一种针对基于OpenFlow的SDN网络中控制层面的DoS攻击研究

楼恒越 窦 军
(西南交通大学信息科学与技术学院 成都 610031)

摘 要 针对OpenFlow协议报文交换机制里所有非数据报文均需要通过PACKET_IN报文上传控制器的弱点,提出一种不停查询未知转发地址从而造成SDN网络控制层面资源耗尽的新型DoS攻击方式,同时基于SDN网络可编程性提出检测攻击与降低网络时延的解决策略。首先通过SDN控制器北向应用接口,使用Defense4ALL应用中自定义功能,针对DoS攻击特性检测网络中恶意流量。然后利用控制器动态配置特性,实时更新交换机配置文件,改变网络转发策略,从而减轻攻击对整个网络造成的影响。实验仿真表明,在大规模高速攻击中,该方法的检测成功率接近100%,在攻击源较少的慢速攻击中检测成功率低于80%,整体网络延迟降低10ms以上。所提出的解决策略可以有效减少针对控制平面的DoS攻击对整个网络的干扰。

关键词 SDN,OpenFlow,网络安全,控制层面,DoS攻击
中图法分类号 TP393 **文献标识码** A

Research on DoS Attacks Against Control Level in OpenFlow-based SDN

LOU Heng-yue DOU Jun
(College of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)

Abstract Based on OpenFlow protocol message exchange mechanism, all non-data packets need uploading by PACKET_IN message. Thus, a new DoS attack on the control plane was proposed. It uses non-stop forwarding unknown address packages to deplete resources in control plane. And a solution strategy was proposed to detect attacks and reduce network latency based on the programmability of SDN network. First, through SDN controller north application interface, Defense4ALL application was used to detect malicious traffic by characteristic of DoS attacks. Then by using the controller feature of dynamical configuration, switch configuration file was updated in real-time, and network forwarding policy was changed. Thereby it could reduce the damage caused by the attack on the entire network. The simulation shows that the success rate of this detection method closes to 100%. But in slow-speed less-source attack detection success rate is less than 80%. The overall network latency is reduced by 10ms or more. The proposed solution strategy can effectively reduce the interference of the DoS attacks against control level for entire network.

Keywords SDN, OpenFlow, Network security, Control level, DoS attack

1 背景介绍

拒绝服务(Denial of Service,DoS)攻击是互联网安全中面临的主要挑战之一。DoS攻击机制主要是使用一些协议缺陷等漏洞造成计算机或服务器产生大量的超过自身承受能力的虚假网络连接,使得网络资源被大量占用,导致正常访问连接得不到处理。

对于现有网络,其承载功能不断扩展,网络中最初定义的"哑的、简单的"数据转发单元已经变得臃肿不堪。面对与日俱增的网络需求,亟需一种高效的网络模型来解决网络性能的瓶颈问题[1-3]。其分布式、自治管理的特性也造成很多安全问题无法被很好地发现与解决。为解决这些问题,众多研究机构和学者提出下一代网络(Next Generation Networks,NGN)的概念,如国外的FIND、GENI、NetSE、AKARI和国内的SOFIA、SUPA等[4,5]。自适应的未来网络不仅应满足可控、可管理、可扩展和可信任的要求,而且还应满足建设和管理成本最优的要求[6]。软件定义网络(Software Defined Networking,SDN)正是为解决这些问题而被提出的新一代网络体系结构。

SDN网络的提出解决了许多现有的网络问题,如控制平面与数据平面分离使得网络资源可以被更加合理地利用,其集中控制性可以改进源IP地址验证以及网络溯源等方面的解决方案[7]。然而,新的网络体系结构在提供了丰富的网络功能的同时,也带来了诸多的安全风险。控制器拥有网络绝对管理权,作为SDN新增的管理层级,它一旦失效就会使整个网络面临瘫痪,因此保证控制器安全至关重要[8]。

2 技术简介

开放网络基金会(Open Networking Foundation,ONF)提供的白皮书[9]中定义了SDN体系结构。ONF把SDN网络

楼恒越(1990—),男,硕士生,主要研究方向为网络安全、SDN,E-mail:279978277@qq.com;窦 军(1963—),男,博士,副教授,主要研究方向为计算机网络、下一代网络体系结构。

分为3个层面，分别为应用层、控制层和基础设施层（也称数据层）。基于软件的SDN控制器可以获取网络的全局视图，向上提供应用程序所需要调用的网络接口，这极大地简化了整个网络的设计与控制，同时也简化了网络设备本身，使其不再需要理解和处理成千上万的协议标准，而只需要接受SDN控制器的指令工作。这使得曾需要大量技术性人员配置与维护的网络可以很轻易地搭建与使用。

