(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 110324337 A
(43)申请公布日 2019.10.11

(21)申请号 201910588118.3

(22)申请日 2019.07.02

(71)申请人 成都信息工程大学
地址 610225 四川省成都市西南航空港经济开发区学府路一段24号

(72)发明人 石磊 王阳军 李飞 王娟 张浩曦 张路桥 吴春旺 丁哲 徐静

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 吴东勤

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 12/40(2006.01)
G06N 3/04(2006.01)

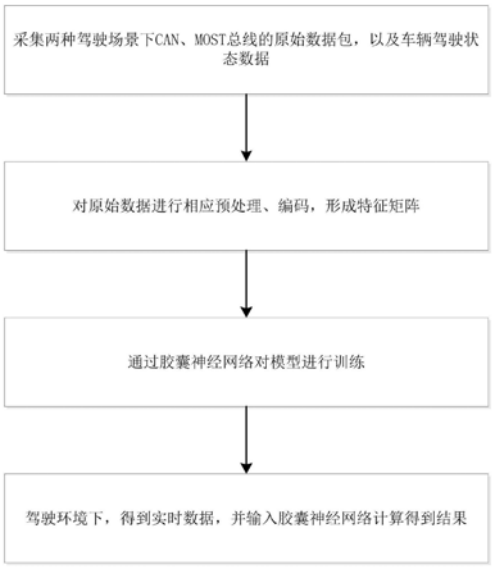
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种基于胶囊神经网络的车内网入侵检测方法及系统

(57)摘要

本发明属于汽车电子技术领域，公开了一种基于胶囊神经网络的车内网入侵检测方法及系统，依靠车辆CAN、MOST总线实时动态数据作为原始数据中的包频率、序列信息作为特征，同时结合车辆驾驶状态信息作为特征，并进行相关的特殊方法，转化为特征矩阵进行处理；胶囊神经网络可以对特征之间的相关性进行高位建模。本发明引入了基于胶囊神经网络的模型，对特征数据之间的结构关系进行挖掘，提高传统神经网络入侵检测方法的准确度，增强了车辆驾驶的安全性，同时模型更具有普遍性，实用性较好。



CN 110324337 A

1.一种基于胶囊神经网络的车内网入侵检测方法,其特征在于,所述基于胶囊神经网络的车内网入侵检测方法结合多种车内网数据总线实时动态数据与驾驶状态动态数据检测;按照一定的时间间隔参数u进行划分,构成总样本集;

对车内网数据转换为特征矩阵,以输出给后面的模块挖掘空间关系结构特征;

引入基于胶囊神经网络处理模型,建立适合车内网环境下数据的处理结构,对特征关系的结构进行高维建模。

2.如权利要求1所述的基于胶囊神经网络的车内网入侵检测方法,其特征在于,所述基于胶囊神经网络的车内网入侵检测方法进一步包括:

第一步,采集两种场景下车内网原始特征数据,并进行预处理:

分别在两种场景下采集车内网中CAN总线、MOST总线数据包数据,以及车辆速度、车辆加速度、转向、刹车数据;两种场景分别是无外网链接的正常驾驶场景与有外网攻击连接的攻击驾驶场景;对采集到的各数据按照一定的时间间隔参数u进行划分,构成总样本集,对两类数据进行胶囊神经网络模型的训练;将该总样本集70%的数据进行模型训练,30%用于模型的效果验证;在进行训练之前,对原始样本数据进行相应的预处理;

第二步,应用胶囊神经网络结构对参考模型参数进行计算,胶囊神经网络结构包括卷积层、一级胶囊层、次胶囊层;特征矩阵的维度为row*col;

卷积层:经过预处理后,特征矩阵通过卷积核运算得到卷积层,卷积层检测特征矩阵的基本特征;

一级胶囊层:共8个主胶囊,接受卷积层检测到的基本特征,生成特征的组合;卷积层得到的每8个卷积结果运算得到一个主胶囊模块;

次级胶囊层:包含2个数字胶囊,每个胶囊对应判断是否存在入侵检测状态的结果,每个数字胶囊的维度为50;一级胶囊层和次级胶囊层通过动态路由算法进行计算得到。

3.如权利要求2所述的基于胶囊神经网络的车内网入侵检测方法,其特征在于,第一步预处理方法包括:

