专题：智能网联汽车

面向车联网的基于卷积神经网络的入侵检测模型

张锐
（驻马店职业技术学院信息工程学院，河南 驻马店 463003）

摘　要：为了提高车联网入侵检测的准确率，提出了基于超参数优化卷积神经网络的集成的入侵检测系统（hyper-parameter optimization convolution neural network-based ensemble Intrusion detection system，CNES）模型。CNES模型利用卷积神经网络构建集成学习的基学习器，并利用粒子群优化算法优化卷积神经网络的超参数，进而优化卷积神经网络模型。利用平均法和级联法的集成策略构建集成学习模型，提高检测攻击的准确率。通过车内网络数据集Car-Hacking和车外网络数据集CICIDS2017验证CNES模型的性能。性能分析表明，提出的CNES模型有效地提高了检测网络攻击的性能。在Car-Hacking数据集上，CNES模型的F1值达到100%。

关键词：车联网；入侵检测；卷积神经网络；粒子群优化算法；集成学习
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024243

An intrusion detection model based on convolution neural network for Internet of vehicles

ZHANG Rui
Department of Information Engineering, Zhumadian Vocatiomal and Technical College, Zhumadian 463003, China

Abstract: In order to improve the accuracy of detecting the cyber-attacks in Internet of vehicles, hyper-parameter optimization convolution neural network-based ensemble Intrusion detection system (CNES) was proposed. In CNES, the convolution neural network (CNN) was adopted to serve as based learner in ensemble learning. Moreover, the particle swarm optimization was utilized to optimize the hyber-parameters of the CNN, and then CNN model was optimized. Confidence averaging and concatenation techniques were constructed to improve the accuracy. The performance of the proposed CNES was measured based on Car-Hacking and CICIDS2017 datasets. This shows the effectiveness of the proposed CNES for cyber-attack detection. The CNES achieves F1 score of 100% on Car-Hacking dataset.

Key words: Internet of vehicles, intrusion detection, convolution neural network, particle swarm optimization algorithm, ensemble learning

收稿日期：2024−07−06；**修回日期：**2024−11−18
基金项目：河南省科技攻关项目（No.212102210515）
Foundation Item: Henan Science and Technology Research Project (No.212102210515)

0 引言

随着物联网（Internet of things，IoT）和车联网（Internet of vehicles，IoV）技术的快速发展，自动驾驶汽车、智能网联汽车等网络控制汽车已经开始取代传统汽车[1]。车联网系统主要由车内网络（intra-vehicle network，IVN）和外部网络组成。在IVN中，控制器区域网络（controller area network，CAN）总线是实现电子控制单元之间通信，进而实现各种功能的核心基础设施[2]。外部车载网络则利用车联网（vehicle to everything，V2X）技术实现智能汽车与其他车联网实体之间的连接，如路边单元、路侧基础设施和智能设备等。

由于网络攻击面不断扩大，车联网系统遭受的安全威胁日益增多，并且，CAN数据包的长度较短，在处理CAN数据包时无须构建认证或加密机制。在缺乏基本安全机制的情况下，攻击者可能将恶意消息插入IVN，并执行各种攻击，如拒绝服务（denial of service，DoS）攻击、模糊（Fuzzy）攻击和欺骗攻击[3]。此外，与外部网络之间的连接，使联网汽车更容易遭受一些传统的网络攻击。

入侵检测系统（intrusion detection system，IDS）已成为检测入侵、保护车联网系统以及智能汽车免受网络攻击的有效方案[4]。为了保护IVN，IDS可部署在CAN总线的顶部，用以识别恶意CAN消息[5]，IDS也可集成到网关中检测来自外部网络的恶意数据包。

文献[6]针对IVN的入侵检测问题，提出了一种基于深度迁移学习的入侵检测系统（deep transfer learning-based IDS，DTLS）模型。类似地，文献[7]也提出，用基于卷积神经网络的入侵检测系统（convolutional neural network-based IDS，CNNS）模型来检测网络的入侵攻击。性能分析表明，CNNS模型可获取99.9%的准确率和99.0%的检测率。此外，文献[8]提出基于深度卷积神经网络的入侵检测系统（deep convolutional neural network-based IDS，DNNS）模型，利用DNNS模型检测入侵车内总线的攻击。

此外，针对车外网的入侵攻击问题，文献[9]提出了基于前馈神经网络的入侵检测系统（feed-forward neural network-based IDS，FFNS）模型，并通过数据集CICIDS2017验证FFNS模型的性能，性能分析表明，FFNS模型可获取99%以上的准确率。文献[10]提出基于改进卷积神经网络的入侵检测系统（novel convolution neural network-based IDS，NCNI）模型，NCNI模型在CICIDS2017数据集上的精确率、召回率和F1值分别为99.5%、99.8%和98.7%。

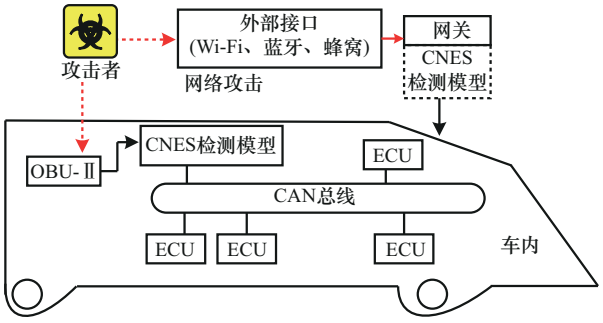
相比于单个分类器，基于集成算法的分类器可提升检测性能。为此，本文结合卷积神经网络（convolution neural network，CNN）、迁移学习（transfer learning，TL）和集成算法，提出基于超参数优化卷积神经网络的集成的入侵检测系统（hyper-parameter optimization convolution neural network-based ensemble Intrusion detection，CNES）模型。CNES模型将5个CNN模型作为基学习器，并利用粒子群优化（particle swarm optimization，PSO）算法对这5个CNN模型的超参数进行优化。再从中选择检测性能在前3位的CNN模型作为元学习器。同时，考虑平均法和级联法两种集成策略。性能分析结果表明，CNES模型的检测准确率优于同类的检测模型，并且基于级联法的集成策略的检测时间短于基于平均法的检测时间。

