回家前：

阅读论文：

1. A Survey of Software-Defined Networking: Past,Present, and Future of Programmable Networks

SDN的发展简介以及以后可能会遇到的困难

2 The Road to SDN: An Intellectual History of Programmalble Networks

这里面介绍的是可编程网络到SDN的发展历程

3 ONF WHITE PAPER Software-Defined Networking: The New Norm for Networks

Openflow白皮书，主要介绍openflow架构

4 OpenFlow: Enabling Innovation in Campus Networks

Openflow的提出，是对中心化网络的一个升华和抽象化，再进一步抽象就叫做SDN

5 Ethane: Taking Control of the Enterprise

Openflow的前身，中心化网络的提出

6 Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks

GPS欺骗攻击的一个预防策略：攻击者的一个发现方法（缺点：至少要有两个aircraft被攻击才能大致准确地找到攻击者位置）。

Mininet与openflow的简单学习

回家后至今：

7 JESS: Joint Entropy-Based DDoS Defense Scheme in SDN

提出一种基于熵检测DDos攻击的方法，内容比较完善，复杂度分析地也比较好

大致了解mininet，Open VSwitch

8 Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks.

借助实现了openflow协议的switch在传统网络中进行异常检测。

9 Efficient Anomaly Detection And Mitigation In Software Defined Networking Enviroment

写得比较水

10 An SDN-Supported Collaborative Approach for DDos Flooding Detection and Containment

本篇提出的一个架构，实验部分做得比较具体。

Monitor 监控，将可疑ip发给correlator,correlator查database，若未注册而丢弃该ip中的所有package(只能检测ip spoof)

11 Software-Defined-Networking-Enabled Traffic Anomaly Detection and Mitigation。

提出一种特征提取算法，并结合聚类对攻击进行分类，与当前现有的特征提取算法进行比较，但是实现部分怎么实现讲得模糊。

13 An Analysis of Using Reflectorsfor Distributed Denial-of-Service Attacks

讲解了DDoS攻击，再讲解基于reflector的DDoS攻击，最后基于各种网络协议的字段进行挨个分析，讲解哪些字段容易受到attacker的利用从而进行攻击。

12 Network Anomaly Detection:Methods,Systems and Tools

一篇很长的文献综关于传统网络异常检测的文献综述

2月24:

阅读论文：

1. Network Anomaly Detection:Methods,Systems and Tools，

这是一篇基于传统网络的IDS研究综述，其中对对入侵检测的方法进行分类并总结并对每个类型的方法进行优缺点的总结，对各种距离测量方法进行总结，对所用到的工具进行总结，对所使用到的数据集进行总结，对实验中用到的评估方法进行总结。

2．a detection method for anomaly flow in software define network

基于knn的一种改进算法提出了一个应用于SDN的异常检测算法。

3．A Novel Anomaly Detection System to Asist Network Management n SDN Enviroment

提出一种辅助网络管理的异常检测系统，算法运行在controller

4．An Analysis of Using Reflectorsfor Distributed Denial-of-Service Attacks

讲解了DDoS攻击，再讲解基于reflector的DDoS攻击，最后基于各种网络协议的字段进行挨个分析，讲解哪些字段容易受到attacker的利用从而进行攻击。

5．FOCES:Detection Forwarding Anomalies in Software Defined Networks.

正在看的一篇

3.8-3.15

1. A Deep Learning Approach to Network Intrusion Detection

提出NDAE+RF方法进行异常检测，主要是利用Auto-Encoder进行特征提取，将提取到的特征传给RF进行分类，在DKK CUP'99和NSL-KDD数据集上进行测试.

2. Automatic test packet generation

一种自动生成测试包来测试路由规则的算法，提出如何进行选择最小的测试包对网络进行测试，从而找到出错的规则。

3. Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective

本文使用受限玻尔兹曼机进行特征提取，并使用SVM对提取到的特征进行分类，还提出了一个实现框架，并在TIET，KDD'99，CMU数据集上进行实验。

3.26-3.29

1. JESS: Joint Entropy-Based DDoS Defense Scheme in SDN

利用混合特征计算熵，从而找出异常熵作为依据，所有有该异常熵的流便定义为异常流。

<https://www.zybuluo.com/EggGump/note/1409872>

2. [SDNScore: A statistical defense mechanism against DDoS attacks in SDN environment](http://www.researchgate.net/publication/319472896_SDNScore_A_statistical_defense_mechanism_against_DDoS_attacks_in_SDN_environment)

利用混合熵的方式进行攻击检测，是1的前身。

<https://www.zybuluo.com/EggGump/note/1440438>

3. A Survey of Security in Software Defined Networks

SDN安全综述，结SDN的安全问题近年研究进行总结

4.1-4，5

1. SDN-RDCD: A Real-Time and Reliable Method for Detecting Compromised SDN Devices

本文目标是通过一个审计器检测被挟持的SDN设备，实验结果并未与其他进行比较，因为他声称自己的正确率有100,但是并没有提供检测具体哪个设备被挟持。

<https://www.zybuluo.com/EggGump/note/1444485>

2.AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks

本文对of作两个改进：1,利用\*Connection Migration\*对TCP连接进行中继，使其可以在data plane过虑掉未完成的TCP连接；2,\*actuating trigger\*改进OF协议，使其支持条件流表，即在某一特定条件下激活流表规则以达到网络监控的目的。

<https://www.zybuluo.com/EggGump/note/1445670>

3.SPHINX: Detecting Security Attacks in Software-Defined Networks

本文很不错，写得十分详细，很贴近实用，作者是精通OF协议的。

本文目的提出一种检测已知和未知网络攻击并可实时发出警告，自动学习新的网络行为。

<https://www.zybuluo.com/EggGump/note/1447915>

4. Gibbs Sampling

本算法的本质是产生以特定概率产生随机数。

<https://www.zybuluo.com/EggGump/note/1442084>

4. Tool support for the evaluation of anomaly traffic classification for network resilience

觉得本文一般，作者对PReSET这篇论文提出的工具进行修改。PReSET是一个对网络可恢复力评估的一个工具，本文利用它来进行流量分类算法的评估

<https://www.zybuluo.com/EggGump/note/1449455>

4.11

1.Athena: A Framework for Scalable Anomaly Detection in Software-Defined Networks

本文相当于一个框架手册，该框架作用为：一个分布式SDN弹性异常检测应用，它提供高抽象的API，可以使管理员以最小的编程代价布署异常检测应用。

<https://www.zybuluo.com/EggGump/note/1452813>

2.提出Header Space Analysis来分析错误类别如：Reachability Failure,Forwarding Loops,Traffic Isolation,Leakage problems。我们装将包头视作一系列位的连接,每个都是一个$\{0,1\}^L$点，L是包头最大长度，而网络box的转换视作将点空间中的一个点转换为另一个（或一些）

<https://www.zybuluo.com/EggGump/note/1453652>

3.对网络可能受攻的情况进行总结。

<https://www.zybuluo.com/EggGump/note/1453209>