基于攻击图的信息物理融合系统渗透测试方法

徐丙凤[1] 何高峰[2]

(南京林业大学信息科学技术学院 南京 210037)[1] (南京邮电大学物联网学院 南京 210003)[2]

摘 要 信息物理融合系统(Cyber-Physical System,CPS)多为安全攸关系统,是网络攻击的高价值目标,需要对其进行有效的安全评估。为此,提出一种基于攻击图的信息物理融合系统渗透测试方法。首先,对传统攻击图进行改进,考虑物理攻击、攻击持续时间以及物理系统的连续变量值,提出适用于 CPS 的攻击图建模技术 AGC(Attack Graph for CPS),并在图中增加攻击可行性参数以表示单步攻击的成功率;其次,基于 AGC 提出最优攻击路径选择策略,包括最小攻击代价、最短攻击时间等,并设计面向 CPS 的智能渗透测试算法;最后,通过应用实例对方法的有效性进行验证。分析结果表明,该方法能够根据渗透测试目标选择最优攻击路径,并能根据实际反馈结果自动调整后续攻击步骤,有效实现 CPS 的安全评估。

关键词 信息物理融合系统,安全评估,攻击图,最优攻击路径

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.11.021

Penetration Testing Method for Cyber-Physical System Based on Attack Graph

XU Bing-feng[1] HE Gao-feng[2]

(College of Information Science and Technology,Nanjing Forestry University,Nanjing 210037,China)[1]

(School of Internet of Things,Nanjing University of Posts and Telecommunications,Nanjing 210003,China)[2]

Abstract As a typical example of security-related system,cyber-physical system (CPS) is the high-value target of network attack. Therefore,its security protection needs to be effectively assessed. To this end,a penetration testing method for CPS based on attack graph is proposed. Firstly,the traditional attack graph is improved and a new attack graph for CPS (AGC) is proposed. Specifically,the physical attack,the duration of the attack and the continuous variable value of physical system are considered in AGC. Additionally,the attack feasibility parameter is added to represent the success rate of single-step attack. Secondly,based on AGC,the optimal attack path selection strategies are represented,including the minimum attack cost,the shortest attack time and so on. Furthermore,the intelligent penetration testing algorithm is designed to accomplish automated penetration. Finally,the effectiveness of the proposed method is verified by case study. The results show that the method can select the optimal attack path to the target,intelligently adjust the subsequent attack steps according to the feedback,and assess the security of CPS effectively.

Keywords Cyber-physical system,Security assessment,Attack graph,Optimal attack path

1 引言

信息物理融合系统是一种深度融合计算、通信与控制技术的复杂系统,被广泛应用于电力、石油石化、核能、通信、交通运输、水处理等关键基础领域。CPS 与关键基础设施相关联,多为安全攸关的系统,因此一旦被攻击成功,物理系统的运行也会被破坏,后果将不堪设想[1-2]。例如,2015 年乌克兰电力网络遭受鱼叉式网络钓鱼(Spear Phishing)攻击,黑客以含有恶意宏的 Microsoft Office 文件为攻击载体,清空 SCADA 系统数据,致使乌克兰西部地区约 70 万居民用户停电数小时[3]。因此,CPS 安全防护已成为国家战略安全的重要组成部分[4],对其开展安全验证与评估研究具有重要意义。

为验证和评估 CPS 的安全性,一种可行的方法是构建网络空间靶场(Cyber Range)[5],通过在靶场中开展真实的网络攻击和渗透测试,来发现 CPS 的安全防护弱点并评估攻击所产生的后果。与基于数值计算或定性分析的 CPS 安全风险评估[6-7]不同,基于网络空间靶场和渗透测试的评估方法能直观反映出攻击步骤和攻击后果,并直接暴露出 CPS 的安全防护弱点,因而具备更好的实际可操作性。为此,世界各国纷纷开展相关研究。如美国从 2008 年开始执行“曼哈顿计划”,建

到稿日期:2017-09-20 返修日期:2017-12-23 本文受南京林业大学高层次人才科研启动基金(GXL016),南京林业大学校青年创新基金(CX2016026),国家自然科学基金青年科学基金项目(61702282),江苏省高等学校自然科学研究项目(17KJB520023),南京邮电大学引进人才科研启动基金(NY217143)资助。

徐丙凤(1986-),女,博士,讲师,CCF 会员,主要研究方向为 CPS 安全、软件安全;**何高峰**(1984-),男,博士,讲师,主要研究方向为 CPS 安全、匿名通信,E-mail:hegaofeng@njupt.edu.cn(通信作者)。

