# 网络靶场研究现状与关键技术分析

● 王海涛　宋丽华　张国敏　/　陆军工程大学

【摘　要】文章针对大规模实时网络靶场建设和试验中存在的诸多问题，在回顾网络靶场发展现状的基础上对未来网络靶场建设任务中涉及的关键技术进行了系统分析和探讨，介绍了网络靶场提出的背景、作用和挑战，对国内外网络靶场的研究现状进行了较为全面的阐述，进而探讨了构造未来网络靶场急需解决的几个关键技术问题，包括大规模业务流量模拟、流量特征建模、高逼真多样化用户模拟和分布式加载控制架构。最后对全文进行了小结并展望了今后工作方向。

【关键词】网络靶场　信息安全　网络战　人在环中　流量建模

## 1 引言

近年来网络空间的信息安全对确保国家安全起到日益重要的作用，直接关系国家政治、经济、国防和社会发展等方方面面。为了谋取网络空间安全优势，西方发达国家纷纷推出网络空间安全战略并启动国家网络靶场建设计划。网络靶场是一种针对信息安全攻防领域，涵盖领域典型应用场景的网络信息安全科研试验平台或信

息系统，它能为多种行业的各类用户提供逼真的网络安全攻防模拟环境，并可以提供网络空间安全体系规划论证、网络安全防御技术演示验证和体系化安全性评估等服务。

网络靶场是全面衡量信息系统是否安全、安全防御装备是否管用好用、对抗条件下作战任务能否确保的试金石，对创新和发展我国网络空间防御的理论、技术和装备能力将起到关键推动作用。我国目前已经建成一些与网络空间防御相关的靶场，如通信靶场、信息安全测试床、电子靶场等，为通信网络、电子防御装备、指挥控制系统的安全能力测试提供了有效保障。随着国家对信息系统防御能力的要求增加，对网络空间防御靶场的建设和试验也面临新的任务：（1）从信息基础设施试验向网络化信息系统体系化试验发展，参试要素体系性更强、规模更大；（2）从信息系统“注入式”功能性试验向“人在环中”的效能试验方向发展，更强调被试系统在接近实战环境下的实际效能测试；（3）从确定型预先编排式试验向“非预期”的事件驱动型试验方向发展，尽量真实反映“不确定性”和“复杂性”。

上述网络靶场发展的新方向决定了大规模网络系统试验过程中，各信息节点上需要大量的“人机交互”，以实现高逼真的业务流量和用户行为仿真。但目前仍存在以下问题：（1）组织成本大、效率低、涉及范围广，难以重复高效地开展试验；（2）真实人之间存在（技能、决策等方面）的差异性，难以建立统一的量化标准，导致试验的结果难以预测。为此，采用“标准化”的“仿真人”在大规模靶场试验中的作用更加实用，通过对“模拟用户”行为进行描述并开展可控的行为仿真试验成为更可行和有效的方法。

## 2 国内外研究现状分析

### 2.1 国外研究现状

近年来，发达国家均将网络靶场建设作为支撑网络空间安全技术演示验证、网络武器装备研制试验、攻防对抗训练演练和网络风险评估分析的重要支撑平台。目前，美国依然处于领头羊地位，已开展了国家级的网络靶场建设。英国和德国等也正在建设自己的国家网络靶场，靶场的任务类型主要包括训练、演习及测试与评估3类。

2008年美国启动了国家网络靶场（National Cyber Range，NCR）项目，NCR的目标是提供虚拟环境来模拟真实的网络攻防作战，针对敌对电子攻击和网络攻击等电子作战的手段进行试验，以实现网络空间作战能力的重大变革，打赢网络战争。美国NCR原型系统的体系结构如图1所示。

NCR部署了流量产生器，提供模拟整个网络活动的能力，产生代表性的网络流量。同时，该靶场还能够模拟各种人员角色（系统用户、管理员、对手和中立方等），提供靶场各节点上人类行为的模拟能力，可产生人类之间真实的系列事件，复制角色可驱动桌面环境的各种应用程序，复制角色可与验证系统进行交互，如身份认证系统等。

美国国防部的信息保障靶场IAR通过使用系统管理员模拟训练系统（SAST）来模拟目标环境。SAST中内含一个网络流量合成套件（ANTS），其中的多用户流量工具（MUTT）插件部署在ANTS之上以描述用户，并产生行为仿真。基于文本界面的邮件客户端（MUTT）合成了电子邮件客户、网页客户和SSH客户等的行为流量。

