**信息论在网络安全领域的应用**

**——在SDN上基于联合熵的DDoS防御方案**

**一、问题背景**

**1.1 DDoS攻击**

分布式网络攻击通常称为分布式拒绝服务 （DDoS） 攻击[2]，针对网络服务的流量瓶颈来实施攻击。具体来讲，分布式拒绝服务攻击利用了适用于任何网络资源的特定容量限制。DDoS攻击通过向受攻击的 Web 资源发送海量的请求，让攻击者发出的请求超出网站处理请求的能力，以达到阻止网站正常运行、回应、处理合法用户请求的能力。DDoS攻击一般可以被分为容积攻击、协议攻击和应用层攻击以上三大类攻击类型。互联网购物与银行网站、任何依赖提供在线服务的企业或组织、以及一些游戏平台等都是DDoS攻击的重点关注对象。

DDoS的攻击威胁不仅仅局限在影响web资源本身的流畅运行，更是能够在在成功阻碍web资源的正常处理与通信后，结合某些协议手段或者是应用层手段，来实现对服务端更大的破坏。为了能够更好地实现大规模的请求泛洪，在拒绝服务攻击的基础上，攻击者会更加倾向于去选择使用分布式的僵尸网络去进行请求的发送，这既能够在低硬件门槛条件下保证了请求量，又能够降低攻击的可检测性。大量不同IP的请求同时也会扰乱服务端的防御架构，让DDoS防御架构难以甄别合法访问。由于攻击媒介不断变化、攻击规模不断扩大。为了实现理想 DDoS 防护效果，供应商必须在保证网络高效运行前提下，还要保证网络对攻击流量的识别效率。这就给工业界和学界提供了一个困难且有意义的研究方向。

**1.2软件定义网络**

SOFTWARE-DEFINED Networking（SDN）软件定义网络，旨在满足未来互联网不断增长的需求和要求，同时应对当前网络和通信基础设施的挑战。它的本质是网络软件化，基于OpenFlow技术实现提升网络可编程能力，通过分离转发和控制平面实现网络的集中管理，可以像升级、安装软件一样对网络进行修改。

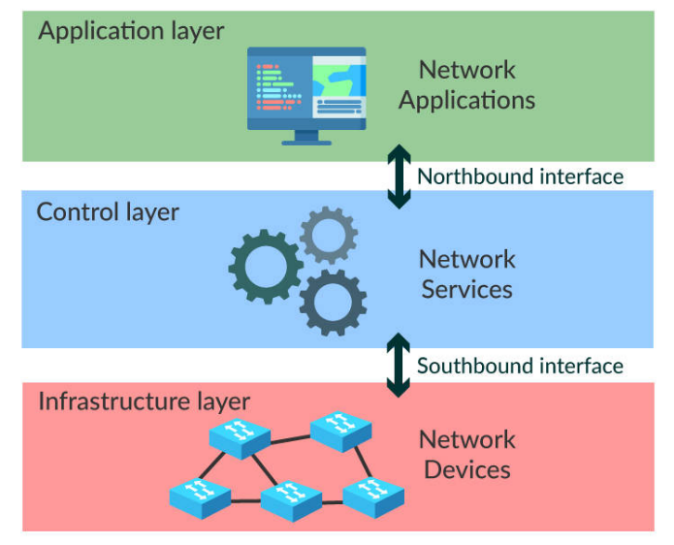


图1

如图1，SDN通过南桥和北桥连接了应用层、控制层和网络设备层，进而组成了软件定义网络。网络虚拟化结合网络功能虚拟化（NFV）和SDN概念，建立了网络软件化和网络切片两个概念。网络软件化组织、管理和重新配置网络组件，而网络切片通过在逻辑和物理上分离网络资源来保证服务的公平共享。然而，这种创新也引入了一些安全漏洞。除了中央管理引入的单点故障问题外，SDN还提供了新的攻击面，例如控制器本身或数据平面元素与控制器之间的连接通信。

**1.3. 现有DDoS防御方案**

针对DDoS的防御方案主要分为了内在网络结构属性的解决方案和基于外部流量属性的解决方案。由于兼容性问题，一般会采用后者作为解决方案。同时，为了提高性能和效率，一般会选择基于统计的方案而不选择基于机器学习的方案。现有的方案仅具有速率限制或检测功能，但缺乏缓解能力。

现有的防御策略有很多。有通过交换机参与提供请求转移与异常流表的插入策略，但存在监控漏洞类型单一等问题；有基于虚拟交换机的覆盖来放大SDN控制平面的方案；有网络交换机监控流量与拥塞状况来判断并限制错误数据流的Flow Fence机制，但该方案仅仅是对速率的一种限制，无法实现完全的攻击阻截；