立国家级的工业控制系统攻防靶场，并于 2014 年在其国家靶场增加了法拉第罩进行无线发射设备的测试，同时支持移动计算设备；2014 年 6 月，北大西洋公约组织在塔林建立 NATO 网络空间靶场，用以支持工控网的攻防测试。

目前，相关研究工作主要集中于解决 CPS 网络空间靶场构建中的大规模网络仿真、网络流量与用户行为模拟、平台安全及管理等问题[8]，对如何在网络空间靶场中有效开展渗透测试的研究较少。但实际上，渗透测试的成功率决定了 CPS 安全风险评估的最终效果；同时，缩短渗透测试所需的时间也有助于提升网络空间靶场的使用效率。为此，本文针对 CPS 网络空间靶场渗透测试技术开展深入研究，提出一种面向 CPS 的智能渗透测试方法。首先，对传统攻击图进行改进，考虑物理攻击、攻击持续时间以及物理系统的连续变量值，提出适用于 CPS 的攻击图建模技术 AGC，并给出攻击可行性等参数值的确定策略；其次，基于 AGC 提出最优攻击路径选择策略，包括最小攻击代价、最短攻击时间等，并设计实现面向 CPS 的智能渗透测试流程。实例分析结果表明，该方法能够根据渗透测试目标选择出最优攻击路径，并能根据实际反馈结果自动调整后续攻击步骤，实现攻击路径的智能切换，从而实现 CPS 安全性的有效评估。

本文第 2 节对 CPS 安全风险评估的相关工作进行分析总结；第 3 节提出 CPS 攻击图建模技术；第 4 节给出智能渗透测试的详细算法和流程；第 5 节进行应用实例分析；最后总结全文，并指出未来的研究工作。

2 相关工作

在 CPS 安全风险评估研究方面，主要有定性分析、定量评估以及渗透测试等。定性分析的典型工作包括故障树[9]以及类似的攻击树[7]等。故障树等按照逻辑关系从上至下构建故障的因果关系图，安全攻击事件之间的关系较清晰，有助于定性分析导致安全风险的事故序列，但分析的准确性受限于已知的攻击事件、分析人员的个人经验和对相关系统的了解程度等因素。同时，定性分析仅基于精确安全事件数据，不利于其他相关联的风险数据的深度挖掘。

定量风险评估技术依据资产识别、威胁识别、脆弱性识别和安全措施识别，通过分析各要素之间的关联程度，计算出系统的风险值。相关研究工作有：卢慧康等[10]针对工业控制系统，提出了基于模糊层次分析法的信息安全风险评估方法；Woo 等[11]通过对系统组件面临的威胁、组件脆弱性与资产值 3 个属性进行量化，实现了电力 SCADA 系统的网络安全风险评估；Bouchti 等[12]同样针对 SCADA 系统，基于着色 Petri 网进行了攻击建模分析，实现了网络入侵过程的量化描述；王作广等[13]结合攻击树和 CVSS，提出工业控制系统风险量化评估方法。但是，量化评估过程中易受人为主观性因素影响，且评估结果缺乏对安全风险的细节描述，如防御措施为何失败、攻击产生的影响等。

基于渗透测试的安全风险评估技术通过在真实系统或网络空间靶场中开展实际网络攻击，能直接暴露出系统的安全防护弱点，攻击产生的后果亦直接明了，因而更具备实际可操作性。目前，针对 CPS 进行渗透测试的研究工作较少，在传统信息网络安全评估研究中，已有相关学者对自动化渗透测试开展研究。文献[14]利用被测试目标网络脆弱点间的逻辑关系，提出一种基于攻击图的渗透测试方案的自动生成方法。文献[15]提出一种基于 Petri 网的渗透测试攻击模型，对已知漏洞列表构建单漏洞利用模型，通过整合形成渗透测试攻击模型。文献[16-17]针对 Web 安全分析提出自动化渗透测试方案。上述研究工作主要针对信息网络，未考虑到 CPS 系统安全的特殊性（如存在物理攻击、攻击需持续一定时间等），研究成果难以直接应用于 CPS 的安全评估。

本文针对 CPS 安全攻击的特点，首先构建适合 CPS 的攻击图，然后以此攻击图为基础，依据多种渗透测试目标，构建最优攻击路径，最后根据实际反馈结果自动调整后续攻击步骤，实现攻击路径的智能切换。

