(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 107454117 A
(43)申请公布日 2017.12.08

(21)申请号 201710939870.9

(22)申请日 2017.09.30

(71)申请人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号

(72)发明人 张曼君 马铮 张小梅 朱安南
高枫 唐磊 姜楠 俞播

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健

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

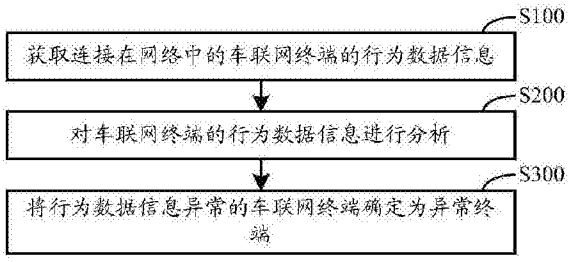
权利要求书2页 说明书7页 附图4页

(54)发明名称

一种车联网的入侵检测方法及系统

(57)摘要

本发明公开一种车联网的入侵检测方法及系统，涉及车联网技术领域，用于对车联网终端是否遭受入侵进行检测。所述车联网的入侵检测方法包括：获取连接在网络中的车联网终端的行为数据信息；对所述车联网终端的行为数据信息进行分析，将所述行为数据信息异常的所述车联网终端确定为异常终端。本发明提供的车联网的入侵检测方法通过在网络侧对车联网终端进行检测，以对车联网终端是否遭受入侵进行检测，本发明提供的车联网的入侵检测方法并不取决于车联网终端的操作者的水平和安全防范意识，且在车联网终端侧未安装安全软件等时也能对车联网终端是否遭受入侵进行检测，因而提高了对车联网终端是否遭受入侵进行检测的及时性。




CN 107454117 A

1.一种车联网的入侵检测方法，其特征在于，包括：

获取连接在网络中的车联网终端的行为数据信息；

对所述车联网终端的行为数据信息进行分析；

将所述行为数据信息异常的所述车联网终端确定为异常终端。

2.根据权利要求1所述的车联网的入侵检测方法，其特征在于，对所述车联网终端的行为数据信息进行分析，包括：

分析所述行为数据信息的数据流量；

判定所述行为数据信息的数据流量是否异常。

3.根据权利要求2所述的车联网的入侵检测方法，其特征在于，

对所述车联网终端的行为数据信息进行分析，还包括：

当所述行为数据信息的数据流量异常时，分析所述行为数据信息的数据流向，判定所述车联网终端的行为类型；

根据恶意攻击类型情报库与所述车联网终端的行为类型，确定所述车联网终端遭受恶意攻击的类型。

4.根据权利要求3所述的车联网的入侵检测方法，其特征在于，获取连接在网络中的车联网终端的行为数据信息之前，所述车联网的入侵检测方法还包括：

建立所述恶意攻击类型情报库。

5.根据权利要求1所述的车联网的入侵检测方法，其特征在于，将所述行为数据信息异常的所述车联网终端确定为异常终端之后，所述车联网的入侵检测方法还包括：

根据异常的所述行为数据信息的数据流向，追踪造成所述异常终端的行为数据信息异常的源头终端，确定所述源头终端为异常终端。

6.根据权利要求1或5所述的车联网的入侵检测方法，其特征在于，所述车联网的入侵检测方法还包括：

对所述异常终端进行处理，并通知所述异常终端；其中，对所述异常终端的处理为：对所述异常终端的固件进行更新、对所述异常终端警告、限制所述异常终端的数据流量或终止对所述异常终端的服务。

7.根据权利要求1或5所述的车联网的入侵检测方法，其特征在于，所述车联网的入侵检测方法还包括：

将所述异常终端在所述网络中的标识号添加至黑名单库。

8.一种车联网的入侵检测系统，其特征在于，包括处理器，所述处理器用于获取连接在网络中的车联网终端的行为数据信息，并对所述车联网终端的行为数据信息进行分析，将所述行为数据信息异常的所述车联网终端确定为异常终端。

