# 软件定义网络 IPv6 安全仿真技术与教学应用

鱼 清[1],胡曦明[1,2*],李 鹏[1,2]
(1. 陕西师范大学 计算机科学学院,陕西 西安 710119;
2. 现代教学技术教育部重点实验室,陕西 西安 710119)

**摘 要**:随着软件定义网络加速向更广领域、更高层次和更深程度融合创新,产学研用协同实现创新驱动发展的迫切需求对软件定义网络的仿真技术与教学应用提出新课题。通过对 2010 ~ 2020 年中国知网收录的软件定义网络仿真技术与教学应用的文献开展跟踪调查以及主题聚类分析,发现当前仿真技术基于 Mininet 平台是主流技术路径、从组网类向安全类升级成为新需求和从 IPv4 向 IPv6 延伸成为新方向。在此基础上,提出了基于"Python+Mininet"的软件定义网络 IPv6 安全仿真技术并给出了仿真技术架构、仿真流程和数据源开发、网络行为管理、数据测量接口等关键技术,详细实现了软件定义网络环境下的 IPv6 邻居发现协议攻击、防御及可视化分析,为高校建设主动布局面向未来网络空间安全的教学改革提供新的技术途径。

**关键词**:软件定义网络;IPv6;网络安全;仿真技术;Mininet
**中图分类号**:TP393 **文献标识码**:A **文章编号**:1673-629X(2021)05-0119-07
doi:10.3969/j.issn.1673-629X.2021.05.021

# IPv6 Security Simulation Technology and Teaching Application Based on SDN

YU Qing[1],HU Xi-ming[1,2*],LI Peng[1,2]
(1. School of Computer Science,Shaanxi Normal University,Xi'an 710119,China;
2. Key Laboratory of Modern Teaching Technology of Ministry of Education,Xi'an 710119,China)

**Abstract**:With the accelerated integration and innovation of SDN to a wider field,a higher level and a deeper degree,the urgent need of industry-university-research-application for collaboration to achieve innovation-driven development puts forward a new subject for simulation technology and teaching application of SDN. Through the tracking survey and subject cluster analysis of SDN simulation technology and teaching application literature collected by CNKI from 2010 to 2020,it is found that the current simulation technology based on Mininet platform is the mainstream technology path,upgrading from networking to security becomes a new demand,and extending from IPv4 to IPv6 becomes a new direction. On this basis,we propose IPv6 security simulation technology of SDN based on "Python+Mininet" and gives the simulation technology architecture,simulation process and key technologies such as data source development,network behavior management and data measurement interface. The IPv6 NDP attack,defense and visual analysis is realized in detail in SDN environment,and a new technical way for the construction of colleges and universities is provided to actively deploy the teaching reform for the future cyberspace security.

**Key words**:SDN;IPv6;cyberspace security;simulation technology;Mininet

## 0 引 言

软件定义网络(SDN)是从最初美国斯坦福大学 Clean Slate 课程组提出的学术性新概念[1],以技术创新驱动发展演变成为涵盖技术标准、设备产品、网络建设和商用运营等上下游各方的高新技术产业,受到包括互联网工程任务组(IETF)等国际标准化组织、思科等设备制造商、谷歌等互联网公司和德国电信等网络运营商的持续高度关注与高投入。SDN 是基于数据层面与控制层面分离的架构,向下将基础设施虚拟化为底层服务资源的同时向上将分散而异构的管理控制功能抽象为可编程可开发的软件平台[2],使得信息网络从互联互通基础设施升级转化为业务响应服务系

**收稿日期**:2020-07-03 **修回日期**:2020-11-05
**基金项目**:陕西省科技计划重点研发项目(2020GY-221)
**作者简介**:鱼 清(1999-),男,研究方向为计算机科学与技术;通讯作者:胡曦明(1978-),男,博士,讲师,教育硕士导师,研究方向为智慧教育、计算机教育;李鹏,博士,副教授,硕导,研究方向为移动计算、教育信息化。

统。在 SDN 技术创新的强劲驱动下,软件定义光网络 SDON[3]、Google 数据中心广域网 B4[4]、开放网络操作系统 ONOS[5]、SDN/NFV 统一编排平台 ECOMP[6] 等新模式新业务新系统蓬勃发展,进一步推动 SDN 向更广领域、更高层次和更深程度融合创新,可以说 SDN 已成为面向未来实施创新驱动发展的战略性热点之一。

