(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107948172 B
(45)授权公告日 2021.05.25

(21)申请号 201711236177.1

(22)申请日 2017.11.30

(65)同一申请的已公布的文献号
申请公布号 CN 107948172 A

(43)申请公布日 2018.04.20

(73)专利权人 恒安嘉新(北京)科技股份公司
地址 100191 北京市海淀区北三环西路25号27号楼五层5002室
专利权人 国家计算机病毒应急处理中心

(72)发明人 陈乔 何文杰 任翔 梁彧 金红 杨满智 刘长永

(74)专利代理机构 北京市万慧达律师事务所 11111
代理人 黄玉东

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

(56)对比文件
US 2014283079 A1,2014.09.18
CN 105897715 A,2016.08.24

审查员 陈翠莹

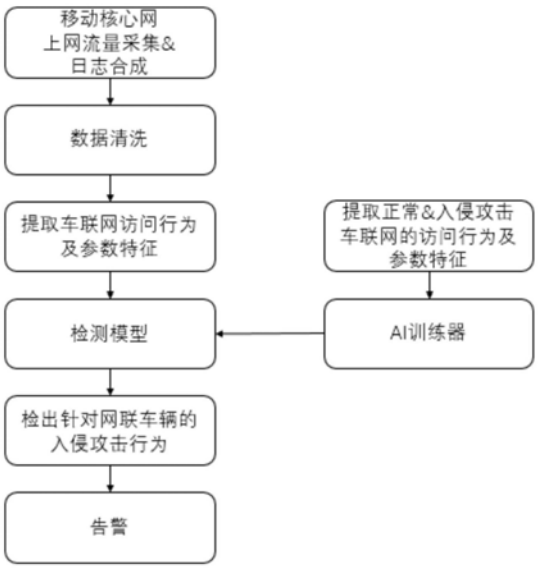
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种基于人工智能行为分析的车联网入侵攻击检测方法和系统

(57)摘要

本发明涉及网络技术领域,公开了一种基于人工智能行为分析的车联网入侵攻击检测方法和系统。所述方法包括:获取上网流量数据,将流量按照通信协议还原,得到上网话单日志;至少根据APN、号段、车联网APP中的一种或多种特征对上述话单日志进行过滤;利用已知的车联网正常访问数据及异常的入侵攻击数据,提取访问参数特征及访问行为特征,并使用人工智能分类器模型进行训练;对实时的车联网访问数据提取访问参数特征及访问行为特征,使用训练好的分类器模型进行判断是否遭遇到入侵攻击,并将入侵攻击行为进行相应处置。本发明的方法及系统能够准确判断外部行为对网联车辆是否进行入侵。



CN 107948172 B

1.一种基于人工智能行为分析的车联网入侵攻击检测方法,其特征在于,所述方法包括步骤:

步骤S1、获取移动核心网的上网流量数据,将流量按照通信协议还原,得到上网话单日志;其中,获取的所述移动核心网的上网流量数据主要在移动网管道侧采集,并基于车联网移动APP、车载终端为访问源或访问目的,至少包括:源IP,源端口,目标IP,目标端口,协议,访问时间,MSISDN号码,IMSI,IMEI,LAC,CI,DNS解析记录,CA认证请求响应;通过部署数据流量采集设备获取经移动核心网的4G上网流量数据,包括S1-U、S10、S11接口原始流量数据;将流量按通信协议还原,提取各接口的上网日志,并对各接口日志进行关联合成,从而得到完整的移动上网话单日志;

步骤S2、根据APN、号段、车联网手机APP中的一种或多种特征对所述完整的移动上网话单日志进行过滤;

步骤S3、利用已知的车联网正常访问数据及异常的入侵攻击数据,提取访问参数特征及访问行为特征,并使用人工智能分类器模型进行训练;

步骤S4、对实时的车联网访问数据提取访问参数特征及访问行为特征,使用训练好的分类器模型进行判断是否遭遇到入侵攻击,并将入侵攻击行为进行相应处置;

