种服务器主机[12]. 其模型如图 1 所示.

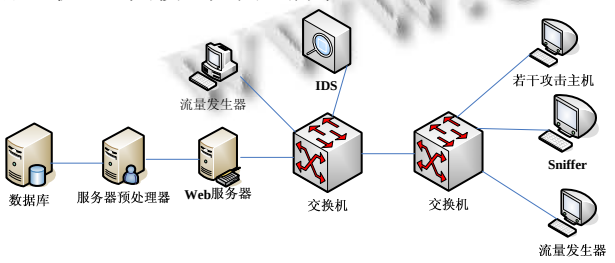

图 1　传统 IDS 评估模型

从以上的分析和图 1 可以看出，目前的入侵检测评估模型都是基于模拟环境而设计的，从网络流量到入侵数据，从攻击类型到攻击手段都是通过模拟实现. 模拟环境虽然在很大程度上解决了入侵检测所需要的数据问题，但仍然还存在很多问题，比如模拟环境的评估结果与真实环境的评估结果之间到底存在多大的差异，评估的准确性和可信度有多高. 由此可见这种方法不能从根本上解决目前入侵检测评估所面临的问题和挑战.

3　基于Openflow的入侵检测评估模型

从以上的分析中不难发现，在目前的网络环境下，因为网络的不可控致使 IDS 测评工作只能在仿真环境下进行，而仿真环境与实际环境相比具有很大的不同，评估结果当然也会存在很大不同. 因此，解决好评估数据来源问题，评估效果会有很大不同，其准确性和可信性都将大大提高. 而评估数据的来源问题主要是: 正常网络流量数据，正常用户行为数据，攻击数据. 如果这些数据来源问题能解决，不利于仿真产生，而是利用真实网络数据完成，就可以打破传统的基于仿真环境的测评技术，而建立基于真实网络环境的测评技术.

基于软件定义网络技术为建立可控的网络提供了可能. 而可控的网络意味着很多的实验数据可以在软件的控制下在真实的网络中传输，从而打破了入侵检测评估环境只能在模拟环境下建立的状况. 本节将重点论述基于 OpenFlow 的入侵检测评估环境的搭建方法.

3.1 基于 Openflow 的 IDS 测试评估框架

基于 OpenFlow 的入侵检测评估框架如图 2 所示，其运行环境是真实的局域网，并以基于网络的入侵检测(NIS)为研究对象. 主要设备包含 Openflow 交换机、控制器、普通交换机、被测 IDS 和攻击流量发生器.

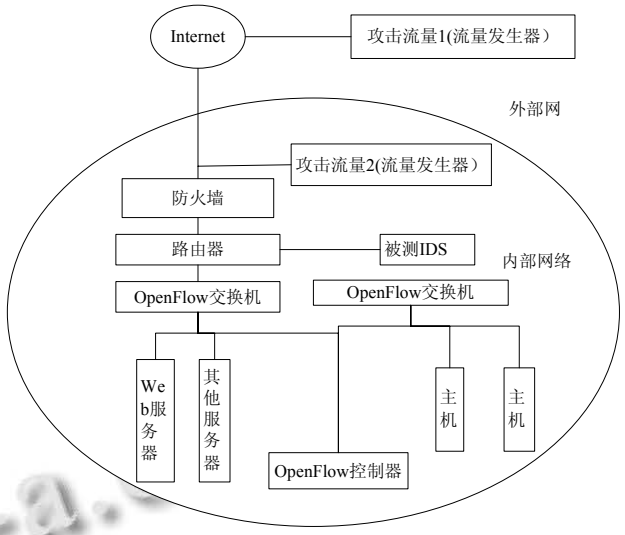

图 2　基于 OpenFlow 的入侵检测评估框架

首先是参数设置模块，提供了自定义测试参数的功能，分为三个主要的子模块，分别是流量控制模块、时间控制模块以及自定义测试脚本模块. 在流量控制模块中，用户可以监测网络流量的各种状态，选择一个合适的网络流量状态开始测试，监测的流量状态包括内外网流量大小、流速、攻击流量的大小及出现频率等，这些参数都有缺省值,如果用户设置了流量参数，则系统参照用户自定义的参数进行测试. 在时间控制模块中，用户可以自定义测试的时间起始时间，也可以选用系统为用户设定的四个等级: 高级、中级、低级及自定义级. 性能测试参数主要用来定义当前的测试主要测试哪些性能，本系统设计的可选的性能有检

测率、误警率、攻击数、抗攻击力等主要性能指标, 用户可以根据被测 IDS 的不同特性选择符合需求的测试性能指标.

