外 文 译 文

软件定义网络中的安全：威胁和对策

摘要：近年来，软件定义网络（SDN）一直是研究的重点。作为一个新型的网络架构，SDN 可能会取代传统的网络，因为它在简单性，可编程性和弹性方面为网络管理带来了便利。尽管目前正在做许多努力来标准化这种新兴的架构，但在这个早期设计阶段也需要认真注意安全问题。本文重点介绍 SDN 的安全性。我们首先讨论 SDN 的特点和标准。在此基础上，我们将安全特性作为一个整体进行讨论，然后基于 SDN 架构的三个部分，即数据转发层，控制层和应用层，从三个方面详细介绍了威胁和对策。还描述了可用于预防，减轻或恢复某些此类攻击的对策技术，同时突出了开发这些防御机制时所遇到的挑战。

1 介绍

随着云时代的发展，云服务提供商对于不同的用户需要满足各种网络服务需求(如带宽、服务质量、安全或可靠性)，这要求网络体系结构具有较高的弹性和灵活性，而网络资源可以通过网络虚拟化功能灵活地分配。然而，在传统的网络体系结构中，常用的封闭的网络设备(如路由器或交换机)，具有以下缺点：a)软件和硬件紧密耦合；b)集成到设备的网络协议过于复杂；c)几乎所有设备都是制造商专有的，改变设备的功能或者更新设备十分困难。并且随着网络规模的不断增加，上述特征使传统的网络越来越复杂，导致云服务提供商不能有效地自定义和优化网络资源，无法实现特定的用户需求。

软件定义网络(SDN)是一种革命性的网络体系结构，可目前被视为网络功能虚拟化的最佳实践。其基本思想是将复杂的控制逻辑从所有网络节点中剥离出来，并形成一个逻辑控制中心来指导包的转发；这种改变将实现在不改变现有网络拓扑结构的情况下，通过软件编程来控制所有网络流量的目标。作为最有前途的技术之一，SDN 相对传统网络架构有无可比拟的优势：a)转发和控制允许应用程序创新和设备升级相互独立，这将加快新的网络应用程序的开发和部署；b)SDN 简化了网络管理模型，它使得网络运营商管理方便；c)集中控制逻辑有一个全局的网络，可以为运营商优化网络设施或改善网络性能提供足够的信息。因此，SDN 弥补了传统网络的缺陷，能够更有效地满足云环境中的多租户网络需求。

目前，OpenFlow 是 SDN 实际的标准，这是由斯坦福大学的研究小组 Cleanslate 提出。学术界和行业对 OpenFlow 的广泛接受使这种 SDN 标准非常成功。在行业中，许多商业化的 SDN 网络被部署，如微软的数据中心网络和谷歌的骨干网。更重要的是，很多使用 SDN 的网络虚拟化软件已经大大发展，诸如 VMWare NSX 等车型的底盘和 Nuage 网络的垂直地震剖面。SIGCOMM 在学术界，建立了一个特殊的国际会议，名叫 hotSD，

自 2012 年 8 月，要求会议的论文报告 SDN 的最新研究成果。此外，许多著名的大学，比如斯坦福大学和普林斯顿大学，也如雨后春笋般涌现 OpenFlow/SDN 相关研究项目，其中包括控制器设计，转发性能、路由决策的优化，网络虚拟化应用程序，可编程的无线网络，数据中心网络的节能，等等。

除了上面提到的研究点，还有一个研究方向，没有吸引了很多注意力，就是 SDN 的安全。如果不能确保 SDN 的安全性，它们的开发将在替换传统网络架构的过程中遇到很多阻力，甚至变得完全不相关。在过去的几年中，为了解决安全威胁，成立了 SDN 相关工作组织，学习相应的安全挑战和解决方案。同时，对 SDN 安全威胁提出了一些解决方案，其中包括控制器复制方案，身份验证和授权机制，针对拒绝服务或分布式拒绝服务(DoS/DDoS)攻击来保护控制器，流量监测和分析，流表槽溢出攻击保护等。

在本文中，我们从安全角度分析 SDN，目的是为了揭示新的安全功能以及伴随这个新体系结构而带来的新的安全威胁。此外，我们还调查了防范这些威胁的对策，从而加强了 SDN 的安全性。本文的主要工作包括：a)从整体架构的安全问题视角比较 SDN 方面与传统网络的优缺点。b)从不同的功能层和攻击类型的角度对 SDN 的安全威胁进行详细的剖析，并指出可能的情况安全对策。

