Ripple: A Programmable, Decentralized Link-Flooding Defense Against Adaptive Adversaries

(Usenix Security ‘21)

动机：缓解链路泛洪攻击

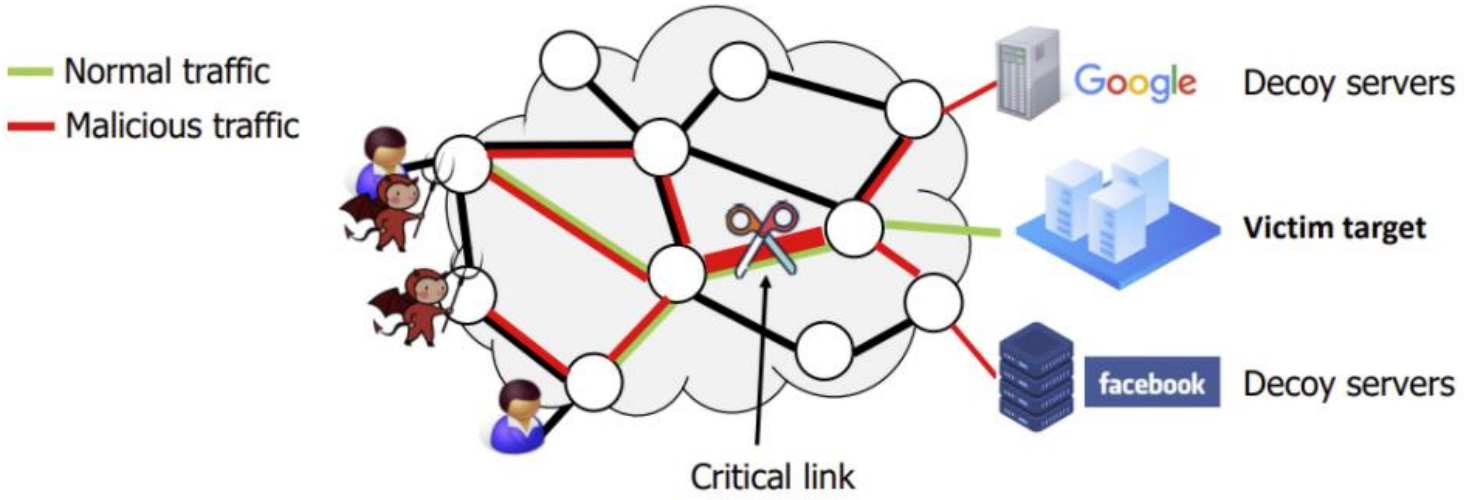
链路泛洪攻击：一种典型的DDoS攻击，攻击者通过botnet或者其他方式向关键链路制造大量流量瘫痪关键链路的交换机。

攻击者视图：

* 构建网络拓扑，识别关键链路（Critical Links）；

* 找到一条，由一系列服务器（被称为decoy，诱饵、托儿）共享的关键链路；

* 发送大量请求给decoy以阻塞关键链路；



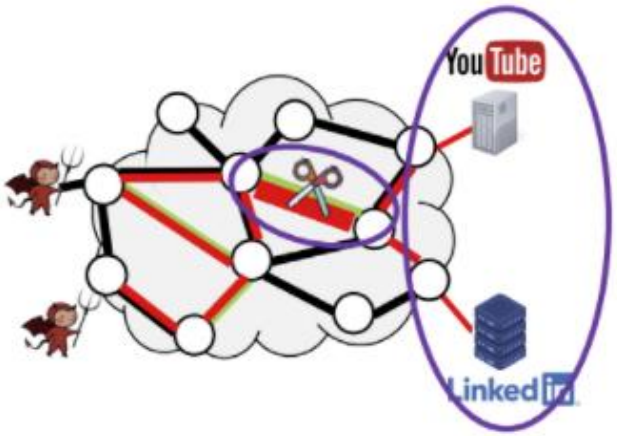
动机：缓解链路泛洪攻击

这种攻击的危险性在于：

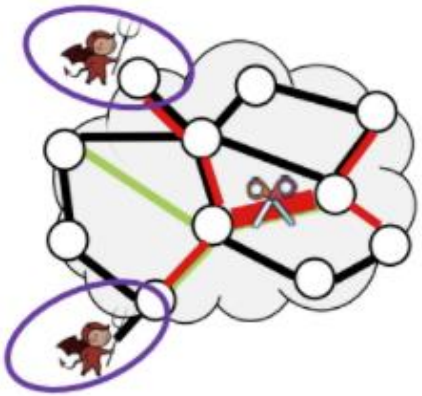
* 攻击者可以通过阻塞关键链路交换机，从互联网中删除边缘网络，边缘网络甚至无法感知攻击（因为是针对链路的）；