依据的所述访问行为特征包括:请求频次、数据流向、请求参数值最大熵值、车辆行驶特征、单位时间内总访问次数,单位时间内访问行为突发程度,单位时间内来访IP最大访问次数占比、指令类型及指令下发的时间、来源、频次的行为特征、访问终端来源、TSP平台的CA证书认证流程、来自车联网终端的上行请求网络行为特征。

2.根据权利要求1所述的方法,其特征在于,获取的所述移动核心网的数据还包括:请求方式,访问域名,URI,访问参数。

3.根据权利要求1所述的方法,其特征在于,在步骤S3中,依据的所述访问参数包括:访问频次、根据上述日志数据计算得到的车辆行驶特征、数据流向、数据载荷字节数、DNS解析记录。

4.一种基于人工智能行为分析的车联网入侵攻击检测系统,其特征在于,所述检测系统部署在移动核心网侧,车载终端或者车联网手机APP通过移动基站与TSP平台实现交互,所述系统包括:

数据采集单元,用于采集移动核心网的上网流量数据并提取和合成车联网相关的数据流量话单;其中,获取的所述移动核心网的上网流量数据主要基于车联网移动APP、车载终端为访问源或访问目的,至少包括:源IP,源端口,目标IP,目标端口,协议,访问时间,MSISDN号码,IMSI,IMEI,LAC,CI,DNS解析记录,CA认证请求响应;通过部署数据流量采集设备获取经移动核心网的4G上网流量数据,包括S1-U、S10、S11接口原始流量数据;将流量按通信协议还原,提取各接口的上网日志,并对各接口日志进行关联合成,从而得到完整的移动上网话单日志;所述数据采集单元根据车联网手机APP、车载终端、TSP三者之间的互访,以及车载终端访问未知目的IP,来采集数据流量话单信息;

数据存储单元,用于存储正常访问的数据及入侵攻击的数据;

特征提取单元,根据已知的车联网正常访问数据及异常的入侵攻击数据,提取访问参数特征及访问行为特征;

模型训练单元,用于训练分类器模型,将已知为正常访问及入侵攻击的数据经过特征

提取单元提取到的特征输入该模型训练单元，经过模型评估后得到训练好的分类器模型；

数据检测单元，对实时数据提取特征后的特征进行判断，检测其是否被入侵或攻击，并将检测结果分别保存到数据存储单元当中；

告警单元，当检测到对车辆的网络入侵攻击行为时，向车主或TSP服务商发送告警，并根据危险级别或车主设置对入侵攻击流量进行过滤处置。

5.根据权利要求4所述的系统，其特征在于，所述数据采集单元以分光方式对经移动核心网传输的数据进行复制读取。

一种基于人工智能行为分析的车联网入侵攻击检测方法和系统

技术领域

[0001] 本发明涉及网络技术领域，具体地，涉及一种基于人工智能行为分析的车联网入侵攻击检测方法和系统。

背景技术

[0002] 根据中国汽车工程协会2017年发布的《智能网联汽车信息安全白皮书》的数据，2015年中国智能驾驶乘用车渗透率已达到15％，预计2019年这一数据将达到50％。智能网联汽车一般由车载传感网、车载智能终端与云端TSP、车主移动APP通过移动网进行通信，通信数据通过公众网传输，因此也给了黑客可乘之机，黑客通过对上述设施的渗透、入侵、攻击，以达到不法目的。

[0003] 网络安全隐患存在于车联网架构的各个组成部分，对车联网的网络安全防护需要通过云管端多个层次配合实施，由于车联网数据通常使用加密方式传输，在移动网管道侧一般无法识别分析车联网数据的明文，传统的入侵检测方法无法判断数据合法性。