面对 SDN 创新驱动要求产学研用协同实现高质量发展的内在需求进一步突显,软件定义网络仿真技术如何以高校学科发展和专业教学改革为引领,探索 SDN 相关仿真技术和教学应用,主动适应 SDN 科技创新和产业变革对复合型拔尖创新人才培养的需求,成为当前高校面向“新工科”建设开展仿真技术创新和实验教学改革富有时代性、前瞻性和教育价值性的新课题。

## 1 软件定义网络仿真技术发展现状与趋势

以中国知网(CNKI)收录的中文期刊为文献统计源,分别以关键词“软件定义网络”或“SDN”并含“仿真技术”或“实验教学”,在“全部期刊”中精确检索,再对检索所得文献集合进行筛选,剔除检索词条匹配但内容与学术研究无关的文献后得到 27 篇论文(如表 1 所示),通过文献调查法和主题聚类分析 SDN 仿真技术与教学应用发展现状与趋势。

表 1 SDN 仿真技术与教学应用文献调查与研究主题聚类分析

(统计来源:2010 ~ 2020 年中国知网 CNKI 收录期刊)

| 主题 | 数量 | 研究方向细分 | 网络体系 |
|---|---|---|---|
| 仿真技术与教学应用 | 9 篇 | 组网通信 8 篇 | IPv4 |
| | | 网络安全 1 篇 | IPv4 |
| 仿真实验教学模式 | 10 篇 | 平台部署 4 篇 | IPv4 |
| | | 方案设计 3 篇 | IPv6 |
| | | 协议分析 3 篇 | IPv6 |
| 仿真技术发展 | 8 篇 | 算法优化 2 篇 | IPv6 |
| | | 过渡技术 6 篇 | IPv4/IPv6 |

(1)仿真技术以基于 Mininet 平台成为主流路径。

从功能上讲,能够用于 SDN 仿真的实验平台类型多样,如美国斯坦福大学 Mininet[7]、台湾思锐科技 EstiNet[8]、美国华盛顿大学 NS-3[9] 以及美国国家航空航天局和 Rackspace 合作研发的 OpenStack[10],但是通过对 SDN 仿真技术文献调查分析发现,基于 Mininet 的仿真技术文献占比高达 80%。中南大学[11-13]、华北电力大学[14] 等多所“双一流”大学和西安思源学院[15]、浙江农林大学暨阳学院[16] 等地方民办院校均以 Mininet 作为平台开展仿真实验教学。Mininet 具有轻量级的仿真环境和友好、便捷的可开发性,事实上已成为将 SDN 快速引入高校课堂的主流路径。

(2)仿真主题从组网类向安全类升级成为新需求。

通过对 SDN 仿真技术文献的研究主题聚类分析发现,现有以 SDN 组网为仿真主题的文献占比达 75%,仿真科目聚焦 SDN 控制器部署、交换设备控制数据转发等 SDN 组网的基础配置与操作,教学模式以教师指令下的 SDN 组网验证性仿真实验为主,例如,广西大学叶进以 OpenDayLight 为 SDN 控制器开展控制数据转发与可视化表项方面的实验教学[17]。

网络空间安全作为重要组成部分被纳入中国特色国家安全能力建设总体布局,2015 年国务院学位委员会、教育部联合发布通知,正式增设“网络空间安全”一级学科[18]。在国家战略和学科发展的双重推动下,SDN 仿真主题从组网类向安全类升级成为增强学科教学服务高质量发展能力的时代性需求[19],也成为专业教学改革新的着力点。从文献调查来看,中南大学黄家玮从前期关注测试验证 Mininet 平台开展 SDN 仿真的可行性、高效性与便捷性[11] 和以 OpenDayLight 的 Web UI 控制转发表项为例开展交换机控制数据转发仿真实验[12],转而聚焦 SDN 架构下网络空间安全的 BGP 路径挟持攻击和 ARP 攻击与防御仿真技术[13];南京邮电大学费宁构建 SDN 下高扩展性防火墙仿真平台,支撑网络安全实验教学新需求[20]。