攻击流量 1: 在局域网外部的某台机器上产生模拟攻击流量, 仿真网络外部攻击;

攻击流量 2: 在局域网内部的某台机器上产生模拟攻击流量, 仿真网络内部攻击;

防火墙: 局域网内部的正常防火墙设备, 保护局域网的安全;

路由器: 局域网内部的正常路由设备, 为局域网提供路由功能;

被测 IDS: 局域网内部的正常入侵检测设备也是本次需要测试和评估的设备;

Web 服务器: 对内对外提供 Web 服务; 其他服务器: 可以是 FTP、DNS 等所需要的相关服务器;

主机: 局域网内部正常使用的个人主机;

OpenFlow 交换机: 非专用 OpenFlow 交换机, 在传统交换机上升级而得到的交换机, 该交换机除了完成传统交换机的数据交换功能还需要完成额外的数据过滤功能, 能从正常的网络流量中分离出攻击数据和流量;

OpenFlow 控制器: 与 OpenFlow 交换机配合使用, 主要完成 OpenFlow 交换机的控制和最后的评估分析. 本模块是本系统的核心模块, 应用 OpenFlow 技术评估被测 IDS, 根据 IDS 设置模块和参数管理模块预先设置的 IDS 和测试条件, 对被测 IDS 进行性能测试, 并分析测试结果, 生成评估分析报告供给使用者进行性能评价. 用户也可以随时查询历史测评结果, 可以针对被测 IDS 的测试数据与系统历史已测试过的 IDS 的测试数据进行对比分析, 最后将测试结果存放入数据库中, 方便用户日后查询, 也为系统的性能分析提供数据.

该模型与传统入侵检测评估模型相比, 其变化的核心是真实外部流量的引入和 OpenFlow 交换机、控制中心的使用.

3.2 Openflow 交换机的规则设置

OpenFlow 交换机和控制器在本模型中起到关键作用, 他利用 OpenFlow 灵活可控的转发功能为入侵检测评估提供了新的思路, 所以 OpenFlow 的规则设置是本模型的关键, 鉴于本模型的工作需要, 并根据如图 3 所示的 OpenFlow 数据流表格式为 OpenFlow 交换机设置如下的转发规则.

(1)从网络特定主机(测试时主要指定从攻击主机)发送来的数据不进行转发, 而是送到控制中心, 由控制中心做统计处理.

(2)一般网络流量按正常处理流水转发.

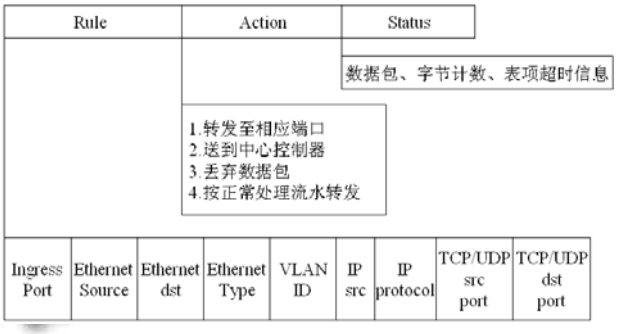

图 3 数据流表项格式

3.3 基于 Openflow 的 IDS 评估模型工作过程

基于 Openflow 的 IDS 评估模型打破传统的使用模拟流量的各种限制, 在真实的网络环境下测评 IDS 的各方面性能. 其具体工作过程如下:

(1)在外部网络和内容网络均利用流量发生器产生攻击流量. 这里不直接使用真实网络中的攻击流量主要基于两方面的考虑, 第一, 网络攻击具有随意性和不可控性, 不能保证在测试的时候有攻击流量正在产生; 第二, 网络攻击种类在同一时间段内不能保证多样性, 而攻击类别的多样性和全面性对于评估系统来说是很关键的因素. 因此在攻击流量的产生问题上还是采用传统的模拟攻击流量的方法, 这样可以比较方便的解决以上两方面的难题.

(2)内部、外部攻击流量和外部网络真实流量经由防火墙进入内部网络, 部署在内部网络的被测 IDS 检测攻击流量并生成检测报告发给内部网络中的 OpenFlow 控制器. 与此同时, 攻击流量和外部网络流量正常进入网络交给 OpenFlow 交换机转发. OpenFlow 交换机根据设置的规则转发正常流量, 同时拦截攻击流量并转发给控制中心. 在规则的设置上可以选择源 MAC 符合规则即被转发, 或者源 IP 地址符合规则即被转发, 也可以是源端口符合规则即被转发.