1 系统模型

与现有的系统模型不同，CNES模型不仅考虑了车内攻击，还考虑了车外网攻击，是一个集成了多个CNN的入侵检测模型。车内攻击主要是指攻击者通过车载单元（on-board unit Ⅱ，

OBU-Ⅱ）接口向CAN总线发起的攻击。而车外网攻击主要是指攻击者通过无线接口向车辆发送恶意流量包，这些无线接口包括Wi-Fi、蜂窝或者蓝牙。

因此，提出的CNES模型既可部署在IVN，也可部署在车体外的外网。在IVN，CNES检测模型部署在CAN总线上，进而检测异常CAN消息。在车外网，将CNES模型集成到网关中，以识别和阻止所有旨在破坏车辆的恶意数据包。CNES模型的部署如图1所示。



注：ECU（电子控制单元）。

图1　CNES模型的部署

CNES模型融合了改进的CNN和TL策略，其框架如图2所示。

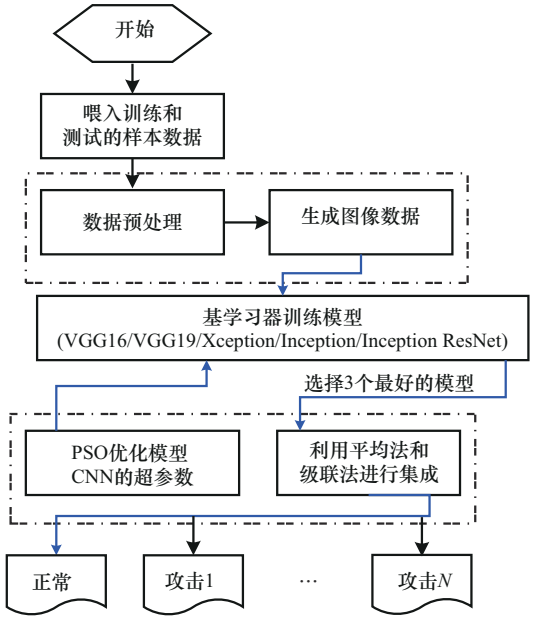


图2　CNES模型框架

步骤1　利用CNES模型收集车内网络和车外网络的数据，然后将这些数据转换成基于时间的数据块，再利用分位数变换法将数据块转化成图像数据。

步骤2　利用CNN训练基学习器。将现有的流行的5个CNN模型——VGG16、VGG19、Xception（XCEP）、Inception（INCE）和Inception ResNet（INCER）——构成基学习器，再利用PSO算法优化CNN模型的超参数，进而得到最优的学习模型，从中选择性能表现在前3位的CNN模型构建集成学习模型。

步骤3　利用平均法和级联法的两个集成策略构建最终的集成模型，输出最终的分类结果。

2　数据集和图数据的生成

2.1　初始数据集

本文采用Car-Hacking和CICIDS2017数据集验证CNES模型的性能。前者为车内数据，它是将CAN数据包传输到真实车辆的CAN总线而形成数据集。CAN数据包主要包含CAN标识号和数据域两个字段，其中数据域是8位，共9个特征。此外，Car-Hacking数据集主要涉及4类攻击：DoS攻击、Fuzzy攻击、装备欺骗（Gear-spoofing）攻击和转速欺骗（RPM-spoofing）攻击。

CICIDS2017数据集为车外网络数据集，它是入侵检测的专用数据集，包含了多个良性和最新的常见网络攻击，被广泛用于车载网络入侵检测算法的性能分析。考虑原CICIDS2017的样本数据较大，笔者从中随机抽取了56 661条样本数据进行训练和测试。表1列出样本数据在良性（Normal）攻击、DoS攻击、端口扫描（Portscan）攻击、暴力（Bruteforce）攻击、网络（Web）攻击和网络机器人（Bot）攻击6类样本的样本数及所占比例。

表1 CICIDS2017数据集样本分布

类型	样本数量	所占比例
Normal	22 731	40.11%
DoS	19 035	33.59%
Portscan	7 946	14.02%
Bruteforce	2 767	4.88%
Web	2 180	3.84%
Bot	2 02	3.52%

2.2 基于分位数归一化处理和图像数据的生成

考虑CNN模型在图像集上工作得更好，而车辆网络交通数据通常是表格数据。并且，现有的多数模型只是进行了数据预处理，如归一化处理，并没有将数据转换成图像数据再进行模型训练。因此，应将原始数据进行归一化处理，并转换为图像数据。

图像的像素值从0至255变化，采用分位数归一化法进行归一化处理，使其归一化后的像素值也在0至255区域。分位数归一化法是典型的多维数据处理方法，其基本思路是将一组数据按照大小排序，再将这些数据划分为多个等份，最终将每个数据映射到对应的分位数上，从而实现将不同量纲的数据转化为统一的尺度。

分位数归一化法将特征分布转换呈正态分布，并基于正态分布重新计算所有特征值。该方法缩短了数据间的差距，可提高数据分析的可比性和可解释性。

数据经归一化处理后，再利用数据的时间戳和特征将数据样本转换成数据块。令R^{CAR}和R^{CIC}分别表示已归一化的Car-Hacking和CICIDS2017数据集。用$X_i^{\mathrm{CAR}} \in R^{\mathrm{CAR}}$表示已归一化的Car-Hacking数据集中第$i$个样本，$Y_i^{\mathrm{CAR}}$表示样本$X_i^{\mathrm{CAR}}$的标签。类似地，用$X_\ell^{\mathrm{CIC}} \in R^{\mathrm{CIC}}$表示已归一化的CICIDS2017数据集中第$\ell$个样本，$Y_\ell^{\mathrm{CIC}}$表示样本$X_\ell^{\mathrm{CIC}}$的标签。

