一种基于 One-Class SVM 和 GP 安全事件关联规则生成方法研究

杜栋栋[1,3],任星彰[2,3],陈 坤[2,3],叶 蔚[3],赵 文[3],张世琨[3]
(1. 北京大学信息科学技术学院,北京 100871;2. 北京大学软件与微电子学院,北京 100871;
3. 北京大学软件工程国家工程研究中心,北京 100871)

摘 要: 随着信息技术的快速发展,网络安全威胁造成的危害日愈严重. 安全信息和事件管理(SIEM)在查找组织内部威胁,可疑行为及其它高级持续攻击(APT)中发挥了重要作用. SIEM 的检测能力主要依赖于准确,可靠的关联规则. 然而,传统的规则生成方式主要基于专家知识人工编写检测规则,因此成本高,效率低. 本文给出了一种具备自适应能力的规则生成框架来自动生成关联规则. 首先为了更好地识别未知攻击,提出一种基于单类支持向量机(One-Class SVM)的安全事件分类算法对安全事件进行有效分类,实验分类效果准确率高达 97%. 其次为了提高规则生成准确率,通过重新定义个体结构,交叉与变异方式,优化了基于遗传编程(GP)的规则生成算法,规则适应度高达 94%. 实验结果表明,本文提出的框架具备自适应能力来识别未知攻击,具备较高的检测准确率,可有效减少人工参与. 同时该框架已经部署在实际生产环境中,和原系统相比可以检测更多攻击类型.

关键词: 安全事件; 关联规则生成; 日志管理; 安全信息和事件管理 (SIEM); 单类支持向量机; 遗传编程
中图分类号: TP311 **文献标识码:** A **文章编号:** 0372-2112 (2018)08-1793-11
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.08.001

A Security Event Correlation Rule Generation Method Research Based on One-Class SVM and Genetic Programming

DU Dong-dong[1,3], REN Xing-zhang[2,3], CHEN Kun[2,3], YE Wei[3], ZHAO Wen[3], ZHANG Shi-kun[3]
(1. *School of Electronics Engineering and Computer Science, Peking University, Beijing* 100871, *China*;
2. *School of Software and Microelectronics, Peking University, Beijing* 100871, *China*;
3. *National Engineering Research Center for Software Engineering, Peking University, Beijing* 100871, *China*)

Abstract: With the rapid development of information technology, enterprise and orgnizations are suffering different kinds of cyber security threats. Security Information and Event Management (SIEM) is playing an essential role in finding insider threats, suspicious behaviors or other advanced attacks based on its correlation capability. The SIEM detection capability relies on accurate and reliable correlation rule, however, traditional way of generating rule depends on human expert knowledge, which is costly and time consuming with low efficiency. In this paper, we propose an adaptive rule generation framework to generate correlation rule automatically. First, in order to identify unknown attack in a better way, we propose a security event classification algorithm based on One-Class Support Vector Machine (One-Class SVM) to classify security events effectively, and results show that classfication rate reaches as high as 97%. Secondly, for purpose of improving rule generation accuracy rate, we propose and optimize Genetice Programming (GP) rule generation algorithm by redefining individual structure, cross and mutation operation, and results show that best individual fitness reaches as high as 94%. Experiments have been performed and results show that our approach has the ability of self-adaption to identify unkown attack, a competitive threat detection accuracy rate as well as reducing human labor engagement. We also implement our approach to a real production system and more attack type could be detected compared with existing system.

Key words: security events; correlation rule generation; log management; security information and event management (SIEM); one-class support vector machine; generic programming

收稿日期:2017-06-27;修回日期:2018-02-28;责任编辑:马兰英
基金项目:国家重点研发计划(No. 2017YFB0802900);北京市自然科学基金(No. 4182024);中国博士后基金(No. 2017M620524)

1 引言

随着高速互联网技术的飞速发展,企业和关键基础设施正面临各种各样的攻击和威胁. 安全信息和事件管理(Security Information Event Management,SIEM)被认为是一种很好的解决方案,来帮助安全分析师和管理员从海量安全事件中挖掘有用的威胁信息与情报. 开源安全信息管理工具 OSSIM(Open Source Security Information Management)[1]作为开源工具中著名的事件管理工具被广泛应用于企业组织机构. SIEM 系统最常见的检测手段是关联分析,它通常基于时序来对相同数据源或来自不同数据源的安全事件,使用关联规则来进行综合的关联分析.

目前 SIEM 在关联分析方面主要存在两方面的挑战. (1)安全信息相互隔离. 通常来说,一次恶意攻击会在多个安全设备或应用程序(如网络防火墙,交换机,Web 应用日志,SQL 日志,审核日志等)中留下痕迹. 然而,所有这些信息都是孤立隔绝的,被保存在不同的设备日志中,缺乏有效的综合关联分析;(2)关联规则的自动化生成. 安全分析师通常具备描述安全目标和业务分析的能力,但是却缺乏相关的编程背景知识来自动化地生成关联规则.

自动规则生成中对攻击事件的识别可以归纳为对安全事件的分类问题,分类精度的高低决定了安全规则对攻击事件的识别能力. 单类支持向量机(One-Class Support Vector Machine,One-Class SVM)主要通过对某一类事件进行训练建立行为基线,基线范围外的事件视为异常事件来进行分类. 该算法较适合于本文检测场景,通常 SIEM 系统中 90% 的日志为正常事件,通过对正常事件训练建模,来检测异常或攻击事件.

当事件被正确分类后,如何快速、高效地生成有效的匹配规则决定了自动规则生成能否应用于实践. 遗传编程(Genetic Programming,GP)是利用遗传算法模拟大自然种群在选择压力下的自然演化从而得到问题近似解的一种方法. 本文利用 GP 通过对个体的变异、交叉、选择来繁殖生成最佳匹配的关联个体,进而转换为实际应用的关联规则,使得规则生成更为高效,具备实际应用能力.

此外,本文提出的方法还具备自适应能力来自动识别未知的攻击行为,对于新出现的异常行为进行自动更新,进一步减少专家人工参与,提高检测效率.

主要研究工作总结如下,首先提出一种基于 One-Class SVM 的安全事件分类算法,并提供更丰富的关键词标签,更多维度特征向量,避免检测精度低或过拟合情况. 算法输入是经过 OSSIM 归一化后具备相同数据结构的安全事件,输出则为带有标记的安全事件,标记分为两类:正常(Negative)与攻击(Positive). 其次提出一种基于 GP 的关联规则自动生成算法. 本文重新定义了个体的结构表达方式和交叉、变异等遗传特征,使生成的关联规则更有效,更准确. 其输入是 One-Class SVM 分类算法输出的带标记的正常与攻击事件. 输出为可以部署在 OSSIM 系统中应用于实践的关联规则. 基于公共安全数据集进行了多组实验对比,并最终将该框架部署应用于实际生产环境. 实验结果表明本文的框架对于安全事件的分类准确率达到 98.84%,对于生成的规则适应度高达 94%.

