计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(12):234−238 [doi: 10.15888/j.cnki.csa.007717]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于图神经网络的工控网络异常检测算法①

刘　杰[1,2], 李喜旺[2]

[1](中国科学院大学, 北京 100049)
[2](中国科学院 沈阳计算技术研究所, 沈阳 110168)
通讯作者: 刘　杰, E-mail: 2276426207@qq.com

摘　要: 网络异常检测技术成为入侵检测领域的重点研究内容, 但由于目前网络异常检测大多都停留在单点网络异常检测, 对不断更新的联合异常攻击和恶意软件无法做出快速及时的相应. 本文提出了一种基于图神经网络的工控网络异常检测算法, 融合网络节点自身属性以及网络拓扑结构中邻域节点的信息实现对网络异常的检测. 首先, 每个网络节点获取蕴含了连接节点的特征信息以及节点之间交互信息的状态向量; 其次, 每个节点使用不动点理论对网络进行迭代更新; 最后, 根据节点自身信息以及邻域节点信息通过神经网络提取更高层次的特征作为该节点的表示, 最后用聚类进行工控网络节点异常行为检测. 实验结果表明, 本文提出算法在具有较高检测率的同时, 也具有较高的鲁棒性.

关键词: 图神经网络; 异常检测; 入侵检测; 信息融合; 聚类

引用格式: 刘杰,李喜旺.基于图神经网络的工控网络异常检测算法.计算机系统应用,2020,29(12):234–238. http://www.c-s-a.org.cn/1003-3254/7717.html

Anomaly Detection Algorithm in Industrial Control Network Based on Graph Neural Network

LIU Jie[1,2], LI Xi-Wang[2]

[1](University of Chinese Academy of Sciences, Beijing 10004, China)
[2](Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China)

Abstract: Network anomaly detection technology has become the focus of research in the field of intrusion detection. However, because most of the current network anomaly detection remains at a single point of network anomaly detection, it cannot respond quickly and timely to joint anomaly attacks and malware that are constantly updated. In this study, a industrial control network anomaly detection algorithm based on graph neural network is proposed, which combines the network node's own attributes and the information of neighbor nodes in the network topology to realize the network anomaly detection. First, each network node obtains a state vector that contains the feature information of the connected nodes and the interaction information between the nodes. Second, each node uses the fixed point theory to iteratively update the network. Thirdly, according to the node's own information and neighbor node's information, extract higher-level features through the neural network as the representation of the node. Finally, clustering is used to detect the abnormal behavior of industrial control network nodes. Experimental results show that the algorithm proposed in this study has high detection rate and high robustness.

Key words: graph neural network; anomaly detection; intrusion detection; information fusion; clustering

① 基金项目: 辽宁省"兴辽英才计划"(XLYC1908019)
Foundation item: Talent Program of Revitalizing Liaoning, Liaoning Province (XLYC1908019)
收稿时间: 2020-04-21; 修改时间: 2020-06-03, 2020-06-15; 采用时间: 2020-06-19; csa 在线出版时间: 2020-11-30

随着科学技术的迅速发展, 人们的日常生活中也逐渐离不开网络. 由于网络信息不断产生和变化, 使得网络安全问题也成为计算机领域的一个热门的研究方向. 目前网络攻击发生在我们生活中的方方面面, 加之网络攻击类型的千变万化, 网络攻击者通过各种不同的手段攻击各种公共设施和用户个人隐私信息[1], 比如“橙风单车”投用第二天就遭到黑客攻击, 导致系统瘫痪, 用户无法正常体验、使用. 随着信息化时代的发展, 目前网络数据已经不仅仅是静态的单个节点的影响, 而是以不断变化的形式存在, 因此传统的网络异常检测算法已不能满足数据实时、准确的检测要求, 对不断更新的新的网络攻击手段无法迅速的做出相应的裁决和相应, 因此我们需要更加快速和准确的检测网络异常的方法, 已保证在高速网络的数据到来时能够对数据及时做出相应[2].

