(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116958701 A
(43)申请公布日 2023.10.27

(21)申请号 202310956833.4

(22)申请日 2023.08.01

(71)申请人 小快(厦门)网络科技有限公司
地址 361024 福建省厦门市火炬高新区软件园三期诚毅北大街65号703室

(72)发明人 王颖伟 干淇任 高振国 游政贤 沈永胜 许庆龙

(74)专利代理机构 北京奇眸智达知识产权代理有限公司 11861
专利代理师 郑超超

(51)Int.Cl.
G06V 10/764(2022.01)
G06V 10/82(2022.01)
G06N 3/0464(2023.01)

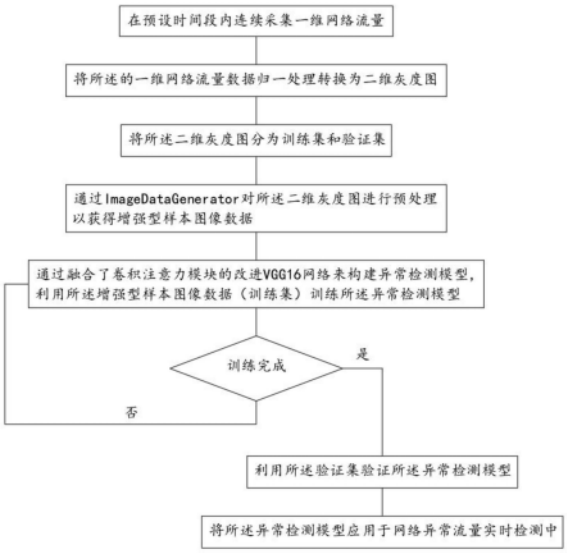
权利要求书2页 说明书4页 附图3页

(54)发明名称

一种基于改进VGG16与图像增强的网络异常流量检测方法

(57)摘要

本发明属于网络安全技术领域,公开了一种基于改进VGG16与图像增强的网络异常流量检测方法,包括:将预设时间段内采集的一维网络流量数据归一化处理转换为二维灰度图;通过ImageDataGenerator对所述二维灰度图进行预处理以获得增强型样本图像数据;通过融合了卷积注意力模块的改进VGG16网络来构建异常检测模型,并利用所述增强型样本图像数据训练所述异常检测模型;将所述异常检测模型应用于网络异常流量实时检测中。综上,本发明将卷积注意力模块融入VGG16网络中,以此有效实现了对网络由浅到深的自特征融合的充分提取,进而提高检测结果的准确度,且将经过ImageDataGenerator增强处理后的图像数据作为异常检测模型的输入,能够有效增强异常检测模型的泛化能力。



CN 116958701 A

1.一种基于改进VGG16与图像增强的网络异常流量检测方法,其特征在于,包括如下步骤:

将预设时间段内采集的一维网络流量数据归一化处理转换为二维灰度图;

通过ImageDataGenerator对所述二维灰度图进行预处理以获得增强型样本图像数据;

通过融合了卷积注意力模块的改进VGG16网络来构建异常检测模型,并利用所述增强型样本图像数据训练所述异常检测模型;

将所述异常检测模型应用于网络异常流量实时检测中。

2.根据权利要求1所述的基于改进VGG16与图像增强的网络异常流量检测方法,其特征在于:所述一维网络流量数据包括正常时序流量信号和异常时序流量信号。

3.根据权利要求1所述的基于改进VGG16与图像增强的网络异常流量检测方法,其特征在于,所述归一化处理转换公式如下:

$$P(i)=\frac{(N(i)-Min(N))}{Max(N)-Min(N)}\times 255, i=1,2,3,...,\mathrm{M}^2$$;式中,P(i)为归一化之后的特征值,N(i)为归一化之前的特征值,Min(N)和Max(N)分别为特征值中的最小值和最大值。

4.根据权利要求1所述的基于改进VGG16与图像增强的网络异常流量检测方法,其特征在于:所述异常检测模型包括基于VGG16网络的特征提取层、基于卷积注意力模块的特征加强层、以及基于Softmax分类器的特征分类层。

5.根据权利要求4所述的基于改进VGG16与图像增强的网络异常流量检测方法,其特征在于:所述特征提取层用于从所述增强型样本图像数据中提取数据特征,且所述特征提取层包括相互配合的五个卷积层和池化层。

