

基于层次化图神经网络的云资产安全性分析

张义莲¹, 周笛青¹, 许力文², 叶天鹏², 林祥²

¹ 国网上海市电力公司 上海 中国 200122

² 上海交通大学 网络安全技术研究院 上海 中国 200240

摘要 云系统有着天然的图结构并且处于动态变化当中, 网络攻击的各个阶段往往也具有空间和时序上的关联性。传统的异常检测算法从单源数据入手, 关联性差、可信度低。同时, 海量冗余的安全日志、告警信息给安全分析工作造成了极大的负担。在这样的场景下, 网络安全数据不仅没有发挥其应有的价值, 还由于检测误警率高, 真正的安全威胁被海量的日志和告警数据淹没, 大量的失陷资产由于安全信息关联性差无法被及时发现, 为系统安全运行埋下了极大隐患。针对该问题, 本文提出了基于层次化图神经网络的云资产安全性分析算法, 综合云中多源异构网络安全信息, 将图神经网络应用于云网络安全异常检测当中。通过对云系统中各类多源异构网络安全数据进行深入分析, 提出了异质、动态、有向并带有属性的图建模方式, 将系统中各个实体和实体之间的关系映射到图空间中。在此基础之上, 使用层次化图神经网络学习云系统的特征, 本文提出了改进的图结构自注意力网络来提取图的结构特征、改进的循环神经网络来提取图的动态时序特征, 最后通过节点分类任务完成失陷资产发现, 从而实现云资产安全性分析。在多源异构网络安全数据集上的仿真实验表明, 该算法具有充分利用云系统各个维度上的信息的能力, 对具有不同特征的系统具有较强的适应性, 可以较好地学习到云系统在结构、时序和动态变化中的特征, 有效支撑云场景下的云资产安全性分析。

关键词 云安全; 图神经网络; 图建模; 多源异构网络安全数据

中图分类号 TP309 DOI号 10.19363/J.cnki.cn10-1380/tn.2024.07.13

Cloud Asset Security Analysis based on Hierarchical Graph Neural Network

ZHANG Yilian¹, ZHOU Diqing¹, XU Liwen², YE Tianpeng², LIN Xiang²

¹ State Grid Shanghai Municipal Electric Power Company, Shanghai 200122, China

² Institute of Cyber Science and Technology, Shanghai Jiao Tong University, Shanghai 200240, China

Abstract Cloud systems, with natural graph structure change dynamically, and the stages of network attacks are often spatially and temporally correlated. Traditional anomaly detection algorithms start from single-source data, leading to poor correlation and low credibility. In the meantime, mass redundant security logs and alarm information are burdensome on the security analysis work. In such a scenario, multi-source heterogeneous data not only fails to fulfill its proper value, but also due to the high false alarm detection rate, the real security threats are overwhelmed by the huge amount of logs and alarm data, and a large number of lost assets cannot be discovered in time due to the poor correlation of security information, which has laid a great hidden danger for the safe operation of the system. To solve this problem, this paper proposes a cloud asset security analysis algorithm based on hierarchical graph neural network, which integrates multi-source heterogeneous network security information in the cloud and applies graph neural networks to cloud network security anomaly detection. Through in-depth analysis of various types of multi-source heterogeneous network security data in the cloud system, a heterogeneous, dynamic, directional and attributed graph modeling approach is proposed, mapping each entity in the system and the relationship between the entities into the graph space. On this basis, the algorithm uses hierarchical graph neural network to learn the features of the cloud system, this paper proposes an improved graph structure self-attentive network to extract structural features of graphs, an improved recurrent neural network to extract dynamic temporal features of graphs and then discovers lost assets through node classification task, which finally reaches the goal of cloud asset security analysis. Simulation experiments on multi-source heterogeneous security data sets show that the algorithm has the ability to make full use of the information in each dimension of the cloud system and is highly adaptable to systems with different characteristics. Thus, it can properly learn the features of cloud systems in structural, temporal and dynamic changes, and effectively perform security threat analyses in cloud scenes.

Key words cloud security; graph neural networks; graph modeling; multi-source heterogeneous network security data

通讯作者: 林祥, 博士, 工程师, Email: lionel@sjtu.edu.cn。

本课题得到国网上海市电力公司科学技术项目云平台安全态势感知与威胁预警研究与应用(No. SGTYHT/21-JS-223)资助。

收稿日期: 2022-07-11; 修改日期: 2022-11-04; 定稿日期: 2024-03-18

1 引言

随着计算机网络规模的扩大和各类网络应用的普及,互联网已经成为了人们日常生活中不可或缺的关键信息基础设施,为了提高网络服务质量、降低运行成本,许多机构和组织逐渐将业务“上云”。云系统(Cloud System)下,网络拓扑复杂、业务场景多样、资产信息变化频繁,给网络安全态势感知带来了新的挑战。同时,近年来针对各类组织,特别是政府机构和关键信息基础设施的攻击越来越频繁。在此背景下,仅仅通过堆砌传统的网络安全防护设备进行单点防御、各自为战的模式已经无法对云系统进行有效的防护。如何充分利用网络中来自各类安全设备、业务终端、威胁情报的多源异构网络安全信息对云网络安全态势进行综合研判是一项十分具有挑战性的工作。

目前,实现云资产安全性分析的难点在于:云架构中资产类型多样、网络结构复杂、业务部署变化频繁。现有的研究工作大都是针对传统网络环境进行研究,仅对各类安全设备产生的日志、告警等文本数据进行分析,没有对系统进行关联建模,忽略云网络环境中容器(Container)等云原生资产、专有网络(Virtual Private Cloud, VPC)等网络连接关系和不断变化的系统结构与属性,无法对动态变化、紧密关联的云系统进行科学描述。

对于云系统中的多源异构网络安全数据,现有的研究大多是对云系统中各类安全设备产生的终端安全软件日志、防火墙告警以及入侵检测系统的告警等单一来源的数据进行分析处理,这些数据仅从网络流量、主机行为等单一视角描述了安全事件,关联性差、可信度低,无法确定攻击是否真实发生。同时,现有的告警关联工作也存在许多问题。例如,基于预定义规则^[1]的方法利用先验知识定义规则,并将实时事件与规则库进行匹配,无法有效地发现未知关联关系;基于概率推理^[2]的方法使用概率推理模型来获得事件之间的条件概率,但在大规模数据上进行计算时面临时间、空间复杂度较高的窘境;基于信念网络^[3]的方法描述不同节点之间产生异常行为的条件概率,然而在节点增多时,将面临状态爆炸的情况。这些方法往往依赖先验的安全知识或者计算复杂度过高,无法应用在真实的安全场景中。