目前常用的网络入侵检测的方法主要有两种: 误用检测和异常检测[3]. 误用检测需要事先建立网络异常的特征规则库, 并将采集到的每个数据包与规则库的每一条规则进行一一匹配, 根据此判断网络中是否存在异常. 误用检测的优点是检测率高、误报率低, 缺点是对未知特征的新异常行为, 误用检测就表现毫无应对能力. 而异常检测完全不同于误用检测, 异常检测所关注的是网络流量的宏观统计特征, 异常检测首先需要提取或者概括网络流量的统计特征, 据此建立一个正常模型. 是将当前产生的活动模型与正常模型作比较, 当当前的活动模型与正常活动模型不匹配时, 异常检测就会发出警报. 异常检测的优点是可以检测出以前从未出现的网络攻击方法, 但缺点是误报率较高[4,5].

1 目前的研究

近年来, 为了应对网络异常入侵的多样性, 加之为提高网络异常检测的检测率, 降低网络异常检测的误报率, 国内外的学者对此已经做了大量的研究工作, 目前网络异常检测方法大致分为两大方面: 动态网络异常检测和静态网络异常检测.

在静态网络异常检测中, 最为代表的是基于阈值的网络检测方法. 在基于阈值检测的方法中, Maxion 等[6]提出根据历史网络流量的特征建立阈值, 一旦超出此阈值即判断为网络异常[7].

在动态网络异常检测中, 典型的方法即基于统计的检测方法, 比如基于用户画像的异常行为检测模型[8]中提出引入用户画像技术, 实现了入侵检测粒度的细化, 并将大数据技术引入网络安全领域, 证明了基于用户画像的入侵检测模型有较好的实用价值. 基于隐马尔可夫模型和条件熵的异常流量检测方法研究中[1]中提出运用统计学的方法对流量分类, 最后通过输出概率值来判断是否是异常类型, 该方法明显的提高了异常检测的精确度和检测率, 但是只能对流量进行笼统的分类为异常和正常, 无法做到更精细的划分.

但由于网络流量不仅存在相似性和周期性的特点, 还存在多点之间的连接性, 因此当网络攻击者对我们的网络进行入侵时, 往往不是单独的某个点对我们的网络造成极大的攻击, 而是多个网络攻击者联合攻击对我们的网络造成网络崩溃, 网络节点关系如图 1 所示. 因此目前的单点网络异常检测已满足不了现阶段对网络攻击者的防御和对其预测. 另外, “网络异常”也是一个很模糊的概念, 工控网络异常检测通常表现为结构和属性的变化, 异常当然也包括网络节点本身的异常以及网络变化的异常, 因此在本文中, 我们基于工控网络中的多点连接性提出了基于图神经网络的工控网络异常检测算法, 将图神经网络应用于工控网络异常检测, 这样就可以同时抓取工控网络结构、属性以及其周围点邻域状态上的异常. 从而使算法能够脱离单点的网络异常检测.

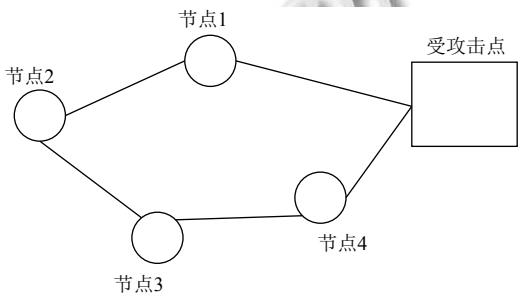

图 1 网络节点图关系

最终将该模型与单点检测算法比较, 证明了该算法具有较高的准确率, 验证了该算法的有效性.

2 基于图神经网络的工控网络异常检测

2.1 问题描述

对于我们日常生活中的网络拓扑结构, 工控网络节点的结构特征和属性以及工控网络节点之间的连接关系, 本文中提出的基于图神经网络的工控网络异常检测算法的目标是: 充分利用工控网络节点之间的属

性信息和工控网络拓扑结构的信息, 挖掘工控网络节点之间的隐含的交互信息, 并学习每个工控网络节点的类标签. 表 1 给出本文中相关的符号定义.

