doi 10.3969/j.issn.1671-1122.2014.09.008

一种安全 SDN 控制器架构设计

薛聪[1,2,3]，马存庆[1,2]，刘宗斌[1,2]，章庆隆[1,2,3]
（1. 中国科学院信息工程研究所，北京 100093 ；2. 信息安全国家重点实验室，北京 100093 ；
3. 中国科学院大学，北京 100049）

摘 要 ：控制器是软件定义网络（SDN）的核心，其安全对 SDN 至关重要。基于开源的 SDN 控制器基础架构，文章分析并总结了控制器在不同管理模式下网络信息保护、应用程序管理、模块处理流程中存在的安全问题。针对这些安全问题，文章提出了一种安全 SDN 控制器架构，通过加入共享网络信息库、冲突检测、入侵容忍模块等多种安全功能，解决控制器单点失效、控制逻辑不一致等问题，可以提高 SDN 的安全性。

关键词 ：SDN ；控制器安全 ；安全性分析 ；架构设计
中图分类号 ：TP309 文献标识码 ：A 文章编号 ：1671-1122（2014）09-0034-05

Design of Secure SDN Controller Architecture

XUE Cong[1,2,3], MA Cun-qing[1,2], LIU Zong-bin[1,2], ZHANG Qing-long[1,2,3]
(1.*Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;* 2. *State Key Laboratory of Information Security, Beijing* 100093*, China;* 3. *University of Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: Controller is the core of Software Defined Network, and its security is crucial for SDN maintenance. Based on open source SDN controller architectures, we analyze its security issues of network information protection, application management and module processing under different control patterns, and further propose a secure SDN controller architecture, which integrates shared network information base, collision detection, intrusion tolerance module etc. This design can solve single controller invalidation and logic inconsistency and improve the robustness of SDN.

Key words: SDN; controller security; security analysis; architecture design

0 引言

传统网络发展至今，网络设备承载的功能不断扩展，耦合越来越多的控制逻辑，已难以满足云计算、大数据、虚拟化及相关业务发展对数据传输处理高速处理、资源灵活管理、新型协议快速部署的需求。软件定义网络（Software Defined Network，SDN）提出将路由器、交换机等网络设备中的控制平面和数据转发平面的分离，通过控制层集中控制，实现网络的可编程性，提供开放的网络接口，进而支持网络资源更加细粒度的管理，使网络和网络数据更接近应用层。SDN 将网络设备从分组过滤、选路、服务区分等控制功能解放出来，使其专注于数据转发，提高网络速率和网络利用率。Google 已在其数据中心中实现 SDN 技术，使数据中心的广域网连接利用率接近 100% ，越来越多的大型互联网公司和网络运营商投入 SDN 部署。

SDN 网络架构利用其可编程性、集中控制、细粒度管理等特点获得更丰富功能的同时，也面临诸多安全挑战。控制器

收稿日期 ：2014-08-06
基金项目 ：国家高技术研究发展计划（863 计划）[2013AA013104]、中国科学院战略性先导科技专项 [XDA06010702]
作者简介 薛聪（1990-），女，河北，硕士研究生，主要研究方向 ：网络与系统安全 ；马存庆（1984-），男，青海，助理研究员，博士，主要研究方向 ：网络与系统安全 ；刘宗斌（1985-），男，宁夏，助理研究员，博士，主要研究方向 ：系统安全 ；章庆隆（1988-），男，浙江，博士研究生，主要研究方向 ：网络与系统安全。

拥有网络绝对管理权，作为 SDN 新增的管理层级，一旦失效会使整个网络面临瘫痪，因此保证控制器安全至关重要。如何在充分发挥 SDN 优势同时，弥补控制器存在的安全缺陷，建立安全控制器架构，已成为 SDN 网络能否满足未来网络需求的关注焦点。