2 相关研究

SIEM 系统的检测能力主要依赖于准确、可靠的关联规则. 因此,规则生成问题也成为学者研究的热点问题. 规则生成研究的主要领域包括安全事件的规则生成,基于复杂事件处理(CEP)系统的规则生成,网络入侵检测(NIDS)规则生成等. 采用的方法主要包括基于统计、概率、数据挖掘的方法,随着技术的发展,基于机器学习的方法也逐步被引入到规则生成中.

传统的关联规则生成主要通过安全专家人工编写,这种方式效率低下,且人工成本难以承受. 对于新出现的攻击和漏洞无法及时作出响应,检测规则的编写往往出现滞后的情况,不具备自适应能力. 学者也提出其它技术方法如数据融合[2]数据挖掘[3]基于概率报警关联[4]等技术用于识别和学习攻击模式和信息并应用于检测安全威胁. 然而,这些方法在实际应用中往往生成的关联规则检测精度较低,检测结果不理想,实际应用效果有限.

Margara 等[5]提出一个基于复杂事件处理(CEP)的规则生成模型,作者定义了事件模型,操作符,及相关的检测模式(Pattern),采用的方法主要是对历史数据频繁项的挖掘. 其主要问题是生成的规则会导致大量重复报警,误报率较高,同时其生成的规则可读性较差. Hasan 等人[6]采用基于概率的方法从事件流中生成复杂事件模式,其主要思路仍然是对历史数据频繁项的整理,该方法对初始模式集要求较高,并且对数据源数据质量要求非常高,直接影响到最终的模式检测效果. Ning 等[7]在对底层入侵检测系统(IDS)报警分析的基础上针对攻击的先决条件及其结果提出了一种自动关联分析的方法,该方法要求所有的先决条件均需满足,而实际情况当其中某一个先决条件被遗漏后,会对后期的关联分析带来较大的影响.

在网络入侵检测系统(NIDS)研究领域,一些技术方法如专家先验知识,统计方法等也被用于识别和学习攻击模式并应用于检测安全威胁. Lunt 在[8]中首次提出了一个专家系统充分利用专家的先验知识来进行

入侵检测,极大地提高了入侵检测的精度,随之带来的问题就是专家知识与人工参与带来的低效及高成本问题. Brugger 等[9] 总结了各类数据挖掘方法来对离线安全连接记录(Connection Record)进行分析并提取攻击特征,强调了特征选取的重要性,对比各类数据发掘技术如基于固有属性的贝叶斯网络,隐马尔科夫模型,决策树,前馈神经网络,聚类算法,支持向量机等算法与相关技术. Bykova 等人[10,11] 则使用了基于统计分析来检测网络异常活动,通过对 IP 报头信息,TCP 报头信息进行统计分析来识别异常活动,这种方法通过统计合并信息可以有效减少警报的数量,但由于仅对数据报头信息进行了分析,忽略了包内容,会导致报警的遗漏.

随着机器学习技术的迅速发展,一些智能化的方法如神经网络(Neural Network)[12,13],遗传编程(GP)[14] 等也被逐渐引入该研究领域. Suarez-Tangil[15] 首先提出一种使用 GP 来自动生成关联规则的方法,描述了 GP 中个体的结构及相关的操作符. 随后,同一作者在文献[16]中提出了结合多层人工神经网络(Multi-layer ANN)和 GP 的改进模型来自动生成关联规则. 但是在实验过程中发现其提到的分类方法存在两个问题,如果采取单层 ANN 中对事件进行分类,其分类的平均准确率仅仅达到 81% 左右,分类效果不理想;而采用多层 ANN 时却又出现过拟合的情况,针对训练集的检测准确率达到 99% 以上,而对测试集和真实数据的检测准确率却非常低. 此外,实验过程中发现基于 GP 的规则生成算法生成的个体存在随机度过高,个体难以解读与阐释,随机生成的个体难以转换为有效的 OSSIM 关联规则等问题. 且生成的个体适应度均值范围为 79% ~81%,使得转换后的规则检测率不够理想.

3　本文主要工作

针对相关研究中其它方法面临的分类精度不足、分类过拟合、及生成的个体适应度均值较低等问题,通过对实际生产环境数据进行分析,发现数据中约 90% 的事件属于正常事件,攻击事件占比较低,且攻击特征与正常事件相比较为明显. 本文提出的方法主要包括两个组成部分:(1)基于 One-Class SVM 的安全事件分类算法. 主要将安全事件划分为正常事件与攻击事件,基本思想是利用 One-Class SVM 为正常事件建立行为基线,基线范围以外的事件视为攻击事件. 因此,对于未知的攻击与威胁也具备相应的识别能力;(2)基于 GP 的安全规则自动生成算法. 采用遗传算法的演化迭代思想,经过变异、交叉、选择等方法找出最佳的匹配个体来生成相应的攻击检测规则.

本文方法的工作流程如图 1 所示. 整体框架的输入来自训练集、测试集及生产环境中的安全事件,然后进行数据预处理,包括归一化、滑动窗口分组、数据统计等操作,经过预处理后的安全事件作为输入由安全事件分类算法对其进行分类,输出带有标签的安全事件. 标签分为两种:攻击事件(Positive)与正常事件(Negative). 接下来规则生成算法将标签事件自动生成一组个体集,然后通过个体的变异、交叉、选择繁殖经过适应度计算公式计算并输出最佳匹配个体,最终转化为 OSSIM 的关联规则.

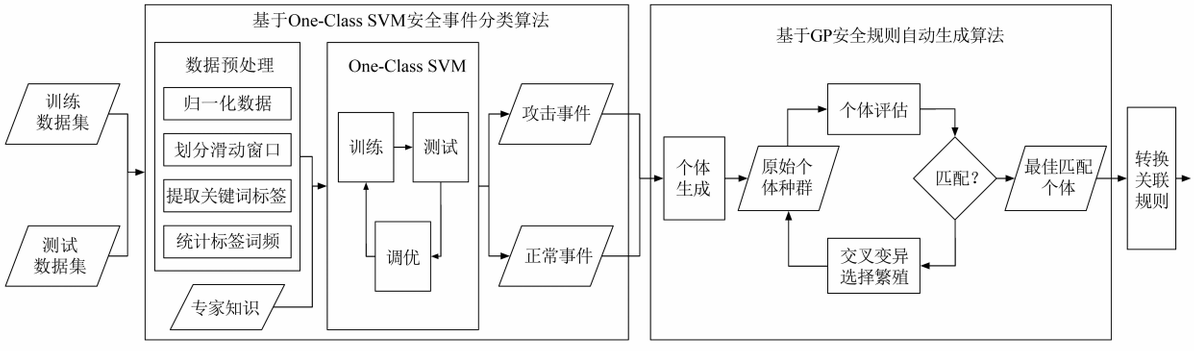


图1 关联规则自动生成工作流程

3.1　基于 One-Class SVM 安全事件分类算法

3.1.1 关键词标签的提取与攻击模式表达

安全日志的关联分析结果通常高度依赖于事件采集传感器配置,相同的解决方案针对不同的生产环境需要做大量自定义配置,效率低下. 本文的分类方法采用基于预定义关键词标签的分类方法,这些关键词标签来源于专家的先验知识及预定义的关联规则.