Car-Hacking数据集有9个重要特征。由于需要转换成三维图像，将27个（$9\times3=27$）连续样本数据作为一个数据块，该数据块总有243（$27\times9=243$）个特征，然后将这243个特征数据转换成三维图像，且该图像应体现原始数据的9个特征，因此，需要将$27\times9=243$的数据块转换成9×9的三维图像。

每个图是具有3个通道（红色、绿色和蓝色）的正方形彩色图。令I_k^{CAR}表示第k幅Car-Hacking数据的数据图，其包含的样本数为：

$$I_k^{\mathrm{CAR}} = \left\langle X_i^{\mathrm{CAR}} \| X_{i+1}^{\mathrm{CAR}}, \cdots, X_{i+26}^{\mathrm{CAR}} \right\rangle \tag{1}$$

其中，“||”表示拼接符。

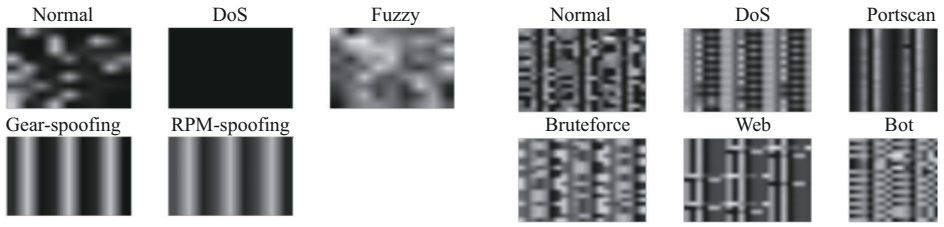
CICIDS2017数据集中的样本有20个重要特征。由于需要转换成三维图像，需要将60个（$20\times3=60$）连续样本构成一个数据块，再将此数据块转换成20×20的三维图像。由于图像是基于数据样本的时间戳生成的，因此，图像数据与保留原始样本数据的时间序列具有一定的相关性。令I_h^{CIC}表示第h幅CICIDS2017数据的数据图，其包含的样本数为：

$$I_h^{\mathrm{CIC}} = \left\langle X_\ell^{\mathrm{CIC}} \| X_{\ell+1}^{\mathrm{CIC}}, \cdots, X_{\ell+59}^{\mathrm{CIC}} \right\rangle \tag{2}$$

接下来，需要给每幅图像标上标签。令y_h^{CIC}和y_h^{CAR}分别表示I_k^{CAR}和I_h^{CIC}所对应的标签。为了保证正常样本（非攻击）的纯粹性，只有图数据所包含的样本全是正常样本，该图像数据的标签才是“Normal”。反之，若该幅图像数据中存在攻击样本，则需要统计每个攻击样本的个数，并将最频繁的攻击类型作为该幅图像的样本标签。例如，Fuzzy攻击在某幅图像中出现的次数最高，则该幅图像数据就被标为“Fuzzy攻击”。

图3给出的是Car-Hacking和CICIDS2017数据集的图像数据示例，其中图3（a）给出了Car-Hacking数据集中的5类样本的图像数据，图3（b）给出了CICIDS2017数据集中的6类样本的图像数据。

从图3（a）可知，Car-Hacking数据集中的5类样本的图像并不相同。Fuzzy攻击图像的特征模式比正常图像更随机化，而DoS攻击样本是高频



（a）Car-Hacking数据集　　（b）CICIDS2017数据集

图3　Car-Hacking数据集和CICIDS2017数据集的图像数据示例

空消息，故呈现纯黑色模式。Gear-spoofing 和 RPM-spoofing 通过注入带有某些 CAN 标识号和数据包的消息来伪装成合法用户，因此，它们的图像也具有属于它们的特征模式。类似地，如图3（b）所示，CICIDS2017数据集中6类攻击样本的图像数据也存在明显的差异。

2.3　CNN和TL

CNN 是一种常见的机器学习模型，广泛用于图像分类和识别领域[8]。图像可以直接输入 CNN 模型，无须额外的特征提取和数据重建过程。典型的 CNN 模型主要有 3 层：卷积层、池化层和全连接层[8]。在卷积层，通过卷积层操作提取图像的特征；在池化层，通过局部相关性避免过拟合，可以在不丢失重要信息的情况下降低数据复杂度；全连接层作为管道，可连接所有特征，并输出。

TL 是将在一个数据集上训练的深度神经网络（deep neural network，DNN）模型的权重转移到另一个数据集的过程[11]。利用 TL 技术，CNN 的底层模型可直接迁移到不同的任务中，即将 CNN 的底层模型进行迁移，而顶层根据应用进行调整。这不仅是因为 CNN 模型底层学习特征的模式适用不同任务的应用场景，还因为顶层所学习的特征是特定数据集的固定特征[11]。

具体而言，为了提升 TL 技术的有效性，可在迁移过程中进行微调。在微调过程中，将已训练模型中的大多数层进行冻结，即保留它们的权重。只解冻模型的顶层，并通过新的数据集训练顶层模型的参数。微调使学习模型能够更新预训练模型中的高阶特征，更好地适应目标任务或数据集[11]。

CNES 模型选择 5 个基础的 CNN 模型作为基学习器，它们分别是 VGG16、VGG19、 Xception、 Inception 和 Inception ResNet。它们在常用的图像分类任务上具有不错的性能，并在 ImageNet 数据集上进行了预训练。这些 ImageNet 数据集是一个基准图像处理数据集，拥有超过 100 万张图像。

视觉几何组（visual geometry group，VGG）是由牛津大学的视觉几何团队提出来的，它探索了通过提升网络深度提高最终的图像识别准确率的重要性。同时，VGG 尝试使用小的卷积核来构建深层的卷积网络。VGG 网络有 VGG16 和 VGG19 两种结构，这两种结构只是网络深度不一样。VGG16 架构[12]有 13 个卷积层、5 个池化层和 3 个全连接层。由于卷积层和全连接层有权重系数，它们也可统称为权重层，共 13+3=16 层，这也是 VGG16 架构中 16 的来源。而池化层不涉及权重，不属于权重层，故不被计数。VGG19 架构[13]比 VGG16 多 3 个卷积层，共 16+3=19 个权重层，这也是 VGG19 架构中 19 的来源。

