基于有限理性的网络防御策略智能规划方法

刘盈泽，郭渊博，方晨，李勇飞，陈庆礼
（信息工程大学密码工程学院，河南 郑州 450001）

摘 要：考虑到网络防御主体通常具有资源受限等特点，基于智能化攻防对抗的理念研究了有限理性条件下的网络防御策略智能规划与自主实施。首先，融合攻击图、通用与领域专有知识构建网络防御安全本体；在此基础上，利用知识推理推荐安全防御策略，以更好地适应受保护网络信息资产的安全需求及当前所面临的攻击威胁；最后，结合有限理性的智能规划方法，实现网络安全防御资源受限、网络信息资产动态变化等约束条件下的防御策略自主规划与实施。实例表明，动态攻击下所提方法具有稳健性。将所提方法与现有基于博弈论及攻击图方法进行对比，实验结果表明在对抗一次典型的 APT 攻击时所提方法的防御有效性提高了 5.6%～26.12%。

关键词：网络防御；防御策略推荐；智能规划；有限理性；安全本体
中图分类号：TN92
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023091

Intelligent planning method for cyber defense strategies based on bounded rationality

LIU Yingze, GUO Yuanbo, FANG Chen, LI Yongfei, CHEN Qingli
Department of Cryptogram Engineering, Information Engineering University, Zhengzhou 450001, China

Abstract: Considering that network defense subjects were usually resource-constrained, an intelligent planning and autonomous implementation of network defense strategies under bounded rationality was studied considering the concept of intelligent confrontation. First, attack graph, general knowledge and domain-specific knowledge were fused to construct a network defense security ontology. On that basis, knowledge reasoning was utilized to recommend security defense strategies to better adapt to the security needs of protected network information assets and current attack threats. Finally, an autonomous planning and implementation of defense strategies was achieved under the constraints of limited network security defense resources and dynamic changes of network information assets with the help of bounded rationality. The example shows that the proposed method is robust under dynamic attacks. The experiments show that the defense effectiveness is improved by 5.6%～26.12% compared with existing game theory and attack graph-based methods against a typical APT attack.

Keywords: cyber defense, defense strategy recommendation, intelligent planning, bounded rationality, security ontology

0 引言

当前，网络攻击门槛低、攻击时间随机且快速见效，对机构与组织的信息资产造成极大威胁。减少网络攻击造成损失的关键在于快速实施有针对性的安全防御措施。机构的办公网络及运营网络等安全防御体系通常与网络信息系统同步建设，其防御资源的部署和安全策略相对静态，难以适应网络

收稿日期：2022−12−30；**修回日期：**2023−03−26
通信作者：郭渊博，yuanbo_g@hotmail.com
基金项目：国家自然科学基金资助项目（No.62276091）；河南省重大公益专项基金资助项目（No.201300311200）
Foundation Items: The National Natural Science Foundation of China (No.62276091), The Major Public Welfare Project of Henan Province (No.201300311200)

入侵者攻击手段的快速演化，在应对高度自动化与智能化的攻击时[1-2]，这种静态安全防御模式的局限性尤其明显。

智能化攻击对网络空间安全造成了极大威胁，覆盖了物理基础设施、网络信息系统和社交媒体信息，同时对虚拟世界、物理世界的诸多方面造成极大影响[3]。为有效抵抗智能化网络攻击的自适应性和快速性，需要以智能应对智能，建立针对网络攻击的智能化安全防御策略自动推演与规划实施机制，从而实现智能化的网络防御。

实施智能化网络防御首先需要建立攻防安全知识与威胁情报体系[4]的支持。网络安全防御现象涉及通用知识、场景领域知识等异质知识集合，需要形式化、规范化地整合契合具体网络安全防御场景的知识。在安全知识体系中建立安全属性并准确定义属性间的关系，可为安全防御提供可靠的理论依据[5]。在此基础上，根据资产所需安全手段及构建的安全知识体系高效地执行推理，可为资产推荐合适的防御策略[6]。进一步地，可针对资产属性衡量防御策略的重要性，并根据资产现存的风险因素优化防御策略推理过程。

实施智能化网络防御最终需要执行防御策略以实现有效防御[7]。为了在入侵行为对系统造成实质伤害之前就阻碍入侵的发生，需要构建有针对性的弹性防御体系，采取主动防御的方式执行合适的防御策略，避免、转移、降低信息系统面临的风险[8]。考虑网络安全防御场景中时间、认知与信息条件的高度有限呈常态化，如何在计算资源高约束、资产环境动态的条件下实现有效防御是亟待解决的问题[9]。

本文针对上述问题开展研究，在假设防御主体具有有限理性的基础上，提出了一种网络防御策略智能规划与自主实施方法，如图 1 所示。首先，融合多源异构安全知识构建安全本体；然后，根据实例化后的安全本体推荐防御策略；最后，利用智能代理和有限理性规划防御策略，并实施最佳防御规划方案。

本文主要贡献如下：1) 建立了安全本体并将其作为安全知识体系，对多源异构安全知识进行形式化、规范化表达，为防御策略推荐提供信息支撑；2) 利用知识推理的方法实现了防御策略推荐，以适应当前所面临的攻击威胁以及受保护网络信息资产的安全需求；3) 提出了一种智能化网络防御方法，在计算资源高约束、资产环境动态的条件下，利用智能规划[10]与有限理性[11]实现自主防御。

1　相关工作

网络安全已经全面进入智能防御时代，融入人工智能技术成为网络攻防的新常态。传统信息安全防御体系多采用被动防御的方式，安全防御措施和策略难以根据入侵者的行为或影响进行动态调整。随着大数据特别是人工智能技术的迅猛发展，及时精准的安全态势分析与预警成为可能，安全防御已呈现出主动化、智能化的发展趋势。

主动防御技术可通过识别威胁获得防御策略、指导防御过程。Li 等[12]提出基于可持续集成学习模型的入侵检测系统，以适应不同攻击并通过不断迭代更新实现增量学习。雷程等[13]提出基于网络攻击面自适应转换的移动目标防御（MTD, moving target defense）技术，通过在分层跳变的架构上设计网络自适应跳变算法实现网络跳变收益的最大化。张红霞等[14]提出基于深度学习模型的蜜罐陷阱合约检测方法，提升检测方法的准确率及模型的泛化能力。为了自动执行防御策略，人工智能被应用到网络安全领域，以实现智能化防御。Kim 等[15]提出一种新的具有人工智能适用性的集成虚拟情感系统，以实现安全网络物理系统（CPS, cyber-physical system）智能城市。Vast 等[16]提出了一种基于 AI 的 SOAR（SQL optimizer and rewriter）系统，使用深度学习