通过深入分析 SIEM 系统的关联规则,其中最常见的配置字段如:event_id, timestamp, plugin_id, plugin_sid, src_ip, src_port, des_ip, des_port, protocol 等. 为了使关联分析规则不依赖于传感器配置,本文从 OSSIM 的规则库中抽取了几个重要的字段 plugin_id_name, plugin_id_description, sid_name,并将所有字段拆分成一个个关键词标签,然后针对每一条检测规则生成其关键

词标签统计模型,利用规则统计模型来代替原始的规则来检测攻击.

关键词标签 $key\_tag_j \in K$ 是用来描述安全事件的一系列关键词标签,其对安全事件属性的描述更为精确.表1显示了部分抽取的关键词标签及其所属攻击分类的样例列表.关键词抽取的过程主要依据:(1)人工专家知识;(2)环境变量特征;(3)关联规则中提取的规则id,security id description(sid 描述);(4)SIEM 系统中最新采集到的安全日志事件.在关键词抽取的过程中,数据挖掘工具的使用可以帮助提高提取效率.

表1 抽取的关键词标签及相关攻击分类样例列表

攻击分类	标签数量	关键词标签示例
SQL	160	Exec, Passwd, HTTP, xp_cmdshell, login, failed, port, probe, Sybase, Database
WEB-ATTACKS	168	wget, uname, id, echo, kill, chmod, chgrp, access, execution, nasm, perl, admin, remote, host, lsof, conf/httpd. conf, . htgroup
SMTP	38	sendmail, CSMMail, exchange, handshake, addresses, AUTH, SSLv2, base64, At-tachment, ActiveX
FTP	448	ftp, login, attempt, forward, passwd, authorized _ keys, pipe, Chown, Vulnerability, ProFTP, Exploit, Buffer, Access, Write, File, MODE, Mkdir, Explorer
EXPLOIT	83	overflow, proxy, sniffit, buffer, SSH, execution, modification, cross-site, mmc. exe, createcab. cmd, overwrite
DOS & DDOS	55	Jolt, attack, Land, Teardrop, UDP, bomb, IGMP, Server, Ascend, Route, arkiea, backup, Winnuke, MSDTC, attempt, DOS, IP, Op-tions, validation, denial, TCP, SACK, range, MX, lookup, generic, hashing, handler- > agent, agent- > handler

接下来划分滑动时间窗口,定义多个不同时间长度分别为10秒,30秒,60秒,300秒,1800秒,3600秒,43200秒,86400秒的滑动时间窗口类型,然后针对不同窗口类型按照安全事件时间戳对事件进行重新分组.在每一个滑动时间窗口内,针对安全事件信息中关键词标签出现的次数进行统计.

本文将关键词标签及其对应的统计信息组成相应的攻击检测模式(pattern),攻击模式 $p_m \in P$ 定义为描述某一种特定攻击或异常活动时,其对应的一组关键词标签在指定的滑动时间窗口内出现频率的直方图信息.在 OSSIM 中,这些模式被用于检测各种攻击.然后一组相关的模式组成某一类特定的攻击分类表达.攻击分类 C_i 则是由一组攻击模式组成,用来代表某一种攻击分类如 FTP 攻击,DOS 攻击等.

3.1.2 特征向量表达

原始日志无法作为算法的直接输入,根据上面的攻击模式定义,抽取关键词标签,在滑动窗口内统计安全日志信息中关键词标签出现的频率值,以此建立特征向量.特征向量的维度由关键词标签的数量及滑动窗口类型决定,样本数目则由一定时间范围内划分的所有不同滑动窗口类型的总数量构成.表2(*a*)包含了特征向量的相关说明,表2(*b*)则是部分特征向量示例.

表2(*a*) One-Class SVM 特征向量及说明

特征	说明
滑动窗口类型	主要包括8种不同类型的滑动窗口
关键词标签	标签数量决定向量维度
标签统计值	每个标签按照窗口类型统计出现频率值

表2(*b*) One-Class SVM 特征向量示例

timeout	ftp	command	overflow	attempt	format	string	snort	tftp	root
1	3	2	2	3	1	1	0	0	0
1	3	13	2	14	0	0	1	0	0
1	6	4	5	6	1	1	0	33	11
2	80	27	51	80	0	0	20	0	0
2	116	36	72	116	2	2	30	0	0
2	117	39	75	117	0	0	30	0	0
3	109	36	70	109	1	1	30	0	0
3	2	13	2	13	0	0	0	60	20
3	5	4	5	5	0	0	0	0	0

3.1.3 分类方法

One-Class SVM 最早在论文[17]中被提出来,然后作为一种无监督学习算法被广泛用于信息安全领域中.其基本思想是训练集中只包含一类数据,然后来寻找此类数据中距离原点的最优边界.本文中将正常数据使用 One-Class SVM 进行训练,攻击数据作为异常数据

对其进行检测,从而使模型具备自适应能力.

