DOI:10.13718/j.cnki.xsxb.2020.11.014

一种防御 SDN 路由欺骗攻击的轻量级解决方案①

王 照[1], 陈恩庆[2]

1. 河南护理职业学院 公共学科部,河南 安阳 455000;2. 郑州大学 信息工程学院,郑州 450052

摘要:针对现有技术对某些特定分布式拒绝服务(Distributed Denial of Service, DDoS)攻击检测精度不够的问题,提出了一种防御软件定义网络(Software Defined Network, SDN)中路由欺骗(Route Spoofing, RS)攻击的轻量级解决方案. 该方案通过分析路由欺骗产生的原因,在数据平面 OpenFlow 交换机上设计了选择性阻塞扩展模块,一旦检测器发现 RS 攻击,交换机将生成的报警包发送给控制器,控制器通过发送转发规则阻止攻击者节点恶意使用其他用户的活动通信路由. 仿真结果表明,本文方法可以有效地检测出 SDN 中的 DDoS 攻击,相关指标也充分显示了解决方案的可行性和正确性.

关 键 词:软件定义网络;网络安全;DDoS 攻击;路由欺骗

中图分类号:TP393 **文献标志码**:A **文章编号**:1000-5471(2020)11-0093-06

随着计算机网络的不断发展,软件定义网络(Software-defined Networking, SDN)[1]在现代网络设计中发挥了重要作用,越来越多地应用于校园网络、企业网络、光网络等场景. 由于 SDN 在各场景的广泛应用,其本身的安全性也日益成为研究人员关注的热点问题[2]. 分布式拒绝服务(Distributed Denial of Service, DDoS)[3]攻击是 SDN 面临的最直接威胁之一,利用 SDN 环境下集中控制的特点攻击控制器和利用交换机基于流表转发的特点泛洪攻击数据平面,可以造成控制器系统资源或者交换机流表缓存耗尽、链路带宽阻塞等问题.

近年来,研究人员提出了各种解决方案来对抗 SDN 网络中的 DDoS 攻击[4]. Ambrosin 等[5]提出了一种有效的解决控制平面饱和攻击的数据平面解,该解充当 TCP(Transmission Control Protocol)代理,使用连接迁移和概率黑名单机制来防止攻击到达控制平面. Mohammadi 等[6]提出一种有效的缓解 SDN 中 TCP-SYN 泛洪攻击的策略 SLICOTS,SLICOTS 作为 OpenDaylight 控制器的扩展模块,利用 SDN 的动态可编程性来监视进行中的 TCP 连接请求和阻止恶意主机. 但是,SLICOTS 容易受到 MAC(Media Access Control)的欺骗,也无法将 Flash 群组与攻击流量进行区分. Liu 等[7]提出的一种基于泛光防护的分布式拒绝服务攻击检测和防御系统,该方法基于 SDN 和集中控制等特点,通过采用动态 IP(Internet Protocol)地址绑定来解决 IP 欺骗问题、集中控制下发流表来阻止源端口攻击的手段,进而检测和抵抗 DDoS 攻击. 文献[8]建议通过基于未修改的现有商用 SDN 交换机的自适应相关分析方法来实时监控 DDOS 攻击,有效抑制泛洪攻击,但是此种方法容易受到 MAC 和 IP 的欺骗攻击. 文献[9]为了减轻 Openflow(OF)网络中的 DoS 攻击,设计了一个基于 NOX 控制器的安全应用模块 SGuard,该模块包括采用六元组作为特征向量对流量进行分类并采用选择算法优化排序,使得 SGuard 模块在 SDN 网络中不增加开销的同时,抑制 DoS 的攻击. 由于控制器容量限制,无法接收和分析来自所有交换机的全部网络流信息. 大多数现有技术利用 OF 交换机对流信息进行预处理,生成汇总统计报告给控制器. 但是这将导致额外的部署成本,也会因为丢失关键原始信息,导致控制器错误地忽略攻击流.

① 收稿日期:2019-12-06
基金项目:国家自然科学基金项目(U1804152).
作者简介:王 照(1980—),男,硕士,副教授,主要从事计算机应用研究.

