文章编号：2095-2163(2021)04-0001-04 中图分类号：TP392 文献标志码：A

面向网络空间靶场的网络行为模拟关键技术研究

刘红日，吕思才，王佰玲
（哈尔滨工业大学（威海）计算机科学与技术学院，山东 威海 264209）

摘 要：在网络空间靶场中构建真实的网络场景，是开展科学研究以及网络攻防研究的基础条件，而在靶场环境下对真实的网络行为模拟，是构建网络场景的主要技术之一。本文针对网络靶场下，模拟真实网络流量的要求，提出了目标网络下多节点网络流量回放算法；针对群体用户的 web 行为无法直接获取和分析的问题，研究了基于网络流量内容的群体用户 web 行为主题分析方法，使模拟出的群体用户 web 行为符合人类动力学规律；针对目前的个体用户行为模拟方法单一，不能模拟出用户应用行为过程的问题，研究了多层次的个体用户应用行为模拟技术。

关键词：网络空间靶场；背景流量模拟；前景流量模拟；网络靶标模拟；流量行为；用户应用行为

Research on Key Technologies of Network Behavior Simulation for Cyber Range

LIU Hongri, LV Sicai, WANG Bailing
(School of Computer Science and Technology, Harbin Institute of Technology (Weihai), Shandong 264209, China)

【Abstract】 Building a real network scenario in a cyberspace range is the basic condition for network attack and defense drills, and scientific studies, while real network behavior simulation in a cyber range is one of the main techniques for building a network scenario. To satisfy the requirements of real network traffic replay in a cyber range, this paper proposed a multi-node network traffic replay algorithm. This paper studies the topic analysis method of collective user web behavior based on network traffic content, which is used to solve the problem that a collective user web behavior cannot be directly analyzed. It makes the simulated result of collective user web behavior follows to the laws of human dynamics. The current simulation method of individual user behavior is too simple to realistically simulate the process of individual user application behavior, a multi-level application behavior simulation technique for individual user is studied.

【Key words】 Cyber range; network background traffic simulation; Network foreground traffic simulation; Network target simulation; Network traffic behavior; User application behavior

0 引 言

随着计算机及网络技术的不断发展，网络安全形势也日益严峻。据互联网安全协会发布的《2018 年网络安全事件和数据泄露趋势报告》，2018 年共有超过 200 万起网络安全事件，至少造成 450 亿美元的经济损失。网络环境由互联发展到了泛在网络空间，网络安全事件已经变成网络攻防常态化下的产物。面对越来越复杂的网络环境和愈演愈烈的网络安全事件，为了进行网络攻防演练以及网络新技术验证，世界大国和有影响力的地区组织已率先开展了网络靶场（Cyber Range）的建设[1]。

众多研究人员和机构在网络流量模拟方面取得了很多成果，产生了很多成熟的流量产生器。例如 Netperf[2] 和 iPerf[3] 等流量产生器，以及商用仿真软件 OPNET 和科研用仿真软件 NS2 及 NS3 等。尽管上述流量产生器及仿真软件在网络设备的性能检测及网络仿真方面发挥了巨大作用，但由于上述网络流量模拟技术主要是为测试网络设备和网络环境而设计的，其注重于高速、大流量、高带宽，而在网络行为的仿真模拟方面能力受限，难以保证模拟网络节点的逼真度以及网络用户行为复制的逼真度，无法满足在网络空间靶场环境下对真实应用场景完成较精准构建的需求。

本文以实现逼真地模拟真实的互联网行为为目标，从流量模拟和用户的应用行为模拟出发为切入点，研究网络空间靶场虚拟网络环境下的网络行为模拟技术。在流量模拟方面，研究了多节点交互式网络流量回放技术，实现多节点网络环境下的流量回放；在应用行为模拟上，分别研究了群体用户和个