表 1 符号定义

名称	描述
$G=(V,E,X)$	网络拓扑结构图
V	网络节点集合
E	网络连边集合
n	网络节点的数量
X	网络节点特征矩阵
H_v	每个节点的状态向量
$softmax(x)_i$	G中第i个节点的标签分布

2.2 图神经网络

图神经网络 (Graph Neural Network, GNN) 是近几年出现的一类以图结构作为网络输入的神经网络模型[9]. 由于图神经网络处理的数据结构是图, 而图是一种主要针对非欧几里得空间结构的数据进行处理, 具有以下优势:

(1) 对输入元素数据的顺序不敏感;

(2) 在图计算过程中, 节点的表示受周围邻居节点的结构和属性的影响, 而图本身的连接不变;

(3) 将网络节点表示为图结构表示, 便于进行基于图的推理, 对网络异常检测具有天然的优势.

同时受到网络嵌入的启发, 本文旨在学习一个图神经网络映射函数, 通过该映射函数将图中的某一节点V_i可以聚合它自己的特征X_i与它相关联的邻居的特征X_j来生成节点V_i的新表示, 然后将其作为 K-means 的输入, 进行聚类算法, 判断该节点是否异常. 图神经网络结构图如图 2 所示.

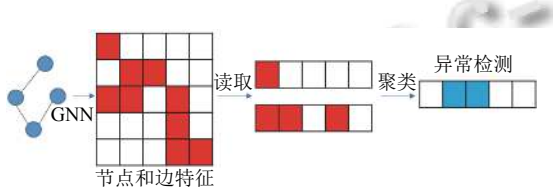

图 2 图神经网络结构图

2.3 基于图神经网络的网络异常检测

图神经网络模型由三大部分组成: 图节点状态向量获取模块、迭代更新模块和损失函数模块[10].

(1) 图节点状态向量获取

首先每个节点V_i都可以用其特征X_i表示, 并与其已标记的标签相关联. 给定部分标记的图$G=(V,E)$, 利用已标记的节点来预测未标记的节点标签. 它可以通过学习得到每个节点的 d 维状态向量表示为H_v, 同时已包含了其相邻节点的状态信息.

$$H_v = f(X_v, X_{co}, H_{ne}, X_{ne}) \tag{1}$$

其中, X_v表示节点的属性特征集合, X_{co}表示边的特征集合, H_{ne}表示样本 v 的邻居节点的嵌入表示, X_{ne}表示节点 v 的邻居节点的属性特征. $f(x)$函数表示将输入节点的特征映射到 d 维向量空间的一个映射函数.

(2) 迭代更新

根据上述算法可以获取到每个节点的 d 维状态向量, 该向量蕴含了连接节点的特征信息以及节点之间的交互信息. 由于我们要求出H_v的唯一解, 在本文中我们选择使用不动点理论重写上述方程进行迭代更新.

$$H^{t+1} = f\left(H^t, X\right) \tag{2}$$

其中, H 和 X 表示所有 h 和 x 的连接.

然而对于每个节点, 其邻域节点的交互信息固然重要, 但其自身节点的原始信息也包含了很多重要的状态信息. 因此将节点的状态向量H_v以及节点的特征X_v同时传递给输出函数g进一步计算, 得到 GNN 的输出, 即是否为异常节点. 即:

$$O_v = g(H_v, X_v) \tag{3}$$

其中, $f(x)$和$g(x)$是全连接前馈神经网络.

(3) 损失函数

给定一个图$G=(V,E,X)$, 经过上述的状态向量获取和迭代更新, 每个节点都可以用一个具有既包含节点自身信息又有样本邻域交互信息的状态向量表示. 在本文中根据词特征向量, 我们使用$softmax(x)$函数为每个节点计算每个类别对应的概率, $softmax(x)$函数定义如下:

$$softmax(x)_i = \frac{e^{x_i}}{\sum_{k=1}^{K} e^{x_k}} \tag{4}$$

最后在该模型中, 我们使用交叉熵计算模型的损失 $loss$, 其计算公式如下:

$$loss = \sum_{i=1}^{n} y_c \log(softmax(x)_i) \tag{5}$$

其中, y 表示真实的标签.

