(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 110958271 A
(43)申请公布日 2020.04.03

(21)申请号 201911348641.5

(22)申请日 2019.12.24

(71)申请人 国家计算机网络与信息安全管理中心
地址 100029 北京市朝阳区裕民路甲三号

(72)发明人 云晓春 李政 李承泽 吴昊 申任远 吴志敏 袁静 肖佃艳 范乐君 陈燕呢 王智勇 李涛

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 马瑞

(51)Int.Cl.
H04L 29/06(2006.01)

权利要求书2页 说明书7页 附图1页

(54)发明名称

一种车载外部网络入侵检测系统

(57)摘要

本发明实施例提供一种车载外部网络入侵检测系统，包括设置于车联网终端中的流量采集模块、规则匹配模块和异常分级模块，其中，所述流量采集模块采集进入车联网终端的流量数据，并将所述流量数据传输给所述规则匹配模块；所述规则匹配模块通过预设规则库中的信息，检测所述流量数据中是否存在异常数据信息，并当检测到存在所述异常数据信息时，将检测到的异常结果和所述异常数据信息发送给所述异常分级模块；所述异常分级模块通过预先设置的异常分级映射表，确定所述异常数据信息的安全威胁等级；其中，所述异常分级映射表中设置有数据内容类型与安全威胁等级之间的预设关系。本发明实施例实现了对入侵行为的有效检测。

CN 110958271 A

1.一种车载外部网络入侵检测系统，其特征在于，包括设置于车联网终端中的流量采集模块、规则匹配模块和异常分级模块，其中，

所述流量采集模块采集进入车联网终端的流量数据，并将所述流量数据传输给所述规则匹配模块；

所述规则匹配模块通过预设规则库中的信息，检测所述流量数据中是否存在异常数据信息，并当检测到存在所述异常数据信息时，将检测到的异常结果和所述异常数据信息发送给所述异常分级模块；

所述异常分级模块通过预先设置的异常分级映射表，确定所述异常数据信息的安全威胁等级；其中，所述异常分级映射表中设置有数据内容类型与安全威胁等级之间的预设关系。

2.根据权利要求1所述的车载外部网络入侵检测系统，其特征在于，所述流量采集模块通过静默方式对所述流量数据进行采集。

3.根据权利要求1所述的车载外部网络入侵检测系统，其特征在于，所述车联网终端还包括解码模块；其中，所述解码模块对待传输给所述规则匹配模块的流量数据进行解码操作，并将进行解码操作后的流量数据传输给所述规则匹配模块。

4.根据权利要求1所述的车载外部网络入侵检测系统，其特征在于，所述车联网终端还包括数据预处理模块；其中，所述数据预处理模块对待传输给所述规则匹配模块的流量数据进行数据清洗操作和/或对所述流量数据进行标准化处理操作。

5.根据权利要求1所述的车载外部网络入侵检测系统，其特征在于，所述车联网终端还包括报警处理模块；其中，

所述异常分级模块还根据所述异常数据信息的安全威胁等级，向所述报警处理模块发送与所述异常数据信息的安全威胁等级相对应的报警指示信息；其中安全威胁等级与报警指示信息之间具有预设对应关系；

所述报警处理模块根据所接收到的所述报警指示信息，进行相对应的报警指示。

6.根据权利要求1所述的车载外部网络入侵检测系统，其特征在于，还包括设置于云端的数据汇聚模块和行为分析模块；其中，当所述异常分级模块确定所述异常数据信息的安全威胁等级为不能判定时，将所述异常数据信息发送给所述数据汇聚模块；

所述数据汇聚模块将接收到的所有异常数据信息发送给所述行为分析模块，所述行为分析模块对所接收到的所有异常数据信息进行关联分析，得到分析结果，并确定所述异常数据信息的安全威胁等级。

7.根据权利要求1-6任一项所述的车载外部网络入侵检测系统，其特征在于，所述安全威胁等级包括威胁程度依次增加的一级安全威胁等级、二级安全威胁等级和三级安全威胁等级。

