

面向 SDN 的移动目标防御技术研究进展

谭晶磊^{1,2}, 张红旗^{1,2}, 雷程^{1,2}, 刘小虎¹, 王硕¹

(1. 信息工程大学密码工程学院, 河南 郑州 450001;

2. 河南省信息安全重点实验室, 河南 郑州 450001)

摘要: 软件定义网络是基于开放标准的灵活架构, 通过控制层管理网络功能和服务, 具有控转分离、集中控制的特性; 移动目标防御技术致力于构建一个不断变换的环境以提高网络系统的视在不确定性, 需要灵活可定制、集中可控制的网络架构加以实施, 因此将移动目标防御与软件定义网络相结合已成为更具应用价值研究热点。首先, 分别介绍了软件定义网络和移动目标防御的基本概念, 概括了软件定义网络所面临的安全威胁, 阐述了面向 SDN 的移动目标防御的实现模型; 其次, 分别从 SDN 数据层、控制层和应用层归纳了移动目标防御的技术方法; 最后, 总结了现有 SDN 动态防御面临的挑战, 对面向 SDN 的移动目标防御技术发展方向进行了展望。

关键词: 软件定义网络; 移动目标防御; 动态化; 多样性; 随机性

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018061

Research progress on moving target defense for SDN

TAN Jinglei^{1,2}, ZHANG Hongqi^{1,2}, LEI Cheng^{1,2}, LIU Xiaohu¹, WANG Shuo¹

1. School of Cryptography Engineering, Information Engineering University, Zhengzhou 450001, China

2. Henan Provincial Key Laboratory of Information Security, Zhengzhou 450001, China

Abstract: Software-defined network is based on flexible and open standards, which manages network functions and services by the control layer. And it has the unique advantages of control-separation and centralized control. The moving target defense technology is dedicated to build an ever-changing environment to increase the uncertainty of the network system, which requires a flexible and customizable, centralized and controllable network architecture to implement it. Therefore, the combination of moving target defense and software-defined network have become a more valuable research hotspot. Firstly, the basic concepts of software-defined network and moving target defense were introduced, the security threats of software-defined network was summarized, and the realization model of moving target defense for SDN network was described. Secondly, the technical methods for moving target defense were summarized respectively from the data layer, control layer and application layer of the SDN. Finally, summing up the challenges of existing SDN dynamic defense, and looking forward to the development direction of moving target defense technologies for the SDN.

Key words: software-defined network, moving target defense, dynamic, diversity, randomness

收稿日期: 2018-06-15; 修回日期: 2018-07-03

通信作者: 谭晶磊, nxutjl@126.com

基金项目: 国家高技术研究发展计划(“863”计划)基金资助项目(No.2012AA012704, No.2015AA7116040); 郑州市科技领军人才基金资助项目(No.131PLJRC644)

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2012AA012704, No.2015AA7116040), Zhengzhou Science and Technology Leader Project (No.131PLJRC644)

1 引言

当前网络空间面临的威胁日益突出, 安全状况不容乐观, 各类网络安全事故层出不穷, 第四届世界互联网大会发布的《世界互联网发展报告 2017》蓝皮书中指出, 截至 2017 年 6 月, 我国网民数量已经达到 7.51 亿, 位于全球首位, 而勒索病毒、僵尸网络等网络安全问题也日渐突出。与此同时, 开放网络基金会 (ONF) 所提出的软件定义网络^[1] (SDN, software defined network) 的体系结构已经得到普遍认可, 被认为是下一代互联网的核心技术之一, 基于 OpenFlow 协议的 SDN 体系结构框架如图 1 所示, 它由数据层、控制层、应用层以及南北向 2 个接口构成^[2], 创造性地提出了数据层和控制层分离以及可编程的思想, 在各种场景 (如企业网络、数据中心网络等) 和各种骨干网络^[3]中的优点已经日益凸显, 但全面实施 SDN 的运营商网络^[4]仍存在挑战, 其中一个最重要的挑战是 SDN 本身的安全性。从 SDN 框架的角度考虑 SDN 安全^[5]的具体问题, 应用层、控制层、数据层以及南北向接口均面临一系列的安全威胁, 因此, 必须探索克服 SDN 安全威胁的技术、方法和策略, 以实现强大和可靠的广域 SDN 部署^[6]。

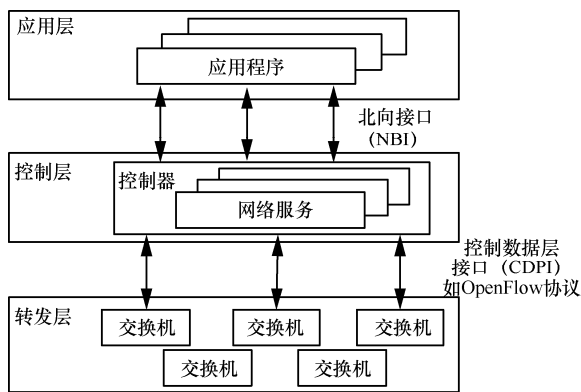


图 1 SDN 体系结构框架

针对当前网络固有的攻防不对称特性, 为了平衡现有网络的攻防环境, 美国网络安全与信息保障研发计划提出了应对新型网络攻击的新概念——移动目标防御技术^[7] (MTD, moving target defense), 作为一项革命性技术, 它的核心思想是利用攻击面^[8]的变化使网络系统动态化, 通过

“化静为动”“反客为主”的机制策略, 提供动态主动的网络防御, 使系统具有更少的确定性、静态性、同构性, 利用随机化和多样化减少攻击者攻击成功的可能性, 以此限制攻击者的攻击, 大大缩短攻击者的攻击周期, 使攻击者难以完成攻击任务^[9]。

近年来, 国家、企业和服务提供商已经将注意力集中在计算机和网络系统部署移动目标防御技术来提供更安全的服务, SDN 是基于开放标准的灵活架构, 具有一系列新的安全威胁与挑战, 而移动目标防御技术致力于构建一个不断变换的环境来防御攻击, 一方面 SDN 可以利用移动目标防御技术保证自身网络的安全性, 与此同时, SDN 集中控制、灵活定制的独特优势可以更好地发挥移动目标防御技术的防御效能, 因此将移动目标防御的动态变换与软件定义网络的灵活编排相结合已成为更具应用价值的研究热点。

2 安全威胁

在 SDN 场景下, 根据 SDN 的逻辑架构, 其面临的安全威胁分为以下 3 大类, 如图 2 所示。

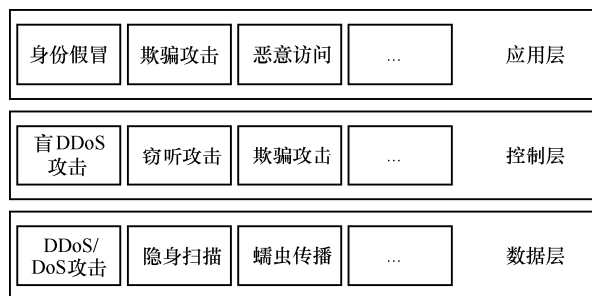


图 2 SDN 各层面临的安全威胁

(1) 数据层面临的安全威胁

软件定义网络中数据层^[10-11]主要是由 OpenFlow 交换机、路由器、中间盒、服务器、虚拟机等设备组成, 其中, OpenFlow 交换机是数据层最重要的设备之一, 负责流表的转发功能, 但现有的基于 SDN 的 OpenFlow 交换机基本使用软件可编程的网络处理器进行数据分组传输, 因此, SDN 数据平面容易受到利用转发设备中的软件漏洞发起未经请求的攻击^[12]。与传统网络中面临的安全威胁相似, 数据层面临的主要安全威胁包