OpenFlow是由斯坦福大学于2008年提出的第一个基于SDN网络结构中控制层与数据层的通信接口标准[10]。OpenFlow使用一套预定义规则的流概念来识别当前网络状况，其规则可以被SDN控制器通过静态或动态编程改变，同时其允许上层应用程序通过参数的形式告知网络设备所需要的资源。由于OpenFlow允许以每个流为单位进行编程操作，这使得基于OpenFlow的SDN网络可以提供精准控制，允许网络对应用程序作出实时响应。

3 问题引入

SDN网络提供了丰富的网络功能，提高了网络使用效率。与此同时，SDN网络也面临着诸多的安全挑战，如恶意数据流、交换机流标篡改、应用软件漏洞、数据管理机密性与可用性威胁等传统网络中常见的攻击在SDN中依然可能发生；而且，基于SDN网络结构的特殊性，其控制平面若发生安全威胁，会导致整个网络出现安全问题，甚至崩溃。所以SDN网络中控制平面的安全问题是重中之重。

如前文所述，SDN控制器是整个SDN的心脏，Tootoonchian[11]、江国龙[12]等人均通过实验证实了SDN网络的整体性能大部分取决于网络中控制器性能的优劣，若其发生故障则会影响整个网络。Braga[13]给出了一种轻量级的DDoS（Distributed Denial of Service）攻击检测机制，通过利用SDN网络的流量统计功能，提取DDoS攻击的特征六元组，并利用神经网络中的自组织映射（Self-Organizing Map，SOM）方法进行相应判断从而识别出攻击流。然而该方案与Wang[14]方案一样，只提供了针对一般DDoS攻击的检测方法，从SDN网络的角度考虑也就是针对数据平面的攻击检测，若攻击者利用DoS攻击直接攻击SDN控制器，则会产生不同的影响。陶治[15]提到日本最大电信运营商NTT公司在2012年就使用SDN网络中的OpenFlow交换机搭配现有的流量清洗设备（IPS）进行针对数据中心的DDoS攻击防护，但同样只是针对传统的数据层的攻击，并没有考虑SDN网络中控制层面的安全性。Jose[16]、Yao[17]同样是基于SDN的可编程性，利用SDN网络之上的应用程序进行相关的网络安全防御。

SDN网络的控制器本身就面临着大量的安全威胁。Dover[18]提出并验证了一种由于OpenFlow协议中控制器与交换机连接过程缺陷导致的DoS攻击。文献假设攻击者已经完全控制了一台或多台处于数据层的OpenFlow交换机，并通过控制器北向API的不安全性获得其需要攻击的交换机相关信息，并利用python脚本生成攻击信息，伪装为攻击目标交换机与控制器建立连接，导致目标交换机失去与控制器的联系，最终导致控制器失去对所有交换机的控制权，造成整个网络遭受DoS攻击。

本文利用另一种协议漏洞，即协议转发机制漏洞，基于控制器在接收与转发相关控制报文时采用的特殊机制，造成网络遭受DoS攻击。这一方式不需要如文献[18]一样提前获取交换机的相关信息，也不需要控制交换机，在假定连接到交换机的用户终端可以被任何人使用的前提下（即使需要攻击者控制用户终端，其付出的代价也远远小于取得一台交换机的完全控制权），只需要运行一些脚本，就可以造成DoS攻击，相比之下更容易实现，使得针对SDN网络攻击的门槛大大降低。这一问题值得研究与探讨。

4 攻击原理及解决策略

4.1节给出实验所实施的攻击原理，其解决方案见4.2节。

4.1 攻击原理

在OpenFlow协议中，若一台主机想要与另一台主机通信，同样需要先知道对方主机的MAC地址（从主机的角度看，它认为它已经得到对方主机的MAC地址），但此时使用的ARP协议不会被直接转发，而是控制器利用OpenFlow协议中的OFP_PACKET_IN与OFP_PACKET_OUT报文进行查询。

在如图1所示的网络拓扑结构中，主机H1想要与主机H2建立一次通信，但并不知道其MAC，所以H1发起一次ARP请求，请求H2的MAC地址。通过抓包软件分析，可以得到首次在不知道对方MAC地址的情况下建立一次Ping过程的时序图（见图2）。

