(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115175192 A
(43)申请公布日 2022.10.11

(21)申请号 202210793631.8

(22)申请日 2022.07.05

(71)申请人 杭州电子科技大学
地址 310018 浙江省杭州市下沙高教园区2号大街

(72)发明人 伍益明 梁巧媛 徐明 郑宁

(74)专利代理机构 杭州君度专利代理事务所(特殊普通合伙) 33240
专利代理师 杨舟涛

(51)Int.Cl.
H04W 12/121(2021.01)
H04W 4/40(2018.01)
G06N 3/04(2006.01)
G06N 3/08(2006.01)

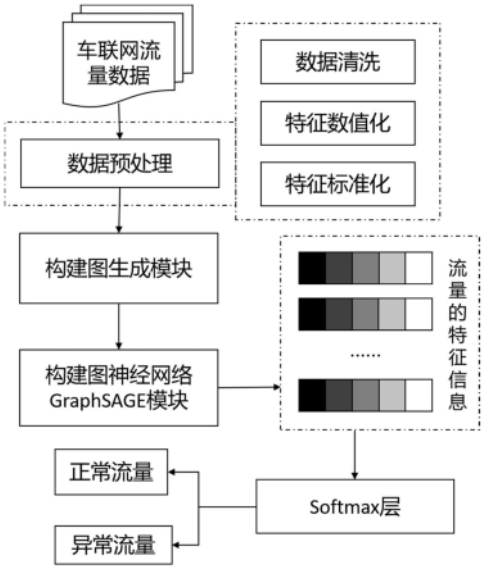
权利要求书2页 说明书6页 附图4页

(54)发明名称

一种基于图神经网络的车联网入侵检测方法

(57)摘要

本发明公开了一种基于图神经网络的车联网入侵检测方法;本发明所述方法包括:收集车联网流量数据并对原始流量数据进行预处理;构建图生成模块,将预处理过的流量数据转化为图结构数据;构建图神经网络模型GraphSAGE作为图特征提取器来提取流量的结构特征和属性特征信息;将提取到的特征作为Softmax层的输入,输出得到是否是攻击流量的概率值来检测入侵。本发明方法在车联网入侵检测任务上展示了巨大的潜力,有效地提高了入侵检测的准确率。



CN 115175192 A

1.一种基于图神经网络的车联网入侵检测方法,其特征在于,该方法具体包括以下步骤:

步骤S1:收集车联网流量数据,对原始流量数据进行预处理;

步骤S2:构建图生成模块,将预处理过的流量数据转化为图结构数据;

所述的图生成模块具体为:

S2.1:构建车辆通信图G:流量数据是由车辆ID标识,并通过一组提供流详细信息的字段进行注释,流量数据以图的形式表示:G=(V,E),其中节点集合V表示车辆,边集E代表车辆之间的通信流;将车联网入侵检测问题建模为一个边分类问题;

引入线图,基于车辆通信图G生成相应的流量连通图G_L;

S2.2:构建流量连通图G_L:$G_L=(V_L,E_L)$表示相应的流量连通图,E_L表示G_L的边集,代表流量之间的相关性,那么G_L的节点集是G的边集,即$V_L=\{(v_i,v_j)\in E\}$且$|V_L|=|E|$,如果G中的两条边共享一个节点,则G_L中存在一条边;G_L的边集用邻接矩阵$A_L\in\mathbb{R}^{|E|\times|E|}$表示

$$A_L(v_i,v_j),(v_j,v_k)=\begin{cases}1 & \text{if } i\neq j \text{ and } j\neq k\\ 0 & \text{otherwise}\end{cases}$$

流量连通图的属性特征定义为$X_L\in\mathbb{R}^{N\times F}$,其中N表示流量的条数,F表示流量的特征维度,借助流量连通图G_L,车联网入侵检测问题转化为节点分类问题;

步骤S3:构建图神经网络模块,将上述图结构数据输入到图神经网络模块中,提取流量的结构特征和属性特征信息;

步骤S4:将提取的特征信息通过Softmax层输出概率分布,根据相关指标对模型进行性能评估。

2.根据权利要求1所述的一种基于图神经网络的车联网入侵检测方法,其特征在于:

所述的步骤S1预处理包括:

S1.1:数据清洗:消除冗余特征,用平均值代替Nan,用最大值代替Inf;

S1.2:特征数值化:使用python中get dummies函数将分类特征转换为数值特征;

S1.3:特征标准化:由于数据各个特征的尺度不同,为了消除特征间尺度差异的影响,对特征进行标准化处理。

3.根据权利要求1所述的一种基于图神经网络的车联网入侵检测方法,其特征在于:所述的图神经网络模块为GraphSAGE模块。

4.根据权利要求3所述的一种基于图神经网络的车联网入侵检测方法,其特征在于:所述的构建GraphSAGE模块,具体操作为:

S3.1:根据构建的流量连通图的结构特征A_L和属性特征X_L,针对每个流量节点$\forall v_i\in V$,从其相邻节点集合$\mathcal{N}(v_i)$随机均匀采样固定数量的节点来进行聚合特征,采样的邻居数为S_k,如果实际邻居数小于S_k,则使用带回放的采样方法,如果实际邻居数大于S_k,则使用不带回放的采样方法;

S3.2:选择池化聚合函数来聚合相邻节点的特征,池化函数是对称的,因为要确保输出不随节点的顺序而变化,即$AGG(v_1,v_2)=AGG(v_2,v_1)$;

第k层的池化聚合函数定义为:

$$AGG^k=\max(\sigma(W\times h^{k-1}_{\mathcal{N}(v_i)}+b))$$

其中$h_{\mathcal{N}(v_i)}^{k-1}$代表节点$v_i$的邻居集合$\mathcal{N}(v_i)$在经GraphSAGE提取的第k-1层的聚合特征，σ表示非线性激活函数，W表示要训练的权重矩阵，b表示偏置量；公式解析为先将所有前一层相邻节点的聚合特征通过一个全连接层，再利用非线性激活函数，最后使用最大池化聚合；

则第k层的相邻节点$\mathcal{N}(v_i)$的聚合信息表示为：

$$h_{\mathcal{N}(v_i)}^{k} = AGG^{k}(\{h_u^{k-1}, \forall u \in \mathcal{N}(v_i)\})$$

S3.3：将聚合生成的相邻节点的表示向量$h_{\mathcal{N}(v_i)}^{k}$与中心节点前一层的特征$h_{v_i}^{k-1}$合并，最后输入到一个全连接层，更新中心节点v_i的特征向量，并对其进行规范化：

$$h_{v_i}^{k} = \sigma\left(W^{k} \cdot CONCAT(h_{v_i}^{k-1}, h_{\mathcal{N}(v_i)}^{k})\right)$$

$$h_{v_i}^{k} = Norm(h_{v_i}^{k})$$

对车联网中所有流量节点进行K层GraphSAGE聚合后，对于每个流量节点v_i得到该节点的聚合特征$h_{v_i}^{K}$，表示捕获其K-hop邻域中的信息。

5.根据权利要求1所述的一种基于图神经网络的车联网入侵检测方法，其特征在于：所述的将提取的特征信息通过Softmax层输出概率分布，根据相关指标对模型进行性能评估，具体为：

根据Softmax层将GraphSAGE模块的输出结果转化成概率分布，具有最高概率所属的类别被视为模型的预测类；经过多次迭代训练后通过计算模型输出的预测值与真实标签的交叉熵损失执行反向传播和更新权重，使用Adam模型优化器不断优化模型参数，使损失达到最小，权重收敛，得到最优的模型参数；然后采用测试集测试模型，获得流量的类别预测值，并根据相关指标对模型性能进行评估，相关指标计算如下：

$$Recall = \frac{TP}{TP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$F - score = 2 \times \frac{Recall \times Precision}{Recall + Precision}$$

其中TP表示正确预测的攻击流量数，FN表示错误识别为正常的攻击流量数，FP表示错误识别为攻击的正常流量数。

一种基于图神经网络的车联网入侵检测方法

技术领域

[0001] 本发明属于车联网安全技术领域，具体涉及一种基于图神经网络的车联网入侵检测方法。

背景技术

[0002] 随着5G和人工智能等新兴技术在智能交通系统的实践应用，车联网可以真正实现车与车，车与基础设施，车与人的全方位网络连接，从而避免交通事故，提高运输安全和效率。车辆相对较快的移动速度使车联网具有高度动态的网络拓扑结构，无线通信信道的开放性会使网络连接不稳定，这些特点为车联网网络安全带来了极大的风险。入侵检测系统通过分析车联网中大量的流量信息可以高效地识别各种恶意攻击行为，使它成为了保障车联网安全问题的一种解决方案。

[0003] 为了降低车联网中存在的安全风险，许多学者借助深度学习技术提出了针对车联网的入侵检测方法。主要是利用深度学习技术捕获车联网原始流量数据的高维特征和其是否为恶意流量之间复杂的非线性关系，从而识别车联网的各种攻击行为。田纳西大学Wyk博士提出将卷积神经网络与基于χ^2检测器的卡尔曼滤波的异常检测方法相结合，用于检测车联网中的异常行为。北京大学曾博士提出首先借助卷积神经网络提取流量空间特征，然后输入长短期记忆网络学习时间相关特征的模型。印度比尔拉科学技术学院Alladi博士提出先将原始流量处理成时间序列数据，再将时间序列数据转换成灰度图像以便输入卷积神经网络，从而将问题转化为图像分类。随后，Alladi博士又提出利用深度学习模型进行序列重构，通过计算原始序列和重构序列之间的误差对序列进行分类来检测未知的网络攻击。