(1)对于每一个时间间隔t采集到的CAN总线、MOST总线数据包数据,按照CAN与MOST数据包类型进行包统计概率的特征计算,构成特征向量x1、x2;

(2)在采集以上CAN与MOST数据包时,按照时间到来的先后顺序,对各类型数据包序列进行记录,构成类型序列原始数据;对CAN、MOST总线数据类型进行one-hot encoding类型编码;采用1/M作为采样间隔对各类型序列数据包进行采样,构成特征序列向量x3、x4;

(3)对于上述时间间隔t,采用更细微的采样频率n,采集车辆驾驶状态数据进行处理,采集的数据包括车辆速度、车辆加速度、转向角度与加速度、刹车数据;计算车辆速度、车辆加速度、转向角度与加速度、刹车数据的20个相关系数作为特征向量x5;计算相关系数算法采用:

$$r(x,y)=\frac{\sum_{i=1}^{n}x_i y_i-n\overline{X}\,\overline{Y}}{n\sigma_x\sigma_y}$$

其中,其中x_i为一种类型驾驶状态数据,y_i为另一种类型数据,$\overline{X}$、$\overline{Y}$分别为两种状

态数据的平均值，σ_x、σ_y分别为两种驾驶状态数据的标准差；

(4)对以上的特征向量x1～x5进行特征矩阵标准化处理；x3向量中有CAN的n1数据包，one-hot encoding编码长度为len1，x4向量中有MOST的n2数据包，one-hot encoding编码长度为len2，则取特征矩阵的列数：

$$col = \max(len1, len2) * \max(\sqrt{n1}, \sqrt{n2});$$

在标准化x3、x4向量时，按照二维矩阵空间位置进行处理；有剩余无法放置某一个类型数据的地方补0，在设置完上述信息后，对x1、x2、x5进行处理，分别放置在标准矩阵后面行的位置，构成整个特征矩阵数据。

4.如权利要求2所述的基于胶囊神经网络的车内网入侵检测方法，其特征在于，一级胶囊层传递给次级胶囊层的运算中，运用的计算环节函数有：

$$\hat{\mathbf{u}}_{j|i} = \mathbf{W}_{ij}\mathbf{u}_i;$$

$$\mathbf{s}_j = \sum_i c_{ij}\hat{\mathbf{u}}_{j|i};$$

$$\mathbf{v}_j = \frac{\|\mathbf{s}_j\|^2}{1+\|\mathbf{s}_j\|^2}\frac{\mathbf{s}_j}{\|\mathbf{s}_j\|};$$

其中，$\hat{\mathbf{u}}_{j|i}$表示胶囊之间的仿射运算、s_j表示输入向量的标量加权运算，以及v_j表示squash压缩函数；c_{ij}通过囊间路由算法迭代得到，计算方法采用softmax函数，即：

$$c_{ij} = \frac{\exp(b_{ij})}{\sum_k \exp(b_{ik})};$$

其中，b_{ij}在迭代过程中初始化为0，然后通过囊间路由算法计算；最后通过次级胶囊计算$||v_j||$得到属于是否入侵判断的概率。

5.如权利要求2所述的基于胶囊神经网络的车内网入侵检测方法，其特征在于，第一步在训练阶段，采用如下方法对损失进行计算：

$L_c = T_c \max(0, m^+ - ||v_c||)^2 + \lambda(1-T_c)\max(0, ||v_c|| - m^-)$；

通过如上的胶囊神经网络对70％样本数据进行训练，并通过剩余的30％样本数据进行测试。

6.一种实施权利要求1所述的基于胶囊神经网络的车内网入侵检测方法的基于胶囊神经网络的车内网入侵检测系统。

7.一种实施权利要求1所述的基于胶囊神经网络的车内网入侵检测方法的车内网入侵检测终端。

一种基于胶囊神经网络的车内网入侵检测方法及系统

技术领域

[0001] 本发明属于汽车电子技术领域，尤其涉及一种基于胶囊神经网络的车内网入侵检测方法及系统。

背景技术

[0002] 目前，最接近的现有技术：

[0003] 智能化、网络化使得汽车内部电子设备数量迅速增加，电控系统日益复杂。这些车载电子设备、电控单元与外界的信息交互也越来越多，而这些车载设备、电控单元绝大部分都连接到了汽车内部的总线网络，来自网络的安全威胁会通过汽车与外部的接口渗透到关键的车载总线网络系统。黑客可以利用安全漏洞进行信息窃取和车辆的安全攻击，如果一旦车辆被恶意超控，将会对人民的生命造成严重威胁。因此，进行车内网入侵检测是加强汽车安全非常重要的手段之一。

