

面向网络层的动态跳变技术研究进展

何威振¹, 陈福才¹, 牛杰², 谭晶磊¹, 霍树民¹, 程国振¹

(1. 信息工程大学, 河南 郑州 450001;
2. 中国人民解放军 61212 部队, 北京 100091)

摘要: 首先, 介绍了网络层跳变技术的基本概念并给出了其所能抵御的安全威胁; 接着, 从传统网络和软件定义网络给出了网络层跳变技术的两种模型和通信方式; 然后, 从跳变属性、跳变的实现方式和跳变的触发方式 3 个方面对网络层跳变技术进行分类, 并给出网络层跳变的两种评估模型; 最后, 总结了网络层跳变技术目前仍然存在的问题, 以及相应的发展方向。

关键词: 移动目标防御; 网络层动态跳变; 软件定义网络; IP 跳变; 扫描攻击

中图分类号: TP393

文献标识码: A

DOI: 10.11959/j.issn.2096-109x.2021104

Research progress on dynamic hopping technology for network layer

HE Weizhen¹, CHEN Fucal¹, NIU Jie², TAN Jinglei¹, HUO Shumin¹, CHENG Guozhen¹

1. Information Engineering University, Zhengzhou 450001, China
2. Unit 61212 of the Chinese People's Liberation Army, Beijing 100091, China

Abstract: Firstly, the basic concept of network layer hopping technology was introduced and the security threats it faced were given. Then, two type of models and communication methods of network layer hopping technology based on traditional networks and software-defined networks were given. And the network layer hopping technology was classified from three aspects of hopping attributes, the method of hopping realization and the method of hopping trigger, two evaluation models of network layer hopping were given. Finally, the problems that still exist in the network layer hopping technology and the corresponding development direction were summarized.

Keywords: moving target defense, network layer dynamic hopping, software defined network, IP hopping, scanning attack

收稿日期: 2020-12-31; 修回日期: 2021-04-27

通信作者: 何威振, weizhen9621@163.com

基金项目: 国家重点研发计划 (2021YFB1006200, 2021YFB1006201); 国家自然科学基金 (62072467)

Foundation Items: The National Key R&D Program of China (2021YFB1006200, 2021YFB1006201), The National Natural Science Foundation of China (62072467)

论文引用格式: 何威振, 陈福才, 牛杰, 等. 面向网络层的动态跳变技术研究进展[J]. 网络与信息安全学报, 2021, 7(6): 44-55.

HE W Z, CHEN F C, NIU J, et al. Research progress on dynamic hopping technology for network layer[J]. Chinese Journal of Network and Information Security, 2021, 7(6): 44-55.

1 引言

近年来,5G、物联网等技术的飞速发展,连接到互联网的设备数量飞速增加,计算机网络的复杂性到达了新的水平。然而传统网络的静态属性为攻击者(如蠕虫、木马、病毒和恶意代码等)发起有效攻击并取得成功提供了很大的优势。攻击者可以通过监视目标系统,获取目标系统配置信息,识别目标系统上可利用的漏洞,选择合适的时间和位置来发起攻击。

传统的网络防御技术(如防火墙、入侵检测系统和杀毒软件等)可以在一定程度上抵御攻击者发起的攻击,然而这些安全系统在本质上是被动且不完整的,仅能检测基于先验知识的已知漏洞,不能防御未知的漏洞和后门。特别是对于最近几年数量和复杂性激增的高级网络攻击^[1],传统的网络防御系统显得苍白而无力,进而给企业和终端用户造成声誉、社会和金融的严重损害^[2],可以看出,网络空间面临“易攻难守”的安全态势。

为了扭转这一局面,美国网络安全与信息保障研发计划提出了改变游戏规则的移动目标防御(MTD, move target defense)技术^[3],其核心思想是不通过构建一个没有漏洞的系统来增强目标系统的安全性,而利用目标系统所处的时间和空间环境,自适应改变攻击表面来增加系统的迷惑性和不确定性,使得攻击者无法在有效的时间内对目标系统制定出有效的攻击策略。即使攻击者在

当前时刻获取到目标系统的信息,但随着时空的转变,攻击者获取的关键信息也会失效,从而减小攻击者成功攻击的概率。

移动目标防御的特性根据 Cho 等^[4]的分类可以划分为3种:轮换性、多样性和冗余性,其中基于轮换的移动目标防御系统通过重新排列和随机化网络配置(如指令集、地址版图、IP、MAC、端口、路由等)来改变网络攻防的不对称格局,增加攻击者成功攻击的难度。而网络层作为网络配置中最关键的网络属性之一,基于网络层的MTD技术受到了广泛关注。然而目前尚未有学者对网络层跳变技术进行总结,尽管目前有MTD的综述^[4]介绍了基于轮换的MTD技术,但这些介绍侧重于描述MTD的发展,没有详细介绍网络层跳变技术,因此本文综述了面向网络层的动态跳变技术。

网络层动态跳变技术的发展脉络如图1所示。2001年,美国国防高级防御研究计划局在信息安全项目中首次提出了基于IP跳变的动态地址转换技术^[5],之后国内外研究机构持续跟进,相继提出APOD^[6]、MT6D^[7]、RHM^[8]、端地址跳变^[9]等网络层跳变技术,这些技术部署于传统网络,需要解决终端之间同步问题,以及部署跳变系统带来的性能损失问题。因此,软件定义网络(SDN)的兴起为网络层动态跳变技术的发展带来了革命性的转变,2012年,网络层跳变技术首次被应用于软件定义网络,并在该技术的基础上涌

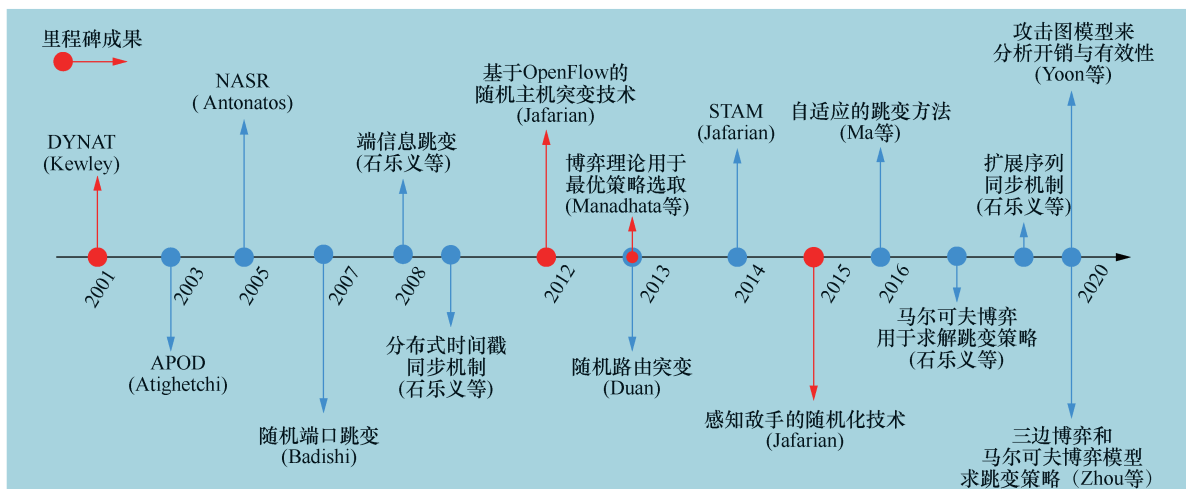


图1 网络层动态跳变技术的发展脉络
Figure 1 The development context of network layer dynamic hopping technology