由于现有技术对某些特定攻击检测精度不够，本文针对SDN中的路由欺骗(Route Spoofing，RS)DDoS攻击提出了有效的解决方案，用以检测和防御该类攻击的发生. 通过分析攻击产生的主要原因，在数据平面OF交换机上设计出一个简单且实际可行的扩展，可以及时有效地解决上述DDoS攻击.

1 软件定义网络

SDN是一种创新型网络架构，其目的主要是对网络的有限资源进行最优利用，并且通过将控制平面与数据转发平面相分离来实现灵活的网络管理. 其中，控制平面是由独立主机构成的控制器来运行，可以控制整个网络的交换机，是整个SDN体系的核心平面，其时延、带宽和吞吐量决定了SDN的性能. SDN具有灵活的软件编程能力，能够满足网络的资源规模扩展、自动化管理和灵活组网的要求[10]. SDN控制架构的发展大致可分为4个阶段：4D架构、Ethane架构、OpenFlow架构以及可扩展性架构. 图1给出了基于OpenFlow架构的典型SDN体系结构.

该结构主要包括3层：底层是基础设施层，该层的主要功能是根据控制层提供的指令对网络数据进行转发；中间层是控制层，由于底层设备复杂的控制逻辑被抽象出来集中在控制层上，因此它具有可编程控制应用程序，主要有拓扑发现、设备管理、路由计算、防火墙等功能模块，为网络设备提供一组有关通信量管理的指令；顶层是应用层或应用平面，它包含一组业务应用程序，可以为网络提供额外的服务，如负载平衡、安全性和监控应用程序.

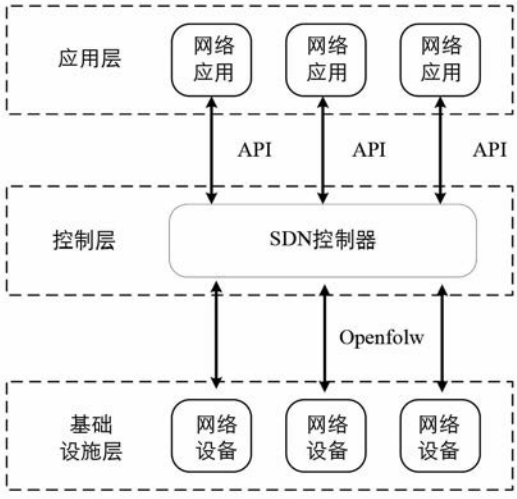

图1 基于OpenFlow的SDN体系结构示意图

通常，SDN架构中存在3种不同类型的组件：远程中央控制器、网络设备(如交换机)和通信协议(如OpenFlow协议[11]).

(1) 远程中央控制器

SDN控制器是网络的核心组件. 控制器的主要任务是根据预先编程的控制应用来进行网络通信量管理. 通过SDN，远程控制器将接收来自网络设备的路由请求，按照要求的说明进行回复. 由于控制器应用程序的处理能力有限，需要对SDN体系结构进行优化.

(2) 网络设备

在基于SDN的网络中，网络设备部署在基础设施层中. 这些设备是SDN体系结构的关键组成部分，它们的主要任务是根据SDN控制器提供的一些路由指令进行交互用以转发网络通信量. 此外，这些设备还可以向控制器提供有关整个网络通信量的统计信息. 这些设备通常需要中央控制器的持续协助. 每个交换机都包含一个存储大量流条目的流表. 每个条目都由控制器提供，并包含路由指令，使交换机能够根据这些指令处理即将到来的通信量.

(3) 通信协议

OpenFlow是一种将网络设备连接到远程中央控制器的通信协议. 当网络设备接收到新的通信量时，它们使用OpenFlow通信通道向远程控制器发送所需操作的请求. 控制器还可以使用此通道来处理和操作网络设备.

2 路由欺骗攻击和解决策略

本文通过分析SDN中路由欺骗RS攻击产生的原因，在数据平面OF交换机上设计了选择性阻塞扩展模块，该模块通过检查OF交换机上的每个传入消息并将可疑恶意消息转发给控制器的方式应对RS攻击.