1 SDN 控制器基础架构

根据开放网络基金会（ONF）给出的 SDN 架构定义[1]，如图 1 所示，SDN 分为基础设施层、控制层和应用层，以及连接各层间数据交换的南北向接口。基础设施层包含支持南向接口协议的网络设备，数据流按照控制层下发信息快速匹配，高速转发；控制层通过南向接口搜集网络信息，屏蔽底层物理网络设备差异，实现网络虚拟化，同时集中整合业务需求，下发交换机控制消息，指挥基础设施层上网络设备的数据转发；应用层通过控制层提供的北向开放接口，下发控制策略，实现网络的灵活管理。SDN 具有集中控制逻辑、可编程性、网络虚拟化、细粒度控制等优势。

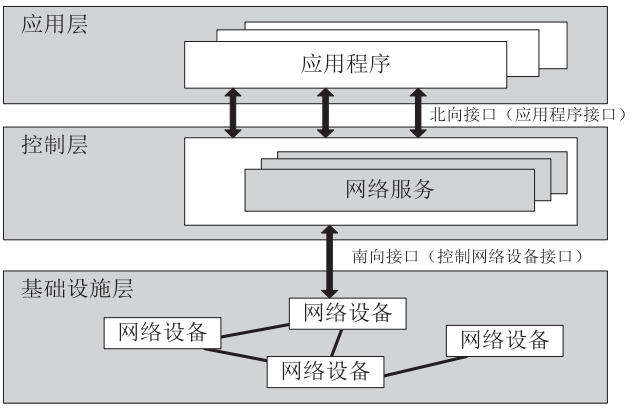
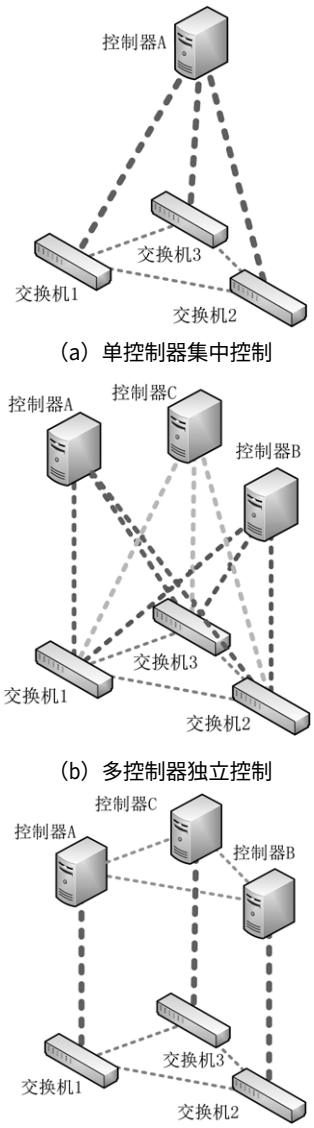


图1 ONF定义的SDN架构

控制层作为 SDN 网络的控制核心，由控制器组成。控制器管理底层网络设备的方式分类可分为三类，如图 2 所示，具体分别为：单控制器集中控制，即单一控制器管理整个物理网络；多控制器独立控制，即在管理相同的网络时，先进行控制逻辑划分，再分配给多个控制器，各控制器执行功能独立；多控制器协同控制，即多个控制器分别管理不同的网络域，分布式管理整个网络。

控制器的基本工作流程为：通过南向接口，控制器搜集、存储、实时更新网络状态信息；通过北向接口，应用程序向控制器下发决策；控制器对应用决策进行模块化处



（a）单控制器集中控制

（b）多控制器独立控制

（c）多控制器协同控制

图2 三种控制器管理模式

理，翻译成交换机能执行处理的消息并发送给底层网络设备。控制器应包括南向协议服务模块，建立与网络设备数据交换；控制管理模块，提供链路发现、拓扑管理、负载均衡等组件；应用程序接口，为应用层提供控制信息调用和决策下发服务。考虑到网络可扩展性、控制器单点失效等因素，一个网络会由多个控制器同时控制，当多个控制器协同执行网络功能时（如图 2（c）所示），控制器间还需要东西向接口，用于控制器间交换网络状态信息或策略信息。

