SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks

Pedro Manso 1, José Moura 2,\* and Carlos Serrão 3

一、整体描述：

所提出的系统使用DDoS攻击检测和缓解机制，其在客户端的SDN架构内集成入侵检测系统（IDS），用于家庭或组织网络场景。

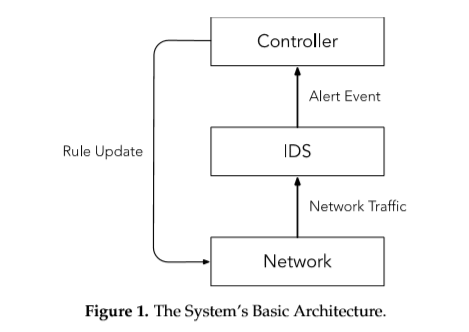
二、架构组件：

系统通过三个基本架构组件（图1）之间的循环控制进行操作：网络，IDS和控制器。

（1）网络代表所有数据流量以及可能发起潜在DDoS攻击的位置。

（2）IDS代表我们的DDoS攻击检测机制，它分析网络上交换的所有流量。当IDS检测到正在进行的DDoS攻击时，IDS会通知控制器。

（3）当控制器被ID通知后，控制器将一些新的流规则的数据路径传输到网络设备，以便尽快恢复网络的正常运行。



三、概念模型

（1）概念说明

图2显示了当前工作的概念模型。我们的提议结合了SDN控制器和入侵检测系统（IDS）提供的功能。通过聚合这两个实体，我们获得了一个基于SDN的IDS监视器。

（2）数据包按流分类

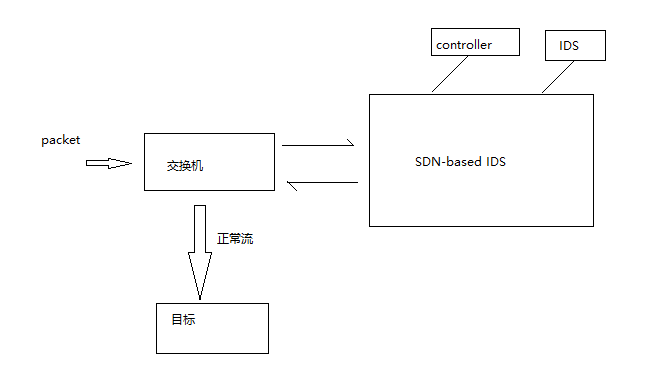
到达系统的每个新数据包（即在交换机端口中接收到的数据包）都被分类为属于一个流并向系统发出请求。

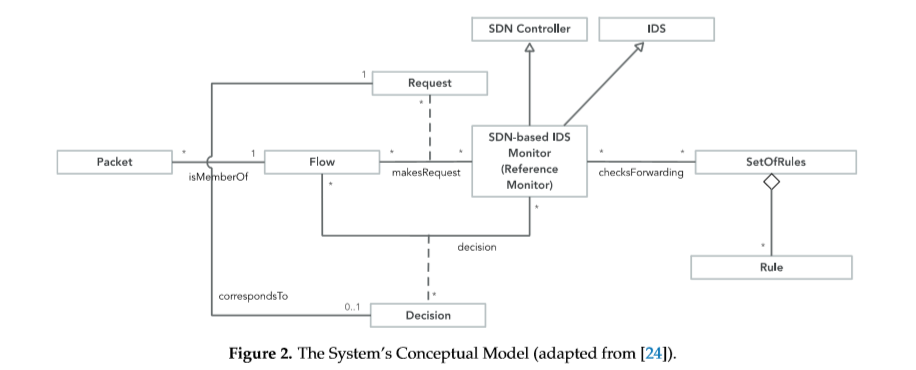
（3）交换机做出决定

以这种方式，交换机根据与数据包所属的流相关联的规则处理所接收的数据包，从而做出决定。

（4）交换机与控制器的交互

在这种情况下，交换机最初没有针对该流的任何规则，然后，交换机将其请求到SDN控制器。 SDN控制器在交换机中安装正确的流规则，只有当数据包属于“行为良好”流时，该规则才允许数据包进入其目标。 否则，在交换机中安装删除规则。IDS使用一组预先配置的规则将流分类为“好”或“坏”。





四、系统部署：

（1）实际概念模型

我们已经实现了虚拟化系统，该系统在图3中可视化为系统模型的概念验证，如图2所示。我们的系统使用三种不同的虚拟机（VM）：VM A，B和C.

