Journal of System Simulation

Volume 32 | Issue 3 Article 9

3-25-2020

Research of Link Acquisition Technology for Virtual-reality Network

Liu Yuan
1. School of Digital Media Institute, Jiangnan University, Wuxi 214122, China;;

Xingbing Feng
1. School of Digital Media Institute, Jiangnan University, Wuxi 214122, China;;

Xiaofeng Wang
2. School of Internet of Things Engineering, Jiangnan University, Wuxi 214122, China;

Zhaohong Deng
1. School of Digital Media Institute, Jiangnan University, Wuxi 214122, China;;

Research of Link Acquisition Technology for Virtual-reality Network

Abstract

Abstract: Network simulation is an important foundation for the cyberspace shooting range, where the data acquisition and evaluation for the emulation network is its key link. Based on the emulation network formed by OpenStack, a distributed link data acquisition system for the diversified emulation links is constructed. The paper studies the collaborative acquisition technology and the efficient link data acquisition technology of 3 kinds of links, such as the virtual link in the host, the virtual link between the host and the virtual-reality link, and the evaluation technology based on the link data. Experiments show that the proposed method improves the acquisition rate by 88.48% compared with the traditional method, and reduces the CPU usage by 45.29%. For a typical LDDoS scenario, the proposed method can collect the required link data and evaluate the effect of LDDoS.

Keywords

network emulation, link data acquisition, effect evaluation, network security test

第 32 卷第 3 期 系统仿真学报© Vol. 32 No. 3
2020 年 3 月 Journal of System Simulation Mar., 2020

面向虚实互联网络的链路采集技术研究

刘渊[1]，冯兴兵[1]，王晓锋[2]，邓赵红[1]
（1. 江南大学 数字媒体学院，江苏 无锡 214122；2. 江南大学 物联网工程学院，江苏 无锡 214122）

摘要：网络仿真是网络空间靶场的重要基础，面向仿真网络的数据采集与评估是关键环节。基于 OpenStack 复现形成的仿真网络，构建面向多样化仿真链路的分布式链路数据采集系统。*研究面向宿主机内、间的虚拟链路和虚实互联等 3 类链路的协同采集技术、高效链路数据采集技术以及基于链路数据的效果评估技术。*实验表明：所提方法在采集速率上相对于传统方法提升了 88.48%，在 CPU 占用率上降低了 45.29%；面向典型的 LDDoS 场景，可采集所需要的链路数据，并进行 LDDoS 的效果评估。

关键词：网络仿真；链路数据采集；效果评估；网安试验
中图分类号：TP393.08 文献标识码：A 文章编号：1004-731X (2020) 03-0421-09
DOI: 10.16182/j.issn1004731x.joss.18-0218

Research of Link Acquisition Technology for Virtual-reality Network

Liu Yuan[1], *Feng Xingbing*[1], *Wang Xiaofeng*[2], *Deng Zhaohong*[1]
(1. School of Digital Media Institute, Jiangnan University, Wuxi 214122, China;
2. School of Internet of Things Engineering, Jiangnan University, Wuxi 214122, China)

Abstract: Network simulation is an important foundation for the cyberspace shooting range, where the data acquisition and evaluation for the emulation network is its key link. Based on the emulation network formed by OpenStack, a distributed link data acquisition system for the diversified emulation links is constructed. *The paper studies the collaborative acquisition technology and the efficient link data acquisition technology of 3 kinds of links, such as the virtual link in the host, the virtual link between the host and the virtual-reality link, and the evaluation technology based on the link data.* Experiments show that the proposed method improves the acquisition rate by 88.48% compared with the traditional method, and reduces the CPU usage by 45.29%. For a typical LDDoS scenario, the proposed method can collect the required link data and evaluate the effect of LDDoS.

Keywords: network emulation; link data acquisition; effect evaluation; network security test

引言

随着网络空间对抗形势日趋严峻，网络攻防已成为各国网络攻防对抗研究的主要内容[1]，建立网络靶场是网络攻防研究的一个重要手段。网络靶场是针对网络攻防演练和网络新技术评测的重要基础设施，可以用来提高现实网络和信息系统的稳定性、安全性和可靠性。网络靶场涉及大规模网络仿真、网络流量/服务与用户行为模拟、试验数据采集与评估、系统安全管理等多项复杂的理论和技术，是一个复杂的综合系统[1]。其中，试验数据采集与评估是针对网络攻防效果评估和网络新技术评测的重要方法，是网络靶场的关键环节。

收稿日期：2018-04-16 修回日期：2018-07-19；
基金项目：国家重点研发计划(2016YFB0800803)，国家自然科学基金(61672264)；
作者简介：刘渊(1967-)，男，江苏无锡，硕士，教授，研究方向为网络安全；冯兴兵(1992-)，女，河北邢台，硕士生，研究方向为网络仿真，数据采集。

在网络靶场的设计中，云计算、SDN 技术[2]和虚拟化技术成为云平台的主要技术，面向大规模、高逼真网络仿真需求，基于云平台与虚拟化的仿真技术已成为趋势[3]。OpenStack 作为目前 IaaS 层活跃度最高的开源基础云平台，集成了主流的 SDN 技术和虚拟化技术，能有效地仿真网络节点，任意构建各种连接关系的虚拟链路，因此基于 OpenStack 的网络仿真正成为趋势。