2.1 路由欺骗攻击

在SDN中，恶意用户可以通过网络中现有活动数据流的信息来发送其消息. 在无线局域网中，存在多

个节点连接到一台 OF 交换机上，攻击方可以对这些 OF 交换机进行窃听攻击来了解活动数据流. 一旦窃听攻击成功，将获得有关活动数据流的信息，进而将其相邻节点的 IP 地址作为自身发送消息的源 IP 地址，以欺骗路由的方式进行数据传输，即通过所属网络中其他用户的活动路由发送流量来执行 RS 攻击. RS 攻击的危害有很多，攻击方可以利用 RS 攻击以相邻节点的 IP 进行免费数据传输，而造成真正用户的额外付费. 同时，由于数据平面的通信带宽有限，RS 攻击可能导致数据平面上不同程度的拥塞.

图 2 和表 1 给出了 RS 攻击的一个实例. 从表 1 可以看出，控制器安装的规则是：源和目标 IP 分别为 192.168.1.1 和 192.168.1.4 的端口 1 将接收到的所有数据包转发到输出端口 3，源和目标 IP 分别为 192.168.1.2 和 192.168.1.3 的端口 2 将接收到的所有数据包转发到输出端口 4. 假设主机 2 是一个攻击节点，根据表 1 中的条目，攻击者只能向主机 3 发送数据. 由于主机 1、2 都连接到交换机，交换机连接到 S1 的端口 1 上，因此主机 2 可以伪造主机 1 的 IP 地址，向主机 3 发送数据，从而可能导致数据平面资源耗尽攻击.

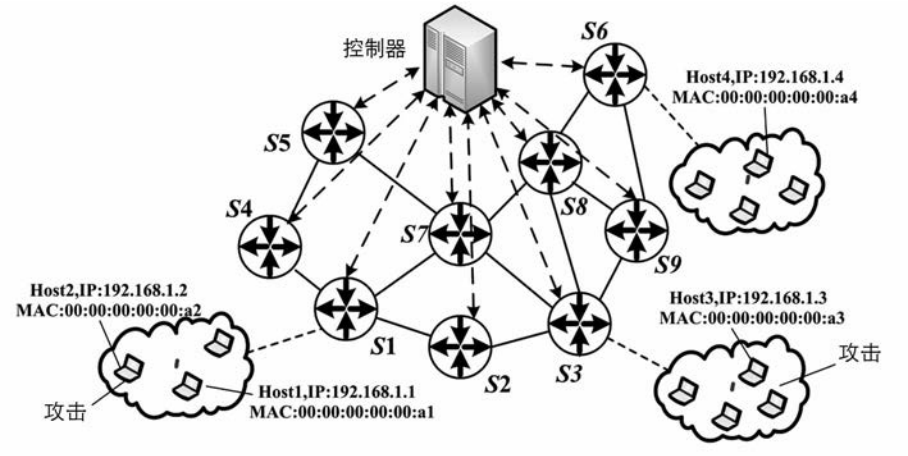

图 2　RS 攻击实例示意图

表 1　S1 交换机中的转发表

P_in	端口 1	端口 2	…
SRC_MAC	*	*	…
DST_MAC	*	*	…
SRC_IP	192.168.1.1	192.168.1.2	…
DST_IP	192.168.1.4	192.168.1.3	…
…	…	…	…
Actions	端口 3	端口 4	…

2.2　解决策略

本文采用选择性阻塞模块来应对 RS 的攻击，该模块由 2 个检测单元(IP 和 MAC 欺骗检测器)组成，如图 3 所示. 从图 3 中可以看到，在接收到新消息时，IP 欺骗检测器会检查 IP 欺骗攻击，如果未检测到 IP 欺骗，则将消息转发到 MAC 欺骗检测器来完成后续检测. 如果 IP 或 MAC 欺骗检测器检测出攻击，则通知控制器采取进一步的措施，若两者都没检测到欺骗，就由交换机处理数据包.