VM A包含两个模块：SDN Ryu控制器和Snort入侵检测系统（IDS）。当特定的基于流的事件发生时（例如，在控制器已经接收到OpenFlow Packet\_in消息之后），SDN Ryu控制器对网络操作进行编程。 SDN控制器通过链路（A）更改网络数据平面，发送OpenFlow转发规则。 Snort IDS是我们基于规则的系统，用于在发生DDoS攻击时“发出警报”。因此，在IDS检测到DDoS攻击后，它会通过Unix域套接字向SDN控制器发送一个警报包，该控制器在图3中显示为链路（D）。

VM B模拟网络域（例如，家庭网络），在该域中可以发起潜在的网络攻击。它运行一个网络仿真器（即MiniNet），它使用一些主机、基于软件的交换机和NAT路由数据部署一个网络域。基于软件的交换机运行OpenFlow协议客户端部分，属于我们测试平台的数据平面。此交换机执行端口镜像，并通过链路（B）将整个流量发送到Snort IDS。 NAT设备用作通过链路（C）访问在线服务器的主机的网关。

VM C代表可能受DDoS威胁攻击的在线服务器。它支持链接（C）通信。

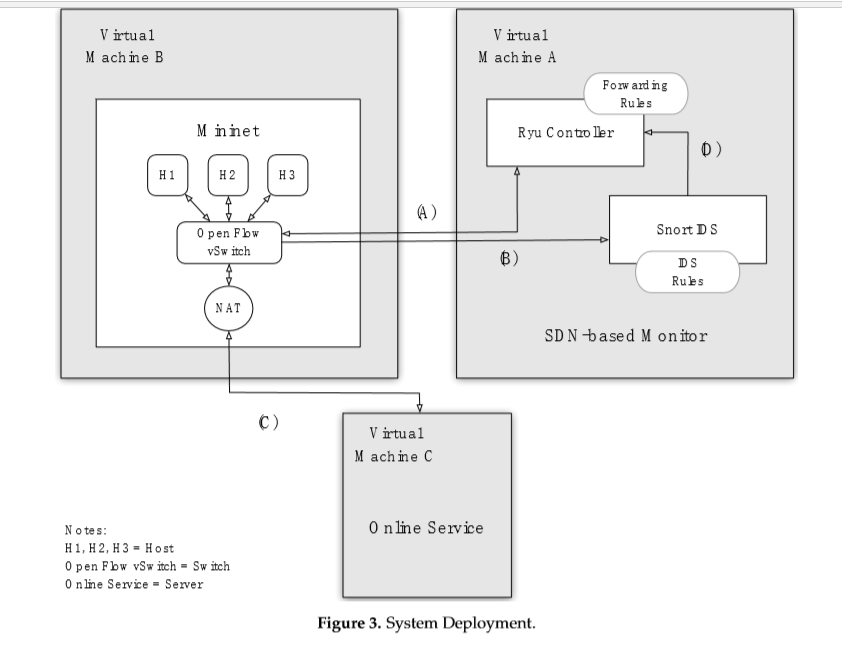
简而言之，我们的测试平台连接如下：

• OpenFlow交换机和SDN控制器之间的双向链路（A），用于交换数据和控制平面之间的控制流量 - 南向应用程序编程接口（API）;

•OpenFlow交换机和SnortIDS之间的单向链路（B），使交换机能够将所有镜像流量发送到IDS进行进一步分析;

•双向链路（C），它将本地网络域（即VM A，B）连接到远程服务;

•单向链路（D），使Snort IDS能够通过Unix域套接字通过警报数据包通知SDN控制器（即Ryu）正在进行的DDoS攻击。



提示---数据包匹配不匹配的问题：

图4表示我们系统的每个数据包到达OpenFlow交换机的工作流程。

OpenFlow交换机接收该数据包并尝试将其与其表的流量规则进行匹配。如果不匹配，则交换机向控制器请求新流程的新规则。然后，控制器通过发送该流程的新转发规则来响应。或者，如果在交换机内发生匹配，则意味着交换机已经具有针对该接收分组的流规则。在这种情况下，交换机根据现有的流规则转发该数据包。以这种方式，分组遍历NAT网关并继续进行在线服务。