针对基于 OpenStack 的网络仿真平台，本文设计了面向仿真网络的链路数据采集体系，实现了多种链路的协同、高性能采集，并可面向典型的网络安全试验，有效地进行基于数据采集的效果评估，实验表明效果良好。

1 研究现状

数据采集是网络安全试验评估的一个重要步骤，对数据采集与评估技术的研究已有如下成果。

在数据采集技术方面，张南[4]等研究链路数据采集技术，提出一种基于分层分布式多域的数据采集模型，根据链路多样性提出了针对无线链路采集方案，国外文献[5]开发了一个基于简单网络管理协议(SNMP)的开源数据采集系统，它能够同时记录大量的 CMLs 的发送和接收信号电平，时间分辨率可达 1 s。面向高速流量采集需求，刘小威等[6]提出一种基于零拷贝思想的专用于报文捕获的网络协议簇 PF_ZEROCOPY，该协议簇借助内存共享技术，减少了内存拷贝次数，提高了报文捕获能力。在云平台的采集研究中，支连意[7]等进行了云环境中集群监控数据采集与分析系统的研究，提出一套完整的云环境集群监控解决方案。面向 OpenStack 平台的采集研究，孙福全[8]等进行了云计算环境中用量信息采集系统的设计与实现，介绍了在基于 OpenStack 云平台的环境下，虚拟机的用量信息采集和云环境的监控控制。在基于数据采集的评估方面，张义荣等[9]提出一种基于网络信息熵的计算机网络攻击效果定量评估模型，陈秀真等[10]提出自下而上、先局部后整体评估策略的层次化安全威胁态势量化评估模型及其相应的计算方法，国外文献[11]以层次分析法(AHP)为基础，对多媒体教学效果进行综合评价。

上述文献并未涉及到仿真技术支撑下的虚拟链路的采集，而且有些文献未对高速流量的采集提出应对方案。有些文献仅仅监控了物理资源，并非是对仿真网络中链路层数据的采集。效果评估的试验数据采用现有的 HoneyNet 数据，缺乏针对实时采集数据的有效评估。针对上述需求，本文研究了面向仿真网络中链路层数据的采集，并对面向高速流量的采集提出有效解决方案，并且基于实时采集的数据，进行试验效果的有效评估。

2 基于云平台的数据采集体系

链路数据采集体系基于开放云平台 OpenStack 所构建的网络仿真系统，该网络仿真系统包括虚拟节点仿真和虚拟链路仿真。虚拟化技术可有效保证网络节点仿真，SDN 技术可实现虚拟链路连接关系的任意构建。OpenStack 平台使用支持 Openflow 协议[12]的 OpenvSwitch(OVS)作为虚拟交换机，为虚拟节点提供二层互联，云平台包含控制节点、网络节点(Network)和多个计算节点(Compute)，网络节点和控制节点相互独立，其中控制节点负责系统的管控功能，网络节点负责提供诸如 DHCP 和路由等网络服务，计算节点负责为虚拟主机的建立提供资源，基于 OpenStack 的网络仿真系统整体搭建架构如图 1 所示。根据虚拟主机间通信所处的计算节点位置不同，分为 3 种链路：同一计算节点内的虚拟主机之间的通信链路(图 1 中 vm1，vm2 之间的通信链路)属于宿主机内的虚拟链路，不同计算节点内的虚拟主机之间的通信链路(图 1 中 vm1，vm3 之间的通信链路)属于宿主机间的虚拟链路，计算节点内的虚拟主机与实物机之间的通信链路(图 1 中 vm1 与 entity 之间的通信链路)属于虚实互联链路，实物机 entity 依靠图 1 中网络节点连接的外网接入云平台中。