IP 欺骗检测器在检测过程中创建一个表，该表存储当前活动流的 IP 和 MAC 地址，如表 2 所示. 对应表中每个条目都包含唯一的〈IP，MAC〉对. 假设在任何时间内单个 IP 地址仅与一个 MAC 地址绑定，因此对应表中〈IP，MAC〉对的每个条目都满足一一对应的映射关系 R：$IP_i \rightarrow MAC_i$. 当 OF 交换机接收到数据包时，运行在其上的 IP 检测器将从数据包中提取出〈IP，MAC〉对，并在对应表中检查其关系 R. 如果网络表中不存在该对，则将其添加. 但是，如果对应表中存在与多个不同的 MAC 地址相关联的 IP 地址时，则可断定存在欺骗攻击.

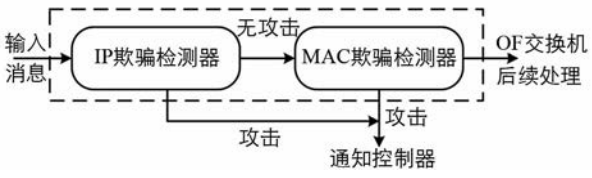

图 3　OF 交换机上运行的检测单元

MAC欺骗检测器通过跟踪每个数据流的序列号来检测MAC欺骗攻击. 当收到一帧后，检测器计算当前帧的序列号与从同一源地址接收的最后一帧的序列号之间的间隙G. 如果$G=0$，代表当前帧为重传帧，如果$G=1,2$，表示当前帧是正确的帧. 但是，如果$G\in[3,4096]$，则被认为是异常序列号. MAC欺骗检测器具有以下优点：不需在终端主机上更改、提取MAC欺骗检测的序列号时不会产生额外的开销、当攻击者预测下一个序列号时检测方法仍然稳健.

表2 IP和MAC对应表

IP地址	MAC地址
96.168.1.1	00:00:00:00:00:a1
96.168.1.2	00:00:00:00:00:a2
96.168.1.3	00:00:00:00:00:a3
96.168.1.4	00:00:00:00:00:a3
…	…

一旦在交换机边缘运行的任何检测单元遇到异常情况时，交换机将生成一个包含源主机〈IP，MAC〉对的报警包. 控制器上的缓解装置在收到警报包后即可被激活. 缓解单元作为OpenDaylight控制器上的一个模块来实现，该模块使用IListenDataPacket服务接口来监听传入的数据包. 特别是在OpenDaylight控制器内，HostTracking模块创建并维护主机配置文件数据结构，以跟踪主机的位置. 主机配置文件包含主机的MAC,IP和位置(即网络地址)，当主机首次与OF交换机连接时，控制器将收集该信息. 预防模块使用主机配置文件识别SDN中的攻击者. 控制器上的预防模块通过OpenFlow南向接口接收到报警包后，首先从报警包中提取〈IP，MAC〉对，用主机配置文件对其检测. 在主机配置文件结构中，IP地址只与一个MAC地址关联，而与接收数据包中的其余MAC地址不关联. 因此，利用此文件可以标识使用邻居IP地址执行RS攻击的主机，进而通过控制器发送转发规则来阻止恶意主机的攻击行为.

当攻击者同时执行IP和MAC欺骗时，提出的检测方法能够识别该攻击，但是无法判断攻击者在识别节点中的具体位置. 即，当MAC欺骗检测器发现2个具有相同序列号的帧且它们不相同时，检测器无法识别具体欺骗帧位置. 因此，本文提出的RS攻击检测方法在阻止攻击者流的同时，也阻止了良性用户流. 但是，本文方法只是在短时间内阻止检测到的恶意流，阻塞周期以最小值(5 ms)开始. 当控制器多次检测到同一流为恶意流时，该值将会递增. 阻塞期允许连接到该流的真正主机并在其端使用特定的对策，以避免将来的IP和MAC欺骗. 本文阻塞方法的结果是让良性主机以其最大容量工作，因为一旦恶意主机高速流量被阻塞，网络资源就可供良性主机使用. 图4给出了针对路由欺骗攻击提出的攻击检测和对抗技术流程示意图.

