基于多启发式信息融合的攻击路径发现算法研究

胡泰然[1], 臧艺超[1], 曹蓉蓉[2], 王清贤[1], 王晓凡[1]

[1]数学工程与先进计算国家重点实验室 郑州 中国 450001
[2]国防大学政治学院 上海 中国 200433

摘要 攻击路径发现对于提高信息系统安全具有重要意义, 传统攻击路径发现技术存在考虑因素有限以及可扩展性不高的问题, 导致其在网络攻击复杂化和网络规模扩大化的趋势下应用价值有限。针对该问题, 本文提出一种基于多启发式信息融合的攻击路径发现算法, 该算法结合攻击路径发现背景知识, 将漏洞威胁程度, 漏洞成功率以及主机资产作为启发式函数计算依据引导攻击路径搜索, 达到减少搜索范围、提高路径可用性的目的; 并且基于 SMHA*(Share Multi-Heuristic A*, SMHA*)框架实现多种启发式信息融合, 共同引导攻击路径搜索。通过与现有规划算法进行对比实验, 验证了本算法能够更加灵活而全面地考虑攻击路径发现中的现实因素, 且规划效率也能够满足实际需求, 能够有效提高规划结果的可行性以及应用价值。

关键词 攻击路径发现; 启发式搜索; 信息融合; Shared Multi-Heuristic A*
中图法分类号 TP.393 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2021.05.13

Research on Attack Path Discovery Algorithm Based on Multi-Heuristic Information Fusion

HU Tairan[1], ZANG Yichao[1], CAO Rongrong[2], WANG Qingxian[1], WANG Xiaofan[1]

[1] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
[2] Political College of National Defense University, Shanghai 200433, China

Abstract Research on attack path discovery is of great significance for improving information system security, but traditional attack path discovery technology has few concerning factors and low scalability, which leads to its limited application value under the trend of network attack complexity and network scale expansion. To tackle this problem, this paper proposes an attack path discovery algorithm based on multi-heuristic information fusion. This algorithm combines the domain knowledge of cybersecurity, taking in the vulnerability threat degree, vulnerability success rate, and host assets level as heuristic functions, to reduce the problem complexity and improve the path availability. Moreover, with the SMHA* (Share Multi-Heuristic A *, SMHA*) framework, a variety of heuristic information is combined to jointly guide the attack path search. Through the comparison with the existing planning algorithms, it is verified that this algorithm can consider more realistic factors in attack path discovery more flexibly and comprehensively, and the planning efficiency can also meet the actual requirements, making attack path discovery more feasible and of great application value.

Key words attack path discovery; heuristic search; information fusion; Shared Multi-Heuristic A*

1 引言

随着网络安全形势日益严峻, 提高信息系统安全性刻不容缓。现有的安全手段大都从防御者角度进行被动式进行脆弱性发现, 不能很好地刻画攻击者意图以及潜在攻击路径。从攻击者的角度进行网络安全分析可以更好的揣摩攻击者心理, 从而制定出更有针对性的防御策略。因此, 攻击路径发现是网络安全领域的重要研究内容之一, 其在自动化渗透测试、安全分析、网络防御等方面都有重要的应用价值[1]。传统的攻击路径发现主要采取首先构建攻击图, 再利用深度优先算法搜索攻击路径的思路[2]。然而, 在面对复杂网络场景时,遍历搜索空间进行搜索会使得算法效率难以满足实际需求。

智能规划是人工智能的重要研究领域之一, 通过对周围环境的分析, 根据预定目标和可用动作,

通讯作者: 臧艺超, 博士生, Email: aipteamzhouty@aliyun.com
收稿日期: 2020-06-23; 修改日期: 2020-09-21; 定稿日期: 2021-03-05

在一定的资源限制和约束条件下进行推理, 从而得到动作序列。将智能规划应用于攻击路径发现成为新的研究方向[3-4]。但是现有的基于智能规划的攻击路径发现研究中, 大多致力于通过提高攻击路径发现模型的实际程度来增加攻击路径发现的可行性, 如 POMDP 模型。但是随着模型不断完善, 算法复杂度也逐渐提高, 求解效率就难以保证。从 90 年代后期开始, 基于启发式搜索的规划方法由于其规划的高效重新成为智能规划领域的热点[5]。启发式搜索利用启发式信息来引导搜索, 能够有效提高搜索的效率, 这给攻击路径发现提供了一个新的思路。

将领域知识融入到启发式函数, 利用启发信息引导搜索, 不仅可以提高规划效率, 而且能够提高规划结果的可行性。为了更充分地发挥启发式函数的作用, 本文提出了基于多启发式融合的攻击路径发现算法。通过引入 SMHA*(Share Multi-Heuristic A*, SMHA*)框架, 将漏洞威胁程度, 漏洞成功率以及主机资产作为启发式信息共同引导攻击路径搜索, 在保证一定的算法效率的基础上, 使规划结果更加符合现实应用需求。

本文结构如下: 第二章主要介绍现有智能规划在网络安全方面以及攻击路径发现方面的应用; 第三章首先提出了针对攻击路径发现领域的启发式函数设计, 然后描述了基于 SMHA*框架的多启发信息融合的攻击路径发现算法; 第四章中通过与现有经典算法对比, 验证本文提出的算法的可行性; 第五章对全文内容进行总结。

2 研究现状

2005 年, Jajodia 等人[6]提出独立地考虑单个漏洞利用效果是不全面的, 应该从整体网络的层面上分析漏洞的组合威胁, 并明确地提出了攻击路径这一概念。并且对网络安全中的攻击, 资产, 动作和目标建立概念模型。同年, Boddy 首次将智能规划用于网络安全。作者将网络脆弱性分析映射为规划问题, 并用 PDDL 语言对其进行描述。文章基于攻击者视角建立了行为对抗建模系统(Behavior Adversary Modeling System, BAMS)用于预测攻击者的行动方案(Course of Action, COA)并验证了该系统可行性[7]。早期的研究中提出的基本概念和模型为后续研究奠定了良好的基础, 并且这些研究也从理论上验证了利用智能规划进行攻击路径发现的可行性[8]。