给定数据集 $X=\{x_1,x_2,\cdots,x_n\}$,n 为样本个数,One-Class SVM 通过最大化原点与目标数据间的最小欧氏距离$\frac{\rho}{\boldsymbol{w}^{\mathrm{T}}\boldsymbol{w}}$来寻找最优超平面,其中 $\boldsymbol{w}$ 是超平面的法向量,ρ 是超平面截距,ξ 是松弛因子.

$$\min_{w,\partial,\xi}\frac{1}{2}\boldsymbol{w}^{\mathrm{T}}\boldsymbol{w}-\rho+\frac{1}{vn}\sum_{i=1}^{n}\xi_i$$

$$\text{subject to } \boldsymbol{w}^{\mathrm{T}}\phi(x_i)\geqslant\rho-\xi_i,\xi_i\geqslant 0,i=1,2,\cdots,n \quad (1)$$

其对偶形式表示为:

$$\min_{\alpha}\frac{1}{2}\boldsymbol{\alpha}^{\mathrm{T}}Q\alpha$$

$$\text{subject to } 0\leqslant\alpha_i\leqslant\frac{1}{(vl)},i=1,2,\cdots,l,\boldsymbol{e}^{\mathrm{T}}\boldsymbol{\alpha}=1 \quad (2)$$

其中 $Q_{ij}=K(x_i,x_j)=\boldsymbol{\phi}(x_i)^{\mathrm{T}}\boldsymbol{\phi}(x_j)$,决策函数为:

$$\operatorname{sgn}\Big(\sum_{i=1}^{l}\alpha_i K(x_i,x)-\rho\Big) \quad (3)$$

3.1.4　参数调优与评估

算法采用线下训练,参数调优,线上运行的工作模式. 初始参数依据经验设置,然后利用评估公式计算准确率,不断优化参数以达到最优分类效果. 具体调优流程如图 2 所示. 对算法的评估使用如下指标:精确率(Precision),召回率(Recall),准确率(Accuracy)分别对应公式(4),(5),(6)及表 3 中定义的预测混淆矩阵.

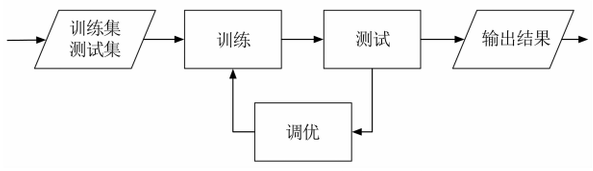


图2　One-Class SVM 算法调优流程

表 3　预测混淆矩阵

Actual Label	Prediction Label	Result
Positive	Positive	True Positive(TP)
Negative	Positive	False Positive(FP)
Positive	Negative	False Negative(FN)
Negative	Negative	True Negative(TN)

$$precision=\frac{TP}{TP+FP}\times 100 \quad (4)$$

$$recall=\frac{TP}{TP+FN}\times 100 \quad (5)$$

$$accuracy=\frac{TP+FN}{TP+FN+FP+FN}\times 100 \quad (6)$$

3.2　基于 GP 安全规则自动生成算法

基于 GP 安全规则的自动生成算法主要利用了遗传编程的演化特性来生成最匹配的关联规则. 自动规则生成可以最大程度上解决人工编写规则带来的低效,人工成本过高等问题,而 GP 的演化特性也非常有助于生成高检测精度的匹配规则. 本文对 GP 算法中的个体结构、交叉、变异方式进行了大量的优化和改进. 通过标准化内部节点树结构,GP 算法输出的最佳匹配个体可以很方便地转换为关联规则,并部署在实际运行中的 OSSIM 系统中. 算法的整体流程如下图 3 所示:

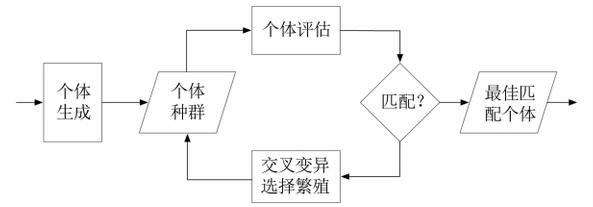


图3　基于GP安全规则自动生成算法工作流程图

3.2.1　个体描述

算法输出的最佳匹配个体最终转换为实际部署的关联规则,OSSIM 系统中的关联规则使用 XML 数据结构来对以下模式进行描述:(1)指令-规则:每条指令包含唯一规则及三种属性标识符,分别为 id,name,priority;(2)唯一规则-规则集:唯一规则至少包含一个规则集;(3)规则集-多条规则:每个规则集中又包含一条或多条规则.

而在 GP 中,个体的描述使用树形结构(Tree Structure),采用操作符与叶子节点组合的方式来对个体进行描述. 默认的树形结构由算法随机生成,其结构随机度很高,难以识别与阐释. 其次,随机树形结构难以转换为合理的关联规则,难以在实际环境中快速部署.

因此,本文重新定义内部个体及其结构,个体树的左侧部分仅包含时间窗口(Time)及出现频率(Occurence)属性值,而右侧部分则包含 SID(Security ID)及 PID(Plugin ID)属性值. 定义了 5 种操作符,分别为 AND(与),OR(或),EQ(相等),LE(小于等于)及 GE(大于等于). 叶子节点内容为属性名称或属性值. 主要的属性包括滑动时间窗口(time window),出现频率(occurrence),插件 id(pid),安全 id(sid)等. 其中根节点(root node)被强制设定为 AND 操作符,如图 4 所示.

此外,个体树的高度由右侧 SID 子树的高度决定,如图 5 阴影部分所示,这样设计目的是由于不同类型的攻击由不同的 SID 值来描述,通过调整 SID 子树的高度可以更准确地获取 SID 数量,这样有利于生成适应度更佳的个体.

3.2.2　种群初始化

GP 种群的初始化指根据预先配置的参数信息如种群规模,交叉概率,变异概率,终止准则等来随机生成一定数量的个体集. 其主要目的是生成尽可能多不同组合的个体,并为下一步的评估做准备. 考虑到种群

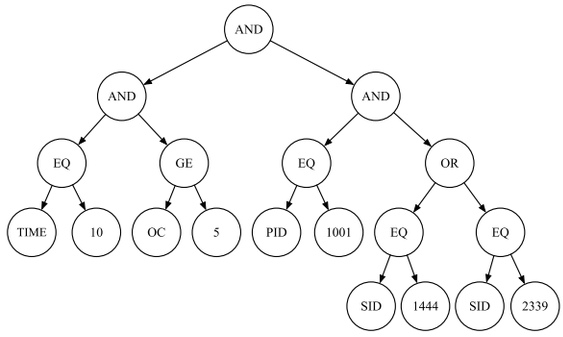


图4 改进后的个体结构样例

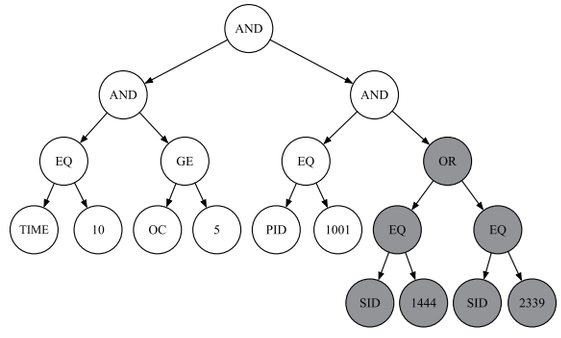


图5 个体数的高度由SID子树高度决定

数目过大会增加运算时间设置初始种群数量为 1000，同时设置迭代次数为 50 次.

