(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 109040019 A
(43)申请公布日 2018.12.18

(21)申请号 201810671805.7

(22)申请日 2018.06.26

(71)申请人 深圳大学
地址 518060 广东省深圳市南山区南海大道3688号

(72)发明人 梁俊威 陈剑勇

(74)专利代理机构 深圳青年人专利商标代理有限公司 44350
代理人 吴桂华

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 4/02(2018.01)
H04W 4/44(2018.01)

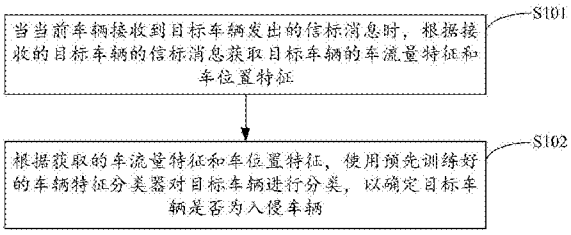
权利要求书2页 说明书6页 附图2页

(54)发明名称

基于车联网的入侵检测方法、装置、终端及存储介质

(57)摘要

本发明适用车联网技术领域，提供了一种基于车联网的入侵检测方法、装置、终端及存储介质，该方法包括：在当前车辆接收到目标车辆发出的信标消息后，根据信标消息获取目标车辆的车流量特征和车位置特征，再根据获取的车流量特征和车位置特征，使用预先训练好的车辆特征分类器对目标车辆进行分类，以确定目标车辆是否为入侵车辆，从而通过目标车辆车的流量特征和车位置特征两个维度来判定目标车辆是否为入侵车辆，进而提高了对入侵车辆检测的效率和准确性。



CN 109040019 A

1.一种基于车联网的入侵检测方法，其特征在于，所述方法包括下述步骤：

当当前车辆接收到目标车辆发出的信标消息时，根据接收的所述目标车辆的信标消息获取所述目标车辆的车流量特征和车位置特征；

根据获取的所述车流量特征和车位置特征，使用预先训练好的车辆特征分类器对所述目标车辆进行分类，以确定所述目标车辆是否为入侵车辆。

2.如权利要求1所述的方法，其特征在于，根据接收的所述目标车辆的信标消息中获取所述目标车辆的车流量特征和车位置特征的步骤，包括：

从所述目标车辆的信标消息中获取所述目标车辆的平均车流量；

根据所述当前车辆的平均车流量、所述目标车辆的平均车流量以及车流量特征公式获取所述目标车辆的车流量特征。

3.如权利要求1所述的方法，其特征在于，根据接收的所述目标车辆的信标消息中获取所述目标车辆的车流量特征和车位置特征的步骤，还包括：

向所述当前车辆的邻居车辆广播请求消息，以得到所述邻居车辆的响应消息；

根据所述邻居车辆的响应消息分别得到当前时刻所述邻居车辆到所述目标车辆的声明距离与当前时刻所述邻居车辆到所述目标车辆的测量距离，获取当前时刻所述邻居车辆和所述目标车辆的第一距离偏差；

根据所述目标车辆的信标消息分别得到当前时刻所述当前车辆到所述目标车辆的声明距离与当前时刻所述当前车辆到所述目标车辆的测量距离，获取当前时刻所述当前车辆和所述目标车辆的第二距离偏差；

根据所述第一距离偏差、所述第二距离偏差以及车位置特征公式获取所述目标车辆的位置特征。

4.如权利要求3所述的方法，其特征在于，获取所述第一距离偏差和所述第二距离偏差的步骤之后，根据所述第一距离偏差、所述第二距离偏差以及车位置特征公式获取所述目标车辆的位置特征的步骤之前，所述方法还包括：

根据所述第一距离偏差和所述第二距离偏差对所述邻居车辆的响应消息进行过滤。

5.如权利要求1所述的方法，其特征在于，根据获取的所述车流量特征和车位置特征，使用预先训练好的车辆特征分类器对所述目标车辆进行分类的步骤，包括：

当所述车流量特征在预设流量偏差范围内、且所述车位置特征在预设位置偏差范围内时，判定所述目标车辆为非入侵车辆，将所述目标车辆分入所述当前车辆的白名单列表，否则，判定所述目标车辆为入侵车辆，将所述目标车辆分入所述当前车辆的黑名单列表。

