基于博弈论的入侵检测与响应优化综述

张杭生[1,2], 刘吉强[3], 梁 杰[1,2], 刘海涛[1,2], 李 婷[1,2], 耿立茹[1], 刘银龙[1,2*]

[1]中国科学院信息工程研究所 北京 中国 100093
[2]中国科学院大学网络空间安全学院 北京 中国 100049
[3]北京交通大学智能交通数据安全与隐私保护北京市重点实验室 北京 100044

摘要 当前网络规模急剧增加, 各类入侵过程也逐渐向复杂化、多样化的趋势发展。网络攻击带来的损失越来越严重, 针对各类安全事件的检测发现以及查处响应也变得日益困难。为了快速识别各类网络安全事件并做出相应的响应, 入侵检测与响应技术变得越来越重要。入侵检测系统(IDS)能否识别复杂的攻击模式以及分析大量的网络流量主要取决于其精度和配置, 这使得入侵检测与响应的优化问题成为网络与系统安全的重要需求, 并且成为一个活跃的研究主题。现有的研究成果已经提出了很多可以优化入侵检测和响应效率的方法, 其中, 将博弈论应用在入侵检测与响应的研究日益增多。博弈论提供了一种框架去捕获攻击者和防御者的交互, 采用了一种定量的方法评估系统的安全性。本文在分析了入侵检测与响应系统和博弈论的基本原理的基础上, 介绍了当前基于博弈论的入侵检测与响应优化问题的现有解决方案, 并且讨论了这些解决方案的局限性以及给出了未来的研究方向。首先, 详细介绍了入侵检测与博弈论的背景知识, 回顾了常用的入侵检测系统基本原理, 评估方法, 常用的数据集以及经典的安全领域中的博弈论模型。其次, 按照基于博弈论的入侵检测与响应优化问题的类型进行了分类介绍, 根据攻击的先后顺序对网络安全架构优化、IDS 配置与效率优化、IDS 的自动化响应优化以及分布式入侵检测架构优化等技术的研究现状进行归纳、分析、总结, 并分析了现有方案的优缺点, 进而分析可能的解决方案。然后针对将博弈论应用于入侵检测与响应中面临的挑战进行了分析与讨论。最后展望了未来的研究方向以及发展趋势。

关键词 博弈论; 入侵检测; 入侵响应; 多智能体强化学习; 网络安全
中图法分类号 TP393 DOI 号 10.19363/J.cnki.cn10-1380/tn.2022.12.06

A Survey on Optimizing Intrusion Detection and Response Based on Game Theory

ZHANG Hangsheng[1,2], LIU Jiqiang[3], LIANG Jie[1,2], LIU Haitao[1,2], LI Ting[1], GENG Liru[1], LIU Yinlong[1,2*]

[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]University of Chinese Academy of Sciences, Beijing 100049, China
[3]Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China

Abstract In recent years, cyber-attacks have caused an increasing number of serious losses. It has become increasingly important to use intrusion detection and response technology in order to identify various security incidents quickly and respond accordingly. Detecting complex attack patterns and analyzing large volumes of network traffic depends largely on the accuracy and configuration of an intrusion detection system (IDS). In this context, intrusion detection and response optimization are important security requirements for networks and systems, and have become an active research topic. Many methods have been proposed in the research literature that can enhance intrusion detection and response efficiency. There has been a rapid growth in the use of game theory among these applications of intrusion detection and response. A quantitative method of evaluating the security of a system is based on the game theory, which provides a framework for capturing the interaction between attackers and defenders. Based on an analysis of the basic principles of intrusion detection and response systems and game theory, the paper discusses existing approaches to improving intrusion detection and response using game theory, discusses their limitations, and offers directions for future research based on these solutions. First of all, the background knowledge of intrusion detection and game theory is presented in detail, reviewing the basic principles of commonly used intrusion detection systems, evaluation methods, commonly used datasets and classical game theoretic models in the security domain. Second, the types of intrusion detection and response optimization problems based on game theory are categorized and introduced. According to the order of attacks, the research status of technologies such as network security architecture optimization, intrusion detection system configuration and efficiency optimization, IDS automated response optimization, and distributed intrusion detection architecture optimization is summarized, ana-

通讯作者: 刘银龙, 博士, 副研究员, Email: liuyinlong@iie.ac.cn。
本课题得到中国国家重点研发计划(No. 2021YFB2910108)和 2021 年重庆市属本科高校与中科院所属院所合作项目(No. HZ2021015)资助。
收稿日期: 2020-06-17; 修改日期: 2020-11-02; 定稿日期: 2022-12-07

lyzed, and concluded. Meanwhile, the advantages and disadvantages of existing solutions are also analyzed, and then possible solutions are analyzed. We then analyze and discuss the challenges associated with applying game theory to intrusion detection and response. Finally, we look forward to the future direction of research and development.

Key words game theory; intrusion detection; intrusion response; multi-agent reinforcement learning; cyber security.

1 概述

由于互联网的快速发展, 网络规模逐渐扩大, 网络面临攻击的情况也显著增加。在人们的生活与互联网变得更加密不可分的同时, 网络安全问题也在影响着整个国家和社会的稳定。因此, 确保网络系统的安全已成为了一项艰巨的任务。然而, 传统的网络安全解决方案, 如防火墙和反病毒系统, 已经无法应对复杂的网络攻击。为了应对这些挑战, 并缓解未知威胁, 作为防火墙技术的合理补充, 入侵检测系统(Intrusion Detection System)被部署并迅速成为保护信息系统的重要组件, 提高了网络安全管理系统的安全管理能力。

入侵检测[1]是对已经发生、正在进行以及即将发生的入侵行为进行识别的技术[2]。它通过收集和分析计算机网络或者操作系统的关键信息, 从中发现违反安全策略的行为以及被攻击的痕迹。一种特殊的入侵检测技术—入侵防御, 可以在攻击到达系统之前对其进行阻止。入侵防御区别于一般的入侵检测, 它不仅能识别潜在威胁, 还能快速做出回应, 是一种能够监控网络传输行为, 同时阻止一些异常的或具有伤害性的网络行为的安全技术。完全针对于入侵进行自动化对策响应的技术称为入侵响应[3-5]。入侵检测与响应打通了检测、发现、预警、响应的闭环防御体系, 提高了系统的安全防护能力。

入侵检测最大的挑战是难以分析成千上万的警报。而将警报按照重要程度进行分类是触发适当的响应并减轻网络威胁所需的重要步骤。很多研究工作在提高入侵检测的检测效率[6-8]上取得了有效的成果, 但是这些工作没有关注入侵检测的优化问题。博弈论为我们提供了新的视角看待安全问题: 安全不是没有威胁, 而是攻击系统比不攻击系统代价更加昂贵。研究人员将博弈论应用于入侵检测优化中, 提供在特定资源约束下对于给定问题的最佳折衷方案, 解决诸如需要优先监视的网络节点的选择或者攻击后需要部署入侵防御系统(Intrusion Prevention System)的最佳选择等问题。

博弈论是一种充分考虑攻击者和系统的行为以及攻击者对防御策略的影响的理论框架。过去十年, 将博弈论应用在网络安全领域已经是一个热门的主题。我们可以在文献[9-13]中充分了解相关的研究工作。由于一些限制导致博弈论的方法没有在 IDS 优化问题上广泛应用, 除了一些特殊的网络, 比如移动自组织网(MANET)[14]。但是博弈论已经成功应用在真实世界的安全问题[15]中, 包括机场安全[16], 海岸警卫队安全[17]以及公共系统安全[18]等。因此我们有理由相信博弈论的方法可以像应用于真实世界的安全问题一样大规模部署在网络安全领域, 特别是将其应用于入侵检测与响应优化问题中。

在本文中, 我们对将博弈论应用于入侵检测与响应优化问题进行了分类, 同时介绍了优化问题所需要解决的挑战。文章的组织如下: 第二节简单介绍了入侵检测技术; 第三节介绍了博弈论的背景; 第四节介绍了博弈论应用于入侵检测与响应优化中的分类, 按照攻击的先后顺序将其分为网络安全架构优化、IDS 配置与效率优化、IDS 的自动化响应优化以及分布式入侵检测架构优化; 第五节讨论了这些方法的局限性; 在第六节中, 我们得出了结论, 并且展望了该领域未来的发展。

2 入侵检测简介

入侵检测技术是为保证计算机网络与操作系统的安全而设计的能及时发现系统中的未授权以及异常行为的一种信息安全技术。它不但能识别计算机网络的外部攻击, 还能发现内部的一些非授权的网络行为。经过几十年的发展, 入侵检测技术从最初单纯的研究思路和理论模型, 已经发展出了种类繁多的原型系统以及商用的产品。

2.1 入侵检测的分类

入侵检测技术发展迅速, 根据不同的分类标准, 可以分为不同的类别。

2.1.1 根据检测数据源区分

根据检测的数据源的不同, 入侵检测可以分为基于主机的入侵检测(HIDS), 基于网络的入侵检测(NIDS)和混合入侵检测(Hybrid IDS)。早期的入侵检测系统是基于主机的入侵检测系统。

(1) 基于主机的入侵检测的数据源主要是: 操作系统和应用程序的日志, 系统调用以及安全审计记录。它的缺点是占用主机的资源, 且需要依赖主机的可靠性; 优点是能直接发现发生在主机上的入侵事

件, 检测的准确性以及效率较高。

(2) 基于网络的入侵检测的数据源是网络数据流, 它通过对网络数据包进行采集分析, 从而发现入侵事件。它的缺点是无法得到主机系统的实时状况, 误报率较高; 优点是独立于被保护网段内的主机, 不影响主机的运行性能。

(3) 结合基于主机和网络的入侵检测的优点, 混合入侵检测应运而生。它分析的数据源来自网络流量和主机操作系统的日志等本地信息, 该系统结合了以上两种入侵检测的数据分析方法, 检测的手段更加科学, 能够更加准确地发现入侵行为。但是需要处理的数据源较多, 覆盖面广, 因此大量的报警日志需要进行聚合以及关联分析。

2.1.2 根据检测方法区分

入侵检测根据不同的检测方法可以分为误用检测, 异常检测和基于规范的检测。

(1) 误用检测(基于规则)

误用检测是基于特征的检测, 该方法首先用特定的模式表示已知的入侵行为, 从而形成网络攻击规则库。然后将待分析的数据流进行适当处理, 提取的特征与规则库中的特征进行对比, 如果匹配成功, 就产生告警。该方法的优点是能准确产生已知攻击的告警, 识别出网络攻击的类型; 缺点是无法识别未知的攻击, 漏报率较高。

