(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 112887302 A
(43)申请公布日 2021.06.01

(21)申请号 202110091222.9

(22)申请日 2021.01.22

(71)申请人 中汽创智科技有限公司
地址 211100 江苏省南京市江宁区秣陵街道胜利路88号(江宁开发区)

(72)发明人 李丰军 周剑光

(74)专利代理机构 南京泰普专利代理事务所(普通合伙) 32360
代理人 张磊

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/24(2006.01)
G06N 3/04(2006.01)
G06N 3/08(2006.01)

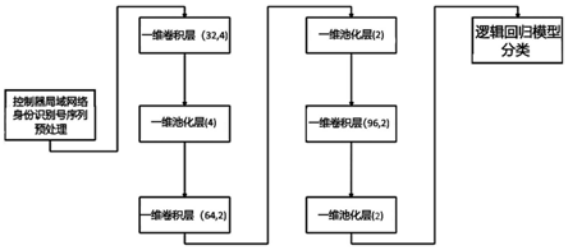
权利要求书1页 说明书5页 附图1页

(54)发明名称

汽车控制器局域网络总线入侵检测方法和系统

(57)摘要

本发明公开了汽车控制器局域网络总线入侵检测方法和系统,所述方法包括:处理预先数据;根据所述处理预先数据,将控制器局域网络总线消息帧身份证标识号序列,进行字符级别的独热编码;根据所述数据预处理得到独热编码进行特征提取;将编码完成的数据送入卷积神经网络,进行特征提取;根据数据预测和卷积神经网络通过全连接结构和逻辑回归模型激活函数构造分类器;进一步把数据库中的数据纪录映射到给定类别中;本发明提出卷积神经网络检测模型作为控制器局域网络总线入侵检测的引擎,对控制器局域网络总线数据进行字符级别的独热编码预处理,降低维度。



CN 112887302 A

1.一种汽车控制器局域网络总线入侵检测方法,包括:

处理预先数据;根据所述处理预先数据,将控制器局域网络总线消息帧身份证标识号序列,进行字符级别的独热编码;

根据所述处理预先数据得到独热编码进行特征提取;

将编码完成的数据送入卷积神经网络,进行特征提取;

根据所述处理预先数据和所述卷积神经网络通过全连接结构和逻辑回归模型激活函数构造分类器;进一步把数据库中的数据纪录映射到给定类别中。

2.根据权利要求1所述的 一种汽车控制器局域网络总线入侵检测方法,其特征在于,所述网络由三个隐藏层组成;每个隐藏层包含至少一个卷积层和至少一个池层;每个隐藏层的卷积核数是不同的,将原始特征映射到高维空间,从而提高了学习特征的能力。

3.根据权利要求1所述的一种汽车控制器局域网络总线入侵检测方法,其特征在于,所述消息帧包括身份证标识号段,控制段和数据段。

4.根据权利要求3所述的一种汽车控制器局域网络总线入侵检测方法,其特征在于,首先对所述身份证标识号段进行预处理由于收集的身份证标识号段的数据是十六进制的,对每一位进行独热编码,从原始的身份证标识号数据序列得到编码过后的身份证标识号序列;每一个所述身份证标识号,用至少三个独热编码向量来表示。

5.一种汽车控制器局域网络总线入侵检测系统,其特征在于,所述系统包括:

处理模块,用于数据预处理;将控制器局域网络总线消息帧身份证标识号序列,进行字符级别的独热编码;

特征提取模块,用于根据所述处理模块得到独热编码进行特征提取;将编码完成的数据送入卷积神经网络,进行特征提取;

分类器,通过全连接结构和逻辑回归模型激活函数构造,进而对处理模块和特征提取模块进行数据预测,把数据库中的数据纪录映射到给定类别中。

6.一种汽车控制器局域网络总线入侵检测设备,其特征在于,所述设备模拟被入侵的电脑控制模组节点,控制器局域网络客户端模拟车载控制器局域网络总线的网络环境,所述节点设置至少3个攻击场景;所述场景如下:

攻击场景一,拒绝服务攻击,通过发送大量的高优先级的报文,高频率的向总线发送0x00 的消息帧,破坏车载总线系统的响应;

攻击场景二,模糊攻击;通过发送大量随机身份证标识号的消息帧,以试探控制器局域网络总线的响应,来探测汽车电脑控制模组的信息;

攻击场景三,重放攻击;通过发送特定的正常报文。

7.根据权利要求6所述的一种汽车控制器局域网络总线入侵检测设备,其特征在于,所述设备还包括:

处理器以及存储有计算机程序指令的存储器;

所述处理器读取并执行所述计算机程序指令,以实现如权利要求1-4任意一项所述的一种汽车控制器局域网络总线入侵检测方法。

8.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质上存储有计算机;

程序指令,所述计算机程序指令被处理器执行时实现如权利要求1-4任意一项所述的一种汽车控制器局域网络总线入侵检测方法。

汽车控制器局域网络总线入侵检测方法和系统

技术领域

[0001] 本发明涉及一种网络安全、软件技术，尤其是汽车控制器局域网络总线入侵检测方法和系统。

背景技术

[0002] 目前，控制器局域网络总线的安全方案分为三个方向：基于密码学的消息身份验证、基于物理特征的消息身份验证和控制器局域网络总线的异常检测；控制器局域网络总线异常检测通过利用通信网络和数据的特性或者通过使用大数据分析和机器学习监控和探测控制器局域网络总线上的网络异常来探测攻击。

[0003] 当前针对控制器局域网络总线的入侵检测已经有一些传统的机器学习方法得到应用；例如，基于决策树的控制器局域网络总线异常检测方法以及使用支持向量机对控制器局域网络总线消息进行异常检测等，近年来，深度学习模型由于有良好的提取复杂特征的能力被应用于入侵检测中，但还缺少针对控制器局域网络总线入侵检测的神经网络模型。

[0004] 控制器局域网络总线网络是现在应用最广泛的车载控制网络，它连接了大多数车的控制单元使得它成为汽车网络入侵的最终目标；一旦黑客成功入侵了汽车的控制器局域网络网络，他可以轻易的干扰甚至控制汽车；当前针对控制器局域网络总线的入侵检测主要方法都存在一定的缺陷。

发明内容

[0005] 本发明实施例提供了一种汽车控制器局域网络总线入侵检测方法，通过对控制器局域网络总线数据进行字符级别的独热编码预处理，以降低维度。

[0006] 第一方面，提供一种汽车控制器局域网络总线入侵检测方法，包括；

处理预先数据；

根据所述处理预先数据，将控制器局域网络总线消息帧身份证标识号序列，进行字符级别的独热编码；

根据所述处理预先数据得到独热编码进行特征提取；

将编码完成的数据送入卷积神经网络，进行特征提取；

在此采用的是一维卷积神经网络，相较于二维卷积结构，在更少的参数下提取序列时间维度的特征；

根据所述处理预先数据和所述卷积神经网络通过全连接结构和逻辑回归模型激活函数构造分类器；进一步把数据库中的数据纪录映射到给定类别中。

[0007] 在第一方面的一些可实现方式中，所述网络由三个隐藏层组成；每个隐藏层包含至少一个卷积层和至少一个池层；每个隐藏层的卷积核数是不同的，将原始特征映射到高维空间，从而提高了学习特征的能力。

[0008] 在第一方面的一些可实现方式中，所述消息帧包括身份证标识号段，控制段和数

据段;在处理控制器局域网络数据过程中,使用身份证标识号段作为入侵检测的原始数据,这样做可以有效减少编码时间,适合实时检测。

[0009] 在第一方面的一些可实现方式中,首先对所述身份证标识号段进行预处理由于收集的身份证标识号段的数据是十六进制的,对每一位进行独热编码,从原始的身份证标识号数据序列得到编码过后的身份证标识号序列;每一个所述身份证标识号,用至少三个独热编码向量来表示,而非采用每一个身份证标识号用一个独热编码表示。

[0010] 第二方面,提供了一种汽车控制器局域网络总线入侵检测系统,包括:

处理模块,用于数据预处理;将控制器局域网络总线消息帧身份证标识号序列,进行字符级别的独热编码;

特征提取模块,用于根据所述处理模块得到独热编码进行特征提取;将编码完成的数据送入卷积神经网络,进行特征提取;

分类器,通过全连接结构和逻辑回归模型激活函数构造,进而对处理模块和特征提取模块进行数据预测,把数据库中的数据纪录映射到给定类别中。

[0011] 第三方面,提供了一种汽车控制器局域网络总线入侵检测设备,所述设备模拟被入侵的电脑控制模组节点,控制器局域网络客户端模拟车载控制器局域网络总线的网络环境,所述节点设置至少3个攻击场景;所述场景如下:

攻击场景一,拒绝服务攻击,通过发送大量的高优先级的报文,高频率的向总线发送0x00 的消息帧,破坏车载总线系统的响应;