6.一种基于车联网的入侵检测装置，其特征在于，所述装置包括：

特征获取单元，用于当当前车辆接收到目标车辆发出的信标消息时，根据接收的所述目标车辆的信标消息获取所述目标车辆的车流量特征和车位置特征；以及

车辆分类单元，用于根据获取的所述车流量特征和车位置特征，使用预先训练好的车辆特征分类器对所述目标车辆进行分类，以确定所述目标车辆是否为入侵车辆。

7.如权利要求6所述的装置，其特征在于，所述特征获取单元包括：

车流量获取单元，用于从所述目标车辆的信标消息中获取所述目标车辆的平均车流量；以及

流量特征获取单元，用于根据所述当前车辆的平均车流量、所述目标车辆的平均车流

量以及车流量特征公式获取所述目标车辆的车流量特征。

8.如权利要求6所述的装置，其特征在于，所述特征获取单元还包括：

请求消息广播单元，用于向当前车辆的邻居车辆广播请求消息，以得到所述邻居车辆的响应消息；

第一偏差获取单元，用于根据所述邻居车辆的响应消息分别得到当前时刻所述邻居车辆到所述目标车辆的声明距离与当前时刻所述邻居车辆到所述目标车辆的测量距离，获取当前时刻所述邻居车辆和所述目标车辆的第一距离偏差；

第二偏差获取单元，用于根据所述目标车辆的信标消息分别得到当前时刻所述当前车辆到所述目标车辆的声明距离与当前时刻所述当前车辆到所述目标车辆的测量距离，获取当前时刻所述当前车辆和所述目标车辆的第二距离偏差；以及

位置特征获取单元，用于根据所述第一距离偏差、所述第二距离偏差以及车位置特征公式获取所述目标车辆的位置特征。

9.一种车载终端，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求1至5项所述方法的步骤。

10.一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至5项所述方法的步骤。

基于车联网的入侵检测方法、装置、终端及存储介质

技术领域

[0001] 本发明属于车联网技术领域，尤其涉及一种基于车联网的入侵检测方法、装置、终端及存储介质。

背景技术

[0002] 车联网(Vehicle Ad Hoc Network,VANET)通过DSRC(Dedicated Short Range Communications,专用短程通信技术)实现了移动车辆之间的无线通信，其中包含了车辆与车辆之间的通信(Vehicle-to-Vehicle,V2V)和车辆基础设施的通信(Vehicle-to-Infrastructure,V2I)。VANET的应用使车辆行驶安全系数得到明显的提升，特别是在极端行驶条件中的车辆行驶安全系数，例如，车辆在大雾、暴雨或其他恶劣环境中行驶时，可通过VANET反馈周围车辆的信息，让驾驶者在危险来临之前，有更充分的时间排除危险。除此之外，VANET还能够连接互联网，为用户带来各种娱乐功能。VANET不仅能够提升人们的生活质量，还保障了车辆行驶安全，因此为了车辆行驶安全，VANET的安全问题就成了人们需要解决的首要问题。VANET被入侵车辆入侵的方式一般分为内部攻击和外部攻击，例如，女巫攻击(Sybil Attack)和假消息攻击等，其中，有入侵行为(异常行为)的车辆称为入侵车辆。

[0003] 入侵检测系统(Intrusion Detection System,IDS)是现有的VANET使用最广泛的检测系统，通过分析VANET中车辆的消息并对这些消息进行分类，从而有效地检测VANET内部和外部的攻击。然而，现有的IDS没有任何公认的数据库可用，这意味着现有的IDS只能凭借局部监视的数据进行工作，而且现有的IDS验证和响应速度不能满足VANET这样的高动态网络，无法快速准确地检测出入侵车辆发出的异常消息。

发明内容

[0004] 本发明的目的在于提供一种基于车联网的入侵检测方法、装置、终端以及存储介质，旨在解决由于现有技术无法提供一种有效的入侵检测方法，导致对收到的其他车辆消息的异常判断效率较低的问题。

