(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114157513 A
(43)申请公布日 2022.03.08

(21)申请号 202210116021.4

(22)申请日 2022.02.07

(71)申请人 南京理工大学
地址 210094 江苏省南京市玄武区孝陵卫街200号

(72)发明人 戚湧 刘洺君 俞建业

(74)专利代理机构 南京知识律师事务所 32207
代理人 熊敏敏

(51)Int.Cl.
*H04L 9/40*(2022.01)
*H04W 4/44*(2018.01)
*G06N 3/08*(2006.01)
*G06N 3/04*(2006.01)

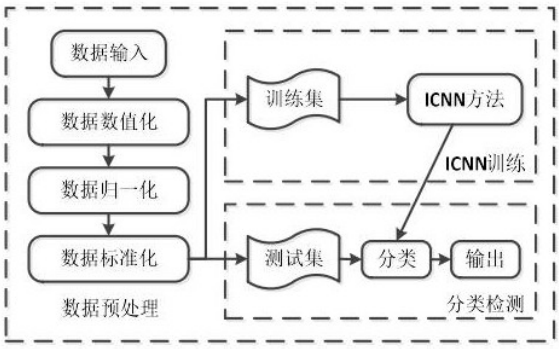
权利要求书3页 说明书8页 附图3页

(54)发明名称

基于改进卷积神经网络的车联网入侵检测方法及设备

(57)摘要

本发明属于车联网安全技术领域，公开了一种基于改进卷积神经网络的车联网入侵检测方法及设备。本发明的方法包括，采集车联网通信过程中的数据流量原始数据，输入到车联网入侵检测数据降维算法模型中进行预处理，得到车联网数据分析的标准化数据；将所述车联网数据分析的标准化数据输入改进卷积神经网络模型中进行计算，包括：将输入的数据进行卷积计算和非线性激活，进行分层；将每一层数据分别进行两次卷积操作、两次池化操作和一次全连接操作；通过SoftMax层对改进卷积神经网络模型输出数据集进行分类。本发明能够解决如何通过高效可靠的入侵检测方法实现车联网通信环境下对车联网的入侵行为数据的精准捕捉的问题。




CN 114157513 A

1.一种基于改进卷积神经网络的车联网入侵检测方法,其特征在于,所述方法包括:

采集车联网通信过程中的数据流量原始数据,输入到车联网入侵检测数据降维算法模型中进行预处理,得到车联网数据分析的标准化数据;

将所述车联网数据分析的标准化数据输入改进卷积神经网络模型中进行计算,包括:将输入的数据进行卷积计算和非线性激活,进行分层;将每一层数据分别进行两次卷积操作、两次池化操作和一次全连接操作;

通过SoftMax层对改进卷积神经网络模型输出数据集进行分类,识别出对车联网的入侵行为数据。

2.根据权利要求1所述的基于改进卷积神经网络的车联网入侵检测方法,其特征在于,所述车联网通信过程中的数据流量原始数据包括:

正常交互数据,包括由车载单元从云服务平台获取的信息;

由车载单元获取路侧设施的红绿灯信息以及路况、盲区信息;

车载单元与车载单元之间传递的信息和路况预警信息;

以及路侧设施将路侧传感数据或者高复杂度的计算结果以不同协议类型、网络连接状态、网络服务类型上传到云服务平台过程中产生的数据;

数据传输过程中不同攻击类型的异常入侵数据。

3.根据权利要求1所述的基于改进卷积神经网络的车联网入侵检测方法,其特征在于,所述预处理包括:

对所述车联网通信过程中的数据流量原始数据进行数据清洗;

对经过数据清洗后各种形式的数据进行数值化操作;

将数值化操作后的数据取值范围变为(0,1)之间的小数,并采用0均值标准化。

4.根据权利要求1所述的基于改进卷积神经网络的车联网入侵检测方法,其特征在于,所述将输入的数据进行卷积计算和非线性激活采用以下函数进行:

$$y_j^l = \sigma\left(\sum_{i\in M_j} y_i^{l-1} w_{ij}^l + b_i^l\right)$$

$$\mathrm{PRelu}(y) = \begin{cases} y(y > 0) \\ \mathrm{ay}(y \le 0) \end{cases}$$

其中,$y_j^l$ 表示第 $l$ 层第 $j$ 个卷积元激活函数的输出值,计算结果作为分层聚合模块的输入数据;$l$ 表示卷积层个数;$\sigma$ 表示激活函数;$y_i^{l-1}$ 表示第 $l-1$ 层中的第 $i$ 个输入特征;$w_{ij}^l$ 表示第 $l-1$ 层中的第 $i$ 个输入矩阵与第 $l$ 层中的第 $j$ 个位置的卷积权重;$b_i^l$ 表示第 $l$ 层卷积层特征图和第 $j$ 个位置的偏置量;当 $y$ 的值大于0时,车联网标准化数据的值为 $y$;当 $y$ 小于等于0时,车联网标准化数据的值为 $\mathrm{ay}$,$\mathrm{a}$ 的取值范围为(0,1)。

5.根据权利要求1所述的基于改进卷积神经网络的车联网入侵检测方法,其特征在于,所述将每一层数据分别进行两次卷积操作、两次池化操作和一次全连接操作包括:

1)经过卷积计算的特征进入池化层进行采样,其函数原型为:

$$z_j^l = \beta\left(w_j^l down\left(z_j^{l-1}\right) + b_j^l\right)$$

其中，$z_j^l$ 表示第 $l$ 层第 $j$ 个位置计算的输入结果；$l$ 表示池化层个数；$\beta$ 表示抽样函数；$w_j^l$ 表示第 $l$ 层特征图中的第 $j$ 个位置的池化权重；$z_j^{l-1}$ 表示第 $l-1$ 层中的第 $i$ 个输入；$down(z)$ 表示对矩阵元素 $z$ 的下采样操作；$b_j^l$ 表示第 $l$ 层池化层特征图中第 $j$ 个位置的偏置量；