在前人的研究基础上, 2009 年, Sarraute 正式地将智能规划算法用于渗透测试中的攻击路径发现。他将渗透测试框架映射为经典规划问题, 并提出了漏洞利用代价, 采用 Metric-FF 和 SGP 算法对规划结果进行求解[9]。同时, 澳大利亚国防科技技术部门将经典规划算法用于自动化网络红队(Cyber red teaming, CRT)推演中, 利用已有算法实现自动化推演, 并针对各种算法的在该领域的性能进行比较[10]。Core Impact 公司也很快开始在其产品 Metasploit 中应用攻击路径发现来提供渗透测试的自动化程度[11]。

但是经典规划问题基于环境是静态, 确定的假设, 这和实际攻击路径发现过程不完全相符, 这也使得基于经典模型的攻击路径发现结果在实际应用中存在欠缺。因此, 后续研究朝着提高攻击路径发现结果的适用性和可行性方向进行。考虑到漏洞利用动作执行成功存在概率性, 2011 年, Sarraute 提出了基于概率规划模型进行攻击路径生成, 该方法提出了 CHOOSE 和 COMBINE 两个原语, 将漏洞利用成功率作为攻击路径搜索的依据之一。该方法考虑了渗透环境中的不确定性, 并且通过实验验证了其有效性[12]。进一步考虑环境的不确定性, Sarraute 等人用部分可观察马尔可夫决策(Partially Observable Markov Decision Process, POMDP)过程对渗透测试建模。该模型对规划问题进行了精确的描述, 将扫描动作看作攻击动作的组成部分一并进行规划。但该算法在求解规模上限制较大, 在只考虑最少的漏洞数量(每个主机上只有一个漏洞)的实验设置中, 当主机数量达到 8 时, 算法就会失效[13-14]。

以上研究主要致力于提高规划模型的对现实攻防场景的逼真程度从而提高规划结果的实际可用性。但随着模型的复杂度提高, 计算效率也逐渐降低, 也在一定程度上削弱了其实际应用价值[15-16]。如何能够在提高规划结果的可用性的同时保证一定的求解效率成为了攻击路径发现的新的研究目标。

要提高攻击路径发现结果的实际性和可行性并不一定只有提高模型的仿真程度。不同于以往提高模型精确程度的思路, 将领域知识融入到启发式并引导搜索也可以用于提高规划结果的可行性。但是启发式规划的效率和效果很大程度上依赖于启发函数的好坏。设计一个好的启发式函数往往能够给问题求解带来巨大提升, 然而, 目前并没有适用于攻击路径发现的完美启发式函数。现有的攻击路径发现算法中的并没有将启发式函数设计作为重点, 只是简单将攻击代价作为启发式进行规划[17], 使得规划时考虑的因素不全面, 不足以完全反映攻击路径发现的特点和需求。或者是将操作成本, 攻击成本, 攻击收益等多个指标通过加权求和的方法构造出一个新的指标[18]。权值分配的合理程度直接影响了新

指标的可靠程度, 但是这一方法在计算时权值并没有给出十分详细的说明。相比只利用单一启发式信息进行搜索, 多启发式信息融合往往能够相互补充, 为搜索提供更好的引导作用。同时, 相比于利用加权求和等方法将多指标进行糅合, 多启发式信息融合的方式更加灵活, 也能够避免权值确定不当造成的问题。

为了避免模型的复杂化带来的计算问题, 同时避免单一启发式搜索存在的信息考虑不全面的问题, 本文提出了基于多启发式信息融合的攻击路径发现算法。该算法通过将复杂的网络安全领域知识转化为多个启发式函数, 灵活地融合多维领域知识引导攻击路径搜索, 提高攻击路径发现结果的适用性, 更好地满足实际应用需求。

3 启发式信息融合的攻击路径发现算法

3.1 攻击路径发现启发式设计

要提高攻击路径发现的可靠性, 重点在于尽可能多的将网络安全领域知识融入到规划过程中, 从而实现在规划中考虑各种实际因素。不同启发式函数都对信息有所侧重, 如果只采用单独的启发式往往不能够完整的体现攻击路径发现中的众多影响因素。而多个启发式同时引导搜索, 则能够融合各个启发式的信息, 提高规划结果的可用性。

考虑到在实际的攻击过程中往往会存在以下选择: a) 若每个主机上存在多个漏洞, 如何选择既能提高攻击效果, 又能保证攻击成功的漏洞进行利用; b) 若子网内的存在众多主机, 如何选择最有利于攻击者的主机作为目标。因此, 本文根据攻击路径发现的实际需求, 以漏洞威胁程度, 漏洞成功率以及主机资产三个指标分别作为启发式函数进行搜索引导。

(1) 漏洞威胁程度

漏洞威胁程度主要反映漏洞利用的价值, 威胁程度大的漏洞在往往能够在攻击过程中发挥更大的破坏力, 其利用难度也相对更小, 往往是攻击者的首选。通常, 会使用通用漏洞评分系统(Common Vulnerability Scoring System, CVSS)作为漏洞威胁程度的评价指标。CVSS 是一个受到广泛认可的漏洞评估标准, 可以用来衡量一个漏洞的严重程度以及威胁程度, 最早于 2007 年发布。CVSS 的度量可以分为三个组: 基本组, 时间组和环境组, 如图 1 所示。基本组描述的是漏洞本身固有的属性, 不随时间和所处环境改变而发生变化。基本组主要涉及攻击途径、攻击复杂度、攻击过程认证、 机密性影响、完整性影响、可用性影响。