括：DDoS/DoS 攻击^[13]、隐身扫描、蠕虫传播、缓冲区溢出攻击等安全威胁，其中，网络扫描攻击是该层面临最大的安全威胁；数据层的 DDoS 攻击通过僵尸网络对交换设备之间的通信进行干扰，通过受干扰的交换机可以向其他交换机发送大量无效消息，很容易造成局部网络瘫痪，甚至将影响扩散到全局网络。

(2) 控制层面临的安全威胁

SDN 控制器大都属于集中式 SDN 控制器，一方面负责将请求从 SDN 应用层转发到 SDN 数据路径，另一方面负责向 SDN 应用提供网络的抽象视图。对于集中式模型控制器而言，单点故障是一个非常普遍的安全威胁^[14]，SDN 控制器容易受到 DDoS 攻击和盲 DDoS 攻击，其中，控制层的 DDoS 攻击危害影响更为突出，与数据层面临的 DDoS 攻击不同，攻击者利用控制器与数据层交换设备的交互发起攻击，通过向控制器发送大量虚假请求而增加控制器的工作负载，从而导致控制器无法提供正常服务功能。此外，解析与编码语言的错误也会增加 SDN 控制器的额外漏洞，由于 SDN 控制器和 SDN 交换机之间缺少加密通信，攻击者同样可以针对控制层发起窃听攻击和欺骗攻击。

(3) 应用层面临的安全威胁

SDN 应用层可用可编程的方式直接向 SDN 控制器发送网络请求，它包括一个 SDN 应用逻辑和一个或多个 NBI 驱动器，由于应用层的应用程序采用分布式布局，未经身份验证的应用程序与 SDN 控制器之间缺乏信任机制^[15]，很容易发生欺骗攻击；此外，不适当的授权可能导致应用程序遭受到攻击者的恶意访问，攻击者通过脆弱的 API 接口获得对整个 SDN 网络控制权，传统网络所面

临的安全威胁在应用层可能会被放大。

表 1 中列出了 SDN 面临的安全威胁的分类，将可能面临的安全威胁与可能受影响的 SDN 3 层之间建立对应关系。

表 1 SDN 网络面临的安全威胁

安全威胁	数据层	控制层	应用层
未经授权的控制器访问	√	√	
未经身份验证的应用程序		√	√
流规则泄露	√		
转发规则泄露	√		
流规则修改	√	√	
欺骗性规则插入		√	√
控制器-交换机通信泛洪	√	√	
交换机流表泛滥			√

3 实现架构

移动目标防御体系结构的理论支持是由 Zhuang^[16]首次提出的，图 3 给出了 MTD 的理论模型，将物理网络映射到逻辑任务模型，由调整引擎获取逻辑任务模型的当前状态，并由配置管理调整产生新状态进行适应，此外分析引擎会获取物理网络的实时事件，利用传统防御中入侵检测、防火墙等检测机制进行脆弱性分析，由逻辑安全模型产生逻辑安全状态发送给调整引擎，形成一个闭合自反馈的动态调整系统。

Kampanakis 等^[17]基于 Zhuang 的 MTD 理论提出了一个 SDN 安全模型，如图 4 所示，根据 SDN 控制器上运行的 MTD 安全模型进行适应性调整。控制器对当前的网络状态进行抽象，适应性引擎定期执行随机网络适应策略，分析引擎从网络元素和当前配置导出实时数据事件，以评估

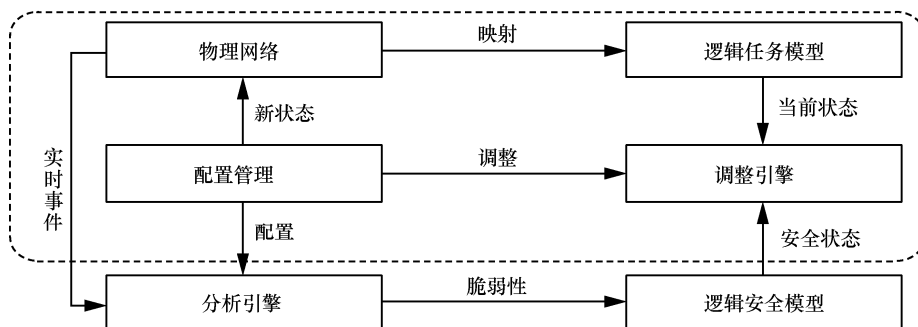


图 3 MTD 理论模型

SDN 网络对威胁和攻击的暴露程度, MTD 模块主要由 MTD 网络模型、分析引擎、适应引擎、计算引擎、配置管理以及可编程等插件构成, 但绝对不仅仅局限于在控制层部署, 可以通过在应用层开发相应的应用程序实现相应的功能。

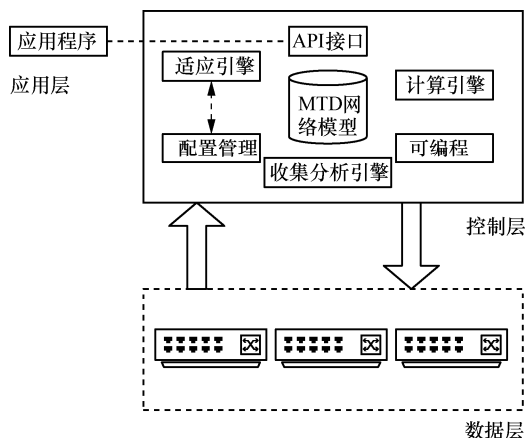


图 4 面向 SDN 的移动目标防御安全模型

随着云计算技术的逐渐兴起, 针对 SDN 多租户数据中心网络基础设施的安全问题, Chun 等^[18]基于提出了安全弹性网络服务架构——SeReNe (secure and resilient networking), 根据网络安全与情制定相应的防御策略, 一方面, 在网络和软件层面建立 MTD 框架; 另一方面, 根据网络带宽分配的有效性, 最大限度地减少对应用的干扰和部署成本, 选择最佳策略, 建立可编程网络 MTD、软件漏洞缓解 MTD 以及安全性流量工程模型。针对 SDN 控制器与交换机的安全问题, Zhou 等^[19]基于生物启发提出了一种演进式防御架构 (EDM), 它由 4 个可独立演变的模块组成: 安全信息检测、变化策略选取、变换策略库以及配置生成器, 协调一致地根据系统、用户或者当前的网络安全状态, 选择一种高效的网络配置变化策略来应对相应的安全威胁。结合 SDN 的实施, EDM 从新的角度解决了安全问题, 并且能够促进新的网络安全技术发展。更进一步地, 针对盲目采用 MTD 策略造成的网络关键服务不可用问题, Wang 等^[20]则提出了 CHAOS 架构, 它可以在网络中区分并混淆具有不同安全级别的主机, 将主机作为移动目标来混淆攻击者, 引入了混沌塔清洗 (CTO) 方法, 该方法使用混沌塔结构 (CTS) 描绘网络中所有主机的层次结构, 并提供更加

