Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow

35th Annual IEEE Conference on Local Computer Networks

LCN 2010, Denver, Colorado

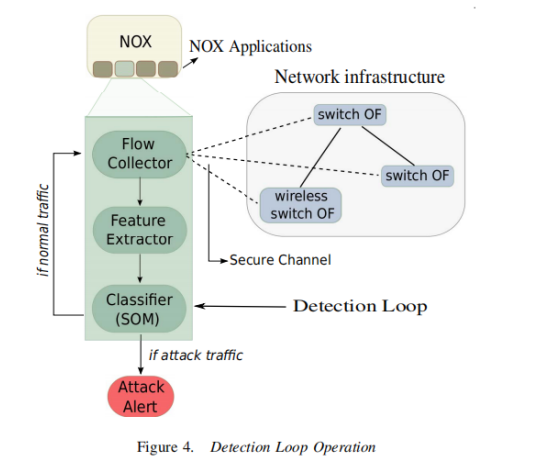
本文提出了一种基于流量特征的分布式拒绝服务（DDOS）攻击检测的轻量级方法，该方法与传统方法相比，具有很低的开销。

在第三节中，我们简要介绍了NOX/OpenFlow和SOM。第四节描述了我们基于SOM流的检测方法的工作原理。

本方法所采用的智能机制是基于自组织映射（SOM）[7]的，这是一种无监督的人工神经网络，具有交通流的特征。我们使用SOM将网络流量分类为正常或异常，即潜在攻击，将流量统计作为SOM计算的参数。

基于轻量级流的ddos攻击检测

我们的分布式拒绝服务（DDOS）攻击检测的轻量级方法包括在预定的时间间隔内监控网络的nox注册交换机。在这段时间内，我们从所有交换机的流条目中提取感兴趣的现有特征，然后将每个样本传递给一个分类器模块，该模块将使用拓扑图中获胜神经元的空间位置指示此信息是否与正常流量或攻击对应。



1. 流量采集模块负责定期从交换机的所有流量表中请求流量输入。此类请求及其相应的答案通过安全通道（即与连接到交换机的主机隔离的通道）传输。

2）Feature Extractor模块接收收集到的流，提取对DDOS洪水攻击检测重要的功能，并将其收集成6个元组，传递给分类器。第IV-B节对这6个元组给出了更详细的解释。每6个元组与它所属的交换机关联一个交换机ID，这很容易通过nox获得。

3）分类器模块分析给定的6元组是否对应于DDOS洪水攻击或合法流量。这种分类可以通过任何统计或学习方法进行。在这项工作中，我们使用SOM作为分类方法。

A.使用Nox/OpenFlow收集流量

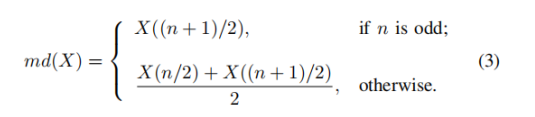
控制器以预定的时间间隔从OF开关收集流量入口。从这个集合中提取重要的特性，将流量分类为正常流量或攻击流量。当收集器从所有通过nox认证的交换机中收集样本时，交换机ID用于帮助分类器模块查明在哪些交换机中检测到ddos洪泛攻击。

默认情况下，在nox注册的每个openflow交换机都会自动添加到检测循环中。但是网络管理员也可以将样本收集限制在那些最相关的交换机上。

由于nox集中管理网络交换机的信息，我们能够从一个ddos攻击的角度监控所有选定的交换机并分析其流量。这种分析是由控制器在我们的方法中完成的。每当一个给定的6元组被SOM归类为攻击时，就会立即向网络管理员发送警报。

1. 提取流量特征
2. 平均每个流包数（APF）：

ddos攻击的主要特点之一是源IP欺骗，这使得跟踪攻击原始源的任务非常困难。副作用是生成具有少量数据包的流，即每个流大约3个数据包。考虑到正常通信通常涉及更多的数据包，我们计算中值。在计算这个值之前，我们根据每个流的包数按升序排列流。然后使用公式3计算中值，其中X是每个流的包数，n是流数



1. 每个流平均字节数（ABF）：

ddos攻击的另一个特点是其有效负载大小，通常非常小，以提高此类攻击的效率。例如，在TCP泛洪攻击中，120字节的数据包被发送给受害者。ABF特性也使用公式3计算为中值，其中x现在表示字节数。

1. 每流平均持续时间(ADf):

类似地，我们建议在流在流表中的持续时间内使用中值。当应用程序之间交换的数 据包数量很少时，此功能会减少误报的数量。方程式3也用于计算，但现在x是交换机中流量的持续时间，n是流量的数量。

1. 成对流的百分比（PPF）：

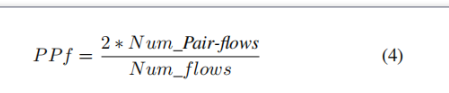
此功能允许验证在某个时间间隔内流中发生了多少对流。例如，对于任意两个流，即流1和流3，检查以下条件以验证这些流是否构成对流。

• 流1的源IP必须等于流3的目标IP；

• 流1的目标IP必须等于流3的源IP；以及

• 两个流必须具有相同的通信协议。

一次DDOS攻击增加了进入网络的单个流的数量，因为它们使用假IP发送数据包。为了计算这种情况的百分比，我们使用公式4。



1. 单流量增长（GSF）：

在泛洪袭击开始时，流量会激增。为了计算这个增长，我们取总流量减去对流量的两倍，然后除以分析流量特征的时间间隔。用公式5计算。



6）不同端口的增长（gdp）：

与ddos攻击生成IP欺骗的方式相同，攻击也可以随机生成端口。因此，我们用方程式6计算这个增长率。



1. 分类

分类器模块是使用SOM实现的。在SOM能够对抽取器模块收集到的任何6元组进行分类之前，需要使用在攻击流量和正常流量期间收集的足够大的6元组样本集对其进行训练。通过这种方式，SOM能够创建一个拓扑图，其中不同的区域表示每种流量。然后，每当训练的SOM被从某些交换机的收集流条目中提取的6元组刺激时，它将能够将其分类为正常流量或攻击流量。