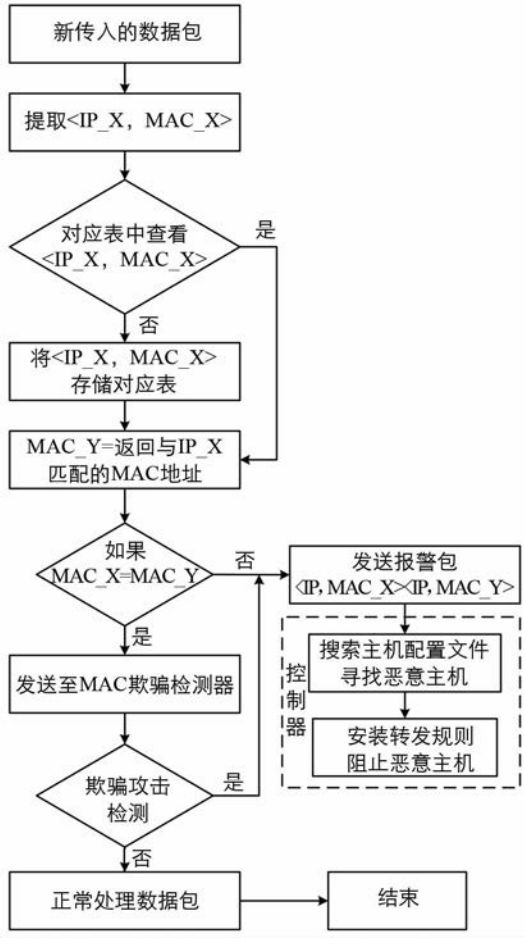

图4 路由欺骗攻击检测和对抗流程图

3 实验结果与分析

为了评价提出对策的效果，本文采用多个网络指标进行度量，通过拓扑结构研究路由欺骗攻击对各种SDN场景的影响以及解决策略的有效性. 采用Mininet模拟器、OpenDaylight网络控制器来模拟SDN中的目标场景，提出的方案在OF交换机内安装检测单元和防护单元. 所有实验均在配置为CPU Intel Core i7-4700MQ-2.4 GHz@6 GB RAM的机器上执行. 目标SDN拓扑网络由9个OF交换机，12个主机(其中8个良性和4个攻击者)和1个控制器组成. 在网络场景中随机选

择源-目标对. 链路带宽设置为 100 Mb，每个链路的延迟设置为 5 ms，模拟时间设置为 500 s.

在 RS 攻击场景中，采用 2 个单独的 Java 应用程序将源节点和目标节点配置为 UDP 客户端和服务器. 设置 4 个良性用户向各自的接收者发送流量，每个良性用户运行 UDP(User Datagram Protocol)客户端应用程序，每秒向良性接收器发送 5～30 个大小为 512 字节的数据包. 图 5－图 7 中 PPS(Packet Percent Second)表示每秒攻击速率. 为了执行攻击，使用 Hping 生成欺骗 IP 地址. 攻击者使用 Hping 工具以不同的速率发送大小为 1 000 字节的 UDP 包. 为了实现网络分布攻击效果，设定首个攻击者在第 40 s 后开始发送数据包，其余攻击者以 20 s 的间隔开始发送数据包. 在控制器不干预的情况下，欺骗数据包沿着良性发送者和接收者之间的现有路径移动.

本文使用分组成功投递率 ρ、平均端到端时延 Λ 和网络带宽消耗 β 指标来显示攻击的影响和解决策略的有效性.

图 5－图 7 显示了 RS 攻击(RS-A)和 RS 防御(RS-C)随攻击率增加对投递率 ρ、时延 Λ 和带宽消耗 β 的影响. 当恶意数据包的速率增加时，良性用户的 ρ 值降低，时延 Λ 和带宽消耗 β 增加. 这种现象的出现是因为恶意流量引起网络链接上拥塞以及 OF 交换机转发队列上拥塞造成的. 通过使用本文提出的对策，恶意用户可以有效地被检测和阻止. 而对于良性用户来说，ρ，Λ 和 β 变化不大.

