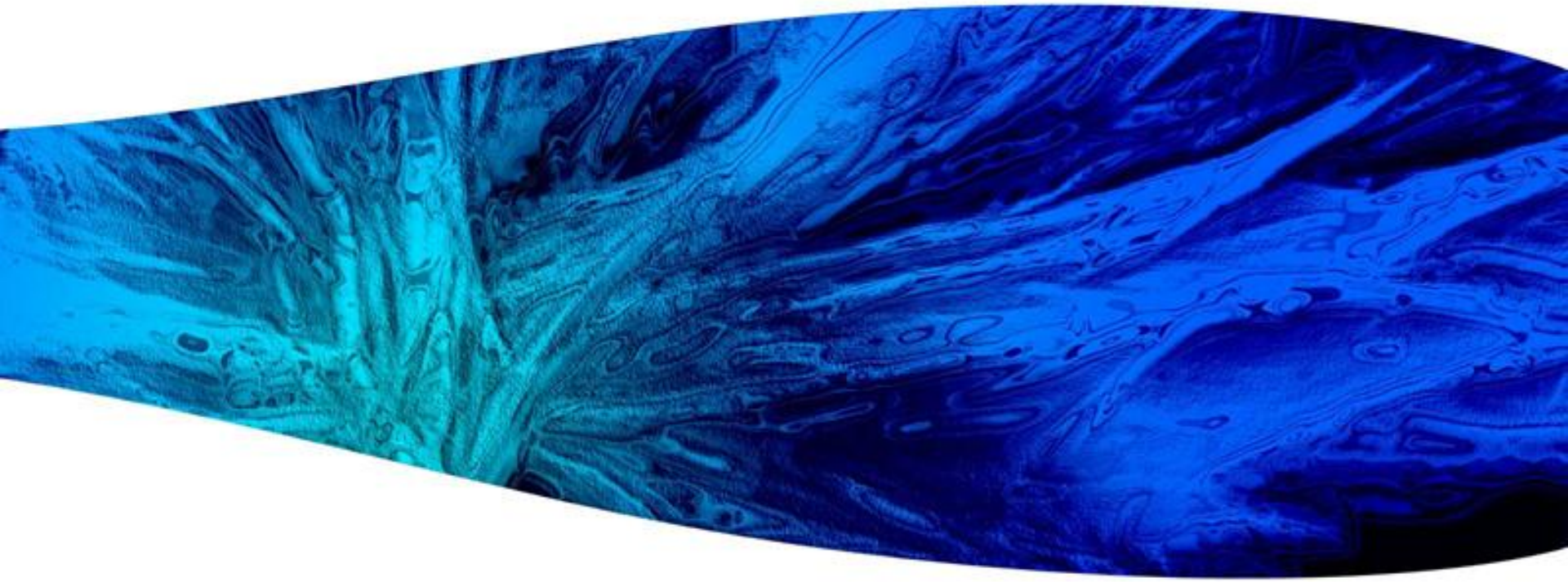
SDN安全的研究

周靖
北京科技大学
计算机与通信工程学院
信息与通信工程系



SDN 安全的特点

SDN 架构实现了传统网络架构中网络管理功能的集中，是对传统网络架构的革命性创新。这种创新除了带来管理、运营等方面的灵活性，也使得SDN 中的安全问题呈现出其特有的特点。

SDN 安全问题的独特性与SDN 的管理集中性和开放性是密不可分的。

管理集中性使得网络配置、网络服务访问控制、网络安全服务部署等都集中于SDN 控制器上。攻击者一旦成功实施了对控制器的攻击，将造成网络服务的大面积瘫痪，影响控制器覆盖的整个网络范围。

开放性是SDN 的另一个重要特征，

首先，开放性使得SDN 控制器的安全漏洞、策略的不完备性等充分地暴露在攻击者面前，给予了攻击者足够的信息制定攻击策略。

其次，SDN 架构通过SDN 控制器给应用层提供大量的可编程接口， 这个层面上的开放性可能会带来接口的滥用，如引发DDoS 攻击等，因而需要对应用层制定准入策略，防止意图不轨的攻击者利用开放接口实施对网络控制器的攻击。