不可预测和灵活的混淆方法, 通过快速的 CTO 算法最大化网络的不可预测性, 实验证明, CHAOS 能够有效降低信息暴露比例, 保证流量正常流动, 在保证关键业务可用性的同时大大降低性能和成本。

4 技术分类

4.1 数据层移动目标防御技术

在攻击者对 OpenFlow 交换机发起攻击之前, 需要获得攻击目标确切的 IP 地址、端口号或转发路径, 因此移动数据层的这些参数会减轻有针对性的侦察攻击的损害范围^[21]。针对数据层的一系列攻击, 当前面向 SDN 的移动目标防御技术主要分类以下 3 种技术: 1) 地址跳变; 2) 路由跳变; 3) 端口跳变。

4.1.1 数据层地址跳变

当前网络 IP 地址的静态配置, 使攻击者可以通过远程扫描准确快速地识别目标, 给现有网络带来了极大的安全隐患。

2012 年, Jafarian 等^[22]提出了一种数据层地址跳变机制, 称为 OF-RHM (OpenFlow 随机主机跳变), 通过 OpenFlow 交换机实现虚拟地址 (vIP, virtual IP) 到真实地址 (rIP, real IP) 的透明跳变, 以最小化的操作开销保证配置完整性, 基于虚拟 IP 地址的通信流程如图 5 所示。实验结果表明, OF-RHM 可有效防御隐身扫描、蠕虫传播和其他基于扫描的攻击, 但对于分布式攻击等其他攻击模型很难达到预期的效果。更进一步地,

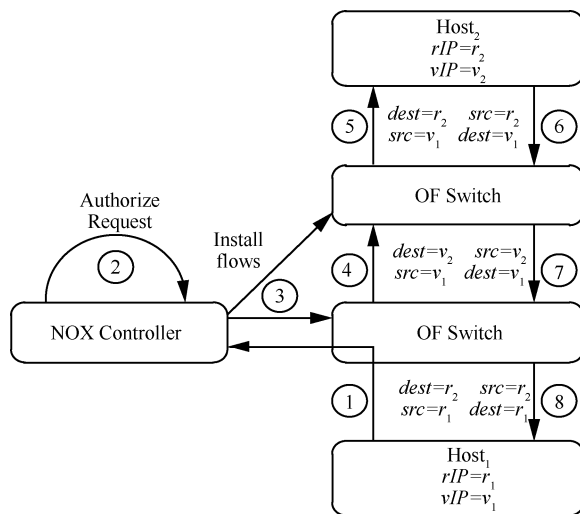


图 5 基于虚拟 IP 地址的通信流程

Corbett 等^[23]采用 OpenFlow 组件完成了 OF-RHM 的硬件测试,与此同时,为了解决同步问题,基于信息调整机制构建协议转换框架,并针对智能干扰攻击对 OF-RHM 系统的防御效果进行了评估,实验结果表明,OF-RHM 系统可以成功抵御智能干扰攻击。

为了进一步防御攻击者的复杂威胁,2014 年, Jafarian 等^[24]又提出了时空地址跳变技术 (STAM),使每个主机的 IP 绑定根据主机源标识 (空间随机化) 和时间参数 (时间随机化) 在网络中随机变化,将每个真实 IP 地址 (rIP) 映射到一个根据源标识和时间参数确定的瞬时 IP 地址 (eIP),2015 年, Jafarian 等^[25]又提出了一种新型主动自适应防御机制,自适应地将网络主机地址重新配置,一方面通过快速准确的非一致性和非重复性假设检验表征攻击行为,另一方面通过终端主机和网络设备管理实现 IP 随机化跳变,这种对抗性侦察的自适应跳变可以有效缓解攻击并提高可检测性,但增加了实际部署的复杂度,在实际应用中可能无法达到预期的实验效果。随后 Jafarian 等^[26]在综合上述研究成果之后提出了随机主机地址跳变机制,通过快速高效且不可预测的地址随机化实现最大化的防御效果,同时尽可能降低操作和配置开销。将地址跳变建模为多级可满足性问题,通过对抗侦察快速表征适应性跳变方案,保证网络的完整性和可管理性。同样, Chavez 等^[27]在进行 IP 地址跳变的同时,利用 SDN 控制器学习拓扑并为流量分配随机流量,使 SDN 更具确定性。

但是这些工作存在以下 2 个问题:一是没有在实际网络中提出相应的框架,二是没有考虑 SDN 交换机的不可信因素。为了检测攻击类型,针对 DoS 攻击以及蠕虫病毒, Smith 等^[28]提出了数据驱动的机制,通过增强拓扑算法 (NEAT) 识别稀疏神经网络拓扑进行轻量级检测,利用 SDN 启动移动目标防御策略,可以有效地干扰恶意用户的攻击行为。而对于 SDN 数据层元素的不可信问题, Nojournian 等^[29]提出了一种博弈论解决方案以防止共谋攻击 (collusion attack),基于 SDN 的平台进行网络欺骗和共谋攻击建模。

Macfarland 等^[30]基于 SDN 提出了一种新的

可扩展的移动目标防御机制,为未修改的客户端提供服务,同时将可信客户与不可信客户区分开来,利用传统网络中的 DNS 和 NAT 流程,允许防御者使用预共享密钥、加密 MAC 或将密码嵌入标准主机名中,以便为传统客户端提供访问控制,从而区分可信和不可信的客户端。实验结果表明,该方法对网络原有性能造成的延迟不会影响用户的正常操作。Chavez 等^[31]提出了基于 SDN 的 IP 地址随机化机制,编写了一个 IP 地址随机化应用程序,其核心组件由以下 3 个部分组成:网络随机化算法、OpenFlow 接口 (NWR) 随机 IP 地址生成器 (GEN)、网络映射数据库模块 (NETMAP)。NWR 组件负责读取流表信息并构建后端数据库;GEN 组件用于跟踪随机化 IP 地址和真实 IP 地址;NETMAP 用于存储网络映射数据库,为 NWR 算法提供必要的函数支持。针对当前地址跳变局限于某一子网变化空间不充分的问题,为了进一步增加不确定性, Wang 等^[32]提出了一种动态地址解决方案,将可供跳变的地址空间从特定的子网扩展到整个网络地址,并提出一种基于交换机自学习算法的新算法部署在 SDN 控制器,可以在很大程度上提高地址跳变的不确定性和不可预测性。

