[关闭]

@EggGump 2019-03-29 13:48 字数 1955 阅读 5

A Survey of Security in Software Defined Networks

sdn survey

Scott-Hayward S , Member, IEEE, et al. A Survey of Security in Software Defined Networks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1):623-654.

本篇是16年的综述，参考 文献不是特别新，内容一般吧。

Introduction

本文的整体框架如图1所示：

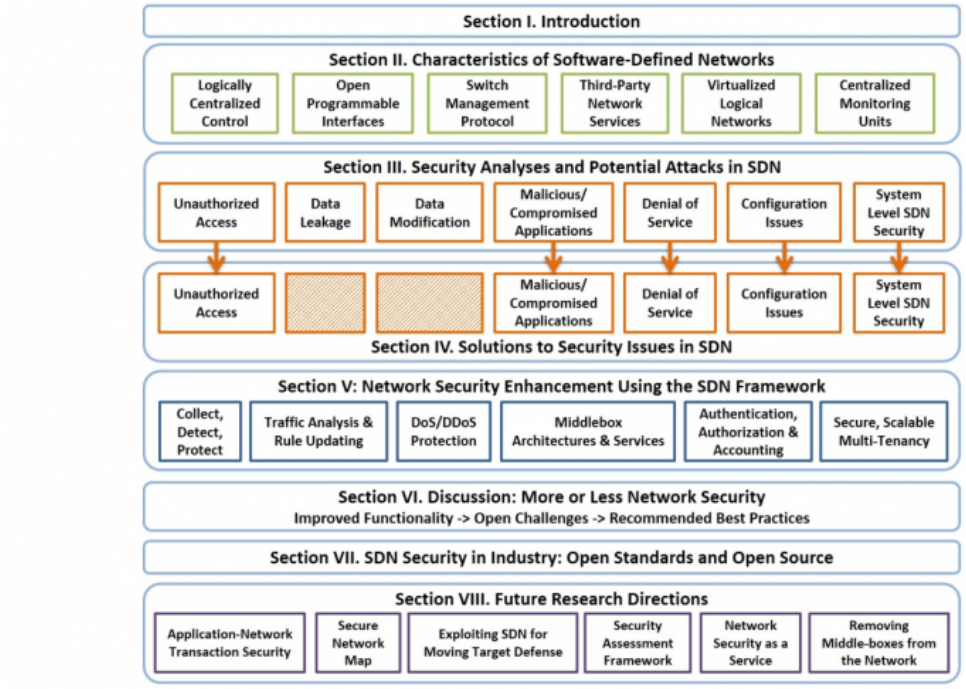

Fig. 1. Overview of the SDN Security Survey