发明内容

[0004] 针对现有技术的缺陷，本发明所要解决的技术问题是如何准确的判断出车联网是否遭遇外部的入侵。

[0005] 为解决该问题，一方面，本发明提供了一种基于人工智能行为分析的车联网入侵攻击检测方法，包括步骤：

[0006] 步骤S1、获取上网流量数据，将流量按照通信协议还原，得到上网话单日志；

[0007] 步骤S2、根据APN、号段、车联网APP中的一种或多种特征对上述话单日志进行过滤；

[0008] 步骤S3、利用已知的车联网正常访问数据及异常的入侵攻击数据，提取访问参数特征及访问行为特征，并使用人工智能分类器模型进行训练；

[0009] 步骤S4、对实时的车联网访问数据提取访问参数特征及访问行为特征，使用训练好的分类器模型进行判断是否遭遇到入侵攻击，并将入侵攻击行为进行相应处置。

[0010] 进一步地，所述步骤S1具体包括：

[0011] 通过部署数据流量采集设备获取移动核心网的4G上网流量数据，包括S1-U、S10、S11接口原始流量数据；

[0012] 将流量按通信协议还原，提取各接口的上网日志，并对各接口日志进行关联合成，从而得到完整的移动上网话单日志。

[0013] 进一步地，获取的所述移动核心网的数据主要基于车联网移动 APP、车载终端为访问源或访问目的，至少包括：源IP，源端口，目标IP，目标端口，协议，访问时间，MSISDN号码，IMSI，IMEI，LAC， CI，DNS解析记录，CA认证请求响应。

[0014] 进一步地，获取的所述移动核心网的数据还包括：请求方式，访问域名，URI，访问

参数。

[0015] 进一步地，在步骤S3中，依据的所述访问参数包括：访问频次、根据上述日志数据计算得到的车辆行驶特征、数据流向、数据载荷字节数、DNS解析记录。

[0016] 进一步地，依据的所述网络行为包括：请求频次、数据流向、请求参数值最大熵值、车辆行驶特征、单位时间内总访问次数，单位时间内访问行为突发程度，单位时间内来访IP最大访问次数占比、指令类型及指令下发的时间、来源、频次的行为特征、访问终端来源、TSP 平台的CA证书认证流程、来自车联网终端的上行请求网络行为特征。

[0017] 另一方面，还提供了一种基于人工智能行为分析的车联网入侵攻击检测系统，所述系统包括：

[0018] 数据采集单元，用于采集移动核心网数据并提取和合成车联网相关的数据流量话单；

[0019] 数据存储单元，用于存储正常访问的数据及入侵攻击的数据；

[0020] 特征提取单元，根据已知的车联网正常访问数据及异常的入侵攻击数据，提取访问参数特征及访问行为特征；

[0021] 模型训练单元，用于训练分类器模型，将已知为正常访问及入侵攻击的数据经过特征提取单元提取到的特征输入该训练单元，经过模型评估后得到训练好的分类器模型；

[0022] 数据检测单元，对实时数据提取特征后的特征进行判断，检测其是否被入侵或攻击，并将检测结果分别保存到数据存储单元当中。

[0023] 告警单元，当检测到对车辆的网络入侵攻击行为时，向车主或TSP 服务商发送告警，并根据危险级别或车主设置对入侵攻击流量进行过滤处置。

[0024] 进一步地，所述数据采集单元根据车联网手机APP、车载终端、 TSP三者之间的互访，以及车载终端访问未知目的IP，来采集数据流量话单信息。

[0025] 进一步地，提取的所述访问参数包括：访问频次、根据上述日志数据计算得到的车辆行驶特征、数据流向、数据载荷字节数、DNS解析记录；提取的所述网络行为包括：请求频次、数据流向、请求参数值最大熵值、车辆行驶特征、单位时间内总访问次数，单位时间内访问行为突发程度，单位时间内来访IP最大访问次数占比、指令类型及指令下发的时间、来源、频次的行为特征、访问终端来源、TSP平台的CA证书认证流程、来自车联网终端的上行请求网络行为特征。