4.1.2 数据层路由跳变

面对数据层不同的攻击行为, Aydeger 等^[33]针对 DDoS 攻击中的新型交火攻击,提出了路由跳变的 MTD 防御机制,设计和部署了 ICMP 监测模块、跟踪路由分析模块、路由跳变模块和拥塞链路监测模块。评估结果表明,该防御机制可有效降低链路泛洪机会,从而减少目标链路拥塞,且不会对网络服务造成任何重路由大的干扰。针对链路洪泛攻击^[34] (LFA, link-flooding attack), Wang 等^[35]提出了一种称为 Linkbait 的主动 LFA 缓解机制,它是由链路筛选、链路混淆和僵尸网络检测 3 部分组成,通过为攻击者提供虚假链路图有效地缓解 LFA,创造性地提出了链路混淆算法和僵尸网络检测算法, Linkbait 能以非常低的网络延迟有效缓解 LFA。而对于网络窃听攻击, Aseeri 等^[36]提出了一种反窃听双向多路由机制,利用 Dijkstra 算法^[37]找到发送方和接收方之间的最短路由以及下一个最短路由。结果表明,

反窃听双向多路由方法可以完全避免数据被捕获,并且与之前已有的多路由方法相比,可以大大减少数据暴露的可能性。针对网络窃听攻击, Liu 等^[38]提出了一种随机路由跳变机制 RRMF,如图 6 所示,它由网络信息采集、跳变路由触发、跳变路由生成以及跳变路由更新 4 个阶段构成,通过攻击者破获节点数、不同网络节点规模、抗 DoS 攻击性能以及转发性能等实验验证,在增加网络窃听难度的同时,有效降低了正常数据转发的时延问题。

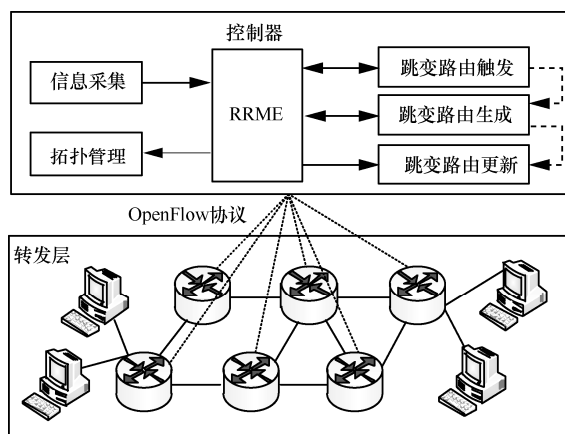


图 6 基于 OpenFlow 协议的随机路由跳变架构

在理论求解方面, Duan 等^[39]使用可满足性模理论 (SMT) 将路由跳变建模为约束补偿问题,并提出一种新的覆盖布局技术以最大化路由跳变的有效性,最后在不同攻击模型以及参数选择下进行了验证评估,更进一步地, Lei 等^[40]通过可满足性模理论形式化规约路径跳变所需满足的约束,以防止路径跳变引起的瞬态问题,提出了基于最优路径跳变的网络移动目标防御技术。Jafarian 等^[41]将博弈论和约束补偿问题的优化相结合,将随机路由防御和 DoS 攻击之间的交互作为一种博弈过程进行建模,并利用 SMT 进行形式化和模型优化,实施表明该方案可以高效部署在网络上,而不会对流量造成任何干扰。与前人工作不同, Rauf 等^[42]将路由跳变形式化为高效和有弹性的端到端 (E2E) 可达性问题,设计并实施了分散式端点路由跳变 (EPRM) 协议,最后,基于 PlanetLab 验证所提方案的正确性、有效性和可扩展性。

Haack 等^[43]提出了基于 Ant 的网络防御机

制 (ABCD, ant-based cyber defense)^[44],其系统架构如图 7 所示。它使用多代理系统和 MTD,根据代理的密度来检测攻击,将具有不同参数的传感器蚂蚁与监控主机的软件相结合,当发生攻击时,传感器蚂蚁聚集在受害主机周围来确定攻击情况,但它采用的是完整的分布式系统,很难检测到对每个主机流量影响不大的攻击,因此, Miyazaki 等^[45]在 ABCD 系统的基础上,基于 SDN 设计了一个采用多代理系统的分布式防御算法,通过蚂蚁代理启发式的控制算法,感知检测攻击威胁并由 SDN 控制器确定数据分组的下一跳地址,以此通过路径的动态迁移完成对攻击的最大化防御。接下来需要进一步验证更大网络规模下以及其他网络拓扑模型下的防御效果。

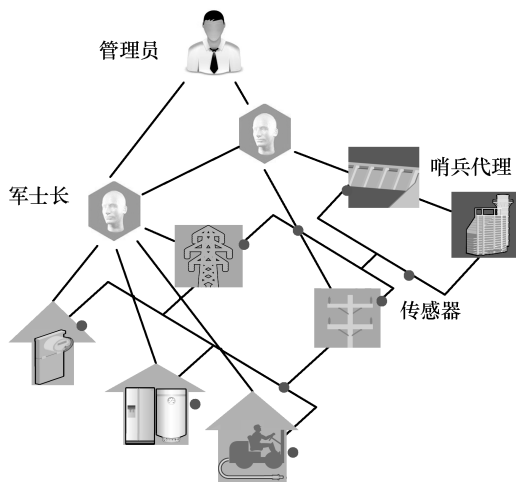


图 7 ABCD 系统架构

4.1.3 数据层端口跳变

SDN 数据层端口跳变的核心思想是将服务端动态随机映射到未使用的端口,使攻击者无法准确找到网路服务所使用的开放端口,以此达到混淆攻击者攻击行为的目的。

Kampanakis 等^[17]利用思科 One PK 实施了基于 SDN 的 MTD 应用程序,在真实的 SDN 环境中进行部署和实验,针对网络映射攻击,提出了基于 MTD 的反网络侦察算法,以便响应 TCP 端口扫描来执行 MTD 模糊处理。每个数据分组的操作都保存在缓冲区中以确保一致的行为。作为这种算法的结果,随机端口将作为开放端口出现在扫描阶段。攻击者需要更多资源深入挖掘以识

别运行在这些虚假开放端口上的服务。接着又提出针对操作系统指纹的 MTD 算法, 确保服务版本和操作系统不被攻击者正确识别。通过对攻击者的时间和流量成本的评估, 实验结果表明, 该方法可以显著增加攻击者的攻击开销, 但没有考虑 SDN 应用程序本身的成本 and 安全性, 仍然存在安全隐患。Lei 等^[46]提出了一种自适应变换的移动目标防御机制, 采用基于策略感知的跳变触发方法, 通过 Sibson 熵感知扫描攻击策略并选取跳变策略, 以提高跳变防御的针对性, 更进一步地, 为了扩大跳变空间, 提出了一种基于协同跳变的移动目标防御技术, 将端信息和转发路径协同变换, 极大地提高了跳变的不确定性。