SDN特性

图2列出了SDN的基本特性

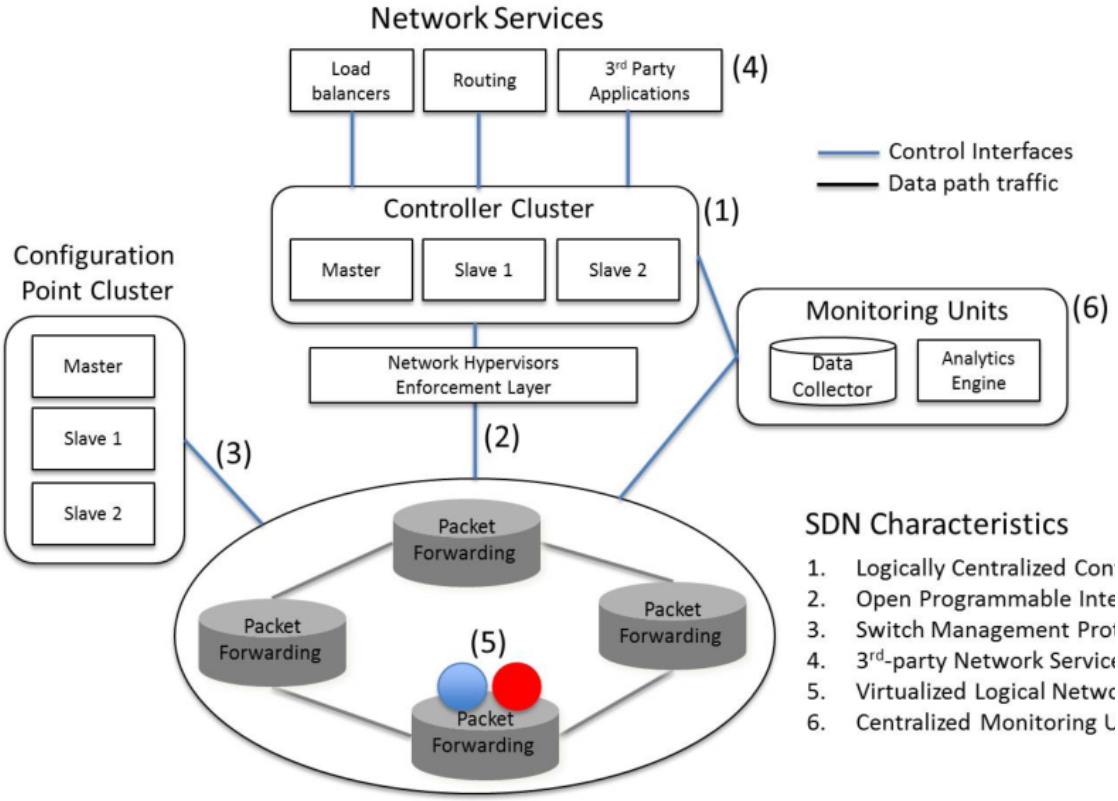

Fig. 2. SDN Characteristics

- 逻辑结构中心化控制
- 东西协议：Controller间通信
- 如何配置switch
- ODL可热加载第三方应用
- 可根据用户需要进行配置，更加灵巧
- 可集成在Controller中的控制单元

分布式Controller和层次式Controller结构如图3：

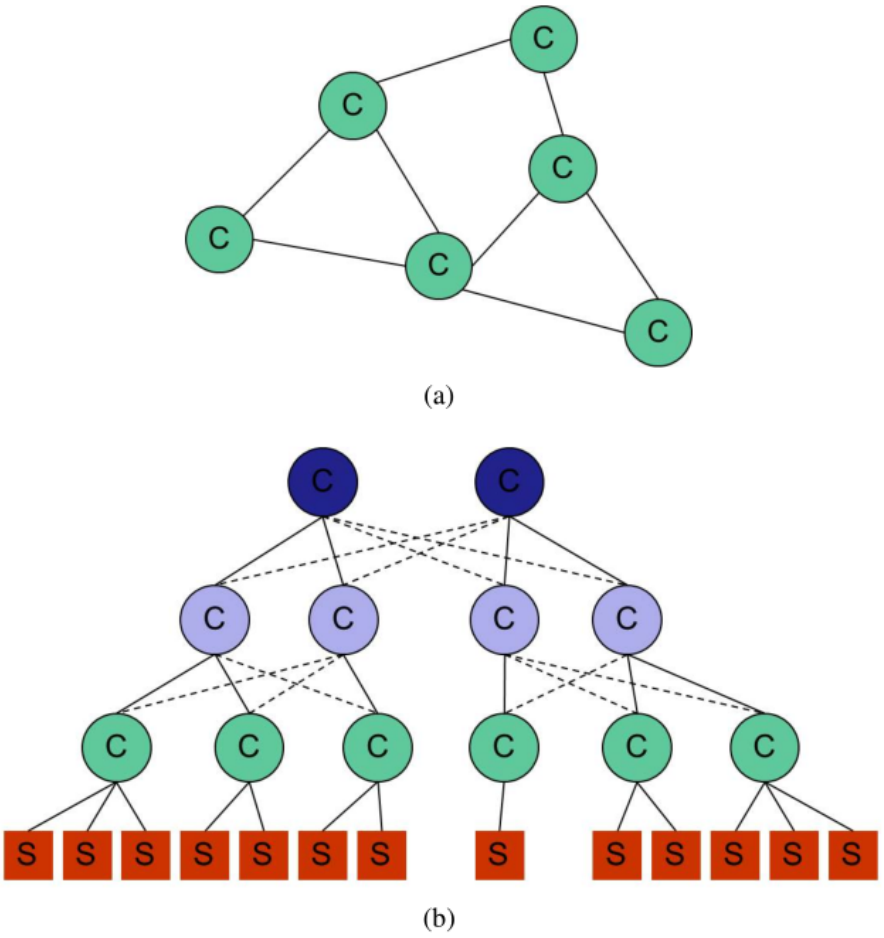

Fig. 3. Distributed Control Frameworks for SDN (a) Controller Clustering, and (b) Hierarchical Control