最后，开放性使得SDN 控制器需要谨慎评估开放的接口， 以防止攻击者利用某些接口进行网络监听、网络攻击等。

SDN 的网络架构特性使得SDN 呈现出以下3 个特点。

- 在传统的网络架构中，网络安全控制集中于OSI 体系架构的4~7 层，在SDN 架构下，通过控制器可以实现2~7 层的安全策略配置，提供了更加细粒度的安全控制。
- SDN 的安全威胁将更加集中，而不是传统的分散在网络中各个相关的网元部分。
- SDN 的安全威胁将更加不可视化。随着网络控制权从用户到网络控制器的更迭，用户对于自己的网络状态将越来越不能很好地监控。

引用文献

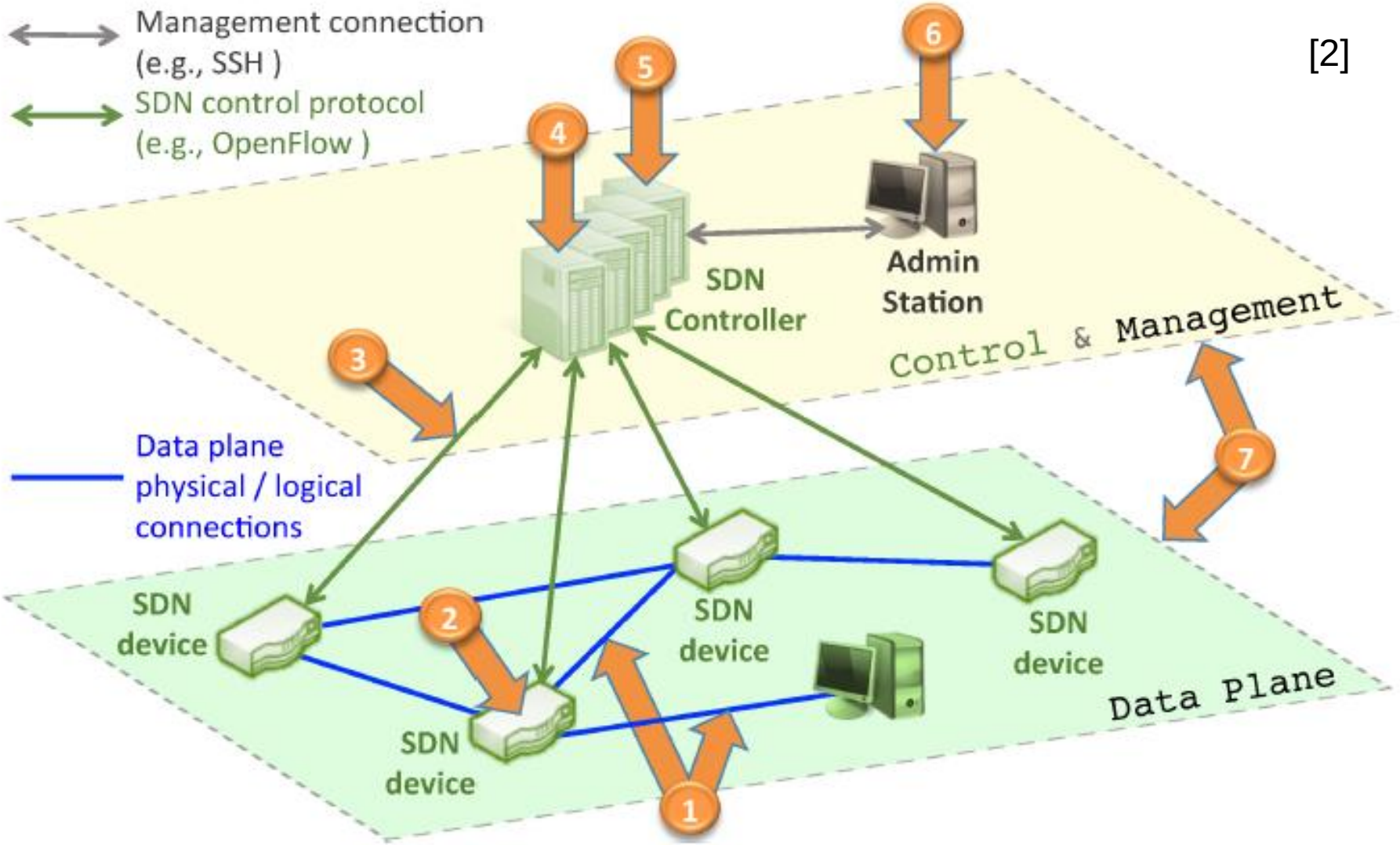
[1] Sandra Scott-Hayward,Gemma O’ Callaghan and Sakir Sezer “SDN Security : A Survey”
[2] Diego Kreutz, Fernando M.V.Ramos, “Towards Secure and Dependable Software-Defined Networks”
[3] K.Benton, L.J.Camp, C.Small, “OpenFlow Vulnerability Assessment”
[4] R.Sherwood et al. “FlowVisor: A Network Virtualization Layer” .Tech.rep.Deutsche Telekom Inc.R&DLab,Stanford,Nicira Networks,2009.
[5] P.Porrasetal.” A security enforcement kernel for OpenFlow networks".In: HotSDN. ACM, 2012.
[6] Radware, “DefenseFlow: The SDN Application that Programs Networks for DoS Security” Available: http://www.radware.com/Products/DefenseFlow/
[7] S.Fayazbakhsh, V.Sekar, M.Yu, J.Mogul, “FlowTags: Enforcing Network-Wide Policies in the Presence of Dynamic Middlebox Actions,” in Proceedings of the second workshop on Hot topics in software defined networks. ACM,2013.
[8] Seungwon Shin, Guofei Gu “Attacking Software-Defined Networks: A First Feasibility Study” HotSDN’13, August16,2013,HongKong,China. ACM 978-1-4503-2178-5/13/08.
[9] Seungwon Shin, Vinod Yegneswaran, Phillip Porras, Guofei Gu,” AVANT-GUARD: Scalable and Vigilant SwitchFlow Management in Software-Defined Networks” . CCS’13, November4–8,2013, Berlin, Germany.
[10] Security-Enhanced FloodlightBeta 3 release6 December 2013 Available: http://www.openflowsec.org/SDNSuite.html