当前网络安全异常检测往往采用基于规则或者特征库匹配算法,存在大量的误警,传统网络安全设备产生的海量冗余的安全日志、告警信息给安全分析工作造成了极大的负担。采用有监督的人工智

能异常检测算法依赖于大量准确的标签数据,然而在云这一庞大复杂并时刻变化的系统中,难以定义在什么时刻表现出什么特征的资产是异常的。同时,由于资产类型多样,针对特定场景训练得到的模型容易产生过拟合的现象,依然会产生大量的误警信息。

因此,本文提出了一种基于层次化图神经网络进行云资产安全性分析的方法,利用图模型和图神经网络对网络中来自各类安全设备、业务终端、威胁情报的多源异构网络信息进行建模和关联分析,实现云资产安全性分析。本文的主要贡献如下:

(1)利用动态图模型^[4]描述云中动态生成的日志及网络安全告警数据,并根据资产信息和网络拓扑进行关联和融合,以解决难点1;

(2)层次化图神经网络算法中的结构注意力层^[5]在已有图模型的基础上充分结合网络层面、主机层面的异常表示,利用节点自身的特征、节点之间的关联关系挖掘图结构上的关联特征;时序特征提取层则根据不同时刻图模型中点边的增删挖掘图时空上以及动态变化中的关联,以解决难点2;

(3)最终通过节点分类^[6]任务使得安全管理人员可以及时从海量安全信息中发现重要的攻击事件,识别失陷资产,消除误警并填充漏警,从而对攻击者的下一步动作进行预测,以解决难点3。

本文的核心思想是利用图模型描述网络中各个实体、实体所拥有的属性以及实体之间的关系,通过将采集到的多源异构网络安全数据填充到动态图模型中,完成信息的聚合与关联,在此基础之上使用层次化图神经网络算法学习系统结构和时序上的特征,最后使用一类分类器完成失陷资产发现,从而实现云资产安全性分析。

2 相关工作

近年来,以卷积神经网络(CNN)^[7]为代表的深度学习方法在自然语言处理、计算机视觉等领域取得了十分优异的效果。但在商品推荐、社交网络发现以及分子性质预测等许多新兴场景中,传统的深度学习方法的表现却仍难以达到实际应用场景的要求。这些新兴场景往往涉及到图这种非欧几里得空间的数据结构,其自身的复杂性和结构中丰富的依赖关系使得现有的深度学习算法无法有效地学习到其中蕴含的特征。因此,用于处理图数据的神经网络结构图神经网络应运而生了。图神经网络(GNN)^[8]是通过图的节点之间的信息传递来捕捉图特征的神经网络模型。根据具体实现方式不同可以分为:循环图神经网络(Recurrent Graph Neural Networks,

RecGNNs)^[9]、卷积图神经网络(Convolutional Graph Neural Networks, ConvGNNs)^[10]、图自编码器(Graph Autoencoders, GAEs)^[11]和时空图神经网络(Spatial-temporal Graph Neural Networks, STGNNs)^[12]等。由于图结构具有丰富的表现能力, 图神经网络会采用层次化的方法设计不同作用的子层, 分别用于学习结构、时序等维度上的图特征, 从而增强全局的特征提取能力。

在异常检测领域, Zheng L 等人^[13]提出了 AddGraph, 在利用 GCN 自动地传播邻居节点的信息、扩散节点的异常概率的基础上, 引入了基于注意力机制的 GRU, 从而获得短时和长时的异常特征; Lei Cai 等人^[14]提出了 StrGNN, 通过学习在给定时间窗口内以目标边为中心的子图结构变化, 判断其是否为异常子图, 最终确定目标边的类别; Wu Y 等人^[15]将 GNN 用于 IoT 智能交通、智能能源和智能工厂中的异常检测, 并将图中的异常分为点异常、上下文异常和集体异常; Liu Y 等人^[16]研究了属性网络的异常检测方法, 将节点属性加入到神经网络的输入中, 并设计了一种基于 GNN 的对比学习模型, 从高位属性和局部特征中学习信息嵌入; Goodge A 等人^[17]提出了 LUNAR, 这种基于 GNN 的异常检测方法使用来自每个节点最近邻居的信息来发现网络中的异常。

近年来, 图神经网络也开始从通用场景的异常检测逐步深入到网络安全异常检测中。例如, J Zhou 等人^[18]将网络中的节点建模成点、节点间的通信行为建模成边, 根据僵尸网络明显的星型结构和网络混合速率高等特征, 无需任何先验知识, 即可完成对 BotNet 的端到端检测; Wan Y 等人^[19]提出了基于日志的异常检测模型 GLAD-PAW, 将每个会话构建一张图, 图中节点为会话中包含的各个事件, 有向边代表事件发生的先后顺序和依赖关系, 最终通过图分类问题实现异常检测; Busch J 等人^[20]提出了 NF-GNN, 通过将 IP 地址和其间的网络通信行为建模成图中的点和边来表征传统检测手段无法利用的丰富通信模式, 实现了恶意软件的检测和分类。

由于云网络有着天然的图结构, 并且网络攻击的各个阶段往往具有空间和时序上的关联性。但现有的基于图神经网络的检测方法在所能支持的维度(例如有向图、属性图、动态图、异质图等)上能力不足或仅从恶意软件行为、网络流量等单一视角进行检测, 无法全面、合理地描述图建模后的云系统。

因此, 本文针对该问题提出了面向云环境的资产安全性分析算法, 综合云中多源异构网络安全信息, 将图神经网络应用于云网络安全异常检测当中。

3 云系统的图建模

图建模是指使用由点和线组成的几何图形来描述实体的建模方式。借助图论, 图模型可用于描述各种实体以及实体之间的关系。构成图模型的图形与一般几何图形相比, 包含更多的物理意义。由于其对复杂系统具有很强的描述能力, 图建模已经开始被应用于反欺诈、反洗钱、反恐、推荐系统以及社交网络等重要领域。

云架构中资产类型多样、网络结构复杂、业务部署变化频繁, 经典的建模和分析方法无法对动态变化、紧密关联的云系统进行科学描述。通过对云系统中资产信息、网络拓扑和多源异构网络安全数据进行深入分析, 可以将系统中各个实体和实体之间的关系映射到图空间中, 并利用图论对其物理意义进行抽象, 以便于进一步分析。