[0004] 但是以上深度学习技术将车联网流量建模为图像或者序列数据存在极大的局限性，忽略了车联网本质上是图结构数据这一事实导致了较高的误报率。如何在图结构数据中挖掘异常元素是比较困难的问题，图神经网络作为处理图结构数据的深度学习技术，展示了其强大的图数据拟合能力。因此，为了解决车联网入侵检测问题，本发明结合车联网的网络结构特征和流量节点的属性特征，提出一种基于图神经网络的车联网入侵检测方法。

发明内容

[0005] 针对现有技术存在的问题，本发明的目的是提供一种基于图神经网络的车联网入侵检测方法，以提高车联网入侵检测的准确率，解决车联网通信网络安全问题。

[0006] 为实现上述目的，本发明方法主要流程包括以下步骤：

[0007] 步骤S1:收集车联网流量数据，对原始流量数据进行预处理；

[0008] 步骤S2:构建图生成模块，将预处理过的流量数据转化为图结构数据；

[0009] 所述的图生成模块具体为：

[0010] S2.1:构建车辆通信图G:流量数据是由车辆ID标识，并通过一组提供流详细信息的字段进行注释，流量数据以图的形式表示:G＝(V,E)，其中节点集合V表示车辆，边集E代表车辆之间的通信流;将车联网入侵检测问题建模为一个边分类问题；

[0011] 引入线图，基于车辆通信图G生成相应的流量连通图G_L；

[0012] S2.2：构建流量连通图G_L：$G_L=(V_L,E_L)$表示相应的流量连通图，E_L表示G_L的边集，代表流量之间的相关性，那么G_L的节点集是G的边集，即$V_L=\{(v_i,v_j)\in E\}$且$|V_L|=|E|$，如果G中的两条边共享一个节点，则G_L中存在一条边；G_L的边集用邻接矩阵$A_L\in\mathbb{R}^{|E|\times|E|}$表示

[0013] $$A_L(v_i,v_j),(v_j,v_k)=\begin{cases}1 & \text{if } i\neq j \text{ and } j\neq k\\ 0 & \text{otherwise}\end{cases}$$

[0014] 流量连通图的属性特征定义为$X_L\in\mathbb{R}^{N\times F}$，其中N表示流量的条数，F表示流量的特征维度，借助流量连通图G_L，车联网入侵检测问题转化为节点分类问题；

[0015] 步骤S3：构建图神经网络模块，将上述图结构数据输入到图神经网络模块中，提取流量的结构特征和属性特征信息；

[0016] 步骤S4：将提取的特征信息通过Softmax层输出概率分布，根据相关指标对模型进行性能评估。

[0017] 作为优选，所述的步骤S1预处理包括：

[0018] S1.1：数据清洗：消除冗余特征，用平均值代替Nan，用最大值代替Inf；

[0019] S1.2：特征数值化：使用python中get dummies函数将分类特征转换为数值特征；

[0020] S1.3：特征标准化：由于数据各个特征的尺度不同，为了消除特征间尺度差异的影响，对特征进行标准化处理。

[0021] 作为优选，所述的图神经网络模块为GraphSAGE模块。

[0022] 作为优选，所述的构建GraphSAGE模块，具体操作为：

[0023] S3.1：根据构建的流量连通图的结构特征A_L和属性特征X_L，针对每个流量节点$\forall v_i\in V$，从其相邻节点集合$\mathcal{N}(v_i)$随机均匀采样固定数量的节点来进行聚合特征，采样的邻居数为S_k，如果实际邻居数小于S_k，则使用带回放的采样方法，如果实际邻居数大于S_k，则使用不带回放的采样方法；

[0024] S3.2：选择池化聚合函数来聚合相邻节点的特征，池化函数是对称的，因为要确保输出不随节点的顺序而变化，即$AGG(v_1,v_2)=AGG(v_2,v_1)$；

[0025] 第k层的池化聚合函数定义为：

[0026] $$AGG^k=\max(\sigma(W\times h_{\mathcal{N}(v_i)}^{k-1}+b))$$

[0027] 其中$h_{\mathcal{N}(v_i)}^{k-1}$代表节点$v_i$的邻居集合$\mathcal{N}(v_i)$在经GraphSAGE提取的第k-1层的聚合特征，σ表示非线性激活函数，W表示要训练的权重矩阵，b表示偏置量；公式解析为先将所有前一层相邻节点的聚合特征通过一个全连接层，再利用非线性激活函数，最后使用最大池化聚合；

[0028] 则第k层的相邻节点$\mathcal{N}(v_i)$的聚合信息表示为：

[0029] $$h_{\mathcal{N}(v_i)}^k=AGG^k(\{h_u^{k-1},\forall u\in\mathcal{N}(v_i)\})$$

