doi:10.11959/j.issn.1000-436x.2017213

攻击图技术应用研究综述

叶子维[1,2]，郭渊博[1,2]，王宸东[1,2]，琚安康[1,2]
（1. 解放军信息工程大学网络空间安全学院，河南 郑州 450001；2. 数学工程与先进计算国家重点实验室，江苏 无锡 214000）

摘 要：攻击图是一种预判攻击者对目标网络发动攻击的方式和过程，指导防御方对网络中的节点采取针对性防御措施，提高网络安全性的技术。首先介绍了攻击图的基本构成，列举了攻击图的几种类型及其各自的优缺点，然后介绍了攻击图技术目前在风险评估和网络加固、入侵检测和告警关联等方面的应用现状以及现有的几种攻击图生成和分析工具，最后指出了攻击图技术面临的挑战和未来可能的研究方向。
关键词：攻击图；安全漏洞；网络加固；告警关联
中图分类号：TP393 **文献标识码**：A

Survey on application of attack graph technology

YE Zi-wei[1,2], GUO Yuan-bo[1,2], WANG Chen-dong[1,2], JU An-kang[1,2]
(1. School of Cyberspace Security, PLA Information Engineering University, Zhengzhou 450001, China;
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi 214000, China)

Abstract: Attack graph technology was a measure to predict the pattern and process used by attacker to compromise the target network, so as to guide defender to take defensive measures and improve network security. The basic component, types of attack graphs and respective advantages and disadvantages of each type were reviewed. The application status of attack graph technology in risk assessment and network hardening, intrusion detection and alarm correlation, and other aspects were introduced. Several kinds of existing attack graph generation and analysis tools were also presented. At last a survey of some challenges and research trends in future research work was provided.
Key words: attack graph, vulnerability, network hardening, alert correlation

1 引言

随着信息技术的高速发展，企业级网络面临的安全问题日益严重，针对国家能源机构、科研单位、基础设施的 APT 攻击日益增多，企业和国家的信息安全面临严峻挑战。根据国家计算机网络应急技术处理协调中心发布的《2016 年中国互联网网络安全报告》[1]，2016 年我国境内有近 1 500 台主机被境外服务器控制；2016 年 8 月针对工业控制行业的“食尸鬼”攻击活动、12 月的乌克兰电网供电故障反映了黑客组织对工业控制系统的攻击能力；“白象”“蔓玲花”等针对我国重要信息系统的 APT 攻击事件，表明部分国家相关机构对我国重要信息系统目标实施网络攻击的事实。由此可见，发现网络中的漏洞，采取高效的安全防护措施，提高网络的整体安全性，对于保证企业、机构乃至国家安全都有着非常重要的意义。

在对企业级网络进行渗透时，攻击者通常需要从网络的某一个边界节点开始，逐步渗透到网络中的其他节点，最终到达目标节点并获取所需的信息。该过程中，攻击者需要多次通过利用漏洞来获取节点上的权限。由于网络的开放性、攻击技术的快速传播以及 0day 漏洞的存在和社会工程学的发展，信息系统面临的安全风险越来越多样化，因此如何在不影响网络正常工作、尽可能节省开销的前提下，预知风险并有效保护目标系统或节点，成为企业级网络在设计和采用安全防护措施时必须要考虑的问题。

收稿日期：2017-02-24；**修回日期**：2017-11-06
基金项目：国家自然科学基金资助项目（No.61602515, No.61501515）
Foundation Item: The National Natural Science Foundation of China (No.61602515, No.61501515)

攻击图技术是一种能满足上述需求的网络安全分析和评估技术。在攻击者对网络进行渗透的过程中，特定的连续攻击行为可称为一条由攻击者节点到目标节点的攻击路径，而攻击图以图形化的方式展示了网络中所有可被防御方发现的攻击路径。对目标网络构建攻击图，一方面可以分析从边界节点到需要进行重点保护节点可能的攻击路径，对路径上的高危节点进行重点防御，达到保护重要节点的目的；另一方面可以在攻击发生时实时分析攻击者的攻击能力和推断攻击者的后续攻击目标，以便采取应对和反制措施。

鉴于攻击图技术在网络安全分析和评估方面的良好前景，学术界和工业界投入了大量人力和经费，用于研究攻击图的自动生成、可视化、动态评估等内容，提出了多种类型的攻击图和基于攻击图的检测技术，将攻击图技术应用到多种场景，并开发了相应工具。目前，攻击图技术在风险评估、网络加固、告警关联等方面已经有了较好的应用，有多种开源和商业工具可用于攻击图的生成和分析。但在自动建立网络模型、简化攻击图、提高分析准确度、结合 0day 漏洞和社会工程学漏洞等方面仍需要进行更深入的研究。

本文从攻击图的基本构成入手，对目前攻击图技术的研究现状和应用场景进行介绍，最后总结并讨论了攻击图技术的未来研究方向。

2 攻击图技术的研究现状

2.1 攻击图的基本构成

20 世纪 90 年代，Philips 和 Swiler[2]首次提出了攻击图的概念，将其应用于网络脆弱性分析。攻击图是一种有向图，展示了攻击者可能发动的攻击顺序和攻击效果，由顶点和有向边两部分构成。根据攻击图类型的不同，顶点可以表示主机、服务、漏洞、权限等网络安全相关要素，也可以表示账户被攻击者破解、权限被攻击者获取等网络安全状态，边用于表示攻击者攻击行为的先后顺序。在理论上攻击图可以构建完整的网络安全模型，反映网络中各个节点的脆弱性并刻画出攻击者攻陷重要节点的所有途径，弥补了以往技术只能根据漏洞数量和威胁等级评估节点和全网的安全性，而不能根据节点在网络中的位置和功能进行评估的缺陷，因此，攻击图技术很快得到了专家学者的广泛认可。

理想情况下，修复网络中所有节点上的所有已知漏洞即可极大程度地保证网络的整体安全性，这种情况下对攻击路径的预测是不必要的。然而在实践中，由于以下几个因素，修复网络中所有已知漏洞是几乎无法实现的。

1) 软硬件环境。软件因素包括部分已公开漏洞不能及时发布官方补丁（如 IE8 远程代码执行漏洞 CVE-2013-1347，WindowsNDProxy 内核提权漏洞 CVE-2013-5065，部分 Linux 系统上存在的 GNU Wget 重定向漏洞 CVE-2016-4971 等），或节点出于兼容性原因不能安装漏洞补丁等；硬件因素包括修复了旧型号硬件中存在的漏洞新型号硬件不能被立即购买和更换等。

2) 时间和经济开销。漏洞修复需要消耗一定的资金、时间和人力，而网络中部分漏洞危害很小但修复开销很大，不值得修复。

3) 节点特性。某些漏洞在修复时需要节点停止提供相应服务或重新启动，而部分重要节点如果停止提供服务会对整个网络的正常工作造成很大的负面影响；或某些节点上的漏洞不需修复，如在某个从不收发邮件的节点上存在的邮件协议漏洞。

攻击图技术可以很好地解决上述问题。对于存在因软硬件环境而无法修复的漏洞节点，或因节点特性暂时不能进行漏洞修复的节点，可以通过修复该节点所在攻击路径上的其他节点漏洞来阻止攻击者攻陷该节点，从而保证目标网络的安全性。根据节点在网络中所处的位置、包含该节点的攻击路径的数目等信息，可以判断如果不修复该节点上的漏洞会带来多大程度的安全风险，从而判断该节点的漏洞是否值得耗费相应的开销去修复。因此，采用攻击图技术对网络进行安全性分析是非常有必要的。