3 CPS 攻击图建模

CPS 安全威胁与传统信息网络存在较多不同。依据文献[18]，抽象的 CPS 运行模式如图 1 所示。其中，传感器获取物理世界的信息，通过网络将数据传输到信息系统；信息系统对数据进行融合处理后综合做出决策，产生控制命令并返回给控制器；控制器控制执行器执行相应动作，从而改变物理过程。因此，CPS 的主要安全威胁在于直接或间接操纵控制参数、传感参数和控制器传递函数，最终对所控制的物理系统产生危害。

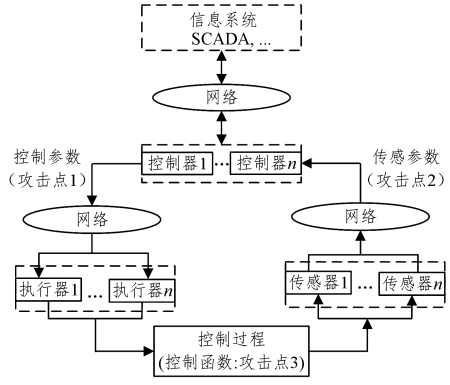

图 1 CPS 运行模式与主要攻击点

Fig. 1 Operation mode and main attack points of CPS

为改变控制参数、传感参数和控制器传递函数，攻击者可采用物理攻击（如直接修改传感器固件，从而改变传感变量），且攻击需持续一定时间（如攻击需持续进行以降低传感器的能耗），同时攻击的输出可能为连续值（如改变传感器数值为任意数字）。传统的攻击图建模技术[19]无法反映出这些新的安全威胁特征。为此，本节提出一种新的适用于 CPS 的攻击图建模技术 AGC，通过增加新的图节点和边来建模 CPS 中新的攻击手段和结果，并在图节点中直接添加攻击可行性参数以便于后续寻找最佳攻击路径，具体说明如下。

在 AGC 建模中，攻击图可表示为 $G=\langle V,E\rangle$，其中 V 表示图节点的集合，E 表示边的集合。进一步，将图节点区分为前置节点 P、攻击节点 A_I 和 A_P、后置节点 C_I 和 C_P 以及连接

节点 O，即 $V=\{A_I, A_P, C_I, C_P, O\}$。而图中的边表示图节点间的连通性，根据是否包含时间信息将其分为 e 和 e_t，即 $E=\{e, e_t\}$，其中 e_t 边上包含的时间表示攻击持续的时间。

定义 1（前置节点）　前置节点 P 表示原子攻击的前提条件，节点中可包括（网络或物理）连通性、主机 IP 地址、CPEID、CVEID、服务种类、攻击可行性、应用名称等 7 类信息。其中，CPEID 和 CVEID 分别表示在通用平台枚举和 CVE 漏洞库中的检索编号，特别地，本文将 CVEID 设置为特殊的 0-day-unknown 来标记 0-day 漏洞；服务种类表示当前主机的主要运行功能，如 Web 服务器、数据库服务器等，当攻击者占据此类主机时，即使不存在漏洞，其也可利用自身权限访问后台数据以便于后续攻击；攻击可行性表示单步攻击成功的概率，具体计算方法将在第 4 节中详细介绍。在 AGC 中，用六边形表示前置节点。

定义 2（攻击节点）　攻击节点表示攻击者执行的具体攻击，分为信息攻击 A_I 和物理攻击 A_P 两类。在节点 A_I 和 A_P 中包含具体的攻击信息，如攻击名称、攻击参数、攻击可行性等。在 AGC 中，用长方形表示信息攻击节点 A_I，用正方形表示物理攻击节点 A_P。

定义 3（后置节点）　后置节点表示攻击产生的后果，如获得 root 权限或使得传感器能效降低至 0。在 AGC 中，用椭圆形表示后置节点。若攻击的输出为连续值，则使用取值范围来表示，如(0,50]。

定义 4（连接节点）　连接节点表示不同边之间的逻辑关系，有“与(and)”和“或(or)”两种。在 AGC 中，用三角形表示连接节点。

定义 5（边）　在 AGC 中，边为有向边，表示图节点间的连通性，用单箭头表示。特别地，为表示攻击持续时间，支持在边上增加时间值，用双箭头表示以作区别。其中，时间值可以为固定值 t，也可以为某一概率分布，如 $e^{-\lambda t}$ 等。