基于控制器工作流程，目前控制器的软件架构包括南向协议管理模块、基础控制组件、开放北向接口三大部分，结合 NOX、Floodlight 等多种开源的控制器软件框架，SDN 控制器的基本设计架构如图 3 所示。

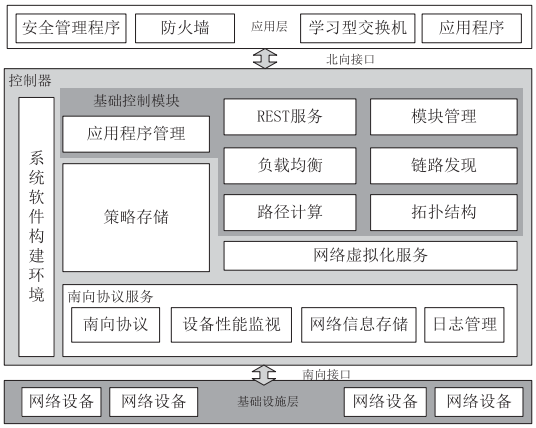


图3 SDN控制器基础架构

2 SDN 控制器存在的安全问题

SDN 技术面临诸多安全挑战，如恶意数据流、交换机流表篡改、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。控制器作为 SDN 核心，一旦失效整个网络崩溃，控制器安全是安全 SDN 架构设计的重中之重。随着 SDN 技术发展，依照基本设计架构的控制器由于设计缺陷，在网络信息保护、应用程序管理、模块处理流程方面暴露了诸多安全问题。

2.1 网络信息保护问题

网络信息在控制器上的维护，通常依赖开辟专门的存储模块。控制器及应用程序根据网络状态信息下发决策。控制器维护的网络信息分为静态信息和动态信息，静态信息主要指网络可达性信息，包括地址、拓扑、链路状态、端口输出、服务质量参数等，更新速度慢。动态信息指网络的实时状态，包括每个交换机上的流表条目、带宽利用率、数据选路等，更新速度快，是应用程序产生的决策存在很大差异的原因[2]。

由于控制器根据网络信息在网络中执行相应功能，当信息被非法写入时才会对网络传输产生破坏，因此控制器上网络信息维护的安全问题主要指数据完整性和可用性被破坏，按照不同控制器管理模式，具体的表现有所不同，如表1所示。

表1 三种管理模式下数据完整性和数据可用性方面的安全威胁

控制器模式	数据完整性	数据可用性
单控制器集中控制	对网络信息恶意篡改	——
多控制器独立控制	对网络信息恶意篡改 网络控制信息冲突	——
多控制器协同控制	对网络信息恶意篡改 被非管理域上的其他控制器非法修改 网络信息读写冲突	协同策略中出现错误结点

1) 数据完整性

网络信息被恶意程序或攻击者篡改，是传统网络中较为常见的安全问题。在多控制器系统工作时，被恶意控制的控制器可以通过东西向接口修改其他控制器信息，扰乱正确控制逻辑。

多个控制器独立执行各自功能时，管理网络静态信息环境可能出现干扰，如图 2 (b) 中，假设控制器 A 在进行拓扑管理时，交换机 1 到 2 可视的链路为 1-3-2，而控制器 B 中则为 1-2，此时出现冲突；若为控制器区分等级，就会造成低级控制器执行功能受限。

多控制器协同控制时，部分信息会在控制器间共享并同步[3]，当控制器的本地信息正在更新，同时又有其他控制器读取时，就会造成整个网络域的网络信息不一致，导致下发策略错误。

2) 数据可用性

多控制器协同管理时存在数据可用性问题。例如，一个控制器节点出现错误将导致与之协商的所有控制器都得到错误网络信息，影响最终策略。如图 2 (c)，若把交换机看成一个由多个网络设备组成的网络域，控制器 A 失效将导致交换机 1 所代表的网络域成为孤岛，整个网络的动态信息相应变化，进而导致控制器 B 和 C 维护错误的网络静态信息。