SDN的应用，控制，数据层架构如图4

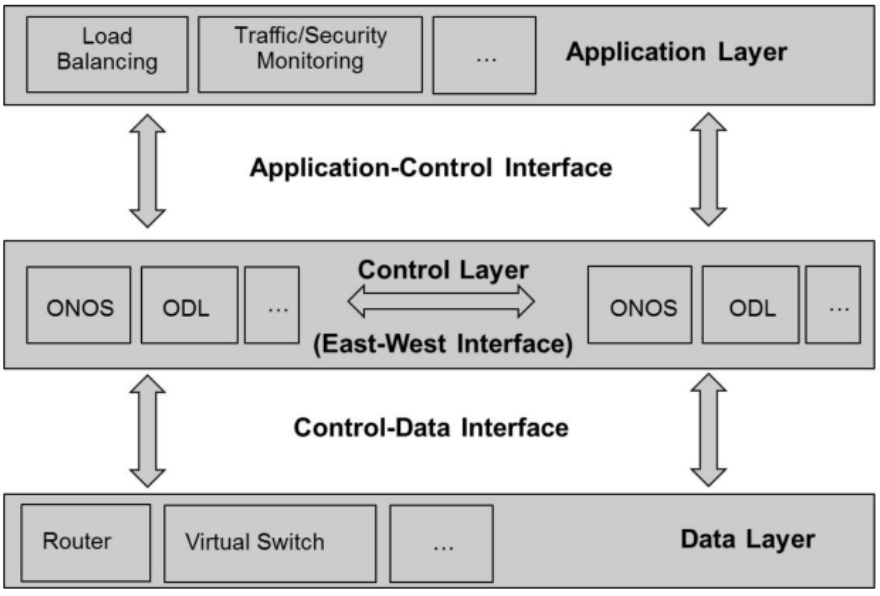

Fig. 4. SDN Functional Architecture illustrating the data, control and application layers and interfaces

潜在的安全因素分析

有关安全因素分析的文献的总结见表1：

TABLE I
COMPARISON OF SECURITY ANALYSES OF SDN AND OPENFLOW

Research Work	Security Analysis		OF	SDN Layer/Interface				
	Vulnerabilities	Enhancements		App	App-Ctl	Ctl	Ctl-Data	Data
SDN Security Survey [24]	✓	✓		✓	✓	✓	✓	✓
OF Security [25], OF Vulnerability [26], ProtoGENI [28]	✓		✓			✓	✓	✓
Secure and Dependable SDN [27]	✓			✓		✓	✓	✓
Comprehensive Survey [21]	✓		✓	✓		✓	✓	✓
Attacking SDN [29]	✓		✓			✓	✓	✓
Vulnerability of FlowVisor [32]	✓		✓			✓	✓	
SDN for Network Security [30]	✓	✓	✓		✓	✓	✓	
Blessing or Curse? [31]	✓	✓	✓			✓	✓	✓
SDN Wireless Mobile [33]	✓	✓	✓	✓		✓	✓	✓
Cloud Computing Security [34]	✓	✓				✓	✓	✓

都是一些一般的论文，应该可以总结出一些需要解决的问题。

存在的安全问题总结见表2：

TABLE II
CATEGORIZATION OF THE SECURITY ISSUES ASSOCIATED WITH THE SDN FRAMEWORK BY LAYER/INTERFACE AFFECTED

Security Issue	SDN Layer Affected or Targeted				
	App Layer	App-Ctl Interface	Ctl Layer	Ctl-Data Interface	Data Layer
Unauthorized Access e.g.					
Unauthorized Controller Access/Controller Hijacking			✓	✓	✓
Unauthorized/Unauthenticated Application	✓	✓	✓		
Data Leakage e.g.					
Flow Rule Discovery (Side Channel Attack on Input Buffer)					✓
Credential Management (Keys, Certificates for each Logical Network)					✓
Forwarding Policy Discovery (Packet Processing Timing Analysis)			✓	✓	✓
Data Modification e.g.					
Flow Rule Modification to Modify Packets (Man-in-the-Middle attack)			✓	✓	✓
Malicious/Compromised Applications e.g.					
Fraudulent Rule Insertion	✓	✓	✓		
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	✓	✓	✓		
Lack of Secure Provisioning	✓	✓	✓	✓	✓
System Level SDN Security e.g.					
Lack of Visibility of Network State			✓	✓	✓