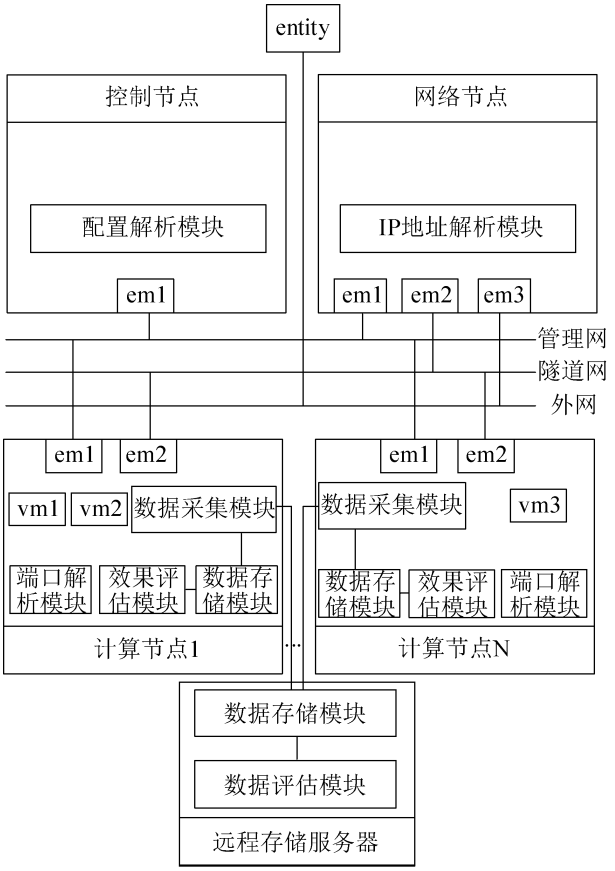

图 1 基于云平台的数据采集与评估体系

Fig. 1 Data acquisition and evaluation system based on cloud platform

2.1 数据采集与评估体系

基于上述网络仿真系统，该数据采集与效果评估体系结构包括采集点映射模块、数据采集模块、数据存储模块以及效果评估模块共 4 个模块。其中采集点映射模块包括配置解析模块、IP 地址解析模块和端口解析模块 3 个子模块，利用这 3 个子模块确定目标链路的目标端口，即采集点；数据采集模块是该体系的核心部分，完成对采集点的数据采集；数据存储模块分为本地存储和远程存储，本地存储是指将采集数据直接存在计算节点本地的数据库中，远程存储是将采集数据存入云平台之外的服务器的数据库中；效果评估模块基于实时采集的数据进行提取、分析和计算，完成对网络安全试验效果的评估。

如图 1 所示，基于云平台的链路数据采集与评估体系的具体部署方法是：将配置解析模块部署在控制节点，IP 地址解析模块部署在网络节点，端口解析模块、数据存储模块和效果评估模块部署在计算节点(注：图 1 中只表示了计算节点 1 和计算节点 N)，数据存储模块和效果评估模块同样部署在远程存储服务器。

2.2 面向 3 种链路的描述分析

为了便于分析 3 种链路的通信，基于图 1 中 3 种链路的存在形式，需要对这 3 种链路用集合进行统一描述。

(1) 宿主机内的虚拟链路集合表示为：

{(VNS1, VND1, ComputeVN1),…,(VNSi, VNDi, ComputeVNi),…, (VNSn, VNDn, ComputeVNn)}，其中 VNSi，VNDi 表示第 *i* 条链路中的源虚拟机和目的虚拟机，ComputeVNi 表示源虚拟机 VNSi，目的虚拟机 VNDi 所在的计算节点；

(2) 宿主机间的虚拟链路集合表示为：

{(VKS1, ComputeVKS1, VKD1, Compute VKD1),…, (VKSi, ComputeVKSi, VKDi, Compute VKDi),…, (VKSn, ComputeVKSn, VKDn, Compute VKDn)}，其中 VKSi，VKDi 表示第 i 条链路中的源虚拟机和目的虚拟机，ComputeVKSi, Compute VKDi 分别表示源虚拟机 VKSi，目的虚拟机 VKDi 所在的计算节点；

(3) 虚实互联链路集合表示为：

{(XSS1, ComputeXSS1, XSD1), …, (XSSi, ComputeXSSi, XSDi),…, (XSSn, ComputeXSSn, XSDn)}，其中 XSSi，XSDi 分别表示第 i 条链路中的源虚拟机、目的实物机，ComputeXSSi 表示源虚拟机 XSSi 所在的计算节点。

基于上述描述的 3 种链路，下面具体分析 3 种链路的通信过程，如图 2 所示。

(1) 对于宿主机内的虚拟链路(vm1，vm2，Compute1)，数据报文直接通过 br-int 进行转发，br-int 是由 OpenvSwitch 虚拟化出来的网桥，具有 L2 层虚拟交换机的功能，能够把它所在的计算节点上的虚拟主机都连接到 br-int 这个虚拟交换机上面；

(2) 对于宿主机间的虚拟链路(vm1，

Compute1，vm3，ComputeN)，数据报文除了经过 br-int，还会经过 br-tun，br-tun 同样是 OpenvSwitch 虚拟化出来的网桥，用来充当通信层，与其他物理机上的 br-tun 进行通信；

(3) 针对虚实互联链路(vm1，Compute1，entity)，数据报文除了经过 br-int、br-tun 之外，还会经过 br-ex，br-ex 是 OVS 中的一个虚拟网桥，负责内部虚拟网络与外部实物设备的通信。

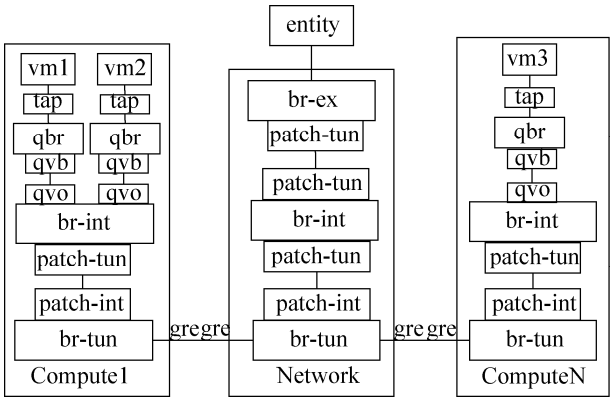

图 2 多样化链路通信图

Fig. 2 Communication graph for diversified link

可以看出 3 种链路的通信都会经过 br-int，qvo 是 br-int 上的一个端口(目标端口)。在 OpenStack 中，虚拟机与 br-int 并非直连，中间有一个虚拟网桥 qbr，qbr 上一端的设备 tap 与虚拟机的虚拟网卡相连，另一端的设备 qvb 与 br-int 上的端口 qvo 相连。因此，本文对链路的采集可以转化为对目标端口(qvo)的采集，而并非对 qbr 及其两端的设备(tap，qvb)的采集。