[0005] 一方面，本发明提供了一种基于车联网的入侵检测方法，所述方法包括下述步骤：

[0006] 当当前车辆接收到目标车辆发出的信标消息时，根据接收的所述目标车辆的信标消息获取所述目标车辆的车流量特征和车位置特征；

[0007] 根据获取的所述车流量特征和车位置特征，使用预先训练好的车辆特征分类器对所述目标车辆进行分类，以确定所述目标车辆是否为入侵车辆。

[0008] 另一方面，本发明提供了一种基于车联网的入侵检测装置，所述装置包括：

[0009] 特征获取单元，用于当当前车辆接收到目标车辆发出的信标消息时，根据接收的所述目标车辆的信标消息获取所述目标车辆的车流量特征和车位置特征；以及

[0010] 车辆分类单元，用于根据获取的所述车流量特征和车位置特征，使用预先训练好的车辆特征分类器对所述目标车辆进行分类，以确定所述目标车辆是否为入侵车辆。

[0011] 另一方面，本发明还提供了一种车载终端，包括存储器、处理器以及存储在所述存

储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如上述基于车联网的入侵检测方法的步骤。

[0012] 另一方面，本发明还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存储有计算机程序，所述计算机程序被处理器执行时实现如上述基于车联网的入侵检测方法的步骤。

[0013] 本发明在当前车辆接收到目标车辆发出的信标消息后，根据信标消息获取目标车辆的车流量特征和车位置特征，再根据获取的车流量特征和车位置特征，使用预先训练好的车辆特征分类器对目标车辆进行分类，以确定目标车辆是否为入侵车辆，从而通过目标车辆车的流量特征和车位置特征两个维度来判定目标车辆是否为入侵车辆，进而提高了对入侵车辆检测的效率和准确性。

附图说明

[0014] 图1是本发明实施例一提供的基于车联网的入侵检测方法的实现流程图；

[0015] 图2是本发明实施例二提供的基于车联网的入侵检测装置的结构示意图；

[0016] 图3是本发明实施例二提供的特征获取单元的优选结构示意图；以及

[0017] 图4是本发明实施例四提供的一种车载终端的结构示意图。

具体实施方式

[0018] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，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。

[0019] 以下结合具体实施例对本发明的具体实现进行详细描述：

[0020] 实施例一：

[0021] 图1示出了本发明实施例一提供的基于车联网的入侵检测方法的实现流程，为了便于说明，仅示出了与本发明实施例相关的部分，详述如下：

[0022] 在步骤S101中，当当前车辆接收到目标车辆发出的信标消息时，根据接收的目标车辆的信标消息获取目标车辆的车流量特征和车位置特征。

[0023] 本发明实施例适用于车联网中的入侵检测系统或入侵检测平台。在本发明实施例中，将被检测是否为入侵车辆的车辆称为目标车辆，将检测目标车辆是否为入侵车辆的车辆称为当前车辆，在当前车辆检测范围内的车辆称为邻居车辆，即目标车辆是邻居车辆中正在被车辆检测的车辆，信标消息包括车辆ID(Identification，身份标识号)、车辆的平均车流量、车辆位置的X坐标和车辆位置的Y坐标。

[0024] 优选地，在获取目标车辆的车流量特征时，从目标车辆的信标消息中获取目标车辆的平均车流量，根据当前车辆的平均车流量、目标车辆的平均车流量以及车流量特征公式获取目标车辆的车流量特征，车流量特征公式为$FlowR=|AvgFlow_{own}-AvgFlow_{tag}|$，其中，FlowR为目标车辆的车流量特征，$AvgFlow_{own}$为当前车辆的平均车流量，$AvgFlow_{tag}$为目标车辆的平均车流量，从而便于后续过程中分类器根据目标车辆的车流量特征快速地判定目标车辆是否为入侵车辆。