Inception（INCE）网络[14]是 Christian Szegedy 在 2014 年提出的全新的深度学习结构。Inception 网络无须人为决定使用哪个过滤器和是否需要池化，而是由网络自行决定并确定相应的参数。

Xception（XCEP）则是 Inception 网络的扩展[15]，它使用依赖可分离卷积来取代标准的网络卷积，使得 Xception 对内存的需求小于 Inception

对内存需求。

Inception ResNet（INCER）[16]是Inception的另一个扩展，它将ResNet的剩余连接合并到Inception网络中。Inception ResNet在图像分类方面优于Inception模型，但它需要的计算操作和内存是Inception的2倍。

通过迁移学习和微调操作，利用车辆数据训练上述5个CNN模型，再选择其中性能最好的3个模型作为基学习器，以构建集成学习模型。

2.4 集成学习模型

集成学习模型是一种将多个基学习器集成在一起而构建的模型。由于集成学习模型的性能通常优于单个学习器的性能，因此它被广泛用于数据分析。平均法指计算多个模型输出的关系类型置信度的平均值。置信度就是概率，概率越大，置信度就越高。通常取置信度平均值最高的关系类型作为最终结果。

在集成学习模型中，Softmax层可输出包含每个样本类的分类置信度的后验概率列表，即每个分类的概率值。利用Softmax函数计算每个类的置信度值（概率值），Softmax函数的表达式如下。

$$\mathrm{Softmax}(z_i)=\frac{e^{z_i}}{\sum_{j=1}^{C}e^{z_j}} \tag{3}$$

其中，z_i表示输入变量，C表示数据集的分类数，e^{z_i}和e^{z_j}分别表示输入矢量和输出矢量的标准指数函数。

平均法是计算各基学习器的输出值（即概率值）的平均值，其表达式为：

$$\hat{y}=\underset{i\in\{1,2,\cdots,C\}}{\arg\max}\frac{\sum_{k=1}^{m}p_k(y=i|B_k,\boldsymbol{x})}{m} \tag{4}$$

其中，B_k表示第k个基学习器；m表示所选择的基学习器数，本文选择3个，即$m=3$；$p_k(y=i|B_k,\boldsymbol{x})$表示利用$B_k$对数据样本$\boldsymbol{x}$所预测的类标签。

与传统的只考虑类别标签的投票方法不同，平均法使集成模型能够检测不确定的分类结果，并通过使用分类置信度来纠正错误分类的样本。集成模型的整个计算复杂度取决于基学习器的复杂度，而平均法本身的时间复杂度为O（$O=N\cdot M\cdot C$），其中N表示样本案例数，M表示基学习器数，C表示分类数。通常M和C越小，执行平均法的速度就越快。

除了考虑平均法，本文还考虑级联的集成方法，并在后续的仿真实验中对比平均法和级联法的性能。级联的CNN模型旨在从基CNN模型的顶部密集层提取最高阶特征，再通过级联操作将所有特征集成到包含所有特征的新的级联层中。级联层之后就是Drop-out层和Softmax层。级联法的优势在于它能联合最高阶的特征，进而构造一个新的模型。然而，由于新模型需要在整个数据集上重新训练，因此，会引入额外的模型训练时间。级联法的复杂度为$O(O=N\cdot F)$，其中F表示从基CNN模型的密集层提取的总的特征数。

2.5 基于PSO的CNN模型超参数的优化

为了修剪出更优的基学习模型，进一步提升模型的性能，利用PSO优化CNN模型的超参数。与其他机器学习模型类似，CNN模型具有较多的超参数可优化。这些超参数可分为基于模型设计的超参数（model-design hyper-parameter，MDHP）和基于模型训练的超参数（model-training hyper-parameter，MTHP）两类。MDHP是指在设计模型时应给定的超参数，包括冻结层数、学习率和Drop-out率。而MTHP是指用于平衡训练速度和模型性能，包括批量尺寸、训练的次数以及提前停止训练的条件。这些超参数直接影响CNN模型的结构、有效性和效率。

作为典型的群体智能算法，PSO算法通过群体中个体间的协作，搜索特定空间内的最优解。对于任意粒子i，它的速度和位置可分别表示为

$\boldsymbol{V}_i$和$\boldsymbol{S}_i$。若粒子的搜索空间是d维，则：

$$\boldsymbol{V}_i=(v_{i1},v_{i2},\cdots,v_{ik},\cdots,v_{id}) \tag{5}$$

$$\boldsymbol{S}_i=(x_{i1},x_{i2},\cdots,x_{ik},\cdots,x_{id}) \tag{6}$$

其中，$i=1,2,\cdots,M$。M表示总的粒子数。

每个粒子根据适度值更新粒子的速度和位置：

$$v_{ik}^{n+1}=\omega v_{ik}^{n}+\ell_1 r_1\left(p_{ik}^{n}-x_{ik}^{n}\right)+\ell_2 r_2\left(G_{ik}^{n}-x_{ik}^{n}\right) \tag{7}$$

$$x_{ik}^{n+1}=x_{ik}^{n}+v_{ik}^{n+1} \tag{8}$$

其中，n表示当前迭代的次数；$\omega\in(0,1)$为惯性权重；ℓ_1和ℓ_2表示学习因子；$r_1,r_2\in(0,1)$为随机数；v_{ik}^{n}和x_{ik}^{n}表示粒子i在第n次迭代时的速度和位置；p_{ik}^{n}和G_{ik}^{n}表示粒子i在第n次迭代时个体极值和全局极值的位置。

为了提升收敛速度，采用自适应衰减的惯性权重策略。惯性权重ω依式（9）衰减：

$$\omega=\omega_{\max}-(\omega_{\max}-\omega_{\min})\left(\frac{n}{N_{\max}}\right)^{\tau} \tag{9}$$

