软件定义的 L2/L3 地址协同拟态伪装策略研究

王鹏超,陈福才,程国振,陈 扬,谷允捷
(国家数字交换系统工程技术研究中心,河南郑州 450002)

摘 要: 从网络内部探测目标终端的脆弱性是网络攻击发起的主要途径,当前网络的静态特性利于攻击者目标侦察的实施,网络内部的 L2/L3 地址是攻击者期望侦察的主要信息. 为了改变目标侦察阶段网络攻防的易攻难守态势,基于拟态伪装的思想,提出了一种 L2 和 L3 地址协同动态化技术,在不影响正常业务条件下有策略地隐藏真实网络主机. 首先,建立网络侦察的博弈模型(CRG),基于 NASH 均衡解指导 L2/L3 地址的拟态伪装策略,并给出最优的跳变周期计算公式;其次,基于软件定义网络架构,设计并实现了协同动态化的内网防护系统(CMID),由 SDN 控制器协同控制 L2/L3 地址的伪装变换;最后,理论分析与实验结果表明:上述方法能够有效切断 L2/L3 地址与真实网络身份、上层服务的关联性,最大化地隐藏网络内部主机,延缓侦察速度,阻断网络攻击的连续性.

关键词: 目标侦察; 软件定义网络; 拟态伪装; 纳什均衡; 网络防御; 地址跳变
中图分类号: TP393.0 **文献标识码:** A **文章编号:** 0372-2112 (2019)10-2032-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.10.003

L2/L3 Address Cooperative Mimicry Strategy Research Based on SDN

WANG Peng-chao, CHEN Fu-cai, CHENG Guo-zhen, CHEN Yang, GU Yun-jie
(*National Digital Switching System Engineering and Technological R&D Center, Zhengzhou, Henan* 450002, *China*)

Abstract: The detection of the vulnerability of the target host from the intranet is the main way to initiate the network attack. The static characteristics of the current network are beneficial to the implementation of attacker reconnaissance, and the L2/L3 address inside the network is the main information that the attacker expects to scout. In order to change the network attack and defense situation in the reconnaissance stage, based on the idea of mimicry camouflage, a collaborative dynamic technology of L2 and L3 addresses is proposed to strategically hide the real network host without affecting normal business conditions. Firstly, the cyber reconnaissance game (CRG) is established. Based on the NASH equilibrium solution, the mimetic camouflage strategy of L2/L3 address is solved, and the optimal mutation period calculation formula is given. Secondly, based on the software-defined network architecture, the cooperative mutation intranet defense system (CMID) is designed and implemented, and the SDN controller cooperatively controls the camouflage transformation of the L2/L3 address. Finally, the theoretical analysis and experimental results show that the above method can effectively cut off the correlation between L2/L3 address and real network identity and upper-layer services, maximally hide the internal hosts of the network, delay the reconnaissance speed, and block the continuity of network attacks.

Key words: reconnaissance; software defined network; mimicry; NASH equilibrium; cyber defense; address mutation

1 引言

目标侦察(reconnaissance)作为绝大多数网络攻击发起的第一阶段,是攻击者确定系统中目标主机,展开后续一系列攻击行为的先决条件[1]. 高级的攻击者在面对有一定防护的高价值目标网络系统时,可以通过探测探针来尽可能多地收集目标网络系统中主机的各种属性信息[2](包括 L2/L3 地址、服务端口、操作系统、运行的服务等),尤其是 L2/L3 地址,即 TCP/IP 网络中的 MAC/IP 地址,是攻击者获取网络拓扑结构、开放服

收稿日期:2018-12-04;修回日期:2019-05-29;责任编辑:蓝红杰
基金项目:信息工程大学新兴方向研究项目(No. 2016610708);国家自然科学基金(No. 61602509);国家自然科学基金创新群体项目(No. 61521003);国家重点研发计划项目(No. 2016YFB0800100, No. 2016YFB0800101)

务等的前提[3].

传统被动式网络安全防御技术(如防火墙、入侵检测等)并不能有效应对攻击者的目标侦察[4].有研究论证过以每分钟一次的速率扫描的扫描蠕虫可以轻易地规避所有主要的检测技术[5].为改变网络空间的这种攻防不对称性,各种动态网络防御技术被相继提出.但目前,对抗攻击者目标侦察阶段的动态网络防御技术多为单一网络属性的动态化,如地址跳变[6,7]、端口跳变[8]、动态拓扑[9]等.在地址跳变方面,研究多局限于IP的动态化上,对MAC动态化的实现尚无具体研究.而相对于服务端口、操作系统、运行的服务等网络属性,MAC的全球唯一性令其具有更高安全研究价值,其次基于MAC来识别固定主机是除IP外,被高级攻击者优先考虑的识别主机的重要方式.

动态网络防御技术分为基于传统网络实现和基于软件定义网络实现,可动态化的网络属性包括IP、MAC、端口、运行服务、操作系统、网络拓扑、传输路径等.早期的相关技术研究如DyNAT[10]、NASR[11]、MT6D[12]、RHM[13]等均是基于传统网络实现,其可动态化的网络属性单一、协同困难,动态化频率低,需要在终端安装安全应用软件或在网络中增加硬件设备,难以大规模部署.