[0025] 在本发明实施例中，车辆在向邻居车辆发送信标信息之前，需计算自身周围的平

均车流量，优选地，通过公式Flow＝AvgSpeed×CalDensity和 $AvgSpeed = MaxSpeed - \frac{CalDensity}{MaxDensity} MaxSpeed$ 获取车辆的车流量，通过公式 $AvgFlow = \frac{1}{n}(\sum_{i=1}^{n-1} AvgFlow' + Flow)$ 计算出车辆的平均车流量，从而提高了信标消息中平均车流量的精确度，其中，Flow为车流量AvgSpeed为车辆的平均速度，MaxSpeed为车辆当前路段的最高车速，CalDensity为周围车辆密度，CalDensity可根据车辆的白名单列表中的邻居数量获取，MaxDensity为当前路段的拥塞密度(路段最为拥塞时的车辆密度)。

[0026] 优选地，在获取目标车辆的车位置特征时，向当前车辆的邻居车辆广播请求消息，以得到邻居车辆的响应消息，根据邻居车辆的响应消息分别得到当前时刻邻居车辆到目标车辆的声明距离与当前时刻邻居车辆到目标车辆的测量距离，获取当前时刻邻居车辆和目标车辆的第一距离偏差，根据目标车辆的信标消息分别得到当前时刻当前车辆到目标车辆的声明距离与当前时刻当前车辆到目标车辆的测量距离，获取当前时刻当前车辆和目标车辆的第二距离偏差，再根据第一距离偏差、第二距离偏差以及车位置特征公式获取目标车辆的位置特征，从而便于后续过程中分类器根据目标车辆的车位置特征快速地判定目标车辆是否为入侵车辆，其中，距离偏差为两车辆的声明距离与该两车辆的测量距离差值的绝对值，声明距离为两车辆的坐标距离，测量距离为车辆通过测量信号强弱而得到的距离，请求消息包括请求车辆(当前车辆)ID和目标车辆ID，响应消息包括邻居车辆ID、目标车辆ID、邻居车辆位置的X坐标、邻居车辆位置的Y坐标和测量距离(邻居车辆与目标车辆之间的距离)。

[0027] 具体地，通过公式 $Bias_{o\&t} = \left| D_{o\&t} - \sqrt{(Xpos_{own} - Xpos_{tag})^2 + (Ypos_{own} - Ypos_{tag})^2} \right|$ 获取第二距离偏差，通过公式 $Bias_{n\&t} = \left| D_{n\&t} - \sqrt{(Xpos_{neg} - Xpos_{tag})^2 + (Ypos_{neg} - Ypos_{tag})^2} \right|$ 获取第一距离偏差，通过公式 $PositionR = \frac{1}{n}(\sum Bias_{n\&t} + Bias_{o\&t})$ 获取目标车辆的位置特征，其中，$D_{o\&t}$为当前车辆与目标车辆的测量距离，$D_{n\&t}$为邻居车辆与目标车辆的测量距离，$(Xpos_{own}, Ypos_{own})$为当前车辆的坐标，$(Xpos_{tag}, Ypos_{tag})$为目标车辆的坐标，$(Xpos_{neg}, Ypos_{neg})$为邻居车辆的坐标，$Bias_{n\&t}$为第一距离偏差，$Bias_{o\&t}$为第二距离偏差，PositionR为目标车辆的位置特征，n为邻居车辆数量。

[0028] 进一步优选地，获取第一距离偏差和第二距离偏差的步骤之后，根据第一距离偏差、第二距离偏差以及车位置特征公式获取目标车辆的位置特征的步骤之前，根据第一距离偏差和第二距离偏差对邻居车辆的响应消息进行过滤，从而排除了入侵车辆数据对检测见过的干扰。具体地，当$|Bias_{o\&t} - Bias_{n\&t}| \geq MaxGap$时，对应的邻居消息将被过滤，MaxGap为偏差最大值，可在训练车辆特征分类器时得到。

[0029] 进一步优选地，在向当前车辆的邻居车辆广播请求消息的步骤之前，判断目标车辆是否在当前车辆的白名单列表中，当目标车辆不在当前车辆的白名单列表中时，跳转至向当前车辆的邻居车辆广播请求消息的步骤，当目标车辆在当前车辆的白名单列表中时，根据目标车辆的信标消息获取当前时刻当前车辆和目标车辆的距离偏差，然后根据公式