8.根据权利要求6所述的车载外部网络入侵检测系统，其特征在于，还包括设置于云端的规则更新模块；其中，所述规则匹配模块按照预设周期向所述规则更新模块发送规则更新请求；

当所述规则更新模块根据所述规则更新请求，检测到所述规则匹配模块中的预设规则库需要更新时，则将更新信息发送给所述规则匹配模块；所述更新信息包括对所述预设规则库中的信息的修改、删除和/或添加信息。

9.根据权利要求8所述的车载外部网络入侵检测系统，其特征在于，所述行为分析模块将所述分析结果作为新增规则发送给所述规则更新模块，以使所述规则更新模块根据所述新增规则更新所述预设规则库。

一种车载外部网络入侵检测系统

技术领域

[0001] 本发明涉及网络入侵技术领域,尤其涉及一种车载外部网络入侵检测系统。

背景技术

[0002] 智能网联汽车通过搭载先进的车载传感器、控制器、执行器等装置,并融合现代通信与网络技术,进一步实现了车对外界智能信息交换共享,达到了安全、舒适、节能和高效行驶的效果。虽然智能汽车给人们带来了诸多便利,但随之而来的安全风险却不可忽视。

[0003] 其中,智能汽车的攻击面通常可以分为内部接口和外部接口两种。外部接口包括蜂窝移动网络、全球定位系统(Global Positioning System,GPS)接收器、WiFi、蓝牙等,特别是蜂窝移动网络,如被攻击者利用,则可从任何地方对车辆实施攻击。使用蜂窝移动网络,攻击者可以通过汽车信息服务系统或车载娱乐系统访问通信卡信息,也可以干扰电话呼叫,跟踪车辆,设置假基站,甚至可以完全控制车辆行动。因此,有必要针对外部接口设计安全策略,抵御安全威胁。

[0004] 而从实现功能角度来看,现有与车载外部网络相关的安全问题研究主要包括如下几种类型:其一,是通过车载移动终端监控车辆自身状态信息和车辆外部环境,是基于移动互联网实现对汽车的安全监控,但并未对网络入侵进行检测;其二,由装备在车辆上并可实现无线通信的车载单元、在道路两边铺设的网络基础建设,以及对车辆加以注册认证的认证中心构成的车联网场景,发现非车联网注册用户恶意向车联网中的车载单元等发送带有病毒的消息以及对车联网入侵的问题;其三,通过在网络侧对车联网终端进行检测以判断车联网终端是否遭受入侵,该种方式需要保证网络侧能够获取到连接在网络中的车联网终端的行为数据信息。即上述几种方式要么侧重于部署在认证中心的车辆与车辆之间、车辆与路基单元之间的场景,要么侧重于部署在网络侧,需要将流量由车联网终端旁路回网络侧的场景。

发明内容

[0005] 本发明实施例提供一种车载外部网络入侵检测系统,以解决车联网终端无法有效检测车载外部网络访问的问题。

[0006] 本发明实施例提供一种车载外部网络入侵检测系统,包括设置于车联网终端中的流量采集模块、规则匹配模块和异常分级模块,其中,

[0007] 所述流量采集模块采集进入车联网终端的流量数据,并将所述流量数据传输给所述规则匹配模块;

[0008] 所述规则匹配模块通过预设规则库中的信息,检测所述流量数据中是否存在异常数据信息,并当检测到存在所述异常数据信息时,将检测到的异常结果和所述异常数据信息发送给所述异常分级模块;

[0009] 所述异常分级模块通过预先设置的异常分级映射表,确定所述异常数据信息的安全威胁等级;其中,所述异常分级映射表中设置有数据内容类型与安全威胁等级之间的预

设关系。

[0010] 可选地，所述流量采集模块通过静默方式对所述流量数据进行采集。

[0011] 可选地，所述车联网终端还包括解码模块；其中，所述解码模块对待传输给所述规则匹配模块的流量数据进行解码操作，并将进行解码操作后的流量数据传输给所述规则匹配模块。

[0012] 可选地，所述车联网终端还包括数据预处理模块；其中，所述数据预处理模块对待传输给所述规则匹配模块的流量数据进行数据清洗操作和/或对所述流量数据进行标准化处理操作。