[0030] S3.3：将聚合生成的相邻节点的表示向量$h_{\mathcal{N}(v_i)}^k$与中心节点前一层的特征$h_{v_i}^{k-1}$合并，最后输入到一个全连接层，更新中心节点v_i的特征向量，并对其进行规范化：

[0031] $$h_{v_i}^k=\sigma\left(W^k\cdot CONCAT(h_{v_i}^{k-1},h_{\mathcal{N}(v_i)}^k)\right)$$

[0032] $h_{v_i}^{k} = \mathrm{Norm}(h_{v_i}^{k})$

[0033] 对车联网中所有流量节点进行K层GraphSAGE聚合后，对于每个流量节点v_i得到该节点的聚合特征$h_{v_i}^{K}$，表示捕获其K-hop邻域中的信息。

[0034] 作为优选，所述的将提取的特征信息通过Softmax层输出概率分布，根据相关指标对模型进行性能评估，具体为：

[0035] 根据Softmax层将GraphSAGE模块的输出结果转化成概率分布，具有最高概率所属的类别被视为模型的预测类；经过多次迭代训练后通过计算模型输出的预测值与真实标签的交叉熵损失执行反向传播和更新权重，使用Adam模型优化器不断优化模型参数，使损失达到最小，权重收敛，得到最优的模型参数；然后采用测试集测试模型，获得流量的类别预测值，并根据相关指标对模型性能进行评估，相关指标计算如下：

[0036] $$\mathrm{Recall} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}$$

[0037] $$\mathrm{Precision} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}$$

[0038] $$\mathrm{F-score} = 2 \times \frac{\mathrm{Recall} \times \mathrm{Precision}}{\mathrm{Recall} + \mathrm{Precision}}$$

[0039] 其中TP表示正确预测的攻击流量数，FN表示错误识别为正常的攻击流量数，FP表示错误识别为攻击的正常流量数。

[0040] 本发明的基于图神经网络的车联网入侵检测方法的优点如下：(1)本发明考虑到车联网本质是图结构数据的事实，引入图神经网络这一深度学习算法应用于车联网入侵检测任务，能够充分捕捉车辆之间的依赖关系，从而提高入侵检测的准确率，减少误报率；(2)本发明能够在即使只有少量异常数据的情况下以相对较高的准确率检测车联网通信过程中的异常流量，具有实际应用价值；(3)本发明设计的图特征提取模块GraphSAGE可以替换成其他的图神经网络模型，具有较好的可扩展性和适用性。

附图说明

[0041] 图1是本发明的基于图神经网络的车联网入侵检测方法流程图。

[0042] 图2是本发明的车辆通信图和对应的流量连通图的示例。

[0043] 图3是本发明的图神经网络GraphSAGE结构示意图。

[0044] 图4是本发明和部分已有方法在F1 score比较图。

[0045] 图5为本发明和部分已有方法召回率比较图。

具体实施方式

[0046] 下面结合说明书附图，对本发明实例中的技术方案进行详细说明：

[0047] 如图1所示，一种基于图神经网络的车联网入侵检测方法，包括以下步骤：

[0048] 步骤S1：收集车联网流量数据，对原始流量数据进行预处理；

[0049] 由于车联网入侵检测数据集较少，本实施例采用传统网络入侵检测数据集UNSW-NB15，其由新南威尔士大学创建，用于生成真实现代正常活动和合成当代攻击行为的混合

体。该数据集有九种攻击类型，分别是Analysis、Backdoors、DoS、Exploits、Fuzzers、Generic、Reconnaissance、Shellcode和Worms。Bro-IDS和Argus工具用于从网络数据的pcap文件中提取所需的特征，这些特征有助于构建流量的正常和攻击行为。

[0050] 本实施例对数据集进行预处理操作如下：

[0051] S1.1:数据清洗:消除冗余特征，当样本特征值的数值类型为Nan，用该特征值的平均值代替，当样本特征值的数值类型为Inf，用该特征值的最大值代替；

[0052] S1.2:特征数值化:使用python中get dummies函数将分类特征转换为数值特征；

[0053] S1.3:特征标准化:由于数据各个特征的尺度不同，为了消除特征间尺度差异对模型性能的影响，对特征进行标准化处理；

[0054] 本实施例采用sklearn库中的MinMaxScaler函数对每个特征值进行缩放，将数据归一到[0,1]之间，计算公式为

[0055] $$x_i(j) = \frac{x_i(j) - \min(x(j))}{\max(x(j)) - \min(x(j))}$$

[0056] 其中max(x(j))表示来自特征j的最大值，min(x(j))表示来自特征j的最小值。

[0057] 步骤S2:构建图生成模块，将预处理过的流量数据转化为图结构数据；

[0058] 所述的步骤S2图生成模块具体为：

[0059] S2.1:构建主机通信图G:流量数据是由通信端点(IP地址、端口号)标识，并通过一组提供流详细信息的字段进行注释，这些流字段提供流的详细信息，如包数、字节数、流持续时间等。流量数据可以自然地以图的形式表示:G＝(V,E)，其中节点集合V表示通信端点，边集E代表通信端点之间的通信流。车联网入侵检测问题即判别通信流是否为攻击流量问题，在本实施例中建模为边分类问题。