其他参考文献

- R.Kloeti, “OpenFlow: A Security Analysis,” April 2013. [Online]. Available: ftp://yosemite.ee.ethz.ch/pub/students/2012-HS/MA-2012-20 signed.pdf
- S.Sezer, S.Scott-Hayward, P.Chouhan,B.Fraser,D.Lake,J.Finnegan, N.Viljoen, M.Miller, N.Rao, “Are we ready for SDN? Implementation challenges for Software defined networks, ” Communications Magazine, IEEE,vol.51,no.7,2013.
- “OpenFlow Switch Specification Version1.4.0,” Open Networking Foundation. [Online]. Available: https://www.opennetworking.org

SDN安全问题分类 [1]

Security Issue/Attack	SDN Layer Affected or Targeted				
	Application Layer	App-Ctl Interface	Control Layer	Ctl-Data Interface	Data Layer
Unauthorized Access e.g.					
Unauthorized Controller Access			✓	✓	✓
Unauthenticated Application	✓	✓	✓		
Data Leakage e.g.					
Flow Rule Discovery (Side Channel Attack on Input Buffer)					✓
Forwarding Policy Discovery (Packet Processing Timing Analysis)					✓
Data Modification e.g.					
Flow Rule Modification to Modify Packets			✓	✓	✓
Malicious Applications e.g.					
Fraudulent Rule Insertion	✓	✓	✓		
Controller Hijacking			✓	✓	✓
Denial of Service e.g.					
Controller-Switch Communication Flood			✓	✓	✓
Switch Flow Table Flooding					✓
Configuration Issues e.g.					
Lack of TLS (or other Authentication Technique) Adoption			✓	✓	✓
Policy Enforcement	✓	✓	✓		


Management connection
(e.g., SSH)
SDN control protocol
(e.g., OpenFlow)
Data plane
physical / logical
connections
SDN
Controller
Admin
Station
Control & Management
SDN
device
SDN
device
SDN
device
SDN
device
Data Plane
1
2
3
4
5
6
7

[2]