现出不同的跳变模型, 如随机路由跳变 (RRM, random route mutation) 技术^[10]在软件定义网络上实现路由跳变。同时, 由于网络层跳变技术跳变网络属性, 给终端之间通信带来很大的性能影响, 因此需要采用合适的理论模型或自适应的机制来平衡网络层跳变的安全有效性和资源开销。2013 年, 有研究者提出用博弈理论来指导跳变策略, 平衡网络跳变系统的有效性和开销。之后的研究一直围绕构建一个高可用、高安全的网络层跳变系统展开研究。

2 安全威胁

Hon 等^[11]根据 MTD 的性质将其划分为基于轮换性的 MTD 技术、基于多样性的 MTD 技术和基于冗余性的 MTD 技术。其中, 基于轮换性的 MTD 技术通过随机化系统的配置 (包括 IP 地址跳变、虚拟机轮换、TCP 端口跳变等) 来混淆攻击者, 使得攻击者花费更多的时间去扫描系统, 并使收集到的目标系统的信息无效。基于多样性的 MTD 技术使用具有同样功能、不同实现方式的系统组件来提高系统的容忍性, 使得系统在面对攻击时能够正常为用户提供服务。基于冗余性的 MTD 技术通过提供具有相同功能的多个系统副本来增加系统的可靠性和可用性。网络层动态跳变技术作为基于轮换性的 MTD 技术的子集, 其轮换的主要目标是网络层的配置, 包括 IP 地址、MAC 地址、端口以及网络拓扑, 该技术能够作为入侵防护系统来防护对目标系统的渗透, 最小化攻击者发现目标系统的概率, 其抵御的攻击类型主要包括扫描攻击、DDoS 攻击、蠕虫攻击、APT 攻击。表 1 列举了典型的网络层跳变技术防御的安全威胁。

(1) 扫描攻击

在扫描攻击中, 攻击者通常使用定制的扫描工具 (Libnmap、Nmap) 向目标网络发送探测报文, 获取目标网络的 IP 地址、开放端口和网络拓扑, 从而根据获得的信息向目标网络发起进一步的攻击。为了使攻击者获取的信息无效, 阻断攻击链的连续性, 文献[8,12-17]相继提出了网络层跳变技术, 理论仿真和实验分析了网络层跳变技术能够有效防御扫描攻击。

表 1 典型的网络层跳变技术防御的安全威胁
Table 1 Security threats defended by typical network layer hopping technology

典型技术	扫描攻击	DDoS 攻击	蠕虫传播	APT 攻击
DYNAT (Kewley 等)	√	√		
NASR (Antonatos 等)	√		√	
MT6D (DUNLOP 等)				
Port Hopping (Lee 等)		√		
RPH (Badishi 等)		√		
RHM (Jafarian 等)	√		√	
OF-RHM (Jafarian 等)	√		√	
STAM (Jafarian 等)	√		√	√
端信息跳变 (Shi 等)	√	√		

(2) DDoS 攻击

DDoS 攻击通过使用大量的僵尸网络向目标系统洪泛 UDP、ICMP、SYN 报文, 使得目标系统因资源耗尽而无法为用户提供正常服务。为了防护 DDoS 攻击对目标系统造成的威胁, 文献[18-23]提出了 IP/PORT 跳变技术来减轻 DDoS 攻击对目标系统的影响, 使得 DDoS 攻击者无法针对指定的 IP 地址进行持久连续性洪泛。

(3) 蠕虫攻击

与扫描攻击不同的是, 蠕虫攻击的攻击过程除了最初的扫描攻击外, 还有后续的攻击、传染和现场处理 3 个阶段。首先, 蠕虫病毒会对选取的指定 IP 地址段进行扫描, 当扫描到活跃主机时, 会通过活跃主机的漏洞把蠕虫病毒复制到目标主机上, 接着对感染主机进行现场处理, 之后, 感染主机也可作为病毒主机对网络系统进行进一步的感染。为了抵御蠕虫病毒的传播, 网络地址随机化 (NASR, network address space randomization) 技术^[24]通过随机化目标主机的 IP 地址, 使得蠕虫无法扫描到活跃主机, 即使扫描到活跃主机, 但随着 IP 地址的跳变, 蠕虫也无法对活跃主机进行感染。

(4) 高级持续性攻击 (APT, advance persistent threat)

APT 通过执行静默、持续、自适应的攻击方式来访问目标系统的资源并控制目标系统。根据

网络杀伤链模型,其可以看成是一个多阶段的攻击方式,即其攻击过程包括目标侦察、武器化、投放、利用、安装、命令和控制、行动7个阶段,因此可以采用网络层跳变技术来防御APT攻击的目标侦察阶段^[25],使得APT者无法获取目标系统的信息,进而无法执行网络杀伤链的后续过程。

3 实现架构

网络层跳变技术通过动态跳变终端的网络属性来减小攻击面,增加攻击者识别终端关键信息的难度,减小攻击的成功率。根据文献[9,22,26-27],基于网络层的跳变技术根据在不同网络场景下的实现方式可以分为基于传统网络的网络层跳变模型和基于软件定义网络的网络层跳变模型。