[0004] 入侵检测作为一种主动防御技术，已逐渐成为确保网络系统安全的关键技术。入侵检测系统(IDS,Intrusion Detection System)是专为提供网络安全主动保护而设计的，它基于一定的安全策略来监控网络系统的运行，发现各种入侵行为，企图或结果，并自动进行响应，有效防止非法访问或入侵。

[0005] 然而随着当前网络环境迈入大数据与智能化时代，传统入侵检测方法及系统逐渐开始难以应对海量数据和复杂网络环境带来的影响。因此为了提升IDS检测性能与效率，近年来国内外研究者们开始在IDS构建中引入机器学习方法并且取得了许多突破性的进展。综上所述，现有技术存在的问题是：

[0006] (1)现有技术中，利用现有的Internet或以太网入侵检测方法，对于车辆内部网络适用性较差；

[0007] (2)某些针对车内网的方法，仅依赖于某一类总线数据，难以对整个车辆内部可能遭受的威胁进行检测；现有方法没有结合车辆自身驾驶状态信息进行分析，增加了误报率；

[0008] (3)同时，现有方法大都没有考虑不同特征类数据之间的相关性，仅依靠简单的神经网络方法难以对特征关系进行高维建模，降低了方法的准确检测率。

[0009] 解决上述技术问题的意义：

[0010] 针对车内网多总线复杂数据类型，且攻击数据报文与汽车状态数据存在着高度的相关性，如何利用神经网络构建数据高维特征关联，实现在车内网的环境下完成入侵行为的检测，提高检测的准确性是非常重要的。

发明内容

[0011] 针对现有技术存在的问题，本发明提供了一种基于胶囊神经网络的车内网入侵检测方法及系统。

[0012] 本发明是这样实现的，一种基于胶囊神经网络的车内网入侵检测方法，所述基于胶囊神经网络的车内网入侵检测方法结合多种车内网数据总线实时动态数据与驾驶状态

动态数据检测;按照一定的时间间隔参数u进行划分,构成总样本集;

[0013] 对车内网数据转换为特征矩阵,以输出给后面的模块挖掘空间关系结构特征;

[0014] 引入基于胶囊神经网络处理模型,建立适合车内网环境下数据的处理结构,对特征关系的结构进行高维建模。

[0015] 进一步,所述基于胶囊神经网络的车内网入侵检测方法进一步包括:

[0016] 第一步,采集两种场景下车内网原始特征数据,并进行预处理:

[0017] 分别在两种场景下采集车内网中CAN总线、MOST总线数据包数据,以及车辆速度、车辆加速度、转向、刹车数据;两种场景分别是无外网链接的正常驾驶场景与有外网攻击连接的攻击驾驶场景;对采集到的各数据按照一定的时间间隔参数u进行划分,构成总样本集,对两类数据进行胶囊神经网络模型的训练;将该总样本集70%的数据进行模型训练,30%用于模型的效果验证;在进行训练之前,对原始样本数据进行相应的预处理;

[0018] 第二步,应用胶囊神经网络结构对参考模型参数进行计算,胶囊神经网络结构包括卷积层、一级胶囊层、次胶囊层;特征矩阵的维度为row*col;

[0019] 卷积层:经过预处理后,特征矩阵通过卷积核运算得到卷积层,卷积层检测特征矩阵的基本特征;

[0020] 一级胶囊层:共8个主胶囊,接受卷积层检测到的基本特征,生成特征的组合;卷积层得到的每8个卷积结果运算得到一个主胶囊模块;

[0021] 次级胶囊层:包含2个数字胶囊,每个胶囊对应判断是否存在入侵检测状态的结果,每个数字胶囊的维度为50;一级胶囊层和次级胶囊层通过动态路由算法进行计算得到。

[0022] 进一步,第一步预处理方法包括:

[0023] (1)对于每一个时间间隔t采集到的CAN总线、MOST总线数据包数据,按照CAN与MOST数据包类型进行包统计概率的特征计算,构成特征向量x1、x2;