(3)仿真体系从 IPv4 向 IPv6 延伸成为新热点。

随着互联网+、人工智能和大数据等国家战略的深入推进,IPv4 地址资源枯竭和技术体系受制于人的格局给国家信息安全带来的隐患和威胁愈加突出,2017 年 11 月中共中央办公厅、国务院办公厅印发《推进互联网协议第六版(IPv6)规模部署行动计划》,强调必须加快部署 IPv6 网络,构建高性能下一代互联网[21]。SDN 作为面向未来网络空间架构的关键技术也必将加快向 IPv6 体系演进,由此带动 SDN 仿真体系从 IPv4 向 IPv6 延伸,成为近年来仿真技术研究的新热点。例如,2017 年北京邮电大学陈蔚瀚提出新的 IPv4/IPv6 过渡技术的流量调度优化模型并基于 Mininet 开展 SDN 环境下的仿真测试[22];2018 年北京工业大学李丹基于 Mininet 平台提出 SDN 下的 IPv6 组播机制并完成了仿真[23]。

## 2 “Python+Mininet”软件定义网络 IPv6 安全仿真技术

基于上述对国内软件定义网络仿真技术与教学应用发展现状与趋势的系统梳理,可以说以 Mininet 为平台聚焦软件定义网络 IPv6 安全仿真技术研究是高校

承接国家网络安全与信息化发展战略对卓越信息安全工程师培养需求的新着力点。在此基础上,该文基于“Python+Mininet”提出轻量级和可开发的软件定义网络 IPv6 安全仿真技术,旨在以软件定义为核心打造个性化学习实验系统,以仿真技术创新赋能软件定义网络实验教学提质升级。

### 2.1　总体设计

(1)技术架构。

将 SDN 仿真平台 Mininet 与 Python 开发相结合,提出“Python+Mininet”的软件定义网络 IPv6 安全仿真技术架构,总体设计如图 1 所示。

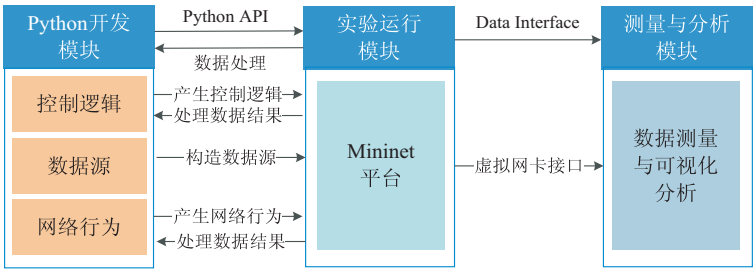


图 1　“Python+Mininet”软件定义网络 IPv6 安全仿真技术架构

从仿真技术和教学应用来看,“Python+Mininet”的模块化设计具有以下优点:模块之间相互独立,灵活而易于实现,适用于开展分组合作式实验和协作学习;支持 Python 开发,满足个性化和定制化的仿真需求;数据测量与可视化适用于对仿真进行过程性分析和精细化管理。

①Python 开发模块。

负责仿真策略的生成,通过 Python 开发在数据层面生成可编程数据源与路由跟踪等网络行为,在控制层面生成实验环境配置、数据处理控制逻辑和网络服务管理,经过 Python 第三方开发套件 API 实现与实验运行模块的交互,从而起到策动仿真的作用。

②实验运行模块。

负责网络仿真的运行,基于 Mininet 平台输入 Python 开发模块生成的数据层面和控制层面的仿真策略,模拟软件定义网络架构下的网络行为与工作过程,经过 Python 第三方开发套件 API 向 Python 开发模块实时反馈运行状态,并通过 Data Interface 向测量与分析模块输出运行数据。

③测量与分析模块。

负责对仿真数据与结果进行可视化分析,通过 Data Interface 实时采集实验运行模块虚拟网卡输入输出的数据,使用常用协议分析工具实现对仿真过程与结果的可视化分析。

(2)仿真流程。

基于“Python+Mininet”开展软件定义网络 IPv6 安全仿真技术的流程,如图 2 所示。

### 2.2　关键技术

(1)数据源开发。

一方面可通过 Python 自主开发数据包构造和发包工具,另一方面也可采用 Python 第三方开发套件作为 Mininet 平台插件。综合考虑开发成本和教学应用需求,该文采用协议报文数据处理软件 Scapy 作为 Python 开发模块的数据源开发工具,通过 Scapy 可以实现网络扫描、协议报文构造与解析和数据包嗅探等多种功能,并且利用 Scapy 为 TCP/IP 协议栈提供的开发类,可以开发更加综合性的数据服务功能。