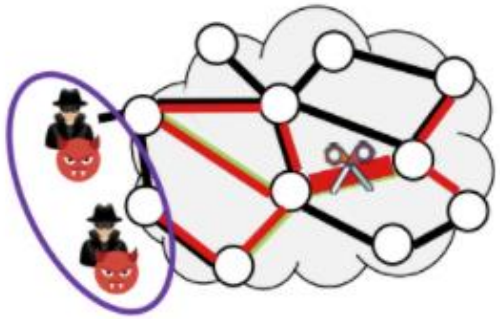
* 受害者会经历严重的网络性能下降甚至断开连接；

* Adaptive Adversaries：动态就动态在攻击者在攻击时，可以随意变换目标的链路（Link）和流量类型；



Different links


Different botnets


Different traffic patterns

之前的工作及其局限

基于SDN的防御手段

SDN强调集中式控制，防御算法作为集中控制器中的应用程序运行：

* SDN的可编程控制性是实现的关键；

* 防御算法运行时接收来自交换机的OpenFlow消息，构建一个全局防御视图，并计算新的防御决策（比如丢掉特定方向发来的packet，或者将流量导向负载较小的链路）；

局限：

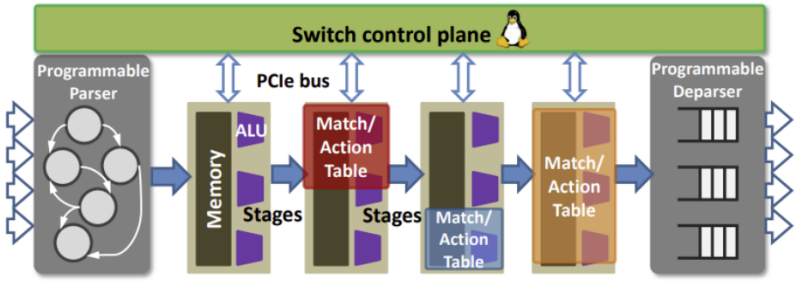
* SDN对网络状况的反馈可能需要多个RTT（收集数据→计算防御策略→应用到各个交换机）；

* 这种动态的对手可以迫使防御程序总是根据陈旧的数据采取行动，这反过来会导致不那么成功的防御，甚至是额外的伤害；（被称为crossfire攻击，Min Suk Kang, Soo Bum Lee, and Virgil D Gligor. The crossfire attack. In Proc. S&P, 2013.）

关键问题

如何对抗自适应的敌手?

关键技术：可编程交换机



* 可以使用高级语言编程（P4）；

* 可以以线速度（linespeed）运行，高达Tbps;

* 现有工作通常将该方案用在单一交换机上;

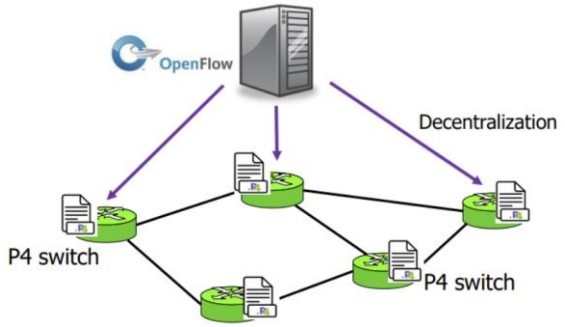
关键思想：去中心化的防御

在可编程交换机上使用去中心化防御
* 反馈回路得到加强（收集数据->分析->选择策略->应用->收集数据）；

* 可以检查每一packet，不再需要对流量采样;

* 以硬件速度运行，比基于SDN控制器的防御要快;

因此该方法可以显著地缓解快速自适应攻击



关键问题 - 2

交换机只能探测本机的数据包，怎样才能让每一台交换机都收到全局的网络视图呢?