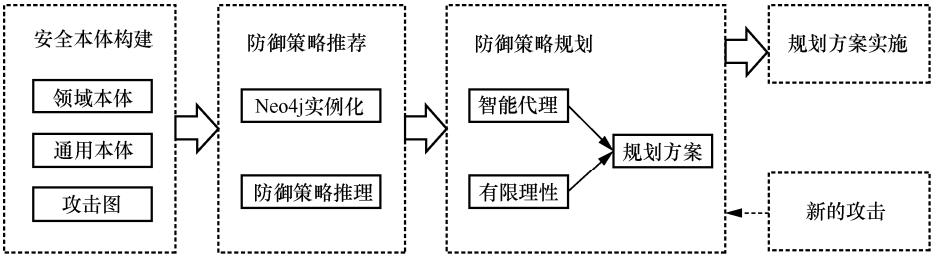

图 1　网络防御策略智能规划与自主实施方法

检测方法分析收集来自防火墙、入侵检测系统等各种来源的数据，以自动生成威胁情报并采取适当/必要的步骤。Theron 等[8]将智能代理用于自主对抗智能恶意软件，根据用户定义的准则，主动制订、调整并执行自主网络安全防御过程，实现自主智能网络防御。进一步，Yan 等[17]利用不完全信息的零和博弈来确定纳什均衡下攻击者和防御者的预期效用，以对电气 CPS 的防御资源进行适当的分配。然而，现实网络安全防御场景中安全信息的获取往往被忽视，对安全信息认知的设定易于理想化，缺乏对实际场景中局限性的应对方法，需要有限理性（BR, bounded rationality）这类方法的支撑，在信息有限、认识有限与时间有限的条件下求取近似优化解[18]。总之，在现有技术条件下，人工智能规划与有限理性最有望在各种受限条件下进行安防规划，通过智能代理自动化实施防御策略。

建立攻防安全知识与威胁情报体系是实施安全防御的信息基础。安全知识种类庞杂、关系繁多，造成安全知识形式化表达困难。本体[19]的思想由此被引入网络安全领域，实践证明可以构建安全本体，用于组织并系统化表达安全现象[20]。Beitollahi 等[7]针对分布式拒绝服务攻击构建安全本体，成功产生有效防御策略。Syed 等[4]提出统一网络安全本体（UCO, unified cybersecurity ontology），旨在支持网络安全系统中的多源异构信息集成和网络态势感知。Kim 等[21]通过构建由通用知识本体与特定领域本体集成的问题域本体（PDO, problem domain ontology），获得高级持续性威胁（APT, advanced persistent threat）攻击的安全需求推荐，并由此拓展给出通用的安全需求建议[22]。上述工作表明，安全本体具有系统性构建安全知识库的潜力，可以为网络安全防御提供高覆盖的安全知识支撑，并为智能代理自动化实施推荐的防御策略带来便利。

针对以上方法的局限性，结合安全本体的思想并同时考虑资源高度约束条件下的主动智能防御需求，本文提出一种以安全本体为推理引擎、AI 自主规划与有限理性主导的智能防御方法，为解决问题提供新思路。

2 本体驱动的防御策略智能推荐

如前所述，系统发现攻击时[23-25]，完善的安全防御知识体系能够有效推理防御策略，为防御策略推荐提供信息支撑。

本节通过整合多源异构安全知识构建安全本体，并在形式化表达安全知识的基础上，针对不同资产类型高效地执行推理，为资产推荐合适的防御策略。

2.1 安全本体构建

在整合多源异构知识方面，本体具有不可替代的优势。领域本体 O 可以用一个五元集合表示，即

$$O=\{C,A,R,I,M\} \tag{1}$$

其中，C 为特定领域的概念集合，A 为概念的属性集合，R 为 A 中概念间的关系集合，I 为实例集合，M 为实例 I 与概念 C 的映射关系集合。

根据本体的特点及五元集合表达式，在仅考虑概念及其相互关系的情况下，设计了面向防御策略推荐的安全本体，为防御策略选择构建适应性强的情报基础。此外，智能代理可以利用安全本体实施推理、执行防御策略。

为了实现自适应于资产安全信息的防御策略推荐，安全本体设计只有同时考虑攻击实施的过程与防御响应的需求，才能为防御策略推荐必需的知识推理打好基础。

根据本体所要描述的目标，可以将其分为通用本体和领域本体[22]。通用本体指的是可以广泛应用于多种应用场景的本体知识，是对通用知识的规范描述；领域本体则指的是对一个具体领域知识的规范描述。本体可以看作知识库，通用本体和领域本体分别对应通用知识和领域专有知识。通用知识是显式的、可重用的，是在整个安全领域中达成共识的知识，例如分类、原则等。领域专有知识是应用于特定领域的、嵌入流程等中的隐性知识，例如该领域/机构架构等。

安全本体将安全知识体系涉及的通用安全知识显性表达，而将专有知识隐性表达；总体设计原则为既涵盖通用安全模型的要件，又便于网络安全防御场景强相关知识的自适应扩展。

在攻击实施方面，攻击发起要成功利用漏洞需要满足一定的条件，如可到达、可访问等；而在漏洞利用成功后，会引入新的风险因素。为保证根据安全本体的概念及其关系推断出可靠的防御策略，安全本体需要充分表达利用漏洞需要的条件以及利用成功后引入的风险因素，而这些因素可以通过攻击图获得。

在防御响应方面，首先定义公认的风险分析模

型中的资产、威胁、风险、漏洞等核心要素，以及安全需求、防御策略相关的通用知识；其次定义领域/机构架构等特定领域专有知识。

根据以上分析的安全本体的特点，构建攻击图增强的安全本体 AG（attack graph）-SO（security ontology），将攻击图、通用知识及特定领域专有知识融合于一体。由于本节只关注本体本身的设计，而不考虑实体及映射关系，因此将 AG-SO 定义为三元集合。

攻击图增强的安全本体为 $\text{AG-SO}=\{\text{SC},\text{SA},\text{SR}\}$，其中，$\text{SC}=\{\text{sc}_1,\text{sc}_2,\cdots,\text{sc}_n\}$ 为概念集合，$\text{SA}=\{\text{sa}_1,\text{sa}_2,\cdots,\text{sa}_n\}$ 为属性集合，$\text{SR}=\{\text{sr}_1,\text{sr}_2,\cdots,\text{sr}_n\}$ 为概念间的关系集合。

AG-SO 组成与关系如图 2 所示。AG-SO 中主要的概念 SC 不仅包括资产、威胁、风险、漏洞、安全需求、防御策略等显性的通用知识，还包括系统/领域的架构等隐性的领域专有知识，以及利用漏洞需要满足的条件及利用成功后引入的风险因素。此外，每个概念都包含了相应的属性 SA，即字符属性、描述属性、布尔属性等。概念关系 SR 中，从攻击实施的视角，通过 AG-SO 可表达满足一定条件的漏洞能够被威胁利用，导致风险因素增加；反之，从防御响应的视角，目标为减少资产中存在的风险因素，通过 AG-SO 推断资产所需安全手段，推理得到可用防御策略并予以实施，从而满足安全需求并减少风险因素使恶意目标无法达成，完成一次有效安全防御。