[0026] 进一步地，所述检测系统部署在移动核心网侧，所述车载终端或者车联网手机APP通过移动基站与TSP平台实现交互。

[0027] 进一步地，所述数据采集单元以分光方式对经移动核心网传输的数据进行复制读取。

[0028] 与现有技术相比，本本发明提供了一种在移动网管道侧对与车联网相关的网络流量进行人工智能检测，能够在不需要对车联网流量进行解密的条件下识别发现入侵攻击的行为，并向经营者或车主发送实时告警，从而达到防范车联网入侵攻击，保护车辆和司乘人员人身财产安全的目的。

附图说明

[0029] 图1是本发明的一个实施例中基于人工智能行为分析的车联网入侵攻击检测方法

的流程示意图；

[0030] 图2为本发明的一个实施例中基于人工智能行为分析的车联网入侵攻击检测系统与外部终端交互的原理图。

[0031] 图3是本发明的一个实施例中基于人工智能行为分析的车联网入侵攻击检测系统的结构原理图。

具体实施方式

[0032] 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，所描述的实施例为实施本发明的较佳实施方式，所述描述是以说明本发明的一般原则为目的，并非用以限定本发明的范围。本发明的保护范围应当以权利要求所界定者为准，基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的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。

[0033] 参照图1所示，本发明实施例所公开的一种基于人工智能行为分析的车联网入侵攻击检测方法，包括如下步骤：

[0034] 步骤S1、获取上网流量数据，将流量按照通信协议还原，得到上网话单日志；

[0035] 步骤S2、根据APN(接入点名称)、号段、车联网APP中的一种或多种特征对上述话单日志进行过滤；

[0036] 步骤S3、利用已知的车联网正常访问数据及异常的入侵攻击数据，提取访问参数特征及访问行为特征，并使用人工智能分类器模型进行训练；

[0037] 步骤S4、对实时的车联网访问数据提取访问参数特征及访问行为特征，使用训练好的分类器模型进行判断是否遭遇到入侵攻击，并将入侵攻击行为进行相应处置。

[0038] 具体来说，在步骤S1中，其过程具体为：

[0039] 步骤S11、通过部署数据流量采集设备获取移动核心网的4G上网流量数据，包括从S1-U、S10、S11接口得到原始流量数据；

[0040] 步骤S12、将流量按通信协议还原，提取各接口的上网日志，并对各接口日志进行关联合成，从而得到完整的移动上网话单日志。

[0041] 其中，获取的所述移动核心网的数据主要是基于车联网移动APP、车载终端为访问源或访问目的，所述数据包括：源IP，源端口，目标 IP，目标端口，协议，访问时间(精确到秒)，MSISDN号码(MSISDN 是指主叫用户为呼叫GSM PLMN中的一个移动用户所需拨的号码，作用同于固定网PSTN号码；是在公共电话网交换网络编号计划中，唯一能识别移动用户的号码。)，IMSI(国际移动用户识别码)，IMEI(国际移动设备识别码)，LAC(位置区码)，CI(小区ID)，DNS解析记录， CA认证(数字证书加密认证)请求响应。其中，所述关联合成具体是指按照IMSI、时间戳、IP五元组(源IP地址，源端口，目的IP地址，目的端口和传输层协议)字段对每个会话进行数据关联合成，从而得到完整的上网话单日志。

[0042] 由于车联网由内置SIM卡的车载Tbox终端、云端TSP、车主手机APP 三种设备或应用联网通信，三者之间的通信通过移动通信网承载。从移动核心网侧采集上述数据，可以识别区分具体的车载终端、TSP平台IP地址、手机APP用户，其中IP层五元组用于标识和关联会话数据， MSISDN、IMSI数据用于区分终端或手机用户，IMEI用于区分终端类型，LAC、CI数据可用于对车载终端进行定位，DNS解析记录可以用于分析记录车载终端或APP通过域名访问