通过丰富SDN交换机功能来实现更有效的流量决策，如基于分组的统计模型SDN Score，交换机与控制器进行协调，并协同对攻击数据包做出决定；同样使用SDN特性，ArOMA将检测任务和环节任务分别由交换机和控制器执行，该控制器提供快速响应以恢复良性流量性能，但与“能力交换机”概念相关的争议问题也存在于本文。为了缓解与“能力交换机”概念相关的争议问题，基于统计的方案也有提出，比如Giotis等人利用sFlow分组采样将数据收集功能与控制器分离方案，使用信息熵进行异常检测，但这种方法不能保护合法的数据包。

**二、基于联合熵的DDoS防御SDN框架**

为了缓解DDoS攻击，本文将介绍基于熵的防御框架JESS[1]。该框架主要被分为以下三步：常态阶段、准备阶段和主动阶段。

**2.1 常态阶段**

在称为标称阶段的无攻击期间，通过为每个属性对创建标称对配置文件来生成基线信息。其步骤主要包括p级标称剖面获取、联合熵计算两步。

2.1.1 p级标称剖面的生成

标称剖面是表示实体重要特征的一组数据，控制器检查TCP和IP数据包报头的特定字段，包括源IP地址、目标IP地址、源端口、目标端口、协议类型、数据包大小、生存时间值和TCP标志，并将其组成一个无序集合。进一步将这个无序集合拆成k阶子集，其中Ai为二元子集的第i个集合。基于分组的周期确定并处理形成周期的分组。对于标称周期内的α包，解析包的集合可以表示为矩阵E。通过为E中的每个不同元组添加新元素PA C来创建Ai的一对标称剖面N。其中PAC为拥有E属性值的包统计量。根据相应周期中分组的不同属性的数量，从Ai中提取m个集合，组成矩阵作为最后的标称剖面。以表1为例，每个交换机通过计数具有相同属性值的数据包的数量，在无攻击期间为每个对属性生成标称配置文件。

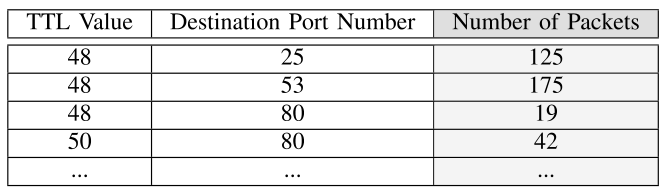


表1

进一步如图3所示，综合统计p个单独的周期，在标称剖面的基础上获取的p级标称剖面。由于每个周期可能有一组不同的，控制器识别每个周期的唯一。在此测量中，每个属性对的不同唯一对的数量表示为。例如图3中的TTL和目的端口数有四组唯一值，则为这里的为4。经过p轮的综合统计，就可以得到各个值和最终的p级标称剖面。为了改进该度量使用了滑动窗口期。