9.根据权利要求8所述的车联网的入侵检测系统，其特征在于，所述处理器对所述车联网终端的行为数据信息进行分析包括：

所述处理器分析所述行为数据信息的数据流量，并判定所述行为数据信息的数据流量是否异常；

当所述车联网终端的行为数据信息的数据流量异常时，所述处理器分析所述行为数据信息的数据流向，并判定所述车联网终端的行为类型；所述处理器根据恶意攻击类型情报库与所述车联网终端的行为类型，确定所述车联网终端遭受恶意攻击的类型。

10.根据权利要求9所述的车联网的入侵检测系统，其特征在于，所述处理器还用于建立所述恶意攻击类型情报库、将所述异常终端在所述网络中的标识号添加至黑名单库。

11.根据权利要求8所述的车联网的入侵检测系统，其特征在于，所述处理器还用于根据异常的所述行为数据信息的数据流向，追踪造成所述异常终端的行为数据信息异常的源头终端，确定所述源头终端为异常终端。

12.根据权利要求8或11所述的车联网的入侵检测系统，其特征在于，所述处理器还用于对所述异常终端进行处理，并通知所述异常终端；其中，对所述异常终端的处理为：对所述异常终端的固件进行更新、对所述异常终端警告、限制所述异常终端的数据流量或终止对所述异常终端的服务。

# 一种车联网的入侵检测方法及系统

## 技术领域

[0001] 本发明涉及车联网技术领域，尤其涉及一种车联网的入侵检测方法及系统。

## 背景技术

[0002] 随着网络技术以及智能车辆技术的发展，车联网越来越受到广泛的关注，车联网将车辆作为一种车联网终端，是一种通过车联网终端与网络之间的协同通信，实现提高交通安全、优化交通效率、方便交通管理的技术。在车联网中，车联网终端需要保持网络连接和数据传输，同时车联网对于传输宽带和传输速率等有较高的要求，因而造成车联网终端容易遭受恶意攻击，即车联网终端遭受入侵。

[0003] 为了检测车联网终端是否遭受入侵，通常在车联网终端安装安全软件，通过安全软件对入侵行为进行查杀，以达到对车联网终端是否遭受入侵进行检测的目的。然而，利用安装在车联网终端的安全软件来检测车联网终端是否遭受入侵时，往往取决于车联网终端的操作者的水平和安全防范意识，因此，采用在车联网终端安装安全软件的方式并不能达到及时对车联网终端是否遭受入侵进行检测的效果。

## 发明内容

[0004] 本发明的目的在于提供一种车联网的入侵检测方法及系统，用于对车联网终端是否遭受入侵进行检测。

[0005] 为了实现上述目的，本发明提供如下技术方案：

[0006] 第一方面，本发明提供一种车联网的入侵检测方法，包括：

[0007] 获取连接在网络中的车联网终端的行为数据信息；

[0008] 对所述车联网终端的行为数据信息进行分析；

[0009] 将所述行为数据信息异常的所述车联网终端确定为异常终端。

[0010] 第二方面，本发明提供一种车联网的入侵检测系统，包括处理器，所述处理器用于获取连接在网络中的车联网终端的行为数据信息，并对所述车联网终端的行为数据信息进行分析，将所述行为数据信息异常的所述车联网终端确定为异常终端。

[0011] 本发明提供的车联网的入侵检测方法中，通过对连接在网络中的车联网终端的行为数据信息进行获取，并对获取得到的车联网终端的行为数据信息进行分析，以确认车联网终端的行为数据信息是否有异常，以便确认车联网终端是否异常，进而检测车联网终端是否遭受入侵，当发现某车联网终端的行为数据信息异常时，则表明该车联网终端极有可能遭受入侵，则将该车联网终端确定为异常终端。因此，本发明提供的车联网的入侵检测方法通过在网络侧对车联网终端进行检测，以对车联网终端是否遭受入侵进行检测，与现有技术相比，本发明提供的车联网的入侵检测方法并不取决于车联网终端的操作者的水平和安全防范意识，甚至在车联网终端侧没有安装安全软件等的情况下也能对车联网终端是否遭受入侵或恶意攻击进行检测，因而提高了对车联网终端是否遭受入侵进行检测的及时性。

## 附图说明

[0012] 此处所说明的附图用来提供对本发明的进一步理解，构成本发明的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0013] 图1为本发明实施例提供的车联网的入侵检测方法的流程图一；