软件定义网络(Software Defined Network,SDN)[14]是一种新型网络创新架构,其核心是在网络中引入SDN控制器,实现转控分离、集中控制与可编程等特性,易于动态网络防御技术的开发与部署.迄今为止,随着传统网络向SDN的逐步迁移,基于SDN实现动态网络防御技术得到重视.Jafarian等人提出的基于OpenFlow的随机主机地址突变(OpenFlow Random Host Mutation,OF-RHM)[15]技术,通过集中的SDN控制器(NOX)控制连接两个通信主机的接入交换机,修改报文中的IP,实现基于虚假IP的通信.OF-RHM对抗攻击者扫描的有效性建立在高频的IP跳变之上,高频的跳变导致其具有通信时延高,流表数目多,开销巨大等缺点.

拟态伪装是生物界"策略性"避免敌手识别的有组织行为,通过关键属性的协同变换以隐藏自身.在TCP/IP网络架构下,L2/L3地址即是网络元素在网络中的身份标识,其也为L4~L7服务提供地址服务.隐藏L2/L3地址能够有效切断网络主机身份与L4~L7服务的关联性.

基于上述分析,本文提出一种基于SDN的L2/L3地址协同拟态伪装策略,在不影响正常业务条件下有组织地隐藏真实网络主机.具体地,首先将目标侦察阶段的网络攻防对抗建立为一个双玩家的非零和混合战略博弈模型,通过求解纳什均衡,得到防御者采用周期性协同跳变是对抗攻击者独立同分布的攻击的最优伪装策略,通过博弈论来指导动态化周期的生成,实现该协同动态化技术的效能最优;其次,基于软件定义网络架构,设计并实现了协同动态化的内网防护系统(Cooperative Mutation Intranet Defense System,CMID),由SDN控制器协同控制L2/L3地址的伪装变换;最后,理论分析和实验评估均表明上述方法能够有效隐藏网络内的主机行为.

2　技术实现

CMID的通信流程涉及DNS域名解析、ARP地址解析、DHCP动态分配真实与虚假资源、流表下发、OF交换机对通信报文的处理等步骤.表1是通信流程涉及的符号说明.

内网中的通信报文分为域内报文和域外报文.域内报文进行地址的跳变,域外报文使用传统的NAT方式处理.域内报文的完整通信流程的时间轴如图1所示.

表1　通信流程的符号说明

符号	含义
*A*_rIP	终端*A*的真实IP
*A*_vIP	终端*A*的虚拟IP
*A*_rMAC	终端*A*的真实MAC
*A*_vMAC	终端*A*的虚拟MAC
*B*_eDomain	终端*B*的临时域名
*G*_MAC	网关的MAC
->	地址修改操作
sRip	通信会话中源端的真实IP
dVmac	通信会话中目的端的虚拟MAC
sPort	通信会话中的源端口
Protocol	通信会话采用的协议类型
TTL	通信会话的生命周期

2.1　DHCP动态分配资源

终端的DHCP_DISCOVER报文进入接入端交换机,交换机匹配预设的流规则将其送达控制器.控制器的动态处理模块查询信息存储模块已存储的管理层面发送的预配置信息,广播携带rIP的DHCP_OFFER消息.当终端的DHCP_REQUEST报文送达控制器,动态处理模块随机生成它的vIP和eDomain,并修改信息存储模块即下发DHCP_ACK消息,完成DHCP动态分配资源过程,即图1中①、②.

2.2　ARP地址解析

由于通信双方的IP必定不在同一网段,终端只会发送询问网关MAC的ARP_REQUEST报文,交换机预设的流规则将ARP类型的报文送达控制器,控制器的

地址解析模块处理 ARP 报文并回复携带网关 G_MAC 的 ARP_REPLY 报文,即图 1 中③.

2.3 通信双方建立会话

CMID 为通信双方建立一个十元数组表示的 Session,S = {sRip, sVip, dRip, dVip, sRmac, dVmac, sPort, dPort, Protocol, TTL}. S 即控制器为交换机下发的流规则的匹配项,会话将在控制器中存储,下发至交换机中的相应的流表则在 TTL 到期时销毁. 通信双方建立会话的具体流程如下.

步骤④、⑤、⑥:终端 A 尝试与终端 B 建立连接. 终端 A 首先通过带外方式请求终端 B 的域名(④),终端 B 通过 DNS 查询报文在控制器的域名解析模块查询获取 B_rIP 对应的 B_eDomain(⑤),终端 B 带外方式向终端 A 回复 B_eDomain.

步骤⑦:终端 A 通过 DNS_QUERY 报文查询 B_eDomain 对应的 IP,DNS 报文按照接入端交换机预设的流规则被上传至控制器,控制器的域名解析模块回复终端 A 携带 B_vIP 的 DNS_RESPONSE 报文.