其中，$\omega_{\max}$和$\omega_{\min}$分别表示最大和最小的惯性权重，n和$N_{\max}$分别表示当前迭代次数和允许最大的迭代次数，τ为衰减因子。在实验中，$\omega_{\max}=0.96$，$\omega_{\min}=0.4$，$\tau=0.5$，$\ell_1=0.5$，$\ell_2=2.4$，$N_{\max}=500$。

为此，利用PSO算法优化CNN模型的超参数，如图4所示，其中m_j表示第j次迭代。图4中的下半部分表示CNN模型的基本结构，其由输入层、卷积层、池化层、全连接层和输出层构成。CNN模型利用前向传播和反向传播算法训练模型和优化网络。前向传播由输入层，再依次到卷积层、池化层、全连接层，最终输出结果。而反向传播正好相反，先计算输出结果与期望值的差值（损失），再计算损失梯度，反向更新模型的参数。

考虑PSO算法的收敛速度快、须设置的参数少，利用PSO算法优化CNN模型超参数[17]的主要步骤如下。

步骤1　建立CNN模型的基本框架，并初始化PSO参数，包括粒子群大小、最大迭代次数、惯性权重、加速因子等。

步骤2　更新粒子位置和速度。

步骤3　以随机方式给CNN模型结构设置权重，并以CNN结构为粒子进行网络训练。

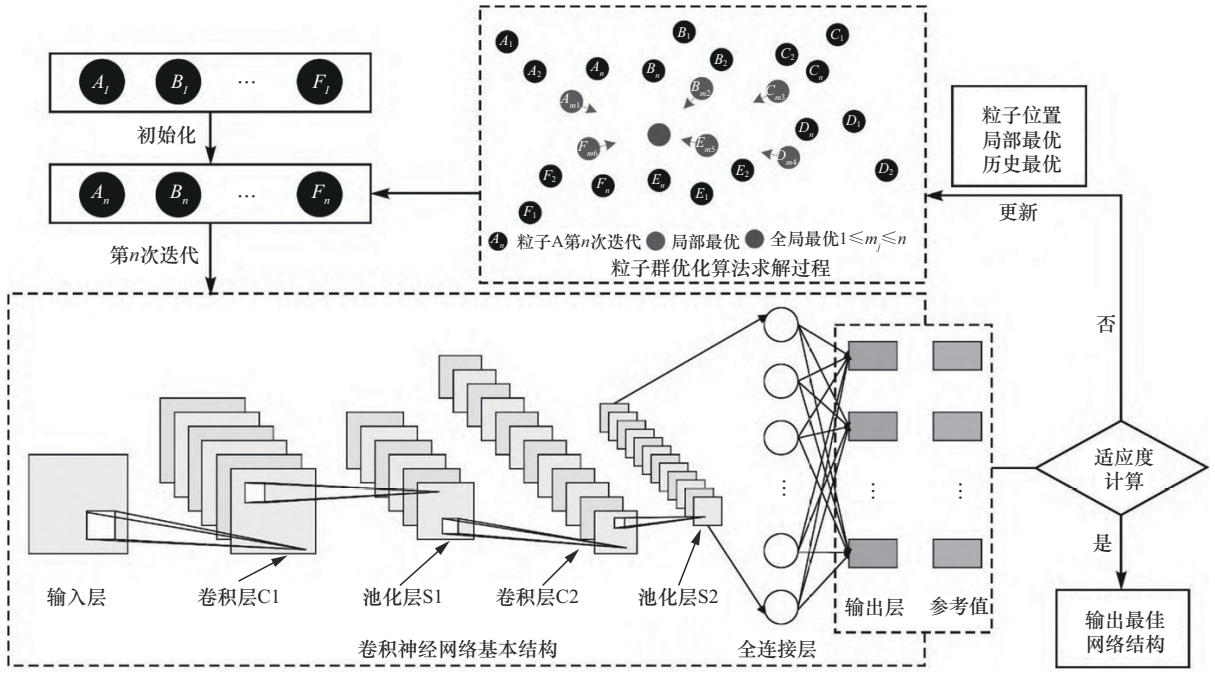


图4　基于PSO算法优化CNN模型的超参数

步骤4 将训练后的输出值（预测值）与真实值的均方根误差设定为适应度（Fitness），其定义如式（10）所示。

$$\text{Fitness}=\sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(y_i-\hat{y}\right)^2} \tag{10}$$

其中，y_i和$\hat{y}_i$分别表示真实值和预测值。

均方根误差反映预测值与真实值的偏差。通过最小化均方根误差，使预测值逼近真实值，进而优化模型参数。

步骤5 判断是否满足停止迭代的条件。当迭代次数达到最大或者均方根误差小于预设值（阈值），则停止迭代，否则就执行步骤2。

3 性能分析

3.1 实验环境

利用Python中的Scikit-learn和Keras库构建实验环境；利用Dell Precision 3630计算机（处理器为i7-8700、内存为16 GB）训练模型；利用Rasperry Pi 3（CPU为BCM2837B0 64位、内存为1 GB）测试模型性能。前者代表车联网中心服务器，后者表示车辆层次的服务器。

VGG16采用13个卷积层，每个卷积层的卷积核为3×3，激活函数为ReLU函数；采用5个池化层，每个池化层使用2×2的池化核，步长为2；采用3个全连接层，每个全连接层包含4 096个神经元，最后一个全连接层为输出层，使用Soft-max激活函数。VGG16与VGG19不同之处在于：VGG19采用了16个卷积层，而VGG16采用了13个卷积层。

Inception网络有多个版本，实验中选择Inception-V3版本。在Inception-V3网络中，输入图像依次经3个3×3的卷积层、3×3池化层、1×1卷积层、3×3卷积层和3×3池化层，各卷积层和池化层的步长分别是2、1、1、2、1、1和2。

Xception是基于Inception-V3改进的深度卷积神经网络架构，将Inception模块替换成深度可分离卷积。Xception与Inception-V3具有相同数量的参数。