攻击图中代表攻击者攻击行为的最小单位称为原子攻击。根据攻击图的类型和需求不同，原子攻击可以是一次漏洞利用、一次社会工程攻击或是一次非授权登录行为，或仅表示网络状态发生了变化而不反映具体的攻击细节。原子攻击在攻击图中可以以边或顶点表示，如在状态攻击图中原子攻击是以边表示，在属性攻击图中原子攻击就是漏洞顶点。

攻击图的输入信息可包括网络拓扑信息、漏洞信息、漏洞利用开销、漏洞被利用概率、攻击收益、攻陷状态等。如 Wang 等[3]使用的基于马尔可夫模

型的攻击图中将网络资产和基于 NVD 的漏洞扫描结果作为参数，将网络流量、应用软件等作为附加信息；Hong 和 Kim[4]提出的双层攻击图模型中，拓扑层以网络的拓扑结构作为参数，顶点表示可能被攻击的资产，而漏洞层是以资产为根节点，以漏洞为非根节点的有向树；Kotenko 和 Stephashkin[5]根据网络配置信息、安全规则和知识库对攻击行为进行建模，构建攻击图；Wang 等[6]提出的基于安全准则的攻击图中主要考虑进程、权限、漏洞信息和被利用概率、攻击者的攻击行为、漏洞间的因果关系等信息；Ou 等[7]在构建攻击图时考虑了攻击者的攻击开销和收益；Huang 等[8]则直接将全局攻击图作为输入，采用交互式方法减小攻击图的规模。

在攻击图的输入信息中，漏洞被利用概率反映了某个漏洞顶点被攻击者成功利用的可能性。由于每个具体漏洞的利用难度不同，利用多个简单的漏洞所付出的代价可能小于利用一个复杂的漏洞。因此，在评估高危攻击路径，确定要进行重点防御的节点时，需考虑每个具体漏洞的利用代价。通常认为漏洞的被利用概率是始终不变的，且存在于不同的节点上的同一个漏洞被利用概率也是相同的。目前最常用的做法是根据通用漏洞评分系统（CVSS，common vulnerability scoring system）评分对漏洞的被利用概率进行赋值。CVSS 是被美国国家漏洞数据库（NVD，national vulnerability database）等主流漏洞数据库采用的评分标准，从漏洞危害程度、利用难度等多个角度为漏洞进行评分。其中，Access Complexity 字段为利用难度，反映了攻击者成功利用此漏洞所需要的技术水平、尝试次数等，因此，目前的攻击图技术研究大多参考利用难度评分确定漏洞的被利用概率。

随着网络规模的增大，攻击图生成和分析所需的时间和空间开销也会快速增加，因此，提高大规模网络的攻击图生成和分析效率是攻击图技术的一个研究热点。陈锋等[9]认为对复杂网络进行子网划分，对每个子网分别生成攻击图，再将各子攻击图合并成完整的全局攻击图，可以有效提高复杂网络攻击图的生成能力。Li 等[10]提出一种基于超图划分的前向搜索攻击图生成算法，采取从目标节点到攻击者的搜索方式生成攻击图，相对于从攻击者到目标节点的搜索方式，减少了存储攻击者当前状态所需的额外资源，提高了大规模复杂网络的攻击图生成效率。而如何在网络本身不存在子网划分的情况下对其进行分割仍需要进一步研究。

当仅需要对指向某个重要节点的攻击路径进行分析，或仅需要了解以某个边界节点为初始节点可能产生的攻击路径时，可以采用攻击树技术。攻击树本质上是全局攻击图的子图，通过将根节点设置为需要进行重点防护的节点或某个边界节点实现所需要的分析。Rick 等[11]提出一种攻击树分析框架，在攻击者发动攻击的过程中根据攻击者的技能、可用于发动攻击的时间窗口、资金预算等参数，推测攻击者可能的攻击意图，是为了造成破坏、获得经济利益还是仅仅为了技术挑战。Wolter 等[12]针对攻击图技术通常假定漏洞被利用概率在攻击过程中是不变的，而实际上攻击者可能对成功率较低的漏洞投入更多时间精力等提高其成功概率的问题，提出一种基于攻击树的框架，在攻击过程中根据攻击者的投入修正漏洞被利用概率。

2.2　攻击图的类型

随着研究的深入，根据图中顶点和边表达意义的不同，学术界提出了多种类型的攻击图，主要包括状态攻击图和属性攻击图等。为实现对攻击图中的顶点到达概率和攻击路径发生概率进行计算，有研究人员将贝叶斯网络和攻击图结合，提出贝叶斯攻击图。由于以往的攻击图技术只关注已知的技术漏洞，忽略了 0day 漏洞和社会工程学漏洞对网络安全性的影响，研究人员又提出了包含这 2 种漏洞的 0day 攻击图和社会工程攻击图。目前，贝叶斯攻击图、0day 攻击图和社会工程攻击图主要应用于属性攻击图中，理论上也可应用到状态攻击图中。

2.2.1　状态攻击图

状态攻击图由 Sheyner 首先提出[13~15]（也有学者认为 Swiler 提出的攻击图概念[2]就是最早的状态攻击图），图中顶点表示主机名、提供的服等网络状态信息，有向边表示状态之间的迁移。图 1 为状态攻击图示例，其中，虚线顶点表示网络的初始状态。状态攻击图可以表示为 $AG=(E, V)$，其中，E 为边集合，即原子攻击集合，任意边 $e\in E$ 都表示全局状态的迁移；V 表示状态顶点集合，对于任意顶点 $v\in V$，可以用四元组$<h, srv, vul, x>$表示，其中，h 为该状态涉及的主机，srv 为涉及的服务，vul 为该状态下存在的漏洞，x 可以是任何其他需要参考的信息，如开放端口、入侵检测系统等。在状态攻击图中可以有多个状态顶点表示同一种全局状态。除 Sheyner 提出以模型检测技术构建状态攻

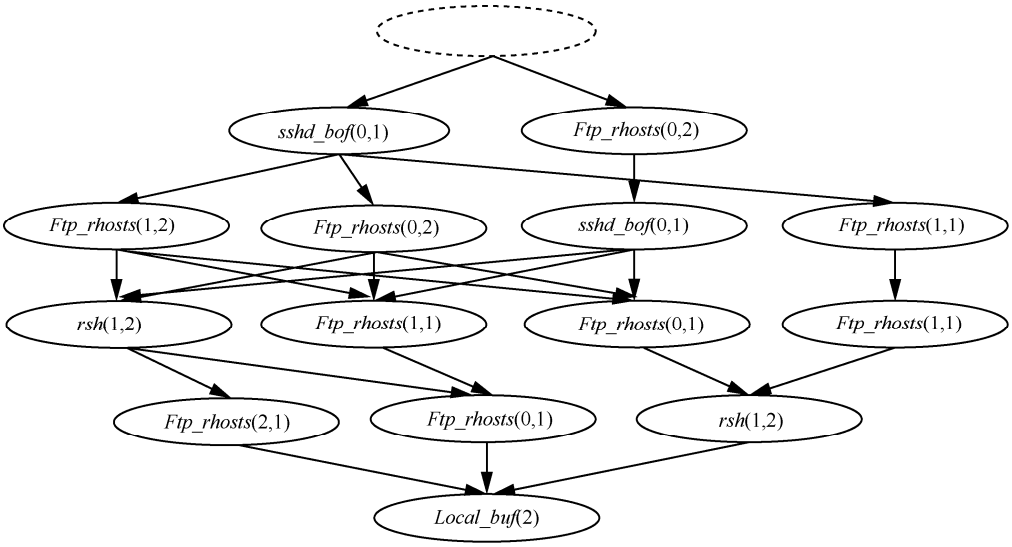


图 1　状态攻击图示例

击图外，其他研究人员对状态攻击图进行了进一步研究，如 Somak 等[16]和冯慧萍等[17]分别采用了智能规划技术和状态搜索技术自动构建状态攻击图。随着状态的迁移，过于快速的状态增长使状态攻击图难以被应用到大规模网络中，且状态攻击图在视觉上不够直观，因此目前已少有针对状态攻击图的研究。