2)对经过两次卷积操作、两次池化操作的抽样数据输入到全连接层进行计算，并利用以下聚合函数对结果进行聚合：

$$y_j^l = \sum_i w_{ij}^l * y_i^{l-1} + b_j^l$$

其中，$y_j^l$ 表示第 $l$ 层全连接层神经元中第 $j$ 个神经元经计算后的输入结果；$w_{ij}^l$ 表示 $l-1$ 层中特征图的第 $i$ 个特征与 $l$ 层中的第 $j$ 个神经元的连接权重；$y_i^{l-1}$ 为 $l-1$ 层中特征图的第 $i$ 个特征值；$b_j^l$ 为第 $l$ 层全连接层神经元中第 $j$ 个神经元的偏置值。

6.根据权利要求1所述的基于改进卷积神经网络的车联网入侵检测方法，其特征在于，所述方法还包括：

训练所述改进卷积神经网络，以找到最优参数组合。

7.根据权利要求6所述的基于改进卷积神经网络的车联网入侵检测方法，其特征在于，训练所述改进卷积神经网络包括：

在通过SoftMax层对改进卷积神经网络模型输出数据集进行分类之后，根据SoftMax层输出的分类检测结果执行反向传播方法找到最优参数组合，采用所述最优参数组合对改进卷积神经网络模型输出数据集进行分类。

8.根据权利要求7所述的基于改进卷积神经网络的车联网入侵检测方法，其特征在于，所述根据SoftMax层输出的分类检测结果执行反向传播方法找到最优参数组合过程包括：

根据SoftMax层输出的分类检测结果计算出总体误差参数值，通过对总体误差参数值经过反向传播操作，不断调整权值和偏差，进行最优参数组合；

所述SoftMax层采用的函数如下：

$$\mathrm{SoftMax}(y^l) = \mathrm{SoftMax}(\sum w^l * y^{l-1} + b^l)$$

其中，$\mathrm{SoftMax}(y^l)$ 为第 $l$ 层分类检测结果；$w^l$ 为第 $l$ 层的权重；$y^{l-1}$ 为第 $l-1$ 层中特征图的特征值；$b_j^l$ 为第 $l$ 层全连接层神经元的偏置值；

所述总体误差参数值计算方法如下：

$$C(w,b) = \frac{1}{2n}\sum_x y^{(x)} - a^2$$

其中，$C(w,b)$ 表示损失函数，用于计算出总体误差参数值，从而找出权值 $w$ 和偏置值 $b$ 最优参数组合，$w$ 表示网络权重；$b$ 表示网络偏移量；$n$ 表示训练输入数据的数量；$y^{(x)}$ 表示当输入为 $x$ 时的全连接层计算的输入；$a$ 表示当输入为 $x$ 时的向量的输入。

9.一种基于改进卷积神经网络的车联网入侵检测方法设备，其特征在于，所述设备包括存储器和处理器；所述存储器存储有实现基于改进卷积神经网络的车联网入侵检测方法

的计算机程序，所述处理器执行所述计算机程序，以实现根据权利要求1-8任一所述方法的步骤。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于：所述的计算机程序被处理器执行时实现根据权利要求1-8任一所述方法的步骤。

# 基于改进卷积神经网络的车联网入侵检测方法及设备

## 技术领域

[0001] 本发明属于车联网安全技术领域，具体涉及一种基于改进卷积神经网络的车联网入侵检测方法及设备。

## 背景技术

[0002] 近年来，随着新兴技术在车联网领域的实践应用，车联网得到更加快速的发展，车与车、与路、与人、与云的通信更加紧密，车联网通信安全对于促进智能交通和智慧城市的发展具有决定性的作用。随着通信能力的提升，大量的网络通信流量也随之而来，但因车联网中计算能力受限、应用环境复杂、分布式多节点和传感网络导致车联网安全问题十分突出，如何确保车联网的安全性，加快车联网落地应用成为汽车厂商和科研人员广泛讨论的话题。因此，利用入侵检测(Intrusion Detection, ID)技术确保车联网通信安全以及识别各种恶意攻击行为成为保障车联网安全的一种重要手段。

[0003] 针对入侵检测的问题，国内外学者提出了多种有效方法，包括机器学习SVM算法、DNN深度神经网络模型、MLP算法模型等，这些算法被用于解决传统入侵检测问题。如Anish Halima等人将SVM方法应用到入侵检测系统(IDS)中。采用SVM和Naive Bayes机器学习算法，应用归一化和特征简约进行分析对比。但是基于机器学习的入侵检测机制的重要缺点是需要大量的训练时间来处理网络先前数据流的大型数据集，在处理大数据网络环境中，尤其是复杂的车联网当中对检测时间极为重要。近年来，随着新兴技术在车联网领域的实践应用，车联网得到更加快速的发展，车与车、与路、与人、与云的通信更加紧密，车联网通信安全对于促进智能交通和智慧城市的发展具有决定性的作用。随着通信能力的提升，大量的网络通信流量也随之而来，但因车联网中计算能力受限、应用环境复杂、分布式多节点和传感网络导致车联网安全问题十分突出，如何确保车联网的安全性，加快车联网落地应用成为汽车厂商和科研人员广泛讨论的话题。因此，利用入侵检测(Intrusion Detection, ID)技术确保车联网通信安全以及识别各种恶意攻击行为成为保障车联网安全的一种重要手段。