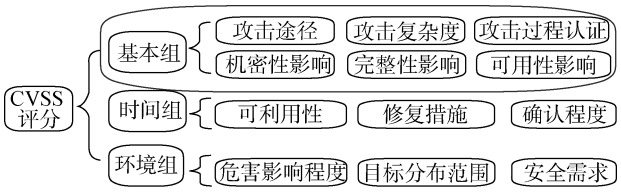

图 1 CVSS 2.0 指标体系

Figure 1 CVSS 2.0 Metric Groups

CVSS 的基本组评分的取值范围为 0~10, 为了方便计算, 本文采用 CVSS 评分的基本组得分的十倍作为漏洞威胁程度启发式的计算依据。

(2) 漏洞成功率

除了漏洞威胁程度, 实际漏洞利用过程中, 漏洞利用的成功率直接影响着整个攻击是否能够顺利进行。如果漏洞成功率低, 即使漏洞的威胁程度大也往往不会选择。因此, 在攻击规划中将漏洞成功率作为部分规划依据是十分有必要的。Metasploit 中针对每个漏洞的可靠性都有进行等级评定, 共分为 7 个等级, 可靠性从高到低依次为 Excellent, Great, Good, Normal, Average, Low 和 Manual。Metasploit 中的评级是可以量化为相应的成功率以用于启发式计算, 如表 1 所示。

表 1 漏洞等级利用成功率

Table 1 Success rate of different vulnerability rank

等级	描述	漏洞成功率(%)
Excellent	漏洞不会使得服务器崩溃, 不会导致内存错误	90
Great	漏洞具有默认的目标或者可以自动检测的目标	80
Good	漏洞可以大部分常见的软件版本设置	70
Normal	漏洞是可靠的, 但是依赖于特定版本	60
Average	不是很可靠, 利用存在一定难度	50
Low	对于通用平台, 成功率低于 50%	30
Manual	漏洞不稳定或者是难易利用	10

(3) 主机资产

在攻击路径选择过程中, 不仅会考虑到漏洞的选择, 同时也会选择合适的主机作为攻击对象。不同主机在一个网络中扮演的角色不同, 其信息资产的重要性程度也有所差异。在攻击过程中, 攻击者往往会考虑渗透具有更高价值的主机, 以期获得更好的攻击效益。主机资产值往往与所处的网络位置, 运行的服务, 存储的资源等有关。主机资产的重要性程度往往和整个网络的资产情况相关[19]。为了简化对主

机资产价值进行度量, 对主机资产重要性程度以等级形式进行表示。参考现有研究, 本文将主机的资产等级分为 5 级, 表示相对的资产重要性程度。主机资产等级与典型主机类型如表 2 所示。主机资产价值越高, 其攻击价值也越高。

表 2 主机资产等级及其典型主机类型

Table 2 Host asset ranks and typical host types

主机资产等级	典型主机类型
高	DNS 服务器、骨干网路由器、数据库服务器;
较高	邮件服务器、FTP 服务器、存储关键信息的主机等;
中	Web 服务器, 防火墙, 关键位置主机;
较低	一般主机等;
低	临时接入的主机等

根据各个主机配置信息以及表 2 可以大致确认其资产等级。以此对各个主机的资产按照其相对价值进行排序和比较, 并且主机的资产价值排序作为启发式函数的计算依据。

由于多个启发式共同引导算法进行, 启发式值会直接影响搜索的实际运行方向。然而, 不同的启发式计算依据不同, 其量纲和数值大小往往不尽相同。如果各启发式的量纲和数据级差距过大会导致算法效果大打折扣。因此, 为了提高算法的可靠性, 需要对各个启发式值进行标准化。取漏洞代价的最大最小值为界, 采用离差标准化方法。离差标准化将数据进行线性变化, 将数据映射到一定的范围内。为了使得三个启发式的取值范围相近, 将漏洞威胁程度值的最大最小值作为标准化上下界, 将漏洞成功率和主机资产值依次代入公式(1)进行数据标准化。

$$y_i = \frac{x_i - \min(x_i)}{\max(x_i) - \min(x_i)}(threat_{\max} - threat_{\min}) \quad (1)$$

其中, x_i 表示标准化前的取值, y_i 表示标准化后的取值, $threat_{\max}, threat_{\min}$ 分别表示漏洞威胁程度的最大值和最小值。

3.2 基于多启发式信息融合的攻击路径发现

本文基于 SMHA*框架, 将漏洞威胁程度, 漏洞成功率, 以及主机资产值三种信息作为启发式计算依据进行攻击路径发现, 提高攻击路径的可用性。

定义 1: 一致性启发函数(Consistent heuristic)是指启发式函数满足以下条件:

① 对于每个节点 s 以及其子节点 s', 有 $h(s) \leqslant h(s') + c(s,s')$;

② 对于目标节点 s_{goal} 有 $h(s_{goal}) = 0$。

一致启发函数保证搜索能够找到最优解。

SMHA*框架基于 A*算法, 同时采用多个启发式引导搜索[20]。如图 2 所示, 为了保证求解质量, SMHA*框架利用一个满足一致性的启发式函数保证求解的次优性, 称为锚启发式搜索(Anchor heuristic search); 同时, SMHA*以轮询的方式吸收其他一般启发式的信息。并且, SMHA*中不同搜索之间当前计算出来的路径信息是共享的。这些特点不仅能够有效组合不同启发式函数的引导能力, 同时也能够提高规划效率。SMHA*框架能够使得各个启发式信息互补, 应用在攻击路径发现问题中, 既可以避免重新设计启发式函数的麻烦, 也能综合考虑攻击路径发现中需要考虑的多种现实因素。