基金项目：国家重点研发计划“网络空间安全”重点专项（2016YFB0800802）；山东省重点研发计划（2016ZDJS01A04，2017CXGC0706）。
作者简介：刘红日（1982-），男，博士，助力研究员，主要研究方向：网络空间靶场；吕思才（1997-），男，硕士研究生，主要研究方向：入侵检测；王佰玲（1978-），男，博士，教授，主要研究方向：网络与信息安全。
通讯作者：王佰玲 Email：wbl@hit.edu.cn
收稿日期：2020-07-29

体用户的应用行为模拟方法,实现了不同层次、不同粒度的应用行为模拟,以满足靶场环境下网络应用场景的构建需求。

1 相关研究介绍

现有的网络行为模拟分类成果可以分为流量行为模拟和用户行为模拟。其中流量行为模拟,按照流量的生成方法,又可以分为如下几种:

(1)基于模型(model-based)的流量生成法。基于网络流量的数学统计模型,通过测量真实网络流量特征来设置模型的参数,生成网络流量。典型的模型有泊松模型、马尔科夫模型,重尾分布的 ON/OFF 源聚集模型[4]、M/G/∞排队模型[5]等。这些模型大部分建立在较强的假设基础之上。例如,泊松模型假设网络事件是独立分布的,但实际的网络事件并不满足这些假设。

(2)基于跟踪(trace-based)的流量生成法。使用已有的真实的网络流量,通过"录制—回放"的方式,实现网络流量的再现。通常使用 TCPDum 等工具对真实的网络流量进行录制,通过 TCPReplay[6]、TCPivo[7]等流量工具进行回放。

(3)基于预测(prediction-based)的流量生成法。根据网络流量在统计上的自相似性和长相关的性质[8],利用现有的网络流量来预测,进而生成新的网络流量。

按照模拟的粒度进行分类,可以分为包级(packer-level)模拟[9]、流级(flow-level)模拟[10]和应用级(application-level)模拟[11]。包级和流级模拟通过构造包的长度和包的到达时间间隔的流量模拟,不研究包之间及流之间的关联关系,适用于网络出口的流量模拟,不能直接用在对网络内每个节点的流量模拟。应用级模拟通过模拟用户操作应用程序来产生流量,是一种更接近真实用户行为的模拟。

在用户行为上,研究用户网络行为,有助于从用户的角度来分析流量产生的机制,进而分析出用户网络行为的规律,为用户网络行为建模及行为模拟提供理论依据。用户行为区别主要体现在操作对象上,按照操作对象的不同,可以分为 web 应用、邮件应用、桌面应用等。

用户的行为从规模上可以分为群体行为和个体行为。个体用户行为主要是通过个人的网络行为产生日志来进行分析。如,鼠标、键盘的动力学特征[12];群体用户行为分析主要是从人类动力学角度,对用户行为进行特征分析,并分析其产生的机制[13]。

2 网络流量回放

在网络测试床和网络靶场中,流量回放被用来生成背景流量和再现网络场景,是网络安全试验不可缺少的支撑技术。通过从真实的网络中捕获流量并在实验中进行回放,可以在网络测试床中生成背景流量,并在网络靶场上再现真实的网络场景。实现点到点流量回放的工具有 TCPreplay、TCPivo 等。然而,这些工具只处理单机到单机的回放,并不能处理多节点到多节点的交互。本文提出多节点流量回放模型,如图 1 所示。