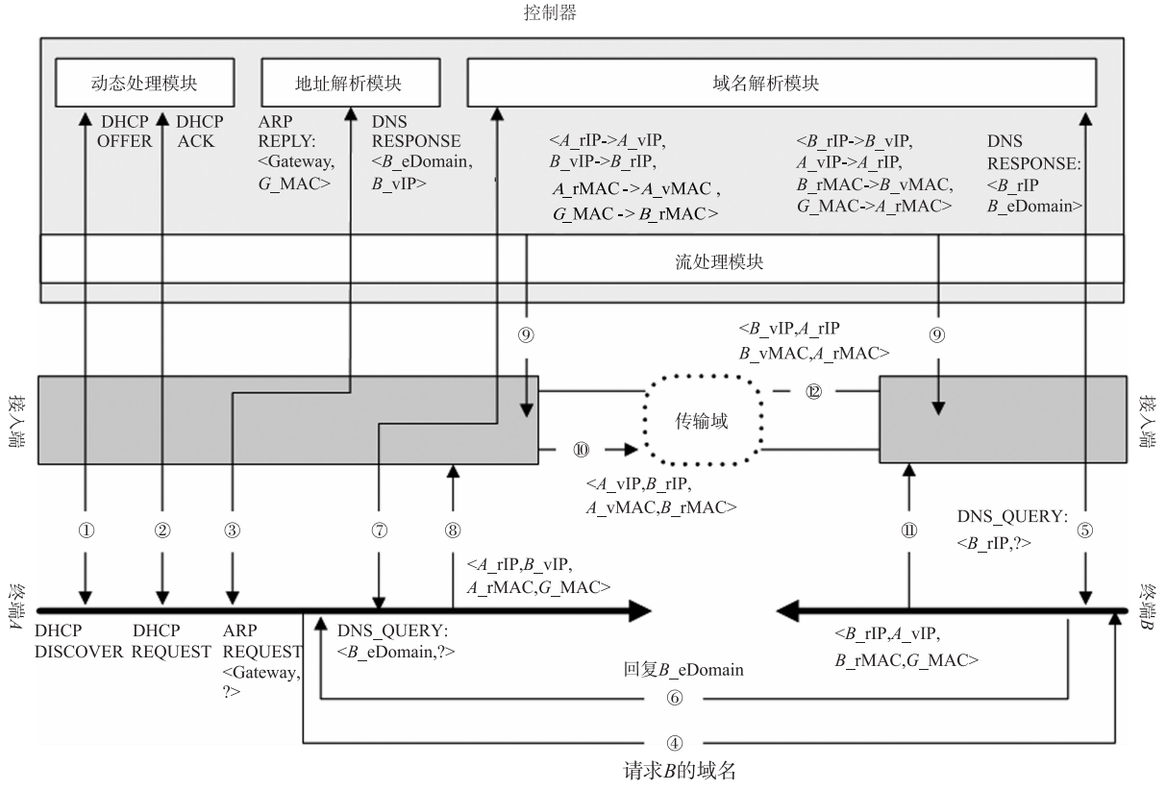

图1 通信流程的时间轴图

步骤⑧~⑫:终端 A 向终端 B 发送报文头为 <A_rIP, B_vIP, A_rMAC, G_MAC> 的数据分组,即源 IP 为 A 的真实 IP、目的 IP 为 B 的虚假 IP、源 MAC 为 A 的真实 MAC、目的 MAC 为网关 MAC 的数据分组. 当该报文头类型的数据分组首次到达接入端交换机时(⑧),由于交换机中并无与之匹配的流表,交换机将其封装为 Packet_In 消息送达控制器. 控制器根据报文头由路由算法计算并建立传输路径,并向该路径上的交换机下发修改 IP、MAC 的流表(⑨). 报文头匹配 <A_rIP, B_vIP, A_rMAC, G_MAC> 的分组,将以修改后的报文头为 <A_vIP, B_rIP, A_vMAC, B_rMAC> 的数据分组按照建立的传输路径达到终端 B(⑩). 终端 B 向终端 A 发送的报文头为 <B_rIP, A_vIP, B_rMAC, G_MAC> 的数据分组在输入端被改为 <B_vIP, A_rIP, B_vMAC, A_rMAC> 后(⑪、⑫),按照同样的传输路径被交换机转发送达终端 A.

3 博弈论指导的最优伪装策略

缺乏理论指导的动态化实现对于复杂的网络攻防防御效果有限. 文献[16]、[17]等采用博弈论来建立网络攻防对抗模型,制定防御策略,有效地实现了防御性能最优化.

3.1 网络侦察博弈模型

网络侦察的博弈(Cyber Reconnaissance Game, CRG)是防御者(系统管理员)和攻击者(黑客)之间的一个基于连续时间的二人博弈模型. 博弈双方关于 $N(t)$ 个独立节点(真实终端)在任意时刻选取行动(攻击或地址跳变),每次行动都要付出一定的开销. 图 2

为 CRG 模型:在任意时刻 t,节点都在 t 之前最后占领该节点的一方的控制下. 攻击者控制节点 H_j 时,每单位时间从节点 H_j 获得的收益为 r_j,攻击者每次攻击节点 H_j 的开销为 P_j^A,攻击从侦察开始到发现该节点需要一段随机的时间 ω_j. 防御者每次执行地址跳变的行动时,即使节点 H_j 处于被攻击状态,节点 H_j 也会立即恢复(目的地址更改后,攻击者需要重新与目标节点建立连接,攻击状态终止),其防御行动的开销为 P_j^D. r_j、P_j^A、P_j^D、ω_j 的分布均是博弈双方的共同知识.