2.2.2　属性攻击图及其拓展

属性攻击图是为解决状态攻击图的属性爆炸问题而提出，将网络中的安全要素作为独立的属性顶点，同一主机上的同一漏洞仅对应图中的一个属性顶点，因此，属性攻击图相对于状态攻击图生成速度快，结构简单，对大规模网络有更好的适应性。

属性攻击图通常包含 2 类顶点和 2 类边。2 类顶点分别表示漏洞和条件，条件顶点表明攻击者当前所具有的权限；漏洞顶点表示存在漏洞的服务和通过利用该漏洞攻击者可以获取的权限。边分为 2 种，由条件指向漏洞的边表示漏洞的前置条件，由漏洞指向条件的边表示漏洞的后置条件。对于属性攻击图，原子攻击节点即漏洞顶点。对于攻击图中任意一个漏洞顶点，当满足全部前置条件时该漏洞才可能被成功利用；而对于任意一个条件顶点，只要将其作为后置条件的任意一个漏洞可以被成功利用，都认为该条件可被满足。因此属性攻击图通常可表示为 $AG=(C,V,E)$[18]，其中，C 表示条件集合（包括所有初始条件、前置条件和后置条件），V 表示漏洞集合，E 表示边集合。AG 满足以下条件：对于$\forall q\in V$，$Pre(q)$为前置条件集合，$Post(q)$为后置条件集合，则有$(\wedge Pre(q))\rightarrow(\wedge Post(q))$，表明满足所有前置条件时可完成漏洞利用，从而满足该漏洞的所有后置条件。图 2 为属性攻击图示例，其中，椭圆顶点为条件顶点，矩形顶点为漏洞顶点。

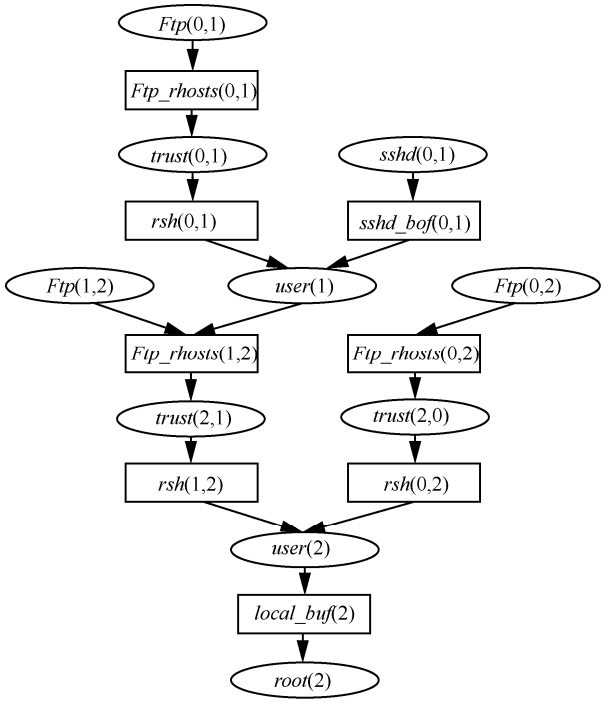
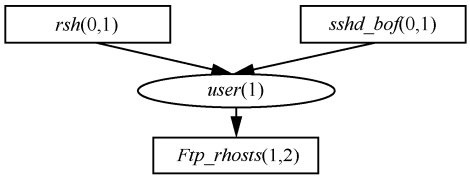


图 2　属性攻击图示例

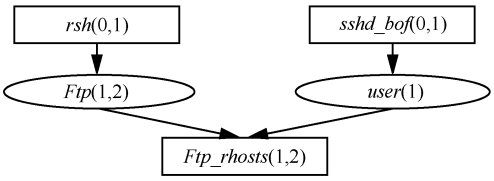
目前，属性攻击图在风险评估[19~21]、告警关联[22]、动态评估[23~25]等方面已经有了广泛的应用。由于同一主机上的同一漏洞仅对应图中的一个属性顶点，因此，Ou[7]首先提出属性攻击图中存在环路问题。闫峰[26]提出属性攻击图中的环路根据漏洞对前置条件的依

赖情况可分为 3 种，其中，2 种可通过在攻击图生成时检测前置条件是否满足并删除部分冗余顶点来解决；第 3 种环路在全局攻击图中无法在不丢失信息的前提下打破环路，但在对指向某个特定节点的全部攻击路径进行分析时，可以根据环路中顶点对攻陷该节点的贡献程度删除部分顶点，打破环路。陈锋等[27]提出无环攻击路径在理论上应具有最大长度 n 的假设，并提出 n-有效攻击路径的概念和发现 n-有效攻击路径的算法，较好地解决了环路问题。

渗透依赖攻击图和属性依赖攻击图是由陈锋等[9]总结的属性攻击图的 2 种拓展。渗透依赖攻击图由 Ritchey[28]和 Wei[29]提出，删除了属性攻击图中的条件顶点，只保留漏洞顶点；而属性依赖攻击图由 Ammann[30]提出，将属性攻击图中的漏洞顶点转化为边，只保留条件顶点。由于这 2 种攻击图都是在属性攻击图的基础上通过减少信息来简化攻击图，因此在视觉上更加直观的同时也带来了一定的应用局限性。如渗透依赖攻击图只能表示图 3(a)所示的情况，无法表示图 3(b)所示的情况；属性依赖攻击图只能表示图 4(a)所示的情况，无法表示图 4(b)所示的情况。



(a)渗透依赖攻击图路径示例1

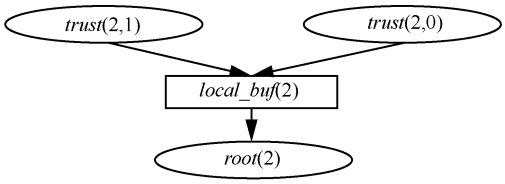


(b)渗透依赖攻击图路径示例2

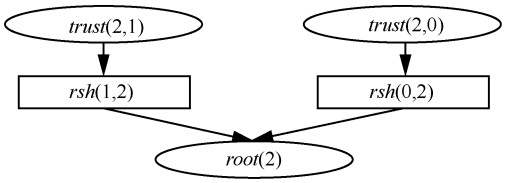
图 3　渗透依赖攻击图的局限性

2.2.3　贝叶斯攻击图

攻击图反映了网络内可能的攻击路径，而判断图中哪些路径更有可能被攻击者使用是攻击图的一个重要功能。贝叶斯网络是一种非常有效的概率推理模型，由 Pearl[31]在 1988 年首先提出。在贝叶斯网络中，初始节点被赋予概率值，有向边表示了节点之间的因果关系，根据初始节点的概率值和节点间的因果关系可推导出后续所有节点的条件概率，因此，目前对攻击路径发生概率和节点被攻陷概率的计算研究大多基于贝叶斯网络进行。通常将基于贝叶斯网络的攻击图称为贝叶斯攻击图[32]。