3.2.3 个体评估

使用适应度计算公式来计算或评估个体. 针对每一次迭代演化，GP 需要同时考虑准确率与召回率，对应生成最终规则检测攻击的误报率与漏报率，因此选用 F1-Score 作为选择最佳个体的适应度计算公式(7). 适应度(*fitness*)的取值范围为[0.0,100.0]，100 表示最优值，0 代表最差值.

$$fitness = F1\ \ Score = 2 \times \frac{precision \times recall}{(precision + recall)} \times 100 \quad (7)$$

3.2.4 遗传操作算子

遗传操作是实现寻优的关键，针对个体结构的更改，本文同时优化更新了交叉及变异方式.

(1)交叉

交叉被重新定义为通过使用 OR 操作组合不同的子树，如下图 6 所示，其设计目的是通过子树的组合来提高最终个体适应度的召回率.

父体 1:(AND (…) (OR (EQ SID 1441)))

父体 2:(AND (OR (EQ PID 801)))

子体:(AND (…) (OR (EQ PID 801)))

(2)变异

变异操作被重新定义并应用于每一个内部节点，如果变异节点具有子节点，则整个子节点被替换为新

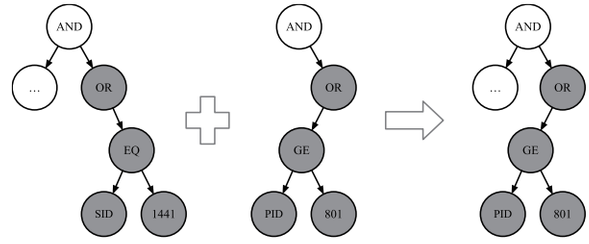


图6 交叉操作

值. 参考下图 7 虚线框中阴影部分值的变化，这样设计的目的为了尽可能提高精确率.

个体:(AND (AND (EQ TIME 1) (EQ OC 10)) (AND (EQ PID 1001) (OR (EQ SID 1444) (EQ SID 2339))))

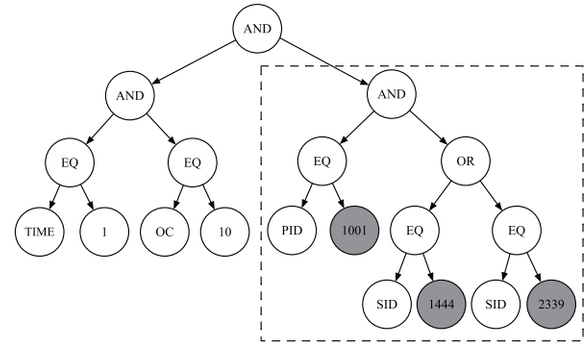


图7 变异操作

通过重新定义个体数的交叉操作与变异操作，使得整棵树的适应度可以达到比较理想的数值.

(3)选择

选择操作发生在交叉变异前后，交叉前运用选择算子从种群中选出一定数量结对父体，然后分别对这些父体对按照概率进行交叉操作与变异操作. 最后将新生成的个体按照适应度再组成下一代种群.

通过对个体的交叉、变异、选择来进行种群的繁殖与演化. 每一代生成的最佳个体会被选中并插入下一代来再次进行适应度计算并获取最优值. 再通过交叉变异操作，来生成尽可能多的个体基因. 上述过程循环运行直至满足终止条件的最佳个体产生.

3.2.5 将最佳个体转换为关联规则

最终由 GP 安全规则生成算法输出的最佳匹配个体如下图 8 所示. 然后将基于树形的最佳个体转换为基于 XML 的安全事件关联规则并部署在 OSSIM 系统中.

3.2.6 参数调优

初始参数主要依据经验值设置，然后根据实际迭代输出值进行逐步调优. 以 FTP 攻击样例数据为例，初始种群数目设置为1000，演化代数设置为50. 适应度

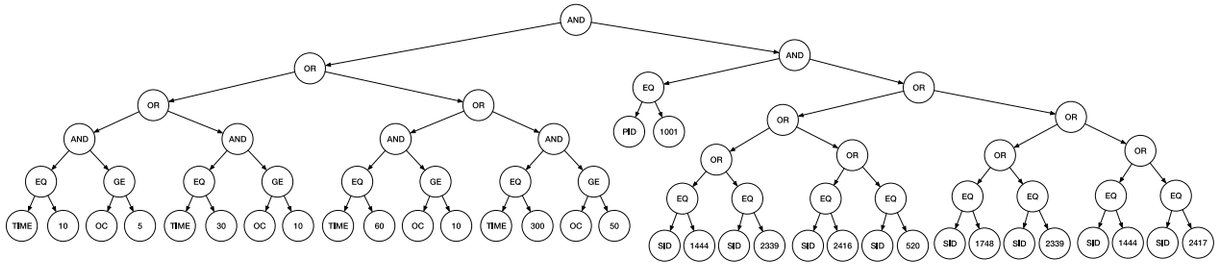


图8　基于GP安全规则生成算法生成的个体样例

公式(7)同时评估了精确率与召回率,得到的实验结果更加均衡.

4　实验结果与分析

本文使用公开数据集 MACCDC[18]（Mid-Atlantic Collegiate Cyber Defense Competition）2012 对提出框架进行实验评估. 测试环境如下图 9 所示. 创建了 10 台虚拟机作为攻击主机来对网络中的用户主机,服务器及用户移动设备进行重放攻击. 所有的攻击数据都会被部署在同一网络下的 OSSIM 服务器捕获并进行关联分析. 被测试 OSSIM 版本为 5. 2. 2,攻击主机采用 Ubuntu 14. 04 操作系统,用户主机包含 Windows7, Windows10 及 macOS 等常见操作系统.

训练与测试数据集使用 MACCDC 2012 数据集,它是一个被广泛使用的网络安全数据集,包含了 16 个 pcap 文件,文件大小共计 16. 63GB. 包含约 22,694,356 个网络连接信息包,几乎覆盖扫描,漏洞,攻击,利用及 webshell 后门等各类攻击数据. 因此是一个非常理想的训练与测试数据集.