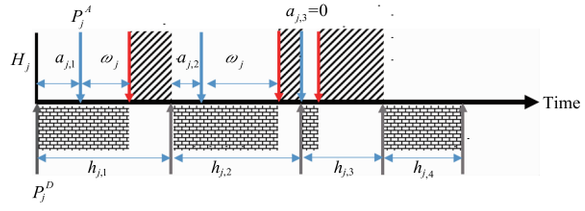

图2　CRG模型

用 $a_{j,k}$ 表示攻击者在节点 H_j 第 k 次地址跳变后发起攻击的等待时间,$a_{j,k}$ 是一个随机变量. 攻击者的策略是确定行动集合 $\{a_{j,k}\}$. 由于每个节点均是独立的,不失一般性,$a_{j,k}$ 关于 j 相互独立. 然而,攻击者可能采取与时间相关的攻击策略[18],$a_{j,k}$ 关于 k 不一定独立. 防御者的策略是确定各个节点每次地址跳变的时间 $\{h_{j,k}\}$,$h_{j,k}$ 表示节点 H_j 的第 k 次地址跳变获取的虚假 IP、虚假 MAC 的持续时间.

3.2　防御者的收益函数

给定攻击者策略 $\{a_{j,k}\}$,防御者的目标是使得关于 $\{h_{j,k}\}$ 的带偏好的收益函数 $\mu_d(\{a_{j,k}\},\{h_{j,k}\})$ 取值达到最大化:

$$\max_{\{h_{j,k}\},M_j} E\left[\sum_{j=1}^{N}\frac{-r_j\left(T-\sum_{k=1}^{M_j}\min(a_{j,k}+\omega_j,h_{j,k})\right)-M_jP_j^D}{T}\right]$$
$$\text{s. t.}\ \sum_{j=1}^{N}\frac{M_j}{T}\le B\ \text{w. p. 1}$$
$$\sum_{k=1}^{M_j}h_{j,k}\le T\ \text{w. p. 1}\ \forall j \tag{1}$$

3.3　攻击者的收益函数

攻击者攻击节点 H_j 的总开销为 $\left(\sum_{k=1}^{M_j}1_{a_{j,k}<h_{j,k}}\right)P_j^A$,对于给定的防御者策略 $\{h_{j,k}\}$,攻击者的目标为使关于其行动集合 $\{a_{j,k}\}$ 的带偏好的收益函数 $\mu_a(\{a_{j,k}\},\{h_{j,k}\})$ 取值最大化:

$$\max_{\{a_{j,k}\},M_j} E\left[\sum_{j=1}^{N}\frac{r_j\left(T-\sum_{k=1}^{M_j}\min(a_{j,k}+\omega_j,h_{j,k})\right)}{T}-\frac{\left(\sum_{k=1}^{M_j}1_{a_{j,k}<h_{j,k}}\right)P_j^A}{T}\right]\text{s. t. }E\left[\sum_{j=1}^{N}\frac{\int_0^T\lambda_j(t)\,\mathrm{d}t}{T}\right]\le R \tag{2}$$

约束条件表示攻击者在任意时刻可以攻击的平均节点数的上限为一个常数 R,$\lambda_j(t)$ 为示性函数.

3.4　NASH 均衡

定义 1　给定 M_j,定义对于节点 H_j 的防御策略集合 Ω_j 为满足以下性质的 $\{h_{j,k}\}$ 的集合:

(a) $\sum_{k=1}^{M_j}h_{j,k}=T$;

(b) $F_{a_{j,k}+\omega_j}(h_{j,k})=F_{a_{j,s}+\omega_j}(h_{j,s})\ \forall k,s$

其中,$F_{a_{j,k}+\omega_j}(\cdot)$ 为 $h_{j,k}$ 的边际分布.

引理 1　当攻击为非适应性时,给定满足 $\sum_{j=1}^{N}\frac{M_j}{T}\le B$ 的节点地址跳变次数集合 $\{M_j\}$,若 $\Omega_j\neq\varnothing$,$\forall j\in N$,则 $\forall\{h_{j,k}\}\in\Omega_j$,$\forall j\in N$ 均是防御者的最优反应.

定义 2　称攻击者的策略为独立同分布的,若攻击满足以下条件:

(a) 攻击是非适应的;

(b) 攻击对各个节点是独立的,$\{a_{j,k}\}$ 关于 j 独立;

(c) 对单个节点的攻击等待时长 $\{a_{j,k}\}$ 关于 k 是独立同分布的.

定理 1　周期性策略是防御者对抗独立同分布的攻击策略的最优反应.

证明　给定 $\{M_j\}$,令

$$h_j=(h_{j,1},h_{j,2},\cdots,h_{j,M_j})\triangleq\left(\frac{T}{M_j},\frac{T}{M_j},\cdots,\frac{T}{M_j}\right)$$

周期性策略 $\{h_j\}$ 满足定义 1 的条件(a). 攻击策略为独立同分布的,由定义 2 的条件(c),周期性策略 $\{h_j\}$ 也满足定义 1 的条件(b). 应用引理 1,即证.

定理 1 表明防御者试图以确定性的方式来平衡其在每个时期的预计损失,周期性的防御策略保证了防御者的防御策略的稳定性,避免防御者在某时刻的大损失.