依据上述定义描述，可以有效构建 CPS 攻击图，体现物理攻击及其攻击特性，如连续时间等。但在实际使用中，还需要考虑如何准确描述攻击行为及其影响，以便于正确分析系统的安全性。在 AGC 建模中，对于信息攻击节点 A_I，其攻击名称和攻击参数可由 CVE 漏洞库[1)] 中描述的攻击向量（Vector）和分析描述（Analysis Description）部分获得，对应的后置节点内容由 CVE 漏洞库中的影响类型（Impact Type）描述。

对于物理攻击节点 A_P，其包含的攻击类型有控制参数攻击、传感参数攻击以及控制过程攻击等 3 类，如图 1 所示。其中，控制参数和传感参数攻击过程的建模过程[18] 如式(1)所示：

$$m(t)=y(t)[A\alpha(t)+B]+C\beta(t)+D \tag{1}$$

其中，$y(t)$ 表示原始正常的参数值；A, B, C 是攻击者选定的攻击参数；D 为扰动变量；$\alpha(t)$ 表示攻击者选择的时变函数。

控制过程攻击涉及控制器中控制逻辑的修改，难以用单一函数表示。为此，可借鉴 CVE 漏洞库的表示方法，采用攻击向量、分析描述和影响类型 3 部分进行物理攻击过程的描述。具体地，分析描述定义为控制过程的模拟仿真[20] 或文字描述；攻击向量表示控制逻辑的修改方式，如修改仿真程序的某项运行逻辑；影响类型即为模拟仿真的输出。通过此种方法，可以将复杂的控制过程攻击转化为易于描述的仿真程序或文字，实现攻击图对物理攻击的建模支持。

与传统的攻击图建模技术[19,21] 相比，AGC 增加了物理攻击节点、连续值表示以及带时间值的边，支持服务种类以及 0-day 漏洞的标识，丰富了攻击图的表达能力。同时，在前置节点和攻击节点中增加攻击可行性参数，便于后续最优攻击路径的分析选择。最终形成的攻击图示例如图 2 所示。

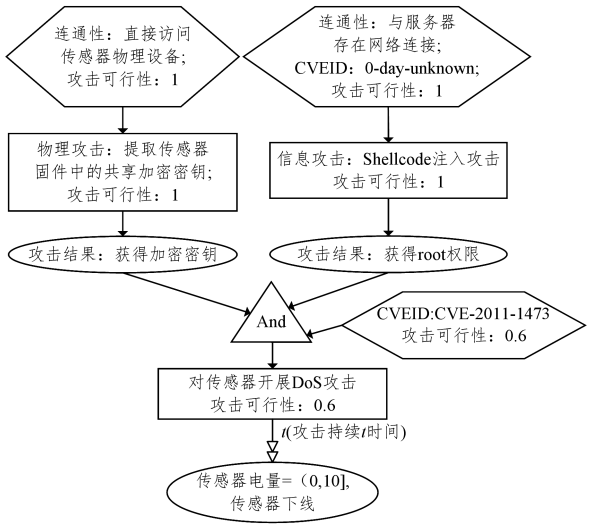

图 2　CPS 攻击图示例

Fig. 2　Example of attack graph for CPS

4　智能渗透测试

本文中智能渗透测试的目的是根据渗透测试目标和 AGC 攻击图，选择最优渗透测试路径，并根据实际攻击反馈结果智能调整后续攻击步骤。为此，本节首先给出 AGC 攻击图中的攻击可行性参数，即单步攻击成功概率的计算过程。

4.1　攻击可行性参数计算

对于信息类攻击，攻击成功概率与漏洞的固有特性相关。对于公开漏洞（具有 CVEID 编号），其攻击可能性受漏洞暴露时间、漏洞利用的难易程度、是否具有公开 POC、漏洞修复程度、攻击者所具备的知识等因素的影响。但漏洞修复程度、攻击者所具备的知识等因素的评估涉及主观判断，量化过程缺乏客观性，因此本文使用漏洞暴露时间、漏洞利用的难易程度、是否具有公开 POC 等三要素来计算特定漏洞的攻击可能性。记 CVE 漏洞 i 的暴露时间为 t_i，则 t_i 的计算方式为：

$$t_i=currentTime-openTime(i) \tag{2}$$

即漏洞公开时间距当前时间的差值。将漏洞利用难度记为 e_i，由 CVSS 3.0 规范[22] 可知：

$$e_i=exploitability\_sub\_score/8.22 \tag{3}$$

其中，$exploitability\_sub\_score = 8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$。