$Bias_{t\&t'}=\left|D_{t\&t'}-\sqrt{(Xpos_{tag}-Xpos_{tag'})^2+(Ypos_{tag}-Ypos_{tag'})^2}\right|$获取上一信标周期的目标车辆与当前时刻的目标车辆的距离偏差，再根据公式$Bias_{o'\&t}=\left|D_{o'\&t}-\sqrt{(Xpos_{own}-Xpos_{tag})^2+(Ypos_{own}-Ypos_{tag})^2}\right|$获取上一信标周期的当前车辆与当前时刻的目标车辆的距离偏差，最后根据公式$PositionR=\frac{1}{3}(Bias_{o\&t}+Bias_{t\&t'}+Bias_{o'\&t})$获取目标车辆的位置特征，从而减少了目标车辆位置特征的获取时间，进而提高了检测效率。其中，$D_{t\&t'}=(\frac{MaxSpeed}{2}\pm\sqrt{\frac{MaxSpeed^2}{4}-\frac{MaxSpeed}{MaxDensity}AvgFlow_{tag}})\times BeaconT$，$D_{t\&t'}$为上一信标周期的目标车辆到当前时刻的目标车辆的测量距离，$D_{o'\&t}=\sqrt{D_{o\&t}{}^2+D_{o\&o'}{}^2-2D_{o\&t}D_{o\&o'}\cos\angle TOO'}$，$D_{o'\&t}$为上一信标周期的当前车辆到当前时刻的目标车辆的测量距离，BeaconT为一个信标消息周期，$Bias_{t\&t'}$为上一信标周期的目标车辆与当前时刻的距离偏差，$Bias_{o'\&t}$为上一信标周期的当前车辆与当前时刻目标车辆的距离偏差，$D_{o\&t}$为当前时刻的当前车辆到当前时刻的目标车辆的测量距离，$D_{o\&o'}$为当前时刻的当前车辆到上一信标周期的当前车辆的测量距离，$(Xpos_{tag},Ypos_{tag})$为当前时刻目标车辆的坐标，$(Xpos_{tag'},Ypos_{tag'})$为上一信标周期目标车辆的坐标，$(Xpos_{own},Ypos_{own})$为当前时刻目标车辆的坐标，$\angle TOO'$为$D_{o\&o'}$和$D_{o\&t}$的夹角，PositionR为目标车辆的位置特征。

[0030] 在步骤S102中，根据获取的车流量特征和车位置特征，使用预先训练好的车辆特征分类器对目标车辆进行分类，以确定目标车辆是否为入侵车辆。

[0031] 在本发明实施例中，车辆的白名单列表为该车辆的检测范围内被检测为正常车辆的车辆ID列表，车辆的黑名单列表为该车辆的检测范围内被检测为入侵车辆的车辆ID列表，车辆特征分类器为多维分类器，可对车辆同时在车流量特征和车位置特征两个维度上进行分类。当前车辆、邻居车辆都处于相同的交通条件中，当前车辆与其邻居车辆检测到的车流量非常相近，当目标车辆为创造不存在的事实而通过发送虚假流量给其他车辆时，其车流量与当前车辆的车流量差别较大，通过目标车辆的车流量来判定目标车辆是否为入侵车辆，从而提高了对目标车辆判断的准确度。再者，目标车辆向其邻居车辆(包括当前车辆)声明的位置(距离)与当前车辆测量目标车辆的位置(距离)的偏差应在一定偏差范围内，通过目标车辆的车位置特征来判定目标车辆是否为入侵车辆，从而进一步提高了对目标车辆判断的准确度。

[0032] 优选地，当车流量特征在预设流量偏差范围内、且车位置特征在预设位置偏差范围内时，判定目标车辆为非入侵车辆，将目标车辆分入当前车辆的白名单列表，否则，判定目标车辆为入侵车辆，将目标车辆分入当前车辆的黑名单列表，从而在判断目标车辆是否为入侵车辆的同时将车辆分入不同的列表，进而便于后续车辆对入侵车辆和非入侵车辆的管理。