2.3 多样化链路协同采集技术

基于上节分析的多样化链路，本文归一化了采集流程，描述如下：

(1) 确定目标端口。利用采集点映射模块获取目标端口，在获取目标端口的过程中，需要依靠采集点映射表，采集点映射表存储了获取目标端口所需要的基本信息，包括虚拟主机的名称、虚拟主机所在的计算节点、虚拟网络的名称、虚拟网络的 IP 地址以及目标端口的 mac 地址。由于一个虚拟主机可能包含多个网络，所以，一个虚拟主机可能对应多个虚拟网络 IP，即一个虚拟实例可能会对应多行信息。采集点映射表的结构如表 1 所示。

(2) 设置端口镜像。若同一计算节点上有多个目标端口，可以对这多个目标端口设置端口镜像。端口镜像(port Mirroring)[13]是将一个或多个源端口的数据流量转发到某一个指定端口来实现对网络的监听，指定端口称之为“镜像端口”或“目的端口”，可以通过镜像端口对经过源端口的报文进行监控和分析。本文中，源端口为 br-int 的 qvo 端口，该端口与虚拟主机相连，目的端口为 veth0，veth0 是自行在 br-int 上添加的端口，通过对 veth0 的采集实现对多个源端口的采集，因此只需要在每个计算节点上部署一个采集程序即可，从而减少进程的启动，降低 CPU 消耗的资源。

(3) 根据目标端口所在的计算节点，启动其上的采集程序，实现多链路协同采集。

2.4 基于虚拟网桥的高性能链路数据采集新技术

在高速流量数据采集时，传统的 libpcap 数据包捕获函数包在捕获数据包时，首先在内核空间复制网络驱动程序读取的数据包，再传递到用户空间，需要二次内存复制，限制了其捕获性能，捕获包的能力明显不足。为提高采集性能，本文研究了 Netmap[14]高速网络 I/O 架构的零拷贝技术，能够在千兆或者万兆网卡上达到网卡的线速收发包速率，并且能够有效地节省 CPU 等计算机资源，提出一种基于虚拟网桥的 Netmap 高性能链路数据采集新技术，该技术实现原理如下：

为计算节点添加虚拟网桥 br1，patch-to-br1 和 patch-to-br-int 是一对 patch 端口，用来连接网桥 br-int 和 br1，通过一条命令“ovs-ofctl add-flow br-int table=0，priority=5，actions=all”为 br-int 添加一条流表规则，使 br-int 上的目标端口向所有的端口转发，这样就可以在 br1 上收到目标端口转发的数据包。

表 1 采集点映射表的结构
Tab. 1 Structure of mapping table for collection point

属性	vm_name	c_node	net_name	ip	mac
类型	VarCh-ar(40)	char	VarCh-ar(40)	VarCh-ar(16)	VarCh-ar(40)
描述	虚拟实例名称	实例所在计算节点	虚拟网络的名称	虚拟网络的 IP 地址	目标端口的 mac 地址

2.5 基于链路数据的网安试验表征参数研究与评估

本采集系统可以应用在网安试验中，在网络安全试验中，为了网安试验能够有效进行，需要基于所采集到的链路数据，研究网安试验表征参数如下：

(1) 吞吐量：单位时间内从端口收到的数据包数量，吞吐量

$$V=n\times b\times 8/t \tag{1}$$

式中：n 为收到的数据包个数；b 为数据包帧长度；t 为所用时间。

(2) 网络延迟：把每个包的时间戳和序列号在传输端和接收端记录下来，进一步计算得到期望值，网络延迟 R 为数据包发送和到达之间的间隔，

$$Ti=TR(i)-TS(i) \tag{2}$$

式中：Ti 为第 i 个包的延迟；$TR(i)$为第 i 个包的收到时间戳，$TS(i)$是第 i 个包的发送时间戳。

(3) 延迟抖动：延迟抖动时间通过 2 个连续的包之间的时间间隔来计算，假设第 i 时刻收到第 i 个数据包，则 i 时刻的延迟抖动

$$Di=[TR(i)-TS(i)]-[TR(i-1)-TS(i-1)] \tag{3}$$

式中：$TR(i)$为第 i 个包的收到时间戳；$TS(i)$为第 i 个包的发送时间戳；$TR(i–1)$为第 $i–1$ 个包的收到时间戳；$TS(i–1)$为第 $i–1$ 个包的发送时间戳。

上述表征参数可反映网络安全试验效果，进一步可通过如下方法来评估：

上述表征参数在试验前后的变化可以通过“熵差”来表示。“熵差” $\Delta H=-\log_2(V2/V1)$ 是对攻击效果的一种描述，式中 $V1$ 为网络系统原来的性能参数，$V2$ 为网络受攻击后的性能参数，在计算时本文考虑 2 种情况。