6.根据权利要求5所述的基于改进VGG16与图像增强的网络异常流量检测方法,其特征在于:所述特征加强层用于将特征提取层中的第三层、第四层与第五层所述卷积层所提取的数据特征筛选融合,以获得新的加强特征。

7.根据权利要求6所述的基于改进VGG16与图像增强的网络异常流量检测方法,其特征在于,所述的获得新的加强特征的步骤包括:

以所述特征提取层中第三层所述卷积层所提取的数据特征为第一输入;

以所述特征提取层中第四层所述卷积层所提取的数据特征为第二输入;

分别筛选所述第一输入和第二输入以得到第一特征向量和第二特征向量;

使用Add函数先拼接融合所述第一特征向量与所述第二特征向量,得到融合特征,然后再将所述融合特征与所述特征提取层中第五层所述卷积层所提取的数据特征进行融合,得到新的加强特征。

8.根据权利要求7所述的基于改进VGG16与图像增强的网络异常流量检测方法,其特征在于:筛选所述第一输入和所述第二输入时,基于所述卷积注意力模块的通道注意力和空间注意力进行分别筛选。

9.根据权利要求8所述的基于改进VGG16与图像增强的网络异常流量检测方法,其特征在于:基于所述通道注意力的筛选公式如下:

$M_c(F)=\sigma(MLP(AvgPooling(F))+MLP(MaxPooling(F)))$;式中,σ为s igmoid函数;F为输入,且$F\in R^{C\times H\times W}$;$M_c(F)$为筛选输出的通道特征向量,且$M_c(F)\in R^{C\times 1\times 1}$。

10.根据权利要求8所述的基于改进VGG16与图像增强的网络异常流量检测方法,其特

征在于:基于所述空间注意力的筛选公式如下:

$M_S(F)=\sigma(f^{7\times7}([AvgPooling(F);MaxPooling(F)]))$;式中,σ为s igmoid函数;F为输入,且$F\in R^{C\times H\times W}$;$M_S(F)$为筛选输出的空间特征向量,且$M_S(F)\in R^{1\times H\times W}$。

一种基于改进VGG16与图像增强的网络异常流量检测方法

技术领域

[0001] 本发明属于网络安全技术领域，具体涉及一种基于改进VGG16与图像增强的网络异常流量检测方法。

背景技术

[0002] 随着科技的发展，网络通信的各种应用已充斥于人们的生活中，且人们对于网络通信的需求亦日益增加，因此网络通信的安全性也随之日益重要。

[0003] 传统的网络防御检测系统大多采用专家规则或机器学习的方式来检测异常流量，其中：专家规则存在一定的人为主观因素，检测准确性较差；机器学习常使用循环神经网络(RNN)、长短时记忆网络(LSTM)等网络模型对一维时序信号的异常数据进行特征学习，但是，这些模型的深度较浅，难以学习数据中的高维特征，从而导致在检测网络流量的实际数据时往往会出现检测准确率较低的问题。

发明内容

[0004] 鉴于此，为解决上述背景技术中所提出的问题，本发明的目的在于提供一种基于改进VGG16与图像增强的网络异常流量检测方法。

[0005] 为实现上述目的，本发明提供如下技术方案：

[0006] 一种基于改进VGG16与图像增强的网络异常流量检测方法，包括：

[0007] 将预设时间段内采集的一维网络流量数据归一化处理转换为二维灰度图；

[0008] 通过ImageDataGenerator对所述二维灰度图进行预处理以获得增强型样本图像数据；

[0009] 通过融合了卷积注意力模块的改进VGG16网络来构建异常检测模型，并利用所述增强型样本图像数据训练所述异常检测模型；

[0010] 将所述异常检测模型应用于网络异常流量实时检测中。

[0011] 优选的，所述一维网络流量数据包括正常时序流量信号和异常时序流量信号。

[0012] 优选的，所述归一化处理转换公式如下：

[0013] $$P(i)=\frac{(N(i)-Min(N))}{Max(N)-Min(N)}\times 255, i=1,2,3,...,\mathrm{M}^2$$；式中，P(i)为归一化之后的特征值，N(i)为归一化之前的特征值，Min(N)和Max(N)分别为特征值中的最小值和最大值。