文章其余的内容是按照以下的方式组织的：第二节对 SDN 体系结构的进行了概述；第三节分析 SDN 的安全问题；第四节讨论 SDN 安全威胁相应的对策；第五节对论文进行了总结，并指出了今后的研究方向。

2 SDN 体系结构概述

SDN 将数据转发控制逻辑，是一种新兴的网络体系结构。目前，在传统的网络中，设备紧密集成，例如交换机和路由器。数据转发和控制逻辑的分离使得网络控制和应用可编程。通常，SDN 体系结构可以划分为三个层，分别称为数据转发层、控制层和应用层。

2.1 数据转发层

数据转发层由许多 SDN 交换机组成，它们通过有线或无线媒体进行物理连接。每个交换机都是一个负责转发网络数据包的简单设备，并有一个转发表，名为流表，它包含数千条用于制定转发决策的规则。流表中的每个规则项由三个字段组成：操作、计数器和模式。模式字段定义了流模式，它基本上是包的头字段值的集合。当接收到数据包时，交换器将搜索它的流表来查找与字段匹配的规则。一旦交换器找到了这样的规则，规则的计数器就会增加，相应的规则就会被执行。否则，该交换机将通知控制器请求帮助，或者干脆丢弃数据包。值得注意的是，转发规则项不是由交换机节点本身生成的，而是由控制器从控制层向下推送的。

2.2 控制层

作为 SDN 的大脑，控制层管理和控制整个网络。我们指的是作为 SDN 控制器实现这些功能的网络节点，它通常作为单独的物理设备部署到特定的软件中。SDN 控制器与南行开关通过一个标准的 API，如 OpenFlow，在数据转发层有整个网络拓扑结构的全局视图，即交换机和链路。各种路由协议，如边界网关协议 BGP 和 OSPF，SDN 控制器上

运行，这样发生在数据层所有的数据转发是基于控制器的指令。

作为 SDN 的实际标准，OpenFlow 最初设计是为简单的单一控制器，这构成了一个潜在的单点故障。然而，几乎最近所有的 SDN 架构实现，比如 Floodlight，NOX 和 OpenDaylight，支持多个分布式控制器，提高了网络资源的可伸缩性和可用性。在多控制器的 SDN 架构中，每个单独的控制器只负责控制交换机的一部分。为了保持网络的状态和工作的一致性协作，每个 SDN 控制器能通过东西向接口的 api 与网络中其他控制器通信，在有关论文中有所讨论。

2.3 应用层

应用层允许网络操作员快速响应各种业务需求。在 SDN 控制器上开发各种功能的应用软件，以便满足各种应用需求，如网络虚拟化，拓扑发现，交通监控，安全增强，负载平衡等等。应用程序层通过北方的 API 与控制层进行通信，比如 REST API。控制层给应用程序层提供了一个网络物理资源的抽象视图，这意味着网络运营商可以改变数据包的数据路径只使用软件编程集中在 SDN 控制器，而不是配置所有的物理交换机的数据路径。

3 SDN 架构安全分析

现在，我们将研究 SDN 架构的特点对安全性的影响。与传统网络架构相比，SDN 的安全威胁将更加集中，与传统网络中网络元素的分散性相反。因此，由于其架构的特点，SDN 具有安全优势和安全缺陷。 其优点包括：

a）有效监测异常流量。由于 SDN 控制器可以同时感知整个网络流量，因此更容易注意到攻击者造成的网络流量异常行为。

b）及时处理漏洞。另一个重要的优点可归因于可编程网络环境的性质。一旦有了新的威胁检测到，运营商可以对新软件进行编程，以立即分析和处理该漏洞，而无需等待更新生产商专有设备中集成的操作系统或应用软件。此外，SDN 控制器可以实现覆盖开放系统互连（OSI）架构的 2-7 层的安全策略配置，并提供更加精细的安全控制。