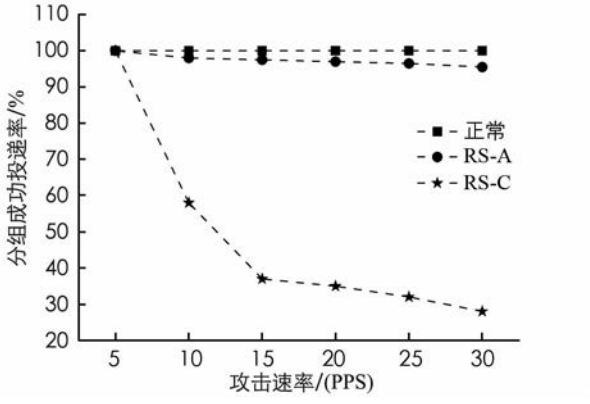

图 5　不同恶意包速率的分组成功投递率

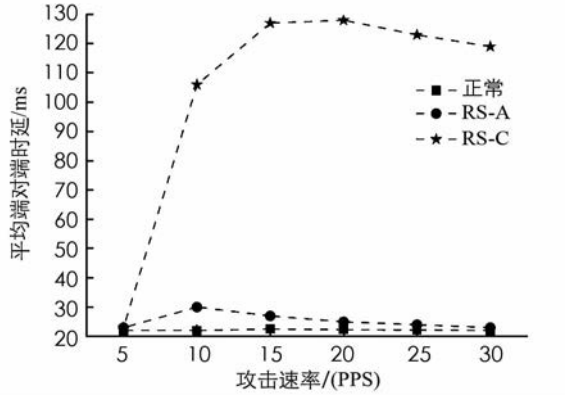

图 6　不同恶意包速率的平均端到端时延

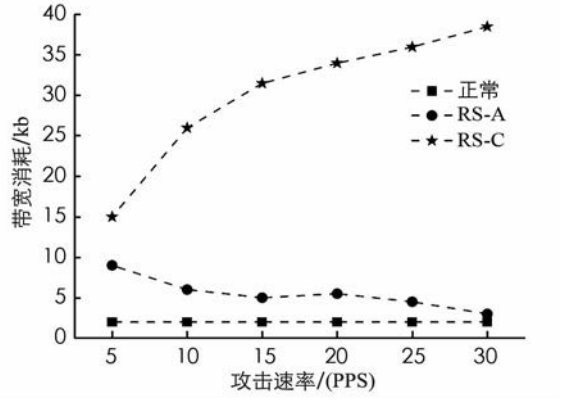

图 7　不同恶意包速率的带宽消耗

图 8 和图 9 给出了不同模拟时间下，不使用和使用本文提出方案时 β 的模拟结果. 实验结果有助于正确地实时调查 RS 的攻击行为和验证解决对策的有效性. 图 9 显示，使用本文解决策略后可以防止恶意数据包注入网络，从而降低网络带宽消耗 β.