[0033] 在本发明实施例中，预设流量偏差范围和预设位置偏差范围可在对当前车辆的车辆特征分类器进行训练时得到，具体地，可设置一定数量的正常车辆供当前车辆对车辆特征分类器进行训练，从而得到预设流量偏差范围和预设位置偏差范围。

[0034] 在本发明实施例中，在当前车辆接收到目标车辆发出的信标消息后，根据信标消息获取目标车辆的车流量特征和车位置特征，再根据获取的车流量特征和车位置特征，使用预先训练好的车辆特征分类器对目标车辆进行分类，以确定目标车辆是否为入侵车辆，

从而通过目标车辆车的流量特征和车位置特征两个维度来判定目标车辆是否为入侵车辆，进而提高了对入侵车辆检测的效率和准确性。

[0035] 实施例二：

[0036] 图2示出了本发明实施例二提供的基于车联网的入侵检测装置的结构，为了便于说明，仅示出了与本发明实施例相关的部分，其中包括：

[0037] 特征获取单元21，用于当当前车辆接收到目标车辆发出的信标消息时，根据接收的目标车辆的信标消息获取目标车辆的车流量特征和车位置特征；以及

[0038] 车辆分类单元22，用于使用预先训练好的车辆特征分类器根据获取的车流量特征和车位置特征对目标车辆进行分类，当车流量特征在预设流量偏差范围内、且车位置特征在预设位置偏差范围内时，将目标车辆分入白名单列表，否则，将目标车辆分入黑名单列表，再根据目标车辆的分类结果判断目标车辆是否为入侵车辆。

[0039] 如图3所示特征获取单元的优选结构，优选地，特征获取单元21包括：

[0040] 车流量获取单元31，用于从目标车辆的信标消息中获取目标车辆的平均车流量；

[0041] 流量特征获取单元32，用于根据当前车辆的平均车流量、目标车辆的平均车流量以及车流量特征公式获取目标车辆的车流量特征。

[0042] 请求消息广播单元33，用于向当前车辆的邻居车辆广播请求消息，以得到所有邻居车辆的响应消息；

[0043] 第一偏差获取单元34，用于根据邻居车辆的响应消息分别得到当前时刻邻居车辆到目标车辆的声明距离与当前时刻邻居车辆到目标车辆的测量距离，获取当前时刻邻居车辆和目标车辆的第一距离偏差；

[0044] 第二偏差获取单元35，用于根据目标车辆的信标消息分别得到当前时刻当前车辆到目标车辆的声明距离与当前时刻当前车辆到目标车辆的测量距离，获取当前时刻当前车辆和目标车辆的第二距离偏差；以及

[0045] 位置特征获取单元36，用于根据第一距离偏差、第二距离偏差以及车位置特征公式获取目标车辆的位置特征。

[0046] 在本发明实施例中，在当前车辆接收到目标车辆发出的信标消息后，根据信标消息获取目标车辆的车流量特征和车位置特征，再根据获取的车流量特征和车位置特征，使用预先训练好的车辆特征分类器对目标车辆进行分类，以确定目标车辆是否为入侵车辆，从而通过目标车辆车的流量特征和车位置特征两个维度来判定目标车辆是否为入侵车辆，进而提高了对入侵车辆检测的效率和准确性。

[0047] 在本发明实施例中，基于车联网的入侵检测装置的各单元可由相应的硬件或软件单元实现，各单元可以为独立的软、硬件单元，也可以集成为一个软、硬件单元，在此不用以限制本发明。各单元的具体实施方式可参考实施例一的描述，在此不再赘述。

[0048] 实施例三：

[0049] 图4示出了本发明实施例三提供的车载终端的结构，为了便于说明，仅示出了与本发明实施例相关的部分，其中包括：

[0050] 本发明实施例的车载终端4包括处理器41、存储器42以及存储在存储器42中并可在处理器41上运行的计算机程序43。该处理器41执行计算机程序43时实现上述基于车联网的入侵检测方法实施例中的步骤，例如图1所示的步骤S101至S102。或者，处理器41执行计