1) https://cve.mitre.org/index.html

记是否具有公开 POC 为 q_i，计算式为：

$$q_i=\begin{cases}0, & \text{without POC}\\ 1, & \text{with POC}\end{cases} \tag{4}$$

为计算漏洞 i 的攻击可行性 $Pr(i)$，还需对 t_i 和 q_i 进行归一化处理，如式(5)－式(7)所示：

$$U(t_i)=\frac{t_i}{\max(t_i,i=1,2,\cdots,m)} \tag{5}$$

$$U(q_i=1)=\frac{\sum_{i=1}^{m}q_i}{m} \tag{6}$$

$$U(q_i=0)=1-U(q_i=1) \tag{7}$$

其中，m 表示攻击图中已知公开的漏洞数量。

漏洞 i 的攻击可行性 $Pr(i)$ 的计算过程如式(8)所示：

$$Pr(i)=U(t_i)\times e_i\times U(q_i) \tag{8}$$

对于未知漏洞和物理攻击，其代表的是攻击者的自身特殊攻击能力，在攻击图中由攻击者自行标记，因此其攻击可行性为 1。对于信息类攻击节点，其攻击可行性直接继承其前置节点的 $Pr(i)$，而并非将前置节点和上一步攻击节点的概率值相乘。此种处理方法避免了随着攻击图的增长而后续攻击节点的攻击可行性数值趋向于 0，同时不影响后续分析。

4.2 最优攻击路径及攻击步骤的自动调整

根据攻击图以及其中的攻击可行性和攻击持续时间参数，可以选择出不同的最优攻击路径，如最短攻击路径、最大成功概率攻击路径以及最少时间攻击路径等。

1)最短攻击路径。可将 AGC 攻击图视为有向无权图且只考虑攻击节点，通过 Dijkstra 等算法选出最短攻击路径。此时，渗透测试所需的攻击步骤最少。

2)最大成功概率攻击路径。将攻击可行性视为攻击节点对应的边的权重值，同样通过使用 Dijkstra 等算法(权重值相乘)选出最短攻击路径，即为最大成功概率攻击路径。此时，针对特定目标的渗透测试成功率最大。

3)最少时间攻击路径。将攻击持续时间作为图中边的权重值。对于单箭头表示的边，可以将其权重值定义为 0。此时，针对特定目标的渗透测试所需时间最短。

在实际中，根据选择出的最优攻击路径进行渗透测试可能会失败，例如攻击路径中的某一攻击节点无法执行预期攻击，因此需要根据实际的攻击反馈结果重新选择路径。一种可能的方法是重新遍历攻击图，选择另一条次优攻击路径，但需要消耗较多时间。为此，本文提出一种攻击步骤自动调整算法，通过节点回退和重新寻找当前节点至原失效节点的下一跳节点间的最优路径，实现攻击步骤的自动调整，如图 3 所示。

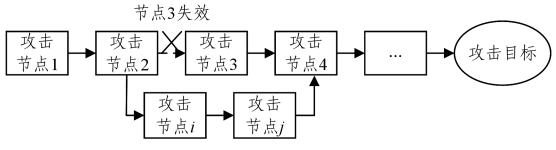

图 3 攻击步骤调整示例

Fig. 3 Example of adjustment of attack steps

在图 3 中，攻击路径上的节点(攻击步骤)3 失效。此时，回退至攻击节点 2，寻找节点 2 与原路径上节点 4 之间(节点 3 的下一跳节点)的最优路径。因此，攻击步骤由原来的〈1，2，3，4，…〉调整为〈1，2，i，j，4，…〉。

特别地，若回退次数超过设定的阈值 α，则在攻击图中删除失效节点，重新遍历选择最优攻击路径。具体流程如算法 1 所示。在算法 1 中，ReceiveFeedBack()函数接收特定节点的攻击反馈结果(success or failed)，findOptimalPath()函数根据 *para* 参数的不同，在源节点和目的节点间选择最优攻击步骤。

算法 1 攻击步骤自动调整算法

输入：攻击图 G，最优攻击路径 Path[0，1，…，n－1]

输出：调整后的攻击步骤

```
1. result=ReceiveFeedBack(Path[i])
2. if (result==success)
3.    steps=null;
4. else // attack failed
5.    count++;
6.    if (count >α)
7.       steps=findOptimalPath(source,target,G,para);
8.    end if
9.    else
10.      previousNode=Path[i-1];
11.      nextNode=Path[i+1];
12.      delete the node Path[i] from the attack graph G;
13.      steps=findOptimalPath(previousNode,nextNode,G,para);
14. end if
15. return steps;
```