[0014] 优选的，所述异常检测模型包括基于VGG16网络的特征提取层、基于卷积注意力模块的特征加强层、以及基于Softmax分类器的特征分类层。

[0015] 优选的，所述特征提取层用于从所述增强型样本图像数据中提取数据特征，且所述特征提取层包括相互配合的五个卷积层和池化层。

[0016] 优选的，所述特征加强层用于将特征提取层中的第三层、第四层与第五层所述卷积层所提取的数据特征筛选融合，以获得新的加强特征。

[0017] 优选的，所述的获得新的加强特征的步骤包括：

[0018] 以所述特征提取层中第三层所述卷积层所提取的数据特征为第一输入；

[0019] 以所述特征提取层中第四层所述卷积层所提取的数据特征为第二输入；

[0020] 分别筛选所述第一输入和第二输入，得到第一特征向量和第二特征向量；

[0021] 使用Add函数先拼接融合所述第一特征向量与所述第二特征向量，得到融合特征，然后再将所述融合特征与所述特征提取层中第五层所述卷积层所提取的数据特征进行融合，得到新的加强特征。

[0022] 优选的，筛选所述第一输入和所述第二输入时，基于所述卷积注意力模块的通道注意力和空间注意力进行分别筛选。

[0023] 优选的，基于所述通道注意力的筛选公式如下：

[0024] $M_c(F)=\sigma(MLP(AvgPooling(F))+MLP(MaxPooling(F)))$；式中，σ为sigmoid函数；F为输入且$F\in R^{C\times H\times W}$；$M_c(F)$为筛选输出的通道特征向量且$M_c(F)\in R^{C\times 1\times 1}$。

[0025] 优选的，基于所述空间注意力的筛选公式如下：

[0026] $M_s(F)=\sigma(f^{7\times 7}([AvgPooling(F);MaxPooling(F)]))$；式中，σ为sigmoid函数；F为输入，且$F\in R^{C\times H\times W}$；$M_s(F)$为筛选输出的空间特征向量，且$M_s(F)\in R^{1\times H\times W}$。

[0027] 本发明与现有技术相比，具有以下有益效果：

[0028] 本发明的网络异常流量检测方法，通过融入卷积注意力模块的方式改进VGG16网络，并且基于改进VGG16网络来构建异常检测模型，以此实现了对网络由浅到深的自特征融合的充分提取，进而有效保证检测结果的准确；将各网络节点的一维网络流量信号归一化处理转化为二维灰度图像，并基于ImageDataGenerator图像处理技术对该二维灰度图像进行加强处理，且以加强处理后的图像特征作为异常检测模型的输入，由此有效增强模型的泛化能力。

附图说明

[0029] 图1为本发明网络异常流量检测方法的流程图；

[0030] 图2为本发明异常检测模型的结构图；

[0031] 图3为本发明卷积注意力模块的结构图。

具体实施方式

[0032] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0033] 如图1所示，本发明所提供的基于改进VGG16与图像增强的网络异常流量检测方法包括如下步骤：

[0034] S1.在预设时间段内连续采集一维网络流量数据；

[0035] 具体的，数据采集从0:00开始直到23:55，其中每5min为一个采样点，共采集n个样本，每个样本为包含288个采样点的信号片段，且所采集的一维网络流量数据包括正常时序流量信号和异常时序流量信号。

[0036] S2.将所述的一维网络流量数据归一化处理转换为二维灰度图；

[0037] 归一化处理公式为：$P(i)=\frac{(N(i)-Min(N))}{Max(N)-Min(N)}\times 255, i=1,2,3,...,M^2$；式中，P(i)为归一化之后的特征值，N(i)为归一化之前的特征值，Min(N)和Max(N)分别为特征值中的最小值和最大值。

[0038] S3.将上述转换得到的二维灰度图分为训练集和验证集；

[0039] 如下表所示，假设正常时序流量信号和异常时序流量信号的一维网络流量数据中分别包括1000份数据样本，且训练集和验证集按照4:1的比例进行随机划分；

[0040]