3.1 云系统中的多源异构数据

面对未知威胁和 APT 等特殊攻击手段, 仅仅利用部署于网络边界或特殊位置的防火墙、防病毒、入侵检测系统、入侵防御系统和网络安全审计等基于已知威胁特征进行被动防御的方法已经不再适用。在这样的场景下, 多源异构数据不仅没有发挥其应有的价值, 还由于检测误警率高, 真正的安全威胁被海量的日志和告警数据淹没, 大量的失陷资产由于安全信息关联性差无法被及时发现, 为系统安全运行埋下了极大隐患。

开展云网络资产安全性分析, 及时发现失陷异常资产, 亟需针对传统的网络安全防御方式进行优化和改进。通过分析现有多源异构数据源, 从中挖掘出对网络安全有价值的数据才能构建能够应对多样化和持续性网络威胁的安全保障体系。

3.1.1 资产信息

由于统一运维管理的特点, 云系统中资产清晰可控, 通过云基础设施 API 等方式, 可以动态获取云中所有的资产信息。

本文将云系统中的资产定义为拥有独立网络地址的物理或虚拟化的节点。对于每个资产, 使用一个 ID 来唯一标识, 属性包括类型、角色、重要性、所属租户、VPC 信息、IP 地址、开放端口以及应用层软件信息。

$$N_{ID} = \left(\begin{matrix} \text{Type, Role, Priority, User, VPC,} \\ \text{IPs, Ports, Applications} \end{matrix} \right) \quad (1)$$

3.1.2 拓扑信息

由于 SDN 等技术的引入, 云系统中的网络拓扑十分复杂, 在逻辑上可划分为不同的区域, 用以承

载不同租户或业务集群的流量。

以华为云 Stack 解决方案为例, 云网络可划分为业务网、管理网和存储网, 每个网络中又根据业务和租户需求划分为不同的 VPC、配置不同的转发规则, 连接关系复杂。因此, 本文设计了一个连接矩阵来描述云网络拓扑, 即云网络内各个节点之间的连接关系。其中, N_i 和 N_j 为云中资产, 对于 C 中每一个元素 C_{ij} , 有:

$$C_{ij} = \begin{cases} 1, & \text{从 } N_i \text{ 到 } N_j \text{ 网络可达} \\ 0, & \text{从 } N_i \text{ 到 } N_j \text{ 网络不可达} \end{cases} \quad (2)$$

3.1.3 日志及告警信息

来自各类安全设备、业务终端的告警信息是威胁分析的关键数据来源。为了充分利用来自于网络、主机和边界等不同视角的安全数据, 采集防火墙、防病毒、入侵检测系统、入侵防御系统、终端安全防护系统和网络安全审计产生的原始日志和告警信息, 用于后续融合分析, 提取高阶安全语义信息。

对于每条日志和告警, 采用一个告警 ID 来唯一标识, 属性包括: 时间戳、告警类型、告警来源、重要性、源 IP 地址、源端口、目标 IP 地址、目标端口和其他信息。

$$R_{ID} = (\text{Timestamp, Type, Source, Priority, srcIP, srcPort, dstIP, dstPort, Others}) \quad (3)$$

3.2 多源异构数据的图映射关系构建

为了对云系统进行科学地描述、充分利用云系统中的多源异构网络安全数据, 本文提出了异质、动态、有向并带有属性的图建模方式。

云系统中资产种类繁多, 资产之间的关系也各不相同。资产类型包括物理服务器、虚拟机、容器、物理网络设备和物理安全设备; 资产之间的关系可以为网络可达或存在可能的攻击行为。给定图 $G = (V, A, C, X, Z)$, 将云中各类资产建模为点, $V = \{v_1, v_2, \dots, v_n\}$ 代表所有资产的集合, 节点 $v_i \in V$ 代表云中的一个具体资产; 将多源异构的告警事件建模为边, $A = \{a_1, a_2, \dots, a_{N_a}\}$ 代表攻击告警的集合。

云系统中的资产和资产之间的关系均包含多个属性。特别地, 不同于其他图建模场景, 云系统中资产之间的关系包含丰富的属性, 是威胁分析的主要数据来源, 需要重点关注。 $X \in R^{N_v \times d_v}$ 是图 G 的节点特征矩阵, 包含了图中每个节点的特征。 $Z \in R^{N_a \times d_a}$ 是图 G 的告警特征矩阵, 包含了图中每条告警的特征。

对于云网络中的连接关系, 本文使用连接矩阵 $C \in R^{N_v \times N_v}$ 描述, 即若从 v_i 到 v_j 网络可达, 则 $C_{ij} = 1$,

否则 $C_{ij} = 0$ 。而对于攻击告警信息, 每条边 $a_k = (v_i, v_j, k) \in A$ 表示存在从 v_i 到 v_j , 告警 ID 为 k 的攻击告警。

一条攻击告警信息所关联的资产不在同一 VPC 中或位于强隔离设备的两侧, 即 $C_{ij}^t = 0$ 则由于网络不可达直接认定为误警予以删除, 不参与后续的检测。删除后的告警信息和告警特征矩阵如下:

$$A' = \{a_k^t \mid a_k^t = (v_i, v_j, k) \in A^t, C_{ji}^t = 1\} \quad (4)$$

$$Z' = \{z_k^t \mid a_k^t = (v_i, v_j, k) \in A^t\} \quad (5)$$

云系统网络结构复杂、业务部署变化频繁, 网络结构、资产属性和资产关系均处于动态变化之中。这种变化体现在节点和边可能会随时序发生增删, 属性信息也会发生修改。因此, 本文在上述图模型基础上进一步构建动态图。

通过给定一个时间步长 T , 根据每条多源异构网络安全数据的时间戳进行切分, 即每组依次包含时间间隔为 T 的数据, 共分为 N 组。

对于图 $\bar{G}$, 将 $\bar{G}$ 按照时间序列表示为由一系列离散的图快照 $G^t = (V^t, A^t, C^t, X^t, Z^t)$ 组成的序列 $\bar{G} = \{G^1, G^2, \dots, G^N\}$ 。所有出现过的点的集合 $\bar{V} = V^1 \cup V^2 \cup \dots \cup V^N$, 图 $\bar{G}$ 即为最终所需的离散动态图。

对图 $\bar{G}$ 中每个元素的节点特征矩阵和告警特征矩阵中的离散特征进行 One-Hot 编码; 对于连续特征进行归一化处理, 映射到 $[0, 1]$ 区间, 作为后续图神经网络的输入。完整的动态图建模算法见算法 1。