SDN可能出现的安全问题

- 欺诈或者伪造的数据流
- 对交换机的攻击
- 对控制器和交换机之间通信的攻击
- 对控制器的攻击
- 在控制器上运行未认证的应用程序
- 对管理站的攻击
- 整个系统被攻击后缺少信任的资源去快速修复

SDN安全问题的解决方案

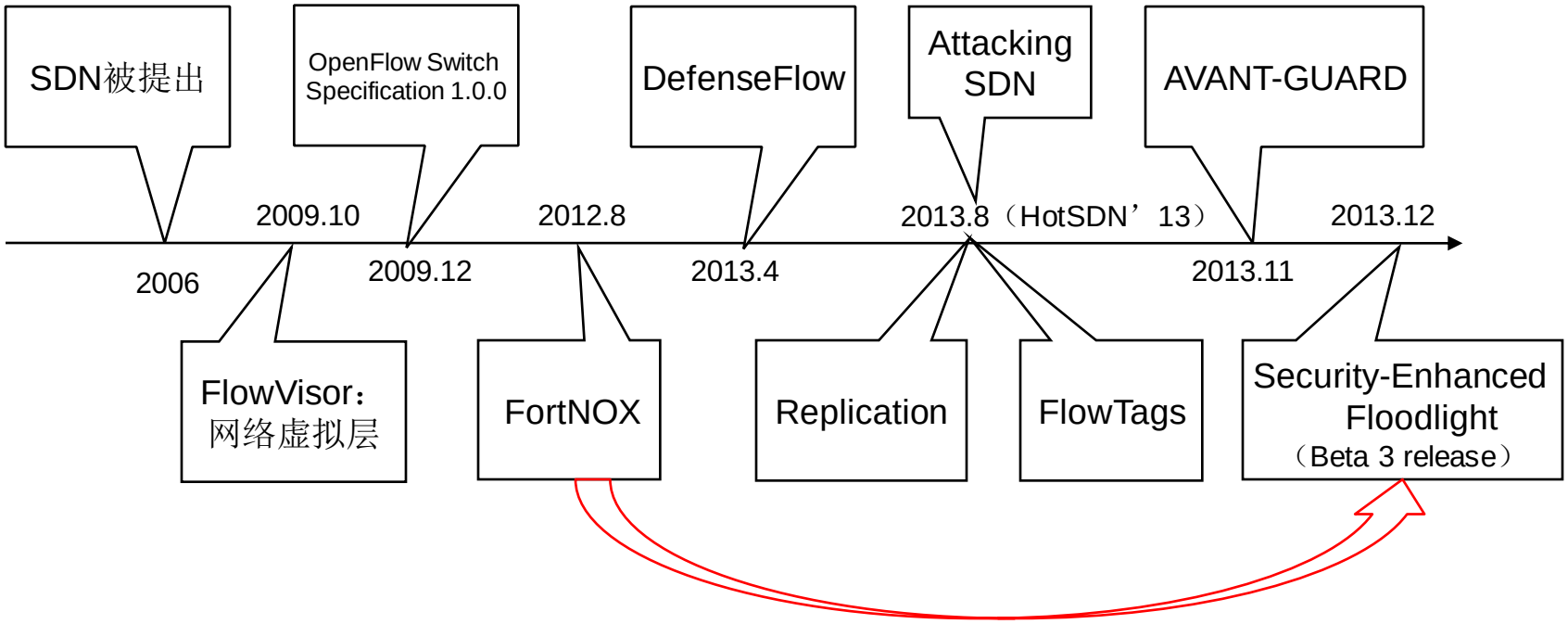
- 应用支持运行时间分析的系统可以检测出问题流，以及对交换机行为的动态控制以确保数据流的安全传输。
- 应用软件认证机制，例如自信任管理方法确保交换机的安全。
- 应用多证书认证机制，或者在控制器之间使用门限密码，以及设备之间应用动态联合确保控制器和交换机通信安全。
- 应用复制，多元化，修复等技术确保控制器的安全。
- 通过自信任管理机制确保应用程序在生命周期内是信任的。
- 使用双凭证认证机制强化对控制器的管理，以及使用有效的修复机制确保重新加载后状态的安全。

目前openflow存在的安全缺陷 [3]