(2) 异常检测

异常检测是应用无监督或弱监督的方法, 针对不平衡数据进行多分类的技术, 且往往异常点对我们更为重要, 检测的结果还需要具有一定的可解释性。异常检测首先统计出正常活动的规律, 建立一个关于系统正常活动的状态模型, 然后将待检测的活动与状态模型进行对比, 与正常活动规律不符的行为被识别为入侵行为。异常检测的优点是能够识别未知的攻击, 而且不需要维护庞大的网络攻击特征库, 漏报率低。缺点是无法识别入侵行为的类型, 误报率高, 且无法应用于大规模的系统中[21]。异常检测经常与人工智能结合, 比如基于自动编码器的异常检测[22]。

(3) 基于规范的检测

基于安全规范的入侵检测技术将异常检测和误用检测有机结合, 减少了误报率和漏报率。首先我们制定相应的安全规范表示程序的期望行为, 然后将用户的行为与安全规范进行对比, 如果不一致则表示发生了异常行为。他不仅能识别已知攻击。还能识别出未知的攻击[23-24]。

2.1.3 根据是否包含响应区分

由于选择响应的成本和复杂度很高, 以及如果选择了不恰当的对策, 可能对系统造成意想不到的后果, 现在的大多数IDS还是被动组件[25-26]。被动 IDS 只检测告警信息而不进行响应, 但是主动 IDS 识别网络攻击之后激活响应, 比如 IPS 和 IRS。

2.2 入侵检测性能评估

评估 IDS 的性能[27]包括评估 IDS 检测攻击的效率以及 IDS 的误报率, 大体的评估性能指标是:

- 真阳性: 恶意的行为被 IDS 成功检测
- 假阳性: 常规的行为被 IDS 检测为恶意行为
- 真阴性: 常规的行为被 IDS 识别正确
- 假阴性: 恶意的行为没有被 IDS 检测出来

IDS的性能会使用(接收者行为特征)ROC曲线[28]来进行对比。

评估 IDS 的相关指标还有阳性预测值(PPV), 这指的是 IDS 发出的警报占实际入侵的概率, 可以使用贝叶斯定理计算[29]:

$$\mathrm{P}(I \mid A)=\frac{\mathrm{P}(I)\mathrm{P}(A \mid I)}{\mathrm{P}(I)\mathrm{P}(A \mid I)+\mathrm{P}(\neg I)\mathrm{P}(A \mid \neg I)}$$

其中, I 表示入侵事件, A 表示告警事件, $\mathrm{P}(A \mid I)$ 表示真阳率, $\mathrm{P}(A \mid \neg I)$ 表示假阳率。我们知道, 正常活动的概率 $\mathrm{P}(\neg I)$ 通常远大于恶意活动的概率 $\mathrm{P}(I)$ 。在 DDOS 攻击中, PPV 可能并不重要, DDOS 检测的 PPV 可能接近于 1, 但是 DDOS 产生真阳性的警报很多, 使得一些重要告警淹没在这些告警中。

2.3 入侵检测的基准数据集

对入侵检测的算法和技术的评估需要有设计良好的数据集, 我们列举一些知名的数据集。

(1) DARPA1998/1999[30]

美国空军在局域网搭建了一个网络环境, 收集了 9 周时间的网络连接和系统日志。仿真各种不同的攻击手段, 主要是四种攻击类型: DOS(拒绝服务攻击), R2L(远程用户攻击), U2R(提权攻击), Probing Attack(端口扫描攻击)。

(2) KDD Cup 99

WenkeLee 等研究者[31]采用数据挖掘等技术对DARPA98/99数据集进行数据预处理与特征提取, 形成了新的数据集, 每个连接用 41 个特征来描述。包括: 9 个 TCP 连接基本特征, 13 个 TCP 连接的内容特征, 9 个基于时间的网络流量统计特征, 10 个基于主机的网络流量的统计特征。

(3) NSL-KDD

加拿大网络安全研究所(CIC) [32]改进了 KDD Cup99 数据集, 克服了 Cup 99 数据集中由于冗余数

据导致的分类器偏向重复出现记录的不足, 对正常和异常的数据比例进行了合适选择, 测试和训练数据更加合理, 我们还列举了其他的知名数据集的情况如表 1 所示。

表 1　IDS 评估数据集的比较

Table 1　Comparison of datasets for IDS evaluation

数据集	引用	N=network H=host	真实的网络流	是否包含标签	时间是否持续	数据格式
DARPA'98/'99	文献[30]	N	×	√	√	PCAP
KDDCup'99	文献[31]	N	×	√	√	CSV
NSL-KDD'09	文献[32]	N	×	√	√	CSV
gureKDDCup'08	文献[33]	N	×	√	√	CSV
Sperotto'2008	文献[34]	N	√	√	×	FLOW
MAWILab'2012	文献[35]	N	√	√	√	PCAP
UNB ISCX'2012	文献[36]	N	×	√	×	CSV
CTU-13	文献[37]	N	√	√	√	P&F
ADFA-2013	文献[38]	H	√	√	×	CSV
UNSW-NB15	文献[39]	N	×	√	×	CSV
UGR'16	文献[40]	N	√	√	√	FLOW
CICID2017	文献[41]	N	×	√	√	PCAP

2.4　入侵检测的集成

入侵检测最大的挑战就是分析入侵检测系统发出的警报。发生入侵时, 选择对策所需的时间应该尽可能短, 确保有效缓解入侵而不会导致系统功能失常。在大规模系统和关键基础架构中, 入侵检测系统通常集成在安全信息和事件管理(SIEM)[42]系统中。

SIEM 的目的是集中各种 IDS 发出的警报, 提供警报排序, 聚合关联和可视化工具。入侵检测过程可以类比为军事战略发展的“观察-导向-决定-行动”的循环过程。在入侵检测方面, 这四个阶段可以描述为: 检测, 关联, 诊断和响应。

- 检测: IDS 系统产生警报和日志
- 关联: 聚合警报以及关联警报
- 诊断: 通过复杂的数据挖掘来制定安全策略
- 响应: 系统中部署对策

该过程的重点是四个环节的动态循环, 以便评估系统对策的效率并根据下一次警报诊断调整安全策略。因此入侵检测应该被看成是一个持续的过程, 而不会随着对策的部署结束。

3　博弈论简介

博弈论[43]是研究具有斗争或者竞争性质现象的数学理论和方法, 主要的要素是局中人、策略和效用函数, 重要的概念是纳什均衡[44], 在该状态下, 所有局中人都没有理由改变自己的策略。

3.1　博弈论的分类

根据是否有约束协议可以分为合作博弈和非合作博弈; 根据双方对信息的了解程度可以分为完全信息博弈和非完全信息博弈; 根据行为的时间序列可以分为静态博弈和动态博弈; 根据表现形式可以分为战略型博弈和展开型博弈。对于入侵检测控制优化问题, 比较重要的两个博弈是双人零和静态博弈和随机博弈。双人零和静态博弈可以使用最小最大算法[45]求解纳什均衡。随机博弈是一种包含一个或多个参与者进行的具有状态概率转移的动态博弈。

3.2　博弈机器学习

机器学习和博弈论是人工智能的两个重要方向。机器学习通常假设数据依赖于要学习的模型, 用于研究的数据是预先存在的, 而且统计规律不因学习的过程本身而发生改变。博弈论假设玩家是完全理性的。但是现在的很多应用场景都不符合这两个假设。现实中的很多数据都是一个智能体和其他智能体博弈产生的, 所以为了更好地建模和研究真实的场景, 我们需要将传统的机器学习和博弈论相结合, 从数据中学习行为模型, 然后在博弈中产生新的数据, 继续辅助学习任务。

而入侵检测与响应是一个动态的过程, 数据是由攻击者和防御者博弈对抗产生的, 所以将博弈论与机器学习结合可以解决入侵检测中的很多优化问题[46]。将博弈论与机器学习最简单的结合就是生成对抗网络。我们可以将生成对抗网络看做是一个二人零和博弈, 生成器的策略是如何更好地生成样本, 判别器的策略则是如何判定样本的真实性。因此, 策

略组(“生成好样本”, “真假难辨”)是一个纳什均衡, 将博弈论和机器学习进行更加紧密结合的研究是刘铁岩等[47]研究员提出的博弈机器学习。人类的行为一般是有规律可行的, 人与人之间的交互可以被建模, 博弈机器学习利用这一特性, 将行为模型和决策模型相结合, 将从数据中学习的任务形成闭环, 更加有效地利用决策产生的数据进行学习, 还能循环更新学习到的模型。

3.3 安全博弈论

安全部门和攻击者之间的博弈通常被建模的Stackelberg博弈, 也称为安全博弈论。Stackelberg博弈是由领导者和跟随者构成的双人博弈。领导者首先选择混合策略, 跟随者通过观察得到领导者策略, 然后选择能够最大化其收益的策略进行博弈。Stackelberg博弈的每个参与者还可以拓展成有多种可能的类型, 每种类型收益值不同, 称为贝叶斯Stackelberg博弈。Stackelberg博弈模型是早在20世纪30年代提出来的[49]。Stackelberg博弈在有限安全资源优化调度中的应用是在2006年Vincent Conitzer和Tuomas Sandolm发表的奠基性论文[50]后迅速发展起来的。近年来, 安全博弈论[48]的研究取得了很大的进展, 研究者们不断提出适用于不同问题场景的Stackelberg博弈均衡策略求解算法。这些算法已经被美国不同领域的安全机构所使用。这些成功的应用为安全博弈论应用在网络安全领域的研究带来的希望。

4 博弈论应用在入侵检测与响应优化中的分类

我们按照攻击的先后顺序将博弈论应用于入侵检测和响应优化问题分为三个阶段和整体架构设计, 其中第二阶段又可以进一步被细分为三个部分。

(1) 第一阶段: 攻击前的网络安全架构优化

(2) 第二阶段: 攻击中IDS配置与效率优化: 包括IDS安全资源分配优化, IDS配置优化以及IDS检测率优化。

(3) 第三阶段: 攻击后的自动化响应优化

(4) 整体架构设计主要是基于合作博弈的分布式入侵检测架构优化。

首先, 我们介绍这些研究工作需要使用的求解算法。

4.1 求解算法

网络安全架构优化的基础模型是Stackelberg博弈模型, Stackelberg博弈的求解算法主要有MultiLPs[50]算法, DOBSS[55]算法和ERASER[56]算法。而IDS配置优化, 自动化响应以及分布式入侵检测架构优化的求解可以使用多智能体近似纳什均衡的求解算法。