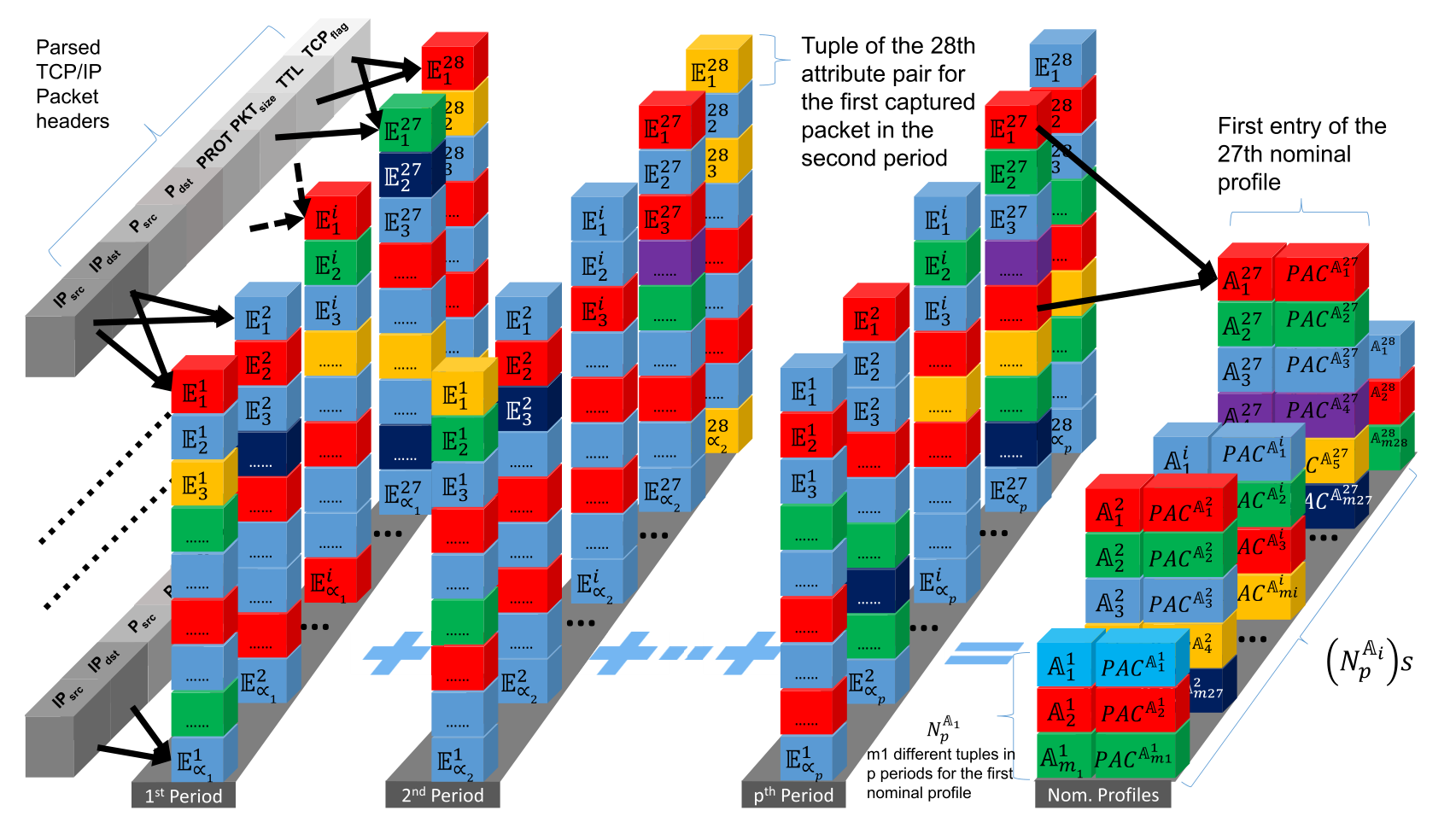


图2

2.1.2联合熵计算：

由于熵显示数据集中的随机性，因此它是DDoS检测的良好指标。当在DDoS攻击者发送的数据包由于攻击特性会相对合法包更为相似，也即熵降低。依据这一规律，防御者就可以基于数据包熵检测到DDoS攻击。

在JESS中，控制器计算每个标称对剖面的联合熵JN，并将其用于检测函数：

接着我们对上式进行归一化处理，得到我们的常态化联合熵：

**2.2 准备阶段**

当业务带宽超过标称阈值时开始准备阶段。交换机开始向控制器发送数据包的报头。控制器为每个属性对生成当前对剖面，并计算归一化联合熵和与标称联合熵的差值。如果其中超过，则系统认为检测到DDoS攻击。然后，具有最大差异对会被当作怀疑对。

**2.3 主动阶段**

在完成准备阶段后，系统就将进入保护阶段。上述机制显然会给交换机造成大量的通信负担，因此这一阶段的开销有所减少。该阶段主要包括五个步骤：

1. 每个周期结束时，交换器将当前剖面SC发送给控制器。
2. 控制器为SC中的每个条目计算相应的分数，并存储至分数表ST。
3. 通过将每对的得分与指定阈值进行对比来区分问题包。首先通过减载算法，根据ST中的积累分布函数确定当前阈值，，结合前一周期的阈值得到阈值结果为：
4. 根据上述阈值和ST生成。如果得分值超过阈值，则认为数据包是恶意的并被丢弃。否则，它将被转发到目的地。
5. 将当前规则表RTC与先前规则表RTP进行比较。只有不同的规则被发送到交换机来更新RT。

**三、实验结论与方案评价**

本文使用MAWI工作组的提供的真实网络流量数据集进行了本次实验，在Mininet的SDN网络模拟器模拟了TCP SYN泛洪攻击、DNS放大攻击、NTP攻击、随机攻击以及混合攻击。