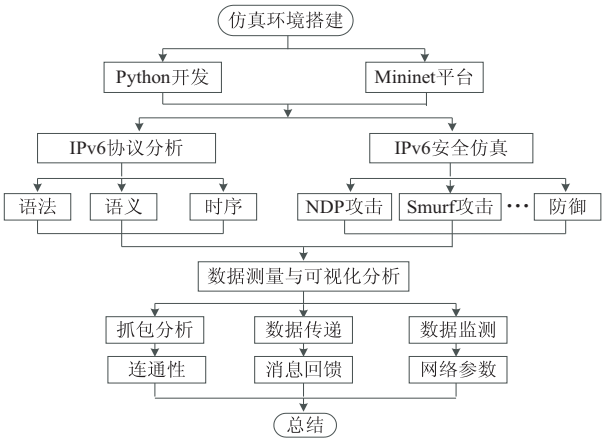


图 2　“Python+Mininet”软件定义网络 IPv6 安全仿真技术流程

(2)网络行为管理。

作为软件定义网络的核心,控制器负责在控制层面上对网络行为进行集中式控制与管理,由此也就成为开展软件定义网络 IPv6 安全仿真的关键。该文针对“Python+Mininet”的仿真技术架构,以基于 Python 的 Ryu 或 POX 作为控制器,通过充分利用其自身具有的丰富 Python API,针对个性化定制化的仿真需求开发不同的网络行为管理策略,通过以可编程的模式从整体上实现网络服务和网络规则的定义、下发等网络行为管理。

(3)数据测量接口。

仿真实验在 Mininet 平台中运行,需要通过数据测量接口从 Mininet 平台中采集实验数据才能开展后续的测量与分析。该文在 VMware Workstation 虚拟机上

安装 Ubuntu 作为 Mininet 的系统环境，通过虚拟机向 Mininet 平台桥接虚拟网卡，然后采用 Wireshark、tcpdump 等协议分析工具监听虚拟网卡从而获得实验数据。Wireshark 提供良好的交互界面，可以实时捕获经过网卡的数据包；tcpdump 通过系统命令对数据包及时可视化显示，操作灵活便捷。

## 3 软件定义网络 IPv6 安全仿真技术的教学应用

### 3.1 拓扑环境

将上述“Python+Mininet”软件定义网络 IPv6 安全仿真技术应用于高校课堂，首先搭建仿真拓扑环境，如图 3 所示。

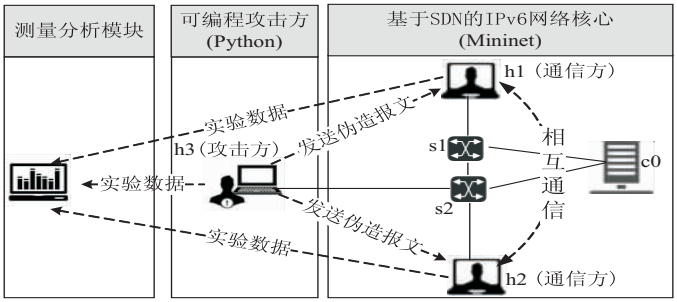


图 3 “Python+Mininet”软件定义网络 IPv6 安全仿真拓扑

从拓扑结构的连接关系来看，c0 为 SDN 控制器，在控制器 c0 下连接交换机 s1 和 s2；交换机 s1 连接主机 h1，交换机 s2 连接主机 h2 和 h3。

从攻击与被攻击的交互关系上，主机 h3 作为攻击方，主机 h1 或 h2 作为被攻击方，当 h1 与 h2 进行通信过程中，攻击方 h3 基于 Python 开发伪造报文，攻击主机 h1 与 h2 从而窃取 h1 与 h2 之间的通信信息，整个攻击过程通过测量分析模块实时进行数据采集、测量与可视化分析。