在任何一种情况下，交换机都会将每个收到的数据包镜像到Snort IDS。然后，IDS分析数据包，通过统计功能对其进行处理。这被指定为异常检测。在此特定情况下，统计函数将镜像数据包评估为恶意流的一部分。然后，IDS通知SDN控制器。然后，SDN控制器向交换机发送阻塞流规则。交换机可以通过与新安装的阻止规则相匹配消除所有数据包来缓解攻击。

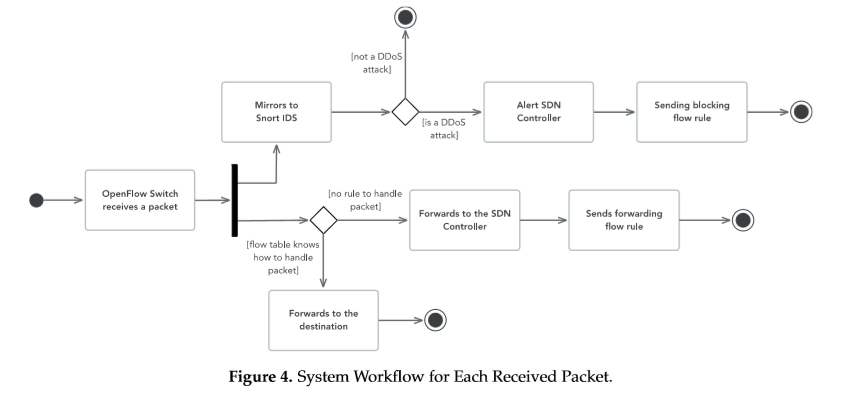


图5给出了有关我们的解决方案如何在存在由用户数据报协议（UDP）泛洪驱动并源自受损内部主机的DDoS攻击的情况下运行的更多细节。我们现在解释数据包在提案中遵循的各种处理步骤。

首先，ICMP Echo Request到达交换机。

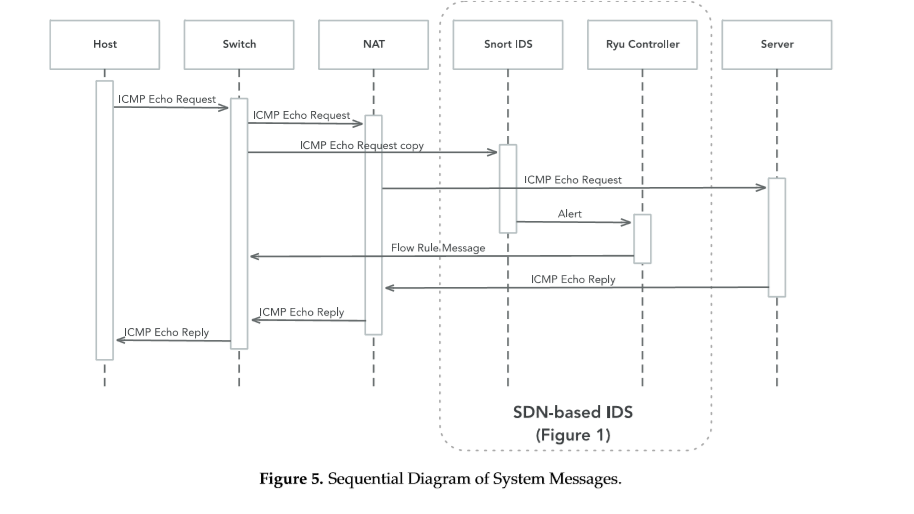
然后，交换机将ICMP Echo Request转发到NAT。

交换机以一定的延迟（这取决于内部交换机结构）将ICMP Echo Request 镜像到Snort ID。

当NAT将ICMP Echo Request 转发到服务器并等待ICMP Echo Reply时，并行的Snort IDS通过统计功能分析ICMP Echo Request。如果Snort认为处理的数据包具有统计上不正确的行为，则该数据包的源节点被分类为恶意主机。然后，IDS通过Unix域套接字通知SDN控制器。

在此之后，控制器通过向交换机发送规则来减轻攻击，该规则阻止来自发现的恶意主机的未来数据包。因此，在接收到先前丢弃的分组规则之后，交换机可以保护网络资源免受恶意分组的影响，以及保护远程服务器免受该攻击。

我们的提议使用端口镜像进行流量监控。不过，由于镜像功能的存在，交换机的处理开销很小。但是，值得注意的是，这种开销在我们的国内情景中并不那么重要。



工具：hping3

为了模拟DDoS攻击，我们使用了发送自定义TCP / IP数据包的hping3工具