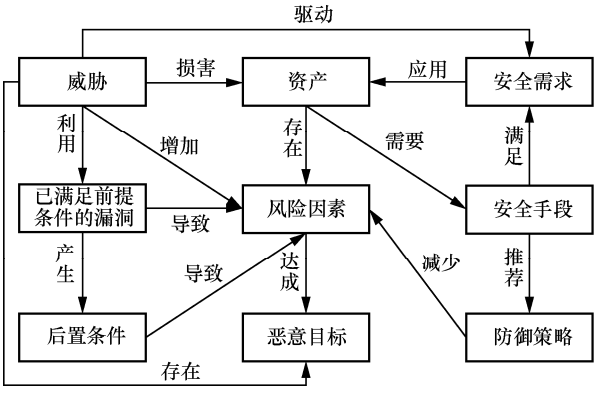

图 2　AG-SO 组成与关系

2.2　防御策略推理

基于所构建的安全本体 AG-SO 可以进行基于知识推理的安全防御措施推理，实现针对不同类型攻击及受保护资产类型的智能防御。AG-SO 驱动的防御策略推理包括两部分：1) 融合防御策略推荐所需通用知识、领域专有知识、利用漏洞需要具备的前提条件及利用成功后引入的风险因素信息；2) 根据资产所需安全手段进行风险评估，支持查询推荐可行的防御策略。换言之，通过实例化 AG-SO 获取防御策略推荐相关的安全信息，利用图形数据库 Neo4j 构建安全知识库。其中，SC 包含通用知识、领域专有知识、利用漏洞需要具备的条件，以及漏洞利用成功后引入的风险因素；SA 包含概念具有的属性；SR 包含概念间的关系。由此进行知识推理可获取资产所需的防御策略。

为了向资产推荐可行的针对性防御策略，可以根据日志确定资产的功能及所需的安全手段。首先，通过日志分析确定资产的功能，如存储数据等；然后，针对资产的功能，确定相关安全属性、恶意目标及防御策略的类型，才能推断所需安全手段。

安全属性一般包括机密性（Co）、完整性（In）、可用性（Av）、鉴别性（Au）、可控性（Ct）与不可否认性（Nr）等，其中，前 4 种属性是基本的安全属性，为简化描述，本文只考虑这 4 种属性。与这些安全属性相对应，破坏性的恶意目标分别为暴露（E）、修改（M）、销毁（Dt）及伪装（F）。防御策略类型包括预防（P）、监测（D）、恢复（R），其重要性则以关键（C）或非关键（N）衡量。C 是最高优先级，表示需要的防御策略类型；N 是最低优先级，表示不需要的防御策略类型。

本文根据资产的功能，衡量各防御策略类型在不同恶意目标下的重要性，最终确定所需的安全手段。资产所需安全手段计算矩阵示例如表 1 所示，资产安全属性 Co 所需安全手段为 P，In 所需安全手段为 PDR，Av 所需安全手段为 DR，Au 所需安全手段为 D。可以推断该资产所需安全手段为：机密性预防（PCo）、完整性预防（PIn）、完整性检测（DIn）、完整性恢复（RIn）、可用性检测（DAv）、可用性恢复（RAv）及鉴别性检测（DAu）。

表 1　　资产所需安全手段计算矩阵示例

安全属性	恶意目标	防御策略类型			资产所需安全手段
		预防(P)	监测(D)	恢复(R)	
Co	E	C	N	N	P
In	M	C	C	C	PDR
Av	Dt	N	C	C	DR
Au	F	N	C	N	D

为了满足资产所需安全手段，需要评估资产现存风险并利用 Cypher 语句查询 AG-SO 中实体的关系，由此推理并实施防御策略。首先，通过表 1 获得当前资产所需安全手段，并查询 AG-SO 实例中的关系，得到危害资产安全的威胁、可被利用的漏洞及恶意目标；然后，获取当前已有的防御策略，分析是否存在风险因素（未采取防御策略防御的恶意目标）；最后，针对资产现存的风险因素推荐所需安全手段，查询 AG-SO 获取可行的防御策略。至此，本文实现了在安全知识形式化表达基础之上的防御策略推理。

3 基于有限理性的防御策略智能规划与自主实施

在上述推荐的防御策略基础上，规划防御方案并予以实施能够有效实现主动防御。

防御者在实施防御时通常面临时间、认知与资源等多方面的约束，例如，对攻击者的攻击手段及能力的认知有限，对攻击的反应时间有限，自身的防御资源有限等。考虑到 BR 方法在支撑网络防御策略选择的优势，设定时间、认知与信息的边界条件，利用有限理性与智能规划智能分配资源，规划当前最佳网络安全防御方案并予以自动化实施，从而实现资源高度约束条件下的智能化防御。

3.1 防御策略智能规划

智能规划旨在通过执行一系列行动以实现期望的目标[26]。将其用于网络安全防御场景，可以模拟人类防御行为，关注系统当前急需的防御措施，并由初始状态通过执行一系列防御策略到达目标状态，以此实现安全目标。

现代规划器大都源于经典智能规划 STRIPS 语言，然而主流规划器很少考虑存储空间的物理限制以及基本知识的可用限制。针对此问题，本文考虑到有限理性方法在支撑网络防御策略选择的优势，设定时间、认知与信息的边界条件，将 STRIPS 语言有限理性拓展为 STRIPS-BR，在有限理性的范围内智能分配资源，规划当前最佳网络安全防御方案并予以自动化实施，从而实现资产安全目标。根据文献[26]，列出智能规划所需的具有有限理性的智能代理术语，如表 2 所示。

表 2 具有有限理性的智能代理术语

术语	说明
BR-$A(T)$	对攻击的反应时间 T 有限，它限制了规划生成和实施期间用于构造和评估搜索树的搜索空间中状态的数量
BR-$A(C)$	规划生成和实施过程中对攻防双方的认知有限，它限制了代理的搜索树深度
BR-$A(I)$	在规划生成和实施期间，自身防御资源有限
S-BR	代理在其认知范围内了解的资产状态
G-BR	代理希望为真的一组目标命题
CM-BR	代理在规划生成期间，使用有限内存知道的防御策略
P^x	STRIPS-BR 规划器为代理制定的规划方案，即一系列待执行防御策略序列
$P^x_{i,j}$	时间步 $t=i$ 和 $t=j$ 之间的部分规划，是 P^x 的子序列
O^x	P^x 执行的结果
$\mathrm{rank}(s_i)$	实际执行的防御策略顺序
cm^x_k	规划方案 P^x 顺序执行的第 k 个防御策略
w^x_k	分配给 P^x 的第 k 个防御策略的权重值
$U(P^x_{0,k})$	P^x 中从开始到第 k 个防御策略的累计规划效用

STRIPS-BR 首先定义了有限理性中的 3 个约束，即时间有限、认知有限与信息有限。其中，时间有限 BR-$A(T)$及认知有限 BR-$A(C)$分别可以通过检查状态的时间计数及认知深度是否已超过各自的限制进行判断；信息有限 BR-$A(I)$包括未知的或错误假设的资产状态 S-BR、目标命题 G-BR 以及可用的有限防御策略 CM-BR。根据这些信息建立搜索树，获取所有可以满足目标状态的规划方案 P^x。P^x 中防御策略序列执行的结果为 O^x，$\mathrm{rank}(s_i)$ 为实际执行的防御策略顺序。