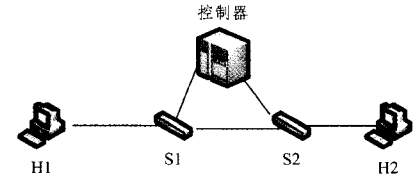


图1 简单的网络拓扑图

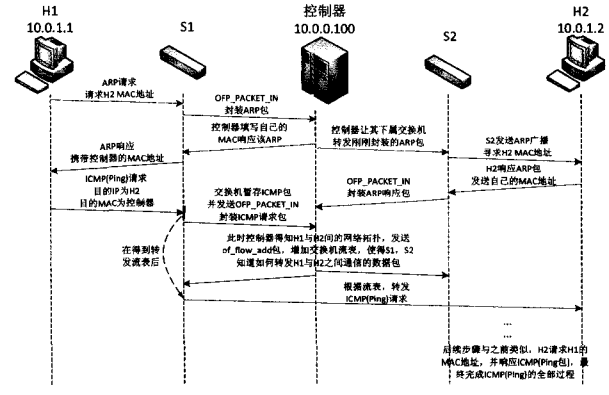


图2 基于OpenFlow的SDN网络中Ping的建立与响应过程时序图

由图2中可以看到，与传统的Ping过程不同，在基于OpenFlow的SDN网络中，控制器通常占据了查询过程中的主要地位，并参与了大量的计算与控制工作。这样可以避免ARP包的报文风暴，但也带来了一定的安全问题。攻击者可以伪造大量无效的ARP请求，使得控制器忙于应对，消耗大量计算资源；同时攻击者也可以发送大量ICMP（Ping）报文，以占用交换机的缓存空间，使得网络效率降低，最终导致网络

遭受 DoS 攻击。下文中所提到的攻击，均指利用该漏洞进行的 DoS 攻击。

4.2 解决策略

由于该攻击是由 OpenFlow 协议中的协议漏洞造成的，在不更改协议转发机制的情况下，只能考虑在控制端给出相应的解决方案。

1)利用北向 API，使用基于控制器软件的 SDN 应用。如在 OpenDayLight 控制器中，有 Defense4ALL 应用，该应用通过北向 API 与控制器进行通信，主要功能为监测网络中的流量，通过流量分析筛选并记录攻击流。

2)利用 SDN 网络中控制器可动态配置特性，实时对交换机进行参数配置，如转发率、转发策略等，在损失一定性能的前提下，保证整个网络的正常运行，在一定程度上保证网络的健壮性。

后文实验中，分别对两种方法进行了实验模拟。

5 实验结果及分析

本文实验中的攻击源均匀分散在每个子网络中。

5.1 实验环境

实验环境中部署了基于 OpenFlow 的交换机，采用开源的 OpenDayLight 软件作为控制器，并利用支持 OpenFlow 的 Mininet 2.2 平台进行网络仿真。整个网络架设在虚拟机中，控制器与 Mininet 平台均有四核 CPU 2.40GHz、2GB 内存，安装 Ubuntu 14.04 操作系统。

图 3 为实验所使用的网络拓扑图。在网络拓扑中，只有唯一一个控制器，控制器同时管理 10 个交换机，每个交换机都直接与控制器相连接，并且每个交换机挂载 5 个用户终端。

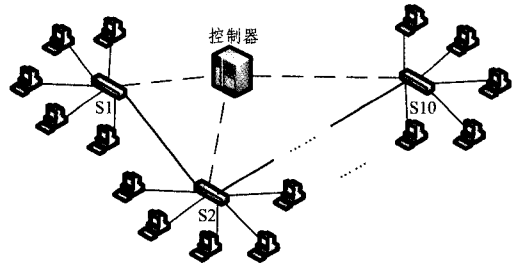
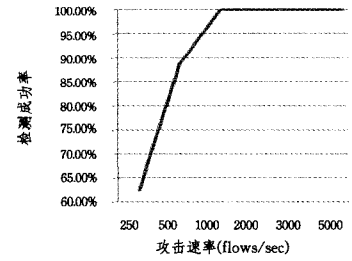


图 3 实验网络拓扑图

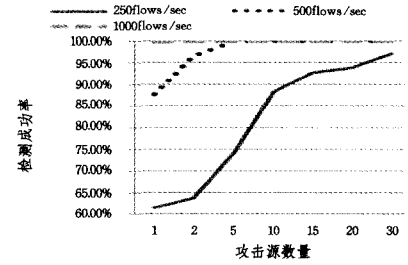
5.2 实验结果分析

利用 Defense4ALL 应用，在单点攻击的检测中作用明显，可以在很短的时间内检测到网络中的攻击，并在报告中记录且报告相应的详细信息。但在分散的攻击源发动慢速攻击时，检测成功几率降低，甚至经常无法检测到网络中的攻击。该软件只能检测攻击流，需要手工操作去禁止攻击行为，增加了防范时间与难度。