[0004] 针对入侵检测的问题，国内外学者提出了多种有效方法，包括机器学习SVM算法、DNN深度神经网络模型、MLP算法模型等，这些算法被用于解决传统入侵检测问题。如Anish Halima等人将SVM方法应用到入侵检测系统(IDS)中。采用SVM和Naive Bayes机器学习算法，应用归一化和特征简约进行分析对比。但是基于机器学习的入侵检测机制的重要缺点是需要大量的训练时间来处理网络先前数据流的大型数据集，在处理大数据网络环境中，尤其是复杂的车联网当中对检测时间极为重要。R. Vinayakumar等人提出混合深度神经网络(DNN)模型用于检测和分类未知的网络攻击。丁红卫等人提出基于深度卷积神经网络的入侵检测方法，将网络数据转换为图像并进行降维。通过训练和识别从而提高检测的准确率、误报率和检测速率。

[0005] 但是以上这些算法不能直接应用在车联网的实际环境中，一是车联网结构复杂，不仅是车与自身需要通信，车与人、车与车、车与路以及车与云都需要交互；二是网络通信

协议和方式众多，不仅有蓝牙、无线、有线还有移动蜂窝网络和LTE-V2X；三是网络拓扑变化快，车辆是处于高速移动过程当中的，所以车联网的网络拓扑也是根据实际的环境在不断变化的。

[0006] 基于上述分析，如何通过高效可靠的入侵检测方法实现车联网通信环境下异常行为数据的精准捕捉，是目前需要解决的技术问题。

## 发明内容

[0007] 本发明目的是：针对现有技术的不足，提供一种基于改进卷积神经网络的车联网入侵检测方法及设备，用来解决如何通过高效可靠的入侵检测方法实现车联网通信环境下对车联网的入侵行为数据的精准捕捉的问题。

[0008] 具体地说，本发明是采用以下技术方案实现的。

[0009] 一方面，本发明提供一种基于改进卷积神经网络的车联网入侵检测方法，其特征在于，所述方法包括：

采集车联网通信过程中的数据流量原始数据，输入到车联网入侵检测数据降维算法模型中进行预处理，得到车联网数据分析的标准化数据；

将所述车联网数据分析的标准化数据输入改进卷积神经网络模型中进行计算，包括：将输入的数据进行卷积计算和非线性激活，进行分层；将每一层数据分别进行两次卷积操作、两次池化操作和一次全连接操作；

通过SoftMax层对改进卷积神经网络模型输出数据集进行分类，识别出对车联网的入侵行为数据。

[0010] 进一步地，所述车联网通信过程中的数据流量原始数据包括：

正常交互数据，包括由车载单元从云服务平台获取的信息；

由车载单元获取路侧设施的红绿灯信息以及路况、盲区信息；

车载单元与车载单元之间传递的信息和路况预警信息；

以及路侧设施将路侧传感数据或者高复杂度的计算结果以不同协议类型、网络连接状态、网络服务类型上传到云服务平台过程中产生的数据；

数据传输过程中不同攻击类型的异常入侵数据。

[0011] 进一步地，所述预处理包括：

对所述车联网通信过程中的数据流量原始数据进行数据清洗；

对经过数据清洗后各种形式的数据进行数值化操作；

将数值化操作后的数据取值范围变为(0,1)之间的小数，并采用0均值标准化。

[0012] 进一步地，所述将输入的数据进行卷积计算和非线性激活采用以下函数进行：

$$y_j^l = \sigma\left(\sum_{i\in M_j} y_i^{l-1} w_{ij}^l + b_i^l\right)$$

$$\mathrm{PRelu}(y) = \begin{cases} y(y > 0) \\ \mathrm{ay}(y \le 0) \end{cases}$$

其中，$y_j^l$ 表示第 $l$ 层第 $j$ 个卷积元激活函数的输出值，计算结果作为分层聚合模块的输入数据；$l$ 表示卷积层个数；$\sigma$ 表示激活函数；$y_i^{l-1}$ 表示第 $l-1$ 层中的第 $i$ 个输入特征；

$w_{ij}^{l}$表示第$l-1$层中的第$i$个输入矩阵与第$l$层中的第$j$个位置的卷积权重；$b_{i}^{l}$表示第$l$层卷积层特征图和第$j$个位置的偏置量；当$y$的值大于0时，车联网标准化数据的值为$y$；当$y$小于等于0时，车联网标准化数据的值为$ay$，a的取值范围为(0,1)。

[0013] 进一步地，所述将每一层数据分别进行两次卷积操作、两次池化操作和一次全连接操作包括：

1)经过卷积计算的特征进入池化层进行采样，其函数原型为：

$$z_{j}^{l}=\beta\left(w_{j}^{l}down\left(z_{j}^{l-1}\right)+b_{j}^{l}\right)$$

其中，$z_{j}^{l}$表示第$l$层第$j$个位置计算的输入结果；$l$表示池化层个数；$\beta$表示抽样函数；$w_{j}^{l}$表示第$l$层特征图中的第$j$个位置的池化权重；$z_{j}^{l-1}$表示第$l-1$层中的第$i$个输入；$down(z)$表示对矩阵元素$z$的下采样操作；$b_{j}^{l}$表示第$l$层池化层特征图中第$j$个位置的偏置量；