攻击场景二,模糊攻击;通过发送大量随机身份证标识号的消息帧,以试探控制器局域网络总线的响应,来探测汽车电脑控制模组的信息;

攻击场景三,重放攻击;通过发送特定的正常报文,如:控制每分钟转数转速表的消息,干扰汽车系统。

[0012] 在第三方面的一些可实现方式中,所述设备还包括:

处理器以及存储有计算机程序指令的存储器;

所述处理器读取并执行所述计算机程序指令,以实现上述第一方面所述的一种汽车控制器局域网络总线入侵检测方法。

[0013] 第四方面,提供了一种计算机可读存储介质,所述计算机可读存储介质上存储有计算机;

程序指令,所述计算机程序指令被处理器执行时实现上述第一方面所述的一种汽车控制器局域网络总线入侵检测方法。

[0014] 有益效果:本发明设计汽车控制器局域网络总线入侵检测方法和系统,本发明提出卷积神经网络检测模型作为控制器局域网络总线入侵检测的引擎,并且对控制器局域网络总线数据进行字符级别的独热编码预处理,以降低维度,作为入侵检测模型的输入,可以有效识别控制器局域网络总线三种不同类别攻击,包括拒绝服务攻击,模糊攻击,重放攻击;汽车控制器局域网络总线入侵检测系统,采用一维卷积神经网络结构;一维卷积结构,在时间维度上进行卷积运算,相较于二维卷积结构,节省很多参数,适用于快速检测,一维卷积可以应用于时间序列分析,同样也可以用于分析具有固定长度周期的信号数据。

附图说明

[0015] 图1是本发明的汽车控制器局域网络总线入侵检测系统神经网络结构图。

[0016] 图2是本发明的控制器局域网络总线消息帧示意图。

[0017] 图3是本发明的0x123为例的消息帧身份证标识号编码示意图。

具体实施方式

[0018] 在该实施例中，一种 汽车控制器局域网络总线入侵检测方法和系统，通过对控制器局域网络总线数据进行字符级别的独热编码预处理，以降低维度；下面通过实施例，并结合附图对本方案做进一步具体说明。

[0019] 目前，控制器局域网络总线的安全方案分为三个方向：基于密码学的消息身份验证、基于物理特征的消息身份验证和控制器局域网络总线的异常检测；控制器局域网络总线异常检测通过利用通信网络和数据的特性或者通过使用大数据分析和机器学习监控和探测控制器局域网络总线上的网络异常来探测攻击。

[0020] 当前针对控制器局域网络总线的入侵检测已经有一些传统的机器学习方法得到应用；例如，基于决策树的控制器局域网络总线异常检测方法以及使用支持向量机对控制器局域网络总线消息进行异常检测等，近年来，深度学习模型由于有良好的提取复杂特征的能力被应用于入侵检测中，但还缺少针对控制器局域网络总线入侵检测的神经网络模型。

[0021] 卷积神经网络被广泛应用于图像与视频等领域，由于其有参数共享和局部感知等特点，可降低网络复杂度，并且对数据平移，缩放等变换具有高度的不变形的良好特性，成为一种常见的神经网络结构。

[0022] 综上，在本申请中，申请人认为现有技术中至少存在以下缺点：控制器局域网络总线网络是现在应用最广泛的车载控制网络，它连接了大多数车的控制单元使得它成为汽车网络入侵的最终目标；一旦黑客成功入侵了汽车的控制器局域网络网络，他可以轻易的干扰甚至控制汽车；当前针对控制器局域网络总线的入侵检测主要方法都存在一定的缺陷。

[0023] 为解决现有技术中存在的缺点，本发明实施例提供了 汽车控制器局域网络总线入侵检测方法和系统，下面结合附图对本发明实施例的技术方案进行描述。

[0024] 实施例一、

根据实施例一提出一种汽车控制器局域网络总线入侵检测方法，所述方法包括；

处理预先数据；

根据所述处理预先数据，将控制器局域网络总线消息帧身份证标识号序列，进行字符级别的独热编码；

根据所述处理预先数据得到独热编码进行特征提取；

将编码完成的数据送入卷积神经网络，进行特征提取；

在此采用的是一维卷积神经网络，相较于二维卷积结构，在更少的参数下提取序列时间维度的特征；

根据所述处理预先数据和所述卷积神经网络通过全连接结构和逻辑回归模型激活函数构造分类器；进一步把数据库中的数据纪录映射到给定类别中。

[0025] 实施例二、

在实施例一的基础之上，所述网络由三个隐藏层组成；每个隐藏层包含至少一个卷积层和至少一个池层；每个隐藏层的卷积核数是不同的，将原始特征映射到高维空间，从而提高了学习特征的能力。