TSP时解析的IP地址,CA认证会话可用于鉴定终端与TSP平台通信的保密性。

[0043] 此外,为了更精确的对数据进行分析和训练,获取的所述移动核心网的数据还包括:请求方式,访问域名,URI(统一资源标识符),访问参数。

[0044] 本发明是在移动网管道侧对与车联网相关的网络流量进行采集提取,并不是采用传统的对车联网流量进行解密的方式,并且提取的多种数据进行综合完全能够作为后续训练器训练的数据依据。

[0045] 现有技术中,已加密的车联网数据无法获取明文,本发明实施例使用的方法是通过分析车联网通信的特征来检测入侵攻击,具体的,所提取的特征包括通信双方的IP五元组特征、域名解析会话特征、终端类型及身份标识特征、通信的时间点、频次、报文大小等行为特征,依靠大量车联网数据通信特征对算法进行训练,从而实现对入侵攻击的异常通信数据进行判断检测。

[0046] 在步骤S2中,根据APN(Access Point Name,即“接入点名称”)、号段 (可区分运营商)、车联网APP特征对上述话单数据进行过滤,过滤掉与车联网通信无关的数据,得到车联网终端、车联网APP的完整话单数据。

[0047] 在步骤S3中,分别依据访问参数特征及访问行为特征进行训练XGBOOST分类模型。XGBOOST算法是一种开源的决策树算法,具体来说,是在GBDT(Gradient Boosting Decision Tree,梯度提升决策树) 的基础上对boosting(提升树)算法进行的改进。其核心为损失函数和求解算法的优化。XGBOOST损失函数建模方式是基于极大似然估计,具体到每个样本上,实际上就是典型的二项分布概率建模式;

[0048] XGBOOST的求解算法,具体到每颗树来说,就是不断地寻找分割点 (split point),将样本集进行分割,初始情况下,所有样本都处于一个结点(即根结点),随着树的分裂过程的展开,样本会分配到分裂开的子结点上。分割点的选择通过枚举训练样本集上的特征值来完成,分割点的选择依据则是减少Loss。

[0049] XGBOOST算法可以给预测模型带来能力的提升。XGBOOST算法具有正则化,并行处理,高度的灵活性,缺失值处理,剪枝,内置交叉验证,在已有的模型基础上继续训练的特点。当然,本领域技术人员应当理解的是,对参数及行为特征的训练不限于本发明所指出的XGBOOST算法训练器,还可以采用其它智能训练器。

[0050] 在本实施例中,所述参数特征包括:访问频次、根据步骤S2输出的日志数据计算得到的车辆行驶特征(路径、速度、方向)、数据流向(APP、TSP平台、车载终端、其他源或目的IP)、数据载荷字节数、DNS解析记录、CA认证记录。上述的访问参数特征,则是针对多个具体请求参数进行统计计算所得。例如,对某一车载终端的接入位置区编码LAC、CI号对应的GPS位置进行持续记录和计算,可以得到车辆的大致行驶速度、路径和方向,此处参数特征用于后续的网络行为分析。

[0051] 所述的网络行为特征包括:请求频次、数据流向、请求参数值最大熵值、车辆行驶特征(时间、道路、方向、速度特征)、单位时间内总访问次数,单位时间内访问行为突发程度,单位时间内来访IP最大访问次数占比、指令类型及指令下发的时间、来源、频次等行为特征、访问终端来源(是否来自车主的手机号码)、TSP平台的CA证书认证流程、来自车联网终端的上行请求网络行为特征。

[0052] 下面来详述通过网络行为特征如何判断访问的异常。

[0053] 请求频次，正常的车联网网络通信请求频次分布按时间周期、位置、速度呈规律性分布，而异常的入侵攻击行为产生的网络通信请求与正常请求频次分布规律存在显著差异。