表3对表2中提出的问题对就原解决方法进行了总结

TABLE III
COMPARISON OF RESEARCH ON SOLUTIONS TO SECURITY ISSUES IN SDN

Solution to Security Issue	Research Work	SDN Layer/Interface				
		App	App-Ctl	Ctl	Ctl-Data	Data
Unauthorized Access	Securing Distributed Control [44], Byzantine-Resilient SDN [45]			✓	✓	
	Authentication for Resilience [46]			✓		
	PermOF [47]	✓	✓			
	OperationCheckpoint [48]	✓	✓	✓		
	SE-Floodlight [49], [50]	✓	✓	✓	✓	
	AuthFlow [51]	✓		✓	✓	✓
Data Leakage						
Data Modification						
Malicious Applications	FortNOX [52]	✓	✓	✓	✓	
	ROSEMARY [53]	✓		✓		
	LegoSDN [54]	✓	✓	✓		
Denial of Service	AVANT-GUARD [55], CPRecovery [56]			✓	✓	✓
	VAVE [57]	✓		✓	✓	✓
	Delegating Network Security [58]	✓	✓	✓	✓	✓
Configuration Issues	NICE [59]	✓	✓		✓	
	FlowChecker [60], Flover [61], Anteater [62], VeriFlow [63], NetPlumber [64]	✓	✓	✓	✓	
	Security-Enhanced Firewall [65], FlowGuard [66], [67], LPM [68]	✓		✓	✓	✓
	Frenetic [69], Flow-Based Policy [70], Consistent Updates [71]	✓	✓	✓	✓	
	Shared Data Store [72]	✓		✓	✓	✓
	Splendid Isolation [73]		✓	✓		
	Verificare [74], Machine-Verified SDN [75], VeriCon [76]		✓	✓	✓	
System Level SDN Security	Debugger for SDN [77]	✓			✓	
	OFHIP [78], Secure-SDMN [79]				✓	
	FRESCO [80]	✓	✓	✓	✓	

未授权准入问题

总结于表4

TABLE IV
PROBLEM AND SOLUTION PROPOSED FOR *Unauthorized Access* ISSUES IN SDN

Research Work	Problem/Goal	Proposed Solution
Securing Distributed Control [44]	Secure the distributed control model against malicious use	Signature algorithm to securely transmit flow installation rules
Byzantine-Resilient Secure SDN [45]	Protect the SDN Control Plane from attack	Multiple controller structure with Byzantine-Fault Tolerant algorithm
Authentication for Resilience [46]	How to structure the SDN architecture to offer more security?	Hierarchical System of controllers/switches to reduce points of serious failure
PermOF [47]	Full privilege of OF exposed to every application	Proposed Permission System to apply minimum privilege to applications
OperationCheckpoint [48]	Controller operations open to every application	Implementation of a Permissions Check Mechanism to secure app-control interface
SE-Floodlight [49], [50]	Lack of security between OF apps/modules and control/data plane communication	Role-based authorization and security constraint enforcement for OF control layer
AuthFlow [51]	Prevent access to the SDN by unauthorized hosts	An authentication and access control mechanism based on host credentials

提出的解决方法有：签名算法下发流表，会境加签名检查信息传输的开销；拜占庭容错分布式Controller,分层Controller系统，给每个应用赋不同的权限，是一种隔离应用机制；应用权限检查机制，使Controller能基于角色进行授权，基于主机证书的授权机制。[50]的质量较好。

被挟持应用或恶意应用问题

controller中的应用需认证，对多个应用下发rule冲突的解决办法即是对高优先级的进行保留。表5是该部分问题的总结。

TABLE V
PROBLEM AND SOLUTION PROPOSED FOR *Malicious/Compromised Application* ISSUES IN SDN

Research Work	Problem/Goal	Proposed Solution
FortNOX [52]	Challenge of detecting and reconciling potentially conflicting flow rules from OF apps	Security enforcement kernel for prioritizing flow rules with role-based authorization
ROSEMARY [53]	Protect against simple/common network app failures leading to loss of network control	A controller implementing a network app containment and resilience strategy
LegoSDN [54]	Make the controller and network resilient to SDN application failures	A controller architecture to improve availability with fault isolation and network transaction management