4.1.1 Stackelberg的求解算法

(1) MultiLPs[50]算法

Conitzer和Sandholm于2006年提出MultiLPs算法, MultipleLPs是针对标准型的Stackelberg博弈求解的最基本多项式时间的算法, 它也可以用来求解贝叶斯Stackelberg博弈, 但是需要将收益矩阵通过海萨尼转换变成标准型, 这会使得求解时间随着追随者类型指数级增长。

(2) DOBSS[55]算法

不同类型的追随者是相互独立的, 所以所有可能追随者的纯策略组合爆炸。如果使用MultiLPs算法求解, 那么算法的时间复杂度会随着跟随者的种类指数级增长。DOBSS算法是第一个成功的应用在实际系统上的算法, 它利用跟随者的类型相互独立的特点将这一问题进行降解, 从而将其转化成求解一个混合整数规划问题(MILP)。

(3) ERASER[56]算法

ERASER算法的基本思想和DOBSS一样, 但是它直接对紧凑型的安全博弈进行求解, 这样, 它就可以避免枚举指数级的保护者的纯策略。

4.1.2 近似纳什均衡求解算法

IDS博弈模型的近似求解算法分为基础算法, 分布式算法以及基于深度强化学习的算法。

(1) 基础算法

Minimax-Q算法试用于零和随机博弈; Nash Q-Learning[72]算法将零和博弈扩展到一般和随机博弈; Friend-or-Foe Q-Learning算法[73]可以将n智能体的一般和博弈转化成一个两智能体的零和博弈; WOLF-PHC算法是一种求解混合策略的多智能体强化学习算法。WOLF-PHC[74]算法能够收敛到纳什均衡策略, 并且具有合理性。如果其他智能体采用固定策略的时候, 该算法也能收敛到最优策略而不是可能效果不好的纳什均衡策略。

(2) 分布式算法

分布式算法是指没有中心控制节点, 且每个智能体在不知道全局信息的情况下通过与环境交互学习到纳什均衡的算法。每个智能体只知道自己的奖励值, 不知道环境和其他智能体的奖励函数, 也不知道其他智能体的策略。该算法的难点是如何在不完全信息的情况下使得每个智能体收敛到那什均衡点。算法分为学习自动机和梯度提升。

- 学习自动机：该算法是通过与环境交互获得奖励值，从而修正动作空间的概率分布，提升优化策略的算法。
- 梯度提升：该算法使策略的更新方向沿着累积回报增加最大的梯度方向。

(3) 多智能体深度强化学习算法

对于多智能系统，环境是动态不稳定的，所以基于经验回放的DQN算法和基于策略梯度的算法都不适用。文献[57]提出了MADDPG算法在不需要知道环境的动力学模型的情况下得到收敛解。该算法不仅能用于合作环境，也能用于竞争环境。

4.2 研究现状

我们对基于博弈论的入侵检测与响应优化问题的类型进行分类介绍。本节我们将对这些主题进行系统性介绍。攻击前的网络安全架构优化关注的是网络系统的安全资源调度问题，优化的目标是使用有限的资源尽可能地加固现有的网络系统。我们将攻击中的 IDS 配置与效率优化问题分成三个部分，第一部分是 IDS 安全资源分配优化，优化目标是使用有限的 IDS 资源去保护相对更加重要的节点和链路，最后安全管理员可以根据博弈均衡的结果重新分配IDS的资源；第二部分是IDS配置优化，关注的是基于规则的 IDS 规则库的动态选择和 IDS 灵敏度调整；第三部分是IDS检测率优化，应用生成对抗网络提高多元数据的异常检测的精度以及僵尸网络的检测效率。攻击后的自动化响应优化使得一旦发现攻击就触发最佳的防御策略，无需依靠管理员的手动干预，该项工作主要是优化系统反应，而不是 IDS 性能。分布式入侵检测架构优化表示为各个入侵检测系统设计良好的通讯机制和协商机制，使得不同的检测传感器可以聚合关联产生高效的告警信息。各个主题优化的具体情况如表 2 所示。

4.2.1 网络安全架构优化

网络安全架构优化的核心模型是 Stackelberg 博弈模型。Stackelberg 安全博弈最开始应用在现实生活的安全领域，进行安全资源调度，后来被运用在网络安全资源调度中。

在文献[58]中，王震等研究者针对企业级网络中存在的漏洞日益增多的情况，将企业网络漏洞之间的复杂依赖关系进行建模，构建漏洞依赖图(漏洞依赖图模型如图 1 所示)，并在此基础上建立 Stackelberg 攻防博弈模型，同时考虑了传统求解算法在求解实际网络规模中存在的困难，引入双模块算法。

文献[59]提出了一种使用有限资源加固网络的方法，建立了一种新的互动博弈模型，将攻击者可能的计划使用攻击图紧凑表示，如图 2 所示。而防御者则添加假目标(蜜罐)欺骗攻击者，攻击者策略的紧凑表示给计算带来了挑战，并且找到攻击者的最佳响应是 NP-hard 问题。作者提出了策略搜索和一系列的修剪技术解决了这个问题。

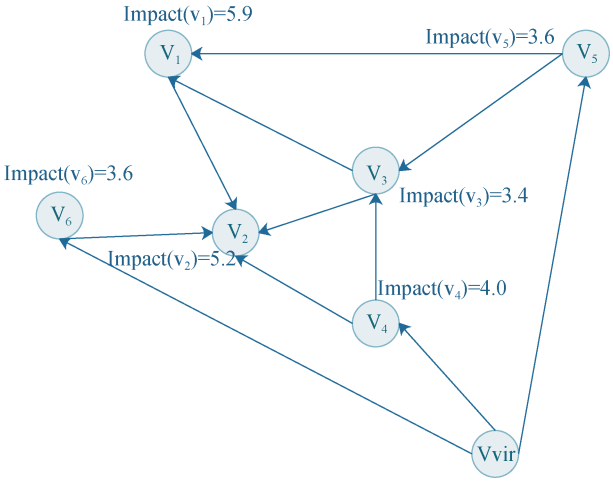


图 1 漏洞依赖图

Figure 1 vulnerability dependency graph

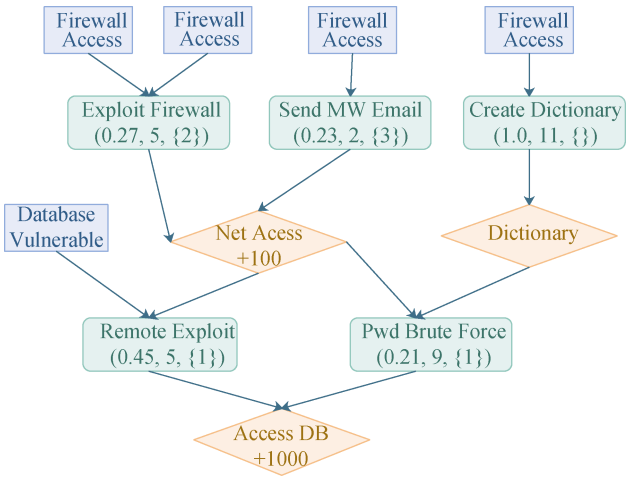


图 2 攻击图

Figure 2 attack graph

4.2.2 IDS 安全资源分配优化

IDS 安全资源优化的作用是识别出网络中重要的节点和链路并加以保护。当识别出重要的组件之后，我们根据博弈均衡的结果提供一种最优的防御资源分配方法。最后允许安全管理员根据博弈均衡的结果重新分配网络安全资源。针对 IDS 安全资源优化建立的博弈模型，我们可以使用多智能强化学习算法求解出近似纳什均衡。

第一项关于使用博弈论识别出重要链路和优化资源分配的研究是文献[60]。我们知道，NIDS 如

表 2 基于博弈论的 IDS 优化分类

Table 2 Classification of Game-Theoretic Approaches for IDS Optimization

攻击阶段	分类	文献	博弈模型	优化问题
攻击前	网络安全架构优化	文献[58]	Stackelberg 博弈	漏洞依赖图的控制优化
		文献[59]	Stackelberg 博弈	蜜罐的最佳部署
	IDS 安全资源分配优化	文献[60]	零和静态博弈	
		文献[61]	零和静态博弈	优化网络采样率
		文献[62]	不完全信息零和静态博弈	
		文献[63]	多玩家的非零和静态博弈	优化每个节点的资源分配
攻击中	IDS 配置优化	文献[65]	零和随机博弈	计算攻击者的攻击行为
		文献[66]	零和随机博弈	优化节点的防御资源部署
		文献[67]	动态信息的非零和博弈	配置 IDS 的灵敏度
		文献[68]	零和随机博弈	
		文献[69]	零和随机博弈	
		文献[70]	N+M 玩家的非零和随机博弈	挑选最优的攻击规则集
		文献[71]	N+M 玩家的非零和随机博弈	
	IDS 检测率优化	文献[75]	零和静态博弈	优化针对用户交互的 IDS 响应
		文献[78]		无监督多元异常检测
		文献[76]	二人零和博弈	僵尸网络检测
		文献[77]		规避入侵检测系统
攻击后	IDS 自动化响应优化	文献[79]	非零和随机博弈	优化网络节点的可用时间
		文献[80]	不完全信息零和贯序博弈	计算多步攻击的最优响应
		文献[81]	不完全信息非零和贯序博弈	
		文献[82]	零和随机博弈	决定何时驱逐检测到的攻击者
		文献[83]	Stackelberg 随机博弈	入侵响应和还原引擎
		文献[84]	非零和随机博弈	计算网络中的最佳对策
攻击整个阶段	分布式入侵检测架构优化	文献[85]		
		文献[86]	合作博弈	入侵检测的激励机制
		文献[87]		

果对每个数据包都检查, 需要很高的处理资源。在文献[60]中, 研究者开发了一种网络分组方法采样数据包, 在总资源预算一定的情况下, 通过合适的采样率采样不同路径的数据包, 减少采样花费, 缺点是一些攻击会被遗漏。作者定义一个简单的静态零和博弈去评估在固定的成本下最优的采样率。

对于网络中的每一条链路 e , 作者定义了链路中的网络流 f_e , 以及采样率 s_e, 总的预算为 $\sum_e s_e \leqslant B$, 使用上面的参数, 作者定义了检测恶意流量的概率为 $p_e = \frac{s_e}{f_e}$ 。攻击者的目的是选择一条路径去最小化检测率, 我们可以表示为如下的最小化问题

$$\min_{q \in V} \max_{P \in U} \sum_{P \in P_t^a} \mathrm{q}(P) \sum_{e \in P} p_e$$