针对端口跳变, 最大的难点就是同步问题, 当前端口跳变的同步方法有严格的时间同步^[48], 基于 ACK (确认) 的同步^[49]和基于时间戳的同步^[50], Luo 等^[51]为了解决端口跳变后可能带来的传输时延、流量阻塞、分组丢失重传等问题, 提出了基于密钥散列的自同步方案 (KHSS), 所提出的方法基于散列 MAC 生成消息认证码, 并将其作用于端口地址编码和解码的同步信息, 该方案为端口跳变通信系统提供了一包一跳和不可见消息认证的功能, 利用 SDN 独有的流表通信机制使客户端和服务端能够不断改变其身份, 并在不可靠的通信介质上执行消息认证, 而无需同步和认证信息传输, 最后在传统网络中进行了 KHSS 同步性能的验证, 实验结果表明, 该方案在安全性和跳变效率这 2 方面明显优于现有的方案, 但是该方案并没有利用 SDN 集中控制的优势进行部署搭建, 只是在理论分析了 SDN 流表转发的跳变优势。

与此同时, Zhang 等^[52]也对这一问题进行了研究, 提出了基于透明同步的 SDN 端口跳变机制, 将源、目节点独立以实现通信双方的透明同步传输, 一方面不需要严格的时间同步, 另一方面也不需要发送额外的同步数据分组, 它的理论分析和实验结果表明, 该方案能够在保证网络低开销的基础上有效抵抗各种攻击。针对 DoS 攻击, Zhang 等^[53]又提出了基于端口跳变的 SDN DoS 缓解机制 (PHS-DM), 它的结构框架如图 8 所示,

利用时间戳反馈实现端口的同步跳变, 在降低网络通信成本开销的基础上, 有效抵御端口扫描和内部攻击, 下一步需要将错误反馈引入到端口跳变中, 通过给攻击者提供虚假的端口跳变信息使防御更有主动性。

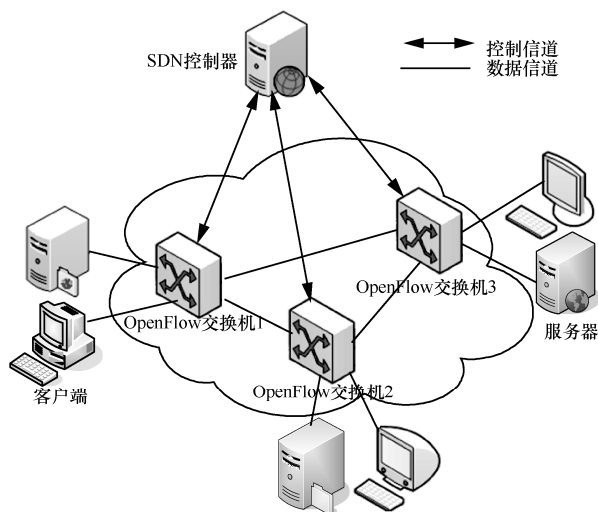


图 8 PHS-DM 结构框架

4.2 控制层移动目标防御技术

SDN 控制器是 SDN 最为核心的部件, 也是整个 SDN 系统安全链中最脆弱和最薄弱的环节, 它决定整个 SDN 的工作状态, 当控制器因受到攻击而无法正常工作, 整个 SDN 将陷入瘫痪, 因此 SDN 控制层的安全问题尤为重要, 针对 SDN 控制层的攻击也日渐常态化、多样化, 越来越多的研究学者将控制层的移动目标防御技术作为研究重点开展。

4.2.1 基于多控制器迁移机制 MTD 技术

为了抵御针对 SDN 控制器的盲 DDoS 攻击, Ma 等^[54]将 SDN 定义为一个半开放半封闭式的混合系统, 利用 SDN 的多控制器架构进行模型设计, 提出了基于多控制器迁移的移动目标防御机制, 采用多控制器池解决饱和问题, 并根据洪流密度动态地将控制器连接到交换机上。该机制将受保护的 SDN 系统分为多个控制器组成的控制器池、MTD 策略管理器, 基于路由映射规则的洪泛过滤设备和 SDN 交换机。其中, MTD 策略管理器负责监控在线控制器的带宽和负载, 当网络受到盲 DDoS 攻击时, MTD 策略管理器将多个离线控制器切换到在线状

态, 为其分配合适的 IP 地址。通过随机延迟扫描报文和路由映射过滤泛洪, 该技术可以有效抵御盲 DDoS 攻击, 保护 SDN 的可用性和可靠性。但是, 该方法仍存在以下局限性: 一方面, 采用随机数据分组传输延迟的方法会影响正常的数据传输性能; 另一方面, 路由表过期可能产生误报影响系统正常运行。

4.2.2 基于 CP 动态防御机制的 MTD 技术

针对使用 DPID 身份伪造对 SDN 控制器发起的 DoS 攻击, Wu 等^[55]研究了基于 OpenFlow 的 SDN 控制器上的数据路径识别 (DPID) 伪造攻击, 提出了一种基于 CP (client-puzzle) 的动态防御机制, 当客户端请求连接时, 服务器产生一个问题发送给客户端解决; 客户端在解决该问题后将答案发送回服务器进行验证。如果答案被成功验证, 完成后续交互; 否则不会有任何后续的交互, 通过生成多级困难问题实现对转发设备请求的动态管理, 从而提高攻击者的难度。该方法可以减少网络负载以及网络攻击流量, 并过滤掉合法流量, 增加攻击者的攻击开销和攻击难度。实验结果表明, 当控制器和转发设备的成本增加 2%~5% 时, 攻击者 CPU 的成本增加近 90%, 这大大增加了攻击者的攻击难度。下一步的工作是研究如何将 MTD 与 SDN 的动态可编程性结合起来, 并将其应用于 SDN 控制器北向接口的防御工作。

4.2.3 基于博弈奖惩机制的 MTD 技术

面对威胁日益严重的 DDoS 攻击, Chowdhary 等^[56]在前人工作基础上构建攻防过程中基于奖惩机制的博弈论机制, 将 DDoS 攻击建模为攻击者和管理员之间的动态博弈, 对实施 DDoS 流量的攻击者进行惩罚, 同时对合作的玩家进行奖励, 从而有效地为网络管理员实施期望的结果, 实现动态防御的目的, 体系架构如图 9 所示, 为解决网络带宽的速率问题, 提出贪心算法进行动态网络博弈中的惩罚机制, 通过研究 DDoS 攻击的 3 种典型攻击: SYN Flood 攻击、UDP Flood 攻击以及 ICMP Flood 攻击, 根据从 SDN 控制器收到的警报处理所有这些攻击, 以减轻对 SDN 控制器的大规模流量攻击, 并在不同的网络拓扑中进行应用, 具有很好的可扩展性。下一步工作是基于

OpenStack 的云框架进行更大规模的网络动态防御, 使用基于人工智能 (AI) 的算法识别攻击, 并使用异常检测以及基于签名的检测机制构建一个全面的攻击缓解解决方案。