[0013] 可选地，所述车联网终端还包括报警处理模块；其中，所述异常分级模块还根据所述异常数据信息的安全威胁等级，向所述报警处理模块发送与所述异常数据信息的安全威胁等级相对应的报警指示信息；其中安全威胁等级与报警指示信息之间具有预设对应关系；所述报警处理模块根据所接收到的所述报警指示信息，进行相对应的报警指示。

[0014] 可选地，还包括设置于云端的数据汇聚模块和行为分析模块；其中，当所述异常分级模块确定所述异常数据信息的安全威胁等级为不能判定时，将所述异常数据信息发送给所述数据汇聚模块；所述数据汇聚模块将接收到的所有异常数据信息发送给所述行为分析模块，所述行为分析模块对所接收到的所有异常数据信息进行关联分析，得到分析结果，并确定所述异常数据信息的安全威胁等级。

[0015] 可选地，所述安全威胁等级包括威胁程度依次增加的一级安全威胁等级、二级安全威胁等级和三级安全威胁等级。

[0016] 可选地，还包括设置于云端的规则更新模块；其中，所述规则匹配模块按照预设周期向所述规则更新模块发送规则更新请求；当所述规则更新模块根据所述规则更新请求，检测到所述规则匹配模块中的预设规则库需要更新时，则将更新信息发送给所述规则匹配模块；所述更新信息包括对所述预设规则库中的信息的修改、删除和/或添加信息。

[0017] 可选地，所述行为分析模块将所述分析结果作为新增规则发送给所述规则更新模块，以使所述规则更新模块根据所述新增规则更新所述预设规则库。

[0018] 本发明实施例提供的车载外部网络入侵检测系统，通过车联网终端中的流量采集模块采集进入车联网终端的流量数据，然后通过规则匹配模块检测流量数据中是否存在异常数据信息，并当检测到存在异常数据信息时，将检测到的异常结果和异常数据信息发送给异常分级模块，最后通过异常分级模块确定异常数据信息的安全威胁等级，实现了入侵检测本地化，使得无需将进入车联网终端的远程通信流量全部转发至云端进行检测，进而使得能够在抵御互联网安全威胁的同时，保护车辆的电子系统资产信息，解决了现有技术中由于车载外部网络访问复杂而导致的车联网终端无法进行有效检测入侵行为，保障汽车安全的问题。

附图说明

[0019] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0020] 图1为本发明实施例中车载外部网络入侵检测系统的示意图之一；

[0021] 图2为本发明实施例中车载外部网络入侵检测系统的示意图之二。

具体实施方式

[0022] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0023] 如图1所示，为本发明实施例中车载外部网络入侵检测系统的示意图之一，该车载外部网络入侵检测系统包括设置于车联网终端1中的流量采集模块11、规则匹配模块12和异常分级模块13；其中，

[0024] 所述流量采集模块11采集进入车联网终端的流量数据，并将所述流量数据传输给所述规则匹配模块12；

[0025] 所述规则匹配模块12通过预设规则库中的信息，检测所述流量数据中是否存在异常数据信息，并当检测到存在所述异常数据信息时，将检测到的异常结果和所述异常数据信息发送给所述异常分级模块13；

[0026] 所述异常分级模块13通过预先设置的异常分级映射表，确定所述异常数据信息的安全威胁等级；其中，所述异常分级映射表中设置有数据内容类型与安全威胁等级之间的预设关系。

[0027] 具体的，车联网终端具备通过通用无线分组业务(General Packet Radio Service，GPRS)支持节点连接到互联网的能力；当车联网终端连接进互联网中时，网络管理平台会给车联网终端下发一个互联网标识，例如IP地址。

[0028] 此外，具体的，流量采集模块11可以为远程通信，且当流量采集模块11采集流量数据时，流量采集模块11可以通过监测相应的网口以静默方式对流量数据进行采集。具体的，所有通过该网口的流量数据均可以认为是属于采集范围，当然也可以以用户实际关心的流量类型为参考，例如若只关心MQTT流量，则可以配置只抓取MQTT流量数据，若只关心JT808流量，则可以配置只抓取JT808流量数据。