其中 P_t^a 表示从节点 a 到目标节点 t 的路径集合, V 表示 P_t^a 上可行的概率分布集合, $\mathrm{q}(P)$ 表示路径 P 被检测系统检测到的概率, U 表示满足采样预算路径的集合。作者使用最大流算法求解这个博弈模型, 预测了攻击者的策略, 推导出了每一条链路的最优采样率, 作者还提出了两个启发式算法发现最优的网络流 f_e 从而最大化博弈的效用。

在文献[61]中, Otrok 扩展了文献[60]的模型, 将优化 NIDS 的问题扩展到 MANET 网络上, 特殊的地方是移动自组织网由一系列的集群组成, 每个集群由不同的节点组成, 为了优化能源消耗, 入侵检测被指派给一个单一的节点, 首先文章提出了一种群组长选举机制将运行 IDS 的节点作为最节省的节点, 然后提出一种非合作博弈建模在给定的集群中的入侵检测问题, 在这个模型中, 来自一般用户和恶意用户的使用者尝试在没有被检测到的情况下到达目标节点, 这个模型和文献[60]很像, 但是检测器事先不知道攻击者的类型, 检测器是非完全信息的, 贝

叶斯那什均衡求解问题被转化成一个最小最大的问题，使用近似那什均衡的求解算法进行求解。

Otrok[62]等研究者还关注了链路采样的碎片化问题。攻击者可以将从一个固定的节点到目标节点的攻击数据包分裂成多个片段。在这个模型中，攻击者的一部分恶意攻击碎片在没有被检测到的情况下到达目标即为攻击成功。对于多重合作的攻击者，恶意片段入侵网络，如果这些片段到达目标节点，则攻击成功。对于以上两种情况，作者建模为零和静态博弈模型。和文献[60]中的一样，恶意数据片段被检测到的概率为

$$\alpha_a = \sum_{P\in P_t^a} \mathrm{q}(P)\left(1-\prod_{e\in P}(1-p_e)\right)$$

防御者的目标是从 n 个数据片段中采样出 m 个恶意数据包，博弈的均衡求解问题像文献[49]中一样被公式化为最小最大问题，解决方法也是最大流算法。

$$\min_{q\in V,n\in N}\max_{P\in U}\sum_{i=m}^{n}\alpha_i^a\left(1-\alpha_a\right)^{n-i}$$

对于多个入侵者的系统，防御者最大化平均检测概率为

$$\min_{q\in V_X}\max_{P\in U}\frac{1}{|\Omega|}\sum_{x\in\Omega}\alpha_x$$

Chen[63]等研究者描述了一个在动态，异质，分布式的网络中 IDS 部署的问题。由于网络的异质性，不同的网络节点对网络的重要性不同，可以用节点的安全资产来表示。在文献[63]中，作者证明了理性的攻击者不会随机攻击节点，他们将攻击安全资产更高的目标节点以获得更高的收益。作者定义了一个非零和静态博弈。假设 IDS 的检测率为 a，误报率为 b，每个节点的安全资产为 W_i，攻击花费为 C_aW_i。作者首先推导出了攻击者将要攻击的目标节点，然后求解出最优的安全资源分配。该模型可以扩展到多个攻击者的情况，双方的行为还可以在斯塔伯格博弈模型框架下进行研究。该项工作后来在文献[64]中得到扩展，考虑了节点的相互依赖性，并建立一些理论成果，可以应用于一系列预算约束的安全博弈。

Sallhammar[65]等研究者介绍了一种随机安全模型，构建了随机安全模型的理论基础。作者提出一个简单的零和随机博弈模型去分析攻击者的预期行为，然后去合理的分配防御者的安全资源。在该博弈中，攻击者可以针对系统状态选择一系列的行动，无论攻击者是否被检测器检测到，都会改变系统的状态。根据攻击行为是否被检测，支付函数和转移概率有所不同。最后，作者提出了一个近似那什均衡的求解算法。该工作给出了很好的随机安全博弈的理论基础，但是没有验证在真实场景下的可行性。

Nguyen[66]等研究者提出了在异质网络下的零和随机博弈。作者充分考虑节点之间漏洞和资产的相关性。在博弈的每一个状态 S_k，攻击者的行动 c_k^i 表示是否攻击节点 i，防御者的行动 d_k^i 和攻击者的定义相似，此时的效用函数为 u_k^{ij}，对于攻击者 c_k^i，防御者 d_k^j，效用函数的定义如下

$$u_k^{ij} = \mathrm{p}_k^s\left(c_k^i, d_k^j\right)x^k\left(i\right)$$

其中，$\mathrm{p}_k^s\left(c_k^i, d_k^j\right)$ 表示攻击者攻击成功的概率，$x^k\left(i\right)$ 表示节点的有效安全资产，当攻击者和防御者行动之后，博弈的状态从 S_k 变成了 S_l，转移概率为 q_{kl}^{ij}，如果攻击失败，系统将返回到原始的状态 S_1。作者最后计算了该博弈的 NE，并给出了最优的防御资源分配。

4.2.3 IDS 配置优化

IDS 优化的第二项重要的工作是 IDS 配置化，包括 IDS 库的选择和 IDS 灵敏度调整。

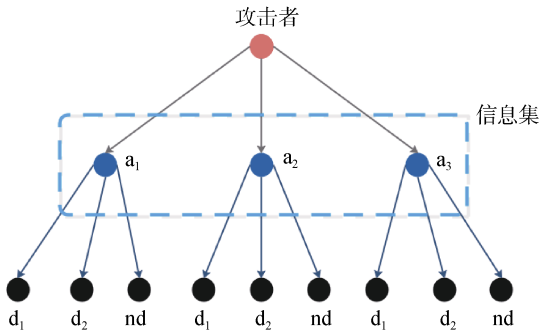


图 3 入侵检测博弈树

Figure 3 The game tree of intrusion detection

在文献[67]中，Alpcan 等研究者第一次提出了使用博弈的方法优化 IDS 的灵敏度从而最大化 IDS 的效率。作者将系统分成几个子系统，这些子系统可能是主机，进程或者系统网络的一部分，系统中部署多个传感器以监视子系统。为了针对每个传感器发出的报警找到最佳响应频率，作者定义了具有动态信息的非零和博弈，攻击者可以选择攻击任何子系统或者什么都不做，传感器可以选择是否产生报警，传感器支持预测哪一个子系统已经被攻击。如图 3 所示，该图展示了两个子系统 s_1, s_2，攻击者的行动

a_1, a_2, n_a 表示攻击子系统 1, 攻击子系统 2 以及都不攻击。防御者的行动 d_1, d_2, n_d 表示在子系统 1 或者 2 上生成告警, 或者都不生成, 定义的效用矩阵如表 3 所示。

表 3 同一信息集中两个子系统的战略形势收益矩阵

Table 3 Payoff Matrix in Strategic Form for Two Subsystems in the Same Information Set

	d_1	d_2	nd
a_1	$-\beta_h, \alpha_h$	$\beta_d, -\alpha_d$	$\beta_s, -\alpha_m$
a_2	$\beta_d, -\alpha_d$	$-\beta_h, \alpha_h$	$\beta_s, -\alpha_m$
na	$0, -\alpha_f$	$0, -\alpha_f$	0,0

其中 β_h 表示攻击花费, β_d 表示攻击欺骗花费, β_s 表示成功入侵收益, α_h 表示攻击检测收益, α_d 表示攻击欺骗花费, α_f 表示误警花费, α_m 表示漏检花费。最后, 作者给出了博弈的混合纳什均衡的分析结果以及最优的子系统的报警生成的概率分布。

在文献[68]中, Alpcan 等研究者扩展了文献[67]的工作, 解决了考虑攻击检测的不确定性的 IDS 灵敏度优化问题。作者定义了不完全信息的零和随机博弈。在这个模型中, 攻击者和防御者选择攻击/防御系统或者什么都不做, 根据是否可以检测到攻击定义了两种状态, 模型充分考虑假阳率和假阴率。作者研究了几种不同的情况: (1)博弈双方对博弈的参数和对手的移动都非常了解; (2)双方只能得到对手移动的一部分信息, 转移概率不确定; (3)每个博弈者仅仅知道自己的移动。对于这些有限的知识的情况, 作者使用 Q-learning 进行训练。

Zhu[69]等研究者提出了一种 IDS 的规则库的动态加载模型。基于规则的 NIDS 如 Snort, 一般会存储对于已知的网络攻击的特征库, 我们需要去配置大量的攻击检测库和一些系统参数, 比如 Snort 有 51 个攻击类别将近 10000 个特征规则, 所以获得最佳的 IDS 配置以有效检测攻击绝非易事, 配置规则库是在系统性能和安全性能之间找到平衡。作者建立一个动态的随机博弈, 对不同的系统状态设计最优的 IDS 配置。使用动态和迭代的方式配置 IDS, 是平衡安全开销和系统性能的方法。作者将攻击者和检测者之间的交互表示成完整的马尔科夫决策过程。我们知道加载一个规则库需要对应的花费, 该模型有一个假设是正确的攻击规则库加载了攻击就会被检测到。具体来说, 系统的状态 $s \in S = \{s_1, s_2, ..., s_n\}$, 如图 4 所示, 系统有三种状态, 状态 1 表示健康状态, 状态 2 表示被入侵状态, 状态 3 表示表示入侵失败状态。有限的策略集 $l \in L = \{l_1, l_2, ..., l_N\}$, 我们定义的子集 $L^s, |L^s| = 2^N$, $F_i \in L^s, i \in \{1, 2, ..., 2^N\}$ 表示策略集的配置。加载不同的规则库需要不同的花费 $c_i = \mathrm{C}(l_i)$ 。

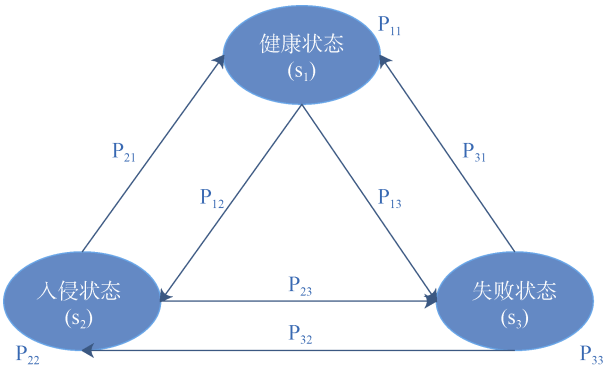


图 4 状态转移矩阵

Figure 4 State transition matrix

最后, 作者使用了两种方法去解决这个问题: 迭代法和强化学习的算法。

文献[70]将文献[69]扩展为分布式 IDS 的规则库的加载问题。作者提出了 $N+M$ 参与者的非零和随机博弈, N 表示负责防御的机器数目, M 表示攻击者的数目, 具体来说, 如图 5 所示, $N = \{n_1, n_2, ..., n_N\}$ 表示 N 个主机节点, $M = \{m_1, m_2, ..., m_M\}$ 表示 M 个恶意攻击者, $V = (N, \varepsilon)$ 表示网络节点之间的连接。每个主机都有有限个状态 $s_i \in S_i^D, i \in N$, $S_i = \{H, C, F\}$ 表示主机的健康水平, $l_i \in L_i = \{l_{i1}, l_{i2}, ..., l_{iL_i}\}$ 表示有限的策略集, C_{F_i} 表示每个策略集的配置的花费。最后, 作者利用数学规划的方法求解 NE 以及计算多项式时间内的 NE 的近似值。