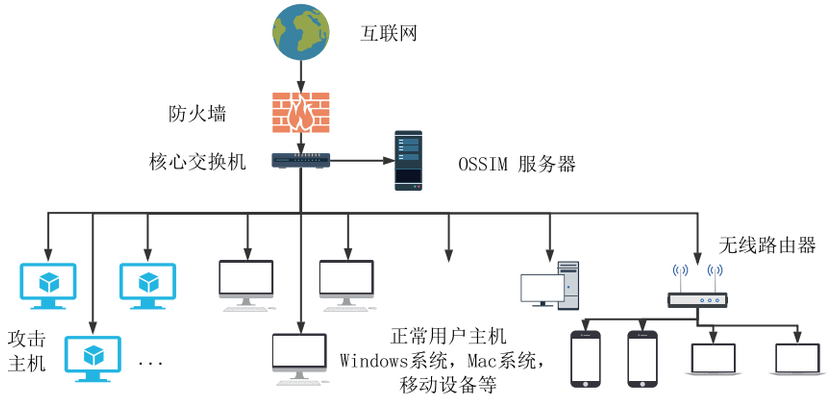


图9　测试环境网络拓扑图：1个OSSIM服务器，20台用户主机，20台虚拟机，25台移动设备及10台攻击主机

4.1　基于 One-Class SVM 安全事件分类算法实验结果与对比分析

对于安全事件分类算法,本文以 MACCDC 2012 数据集中 FTP 攻击为例来对算法的分类效果进行评估. 实验用于训练的 FTP 攻击事件共计 9051 条,正常事件抽样后计 9050 条. 根据事件时间戳进行滑动窗口划分,下表 4 是 One-Class SVM 分类算法针对 FTP 攻击进行分类的详细实验结果. 对于每一种滑动窗口类型,均记录了正负样本窗口数量,精确率,召回率及准确率. 参数优化主要参考准确率,因为准确率公式(6)对于正负样本的区分衡量更平衡.

其它常见的类似异常检测算法或对事件分类算法主要有基于统计方法[10,11],基于规则的方法[19]和基于神经网络[12,13,16]方法等. 不同方法的适用场景稍有不同,如基于统计方法主要根据事件中某个变量、多个变量或基于时序历史数据进行统计分析,但同时面临的问题一是需要依赖某个假设的统计分布变量,二

表 4　SVM 安全事件分类算法对 FTP 攻击进行分类的实验结果

滑动时间窗口种类	滑动窗口数		分类率(%)		
	正常事件	攻击事件	精确率	召回率	准确率
10s	224	578	96. 31	99. 48	96. 79
30s	256	325	99. 99	93. 23	95. 86
60s	214	217	99. 99	93. 55	96. 76
300s	186	75	99. 99	96. 00	98. 94
1800s	196	22	99. 99	95. 45	99. 54
3600s	157	16	71. 43	93. 75	96. 85
Total	1233	1233	97. 70	96. 43	**97. 08**

是设置正确的参数矩阵比较困难,特别是在误报率与漏报率之间无法找到平衡点. 文献[11]中使用了统计推断和 α 稳定模型来识别网络流量中的异常,针对两种流量类型 flood 和 flash 合计 8 种类别的实验识别率为 77.4% ~93.0%.

基于规则的分类方法主要由专家编写检测规则,其检测准确率高,但是过于依赖专家知识与规则,对于新出现的、未知的的攻击则无法有效识别. 比如文献[19]中采用的基于行为规则的入侵检测系统其实验检测精度高达 99.3%,但同时其误报率也高达 6.87%.

基于神经网络的方法在实践中面临的主要问题是单层 ANN 对事件的分类准确率仅仅达到 81% 左右,分类效果不够理想,而多层 ANN 对训练集的分类准确率达到 99% 以上,但对实际真实数据的分类效果却非常差,出现了过拟合情况,无法应用于实践.

4.2 基于 GP 安全规则自动生成算法实验结果及对比分析

而对于安全规则自动生成算法,其实验样例数据仍是 MACCDC 2012 数据集中的 FTP 攻击,但安全规则自动生成算法的输入则来自于 4.1 中事件分类算法输出的分类结果。下表 5 显示了生成算法针对 FTP 攻击每一次演化迭代时生成的个体数目及最小,平均及最优适应度数值. 图 10 显示了整体适应度数值的趋势图,其中最佳匹配个体在第 33 次迭代时产生,其适应度值为 94.0029%.

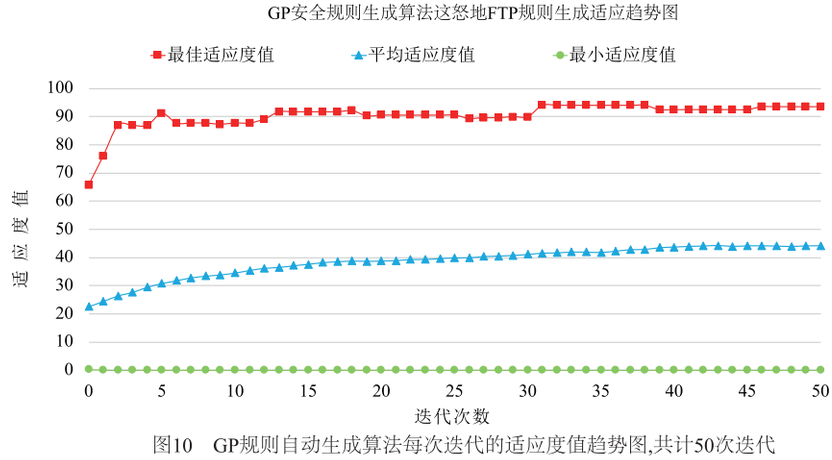


图10 GP规则自动生成算法每次迭代的适应度值趋势图,共计50次迭代

表 5 GP 安全规则生成算法针对 FTP 攻击生成检测规则时每代个体数目与适应度数值列表

迭代次数	个体数目	适应度均值	适应度最小值	最佳适应度值(%)
0	1000	9.0213	0.0458	50.7856
1	747	12.1574	0	86.8334
2	743	14.0704	0	86.8334
…	…	…	…	…
30	743	41.1015	0	89.9445
31	757	41.5572	0	94.0029
32	731	41.6551	0	94.0029
33	**743**	**41.9451**	**0**	**94.0029**
34	748	41.9121	0	93.9832
…	…	…	…	…
48	750	43.9318	0	93.4891
49	728	44.138	0	93.4891
50	746	44.1772	0	93.4891

本文通过对 GP 规则生成算法中个体结构、交叉、变异方式进行优化和改进,有效地提高了匹配适应度值,经过多次重复迭代实验,寻找到最佳适应度出现的迭代次数范围,进行逐步优化. 下表 6 显示了规则生成算法针对不同攻击类型的实验结果对比分析. 可以看出,本文工作生成的安全规则适应度值和文献[16]相比得到了明显提升. 其它方法如文献[20]提出一种基于攻击图(Attack Graph)的关联规则算法,具备关联多步骤攻击的能力,实验显示其过滤率达到 95.58%,但其最大的问题是其检测能力主要基于已公布的漏洞信息如 CVE 等,对无法识别的、未知的攻击无法进行有效关联. 文献[21]提出一种使用隐马尔可夫模型(Hidden Markov Model,HMM)来对事件流进行数据挖掘的方法,其主要思路也是使用警报频率配合不同的时间窗口构建攻击场景并进行相应的报警关联,该方法具备对未知的新攻击事件进行预测的能力,其主要不足是实验结果的误报率较高,而且其实验结果仅仅分析了 DOS 攻击这一种攻击类型,普适性不足.