(3)控制中心接收攻击流量后对攻击流量进行统计计算, 然后与 IDS 的检测报告对比, 最后给出 IDS 的测评结果.

4 仿真实验与分析

入侵检测评估模型可以比较方便的移植到真实的网络环境, 但是目前工作的网络环境还不足以支撑该网络环境, 所以为了测试该模型的可行性, 利用 GNS 3 网络模拟器来建立的网络环境.

4.1 评估测试环境拓扑图

因为实验条件和各方面的限制, 本次的实验验证不能在现有局域网环境下进行, 因此选用了 GNS 来模拟实验中所需要的各种环境, 其拓扑结构图如图 4 所示.

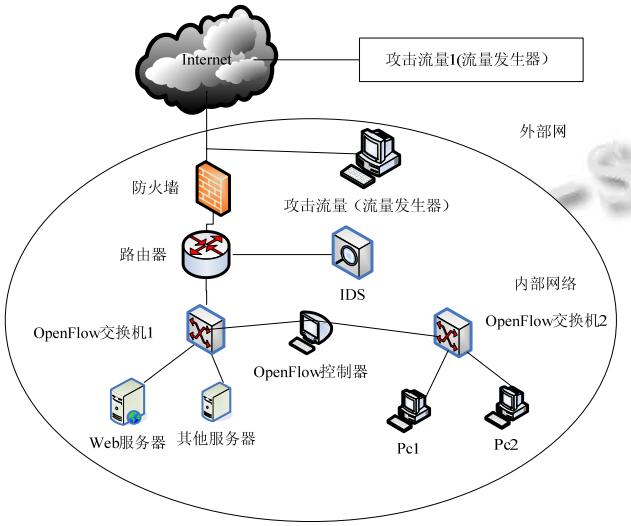

图 4　基于 Openflow 的入侵检测评估测试环境拓扑图

4.2 基于实验环境的运行测试

(1)测试对象

目前网络和市场中有大量的 IDS, 选取了开源的入侵检测系统: Snort. snort 是一个功能强大的轻量级的网络入侵检测系统. 下面对 Snort 进行一个简单的介绍. 它与 1998 年问世, 目前已发展成为集实时流量分析, 网络数据包记录, 入侵检测、防御于一体的开源入侵检测系统, 是目前使用人数最多的 IDS. 从网络下载 snort 并安装后 , 会发现 snort 具有很多种功能, 最简单的功能就是流量监控, 可以把网络上所有的流量情况连续不断显示给网络管理人员, 这一功能主要是靠抓包模块完成; 稍微复杂点的功能是数据包记录, 这一功能是在抓包的基础上把所有的数据信息记录在硬盘上, 形成数据日志, 这一功能对管理员分析网络故障或者攻击行为有很好的作用; 第三个功能是入侵检测, 这个是 Snort 的核心功能, 也是最为复杂的功能, 该功能是在抓包的基础上, 根据用户已经定义的规则, 或者是默认的规则分析判断网络中的入侵行为, 并产生报警. 关于 Snort 的入侵检测工作过程在此不做详细介绍.

总之, Snort 因为良好的扩展性和可移植性, 以及源代码是完全公开的, 用户可自己添加新的检测规则等因素, 使他成为开放源代码之中安全领域最活跃的工程之一, 是商业入侵检测系统较好的替代产品.

(2)测试结果及分析

选定测试对象后, 利用图 4 所示的拓扑结果图, 在 IDS 上运行 Snort, 在外部攻击流量发生器和内部攻击流量发生器上分别产生攻击流量, 安装在 OpenFlow 控制器上的测评系统利用 NOX 负责对 Snort 的测试能力进行评估. 评估指标的选取上因为受到环境和开发时间的现在, 本次的测评指标只是选中以上所分析的测评指标中最为重要和基础的指标, 即检测率和误报率, 因为这指标两个最能反映 IDS 检测能力和优劣的重要指标. 其他的指标在以后的研究中逐步加以验证, 在此就不多做说明. 具体测试方法是这样:

根据常用的性能指标检测方法, 在实验测试中使用小数据, 只仿真 5 次正常的 http 使用, 5 次攻击, 表 1 是的测评系统根据不同的攻击情况给出的异常指数检测报告. 表 2 是选取不同的阈值(异常指数高于阈值被认定为攻击行为)在不同攻击情况下所得到的误报次数与检测率关系的测评报告, 此处的每种攻击次数均为 100 次.