引理 2　当给定防御者的策略,攻击者的最优反应一定满足以下条件:

$$a_{j,k}^{*}=\begin{cases}0, & \text{w. p. } p_{j.k}\\ \ge h_{j,k}, & \text{w. p. } 1-p_{j.k}\end{cases} \tag{3}$$

证明　将式(2)分割为 N 个独立的子问题,对每个节点,每个子问题都有一个类似的目标函数和一个常数值 R_j,满足 $\sum_{j=1}^{N}R_j=R$,形式如下:

$$\max_{a_{j,k}} \sum_{k=1}^{M_j} \frac{r_j \cdot E[\min(a_{j,k}+\omega_j, h_{j,k})] + P(a_{j,k} < h_{j,k}) P_j^A}{T}$$
$$\text{s.t.} \sum_{k=1}^{M_j} \frac{E[\min(a_{j,k}+\omega_j, h_{j,k})] - E[\min(a_{j,k}, h_{j,k})]}{T} \leq R_j \tag{4}$$

每一个子问题可再进一步分解为 M_j 个独立子问题,每个子问题都有一个常数值 $R_{j,k}$, $\sum_{k=1}^{M_j} R_{j,k} = M_j$. 由于节点独立,引理 2 的证明等价于证明这些子问题.

引理 2 表明对于每个节点 H_j,攻击者的最优策略是在节点 H_j 地址跳变完成后立即发起对该节点的攻击步骤(从扫描嗅探开始),或者在防御者的下一次地址跳变完成前放弃攻击. 式(2)的约束 R 实际上确定了攻击者立刻发起攻击的概率. 若上限 R 足够大,则攻击者可以在防御者每次地址跳变后立即发起攻击.

定理 2 当防御者的地址动态化为周期性的,攻击者的最优反应为独立同分布的攻击.

证明 若防御者周期性地址动态化,对于每个节点,均有 $h_{j,k} = \frac{T}{M_j}$, $\forall k$,式(2)为一个部分背包问题(fractional knapsack problem),且所有 $p_{j,k}$ 的单位报酬(目标函数的报酬除以约束的权重)是相等的. 因此,令所有的 $p_{j,k}$ 相等,可以使得 $a_{j,k}$ 关于 j 是独立同分布的,对任意给定的 R_j, $a_{j,k}$ 是式(4)的最优解. 因此,发起独立同分布的攻击的策略是式(2)的最优解,即证得攻击者的最优反应为独立同分布的攻击.

由定理 1 和定理 2,攻击者独立同分布攻击策略与防御者周期性策略互为最优反应,为 CRG 的一个纳什均衡.

3.5 动态化周期的最优选取

对于给定的系统运行时间 T,选定周期性动态化策略(给定周期 h),系统的当前节点数为 $N(T)$,对每个节点 $H_j, j \in N(T)$ 有 $M_j = M = \left[\frac{T}{h}\right]$(取整数). 由凸优化问题式(1)可知(引理 1),求解最优周期 h 的问题即为寻找某个整数 h^*(秒级跳变),使得防御者的收益最大化. 将式(2)化为混合整数线性规划问题(MILP 问题)可求解 h^*:

$$\max_h E\left[\sum_{j=1}^{N(T)} \frac{-r_j\left(T - \sum_{k=1}^{[\frac{T}{h}]} \min(a_{j,k}+\omega_j, h)\right) - \left[\frac{T}{h}\right] P_j^D}{T}\right]$$
$$\text{s.t.}\ 0 \leq T - \left[\frac{T}{h}\right] < h$$
$$0 < \frac{1}{h} \leq B' \tag{5}$$

MILP 问题通常是 NP-hard 的. 上述 MILP 问题可处理为简单的线性规划问题(LP):

$$h^* = \arg\max_{h \in (0,T)} E\left[\sum_{j=1}^{N(T)} \frac{-r_j\left(T - \sum_{k=1}^{[\frac{T}{h}]} \min(a_{j,k}+\omega_j, h)\right)}{T} - \left[\frac{T}{h}\right] P_j^D\right] \tag{6}$$

4 实验与性能分析

本节对采取周期性伪装策略的 CMID 进行通信性能、控制器性能、防御性能三个方面的实验测试与性能分析.

4.1 通信性能

使用 FileZilla 经由 FTP 协议传输一个 68MB 大小的文件. 图 3 为分别在 CMID、OF-RHM、普通模式下测试得到的传输速率.

普通模式、CMID、OF-RHM 达到一个基本稳定的传输速率的时间分别为 α、β、γ, $\alpha < \gamma$, $\alpha < \beta$ 表明相较于普通模式(无地址跳变的内网系统),地址跳变技术(CMID、OF-RHM)由于第一个报文需要上传控制器,并由控制器下发相应的流规则,其达到稳定传输速率的时间更长. CMID 仅需控制器向接入端交换机下发修改报文 IP、MAC 的流规则,OF-RHM 则需要控制器向接入端与末端交换机均下发修改报文流规则,故 $\beta < \gamma$. 其次,在后续的报文的传输过程中,CMID 需要在接入端交换机依照流规则修改源 MAC、源 IP、目的 MAC、目的 IP,其稳定传输速率低于普通模式. 而 OF-RHM 需额外在末端交换机修改 IP,且 CMID 的 IP 与 MAC 同时修改,CMID 的稳定传输速率高于 OF-RHM,性能开销优于 OF-RHM.

