

中文题目：一种高效针对软件定义网络中 **Data-To-Control-Plane** 饱和和攻击的防御方案

中文长摘要：

1、研究背景（context）：

在软件定义网络（Software-Defined Networking）环境中，当控制平面遭到数据-控制平面饱和攻击（Data-to-Control-Plane Saturation Attack，以下简称饱和攻击）而过载时，整个网络系统都可能会停止运行。饱和攻击是一种拒绝服务攻击。在这种攻击中，恶意主机通过发送大量的 Table-Miss 数据包以耗尽控制平面资源。本文给出的策略旨在监测和缓解饱和攻击带来的威胁。本文是我们会议版本文章[1]的扩展版。

2、目的（Objective）：

当前，尽管在此类型问题上有许多类型的研究，但是仍有许多问题亟待优化。一方面，集中化的缓解策略影响了合法交换机和合法流量。在一些典型的方案中[2]，一部分合法流和攻击流均要被导入至缓解中心。这导致了原本未受到攻击的交换机性能下降，并且导致了其他用户的合法流延迟变长。本文中，我们使用了分布式的缓解策略。通过在边缘网关部署虚拟功能体形式的缓解代理

（Mitigation Agent），以及对来自不同端口的攻击流量采取不同的策略，我们减少了受影响的交换机和合法网络流的数量。

另一方面，当前的解决方案大多面临着较长的恢复延迟。通过我

们的研究，我们发现长时间的恢复延迟来自于控制平面中遗留的攻击流（Remaining Attack Flows）。而这些遗留攻击流的清理工作往往被先前的工作所忽视了。为减少系统恢复延迟，我们提出了一个名为 Force_Checking 的新颖功能模块，该模块使整个系统能够快速清理剩余的攻击流并更快地恢复。

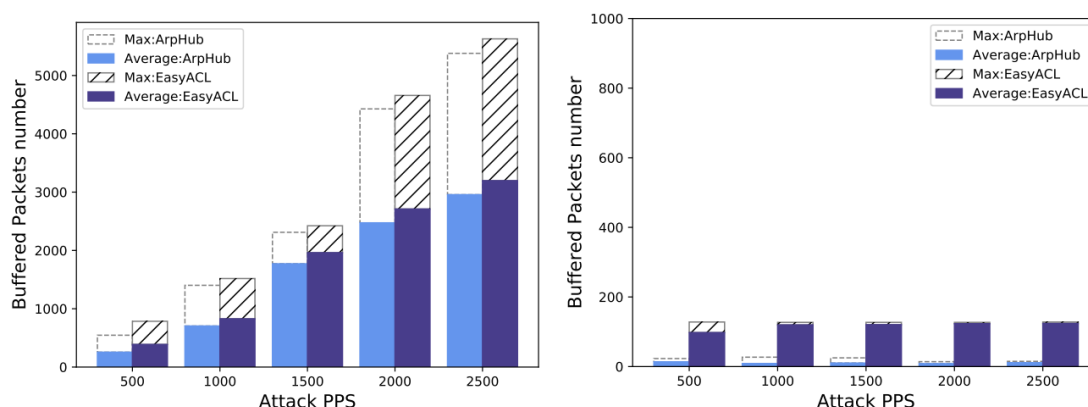
3、方法（Method）：

为了解决这些问题，我们提出了 LFSDM，一种快速恢复饱和攻击检测和缓解框架。系统的架构如图所示。LFSDM 分为三个部分。第一部分是部署在 SDN 控制器上的 App，其中包含 Mitigation Server 和 Attack Detector，它们负责攻击的监测和缓解策略的确定。第二部分是部署在各个边缘网关上的 Mitigation Agent，它负责对攻击流做一线的过滤，并且保证合法流量的通信。第三部分是部署在控制器平台内核上的 Force Checking 模块，它负责在攻击发生后快速清理攻击流量保证系统快速恢复。

4、结果（Result & Findings）：

- （1）我们在 SDN 模拟环境中进行了实验。首先，我们通过实验验证了 Remaining Attack Flows 对网络恢复时间的影响，如图（a）所示，可以看到随着攻击流量增大，系统的 Remaining Attack Flows 显著增加。如图（b）所示，在我们部署了 Force_Checking 模块后，系统的 Remaining

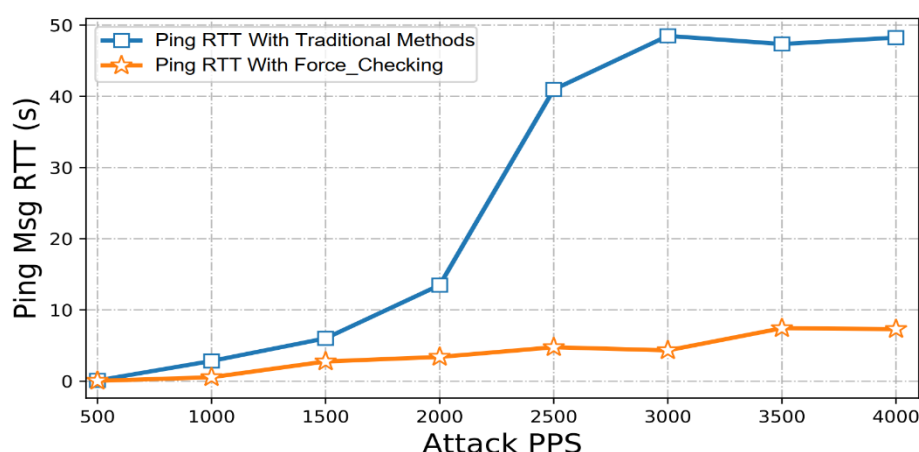
Attack Flows 数量被显著的减少了。这对于释放系统资源、减少交换机、控制器负载都具有较大的意义。