	训练集（样本数量）	验证集(样本数量)
正常时序流量信号	800	200
异常时序流量信号	800	200

[0041] S4.通过ImageDataGenerator对所述二维灰度图进行预处理以获得增强型样本图像数据。

[0042] S5.通过融合了卷积注意力模块的改进VGG16网络来构建异常检测模型，并利用所述增强型样本图像数据(训练集)训练所述异常检测模型；

[0043] 如图2所示，异常检测模型包括基于VGG16网络的特征提取层、基于卷积注意力模块的特征加强层、以及基于Softmax分类器的特征分类层；

[0044] 具体的：

[0045] a)特征提取层以VGG16网络为主干网络结构，具体包括了相互配合的五个卷积层和池化层；

[0046] 卷积层(conv3-64/conv3-128/conv3-256/conv3-512/conv3-512)对输入数据做卷积操作，提取输入数据的局部特征，将输出作为下一层的输入，每个卷积核大小相同。设$x_k^{(m)}$为第k层第m个卷积核的输出特征映射，$W_k^{(c,m)}$为权重矩阵，$X_{k-1}^{(m)}$为第k层第c次卷积操作的局部输入特征，*表示卷积操作，$b_j^{(m)}$为偏置，则卷积层工作过程可用下述公式描述：

[0047] $$X_k^{(m)}=\sum_{c=1}^{c}W_k^{(c,m)}*X_{k-1}^{(c)}+b_j^{(m)}$$。

[0048] 池化层(maxpool)减小输入特征的大小，扩大感知野，实现输入的平移不变性、旋转不变性、尺度不变性，并且可以减少网络参数数量。设$P_k^{(i,j)}$为第k层第i个输入映射的第j个池化值，$q_k^{(i,t)}$为第k层第j次池化操作的局部输入特征，w为池化区域的宽度，则池化层工作过程可用下述公式描述：

[0049] $$P_k^{(i,j)}=\max_{(j-1)w+1<i<jw}\left\{q_k^{(i,t)}\right\}, j=1,2,...,m$$。

[0050] b)特征加强层以卷积注意力模块为特征筛选基础，以所述特征提取层中第三层和第四层所述卷积层所提取的数据特征为(第一/第二)输入，以筛选得到(第一/第二)特征向量；

[0051] 如图3所示，卷积注意力模块由通道注意力和空间注意力组成，由此在进行特征筛

选时分别从通道维度和空间维度进行筛选：

[0052] 关于通道维度特征筛选：设输入特征图为F，且$F \in R^{C\times H\times W}$；设通道特征向量为$M_c(F)$，且$M_c(F) \in R^{C\times 1\times 1}$。具体通道注意过程可用下述公式描述：

[0053] $M_c(F)=\sigma(MLP(AvgPooling(F))+MLP(MaxPooling(F)))$；

[0054] 关于空间维度特征筛选：设输入特征图为F，且$F \in R^{C\times H\times W}$；设空间特征向量$M_s(F)$，$M_s(F) \in R^{1\times H\times W}$。具体空间注意过程可用下述公式描述：

[0055] $M_s(F)=\sigma(f^{7\times 7}([AvgPooling(F);MaxPooling(F)]))$；

[0056] 上述σ为sigmoid函数，且$f^{7\times 7}$表示为特征加强层中的卷积核大小为7×7。

[0057] 使用Add函数将上述筛选的(第一/第二)特征向量由浅至深进行拼接融合，得到融合特征，然后再将所述融合特征与所述特征提取层中第五层所述卷积层所提取的数据特征进行融合，得到新的加强特征。具体的，基于Add函数的特征融合，设特征一为$X'=[x_1,x_2,x_3,\cdots,x_n]$、特征二为$Y'=[y_1,y_2,y_3,\cdots,y_n]$，则融合后的新特征$F_1=Add(X',Y')=X'+iY'$，其中i表示融合系数。

[0058] c)将结合了不同层特征的加强特征输入至基于Softmax分类器的特征分类层，以此获得分类结果，并完成对所述异常检测模型的训练。

[0059] S6.向训练后的异常检测模型中输入验证集，异常检测模型通过特征分类层(Softmax分类器)输出分类检测结果(正常或者异常的二元分类标签)，并基于该验证集对训练后的异常检测模型的检测准确度进行判断，从而有效保证异常检测模型的检测精度。

[0060] S7.将所述异常检测模型应用于网络异常流量实时检测中；

[0061] 采集实时网络状态下的一维网络流量数据，并将该一维网络流量数据归一化处理转换为二维灰度图；

[0062] 通过ImageDataGenerator对所述二维灰度图进行图像增强预处理；

[0063] 将增强预处理后的图像数据输入所述异常检测模型中、对应输出得到关于实时网络状态的检测结果。

[0064] 综上所述，本发明将一维网络时序流量信号转化为二维灰度图，然后基于ImageDataGenerator图像处理技术进行图像增强处理，接着通过融合了卷积注意力模块的改进VGG16模型对增强图像实现了由浅到深的自特征融合的充分提取，实现高精度、高效率的网络异常流量检测。