(a)属性依赖攻击图路径示例1



(b)属性依赖攻击图路径示例2

图 4　属性依赖攻击图的局限性

在贝叶斯攻击图中，漏洞被利用概率的计算有 3 种情况，以图 5 为例进行说明。p 表示漏洞顶点被独立成功利用的概率，P 表示漏洞顶点在攻击图中的被利用概率。第一种情况，对于图 5 中漏洞 *exec*(0,1)和 *sshd_bof*(0,1)，其各自被成功利用概率分别为 p_3 和 p_5，且 *sshd_bof*(0,1)的唯一前置条件是成功利用漏洞 *exec*(0,1)，则显然在该攻击图中 *sshd_bof*(0,1)被成功利用的概率 $P_5=p_5P_3$。第二种情况，对于图中漏洞 *Ftp_rhosts*(0,1)、*UAF*(0,1)和 *rsh*(0,1)，其各自被成功利用概率分别为 p_1、p_2 和 p_4，且三者之间的关系为要利用漏洞 *rsh*(0,1)必须先至少成功利用 *Ftp_rhosts*(0,1)和 *UAF*(0,1)中的任意一个漏洞，即 $Pre(rsh(0,1))=Post(Ftp\_rhosts(0,1)) \vee Post(UAF(0,1))$，则在该攻击图中，*rsh*(0,1)被成功利用的概率为 $P_4=(1-(1-P_1)(1-P_2))p_4$。第三种情况，对于图中漏洞 *rsh*(0,1)、*sshd_bof*(0,1)和 E_6，E_6 被独立成功利用的概率为 p_6，且三者之间的关系为要利用漏洞 *Ftp_rhosts*(1,2)必须先同时成功利用 *rsh*(0,1)和 *sshd_bof*(0,1)，即 $Pre(Ftp\_rhosts(1,2))=Post(rsh(0,1)) \wedge Post(sshd\_bof(0,1))$，则在该攻击图中 *Ftp_rhosts*(1,2)被成功利用的概率为 $P_6=p_6P_4P_5$。根据贝叶斯定理，可将上述 3 种情况的概率计算式推广到涉及更多节点的情况中，并以此计算攻击路径的发生概率。

在贝叶斯攻击图的基础上，张少俊等[33]提出一种方法，基于贝叶斯攻击图和攻击推理引擎对节点的置信度进行计算。Frigault 等[34]提出一种动态贝叶斯攻击图模型，在攻击图构建时加入时间因素，

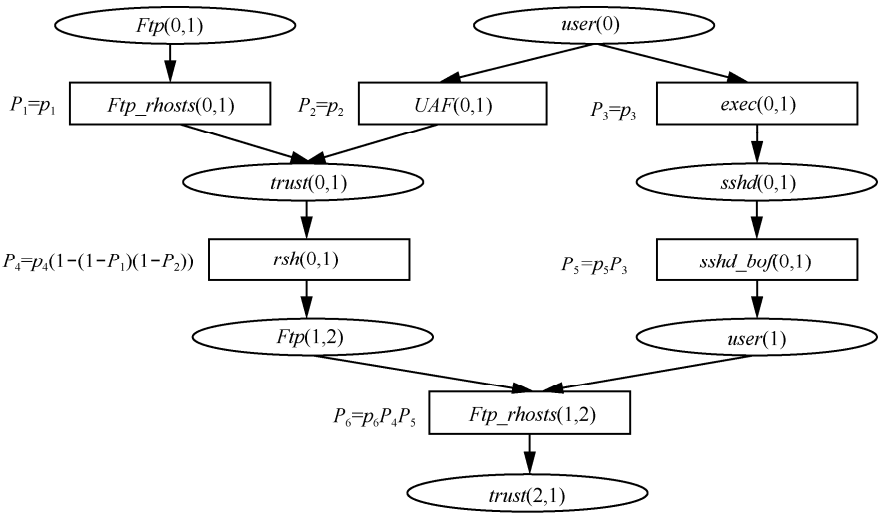


图 5　漏洞被利用概率计算示例

随着网络中漏洞情况地变化动态更新全局攻击图中的漏洞被利用概率。Poolsappasit 等[35]在贝叶斯攻击图中加入入侵告警信息，动态更新概率。方研等[20]又对 Poolsappasit 的方法进行了进一步优化以提高分析效率。

2.2.4　0day 攻击图和社会工程攻击图

相对于已公开漏洞，0day 漏洞和社会工程学漏洞具有极强的不可预知性，即在攻击者利用这 2 种漏洞进行攻击之前防御方很难预知到这 2 种漏洞的存在并加以针对性防范。而在现在的网络攻击，特别是有组织、有针对性的 APT 攻击中，攻击者往往大量使用 0day 漏洞和社会工程学漏洞对目标网络实施渗透、窃密和破坏等行为。

以往的攻击图技术主要关注已知的技术漏洞，0day 漏洞和社会工程学漏洞由于其不可预知性，以及社会工程学漏洞受非技术因素影响太大的原因，很难结合到攻击图中。而国内外大量的 APT 攻击实例证明，利用这 2 种漏洞是攻击者攻克目标网络的最有效手段，将这 2 种漏洞结合到攻击图技术中势在必行。

为解决以往的攻击图技术没有考虑 0day 漏洞的问题，自 2010 年起 Wang 等[36~39]提出了结合 0day 漏洞的攻击图方案，假定网络内所有的远程服务都可能存在 0day 漏洞，根据攻击者攻陷目标节点所需要利用的最小 0day 漏洞数量评估网络安全性，并陆续在此基础上提出了评估设备和服务的多样性以及已知漏洞和非必要服务对网络安全性的影响的方法。

为将社会工程学漏洞作为基于攻击图的网络风险评估的参考要素，Kristian 等[40]提出一种基于攻击图的社会工程学威胁分析方法，通过总结已知的社会工程攻击知识、对社会工程攻击方法进行聚类和模式识别、分析相关权限，将社会工程漏洞作为漏洞顶点加入到属性攻击图中，在分析时将其与技术漏洞同等对待。该方法首次将社会工程学漏洞结合到攻击图技术中，但仅以 5 种社会工程攻击方法为例提供了理论说明，没有具体阐述还有哪些社会工程攻击方法可以应用到攻击图中，以及如何对这些方法进行分类和被利用概率赋值。

3　攻击图技术的应用现状

攻击图技术主要包含 2 方面应用：1)在尚未遭受攻击时对网络进行风险评估和网络加固，提高网络抵御潜在攻击的能力；2)在网络遭受攻击时对已经发现的攻击行为进行告警关联，从而推断出已经发生但未被发现的攻击和攻击者下一步可能发动的攻击，进行损失评估和实时防御。此外，攻击图技术在工业控制网络、蜜网等特种网络中的应用也已有了一定的研究。

3.1　风险评估和网络加固方面

风险评估是攻击图技术最重要的应用之一。通过对全网构建攻击图，可以分析出重要节点被攻击者攻陷的可能性，网络中各个节点的风险等级，最容易成为安全隐患的程序或服务等信息。根据这些信息，防御方可以有针对性地采取增加防护机制、使用更安全的软件等措施来降低网络的安全风险，对网络进行加固。