(1) 当网络性能指标值与攻击效果成反比时，设测得网络受攻击前的指标值为 $V1$，受攻击后的指标值为 $V2$，将它们进行归一化，得到归一化的指标值分别为：$V1/Vg$，$V2/Vg$，其中 Vg 为该指标最大值，且 $0\le V2\le V1\le Vg$ 。则在该指标上的攻击效果为：

$$\Delta H=-\log_2(V2/Vg)-(-\log_2(V1/Vg))=-\log_2(V2/V1) \tag{4}$$

(2) 当网络性能指标值与攻击效果成正比时，设测得网络受攻击前的指标值为 $V1$，受攻击后的指标值为 $V2$，将它们进行归一化，得到归一化的指标值分别为：$V1/Vg$，$V2/Vg$，其中 Vg 为该指标的最大值，且 $0\le V1\le V2\le Vg$ 。则在该指标上的攻击效果为：

$$\Delta H=-\log_2(V1/Vg)-(-\log_2(V2/Vg))=-\log_2(V1/V2) \tag{5}$$

显然，若 $V1$=$V2$，则 ΔH=0，说明攻击未取得任何效果。$V2$ 变化(包括增加或减小)的越厉害，表明攻击的效果越明显，ΔH 也越大，可见 ΔH 可以作为攻击效果的一项表征。

2.6 数据采集存储流程

传统的数据采集存储只提供了本地存储的功能，利用本文的数据采集系统，实现了本地存储和远程服务器实时存储的双重功能，远程存储通过将采集数据复制备份到独立的服务器，实现了实验数据的安全隔离，为后续的进一步研究提供了数据保障。对采集点进行采集并实时对所采集数据进行存储的具体步骤为：

step 1：启动数据采集程序，使用监测进程对数据文件目录进行监听；

step 2：对生成的数据文件，采用压缩算法进行压缩；

step 3：将压缩文件发送给接收端服务器；

step 4：服务端接收到压缩文件，先进行解压缩，再将数据文件解析入库；

step 5：通过对数据库中的数据进行提取、分析、计算，完成试验效果评估。

通过试验验证，远程存储数据可以用来支持后面的效果评估。

3 实验验证与评估

本文实验平台中采用九台 Dell R730 服务器(CPU 类型为 2 个 Intel E5620 处理器，内存为 16GB)，服务器与交换机之间通过千兆以太网交换机连接，服务器上安装的 OpenStack 版本为 Mitaka，采用 OVS 提供虚拟网络二层连接，并基于 VLAN 方式进行租户内子网隔离。基于此硬件环境，做了 2 个试验，验证数据采集系统的协同、高效采集能力，并且可以针对典型的网安试验进行链路数据采集，基于实时采集的数据进行有效评估。

3.1 基本测试

在 OpenStack 中构建虚拟网络，网络拓扑如图 3 所示，图中 vm1，vm2，vm3 表示虚拟主机，IP 地址分别为 11.0.0.4，13.0.0.5，11.0.0.5，vm5 是实物机 PC，通过虚实互联方式接入 OpenStack 平台，router 是虚拟路由器，IP 地址为 11.0.0.3,13.0.0.3, 15.0.0.3，net11，net13，net15 代表虚拟网络，网络地址分别为 11.0.0.0/24，13.0.0.0/24，15.0.0.0/24，其中 vm1，vm2 在同一计算节点(Compute1)上，vm3 在另一计算节点(Compute2)上。

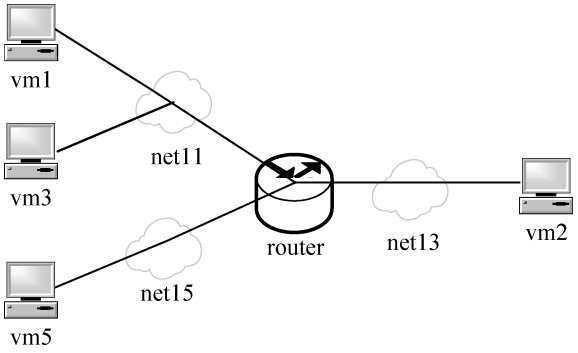

图 3 实验网络拓扑
Fig. 3 Topology for experiment

选择图中 3 条链路：(vm1, vm2, Compute1)，(vm3, Compute2, vm2, Compute1)，(vm2, Compute1, vm5)。上述三条链路的通信都通过 router，首先确定采集点，router 有 3 个网卡，此处需要的是与 router 在 net11 和 net15 的网卡相连的 br-int 的两个目标端口(端口 1，端口 2)，获取 router 的采集点映射表，得出两个目标端口位于同一计算节点 Compute1 上，需要对这两个端口设置端口镜像。为验证端口镜像的有效性，用 vm1，vm3，vm5 分别向 vm2 发送 10 个 ICMP 数据包，结果从镜像口接收到 60 个 ICMP 数据包(ICMP 数据包是双向的)，验证端口镜像设置成功。

为验证该系统的链路数据采集性能，对图 3 中的链路(vm1, vm2, Compute1)进行测试，用 vm1 上的 iperf 发包工具向 vm2 发包，采集端口 1，分别测试 libpcap(Linux 自带的传统采集方法)，pf_ring[15]和该系统测试在捕获不同长度数据包时的采集速率，测试结果通过图 4 显示。