另一方面，SDN 的自然安全缺陷包括：

a）控制器易受攻击。大多数功能，如网络信息收集，网络配置和路由计算，都集中在 SDN 控制器中。SDN 的体系结构提供了更集中的目标，大大降低了这种攻击的难度。同时，云计算的发展为攻击者提供了非常大的计算能力；在云计算平台的支持下，攻击者可以轻松实施攻击。如果攻击者成功抢占 SDN 的控制器，可能导致网络服务大量瘫痪，影响到控制器覆盖的整个网络。

b）开放可编程接口引起的风险。由于其开放性，SDN 更容易遭受安全威胁。 首先，它使得 SDN 控制器的软件漏洞充分暴露给攻击者，使得后者将有足够的信息来制定攻击策略。第二，SDN 控制器为应用层提供了大量的可编程接口，这种开放程度可能会导致滥用接口，如嵌入恶意代码（如病毒）。因此，SDN 控制器的开放接口需要仔细评估和审查。

c）更多的攻击点。由于 SDN 被分为三层，每层的实体可以分布在网络的不同位置；

这些实体之间的通信将是必要和频繁的。因此，与传统网络相比，SDN 为攻击者提供了更多可能的攻击点。我们指出了 SDN 架构中的六个可能的攻击点，将按照以下的顺序描述它们。

SDN 交换机。SDN 交换机通常是由相关硬件和软件组成的单独设备，易受攻击。一个很明显的漏洞是流表的大小限制。

SDN 交换机之间的链路。在 SDN 交换机之间传输的几乎数据包不被加密，并且可能包含用户的敏感信息。这些数据包可以容易地被攻击者拦截，特别是当交换机之间的链路是无线介质时。

SDN 控制器。如前所述，控制器是攻击者最有吸引力的目标 由于可编程性的开放性和功能的复杂性，控制器的软件不可避免地是易受攻击的，因此可以用于恶意攻击。

控制器和交换机之间的链路。所有转发规则都由控制器插入交换机。攻击者可以通过窃听控制器和交换机之间的链路来篡改包含这些规则的数据包，这将导致虚假规则插入或恶意规则修改。一旦交换机中安装了欺诈规则，数据包将不会被正确转发。

控制器之间的链路。在多控制器环境中，不同控制器之间的通信对于保持整个网络的一致状态是必要的。可以拦截控制器之间的链路中的数据包，这可能为攻击者提供可能的线索来威胁控制器。

应用软件。应用软件直接构建在控制器上，通常与控制器位于同一物理设备上。当应用软件通过北面的 API 调用控制器的功能的时候，恶意代码可能嵌入到控制器中。因此，应用程序软件被认为是控制器最方便的攻击点。

4 SDN 的安全威胁和相应的对策

随着 SDN 研究的深入，SDN 的安全问题越来越受到制造商和运营商的关注。 在本节中，我们将详细说明主要的安全威胁和对策呈现。根据上述 SDN 架构和相关安全分析，我们将威胁和相应的对策分为三类，分别是 SDN 架构中三层中包含相应的攻击目标，即转发层，控制层和应用层。

4.1 数据转发层的威胁和对策

数据转发层位于 SDN 架构的底部，并包含数千个互相互连的交换机。这些交换机负责转发数据包。如果交换机受到威胁，流经它的数据包将不会正确转发。另外，交换机是最终用户的网络访问的直接入口点，攻击者可以通过简单地将链路附加到交换机的端口来攻击交换机。因此，识别安全威胁和找到SDN交换机的相应对策是非常重要的。我们考虑到符合 OpenFlow 规范的 SDN 交换机的架构和工作原理。OpenFlow 开关通常包含三个功能模块，即 OpenFlow 客户端，流表和流缓冲区。当交换机从输入端口接收到一个数据包时，它将把这个数据包放在流缓冲器中，搜索流表，尝试找到一个匹配该数据包的消息字段的规则，如 MAC/IP 地址和 TCP/UDP 端口如果找到适当的规则，则该数据包将从流缓冲区中删除并转发到输出端口。否则，交换机将通过 OpenFlow 客户端发送 Packet_In 消息给控制器以请求指令。收到新消息后，控制器将进行路由计算并将新规则插入到流表中。根据上述过程，我们可以确定三个主要的安全威胁；它们是交