5 应用实例

本文以一个污水处理系统为例，对所提方法进行验证。为便于分析，本文仅给出该污水处理系统中含有漏洞的主要组成部件，简化后的系统环境如图 4 所示。图 4 中，网络拓扑主要由互联网、企业外网、企业生产网、控制网以及现场执行设备等部分组成，典型的功能主机包括 Web 服务器、数据库服务器、文件服务器以及工程师站和 PCS7 服务器等。其中，各主机所含有的漏洞信息如表 1 所列。

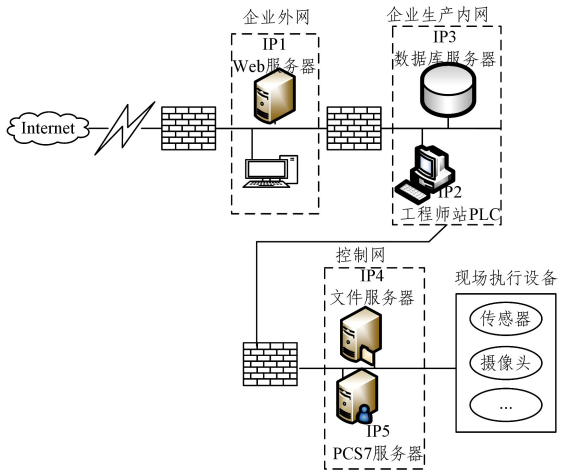

图 4 实验系统网络拓扑结构

Fig. 4 Network topology of experimental system

表 1　漏洞信息表

Table 1　List of vulnerability information

主机	CVEID	攻击描述及后果	攻击可行性
IP1	CVE-2016-0187	HTML 代码执行，实现权限提升	0.73
IP2	CVE-2017-8461	RPC 远程代码执行，可执行任意程序	0.62
IP3	CVE-2015-9098	执行任意 SQL 语句，提升权限	0.91
IP4	CVE-2013-4730	FTP 服务器缓冲期溢出，可执行任意程序	0.98
IP4	0-day-unknown	自动感染插入的任何存储设备	1
IP5	CVE-2016-5743	WinCC 缓冲期溢出，可执行任意程序	0.43

图 4 中，互联网、企业外网、内网和控制网之间通过防火墙进行访问控制，避免恶意访问。攻击者的目标是控制 IP5，通过执行恶意程序代码修改具体的业务控制逻辑，从而破坏物理过程。由于攻击者处于互联网中，其攻击过程需要突破企业外网、内网直至控制网，具体的攻击图如图 5 所示。图 5 和表 1 中的攻击可行性数值由式(8)计算所得。