[0065] 尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由所附权利要求及其等同物限定。

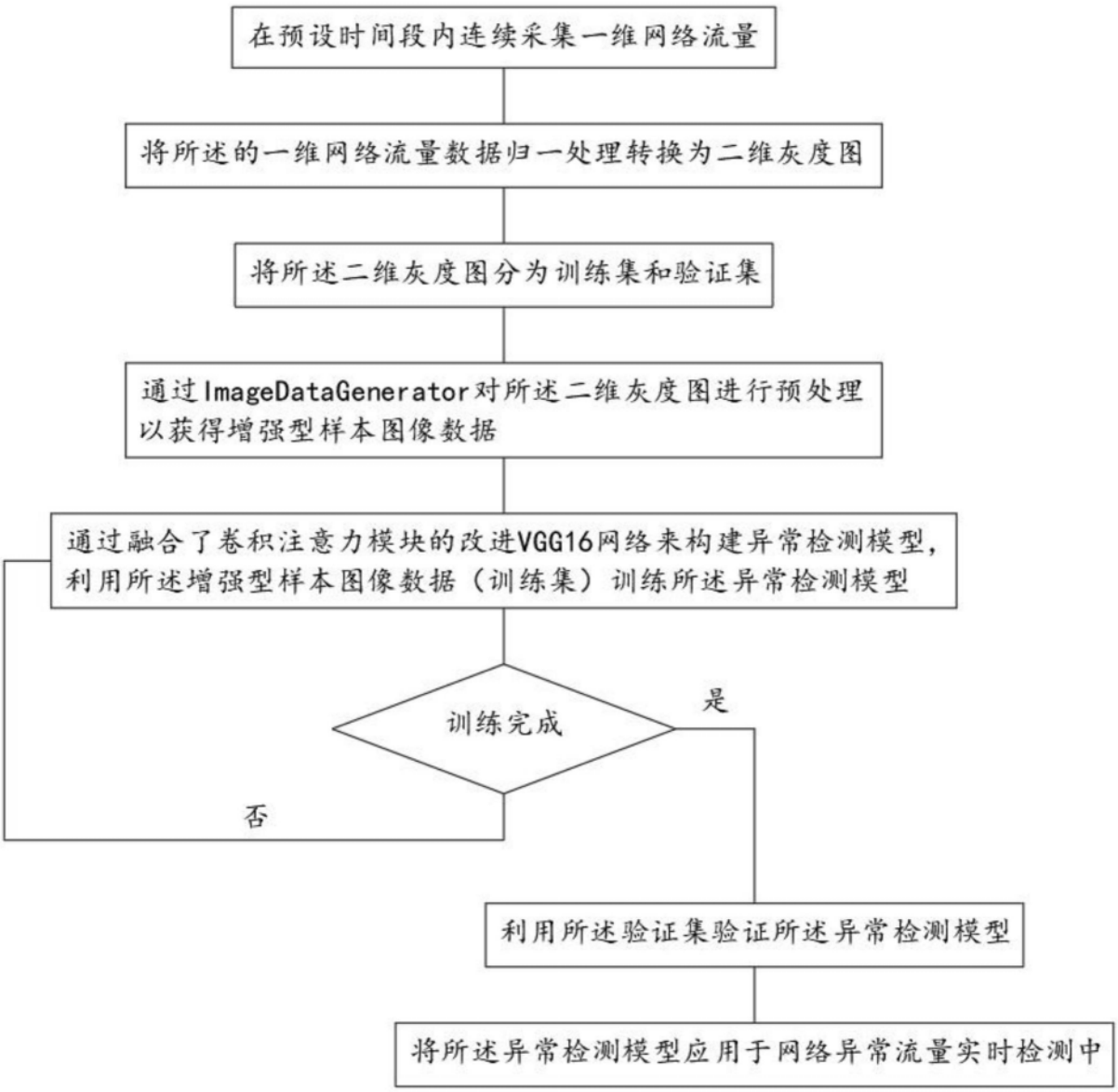

在预设时间段内连续采集一维网络流量
将所述的一维网络流量数据归一处理转换为二维灰度图
将所述二维灰度图分为训练集和验证集
通过ImageDataGenerator对所述二维灰度图进行预处理以获得增强型样本图像数据
通过融合了卷积注意力模块的改进VGG16网络来构建异常检测模型，利用所述增强型样本图像数据（训练集）训练所述异常检测模型
训练完成
是
否
利用所述验证集验证所述异常检测模型
将所述异常检测模型应用于网络异常流量实时检测中