为了确定最佳（效用最高）防御规划方案，定义 $U(P^x_{0,k})$ 为规划 P^x 中从开始到第 k 个防御策略的累计规划效用，即

$$U(P^x_{0,k})=\sum_{t=0}^{k} w^x_t \tag{2}$$

其中，w^x_k 为 P^x 中第 k 个防御策略 cm^x_k 的权重，即

$$w^x_k=\text{in-degree}+0.1\sum_v \mathrm{cvss}_v+\lambda \tag{3}$$

$$\mathrm{cvss}_v=\alpha \mathrm{CVSS}_v \tag{4}$$

其中，in-degree 为防御策略 cm^x_k 的入度；cvss_v 为采用防御策略 cm^x_k 对漏洞 v 的防御概率 α 与漏洞 v 的 CVSS 评分之积；$\sum_v \mathrm{cvss}_v$ 为执行防御策略 cm^x_k 能解决的现存漏洞 v 的 cvss_v 值之和，反映该策略对现存

漏洞的重要性；λ 是一个相关因子，代表当前防御策略 cm_k^x 与前一个防御策略的相关度，若当前防御策略与前一个防御策略相关（属于同一个安全手段），则 λ=0.3，否则 λ=0 。

防御策略入度示例如图 3 所示。DIn、PIn 与 RIn 分别表示资产所需的安全手段，CM_1、CM_2 与 CM_3 表示待执行的防御策略，且 CM_1 属于 DIn、PIn，CM_2 属于 PIn，CM_3 属于 RIn。由于 CM_1 与 DIn 及 PIn 都相关，因此其入度值记为 2。同理，CM_2 与 CM_3 入度值都为 1。防御策略的入度值反映当前策略的重要程度，入度值越高表示执行该防御策略后可以满足的安全手段需求越多。获得每个防御策略的入度后，在每个时间步由式(3)计算 w_k^x 。

然后，在有限理性 BR-$A(T)$以及 BR-$A(C)$的约束下，根据防御策略的权重选择效用最高的规划方案。通过计算时间步 t 及 t+1 各个规划的效用，选择当前效用最高的一个或多个规划方案作为候选方案，再移动到下一个时间步。随着时间步的增加，认定在认知有限内的最后一个时间步时具有最高效用的规划方案为最佳防御方案，若有多个规划方案的效用相同，则执行防御策略权重较高的规划方案。

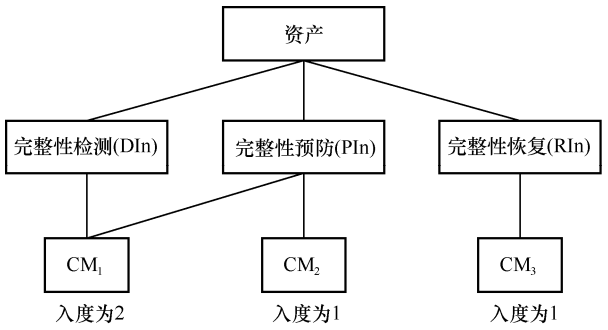

图 3　防御策略入度示例

STRIPS-BR 通过引入时间、认知与信息的有限约束，可以在有限理性的范围内进行网络安全防御规划，选择当前最佳防御方案作为初始规划方案。

3.2　防御策略自主实施

获得初始规划方案后，即可实施该规划方案。执行方案期间，资产可能仍会遭受新的攻击，因此，智能代理会在每个时间步 t 监控并分析日志数据，以确定是否有必要重新规划并分配资源，以实现智能化防御。

当资产受到连续攻击时，若针对之前攻击的防御规划方案尚未执行完毕，则暂停执行该方案并对与当前所遭受攻击相关的未执行防御策略构建搜索树，实施具有最高效用的新规划方案。新规划方案执行完毕后，再对之前未执行防御策略制定并实施规划方案。通过监控方案的执行过程并在必要时重新规划，可以关注资产当前急需的防御措施，智能化调整防御方案，实现动态环境下及资源高度约束条件下的智能化防御。

总体来说，有限理性智能规划的防御策略自主实施方法可以针对资产所需安全手段部署防御策略，具备可行性。此外，本文方法适用于不同资产类型，且可在执行过程中根据环境变化重新规划，能够在动态攻击场景下智能化规划及调整最优防御策略，具备稳健性。

4　实例演示

本文提出了一种以安全本体为推理引擎、智能规划与有限理性为主导的智能防御机制，以解决计算资源高约束、资产环境高动态下的智能化防御问题。

本节以一个典型办公网络场景为应用实例，演示了网络防御策略智能推荐方案、防御策略智能规划方案与自主实施方案，以验证所提方法的有效性。安全防御场景网络中共包含一个硬件防火墙、3 台内部主机和一个数据库服务器，如图 4 所示。

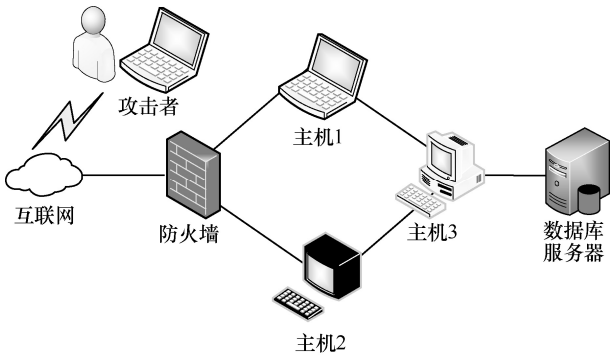

图 4　安全防御场景网络设置

防火墙用于对出入内部网络的流量进行过滤，阻止来自外部的各种攻击和来自内部的信息泄露。主机 1 和主机 2 用于接收和处理来自外部网络的各类请求，并将请求分类汇总到主机 3。主机 3 负责向数据库服务器发出数据查询请求和接收查询结果，并将结果反馈给主机 1 和主机 2。假设攻击者已攻陷防火墙，接下来将对目标网络内的主机和服务器进一步渗透。网络中资产都采用 Windows10 系

统，且资产主要功能为数据存储。

4.1　防御策略智能推荐实例

根据与安全相关的通用知识、与领域相关的领域专有知识、攻击图中所涉及的利用漏洞发起攻击需要满足的条件以及攻击发生后引入的风险因素，构建全面的面向防御策略推荐的本体 AG-SO。

根据 AG-SO 的概念定义及其之间的关系，Neo4j 实例化后的安全知识图谱如图 5 所示。以存放日志数据为例，展示与之相关的信息及关系。节点代表不同类型的实体，包括资产、资产所需安全手段、恶意目标、威胁、风险、漏洞、安全需求、架构、推理得到的防御策略及利用漏洞需要具备的前提条件。发起攻击所需要的条件为需要具备访问权限（可到达、可访问），同时引入了攻击成功后可能带来的风险因素。

为了采取防御策略以达到安全目标，首先利用表 1 分析日志明确资产所需安全手段，即完整性检测（DIn）、完整性预防（PIn）与完整性恢复（RIn）。而后，通过查询 AG-SO 中实体及关系推理出资产日志数据存在由威胁 CAPEC-268（审计日志操作）利用弱点 CWE-440（违反预期行为）导致的数据误用风险，以此修改日志数据。为了利用弱点 CWE-440 需要拥有访问权限（即图 5 中的 0），利用成功后可引入数据误用风险因素。为了降低该风险，可以采用文件完整性监测（FIM）的防御策略对日志的完整性进行监测，以达到资产安全手段 DIn 及 PIn，从而满足安全需求 SR-11-6-2（日志及备份系统）。依此类推，可从 AG-SO 中查询推理获得所有防御策略推荐，其中，文件完整性监测（FIM）属于完整性检测（DIn）与完整性预防（PIn），疫苗剂（VA）属于完整性预防（PIn），同步日志数据（SLD）属于完整性恢复（RIn）。资产所需防御策略如图 6 所示。