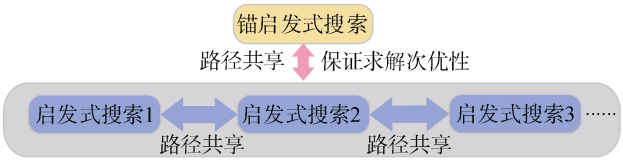

图 2 SMHA*算法框架

Figure 2 SMHA* algorithm frame

设 SMHA*中使用的启发式函数分别为 $h_i, i = 0,1,2,\cdots$。其中, 满足一致性的锚启发式记为 h_0; 并且, 对于每个启发式都维护一个优先队列 $OPEN_i, i = 0,1,2,\cdots$。此外, 在 SMHA*中维护两个 $CLOSE$ 列表, $CLOSE_0$ 记录在锚搜索中扩展过的节点, 而 $CLOSE_{inad}$ 记录在所有一般搜索中被扩展的节点。SMHA*的不同搜索队列之间存在路径共享, 如果在某个搜索中发现了一条更优路径, 则所有优先队列中都会更新信息。因此, 每个节点的 $g(s)$ 和 $bp(s)$ 值都是共享的。这也保证了每个节点最多被扩展两次。SMHA*中, 有两个重要的权值 w_1, w_2。其中, w_1 用于计算优先队列中的键值; 而 w_2 用于控制当前进行的搜索是一般搜索还是锚启发式搜索。在攻击路径发现中, 取漏洞威胁值为作为依据进行锚启发式搜索, 并且采用最大值启发式计算方法, 将漏洞成功率和主机资产值作为 h_1, h_2 计算依据。

定义 2: 攻击路径发现问题可以表示为 $\sum =< S, A, E >$。其中,

- $S = \{s_{attack}, s_1, \cdots, s_{target}\}$ 表示所有主机集合, 其中, s_{attack} 表示攻击者主机, s_{target} 表示攻击目标主机;
- $A = \{a_1, a_2, \cdots\}$ 为所有漏洞利用动作集合;
- $E = \{e_1, e_2, \cdots\}$ 表示主机之间的连通关系。

进一步, 单个主机 s 可以表示为 $s =< name,$

$asset, g, bp>$，分别表示主机的名称，主机资产情况以及主机当前路径代价值及其对应的前向节点；单个漏洞利用动作可以表示为 $a=<name, risk, successrate>$，分别表示漏洞利用动作的名称，漏洞威胁程度以及漏洞成功率。单个连通关系可以表示为 $e=<s, s', c>$，代表从主机 s 可以访问 s'，并且当从主机 s 发动攻击 s' 时的代价为 c。注意，主机之间的连通关系具有方向性。同时，定义 $Succ(s)$ 为主机 s 所有能够访问的主机集合，有 $Succ(s)=\{s' \in S \mid c(s,s') \neq \infty\}$。$g^*(s)$ 表示集合从攻击者主机 s_{attack} 到主机 s 的最佳路径代价，$g(s)$ 表示集合从攻击者主机 s_{attack} 到主机 s 的当前最佳路径代价。

本文提出的基于多启发式攻击路径发现算法同时采用漏洞威胁值，漏洞成功率以及主机资产值三种启发式函数进行规划引导，分别记为 h_0, h_1, h_2。算法代码如图 3。算法首先进行初始化操作(行 14~16)，设置目标主机的 g 值为无穷大，初始攻击主机 g 值为 0，将初始攻击主机和目标主机的 $bp()$ 值设为空，同时将初始主机节点插入到各优先队列中；接着，当满足一般优先队列中的最小值小于 w_2 倍锚搜索队列最小值 $OPEN_i.Minkey() \leqslant w_2 * OPEN_0.Minkey()$，$i$=1,2 时(行 24~28)，算法以轮询方式对每个其他搜索队列 $OPEN_i, i=1,2$ 以最佳优先方式进行扩展；反之，则扩展 $OPEN_0$ (行 30~33)。$Key()$ 函数(行 1~2)用于计算扩展节点在优先队列中的键值。扩展节点时，首先需要将当前节点从所有优先队列中删除来保证该节点不会被再次扩展(行 4)。然后考虑当前主机的所有后继主机节点 $s' \in Succ(s)$；如果 s' 没有被扩展过，那么 $Key(s)=g(s)+w_1 * h_i(s)$ 其信息同时在所有优先队列中更新；如果 s' 在某个一般搜索中扩展过但没有在锚搜索中扩展过，那么只将 s' 插入到 $OPEN_0$ 中。如果 s' 已经在锚搜索中扩展过，那么该节点不会被插入到任何优先队列中，也就不会被再次扩展。当 $g(s_{target})$ 在任意 $OPEN_i, i=0,1,2$ 中都具有最小键值时，算法终止。此时，规划结果可以根据 $bp(s)$ 从 s_{target} 追溯到 s_{attack} 得到规划路径。此时，路径代价满足 $cost(s_{attack}, s_{target}) \leqslant w_1 * w_2 * cost^*(s_{attack}, s_{target})$。

4 实验

本实验场景整体网络结构如图 4 所示。

算法 1 基于多启发式信息融合的攻击路径规划算法

```
1:  FUNCTION Key(s, i)
2:      RETURN g(s) + w1 * hi(s)
3:  FUNCTION Expand(s)
4:      Remove s from OPENi ∀i = 0...2
5:      FOR each host s' in Succ(s)
6:          IF s' was never visited THEN
7:              g(s') = ∞; bp(s') = null
8:          IF g(s') > g(s) + c(s, s') THEN
9:              g(s') = g(s) + c(s, s');bp(s') = s
10:             IF host s' has not been expanded in the anchor search THEN
11:                 insert/update host s'in OPEN0 with Key(s', 0)
12:                 IF s' hasn't been expanded in OPENi, i = 1, 2 THEN
13:                     FOR i = 1, 2
14:                         IF Key(s', i) ⩽ w2 * OPEN0.Minkey() THEN
15:                             insert/update host s'in OPENi with Key(s', i)
16: FUNCTION Main()
17:     g(starget) = ∞;bp(sattack) = bp(starget) = null;
18:     g(sattack) = 0
19:     FOR i = 0, 1, 2
20:         OPENi = ∅
21:         insert sattack into OPENi with Key(sattack,i)
22:     WHILE OPEN0 is not empty
23:         FOR i = 1, 2
24:             IF OPENi.Minkey() ⩽ w2 * OPEN0.Minkey() THEN
25:                 IF g(starget) ⩽ OPENi.Minkey() THEN
26:                     terminate and return path point by bp(starget)
27:                 s = OPENi.Top()
28:                 Expand(s)
29:             ELSE
30:                 IF g(starget) ⩽ OPEN0.Minkey() THEN
31:                     terminate and return path point by bp(starget)
32:                 s = OPEN0.Top()
33:                 Expand(s)
```