### 3.2 配置与操作

具体仿真实验步骤以及对应的配置与操作过程，如图 4 所示。

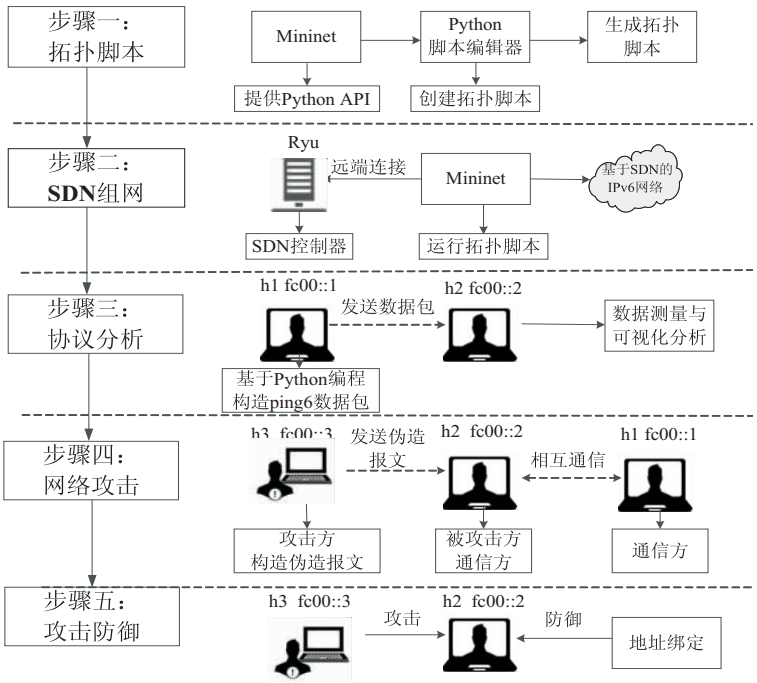


图 4 配置与操作

(1)拓扑脚本。

使用 Mininet 提供的 Python API，创建拓扑脚本。

```
from mininet. topo import Topo

class MyTopo( Topo) :

def __init__( self) :
# initialize topology
Topo. __init__( self)
# add switches and hosts
s1 = self. addSwitch( 's1')
s2 = self. addSwitch( 's2')
h1 = self. addHost( 'h1', mac = "00:00:00:00:00:01")
h2 = self. addHost( 'h2', mac = "00:00:00:00:00:02")
h3 = self. addHost( 'h3', mac = "00:00:00:00:00:03")
# add links
```

```
self.addLink(h1,s1)
self.addLink(h2,s2)
self.addLink(h3,s2)
self.addLink(s1,s2)

topos={'myTopo':(lambda:SdnTopo())}
```

在网络拓扑脚本中,首先导入 Mininet 中的 Topo 模块,然后创建自定义网络拓扑类 MyTopo,依次添加交换机(s1 和 s2)、主机(h1、h2 和 h3)和网络链路(h1-s1、h2-s2、h3-s2 以及 s1-s2)。在添加主机时,自定义该主机网卡 MAC 地址;如未自定义 MAC 地址,系统会默认分配。

(2)SDN 组网。

①搭建拓扑环境。

首先开启控制器 Ryu,生成并下发 SDN 交换机流规则,以让拓扑脚本所描述的网络拓扑在 Mininet 平台上运行起来。通过源码方式安装 Ryu,从终端进入 ryu/ryu/app 目录,执行 ryu-manager 命令运行 Ryu 控制器默认的 simple_switch_13.py 文件,从而定义交换机功能。

获取运行 Mininet 的虚拟机本地 IP 地址,作为 Mininet 连接控制器的 IP 地址,然后以超级管理员运行拓扑脚本,让 Mininet 在虚拟机中生成相应的网络,具体命令为:mn --custom script-directory --topo topo-name [--switch ovsk, protocol = OpenFlow13] --controller=remote,ip=ip_adderss,port=port_number。

命令中参数的含义分别为:custom(创建的脚本文件目录);topo(拓扑脚本中定义拓扑结构的类);switch(指定交换机类型与通信协议类型);controller(指定控制器)。

Mininet 运行网络拓扑脚本的过程,可以通过控制器 Ryu 来监视。当 Mininet 生成网络拓扑时,Ryu 会收到由网络中交换机发往 Ryu 的大量 packet in 消息,说明 Mininet 与控制器 Ryu 连接成功并且网络拓扑搭建完成。

②配置 IPv6 环境。

使用拓扑脚本搭建的网络环境默认为 IPv4,需在此基础上进一步配置 IPv6 网络环境,本次仿真需配置主机 IPv6 地址。配置主机 IPv6 地址,首先需要通过 net 命令查询到主机模拟网卡的名称,本次仿真 net 命令查询结果为:主机 h1(h1-eth0)、主机 h2(h2-eth0)和主机 h3(h3-eth0)。