解决方案：去中心化地构建一个“全局”视图

* 需要一种语言来描述不同攻击发生时的全局视图

* 需要一个编译器来生成交换机程序

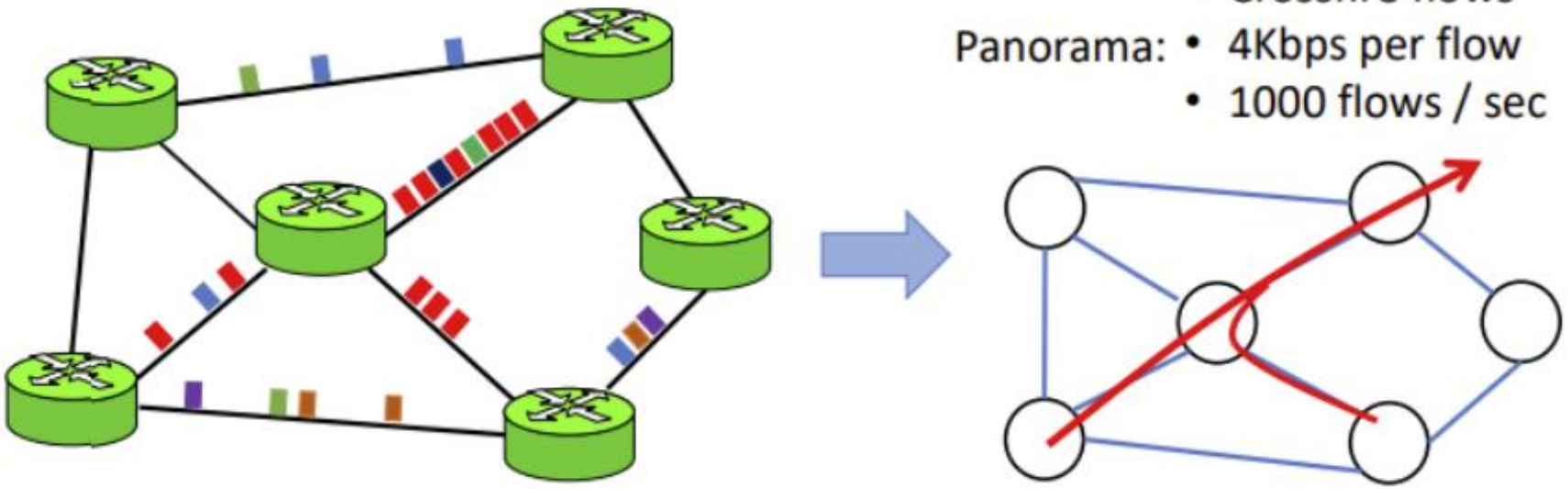
* 一个运行时协议来构建完整的全局视图

全局视图（全景视图）

将实际网络中的链路抽象为一个全局图，它描述的是与链路防护相关的信号类型。

* 捕捉了一系列整个网络的全景快照（链路和链路负载被抽象成键-值）；

* 根据一系列攻击的特征指定防御策略;



zip(key, l1, l2)	按键连接两个列表l1和l2

不同攻击类型的单机检测示例

*以防御 coremelt 攻击为例，攻击者会向链路发送重UDP负载或者假的TCP流

作者还描述了如何使用Ripple编写防御crossfire、SPIFFY攻击，还给出了几种全新的防御策略：

- 阻断向受害者产生高速率、短寿命脉冲波的流
- 区分普通拥塞攻击和链路泛洪攻击，检查拥塞是否对所有IP范围的影响大致相同，或者是否有受害IP的丢包率明显较高；传送到受害IP范围的流量会被重定向到拥塞最少的链路，以获得特别保护
- 保护关键网络；运营商可进一步订定上述"受害者"防御政策，特别保护重要的客户
- 分别执行多个防御攻击策略

检测：检测策略在网络的任何地方寻找显著的拥塞(>80%的链路利用率)；

分类：如果出现严重拥塞(超过3条拥塞的链路)，将触发分类。reduce行用来聚合（统计）每个源IP地址发送来多少流量，然后filter行将可以的源IP列表过滤出来；