图 3　基于多启发式信息融合的攻击路径发现算法

Figure 3　Attack Path Discovery Algorithm Based on Multi-Heuristic Information Fusion

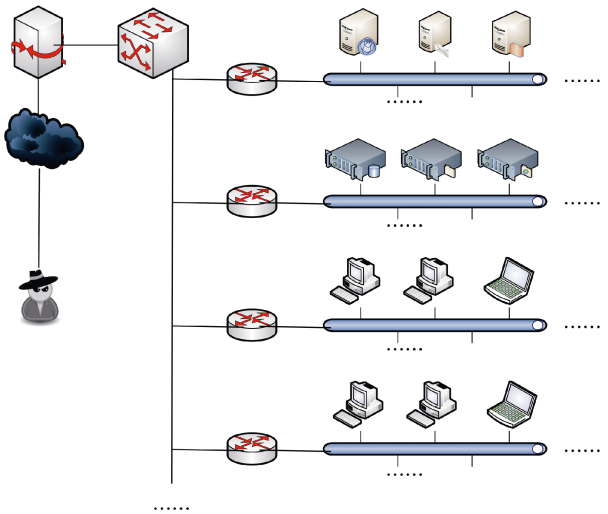

图 4　网络结构示意

Figure 4　Network structure schematic

攻击者从通过互联网连接到内部网络；整个内网分为若干个子网，相邻子网之间可以相互访问；每个子网中包含若干个主机。具体的，在每个主机上存在若干个可利用漏洞。本文选取了五个具有不同

子网数, 子网内主机数以及主机漏洞数的场景进行实验。如表 3 所示, 从场景 A 到场景 E, 网络结构复杂程度递增。子网数量的增加意味着攻击者需要在内网中攻击的跳板主机数量增加, 攻击路径长度增加。子网内主机数量以及各主机漏洞数量的增加意味着攻击者在进行攻击时可选动作增加, 在一定程度上增加了攻击者的选择难度。各个场景的主机信息以及漏洞情况均随机指定, 场景之间漏洞情况不具有相关性。实验中所用到的漏洞信息均来源于公开漏洞库。采用规划领域定义语言(Planning domain definition language, PDDL)[21]对所有实验场景进行描述。

表 3 实验场景信息

Table 3 Information of scenes in experiment

场景 ID	子网数	各子网内主机数	各主机漏洞数
场景 A	4	2	2
场景 B	4	4	2
场景 C	6	4	2
场景 D	6	6	4
场景 E	10	10	6

在各个实验场景中, 分别采用本文提出的多启发式融合攻击路径发现算法与 WA*, Metric-FF 以及基于 POMDP 模型的算法进行路径规划。与 SMHA*框架类似, WA*算法是 A*算法的扩展, 通过增大启发式计算因子来提高搜索效率; 同样, WA*算法并不保证最优性; Metric-FF 采用忽略可用动作的删除效果的启发式来提高规划效率, 是经典规划问题域中最流行和成功的规划算法之一; POMDP 是环境状态部分可知动态不确定环境下序贯决策的理想模型, 实验中采用 POMDP-Solve 求解器进行实验。

对于 SMHA*取 w_1 为 1.5, w_2 为 2, WA*取 $w = w_1 * w_2 = 3$。启发式计算策略采用最大值启发式。主要比较的指标为攻击路径威胁程度, 攻击路径成功率, 平均主机资产排名以及算法运行时间。攻击路径威胁程度为路径中各个漏洞的威胁程度之和, 路径威胁程度越大越好(计算时采用最小化 100 减去漏洞威胁值, 后续结果已转换为正常值); 攻击路径成功率为各漏洞成功率乘积, 表示整个路径能够执行成功的概率, 取值越大越好, 但随着攻击路径长度增加, 路径成功率呈现减小趋势; 而平均主机资产排名为各个主机资产值排名的平均值(除去目标节点), 排名平均值越小表示路径中选择的主机重要程度越高; 创建节点数为规划过程中扩展节点及其子节点数量。实验结果见图 5 至图 9。

在场景 A 中, 本文提出的算法的在路径威胁程度上和 WA*相同且高于 Metric-FF 以及 POMDP, 而且本文算法的漏洞成功率以及主机资产排名也表现最佳。虽然在运行时间上比 Metric-FF 以及 WA*长, 但是明显好于 POMDP。