根据查询到的主机网卡名,对拓扑中的三台主机逐个配置 IPv6 地址,配置命令如表 2 所示。

为主机配置 IPv6 地址之后,可以使用 ping6 命令依次测试 IPv6 环境下各主机之间的连通性,从而完成 IPv6 仿真环境搭建。

表 2　配置主机 IPv6 地址

| 主机 | 配置命令 | 配置信息 |
|---|---|---|
| h1 | h1 ifconfig h1-eth0 inet6 add fc00::1/64 | IPv6: fc00::1/64 MAC: 00:00:00:00:00:01 |
| h2 | h2 ifconfig h2-eth0 inet6 add fc00::2/64 | IPv6: fc00::2/64 MAC: 00:00:00:00:00:02 |
| h3 | h3 ifconfig h3-eth0 inet6 add fc00::3/64 | IPv6: fc00::3/64 MAC: 00:00:00:00:00:03 |

(3)协议分析。

在虚拟机中安装 Scapy,然后在 Mininet 平台上运行的主机 h1 中引入 Scapy,以 Scapy 提供的 Python API 构造 IPv6 网络 ping6 数据包,分析 ICMPv6 协议工作过程,关键开发代码如表 3 所示。

表 3　基于 Python 开发构造 IPv6 网络 ping6 数据包

| 关键步骤 | Python 脚本 |
|---|---|
| 步骤一:设定数据包的目的地址 | a=IPv6(dst="fc00::2") |
| 步骤二:ICMPv6 协议使用默认参数 | b=ICMPv6EchoRequest() |
| 步骤三:将构造的数据包发送 | send(a/b) |

通过在虚拟机上运行 Wireshark 对流经主机 h2 网卡的数据包进行分析。在此次 ping6 报文的交互过程中,主机 h1 向主机 h2 发出 ping6 请求数据包,主机 h2 及时响应,发出 ping6 回复数据包给主机 h1。

(4)网络攻击。

①主机 h1 与主机 h2 正常通信。

使用 ping6 命令模拟主机 h1 与 h2 之间的正常通信。在主机 h1 中以命令"h1 ping6 -c 3 fc00::2"给主机 h2 发送 3 个 ping6 请求数据包,同时主机 h2 给主机 h1 及时回复 3 个 ping6 回复数据包。

②攻击方 h3 发起攻击。

攻击方 h3 开启虚拟终端启动 Scapy,通过 Python 开发伪造 NS 报文,欺骗主机 h2。伪造报文中源 IPv6 地址是主机 h1 的 IPv6 地址(fc00::1),目的 IPv6 地址是主机 h2 的 IPv6 地址(fc00::2),而源 MAC 地址是攻击方 h3 的 MAC 地址(00:00:00:00:00:03)。关键步骤如表 4 所示。

③主机 h1 与主机 h2 通信中断。

主机 h3 发起攻击,此时主机 h1 再以命令"h1 ping6 -c 3 fc00::2"给主机 h2 发送 3 个 ping6 请求数据包,发现它不会再收到主机 h2 的响应。主机 h1 与 h2 的正常通信中断。

(5)攻击防御。

在上述攻击仿真实验中,攻击方 h3 通过不断发送

伪造报文,欺骗主机 h2 更新错误的邻居列表,从而达到中断正常通信并截获主机 h1 与 h2 的通信信息的攻击效果。针对这种攻击方式,可以通过给主机 h2 添加静态邻居表项进行防御。

表 4 攻击脚本的关键步骤

| 关键步骤 | Python 攻击脚本 |
|---|---|
| 步骤一:设定报文中的源地址与目的地址 | a=IPv6(src="fc00::1",dst="fc00::2") |
| 步骤二:设定发往目的主机的 IPv6 地址 | b=ICMPv6ND_NS(tgt="fc00::2") |
| 步骤三:设定报文中的源链路地址 | c=ICMPv6NDOptSrcLLAdd<br>r(lladdr="00:00:00:00:00:03") |
| 步骤四:使用默认的参数 | d=ICMPv6NDOptMTU() |
| 步骤五:以每秒一次的频率发送报文 | send(a/b/c/d,inter=1,loop=1) |

通过命令“h2 ip neighbor add fc00::1 lladdr 00:00:00:00:00:01 nud permanent dev h2-eth0”,将主机 h1 的 IPv6 地址(fc00::1)与 MAC 地址(00:00:00:00:00:01)绑定在主机 h2 的邻居列表中,可以达到防御 NDP 中间人攻击的效果。当添加静态邻居表项后,即使攻击方 h3 发出大量伪造数据包,主机 h2 也不会更新自己的邻居列表,攻击方 h3 不能截获通信信息。