图1

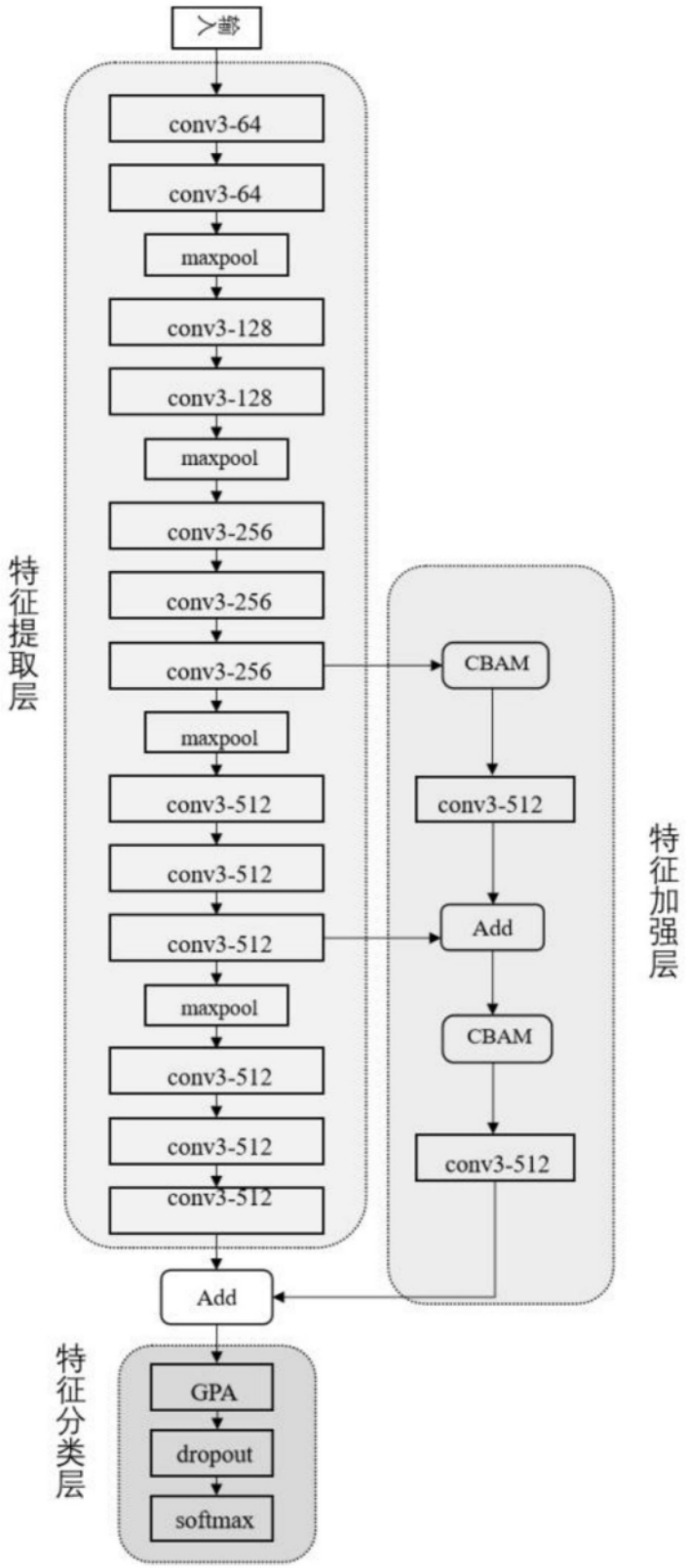

conv3-64
conv3-64
maxpool
conv3-128
conv3-128
maxpool
conv3-256
conv3-256
conv3-256
maxpool
conv3-512
conv3-512
conv3-512
maxpool
conv3-512
conv3-512
conv3-512
特征提取层
CBAM
conv3-512
Add
CBAM
conv3-512
特征加强层
Add
GPA
dropout
softmax
特征分类层