[0026] 实施例三、

在实施例一的基础之上，如图2所示，所述消息帧包括身份证标识号段，控制段和数据段；在处理控制器局域网络数据过程中，使用身份证标识号段作为入侵检测的原始数据，这样做可以有效减少编码时间，适合实时检测。

[0027] 实施例四、

在实施例三的基础之上，如图3所示，首先对所述身份证标识号段进行预处理，由于收集的身份证标识号段的数据是十六进制的，对每一位进行独热编码，从原始的身份证标识号数据序列得到编码过后的身份证标识号序列；每一个所述身份证标识号，用至少三个独热编码向量来表示，而非采用每一个身份证标识号用一个独热编码表示；减少编码后的空间。

实施例五、

根据实施例五提出一种汽车控制器局域网络总线入侵检测系统，所述系统包括：

处理模块，用于数据预处理；将控制器局域网络总线消息帧身份证标识号序列，进行字符级别的独热编码；

特征提取模块，用于根据所述处理模块得到独热编码进行特征提取；将编码完成的数据送入卷积神经网络，进行特征提取；

分类器，通过全连接结构和逻辑回归模型激活函数构造，进而对处理模块和特征提取模块进行数据预测，把数据库中的数据纪录映射到给定类别中。

[0028] 实施例六、

根据实施例六提出一种汽车控制器局域网络总线入侵检测设备，所述设备模拟被入侵的电脑控制模组节点，控制器局域网络客户端模拟车载控制器局域网络总线的网络环境，所述节点设置至少3个攻击场景；所述场景如下：

攻击场景一，拒绝服务攻击，通过发送大量的高优先级的报文，高频率的向总线发送0x00 的消息帧，破坏车载总线系统的响应；

攻击场景二，模糊攻击；通过发送大量随机身份证标识号的消息帧，以试探控制器局域网络总线的响应，来探测汽车电脑控制模组的信息；

攻击场景三，重放攻击；通过发送特定的正常报文，如：控制每分钟转数转速表的消息，干扰汽车系统。

[0029] 实施例七、

在实施例六的基础之上得出场景中收集控制器局域网络总线消息帧序列，训练入侵检测模型。

[0030] 实施例八、

在实施例六的基础之上，所述设备还包括：

处理器以及存储有计算机程序指令的存储器；

所述处理器读取并执行所述计算机程序指令，以实现上述实施例一所述的一种汽车控制器局域网络总线入侵检测方法。

[0031] 实施例九、

根据实施例九提出一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机；

程序指令，所述计算机程序指令被处理器执行时实现上述实施例一所述的一种汽车控制器局域网络总线入侵检测方法。

[0032] 实施例十、

根据实施例十得出，如图1所示，一维卷积层(32,4)表示卷积核的个数为64，卷积核的大小为4；一维池化层(4)，下采样的方式为取特征最大值，下采样的尺寸为4；值最后用逻辑回归模型分类函数作为分类器，以确定控制器局域网络 身份证标识号数据序列，是否含有入侵行为；

其中，一维卷积层(64,2)表示一维卷积层，卷积核的个数为128，卷积核的大小为2；一维池化层(2)表示一维池化层，下采样的方式为取特征最大值，下采样的尺寸为2；一维卷积层(96,2) 表示一维卷积层，卷积核的个数为192，卷积核的大小为2。

[0033] 还需要说明的是，本发明中提及的示例性实施例，基于一系列的步骤或者装置描述一些方法或系统。但是，本发明不局限于，上述步骤的顺序，也就是说，可以按照实施例中提及的顺序执行步骤，也可以不同于实施例中的顺序，或者若干步骤同时执行。

[0034] 以上，仅为本发明的具体实施方式，所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、模块和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。应理解，本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本发明的保护范围之内。