图神经网络的算法进行节点特征表示的过程图如图 3 所示.

2.4 K-means 数据聚类

聚类算法是一个将数据集划分成若干个聚类的过程, 使得同一聚类的类内相似性最大, 类间相似性最小.

相似性的度量我们选用基于距离的方法. 在本文中我们选用欧几里得距离, 计算公式如下:

$$d(i,j)=\sqrt{|x_{i1}-x_{j1}|^2+|x_{i2}-x_{j2}|^2+\cdots+|x_{ip}-x_{jp}|^2} \quad (6)$$

常用的聚类算法包括 K 均值聚类、密度聚类、层次聚类. 在本文中我们选择 K-means 聚类, K-means 聚类算法是将 n 个样本点划分成 k 个子集, 每个子集都代表一个聚类.

K-means 算法的步骤:

① 在已研究的基础上, 将所有的样本根据类标种类分为 k 个类, 记为 k 个种子聚类中心.

② 计算每个样本与种子聚类中心之间的距离, 并把每个样本点分配到距离最近的聚类中心点, 即聚类中心及分配的样本点代表一个簇.

③ 计算每个簇的均值作为每个簇的质心, 重复步骤②, 直至质心不再发生变化, 确定 k 的值.

将上述图神经网络的网络节点输出特征作为 K-means 聚类的输入, 判断网络节点是否是异常节点.

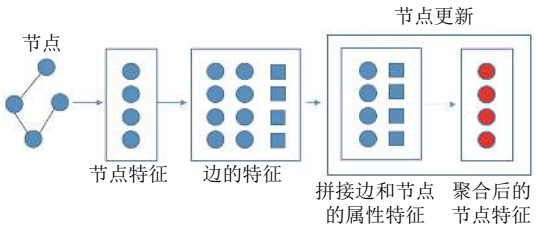

图 3 节点特征表示的过程图

3 实验部分

3.1 数据说明与预处理

为了评价本文提出的网络异常检测算法, 使用 Libpcap 网络工具获取中科院沈阳计算技术研究所使用的内部网络数据, 主要是原始网络的流量数据.

在本文中选取 TCP 连接的基本特征比如连续时间, 协议类型、传送的字节数、连接正常或错误的状态和 TCP 连接的内容特征比如登录尝试失败的次数、成功登录的次数, root 用户访问次数和文件创建操作次数等属性对网络节点数据进行分析.

为了剔除数据集中的“脏数据”, 与网络节点异常无关的数据、重复采集的数据、数据格式错误或 null 值的数据, 需要先对数据进行预处理, 找出数据的特征表示, 为算法提供可靠的数据保证. 对于数据的预处理主要包括两大部分, 首先利用 Python 3 将获取的字符型特征转换为数值型特征, 其次对数据进行标准化和归一化处理. 在本文中使用的是 min-max 标准化方法, 即对原始数据的线性变换, 使数据结果归一化到 [0,1] 区间转换函数如下:

$$y_i=\frac{x_i-\min\limits_{i\le j\le n}\{x_j\}}{\max\limits_{i\le j\le n}\{x_j\}-\min\limits_{i\le j\le n}\{x_j\}} \quad (7)$$

其中, max 为样本数据的最大值, min 为样本数据的最小值.

3.2 实验平台

使用基于 Python3 环境的 Tensorflow 开源深度学习框架实现图神经网络的模型构建与异常检测. 本文实验采用 PC 机, 内存为 16 GB, 操作系统为 Windows、Linux.

3.3 实验结果与分析

在该网络异常检测算法中, 模型的结果评估使用准确率和误判率来评价模型的性能. 具体如表 2.