图2

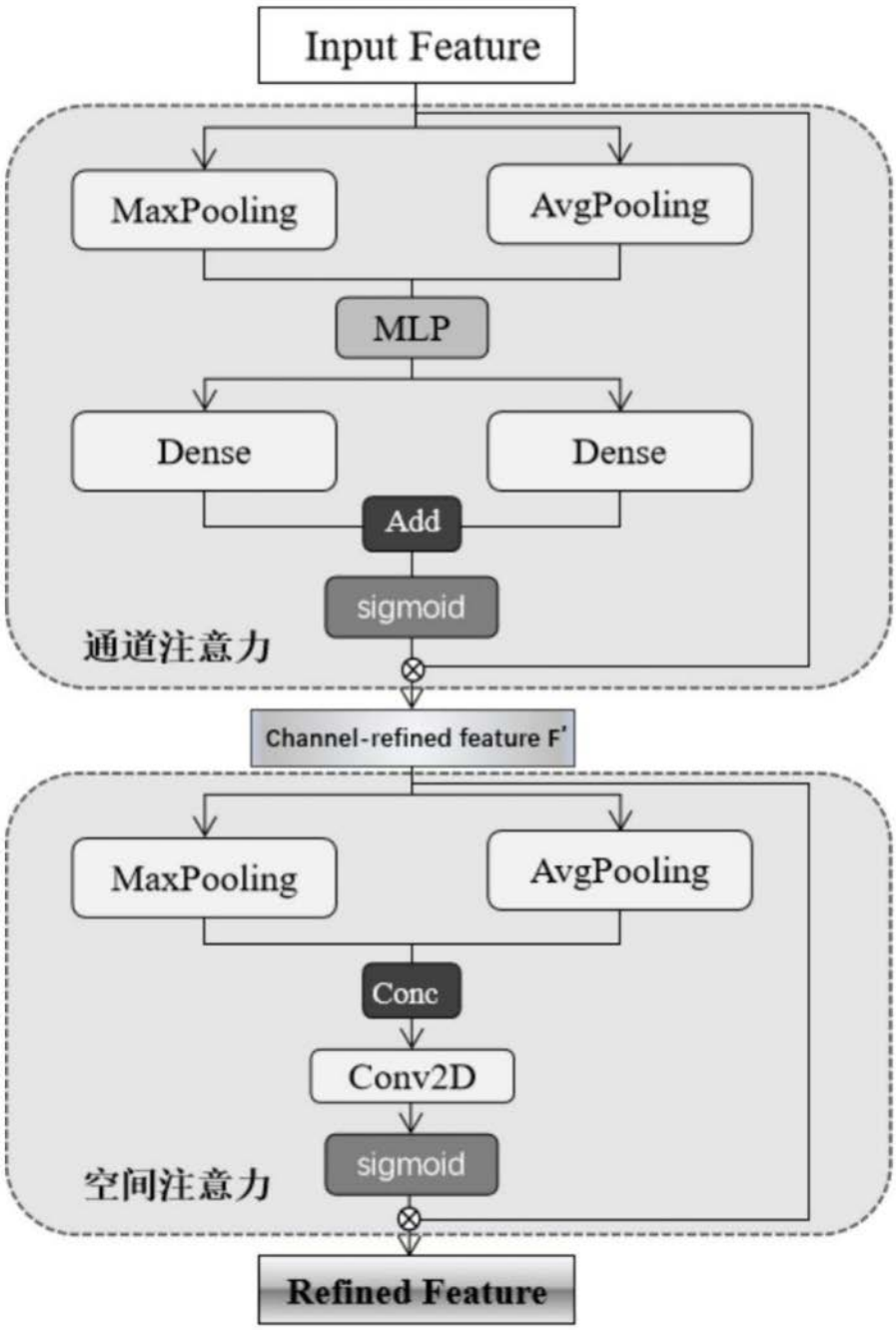

Input Feature
MaxPooling
AvgPooling
MLP
Dense
Dense
Add
sigmoid
通道注意力
Channel-refined feature F'
MaxPooling
AvgPooling
Conc
Conv2D
sigmoid
空间注意力
Refined Feature

图3