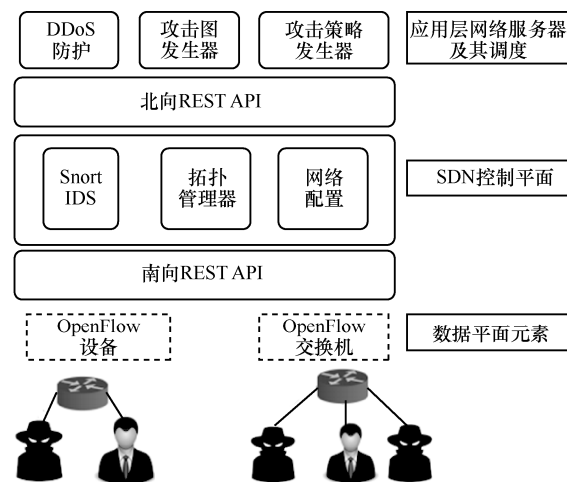


图 9 基于奖惩机制的体系架构

4.3 应用层移动目标防御技术

SDN 应用层中的漏洞可以给攻击者提供访问或修改受限数据的机会, 这使防御者必须尽可能地保护应用程序免受攻击者侦察, 由于当前 SDN 北向接口的定义尚不明确, 对于应用层的研究尚处在初步阶段, 因而对于应用层网络攻击防御问题研究较少, 很难从现有的文献中进行相关的总结分析。但是, 云计算体系架构以及网络功能虚拟化 (NFV) 的迅速兴起, SDN 应用层的虚拟机租户管理已经成为下一步的发展趋势, 因此, 针对 SDN 应用层虚拟化资源也将面临巨大的安全隐患。

4.3.1 基于动态访问控制的 MTD 技术

传统网络中的应用程序极易受到攻击者的 DDoS 攻击, Jantila 等^[57]在 Devi 等^[58]的基础上, 针对 SDN 应用层可能遭受 DDoS 攻击这一情况, 利用 STRIDE 威胁模型, 通过分析基于客户访问行为的信任值以及熵值区分攻击者与合法用户, 以确定应用层相关应用程序的脆弱性问题, 在允许它们访问服务器之前授权每个客户端, 网络元素本身根据流量信息和实时警报实施动态访问控制策略, 以此动态智能地保护网络和资源不被篡改数据、泄露信息, 但并没有对该方法的效率和有效性进行评估验证。

4.3.2 基于虚拟机迁移技术的 MTD 技术

针对 SDN 应用层的应用程序虚拟机极易受到 DoS 攻击这一安全问题, Debroy 等^[59]提出了一种基于智能 MTD 的主被动结合的虚拟机迁移机制,如图 10 所示,基于攻击概率的频率最小化和跨异构虚拟机的目标移动的位置选择,在保证云资源浪费最小化的情况下不影响应用性能,大大优化了迁移频率,很好地减少了网络资源的浪费,同时限制了攻击效应。此外,该方案还根据候选虚拟机容量、可用网络带宽以及攻击历史记录中虚拟机的信誉计算出理想的迁移位置,使用大规模 GENI 测试平台评估了方案的有效性,实验结果表明,该方案可以降低攻击成功率,提高应用性能。下一步工作将基于 MTD 解决方案的云管理考虑成本问题,以便在系统混淆和资源管理之间进行权衡,更好地实现系统地可用性。

类似地, Gillani 等^[60]提出在虚拟网络(VN)下动态地改变 VN 来重新分配网络资源,并向新资源提供持续的 VN 迁移,以此抵御大规模持续的 DDoS 攻击,整个防御过程基于 SMT 的形式化方法,利用非关键资源替代关键资源规避攻击的同时,建立了一种 VM 迁移机制,由虚拟化物理网络上框架生成的 VN 迁移策略,最后,利用 Mininet 工具进行实验仿真,仿真结果表明该方法可以在保证网络可用性的前提下很好地抵御 DDoS 攻击。

5 结束语

随着 SDN、云计算以及网络功能虚拟化的不

断结合,安全问题日益突出,面向 SDN 的移动目标防御技术还存在很多未解决的挑战,SDN 仍缺乏细粒度的安全性和可靠性,具有很大的发展潜力,打造一个真正安全可靠的软件定义网络还需要付出很多努力。

5.1 优化防御体系架构

目前,面向 SDN 的移动目标防御架构尚不成熟,缺乏相关的理论体系支持,可以考虑利用最新的相关技术进行 SDN 安全防御体系架构的设计与实施,设计更加弹性动态化的 SDN 动态防御体系架构,利用不断变换的攻击面暴露攻击者在侦察 SDN 信息时的攻击意图,以此实现更加主动的防御策略。

针对网络攻击中的 LM 网络杀伤链模型映射相应的网络动态防御链,在攻击者的每个攻击阶段都部署相应的移动目标防御策略,使整个 SDN 防御体系串联成链,统筹联动,给攻击者营造一个更加不可预测的网络环境,从而使整个网络攻防天平向利于防御者的一端倾斜。

5.2 层间联动防御技术

从具体实现技术来看,在数据层面的移动目标防御技术考虑从时间和空间 2 个维度同时进行动态变化,与此同时考虑变化频率的问题,在保证可用性的基础上,最大限度地减少网络管理人员的成本,此外,多个网络参数同时变化成为下一步的研究趋势,使端口、IP 地址以及路径路由等网络参数的变化更加不可预测,但网络可用性和安全性之间的平衡是一个很突出的研究问题。

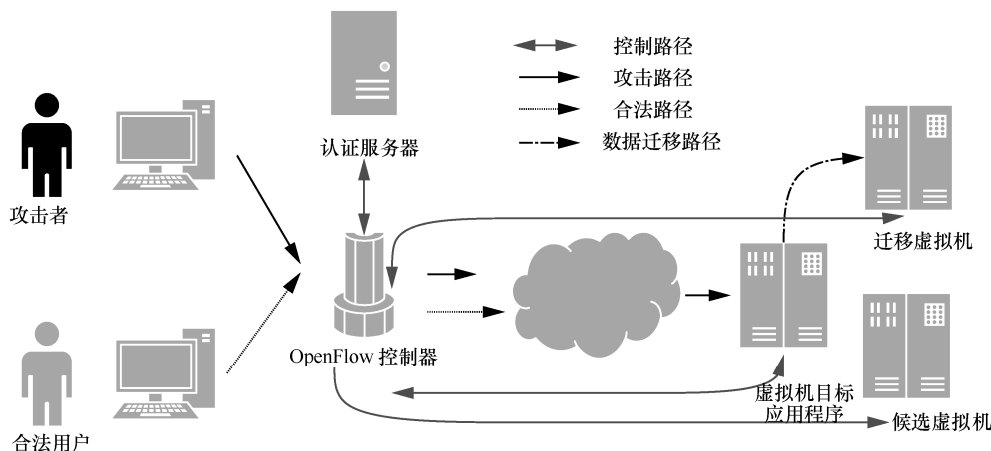


图 10 基于智能 MTD 的主被动结合的虚拟机迁移方案

对于控制层面而言,作为整个 SDN 的核心部件,要具备防御各种攻击的能力,仅仅解决某一攻击行为对控制器来说远远不够,需要建立攻击威胁数据库,确保在面对不同攻击时可以采取不同的移动目标防御策略进行防御,与此同时,如何快速有效地进行策略选取是一个值得关注的问题。