[0024] (2)在采集以上CAN与MOST数据包时,按照时间到来的先后顺序,对各类型数据包序列进行记录,构成类型序列原始数据;对CAN、MOST总线数据类型进行one-hot encoding类型编码;采用1/M作为采样间隔对各类型序列数据包进行采样,构成特征序列向量x3、x4;

[0025] (3)对于上述时间间隔t,采用更细微的采样频率n,采集车辆驾驶状态数据进行处理,采集的数据包括车辆速度、车辆加速度、转向角度与加速度、刹车数据;计算车辆速度、车辆加速度、转向角度与加速度、刹车数据的20个相关系数作为特征向量x5;计算相关系数算法采用:

[0026] $$r(x,y)=\frac{\sum_{i=1}^{n}x_i y_i - n\overline{X}\,\overline{Y}}{n\sigma_x\sigma_y}$$

[0027] 其中,其中x_i为一种类型驾驶状态数据,y_i为另一种类型数据,$\overline{X}$、$\overline{Y}$分别为两种状态数据的平均值,σ_x、σ_y分别为两种驾驶状态数据的标准差;

[0028] (4)对以上的特征向量x1～x5进行特征矩阵标准化处理;x3向量中有CAN的n1数据包,one-hot encoding编码长度为len1,x4向量中有MOST的n2数据包,one-hot encoding编码长度为len2,则取特征矩阵的列数:

[0029] $col = \max(len1, len2) * \max(\sqrt{n1}, \sqrt{n2})$；

[0030] 在标准化x3、x4向量时，按照二维矩阵空间位置进行处理；有剩余无法放置某一个类型数据的地方补0，在设置完上述信息后，对x1、x2、x5进行处理，分别放置在标准矩阵后面行的位置，构成整个特征矩阵数据。

[0031] 进一步，一级胶囊层传递给次级胶囊层的运算中，运用的计算环节函数有：

[0032] $\hat{\mathbf{u}}_{j|i} = \mathbf{W}_{ij}\mathbf{u}_i$；

[0033] $\mathbf{s}_j = \sum_i c_{ij} \hat{\mathbf{u}}_{j|i}$；

[0034] $\mathbf{v}_j = \frac{\|\mathbf{s}_j\|^2}{1+\|\mathbf{s}_j\|^2} \frac{\mathbf{s}_j}{\|\mathbf{s}_j\|}$；

[0035] 其中，$\hat{\mathbf{u}}_{j|i}$表示胶囊之间的仿射运算、s_j表示输入向量的标量加权运算，以及v_j表示squash压缩函数；c_{ij}通过囊间路由算法迭代得到，计算方法采用softmax函数，即：

[0036] $c_{ij} = \frac{\exp(b_{ij})}{\sum_k \exp(b_{ik})}$；

[0037] 其中，b_{ij}在迭代过程中初始化为0，然后通过囊间路由算法计算；最后通过次级胶囊计算$||v_j||$得到属于是否入侵判断的概率。

[0038] 进一步，第一步在训练阶段，采用如下方法对损失进行计算：

[0039] $L_c = T_c \max(0, m^+ - ||v_c||)^2 + \lambda(1-T_c)\max(0, ||v_c|| - m^-)$；

[0040] 通过如上的胶囊神经网络对70％样本数据进行训练，并通过剩余的30％样本数据进行测试。

[0041] 本发明的另一目的在于提供一种实施所述的基于胶囊神经网络的车内网入侵检测方法的基于胶囊神经网络的车内网入侵检测系统。

[0042] 本发明的另一目的在于提供一种实施所述的基于胶囊神经网络的车内网入侵检测方法的车内网入侵检测终端。

[0043] 综上所述，本发明的优点及积极效果为：

[0044] 本发明提出了一种基于胶囊神经网络的车内网入侵检测方法。该方法不仅依靠车辆CAN、MOST总线实时动态数据作为原始数据中的包频率、序列信息作为特征，同时结合车辆驾驶状态信息作为特征，并进行相关的特殊方法，转化为特征矩阵进行处理。胶囊神经网络可以对特征之间的相关性进行高位建模，本发明引入了基于胶囊神经网络的模型，对特征数据之间的结构关系进行挖掘，提高传统神经网络入侵检测方法的准确度，增强了车辆驾驶的安全性，同时模型更具有普遍性，实用性较好。