[52]提出的是一种授权机制，每个应用都在一个的沙箱中运行，网络范围支持事务的原子更新和回滚。
[53,54]则隔离应用。

DOS

总结表6

TABLE VI
PROBLEM AND SOLUTION PROPOSED FOR *Denial of Service* ISSUES IN SDN

Research Work	Problem/Goal	Proposed Solution
AVANT-GUARD [55]	Protect against Control Plane DoS attack and detect and respond to changing flow dynamics	Connection Migration Tool reducing data-control plane interaction and Actuating Trigger to install flow rules
CPRecovery [56]	Protect centralized network OS from failure due to DoS attack	CPRecovery component provides seamless primary controller backup
VAVE [57]	Source Address Validation	NOX controller determines validation rules with global view
Delegating Network Security [58]	Remove network administration bottleneck	ident++ protocol to delegate aspects of network security policy

[55]提出通过减少数据层发送的包数来缓解Controller-Data的连接瓶颈问题，并利用工具移除未完成的TCP会话。
[56]提出失败交换机到备份交换机的无缝转换方法
[57]对源IP进行检测，如果没过关就将该ip发的包全丢弃。
[58]委派授权的方式解决控制器瓶颈问题
[55]和[57]可以看一下。

Configuration Issues

总结表7

TABLE VII
PROBLEM AND SOLUTION PROPOSED FOR *Configuration Issues* IN SDN

Research Work	Problem/Goal	Proposed Solution
Detecting Network Errors		
NICE [59]	Test OF applications for correctness	Automated OF application testing to remove bugs in controllers
FlowChecker [60]	Avoid misconfiguration issues in OF due to conflicting flow rules	Use binary decision diagrams (BDDs) to test for intra-switch misconfigurations
Flover [61]	Verify that dynamically inserted flow policies do not violate the underlying network security policy	Use Satisfiability Modulo Theories (SMT) solver to detect if the aggregate of flow policies violates network security policy
Anteater [62]	Diagnose problems in the network data plane	Static analysis tool for checking invariants
Real-Time Policy Checking		
VeriFlow [63]	Real-time network invariant detection	Slice the OF network to check for invariant property violations
NetPlumber [64]	Verify network correctness in real time	Incremental computation to validate policy updates in real time
Security-Enhanced Firewall [65]	Detect and resolve firewall bypass threats in OF networks	Track flows using a shifted flow graph (HSA) and block conflicting flow path
FlowGuard [66], [67]	Detect and resolve firewall policy violations in dynamic OF network	Track network flow paths and check rule dependencies for automatic, real-time violation resolution
Language-Based Resolution		
Frenetic [69]	Resolve policy conflicts	Run-time system to convert flow rules into non-overlapping policies
Flow-Based Policy [70]	Simplify implementation of network security mechanisms in SDN	Flow-based network security policy language and framework
Consistent Abstractions/Network View		
Consistent Updates [71]	Overcome instability of configuration changes in SDN	Per-packet and per-flow consistency abstractions for configuration updates
LPM [68]	Manage complex network dynamics in SDN	Layered policy management framework (resolve inter-module, inter-application and intra-table dependencies)
Shared Data Store [72]	Maintain network performance while supporting a strongly consistent network view in SDN	Distributed, highly-available, strongly consistent controller for SDN based on fault-tolerant data store
Formal Verification Methods		
Splendid Isolation [73]	How to program shared networks in a secure and reliable manner?	Introduce slice-based network programming to isolate program traffic
Verificare [74]	A means to guarantee that SDN systems are safe, correct, or secure	Methodology and Tools for formally verifiable distributed system design
Machine-verified SDN [75]	Automatic checking of network-wide properties	Machine-verified SDN controller
VeriCon [76]	Formal method to prove the correctness of an SDN	Verification Tool for infinite-state SDN programs

[59]提出当网络出错时进行检测
[62]提出利用静态分析工具诊断网络
缺点：不能实时
[63]提出将网络作为一个图来检测路由表中的环和不可达路径。
[64]利用包头分析增量检查状态改变
[66,67]自动，实时地跟踪网络流路径和检查规则依赖
[69]转换流规则成非重叠规则
[68]分层管理策略，不大能满足可伸缩性
[62][63][64][75][76]还可以。

System Level SDN Security

总结表8

TABLE VIII
PROBLEM AND SOLUTION PROPOSED FOR *System Level Security* ISSUES IN SDN