对于应用层而言,利用软件驱动网络进行自主通信,可完成自动测试、集成和网络功能部署等一系列安全防御机制,还可结合移动目标防御的思想利用机器学习技术进行网络安全动态的自我管理和优化,确保应用程序的安全性,在 SDN 安全应用程序开发方面,已经提出诸如 FRESKO^[61]、CloudWatcher^[62]以及 OrchSec^[63]等 OpenFlow 安全应用程序开发框架,鲜有学者将移动目标防御技术融入这一开发框架中实施动态防御。

下一步的研究方向不能仅仅考虑 SDN 单个层面的移动目标防御技术,要增加三层体系结构之间的联动配合,在优化后的防御系统架构之上,进行体系化的更加全面的移动目标防御技术部署,将整个面向 SDN 的移动目标防御技术环环相扣,构筑起更加安全可靠的 SDN。

随着学科交叉与融合的不断推进,可以通过跨学科、多领域的研究对 SDN 的移动目标防御技术进行新的探索,与此同时,随着越来越多的人将传统科学应用到计算机和互联网安全研究,跨学科跨领域研究应用必将在多样复杂的网络空间环境中发挥愈加重要的作用。

参考文献:

- [1] LANTZ B, HELLER B, McKeown N. A network in a laptop: rapid prototyping for software-defined networks[C]// ACM Workshop on Hot Topics in Networks. HOTNETS 2010, Monterey, Ca, Usa - October. DBLP, 2010:1-6.
- [2] KREUTZ D, RAMOS F M V, et al. Software-defined networking: a comprehensive survey[J]. Proceedings of the IEEE, 2014, 103(1): 10-13.
- [3] SCOTT-HAYWARD S, O'CALLAGHAN G, SEZER S. SDN security: a survey[C]// Future Networks and Services. IEEE, 2013:1-7.
- [4] EATHERTON W. The push of network processing to the top of the pyramid[C]// Architecture for Networking and Communications Systems. 2005.
- [5] BENTON K, CAMP L J, SMALL C. OpenFlow vulnerability assessment[C]// ACM SIGCOMM Workshop on Hot Topics in Software Defined NETWORKING. ACM, 2013:151-152.
- [6] OpenFlow Switch Specification v1.3.0 (2013)[S]. <https://www.open-networking.org/images/stories/downloads>
- [7] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense: creating asymmetric uncertainty for Cyber Threats[M]. Berlin: Springer, 2011, 54.
- [8] MANADHATA P K, WING J M. A formal model for a system's attack surface[J]. Advances in Information Security, 2011, 54:1-28.
- [9] ZHANG H G, HAN W B, LAI X J, et al. Survey on cyberspace security[J]. Science China Information Sciences, 2015, 58(11):1-43.
- [10] 雷程,马多贺,张红旗,杨英杰,王利明.基于网络攻击面自适应转换的移动目标防御技术[J/OL].计算机学报,2017(5):1-23.
LEI C, MA D, ZHANG H, et al. Moving target defense technology based on network attack surface self-adaptive mutation[J]. Chinese Journal of Computers, 2017(5):1-23.
- [11] MA D, LEI C, WANG L, et al. A Self-adaptive hopping approach of moving target defense to thwart scanning attacks[C]//International Conference on Information and Communications, Security, 2016.
- [12] PAPPAS A C, ASHOK A, GOVINDARASU M. Moving target defense for securing smart grid communications: architecture, implementation & evaluation[C]// Power & Energy Society Innovative Smart Grid Technologies Conference. IEEE, 2017:1-5.
- [13] ZARGAR S T, JOSHI J, TIPPER D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks[J]. IEEE Communications Surveys & Tutorials, 2013, 15(4): 2046-2069.
- [14] TOOTONCHIAN A, GORBUNOV S, SHERWOOD R, et al. On controller performance in software-defined networks[C]// Usenix Conference on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services. USENIX Association, 2012.
- [15] FEGHALI A, KILANY R, CHAMOUN M. SDN security problems and solutions analysis[C]// International Conference on Protocol Engineering. IEEE, 2015:1-5.
- [16] ZHUANG R. A theory for understanding and quantifying moving target defense[J]. Dissertations & Theses - Gradworks, 2015.
- [17] KAMPANAKIS P, PERROS H, BEYENE T. SDN-based solutions for moving target defense network protection[C]// World of Wireless, Mobile and Multimedia Networks. IEEE, 2014:1-6.
- [18] CHUN C J, XING T, HUANG D, et al. SeReNe: on establishing secure and resilient networking services for an SDN-based multi-tenant datacenter environment[C]// IEEE International Conference on Dependable Systems and Networks Workshops. IEEE, 2015:4-11.
- [19] ZHOU H, WU C, JIANG M, et al. Evolving defense mechanism for future network security[J]. IEEE Communications Magazine, 2015, 53(4):45-51.
- [20] WANG J, XIAO F, HUANG J, et al. CHAOS: an SDN-based moving target defense system[J]. arXiv: 1704.01482, 2017.
- [21] KOPONEN T, CASADO M, GUDE N, et al. Onix: a distributed control platform for large-scale production networks[C]//Usenix Conference on Operating Systems Design and Implementation. USENIX Association, 2010:351-364.
- [22] JAFARIAN J H, AL-SHAER E, DUAN Q. Openflow random host mutation: transparent moving target defense using software defined