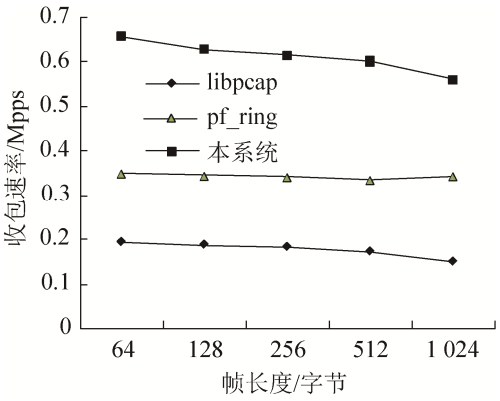

图 4 采集速率结果
Fig. 4 Results for acquisition rate

可以看出，随着帧长度增大，libpcap 和本系统每秒钟收包速率均逐渐减小，pf_ring 的收包速率趋于稳定，说明在数据传输过程中小包比较容易被接收，且利用本系统达到的采集速率明显优于 libpcap 和 pf_ring 的采集速率，采集速率相较于 pf_ring 最高提升了 88.48%，验证了该采集系统的高效性。

评判采集性能的重要指标还包括 CPU 占用

DOI: 10.16182/j.issn1004731x.joss.18-0218

率，程序运行时 CPU 占用率越小，程序性能越好。为了测试本系统的 CPU 占用率，将 libpcap 和 pf_ring 作为对照组，测试 3 种数据包捕获方法在捕获不同长度数据包时的 CPU 占用率，测试结果如图 5 所示。

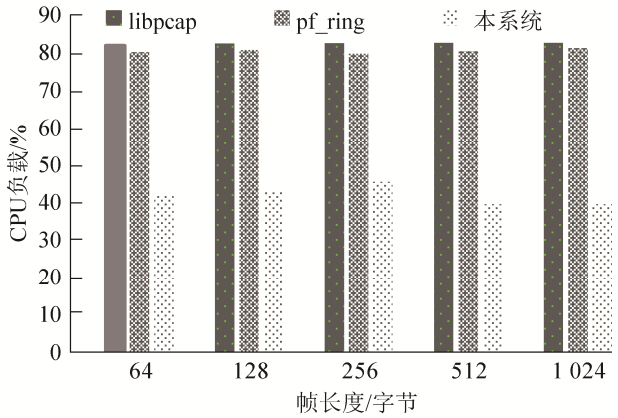

图 5 CPU 占用率
Fig. 5 CPU usage

可以看出，在帧长增大时，3 种采集方法的 CPU 利用率有轻微波动，整体趋于稳定，libpcap 的 CPU 占用率在 82%~83%，pf_ring 的 CPU 占用率在 80%~81%，二者在 CPU 负载平衡方面性能相当，而用本系统 CPU 占用率平均在 43%，相较于 libpcap 和 pf_ring，使用本系统，CPU 占用率降低了 45.29%，大大降低 CPU 使用率，有效提高了采集效率。

由此可见，无论在收包速率还是 CPU 利用率方面，本系统均优于传统方法，使用本系统能够有效提高采集速率，降低 CPU 使用率。

3.2 网安试验链路采集

域间路由系统作为互联网的关键基础设施，其安全性对互联网健康稳定运行具有重要影响。为了测试本文中的数据采集系统在网络攻击试验中应用的有效性，本文选用针对域间路由系统的 LDDoS 攻击(低速率分布式拒绝服务攻击)。域间路由系统主要采用 BGP(border gateway protocol)[16] 协议，近年来，针对域间路由系统的攻击手段不断更新，其造成的危害也越来越严重[17]。由于 BGP 运行在传输层 TCP 协议之上，针对 TCP 协议的攻击就可以威胁 BGP 会话的安全：Zhang 等人提出的 ZMW 攻击[18]能够导致网络收敛时间的延长和 BGP 会话的重置；在 ZMW 攻击的基础之上，Schuhard 等提出了基于 BGP 数据平面的跨平面攻击方式 CXPST(coordinated cross plane session termination)，这种攻击通过精心选择系统中的部分关键路径，利用大规模的僵尸网络对这些关键路径同时进行 LDDoS 攻击，通过引发大量的路由更新，耗尽路由器的存储和计算资源，从而达到瘫痪整个系统的目的。

在 OpenStack 中构建如图 6 所示的试验网络，图中 BGP1~BGP9 是虚拟路由器，BGP10 是实物路由器，通过虚实互联的方式接入 OpenStack 平台中，net161，net167，net168 是虚拟网络。VM1~VM6 是虚拟主机，其中，VM1，VM3，VM5 上有攻击程序，负责产生攻击流量，分别攻击虚拟主机 VM2, VM4, VM6。BGP1，BGP2 位于同一计算节点(Compute2)，BGP4，BGP6，BGP8 分别位于计算节点 6(Compute6)，计算节点 4(Compute4)，计算节点 1(Compute1)。