Algorithm 1 Dynamic Graph Construction

Input: N, C, R, T

Output: $\bar{G}$

```

1: Initialize: SET  $\bar{G} = \emptyset$ 
2: FOREACH  $r \in R$  DO
3:    $t = r.\text{Timestamp} // T$ 
4:   IF  $\exists n_i \in N$  such that  $r.\text{srcIP} \in n_i.\text{IPs}$  THEN
5:     IF  $\exists n_j \in N$  such that  $r.\text{dstIP} \in n_j.\text{IPs}$  THEN
6:       IF  $C_{ij}^t = 1$  THEN
7:         add  $i, j$  to  $V^t$ 
8:         add  $n_i, n_j$  to  $X^t$ 
9:         add  $(i, j)$  to  $A^t$ 
10:        add  $r$  to  $Z^t$ 
11:       ELSE
```

```

12:      discard  $r$ 
13:    END IF
14:  ELSE
15:    discard  $r$ 
16:  END IF
17: ELSE
18:   discard  $r$ 
19: END IF
20: END FOR
21: FOR  $i \in [0, t]$  DO
22:   LET  $G^i = (V^i, A^i, C^i, X^i, Z^i)$ 
23:   add  $G^i$  to  $\bar{G}$ 
24: END FOR
25: RETURN  $\bar{G}$ 

```

4 云资产安全性分析算法

本文提出了一种基于层次化图神经网络进行云资产安全性分析的方法, 尝试利用图模型和图神经网络对云网络中来自各类安全设备、业务终端、威胁情报的多源异构网络信息进行建模和关联融合, 实现云资产安全性分析。

层次化图神经网络算法中的结构注意力层在已有图模型的基础上充分结合网络层面、主机层面的异常表示, 利用节点自身的特征、节点之间的关联关系挖掘图结构上的关联特征; 时序特征提取层则根据不同时刻图模型中点边的增删挖掘图时空上以及动态变化中的关联关系; 最终通过节点分类任务使得安全管理人员可以及时发现重要的攻击事件, 识别失陷资产。算法的整体结构如图 1 所示。

4.1 基于自注意力机制的图结构特征提取层

为了充分利用图中的结构信息, 本文提出了基于自注意力机制的图结构特征提取层, 其包含与特定主机相关联的资产和告警信息的汇聚操作, 利用当前时刻各个节点和关联边的特征对节点原始特征进行两轮更新。

特别地, 攻击告警的方向为资产之间的邻接关系提供了关键信息, 在一般的图神经网络模型的基础上, 本文提出的模型限制图采样过程中对于邻节点和邻边的判定。规则如下:

$$\mathcal{N}_i^t = \{v_j \mid a_k = (v_j, v_i, k) \in A^t\} \quad (6)$$

$$\mathcal{A}_i^t = \{a_k \mid a_k = (v_j, v_i, k) \in A^t\} \quad (7)$$

即当且仅当有向边 a_k 以 v_i 为终点时, 起点 v_j 为 v_i 的邻节点, a_k 为 v_i 的邻边。

第 l 层的节点 Embedding 为 $H_v^{(l)}$ 。特别地, 第 0 层的节点 Embedding $H_v^{(0)} = X$, 即节点的初始特征。

为了充分利用多源异构数据中的安全语义信息, 对于节点 v_i 的每个邻节点, 其对于节点 v_i 的重要性为与该邻节点相关联的告警事件重要性 P_k 的和:

$$W_{ij} = \sum_{j \in \mathcal{N}_i, (v_i, v_j, k) \in A} P_k \quad (8)$$

在邻节点信息汇聚阶段, 通过拼接操作融合节点自身特征 x_i 和其关联资产的特征 x_j , 对应邻居节点的图结构自注意力层的 Attention 系数为:

$$\alpha_{ij} = \frac{\exp(\sigma(W_{ij} \cdot a^\top [W^s x_i \parallel W^s x_j]))}{\sum_{k \in \mathcal{N}_i} \exp(\sigma(W_{ik} \cdot a^\top [W^s x_i \parallel W^s x_k]))} \quad (9)$$

考虑 v_i 的所有邻居节点, 可知经过一轮特征更新后 v_i 的特征为:

$$x_{\mathcal{N}_i} = \sigma \left(\sum_{j \in \mathcal{N}_i} \alpha_{ij} W^s x_j \right) \quad (10)$$

在邻边信息汇聚阶段, 首先对 v_i 的所有邻边的特征向量进行加权求和:

$$x_{\mathcal{A}_i} = \sigma \left(\sum_{k \in \mathcal{A}_i} P_k \cdot Z_k \right) \quad (11)$$

在第二轮更新时, 对应聚合邻居节点和关联边后的节点 Embedding 为:

$$\bar{x}_i = \text{CONCAT}(x_{\mathcal{N}_i}, x_{\mathcal{A}_i}) \quad (12)$$

其中, α_{ij} 为结构重要性系数、 $\exp(\cdot)$ 为以自然常数 e 为底的指数函数、 $\sigma(\cdot)$ 为非线性激活函数、 W_{ij} 为节点 v_i 到 v_j 告警事件的权重求和, $a^\top$ 为权重向量、 W^s 为权重转换矩阵、 $\mathcal{N}_i$ 为节点 v_i 在一张图中的邻节点、 $\mathcal{A}_i$ 为节点 v_i 在一张图中的邻边、 $\text{CONCAT}(\cdot)$ 表示拼接操作、 $\bar{x}_i$ 为经过结构自注意力网络后的节点特征表示。

4.2 基于循环神经网络的图时序特征提取层

为了充分聚合同一节点在不同时刻的特征表示, 本文提出了基于循环神经网络的图时序特征提取算法。节点在每个时刻的特征表示都依赖于前一个时刻的特征表示, 有效地利用了长距离的时序信息, 学习节点在动态变化中体现出的特征。