利用Car-Hacking和CICIDS2017数据集验证CNES模型的性能。为了防止过拟合，选择精确率（Precision）、召回率（Recall）、F1值和准确率（Accuracy）4个性能指标，采用k交叉验证（k=5）。

F1值融合了精确率和召回率性能，是精确率和召回率的调和平均值，其表达式如式（11）所示。

$$\text{F1}=2\cdot\frac{\text{Precision}\cdot\text{Recall}}{\text{Precision}+\text{Recall}} \tag{11}$$

其中，Precision和Recall可由式（12）计算：

$$\begin{cases}\text{Precision}=\dfrac{\text{TP}}{\text{TP}+\text{FP}}\\ \text{Recall}=\dfrac{\text{TP}}{\text{TP}+\text{FN}}\end{cases} \tag{12}$$

其中，TP表示发生真阳性的次数；FP表示发生假阳性的次数；FN表示发生假阴性次数。

准确率（Accuracy）的表达如式（13）所示。

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{FP}+\text{TN}+\text{FN}} \tag{13}$$

其中，TN表示发生真阴性次数。

3.2 数据分析和讨论

依据第2.5节的表述，利用PSO算法优化通用的CNN模型参数以及VGG16、VGG19、Xception、Inception和Inception ResNet模型的超参数。图5给出了Fitness值随迭代次数变化的情况。从图5可知，随着迭代次数的增加，Fitness值快速下降。当迭代至约20次，Fitness值不再随迭代次数增加而下降。因此，可将20作为CNN模型的最优超参数值。

表2给出了超参数的搜索范围和经PSO算法优化后的最终参数值。例如，学习率的取值范围为（0.001，0.1），经PSO算法优化，得到最优学

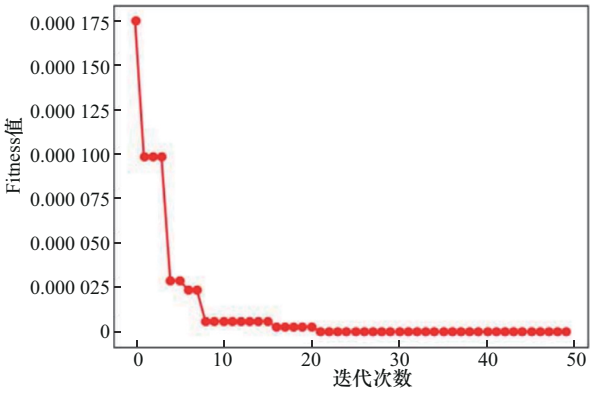


图5　Fitness值随迭代次数的变化曲线

习率为0.003。

表2　经PSO优化的超参数

超参数	模型	搜索范围	最优值
迭代次数	通用模型（CNN模型）	[5, 50]	20
批量尺寸		[32, 128]	128
提前停止耐力值		[2, 5]	3
学习率		（0.001, 0.1）	0.003
丢弃率		（0.2, 0.8）	0.5
冻结层数	Xception	[60, 125]	121
	VGG 16	[8, 16]	15
	VGG 19	[10, 19]	19
	Inception	[80, 159]	148
	InceptionResNet	[300, 572]	522

3.2.1　基于Car-Hacking数据集的检测性能分析

经PSO算法设定最优超参数后，首先利用Car-Hacking数据集验证CNES模型的性能。为此，选择针对IVN的入侵检测模型作为基准算法，对比分析它们的检测性能。这些基准算法是DTLS模型[6]、CNNS模型[7]和DNNS模型[8]。选择它们作为基准算法，主要是基于以下两点考虑：它们均针对IVN讨论了IVN的攻击检测问题，它们均利用Car-Hacking数据集验证算法性能。

基于Car-Hacking数据集的检测性能见表3，列出了DTLS模型、CNNS模型和DNNS模型的检测性能，包括准确率、精确率、召回率和F1值。由于CNES模型为集成模型，表3中还列出了5个基学习器（VGG16、VGG19、XCEP、INCE、INCER）的检测性能。此外，表3中的CNES-A模型和CNES-C模型分别表示CNES模型采用基于平均法和级联法的集成模型。

表3　基于Car-Hacking数据集的检测性能

	模型	准确率	精确率	召回率	F1值
基准模型	DTLS	98.10%	98.14%	98.04%	97.83%
	CNNS	99.60%	99.94%	99.63%	99.80%
	DNNS	99.93%	99.84%	99.87%	99.91%
基学习器	VGG16	999 7%	99.97%	99.97%	99.97%
	VGG19	100%	100%	100%	100%
	XCEP	100%	100%	100%	100%
	INCE	100%	100%	100%	100%
	INCER	100%	100%	100%	100%
	CNES-A	100%	100%	100%	100%
	CNES-C	100%	100%	100%	100%

从表3可知，5个基学习器中，除了VGG16检测性能未达到100%，其他4个基学习器的检测性能均达到100%。此外，CNES-A模型和CNES-C模型的准确率、精确率、召回率和F1值均达到100%。一方面，Car-Hacking数据集中正常类型与攻击类的图像差别较大，如图3所示，这有利于提升检测性能；另一方面，利用PSO算法优化CNN模型的超参数，也有助于提升CNES模型的收敛速度和检测性能。

相比于DTLS模型、CNNS模型和DNNS模型，CNES模型的检测性能提升了约0.09%。以F1值指标为例，DTLS、CNNS和DNNS模型的F1值分别为0.978 3、0.998 0和0.999 1，而CNES-A模型和CNES-C模型的F1值均

为1.00。

图6列出了CNES-A模型、CNES-C模型和5个基学习器的检测时间。从图6可知，5个基学习器的检测时间较短，且短于CNES-A模型和CNES-C模型的检测时间。CNES-A模型和CNES-C模型检测时间较长的原因在于：它们属于集成算法，需要先训练基学习器，再利用平均法或级联法进行最终的预测。