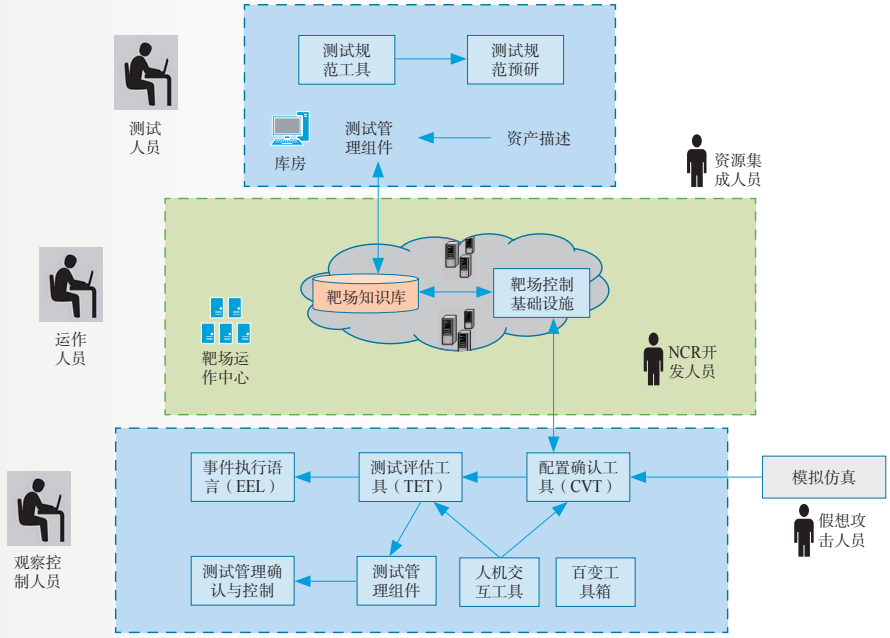


**图1　国家网络靶场原型系统的体系结构**

2010年，英国国防部宣布成立英国联合网络靶场。联合网络靶场可以与其他网络设施进行组网，是英国第一个可以用于商业用途的网络靶场。尽管从外表上看联合网络靶场类似一个企业数据中心，但它拥有可实现网络靶场各种关键能力的专用软硬件。而且，联合网络靶场可以对某些无法在实际系统上测试的事情进行试验。联合网络靶场的用途包括体系结构评估、组件测试、研发和训练4个方面。联合网络靶场可以为网络行动提供高度可控的测试和训练环境，并通过可配置的网络体系结构来开展灵活的通信业务。

在企业层面，BreakingPoint公司研发了包括业务流量模拟产生器（CTM）、Strike Pack网络安全和恶意代码攻击模拟系统在内的网络靶场相关设备和产品。其中，CTM系统具有模拟上百万互联网用户环境下真实网络应用与安全事件的能力。Strike Pack可模拟4500种攻击行为和28000多种恶意代码攻击。目前，相关产品已经应用于DISA以模拟真实用户流量，仿真MPLS和IPv6。

## 2.2 国内研究现状

与美英等发达国家相比，我国网络靶场建设目前处于起步阶段，仅有部分科研实验室和行业专用试验场等，其主要功能是研究电子信息对抗与仿真技术、对行业产品进行试验及检测等。从体系应用角度来讲，我国现有网络试验环境或测试床规模较小，且主要针对某一专业领域，尚不适用于体系化的网络空间安全科研试验与测试评估。在国家网络靶场建设方面，无论从靶场基础理论研究、关键技术和产品研发，还是网络空间安全风险评估研究，我国都存在不小差距。

随着政策扶持和资金投入的加大，近几年我国在网络靶场上的研究和应用发展势头迅猛。目前，国内部分高等院校、科研院所等单位已研制搭建了初具规模的

网络安全试验模拟平台，开展了小规模的网络对抗训练、演习等，建立了可支持试验和评估网络对抗能力、网络武器攻防效果和人员训练的相关试验平台，可支持部署网络防护类、保障类等装备，还能模拟大规模的复杂网络环境。

但是，目前国内网络试验与仿真平台普遍采用的业务流量发生器仍存在以下问题：（1）缺乏对军用网络业务的准确建模和分析，所产生的流量难以反映真实军用网络环境中的流量模式，影响了试验结果的准确性；（2）缺乏用户行为层面的建模分析和仿真技术，难以在网络靶场中反映典型用户行为对试验结果的影响；（3）缺乏大规模仿真场景的支持能力，限于所采用的仿真模型和流量生成机制的限制，难以支持百万级别的数据流并发生成能力；（4）缺乏一种灵活有效的仿真任务和资源的定义、调度和管控手段，导致难以在上层任务需求和底层仿真资源之间进行高效映射调度，难以根据仿真进度和仿真脚本动态调整仿真场景等。