2.2 应用程序管理问题

应用程序通过控制器提供的北向接口接入控制器，调用控制器管理资源。控制器在管理应用程序时，如果没有身份认证、权限管理、日志管理等功能模块，依然会出现传统网络中常见的非法应用程序接入、应用程序越权操作、绕过审计追踪等安全问题。

此外，多个应用程序同时运行时可能出现新的安全问题。应用程序间可能由于控制逻辑完备性缺失，导致策略不一致，主要表现为策略冲突和局部策略失效。

1) 单个控制器上的多种应用程序策略冲突

当多个应用程序对同一条流执行操作时，此时如果没有设置应用程序的访问优先级，或没有对不可重复的操作，如数据包选路、VLAN 划分等级，就可能导致操作冲突。多条策略的组合操作也可能出现与已知策略冲突的情况[4]。如图 4 所示，控制器部署在交换机 1 上部署防火墙服务，用来过滤主机 A 到 B 的数据流；同时，其他应用程序向交换机 2 和 3 下发了流表，使所有的流都流向交换机 3 端口

2,这 3 条策略的组合结果使 A 发往 C 的数据包可以到达 B，这就与防火墙服务规则冲突。

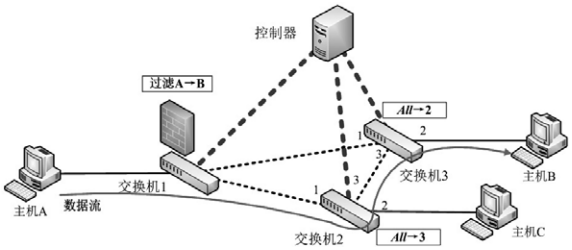


图4 一种策略冲突实例

2) 多个控制器上同类应用程序出现局部策略失效 [5]

在图 2 (c) 中分布式控制器间需要保持最终一致性，控制器间异步地更新所有的备份，在当多控制器上同类应用程序协同达成一项策略时，每个控制器上应用程序的运行结果都是最终策略的一部分，如果出现控制器局部失效或产生错误结果，将会干扰最终策略。

2.3 模块处理流程问题

控制器除了处理底层网络设备请求和上层应用程序策略外，核心任务是提供链路发现、拓扑管理、负载均衡等核心控制逻辑组件供其他模块调用，以提升系统可扩展性和配置灵活性。如果各模块出现编排不合理、处理速度时序不一致、系统设计漏洞等问题，影响全局网络运行。

1) 处理时序不一致破坏控制逻辑一致性 [6]

网络设备是分布式的，控制逻辑的先后配置顺序使流表下发可能存在时延，如图 5 所示，数据包到达交换机 1 请求控制器下发流表，交换机 2 的收到的规则速率慢于数据包转发速率，向控制器再次提出请求，两次请求返回的流表如果不同，将难以保证数据转发前后的一致性，可能造成网络中丢包、环路、冲突等现象。

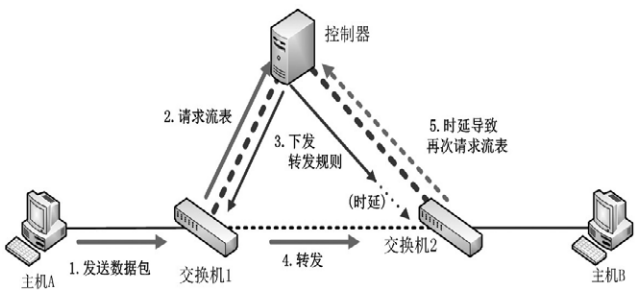


图5 时延导致控制逻辑一致性被破坏

2) 根据响应流程特点，消耗系统资源

新型应用需求逐渐增加，控制器的管控功能日益复杂，当面临多时间多项任务请求时，由于控制器处理流程特点，将造成某个模块的处理负担急剧增加，控制器整体性能下降，从而带来稳定性威胁。在基于 OpenFlow 南向协议的控制器上已存在此类攻击 [7]，即首先通过 SDN 扫描器探测出一个网络是 SDN 架构，而后通过向控制器发送大量数据流请求迫使控制器不断响应，极大地消耗控制器的处理能力。