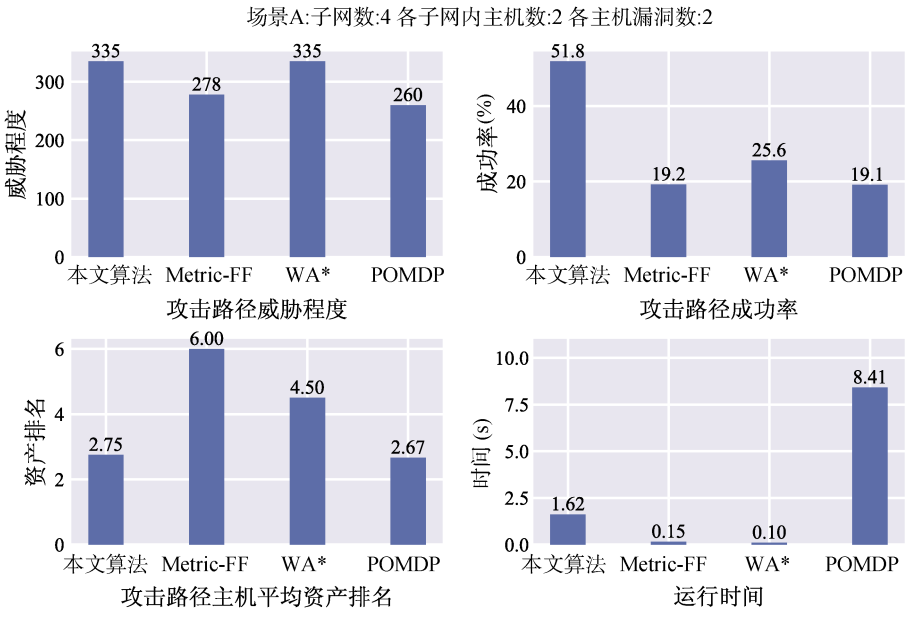

图 5 场景 A 实验结果

Figure 5 Results in Scene A

场景 B 中, 本文算法, Metric-FF, WA*三个算法计算结果十分相近, 这与具体场景配置有关, 说明当场景中最佳攻击路径选择较为单一时, 本文提出的算法的计算结果可能与传统的 Metric-FF 和 WA*相同。并且从场景 B 的实验数据来看, POMDP 的各项指标均较差, 并且计算时间明显高于其他算法, 并且与场景 A 相比, 时间大大增加。

从场景 C 的实验结果可以看出, 此时, 本文算法的路径威胁程度稍差于 WA*, 但优于其他两种算法; 主机资产排名和 Metric-FF 相同, 但路径成功率更优; 运行时间上, 虽然比 Metric-FF 以及 WA*较差, 但运行时间也较短。

场景 D 中的子网数量, 主机数量以及漏洞数量都有了明显增加, 此时 POMDP 已经无法求解。在路径规划威胁程度上来说, 本文提出的算法较 Metric-FF 和 WA*来说较弱, 但是路径成功率以及攻击主机资产价值明显好于这两种算法。随着攻击路径长度增加, 路径成功率对于攻击是否成功具有十分重要的意义, 因此, 本文算法得到的攻击路径更具有实际意义。