Research Work	Problem/Goal	Proposed Solution
Debugger for SDN [77]	Simplify SDN debugging	Prototype network debugger for SDN
OFHIP [78]	Introduce Secure Mobility into OF switches and improve resilience against known TCP attacks	Global ID-based architecture enables OF switches to securely change IP address during mobility
Secure-SDMN [79]	Protect the Control Channel of Software-Defined Mobile Networks	Secure Control Channel Architecture based on IPSec tunnels and security gateways
FRESCO [80]	Simplify the development and deployment of complex security services for OF networks	Application Development Framework for Security Services Composition

系统级SDN安全可以在云，数据中心，移动方面布署。
[78]结合HIP和OpenFlow进行安全地改变移动过程中的IP
[79]对78进行改进，提高控制信道的安全
[80]提供了一个基于FortNOX的应用开发框架

使用SDN框架对网络安全进行加固

表9总结了6种可提升安全的方法，利用SDN特性，应用-控制，接口安全性作为未来研究方向。

TABLE IX
COMPARISON OF NETWORK SECURITY ENHANCEMENTS IN SDN

Security Enhancement	Research Work	SDN Layer/Interface				
		App	App-Ctl	Ctl	Ctl-Data	Data
Collect, Detect, Protect	Combining OpenFlow/sFlow [88], Active Security [89]	✓		✓	✓	✓
	Learning-IDS (L-IDS) [90], NetFuse [91], OrchSec [92]	✓		✓	✓	✓
	Cognition [93]	✓	✓	✓		
Traffic Analysis & Rule Updating	Resonance [94]	✓		✓	✓	✓
	AVANT-GUARD [55], Pedigree [95], OF-RHM [96]			✓	✓	✓
	SDN-MTD [97]	✓		✓	✓	✓
	NICE:NIDS [98], SnortFlow [99], SDNIPS [100], ScalableIDS [101]	✓		✓	✓	
	Revisiting Anomaly Detection [102]	✓		✓	✓	
	Fuzzy Logic SDN IDS [103]	✓		✓	✓	✓
DoS/DDoS Protection	Lightweight DDoS [104]	✓		✓	✓	
	CONA [105], DDoS Defender [106], DDoS Blocker [107]	✓		✓	✓	✓
Security Middleboxes - Architectures and Services	Slick [108], FlowTags [109]	✓	✓	✓	✓	✓
	SIMPLE-fying Middlebox [110]	✓		✓		✓
	OSTMA [111]			✓	✓	✓
	Covert Channel Protection [112]	✓		✓	✓	✓
	OpenSAFE [113], CloudWatcher [114]	✓	✓	✓	✓	
	Secure-TAS [115]				✓	✓
	Secure Forensics [116]			✓	✓	✓
AAA	AAA SDN [117]			✓	✓	✓
	C-BAS [118]	✓	✓	✓	✓	✓
Secure, Scalable Multi-Tenancy	vCNSMS [119], OpenvNMS [120], Tualatin [121]	✓		✓	✓	✓
	NetSecCloud [122]	✓		✓		

Collect,Detect,Protect

总结见表10

TABLE X
PROBLEM AND SOLUTION PROPOSED FOR *Collect, Detect, Protect* NETWORK SECURITY ENHANCEMENTS IN SDN

Research Work	Problem/Goal	Proposed Solution
Combining OpenFlow/sFlow [88]	Avoid control plane overload (DoS) during OF statistics collection	SDN IDS/IPS based on Statistics Collection, Anomaly Detection and Anomaly Mitigation Modules
Active Security [89]	Dynamic and Programmable Security Infrastructure	Network Feedback Control providing integrated security
L-IDS [90]	Intrusion detection for embedded mobile devices	Use OF SDN to detect traffic anomalies and reconfigure network
NetFuse [91]	Prevent data center network overloading problems	OF proxy device to detect overload behaviour based on flow aggregation
OrchSec [92]	Overcome limitations of existing network security applications	Orchestrator-based SDN architecture to develop security applications
Cognition [93]	Enhance the security level of SDNs by applying cognitive functions at the app plane	A cognitive module implemented in the app plane (via dynamic multi-objective optimization)