[0029] 此外，具体的，规则匹配模块12中配备有预设规则库，该预设规则库可以用于检测流量数据中是否存在异常数据信息；此时，当规则匹配模块12基于该预设规则库中的信息，检测到流量数据中存在异常数据信息时，可以将检测到的异常结果和异常数据信息发送给异常分级模块13。

[0030] 具体的，该预设规则库中的信息(即检测规则)可以具体由用户决定，形式上可以表现为基于正则表达式的特征库，每个规则表征了针对流量数据中相应攻击的匹配情况，即可以根据不同的协议类型制定不同的检测规则，这些协议类型可以是标准协议，也可以是私有协议；例如可以包含snort中与浏览器相关的规则，也可以是自定义的规则例如与JT808相关的规则，也可以是与私有车联网流量相关的规则。该预设规则库反映了用户对于系统在安全性和隐私性等层面的特定安全需求。

[0031] 另外，具体的，异常分级模块13中配备有异常分级映射表，该异常分级映射表中设置有数据内容类型与安全威胁等级之间的预设关系，即该异常分级映射表能够清晰表明异

常数据信息属于哪一安全威胁等级。

[0032] 其中，安全威胁等级包括威胁程度依次增加的一级安全威胁等级、二级安全威胁等级和三级安全威胁等级。此时一级安全威胁等级可以为一般威胁、二级安全威胁等级可以为严重威胁，三级安全威胁等级可以为重度严重威胁。此外，数据内容类型可以包括用户信息的请求类型信息、鉴权类型信息以及访问类型信息等。

[0033] 例如，当数据内容类型为请求车辆识别号码(Vehicle Identification Number，VIN)或请求个人信息和账单信息时，则对应属于一般威胁等级的一级安全威胁等级，例如如果检测到异常数据信息为请求VIN码或请求个人信息和账单信息异常，则确定异常数据信息的安全威胁等级为一级安全威胁等级；当数据内容类型为进行鉴权时，则对应属于严重威胁等级的二级安全威胁等级，例如如果检测到异常数据信息为鉴权异常，则确定异常数据信息的安全威胁等级为二级安全威胁等级；当数据内容类型为进行升级访问时，则对应属于重度严重威胁的三级安全威胁等级，例如如果检测到异常数据信息为不明来源固件访问升级异常，则确定异常数据信息的安全威胁等级为三级安全威胁等级。

[0034] 这样，本实施例通过车联网终端中的流量采集模块采集进入车联网终端的流量数据，然后通过规则匹配模块检测流量数据中是否存在异常数据信息，并当检测到存在异常数据信息时，将检测到的异常结果和异常数据信息发送给异常分级模块，最后通过异常分级模块确定异常数据信息的安全威胁等级，实现了入侵检测本地化，使得无需将进入车联网终端的远程通信流量全部转发至云端进行检测，进而使得能够在抵御互联网安全威胁的同时，保护车辆的电子系统资产信息，解决了现有技术中由于车载外部网络访问复杂而导致的车联网终端无法进行有效检测入侵行为，保障汽车安全的问题。

[0035] 在此需要说明的是，车联网终端可以部署于汽车外部网络入口处，例如当前负责汽车与云端远程通信的汽车信息服务系统(TBOX)或具有互联网通信功能的车载信息娱乐系统(IVI)。另外，虽然不同车联网终端在实现远程网络通信时所采用物理单元的设计结构会有不同，但本实施例的车联网终端部分逻辑上兼容于任意这样的结构。

[0036] 此外，进一步地，如图2所示，所述车联网终端还包括解码模块14；其中，所述解码模块14对待传输给规则匹配模块12的流量数据进行解码操作，并将进行解码操作后的流量数据传输给规则匹配模块12。

[0037] 即流量采集模块11可以先将流量数据传输给解码模块14，由解码模块14对流量数据进行解码，得到具体内容，然后将解码后的流量数据传输给规则匹配模块12，由规则匹配模块12检测是否存在异常数据信息。