### 3.3 可视化分析

当攻击方 h3 发起攻击之后,对主机 h1 与 h2 的通信过程的数据包进行可视化分析,如图 5 所示。

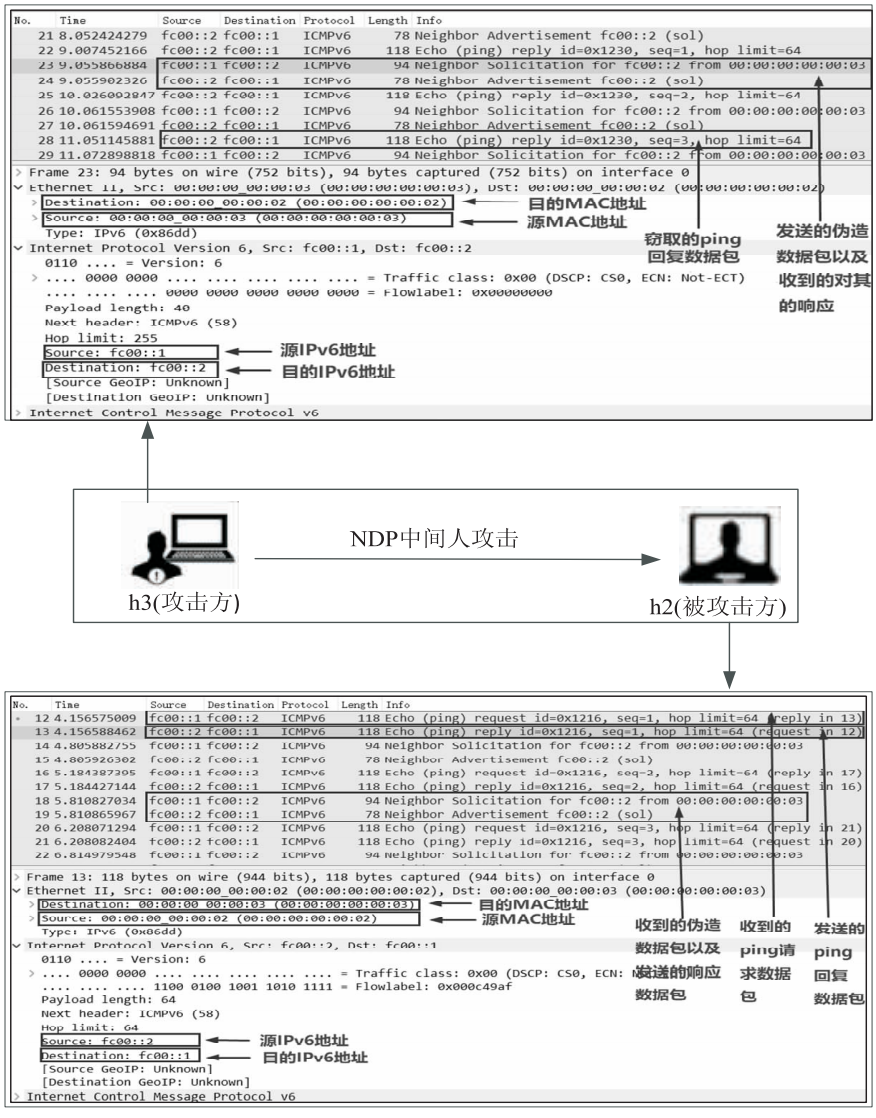


图 5 NDP 中间人攻击可视化分析

对于主机 h2 而言,收到大量由 fc00::1 发出的数据包,并且告诉它,IPv6 地址为 fc00::1 的主机的网卡地址为 00:00:00:00:00:03,此时它将更新自己的邻居列表。当收到来自 fc00::1 的 ping6 请求数据包时,它

必须对其响应,发出回复数据包。要对 fc00::1 发回复数据包时,需要查看自己的邻居列表,发现 fc00::1 对应的网卡地址为 00:00:00:00:00:03,于是对该网卡发出回复数据包。

对攻击方 h3 而言,在发出大量伪造报文的同时,收到来自 fc00::2 的 ping6 回复数据包,即成功截获到了主机 h1 与 h2 的通信信息。

## 4　结束语

面对软件定义网络以创新驱动发展加快形成战略性高技术产业的态势,以“新工科”产教融合协同创新为引领开展软件定义网络 IPv6 安全仿真技术探索既可有效促进软件定义网络产业链与人才链更加紧密契合,又可通过仿真技术创新赋能学科专业主动布局软件定义网络前沿发展。

该文针对软件定义网络 IPv6 体系下的安全仿真技术缺乏的现状,提出了基于“Python+Mininet”的软件定义网络 IPv6 安全仿真技术,通过 IPv6 邻居发现协议攻击与防御及可视化分析的教学应用表明该技术具有轻量级、可开发和一体化等优点,为高校面向未来网络空间安全教学改革提供新的技术途径。

**参考文献:**


[1] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow: enabling innovation in campus networks[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74.