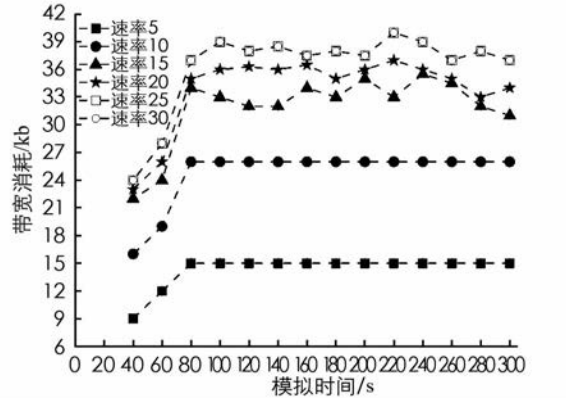

图 8　不使用本文方案时的带宽消耗

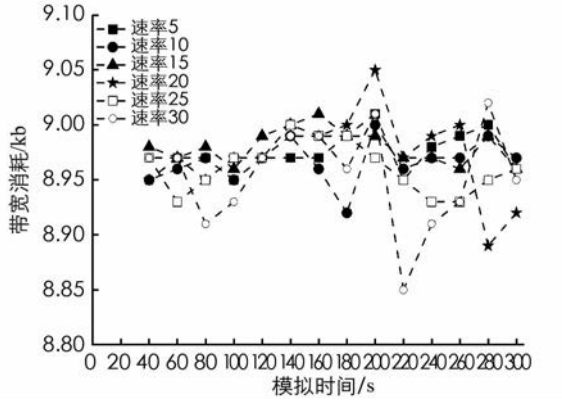

图 9　使用本文方案时的带宽消耗

4 结 语

针对当前方法对SDN中路由欺骗攻击检测不够的问题，本文提出了一种轻量级解决方案. 该方案利用安装在OF交换机上的选择性阻塞扩展模块来检测RS攻击. 当RS攻击出现时，交换机将产生报警包并发送给控制器，控制器根据报警包的信息确定恶意主机的位置，通过发送转发规则阻止攻击者恶意使用其他用户的活动通信路由. 仿真结果表明，本文提出的方案可以有效地检测和解决SDN中出现的路由欺骗攻击.

参考文献：

[1] LI Y, CAI Z P, XU H. LLMP: Exploiting LLDP for Latency Measurement in Software-Defined Data Center Networks [J]. Journal of Computer Science and Technology, 2018, 33(2): 277-285.

[2] 田俊峰，齐鎏岭. SDN中基于条件熵和GHSOM的DDoS攻击检测方法 [J]. 通信学报，2018，39(8)：140-149.

[3] CHEN C C, CHEN Y R, LU W C, et al. Detecting Amplification Attacks with Software Defined Networking [C]//2017 IEEE Conference on Dependable and Secure Computing. Taipei: IEEE, 2017.

[4] KALKAN K, GUR G, ALAGOZ F. Defense Mechanisms Against DDoS Attacks in SDN Environment [J]. IEEE Communications Magazine, 2017, 55(9): 175-179.

[5] AMBROSIN M, CONTI M, DE GASPARI F, et al. LineSwitch: Tackling Control Plane Saturation Attacks in Software-Defined Networking [J]. IEEE/ACM Transactions on Networking, 2017, 25(2): 1206-1219.

[6] MOHAMMADI R, JAVIDAN R, CONTI M. SLICOTS: an SDN-Based Lightweight Countermeasure for TCP SYN Flooding Attacks [J]. IEEE Transactions on Network and Service Management, 2017, 14(2): 487-497.

[7] LIU J, LAI Y X, ZHANG S X. FL-GUARD: a Detection and Defense System for DDoS Attack in SDN [C]//Proceedings of the 2017 International Conference on Cryptography, Security and Privacy-ICCSP 17. New York: ACM Press, 2017.

[8] ZHENG J, LI Q, GU G F, et al. Realtime DDoS Defense Using COTS SDN Switches via Adaptive Correlation Analysis [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(7): 1838-1853.

[9] WANG T, HONGCHANG CHEN D S S E A T R C. SGuard: a Lightweight SDN Safe-guard Architecture for DoS Attacks [J]. China Communications, 2017, 14(6): 113-125.

[10] 樊自甫，周凯恒，姚 杰. 基于博弈论的SDN主控制器重选机制 [J]. 计算机应用，2018，38(3)：776-779，865.

[11] ZHANG Q Y, WANG X W, HUANG M, et al. Software Defined Networking Meets Information Centric Networking: a Survey [J]. IEEE Access, 2018, 6: 39547-39563.

A Lightweight Solution to Defend SDN Routing Spoofing Attack

WANG Zhao[1], CHEN En-qing[2]

1. *Department of Public Studies, Henan Vocational College of Nursing, Anyang Henan 455000, China;*

2. *School of Information Engineering, Zhengzhou University, Zhengzhou 450052, China*

Abstract: Aiming at the problem that the detection accuracy of existing technology is not enough for some specific DDoS attacks, a lightweight solution to defend against route spoofing (RS) attacks in SDN is proposed. By analyzing the causes of route spoofing, the scheme designs a selective blocking extension module on the data plane OpenFlow switch. Once the detector discovers RS attacks, the switch sends the generated alarm packet to the controller, which prevents the attacker node from maliciously using the active communication path of other users by sending forward rules. The simulation results show that the proposed method can effectively detect DDoS attacks in SDN, and the relevant indicators fully show the feasibility and correctness of the solution.

Key words: software-defined networking; network security; DDoS attack; route spoofing

责任编辑 夏 娟