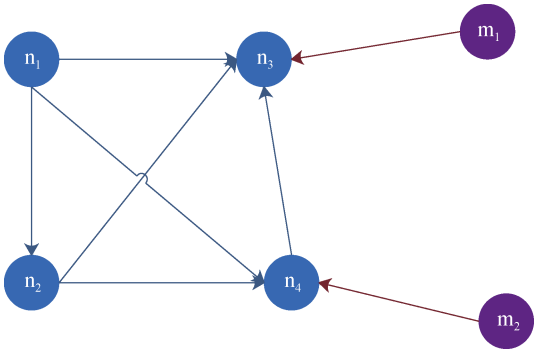


图 5 分布式入侵检测模型

Figure 5 Distributed intrusion detection

Ghorbani[71]等研究者将文献[70]的 $N+M$ 的规则库的加载问题扩展到了异质网络中，作者充分考虑了网络资产的依赖性和漏洞之间的依赖性，除了考虑加载规则库的花费，还考虑了 IDS 的检测率。最后提出了近似纳什均衡的求解算法。

Cabrera[75]等研究者将博弈论应用于内部的伪装者检测。机器学习系统经常被部署在很多对抗性系统中，比如入侵检测系统，分类器的作用是识别操作系统是否来自合法的操作者，用于内部伪装者检测。但是攻击者是对抗代理，可以对分类器进行反向工程并成功伪装成合法用户。作者提出了主动入侵检测系统的概念，可以通过将反馈整合处理进行主动入侵检测。主动 IDS 会改变自己的行为影响用户的操作，观察他们在不同情况的反应，去决定使用者是否是入侵者。

4.2.4 IDS 检测率优化

基于博弈论的 IDS 检测率的优化主要是利用生成对抗网络提高异常检测的检测率。

网络监控传感器会生成大量的多元时间序列，我们可以连续监视丰富的传感器数据以防止入侵，由于系统的动态复杂性，常规的基于阈值的异常检测方法存在不足，监督学习缺少标记数据。因此正向检测效果不好，Li[78]等人逆向研究，提出了基于生成对抗的无监督多元异常检测方法，使用 LSTM 作为 GAN 框架中的模型(即生成器和鉴别器)以捕获时间序列分布，使用一种称为 DR 得分的新颖的异常检测评分来辨别和检测异常。

在文献[76]中，Yin 等研究者提出了基于生成对抗网络的方法提高了僵尸网络的检测效率，借助生成对抗网络对抗交互训练的思想。框架在训练的阶段引入了生成模型，由生成模型不断生成样本，扩充了原有标签样本集，可辅助入侵检测模型进行分类，提高了模型检测准确率，提升了执行多分类任务时对入侵行为的识别能力。

Lin[77]等研究者提出一种基于生成对抗网络的攻击流量生成模型，可以欺骗和逃避入侵检测系统。利用生成器将原始恶意流量转换成对抗性恶意流量，判别器将流量分类。

如图 6 所示，训练数据集被分成恶意流量和普通流量，增加噪音之后被送到生成器。对抗性恶意流量和普通流量被黑盒 IDS 预测，预测的标签和原始的标签在判别器中被使用，生成器的损失由判别器的结果和黑盒 IDS 预测的标签决定。作者在 NSL-KDD 数据集上进行了实验，证明了模型的有效性，在很多不同的基于机器学习的检测算法上取得了很好的效果。

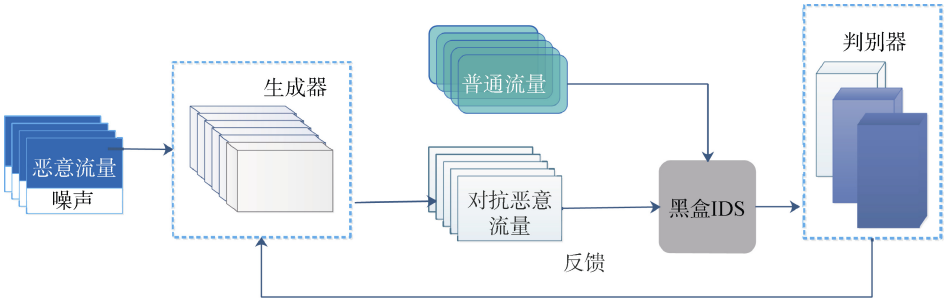


图 6　基于生成对抗网络的攻击生成模型

Figure 6　Attack generation model based on GAN

4.2.5 攻击自动化响应优化

攻击之后的自动化选择，主要涉及 IPS 和 IRS，研究工作主要是一旦发现攻击就触发最佳的防御策略，无需依靠管理员的手动干预。该项工作主要是优化系统反应，而不是 IDS 性能，因此假定总能够成功检测到攻击。

Lye[79]等研究者提出了一个多节点的入侵响应模型，这些节点可以是不同攻击的目标，可以使用不同的对策去应对这些攻击。作者将模型表示成一个非零和的随机博弈，其中系统的状态取决于每个节点的状态。节点的状态取决于节点上面运行的应用以及使用账户的数据。作者给出了来自攻击者的三种攻击场景以及不同状态之间转移概率的估计值。

在文献[80]中，Luo 等研究者对网络上的多阶段攻击进行风险和影响分析。作者提出一种算法，该算法计算每次攻击的每个阶段的最佳防御者反应。该项工作的主要贡献是定义了多阶段攻击的风险和影响。目的是识别和评估相关参数，例如攻击的即时影响，响应成本以及攻击的未来影响。这些参数在连续的零和博弈中用作输入的有效值。该博弈中，攻击者和防御者依次采取行动，博弈表示为博弈树，其中

的弧线对应于每个玩家的可用动作。作者量化了两个参与者对彼此策略的信念，并提出了一种能够计算防御者最佳行动的算法。

Luo[81]等研究者还提出了一种非完全信息的多阶段非零和博弈。博弈双方都被认为是理性的，他们使用贝叶斯方法分析对手先前可能的交互，每一次交互都更新对手的知识。作者提出一种动态虚拟博弈树的方法描述双方的交互对策。还引入了一个参数来表示攻击者的风险，并将未来攻击的预期影响表示为概率，代替搜索整个博弈树。由于其非唯一性和所需的时间，因此不需要计算对策的 NE。

在文献[82]中，Bao 等研究者考虑了一种情况：攻击者被驱逐出系统之后返回的情况。入侵者一旦被检测到，那么他有可能会尝试重新进入系统，同时更加小心防止被检测。攻击者和防御者都在学习对方的弱点，意图和方法。当攻击者重新进入系统而没有被发现时，他可能比防御者学的更快，得到的信息更多，成功的机会更大。作者研究防御者的最佳驱逐策略，但是驱逐攻击者的策略未必是最优的。

Zonouz[83]等研究者提出了一种基于博弈论的入侵反应与还原模型。作者将该模型建模为双人的斯塔伯格随机博弈。该系统可以计算出在一些因素限制的情况下的最优响应。该系统提出了入侵响应树，分析不希望发生的安全事件以及其对策，然后通过求解一个部分可观察的 MDP 来选择最优的响应行为。实验结果表明使用 Snort 的警报，入侵响应和恢复模型可以保护大型网络。

Shen[84]等研究者提出了一种基于信息融合的决策和控制框架来检测和预测多阶段网络攻击，作者将问题定义为三人的非零和随机博弈，该架构建立在不同水平的架构上，包括日志，告警分析，通过分析得到一个 MDP 模型。如图 7 所示，该系统包含两个完全耦合的部分：1 数据融合模块：提取原始的信息，评估并确定新的网络攻击 2 动态自适应特征识别模块：生成原始的评估，识别未知的网络攻击。整个框架分层融合，动态学习，使得决策的结果更加准确。

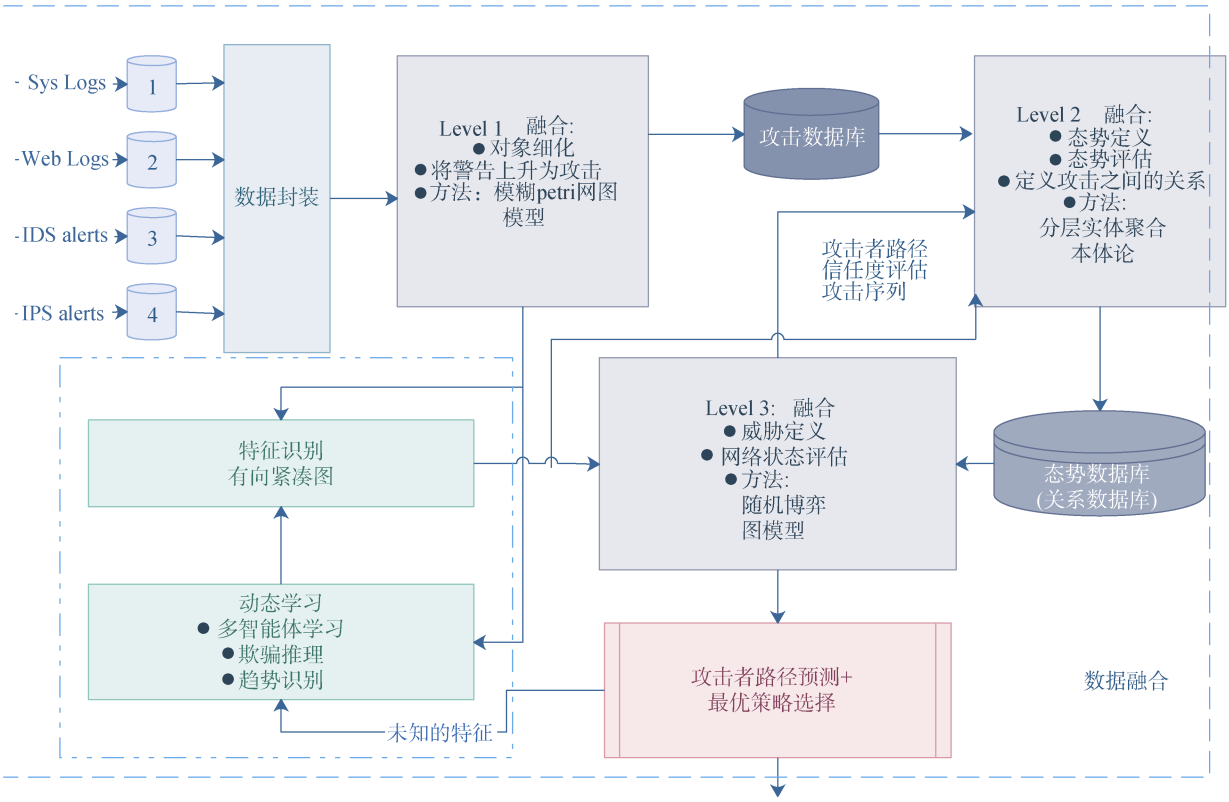


图 7 基于信息融合的决策和控制框架

Figure 7 Decision and control framework based on information fusion

4.2.6 分布式入侵检测架构优化

博弈论应用于入侵检测架构设计方面主要是分布式入侵检测系统的架构设计。

Guo[85]等研究者研究了移动 Ad-Hoc 网络中的协同入侵检测架构的设计。在移动 Ad-Hoc 网络中，协同入侵检测对大规模并行处理攻击具有高效和可扩展性。 然而，由于对隐私泄露和资源成本的担忧，如果没有足够的激励，大多数用户往往是自私的，