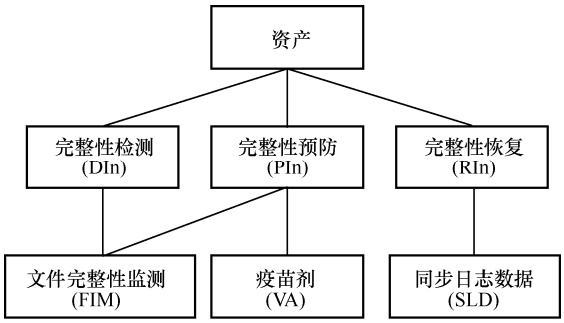

图 6　资产所需防御策略

与传统网络安全防御技术相比，AG-SO 提高了安全知识的覆盖面，为推荐防御策略提供了更全面、更精确的信息。通过 AG-SO 获得防御策略后，如何自主实施防御策略是重中之重。

4.2　防御策略智能规划实例

利用智能规划对上述可用防御策略生成规划方案并执行防御策略组合，实现防御策略的自主实施。进一步，本文引入有限理性寻找最佳防御方案，在多种资源高度受限的常规网络安全防御场景下智能化分配资源。

智能规划通过对待执行防御策略打分，选取最佳（具有最高效用）的防御规划方案作为初始规划方案。

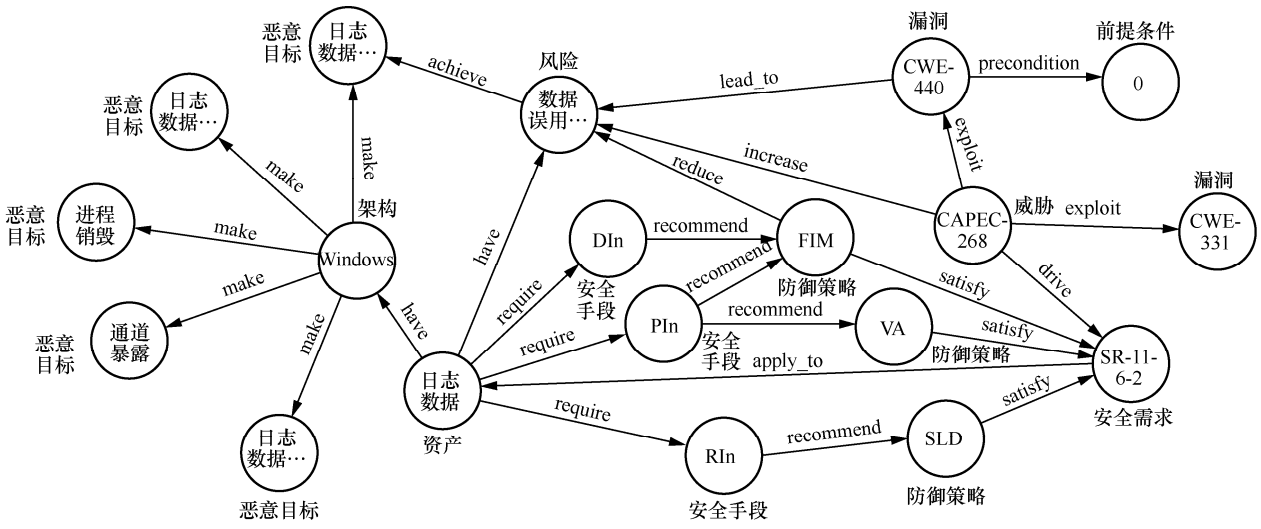

图 5　Neo4j 实例化后的安全知识图谱

计算每个时间步下防御策略 cm_k^x 的权重 w_k^x，并相加获得每个规划的效用 $U(P_{0,k}^x)$，从而选择具有最高效用的规划方案作为初始规划方案。首先，利用现有漏洞评估工具 Nessus[27]扫描并确定现存漏洞 CVE-2017-0143、CVE-2017-0267 及 CVE-2021-1074；然后，根据当前防御策略能够解决漏洞的程度赋予防御策略 cm_k^x 权重 w_k^x。通过查询相关信息可知，漏洞 CVE-2017-0143 被攻击者成功利用时会导致任意代码执行；漏洞 CVE-2017-0267 和 CVE-2021-1074 被攻击者成功利用时会导致信息泄露。此外，假设攻击者每次利用上述漏洞都能成功发起攻击，网络中采用防御策略 FIM、VA、SLD 对上述 3 种漏洞的防御概率如表 3 所示，其中，防御概率为 0 表示没有防御效果，防御概率为 1 表示完全防御，防御概率介于区间(0,10)表示有部分防御效果。

表 3　　防御概率

所在位置	漏洞 ID	FIM	VA	SLD
主机 1	CVE-2017-0143	0.2	0.5	0.6
主机 2	CVE-2017-0267	0.3	0.6	0.8
主机 3	CVE-2021-1074	0.2	0.5	0.6

进一步地，由式(4)及表 4 计算防御策略 FIM 针对现存漏洞 CVE-2017-0143 的防御权重部分为 $\mathrm{cvss}_{\mathrm{CVE-2017-0143}}=0.2\times8.1=1.62$；再根据所有现存漏洞 v 的 cvss_v 值，利用式(3)得到防御策略的权重；最后由式(2)计算规划效用，选择最高效用的规划方案作为初始规划方案，具体过程如图 7 所示。

表 4　防御策略权重（基于 CVSS 3.0 标准）

漏洞 ID	CVSS 评分	FIM	VA	SLD
CVE-2017-0143	8.1	1.62	4.05	4.86
CVE-2017-0267	5.9	1.77	3.54	4.72
CVE-2021-1074	7.3	1.46	3.65	4.38

从时间步 t=0 的“开始”节点开始规划。因为本文更关注短期的防御效果，所以设定认知有限约束 BR-$A(C)$=2。根据防御方想要快速响应攻击并部署防御措施的急切性，设定 BR-$A(T)$=13。在这种约束下，无法得到搜索树中超过前 13 个状态的状态，因此不考虑最后一条路径，应计算所有规划从时间步 t=0 至时间步 t=2 的效用。

