

### 题目

GLASS：一种基于软件定义网络的智能网格DDoS安全的图形学习方法

SDN-SGC（软件定义网络-智能电网通信）

本文提出了一种检测和识别SDN-SGC系统中的分布式拒绝服务(DDoS)攻击的图学习方法。Glass是一个两阶段框架，（1）使用监督图深度学习检测SDN-SGC是否受到DDoS攻击，然后（2）使用无监督学习方法识别受损的实体。网络性能统计数据用于SDN-SGC图的建模，它训练图卷积神经网络(GCN)来提取由DDoS攻击引起的潜在表示。最后，利用光谱聚类来识别被损坏的实体。

一个有弹性的SG应该能够通过自然原因或对网络的故意攻击来检测、识别和响应突发的系统故障。例如，在对SG的拒绝服务攻击期间，一个阶段测量单元(PMU)或多个PMUs可能会受到损害，这将导致来自网格相关部分的测量数据丢失。在这种情况下，SG将失去电网中所有相关变电站的系统可观测性，这可能导致暂时停电或停电。

软件定义网络(SDN)已被证明是一种处理不同通信系统的可靠和高效的体系结构。SDN能够将数据平面与控制平面分离出来，可以为各种SG实体，如实用工具和智能电表和AMI提供控制和管理，并在SG的发展中发挥重要作用，随着SG的发展，集成新的服务、资源、技术和需求。在本文中，我们提出了一种基于SDN的SG安全框架的图形学习方法。GLASS采用了一个两阶段的策略来检测和识别分布式拒绝服务(DDoS)攻击。据我们所知，这是第一个使用监督和无监督图学习方法来在SDN-SGC系统中检测和识别网络攻击的研究。

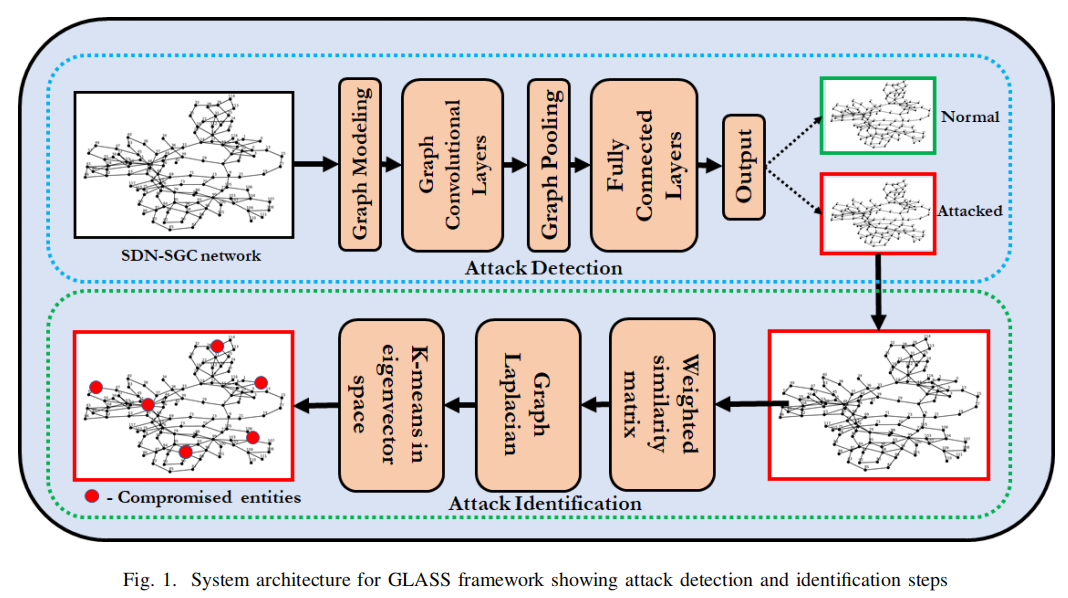
### 贡献

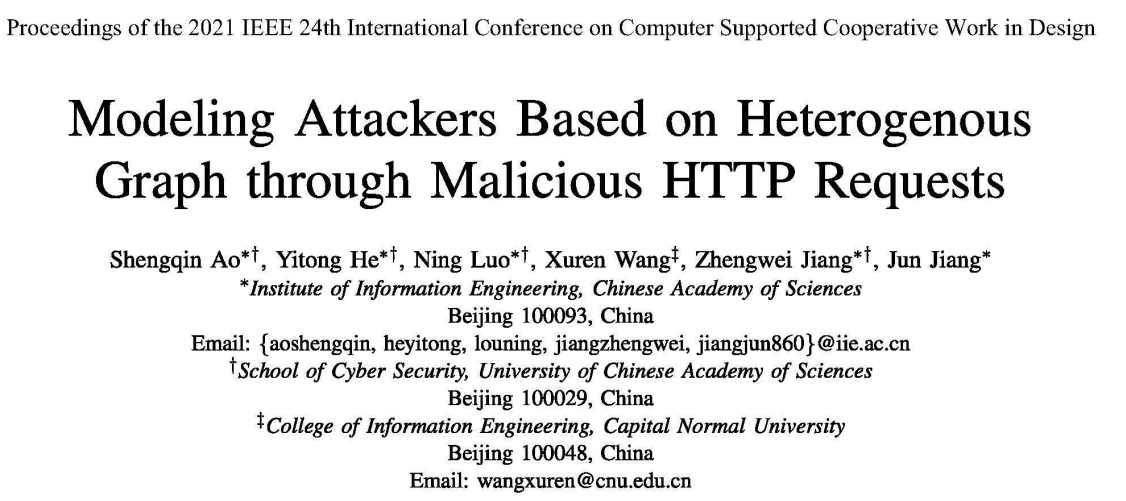
利用图卷积神经网络(GCN)来检测各种攻击场景中的DDoS攻击；

使用光谱聚类来识别DDoS损坏的实体；

分析检测、识别和减轻DDoS攻击对网络性能（吞吐量、传输延迟）的影响。

### 模型





### 题目

通过恶意HTTP请求进行基于异源图的攻击者建模

传统方法中，研究人员使用机器学习或深度学习的方法检测网络日志中的恶意请求，但是只关注了请求本身的内容，没有考虑攻击来源。

近年来，一些研究人员专注于获取IP地址表示来对整个网络中的IP角色进行分类。然而，有一些研究基于其恶意活动获得IP地址嵌入。

恶意的请求会提供一些有价值的信息，如源IP地址、目标域、发布数据、Cookie等。这些包含有关攻击者的活动和攻击方法的信息，提供了发现哪些IP地址属于同一攻击者的可能性。

在本文中，我们基于从各种网站收集的恶意HTTP请求对攻击者活动进行建模，记录了IP地址的行为，并提供了基于HTTP请求来描述攻击者的可能性。首先，我们提出了一种新的方法得到IP地址嵌入：我们设计了一个异构图，称为IP-domain-图，捕获IP地址和域发送恶意请求，我们设计了一个请求内容的嵌入方法来捕获IP地址的行为特征。然后利用相似度计算对IP地址进行聚类来描述攻击者。