在基于攻击图的风险评估和网络加固方面，

John 等[18]提出一种方法，在基于 CVSS 评分给定企业级网络中所有漏洞的被利用概率的前提下，可以计算出攻击者在全网中获取某个特定权限或发动某次特定攻击的概率。Kun 等[41]为了缓解计算开销过大的问题，设计算法动态计算针对指定节点发生概率最大的 K 条攻击路径。由于没有生成完整的攻击图，该方法节省了一定开销。但实验部分仅用了一个很简单的网络模型证明该算法的结果是正确的，在复杂网络中是否始终能保证结果的正确性有待进一步研究。Wang 等[42]提出一种启发式搜索策略的攻击图生成方法，通过引入匹配索引表用于存储原子攻击的最新匹配结果来提高攻击图的生成效率。

Kaynar 等[43]提出一种分布式攻击图生成算法，由多个代理节点分别生成子攻击图，再由中心节点将全部子攻击图合并成全局攻击图，实验结果表明当目标网络发生变化时并行分布式计算可以有效提高攻击图的生成速度。但在该算法中漏洞的前置条件和后置条件需要手动生成，不能实现完全的自动化。

Erik 等[44]提出一种基于贝叶斯攻击图和马尔可夫决策过程，结合移动目标防御来做出最佳防御决策的方法。该方法同样只在简单网络中有较好的效果，对于大规模网络仍然缺乏高效的解决算法。

Karel 等[45]提出一种基于攻击图的博弈论模型，使防御方可以通过在网络中增加蜜罐来提高网络的安全性。通过将攻击图转换为马尔可夫决策过程，并采用修剪技术，该方法可以应用到现实的网络环境中。Polad 等[46]通过实验验证了在真实的企业级网络中增加虚假漏洞可有效提高攻击者的攻击成本。

Johnson 等[47]提出一种用于自动生成攻击图的概率威胁建模方法，内置的威胁分析功能使用户不需具有安全相关经验，可以对数据篡改、信息泄露、拒绝服务等攻击进行自动识别和量化。实验部分未给出具体性能数据。

针对现有攻击图技术研究没有考虑到漏洞情况发生变化对网络产生影响的问题，如漏洞已发布补丁或已知的利用代码由于各种原因无法继续使用，Subil 等[48]提出一种非齐次的马尔可夫模型，将漏洞的生存周期和 CVSS 评分结合，在攻击图中综合评估其危害性，从而对网络安全性进行评估。

3.2　入侵检测和告警关联方面

风险评估和网络加固是攻击图技术的静态应用。而在攻击者发动攻击的过程中，根据攻击者已经采取的攻击行为，预判攻击者后续的攻击行为，并采取相应的紧急防护措施或诱捕措施则是攻击图技术的动态应用。Ahmad 等[49]通过将攻击图生成工具 MulVAL 和入侵检测系统 SNORT 结合，从概念上证明了将攻击图工具与入侵检测系统结合，可以在攻击者发动攻击时动态判断攻击者可能的后续攻击目标，从而实现攻击过程中的实时防御。

告警关联是在攻击者发动攻击的过程中，根据入侵检测系统的告警信息，在攻击图中判断攻击者发动的攻击在攻击路径上的关联关系，从而进行漏报攻击的推断和后续攻击的预测。Wang 等[50]首次提出基于队列图的攻击图匹配结构，采用广度优先搜索的方法遍历告警节点的前件和后件节点，由于未加阈值等限制该方法在无关路径上的遍历开销很大。Sayed 等[51]提出了一种基于攻击图的混合告警关联模型，在产生新的告警时可以将其关联到攻击图中已知的告警，减少了前件节点的漏报，但未能解决后件节点的漏报，且只进行了告警关联，未能对后续攻击进行准确的推断和预测。刘威歆等[52]提出一种基于攻击图的多源告警关联分析方法，在综合考虑了前后件关联、提高了告警分析的准确性的同时，将节点映射和告警分析并行化处理，提高了基于攻击图的告警分析速度。

3.3　在特种网络中的应用

除了通常的企业级网络外，科研人员对攻击图在工业控制网络、蜜网等特种网络中的应用也已有了一定的研究。

在工业控制网络方面，徐丽娟等[53]在研究了工控网络相对于一般企业级网络的特点、分析了现有攻击图生成和分析工具在工控网络中适用性的基础上，提出了适用于工控系统的攻击图分层生成算法，实验结果表明基于该算法的攻击图生成和分析工具在工控网络中比 MulVAL 有更高的效率。黄家辉等[54]提出一种基于攻击图的工控系统脆弱性量化方法，根据工控系统的工艺流程对多项指标进行综合评估，制定工控系统的漏洞等级划分标准，用于在攻击图中评估漏洞的攻击期望。

在蜜网方面，胡双双等[55]提出一种基于攻击图的蜜网攻击行为分析模型，利用攻击图具有较为完整的拓扑信息、漏洞信息的特点，弥补了以往蜜网

攻击行为分析技术主要基于专家经验和历史数据、脱离具体环境的缺点，提高了告警关联的准确性。但文章仅研究了所提出方法的可行性和准确性，未测试其性能，在面对长时间高强度的攻击时可能无法及时处理由此产生的海量告警。

由单一设施故障引发的级联故障是关键基础设施网络中很容易出现的安全问题。Kirsty 等[56]通过对关键基础设施网络进行仿真，讨论了使用分布式攻击图进行关键基础设施网络的级联故障预警的重要性和可行性。

信息物理系统（CPS, cyber-physical system）是一种类似于物联网、集成了计算通信与控制于一体的下一代智能系统，注重计算资源与物理资源的结合与协调，与物联网相比更注重对物理世界的反馈。在对信息物理系统的风险评估方面，Hawrylak 等[57]对信息物理系统可能遭受的攻击进行建模并生成了全局攻击图，但没有对安全风险进行定量评估。武文博等[58]提出一种基于攻击图的风险评估模型，在攻击后果的评估上参考了经济损失、人员伤亡、环境破坏、修复费用等因素，结合漏洞被利用概率对信息物理系统进行风险评估，但仅用案例分析说明了风险值计算方法，没有在现实系统或实验环境下进行仿真。Nithols 等[59]针对评估信息物理系统用到的混合攻击图的状态爆炸问题，引入优先级概念，在缩小状态空间的同时保持了重要攻击路径，该方法也可用于传统攻击图。

此外，Patrick 等[60]将攻击图技术引入移动医疗设备网络，用于评估移动医疗设备的安全性。

4 现有攻击图生成和分析工具

目前，已有多种攻击图生成和分析工具可用于学术研究和商业目的。表 1 所示为本文列举的几种工具在开源、商业化等方面的对比。

1) MulVAL

MulVAL（multihost, multistage, vulnerability analysis）是由普林斯顿大学的 Ou 等[7,61]开发的 Linux 平台开源攻击图生成工具，基于 Nessus 或 OVAL 等漏洞扫描器的漏洞扫描结果、网络节点的配置信息以及其他相关信息，使用 graphviz 图片生成器绘制攻击图。可以用 pdf 和 txt 格式的输出文件描述攻击图。对于具有 n 个节点的网络其复杂度为 $O(n^2)$。由于是开源工具，且相对于其他工具有更好的准确度和可扩展性，因此，很多理论研究成果都选择 MulVAL 进行可行性验证和性能测试。Diptikalyan[62]对 MulVAL 的安全规则进行了扩展，使其可以发现 Windows XP 和 SELinux 等操作系统中的访问控制漏洞。