2)对经过两次卷积操作、两次池化操作的抽样数据输入到全连接层进行计算，并利用以下聚合函数对结果进行聚合：

$$y_{j}^{l}=\sum_{i}w_{ij}^{l}*y_{i}^{l-1}+b_{j}^{l}$$

其中，$y_{j}^{l}$表示第$l$层全连接层神经元中第$j$个神经元经计算后的输入结果；$w_{ij}^{l}$表示$l-1$层中特征图的第$i$个特征与$l$层中的第$j$个神经元的连接权重；$y_{i}^{l-1}$为$l-1$层中特征图的第$i$个特征值；$b_{j}^{l}$为第$l$层全连接层神经元中第$j$个神经元的偏置值。

[0014] 进一步地，所述基于改进卷积神经网络的车联网入侵检测方法还包括：

训练所述改进卷积神经网络，以找到最优参数组合。

[0015] 进一步地，训练所述改进卷积神经网络包括：

在通过SoftMax层对改进卷积神经网络模型输出数据集进行分类之后，根据SoftMax层输出的分类检测结果执行反向传播方法找到最优参数组合，采用所述最优参数组合对改进卷积神经网络模型输出数据集进行分类。

[0016] 进一步地，所述根据SoftMax层输出的分类检测结果执行反向传播方法找到最优参数组合过程包括：

根据SoftMax层输出的分类检测结果计算出总体误差参数值，通过对总体误差参数值经过反向传播操作，不断调整权值和偏差，进行最优参数组合；

所述SoftMax层采用的函数如下：

$$\mathrm{SoftMax}(y^{l})=\mathrm{SoftMax}(\sum w^{l}*y^{l-1}+b^{l})$$

其中，$\mathrm{SoftMax}(y^{l})$为第$l$层分类检测结果；$w^{l}$为第$l$层的权重；$y^{l-1}$为第$l-1$层中特征图的特征值；$b_{j}^{l}$为第$l$层全连接层神经元的偏置值；

所述总体误差参数值计算方法如下：

$$C(w,b)=\frac{1}{2n}\sum_x y^{(x)}-a^2$$

其中，$C(w,b)$表示损失函数，用于计算出总体误差参数值，从而找出权值$w$和偏置值$b$最优参数组合，$w$表示网络权重；$b$表示网络偏移量；n表示训练输入数据的数量；$y^{(x)}$表示当输入为$x$时的全连接层计算的输入；$a$表示当输入为x时的向量的输入。

[0017] 另一方面，本发明还提供基于改进卷积神经网络的车联网入侵检测方法设备，所述设备包括存储器和处理器；所述存储器存储有实现基于改进卷积神经网络的车联网入侵检测方法的计算机程序，所述处理器执行所述计算机程序，以实现上述方法的步骤。

[0018] 再一方面，本发明提供一种计算机可读存储介质，其上存储有计算机程序，其特征在于：所述的计算机程序被处理器执行时实现上述基于改进卷积神经网络的车联网入侵检测方法的步骤。

[0019] 本发明的基于改进卷积神经网络的车联网入侵检测方法及设备的有益效果如下：

本发明的基于改进卷积神经网络的车联网入侵检测方法，通过分层训练学习提升训练精度，利用卷积神经网络的端到端分类和反向传播方法检测网络数据、学习数据特征值和分类查找数据，实现卷积神经网络的参数值调整自动化并简化算法的流程。

[0020] 本发明的基于改进卷积神经网络的车联网入侵检测方法，能够精准捕捉车联网通信过程中的异常行为数据，提高车联网入侵检测的准确率，降低车联网入侵检测的假阳率(误报率)，有效地确保车联网通信的安全性。

[0021] 本发明能够在车联网环境下车与车、车与路、车与人、车与云的通信交互过程中使用，具有良好的可迁移性。

## 附图说明

[0022] 图1是本发明的基于改进卷积神经网络的车联网入侵检测方法流程图。

[0023] 图2是本发明的改进卷积神经网络模型示意图。

[0024] 图3是本发明和现有技术中相关方法效果对比图(148517条数据)。

[0025] 图4是本发明和现有技术中相关方法效果对比图(121981条数据)。

## 具体实施方式

[0026] 下面结合实施例并参照附图对本发明作进一步详细描述。

[0027] 实施例1：

本发明的一个实施例，为一种基于改进卷积神经网络的车联网入侵检测方法，对车联网数据流量进行入侵检测，获取检测结果。如图1所示，包括以下步骤：

一、采集车联网通信过程中的数据流量原始数据，输入到车联网入侵检测数据降维算法模型中进行预处理，得到车联网数据分析的标准化数据。

[0028] 1)所有交互数据不论采用怎样的交互手段，最终都会通过光纤等有线的方式进行汇聚。因此在传输节点(例如交换机或路由器)上连接入侵检测设备，对数据进行采集、去重、分析。

[0029] 数据流量主要是指在车联网通信过程中产生的数据交互相关数据，包括：

●正常交互数据，包括由车载单元(OBU)从云服务平台获取的娱乐信息服务、地图、路况、辅助驾驶等；

●由车载单元(OBU)获取路侧设施(RSU)的红绿灯信息以及路况、盲区信息；

●由车载单元与车载单元之间进行信息传递和路况预警等信息；

●以及路侧设施(RSU)将路侧传感数据或者高复杂度的计算结果上传到云服务平台等过程中产生的数据，共包括采集3种协议类型(TCP、UDP、ICMP)、11种网络连接状态(如0TH、REJ、RST0等)、70种网络服务类型(包括auth、bgp、http、ftp、telent等)；

●数据传输过程中的对车联网的入侵行为数据，包括DoS(拒绝服务)攻击、Probing(探测攻击)、R2L(远程非法访问)、U2R(越权访问)等。具体分类标识为back、land、neptune、pod、ipsweep、nmap等共计4大类39种攻击类型。