[0060] 由于图神经网络建模节点相对容易，而建模边则要复杂得多。因此考虑引入线图，基于主机通信图G生成相应的流量连通图G_L。

[0061] S2.2:构建流量连通图G_L:如图2所示，给出由主机通信图到对应的流量连通图的示例。定义$G_L＝(V_L,E_L)$为相应的流量连通图，流量格式表示为[ID编号，流量特征，标签]，其中ID编号由通信端点(IP地址、端口号)映射而成，节点v_i表示第i条流量，则G_L的节点集是G的边集，即$V_L＝\{(v_i,v_j)\in E\}$且$|V_L|＝|E|$，如果G中的两条边共享一个节点，即若两条流量来自同一通信端点，则G_L中存在一条边表示流量的相关性。G_L的边集用邻接矩阵$A_L\in\mathbb{R}^{|E|\times|E|}$表示

[0062] $$A_L(v_i,v_j),(v_j,v_k)=\begin{cases}1 & \text{if } i\neq j \text{ and } j\neq k\\ 0 & \text{otherwise}\end{cases}$$

[0063] 流量连通图的属性特征定义为$X_L\in\mathbb{R}^{N\times F}$，其中N表示流量的条数，F表示流量的特征维度。借助流量连通图G_L，车联网入侵检测问题转化为节点分类问题。

[0064] 步骤S3:构建GraphSAGE模块，将上述图结构数据输入到图神经网络GraphSAGE模块中，提取流量的结构特征和属性特征信息；

[0065] 所述的步骤S3中构建GraphSAGE模块，本实施例中GraphSAGE模块包含三个GraphSAGE层，如图3所示，每一层中又包括SAGEConv层和AGG层，分别为采样邻居卷积和聚合邻居，具体操作为：

[0066] S3.1:根据构建的流量连通图的结构特征A_L和属性特征X_L,针对每个流量节点$\forall v_i \in V$,从其相邻节点集合$\mathcal{N}(v_i)$随机均匀采样固定数量的节点来进行聚合特征。采样的邻居数为S_k,如果实际邻居数小于S_k,则使用带回放的采样方法,如果实际邻居数大于S_k,则使用不带回放的采样方法。本实施例中,每层GraphSAGE层采样邻域范围不同,对于某个节点v_i,第一层采样其一阶邻居$S_k=15$,第二层采样其二阶邻居$S_k=10$,第三层采样其三阶邻居$S_k=5$。

[0067] S3.2:选择池化聚合函数来聚合相邻节点的特征,池化函数是对称的,因为要确保输出不随节点的顺序而变化,即$AGG(v_1,v_2)=AGG(v_2,v_1)$。

[0068] 第k层的池化聚合函数定义为:

[0069] $$AGG^k = \max(\sigma(W \times h_{\mathcal{N}(v_i)}^{k-1} + b))$$

[0070] 其中$h_{\mathcal{N}(v_i)}^{k-1}$代表节点$v_i$的邻居集合$\mathcal{N}(v_i)$在经GraphSAGE提取的第k-1层的聚合特征,σ表示非线性激活函数,W表示要训练的权重矩阵,b表示偏置量。公式解析为先将所有前一层相邻节点的聚合特征通过一个全连接层,再利用非线性激活函数,最后使用最大池化聚合。

[0071] 则第k层的相邻节点$\mathcal{N}(v_i)$的聚合信息可以表示为:

[0072] $$h_{\mathcal{N}(v_i)}^k = AGG^k(\{h_u^{k-1}, \forall u \in \mathcal{N}(v_i)\})$$

[0073] S3.3:将聚合生成的相邻节点的表示向量$h_{\mathcal{N}(v_i)}^k$与中心节点前一层的特征$h_{v_i}^{k-1}$合并,最后输入到一个全连接层,更新中心节点v_i的特征向量,并对其进行规范化:

[0074] $$h_{v_i}^k = \sigma\left(W^k \cdot CONCAT(h_{v_i}^{k-1}, h_{\mathcal{N}(v_i)}^k)\right)$$

[0075] $$h_{v_i}^k = Norm(h_{v_i}^k)$$

[0076] 对车联网中所有流量节点进行3层GraphSAGE聚合后,对于每个流量节点v_i得到该节点的聚合特征$h_{v_i}^K$,表示捕获其3-hop邻域中的信息。

[0077] 步骤S4:经GraphSAGE提取的特征信息通过Softmax层输出概率分布,根据相关指标对模型进行性能评估;