表 1 各攻击图工具对比

工具	是否开源	是否图形界面	是否商用	复杂度
MulVAL	是	命令行界面	否	$O(n^2)$
NetSPA	否	图形界面	是	$O(n\log n)$
NAVIGATOR	否	图形界面	是	$O(n\log n)$
GARNET	否	图形界面	是	$O(n\log n)$
TVA	否	图形界面	否	$O(n^2)$
Cauldron	否	图形界面	是	$O(n^2)$
Attack Graph Toolkit	是	图形界面	否	指数级

2) NetSPA

NetSPA（network security planning architecture）由 Lippmann[63]提出，是一种基于图论的攻击图生成工具。目前，该工具已得到美国政府支持，成为一款商业软件。该工具使用防火墙规则和漏洞扫描结果构建网络模型，并依此计算网络可达性和攻击路径。由于缺少攻击模式学习功能，其规则库的建立需要依赖于手工输入。生成的攻击图中包含环路，不利于使用者理解。复杂度为 $O(n\log n)$。由于展示的攻击图不够直观，在 NetSPA 的基础上又推出了 NAVIGATOR 和 GARNET 两款增强图像显示效果的工具。

3) TVA

TVA（topological vulnerability analysis）是一种具有多项式级时间复杂度的攻击图生成工具，可用于对网络渗透进行自动化分析，其输出结果为由攻击步骤和攻击条件构成的状态攻击图。同 NetSPA 类似，该工具也需要通过手工输入建立规则库。同时该工具未能解决状态攻击图固有的状态爆炸问题，在复杂网络中生成的攻击图极大，不利于分析，因此自 2009 年后已少有对该工具的研究。复杂度为 $O(n^2)$。

4) Cauldron

Caludron 是 TVA 的商用版，由 NSA 支持开发，根据可支持的子网数目不同其价格也有所不同。作为图形界面的攻击图生成和分析工具，Caludron 采用了全局缩略图、主机目录树、漏洞列表、防护建

议等功能以便使用者能直观地看出分析结果。

5) Attack Graph Toolkit

Attack Graph Toolkit 是开源的、具有图形界面的攻击图生成工具，但自 2007 年后就没有更新过源代码。该工具生成的是全局状态攻击图，可视性差，攻击图构建时间长，因此对该工具的研究也很少。复杂度为指数级。

5 未来研究方向

5.1 自动构建攻击图

攻击图构建的基础是获取网络拓扑、运行的服务和存在的漏洞等安全相关信息。由于网络连通性复杂，防火墙、VPN 等网络组件繁多，现有网络拓扑扫描工具难以根据需要构建完全的网络模型，特别是对于企业自研软件或协议的网络。同时，漏洞扫描工具多需要进行在线扫描或定期更新本地漏洞数据库，对于与互联网隔离程度较高的网络存在一定的管理问题。因此，自动获取这些输入信息需要更加有效的手段。

其次，复杂网络的攻击图构建需要耗费大量的时间和空间。尽管已有 Ingols 等算法实现了复杂度与网络中的节点数的线性相关，但其在实际应用中有很多限制，如只能针对某些特定的攻击类型、需要限制节点的出入度等。攻击树作为全局攻击图的子图，在自动构建方面比全局攻击图有更快的速度，但无法反映节点对于网络整体安全性的影响，因此使用上仍有一定的局限性。

此外，现有攻击图技术较少考虑攻击者的能力，而显然在真实的攻击者能力的基础上构建的攻击图对网络防御的指导意义更大。Rick 等[11]和 Wolter 等[12]提出的方法对于攻击溯源、提高判断精确度有一定的意义，但由于从防御方的视角无法准确判断攻击者的技术、预算、对某个特定漏洞的投入程度等信息，因此，这 2 种方法难以应用到实践中。

5.2 简化攻击图

限制攻击图技术被广泛应用的另一个重要原因是节点数较多的网络生成的攻击图过于复杂，难以直观地向防御方反映网络中的脆弱点。以常用工具 MulVAL 为例，对于一个有 10 个节点、每个节点存在 2~3 个漏洞的网络，生成的攻击图中的攻击路径可达到近百条。而在现实环境中，企业级网络的节点数量远多于 10 个，每个节点上存在的漏洞数量也不止 3 个，生成的攻击图将更为复杂，难以解读。如何生成简洁、准确、视觉效果好的攻击图仍然是一个重要的研究方向。

5.3 精确评估漏洞被利用概率

如 2.1 节所述，目前，对漏洞被利用概率的估值主要基于 CVSS 评分。而实际上在不同的软硬件环境以及不同的攻击者能力的条件下，同一个漏洞的被利用概率也是不同的。针对不同的网络环境评估漏洞被利用概率，在攻击者发动攻击的过程中通过评估攻击者能力动态修改漏洞被利用概率，可以更好地指导防御方进行针对性防御。

5.4 提高动态评估效率

尽管 Ahmad 等[49]已经证明了攻击图与入侵检测系统结合可以实现后续攻击目标判定，也有很多学者提出了相关的方法和模型，但由于在对大规模网络的动态评估过程中判断后续攻击路径所用时间可能大于攻击者的攻击时间，导致动态评估实际上很难发挥作用，因此，能否在动态评估中快速准确地定位攻击路径决定了动态评估的可行性和可靠性。

5.5 提高攻击路径预测准确度

攻击图生成和分析工具能否准确预测攻击是攻击图技术是否具有现实意义的重要评估内容，只有既能被攻击图生成工具分析出又能被攻击者采用的攻击路径才是准确的预测。Fredrick[64]对现有攻击图工具中准确度较高的 MulVAL 进行了测评，结果表明 MulVAL 生成的攻击图中的大量攻击路径不能被攻击者发现或没有被攻击者采用，只有少量的攻击路径是成功的预测。在综合了各项指标后，得出的结论为 MulVAL 生成的攻击图在实验环境下的准确度为 57%，而在接入互联网的蜜网环境下准确度为 0.02%。显然这一结果还有很大的提升空间。

5.6 评估未知漏洞的存在和被利用概率

随着攻击技术的发展，0day 漏洞的存在和利用形式越来越复杂和多样化，如著名的心脏出血漏洞 CVE-014-0160 以传统的模糊测试技术几乎不可能被挖掘，利用过程中也未对目标主机造成任何破坏性修改，因此，防御方很难在漏洞被公开前就发现攻击者对该漏洞的利用行为并加以防御。而社会工程学攻击也随着生活方式的变化、办公环境的进步产生各种新的攻击方式。尽管已有 Wang[36~39]和 Kristian 等[40]在 0day 漏洞和社会工程学漏洞方面做出了一定的工作，但现有攻击图技术仍然主要着眼于根据已知漏洞进行分析。如何进一步拓展这 2 方面的工作，如对可能存在 0day 漏洞的服务根据其

历史安全性和重要程度进行 0day 漏洞存在概率评估，进一步细分可应用到攻击图中的社会工程学攻击方法并进行概率评估，将是未来的一个重要研究内容。

6 结束语

本文介绍了攻击图的功能和构成，总结了攻击图技术的应用研究现状，阐述了其应用场景和未来可能的研究方向。攻击图根据顶点和边表达的意义不同可分为状态攻击图、属性攻击图和其他几种类型的攻击图，状态攻击图由于不够直观已经很少被研究，属性攻击图适用于对各种规模的网络进行安全性分析。贝叶斯网络作为一种概率推理模型，将其与攻击图结合可有效判断攻击路径的发生概率，为决策者提出有针对性的防御提供依据。已有多种攻击图生成和分析工具可应用到各类现实场景中。提高攻击图自动构建能力、简化攻击图、更精确地对漏洞被利用概率进行评估、提高攻击路径预测能力、评估 0day 漏洞和社会工程学漏洞的存在情况等都是未来的重要研究方向。

参考文献：

[1] 国家计算机网络应急技术处理协调中心.2016 年中国互联网网络安全报告[M].北京：人民邮电出版社，2017：15-89.
National Internet Emergency Center. Report on China Internet network security in 2016[M]. Beijing: Posts & Telecommunications Press, 2017:15-89.