合法数据包和攻击数据包的系统性能。显然，在TCP SYN Flood、NTP和DNS放大攻击期间，JESS的准确性几乎是完美的，能够提供超出95%的正确率，正确的将攻击包区分出来。JESS在随即攻击期间提供约80%的准确度，说明该防御框架能够适应较为复杂且多变的DDoS攻击，如图4。进一步，本文实验了滑动窗口代替固定周期，并取得了更好的结果。TCP和DNS的峰值大多约为0.1，而NTP的峰值也低于0.15。

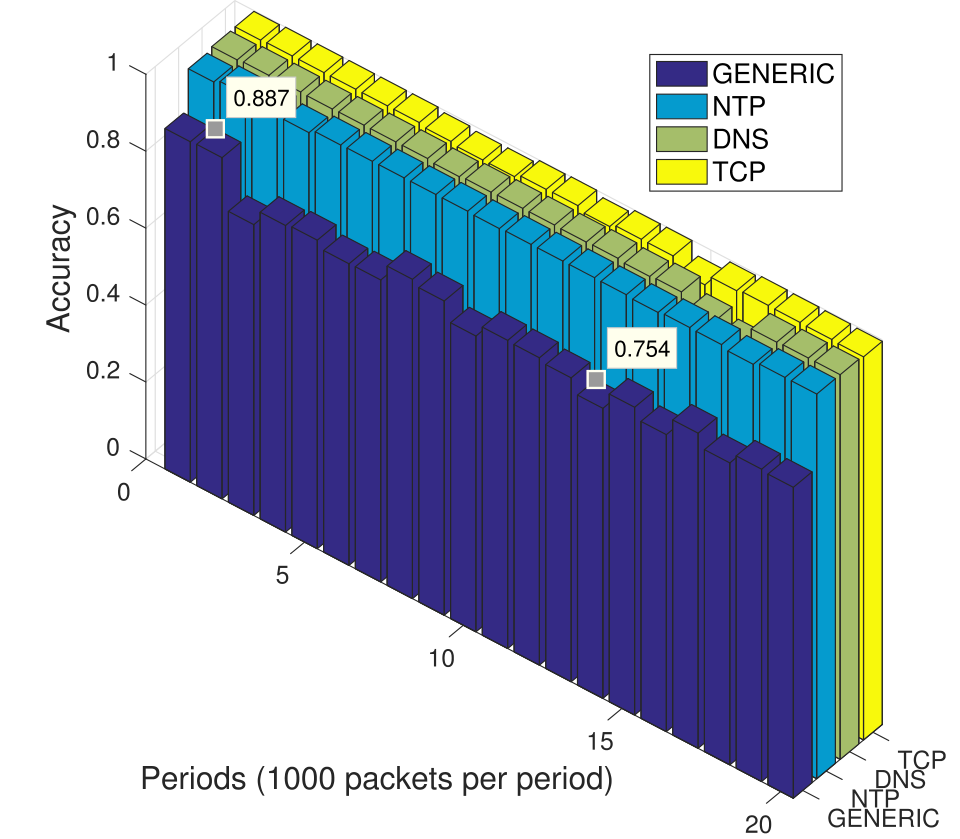


图3

接着再讨论框架的复杂性。在实验中，在标称阶段使用了1000个数据包，需要184 KB。在主动缓解阶段一个对配置文件需要大约311KB，并且其标头长度将为字节的数量级，它就需要大约311 KB。在网络中这个数据量的通信负担较小，不会影响到正常的网络流量。从计算复杂度考虑JESS的各个架构，如表2所示，除了初始化各类数据和规则表变化生成和比较复杂度均为O(N)。规则图的体积时较低的，因此成本也是可以接受的。