[0045] 针对未来的车辆具有更加智能化、信息化的特征，本发明中提出的入侵检测方法，结合了对可以对高维特征结构进行建模的神经网络方法，研究成果可以用于车企的汽车生产与设计，能够更好的对复杂的车内信息数据进行分析处理，监控车内网中与安全紧密相

关的控制系统，识别影响车辆安全的异常情况，以保证车辆安全性能的提高。对于提高汽车安全性能有非常有力的理论指导和实践意义。同时，在避免危害公共交通安全方面具有重要的实用价值，可以应用于实际车辆生产的安全加固。

[0046] 本发明与传统方法不同，结合了多种车内网数据总线实时动态数据与驾驶状态动态数据。

[0047] 针对车内网数据特点，数据处理方法具有其特殊性，最后需要转换为特征矩阵，以输出给后面的模块挖掘空间关系结构特征。

[0048] 引入一种基于胶囊神经网络的特殊处理模型，建立适合车内网环境下数据的处理结构，对特征关系的结构进行高维建模。本发明中，对车内网高维特征数据进行建模，利用胶囊结构的神经网络中动态路由进行检测关联，对入侵数据进行检测，可以提高车辆安全状态的判断率，提高车辆安全性。

附图说明

[0049] 图1是本发明实施例提供的基于胶囊神经网络的车内网入侵检测方法流程图。

[0050] 图2是本发明实施例提供的胶囊神经网络结构图。

具体实施方式

[0051] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0052] 现有技术中，利用现有的Internet或以太网入侵检测方法，对于车辆内部网络适用性较差；某些针对车内网的方法，仅依赖于某一类总线数据，难以对整个车辆内部可能遭受的威胁进行检测；现有方法没有结合车辆自身驾驶状态信息进行分析，降低了误报率；同时，现有方法大都没有考虑不同特征类数据之间的相关性，仅依靠简单的神经网络方法难以对特征关系进行高维建模，降低了方法的准确检测率。

[0053] 为解决上述问题，下面结合附图对本发明作详细描述。

[0054] 如图1所示，本发明实施例提供的基于胶囊神经网络的车内网入侵检测方法结合多种车内网数据总线实时动态数据与驾驶状态动态数据。针对车内网数据特点，数据处理方法具有其特殊性，最后需要转换为特征矩阵，以输出给后面的模块挖掘空间关系结构特征。引入一种基于胶囊神经网络的特殊处理模型，建立适合车内网环境下数据的处理结构，对特征关系的结构进行高维建模。

[0055] 具体包括：

[0056] 第一步，采集两种场景下车内网原始特征数据，并进行预处理：

[0057] 分别在两种场景下采集车内网中CAN总线、MOST总线数据包数据，以及车辆速度、车辆加速度、转向、刹车数据。这两种场景分别是无外网链接的正常驾驶场景与有外网攻击连接的攻击驾驶场景。对采集到的各数据按照一定的时间间隔参数u进行划分，构成总样本集，对两类数据进行胶囊神经网络模型的训练。将该总样本集70％的数据进行模型训练，30％用于模型的效果验证。在进行训练之前，对原始样本数据进行相应的预处理，预处理过程包括：

[0058] (1)对于每一个时间间隔t采集到的CAN总线、MOST总线数据包数据，按照CAN与MOST数据包类型进行包统计概率的特征计算，构成特征向量x1、x2。

[0059] (2)在采集以上CAN与MOST数据包时，按照时间到来的先后顺序，对各类型数据包序列进行记录，构成类型序列原始数据。对CAN、MOST总线数据类型进行one-hot encoding类型编码。由于类型序列数据包数量较多，直接作为特征维度太高，采用1/M作为采样间隔对其进行采样，构成特征序列向量x3、x4。

[0060] (3)对于上述时间间隔t，采用更细微的采样频率n，采集车辆驾驶状态数据进行处理，采集的数据包括车辆速度、车辆加速度、转向角度与加速度、刹车数据。计算这5类数据的20个相关系数作为特征向量x5。计算相关系数算法采用：

[0061] $$r(x,y)=\frac{\sum_{i=1}^{n}x_i y_i - n\overline{X}\,\overline{Y}}{n\sigma_x\sigma_y}$$

[0062] 其中，其中x_i为一种类型驾驶状态数据，y_i为另一种类型数据，$\overline{X}$、$\overline{Y}$分别为两种状态数据的平均值，σ_x、σ_y分别为两种驾驶状态数据的标准差。