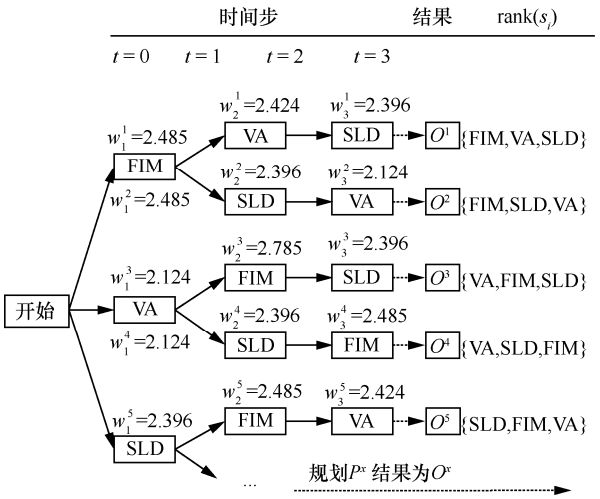

图 7　选取初始规划方案过程

首先，计算每个规划方案中防御策略的权重，如规划 P^1 中 w_1^1=2+0.1×(1.62+1.77+1.46)+0 =2.485，w_2^1=1+0.1×(4.05+3.54+3.65)+0.3=2.424，w_3^1= 1+0.1×(4.86+4.72+4.38)+0=2.396；然后，计算从时间步 t=0 至时间步 t=2 的规划效用；接着，比较所有规划效用，得出规划 $P_{0,2}^1$ 与 $P_{0,2}^3$ 的效用 $U(P_{0,2}^1)$ 与 $U(P_{0,2}^3)$ 最高，为 4.909，因此选择规划 P^1 与 P^3 作为候选规划；最后，进入下一时间步计算规划效用直到选出最佳（最高效用）防御规划方案作为初始规划方案，若存在多个同样效用的规划方案，选择最先执行较高效用的规划。当时间步 t=1 时，规划 $P_{1,3}^1$ 的效用 $U(P_{0,3}^1)$ 与规划 $P_{1,3}^3$ 的效用 $U(P_{0,3}^3)$ 相同，都为 7.305。但规划 P^1 首先执行权重较高的防御策略 FIM，因而选择 P^1 作为初始规划方案，执行顺序为{FIM, VA, SLD}。

4.3　防御策略智能实施实例

确定规划方案 P^1 后，在时间步 t=1 执行 FIM。由于 BR-$A(C)$=2，因此在时间步 t=2,3 时会转移到一个新的状态，通过分析确定是否需要重新规划防御方案，实现智能化防御。

当时间步 t=2 时，代理对方案进行监控并对日志进行分析，发现攻击者尝试篡改数据，触发重新规划。此时立即停止执行 P^1，通过 AG-SO 寻找与此攻击相关的防御策略 SLD，并推迟剩余的防御策略 VA。同时，对与此攻击有关的防御策略 SLD 进行规划，规划方案 P^{11} 如图 8 所示。如果有更多规划方案，代理将计算所有规划的效用并选择具有最高效用的规划方案。从时间步 t=2 开始，代理执行结果为 O^{11} 的规划 P^{11}。将部分执行的规划 $P_{0,1}^1$ 与新

规划 P^{11} 结合起来得到 $P^{1\cup 11}$。这个新规划的实际顺序为 $O^{1\cup 11}$，即{FIM, SLD}。在新顺序中，与原计划 P^{1} 的防御策略执行顺序不同，目标 VA 被推迟且不包括在结果 $O^{1\cup 11}$ 中。

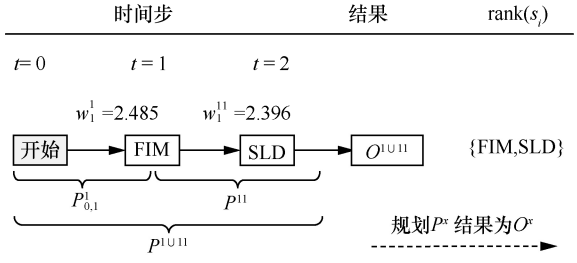

图 8 规划方案 P^{11}

在执行新规划 $P^{1\cup 11}$ 期间，代理先尝试满足其前提条件，然后在时间步 t=2 时执行防御策略 SLD，成功执行规划 $P^{1\cup 11}$ 获得结果 $O^{1\cup 11}$。达成新规划的目标 SLD 后，为剩余的防御策略 VA 构建一个新的搜索树，VA 在时间步 t=3 被添加执行。图 9 显示了通过新规划 P^{12} 产生的最终规划 $P^{1\cup 11\cup 12}$。在时间步 t=3 执行后，所有目标均已实现。最终的实际防御策略顺序是{FIM,SLD,VA}，可以看出其结果 $O^{1\cup 11\cup 12}$ 与没有重新规划的 P^{1} 顺序{FIM,VA,SLD}不同。

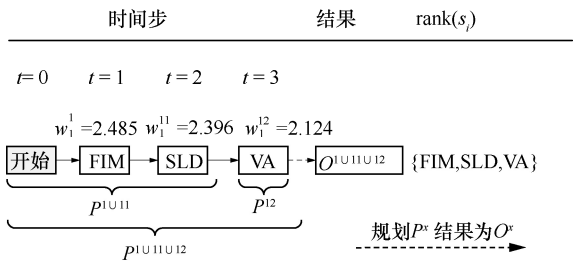

图 9 通过新规划 P^{12} 产生的最终规划 $P^{1\cup 11\cup 12}$

至此，所有防御策略执行完毕，实现了网络动态环境下及资源高度约束条件下的智能化防御，证明了本文方法的有效性。

4.4 讨论

虽然办公网络及企业运营网络等拓扑相对固化，但是仍有拓扑结构发生变化的情况。此时需要更新本体中架构等特定领域知识，而通用知识由于其通用性以及可重复使用不需要更改。然后，依据新构建的知识按照前述方案执行即可。

此外，本文方法保留执行过的历史记录，包括受到的攻击、资产的主要功能、有限理性的约束、资产所需防御手段以及规划并执行的防御方案。如果再遇到类似攻击，可依据历史知识快速进行响应。

5 性能评估

CALDERA[28]是 MITRE 公司研发的一个攻击模拟工具，该工具的攻击流程是建立在 ATT&CK 攻击行为模型和知识库之上的，接近 APT 攻击行为模式。MITRE ATT&CK[29]是由 MITRE 创建并维护的一个对抗战术和技术的知识库，反映了攻击者攻击生命周期以及各个攻击阶段的目标。本文借助 CALDERA 模拟 ATT&CK 中描述的典型 APT29 攻击评估本文方法的有效性及所提本体的知识完备性。

5.1 防御方法性能评估

为了验证本文方法的有效性及优越性，将本文方法与文献[30-32]中的典型防御方法应对 CALDERA 模拟的 APT29 攻击的防御效果进行对比。从网络安全防御资源的有限性、防御策略选择基准、时效性及防御有效性几个方面，定性定量地评估本文方法，如表 5 所示。

1) 网络安全防御资源的有限性方面。文献[30]方法考虑防御策略的部署成本，引入纳什均衡获取并实施最佳防御策略以保护关键基础设施；文献[31-32]未

表 5 本文方法与典型防御方法比较

方法	网络安全防御资源的有限性	防御策略选择基准		时效性		防御有效性
		CVSS/攻击概率	攻击特性	预先分析	实时更新	
文献[30]方法	√	×	√	√	×	38.70
文献[31]方法	×	√	×	√	×	43.51
文献[32]方法	×	√	×	√	×	49.43
本文方法	√	√	√	√	√	52.38

考虑网络安全防御资源的有限性；本文引入有限理性，与文献[30]仅考虑防御部署的成本相比较，从实际角度出发，考虑时间、认知与信息资源的受限问题，实现在多种资源高度受限的常规网络安全防御场景下实施自主防御过程。