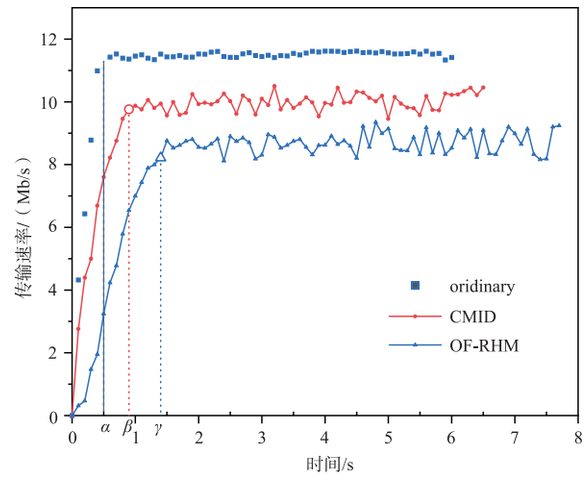

图3 传输速率

4.2 控制器性能

在服务器上分别运行 Carbon 版本的 ODL 控制器与 CMID 控制器(基于 0.5.2-Carbon 版本 ODL 控制器开发),控制器接入 Mininet 生成的 1024 个主机的树状拓扑,使用 Dstat 工具记录服务器的 CPU 与内存负载情况. 控制器负载的对比如图 4、图 5.

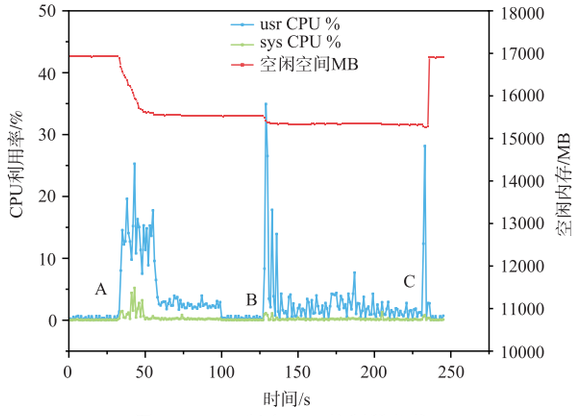

图4　Carbon版本ODL控制器负载

图 4、图 5 中标注的 *A*、*D* 表示控制器启动,*B*、*E* 表示虚拟拓扑的接入与虚拟主机两两互相通信,*C*、*F* 表示控制器关闭. 控制器启动与关闭时,CMID 控制器的 CPU 使用率与内存占用均略高于 Carbon 版本的控制器. 在虚拟拓扑接入以及虚拟主机两两通信的过程中,CMID 控制器的负载相对较高,这是由于 CMID 控制器需要为每个接入的主机周期性地生成虚拟地址并实时

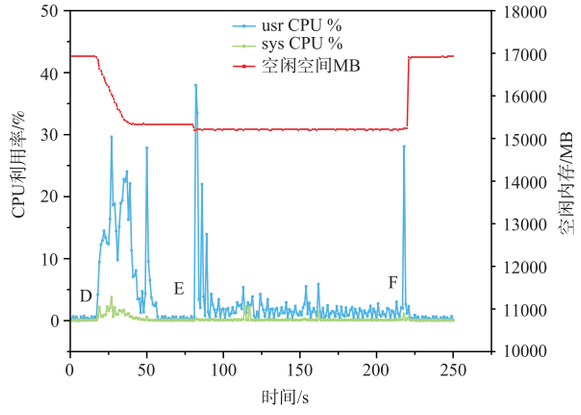

图5　CMID控制器负载

地维护一个地址映射表,这些功能带来了额外的控制器负载开销.

4.3 防御性能

4.3.1 地址动态化

主机 *A* 与 *B* 通信,*B* 端用 Wireshark 抓取通信报文,如图 6.

图 6 表明 *B* 获知 *A* 的 IP 与 MAC 均为虚假的,但仍可正常通信,CMID 提供了透明的地址跳变,终端对地址跳变无感. 式(6)设定的最优频率取值为 80s,跳变周期到时后,系统中主机的虚假地址跳变,此时 *A* 的虚假 IP 为 171.15.228.5,虚假 MAC 为 52:54:00:b9:83:d4,*B* 仍只可知 *A* 的虚假 IP 与虚假 MAC.