[0014] 图2为本发明实施例提供的车联网的入侵检测方法的流程图二；

[0015] 图3为本发明实施例提供的车联网的入侵检测方法的流程图三；

[0016] 图4为本发明实施例提供的车联网的入侵检测方法的流程图四；

[0017] 图5为本发明实施例提供的车联网的入侵检测系统的结构示意图。

[0018] 附图标记：

[0019] 10-处理器，11-分光器，

[0020] 12-数据分析单元，121-数据流量判定模块，

[0021] 122-行为类型判定模块，123-恶意攻击类型确定模块，

[0022] 13-行为类型判定单元，14-恶意攻击类型情报库建立单元，

[0023] 15-黑名单库建立单元，16-存储器，

[0024] 17-恶意攻击源头追踪单元，18-异常处置单元，

[0025] 20-车联网终端，30-GGSN，

[0026] 40-网络，50-网络管理平台。

## 具体实施方式

[0027] 为了进一步说明本发明实施例提供的车联网的入侵检测方法及系统，下面结合说明书附图进行详细描述。

[0028] 请参阅图1，本发明实施例提供的车联网的入侵检测方法包括：

[0029] 步骤S100、获取连接在网络中的车联网终端的行为数据信息。

[0030] 步骤S200、对车联网终端的行为数据信息进行分析。

[0031] 步骤S300、将行为数据信息异常的车联网终端确定为异常终端。

[0032] 举例来说，网络中包括多个网关GPRS支持节点(Gateway GPRS Support Node，GGSN)，车联网终端通过其中一个GGSN连接在网络中，每个车联网终端通过其中一个GGSN连接在网络中时，网络管理平台则给车联网终端下发一个标识号，例如IP地址。当检测车联网终端是否遭受入侵时，即当检测车联网终端是否异常时，请继续参阅图1，先获取连接在网络中的车联网终端的行为数据信息，其中，获取连接在网络中的车联网终端的行为数据信息可以采用多种方式，例如，可以在每个GGSN上安装分光器，通过分光器获取通过对应的GGSN连接在网络中的车联网终端的行为数据信息，车联网终端的行为数据信息可以包括行为类型(如接收文件、发送文件等)、数据流量、数据流向等；完成车联网终端的行为数据信息的获取后，则对车联网终端的行为数据信息进行分析，以确认车联网终端的行为数据信息是否有异常，以便确认车联网终端是否异常，进而确认车联网终端是否遭受恶意攻击，即进而确认车联网终端是否遭受入侵，实现对车联网终端是否遭受入侵进行检测，其中，当发现某车联网终端的行为数据信息异常时，则表明该车联网终端遭受入侵，则将该车联网终端确定为异常终端。

[0033] 根据上述分析可知，在本发明实施例提供的车联网的入侵检测方法中，通过对连接在网络中的车联网终端的行为数据信息进行获取，并对获取得到的车联网终端的行为数据信息进行分析，以确认车联网终端的行为数据信息是否有异常，以便确认车联网终端是否异常，进而检测车联网终端是否遭受入侵，当发现某车联网终端的行为数据信息异常时，则表明该车联网终端极有可能遭受入侵，则将该车联网终端确定为异常终端。因此，本发明实施例提供的车联网的入侵检测方法通过在网络侧对车联网终端进行检测，以对车联网终端是否遭受入侵进行检测，与现有技术相比，本发明实施例提供的车联网的入侵检测方法并不取决于车联网终端的操作者的水平和安全防范意识，甚至在车联网终端侧没有安装安全软件等的情况下也能对车联网终端是否遭受入侵或恶意攻击进行检测，因而提高了对车联网终端是否遭受入侵进行检测的及时性。