换机和控制器之间的中间人攻击，其目标是篡改规则，DoS 攻击溢出流表，以及 DoS 攻击以溢出流缓冲区。

4.1.1 交换机与控制器之间的中间人攻击

1. 威胁描述

中间人攻击是一种经典的网络入侵方法，其主要原理是在源节点和目的节点之间插入一个代理节点，并且用于拦截通信数据并篡改它们而不被通信侧检测到。中间人攻击的具体攻击方法包括会话劫持，DNS 欺骗，端口镜像等。控制器和开关之间的中间人发生攻击是理想的选择攻击 SDN，因为它可以用于拦截和篡改发送给交换机的转发规则，以获得网络数据包转发的控制权。攻击者可以进一步攻击，如黑洞攻击。另外，我们知道控制器和开关可能不是物理上直接连接的，即从交换机到控制器的分组可以通过多个其他交换机。因此，直接在通信路径上连接到它们的所有交换机和主机容易被转换为代理节点，在他们的中间人攻击中。

2. 对策

为了防范中间人的袭击，在学术界和业界都做了大量的研究工作。最明显的做法是在控制器和交换机之间创建一个安全通道。在 OpenFlow 规范 v1.0 中，传输层安全（TLS）被用来保护控制器开关通讯。但是，TLS 的配置非常复杂，许多供应商在 OpenFlow 交换机中不支持 TLS。因此，更高版本的 OpenFlow 规范声明 TLS 的配置是可选的。而且，TLS 不能提供任何 TCP 级别的保护意味着网络易受 TCP 级攻击。由于 TLS 不被执行，我们在这种情况下的主要安全挑战是区分正常和伪造流规则，并在造成不良影响之前消除伪造规则。已经提出了一些替代的对策来应对这一威胁。FlowChecker 是能够识别内部配置的配置验证工具有效切换开关错误。具体来说，它首先创建所有互连交换机的模型，然后通过二进制决策图对所有交换机配置执行端到端的快速分析和验证和模式 1 检查技术，由此可以检测到错误配置。作为 NOX 控制器的软件扩展模块，FortNOX 提供基于角色的授权和身份验证安全增强策略。通过其新颖的分析算法，可以检测各种转发的冲突规则。该算法具有良好的鲁棒性，即使在恶意应用攻击的情况下也能正确地执行其功能。同时，在申请之前修改转发规则，FortNOX 将通过数字签名或安全约束验证修改的合法性.VeriFlow 作为中间控制器与交换机之间的层次，主要负责整个网络范围内网络变量的动态验证，特别是当插入新的转发规则时。基于 Mininet 的 OpenFlow 仿真环境进行了实验，结果显示通过跟踪路由数据，VeriFlow 可以在几百毫秒内完成新的转发规则的检测，这是非常有效的。

由于控制器连接对于交换机的正确操作非常重要，冗余链路或快速链路恢复机制是有帮助的减轻控制器和交换机之间的中间人攻击的影响。OpenFlow 协议本身具有连接稳定性测试机制，由此每个交换机周期性地向控制器发送保存消息的活动。如果主控制器无法响应，则可以自动指示切换到连接到备份控制器。控制器复制类似于中提出的机制，也就是说，如果交换机在一段时间内没有收到控制器的响应，交换机会认为控制器发生故障，并迅速建立与另一个控制器的连接，允许网络连续工作。

4.1.2 DoS 攻击使流表和流缓冲区饱和

1. 威胁描述

OpenFlow 的反应规则设计使交换机容易受到拒绝服务（DoS）攻击。由于目的地址不明的报文导致在交换机中插入新规则，攻击者可以在短时间内生成大量未知网络主机的数据包，从而快速填写交换机的有限流表存储容量。当流量表被不规则流量饱和时，合法流量将不会被正确转发，因为没有更多可用的插入新规则的能力。除流表外，DoS 攻击的另一个目标是流缓冲区。如上所述，在数据包被转出之前，它们被缓冲在流中缓冲区等待规则搜索或插入新规则的结果。流缓冲区中的数据包将被标记为先进先出（FIFO）中的删除释放存储空间的基础。如流程表的情况，流缓冲器的存储容量也受到限制。攻击者可以正常洪泛流量大于交换机遇到的流量；交换机必须缓冲这些大数据包，这会导致流量缓冲区的饱和。当收到合法数据包时，流缓冲区将没有足够的空间存储这些包，这些新数据包将被丢弃。