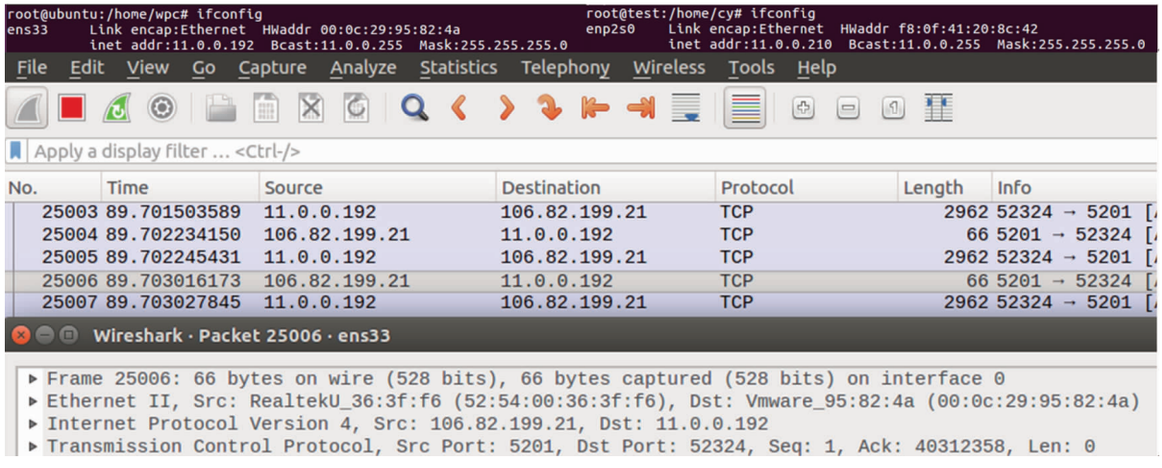

图6　主机真实地址与Wireshark抓取的通信报文

4.3.2 扫描测试

扫描测试使用 Mininet 生成多终端拓扑(150 个主机)进行仿真实验,使用 zenamp 扫描工具模拟攻击者对内网进行扫描,在 4h 内随机扫描各个网段. 对于普通模式,当攻击者确定目标系统所在的网段后,可以轻易标记出系统内所有主机. 在开启 CMID 的系统,设定不同的跳变周期(20s,40s,80s,600s,1200s,3600s),攻击者随着扫描时间嗅探到的节点个数如图 7 所示.

跳变频率较高时,由于 CMID 提供了大量的虚假 IP,虚假 IP 可能选自不同网段,攻击者需要在所有的地

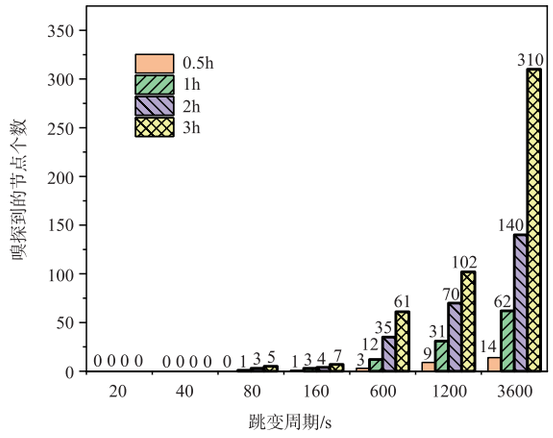

图7 扫描结果

址空间下(IPv4 地址空间最大为 2^{32})寻找主机,在一个很小的跳变周期内扫描到主机的概率为基本为 0. 当选取较大的跳变周期时,攻击者有了相对充裕的时间来扫描当前的主机地址池,如由 $T=3600$s 扫描 4h 的结果可见,攻击者可扫描到远超当前系统主机个数的 310 个节点,其中包括使用不同虚假地址的同一个真实节点. 虽然多节点的假象可以起到迷惑攻击者的目的,但攻击者仍可在残留跳变时间内(下一个跳变时刻与嗅探到主机的时刻之差)发起对嗅探到的节点的攻击. 而由于地址的周期性跳变,若攻击者在周期内没有完成攻击目的,在下一个跳变周期内,攻击者需要重新扫描建立攻击连接.

表 2 比较开启 MAC 跳变的 CMID 与关闭 MAC 跳变的 CMID 的嗅探数据. rIP/diff_MAC × 100% 为真实节点数与攻击者嗅探到的 MAC 个数的比值,该值越大,说明攻击者基于 MAC 标记主机的成功率越高. 无 MAC 跳变情况下,由不变的 MAC,高级的攻击者在分析嗅探结果后,会发现多个具有不同 IP 的节点实际为同一节点. 开启 MAC 跳变后,系统呈现给攻击者的是不同的 IP 与 MAC 地址对. MAC 动态化避免了攻击者基于 MAC 的唯一性来标记主机,在上一次攻击的基础上对标记主机执行后继攻击. MAC 的动态化有效切断了攻击者的攻击持续性,增强内网的欺骗能力.

表 2 MAC 跳变对嗅探数据的影响

	$T=3600$s 扫描 2h		$T=3600$s 扫描 6h		$T=1800$s 扫描 6h	
是否 MAC 跳变	√	×	√	×	√	×
嗅探到的节点个数	151	127	502	541	354	338
真实节点数(rIP)	83	46	147	110	121	78
不重复的 MAC 个数(diff_MAC)	151	46	502	110	354	78
rIP/diff_MAC × 100%	54.97%	100%	29.28%	100%	34.18%	100%

由式(6),求解出具有 150 个终端的内网的最优跳变周期为 128s. 攻击者扫描跳变周期为 128s 的已开启 CMID 的内网 0.5h,1h,2h,4h,嗅探到的节点数分别为 0,1,4,6,与图 7 扫描结果进行对比,采取最优跳变周期的 CMID 的抗嗅探能力比采用高频跳变的要差. 虽然越高的跳变频率提供了更高的安全性,但高频跳变需要更大的防御开销. 不同跳变周期(T)、不同终端数(N)的系统中各个终端稳定通信时内网交换机中的流表数目 M 满足:$M\propto\frac{1}{T}\cdot C_N^2$,流表数目与终端对个数 C_N^2 成正比,与跳变周期成反比. 流表数目愈多,对交换机性能的要求愈高,性能开销越大. 所以,基于博弈论指导的 CMID 综合考虑了防御性能与开销,给出了防御者对抗目标侦察的最优策略.

5 结论

本文在软件定义网络的基础上,实现了一种 L2/L3 地址的协同拟态伪装来有效欺骗发起内网侦察的攻击者. 基于博弈论权衡开销与防御性能,给出最优的拟态伪装策略. 攻击者仅能获取目的主机的虚假 IP,周期性的虚假地址跳变有效地缩短了可利用的攻击时间,MAC 的动态化使得攻击者标识主机的难度增大,无法利用 MAC 来将不同时刻采用不同虚假 IP 的同一节点进行标识,破坏攻击者基于 MAC 延续先前攻击步骤的企图. 今后的工作将继续围绕目标侦察阶段改变网络攻防的不对称性格局,结合 SDN 的开放性,增添蜜罐等虚假节点,为目标侦察阶段的攻防博弈提供威胁感知机制,创建适应性的主动防御系统.