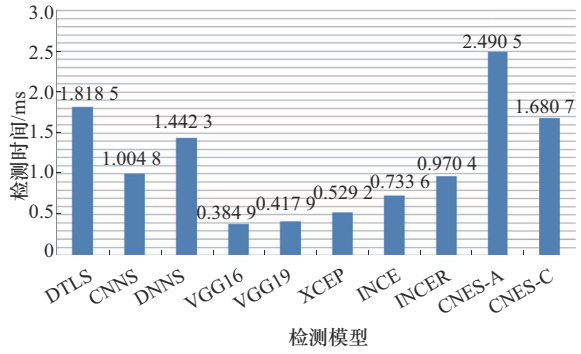


图6　基于Car-Hacking数据集的检测时间

3.2.2　基于CICIDS2017数据集的检测性能分析

CICIDS2017数据集是车外网络数据集，因此，选择FFNS模型[9]和NCNI模型[10]为基准算法参照。选择它们作为基准算法主要是基于以下两点考虑：它们均针对车外网络讨论了车外网络的攻击检测问题，它们均利用CICIDS2017数据集验证算法性能。

表4列出了基于CICIDS2017数据集的CNES模型、FFNS模型和NCNI模型的检测性能。

从表4可知，5个基学习器的F1值均达到0.99。VGG16的F1值属5个基学习器中的最低，但也达到0.996 7。这说明通过TL技术和PSO算法优化参数，可有效地提升模型的检测性能。此外，CNES-A和CNES-C模型的F1值均达到0.998 9和0.999 2，优于FFNS模型和NCNI模型。

将表3和表4进行对比不难发现，CNES模型在CICIDS2017数据集上的检测性能劣于在Car-Hacking数据集的性能。原因在于：Car-Hacking数据集的各类样本的特征更显著，显著的特征数据更容易分类。

表4　基于CICIDS2017数据集的检测性能

	模型	准确率	精确率	召回率	F1值
基准模型	FFNS	0.995 3	0.995 0	0.998 0	0.987 0
	NCNI	0.996 0	0.999 4	0.996 3	0.998 0
基学习器	VGG16	0.997 2	0.996 2	0.997 2	0.996 7
	VGG19	0.998 4	0.998 5	0.998 4	0.998 5
	XCEP	0.996 9	0.997 0	0.996 9	0.996 9
	INCE	0.997 5	0.997 2	0.997 5	0.997 2
	INCER	0.998 4	0.998 5	0.998 4	0.998 5
	CNES-A	0.998 9	0.999 0	0.998 9	0.998 9
	CNES-C	0.999 2	0.999 2	0.999 2	0.999 2

图7给出了CNES模型和5个基准模型的检测时间。从图7可知，CNES-A模型和CNES-C模型的检测时间仍高于其他模型，这也是集成算法存在的普遍问题。此外，相比于CNES-A模型，CNES-C模型的检测时间较短，降低了约1 ms。

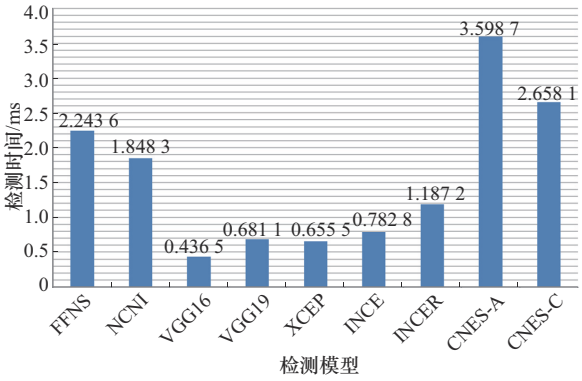


图7　基于CICIDS2017数据集的检测时间

此外，考虑车联网对处理数据包时延的苛刻要求，接下来分析模型的检测时延。若模型的检测时延过长，未达到车联网时延要求，则CNES模型无法应用到车联网的实际场景。检测时延标准依据文献[18]的研究：车联网中要求检测一个

数据包是否异常的时延应低于10 ms。

图8给出CNES模型和基准模基于CICIDS2017数据集检测单个样本的时延。从图8可知，5个基学习器检测单个样本的时延均低于1 ms，而CNES-A模型和CNES-C模型的检测单个样本的时延分别为1.8 ms和1.5 ms。尽管它们处理单个样本的时延较高，但均远低于10 ms。因此，CNES模型能满足车联网的检测时延性能。

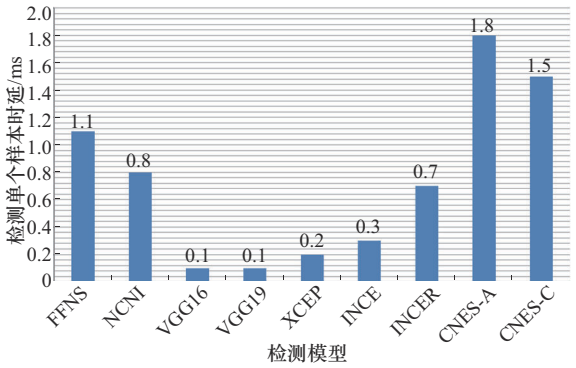


图8　检测单个样本的时延（基于CICIDS2017数据集）

4　结束语

现代汽车内广泛使用的CAN协议因缺乏认证和其他的安全措施，容易受到网络攻击。为此，本文提出一种基于CNN的集成学习的入侵检测模型CNES。CNES模型先将数据转换成图像，再利用当前5个先进CNN模型构建基学习器，并利用POS算法优化模型的超参数。依据基学习器的训练性能，从中选择3个性能优异的基学习器作为元学习器，并引用交叉验证策略避免过拟合。

利用Car-Hacking和CICIDS2017数据集验证各模型的监测性能，结果表明，CNES模型在Car-Hacking数据集上的准确率、精确率和F1值均达到100%，而在CICIDS2017数据集上的准确率、精确率和F1值也达到99%以上。

目前，本文只通过仿真实验验证了CNES模型的性能，还未能利用实际的车联网环境分析CNES模型的性能。未来，将进一步优化模型，并将模型应用于真实的车联网环境。

参考文献：

[1] 朱冰, 张培兴, 刘斌, 等. 基于自然驾驶数据的自动驾驶汽车安全性评价方法[J]. 中国公路学报, 2022, 35(7): 283-291.
ZHU B, ZHANG P X, LIU B, et al. Safety evaluation method of automated vehicle based on naturalistic driving data[J]. China Journal of Highway and Transport, 2022, 35(7): 283-291.