[2] PHILLIPS C, SWILER L P. A graph-based system for network-vulnerability analysis[C]//The 1998 Workshop on New Security Paradigms. ACM, 1998: 71-79.

[3] WANG S, ZHANG Z, KADOBAYASHI Y. Exploring attack graph for cost-benefit security hardening: a probabilistic approach[J]. Computers & Security, 2013, 32(1):158-169.

[4] HONG J, KIM D S. Harms: hierarchical attack representation models for network security analysis[C]//The 10th Australian Information Security Management Conference. Western Australia, 2012.

[5] KOTENKO I, STEPASHKIN M. Attack graph based evaluation of network security[C]//IFIP International Conference on Communications and Multimedia Security. Springer Berlin Heidelberg, 2006: 216-227.

[6] WANG L, ISLAM T, LONG T, et al. An attack graph-based probabilistic security metric[C]//IFIP Annual Conference on Data and Applications Security and Privacy. Springer Berlin Heidelberg, 2008: 283-296.

[7] OU X, BOYER W F, MCQUEEN M A. A scalable approach to attack graph generation[C]//The 13th ACM conference on Computer and Communications Security. ACM, 2006: 336-345.

[8] HUANG H, ZHANG S, OU X, et al. Distilling critical attack graph surface iteratively through minimum-cost sat solving[C]//27th Annual Computer Security Applications Conference. ACM, 2011: 31-40.

[9] 陈锋, 毛捍东, 张维明,等. 攻击图技术研究进展[J]. 计算机科学, 2011, 38(11):12-18.
CHEN F, MAO H D, ZHANG W M, et al. Survey of attack graph technique[J]. Computer Science, 2011, 38(11):12-18.

[10] LI H, WANG Y, CAO Y. Searching forward complete attack graph generation algorithm based on hypergraph partitioning[J]. Procedia Computer Science, 2017, 107: 27-38.

[11] RICK V H. The motivation of attackers in attack tree analysis[D]. Holland, Delft: Delft University of Technology, 2015.

[12] PIETERS W, DAVARYNEJAD M. Calculating adversarial risk from attack trees: control strength and probabilistic attackers[M]//Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Springer International Publishing, 2015: 201-215.

[13] JHA S, SHEYNER O, WING J. Two formal analyses of attack graphs[C]//The 2002 Computer Security Foundations Workshop. IEEE, 2002: 49-63.

[14] SHEYNER O, HAINES J, JHA S, et al. Automated generation and analysis of attack graphs[C]//The 2002 Security and Privacy Symposium. 2002: 273-284.

[15] SHEYNER O. Scenario graphs and attack graphs[D]. US Air Force Research Laboratory, 2004.

[16] BHATTACHARYA S, GHOSH S K. An artificial intelligence based approach for risk management using attack graph[C]//Computational Intelligence and Security, 2007 International Conference on IEEE. 2007: 794-798.

[17] 冯萍慧, 连一峰, 戴英侠, 等. 基于可靠性理论的分布式系统脆弱性模型[J].软件学报，2006,17(7): 1633-1640.
FENG P H, LIAN Y F, DAI Y X, et al. A vulnerability model of distributed systems based on reliability theory[J]. Journal of Software, 2006, 17(7):1633-1640.

[18] HOMER J, ZHANG S, OU X, et al. Aggregating vulnerability metrics in enterprise networks using attack graphs[J]. Journal of Computer Security, 2013, 21(4):561-597.

[19] 吴迪, 连一峰, 陈恺,等. 一种基于攻击图的安全威胁识别和分析方法[J]. 计算机学报, 2012, 35(9):1938-1950.
WU D, LIAN Y F, CHEN K, et al. A security threats identification and analysis method based on attack graph[J]. Chinese Journal of Computers, 2012, 35(9):1938.

[20] 方研, 殷肖川, 李景志. 基于贝叶斯攻击图的网络安全量化评估研究[J]. 计算机应用研究, 2013, 30(9):2763-2766.
FANG Y, YIN X C, LI J Z. Research of quantitative network security assessment based on Bayesian-attack graphs[J]. Application Research of Computers, 2013, 30(9):2763-2766.

[21] ALHOMIDI M, REED M. Risk assessment and analysis through population-based attack graph modelling[C]//2013 World Congress on Internet Security (WorldCIS) . 2013: 19-24.

[22] ROSCHKE S, CHENG F, MEINEL C. High-quality attack graph-based IDS correlation[J]. Logic Journal of the IGPL, 2013, 21(4):571-591.

[23] WANG L, YAO C, SINGHAL A, et al. Implementing interactive analysis of attack graphs using relational databases[J]. Journal of Computer Security, 2008, 16(4):419-437.

[24] WANG L, YAO C, SINGHAL A, et al. Interactive analysis of attack graphs using relational queries[C]//IFIP Annual Conference on Data and Applications Security and Privacy. Springer Berlin Heidelberg, 2006: 119-132.

[25] 陈靖, 王冬海, 彭武. 基于动态攻击图的网络安全实时评估[J]. 计算机科学, 2013, 40(2):133-138.
CHEN J, WANG D H, PENG W. Real-time network security assessment based on dynamic attack graph[J]. Computer Science, 2013, 40(2):133-138.

[26] 闫峰. 基于攻击图的网络安全风险评估技术研究[D]. 长春: 吉林大学, 2014.
YAN F. The technology research of network security assessment based on attack graphs[D]. Changchun: Jilin University, 2014.

[27] 陈锋, 张怡, 苏金树,等. 攻击图的两种形式化分析[J]. 软件学报, 2010, 21(4):838-848.
CHEN F, ZHANG Y, SU J S, et al. Two formal analyses of attack graphs[J]. Journal of Software, 2010, 21(4):838-848.

[28] RITCHEY R, O'BERRY B, NOEL S. Representing TCP/IP connectivity for topological analysis of network security[C]//The 2002 Computer Security Applications Conference. 2002: 25-31.

[29] LI W, VAUGHN R B, DANDASS Y S. An approach to model network exploitations using exploitation graphs[J]. Simulation, 2006, 82(8): 523-541.

[30] AMMANN P, WIJESEKERA D, KAUSHIK S. Scalable, graph-based network vulnerability analysis[C]//The 9th ACM Conference on Computer and Communications Security. ACM, 2002: 217-224.

[31] PEARL J. Probabilistic reasoning in intelligent system[M]. Morgan Kaufinann: Network of Plausible Inference, 1988:1-86.

[32] LIU Y, MAN H. Network vulnerability assessment using Bayesian networks[C]//Defense and Security. International Society for Optics and Photonics, 2005: 61-71.