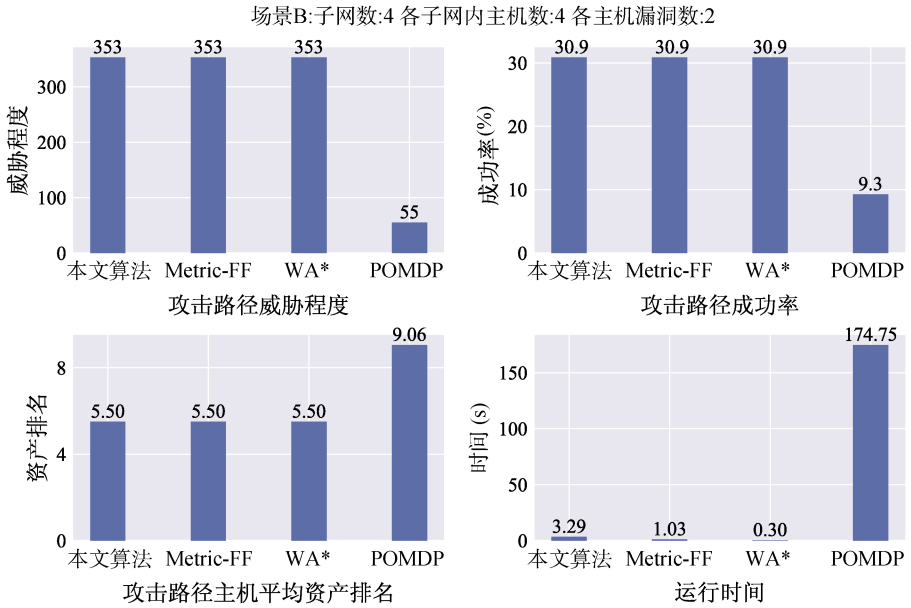

图 6　场景 B 实验结果

Figure 6　Results in Scene B

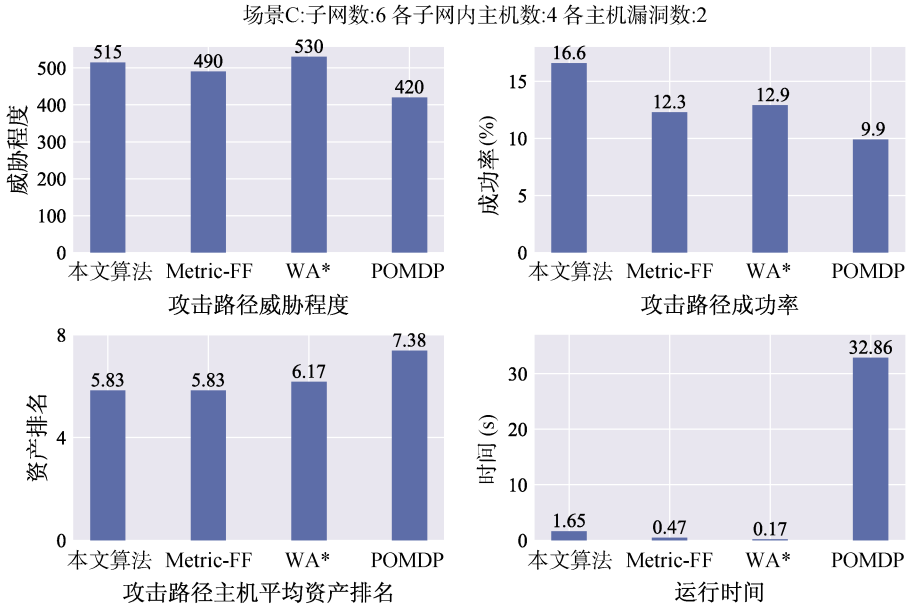

图 7　场景 C 实验结果

Figure 7　Results in Scene C

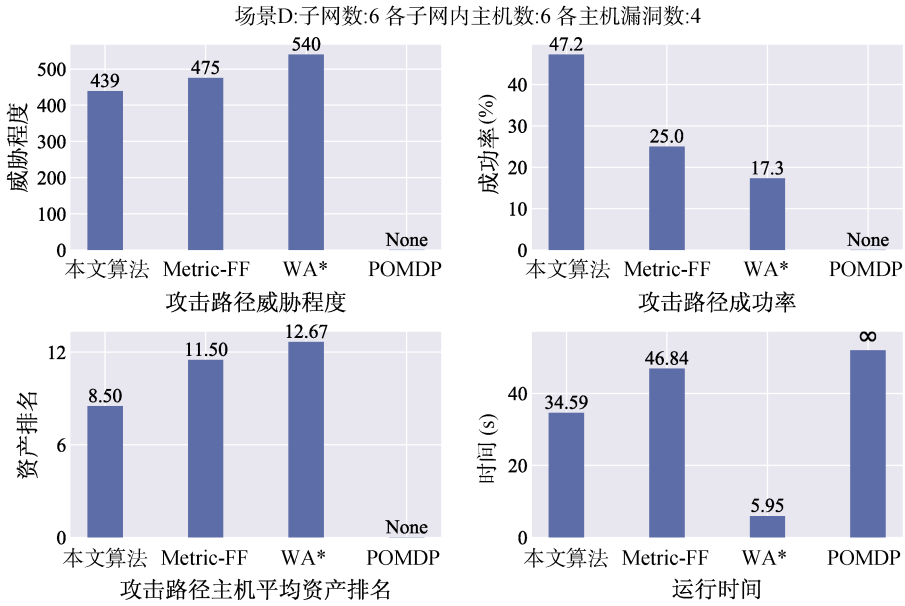

图 8　场景 D 实验结果

Figure 8　Results in Scene D

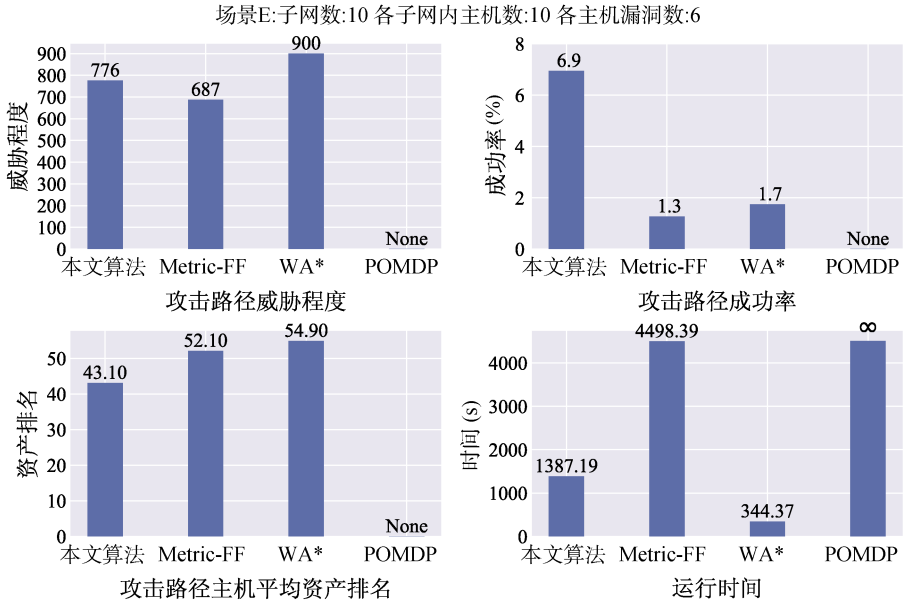

图 9　场景 E 实验结果

Figure 9　Results in Scene E

在场景 E 中, 网络规模以及复杂度进一步增加, 同理, POMDP 算法求解失效。此时, 本文提出的算法在路径威胁程度上介于 Metric-FF 算法以及 WA*中间; 但明显可以发现此时, 本文算法的路径成功率和攻击主机资产价值排名明显好于其他算法。在运算时间上, 此时, Metric-FF 算法的运算时间已经明显大于本文算法。

从实验结果来看, 本文提出的基于多启发式信息融合的攻击路径规划算法具有以下特点:

(1) 在路径威胁程度方面, 本文提出的算法计算结果略弱于 WA*, 但与 Metric-FF 相近;

(2) 在路径成功率以及攻击主机平均资产价值排名两个方面, 本文提出的算法在多数场景中均优于其他算法, 尤其随着攻击路径增加, 本文算法的计算结果优势更加突出;

(3) 在运算时间方面, 虽然本文提出的算法在场景 A 到场景 D 中比 WA*和 Metric-FF 算法大, 但是运算时间绝对值也相对合理; 并且随着网络复杂程度增加, Metric-FF 的运算时间增加速度明显大于本文算法。

综上所述, 传统的规划算法如 Metric-FF, WA*算法在进行攻击路径发现时考虑的因素较为有限, 并且当网络复杂程度增加时, 这些算法在运行时间的增加速度, 路径成功率以及主机选择上均存在一定问题。而 POMDP 算法的明显问题就在于其运算时间, 当网络场景稍微增加就出现无法求解的情况。

相比之下, 本文提出的基于多启发式信息融合的攻击路径发现算法能够更好的均衡攻击路径发现中多个因素的信息, 使得所发现的攻击路径更加符合攻击者的实际需求。特别随着网络复杂程度的增加, 本文提出的攻击路径发现算法的优越性体现的更加明显。

5 小结

作为从攻击者角度对网络分析的一种手段, 攻击路径发现在网络安全领域中具有重要的研究价值。现有研究大多通过不断完善模型对现实网络攻防的逼真程度来提高规划的适应性与可行性, 但这也使得模型复杂度大大增加, 计算效率难以满足实际使用需求。不同于以往的研究方向, 本文以启发式函数作为切入点, 将多维攻防领域知识作为启发式计算依据, 共同引导攻击路径搜索。