[88]结合OpenFlow和sFlow进行异常检测，目的是为了防止Control plane过载。
[89]一个完 整的反馈控制方法的动态可编程架构。
[90]L-IDS，利用SDN进行异常检测并重配网络，解决移动设备的入侵检测问题
[91]基于流收集检测过载行为，解决数据中心网络的过载问题
[92]利用多Controller，使用sFlow监控网络，开发利用北向接口通信的应用而不是直接运行在控制器上，克服一些限制。
[93]利用动态多优化实现的一个认知模型，目的是加强SDN的安全。
[89][93]还可以。

Attack Detection and Prevention

总结表11

TABLE XI
PROBLEM AND SOLUTION PROPOSED FOR *Attack Detection (Traffic Analysis) & Prevention (Rule Updating)* NETWORK SECURITY ENHANCEMENTS IN SDN

Research Work	Problem/Goal	Proposed Solution
Resonance [94]	Improve enterprise network attack response capability	Dynamic access control system for securing enterprise networks
AVANT-GUARD [55]	Protect against Control Plane DoS attack and detect and respond to changing flow dynamics	Connection Migration Tool reducing data-control plane interaction and Actuating Trigger to install flow rules
Pedigree [95]	Defend enterprise networks against malware spread and data exfiltration	Traffic tainting (tagging) for flow tracking and filtering
OF-RHM [96]	Frequently change host IP addresses for moving target defense	Random Host Mutation using virtual-to-real IP translation
SDN-MTD [97]	Protect against network reconnaissance, service discovery and OS fingerprinting	SDN-based Moving Target Defense network protection application
NICE:NIDS [98]	Prevent vulnerable virtual machines in the cloud from being compromised	Network intrusion detection, measurement, and countermeasure selection mechanism
SnortFlow [99]	Overcome the latency, accuracy and flexibility issues of current IPS	OpenFlow-based IPS
SDNIPS [100]	A comprehensive IPS solution to reconfigure cloud networking on-the-fly	An SDN-based IPS solution
ScalableIDS [101]	Construct a scalable IDS to cope with increasing volume of network traffic	Scalable IDS architecture with sampling rate adjustment algorithm
Revisiting Anomaly Detection [102]	Use SDN to detect and contain home/home office network security problems	Anomaly Detection Algorithms deployed in NOX controller
Fuzzy Logic Sec. Mgmt. [103]	Use SDN to detect and protect the network from malicious attack	A fuzzy logic-based information security management system for SDN

[94]动态授权控制，提升企业网的攻击响应能力
[55]前面已提到，解决瓶颈问题
[95]对流进行加标签，目的是防预企业网中恶意软件和数据泄露
[96]利用虚拟，真实地址映射来防止地址发现。
[97]通过混淆来保护网络
[98]利用基于OF的入侵检测监控网络流量，保护云端虚拟机
[96,98]可以看一看

DDoS 保护

总结表12

TABLE XII
PROBLEM AND SOLUTION PROPOSED FOR *DoS/DDoS Protection* NETWORK SECURITY ENHANCEMENTS IN SDN

Research Work	Problem/Goal	Proposed Solution
Lightweight DDoS [104]	DDoS attack detection	Statistical information with self-organizing maps to classify traffic as normal or malicious
CONA [105]	DDoS attack detection and response in content-oriented network	Rate and pattern of content requests are analysed to detect DDoS attack
DDoS Defender [106]	DDoS attack detection and response	Use OF and LISP to detect and drop DDoS traffic based on traffic volume
DDoS Blocker [107]	Overcome difficulty of detecting and blocking DDoS attack by botnet	DDoS blocking scheme for SDN-managed network

[104]通过统计流并发送给Controller来计算异常还是正常从而检测DDoS攻击检测
[105]当对一个主机的请求超过一个给定阈值时认定为攻击，Controller对发送率限制从而进行阻止攻击传播
[106]利用OF和LISP基于流容量进行异常检测
[107]在Controller里运行应用监控流并检测异常