[33] 张少俊, 李建华, 宋珊珊,等. 贝叶斯推理在攻击图节点置信度计算中的应用[J]. 软件学报, 2010, 21(9):2376-2386.
ZHANG S J, LI J H, SONG S S, et al. Using Bayesian inference for computing attack graph node beliefs[J]. Journal of Software, 2010, 21(9):2376-2386.

[34] FRIGAULT M, WANG L. Measuring network security using Bayesian network-based attack araphs[C]//The 3rd IEEE International Workshop on Security, Trust, and Privacy for Software Applications. 2008:698-703.

[35] POOLSAPPASIT N, DEWRI R, RAY I. Dynamic security risk management using Bayesian attack graphs[J]. IEEE Transactions on Dependable & Secure Computing, 2011, 9(1):61-74.

[36] WANG L, JAJODIA S, SINGHAL A, et al. *k*-zero day safety: measuring the security risk of networks against unknown attacks[J]. Lecture Notes in Computer Science, 2010, 11(1):573-587.

[37] WANG L, JAJODIA S, SINGHAL A, et al. *k*-zero day safety: a network security metric for measuring the risk of unknown vulnerabilities[J]. IEEE Transactions on Dependable & Secure Computing, 2014, 11(1): 30-44.

[38] WANG L, ZHANG M, JAJODIA S, et al. Modeling network diversity for evaluating the robustness of networks against zero-day attacks[C]//European Symposium on Research in Computer Security. Springer International Publishing, 2014: 494-511.

[39] ZHANG M, WANG L, JAJODIA S, et al. Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(5): 1071-1086.

[40] BECKERS K, KRAUTSEVICH L, YAUTSIUKHIN A. Analysis of social engineering threats with attack graphs[M]//Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Springer International Publishing, 2015:67-73.

[41] BI K, HAN D, WANG J. K maximum probability attack paths dynamic generation algorithm[J]. Computer Science and Information Systems, 2016, 13(2): 677-689.

[42] WANG S, TANG G, KOU G, et al. An attack graph generation method based on heuristic searching strategy[C]// 2016 2nd IEEE International Conference on Computer and Communications (ICCC), 2016: 1180-1185.

[43] KAYNAR K, SIVRIKAYA F. Distributed attack graph generation[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(5): 519-532.

[44] MIEHLING E, RASOULI M, TENEKETZIS D. Optimal defense policies for partially observable spreading processes on Bayesian attack graphs[C]//The Second ACM Workshop on Moving Target Defense. ACM, 2015: 67-76.

[45] DURKOTA K, LISY V, BOSANSKY B, et al. Optimal network security hardening using attack graph games[C]//IJCAI. 2015: 7-14.

[46] POLAD H, PUZIS R, SHAPIRA B. Attack graph obfuscation[C]//International Conference on Cyber Security Cryptography and Machine Learning. Springer, Cham, 2017: 269-287.

[47] JOHNSON P, VERNOTTE A, EKSTEDT M, et al. pwnPr3d: an attack-graph-driven probabilistic threat-modeling approach[C]//2016 11th International Conference on Availability, Reliability and Security (ARES). 2016: 278-283.

[48] ABRAHAM S,NAIR S. Predictive cyber security analytics framework: a non-homogenous Markov model for security quantification[J]. Journal of Communications, 2014, 12(9):899-907.

[49] FADLALLAH A, SBEITY H, MALLI M, et al. Application of attack graphs in intrusion detection systems: an implementation[J]. International Journal of Computer Networks, 2016, 8(1):1-12.

[50] WANG L, LIU A, JAJODIA S. Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts[J]. Computer Communications, 2006, 29(15):2917-2933.

[51] AHMADINEJAD S H, JALILI S, ABADI M. A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs[J]. Computer Networks, 2011, 55(9): 2221-2240.

[52] 刘威歆, 郑康锋, 武斌,等. 基于攻击图的多源告警关联分析方法[J]. 通信学报, 2015, 36(9):135-144.
LIU W X, ZHENG K F, WU B, et al. Alert processing based on attack graph and multi-source analyzing[J]. Journal on Communications, 2015, 36(9):135-144.

[53] 徐丽娟. 基于攻击图的工业控制网络安全隐患分析[D]. 北京：北京邮电大学, 2015.
XU L J. Industrial control system network's potential risk analysis based on attack graph[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[54] 黄家辉, 冯冬芹, 王虹鉴. 基于攻击图的工控系统脆弱性量化方法[J]. 自动化学报, 2015, 42(5):792-798.
HUANG J H, FENG D Q, WANG H J. A method for quantifying vulnerability of industrial control system based on attack graph[J]. Acta Automatica Sinica, 2015, 42(5):792-798.

[55] LEVER K E, MACDERMOTT Á, KIFAYAT K. Evaluating interdependencies and cascading failures using distributed attack graph generation methods for critical infrastructure defence[C]//The 2015 De-

velopments of E-Systems Engineering (DeSE). 2015: 47-52.

[56] 胡双双. 基于蜜网的攻击行为分析[D]. 北京：北京邮电大学, 2015.
HU S S. Analysis of attack based on honeynet[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[57] HAWRYLAK P J, HARTNEY C, PAPA M, et al. Using hybrid attack graphs to model and analyze attacks against the critical information infrastructure[M]//Critical Information Infrastructure Protection and Resilience in the ICT Sector. IGI Global, 2013: 173-197.

[58] 武文博, 康锐, 李梓. 基于攻击图的信息物理系统信息安全风险评估方法[J]. 计算机应用, 2016, 36(1):203-206.
WU W B, KANG R, LI Z. Attack graph based risk assessment method for cyber security of cyber-physical system[J]. Journal of Computer Applications, 2016, 36(1):203-206.

[59] NICHOLS W, HAWRYLAK P, HALE J, et al. Introducing priority into hybrid attack graphs[C]//The 12th Annual Conference on Cyber and Information Security Research. ACM, 2017: 12.

[60] LUCKETT P, MCDONALD J, GLISSON W. Attack-graph threat modeling assessment of ambulatory medical devices[C]//The 50th Hawaii International Conference on System Sciences. 2017: 3648-3657.

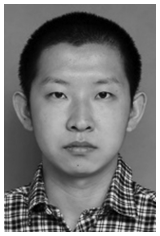
[61] OU X, GOVINDAVAJHALA S, APPEL A W. MulVAL: a logic- based network security analyzer[C]//14th USENIX Security. 2005: 1-16.

[62] SAHA D. Extending logical attack graphs for efficient vulnerability analysis[C]//The 15th ACM Conference on Computer and Communications Security. 2008: 63-74.

[63] LIPPMANN R, INGOLS K, SCOTT C, et al. Validating and restoring defense in depth using attack graphs[C]//Milcom 2006 Military Communications Conference. 2006:1-10.

[64] FREDRIK J S. A test of attack graph-based evaluation of IT-security[D]. Sweden, Västerbotten: Umeå University, 2014.

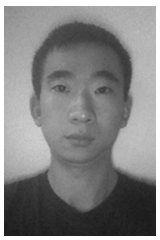
作者简介：



叶子维（1990-），男，吉林通化人，解放军信息工程大学博士生，主要研究方向为网络安全、态势感知。

郭渊博（1975-），男，陕西周至人，解放军信息工程大学教授、博士生导师，主要研究方向为大数据安全、态势感知。

王宸东（1992-），男，江西抚州人，解放军信息工程大学硕士生，主要研究方向为网络安全。



琚安康（1995-），男，河南新乡人，解放军信息工程大学博士生，主要研究方向为多步网络攻击检测、威胁情报。