缓解：对这个源IP发来的packet，进行一个包的丢弃；

实现——从单机到去中心化地构建全景

1.利用了可编程交换机的特点，全局视图使用键值数据库表示，实现了上面提到的原语;

2. 交换机之间的去中心化沟通：运行分布式协议来实现视图同步

本地分片将被这个同步协议携带到所有交换机，交换机将基于全景定义构建一个全景视图

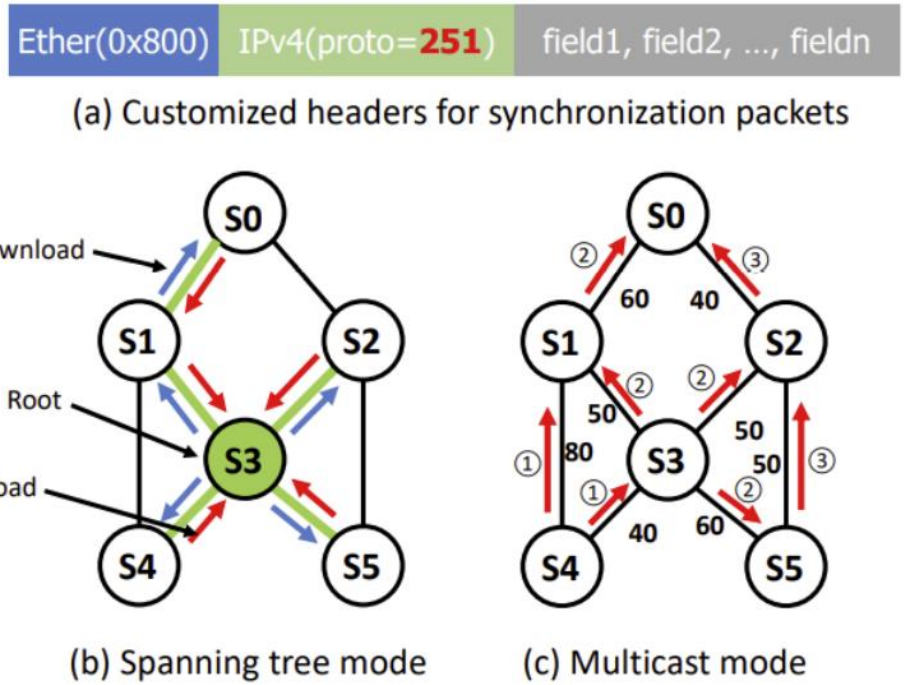
运行时协议在每个时间窗口执行一次沟通

*每个交换机生成一个本地分片;

*与其他交换机交换分片;

*当所有的片段交换完毕，协议执行完毕;