2) 防御策略选择基准方面。攻击特性代表攻击的特点，如 APT 攻击通常利用恶意软件、0Day 漏洞等对目标系统进行渗透，以此展开持续有效的攻击活动。文献[30]考虑攻击特性利用纳什均衡最小化攻击造成的损害；文献[31]利用贝叶斯攻击图对基础设施进行安全风险评估；文献[32]依据 CVSS 计算主机的攻击概率评估主机的安全性；本文从防御策略角度出发，通过分析漏洞 CVSS 评分及针对攻击特性引入的策略相关度等，全面评估对现有漏洞的防御效果。

3) 时效性方面。文献[30-32]都是通过预先分析的方式确定并实施防御策略，虽然文献[31-32]可以通过更新攻击图的方式动态更新防御策略，但对于大型复杂网络攻击图的构建及更新较困难，难以达到实时更新；本文利用安全本体作为知识库，不仅可以预先分析获得防御策略，还可以根据实际情况实时更新防御策略。

4) 防御有效性方面。考虑防御者实施防御时所需的开销情况，根据式(5)评估文献[30-32]及本文方法每 100 次防御行为能使多少次攻击失效，以此计算各方法的防御有效性[33]。其中，η_{defense} 表示防御有效性，$N_{\text{A,total}}$ 表示攻击实施的总次数，$N_{\text{A,success}}$ 表示攻击成功的次数，N_{D} 表示防御行为实施的次数。当防御完全无效时，$\eta_{\text{defense}}=0$，其他情况下 $\eta_{\text{defense}}>0$（无上限）。η_{defense} 的含义是每 100 次防御行为能使多少次攻击失效，该值越大，表明防御越有效。

$$\eta_{\text{defense}}=\frac{N_{\text{A,total}}-N_{\text{A,success}}}{N_{\text{D}}}\times 100 \tag{5}$$

根据 ATT&CK 中描述的 APT29 攻击技术，分别计算文献[30-32]及本文方法的防御有效性 η_{defense}。具体而言，为应对 APT29 中列出的某种攻击技术，不同方法采取不同防御措施，对该攻击技术的防御效果如何，考虑所有攻击技术后即可评估不同方法的防御有效性。表 5 结果表明，考虑到防御资源的有限性和动态环境中防御策略更新的及时性，所提方法优于最先进的方法，具有最高的防御效果，防御有效性提高了 5.6%～26.12%。

5.2　本体性能评估

知识完备性通常作为本体的评价指标[34]，本文主要考虑本体构建时是否考虑到攻击双方的知识库以及攻击发起的条件。

对比本文方法所采用的 AG-SO 与 UCO[4]和 PDO[21]应对 APT29 攻击的防御效果，从知识完备性以及在本文方法中使用相应本体的防御有效性两方面证明本文提出的 AG-SO 的优越性，如表 6 所示。

表 6　AG-SO 与常见本体比较

本体	知识完备性		防御有效性
	攻防双方	攻击条件	
UCO	×	√	39.45
PDO	√	×	44.26
AG-SO	√	√	52.38

UCO 整合了攻击相关的多源异构知识，缺乏与防御方的知识交互；PDO 整合了攻防双方的多源异构知识，但未考虑攻击条件对整个攻防过程的影响；本文的 AG-SO 既融合了攻防双方的多源异构信息，又在构建本体时考虑到攻击条件的影响。在只改变本体的情况下评估本文方法的防御有效性发现，利用 AG-SO 的防御有效性较好。

综上所述，常见防御策略实施方法大多通过分析漏洞的 CVSS 评分或漏洞被攻击的概率找到最可能被攻击的节点，或通过训练攻击特性识别网络威胁从而实施相关防御策略。然而，这些方法在资源高约束下防御策略实施效果欠佳，同时实时更新的效能难以保证。而本文方法从资产所需安全手段出发，获得资产当前最紧急的安全需求，并从防御策略角度分析对现有漏洞的防御效果，同时引入有限理性，实现在时间、认知与信息资源均高度受限的常规网络安全防御场景下的自主防御，预期时效性较好，防御有效性较高。与常见防御策略实施方法相比，结果表明构建的安全本体更加完备，所提防御方法具备创新性。

总体来说，所提出的网络防御策略的有限理性智能规划与自主实施方法可以在防御资源有限的情况下实现智能化网络防御，在缓解大型网络中计算资源的高度限制和动态资产环境造成的安全问题方面具有潜力。

6 结束语

针对机构的办公网络及运营网络等相对固化，其安全防御资源的部署和安全策略相对静态，在面对高度智能化的网络入侵时经常难以完全发挥防御效能的问题，本文提出了网络防御策略的有限理性智能规划与自主实施方法。首先设计了安全本体，整合高度多源异构且呈动态更新的安全知识，建立形式化、规范化的知识表达，准确定义安全属性及其间关系；然后，根据资产所需安全手段，针对不同恶意目标通过知识推理推荐防御策略；最后，在网络安全防御场景中时间、认知与信息条件高度有限的情况下实施智能化网络防御，缓解计算资源高约束、资产环境动态带来的网络安全防御难题。实验结果表明，所提方法可行性高，具备自主规划防御策略的能力，且能够在动态攻击场景下及时规划出最优防御策略，具有稳健性。对比结果表明，与常见防御策略实施方法相比，所提方法在计算资源高约束、资产环境动态的条件下，防御有效性提高了 5.6%～26.12%。

下一步工作将进一步研究所提方法的实用化问题，重点深化在“互联网+”时代移动办公等高度动态变化的网络场景下本文方法的适用性。拟结合强化学习方法根据环境变化训练并调整有限理性预定义参数，以更新后的时间、认知与信息有限在新环境下规划防御方案。

参考文献：

[1] YUAN X Y, HE P, ZHU Q L, et al. Adversarial examples: attacks and defenses for deep learning[J]. IEEE Transactions on Neural Networks and Learning Systems, 2019, 30(9): 2805-2824.

[2] LAKHDHAR Y, REKHIS S. Active, reactive and proactive visibility-based cyber defense for defending against attacks on critical systems[C]//Proceedings of International Wireless Communications and Mobile Computing. Piscataway: IEEE Press, 2020: 439-444.

[3] JIANG F, FU Y S, GUPTA B B, et al. Deep learning based multi-channel intelligent attack detection for data security[J]. IEEE Transactions on Sustainable Computing, 2020, 5(2): 204-212.

[4] SYED Z, PADIA A, MATHEWS M L, et al. UCO: a unified cybersecurity ontology[C]//AAAI Workshop: Artificial Intelligence for Cyber Security. Palo Alto: AAAI Press, 2016: 195-202.

[5] ZHANG K, LIU J J. Ontology construction for security analysis of network nodes[C]//Proceedings of International Conference on Communications, Information System and Computer Engineering. Piscataway: IEEE Press, 2020: 292-297.

[6] PUJARA J, MIAO H, GETOOR L, et al. Ontology-aware partitioning for knowledge graph identification[C]//Proceedings of the 2013 workshop on Automated knowledge base construction. New York: ACM Press, 2013: 19-24.