[2] 于天放,芮兰兰. 基于 OpenFlow 的 SDN 架构研究与实践[J]. 计算机技术与发展,2018,28(7):159-164.

[3] THYAGATURU A S, MERCIAN A, MCGARRY M P, et al. Software defined optical networks (SDONs): a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2016, 18(4): 2738-2786.

[4] JAIN S, KUMAR A, MANDALS, et al. B4: experience with a globally-deployed software defined WAN[C]//Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM. Hong Kong, China: ACM, 2013: 3-14.

[5] BERDE P, GEROLA M, HART J, et al. ONOS: towards an open, distributed SDN OS[C]//Hot topics in software defined networking (HotSDN). Chicago, USA: ACM, 2014: 1-6.

[6] 赵　鹏,段晓东. SDN/NFV 发展中的关键:编排器的发展与挑战[J]. 电信科学,2017,33(4):18-25.

[7] LANTZ B, HELLER B, MCKEOWN N. A network in a laptop: rapid prototyping for software-defined networks[C]//Proceedings of the 9th ACM SIGCOMM workshop on hot topics in networks. Monterey, California: ACM, 2010: 1-6.

[8] WANG S, CHOU C, YANG C. EstiNet openflow network simulator and emulator[J]. IEEE Communications Magazine, 2013, 51(9): 110-117.

[9] 蔡文郁,刘晓玲. 计算机网络启发式 NS-3 仿真案例教学模式[J]. 实验室研究与探索,2018,37(9):95-100.

[10] TKACHOVA O, SALIM M J, YAHYA A R. An analysis of SDN-OpenStack integration[C]//2015 second international scientific-practical conference problems of infocommunications science and technology (PIC S&T). Kharkiv: IEEE, 2015: 60-62.

[11] 黄家玮,韩　瑞,钟　萍,等. 基于 Mininet 的计算机网络实验教学方案[J]. 实验技术与管理,2015,32(10):139-141.

[12] 黄家玮,刘敬玲,徐文茜,等. 软件定义网络的实验教学方案设计[J]. 计算机教育,2017(3):152-154.

[13] 黄家玮,李淑平,计　玮,等. 基于 SDN 架构的网络空间安全实验教学设计[J]. 实验科学与技术,2018,16(5):43-46.

[14] 徐　磊. 基于软件定义网络的计算机网络课程实验教学研究[J]. 计算机教育,2017(5):150-153.

[15] 申海杰,陈　靖,陈晓范,等. 基于 SDN 的网络虚拟化实验教学方案[J]. 微型电脑应用,2018,34(1):32-36.

[16] 宋广佳,崔坤鹏. SDN 技术在计算机网络实验教学中的应用-以 MAC 地址学习为例[J]. 科学技术创新,2018(17):67-69.

[17] 叶　进,冯露葶,何华光,等. 基于虚拟化技术的软件定义网络实验教学方案[J]. 实验室研究与探索,2017,36(3):79-82.

[18] 国务院学位委员会 教育部. 国务院学位委员会 教育部关于增设网络空间安全一级学科的通知[A]. 2015-06-11.

[19] 王　月,吕光宏,曹　勇. 软件定义网络安全研究[J]. 计算机技术与发展,2018,28(4):128-132.

[20] 费　宁,刘春秋. 基于 OpenDaylight 防火墙的研究与实现[J]. 计算机技术与发展,2019,29(6):112-115.

[21] 中共中央办公厅 国务院办公厅印发《推进互联网协议第六版(IPv6)规模部署行动计划》[J]. 中华人民共和国国务院公报,2017(34):6-12.

[22] 陈蔚瀚,黄小红,苑婷婷,等. 基于 SDN 的跨 IP 协议的流量调度优化模型[J]. 东南大学学报:自然科学版,2017,47(S1):34-38.

[23] 李　丹,秦　华. SDN 网络 IPv6 组播机制研究[J]. 通信技术,2018,51(5):1110-1116.