[0063] (4)对以上的特征向量x1～x5进行特征矩阵标准化处理。假设x3向量中有CAN的n1数据包，one-hot encoding编码长度为len1，x4向量中有MOST的n2数据包，one-hot encoding编码长度为len2，则取特征矩阵的列数：

[0064] $$col=\max(len1,len2)*\max(\sqrt{n1},\sqrt{n2})$$

[0065] 在标准化x3、x4向量时，按照二维矩阵空间位置进行处理。有剩余无法放置某一个类型数据的地方补0，col的是指可以尽量保证补0的数据尽可能少。在设置完如上的信息后，对x1、x2、x5进行处理，分别放置在标准矩阵后面行的位置，构成整个特征矩阵数据。

[0066] 第二步，对参考模型参数进行计算：

[0067] 本发明中应用到了胶囊神经网络结构如图2所示，整个模型参数计算结构主要分为卷积层、一级胶囊层、次胶囊层。特征矩阵的维度为row*col。

[0068] 卷积层：经过预处理后，特征矩阵通过卷积核运算得到卷积层，卷积层检测特征矩阵的基本特征。在本发明中，卷积层有64个步长为1的卷积核，使用ReLU方法激活。

[0069] 一级胶囊层：这级胶囊层一共8个主胶囊，接受卷积层检测到的基本特征，生成特征的组合。卷积层得到的每8个卷积结果运算得到一个主胶囊模块。

[0070] 次级胶囊层：这一层包含2个数字胶囊，每个胶囊对应判断是否存在入侵检测状态的结果，每个数字胶囊的维度为50。一级胶囊层和次级胶囊层通过动态路由算法进行计算得到。

[0071] 以上一级胶囊层传递给次级胶囊层的运算中，运用到的主要计算环节函数有：

[0072] $$\hat{\mathbf{u}}_{j|i}=\mathbf{W}_{ij}\mathbf{u}_i;$$

[0073] $$\mathbf{s}_j=\sum_i c_{ij}\hat{\mathbf{u}}_{j|i};$$

[0074] $$\mathbf{v}_j = \frac{\|\mathbf{s}_j\|^2}{1+\|\mathbf{s}_j\|^2}\frac{\mathbf{s}_j}{\|\mathbf{s}_j\|};$$

[0075] 其中，$\hat{\mathbf{u}}_{j|i}$表示了胶囊之间的仿射运算、s_j表示输入向量的标量加权运算，以及v_j表示squash压缩函数。这里的c_{ij}通过囊间路由算法迭代得到，计算方法采用softmax函数，即：

[0076] $$c_{ij}=\frac{\exp(b_{ij})}{\sum_k \exp(b_{ik})};$$

[0077] 其中，b_{ij}在迭代过程中初始化为0，然后通过囊间路由算法计算。最后通过次级胶囊计算$||v_j||$得到属于是否入侵判断的概率。在训练阶段，采用如下方法对损失进行计算：

[0078] $L_c=T_c\ \max(0,m^+-||v_c||)^2+\lambda(1-T_c)\max(0,||v_c||-m^-)$；

[0079] 通过如上的胶囊神经网络对70％样本数据进行训练，并通过剩余的30％样本数据进行测试，如果验证数据分析准确率较低，则随机打乱样本数据重新进行试验，直到取得数据较高检测率。

[0080] 当车辆启动驾驶时，实时采集前面叙述的车内网内部和相关状态数据，对其进行相同的预处理。将该数据作为胶囊神经网络的输入，实时计算检测车辆驾驶安全状态，得到实时判断输出，当输出判定为攻击行为的存在时，上报给系统。