3.1 基于传统网络的网络层跳变模型

由于目前终端设备主要部署于传统网络,基于传统网络的网络层跳变技术研究广泛。石乐义^[9]在2008年提出了端信息跳变技术,通信双方或一方通过协商跳变图案来伪随机地跳变端口、IP地址,实现网络层跳变技术。随后国内外学者对基于传统网络的网络层跳变模型开展进一步的研究,并取得了一定的成果,总结这些成果可以得到如图2所示的基于传统网络的端信息跳变模型。在该模型下,终端需要部署跳变代理,跳变代理负责终端虚假网络属性与真实网络属性的转换,且完成终端之间的认证以及终端之间的跳变速率和跳变图案的协商。基于传统网络的端信息跳变技术通信流程如图3所示,客户端与服务端通信之前,客户端和服务端需要完成相互认证,且交换各自的跳变图案(包括跳变序列和周期),以保证通信时跳变代理能够准确完成虚假网络属性和真实网络属性的变换。在通信过程中,客户端和服务端的跳变图案需要保持严格同步,即客户端和服务端需要及时知道彼此的跳变图案,避免客户端和服务端因更新跳变图案而导致彼此无法具有一致的跳变图案,进而导致正常网络通信失败。因此基于时间的同步机制^[22]和不需要严格时间耦合的ACK应答同步机制^[26]被用于解决端信息跳变的同步问题,基于时间的同步机制将时间划分为不同的定长,不同的时间定长具有不同网络属性,可以有效隐蔽终端的网络属性,但这种同步机制

会受到网络时延和拥塞的影响。基于ACK应答的同步机制不需要采用时间同步,而是将下一阶段的网络属性放置到ACK报文中来通知对方,但该方法存在ACK报文被截获的可能,迫使通信双方在一段时间内只能使用相同的端信息。

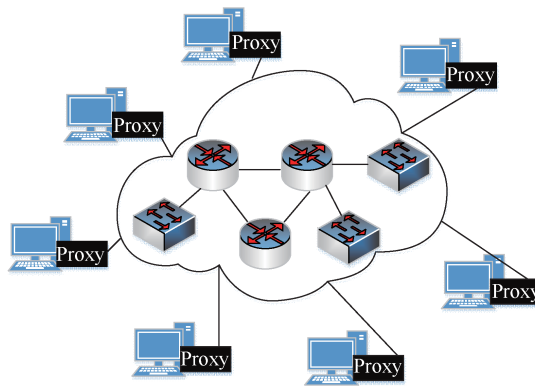


图2 基于传统网络的端信息跳变模型
Figure 2 Terminal information hopping model based on traditional network

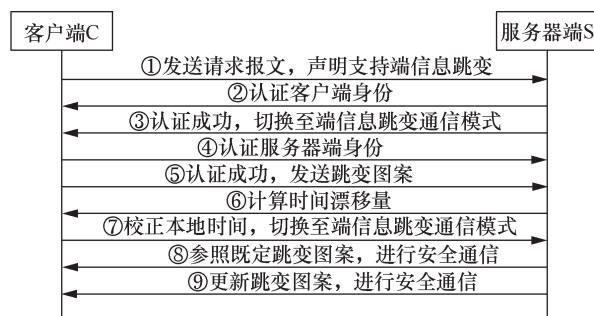


图3 基于传统网络的端信息跳变技术通信流程
Figure 3 Communication process of terminal information hopping technology based on traditional network

3.2 基于软件定义网络的网络层跳变模型

针对基于软件定义网络的网络层跳变模型,由于软件定义网络^[27]控制平面和数据平面的分离以及开放的可编程性,使得网络层跳变技术很容易在软件定义网络中部署。因此,国内外学者针对基于软件定义网络的网络层跳变技术开展了广泛的研究,总结起来可以得到如图4所示的基于软件定义网络的网络层跳变技术模型。在该模型下,系统主要由控制器和SDN交换机组成。控制器是系统的核心,其为终端分配两类网络属性,即真实网络属性和虚拟网络属性,并通过动态跳变虚假网络属性来保持终端的透明性。SDN交换机负责接收控制器下发的流表,并根据控制器两类网络属性的映射关系完成终端发送数据包真实网络属性和虚拟网

络属性的转换。当系统中的两个终端进行通信时，终端通过如图5所示的两种方式完成会话。

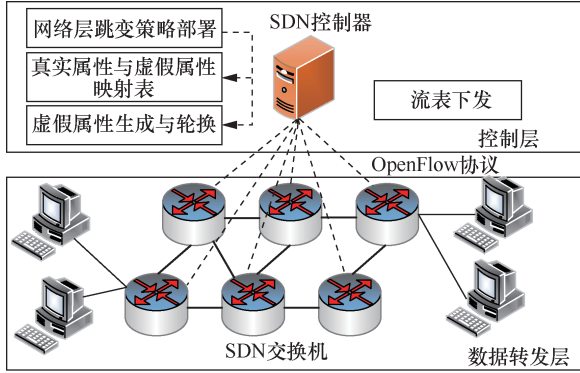


图4 基于软件定义网络的网络层跳变技术模型
Figure 4 Network layer hopping technology model based on software defined network

方式一是通过DNS服务器完成会话，具体地，终端1通过终端2的域名向DNS服务器发起DNS请求进而获取终端2的虚拟网络属性，然后终端1根据源地址为终端1的真实网络属性和目的地址为终端2的虚拟网络属性建立连接，当数据报文通过与源端相连的SDN交换机时，修改源地址为终端1的虚拟网络属性后，将数据报文发送到目的端的跳变代理，与目的端相连的SDN交换机将目的地址变换为终端2的真实网络属性，终端2接收到数据报文后，向终端1发送响应报文，SDN交换机完成

与请求相应的变换操作。方式二是通过控制器授权完成会话，当终端1与终端2进行会话时，终端1首先需要向控制器发送授权请求，当授权成功数据报文才能发送到终端2，未被授权的报文被直接丢弃，数据报文经过与源端和目的端相连的SDN控制器时完成与方式一相同的操作。

4 分类

Cho等^[4]将移动目标防御技术总结为3个关键问题，即哪些系统配置属性能够改变来迷惑攻击者；如何移动目标系统的属性来增加攻击的不确定性和不可预测性；如何选择轮换的时间来平衡开销和有效性。本文基于这3个关键问题，将网络层跳变技术从跳变属性、跳变的实现方式和跳变的触发方式3个层面进行划分。具体的分类方法如表2所示。

4.1 跳变属性

针对网络层跳变技术的跳变属性，主要分为单一属性的跳变机制和多维属性协同跳变机制。

在网络层跳变技术中，对于单一属性的跳变机制，主要分为IP地址跳变、MAC地址跳变、端口地址跳变和路由地址跳变。针对IP地址跳变，Antonatos等^[24]提出了网络地址随机化(NASR, network address space randomization)技术，其通