[0038] 具体的，解码模块14根据协议栈要求对采集到的流量数据依次执行解码操作。举例来说，道路运输车辆卫星定位系统终端通讯协议JT/T808采用传输控制协议(Transmission Control Protocol，TCP)或用户数据报协议(UserDatagram Protoco，UDP)，监管平台作为服务器端，车联网终端作为客户端。此外，每条流量数据由标识位、消息头、消息体和校验码组成，标识位采用0x7e表示，若校验码、消息头以及消息体中出现0x7e，则要进行转义处理。转义规则可以定义为：0x7e<——>0x7d后紧跟一个0x02；0x7d<——>0x7d后紧跟一个0x01；转义处理过程为：发送流量数据时——消息封装——>计算并填充校验码——>转义；接收流量数据时-转义还原——>验证校验码——>解析消息。例如可以为：发送一包内容为0x30 0x7e 0x08 0x7d 0x55的数据包，则经过封装如下：0x7e 0x30 7d

0x02 0x08 0x7d 0x01 0x55 0x7e。

[0039] 再例如,电动汽车远程服务与管理系统技术规范GB/T 32960也提供了客户端平台与服务端平台之间的通讯连接方式。一个完整的数据包由起始符、命令单元、识别码、数据加密方式、数据单元长度、数据单元和校验码组成。起始符与校验码是本标准中报文边际界定符号,其中起始符(0x23 0x23)在报文中并无解析意义,仅作为报文起始标记存在,校验码作为报文终止标记存在,通过将除校验码以外的完整报文进行异或校验获得;命令标识作为报文种类标识存在,解析时应通过命令标识的不同进行报文种类的区分,应答标志作为报文发送方向的区分,当报文为上行时,应答标志应为0xFE。在传输车辆数据时,采用车辆VIN作为唯一识别码进行传输;当进行平台传输时由服务端平台提供,可以采用以下规则:城市邮政编码+VIN前三位+两位自定义数据+“000000”。

[0040] 另外,具体的,解码模块工作过程严格遵循互联网协议、车联网协议以及具体行业应用协议规范执行解码操作,从而使得既可抵御互联网安全威胁,也可保护汽车电子系统资产,例如车辆状态数据(如位置、速度和目的地等)、与特定车辆相关的信息(如个人信息、身份认证信息、账单信息、用户使用历史和操作历史等信息)。

[0041] 另外,进一步地,继续参见图2,所述车联网终端还包括数据预处理模块15;其中,所述数据预处理模块15对待传输给所述规则匹配模块12的流量数据进行数据清洗操作和/或对所述流量数据进行标准化处理操作。

[0042] 具体的,在对流量数据进行数据清洗操作时,如填补缺失数据、消除噪声数据等。即可以通过分析脏数据的产生原因和存在形式,将脏数据转化为满足数据质量或应用要求的数据,从而提高数据质量。

[0043] 此外,具体的,还可以将所有流量数据统一存储在数据库或文件中,形成一个完整的数据集,并在该集成过程中,消除冗余数据。

[0044] 另外,具体的,还可以对流量数据进行标准化处理操作,比如将数据值限定在特定的范围之内,或是把原始数据转化为满足一定要求的格式数据。

[0045] 另外,具体的,还可以对流量数据印象数据规约,即将不能够刻画关键特征的属性剔除掉,从而得到精练的属性集合。

[0046] 另外,进一步地,继续参见图2,所述车联网终端还包括报警处理模块16;其中,

[0047] 所述异常分级模块13还根据所述异常数据信息的安全威胁等级,向所述报警处理模块16发送与所述异常数据信息的安全威胁等级相对应的报警指示信息;其中安全威胁等级与报警指示信息之间具有预设对应关系;

[0048] 所述报警处理模块16根据所接收到的所述报警信息,发出与所述报警信息相对应的报警信号。

[0049] 具体的,在异常分级模块13确定异常数据信息的安全威胁等级之后,可以向报警处理模块16发送与该安全威胁等级相对应的报警指示信息,从而使得报警处理模块16能够根据所接收到的报警信息,发出与报警信息相对应的报警信号。