[7] BEITOLLAHI H, DECONINCK G. Analyzing well-known countermeasures against distributed denial of service attacks[J]. Computer Communications, 2012, 35(11): 1312-1332.

[8] THERON P, KOTT A. When autonomous intelligent goodware will fight autonomous intelligent malware: a possible future of cyber defense[C]//Proceedings of IEEE Military Communications Conference. Piscataway: IEEE Press, 2020: 1-7.

[9] ZHOU Z, KUANG X H, SUN L M, et al. Endogenous security defense against deductive attack: when artificial intelligence meets active defense for online service[J]. IEEE Communications Magazine, 2020, 58(6): 58-64.

[10] BASALLO Y A, SENTI V E, SANCHEZ N M. Artificial intelligence techniques for information security risk assessment[J]. IEEE Latin America Transactions, 2018, 16(3):897-901.

[11] CHEN J, ZHU Q. Interdependent strategic security risk management with bounded rationality in the internet of things[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(11):2958-2971.

[12] LI X H, ZHU M Y, YANG L T, et al. Sustainable ensemble learning driving intrusion detection model[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(4): 1591-1604.

[13] 雷程, 马多贺, 张红旗, 等. 基于网络攻击面自适应转换的移动目标防御技术[J]. 计算机学报, 2018, 41(5): 1109-1131.
LEI C, MA D H, ZHANG H Q, et al. Moving target defense technique based on network attack surface self-adaptive mutation[J]. Chinese Journal of Computers, 2018, 41(5): 1109-1131.

[14] 张红霞, 王琪, 王登岳, 等. 基于深度学习的区块链蜜罐陷阱合约检测[J]. 通信学报, 2022, 43(1): 194-202.
ZHANG H X, WANG Q, WANG D Y, et al. Honeypot contract detection of blockchain based on deep learning[J]. Journal on Communications, 2022, 43(1): 194-202.

[15] KIM H, BEN-OTHMAN J. Toward integrated virtual emotion system with AI applicability for secure CPS-enabled smart cities: AI-based research challenges and security issues[J]. IEEE Network, 2020, 34(3): 30-36.

[16] VAST R, SAWANT S, THORBOLE A, et al. Artificial intelligence based security orchestration, automation and response system[C]//Proceedings of 2021 6th International Conference for Convergence in Technology. Piscataway: IEEE Press, 2021: 1-5.

[17] YAN B J, YAO P C, WANG J M, et al. Game theoretical dynamic cybersecurity defense strategy for electrical cyber physical systems[C]//Proceedings of 2021 IEEE 5th Conference on Energy Internet and Energy System Integration. Piscataway: IEEE Press, 2022: 2392-2397.

[18] JIANG Y, CEDER A A. Incorporating personalization and bounded rationality into stochastic transit assignment model[J]. Transportation Research Part C: Emerging Technologies, 2021, 127: 1-26.

[19] ZHENG H J, WANG Y C, HAN C, et al. Learning and applying ontology for machine learning in cyber attack detection[C]//Proceedings

of 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering. Piscataway: IEEE Press, 2018: 1309-1315.

[20] WOTAWA F, BOZIC J, LI Y H. Ontology-based testing: an emerging paradigm for modeling and testing systems and software[C]//Proceedings of 2020 IEEE International Conference on Software Testing, Verification and Validation Workshops. Piscataway: IEEE Press, 2020: 14-17.

[21] KIM M, DEY S, LEE S W. Ontology-driven security requirements recommendation for APT attack[C]//Proceedings of 2019 IEEE 27th International Requirements Engineering Conference Workshops. Piscataway: IEEE Press, 2019: 150-156.

[22] KIM B J, LEE S W. Understanding and recommending security requirements from problem domain ontology: a cognitive three-layered approach[J]. Journal of Systems and Software, 2020, 169: 110695.

[23] MOHAMMADI S, MIRVAZIRI H, GHAZIZADEH-AHSAEE M, et al. Cyber intrusion detection by combined feature selection algorithm[J]. Journal of Information Security and Applications, 2019, 44:80-88.

[24] AZWAR H, MURTAZ M, SIDDIQUE M, et al. Intrusion detection in secure network for cybersecurity systems using machine learning and data mining[C]//Proceedings of IEEE 5th International Conference on Engineering Technologies and Applied Sciences. Piscataway: IEEE Press, 2019: 1-9.

[25] INJADAT M, MOUBAYED A, NASSIF A B, et al. Multi-stage optimized machine learning framework for network intrusion detection[J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 1803-1816.

[26] GAJDEROWICZ B. Artificial intelligence planning techniques for emulating agents with application in social services[D]. Toronto: University of Toronto, 2019.

[27] HARRISON L, SPAHN R, IANNACONE M, et al. NV: Nessus vulnerability visualization for the Web[C]//Proceedings of the Ninth International Symposium on Visualization for Cyber Security. New York: ACM Press, 2012: 25-32.

[28] ALFORD R, LAWRENCE D, KOUREMETIS M. CALDERA: a red-blue cyber operations automation platform[C]//Proceedings of the 32nd International Conference on Automated Planning and Scheduling. Palo Alto: AAAI Press, 2022:375-376.

[29] STROM B E, APPLEBAUM A, MILLER D P, et al. MITRE ATT&CK: design and philosophy[R]. 2018.

[30] PANFILI M, GIUSEPPI A, FIASCHETTI A, et al. A game-theoretical approach to cyber-security of critical infrastructures based on multi-agent reinforcement learning[C]//Proceedings of 26th Mediterranean Conference on Control and Automation. Piscataway: IEEE Press, 2018: 460-465.

[31] ASVIJA B, ESWARI R, BIJOY M B. Bayesian attack graphs for platform virtualized infrastructures in clouds[J]. Journal of Information Security and Applications, 2020, 51: 102455.

[32] 杨宏宇, 袁海航, 张良. 基于攻击图的主机安全评估方法[J]. 通信学报, 2022, 43(2): 89-99.
YANG H Y, YUAN H H, ZHANG L. Host security assessment method based on attack graph[J]. Journal on Communications, 2022, 43(2): 89-99.

[33] SANDOVAL J E, HASSELL S P. Measurement, identification and calculation of cyber defense metrics[C]//Proceedings of 2010 Military Communications Conference. Piscataway: IEEE Press, 2011: 2174-2179.

[34] ZHENG L, PERL Y, ELHANAN G, et al. Summarizing an ontology: a big knowledge coverage approach[J]. Studies in Health Technology and Informatics, 2017, 245: 978-982.

[作者简介]

刘盈泽（1994− ），女，河南郑州人，信息工程大学博士生，主要研究方向为网络安全防御。

郭渊博（1975− ），男，陕西周至人，博士，信息工程大学教授、博士生导师，主要研究方向为网络防御、数据挖掘、机器学习和人工智能安全等。

方晨（1993− ），男，安徽宿松人，信息工程大学讲师，主要研究方向为机器学习、隐私安全。

李勇飞（1998− ），男，河南开封人，信息工程大学硕士生，主要研究方向为威胁情报实体抽取及关系抽取。

陈庆礼（1998− ），男，河南新乡人，信息工程大学硕士生，主要研究方向为人工智能安全。