图 4(a)中，当攻击速率超过 1000 flows/sec 后，其检测成功率接近 100%。由于通过性能测试软件测得实验平台中交换机的转发效率大约为 3000 flows/sec，因此当攻击者的攻击速率达到 3000 flows/sec 后，增加攻击速率，其对应实验结果与该点差异不大。图 4(b)中，其攻击源均匀分散在网络中，并以不同的攻击速率进行测试，当少于 10 个的攻击源以 250 flows/sec 速率进行攻击时，检测软件经常无法正确识别出攻击，导致检测成功率低于 80%。当攻击源数量增加后，网络中攻击报文增加，检测成功率大大提升。



(a)单一攻击源检测



(b)多攻击源检测

图 4 Defense4ALL 应用检测成功率

利用控制器进行动态配置，可以实时调整路由器的性能配置，使得攻击源所处的网络交换性能降低，从而降低攻击对整个网络造成的影响。该方法虽然可以有效地保证整个网络的健壮性，但并不能从根本上解决网络的攻击威胁，若用户处于与攻击者相同的网络区域，则其所使用的网络性能会受到很大影响；并且该方法只是减缓了攻击造成的影响，同样需要配合其他相应手段，才能最终解决安全问题。

图 5 中，网络的转发性能由 Ping 延迟体现，所有延迟均为所指网络中的平均延迟；攻击源所在网络延迟指与攻击源的终端连接在同一个交换机下的其他终端与该网络外其他节点测试得到的网络延迟，该延迟均为控制器作出动态配置后的网络状态表现；攻击源均匀分布在网络中，攻击速率均为 1500 flows/sec。在攻击源数量少于 20 时，该方法可以很好地保证攻击源以外的网络处于很好的传输状态中，网络平均时延降低 10ms 以上。但当攻击源数量超过 20 后，由于网络整体延迟过高，该方法受到交换机制约，并不能很好地保证网络的传输质量。

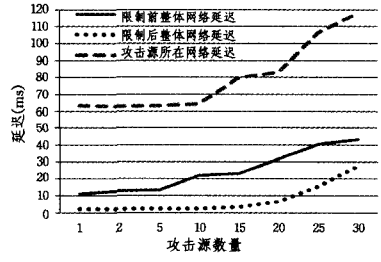


图 5 基于动态配置策略的网络性能对比

结束语 本文着重对基于 OpenFlow 的 SDN 网络中，控制层受到基于 OpenFlow 中控制报文的转发机制漏洞导致的 DoS 攻击及相应的解决策略方面做了初步的探讨，通过实验证实了 SDN 网络中控制器极易受到安全威胁，在一些解决策略下可以减缓攻击造成的影响。但还有许多相关问题没有深入研究，诸如流表策略、控制器安全备份、流量识别与监测等。随着 SDN 的发展，会涌现越来越多的问题，希望能在今后有更多更深入的研究。

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] 左青云，陈鸣，赵广松，等. 基于 OpenFlow 的 SDN 技术研究[J]. 软件学报，2013，24(5)：1078-1097

[3] 李丹，陈贵海，任丰原，等. 数据中心网络的研究进展与趋势[J]. 计算机学报，2014，37(2)：259-274

[4] 窦军，陈文佳. SUPANET 基 OAM 的保护交换研究[J]. 计算机科学，2011，38(4)：87-92

[5] 窦军. 单层用户数据交换平台体系结构研究[D]. 成都：西南交通大学，2011

[6] 林闯，贾子骁，孟坤. 自适应的未来网络体系架构 [J]. 计算机学报，2012，35(6)：1077-1093

[7] 戴彬，王航远，徐冠，等. SDN 安全探讨：机遇与威胁并存[J]. 计算机应用研究，2014，31(8)：2254-2262

[8] 薛聪，马存庆，刘宗斌，等. 一种安全 SDN 控制器架构设计[J]. 信息网络安全，2014(9)：34-38

[9] ONF Market Education Committee. Software-Defined Networking: The new norm for networks[EB/OL]. (2012-04-13). https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

[10] 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

[11] Tootoonchian A, Gorbunov S, Ganjali Y, et al. On controller performance in software-defined networks[C]// USENIX Workshop on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services (Hot-ICE). 2012: 10

[12] 江国龙，付斌章，陈明宇，等. SDN 控制器的调研和量化分析[J]. 计算机科学与探索，2014，8(6)：653-664

[13] Braga R, Mota E, Passito A. Lightweight DDoS flooding attack detection using NOX/OpenFlow[C]// 2010 IEEE 35th Conference on Local Computer Networks (LCN). IEEE, 2010: 408-415