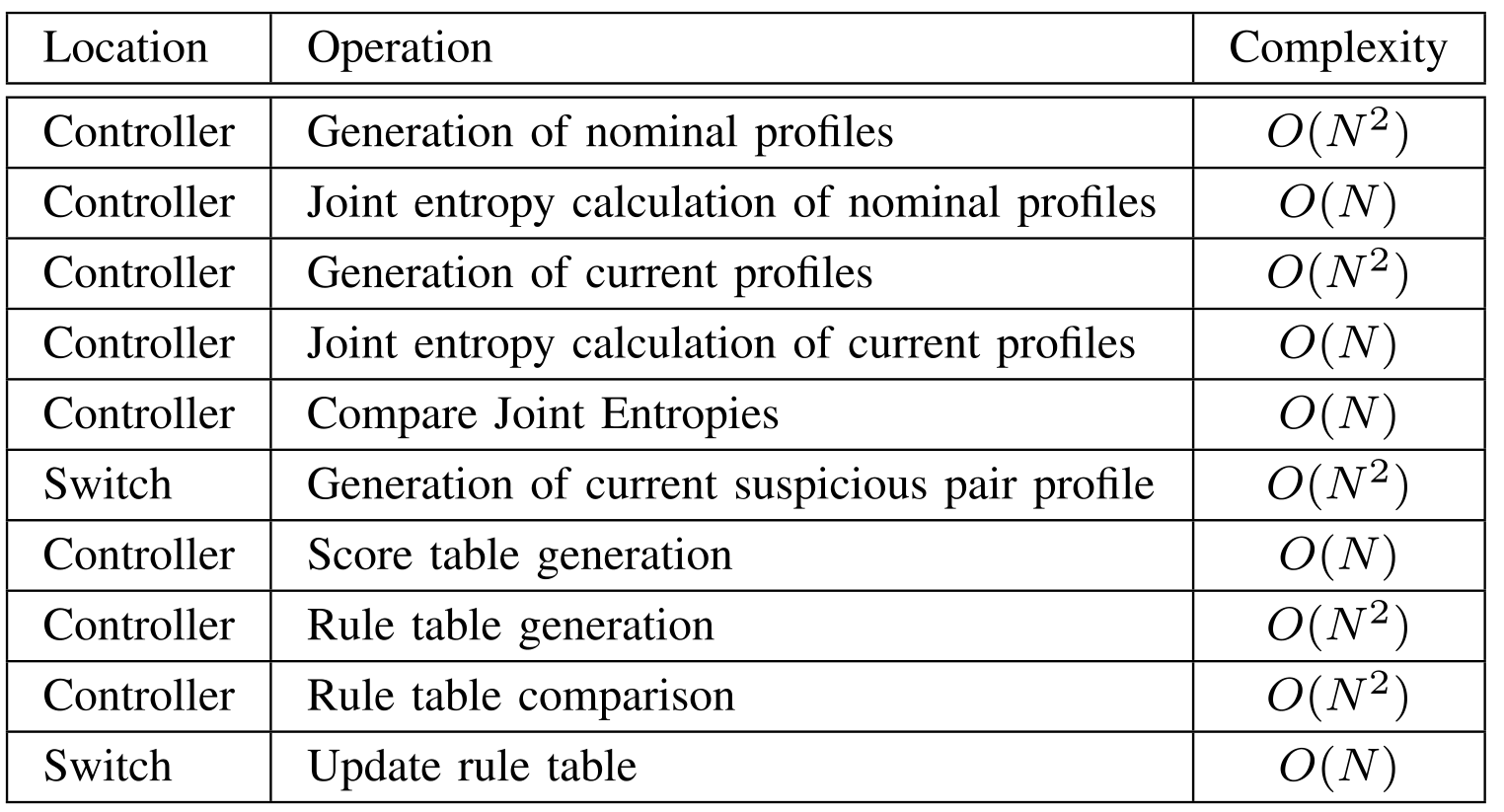


表2

综上所述，对DDoS攻击的防御是一件十分困难的事情，甚至会出现随机攻击这种扰乱防御框架的攻击。而本文介绍的JESS框架使用熵这一统计值来检验数据包之间的差异性。相对于目前十分受人欢迎的人工智能方案，框架复杂度、所需的通信占有量，JESS都十分的少，并且先对于现有其他规则分析模型，熵分析复杂度也更加的低。

但是这样的分析模式仍然存在了许多问题。首先本文介绍的JESS从统计学角度来讲，窗口的大小直接影响了一个网络内能够辨别的攻击数据包范围。在较大的网络服务防御框架中，我们就需要更大的成本来存储、计算以及更新，在功能复杂的政务、游戏类服务端由于功能性复杂，更加能够辨别出攻击数据流，但在行为单一的，例如购物平台，网站中效果就会大打折扣。其次，由于这个框架是由短期固定周期或移动窗口作为步长的，因此它只能够让框架记忆到短期的数据包的多样性。这就导致了不同时间段，网络的性能、参数的剖面、防御的规则都会有很大的不同。同时，JESS也仍然无法解决闪电群效应带来的误判现象，导致合法数据包的丢失。

**参考文献**

[1] K. Kalkan, L. Altay, G. Gür and F. Alagöz, "JESS: Joint Entropy-Based DDoS Defense Scheme in SDN," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 10, pp. 2358-2372, Oct. 2018, doi: 10.1109/JSAC.2018.2869997.

[2] I. Farris, T. Taleb, Y . Khettab, and J. S. Song, “A survey on emerging

SDN and NFV security mechanisms for IoT systems,” IEEE Commun.

Surveys Tuts., to be published.