[0034] 请参阅图2，在上述实施例中，步骤S200中，对车联网终端的行为数据信息进行分析可以包括：

[0035] 步骤S210、分析行为数据信息的数据流量。

[0036] 步骤S220、判定行为数据信息的数据流量是否异常。

[0037] 举例来说，分析行为数据信息的数据流量时，可以分析车联网终端在获取得到的该车联网终端行为数据信息中总的数据流量，也可以分析车联网终端在单位时间内所使用的数据流量，也可以分析车联网终端在一定时间内所使用的数据流量。完成对行为数据信息的数据流量的分析后，则对行为数据信息的数据流量是否出现异常进行判定，此时，对行为数据信息的数据流量是否出现异常进行判定时的方式有多种，例如，可以将车联网终端的行为数据信息中单位时间内所使用的数据流量与该车联网终端的历史单位时间数据流量进行比较，当车联网终端的行为数据信息中单位时间内所使用的数据流量超过该车联网终端的历史单位时间数据流量的一定倍数时，如车联网终端的行为数据信息中单位时间内所使用的数据流量超过该车联网终端的历史单位时间数据流量的1.5倍及1.5倍以上时，则表明该车联网终端的行为数据信息中数据流量异常，此时，该车联网终端的行为数据信息异常；或者，可以将车联网终端的行为数据信息中单位时间内所使用的数据流量与根据历史调查获取得到的所有车联网终端的平均单位时间数据流量进行比较，当车联网终端的行为数据信息中单位时间内所使用的数据流量超出根据历史调查获取得到的所有车联网终端的平均单位时间数据流量的一定倍数时，如车联网终端的行为数据信息中单位时间内所使用的数据流量超出根据历史调查获取得到的所有车联网终端的平均单位时间数据流量的1.5倍及1.5倍以上时，则表明该车联网终端的行为数据信息中数据流量异常，此时，该车联网终端的行为数据信息异常。当判定得知车联网终端的行为数据信息的数据流量异常时，则该车联网终端的行为数据信息也为异常，表明该车联网终端异常，该车联网终端极有可能遭受入侵。

[0038] 请继续参阅图3，在上述实施例中，当在步骤S220、判定行为数据信息的数据流量是否异常中，确认该车联网终端的行为数据信息中数据流量异常时，步骤S200中，对车联网终端的行为数据信息进行分析还可以包括：

[0039] 步骤S230、当行为数据信息中的数据流量异常时，分析行为数据信息的数据流向，判定车联网终端的行为类型。

[0040] 步骤S240、根据恶意攻击类型情报库与车联网终端的行为类型，确定车联网终端

遭受恶意攻击的类型。

[0041] 具体地，当在步骤S220、判定行为数据信息的数据流量是否异常中，确认该车联网终端的行为数据信息中数据流量异常时，则对行为数据信息的数据流向进行分析，例如对车联网终端所使用的数据流量是用于向外界发送文件还是用于接收外界向该车联网终端发送的文件进行分析，以判断车联网终端的行为类型，当车联网终端所使用的数据流量是用于向外界发送文件时，表明车联网终端的行为类型为发送文件，当车联网终端所使用的数据流量是用于接收外界向该车联网终端发送的文件时，表明车联网终端的行为类型为接收文件。

[0042] 完成对车联网终端的行为类型的判定后，将车联网终端的行为类型与恶意攻击类型情报库中各种恶意攻击类型的特征进行匹配，以确定车联网终端遭受恶意攻击的类型，也可以理解为确定车联网终端遭受入侵的类型，即车联网终端遭受何种类型的恶意程序或病毒入侵，其中，恶意攻击类型情报库中包括恶意程序特征库、病毒特征库(如僵尸、木马、蠕虫等)等，每一种恶意程序对应有特定的特征，每一种恶意程序的特征与车联网终端被对应的恶意程序入侵后产生的行为类型对应，每一种病毒也对应有特定的特征，每一种病毒的特征与车联网终端被对应的病毒入侵后产生的行为类型对应，从而可以根据数据流量异常的车联网终端的行为类型，判定车联网终端遭受恶意攻击的类型，从而方便后续对遭受恶意攻击的车联网终端采取对应的处置办法。

[0043] 当车联网终端的行为数据信息中数据流量异常时，分析行为数据信息中的数据流向，以判定车联网终端的行为类型，然后根据车联网终端的行为类型和恶意攻击类型情报库，确定车联网终端遭受恶意攻击的类型，以进一步确定车联网终端是否遭受入侵，并确定车联网终端遭受何种恶意程序或病毒的恶意攻击或入侵，如此设计，可以提高对车联网终端是否遭受入侵进行检测时的准确性，防止对车联网终端是否遭受入侵的误判，同时还可以确定车联网终端遭受何种恶意程序或病毒的恶意攻击或入侵，从而方便后续对遭受恶意攻击的车联网终端采取对应的处置办法。