[0050] 例如,第一安全威胁等级可以与发出报警信号的报警指示信息相对应,第二安全威胁等级可以与发出报警信号、暂停汽车内预设功能模块的外部连接的报警指示信息相对应,第三安全威胁等级可以与发出报警信号、切断车载外部网络通信的报警指示信息相对应。另外,报警信号可以通过指示灯颜色、指示灯闪烁快慢以及蜂鸣声的尖锐程度或快慢等

进行展示。

[0051] 另外，进一步地，具体参见图2，车载外部网络入侵检测系统还包括设置于云端2的数据汇聚模块21和行为分析模块22；其中，当所述异常分级模块13确定所述异常数据信息的安全威胁等级为不能判定时，将所述异常数据信息发送给所述数据汇聚模块21；

[0052] 所述数据汇聚模块21将接收到的所有异常数据信息发送给所述行为分析模块22，所述行为分析模块22对所接收到的所有异常数据信息进行关联分析，得到分析结果，并确定所述异常数据信息的安全威胁等级。

[0053] 具体的，当所述异常分级模块13确定异常数据信息的安全威胁等级为不能判定时，将异常数据信息发送给数据汇聚模块21；即所有车联网终端的异常分级模块13均可以将安全威胁等级为不能判定的异常数据信息发送给云端2中的数据汇聚模块21中，然后由数据汇聚模块21将接收到的所有异常数据信息发送给行为分析模块22，此时行为分析模块22对所接收到的所有异常数据信息进行关联分析，得到分析结果，并确定所述异常数据信息的安全威胁等级。

[0054] 此外，具体的，入侵行为有可能是极端隐蔽，单独车联网终端无法识别、从而需要结合大数据样本加以分析，也有可能是因为入侵行为本身就是涉及到针对多个车联网终端开展的存在关联关系的入侵，此时行为分析模块22可以根据汇聚而来的异常数据信息，结合大数据分析技术执行关联分析，以发现入侵行为。

[0055] 这样，云端通过汇集不同车联网终端上报的异常数据信息执行关联分析，发挥了大数据优势，提高了分析准确率。

[0056] 另外，进一步地，车载外部网络入侵检测系统还包括设置于云端2的规则更新模块23；其中，所述规则匹配模块12按照预设周期向所述规则更新模块23发送规则更新请求；

[0057] 当所述规则更新模块23根据所述规则更新请求，检测到所述规则匹配模块12中的预设规则库需要更新时，则将更新信息发送给所述规则匹配模块12；所述更新信息包括对所述预设规则库中的信息的修改、删除和/或添加信息。