(a) Without Force_Checking

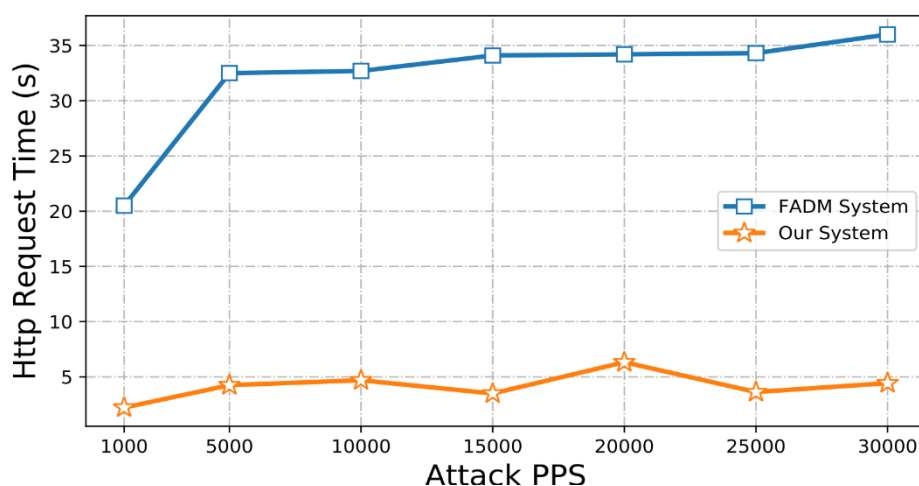
(b) With Force_Checking

(2) 然后，我们验证了 Force Checking 模块对系统恢复时间的增益。如下图，蓝线阐述了在传统方法下的情况，系统的恢复时间随着攻击速率的增长显著。但是在使用了 Force Checking 模块后，系统的恢复时间稳定在 8s 以下，呈现平缓态势。我们的工作 1000 到 4000 PPS 的攻击速率下节省了 81% 的系统恢复时间。

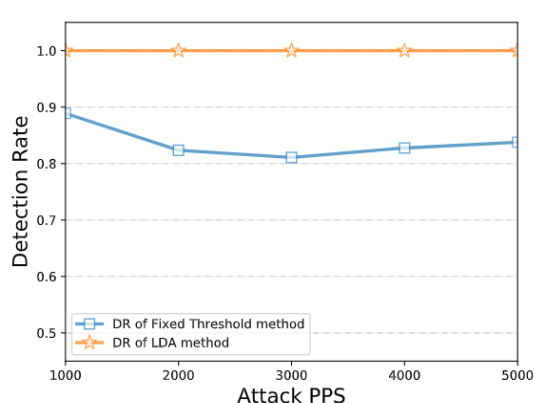


(3) 接着，我们将我们的方案和 FADM[2] 方案进行了对比，对比结果如下图所示，相比 FADM 系统，我们的方案在 5000 -

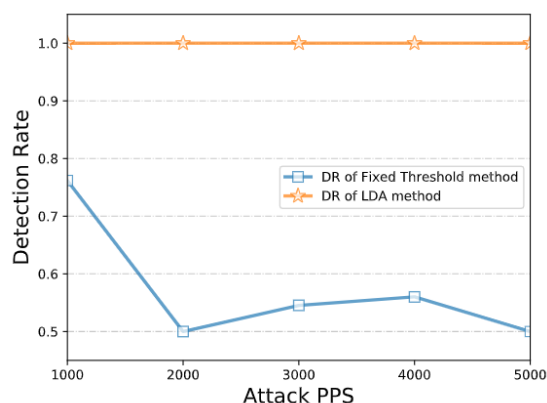
30000PPS 的大规模攻击速率下成功减少了 87% 的系统恢复时间。



(4) 最后，我们和我们自己的会议版本[1]进行了监测效率的对比。在本文中，我们通过使用 LDA (Linear Discriminant Analysis)、降噪两种方式，有效地提升了监测的准确率。下图表示了在不同背景噪声、攻击频率下的实验结果。在我们的解决方案中，攻击的误报率几乎可以忽略不计。



(a) DR under 1M traffic



(b) DR under 10M traffic

5、结论 (Conclusions)：

本文提出了一个高效的针对 SDN 网络中饱和攻击的监测、缓解方案。在监测方面，我们使用了 LDA 分析方法，结合了 PACKET_IN 消息的速率和控制信道占用分布（CCOR）熵分析方法来进行攻击监测。在缓解方面，我们使用了分布式的缓解代理节点来保护控制信道；并创新地提出了缓存攻击流清空模块（ForceChecking）来进行攻击流量的快速清理，以实现快速恢复。

模拟环境的实验表明，相比我们会议版本的文章[1]，监测的准确率得到了有效地提升。相比 FADM[2]，我们减少了约 87%的系统恢复时间。

参考文献：

- [1] X. Huang, K. Xue, Y. Xing, D. Hu, R. Li and Q. Sun, "FSDM: Fast Recovery Saturation Attack Detection and Mitigation Framework in SDN," *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2020, pp. 329-337, doi: 10.1109/MASS50613.2020.00048.
- [2] D. Hu, P. Hong, and Y. Chen, "FADM: DDoS flooding attack detection and mitigation system in software-defined networking," in *Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2017, pp. 1-7.