为了有效解决时序变化中节点增删的问题, 本文提出一种基于 LSTM^[21] 的改进算法。在一般 LSTM 网络的基础上, 设置一个滑动时间窗口 W , 对于每

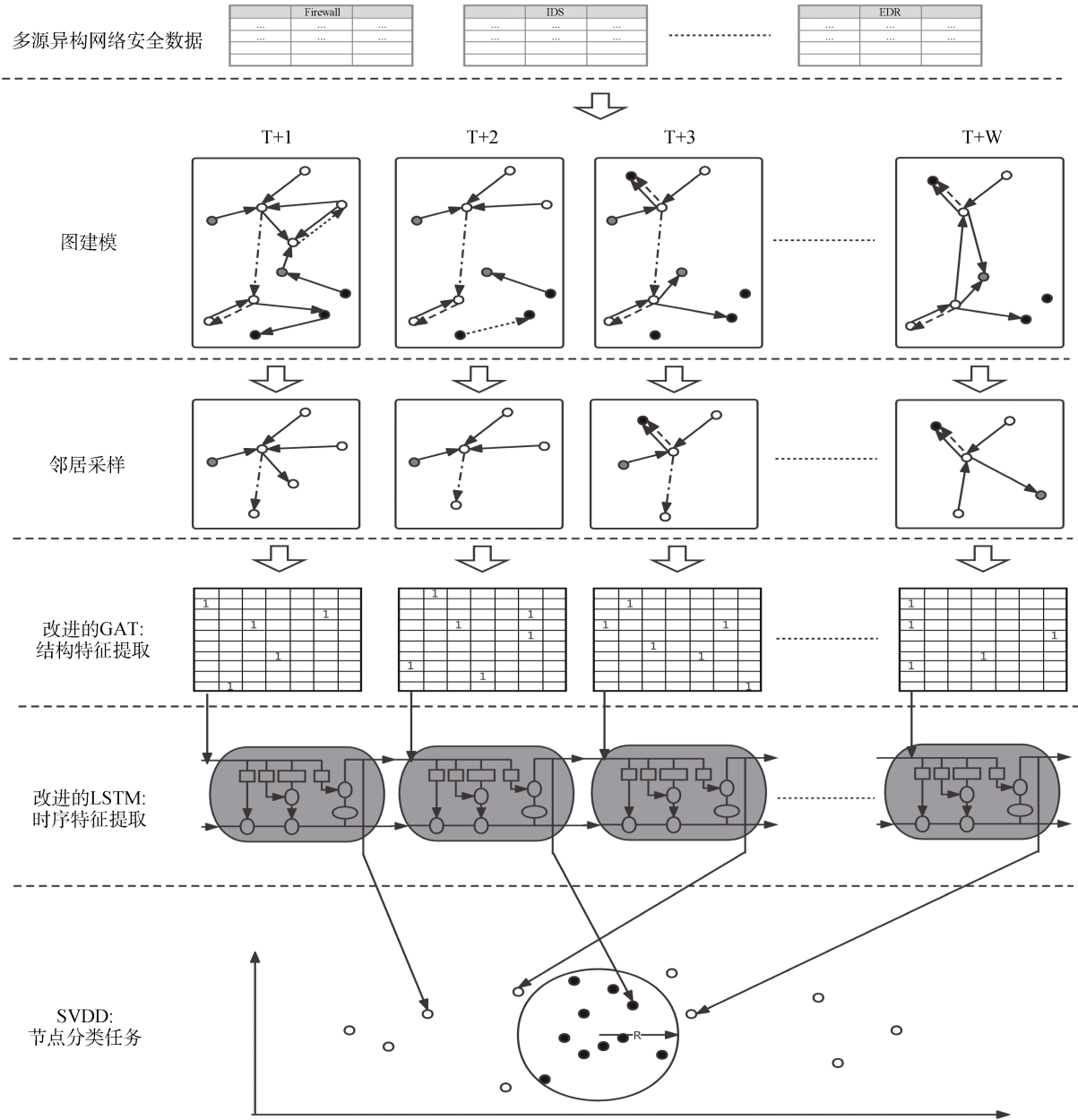


图1 云资产安全性分析算法

Figure 1 Cloud asset security analysis algorithm

(注: 节点颜色代表节点类型; 边的样式代表边的类型; 箭头代表边的方向; W 张快照构成了一张离散动态图)

一个 $v_i \in \bar{V}$, 其在各个快照中出现的次数为 $w = \left| \left\{ G^t \mid v_i' \in G^t \right\} \right|$ 。

对于少数节点, 若 $w \leq W$, 则将 $(x_i^{t_0}, x_i^{t_0+1}, \dots, x_i^{t_0+w-1})$ 作为序列依次输入到 LSTM Cell 中, 共循环 w 次; 若 $w > W$, 则根据时间窗口大小 W , 以步长为 1, 将 $(x_i^{t_0}, x_i^{t_0+1}, \dots, x_i^{t_0+w-1})$ 拆分成 $w - W + 1$ 个长度为 W 的时间窗口, 每个窗口循环 W 次, 共 $W \times (w - W + 1)$ 次。

特别地, 在模型训练过程中仅将 $w > W$ 所对应的节点作为训练样本输入模型。

4.3 无监督单分类威胁分析算法

由于云系统中有标签的时序同步的多源异构网络安全数据往往难以获得, 因此本文使用无监督的支持向量数据描述 (Support Vector Data Description, SVDD)^[22] 来实现正常资产和失陷资产的区分。

在训练过程中, 输入为不包含异常行为的正常数据, 利用神经网络来计算能包含正常节点特征的最小超球面, 形成云系统的行为基线。在检测阶段, 比较球心到测试样本点间的距离和超球面半径来判断输入是否为异常节点。

在 SVDD 中, 输入为 $\mathcal{X} \subseteq \mathbb{R}^d$, 输出为 $\mathcal{F} \subseteq \mathbb{R}^p$,

整个模型完成一个特征映射 $\phi(x_i; \mathcal{W}): \mathcal{X} \rightarrow \mathcal{F}$ 。在这个过程中需要学习的参数为 $\mathcal{W} = \{W^1, W^2, \dots, W^L\}$, 对于输入 $x \in \mathcal{X}$, 其特征为 $\phi(x; \mathcal{W})$, 超球面可以使用球心 c 和半径 $\mathcal{R}$ 进行表示。训练过程中优化的目标函数为:

$$\min_{\mathcal{W}} \frac{1}{n} \sum_{i=1}^n \|\phi(x_i; \mathcal{W}) - c\|^2 + \frac{\lambda}{2} \sum_{\ell=1}^L \|W^\ell\|_F^2 \quad (13)$$

对于每一条测试数据 $x \in \mathcal{X}$, 若其落在了训练所获得的超球面之外, 还可以通过计算该点到球心的距离来定义节点异常的程度:

$$s(x) = \|\phi(x; \mathcal{W}^*) - c\|^2 \quad (14)$$

其中, $\mathcal{W}^*$ 表示训练后模型的权重。训练完成后模型学习到一个超球面, 每当有新的节点到来时, 若落在球面内部则判定为正常节点; 若落在球面外部则说明该节点为需要关注的异常资产。

本文针对云系统中已有的网络安全数据进行进一步分析, 对于被正确分类的资产, 所提出算法的实际效果在于:

若该资产为失陷资产, 但并没有与其相关的告警信息, 则实现了漏警的填充; 若该资产为正常资产, 但存在与其相关的告警信息, 则实现了误警的消除。

对于云环境下的各种网络安全威胁, 在本文所提出的算法中不对具体威胁类别进行检测, 考虑在后续的研究工作中做进一步探索。

5 实验与评估

5.1 数据集

事实上, 由于采集难度以及数据共享的障碍, 现实云环境中时序上同步的多源异构网络安全数据非常难以获得, 不存在完全符合要求的开源数据集。因此, 本文使用 VAST Challenge 2012 Mini Challenge 2 数据集^[23]和 Los Alamos National Laboratory (LANL) 数据集^[24]来评估所提出算法的有效性。

VAST Challenge 2012 Mini Challenge 2 来自 Bank of Money 银行的地区办公室网络, 该网络包含大约 4000 台工作站和 1000 台服务器, 24 h 对外提供服务。整个网络被划分为不同的子网, 以承载不同的业务交互数据。数据集共包括时序上同步的入侵检测系统告警和防火墙告警数据, 网络配置信息和统计信息如图 2 和表 1 所示。

LANL 数据集来自连续 58 天从洛斯阿拉莫斯国家实验室公司内部计算机网络中采集的网络安全数据。数据集包括时序上同步的来自个人计算机和集

中式 Active Directory 域控制器的身份验证事件、主机的进程启动停止事件、内部 DNS 服务器上的域名服务(DNS)查找事件、关键网络位置收集的网络流数据和一组定义明确的红队攻击事件, 这些事件包含 58 天内的各种攻击行为。

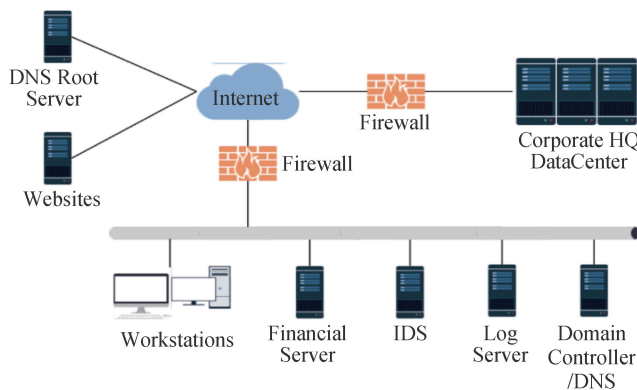


图 2 VAST Challenge 2012 MC 2 网络拓扑
Figure 2 VAST Challenge 2012 MC 2 network topology

表 1 VAST Challenge 2012 MC 2 数据集统计信息
Table 1 Statistical information on VAST Challenge 2012 MC 2

类别	时间	记录条数	特征维度
IDS Log	2012/04/05 17:55 – 2012/04/07 08:59	35948	11
Firewall Log	2012/04/05 17:51 – 2012/04/06 19:39	2097150	15

完整的数据集包括 12425 个用户、17684 台计算机和 62974 个进程提供的 1648275307 个事件。

5.2 算法能力分析

本节对本文所提出的算法的能力进行分析。由于现实场景, 特别是云系统具有较高的复杂性, 为了更加全面地评价算法对于复杂图模型的分析能力, 本文共选取了是否利用边特征、是否支持有向图、是否支持动态图、是否支持属性图和是否支持异质图五个维度进行分析, 对比结果如表 2 所示。

表 2 算法能力对比
Table 2 Algorithm capability comparison

模型	编码器	边特征	有向	动态	属性	异质
This paper	GAT & LSTM	Yes	Yes	Yes	Yes	Yes
CensNet ^[25]	GCN	Yes	No	No	Yes	Yes
DySAT ^[26]	GAT & temporal attention	No	No	Yes	Yes	Yes
Botnet-detection ^[18]	GNN	No	No	No	No	No
GraphSage ^[27]	Aggregation	No	No	No	Yes	No

由表 2 可知, 从所有支持的维度的数量上来分析, 本文所提出的威胁分析算法是唯一一种在五个维度上均可提供支持能力的算法, 其余算法最多支持其中三种能力; 从单个维度上来分析, 本文所提出的威胁分析算法是唯一一种支持有向图的算法。因此, 本文所提出的算法具有充分利用云系统各个维度上的信息的能力, 对具有不同特征的系统具有较强的适应性。

5.3 算法性能评估

为了进一步评估本文所提出算法的有效性, 本节用 VAST Challenge 2012 Mini Challenge 2 数据集和 Los Alamos National Laboratory (LANL)数据集进行仿真实验。

特别地, 由于前者没有明确标注攻击阶段和目标资产, 无法直接作为有标签数据使用。L. Shi 等^[28]和 J. Hildenbrand 等^[29]对 VAST Challenge 2012 Mini Challenge 2 进行的分析表明, 172.23.0.0/16、10.32.5.0/24 等网段下部分资产在特定时间段内存在异常行为, 在分析时将该网段下的主机作为异常资产进行处理。此外, 由于本文所提出的算法以动态图为基础进行分析, 因此上述异常资产在非攻击时间段内仍然被视为正常资产。

对于 LANL 数据集, 则可以通过明确定义的红队攻击事件来判断特定节点在某一时间段中是否为失陷资产。

实验在具有两个 Intel(R) Xeon(R) CPU E5-2678 v3 @ 2.50GHz CPU 的服务器上进行, 操作系统为 Ubuntu 18.04.5 LTS, 模型训练使用 Nvidia Ampere A40 GPU 进行加速, 模型超参数设定如表 3 所示。

模型评判标准采用以下 5 个维度: 精度(Accuracy)、精确率(Precision)、召回率(Recall)、F1 分数(F1 Score)、浮点运算数量(FLOPs)。

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + FN + TN} \quad (15)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad (16)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (17)$$

$$F_1 \text{ Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \quad (18)$$

表 3 实验超参数设定

Table 3 Hyperparameter settings

参数名	值
timesteps	16
epoch	200
batch size	64
learning rate	0.01
weight decay	0.0005
spatial drop	0.1
window size	12

其中, TP(True Positive, 真阳性)表示预测为正, 实际也为正; FP(False Positive, 假阳性)表示预测为正, 实际为负; FN(False Negative, 假阴性)表示预测为负, 实际为正; TN(True Negative, 真阴性)表示预测为负, 实际也为负; FLOPs: Floating point Operations, 指前向推理的计算量, 用来衡量算法/模型的复杂度。