## 3 关键技术问题分析

未来网络靶场的发展方向决定了大规模网络系统试验过程中，各信息节点上需要大量的“人机交互”，以实现高逼真的业务流量和用户行为仿真。网络靶场的核心技术之一是构建大规模仿真支撑平台，以承载大规模的用户业务流量以及多种多样的用户行为的动态组合。待解决的关键技术问题包括：（1）大规模业务流量模拟；（2）流量特征建模；（3）高逼真多样化用户模拟；（4）分布式加载控制架构。

### 3.1 大规模业务流量模拟

当前，模拟生成网业务流量的方法和技术大致有两种：（1）流量回放：即使用网络工具，如Sniffer，对某个实际网络中的数据包进行捕获，并将结果记录在日志文件中。当需要在一个新的网络环境中生成业务流量时，就以该日志文件为基础，通过流量回放的方式将捕获的数据包注入新的网络中，实现业务流量的生成。该方法生成的网络流量是真实网络环境中的业务流量，但不足之处是，这些业务流量及其用户只是在某个时段（流量捕获期）、某个或某些已有的特定网络的业务流量，其用户行为模式和业务流量特征并不能适应每个网络的条件和特征。（2）基于业务流量特征和用户行为模型来生成网络流量。网络中的业务流量呈现一定的特征，并可用一些数学模型来刻画，如泊松过程和自相似模型等，然后相应的流量生成工具可以这些模型为基础，模拟生成总体业务流量。这种方法可以针对不同网络环境，通过调节模型中的参数，如数据包到达速率，以适应特定的网络环境和需求。但是，流量模型仅能从宏观上考虑网络业务应用使用的状况和特征，通常只能反映网络中所有用户的整体访问结果，难以体现微观层面上每个用户的行为特征。从微观层面来看，每个用户的网络访问行为才是网络业务应用的根本，而流量特征只是所有用户独立访问网络行为结果的叠加。因此，近年来许多学者开始研究基于用户行为模型的流量生成方法和相关算法：即根据用户行为模型，研究规模化的模拟用户在各自独立访问业务应用时的流量生成方法及其相关算法。

### 3.2 流量特征建模

流量模型是流量行为特征的数学近似，网络流量建模的基本原则是以流量的重要特性为出发点，设计流量模型以刻画

实际流量的突出特性。从理论角度来看，网络业务流的数学模型提供了对流量特性简明的、抽象化的描述，其价值在于能够提取出网络流量的一些重要特性，并给出明确的量化表示。随着网络规模的扩大和网络服务应用数量的激增，建立一个能够准确、有效描述网络流量特性的流量模型成为富有挑战的任务。按照不同时段，流量模型相关研究可分为传统模型、自相似模型和新型模型，当前网络流量公认的重要统计特征是大时间尺度下的自相似性和小时间尺度下的多分形性。这些特性不仅存在于互联网络中，同时也存在于Ad Hoc网络和卫星网络中。

此外，针对IPv6的流量特征，业界也进行了大量分析和研究，通过自相似、自相关以及功率谱密度方法，发现IPv6与IPv4流量特征都具有重尾和自相似特性，并且是长距离依赖的和自相关的，具有突发特性。但是，IPv6相比而言具有较为明显的重尾特性以及更高的Hurst参数值和分形维数。IPv4流量的数据包长，数据包平均间隔时间基本服从对数正态分布；IPv6的数据包大小基本服从Logistic回归模型，其数据包间隔时间基本服从Weibull分布。

### 3.3 高逼真多样化用户模拟

用户行为模型是利用多学科知识研究和分析网络用户的构成、特点及其在网络应用过程中行为活动所表现出来的规律。网络用户行为是一个广义的概念，它属于网络信息知识发现的范畴。通过全面了解并熟悉用户的访问行为，才能更好地理解网络流量构成和变化情况，发现用户的异常行为。用户行为分析是进行流量仿真的重要依据，尤其是进行大规模网络流量仿真时，对大量用户的网络流量数据进行建模，了解用户流量特征具有重要意义。