Security Middlebox

总结表13

TABLE XIII
PROBLEM AND SOLUTION PROPOSED FOR *Security Middlebox* NETWORK SECURITY ENHANCEMENTS IN SDN

Research Work	Problem/Goal	Proposed Solution
Slick [108]	Provide richer match/action set for improved network traffic management	Slick Controller and Middleboxes dynamically place network functions and direct traffic to those functions
FlowTags [109]	Ensure consistent network policy enforcement in the presence of middleboxes	Middleboxes add tags to outgoing packets to provide correct context
SIMPLE-fying Middlebox [110]	Efficient middlebox-specific traffic steering	Tag and tunnel packets between middleboxes
OSTMA [111]	Overcome the problem of QoS guarantee in security traversal	Dynamic security traversal scheme with middlebox addition for OF networks
Covert Channel Protection [112]	Restrict covert channels	Multi-level security network switch using OF filter
OpenSAFE [113]	Line-rate network traffic direction through security monitoring applications	Use OF to implement ALARMS policy for specifying and managing paths
CloudWatcher [114]	Provide monitoring services for cloud networks	SDN Application to control and direct network flows through security services
Secure-TAS [115]	Use SDN to protect the internal network from attack	Secure traffic analysis system to trace malicious activities on internal networks
Secure Forensics [116]	SDN-based forensic system to investigate faults including data exfiltration and collusion between compromised nodes	Lightweight middleboxes (Provenance Verification Points) to monitor and track network activity

- **内容目录**

-

-
  - NLP 2
    - GloVe原理
    - NLP
  - algorithm 2
    - Chaotic differential evolutionary algorithm
    - Introduction to Restricted Boltzmann Machines
  - database 2
    - MongoDB安装
    - （胡兵）null值选择，in操作符，为已有节点创建关系
  - java 3
    - java注释
    - java file io
    - 可以运行，但是打包后运行出错总结
  - keycloak 2
    - 将keycloak用于保护rest资源
    - keycloak 基本操作
  - linux 2
    - 常用命令
    - 命令后台运行总结
  - python 3
    - pickle简单使用
    - ctypes数组部分学习记录
    - python多版本并存
  - scrapy 7
    - 动态代理池 centos
    - 动态Cookies池
    - Selectors
    - 爬知乎用户信息
    - Downloader Middleware

- Item Pipeline
- spider
- sdn 8
- A Survey of Software-Defined Networking: Past,Present, and Future of Programmable Networks
- The Road to SDN: An Intellectual History of Programmalble Networks
- R Software-Defined Networking: The New Norm for Networks
- ation in Campus Networks
- Ethane: Taking Control of the Enterprise
- A Survey of Security in Software Defined Networks
- A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges
- net初级
- urity 13
- SDNScore: A statistical defense mechanism against DDoS attacks in SDN environment
- A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)
- Adaptive Performance Anomaly Detection in Distributed Systems Using Online SVMs
- JESS: Joint Entropy-Based DDoS Defense Scheme in SDN
- Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks
- A Deep Learning Approach to Network Intrusion Detection
- Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective
- Automatic test packet generation
- FOCES: Detecting Forwarding Anomalies in Software Defined Networks
- Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks
- An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks
- A Novel Anomaly Detection System to Asist Network Management in SDN Enviroment
- A detection method for anomaly flow in software defined network
- spring,maven相关 3
- spring boot +themyleaf+vue前后端分离
- 备工作
- Spring注解
- springboot 2
- spring boot做安全请求https
- 依赖 spring data jpa
- survey 2
- A Survey of Security in Software Defined Networks
- A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges
- tensorflow 2
- TransD说明文档
- tensorflow 学习率下降用法 tf.train.exponential_decay
- 东大研究生毕设 1
- 毕设实验记录
- 同义词发现算法论文 4
- Graph-based Word Clustering using a Web Search Engine
- 吴云芳_基于图的同义词集自动获取方法
- 宋文杰,顾彦慧,周俊生,孙玉杰,严杰,曲维光.多策略同义词获取方法研究):
- 陆勇. 基于词典注释的汉语同义词自动识别[A].
- 未分类 13
- 在此处输入标题
- 在此处输入标题
- HTTPS原理
- 欢迎使用 Cmd Markdown 编辑阅读器
- latex数学公式学习
- 日报记录
- 中文文本分类
- 词林
- JSON
- 医学知识
- TF-IDF
- Spring第一个 hello
- neo4j 创建关系，多标签,where,delete,remove,set,match,return,create,merge,union,sorting,limit,skip

搜索 EggGump 的文稿标题，

以下【标签】将用于标记这篇文稿

下载客户端

关注我们

报告问题

联系我们

添加新批注

保存 取消

在作者公开此批注前，只有你和作者可见。

保存 取消

修改 保存 取消 删除

- 私有
- 公开
- 删除

查看更早的 5 条回复

回复批注

×

通知

取消 确认