需要特别指出的是, 为了方便比较, 对于表征模型计算复杂度的指标 FLOPs, 由于 Bot-net- detection 和 CensNet 不支持动态图检测, 因此根据超参数中设置的 timesteps 的值, 上述两个模型的 FLOPs 值均为对 16 张图进行检测的总计算量。

由表 4 可知, 在 VC2012 数据集上, 本文所提出的模型与不支持边特征的 DySat 相比, 由于边特征的加入, 算法的召回率提升了近 15%、精度提升了近 14%。

表 4 算法性能对比

Table 4 Algorithm performance comparison

模型	VAST Challenge 2012 Mini Challenge 2					Los Alamos National Laboratory				
	召回率(%)	精确率(%)	精度(%)	F1 分数(%)	GFLOPs	召回率(%)	精确率(%)	精度(%)	F1 分数(%)	GFLOPs
Spacial	79.96	98.10	79.27	87.74	13.68	81.87	96.55	79.66	88.60	5.67
Spacial + Temporal (without features)	74.79	96.19	72.95	84.15	3.09	75.67	94.43	73.47	84.02	6.29
Spacial + Temporal	86.62	99.90	86.70	92.79	24.72	84.34	97.91	82.94	90.61	9.44
Bot-net-detection ^[18]	70.59	88.89	66.68	78.69	0.96	73.68	90.32	69.76	81.15	0.64
DySat ^[26]	71.82	96.92	72.08	82.50	11.78	73.46	94.43	71.65	82.77	8.97
CensNet ^[25]	88.22	93.81	83.42	90.93	27.84	80.34	93.96	77.32	86.62	15.73

对于 VC2012 数据集, 从本文所提出的模型中剔除边特征融合的相关部分后, 算法的召回率由 86.62% 下降至 74.79%、精度由 86.70% 下降至 72.95%、精确率也有 4% 左右的下降; 由于 LANL 数据集边特征维度较低, 剔除边特征后, 各项指标下降幅度明显小于 VC2012 数据集, 证明了边特征对于算法性能的重要性。

由于本文所提出的模型支持的能力维度较多, 对于边特征、有向图、动态图、属性图和异质图的分析能力均会导致模型趋于复杂, 在特征维度较高的 VC2012 数据集下比 DySat 高出 12.94GFLOPs。但对层次化图神经网络中的时序特征提取层和边特征的消融实验表明, 在模型能力大致相同的情况下, 本文所提出的模型计算量却比 DySat 低 8.69GFLOPs, 而原模型比本就支持边特征的 CensNet 低 3.12GFLOPs。同时, 由于本文所提出的模型并不针对实时检测进行设计, 在高性能 GPU 的加速下, 训练和检测耗时均在工程上能接受的时间范围内。因此, 本文所提出的模型仍具有计算复杂度上的先进性。

CensNet 采用交替更新原图和线图的方式来将边特征融入节点 Embedding 中, 这种方法默认邻边也具有与邻点相似的关联关系, 本文则是通过判断邻边对于点的重要程度来有选择地将边特征融入节点 Embedding 中, 在 VC2012 数据集上前者虽然在召回率上有 1.6% 的小幅提升但是其他三项指标均有所下降; 而在 LANL 数据集上, 四项指标均低于本文所提出的算法。

对于支持维度最少的 Bot-net-detection, 虽然其拥有最低的算法复杂度, 相比于更加复杂、维度更高的 VC2012 数据集, 其在 LANL 数据集上的表现相对更好, 是简单场景下一种较为轻量级的检测算法。但由于该算法不能利用图中的边特征、时序变化特征等维度信息, 无法针对云这种复杂系统提供可靠的检测能力, 与其他模型相比各项指标差距较大, 无法满足检测要求。

综上所述, 本文所提出的算法在各类指标上的表现均较为突出, 可以更好地利用云系统中的多源异构网络安全数据, 将失陷节点从正常节点中区分开来, 具有更强的威胁分析能力, 验证了云安全场景下算法的有效性。

6 总结与展望

本文提出了一种基于层次化图神经网络进行云资产安全性分析的方法, 通过将云系统在异质、动态、有向的属性图上进行建模并使用改进的图结构注意力网络和改进的循环神经网络分别对云中多源异

构网络信息进行结构和时序上的关联分析, 获得节点在不同时刻的特征表示, 最后通过一类分类器来判别节点是否为失陷资产, 实现了云资产安全性分析。

在算法的能力维度上, 本文所提出的算法完全覆盖了五种描述系统特征的图特性。仿真实验结果表明, 该算法具有较强的多源异构数据关联分析能力, 在精度、准确率和召回率上实现了较好的平衡, 可以有效地挖掘出失陷节点, 支撑云安全态势感知。

由于云系统的图模型中边具有丰富的特征信息, 因此, 如何在图神经网络中更好地利用边特征, 使得节点和边的特征表示能够互相验证、互相增强, 仍需深入研究。同时, 本文所提出的算法可以有效识别出失陷资产, 但如何识别威胁种类、分析云系统中资产失陷的原因以及评估威胁所造成的损失, 仍需要进行深入研究。

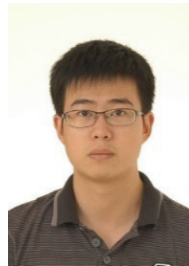
参考文献

- [1] Bahareth F A, Bamasak O O. Constructing attack scenario using sequential pattern mining with correlated candidate sequences[J]. *Res Bull Jordan ACM, II (III)*, 2013: 102-108.
- [2] Fine S, Singer Y, Tishby N. The Hierarchical Hidden Markov Model: Analysis and Applications[J]. *Machine Learning*, 1998, 32(1): 41-62.
- [3] Hinton G E, Osindero S, Teh Y W. A Fast-Learning Algorithm for Deep Belief Nets[J]. *Neural Computation*, 2006, 18(7): 1527-1554.
- [4] Harary F, Gupta G. Dynamic Graph Models[J]. *Mathematical and Computer Modelling*, 1997, 25(7): 79-87.
- [5] Veličković P, Cucurull G, Casanova A, et al. Graph Attention Networks [EB/OL]. 2017: arXiv: 1710.10903. <http://arxiv.org/abs/1710.10903.pdf>.
- [6] Bhagat S, Cormode G, Muthukrishnan S. Node Classification in Social Networks[M]. *Social Network Data Analytics*. Boston, MA: Springer, 2011: 115-148.
- [7] Yamashita R, Nishio M, Do R K G, et al. Convolutional Neural Networks: An Overview and Application in Radiology[J]. *Insights into Imaging*, 2018, 9(4): 611-629.
- [8] Scarselli F, Gori M, Tsoi A C, et al. The Graph Neural Network Model[J]. *IEEE Transactions on Neural Networks*, 2009, 20(1): 61-80.
- [9] Ioannidis V N, Marques A G, Giannakis G B. A Recurrent Graph Neural Network for Multi-Relational Data[C]. *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2019: 8157-8161.
- [10] Zhou J, Cui G Q, Hu S D, et al. Graph Neural Networks: A Review of Methods and Applications[J]. *AI Open*, 2020, 1: 57-81.
- [11] Salha G, Hennequin R, Vazirgiannis M. Keep it Simple: Graph Autoencoders without Graph Convolutional Networks [EB/OL]. 2019: arXiv: 1910.00942. <http://arxiv.org/abs/1910.00942>.
- [12] Wu Z H, Pan S R, Long G D, et al. Graph WaveNet for Deep Spatial-Temporal Graph Modeling [EB/OL]. 2019: arXiv: 1906.00121. <http://arxiv.org/abs/1906.00121>.