[0078] 根据Softmax层将GraphSAGE模块的输出结果转化成概率分布,具有最高概率所属的类别被视为模型的预测类。

[0079] 本实例使用Pytorch库和DGL库实现,GraphSAGE模块的性能很大程度上取决于最佳超参数,因此使用微软发布的AutoML平台NNI来自动化超参数调整。最佳超参数设置为学习率为0.0001,训练迭代次数为500,批量尺寸为1024,采用Glorot对每层的权重初始化,而偏置量则使用零均值的高斯函数初始化。

[0080] 经过多次迭代训练后通过计算模型输出的预测值与真实标签的交叉熵损失执行反向传播和更新权重,本实施例使用Adam模型优化器不断优化模型参数,使损失达到最小,权重收敛,得到最优的模型参数。然后采用测试集测试模型,获得流量的类别预测值,并根据相关指标对模型性能进行评估。

[0081] 本实施例设立了对照组实验,在基于UNSW-NB15数据集上与已有的四种基于深度学习的入侵检测方法进行了对比分析,F1分数结果如图4所示,召回率结果如图5所示,可以

看出本发明方法在车联网入侵检测任务上,总体性能优于其他深度学习模型。

[0082] 本发明的具体实施方式中凡未涉到的说明属于本领域的公知技术,可参考公知技术加以实施。

[0083] 以上具体实施方式是对本发明提出的基于卷积神经网络的多智能体系统网络鲁棒性方法技术思想的具体支持,不能以此限定本发明的保护范围,凡是按照本发明提出的技术思想,在本发明技术方案基础上所做的任何等同变化或等效的改动,均仍属于本发明技术方案保护的范围。