算机程序43时实现上述基于车联网的入侵检测装置实施例中各单元的功能，例如图2所示单元21至22的功能。

[0051] 在本发明实施例中，该处理器执行计算机程序时，在当前车辆接收到目标车辆发出的信标消息后，根据信标消息获取目标车辆的车流量特征和车位置特征，再根据获取的车流量特征和车位置特征，使用预先训练好的车辆特征分类器对目标车辆进行分类，以确定目标车辆是否为入侵车辆，从而通过目标车辆车的流量特征和车位置特征两个维度来判定目标车辆是否为入侵车辆，进而提高了对入侵车辆检测的效率和准确性。

[0052] 该处理器执行计算机程序时实现上述基于车联网的入侵检测方法实施例中的步骤可参考实施例一的描述，在此不再赘述。

[0053] 实施例四：

[0054] 在本发明实施例中，提供了一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，该计算机程序被处理器执行时实现上述基于车联网的入侵检测方法实施例中的步骤，例如，图1所示的步骤S101至S102。或者，该计算机程序被处理器执行时实现上述基于车联网的入侵检测装置实施例中各单元的功能，例如图2所示单元21至22的功能。

[0055] 在本发明实施例中，在计算机程序被处理器执行后，在当前车辆接收到目标车辆发出的信标消息后，根据信标消息获取目标车辆的车流量特征和车位置特征，再根据获取的车流量特征和车位置特征，使用预先训练好的车辆特征分类器对目标车辆进行分类，以确定目标车辆是否为入侵车辆，从而通过目标车辆车的流量特征和车位置特征两个维度来判定目标车辆是否为入侵车辆，进而提高了对入侵车辆检测的效率和准确性。

[0056] 本发明实施例的计算机可读存储介质可以包括能够携带计算机程序代码的任何实体或装置、存储介质，例如，ROM/RAM、磁盘、光盘、闪存等存储器。

[0057] 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。

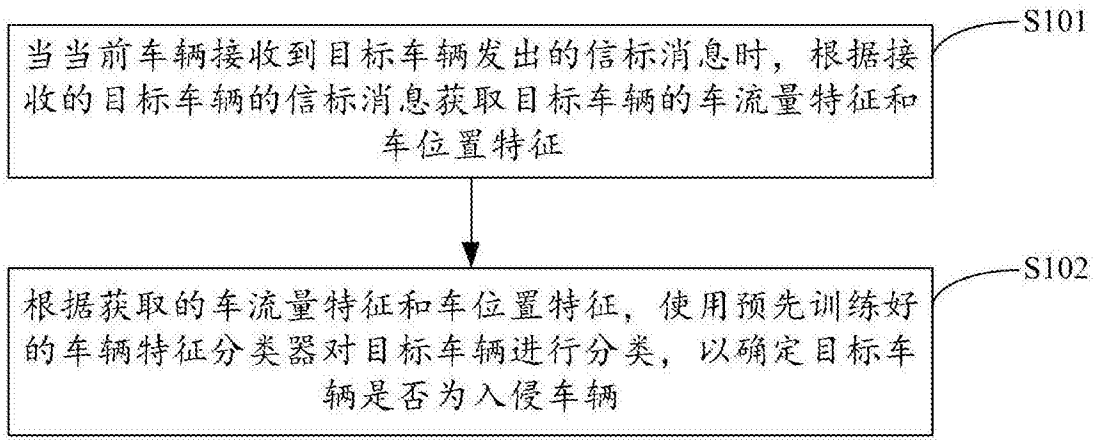

当当前车辆接收到目标车辆发出的信标消息时，根据接收的目标车辆的信标消息获取目标车辆的车流量特征和车位置特征
S101
根据获取的车流量特征和车位置特征，使用预先训练好的车辆特征分类器对目标车辆进行分类，以确定目标车辆是否为入侵车辆
S102