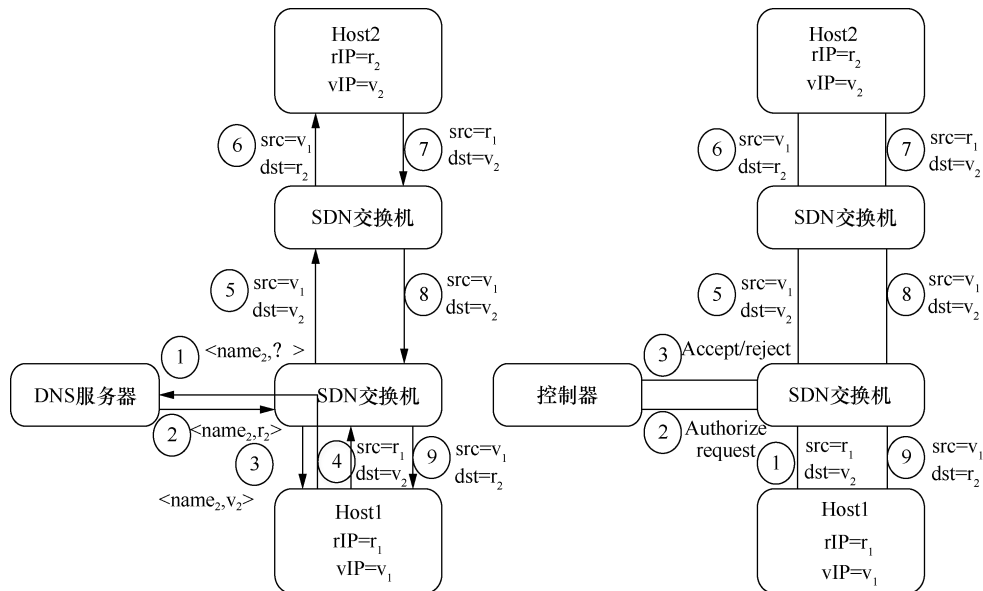


图5 基于软件定义网络的跳变模型下两种通信模式
Figure 5 Two communication modes under the hopping model based on software defined network

表 2 网络层跳变技术分类方法及其优缺点

Table 2 Network layer hopping technology classification method and its advantages and disadvantages

分类方法		优点	缺点	参考文献
跳变属性	单一属性的跳变	跳变系统的实现较为简单	无法防御高级的攻击者根据其他网络属性进行攻击	文献[8,10,22]
	多维属性协同跳变	多维属性协同跳变, 进一步缩小攻击面, 增加了系统的安全性	对网络传输性能影响更大, 且需要考虑多种跳变方式如何协同	文献[28-32]
跳变的实现方式	基于传统网络实现	可以实现高速率跳变, 增加跳变的不可预测性	改变现有的网络协议; 网络性能损失严重	文献[5,22,26,33-36]
	基于 SDN 实现	灵活的网络架构, 便于部署动态跳变系统	需要部署 SDN 控制器和 SDN 交换机, 部署成本高; SDN 控制器存在固有的网络威胁	文献[12,25,37-40]
跳变的触发方式	非自适应跳变	部署方式简单	难以平衡系统的安全性和通信性能, 较大的跳变周期无法防御攻击者, 较小的跳变周期影响通信性能	文献[5-10,12,21-26, 28-40]
	自适应跳变	能够根据攻击行为作出相应的反应, 在一定程度上可以降低跳变对通信性能的影响	很难对攻击行为进行完美刻画, 存在漏报率和误报率	文献[41-45]

过 DHCP 服务器来周期性改变终端的 IP 地址, 实现 IP 地址的动态化, 能够有效防御蠕虫的传播。但是 NASR 无法对终端保持透明, 每次轮换的都是主机的真实 IP 地址。因此, 2012 年, Jafarian 等^[8]提出了随机主机跳变 (RHM, random host mutation) 技术, 其采用两级跳变机制来增加跳变随机性, 即低频跳变为主机分配一个地址空间, 而高频跳变从分配的地址空间中为主机选择一个地址, 主机保持真实 IP 地址不变, 动态跳变虚拟 IP 跳变, 保证了终端的透明性。针对端口地址跳变, 文献[22]提出在不改变现有 UDP/TCP 的前提下, 根据时间和客户端与服务器端共享密钥来随机生成服务器对外的 UDP/TCP 端口号。针对路由跳变, 文献[10]提出了一种主动随机路由突变 (RRM, random route mutation) 技术, 通过可满足性模理论将 RRM 建模为约束满足问题进而求解得到最优的跳变路径, 它可以同时随机改变网络中多个流的路由, 以防御侦察、窃听和 DoS 攻击, 同时保持端到端的 QoS 属性。实验结果证明, 与静态路由相比, RRM 可以保护至少 90% 的报文免受真实攻击者的攻击, 且 RRM 可以有效地部署在常规网络和 SDN 上, 而不会对会话报文造成任何影响。

由于单一属性的跳变技术仅从单一网络属性进行变化, 攻击者通过其他网络属性获取网络系统未知的漏洞后门, 进而获取目标系统的控制权。

因此, 多属性协同跳变可以进一步缩小攻击面, 增强网络系统的安全性。Chen 等^[28]提出将 IP 跳变和路径跳变结合起来实现内网的主动防护, 可以有效阻断零日漏洞和 DoS 攻击。Jafarian 等^[29]提出主机身份匿名 (HIDE, host identity anonymization) 技术, 从跳变主机地址、跳变主机指纹、匿名主机指纹、部署具有上下文感知指纹的高保真蜜罐和在这些蜜罐上部署上下文感知的内容这 5 个维度防御高级攻击者, 在保证合理开销的基础上, 能够有效防御来自红帽子黑客的攻击。Luo 等^[30]提出一种根据源属性、服务属性和时间来高速率、不可预测的跳变终端的 IP 地址和端口的方法, 在引入可接受操作开销的前提下能够有效防御内部和外部威胁。Sharma 等^[31]提出随机主机和服务复用 (RHSM, Random Host and Service Multiplexing) 技术, 其允许主机及运行的服务具有多个虚拟 IP 地址和端口号, 且这些端口号随着时间的改变而不断变化, 并以多对多的方式和解复用的方式复用到真实 IP 和端口上, 能够有效地混淆网络和传输层服务的真实身份。文献[32]认为单一的网络地址跳变方法无法防御知道目标域名的攻击者, 因此提出了一种基于随机域名和地址突变的网络防御 (RDAM, random domain and address mutation) 方法, 该方法通过动态域名方法增加了攻击者的扫描空间, 降低了攻击者扫描成功的可能性。