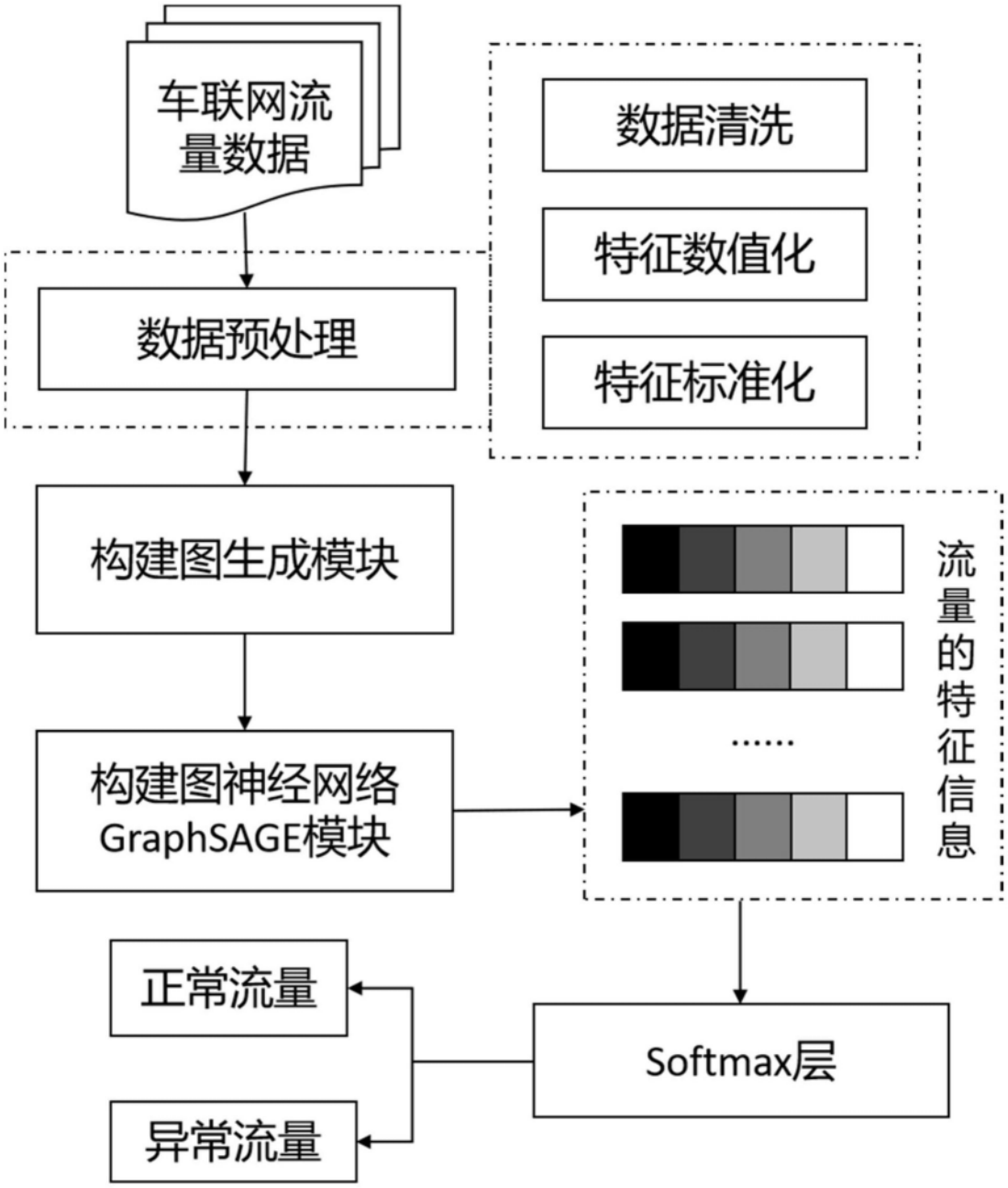

车联网流量数据
数据清洗
特征数值化
特征标准化
数据预处理
构建图生成模块
构建图神经网络GraphSAGE模块
流量的特征信息
.....
正常流量
异常流量
Softmax层