参考文献

[1] Yadav, Tarun, and R A Mallari. Technical aspects of cyber kill chain[A]. Third International Symposium on Security in Computing and Communications[C]. London: Springer International Publishing, 2015. 438 – 452.

[2] Cai G, Wang B, Wei H U, et al. Moving target defense: state of the art and characteristics[J]. Journal of Zhejiang University Science C, 2016, 17(11): 1122 – 1153.

[3] Célestin Matte, Cunche M, Rousseau F, et al. Defeating MAC address randomization through timing attacks[A]. Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks[C]. Darmstadt: ACM, 2016. 15 – 20.

[4] Achleitner S, et al. Cyber deception: virtual networks to de-

fend insider reconnaissance[A]. Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats[C]. Vienna:ACM,2016. 57 – 68.
[5] Stafford S,Li J. Behavior-based worm detectors compared [A]. International Workshop on Recent Advances in Intrusion Detection[C]. Berlin:Springer,2010. 38 – 57.
[6] Kai W,Xi C,Zhu Y. Random domain name and address mutation (RDAM) for thwarting reconnaissance attacks [J]. Plos One,2017,12(5):e0177111.
[7] 陈扬,扈红超,等. 软件定义的内网动态防御系统设计与实现[J]. 电子学报,2018,46(11):2604 – 2611.
CHEN Y,HU H,et al. The design and implementation of a software-defined intranet dynamic defense system[J]. Acta Electronica Sinica,2018,46(11):2604 – 2611. (in Chinese)
[8] Badishi G,Herzberg A,Keidar I. Keeping denial-of-service attackers in the dark[J]. IEEE Transactions on Dependable & Secure Computing,2007,4(3):191 – 204.
[9] Duan Q,Al-Shaer E,Jafarian H. Efficient random route mutation considering flow and network constraints[A]. IEEE Conference on Communications and Network Security[C]. Washington:IEEE,2013. 260 – 268. .
[10] Kewley D,Fink R,Lowry J,et al. Dynamic approaches to thwart adversary intelligence gathering[A]. DARPA Information Survivability Conference & Exposition II[C]. Piscataway:IEEE,2001. 176 – 185.
[11] Antonatos S,Akritidis P,Markatos E P,et al. Defending against hitlist worms using network address space randomization[J]. Computer Networks,2007,51(12):3471 – 3490.
[12] Dunlop M,Groat S,Urbanski W,et al. MT6D:A moving target IPv6 defense[A]. Military Communications Conference[C]. Baltimore:IEEE,2011. 1321 – 1326.
[13] Jafarian J H,Al-Shaer E,Duan Q. An effective address mutation approach for disrupting reconnaissance attacks [J]. IEEE Transactions on Information Forensics and Security,2015,10(12):2562 – 2577.
[14] Kreutz D,Ramos F M V,Esteves Verissimo P,et al. Software-defined networking:a comprehensive survey[J]. Proceedings of the IEEE,2015,103(1):14 – 76.
[15] Jafarian J H,Al-Shaer E,Duan Q. Openflow random host mutation:transparent moving target defense using software defined networking[A]. Workshop on Hot Topics in Software Defined Networks[C]. Helsinki:ACM,2012. 127 – 132.
[16] Carter K M,Riordan J F,Okhravi H. Agame theoretic approach to strategy determination for dynamic platform defenses[A]. Proceedings of the First ACM Workshop on Moving Target Defense[C]. Scottsdale:ACM,2014. 21 – 30.
[17] Schlenker A,Thakoor O,Xu H,et al. Deceiving cyber adversaries:a game theoretic approach[A]. Proceedings of the 17th International Conference on Autonomous Agents and Multi-agent Systems (AAMAS)[C]. Stockholm:Springer,2018. 892 – 900.
[18] Clark A,Sun K,Bushnell L,et al. A game-theoretic approach to IP address randomization in decoy-cased cyber defense[A]. International Conference on Decision and Game Theory for Security[C]. London:Springer International Publishing,2015. 3 – 21.

作者简介

王鹏超　男,1995 年出生,山东烟台人. 国家数字交换系统工程技术研究中心硕士研究生,主要研究方向为网络安全和 SDN.
E-mail:17616247471@163. com

陈福才　男,1974 年出生,江西南昌人. 国家数字交换系统工程技术研究中心研究员,主要研究方向为电信网关防和网络安全.
E-mail:fucai0309@163. com

程国振　男,1986 年出生,山东菏泽人. 国家数字交换系统工程技术研究中心助理研究员,主要研究方向为云数据中心、SDN、网络安全.
E-mail:guozhencheng@hotmail. com

陈　扬　男,1994 年出生,四川南充人. 国家数字交换系统工程技术研究中心硕士研究生,主要研究方向为云计算、网络安全、SDN.
E-mail:2547756390@qq. com

谷允捷　男,1994 年出生,山东济宁人. 国家数字交换系统工程技术研究中心硕士研究生,主要研究方向为网络功能虚拟化.
E-mail:lizardwhite@163. com