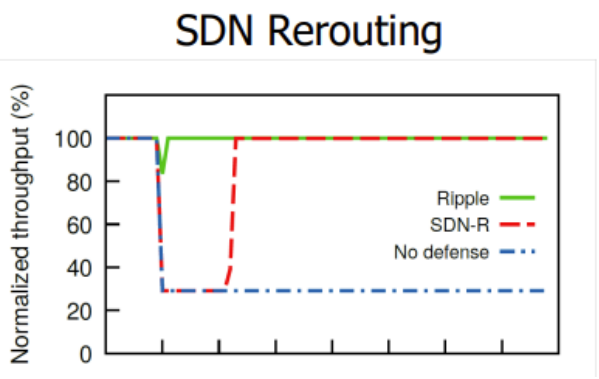
实现——从单机到去中心化地构建全景

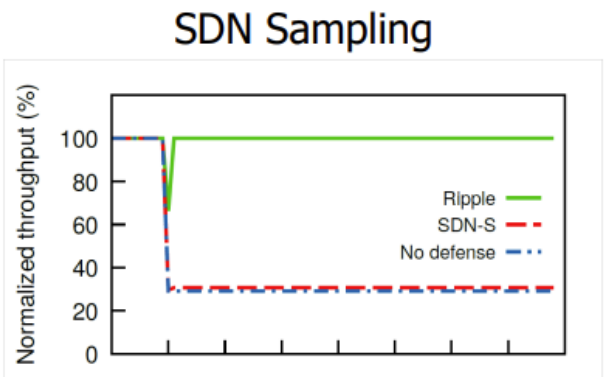


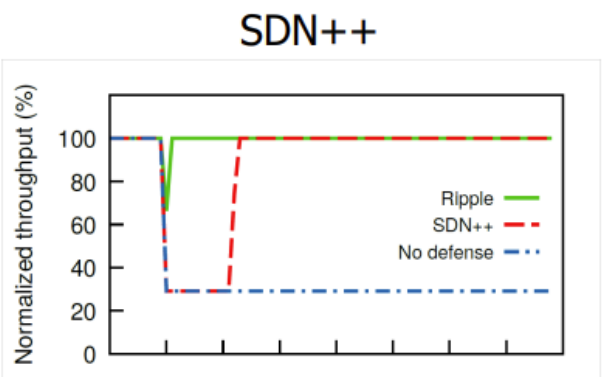
- 生成树 -- 交换机运行一个生成树协议来标识一个根交换机，所有其他交换机使用这个根作为汇聚点

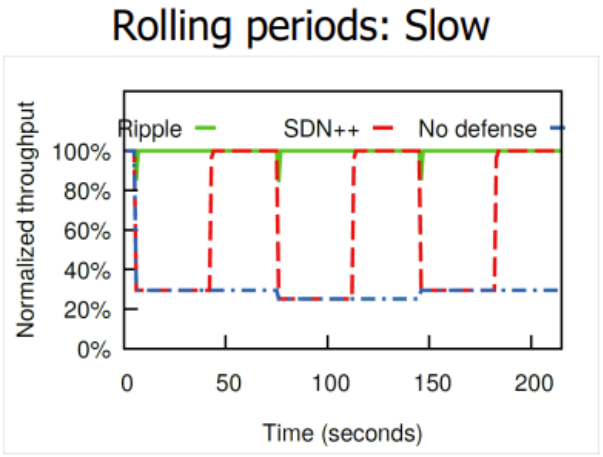
- 组播（multicast）-- 所有交换机组播片段给所有邻居，每个交换机将接收所有其他交换机的所有片段

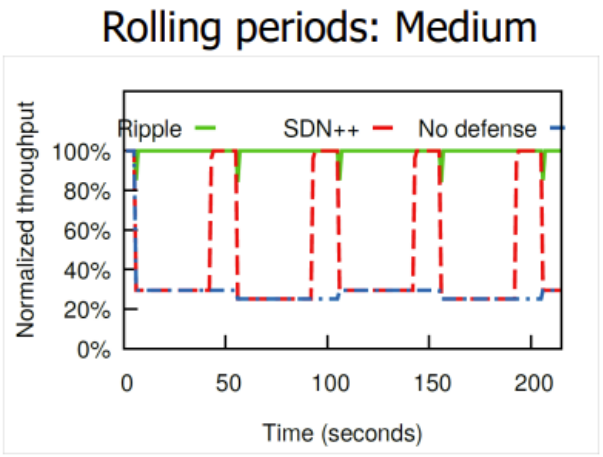
测试 – 评估

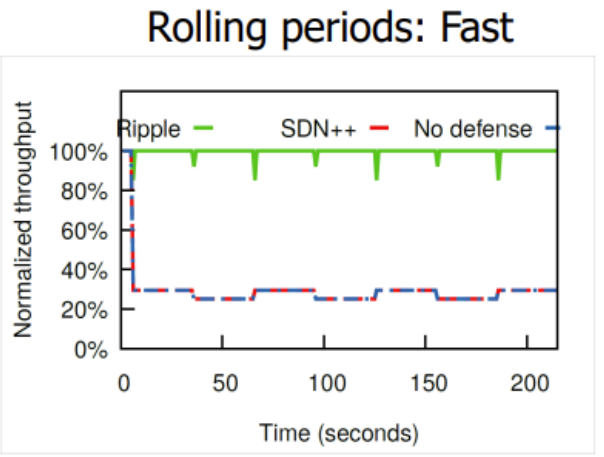












Adaptive attacks with decreased rolling periods

结果显示，在缓解链路泛洪和自适应攻击方面，Ripple有立竿见影的效果

想法

在敌手模型为链路泛洪的情况下

也许可以结合一下军工网络的特殊需求，改进这个方法