图1

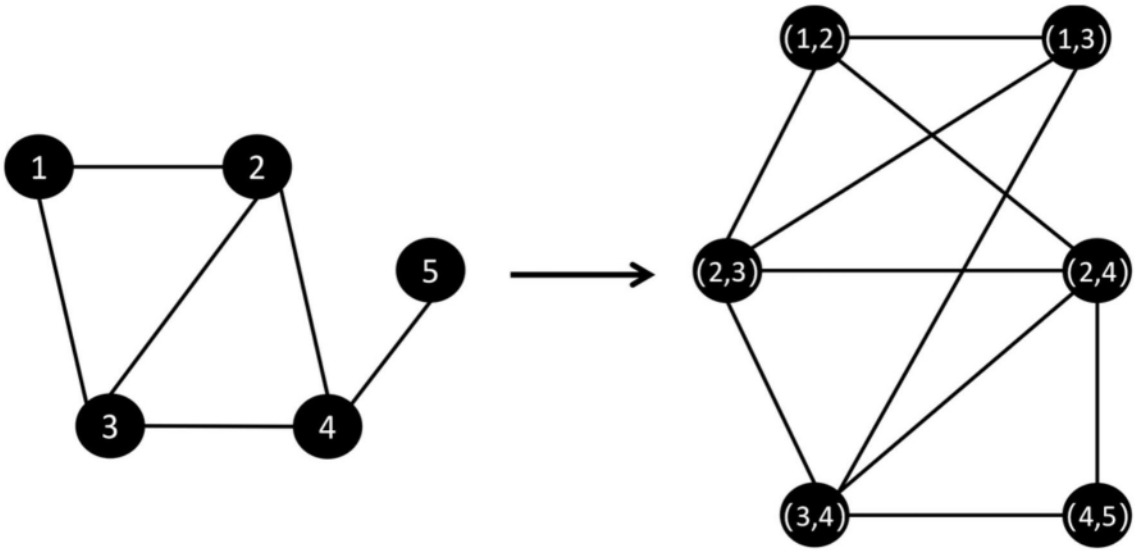


图2

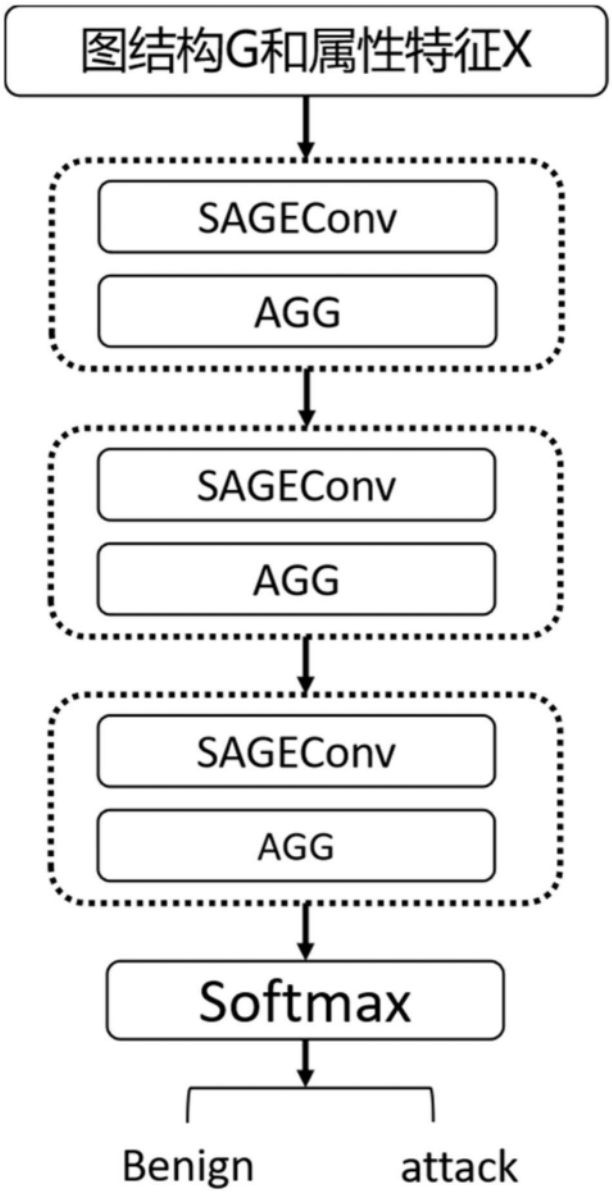

图结构G和属性特征X
SAGEConv
AGG
SAGEConv
AGG
SAGEConv
AGG
Softmax
Benign
attack

图3

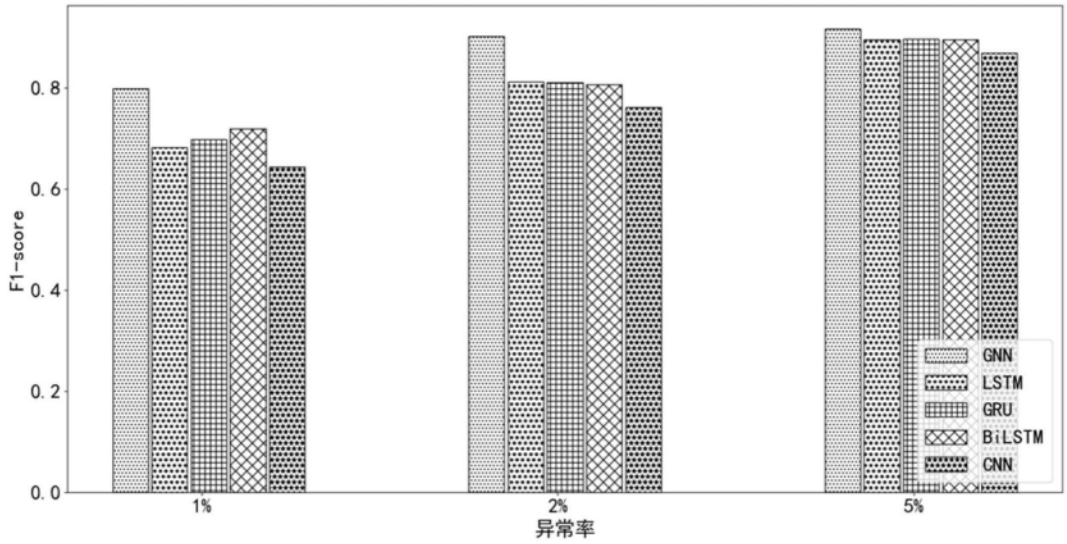

F1-score
0.0
0.2
0.4
0.6
0.8
1%
2%
5%
异常率
GNN
LSTM
GRU
BiLSTM
CNN

图4

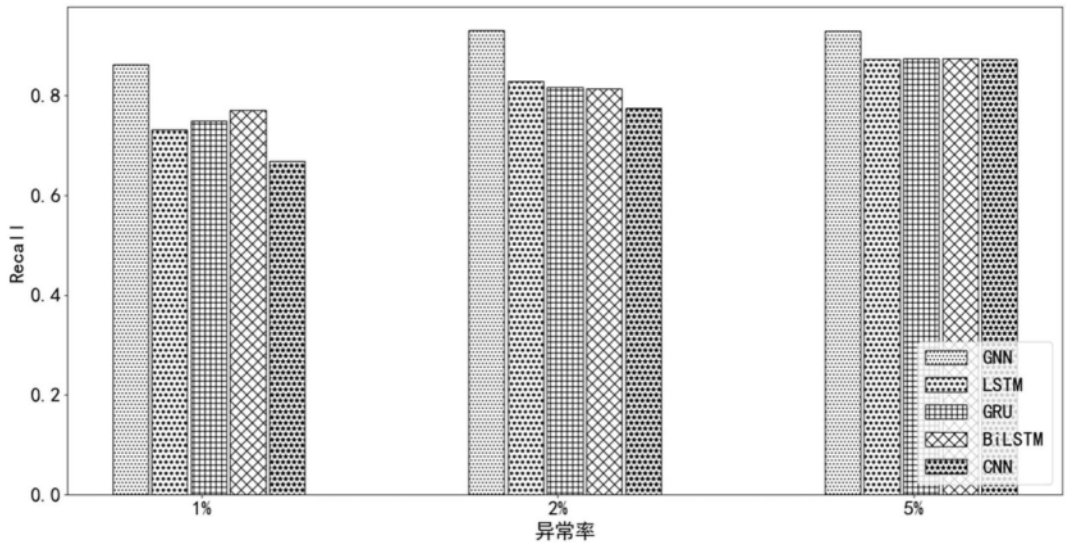

Recall
0.0
0.2
0.4
0.6
0.8
1%
2%
5%
异常率
GNN
LSTM
GRU
BiLSTM
CNN

图5