不会帮助他人检测入侵事件，因此需要一个有效的激励机制。考虑到用户的有限理性和协同入侵检测的动态性，作者将协同检测的激励机制制定为一个演化博弈。 在演化博弈中，作者设计了一种预算分配机制，鼓励节点及时合作，实现进化稳定策略。考虑到合作者的声誉，作者还提出了一种惩罚-申诉机制来降低恶意节点的声誉得分，防止所提出的激励机制被滥用。最后，作者提出了一个基于 ess 的那什均衡求解算法并进行了仿真，仿真结果表明，该策略能有效地激励非恶意节点参与合作，防止恶意节点滥用我们的激励，降低误检率。

在文献[86]中，Abusitta 等研究者提出了一种在云计算的环境中基于机器学习的协作式入侵检测系统。在合作环境中，IDS 可以联系其他 IDS 来获取有关可疑入侵的信息，并进行聚合决策。但是，聚合决策会产生不希望的延迟，等待从咨询的 IDS 接受反馈的过程，这些限制使得现有的合作 IDS 生成的决策方法实时无效。作者提出了一种基于机器学习的协作式 IDS 有效的利用历史反馈数据来提高主动决策的能力，所提出的模型基于降噪自动编码器，学习如何从部分反馈中重建 IDS 的反馈。使得我们能够即使在没有 IDS 的完整反馈的情况下主动做出决策。最后作者使用真实数据集进行了评估，实验结果表明，模型可以达到 95%的检测精度。

Abusitta 等研究者在文献[87]提出了一种基于联盟博弈的分布式入侵检测模型。 单一的入侵检测系统识别云中的攻击变得越来越困难，因为 IDS 对于攻击的知识不完整，云中的 IDS 之间的合作可以带来更高的检测精度，通过合作，基于云的 IDS 可以咨询其他 IDS 来获取有关可疑的入侵，并提高决策准确性。现有的合作 IDS 方法的问题是忽略了不受信任(恶意或者非恶意)IDS 可能会对有关可疑的决定产生负面影响。作者设计了一个框架使 IDS 能够分布式形成可信赖的 IDS 社区。最后作者提出了一个新颖的分散式算法，基于联盟博弈论，基于云的 IDS 合作建立联盟。

Zhu[88]等研究者介绍了一种协作入侵检测网络的激励机制设计方法。相对于普通的基于信任的系统，为了确保所有的 IDS 主动为入侵检测做贡献，作者建立 N 个玩家的静态合作博弈，如图 8 所示。充分考虑每个节点的资源预算。目标是最大化每个节点的利他效益。

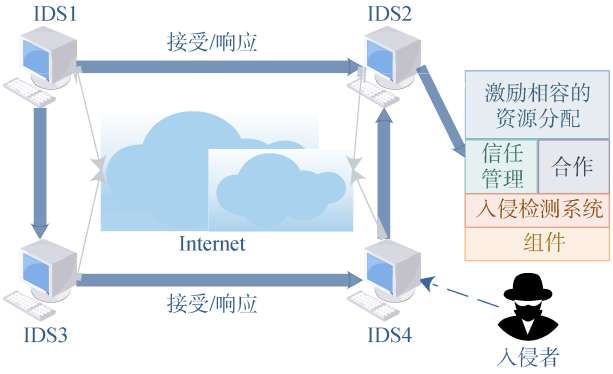


图 8 协作式入侵检测网络的激励机制设计

Figure 8 Incentive mechanism design of collaborative intrusion detection network

5 博弈模型局限性

大量的基于博弈论的入侵检测与响应优化的工作表明这是一个非常活跃的研究主题。我们知道，博弈论是少数可以捕获入侵者行为的机制。但是博弈论的缺点是太过于理论，存在一定的局限性。首先需要依赖一些理想的假设，其次博弈论在实际系统配置中存在很大的挑战。在本节中，我们将介绍各种博弈模型中假设的含义以及验证方法，给未来的工作指明了方向。

5.1 博弈模型假设

(1) 博弈模型的选择

第一组假设是博弈模型的假设。静态博弈定义过于简单，零和博弈假设攻击者和防御者收益是相等的，这个假设使得博弈的那什均衡求解更加简单，但是在实际中没有什么意义，一般来说，攻击者和防御者的收益和损失之间不存在联系。所以，越来越多的研究者关注更加接近实际情况的随机博弈，随机博弈是一种动态博弈，博弈双方根据对手的策略改变自己的决策。如果将 IDS 优化问题建模成更加符合实际情况的随机博弈，能有效提高将博弈论应用在 IDS 优化工作的实用性。

(2) 完全理性人假设

我们建立的博弈模型假设攻击过程中攻击者和防御者都是完全理性的，有研究者尝试前景理论和量化反应模型，大多数的这些模型具有不同于理性人假设的表现，当然也增加了优化问题的求解难度。但是随着计算机算力的增长，这些优化问题的求解难度也会随之降低。

(3) 完全信息假设

如果一个玩家要在几个动作之间做出选择的话，那么他总是会选择能够带来最高回报的行为，这个假设也依赖一个事实，即玩家拥有与他们每个行动相关的成本和收益的完整信息，然而不同的攻击者针对不同的系统，具有不同的目标和状态行为。根据

不同的状态建立精细化的动态博弈模型可以有效地弱化假设, 提高实用性。

(4) 博弈进行次数

我们一般假设博弈双方的博弈进行一次。但是博弈者的策略会影响系统参数的改变。博弈论虽然提供了一个工具研究防御者和攻击者的交互行为, 但是没有提供如何有效解决的方法。因此, 我们需要在不同的系统状态下求解博弈模型。

表 4 基于博弈论的验证方法对比

Table 4 Comparison of Validation Experiments in the Game-Theoretic Approaches

文献	数值仿真	入侵仿真	参数评估	其他评估指标
文献[60]	√	×	√	False-positive rate
文献[62]	√	×	×	True-positive rate
文献[65]	√	×	×	×
文献[67]	√	×	×	Received resources
文献[68]	√	×	×	×
文献[69]	√	×	×	×
文献[70]	×	×	×	×
文献[71]	×	×	×	×
文献[79]	√	×	×	×
文献[80]	√	×	√	×
文献[81]	√	×	×	×
文献[82]	√	×	×	Successful intrusion rate
文献[83]	√	√	×	Recovery cost

5.2 验证方法

将博弈论集成到入侵检测和响应系统中的验证方法仍然存在很大的局限性。首先大规模的网络攻击数据集很难构建, 其次博弈论的理论抽象程度太高, 给其验证方法提高了门槛。在本节中, 我们提出了一些验证方法的缺陷, 并给出了一些实践准则, 以更好的将博弈论方法整合到实际应用中。

5.2.1 主要的验证方法

主要验证的方法有数值仿真和网络模拟仿真。数值仿真是对博弈模型结果的仿真。网络仿真是在实际应用中部署物理或虚拟网络从而验证博弈模型的过程。很少有文章对系统的入侵进行网络模拟仿真, 缺少成熟的方法评估博弈的结果, 因此在专用测试平台上测试 IDS 的难度很大。不同的验证方法如表 4 所示。

5.2.2 真实场景的集成

将博弈论集成到入侵检测与响应系统需要加强理论和实践的联系。具体需要考虑以下几点:

(1) 充分考虑系统的约束

不同的网络和系统都会有相对应的约束, 我们在构建实际场景中需要将这些约束纳入博弈模型中。比如, WSN 网络节点计算能力有限, MANET 由于节点的移动性导致可用带宽随时间变化, IRS 需要在预算有限的系统中运行, 这可能会使一些理论上可接受的对策失效。目前有两种方法解决这个问题, 第一种方法是将效用函数乘以一定的折扣因子, 第二种方法是将约束与效用函数分开, 并且在博弈期间将他们考虑在内。

(2) 标准化博弈引擎与 IDS 的交互

网络环境是在动态变化的, 网络拓扑也可能发生变化, 系统也有可能发生故障, 所以我们需要动态配置系统, 在配置的过程中, 如果频繁的使用博弈引擎来重新配置系统可能会导致系统不稳定, 而以较低的频率更新配置会使得系统使用过时的配置。所以按照博弈的结果更新系统的状态不能过于频繁, 也不能过低。

攻击前的网络安全架构优化基于 Stackelberg 博弈, 该博弈模型是离实际应用最近的模型。在机场安全和公共系统安全中得到了实用性的评估。有研究者将其应用于网络安全架构优化, 提高了网络系统的安全性。由于实际的网络系统庞大且复杂, 自动化程度低, 而入侵检测与响应系统的部署需要很多网络设备共同配合, 所以攻击中的 IDS 配置与效率优化以及攻击后的自动化响应面临最大的挑战是将博弈论集成到网络系统进行验证。但是随着软件定义网络的发展, 网络设备的软件化给该项研究的落地提供强大的支持。