- networking[C]// The Workshop on Hot Topics in Software Defined Networks. ACM, 2012:127-132.
- [23] CORBETT C, UHER J, COOK J, et al. Countering intelligent jamming with full protocol stack agility[J]. IEEE Security & Privacy, 2014, 12(2):44-50.
- [24] JAFARIAN J H, AL-SHAER E, DUAN Q. Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers[C]// ACM Workshop. ACM, 2014:69-78.
- [25] JAFARIAN J H, AL-SHAER E, DUAN Q. Adversary-aware IP address randomization for proactive agility against sophisticated attackers[C]// Computer Communications. IEEE, 2015:738-746.
- [26] JAFARIAN J H, AL-SHAER E, DUAN Q. An effective address mutation approach for disrupting reconnaissance attacks[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(12): 2562-2577.
- [27] CHAVEZ A R, STOUT W M S, Peisert S. Techniques for the dynamic randomization of network attributes[C]// International Carnahan Conference on Security Technology. IEEE, 2016:1-6.
- [28] SMITH R J, ZINCIR-HEYWOOD A N, JACOBS J T, et al. Initiating a moving target network defense with a real-time neuro-evolutionary detector[C]// Genetic and Evolutionary Computation Conference Companion. ACM, 2016:1095-1102.
- [29] NOJOUMIAN M, GOLCHUBIAN A, SAPUTRO N, et al. Preventing collusion between SDN defenders and attackers using a game theoretical approach[C]// Computer Communications Workshops. IEEE, 2017.
- [30] MACFARLAND D C, SHUE C A. The SDN Shuffle: creating a moving-target defense using host-based software-defined networking[C]// ACM Workshop on Moving Target Defense. ACM, 2015: 37-41.
- [31] CHAVEZ A R, STOUT W M S, PEISERT S. Techniques for the dynamic randomization of network attributes[C]// International Carnahan Conference on Security Technology. IEEE, 2016:1-6.
- [32] WANG S, ZHANG L, TANG C. A new dynamic address solution for moving target defense[C]// Information Technology, Networking, Electronic and Automation Control Conference, IEEE, 2016: 1149-1152.
- [33] AYDEGER A, SAPUTRO N, AKKAYA K, et al. Mitigating cross-fire attacks using sdn-based moving target defense[C]// Local Computer Networks. IEEE, 2016:627-630.
- [34] MIN S K, LEE S B, GLIGOR V D. The crossfire attack[C]// IEEE Symposium on Security and Privacy. IEEE Computer Society, 2013:127-141.
- [35] WANG Q, XIAO F, ZHOU M, et al. Linkbait: active link obfuscation to thwart link-flooding attacks[J]. arXiv:1703.09521, 2017.
- [36] ASEERI A, NETJINDA N, HEWETT R. Alleviating eavesdropping attacks in software-defined networking data plane[C]// Conference on Cyber and Information Security Research. ACM, 2017:1.
- [37] FEAMSTER N, REXFORD J, ZEGURA E. The road to SDN: an intellectual history of programmable networks[M]. ACM, 2014.
- [38] LIU J, ZHANG H, GUO Z. A Defense mechanism of random routing mutation in SDN[J]. IEEE Transactions on Information & Systems, 2017, 100(5):1046-1054.
- [39] DUAN Q, AL-SHAER E, JAFARIAN H. Efficient random route mutation considering flow and network constraints[C]// Communications and Network Security. IEEE, 2013:260-268.
- [40] 雷程, 马多贺, 张红旗, 等. 基于最优路径跳变的网络移动目标防御技术[J]. 通信学报, 2017, 38(3):133-143.
- LEI C, MA D H, ZHANG H Q, et al. Network moving target defense technique based on optimal forwarding path migration[J]. Journal on Communications, 2017, 38(3): 133-143.
- [41] JAFARIAN J H, AL-SHAER E, DUAN Q. Formal approach for route agility against persistent attackers[C]// European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2013:237-254.
- [42] RAUF U, GILLANI F, AL-SHAER E, et al. Formal approach for resilient reachability based on end-system route agility[C]// ACM Workshop on Moving Target Defense. ACM, 2016:117-127.
- [43] HAACK J N, FINK G A, MAIDEN W M, et al. Ant-based cyber security[C]// Eighth International Conference on Information Technology: New Generations. IEEE, 2011:918-926.
- [44] FINK G A, HAACK J N, MCKINNON A D, et al. Defense on the move: ant-based cyber defense[J]. IEEE Security & Privacy, 2014, 12(2):36-43.
- [45] MIYAZAKI R, KAWAMOTO J, MATSUMOTO S, et al. Host independent and distributed detection system of the network attack by using OpenFlow[C]// International Conference on Information NETWORKING. IEEE, 2017:236-241.
- [46] LEI C, ZHANG H Q, MA D H, et al. Network moving target defense technique based on self-adaptive end-point hopping[J]. Arabian Journal for Science & Engineering, 2017, 42(8):1-14.
- [47] ZHANG H Q, LEI C, CHANG D X, et al. Network moving target defense technique based on collaborative mutation[J]. Computers & Security, 2017, 70:51-71.
- [48] LEE H C J, THING V L L. Port hopping for resilient networks[C]// Vehicular Technology Conference, IEEE, 2004:3291-3295.
- [49] 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.
- [50] SHI L, JIA C, LÜ S, et al. Port and address hopping for active cyber-defense[M]// Intelligence and Security Informatics. Springer Berlin Heidelberg, 2007:295-300.
- [51] LUO Y B, WANG B S, WANG X F, et al. A keyed-hashing based self-synchronization mechanism for port address hopping communication[J]. Frontiers of Information Technology and Electronic Engineering, 2017, 18(5):719-728.
- [52] ZHANG L, WANG Z, GU K, et al. Transparent synchronization based port mutation scheme in SDN network[C]// International Conference on Computer Science and Network Technology. 2016: 581-585.
- [53] ZHANG L, GUO Y, YUWEN H, et al. A port hopping based dos mitigation scheme in SDN network[C]// International Conference on Computational Intelligence and Security. IEEE, 2017:314-317.
- [54] MA D, XU Z, LIN D. Defending blind DDoS attack on SDN based on moving target defense[C]// International Conference on Security and Privacy in Communication Networks. 2014:463-480.
- [55] WU Z, WEI Q, REN K, et al. A dynamic defense using client puzzle

- zle for identity-forgery attack on the south-bound of software defined networks[J]. Ksii Transactions on Internet & Information Systems, 2017, 11(2):846-864.
- [56] CHOWDHARY A, PISHARODY S, ALSHAMRANI A, et al. Dynamic game based security framework in SDN-enabled cloud networking environments[C]// ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. ACM, 2017:53-58.
- [57] JANTILA S, CHAIPAH K. A Security analysis of a hybrid mechanism to defend DDoS attacks in SDN [J]. Procedia Computer Science, 2016, 86:437-440.
- [58] DEVI S R, YOGESH P. A Hybrid approach to counter application layer DDoS attacks[J]. International Journal on Cryptography & Information Security, 2012.
- [59] DEBROY S, CALYAM P, NGUYEN M, et al. Frequency-minimal moving target defense using software-defined networking[C]// International Conference on Computing, Networking and Communications. IEEE, 2016:1-6.
- [60] GILLANI F, AL-SHAER E, LO S, et al. Agile virtualized infrastructure to proactively defend against cyber attacks[C]// Computer Communications. IEEE, 2015:729-737.
- [61] SHIN S, PORRAS P, YEGNESWARAN V, et al. FRESKO: modular composable security services for software defined networks[J]. Proceedings of Network & Distributed Security Symposium, 2013.
- [62] SHIN S, GU G. CloudWatcher: network security monitoring using openflow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)[C]// IEEE International Conference on Network Protocols. IEEE Computer Society, 2012:1-6.
- [63] ZAALOUK A, KHONDOKER R, MARX R, et al. OrchSec: anorchestrator-based architecture for enhancing network-security using Network Monitoring and SDN Control functions[C]//Noms. IEEE, 2014:1-9.

[作者简介]



谭晶磊（1994-），男，山东章丘人，信息工程大学研究生，主要研究方向为网络信息安全、移动目标防御。

张红旗（1962-），男，河北遵化人，信息工程大学教授、博士生导师，主要研究方向为网络安全、移动目标防御、等级保护和信息安全管理。

雷程（1989-），男，北京人，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、数据安全交换和网络流指纹。

刘小虎（1989-），男，河南太康人，信息工程大学讲师，主要研究方向为动态网络防御。

王硕（1991-），男，河南南阳人，信息工程大学博士生，主要研究方向为网络系统安全。