图1

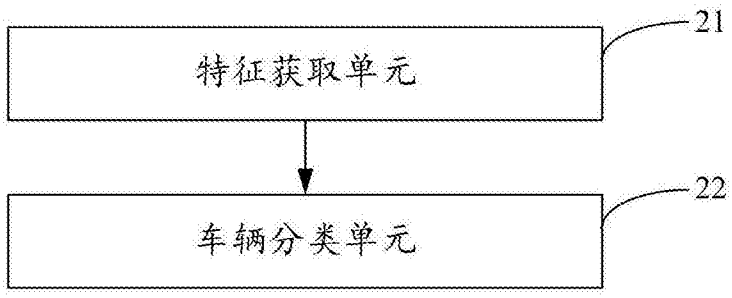

特征获取单元
21
车辆分类单元
22

图2

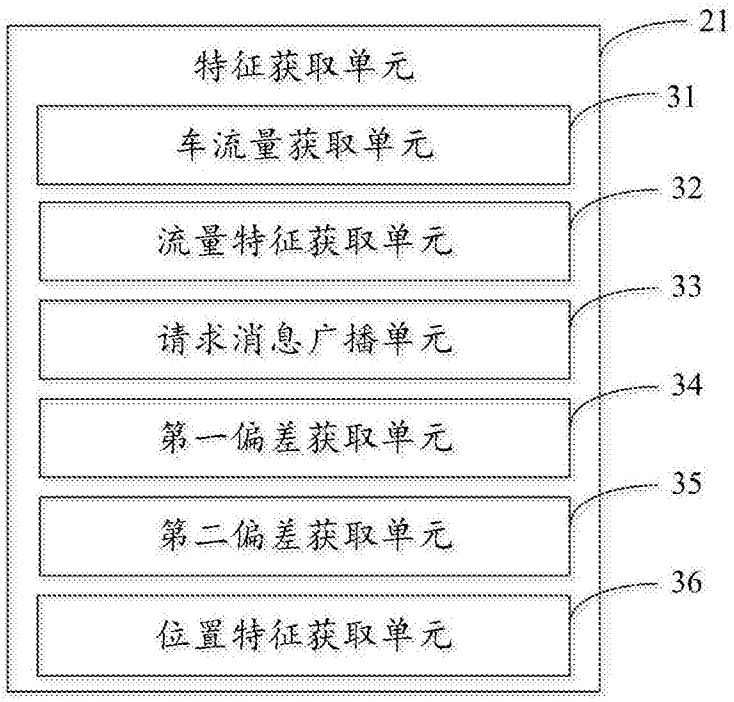

特征获取单元
21
车流量获取单元
31
流量特征获取单元
32
请求消息广播单元
33
第一偏差获取单元
34
第二偏差获取单元
35
位置特征获取单元
36

图3

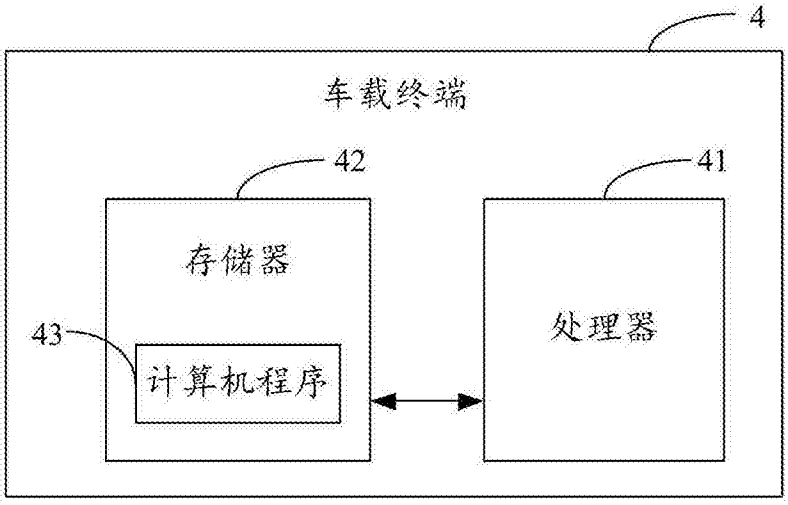


图4