综合所述,SDN 控制器存在的安全问题主要如表 2 所示。

表2 SDN控制器的安全问题

威胁分类	安全问题
网络信息保护	恶意程序、攻击者、其他控制器非法修改管理网络信息冲突 网络信息读写不一致 协同策略中出现错误节点
应用程序管理	非法应用程序接入 应用程序越权管理 绕过审计追踪 多类策略冲突
模块处理流程	时序不一致 控制器响应流程局限性

3 一种安全 SDN 控制器架构设计

控制器应遵循统一南向接口、开放北向 API、功能组件化等设计原则。设计 SDN 控制器架构时，除了要考虑功能模块，在部署时就应该考虑安全问题。基于上述分析，控制器的安全问题覆盖了整个控制器的工作流程，根据控制器管理资源层级和处理顺序，本文设计了一种 SDN 控制器的安全设计架构。如图 6 所示，在南向接口处增加逻辑分层组件，在控制器原有设计基础上新增加了资源池、应用管理模块、入侵容忍等模块，并对各数据交换接口和基础控制模块的业务编排进行安全改进。图 6 中灰色部分代表根据控制器安全需求重新进行了业务编排，黑框部分为新增的安全组件。

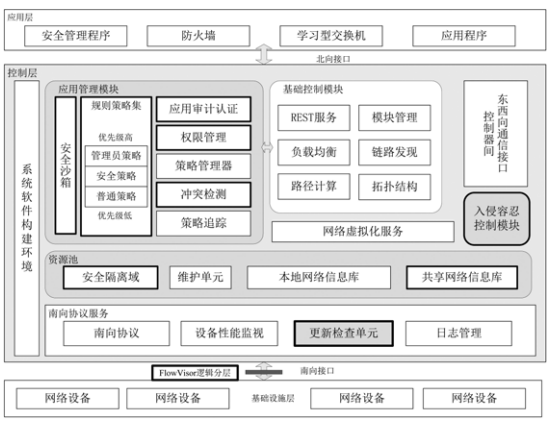


图6 一种SDN控制器安全设计架构

在网络信息进入控制器之前,先通过虚拟化逻辑分层[8],将真实物理网络划分成多个网络层，每个网络层专享独立的网络静态信息，并对链路利用率等网络动态信息进行分割，使每个控制器控制的网络层在逻辑上相互独立，避免在图 2 (b) 情况下出现冲突 ;同时，某一台控制器控制的网络被入侵后，其余网络层仍可正常工作。

网络信息存储在基础设计架构中，作为南向协议服务模块中的一部分，当控制器间进行数据交换时，网络信息就属于东西向接口的通信内容，因此在安全的控制器设计中应设计一个独立的资源池模块，使其位于南向接口和东西向接口之间。资源池有两个基础模块 :本地网络信息库和共享网络信息库，分别用于存储本地数据和分布式数据存储 ;维护单元负责管理资源池读写逻辑一致性。

应用管理模块用于保证应用程序在控制器上有可靠的运行环境，应用管理模块位于北向接口与资源池之间，能够调用基础控制模块提供的调用接口。应用程序可通过该模块调用网络信息和基础控制信息，制定相应策略，并通过基础控制模块和南向协议服务模块，将策略翻译成网络设备能执行的表项信息，使 SDN 网络可以更细粒度的进行策略管理。应用管理模块的基础部分是策略管理和策略存储集合。

由于控制器集中了 SDN 网络的所有控制逻辑，所以必须保证其可用性和健壮性。入侵容忍控制模块利用东西向接口以保证控制器间能够进行控制策略和网络信息交互，共享网络信息库提供其他控制器信息存储。当单一控制器集中控制时，该模块不发挥作用 ;当多控制器协同控制时，该模块提供分布式存储的入侵容忍功能 ;同时，可在多控制器独立控制模型基础上，建立控制器间的数据通信链路，统一控制功能，使得控制器间互为副本，形成拜占庭式入侵容忍系统[5]，在部分控制器节点出现错误时，其他控制器通过协商仍能得出正确决策。