[0054] 数据流向，正常车联网通信的数据流向是在移动APP与车载终端之间、车载终端与TSP平台之间、移动APP与TSP平台之间，超出上述范围的源或目的IP属于异常访问行为，此外，数据流向与指令类型高度相关。

[0055] 请求参数值最大熵值，正常车联网通信的数据与指令类型呈现相关性，而入侵攻击等异常通信行为可能携带的参数超出正常范围，如上传用户隐私数据等，造成熵值超大。

[0056] 车辆行驶特征(时间、道路、方向、速度特征)，根据步骤S1、S2所得到的车辆位置更新数据计算得到车辆的行驶特征，结合车联网通信行为与行驶特征进行关联分析，检测出入侵攻击等异常通信行为 (例如，当高速行驶时收到熄火或开车门指令，如行驶中多次发出开关车门指令、点火熄火等)。

[0057] 单位时间内总访问次数，车联网通信的单位时间总访问次数呈现与车辆行驶特征呈现关联规律，明显超出规律的访问次数可能为攻击行为。

[0058] 单位时间内访问行为突发程度，正常车联网通信不存在大量的突发访问，当检测到大量突发访问行为时，视为异常入侵或攻击。

[0059] 单位时间内来访IP最大访问次数占比，正常车联网通信中，APP、车载终端、TSP三者之间互访的次数占比较为稳定，呈现规律性，明显违背正常规律的，可判定为异常入侵或攻击。

[0060] 指令类型及指令下发的时间、来源、频次等行为特征，从TSP或 APP向车载终端下发指令的行为呈现规律性，与时间、访问来源、频次等参数高度相关。异常通信行为则表现为随机性。

[0061] 访问终端来源(是否来自车主的手机号码)，根据步骤S1、S2输出的日志数据中包含访问来源的MSISDN号码，若访问来源为非车主注册的号码，即为异常行为。

[0062] TSP平台的CA证书认证流程，部分车联网服务提供车载终端、手机APP到TSP的CA认证服务，通过对CA证书和认证过程中的服务端、客户端验证，识别CA服务流程是否为正常流程。当发现服务端或客户端异常或CA证书异常时，即判定为入侵行为。

[0063] 来自车联网终端的上行请求网络行为特征，车联网终端上行请求一般为上传行驶数据、车载传感器数据等，其频次、时间、车辆状态、请求类型、请求参数大小呈现规律性。当出现随机性请求时，判定为入侵攻击行为。

[0064] 在步骤S4中，对实时的车联网访问数据提取访问参数特征及访问行为特征，使用训练好的分类器模型进行判断是否遭遇到入侵攻击，并将入侵攻击行为进行相应处置，处置方式包括将入侵攻击行为进行存储、告警及数据过滤处置。

[0065] 进一步地，本发明还包括对训练好的模型进行迭代更新，形成新的模型，以不断适应各种网络攻击的模式。

[0066] 此外，本领域技术人员应理解，实现上述实施例方法中的部分或全部步骤是可以通过程序来指令相关的硬件来完成，所述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，包括上述实施例方法的相应步骤，而所述的存储介质可以是:ROM/RAM、磁碟、光盘、存储卡等。因此，如图2、图3所示，与上述方法相对应的，本发明还同时提供一种基

于人工智能行为分析的车联网入侵攻击检测系统，所述检测系统，部署在移动核心网与移动基站之间、移动核心网与TSP平台之间，通过移动基站，分别与车联网手机应用APP及网联车辆(即车载终端)进行交互。

[0067] 图2所示为本发明实施例中的所述检测系统与采集移动核心网数据的连接关系，以车载终端与TSP之间通信为例，当车载终端向TSP上报数据时，数据会通过移动基站，经过移动核心网各设备，经公网出口传输到TSP平台，当TSP平台向某一车载终端下发指令时，TSP平台通过终端编码(MSISDN)经过公网到移动核心网、无线网寻址到该终端，与之建立通信，此通信过程与普通移动终端与公众互联网服务进行通信的流程相同。所述检测系统在上述通信过程中以分光方式对经移动核心网传输的数据进行复制读取。