[14] Wang B, Zheng Y, Lou W, et al. DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking[C]// 2014 IEEE 22nd International Conference on Network Protocols (ICNP). IEEE, 2014: 624-629

[15] 陶冶，张尼，张云勇，等. SDN 安全防护技术研究[J]. 电信技术，2014(6)：14-17

[16] Jose L, Yu M, Rexford J. Online measurement of large traffic aggregates on commodity switches[C]// Proc. of the USENIX HotICE workshop. 2011: 13-13

[17] Yao G, Bi J, Xiao P. Source address validation solution with OpenFlow/NOX architecture[C]// 2011 19th IEEE International Conference on Network Protocols (ICNP). IEEE, 2011: 7-12

[18] Dover J M. A denial of service attack against the Open Floodlight SDN controller[EB/OL]. [2013-12-30]. http://dovernetworks.com/wp-content/uploads/2013/12/OpenFloodlight-12302013.pdf

(上接第 328 页)

3. if 执行 LinkSearch()过程成功 then do;
4. 成功返回；
5. else if 执行 LinkBuild()过程成功；
6. 成功返回；
7. end if
8. else do
9. if 执行 NodeSearch()过程成功 then do;
10. 成功返回；
11. else do
12. 执行 StandbyNodeSort()过程，得到排序的节点集 V；
13. if 节点集 V 为空集 then do
14. 失败退出；
15. else do
16. 按序从 V 中取节点 v_k；
17. if 执行 PathSolve()过程成功 then do
18. 成功返回；
19. end if
20. end if
21. end if
22. 失败退出

结束语 对本文提出的拟态网络拓扑等效变换方法总结如下：1)通过多次对网络局部子网的拓扑等效变换达到整体网络拓扑变换的效果，由于拓扑变换的目标是网络中的子网，而非整个网络，因此可以减小拓扑变换的网络规模，降低网络拓扑变换的难度；2)基于本文提供的子网描述方法，可以对网络中的任意部分进行抽象描述，可以是一条链路、一个节点或一个连通子网，甚至是整个网络，从而可以增加网络拓扑变换的灵活性。

本文提出的拟态网络拓扑变换方法只是一些基础性工作，在此基础上还可以开展更多的工作，如：1)细化资源判定条件，为算法选择提供理论依据；2)丰富算法类型，为同等条件下生成异构子网提供更多方法。

参 考 文 献

[1] Unruh I, Bardas A G, Zhuang Rui, et al. Compiling abstract specifications into concrete systems-bringing order to the cloud [C]// Proceedings of the 28th Large Installation System Administration Conference (LISA14). Seattle, WA, 2014: 17-33

[2] Deloach S, Ou Xin-ming, Zhuang Rui, et al. Model-driven, moving-target defense for enterprise network security[J]. Lecture Notes in Computer Science, 2014, 8378: 137-161

[3] 林闯，贾子骁，孟坤. 自适应的未来网络体系架构[J]. 计算机学报，2012，35(6)：1077-1093

[4] 王淑玲，李济汉，张云勇，等. SDN 架构及安全性研究[J]. 电信科学，2013，3：117-122

[5] 刘强，汪斌强，徐恪. 基于构件的层次化可重构网络构建及重构方法[J]. 计算机学报，2010，33(9)：1557-1568

[6] 王会勇，赵海良，杨晓伟. 基于拓扑变换的一种不确定性推理方法[J]. 重庆交通学院学报(自然科学版)，2004，23(1)：112-115

[7] 刘军，于耕，张慧鹏. 基于节点控制的空间信息网拓扑重构算法[J]. 电子学报，2011，39(8)：1837-1844

[8] 齐宁，汪斌强，郭佳. 逻辑承载网构建方法的研究[J]. 计算机学报，2010，33(9)：112-119

[9] 李黎，郑庆华，管晓宏. 基于有限资源提升网络可生存性的拓扑重构方法[J]. 物理学报，2014，63(17)：170-201

[10] 王志明，汪斌强. 基于备份的可重构服务承载网可靠性映射方法[J]. 电子与信息学报，2013，35(1)：126-132

[11] 李稳国，邓曙光，杨冰，等. 相互依存网络间的拓扑构建方法[J]. 计算机工程与应用，2014，50(11)：85-89

[12] 吕书明，张明磊，孙树立. 基于简化和细分技术的三角形网络拓扑优化方法[J]. 计算机辅助设计与图形学报，2014，26(8)：156-162

[13] 王子厚，韩言妮，林涛，等. 可重构网络中基于中心度与拓扑势排序的资源分配算法[J]. 通信学报，2012，33(8)：10-20