[2] 孙扬威, 戚湧. 基于聚类混合采样与PSO-Stacking的车载CAN入侵检测方法[J]. 计算机工程, 2023, 49(1): 138-145.
SUN Y W, QI Y. Intrusion detection method for in-vehicle CAN based on cluster mixed sampling and PSO-stacking[J]. Computer Engineering, 2023, 49(1): 138-145.

[3] 宋秀兰, 李洋阳, 何德峰. 外部干扰和随机DoS攻击下的网联车安全H_∞队列控制[J]. 自动化学报, 2024, 50(2): 348-355.
SONG X L, LI Y Y, HE D F. Secure H_∞ platooning control for connected vehicles subject to external disturbance and random DoS attacks[J]. Acta Automatica Sinica, 2024, 50(2): 348-355.

[4] 崔英祥, 张幽彤, 魏洪乾. 基于样本熵的车载CAN网络入侵检测[J]. 汽车工程, 2023, 45(7): 1184-1191.
CUI Y X, ZHANG Y T, WEI H Q. An intrusion detection system for in-vehicle CAN network based on sample entropy[J]. Automotive Engineering, 2023, 45(7): 1184-1191.

[5] 张瑶, 卢焕章, 王珏, 等. 短时记忆与CenterTrack的车辆多目标跟踪[J]. 中国图象图形学报, 2023, 28(10): 3107-3122.
ZHANG Y, LU H Z, WANG J, et al. Short-term memory and CenterTrack based vehicle-related multi-target tracking method[J]. Journal of Image and Graphics, 2023, 28(10): 3107-3122.

[6] MEHEDI S T, ANWAR A, RAHMAN Z, et al. Deep transfer learning based intrusion detection system for electric vehicular networks[J]. Sensors, 2021, 21(14): 4736.

[7] HOSSAIN M D, INOUE H, OCHIAI H, et al. An effective in-vehicle CAN bus intrusion detection system using CNN deep learning approach[C]//Proceedings of the GLOBECOM 2020 - 2020 IEEE Global Communications Conference. Piscataway: IEEE Press, 2020: 1-6.

[8] SONG H M, WOO J, KIM H K. In-vehicle network intrusion detection using deep convolutional neural network[J]. Vehicular Communications, 2020, 21: 100198.

[9] ROSAY A, CARLIER F, LEROUX P. Feed-forward neural network for network intrusion detection[C]// 2020 IEEE 91st Ve-

hicular Technology Conference (VTC2020-Spring). Piscataway: IEEE Press, 2020: 1-6.

[10] ROS S R, CAR V S. An improving intrusion detection model based on novel CNN technique using recent CIC-IDS datasets [C]// 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT). Piscataway: IEEE Press, 2024: 1-6.

[11] LEONARDO M M, CARVALHO T J, REZENDE E, et al. Deep feature-based classifiers for fruit fly identification (Diptera: Tephritidae) [C]// 2018 31st SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI). Piscataway: IEEE Press, 2018: 41-47.

[12] 岳洋, 张维, 苗耀锋. 基于自适应调整VGG16模型的乳腺癌风险预测[J]. 信息技术, 2024, 48(5): 138-143.
YUE Y, ZHANG W, MIAO Y F. A novel risk prediction based on adaptive adjustment VGG16 for breast cancer[J]. Information Technology, 2024, 48(5): 138-143.

[13] 王钰炜, 王雷, 郭新萍, 等. 基于复剪切波变换与VGG19模型的医学图像融合方法[J]. 山东理工大学学报(自然科学版), 2024, 38(4): 53-60.
WANG Y W, WANG L, GUO X P, et al. The medical image fusion method based on the complex shearlet transform and the VGG19 model[J]. Journal of Shandong University of Technology (Natural Science Edition), 2024, 38(4): 53-60.

[14] 张会影, 圣文顺, 金鑫. 基于深度流形学习的人脸年龄识别[J]. 无线电通信技术, 2024, 50(4): 799-806.
ZHANG H Y, SHENG W S, JIN X. Facial age recognition based on deep manifold learning[J]. Radio Communications Technology,2024,50(4) : 799-806.

[15] 张琦, 区锦锋, 周华英. 基于Xception与迁移学习的中药饮片图像识别研究[J]. 现代电子技术, 2024, 47(3): 29-33.
ZHANG Q, OU J F, ZHOU H Y. Research on traditional Chinese medicine piece image recognition based on Xception and transfer learning[J]. Modern Electronics Technique, 2024, 47 (3): 29-33.

[16] 李长文, 李鹏, 丁华. 基于GAF-inceptionResNet的齿轮箱故障诊断[J]. 机械传动, 2022, 46(6): 134-140.
LI C W, LI P, DING H. Gearbox fault diagnosis based on GAF-inceptionResNet[J]. Journal of Mechanical Transmission, 2022, 46(6): 134-140.

[17] 何佳星, 郑南山, 丁锐, 等. 粒子群优化卷积神经网络GNSS-IR土壤湿度反演方法[J]. 测绘学报, 2023, 52(8): 1286-1297.
HE J X, ZHENG N S, DING R, et al. A GNSS-IR soil moisture inversion method based on the convolutional neural network optimized by particle swarm optimization[J]. Acta Geodaetica et Cartographica Sinica, 2023, 52(8): 1286-1297.

[18] MOUBAYED A, SHAMI A, HEIDARI P, et al. Edge-enabled V2X service placement for intelligent transportation systems[J]. IEEE Transactions on Mobile Computing, 2021, 20(4): 1380-1392.

[作者简介]

张锐（1980− ），女，驻马店职业技术学院信息工程学院副教授，主要研究方向为计算机多媒体技术。