[0081] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

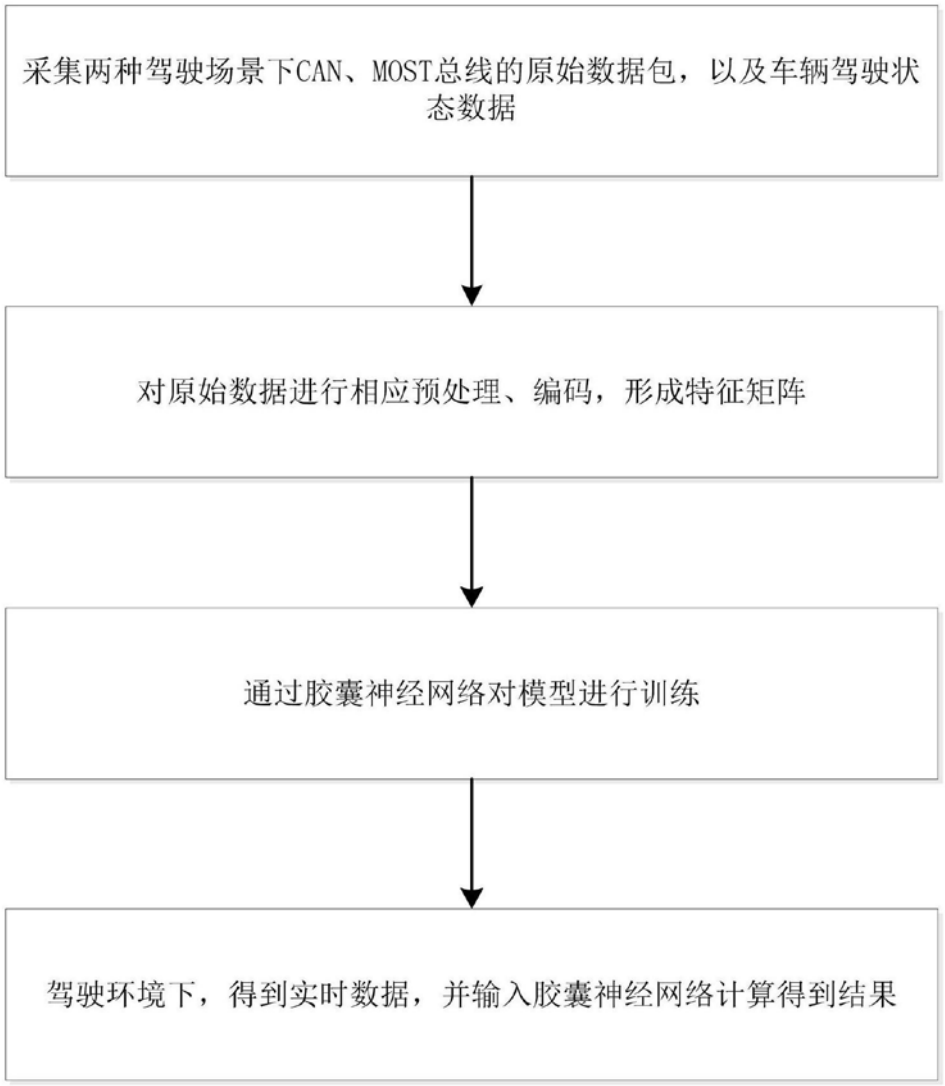

采集两种驾驶场景下CAN、MOST总线的原始数据包，以及车辆驾驶状态数据
对原始数据进行相应预处理、编码，形成特征矩阵
通过胶囊神经网络对模型进行训练
驾驶环境下，得到实时数据，并输入胶囊神经网络计算得到结果

图1

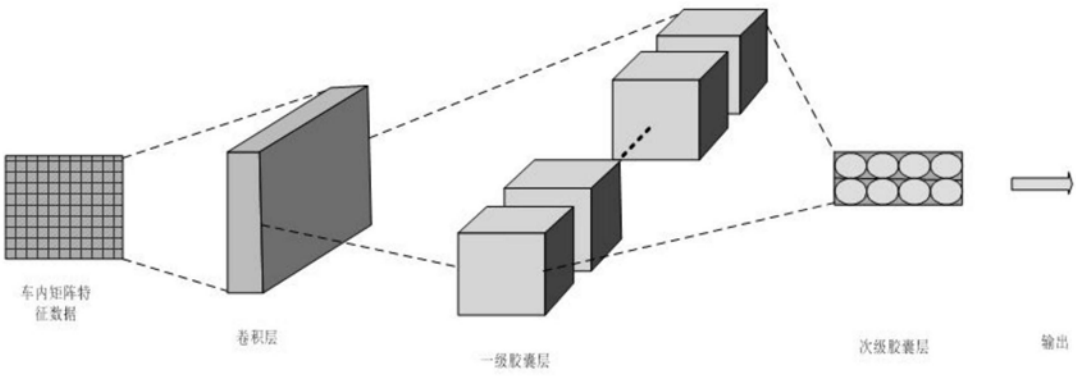

车内矩阵特征数据
卷积层
一级胶囊层
次级胶囊层
输出

图2