2. 对策

我们将讨论一些可以减轻这种攻击的相关对策的例子。FlowVisor 可以使网络运营商区分网络数据包根据报文的报头字段.FlowVisor 作为交换机和控制器之间的代理；它接受来自控制器和重写的规则因此，所产生的规则仅影响给定控制器被允许控制的网络部分。例如，控制器可以被分配到组织的 web 服务器和从组织的 web 服务器组成的所有流量的网段。然后，该控制器可以创建一个规则来删除所有 UDP 流量 DoS 攻击。当 FlowVisor 收到此规则时，它将重写它以将所有 UDP 流量从 Web 服务器中删除，从而使网络的其余部分不受影响。

虚拟源地址验证边缘（VAVE）是具有 OpenFlow/NOX 架构的抢占式保护方案，旨在减轻通过 IP 欺骗引起的 DoS 攻击。新的数据包不符合任何规则流表将被发送到控制器进行源地址验证，在此期间可以检测到 IP 欺骗，在这种情况下，控制器将创建一个规则 FlowTable 可以停止源地址的具体流程.此外，VAVE 中的地址验证非常灵活，而与其他相关工作相比，数据包流程开销和所需资源大大减少。R.Baraga 等人 提出了一种针对 DDoS 攻击的轻量级防御方法，其基于流量特性。该方法在攻击检测分析中表现出良好的性能。

入侵检测系统的使用可以帮助您识别由 DoS 攻击引起的异常流量。这样的系统可以与用于动态访问控制开关的行为的相关机制相结合,例如控制层请求的速率限制。共振是可以加强控制器动态访问控制策略的系统。该系统基于实时警报和数据包流级别信息，直接向 SDN 架构中的转发数据层发布动态安全策略。

4.2 控制层的威胁和对策

在 SDN 架构中，控制层，即 OpenFlow 控制器及其安全性对数据转发层有着直接的影响。如果控制器受到威胁，整个网络（包括潜在的大量交换机）可能会受到影响。这是因为如果交换机无法从控制器接收到转发规则，则不知道如何转发数据包。因此，由于其重要作用，控制器可能成为攻击者的主要目标。控制层的主要安全威胁和对策如下所述。

4.3 应用层的威胁和对策

在应用层，攻击者可以篡改网络配置，窃取网络信息，抢占网络资源等，通过插入间谍软件或恶意软件计算机程序到应用程序。以这种方式，它们可能会干扰控制层的正常运行，并影响网络的可靠性和可用性。

虽然 OpenFlow 可以为安全应用程序部署安全检测算法，但这些安全应用程序不是强制性的。使用不同编程语言的不同独立组织开发的各种应用程序可能会产生互操作性不一致或安全策略冲突。下面描述应用层的一些安全威胁和对策。

4.4 安全问题总结

为方便起见，在表 4-1 中概述了 SDN 网络所面临的安全威胁，以及本节讨论的可能的对策。

表 4-1 SDN 架构中的安全威胁和典型对策

威胁层次	威胁类型	产生原因	典型的对策
数据转发层	控制器和交换机之间的中间人攻击	没有 TLS 支持的信道安全通信	FlowChecker ForNOX VenFlow
	Dos 攻击使流表和流缓冲区饱和	流表和流缓冲区有限的存储容量	Controller-replication FlowVisor
		短时间内大量的数据包	VAVE Resourance
控制层	Dos/DDos 攻击	难以区分混合的恶意流量和正常流量 控制器的计算和存储资源有限	FloodGuard DDos-Blocking CONA
	基于分布式多控制器的威胁	分布式的协同访问控制 多个控制器配置不一致	DISCO HyperFlow McNettle
	应用威胁	开放的编程接口 恶意应用	SE-Floodlight FRESCO

应用层	非法访问 安全规则和配置冲突	缺乏认证机制 控制器的软件漏洞 应用程序的多样性 应用策略的冲突	PermOF NICE VeriCon Flover Anteater NetPlumber

5 结论

在本文中，我们简要回顾了 SDN 的特点和架构。我们解释了 SDN 的功能和从安全的角度分析 SDN 所面临的问题和对策，基于 SDN 的独特性和开放性分析了其安全特性。然后，我们讨论了 SDN 安全的现状，从三个方面分析了 SDN 的安全问题：数据转发层，控制层和应用层。还介绍了一些预防和缓解技术来解决其中一些安全问题。未来，基于云计算的网络虚拟化和中间件将被视为 SDN 的重要应用，也将带来额外的安全威胁。因此，这些应用程序的安全性问题预计将引起越来越多的关注。