[0030] 2)对采集的通信数据进行预处理，包括数据清洗、数据数值化、归一化以及标准化处理。

[0031] 2-1)对所述车联网通信过程中的数据流量原始数据进行数据清洗。具体来说就是发送和接收车辆消息的车载单元(OBU)以及路侧设施(RSU)在进行交互的过程中对其中传输的数据进行检测和处理。清洗错误数据和丢失不全的数据，对没有数值化的数据进行数值化，成为有价值的新数据。

[0032] 2-2)对经过数据清洗后各种形式的数据进行数值化操作。就是将步骤2-1)得到的数据，由原来的字符型转化为数值型数据，从而能够更好地分析和识别数据的内容。例如将属性特征中的协议类型TCP、UDP、ICMP分别编码为1、2、3。

[0033] 2-3)将数值化操作后的数据取值范围由[0,58329]变为(0,1)之间的小数，便于更加快速地提取数据，消除数值化带来的不同量纲的影响。采用0均值标准化，通过数据的均值和标准差进行数据的标准化，经过处理的车联网数据符合标准正态分布，即均值为0，标准差为1，函数原型为：

$$X^* = \frac{X-\mu}{\sigma} \quad (1)$$

其中，$X^*$为标准化后输出矩阵，$X$为输入数据矩阵，$\mu$为当前车联网采集到的数据的均值，$\sigma$为当前车联网采集到的数据的标准差。

[0034] 经过预处理的数据一部分作为训练集，输入分层卷积神经网络模型进行训练，得到训练好的分层卷积神经网络模型；另一部分作为测试集，输入训练好的分层卷积神经网络模型中，进行入侵分类检测。

[0035] 二、将车联网数据分析的标准化数据输入改进卷积神经网络模型中进行计算。

[0036] 如图2所示，分层卷积神经网络模型结构的第一部分为数据输入模块，包含卷积计算和非线性激活(Conv1)，函数原型为：

$$y_j^l = \sigma\left(\sum_{i\in M_j} y_i^{l-1} w_{ij}^l + b_i^l\right) \quad (2)$$

$$PRelu(y) = \begin{cases} y(y>0) \\ ay(y\le 0) \end{cases} \quad (3)$$

其中，$y_j^l$表示第$l$层第$j$个卷积元激活函数的输出值，计算结果作为分层聚合模块的输入数据；$l$表示卷积层个数；$\sigma$表示激活函数；$y_i^{l-1}$表示第$l-1$层中的第$i$个输入特征；

$w_{ij}^{l}$表示第$l-1$层中的第$i$个输入矩阵与第$l$层中的第$j$个位置的卷积权重；$b_{i}^{l}$表示第$l$层卷积层特征图和第$j$个位置的偏置量；当$y$的值大于0时，车联网标准化数据的值为$y$；当$y$小于等于0时，车联网标准化数据的值为$ay$，a的取值范围为(0,1)。优选的，a的值为0.25。

[0037] 分层卷积神经网络模型结构的第二部分为分层聚合模块，在该模块中对输入的各层数据进行分层分批计算，包括对每一层数据进行两次卷积操作、两次池化操作和一次全连接操作：

1)经过卷积计算的特征进入池化层进行抽样，其函数原型为：

$$z_{j}^{l}=\beta\left(w_{j}^{l}down\left(z_{j}^{l-1}\right)+b_{j}^{l}\right) \quad (4)$$

其中，$z_{j}^{l}$表示第$l$层第$j$个位置计算的输入结果；$l$表示池化层个数；$\beta$表示抽样函数；$w_{j}^{l}$表示第$l$层特征图中的第$j$个位置的池化权重；$z_{j}^{l-1}$表示第$l-1$层中的第$i$个输入；$down(z)$表示对矩阵元素$z$的下采样操作；$b_{j}^{l}$表示第$l$层池化层特征图中第$j$个位置的偏置量。

[0038] 2)随后对经过两次卷积操作、两次池化操作的抽样数据输入到全连接层进行计算，并利用聚合函数对结果进行聚合：

$$y_{j}^{l}=\sum_{i}w_{ij}^{l}*y_{i}^{l-1}+b_{j}^{l} \quad (5)$$

其中，$y_{j}^{l}$表示第$l$层全连接层神经元中第$j$个神经元经计算后的输入结果；$w_{ij}^{l}$表示$l-1$层中特征图的第$i$个特征与$l$层中的第$j$个神经元的连接权重；$y_{i}^{l-1}$为$l-1$层中特征图的第$i$个特征值；$b_{j}^{l}$为第$l$层全连接层神经元中第$j$个神经元的偏置值。

[0039] 图2给出了经过预处理的数据输入分层卷积神经网络模型中进行计算的过程。

[0040] 1，输入的数据首先通过一个卷积层(Conv1)，对输入的所有数据需要进行一次卷积和非线性激活计算，进行降维，计算的结果作为分层聚合模块的输入数据。

[0041] 2．分层聚合模块对经过卷积(Conv1)计算后的输入数据进行分层卷积处理。Conv2和Conv3为一组、Conv4和Conv5为一组，每经过一次卷积计算所得到的特征图都要被池化层采样。即卷积层(Conv2)卷积的结果经过池化层(Max_Pooling1)采样之后，结果输入到卷积层(Conv3)卷积计算，得到的结果再经过池化层(Max_Pooling2)采样，这样做的目的是为了降低数据的维度，尽可能的提取到数据的区域特征，分层卷积计算的结果(即Max_Pooling1和Max_Pooling4的输出)再分别通过各自全连接层(FC1_Layer1、FC1_Layer2)，得到数据集。