- [13] Zheng L, Li Z, Li J, et al. AddGraph: Anomaly Detection in Dynamic Graph Using Attention-based Temporal GCN[C]. *IJCAI*. 2019: 4419-4425.
- [14] Cai L, Chen Z Z, Luo C, et al. Structural Temporal Graph Neural Networks for Anomaly Detection in Dynamic Graphs[C]. *The 30th ACM International Conference on Information & Knowledge Management*, 2021: 3747-3756.
- [15] Wu Y L, Dai H N, Tang H N. Graph Neural Networks for Anomaly Detection in Industrial Internet of Things[J]. *IEEE Internet of Things Journal*, 2022, 9(12): 9214-9231.
- [16] Liu Y X, Li Z, Pan S R, et al. Anomaly Detection on Attributed Networks via Contrastive Self-Supervised Learning[J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2022, 33(6): 2378-2392.
- [17] Goodge A, Hooi B, Ng S K, et al. LUNAR: Unifying Local Outlier Detection Methods via Graph Neural Networks[J]. *Proceedings of the AAAI Conference on Artificial Intelligence*, 2022, 36(6): 6737-6745.
- [18] Zhou J W, Xu Z Y, Rush A M, et al. Automating Botnet Detection with Graph Neural Networks [EB/OL]. 2020: arXiv: 2003.06344. <http://arxiv.org/abs/2003.06344>.
- [19] Wan Y, Liu Y L, Wang D, et al. GLAD-PAW: Graph-Based Log Anomaly Detection by Position Aware Weighted Graph Attention Network[C]. *Pacific-Asia Conference on Knowledge Discovery and Data Mining*, 2021: 66-77.
- [20] Busch J, Kocheturov A, Tresp V, et al. NF-GNN: Network Flow Graph Neural Networks for Malware Detection and Classification[C]. *The 33rd International Conference on Scientific and Statistical Database Management*, 2021: 121-132.
- [21] Yu Y, Si X S, Hu C H, et al. A Review of Recurrent Neural Networks: LSTM Cells and Network Architectures[J]. *Neural Computation*, 2019, 31(7): 1235-1270.
- [22] Zhao Y, Wang S W, Xiao F. Pattern Recognition-Based Chillers Fault Detection Method Using Support Vector Data Description (SVDD)[J]. *Applied Energy*, 2013, 112: 1041-1048.
- [23] VAST Challenge 2012 [EB/OL]. <http://www.vacommunity.org/VAST+Challenge+2012>.
- [24] A. D. Kent, Comprehensive, Multi-Source Cybersecurity Events, Los Alamos National Laboratory, <http://dx.doi.org/10.17021/1179829>, 2015.
- [25] Jiang X, Ji P, Li S. CensNet: Convolution with Edge-Node Switching in Graph Neural Networks[C]. *IJCAI*. 2019: 2656-2662.
- [26] Sankar A, Wu Y H, Gou L, et al. DySAT: Deep Neural Representation Learning on Dynamic Graphs via Self-Attention Networks[C]. *The 13th International Conference on Web Search and Data Mining*, 2020: 519-527.
- [27] Oh J, Cho K, Bruna J. Advancing GraphSAGE with a Data-Driven Node Sampling [EB/OL]. 2019: arXiv: 1904.12935. <http://arxiv.org/abs/1904.12935>.
- [28] Shi L, Liao Q, Yang C X. Investigating Network Traffic through Compressed Graph Visualization: VAST 2012 Mini Challenge 2 Award: "Good Adaptation of Graph Analysis Techniques" [C]. *2012 IEEE Conference on Visual Analytics Science and Technology*, 2012: 279-280.
- [29] Hildenbrand J, Pavall D I, Thapa P, et al. VAST 2012 Mini-Challenge 2: Chart- and Matrix-Based Approach to Network Operations Forensics[C]. *2012 IEEE Conference on Visual Analytics Science and Technology*, 2012: 287-288.



张义莲 于 2013 年在东南大学电气工程专业获得硕士学位。现任国网上海市电力公司数字化工作部高级工程师。研究领域: 云技术、信息网络安全、信息系统运行。研究兴趣包括: 信息运行及网络安全, 云平台技术。Email: zhangyilian@sh.sgcc.com.cn



周笛青 于 2013 年在上海大学电力电子与电力传动专业获得硕士学位。现在国网上海市电力公司调控中心任中级工程师。研究领域: 电网调度运行控制、调控云平台。研究兴趣包括: 信息网络技术, 调控云、电力市场交易。Email: zhoudq@sh.sgcc.com.cn



许力文 于 2021 年在西安电子科技大学网络空间安全专业获得学士学位。现在上海交通大学网络空间安全专业攻读硕士学位。研究领域为网络安全态势感知。研究兴趣包括: 多源异构网络安全数据融合分析。Email: livingxu@sjtu.edu.cn



叶天鹏 于 2018 年在上海交通大学网络空间安全专业获得硕士学位。现在上海交通大学网络空间安全专业攻读博士学位。研究领域为移动边缘计算, 网络安全态势感知。研究兴趣包括: 多模态入侵检测、人工智能。Email: ytp_sjtu_2015@sjtu.edu.cn



林祥 于 2019 年在上海交通大学通信与信息系统专业获得工学博士学位。现任上海交通大学网络安全技术研究院院长助理, 研究领域为互联网内容安全、网络安全综合管理。Email: lionel@sjtu.edu.cn