doi:10.1631/FITEE.1800436

题目：基于特征-模式图的 SDN 下分布式拒绝服务攻击发现方法

概要：由于软件定义网络（software-defined networks, SDN）的开方式结构，软件定义网络环境下的安全威胁已成为一个重要问题。在所有威胁中，分布式拒绝服务攻击（distributed denial-of-service, DDoS）对网络具有巨大影响。本文提出一种基于特征-模式图模型的方法来发现软件定义网络环境下的DDoS攻击行为。所提出的特征-模式图采用网络模式作为节点，将其相似度作为加权边。该图模型可同时表示网络包的头信息和各网络模式之间的关系信息。节点之间的相似度由度量学习和马氏距离表示。所提方法可以基于图的邻近分类模型发现DDoS攻击，并具有自动发现未知攻击的能力且可通过全局或局部插入新节点的方式扩展已有图结构。两个数据集上的实验证明了所提方法在攻击行为检测和图更新任务上的可行性，并证明了本文基于图的模型在DDoS攻击检测上优于对比模型。

关键词：软件定义网络；分布式拒绝服务攻击；行为检测；距离度量学习；特征-模式图