[0042] 3．利用Concat函数对各层的全连接层(FC1_Layer和FC2_Layer)的输出结果进行聚合操作，生成完整的数据集。优选的，可以通过TensorFlow中的Concat函数对全连接层的结果进行合并操作。

[0043] 三、通过SoftMax层对改进卷积神经网络模型输出数据集进行分类，识别出对车联网的入侵行为数据。

[0044] SoftMax函数如下：

$$\mathrm{SoftMax}(y^{l})=\mathrm{SoftMax}(\sum w^{l}*y^{l-1}+b^{l}) \quad (6)$$

其中，$\mathrm{SoftMax}(y^l)$为第$l$层分类检测结果；$w^l$为第$l$层的权重；$y^{l-1}$为第$l-1$层中特征图的特征值；$b_j^l$为第$l$层全连接层神经元的偏置值。

[0045] 由于经过SoftMax层输出的分类检测结果与实际需要的值之间存在误差，在另一个实施例中，在对改进卷积神经网络进行训练时，根据SoftMax层输出的分类检测结果执行反向传播方法找到最优参数组合。具体包括：根据分类检测结果计算出总体误差参数值，通过对误差经过反向传播操作，不断调整权值和偏差，进行最优参数组合，从而输出需要的结果，减少误差带来的影响，达到较好的收敛效果。所述总体误差参数值计算方法如下：

$$C(w,b)=\frac{1}{2n}\sum_x y^{(x)}-a^2 \qquad (7)$$

其中，$C(w,b)$表示损失函数，用于计算出总体误差参数值，从而找出权值$w$和偏置值$b$最优参数组合，$w$表示网络权重；$b$表示网络偏移量；n表示训练输入数据的数量；$y^{(x)}$表示当输入为x时的全连接层计算的输入；a表示当输入为x时的向量的输入。

[0046] 为了验证本发明方法相较于现有技术具有较好的效果，使用相关数据集对方法进行对比验证。图3和图4为本发明的改进卷积神经网络(ICNN)和部分现有技术(LeNet-5、DBN、RNN、CNN、LSTM)的比较结果。其中图3在NSL-KDD数据集上比较，总共使用148517条数据，图4在UNSW-NB15数据集上比较，总共使用121981条数据，通过对五种不同方法与本方法的比较，改进卷积神经网络ICNN方法分别达到了97.01%和96.92%的准确率，95.55%和94.76%的真阳率，0.75%和0.88%的假阳率(误报率)因此，改进卷积神经网络ICNN方法的检查结果相比于其他检测方法在入侵检测数据样本中有较好的效果，能够提高入侵检测的准确率，降低入侵检测的假阳率(误报率)。

[0047] 在一些实施例中，上述技术的某些方面可以由执行软件的处理系统的一个或多个处理器来实现。该软件包括存储或以其他方式有形实施在非暂时性计算机可读存储介质上的一个或多个可执行指令集合。软件可以包括指令和某些数据，这些指令和某些数据在由一个或多个处理器执行时操纵一个或多个处理器以执行上述技术的一个或多个方面。非暂时性计算机可读存储介质可以包括例如磁或光盘存储设备，诸如闪存、高速缓存、随机存取存储器(RAM)等的固态存储设备或其他非易失性存储器设备。存储在非临时性计算机可读存储介质上的可执行指令可以是源代码、汇编语言代码、目标代码或被一个或多个处理器解释或以其他方式执行的其他指令格式。

[0048] 计算机可读存储介质可以包括在使用期间可由计算机系统访问以向计算机系统提供指令和/或数据的任何存储介质或存储介质的组合。这样的存储介质可以包括但不限于光学介质(例如，光盘(CD)、数字多功能光盘(DVD)、蓝光光盘)、磁介质(例如，软盘、磁带或磁性硬盘驱动器)、易失性存储器(例如，随机存取存储器(RAM)或高速缓存)、非易失性存储器(例如，只读存储器(ROM)或闪存)或基于微机电系统(MEMS)的存储介质。计算机可读存储介质可以嵌入计算系统(例如，系统RAM或ROM)中，固定地附接到计算系统(例如，磁性硬盘驱动器)，可移除地附接到计算系统(例如，光盘或通用基于串行总线(USB)的闪存)，或者经由有线或无线网络(例如，网络可访问存储(NAS))耦合到计算机系统。

[0049] 请注意，并非上述一般性描述中的所有活动或要素都是必需的，特定活动或设备的一部分可能不是必需的，并且除了描述的那些之外可以执行一个或多个进一步的活动或包括的要素。更进一步，活动列出的顺序不必是执行它们的顺序。而且，已经参考具体实施

例描述了这些概念。然而，本领域的普通技术人员认识到，在不脱离如下权利要求书中阐述的本公开的范围的情况下，可以进行各种修改和改变。因此，说明书和附图被认为是说明性的而不是限制性的，并且所有这样的修改被包括在本公开的范围内。

[0050] 上面已经关于具体实施例描述了益处、其他优点和问题的解决方案。然而，可能导致任何益处、优点或解决方案发生或变得更明显的益处、优点、问题的解决方案以及任何特征都不应被解释为任何或其他方面的关键、必需或任何或所有权利要求的基本特征。此外，上面公开的特定实施例仅仅是说明性的，因为所公开的主题可以以受益于这里的教导的本领域技术人员显而易见的不同但等同的方式进行修改和实施。除了在权利要求书中描述的以外，没有意图限制在此示出的构造或设计的细节。因此明显的是，上面公开的特定实施例可以被改变或修改，并且所有这样的变化被认为在所公开的主题的范围内。