除了上述功能模块，本文提出的安全 SDN 控制器架构还在南向协议服务模块添加了更新检查单元，用于解决控制器间系统性能不一致问题 ;将控制器的东西向通信接口添加到控制器设计基础模块，与入侵容忍模块相结合 ;从基础控制模块中独立出应用管理功能，并在控制器内部提供编程接口，提高各模块功能的独立性。

本文提出的安全 SDN 控制器架构中新增安全组件如表 3 所示。

表3 安全SDN控制器架构中的安全组件

所属模块	安全组件	功能
逻辑分层	FlowVisor[8]	在软件实现了网络的虚拟化分层，使在同一个网络域上的控制器执行决策互不影响
南向协议服务	更新检查单元	通过设置控制逻辑的原子操作或设置同步锁，解决控制器间系统性能不一致
资源池	安全隔离域	存储待验证的网络信息，同时可疑应用程序的运行环境安全沙箱会调用部分信息
	共享网络信息库	控制器间冗余备份，并为实现入侵容忍功能提供基础资源
入侵容忍模块	入侵容忍模块	在多控制器管理网络域上执行入侵容忍控制逻辑
应用管理模块	安全沙箱	为急需执行又无法验证安全性的应用程序提供运行环境
	规则策略集	策略分优先级存储，管理员直接下发的策略优先级最高，安全应用程序次之，优先级最低的普通应用程序策略按时序先后排序
	应用审计认证	高效的认证方案、日志管理
	权限管理	规定和管理应用程序访问网络资源和策略集的权限
	冲突检测	建立冲突检测集合，应用程序产生的新的策略会与已有策略扩展集合比对，根据策略优先级或时序进行更新[9]

4 结束语

SDN 网络具有集中控制逻辑、可编程性、网络虚拟化、细粒度控制等诸多优势，并在数据中心网络中迅速发展，其安全性正在引起高度关注。控制器作为 SDN 网络核心，其设计架构决定其网络管理服务性能的优劣。本文提出了一种安全的 SDN 控制器架构设计，通过增加资源池、应用管理模块、入侵容忍等模块，并融入数据共享、冲突检测等安全组件，用以解决控制器在网络信息维护、应用程序管理、控制器模块处理流程等方面出现的安全问题，增强 SDN 网络的健壮性，利于不同控制器间进行安全的服务扩展。（责编 潘静）

参考文献

[1] ONF(Open Networking Foundation).Software - Defined Networking: The New Norm for Networks[M]. ONF Whitepaper, 2012.7 - 11.

[2] Pingping L, Jun Bi, Yangyang W. East - West Bridge for SDN Network Peering[C] ICoC 2013, CCIS 401, 2013. 170 - 181.

[3] Botelho F A, Ramos F M V, Kreutz D. On the feasibility of a consistent and fault - tolerant data store for SDNs[C] 2013 Second European Workshop on, IEEE, 2013. 38 - 43.

[4] PHILIP P, SEUNGWON S, VINOD Y, et al.. A security enforcement kernel for OpenFlow networks: proceedings of the first workshop on hot topics in software defined networks(HotSDN)[C].Helsinki:ACM Press, 2012.

[5] Kreutz D, Ramos F, Verissimo P. Towards secure and dependable software - defined networks[C] Proceedings of the second ACM SIGCOMM workshop on Hot topics in SDN. ACM, 2013. 55 - 60.

[6] 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（05）:1078 - 1097.

[7] Seungwon Shin, Guofei Gu. Attacking software - defined networks: a first feasibility study[C] HotSDN 2013. 165 - 166.

[8] ROB S, GLEN G, KOK - KIONG Y, et al. FlowVisor: a network virtualization layer[R]. Technical Report, OpenFlow Switch Consortium, 2009.