本文提出的基于多启发式信息融合的攻击路径发现算法。该算法基于攻击路径发现的背景需求, 将漏洞威胁程度, 漏洞成功率以及主机资产情况作为启发式计算依据, 并且基于 SMHA*框架, 融合多种启发式信息引导搜索, 提高攻击路径发现的可行性, 同时保证一定的计算效率。最后通过实验验证了该算法相比于常规算法确实能够在规划时更全面的考虑多方面因素, 并且计算效率能够满足实际需求。

本文提出基于多启发式信息融合的攻击路径发现算法不仅能够避免建立复杂的模型, 还能合理结合领域知识提高攻击路径发现结果的可行性, 并且算法的计算效率控制在合理范围内, 能够很好的促进攻击路径发现的现实应用, 进一步发挥攻击路径发现在信息安全领域中的作用。

参考文献

[1] Veksler V D, Buchler N, Hoffman B E, et al. Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users[J]. *Frontiers in Psychology*, 2018, 9: 691.

[2] Ye Z W, Guo Y B, Wang C D, et al. Survey on Application of Attack Graph Technology[J]. *Journal on Communications*, 2017, 38(11): 121-132.
(叶子维, 郭渊博, 王宸东, 等. 攻击图技术应用研究综述[J]. *通信学报,* 2017, 38(11): 121-132.)

[3] Geluvaraj B, Satwik P M, Ashok Kumar T A. The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace[D]. International Conference on Computer Networks and Communication Technologies, Springer Singapore, 2019, 15.

[4] Bozic J, Wotawa F. Planning the Attack! Or How to use AI in Security Testing?. Technical report. 2017, 50.

[5] Ghallab M, Nau D, Traverso P. Heuristics in Planning[M]. Automated Planning. Amsterdam: Elsevier, 2004: 199-215.

[6] Jajodia S, Noel S, O'Berry B. Topological Analysis of Network Attack Vulnerability[J]. *Managing Cyber Threats*, 2005: 247–266.

[7] Boddy M, Gohde J, Haigh T, et al. Course of action generation for cyber security using classical planning[J]. *The 15th International Conference on Automated Planning and Scheduling*, 2005: 12–21.

[8] Gutesman E, Waissbein A. The Impact of Predicting Attacker Tools in Security Risk Assessments[C]. *The Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '10*, 2010: 1-4.

[9] Sarraute C. New Algorithms for Attack Planning[EB/OL]. 2009

[10] Yuen J. Automated Cyber Red Teaming. Technical report. DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) CYBER AND ELECTRONIC WARFARE, 2015: 41.

[11] Futoransky A, Notarfrancesco L, Richarte G, et al. Building Computer Network Attacks. Technical report. 2003.

[12] Sarraute C, Richarte G, Lucángeli Obes J. An Algorithm to Find Optimal Attack Paths in Nondeterministic Scenarios[C]. *The 4th ACM workshop on Security and artificial intelligence - AISec '11, 2011*: 71–79.

[13] Sarraute C, Buffet O, Hoffmann J. Penetration Testing == POMDP Solving[EB/OL]. 2013: arXiv: 1306.4714[cs.AI]. https: //arxiv.org/abs/1306.4714.

[14] Sarraute C, Buffet O, Hoffmann J. POMDPs make better hackers: Accounting for uncertainty in penetration testing[C]. *The National Conference on Artificial Intelligence*, 2012.

[15] Geffner H, Bonet B. A Concise Introduction to Models and Methods for Automated Planning[J]. *A Concise Introduction to Models and Methods for Automated Planning*, 2013.

[16] Felderer M, Büchler M, Johns M, et al. Security Testing: A Survey[J]. *Advances in Computers*, 2016, 101: 1-51.

[17] Obes J L, Sarraute C, Richarte G. Attack Planning in the real world[C]. *AAAI Workshop on Intelligent Security* , 2010.

[18] Jiang W. *Research on Active Defense Based on Attack-Defense Game Model*[D]. Harbin: Harbin Institute of Technology, 2010.

(姜伟. 基于攻防博弈模型的主动防御关键技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2010.)

[19] Northcutt S. Network Intrusion Detection: An Analyst's Hand-Book[J]. *EDPACS*, 2000, 27(7): 1-2.

[20] Aine S, Swaminathan S, Narayanan V, et al. Multi-Heuristic A[J]. *The International Journal of Robotics Research*, 2016, 35(1/2/3): 224-243.

[21] McDermott D, Ghallab M, Howe A, et al. PDDL - The Planning Domain Definition Language[C]. *The AIPS-98 Planning Competition Committee*, 1998.

胡泰然 于 2014 年在信息工程大学网络工程专业获得学士学位。现在信息工程大学网络空间安全专业攻读硕士学位。研究领域为网络空间安全。Email: vanessa_htr@163.com

臧艺超 于 2017 年在信息工程大学软件工程专业获得硕士学位, 现在信息工程大学计算机科学与技术专业攻读博士学位。研究领域为网络安全, 强化学习。 Email: zangyeechao@sina.com

曹蓉蓉 于 1992 年在国防科技大学计算机软件专业获得硕士学位, 现任国防大学政治学院副教授, 研究领域为信息系统与信息安全。研究兴趣包括: 信息安全、政治工作信息化。Email: crr1001@163.com

王清贤 于 1982 年在北京大学计算机科学技术专业获得硕士学位; 现任信息工程大学教授, 博士生导师。研究领域为网络安全, 移动安全, 入侵检测, 恶意代码分析以及漏洞挖掘。Email: aipteamzhouty@aliyun.com

王晓凡 于 2015 年在信息工程大学网络工程专业获得学士学位。现在信息工程大学软件工程专业攻读硕士学位。研究领域为网络安全。研究兴趣包括自动化渗透测试。Email: 598378941@qq.com