目前这方面的主要工作是对网络用户及其行为进行归类和分析。由于网络中庞大的用户群体和复杂的应用环境等因素，导致目前的研究多是针对特定应用场景或者服务类型进行讨论，难以用完整统一的行为模型进行刻画。另一方面，现阶段的用户行为分析大都是在收集数据的基础上，通过统计分析、聚类分析、关联数据分析、时序数据挖掘、神经网络等方法对用户数据进行拟合进而预测用户行为，所以当前主流数据分析方法的效果与数据本身的特点是密不可分的。

除了常见的HTTP访问遵循简单的请求和返回资源模式，更多网站则是基于工作流的工作模式。工作流要解决的主要问题是：为实现某个业务目标，在多个参与者之间，利用计算机按某种预定规则自动传递文档、信息或是任务。工作流管理系统的主要功能是通过计算机技术的支持去定义、执行和管理工作流，协调工作流执行过程之间以及群体成员之间的信息交互。用户行为则需要根据工作流系统背景进行定义和仿真。

### 3.4 分布式加载控制架构

对于分布式加载控制架构，目前主要采用基于策略的调度机制。分布式并行技术的核心在于设计良好的分布式并行调度算法。在分布式实时系统领域，目前已有一些较为可行的调度理论和方法。例如，SymTA/S是基于Holistic调度分析方法的扩展，使用了标准事件模型来耦合分布式系统各个组件之间的联系，从而支持在系统级进行调度分析；实时演算（real-time calculus）是基于网络演算（network calculus）的扩展，通过建立合适的任务

到达曲线和系统服务曲线来对任意模式的事件流进行建模，从而不再局限于将非周期事件流近似估计为带最小到达间隔时间的事件流。

策略管理（Policy Based Management，PBM）是指一种用于管理网络和分布式系统的方法，它把系统的管理逻辑和应用逻辑相分离，并将管理逻辑表示为控制系统行为选择的策略。策略可以动态部署、更新或删除，因此，可以在不改变软件编码或停止系统运行的前提下，通过改变策略来支持系统行为的动态适应，这意味着可以通过动态更新由分布式实体解释的策略规则来改变它们的行为。基于策略的管理已在访问控制、数据备份、网络安全、资源提供、配置检查和服务规划等领域得到了应用。通过基于策略的管理系统，管理员无需逐个手工配置网络设备或应用资源，通过预定义的策略来实施业务规则和目标，从而提高了管理效率。

## 4 结语

网络靶场是支持网络空间信息安全攻防能力研究和信息化武器装备验证的试验床。本文对网络靶场的起源和发展进行了说明，梳理了国内外网络靶场的研究现状，并探讨了建设未来网络靶场急需解决的几个关键技术问题。当前，网络靶场对于我国仍属于新事物，需要突破网络防御、测试、评估等相关技术难题，还要密切关注网络靶场的研究热点，包括网络空间安全自动化多维度测试技术、面向任务的靶场引擎构建技术、靶场资源自动配置与快速释放技术以及靶场安全隔离与网络追踪溯源技术等。

参考文献

[1] 周芳，周正虎．国外信息保障靶场建设 [J]. 指挥信息系统与技术，2013,4(01):5~8.

[2] 周芳，毛少杰，朱立新．美国国家赛博靶场建设 [J]. 指挥信息系统与技术，2016(05):5~9.

[3] 吴巍．赛博空间与通信网络安全问题研究 [J]. 中国电子科学研究院学报，2011,6(05):473~476.

[4] 刘鹏．网络用户行为分析的若干问题研究 [D]. 北京：北京邮电大学，2015.

[5] C. Jaiswal Rupesh and D. Lokhande Shashikant, Measurement, Modelling and Analysis of HTTP Web Traffic[J].International Conference on Communication and Computing, 2014.

[6] 李立耀，孙鲁敬，杨家海．社交网络研究综述 [J]. 计算机科学，2015(11): 8~21, 42.

[7] Hamann A, Henia R, Racu R, Jersak M, Richter K, Ernst R. SymTA/S-Symbolic timing analysis for systems[C]. WIP Proc. of the 16th ECRTS. Catania: IEEE Press, 2016:17~20.

[8] 刘巍峰．基于框架模式的工作流程网站设计与实现 [D]. 长春：吉林大学，2018.

[9] Dimmock N. Belokosztolszki A. Eyers D. et al. Using Trust and Risk in Role-based Access Control Policies[C].In Proceedings of the Ninth ACM Symposium on Access Control Models and Technologies, 2009.