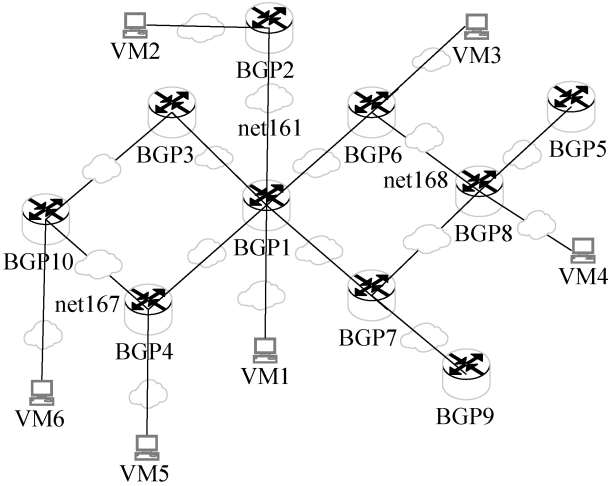

图 6 网络试验拓扑
Fig. 6 Topology for network test

对图 6 中的拓扑结构进行分析，选择路由系统中的关键链路，即连接中心度高的链路作为目标链路，本实验选取的 3 条关键链路为:(BGP1, BGP2,

Compute2)，(BGP6, Compute4, BGP8, Compute1)，(BGP4, Compute6, BGP10)。首先确定 3 条链路的 3 个目标端口，用 Compute2，Compute4，Compute6 上的数据采集程序采集 3 个端口实现协同采集。3 条链路同时攻击，攻击过程中，当有路由被发布到 BGP 中或有路由失效时，会发送 update 报文，通过采集链路中产生的 update 报文分析判断链路通断次数。设置链路带宽 1 M，测试在攻击流量大小和攻击时间长短不同的情况下，3 条链路的总断开次数，测试结果如图 7 所示。

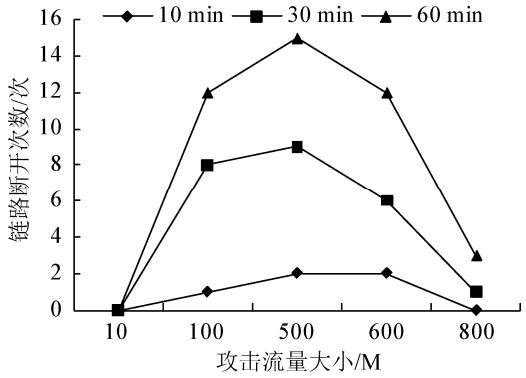

图 7 不同规模攻击流量下的链路断开次数
Fig. 7 Link disconnection under different scale attacks

可以看出，链路带宽为 1 M 时，在攻击流量为 10 M 时，攻击时间为 10 min，30 min，60 min 时链路均没有断开；攻击流量在 10~500 M 之间时，随着攻击流量增大，攻击时间增长，链路中产生的 update 报文增多，链路断开次数增多；在攻击流量在 500~800 M 时，断开次数又呈下降趋势，可见本实验的最佳攻击流量为 500 M，此时链路断开次数最多，攻击效果最明显。

3.3 网安试验效果评估

为了定量描述试验攻击效果，设置每条链路带宽为 10 M，攻击流量为 20 M，对上述 3 条链路的 3 个目标端口进行采集，并基于实时采集到的数据利用公式(1)~(3)计算试验前后吞吐量、网络延迟和延迟抖动 3 项网络性能指标，计算结果吞吐量试验前后分别为 8.496 Mbits/sec 和 0.656 Mbits/sec，网络延迟试验前后分别为 4.330 ms 和 3 613.618 ms，延迟抖动试验前后分别为 0.024 ms 和 6 465.501 ms。进一步根据公式(4)计算吞吐量的熵差 $\Delta H1$=1.413 3，根据公式(5)计算网络延迟、延迟抖动的熵差分别为 $\Delta H2$=3.222 5，$\Delta H3$=5.731 4。

根据网络性能降低的程度，对网络攻击效果进行分级描述，例如把攻击效果简单的划分为无、轻、中、较重、严重、网络被瘫痪等 6 个等级，相应的网络性能降低程度分别为小于 5%，5%~20%，20%~50%，50%~70%，70%~90%和大于 90%，对应 ΔH 的范围分别为小于 0.07，0.07~0.26，0.26~1，1~1.74，1.74~3.32 和大于 3.32，查找吞吐量、网络延迟与延迟抖动的熵差在上述等级描述中对应的等级，可得基于吞吐量、网络延迟、延迟抖动的网络熵对此次网络攻击效果评估分别为较严重、严重、网络几乎被瘫痪。从试验结果可以看出，相比于吞吐量，LDDoS 攻击对网络延迟、延迟抖动的影响更大一些。

4 结论

数据采集是网络安全评估的一个重要手段。针对仿真网络，本文提出一种面向云平台仿真网络的多样化链路数据采集方法，可对云平台中多样化链路进行协同、高效采集，本文所提方法在采集速率上相对于传统方法提升了 88.48%，在 CPU 占用率上降低了 45.29%，从而验证了本系统的高效性。

另外，通过网安试验，验证了该采集系统针对网络攻防试验链路的有效采集，并且可以基于实时采集的数据对网安试验效果进行评估，并取得良好效果。

网络安全试验效果评估数据来源一方面是链路数据采集数据，另一方面是虚拟机内部的采集数据。为此，后期将重点研究虚拟机内部的数据采集方法，尤其是虚拟机的低损实时采集技术。此外，基于链路数据采集数据与虚拟机内部的采集数据，如何建立攻防效果评估指标体系以及进一步构建实时绩效评估计算模型，是接下来可能的发展方向。

DOI: 10.16182/j.issn1004731x.joss.18-0218

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.
Fang Binxing, Jia Yan, Li Aiping, et al. Research on Network Space Shooting Range Technology[J]. Journal of Cyber Security, 2016, 1(3): 1-9.