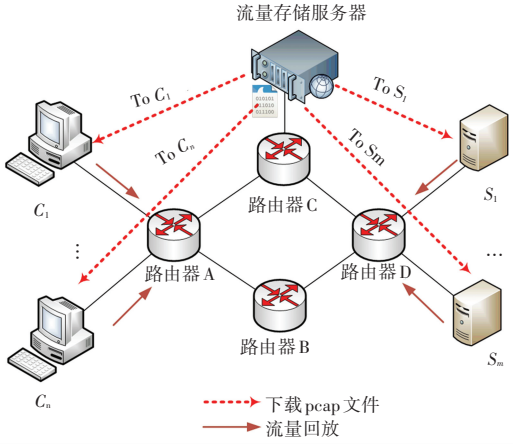

图 1 多节点网络流量回放模型

Fig. 1 The traffic replay model for multi-node network

将多节点流量回放抽象为一个模型,原始流量(pcap 文件)从网管交换机中抓取并存储在存储服务器中。按照流量的源地址将流量分为两类:一类是客户机流量,另一类是服务器流量。假设本地计算机(客户机)为 c_1, …, c_n,远程计算机(服务器)为 s_1, …, s_m。$c_i(i = 1, 2, \cdots, n)$ 和 $s_j(j = 1, 2, \cdots, m)$ 从存储服务器下载 *pcap* 文件后,保持原有的交互关系,实现流量回放。该模型实现了:

(1)IP 映射。目标网络中的 IP 与原始流量文件中的 IP 不同,同时原始流量文件中的 IP 数量要多于目标网络中的 IP 数量。因此,需要将原始流量中的 IP 映射到目标网络中的 IP 上。

(2)流量规约。由于有限的硬件资源,在目标网络的服务器数量比在真实网络中的数量少得多。因此,需要将真实网络中服务器流量进行规约,并将规约的流量分配给指定数量的服务器。要解决的问题是如何将所有的服务器流量平均分配到指定数量的服务器中的同时保持原有的交互关系。

(3)低延迟交互。部署在操作系统上的 agent 转发原始流量的负载实现流量回放,其需要尽可能

与原始网络中 IP 的节点保持时序一致。

3　用户行为模拟

3.1　群体用户行为模拟

本文基于人类动力学规律，给出一种基于 agent 的大规模用户网络 web 行为模拟方法。该方法将个体用户建模为一个独立的 agent，多个 agent 构成了一个虚拟的社交网络。在这个虚拟社交网络上，研究基于 SIR 模型的感染消息传播机制，去驱动 agent 的网络行为模拟，最终使群体用户的 web 行为时间间隔服从幂律分布。基于 SIR 模型的 web 行为模拟算法（s-SIR）如算法 1 所示。

算法 1　s-SIR 群体用户 web 行为模拟算法

Algo. 1　collective user web behavior simulation algorithm based on SIR model

Input：

a virtual social network $G = (V, E)$, where v_i is the susceptible agent and e_i is the connection. A collection $\{ < v_i, t_i, p_i > | i = 1, \cdots, n \}$, where v_i is the agent name, t_i is the waiting time of v_i from being infected to performing web behavior simulation and p_i is the probability of being infected.

Output：

The web behavior simulation of collective user.

Begin

1. random select an agent v_i as the first infected agent;
2. v_i waits for t_i length of time and then perform web behavior simulation;
3. for each uninfected neighour of v_i, denoted as v_j do
4. v_i infect v_j with probability $p_j (j = 1, \cdots, k$, where k is the number of susceptible neighbor agents);
5. if v_j is infected then jump to 2; end if
6. end for
7. if v_j is all infected then v_i becomes a recovered agent; endif

End

基于 s-SIR 算法来驱动每一个 agent 在指定的时间间隔进行 web 行为模拟，最终使全部用户的 web 行为的时间间隔符合幂律分布，以实现群体用户 web 行为的模拟。

3.2　个体用户行为模拟

用户操作应用软件的行为一方面可以为网络空间靶场产生前景流量，另一方面为靶场中的网络攻防演习提供比较真实的靶标。用户操作所有的软件，本质上是鼠标对屏幕特定位置的点击、拖拽以及敲击键盘中特定按键等动作，将这些操作定义为微观行为。用户对某个应用软件的使用，建立在对软件功能的理解基础上，通过鼠标和键盘对功能的操作，实现了对应用软件的操作，将用户操作单个应用的行为称为中观行为。为了完成一项任务，用户通常是通过操作一系列应用软件，形成应用操作序列来实现任务目标，将用户行为序列称为宏观行为。