[0068] 所述车联网入侵攻击检测系统包括：

[0069] 数据采集单元，用于采集移动核心网数据并提取和合成车联网相关的数据流量话单；所述数据采集单元根据车联网手机APP、车载终端、TSP三者之间的互访，以及车载终端访问未知目的IP来确定数据流量话单。

[0070] 数据存储单元，用于存储正常访问的数据及入侵攻击的数据；

[0071] 特征提取单元，根据已知的车联网正常访问数据及异常的入侵攻击数据，提取访问参数特征及访问行为特征；

[0072] 模型训练单元，用于训练分类器模型，将已知为正常访问及入侵攻击的数据经过特征提取单元提取到的特征输入该训练单元，经过模型评估后得到训练好的分类器模型；

[0073] 数据检测单元，对实时数据提取特征后的特征进行判断，检测其是否被入侵或攻击，并将检测结果分别保存到数据存储单元当中。

[0074] 所述系统还包括：告警单元，当检测到对车辆的网络入侵攻击行为时，向车主或TSP服务商发送告警，并根据危险级别或车主设置对入侵攻击流量进行过滤处置。

[0075] 本发明中方法的实施例采用递进的方式描述，对于系统的实施例而言，由于其基本相似于方法的实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0076] 上述说明示出并描述了本发明的若干优选实施例，但如前所述，应当理解本发明并非局限于本文所披露的形式，不应看作是对其他实施例的排除，而可用于各种其他组合、修改和环境，并能够在本文所述发明构想范围内，通过上述教导或相关领域的技术或知识进行改动。而本领域人员所进行的改动和变化不脱离本发明的精神和范围，则都应在本发明所附权利要求的保护范围。

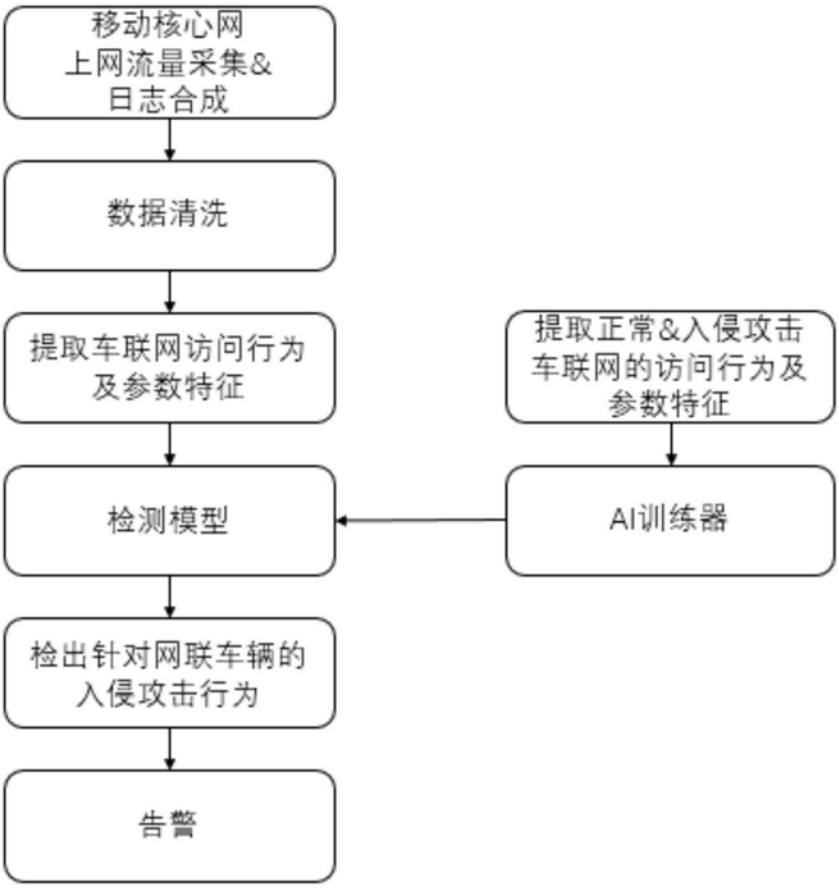

移动核心网
上网流量采集&
日志合成
数据清洗
提取车联网访问行为
及参数特征
提取正常&入侵攻击
车联网的访问行为及
参数特征
检测模型
AI训练器
检出针对网联车辆的
入侵攻击行为
告警