[2] Murat K, Arjan D. Quality of Service (QoS) in Software Defined Networking (SDN): A Survey[J]. Journal of Network and Computer Applications (S1084-8045), 2017, 80: 200-218.

[3] 李伯虎, 柴旭东, 侯宝存, 等. 一种基于云计算理念的网络化建模与仿真平台—“云仿真平台”[J]. 系统仿真学报, 2009, 21(17): 5292-5299.
Li Bohu, Chai Xudong, Hou Baocun, et al. A Networked Modeling and Simulation Platform Based on Cloud Computing Concept-“Cloud Simulation Platform”[J]. Journal of System Simulation, 2009, 21(17): 5292-5299.

[4] 张南. 系统链路数据采集技术研究[D]. 沈阳: 沈阳理工大学, 2009.
Zhang Nan. Research on System Link Data Acquisition Technology [D]. Shenyang: Shenyang Ligong University, 2009.

[5] Chwala C, Keis F, Kunstmann H. Real-time Data Acquisition of Commercial Microwave Link Networks for Hydrometeorological Applications[J]. Atmospheric Measurement Techniques (S1867-1381), 2016, 8(11): 12243-12262.

[6] 刘小威, 陈蜀宇, 卢尧, 等. 零拷贝技术在网络分析工具中的应用[J]. 计算机系统应用, 2012, 21(4): 169-173.
Liu Xiaowei, Chen Shuyu, Lu Yao, et al. Application of Zero Copy Technology in Network Analysis Tools[J]. Computer Systemsand Applications, 2012, 21(4): 169-173.

[7] 支连意. 云环境中集群监控数据采集与分析系统的研究与实现[D]. 南京: 东南大学, 2016.
Zhi Lianyi. Research and Implementation of Cluster Monitoring Data Acquisition and Analysis System in Cloud Environment [D]. Nanjing: Southeast University, 2016.

[8] 孙福全. 云计算环境中用量信息采集系统的设计与实现[D]. 北京: 北京邮电大学, 2013.
Sun Fuquan. Design and Implementation of Consumption Information Collection System in Cloud Computing Environment [D]. Beijing: Beijing University of Posts and Telecommunications, 2013.

[9] 张义荣, 鲜明, 王国玉. 一种基于网络熵的计算机网络攻击效果定量评估方法[J]. 通信学报, 2004, 25(11): 158-165.
Zhang Yirong, Xian Ming, Wang Guoyu. A Quantitative Evaluation Method of Computer Network Attack Effect Based on Network Entropy [J] .Journal on Communications, 2004, 25(11): 158-165.

[10] 陈秀真, 郑庆华, 管晓宏, 等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885-897.
Chen Xiuzhen, Zheng Qinghua, Guan Xiaohong, et al. Quantitative Evaluation Method of Hierarchical Cyber Security Threat Situation[J]. Journal of Software, 2006, 17(4): 885-897.

[11] Li L G. Study of Multimedia Teaching Effect Evaluation Based on AHP[J]. Energy Procedia (S1876-6102), 2011, 13: 8371-8375.

[12] Mendiola A, Fuentes V, Matias J, et al. An Architecture for Dynamic QoS Management at Layer 2 for DOCSIS Access Networks Using OpenFlow[J]. Computer Networks (S1389-1286), 2016, 94: 112-128.

[13] 胡显成, 任新, 向涛. 网络端口镜像获取流量分析数据源[C]. 中国计算机用户协会网络应用分会 2013 年网络新技术与应用年会. 2013: 212-214.
Hu Xiancheng, Ren Xin, Xiang Tao. Port Mirroring for Traffic Analysis Data Sources [C]. China Computer User Association Network Application Branch 2013 Network New Technology and Application Annual Meeting. 2013: 212-214.

[14] Rizzo L, Landi M. Netmap[J]. ACM SIGCOMM Computer Communication Review (S0146-4833), 2011, 41(4): 339-350.

[15] 张潇晓, 唐勇, 苏金树, 等. 网络流量分析系统的设计与实现[J]. 计算机应用, 2011, 31(增 2): 25-28.
Zhang Xiaoxiao, Tang Yong, Su Jinshu, et al. Design and Implementation of Network Traffic Analysis System [J]. Journal of Computer Applications, 2011, 31(S2): 25-28.

[16] Sapegin A, Uhlig S. On the Extent of Correlation in BGP Updates in the Internet and What It Tells Us About Locality of BGP Routing Events[J]. Computer Communications (S0140-3664), 2013, 36(15/16): 1592-1605.

[17] 黎松,诸葛建伟, 李星. BGP 安全研究[J]. 软件学报, 2013, 24(1): 121-138.
Li Song, Zhuge Jianwei, Li Xing. Research on BGP Security[J]. Journal of Software, 2013, 24(1): 121-138.

[18] 郑庆棠. 基于仿真平台的典型动态路由协议攻击技术研究[D]. 北京: 北京邮电大学, 2014.
Zheng Qingtang. Research on Typical Dynamic Routing Protocol Attack Technology Based on Simulation Platform[D]. Beijing: Beijing University of Posts and Telecommunications, 2014.