在微观行为上，根据鼠标移动的起点和终点坐标的元数据，采用归一化方法匹配已采集的用户鼠标数据，找到最优模板后进行轨迹拟合，生成本次鼠标移动轨迹，最后通过消息插入的方式模拟出鼠标的移动动作，其步骤如下：

3.2.1　静态匹配的鼠标模板生成

通过录制用户鼠标的行为，存储用户的移动轨迹，构建用户鼠标行为数据库。通过比较待模拟的距离 d_0 和角度 a_0，与模板库中待匹配鼠标轨迹的距离 d_i 和角度 a_i 的距离公式(1)，来确定命中的模板 $fitL$。

$$fitL = \arg_{(x,y,t)} (\min (d_0 - d_i)^2 + (a_0 - a_i)^2) \quad (1)$$

其中，$fitL = \{(x_1, y_1, t_1), (x_2, y_2, t_2), \cdots\cdots, (x_n, y_n, t_n)\}$，是 n 个鼠标消息记录。

3.2.2　动态拟合的鼠标轨迹生成

待模拟操作鼠标移动的起止点与 $fitL$ 不重合，需对 $fitL$ 进行轨迹拟合。轨迹拟合操作包括：

(1)坐标平移：使待模拟操作的起始点平移到模板序列起点位置；

(2)坐标伸缩：保证鼠标模拟操作的起止点与命中模板的起止点的直线距离相等；

(3)坐标旋转变换：使模板的起止点的水平夹角与待模拟操作的起止点的水平夹角方向一致；

(4)时间补偿：命中模板的坐标进行缩放，移动的时间也发生了变化，需修正。

通过以上静态匹配和动态拟合，可以生成鼠标模拟的移动轨迹。

在中观行为上，基于 agent 进行用户单应用行为模拟。agent 通过强化学习方法来学习某个软件的功能，生成软件行为知识库。在模拟用户操作软件行为时，通过从知识库获取 agent 学到的软件功能菜单的操作序列，来实现软件行为的模拟。

Agent 通过强化学习，可在形成软件的各个状

态和动作之间建立逻辑连接(知识),将知识存储在数据库中,构建知识库。进行行为模拟任务时,检索知识库进行知识回忆,通过 Windows 消息驱动和 OCR 驱动混合实现行为模拟。

在宏观行为上,基于序列预测,实现了用户连续多应用软件行为模拟。借助于生成式对抗网络(Generative Adversarial Networks, GAN)在本文生成方面的优势,提出了基于 SeqGan[14] 的用户软件行为序列生成算法。将用户使用的软件进程(一个软件对应一个进程名称)进行统一编码,用户在一段时间内使用的软件构成一个序列,该序列被定位为输入样本。算法的目的是生成用户新的行为序列,作为用户未来的行为序列,如图 2 所示。

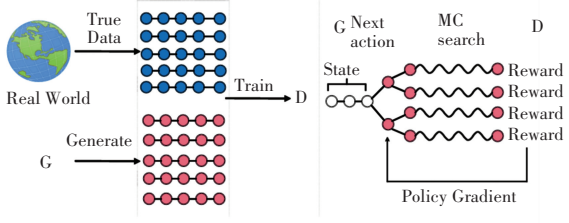

图 2 SeqGan 示意图

Fig. 2 SeqGan schematic

图 2 中,左侧输入的数据为用户操作的软件编号,D 和 G 分别代表判别器和生成器, D 通过真实数据和 G 的生成数据进行训练。在图的右侧,G 由 policy gradient 训练,其中最终的奖励信号由 D 提供,并通过蒙特卡洛搜索传递回途经的动作价值。已经存在的白色圆点称为现在的状态(state),要生成的下一个白色圆点称作动作(action)。因 D 需要对一个完整的序列评分,所以用 MCTS(蒙特卡洛树搜索)将每一个动作的各种可能性补全,D 对这些完整的序列产生 reward,回传给 G,通过增强学习更新 G。用强化学习的方式,训练出一个可以产生下一个最优的 action 的生成网络。生成器为强化学习中的 agent,状态是生成的 token,动作为下一个生成的 token,利用蒙特卡洛搜索去估计状态行为值,策略梯度去训练梯度。