依据图 5 可知，可能的攻击路径包括：

1) IP1－＞IP2－＞IP5；

2) IP1－＞IP3－＞IP5；

3) IP1－＞IP2－＞IP4－＞IP5；

4) IP1－＞IP3－＞IP4－＞IP5。

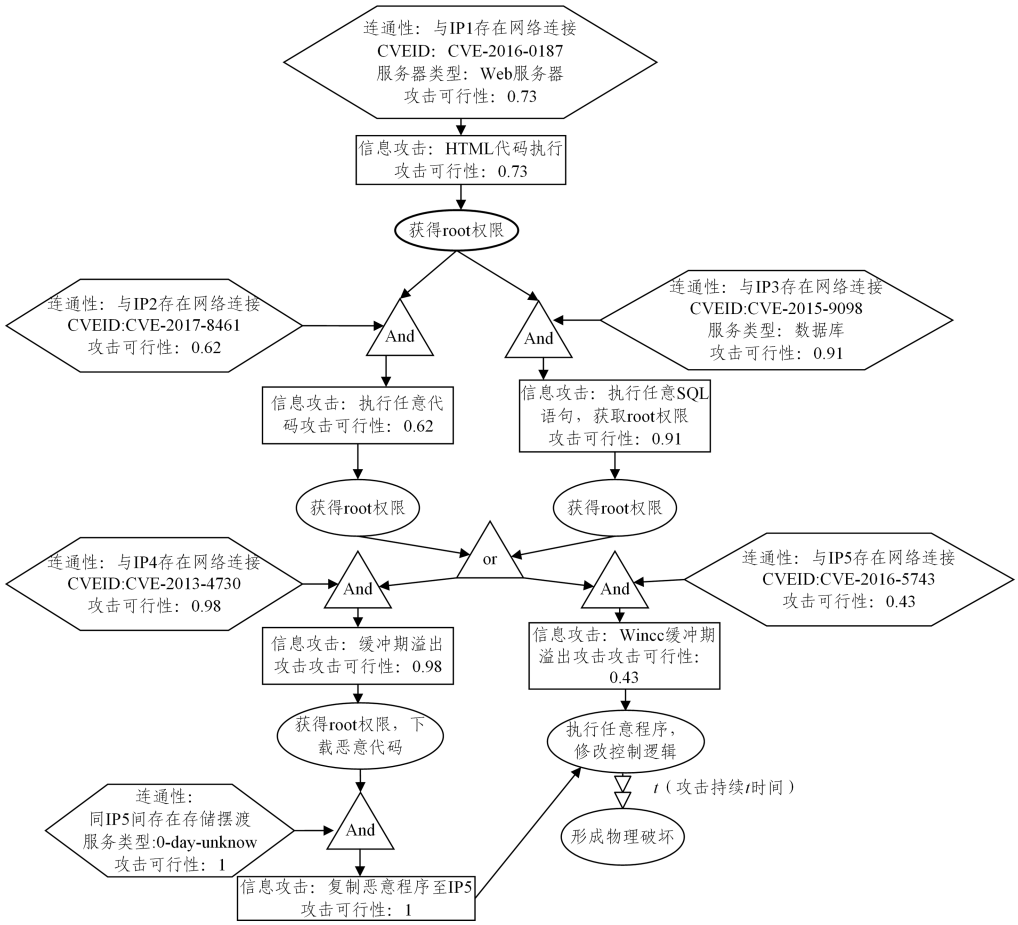

图 5　生成的攻击图

Fig. 5　Generated attack graph

不同攻击路径及渗透测试成功率如表 2 所列。若以最短攻击路径为最优目标，则渗透测试时选择路径 1)或 2)进行。若以最大成功概率为最优目标，则应选择路径 4)，此时攻击节点上的攻击可能性相乘数值最大。

表 2　渗透测试路径及成功概率

Table 2　Penetration testing paths and probabilities of success

序号	攻击序列	路径长度	成功概率
1	IP1－＞IP2－＞IP5	3	0.1946
2	IP1－＞IP3－＞IP5	3	0.2856
3	IP1－＞IP2－＞IP4－＞IP5	4	0.4435
4	IP1－＞IP3－＞IP4－＞IP5	4	0.6510

在某次渗透测试中，假定选择的是最短攻击路径 IP1－＞IP3－＞IP5，但在 IP3 节点上攻击失效。根据算法 1，回退至 IP1 节点，在攻击图中删除 IP3 节点并以最大成功概率寻找 IP1 至 IP5 间的最优路径。最终将攻击步骤调整为：IP1－＞IP2－＞IP4－＞IP5。

结束语　本文针对 CPS 的渗透测试安全评估问题，首先提出一种适用于 CPS 的攻击图建模技术 AGC。与传统攻击图技术相比，AGC 支持服务种类、0-day 漏洞的标识，增加了物理攻击节点、连续值表示以及带时间值的边，增强了攻击图的表达能力，适合 CPS 攻击建模。其次，基于 AGC 攻击图建模，提出最小攻击代价、最短攻击时间等最优攻击路径选择策略，并提出一种基于节点回退的攻击步骤自动调整算法。典型应用实例表明了所提方法的有效性。未来工作包括：研究基于域划分的 CPS 攻击图分布式并行生成算法；提出基于图

节点缩放的攻击图可视化技术等。

参 考 文 献

[1] AYAN B, TRIDIB M. Ensuring Safety, Security and Sustainability of Mission-Critical Cyber-Physical Systems [J]. Proceedings of the IEEE, 2012, 100(1): 283-299.

[2] PENG K L, PENG W, WANG D X, et al. Research Survey on Security Issues in Cyber-Physical Systems [J]. Netinfo Security, 2016(7): 20-28. (in Chinese)
彭昆仑, 彭伟, 王东霞, 等. 信息物理融合系统安全问题研究综述[J]. 信息网络安全, 2016(7): 20-28.

[3] TANG Y, CHEN Q, LI M Y, et al. Overview on Cyber-attacks Against Cyber Physical Power System [J]. Automation of Electric Power Systems, 2016, 40(17): 59-69. (in Chinese)
汤奕, 陈倩, 李梦雅, 等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化, 2016, 40(17): 59-69.