4.2 跳变的实现方式

网络层跳变技术的实现方式,主要分为基于传统网络的实现方式和基于 SDN 的实现方式。

在基于传统网络实现网络层跳变技术方面,端信息跳变是其主要的实现形式,其关键性问题主要包括合理的跳变策略和有效的同步机制。2001 年, Kewley 等^[5]首次提出采用动态地址转换(DyNAT, dynamic network address translation)技术来增强网络的安全性,其在客户端部署 DyNAT 插件,在服务器端部署 DyNAT 网关, DyNAT 插件负责处理来自客户端的请求报文和进入客户端的响应报文, DyNAT 网关负责处理到达服务端的请求报文和离开服务端的响应报文。之后,针对端信息跳变的跳变策略问题,文献[22]提出通过时间和密钥来动态生成服务端的端口号,使得授权的用户才能访问服务端,有效地减轻了 DDoS 攻击。文献[33]提出将数据流分布多个传输连接上来增强数据的隐蔽性。针对端信息跳变的同步机制问题,文献[26]提出基于 ACK 的端口跳变机制,通过共享密钥和数据包的发送个数来确定下一跳变间隔的端口。文献[34-35]提出了分布式时间戳同步机制,有效地避免集中式的时间戳同步机制面临的单节点故障问题。文献[36]针对当前同步机制无法适应亚秒、毫秒级的高速率跳变,提出端信息扩展认证同步机制,有效地解决了高隐蔽要求下的高速跳变问题。实验结果表明,提出的端信息跳扩混合机制能够提高在高跳变场景下的可用性和隐蔽性。

在基于 SDN 实现网络层跳变技术方面,2012 年, Jafarian 等^[12]首次提出将网络层跳变技术应用于 SDN 网络中,并实现了基于 OpenFlow 的主机突变(OF-RHM, OpenFlow random host mutation)技术,其通过 NOX 控制器为终端分配两类 IP,即虚拟 IP 和真实 IP,且终端保持真实 IP 不变,周期性变换虚拟 IP,使得终端保持透明,能够较好地防御网络扫描和蠕虫传播,但无法有效地防御高级持续性攻击。因此,2014 年, Jafarian 等^[25]提出在时间和空间两个维度上对终端的 IP 地址进行变化,即通过时间间隔和源属性进行跳变,增加了虚拟 IP 选择的不确定性,能够有效地防御

高级持续性攻击。2015 年, Jafarian 等在前面研究的基础上提出一种高效的主机跳变机制^[37],在保证跳变的不可预测性的前提下实现最大化的防御效果。更进一步, Hu 等^[38]提出了一种基于 OpenFlow 的网络层移动目标防御方案,能够实现终端在全网的防护,在域内终端通过 IP 地址跳变进行防御,在跨域的情况下终端通过端口跳变进行防御。Sharma 等^[39]提出灵活随机的 IP 多路复用(FRVM, flexible random virtual IP multiplexing)技术,通过多个随机的、随时间变化的虚拟 IP 地址复用到真实 IP 来增强系统的安全性。文献[40]提出不仅在终端进行 IP 跳变,而且将 IP 跳变应用于数据平面交换机,并通过基于哈希链的同步签名来同步网络路径中的各个节点。

4.3 跳变的触发方式

网络层跳变技术的跳变方式主要分为非自适应跳变和自适应跳变。对于非自适应的网络层跳变技术,其主要实现形式是周期性跳变,周期性跳变是网络层跳变机制以固定的时间间隔去跳变网络层属性。早期提出的 RHM、OF-RHM 以及端信息跳变技术均以固定的周期去轮换终端的关键属性,如果跳变时间间隔过长,攻击者在跳变间隔内能够渗透进目标系统,导致防御失效。而如果跳变周期过短,会严重影响网络性能并且浪费网络资源,特别是当无攻击者渗透目标系统时,高速跳变网络属性也显得毫无意义,因此合理的跳变方式可以有效保证安全性和提高通信质量。

自适应跳变机制在保证系统安全性的同时将网络性能的损失降到最小。Jafarian 等^[41]提出一种自适应敌手的 IP 地址随机化技术,其通过将敌手的扫描行为假设为非均匀的扫描和非重复的扫描,然后根据这种假设行为判断攻击者的扫描行为,进而做出自适应的跳变。Ma 等^[42]提出一种自适应的端点跳变技术(SEHT, self-adaptive end-point hopping technique),通过可满足性模理论(SMT)来描述跳变的限制,保证跳变的低开销和高可用性,同时根据假设测试分析扫描策略进而指导跳变策略的选择。实验结果表明,SEHT 在保证低开销的前提下能够防御 90%的扫描攻击。Wang 等^[43]在软件定义网络中设计并实现 IP

地址和 MAC 地址协同化的内网防护系统,并采用网络侦察的博弈模型求解最优的跳变周期,使得跳变网络层属性不影响正常的网络服务。Yoon 等^[44]提出一种分层架构的攻击图模型,该模型提供了网络的漏洞和网络拓扑,可用于在指定网络中选择高优先级的主机进行轮换并且确定主机轮换的频率,以最小的防御开销降低攻击成功的概率。实验结果表明,该方法能够有效降低攻击成功的概率,且具有跳变的系统与无跳变的系统在转发数据包时的时延相差不大。Wang 等^[45]通过研究 MTD 时序问题提出了一个基于更新奖励理论的算法,并在综合考虑自适应开销和攻击成本的基础上,用来自 9 026 个不同 IP 的 50 704 种不同的 DDoS 攻击来评估该算法,实验结果表明,与现有的周期性和随机自适应算法相比,提出的算法在相同的安全保证下更具成本效益。

5 模型及评估

为了评估网络层跳变技术的有效性和平衡网络层跳变的有效性和性能损失,增强网络层跳变系统的可用性,国内外研究者提出了不同的模型去分析网络层动态跳变技术,主要分为基于概率的评估模型和基于博弈的跳变策略选取机制模型。

5.1 概率模型

针对基于概率的评估模型,研究者主要从扫描攻击、DDoS 攻击、蠕虫传播、APT 攻击这 4 种攻击方式入手,分析当部署动态跳变系统时,攻击者成功攻击目标的概率。

Carroll 等^[46]提出使用瓮模型对静态网络和动态网络进行分析,并比较在不同的网络大小、漏洞系统数目、扫描地址空间、轮换频率的条件下攻击成功的概率。实验结果表明,动态网络能够有效降低攻击者攻击成功的概率。文献[25]提出从威慑率、欺骗率、检测率 3 个方面对动态防御系统进行评估。同时,从协作扫描、本地偏好扫描来分析攻击成功的概率。