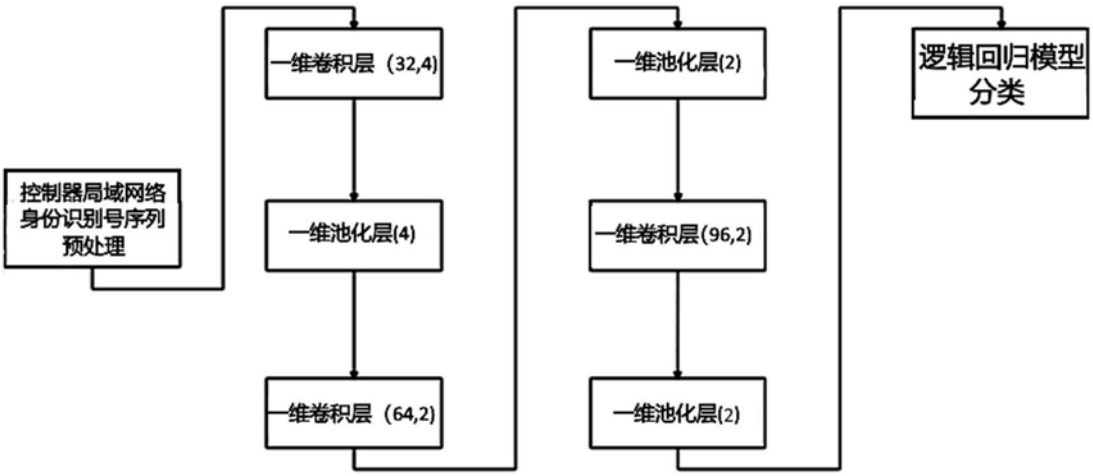

控制器局域网络身份识别号序列预处理
一维卷积层（32,4)
一维池化层(4)
一维卷积层（64,2)
一维池化层(2)
一维卷积层(96,2)
一维池化层(2)
逻辑回归模型分类

图1

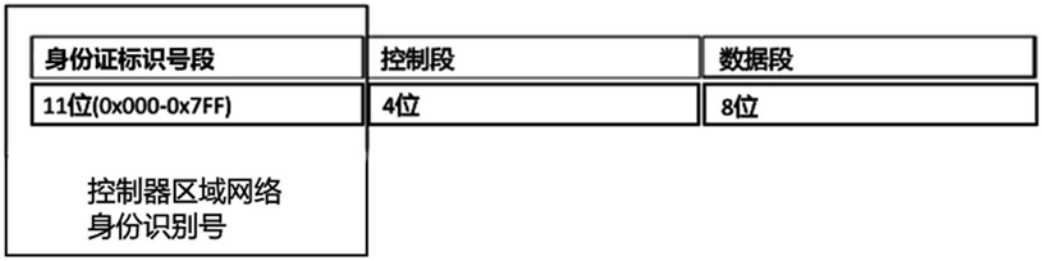

身份证标识号段
控制段
数据段
11位(0x000-0x7FF)
4位
8位
控制器区域网络身份识别号

图2

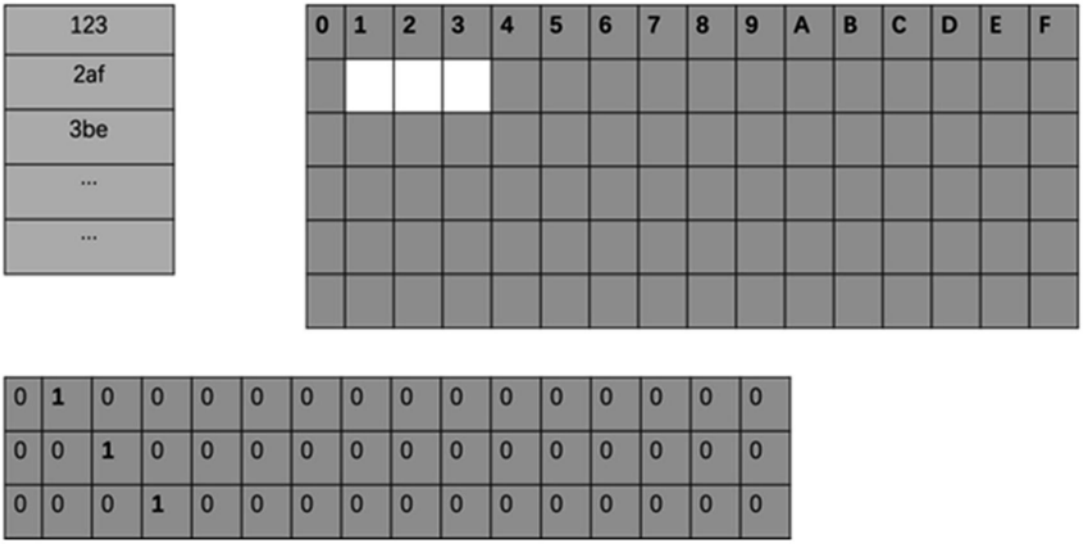

123
2af
3be
...
...
0 1 2 3 4 5 6 7 8 9 A B C D E F
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0

图3