表 6　GP 安全规则生成算法对不同攻击类型检测的实验结果对比分析

(a) 文献[16]规则生成算法针对不同攻击类型的适应度值		(b) 本文工作规则生成算法针对不同攻击类型的适应度值	
攻击类型	Best Fitness	攻击类型	Best Fitness
Bredavi trojan A	75.7	FTP	94.00
Bredavi trojan B	79.1	SMTP	93.44
Conficker solaris	79.5	SQLInj	78.14
Dell remote access	79.5	DNS	75.36
Brute force SSHD	77.5	DDOS	88.76
Port scan	79.4	SCAN	88.01
Spyware	80.6	EXPLOIT	90.79
Telnet worm	80.9	ICMP	86.88
Web scan	79.5	WEB	81.70

4.3　整体实验结果及分析

实验 4.1 及 4.2 中均使用了 FTP 的攻击样例数据对算法进行了评估与分析。由于前人相关工作中并未出现相同数据类型的实验数据结果,仅出现了 DDOS 攻击类型的实验结果,因此,本文使用 MACCDC 2012 数据集中 DDOS 攻击和文献[16]中的分类及规则适应度结果进行了对比分析. 文献[16]对 DDOS 攻击的分类准确率为 81%,而本文方法分类效果准确率达到了 97.08%,分类效果明显提高. 使用 GP 规则生成算法中的适应度则由平均 79.5% 提高至 88.76%,得益于本文工作对 GP 个体结构,变异方式的重新定义,提高了精确率与召回率.

此外,本文提供了攻击类型更加丰富的实验结果,针对多种其它类型攻击如 DDOS,DNS,SMTP,WEB-ATTACK,SQL-INJECTION,EXPLOIT,SCAN 和 ICMP 等其它类型攻击也分别进行了实验验证. 详细实验数据见下表 7. One-Class SVM 分类算法的分类准确率范围为 88.85 ~ 98.84(%),其中 EXPLOIT 攻击由于数据样本偏少导致其分类结果偏低,其他攻击类型准确率均高于 94%,分类效果较好. 而 GP 安全规则生成算法由于以 F1-Score 作为其适应度指标,结果更为均衡,适应度值范围为 75.36 ~ 94.0(%). 而文献[16]中针对不同攻击的适应度均在 75.7 ~ 80.9(%)区间.

文献[16]的实验结果仅包含两类攻击 DDOS 和几种 Metasploit Exploit 漏洞利用,并没有给出具体的实验分类精确率,召回率及准确率结果,仅给出部分适应度结果. 本文提供了更多的攻击种类,且每种攻击的分类效果更为突出,生成的规则适应度更优,丰富了 OSSIM 的检测攻击种类.

表 7　SVM 安全事件分类算法和 GP 安全规则生成算法对不同攻击类型检测的实验结果

攻击类型	One-Class SVM 安全事件分类算法(%)			GP 安全规则生成算法(%)				
	Precision	Recall	Accuracy	TP	FP	TN	FN	Best Fitness
FTP	97.70	96.43	97.08	96.26	3.74	71.84	28.16	94.00
DDOS	88.89	88.89	94.32	91.48	8.52	69.23	30.77	88.76
DNS	82.35	89.36	98.47	63.96	36.04	95.90	4.10	75.36
SMTP	91.67	89.79	94.51	96.03	3.97	87.88	12.12	93.44
WEB	94.07	96.88	96.31	76.71	23.29	87.37	12.63	81.70
SQLInj	92.29	82.92	97.51	72.75	27.25	96.36	3.64	78.14
EXPLOIT	93.91	83.08	88.85	99.04	0.96	76.47	23.53	90.79
SCAN	97.51	91.32	95.14	83.89	16.11	91.54	8.46	88.01
ICMP	98.82	98.85	98.84	81.47	18.53	87.09	12.91	86.88

4.4　部署于生产环境 OSSIM 系统实验结果及分析

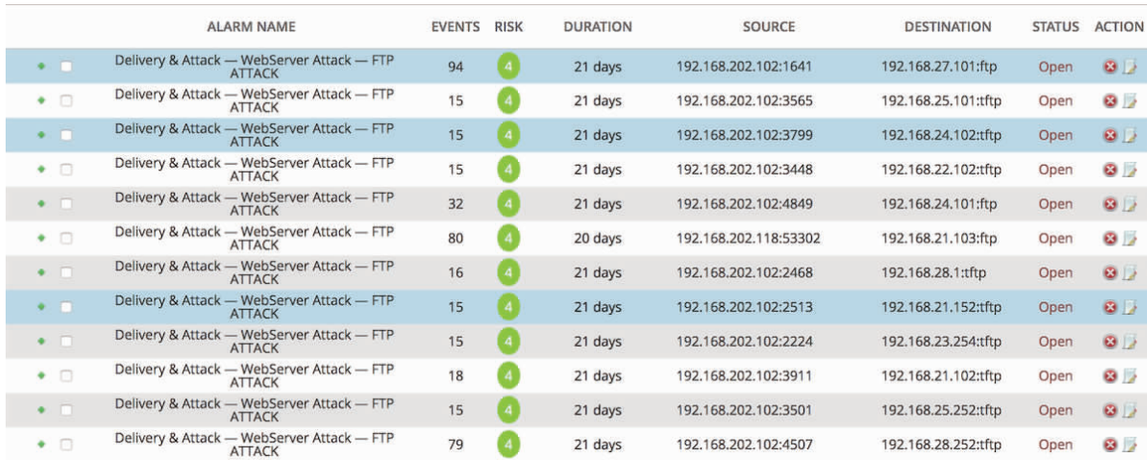
为了评估本文方法的实际效果,在实际生产环境中同时部署了两套 OSSIM 系统,其中一个是单独的 OSSIM 系统,另外一套则添加了本文提出的规则生成框架. 以 FTP 攻击检测为例,实际检测结果如图 11 所示.

默认 OSSIM 系统无法检测 FTP 攻击,仅由传感器报告出少量的 INFO 事件.

部署本文框架后的 OSSIM 系统共检测到 10,008 次攻击事件,生成 340 个警报. 除此之外,实验结果显示相似攻击被分组到一起,减少了冗余报警,每个分组事件的数量范围从 15 至 712,表明最低仅 15 次安全事件即可生成报警,本文提出的方法具有很高的检测灵敏度.