[4] 国家互联网信息办公室. 国家网络空间安全战略[EB/OL]. (2016-12-27). http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

[5] FANG B X, JIA Y, LI A P, et al. Cyber Ranges: state-of-the-art and research challenges [J]. Journal of Cyber Security, 2016, 1(3): 1-9. (in Chinese)
方滨兴, 贾焰, 李爱平, 等. 网络空间靶场技术研究[J]. 信息安全学报, 2016, 1(3): 1-9.

[6] BYES E J, FRANZ M, MILLER D. The use of attack trees in assessing vulnerabilities in SCADA systems [C]// Proceedings of the 2004 IEEE Conference on International Infrastructure Survivability Workshop. Lisbon, Portugal: IEEE, 2004: 210-217.

[7] XIE F, LU T, GUO X, et al. Security analysis on cyber-physical system using attack tree [C]// Proceedings of the 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Piscataway, NJ: IEEE, 2013: 429-432.

[8] DAMODARAN S K, COURETAS J M. Cyber modeling & simulation for cyber-range events[C]// Proceedings of the Conference on Summer Computer Simulation. Chicago, Illinois: Society for Computer Simulation International, 2015: 1-8.

[9] SABALIAUSKAITE G, MATHUR A P. Aligning cyber-physical system safety and security [M]// Complex Systems Design & Management Asia. Springer International Publishing, 2015: 41-53.

[10] LU H K, CHEN D Q, PENG Y, et al. Quantitative research on risk Assessment for information security of industrial control system [J]. Process Automation Instrumentation, 2013, 35(10): 21-25. (in Chinese)
卢慧康, 陈冬青, 彭勇, 等. 工业控制系统信息安全风险评估量化研究[J]. 自动化仪表, 2013, 35(10): 21-25.

[11] WOO P S, KIM B H, HUR D. Towards Cyber security risks assessment in electric utility SCADA systems[J]. Journal of Electrical Engineering and Technology, 2015, 10(3): 888-894.

[12] BOUCHTI A E, HAQIQ A. Modeling cyber-attack for SCADA systems using CoPNet approach [C]// Proceedings of International Conference on Complex Systems. Agadir, Morocco: IEEE Press, 2012: 1-6.

[13] WANG Z G, WEI Q, LIU W W. Quantitative risk assessment of industrial control systems based on attack-tree and CVSS [J]. Application Research of Computers, 2016, 33(12): 3785-3790. (in Chinese)
王作广, 魏强, 刘雯雯. 基于攻击树与 CVSS 的工业控制系统风险量化评估[J]. 计算机应用研究, 2016, 33(12): 3785-3790.

[14] CUI Y, ZHANG L J, WU H. Automatic generation method for penetration test programs based on attack graph [J]. Journal of Computer Applications, 2010, 30(8): 2146-2150. (in Chinese)
崔颖, 章丽娟, 吴灏. 基于攻击图的渗透测试方案自动生成方法[J]. 计算机应用, 2010, 30(8): 2146-2150.

[15] LUAN J, WANG J, XUE M. Automated Vulnerability Modeling and Verification for Penetration Testing Using Petri Nets[C]// International Conference on Cloud Computing and Security. Springer International Publishing, 2016: 71-82.

[16] MAINKA C, SOMOROVSKY J, SCHWENK J. Penetration testing tool for web services security[C]// Proceedings of 2012 IEEE Eighth World Congress on Services (SERVICES). Honolulu, HI, USA: IEEE, 2012: 163-170.

[17] ANTUNES N, VIEIRA M. Penetration testing for web services [J]. Computer, 2014, 47(2): 30-36.

[18] PENG Y, JIANG C Q, XIANG T, et al. Cyber-physical attack modeling and impact on critical infrastructure [J]. Journal of Tsinghua University (Science and Technology), 2013, 53(12): 1653-1663. (in Chinese)
彭勇, 江常青, 向憧, 等. 关键基础设施信息物理攻击建模和影响评价[J]. 清华大学学报(自然科学版), 2013, 53(12): 1653-1663.

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

[20] QIU J, WANG T, YIN S, et al. Data-based optimal control for networked double-layer industrial processes[J]. IEEE Transactions on Industrial Electronics, 2017, 64(5): 4179-4186.

[21] LI H, WANG Y, CAO Y. Searching Forward Complete Attack Graph Generation Algorithm Based on Hypergraph Partitioning [J]. Procedia Computer Science, 2017, 107(C): 27-38.

[22] Common vulnerability scoring system v3.0: specification document[R]. North Carolina: FIRST-Forum of Incident Response and Security Teams, 2015.