4 结束语

本文针对网络靶场中的网络行为模拟进行研究,将网络行为抽象建模,从用户行为和流量行为两个方面来模拟网络行为,实现网络场景的背景流量模拟、前景流量模拟和靶标模拟。在流量模拟方面,提出了多节点交互式流量回放算法,实现了录制流量在靶场中的逼真回放;在用户行为模拟方面,提出了粗粒度的群体用户行为模拟和细粒度个体用户行为模拟,又进一步对个体行为模拟从模拟层次上提出了宏观行为模拟、中观行为模拟和微观行为模拟,研究了 3 种层面用户行为模拟的算法。

未来工作中,在流量回放上可以围绕流量回放资源计算问题展开,计算出回放需要的最少资源,这对于未来进行大规模的网络攻防演习具有极高的应用价值;在用户行为建模上,目前研究的用户行为模拟是从个人细粒度行为的模拟,没有区分出用户在组织中的角色,可以从网络攻防演练下的用户角色的建模方法进行深入研究。

参考文献

[1] 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.

[2] CS.KENT. Netperf Manual[EB/OL]. http://www.cs.kent.edu/~farrell/dist/ref/Netperf.html 2020[04.01]

[3] WISCONSIN - MADISON U O. IPERF[EB/OL].https://kb.wisc.edu/uwsysnet/page.php? id=41947

[4] Willinger W, Taqqu M S, Sherman R, et al. Self-similarity through high-variability: statistical analysis of ethernet LAN traffic at the source level [J]. ACM SIGCOMM Computer Communication Review, 1995.

[5] KRUNZ M, MAKOWSKI A M. Modeling video traffic using M/G//spl infin/ input processes: a compromise between Markovian and LRD models [J]. IEEE Journal on Selected Areas in Communications, 1998, 16(5): 733-48.

[6] TCPREPLAY. Tcpreplay - Pcap editing and replaying utilities [EB/OL].https: //tcpreplay.appneta.com/

[7] FENG W, BEZZAZ A, FENG W, et al. NetVCR: a high-performance packet replay engine [M]. 2002.

[8] BERAN J, SHERMAN R P, TAQQU M S, et al. Long-range dependence in variable-bit-rate video traffic [J]. IEEE Transactions on Communications, 1995, 43(234): 1566-79.

[9] DYMORA P, MAZUREK M, STRZALKA D. Computer network traffic analysis with the use of statistical self-similarity factor [J]. Annales Umcs, Informatica, 2013, 13(1): 69-81.

[10] SOMMERS J, BARFORD P. Self-Configuring Network Traffic Generation[C]// Proceedings of the 2004 ACM(Association for Computing Machinery) SIGCOMM Internet Measurement Conference(IMC 2004). University of Wisconsin - Madison, 2004:68-81.

[11] MOLNÁR S, MEGYESI P, SZABÓ G. Multi-functional traffic generation framework based on accurate user behavior emulation [C]// Computer Communications Workshops. IEEE, 2013.

[12] SHEN C, CAI Z, GUAN X, et al. User authentication through mouse dynamics [J]. IEEE Transactions on Information Forensics and Security, 2012, 8(1): 16-30.

[13] GYARMATI L, TRINH T A. Measuring user behavior in online social networks [J]. IEEE Network, 2010, 24(5): 26-31.

[14] YU L, ZHANG W, WANG J, et al. Seqgan: Sequence generative adversarial nets with policy gradient//[C] proceedings of the Thirty-First AAAI Conference on Artificial Intelligence, F, 2017.