5　结论

本文提出了一种基于 One-Class SVM 和 GP 的关联规则自动生成方法来自动生成关联规则. 该方法具备了自适应能力来对未知的攻击或漏洞进行检测和报警,可自动化生成部署于实际生产环境中的关联规则,减少了人工专家参与,提高了效率. 生成的规则检测准



ALARM NAME	EVENTS	RISK	DURATION	SOURCE	DESTINATION	STATUS	ACTION
Delivery & Attack — WebServer Attack — FTP ATTACK	94	4	21 days	192.168.202.102:1641	192.168.27.101:ftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	15	4	21 days	192.168.202.102:3565	192.168.25.101:tftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	15	4	21 days	192.168.202.102:3799	192.168.24.102:tftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	15	4	21 days	192.168.202.102:3448	192.168.22.102:tftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	32	4	21 days	192.168.202.102:4849	192.168.24.101:ftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	80	4	20 days	192.168.202.118:53302	192.168.21.103:ftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	16	4	21 days	192.168.202.102:2468	192.168.28.1:tftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	15	4	21 days	192.168.202.102:2513	192.168.21.152:tftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	15	4	21 days	192.168.202.102:2224	192.168.23.254:tftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	18	4	21 days	192.168.202.102:3911	192.168.21.102:tftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	15	4	21 days	192.168.202.102:3501	192.168.25.252:tftp	Open	
Delivery & Attack — WebServer Attack — FTP ATTACK	79	4	21 days	192.168.202.102:4507	192.168.28.252:tftp	Open	

图11 本文方法生成的规则应用在OSSIM系统中可成功检测到FTP攻击

确率高,具备良好的实际应用能力.

下一步工作主要基于以下三点继续对框架进行增强:(1)对于攻击事件的 IP 及端口分布信息,可结合威胁交换社区信息对攻击进行精确定位,以快速准确检测恶意活动.(2)优化与改进现有的分类模型,以支持更多的分类能力.(3)为 GP 规则生成算法添加更多个体属性以生成适应度更佳的匹配个体.

参考文献

[1] OSSIM:The Open Source SIEM AlienVault [EB/OL]. https://www. alienvault. com/products/ossim,2017-6-20.

[2] Hall D L,Llinas J. An introduction to multisensor data fusion[J]. Proceedings of the IEEE,1997,85(1):6 – 23.

[3] Lee W,Stolfo S J. Data mining approaches for intrusion detection[A]. USENIX Security Symposium[C]. San Antonio,TX:USENIX,1998. 79 – 93.

[4] Valdes A,Skinner K. Probabilistic alert correlation[A]. International Workshop on Recent Advances in Intrusion Detection[C]. Berlin,German:Springer,2001. 54 – 68.

[5] Suarez-Tangil G,Palomar E,de Fuentes J M,et al. Automatic Rule Generation Based on Genetic Programming for Event Correlation[M]. Computational Intelligence in Security for Information Systems. Berlin,German: Springer,2009. 127 – 134.

[6] Margara A,Cugola G,Tamburrelli G. Learning from the past:automated rule generation for complex event processing[A]. Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems[C]. New York,NY:ACM,2014. 47 – 58.

[7] Hasan A,Teymourian K,Paschke A. Probabilistic event pattern discovery[A]. International Symposium on Rules and Rule Markup Languages for the Semantic Web[C]. Berlin,Germany:Springer,2015. 241 – 257.

[8] Ning P,Cui Y,Reeves D S. Constructing attack scenarios through correlation of intrusion alerts[A]. Proceedings of the 9th ACM Conference on Computer and Communications Security [C]. New York,NY: ACM,2002. 245 – 254.

[9] Lunt T F,Tamaru A,Gillham F. A Real-Time Intrusion-Detection Expert System (IDES)[M]. Menlo Park,CA: SRI International. Computer Science Laboratory,1992.

[10] Mitchell R,Chen R. Behavior-rule based intrusion detection systems for safety critical smart grid applications[J]. IEEE Transactions on Smart Grid,2013,4(3):1254 – 1263.

[11] Brugger S T. Data mining methods for network intrusion detection[J]. University of California at Davis,2004:234 – 237.

[12] Bykova M,Ostermann S,Tjaden B. Detecting network intrusions via a statistical analysis of network packet characteristics[A]. System Theory,2001. Proceedings of the 33rd Southeastern Symposium on[C]. Piscataway,NJ: IEEE,2001. 309 – 314.

[13] Simmross-Wattenberg F,Asensio-Perez J I,Casaseca-de-la-Higuera P,et al. Anomaly detection in network traffic based on statistical inference and \alpha-stable modeling [J]. IEEE Transactions on Dependable and Secure Computing,2011,8(4):494 – 509.

[14] Lee O J,Jung J E. Sequence clustering-based automated rule generation for adaptive complex event processing [J]. Future Generation Computer Systems,2017,66:100 – 109.

[15] Javaid A,Niyaz Q,Sun W,et al. A deep learning approach for network intrusion detection system[A]. Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)[C]. Brussels,Belgium: ICST

(Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016. 21 – 26.

[16] Bankovic′ Z, Stepanovic′ D, Bojanic′ S, et al. Improving network security using genetic algorithm approach[J]. Computers & Electrical Engineering, 2007, 33(5): 438 – 451.

[17] Schölkopf B, Smola A J, Williamson R C, et al. New support vector algorithms[J]. Neural Computation, 2000, 12(5): 1207 – 1245.

[18] MACCDC: National cyberWatch mid-atlantic collegiate cyber defense competition (MACCDC)[EB/OL]. https://www.netresec.com/? page = MACCDC, 2017-6-20.

[19] Suarez-Tangil G, Palomar E, Ribagorda A, et al. Providing SIEM systems with self-adaptation[J]. Information Fusion, 2015, 21: 145 – 158.

[20] Roschke S, Cheng F, Meinel C. A new alert correlation algorithm based on attack graph[J]. Computational Intelligence in Security for Information Systems, 2011: 58 – 67.

[21] Farhadi H, AmirHaeri M, Khansari M. Alert correlation and prediction using data mining and HMM[J]. The iSC international Journal of information Security, 2011, 3(2): 77 – 101.

作者简介

杜栋栋　男,1983 年生于河南安阳. 2013 级北京大学信息科学技术学院博士研究生,主要研究领域为网络信息安全,领域知识图谱,大数据与机器学习.

E-mail:dudong@pku.edu.cn

任星彰　男,1993 年生于山西孝义,2016 级北京大学软件与微电子学院硕士生,主要研究领域为情景感知,网络安全,机器学习.

赵　文(通信作者)　男,1967 年出生于辽宁大连,北京大学软件工程国家工程研究中心研究员,博士生导师. 主要研究领域为软件工程,领域知识图谱.

E-mail:zhaowen@pku.edu.cn