[0058] 此外，行为分析模块22将所述分析结果作为新增规则发送给所述规则更新模块23，以使所述规则更新模块根据所述新增规则更新所述预设规则库。

[0059] 具体的，行为分析模块22执行完行为分析后，可以将分析结果以规则的形式提交给规则更新模块23，从而使得规则更新模块23能够对预设规则库进行更新。

[0060] 这样，云端对汇聚数据进行分析后的分析结果以规则更新的方式反馈回车联网终端，从而提高了系统检测能力。

[0061] 在此需要说明的是，本实施例的云端独立于智能网络汽车结构，云端与车联网终端部分之间的通信过程可以使用安全信道完成。

[0062] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

[0063] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管

参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

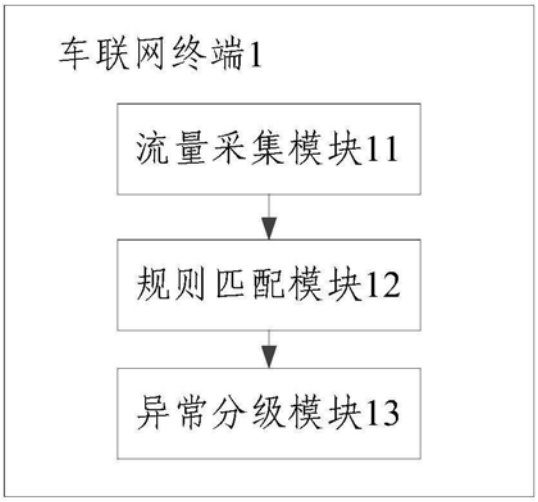
车联网终端1
流量采集模块11
规则匹配模块12
异常分级模块13

图1

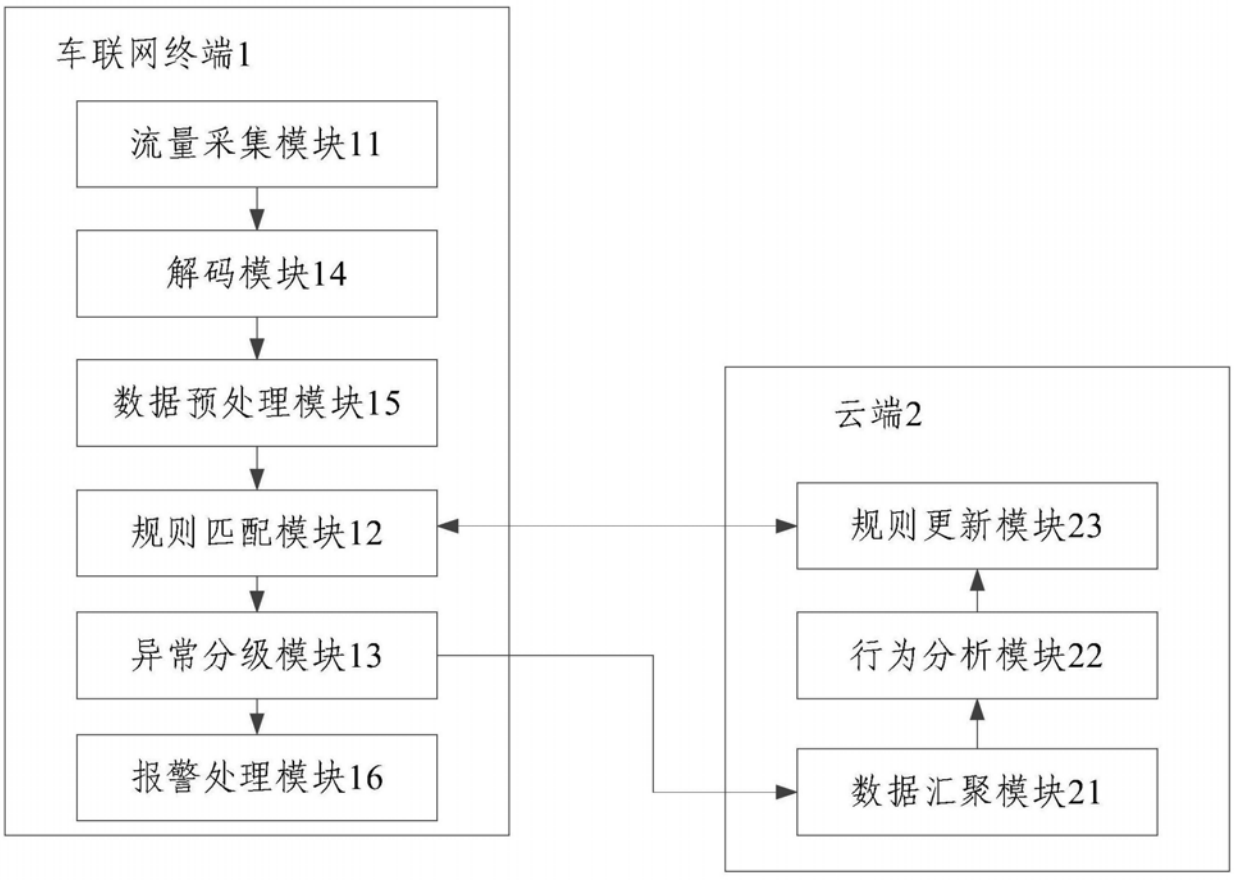
车联网终端1
流量采集模块11
解码模块14
数据预处理模块15
规则匹配模块12
异常分级模块13
报警处理模块16
云端2
规则更新模块23
行为分析模块22
数据汇聚模块21

图2