4.3 仿真结果与分析

表 1　基于 Openflow 的 IDS 检测报告

	传统方法异常指数	本文所提方法异常指数
正常 1	0	0
正常 2	0.43	0.33
正常 3	0	0.09
正常 4	0.10	0.46
正常 5	0.55	0
攻击 1	44.5	40.13
攻击 2	9.52	8.56
攻击 3	11.43	10.23
攻击 4	15.75	13.67
攻击 5	20.13	18.58

根据表 2, 可以看出在阈值较高的情况传统方法和本问说提出的方法差别不大, 可以实现误报率为 0 的情况下, 检测率可以达到 100%, 但在阈值降低, 检

测准确性要求较高的情况下, 本文所提出方法的检测率要低于传统方法的检测率.

表 2 被测体系的误报次数与检测率关系

阈值	攻击类型	传统IDS测评误次数	本文IDS测评误报次数	传统IDS测评检测率	本文IDS测评检测率
>10	Scan	0	0	100%	100%
	backdoor	0	0	100%	100%
	mysql	0	0	100%	100%
	ddos	0	0	100%	100%
	dos	0	0	100%	100%
	chat	0	0	100%	100%
	Arp	0	0	100%	100%
	dns	0	0	100%	100%
>1	Scan	1	1	1%	1%
	backdoor	31	34	31%	31%
	mysql	1	1	1%	1%
	ddos	0	1	0%	1%
	dos	3	4	4%	4%
	chat	1	1	4%	1%
	Smtp	7	8	7%	8%
	dns	4	5	4%	5%
>0.1	Scan	1	1	1%	1%
	backdoor	37	41	37%	41%
	mysql	2	3	2%	3%
	ddos	0	1	0%	1%
	dos	4	4	4%	4%
	chat	1	1	4%	1%
	Smtp	7	9	7%	9%
	dns	4	5	4%	5%

通过以上实验结果表明, 本文所提出的测评模型对 IDS 的测评结果更为苛刻, 充分体现 IDS 在复杂真实的网络环境中对攻击行为的检测能力要低于模拟环境下的检测能力, 这正是所要的结果, 也充分说明基于 OpenFlow 的 IDS 测评系统能更好的反映被测评系统的真实检测能力, 为用户提供更为科学、正确的入侵检测产品.

5 结语

通过分析当前的入侵检测评估技术所采用的模型和方法, 以及当前热门的 OpenFlow 技术, 因此, 本文所提出基于 OpenFlow 的 IDS 测评方法改变了传统测评方法依赖模拟环境来仿真真实网络流量的现状, 是一种技术上的进步, 从实验结果也可以看出这种新的方法所测评的结果与传统方法有差别, 这也为 IDS 测评研究提出了新的疑问和挑战, 同时也为测评方法提供了新的研究思路.

参考文献

1 董晓梅,肖珂,于戈.入侵检测系统评估技术述评.计算机科学,2004,31(2),22–25.

2 吴庆涛,邵志清.入侵检测研究综述.计算机应用研究,2005,1(12),11–15.

3 卿斯汉,蒋建春.入侵检测技术研究综述.通信学报,2004,25(7),19–30.

4 王丽君,刘永强,张健.基于 OpenFlow 的未来互联网试验技术研究.电信网技术,2011,1(6),1–4.

5 Tian JF, Liu T, Chen XX. Survey in evaluation of intrusion detection system. Computer Engineering and Applications, 2008, 44(9): 113–117.

6 林果园,曹天杰.入侵检测系统研究综述.计算机应用与软件,2009,26(3):14–17.

7 Deng H, Zeng PA, Agrawal DP. An unsupervised network a-nomaly detection system using random projection technique. Proc. of the 2003 International Workshop on Cryp-tology and Network Security. 2003.

8 高苗粉,秦勇.网络入侵检测系统自体集检测中的概率匹配高效寻优机制.计算机应用,2013,33(1),156–159.

9 蒋一波,王雨晨,王万良,张祯,陈琼.一种基于机器学习的 MANET 网络入侵检测性能评估方法研究.计算机科学,2013,40(S2):258–263.

10 刘明珍.基于 CPSO-LSSVM 的网络入侵检测.计算机工程,2013,36(11):208–211.

11 柳强,丁岳伟.入侵检测系统的测试评估及存在问题的探讨.上海理工大学学报(社会科学版),2006,28(2):72–75.

12 黄庆涛.网络入侵特征优化检测方法仿真.计算机仿真,2013,42(9):196–199.