图1

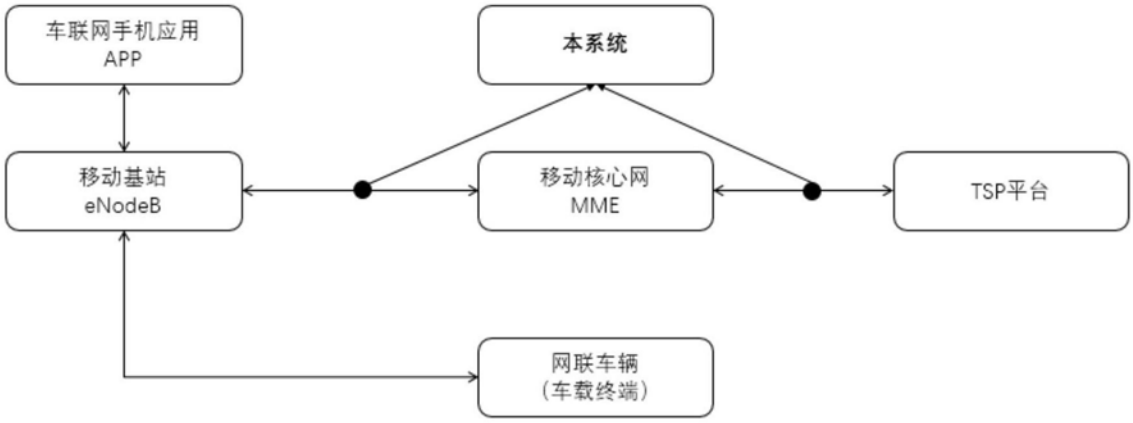

车联网手机应用
APP
本系统
移动基站
eNodeB
移动核心网
MME
TSP平台
网联车辆
(车载终端)

图2

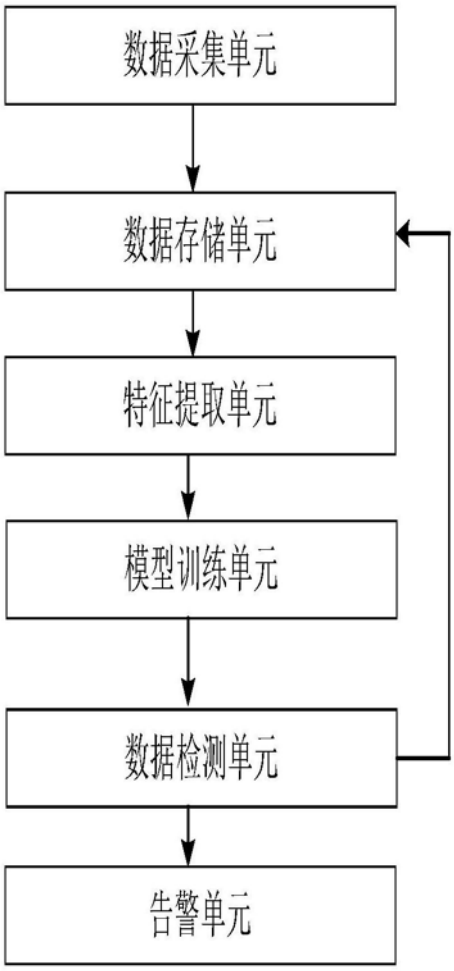


图3