此外,相关研究者也将概率模型引入网络层跳变策略选取的研究中,通过将攻击者和防御者的行为建模为概率模型,在保证安全性的前提下,得到增强系统可用性的跳变策略。

Clark 等^[47]将跳变周期的选取建模为最优停止问题,并在综合分析攻击成功的概率和资源开销的基础上,给出最优的跳变周期。Maleki 等^[48]通过使用马尔可夫模型来分析网络层跳变,根据目标隐藏的数量将网络系统建模为单目标隐藏和多目标隐藏,并给出各自的状态转移图,在状态转移图的基础上,给出两种情况下目标系统的安全指标。Yoon 等^[44]提出采用三层攻击图模型对目标系统的关键资产进行建模,进而评估这些关键资产的漏洞等级。进一步,根据这些漏洞等级提出两种关键资产指标,即基于角色的关键性和基于影响的关键性来区分关键资产的优先级,选择优先级高的资产进行轮换。

5.2 博弈模型

针对网络空间的攻防模型,从防御者的角度来看,网络层动态跳变技术的主要目标是确定一组最佳的网络配置来改变攻击面,最大限度地减少攻击者行动带来的风险。从攻击者的角度来看,攻击者旨在以最小的精力和最大的效率成功地发起攻击。因此,博弈论很好地模拟了攻击者和网络层跳变之间的竞争情况,可以有效指导网络层跳变策略选取。本节主要基于完全信息博弈和不完全信息博弈对网络层跳变技术进行分类。

对于完全信息博弈,Manadhata 等^[49]在考虑安全性和可用性的基础上,提出采用二人随机博弈模型选取最优的移动目标轮换策略。Lei 等^[50]提出将马尔可夫决策过程和动态博弈结合起来塑造 MTD 场景下防御者与攻击者的多阶段博弈行为,进而得到最优的跳变策略平衡防御的有效性和网络服务质量。Feng 等^[51]提出将非零和斯坦伯格博弈应用于求解 MTD 策略,假设攻击者可以观察到防御者先前的配置,通过将防御者建模为马尔可夫决策过程,进而通过有效的迭代算法求出最佳的跳变策略。

对于不完全信息博弈,Chen 等^[52]针对网络攻防过程中攻防双方无法获取对方信息以及无法判断对方收益的问题,提出了基于模糊静态贝叶斯博弈的网络主动防御策略。在求解双方的效用函数时引入了三角模糊数并采用模糊概率及其均值的方法得到精确效用值,进而通过纳什均衡解得最优跳变策略。Zhu 等^[53]提出了一种多阶段反馈

表 3 网络层跳变技术的关键模型及其优缺点

Table 3 The key model of network layer hopping technology and its advantages and disadvantages

理论模型	相关技术	优点	缺点	相关文献
博弈模型	完全信息博弈	能够有效建模攻击者与防御者的行为；能够通过多方的博弈行为得到最优的跳变周期	求解的复杂度比较高	文献 [25,44,46-48]
	不完全信息博弈			
概率模型	攻击图 概率论	便于分析跳变技术的有效性；便于求解最优的跳变策略	对攻击者和防御者的抽象层次太高；模型是静态的，无法建模复杂的网络攻防场景	文献[49-54]

博弈模型，将其中带有 MTD 的攻击防御形式化为零和博弈。在该模型中，网络系统被分解为不同的部分，并将网络攻击行为建模为多阶段攻击过程。此外，还分析了 MTD 实施对系统性能开销和攻击成本的影响，以确定 MTD 机制的最佳策略，从而将防御成本和系统安全风险最小化。Lei 等^[54]提出一种新颖的不完全信息马尔可夫博弈理论，通过引入移动攻击面和移动勘测面的概念，扩展具有不完全信息的最优策略选择。同时，综合考虑防御成本和防御收益，设计了一种最优策略生成算法，以防止所选策略与实际网络状况发生偏差，从而保证了最优策略生成的正确性。Tan 等^[55]将马尔可夫决策过程与鲁棒博弈结合，提出了一种基于马尔可夫鲁棒博弈模型。作者通过定义基于移动攻击和探索面的移动目标防御模型，描述了漏洞的随机出现以及由防御转换引起的攻击方和防御方在认知行为上的差异。在此基础上，构造了马尔可夫鲁棒博弈模型，描述了运动目标防御对抗的多阶段、多状态特征，给出不完全信息假设下的未知先验信息。最后通过将最优策略选择等效转换为非线性规划问题，设计了一种有效的最优防御策略选择算法。

6 存在挑战及下一步研究方向

(1) 网络层跳变系统的易用性还有待提高

目前针对无论是基于传统网络的还是基于 SDN 的网络层动态跳变技术，都无法完美解决因跳变产生的会话维持问题，而目前用户对网络性能要求苛刻，因会话维持产生的链接关闭将会严重影响网络体验。

(2) 网络层跳变技术的安全性还需要进一步改善

基于网络层的跳变技术无法防御高级攻击者

发起网络攻击，如侧信道攻击、高级持续性攻击等。因此，可以尝试结合其他防御手段，如结合人工智能技术^[57]和欺骗技术来发现潜在的攻击者，对跳变策略进行最优化设置。

(3) 拓展应用范围和场景

随着 IPv4 地址的耗尽，网络协议从 IPv4 向 IPv6 网络转变，基于 IPv4 的网络层跳变技术无法直接过渡到 IPv6 网络中，且目前针对 IPv6 网络的动态跳变技术研究很少，所以在 IPv6 网络中部署网络层跳变具有重要的研究意义。同时，随着物联网的发展，万物互连的时代到来，必然带来更多的安全威胁，所以将网络层跳变技术引入物联网去防范未知的漏洞和后门也具有重要的研究价值^[58]。

7 结束语

随着移动目标防御其他相关技术的提出和应用，网络层动态跳变技术的发展趋势渐缓。但是网络层动态防御技术仍然存在关键问题没有解决。

网络层动态跳变引起的服务性能下降仍然是迫切需要解决的问题。部署在传统网络的动态跳变技术需要改变现有的通信协议方式，增加额外的通信报文，引入了额外的时延开销。而部署在 SDN 中的网络层跳变技术，SDN 本身固有的数据层和控制层威胁，使得在没解决现有威胁的前提下，引入新的威胁。因此，可以考虑新的网络层相关技术来部署网络层跳变，在保证安全性的同时，保证通信服务质量不下降。

网络层动态跳变技术仍然需要更加合理模型进行评估。当前，针对网络层跳变技术的评估主要是概率模型和博弈论模型，然而这两种模型的抽象层次太高，忽略了很多关键因素，对实际网络跳变系统的指导作用有限。因此，可以考虑其

他的模型对网络层跳变系统进行建模, 如可以采用排队论模型对网络层跳变进行评估, 分析因系统跳变带来的通信时延。

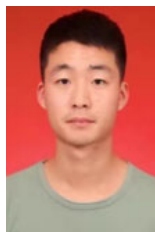
参考文献:

- [1] Symantec. Internet Security Threat Report[R]. 2016.
- [2] Trend Micro. Understanding Targeted Attacks: The Impact of Targeted Attacks[R]. 2015.
- [3] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense[M]. New York, NY: Springer New York, 2011.
- [4] CHO J H, SHARMA D P, ALAVIZADEH H, et al. Toward proactive, adaptive defense: a survey on moving target defense[J]. IEEE Communications Surveys & Tutorials, 2020, 22(1): 709-745.
- [5] KEWLEY D, FINK R, LOWRY J, et al. Dynamic approaches to thwart adversary intelligence gathering[C]//Proceedings of Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01. 2001: 176-185.
- [6] ATIGHETCHI M, PAL P, WEBBER F, et al. Adaptive use of network-centric mechanisms in cyber-defense[C]//Proceedings of Sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, 2003. 2003: 183-192.
- [7] DUNLOP M, GROAT S, URBANSKI W, et al. MT6D: a moving target IPv6 defense[C]//Proceedings of 2011 - MILCOM 2011 Military Communications Conference. 2011: 1321-1326.
- [8] AL-SHAER E, DUAN Q, JAFARIAN J H. Random host mutation for moving target defense[M]//Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin, Heidelberg: Springer, 2013: 310-327.
- [9] 石乐义, 贾春福, 吕述望. 基于端信息跳变的主动网络防护研究[J]. 通信学报, 2008, 29(2): 106-110.
SHI L Y, JIA C F, LYU S W. Research on end hopping for active network confrontation[J]. Journal on Communications, 2008, 29(2): 106-110.
- [10] DUAN Q, AL-SHAER E, JAFARIAN H. Efficient Random Route Mutation considering flow and network constraints[C]//Proceedings of 2013 IEEE Conference on Communications and Network Security (CNS). 2013: 260-268.
- [11] HONG J B, KIM D S. Assessing the effectiveness of moving target defenses using security models[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(2): 163-177.
- [12] JAFARIAN J H, AL-SHAER E, DUAN Q. OpenFlow random host mutation: transparent moving target defense using software defined networking[C]//Proceedings of the First Workshop on Hot Topics in Software Defined Networks. 2012: 127-132.
- [13] YOON S, CHO J H, KIM D S, et al. Poster: address shuffling based moving target defense for in-vehicle software-defined networks[C]//Proceedings of MobiCom '19: The 25th Annual International Conference on Mobile Computing and Networking. 2019: 1-3.
- [14] CARROLL T E, CROUSE M, FULP E W, et al. Analysis of network address shuffling as a moving target defense[C]//Proceedings of 2014 IEEE International Conference on Communications (ICC). 2014: 701-706.
- [15] DUAN Q, AL-SHAER E, JAFARIAN H. Efficient Random Route Mutation considering flow and network constraints[C]//Proceedings of 2013 IEEE Conference on Communications and Network Security (CNS). 2013: 260-268.
- [16] ZHOU Z, XU C Q, KUANG X H, et al. An efficient and agile spatio-temporal route mutation moving target defense mechanism[C]//Proceedings of ICC 2019 - 2019 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2019: 1-6.
- [17] LUO Y B, WANG B S, WANG X F, et al. RPAH: random port and address hopping for thwarting internal and external adversaries[C]//Proceedings of 2015 IEEE Trustcom/BigDataSE/ISPA. 2015: 263-270.
- [18] AYDEGER A, SAPUTRO N, AKKAYA K, et al. Mitigating cross-fire attacks using SDN-based moving target defense[C]//Proceedings of 2016 IEEE 41st Conference on Local Computer Networks (LCN). 2016: 627-630.
- [19] CLARK A, SUN K, BUSHNELL L, et al. A game-theoretic approach to IP address randomization in decoy-based cyber defense[M]//Lecture Notes in Computer Science. 2015: 3-21.
- [20] GROAT S, DUNLOP M, URBANSKI W, et al. Using an IPv6 moving target defense to protect the smart grid[C]//Proceedings of 2012 IEEE PES Innovative Smart Grid Technologies (ISGT). 2012: 1-7.
- [21] 吴桦, 陈廷政. SDN 环境中基于端址跳变的 DDoS 防御方法[J]. 网络空间安全, 2020, 11(8): 17-22.
WU H, CHEN T Z. A DDoS defense method based on port and address hopping in SDN[J]. Cyberspace Security, 2020, 11(8): 17-22.
- [22] LEE H C J, THING V L L. Port hopping for resilient networks[C]//Proceedings of IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004. 2004: 3291-3295.
- [23] SHI L Y, JIA C F, LÜ S, et al. Port and address hopping for active cyber-defense[M]//Intelligence and Security Informatics. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007: 295-300.
- [24] 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.
- [25] JAFARIAN J H H, AL-SHAER E, DUAN Q. Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers[C]//Proceedings of the First ACM Workshop on Moving Target Defense - MTD '14. 2014: 69-78.
- [26] BADISHI G, HERZBERG A, KEIDAR I. Keeping denial-of-service attackers in the dark[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(3): 191-204.
- [27] REHMANI M H, DAVY A, JENNINGS B, et al. Software defined networks-based smart grid communication: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2637-2670.
- [28] 陈扬, 扈红超, 程国振. 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 C, CHENG G Z. The design and implementation of a software-defined intranet dynamic defense system[J]. Acta Electronica Sinica, 2018, 46(11): 2604-2611.
- [29] JAFARIAN J H, NIAKANLAHIJI A, AL-SHAER E, et al. Mul-