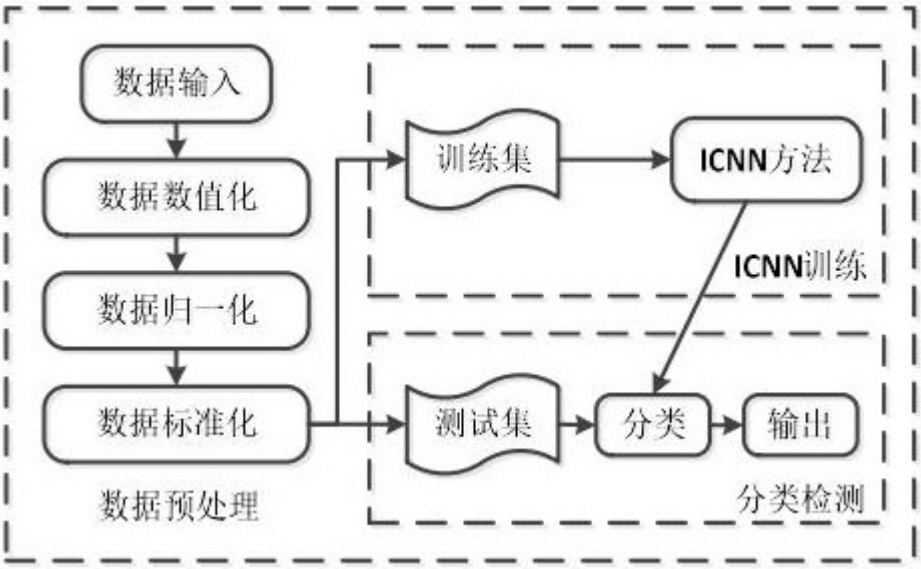

数据输入
数据数值化
数据归一化
数据标准化
数据预处理
训练集
ICNN方法
ICNN训练
测试集
分类
输出
分类检测

图1

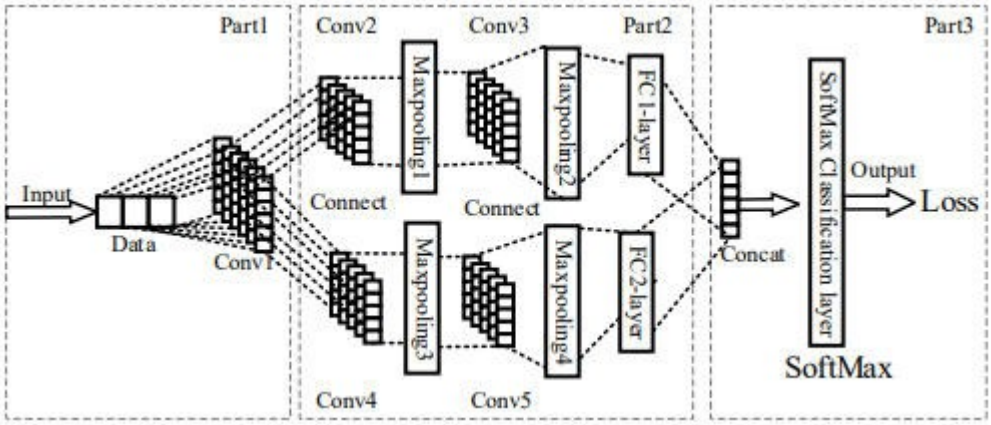

Part1
Conv2
Conv3
Part2
Part3
Input
Data
Conv1
Maxpooling1
Maxpooling2
FC1-layer
Connect
Connect
Maxpooling3
Maxpooling4
FC2-layer
Concat
SoftMax Classification layer
Output
Loss
SoftMax
Conv4
Conv5