表 2 混淆矩阵

混淆矩阵		样本数	
		Positive	Negative
检测数	Positive	*TP*	*FP*
	Negative	*FN*	*TN*

准确率表示为:

$$Acc=\frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

传统聚类单点检测算法得到的聚类结果图和经图神经网络处理后网络节点异常检测结果分别如图 4 和图 5 所示.

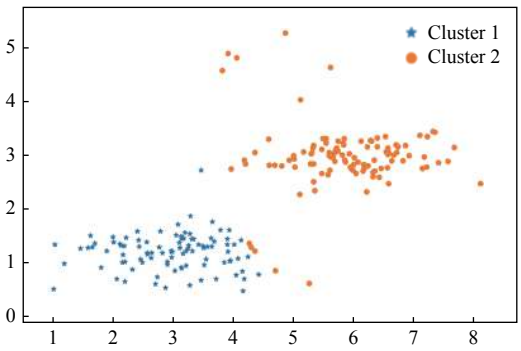

图 4 传统聚类结果

本文模型在准确率和误报率与其他传统网络异常检测模型比较, 具体如表 3.

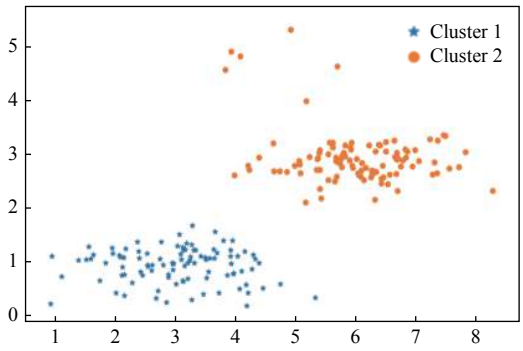

图 5 图神经网络处理聚类结果

表 3 结果对比表 (%)

模型	准确率	误报率
聚类	83.4	1.2
本文模型	90.6	0.8

4 结束语

网络异常检测已经成为网络安全的一个重要研究方向, 本文提出的基于图神经网络的网络异常检测算法可以融合网络节点自身属性以及其邻域节点的属性信息进行训练, 弥补了以往的单节点的动态预测方法的不足, 实验证明该方法具有较好的鲁棒性, 但是该算法也具有一定的局限性, 对于进一步的节点之间的相关性研究及图神经网络更精确精准的异常检测是我们下一步的研究重点.

参考文献

1 肖林英, 王怀彬. 基于隐马尔可夫模型和条件熵的异常流量检测方法研究. 天津理工大学学报, 2019, 35(5): 18–22, 28.
2 陈胜, 朱国胜, 祁小云, 等. 基于深度神经网络的自定义用户异常行为检测. 计算机科学, 2019, 46(S2): 442–445, 472.
3 Bykova M, Ostermann S, Tjaden B. Detecting network intrusions via a statistical analysis of network packet characteristics. Proceedings of the 33rd Southeastern Symposium on System Theory. Athens, OH, USA. 2001. 309–314.
4 李洋, 方滨兴, 郭莉, 等. 基于直推式方法的网络异常检测方法. 软件学报, 2007, 18(10): 2595–2604.
5 王子玉. 网络异常检测算法研究 [博士学位论文]. 北京: 清华大学, 2017.
6 Maxion RA, Feather FE. A case study of Ethernet anomalies in a distributed computing environment. IEEE Transactions on Reliability, 1990, 39(4): 433–443. [doi: 10.1109/24.58721]
7 邹柏贤. 一种网络异常实时检测方法. 计算机学报, 2003, 26(8): 940–947.
8 赵刚, 姚兴仁. 基于用户画像的异常行为检测模型. 信息网络安全, 2017, (7): 18–24.
9 Battaglia PW, Hamrick JB, Bapst V, *et al*. Relational inductive biases, deep learning, and graph networks. arXiv: 1806.01261, 2018.
10 郝志峰, 柯妍蓉, 李烁, 等. 基于图编码网络的社交网络节点分类方法. 计算机应用, 2020, 40(1): 188–195.