对于安全问题一带而过，没有细致的分析，例如：

- openflow协议将控制器与交换机之间的TLS定义为可选择项，并且大多数厂商考虑到认证的代价并没有采取TLS
- 规定了控制器与交换机之间的回话与握手机制，但是对于交换机频繁发起会话而导致的拒绝服务，没有很好地处理。

SDN安全问题研究状况



FlowVisor [4]

- FlowVisor可以将硬件设备虚拟化成多个网络，这样一方面可以提高网络安全，某一层虚拟网络被入侵后，其余虚拟层可以正常工作。
- 另一方面，虚拟化是基于软件实现的，增加对软件安全认证的要求。同时在同一物理设备上虚拟化的多个网络使得各节点之间的认证也变得更加繁琐。

FortNOX [5]

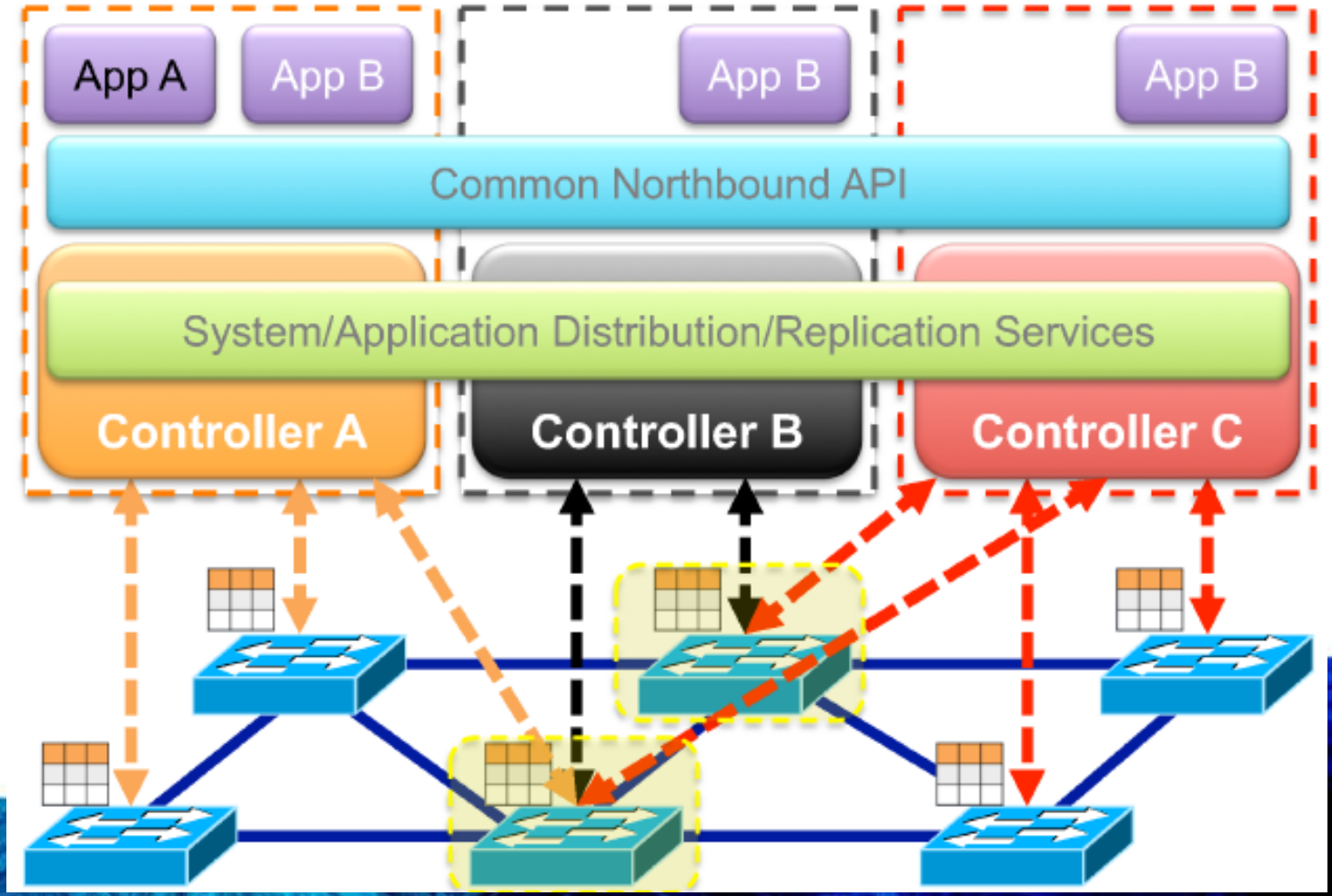
- 对控制器处理策略信息进行了强化，提出了解决多个策略发生冲突的新方法。
- 提出了基于角色的流策略授权