虽然将博弈论应用在入侵检测与响应系统有一定的困难, 但是云计算的发展提高了资源配置的灵活度, 算力得到了极大的增长。同时, 博弈论与机器

学习的相互融合提高了算法的实用性。这些技术改进给该项研究提供良好的部署环境, 足够的算力以及强大的算法。那么该项研究的局限性也可以随之得到解决。

6 结论

入侵检测和响应优化是网络和系统安全的重要组成部分, 也是一个活跃的研究领域, 包括网络安全架构优化、IDS 配置与效率优化, 攻击的自动化响应优化以及分布式 IDS 的架构优化。博弈论方法的优势在于能够考虑安全性的同时考虑攻击者和防御者的行为。此外, 它为 IDS 优化提供了理论指导。但是将博弈论的方法大范围应用在实际场景中仍存在很大的局限性。未来, 我们认为以下两个方向是联系理论和实际最有前景的研究方向:

(1) 基于历史数据的学习

攻击者和入侵检测系统进行频繁的对抗积累了大量的数据。这使得研究人员能够通过收集的数据学习到博弈模型。现有的安全博弈的收益函数都是专家指定的, 但是很多情况我们无法设计良好的收益函数, 收益函数也会随着时间动态发生改变, 进而影响博弈的结果。因此, 如何从博弈产生的数据中学习出攻击者的攻击行为偏好, 进而进行有效的保护是一个未来的研究重点。

(2) 分布式入侵检测

现实的网络规模不断增大, 云计算的普及给单一的入侵检测系统带来了很多的挑战。分布式入侵检测系统是未来的趋势。不同的检测传感器收集各自的数据之后, 需要进行聚合关联, 共同决策。因此, 各个入侵检测系统之间需要良好的通讯机制和协商机制。一个设计良好的分布式入侵检测系统应该是高级的多智能系统, 这些智能体共同优化一个目标, 产生高效的告警信息, 自动化响应一部分告警, 然后人机联动, 动态迭代优化系统, 让整体的入侵检测系统处于学习进化中。

参考文献

[1] Denning D E. An Intrusion-Detection Model[J]. *IEEE Transactions on Software Engineering*, 1987, SE-13(2): 222-232.

[2] Qing S H, Jiang J C, Ma H T, et al. Research on Intrusion Detection Techniques: A Survey[J]. *Journal of China Institute of Communications*, 2004, 25(7): 19-29.
(卿斯汉, 蒋建春, 马恒太, 等. 入侵检测技术研究综述[J]. *通信学报*, 2004, 25(7): 19-29.)

[3] Inayat Z, Gani A, Anuar N B, et al. Intrusion Response Systems: Foundations, Design, and Challenges[J]. *Journal of Network and Computer Applications*, 2016, 62: 53-74.

[4] Shameli-Sendi A, Cheriet M, Hamou-Lhadj A. Taxonomy of Intrusion Risk Assessment and Response System[J]. *Computers & Security*, 2014, 45: 1-16.

[5] Moustafa N, Hu J K, Slay J. A Holistic Review of Network Anomaly Detection Systems: A Comprehensive Survey[J]. *Journal of Network and Computer Applications*, 2019, 128: 33-55.

[6] García-Teodoro P, Díaz-Verdejo J, Maciá-Fernández G, et al. Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges[J]. *Computers & Security*, 2009, 28(1/2): 18-28.

[7] Kolias C, Kambourakis G, Maragoudakis M. Swarm Intelligence in Intrusion Detection: A Survey[J]. *Computers & Security*, 2011, 30(8): 625-642.

[8] Buczak A L, Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection[J]. *IEEE Communications Surveys & Tutorials*, 2016, 18(2): 1153-1176.

[9] Roy S, Ellis C, Shiva S, et al. A survey of game theory as applied to network security[C]. *2010 43rd Hawaii International Conference on System Sciences*, 2010: 1-10.

[10] Liang X N, Xiao Y. Game Theory for Network Security[J]. *IEEE Communications Surveys & Tutorials*, 2013, 15(1): 472-486.

[11] Manshaei M H, Zhu Q Y, Alpcan T, et al. Game Theory Meets Network Security and Privacy[J]. *ACM Computing Surveys*, 2013, 45(3): 25.

[12] Do C T, Tran N H, Hong C, et al. Game Theory for Cyber Security and Privacy[J]. *ACM Computing Surveys*, 2018, 50(2): 30.

[13] Zhu Q Y, Rass S. Game Theory Meets Network Security: A Tutorial[C]. *The 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018: 2163-2165.

[14] Paramasivan B, Pitchai K M. Comprehensive survey on game theory based intrusion detection system for mobile adhoc networks[J]. *IJCA Special Issue on "Network Security and Cryptography*, 2011: 23-29.

[15] Jain M, An B, Tambe M. Security Games Applied to Real-World: Research Contributions and Challenges[M]. Moving Target Defense II. New York, NY: Springer New York, 2012: 15-39.

[16] Pita J, Jain M, Ordóñez F, et al. ARMOR Security for Los Angeles International Airport[J]. *Proceedings of the National Conference on Artificial Intelligence*, 2008, 3: 1884-1885.

[17] An B, Shieh E, Tambe M, et al. PROTECT — a Deployed Game Theoretic System for Strategic Security Allocation for the United States Coast Guard[J]. *AI Magazine*, 2012, 33(4): 96.

[18] Delle Fave F M, Jiang A X, Yin Z, et al. Game-Theoretic Patrolling with Dynamic Execution Uncertainty and a Case Study on a Real Transit System[J]. *Journal of Artificial Intelligence Research*, 2014, 50: 321-367.

[19] Lakshminarayana D H, Philips J, Tabrizi N, et al. A survey of intrusion detection techniques[C]. *2019 18th IEEE International Conference on Machine Learning and Applications*, 2020: 1122-1129.

[20] Ślezak D, Chadzyńska-Krasowska A, Holland J, et al. Scalable cyber-security analytics with a new summary-based approximate query engine[C]. *2017 IEEE International Conference on Big Data*,

2018: 1840-1849.

[21] Catania C A, Garino C G. Automatic Network Intrusion Detection: Current Techniques and Open Issues[J]. *Computers & Electrical Engineering*, 2012, 38(5): 1062-1072.

[22] Mirsky Y, Doitshman T, Elovici Y, et al. Kitsune: an ensemble of autoencoders for online network intrusion detection[J]. *arXiv preprint arXiv:*1802.09089, 2018.

[23] Kumar S. Classification and detection of computer intrusions[D]. PhD thesis, Purdue University, 1995.

[24] Porras P A, Kemmerer R A, Processing C A, et al. Penetration state transition analysis: A rule-based intrusion detection approach[C]. *[1992] Proceedings Eighth Annual Computer Security Application Conference*, 2002: 220-229.

[25] Anwar S, Mohamad Zain J, Zolkipli M F, et al. From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions[J]. *Algorithms*, 2017, 10(2): 39.

[26] Kilincer I F, Ertam F, Sengur A. Machine Learning Methods for Cyber Security Intrusion Detection: Datasets and Comparative Study[J]. *Computer Networks*, 2021, 188: 107840.

[27] Milenkoski A, Vieira M, Kounev S, et al. Evaluating Computer Intrusion Detection Systems[J]. *ACM Computing Surveys*, 2015, 48(1): 1-41.

[28] Fawcett T. An Introduction to ROC Analysis[J]. *Pattern Recognition Letters*, 2006, 27(8): 861-874.

[29] Axelsson S. The Base-Rate Fallacy and the Difficulty of Intrusion Detection[J]. *ACM Transactions on Information and System Security*, 2000, 3(3): 186-205.

[30] DARPA'98 and DARPA'99 datasets. 1999. Available from: https://www.ll.mit.edu/ideval/docs/index.html. [Accessed 11 October 2017].

[31] KDD Cup 99 Dataset. Available from: https://kdd.ics.uci.edu/ databases/kddcup99/kddcup99.html. [Accessed 11 October 2017].

[32] Tavallaee M, Bagheri E, Lu W, et al. A detailed analysis of the KDD CUP 99 data set[C]. *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009: 1-6.

[33] Perona I, Gurrutxaga I, Arbelaitz O, et al. Service-Independent Payload Analysis to Improve Intrusion Detection in Network Traffic[C]. *The 7th Australasian Data Mining Conference - Volume 87*, 2008: 171-178.

[34] Sperotto A, Sadre R, van Vliet F, et al. A Labeled Data Set for Flow-Based Intrusion Detection[M]. IP Operations and Management. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 39-50.

[35] Fontugne R, Borgnat P, Abry P, et al. MAWILab: Combining Diverse Anomaly Detectors for Automated Anomaly Labeling and Performance Benchmarking[C]. *The 6th International COnference*, 2010: 1-12.

[36] Shiravi A, Shiravi H, Tavallaee M, et al. Toward Developing a Systematic Approach to Generate Benchmark Datasets for Intrusion Detection[J]. *Computers & Security*, 2012, 31(3): 357-374.

[37] García S, Grill M, Stiborek J, et al. An Empirical Comparison of Botnet Detection Methods[J]. *Computers & Security*, 2014, 45: 100-123.

[38] Creech G, Hu J K, Communication N A B T, et al. Generation of a new IDS test dataset: Time to retire the KDD collection[C]. *2013 IEEE Wireless Communications and Networking Conference*, 2013: 4487-4492.

[39] Moustafa N, Slay J, Communication N A B T, et al. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)[C]. *2015 Military Communications and Information Systems Conference*, 2015: 1-6.

[40] Maciá-Fernández G, Camacho J, Magán-Carrión R, et al. UGR'16: A New Dataset for the Evaluation of Cyclostationarity-Based Network IDSs[J]. *Computers & Security*, 2018, 73: 411-424.

[41] Sharafaldin I, Habibi Lashkari A, Ghorbani A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]. *The 4th International Conference on Information Systems Security and Privacy*, 2018: 108-116.

[42] SIEM, AIOps, Application Management, Log Management, Machine Learning, and Compliance. https://www.splunk.com/.

[43] Osborne M J, Rubinstein A. A course in game theory[M]. Cambridge, Mass.: MIT Press, 1994

[44] Nash J. Non-Cooperative Games[J]. *The Annals of Mathematics*, 1951, 54(2): 286.

[45] Neumann, J. Zur Theorie Der Gesellschaftsspiele[J]. *Mathematische Annalen*, 1928, 100(1): 295-320.

[46] Rezek I, Leslie D S, Reece S, et al. On Similarities between Inference in Game Theory and Machine Learning[J]. *Journal of Artificial Intelligence Research*, 2008, 33: 259-283.