图2

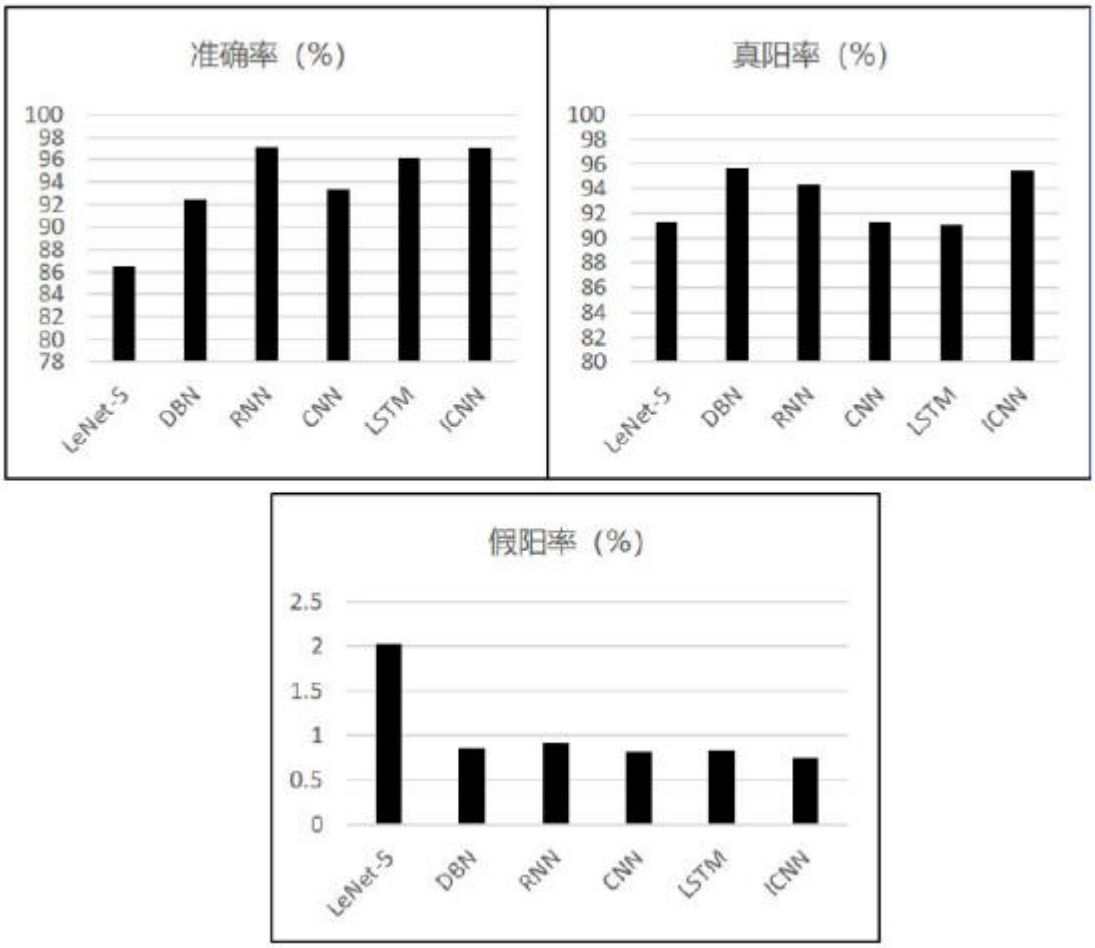

准确率（%）
100
98
96
94
92
90
88
86
84
82
80
78
LeNet-5
DBN
RNN
CNN
LSTM
ICNN
真阳率（%）
100
98
96
94
92
90
88
86
84
82
80
LeNet-5
DBN
RNN
CNN
LSTM
ICNN
假阳率（%）
2.5
2
1.5
1
0.5
0
LeNet-5
DBN
RNN
CNN
LSTM
ICNN

图3

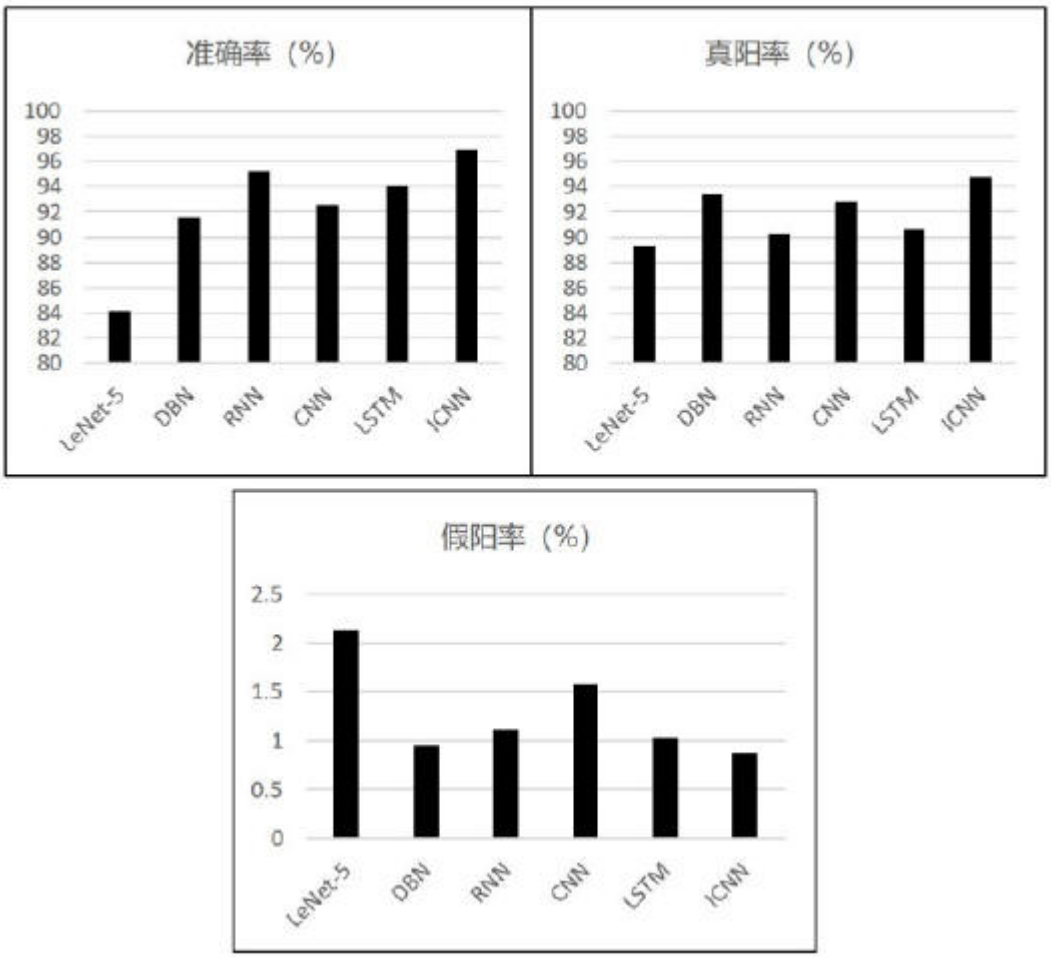

准确率（%）
100
98
96
94
92
90
88
86
84
82
80
LeNet-5
DBN
RNN
CNN
LSTM
ICNN
真阳率（%）
100
98
96
94
92
90
88
86
84
82
80
LeNet-5
DBN
RNN
CNN
LSTM
ICNN
假阳率（%）
2.5
2
1.5
1
0.5
0
LeNet-5
DBN
RNN
CNN
LSTM
ICNN

图4