DefenseFlow [6]

DefenseFlow是由Radware公司开发可以防止拒绝服务攻击的软件。充分利用控制器的数据搜集功能，对攻击行为进行检测。区别于以往的只局限于速率方面的检测，DefenseFlow还考虑非速率因素比如流量分布情况。当流量超过一定阈值，传统的检测机制会判决为攻击行为，但是可能这些流量来自不同的地点，属于正常情况。

Replication [2]

- 控制器被复制成多个，运行的应用程序也被复制成多个。这样可以抵抗或者减少软硬件故障、恶意行为带来的损失。



FlowTags [7]

- 对流添加标签项，使它成为交换器路由和进程的一部分。通过修改标签替代原来的修改网络中一系列的流表项或者策略信息，从而实现网络动态管理。

Attacking SDN [8]

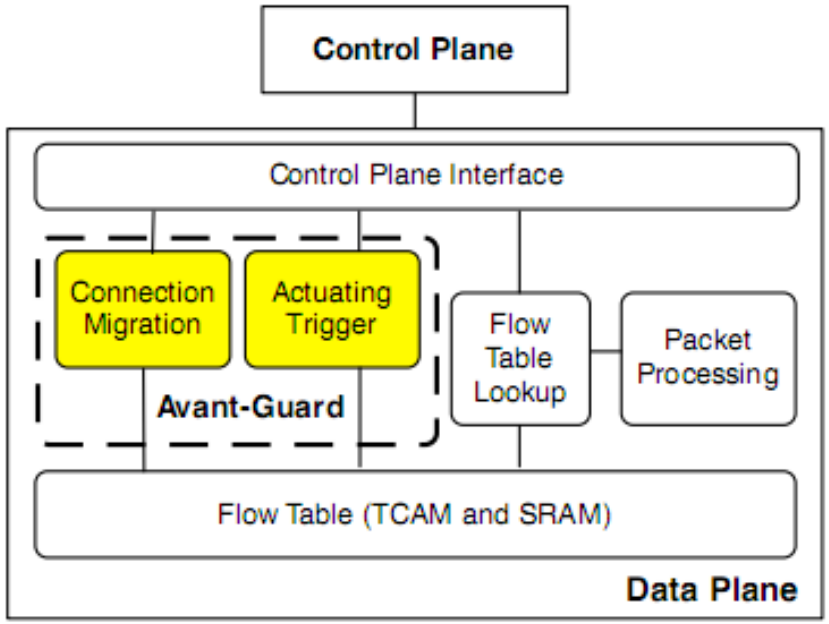
先通过SDN scanner利用数据包的转发延时试探出网络是否为SDN结构。若为SDN结构则发送大量新数据包，将会造成：

- 交换机不断向控制器发送询问消息而导致的控制平面资源耗尽或者拒绝服务攻击
- 控制器向交换机回应大量无用规则而导致的数据平面资源耗尽或者

AVANT-GUARD [9]

AVANT-GUARD 通过包含connection migration和actuating triggers两个技术对数据平面以及数据到控制平面的安全性能进行了强化。同时在最小化修改系统的前提下保证了系统的灵活性和健壮性。

- connection migration用以防止数据平面的饱和攻击。
- actuating triggers通过给SDN交换机提供条件触发器解决了响应性的挑战。



Security-Enhanced Floodlight（Beta 3）[10]

SE Floodlight 是对FortNOX的强化。除了包含规则冲突检测和基于角色的流策略授权技术外，还具有如下技术或特点：

- 权限分离，使SE Floodlight成为不依赖于应用层和数据平面的独立媒介。
- 对规则产生器进行运行时间监测
- 基于角色规则冲突解决
- 管理人员可以干预由软件决定的出包消息
- 对控制器的安全行为进行监察