[47] He D, Chen W, Wang L W, et al. A Game-Theoretic Machine Learning Approach for Revenue Maximization in Sponsored Search[EB/OL]. 2014: arXiv: 1406.0728. https://arxiv.org/abs/1406.0728

[48] Wang Z, Yuan Y, An B, et al. An Overview of Security Games[J]. *Journal of Command and Control*, 2015, 1(2): 121-149.
(王震, 袁勇, 安波, 等. 安全博弈论研究综述[J]. *指挥与控制学报*, 2015, 1(2): 121-149.)

[49] Stackelberg H V. Marktform und Gleichgewicht[M]. Wien und Berlin: J. Springer, 1934

[50] Conitzer V, Sandholm T. Computing the Optimal Strategy to Commit to[C]. *The 7th ACM conference on Electronic commerce*, 2006: 82-90.

[51] Pita J, Jain M, Ordóñez F, et al. Using Game Theory for Los Angeles Airport Security[J]. *AI Magazine*, 2009, 30(1): 43.

[52] Tsai J, Rathi S, Kiekintveld C, et al. IRIS - a Tool for Strategic Security Allocation in Transportation Networks[M]. Security and Game Theory. Cambridge: Cambridge University Press, 2011: 88-106.

[53] Shieh E, An B, Yang R, et al. PROTECT: A Deployed Game Theoretic System to Protect the Ports of the United States[C]. *The 11th International Conference on Autonomous Agents and Multiagent Systems - Volume 1*, 2012: 13-20.

[54] Yin Z Y, Jiang A X, Tambe M, et al. TRUSTS: Scheduling Randomized Patrols for Fare Inspection in Transit Systems Using Game Theory[J]. *AI Magazine*, 2012, 33(4): 59.

[55] Paruchuri P, Pearce J P, Marecki J, et al. Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games[C]. *The 7th international joint conference on Autono-*

Autonomous agents and multiagent systems - Volume 2, 2008: 895-902.

[56] Kiekintveld C, Jain M, Tsai J, et al. Computing Optimal Randomized Resource Allocations for Massive Security Games[C]. *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems - Volume 1*, 2009: 689-696.

[57] Lowe R, Wu Y, Tamar A, et al. Multi-Agent Actor-Critic for Mixed Cooperative-Competitive Environments[C]. *The 31st International Conference on Neural Information Processing Systems*, 2017: 6382-6393.

[58] Wang Z, Duan C J, Wu T, et al. Research on Optimizing Security Control Mechanism of Networked System Based on Stackelberg Defender-Attacker Game[J]. *Journal of Cyber Security*, 2019, 4(1): 101-115.
(王震, 段晨健, 吴铤, 等. 基于 Stackelberg 攻防博弈的网络系统安全控制机制优化研究[J]. *信息安全学报*, 2019, 4(1): 101-115.)

[59] Durkota K, Lisy V, Bošansky B, et al. Optimal Network Security Hardening Using Attack Graph Games[C]. *The 24th International Conference on Artificial Intelligence*, 2015: 526-532.

[60] Kodialam M, Lakshman T V, Communication N A B T, et al. Detecting network intrusions via sampling: a game theoretic approach[C]. *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies*, 2003: 1880-1889.

[61] Otrok H, Mohammed N, Wang L Y, et al. A Game-Theoretic Intrusion Detection Model for Mobile Ad Hoc Networks[J]. *Computer Communications*, 2008, 31(4): 708-721.

[62] Otrok H, Mehrandish M, Assi C, et al. Game Theoretic Models for Detecting Network Intrusions[J]. *Computer Communications*, 2008, 31(10): 1934-1944.

[63] Chen L, Leneutre J. A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks[J]. *IEEE Transactions on Information Forensics and Security*, 2009, 4(2): 165-178.

[64] Ismail Z, Kiennert C, Leneutre J, et al. A Game Theoretical Model for Optimal Distribution of Network Security Resources[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017: 234-255.

[65] Sallhammar K, Helvik B E, Knapskog S J. Incorporating Attacker Behavior in Stochastic Models of Security[C]. *Security and Management*. 2005: 79-85.

[66] Nguyen K C, Alpcan T, Basar T, et al. Stochastic games for security in networks with interdependent nodes[C]. *2009 International Conference on Game Theory for Networks*, 2009: 697-703.

[67] Alpcan T, Basar T, Systems R A C, et al. A game theoretic approach to decision and analysis in network intrusion detection[C]. *42nd IEEE International Conference on Decision and Control*, 2004: 2595-2600.

[68] Alpcan T, Ba\csar T. An Intrusion Detection Game with Limited Observations[J]. *12th Int Symp on Dynamic Games and Applications*, 2006: 343-346.

[69] Zhu Q Y, Başar T, Systems R A C, et al. Dynamic policy-based IDS configuration[C]. *The 48h IEEE Conference on Decision and Control held jointly with 2009 28th Chinese Control Conference*, 2010: 8600-8605.

[70] Zhu Q Y, Tembine H, Başar T, et al. Network security configurations: A nonzero-sum stochastic game approach[C]. *The 2010 American Control Conference*, 2010: 1059-1064.

[71] Ghorbani M, Hashemi M R, Bioengineering, et al. Networked IDS configuration in heterogeneous networks—a game theory approach[C]. *2015 23rd Iranian Conference on Electrical Engineering*, 2015: 1000-1005.

[72] Hu J, Wellman M P. Nash Q-learning for general-sum stochastic games[J]. *Journal of machine learning research*, 2003, 4(Nov): 1039-1069.

[73] Littman M L. Friend-or-foe Q-learning in general-sum games[C]. *ICML*. 2001, 1: 322-328.

[74] Bowling M, Veloso M. Multiagent Learning Using a Variable Learning Rate[J]. *Artificial Intelligence*, 2002, 136(2): 215-250.

[75] Cabrera J B D, Lewis L, Qin X Z, et al. Proactive Intrusion Detection[M]. Advances in Information Security. Boston, MA: Springer US, 2002: 195-227.

[76] Yin C L, Zhu Y F, Liu S L, et al. An enhancing framework for botnet detection using generative adversarial networks[C]. *2018 International Conference on Artificial Intelligence and Big Data*, 2018: 228-234.

[77] Lin Z L, Shi Y, Xue Z. IDSGAN: Generative Adversarial Networks for Attack Generation Against Intrusion Detection[EB/OL]. 2018: arXiv: 1809.02077. https://arxiv.org/abs/1809.02077

[78] Li D, Chen D C, Jin B H, et al. MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks[M]. Artificial Neural Networks and Machine Learning - ICANN 2019: Text and Time Series. Cham: Springer International Publishing, 2019: 703-716.

[79] Lye K W, Wing J M. Game Strategies in Network Security[J]. *International Journal of Information Security*, 2005, 4(1): 71-86.

[80] Luo Y, Szidarovszky F, Al-Nashif Y, et al. A game theory based risk and impact analysis method for Intrusion Defense Systems[C]. *2009 IEEE/ACS International Conference on Computer Systems and Applications*, 2009: 975-982.

[81] Luo Y, Szidarovszky F, Al-Nashif Y, et al. A Fictitious Play-Based Response Strategy for Multistage Intrusion Defense Systems[J]. *Security and Communication Networks*, 2014, 7(3): 473-491.

[82] Bao N, Musacchio J. Optimizing the Decision to Expel Attackers from an Information System[C]. *The 47th annual Allerton conference on Communication, control, and computing*, 2009: 644-651.

[83] Zonouz S A, Khurana H, Sanders W H, et al. RRE: A Game-Theoretic Intrusion Response and Recovery Engine[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2014, 25(2): 395-406.

[84] Shen D, Chen G S, Cruz J B Jr, et al. A Markov game theoretic data fusion approach for cyber situational awareness[C]. Defense and Security Symposium. *Proc SPIE 6571, Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2007*, Orlando, Florida, USA. 2007, 6571: 143-154.

[85] Guo Y C, Zhang H, Zhang L C, et al. A Game Theoretic Approach to Cooperative Intrusion Detection[J]. *Journal of Computational Science*, 2019, 30: 118-126.

[86] Abusitta A, Bellaiche M, Dagenais M, et al. A Deep Learning Approach for Proactive Multi-Cloud Cooperative Intrusion Detection System[J]. *Future Generation Computer Systems*, 2019, 98: 308-318.

[87] Abusitta A, Bellaiche M, Dagenais M, et al. A trust-based game theoretical model for cooperative intrusion detection in multi-cloud environments[C]. *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops*, 2018: 1-8.

[88] Zhu Q Y, Fung C, Boutaba R, et al. A game-theoretical approach to incentive design in collaborative intrusion detection networks[C]. *2009 International Conference on Game Theory for Networks*, 2009: 384-392.

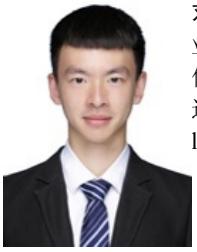
张杭生 于 2017 年在浙江工业大学数字媒体技术专业获得工学学士学位, 现于中国科学院大学网络空间安全专业攻读博士学位。研究领域为大数据安全分析, 网络安全溯源分析, 基于博弈机器学习的入侵检测与响应。Email: zhanghangsheng@iie.ac. cn

梁杰 于 2016 年在青岛大学网络工程专业获得学士学位。于 2021 年毕业于中国科学院信息工程研究所。研究领域为未来网络中的缓存优化技术研究。研究兴趣包括: 内容中心网络、缓存优化、内容流行度预测。Email: liangjie@iie.ac.cn

李婷 于 2018 年在重庆大学通信工程专业获得学士学位。现于中国科学院信息工程研究所攻读博士学位。研究领域为 5G、未来网络。研究兴趣为移动边缘计算和内容中心网络。Email: liting0715@iie.ac.cn.

刘银龙 于 2011 年在北京邮电大学通信与信息系统专业获得博士学位。现任中国科学院信息工程研究所副研究员。研究领域为: 未来网络理论、移动通信与安全。研究兴趣: 信息中心网络理论与应用、移动通信业务管控等。Email: liuyinlong@iie.ac.cn

刘吉强 1999 年在北京师范大学获理学博士, 现任北京交通大学教授, 研究领域为可信计算, 应用密码学, 安全协议, 隐私保护。Email: jqliu@bjtu.edu.cn



刘海涛 于 2018 年在湖南大学通信工程专业获得学士学位。于 2021 年于中国科学院信息工程研究所获得硕士学位。研究领域为通信网络。研究兴趣为边缘计算。Email: liuhaitao@iie.ac.cn

耿立茹 于 2018 年在北京邮电大学信息与通信工程专业获得硕士学位。现任中国科学院信息工程研究所研究实习员。研究领域为: 移动通信与安全。研究兴趣包括: 5G 网络安全、移动通信业务管控等。Email: gengliru@iie.ac.cn