- ti-dimensional host identity anonymization for defeating skilled attackers[C]//MTD '16: Proceedings of the 2016 ACM Workshop on Moving Target Defense. 2016: 47-58.
- [30] LUO Y B, WANG B S, WANG X F, et al. RPAH: random port and address hopping for thwarting internal and external adversaries[C]//Proceedings of 2015 IEEE Trustcom/BigDataSE/ISPA. Piscataway: IEEE Press, 2015: 263-270.
- [31] SHARMA D P, CHO J H, MOORE T J, et al. Random host and service multiplexing for moving target defense in software-defined networks[C]//Proceedings of ICC 2019 - 2019 IEEE International Conference on Communications (ICC). 2019: 1-6.
- [32] WANG K, CHEN X, ZHU Y F. Random domain name and address mutation (RDAM) for thwarting reconnaissance attacks[J]. PLoS One, 2017, 12(5): e0177111.
- [33] SIFALAKIS M, SCHMID S, HUTCHISON D. Network address hopping: a mechanism to enhance data protection for packet communications[C]//Proceedings of IEEE International Conference on Communications, 2005. ICC 2005. 2005: 1518-1523.
- [34] LIN K, JIA C. Distributed timestamp synchronization for end hopping[J]. China Communications, 2011, 8(4): 164-169.
- [35] 林楷, 贾春福, 石乐义. 分布式时间戳同步技术的改进[J]. 通信学报, 2012, 33(10): 110-116.
- LIN K, JIA C F, SHI L Y. Improvement of distributed timestamp synchronization[J]. Journal on Communications, 2012, 33(10): 110-116.
- [36] 石乐义, 郭宏彬, 温晓, 等. 端信息跳扩混合的主动网络防御技术研究[J]. 通信学报, 2019, 40(5): 125-135.
- SHI L Y, GUO H B, WEN X, et al. Research on end hopping and spreading for active cyber defense[J]. Journal on Communications, 2019, 40(5): 125-135.
- [37] 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.
- [38] 胡毅勋, 郑康锋, 杨义先, 等. 基于 OpenFlow 的网络层移动目标防御方案[J]. 通信学报, 2017, 38(10): 102-112.
- HU Y X, ZHENG K F, YANG Y X, et al. Moving target defense solution on network layer based on OpenFlow[J]. Journal on Communications, 2017, 38(10): 102-112.
- [39] SHARMA D P, KIM D S, YOON S, et al. FRVM: flexible random virtual IP multiplexing in software-defined networks[C]//Proceedings of 2018 17th IEEE International Conference on Trust, Security and Privacy In Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). 2018: 579-587.
- [40] CHANG S Y, PARK Y, ASHOK BABU B B. Fast IP hopping randomization to secure hop-by-hop access in SDN[J]. IEEE Transactions on Network and Service Management, 2019, 16(1): 308-320.
- [41] JAFARIAN J H, AL-SHAER E, DUAN Q. Adversary-aware IP address randomization for proactive agility against sophisticated attackers[C]//Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM). 2015: 738-746.
- [42] MA D H, LEI C, WANG L M, et al. A self-adaptive hopping approach of moving target defense to thwart scanning attacks[M]//Information and Communications Security. Cham: Springer International Publishing, 2016: 39-53.
- [43] 王鹏超, 陈福才, 程国振, 等. 软件定义的 L2/L3 地址协同拟态伪装策略研究[J]. 电子学报, 2019, 47(10): 2032-2039.
- WANG P C, CHEN F C, CHENG G Z, et al. L2/L3 address cooperative mimicry strategy research based on SDN[J]. Acta Electronica Sinica, 2019, 47(10): 2032-2039.
- [44] YOON S, CHO J H, KIM D S, et al. Attack graph-based moving target defense in software-defined networks[J]. IEEE Transactions on Network and Service Management, 2020, 17(3): 1653-1668.
- [45] WANG H X, LI F, CHEN S Q. Towards cost-effective moving target defense against DDoS and covert channel attacks[C]//Proceedings of the 2016 ACM Workshop on Moving Target Defense. 2016: 15-25.
- [46] CARROLL T E, CROUSE M, FULP E W, et al. Analysis of network address shuffling as a moving target defense[C]//Proceedings of 2014 IEEE International Conference on Communications (ICC). 2014: 701-706.
- [47] CLARK A, SUN K, POOVENDRAN R. Effectiveness of IP address randomization in decoy-based moving target defense[C]//Proceedings of 52nd IEEE Conference on Decision and Control. 2013: 678-685.
- [48] MALEKI H, VALIZADEH S, KOCH W, et al. Markov modeling of moving target defense games[C]//Proceedings of the 2016 ACM Workshop on Moving Target Defense. 2016: 81-92.
- [49] MANADHATA P K. Game theoretic approaches to attack surface shifting[M]//Moving Target Defense II. New York, NY: Springer New York, 2012: 1-13.
- [50] LEI C, MA D H, ZHANG H Q. Optimal strategy selection for moving target defense based on Markov game[J]. IEEE Access, 2017, 5: 156-169.
- [51] FENG X T, ZHENG Z Z, MOHAPATRA P, et al. A stackelberg game and Markov modeling of moving target defense[M]//Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017: 315-335.
- [52] 陈永强, 吴晓平, 付钰, 等. 基于模糊静态贝叶斯博弈的网络主动防御策略选取[J]. 计算机应用研究, 2015, 32(3): 887-889, 899.
- CHEN Y Q, WU X P, FU Y, et al. Active defense strategy selection of network based on fuzzy static Bayesian game model[J]. Application Research of Computers, 2015, 32(3): 887-889, 899.
- [53] ZHU Q Y, BAŞAR T. Game-theoretic approach to feedback-driven multi-stage moving target defense[M]//Lecture Notes in Computer Science. Cham: Springer International Publishing, 2013: 246-263.
- [54] LEI C, ZHANG H Q, WAN L M, et al. Incomplete information Markov game theoretic approach to strategy generation for moving target defense[J]. Computer Communications, 2018, 116: 184-199.
- [55] TAN J L, LEI C, ZHANG H Q, et al. Optimal strategy selection approach to moving target defense based on Markov robust game[J]. Computers & Security, 2019, 85: 63-76.
- [56] LEI C, ZHANG H Q, TAN J L, et al. Moving target defense techniques: a survey[J]. Security and Communication Networks, 2018, 2018: 1-25.
- [57] 张明悦, 金芝, 赵海燕, 等. 机器学习赋能的软件自适应性综述[J]. 软件学报, 2020, 31(8): 2404-2431.
- ZHANG M Y, JIN Z, ZHAO H Y, et al. Survey of machine learning enabled software self-adaptation[J]. Journal of Software, 2020, 31(8): 2404-2431.

- [58] CHENG K, BAI Y B, ZHOU Y, et al. CANeleon: protecting CAN bus with frame ID chameleon[J]. IEEE Transactions on Vehicular Technology, 2020, 69(7): 7116-7130.

[作者简介]



何威振（1996-），男，安徽亳州人，信息工程大学硕士生，主要研究方向为网络安全、移动目标防御。



陈福才（1974-），男，江西南昌人，信息工程大学研究员，主要研究方向为网络安全、网络通信。

牛杰（1982-），男，河南郸城人，中国人民解放军 61212 部队工程师，主要研究方向为网络信息前沿技术发展。



谭晶磊（1994-），男，山东章丘人，信息工程大学博士生，主要研究方向为网络信息安全、移动目标防御、攻防博弈对抗等。



霍树民（1985-），男，山西长治人，信息工程大学副研究员，主要研究方向为网络安全。



程国振（1986-），男，山东菏泽人，信息工程大学副教授，主要研究方向为云数据中心、SDN、网络安全。