[0044] 值得一提的是，请参阅图2，步骤S200中，对车联网终端的行为数据信息进行分析，可以包括步骤S210、步骤S220，此时，当步骤S220、判定行为数据信息的数据流量是否异常中，确认该车联网终端的数据流量异常时，即车联网终端的行为数据信息发生异常，则将该车联网终端确定为异常终端。

[0045] 或者，请参阅图3，步骤S200中，对车联网终端的行为数据信息进行分析，可以包括步骤S210、步骤S220、步骤S230、步骤S240，此时，当步骤S220、判定行为数据信息的数据流量是否异常中，确认该车联网终端的数据流量异常时，则执行步骤S230、分析行为数据信息的数据流向，判定车联网终端的行为类型，然后，执行步骤S240、根据恶意攻击类型情报库与车联网终端的行为类型，确定车联网终端遭受恶意攻击的类型。

[0046] 请继续参阅图3，在步骤S100、获取连接在网络中的车联网终端的行为数据信息之前，本发明实施例提供的车联网的入侵检测方法还包括：

[0047] 步骤S10、建立恶意攻击类型情报库。

[0048] 恶意攻击类型情报库中包括恶意程序特征库、病毒特征库(如僵尸、木马、蠕虫等)等，恶意程序特征库包括恶意程序类型及其对应的特征，病毒特征库包括病毒类型及其对应的特征，需要说明的是，恶意攻击类型情报库需要进行不定时的更新，以将新出现的恶意

程序或病毒及相应的特征添加至恶意攻击类型情报库，以便后续对车联网终端是否遭受入侵进行检测。

[0049] 值得一提的是，在本发明实施例提供的车联网的入侵检测方法中，还可以通过网络管理平台触发车联网终端固件更新，例如，更新车联网终端的操控系统、安全软件等，以加强车联网终端本身对恶意程序或病毒的查杀力度，进一步对车联网终端是否遭受入侵进行检测，并防范车联网终端遭受入侵。

[0050] 请参阅图4，步骤S300、将行为数据信息异常的车联网终端确定为异常终端之后，本发明实施例提供的车联网的入侵检测方法还可以包括：

[0051] 步骤S400、根据异常的行为数据信息的数据流向，追踪造成异常终端的行为数据信息异常的源头终端，确定源头终端为异常终端。

[0052] 对车联网终端的行为数据信息分析后得知，车联网终端的行为数据信息异常时，表明该车联网终端遭受入侵，确认该车联网终端为异常终端，此时，对异常的车联网终端的行为数据信息的数据流向进行分析，并根据异常的车联网终端的行为数据信息的数据流向，即根据异常的行为数据信息的数据流向，追踪造成异常终端的行为数据信息异常的源头终端，即追踪使异常终端遭受恶意程序或病毒入侵的源头终端，也可以理解为追踪恶意程序或病毒的来源，并将源头终端确定为异常终端。如此设计，可以防止车联网终端成为攻击者手中的武器而造成对网络或其它车联网终端发起恶意攻击。

[0053] 在上述实施例中，当检测出异常终端后，请参阅图4，本发明实施例提供的车联网的入侵检测方法还包括：

[0054] 步骤S500、对异常终端进行处理，并通知异常终端。

[0055] 其中，对异常终端进行处理时，可以对异常终端的固件进行更新，以提高异常终端自身的防范能力；或者，可以对异常终端警告，以提醒异常终端进行恶意程序或病毒的查杀；或者，结合网络管理平台及网络中的防火墙，限制异常终端的数据流量，以防止异常终端中的大量数据被窃取或防止异常终端窃取其它车联网终端中的大量数据；或者，结合网络管理平台及网络中的防火墙，终止对异常终端的服务，以防止异常的行为数据信息中的行为内容扩散至其它车联网终端以及网络。对异常终端进行处理包括上述方式，但不限于上述方式，在此不一一列举。

[0056] 请参阅图4，本发明实施例提供的车联网的入侵检测方法还可以包括：

[0057] 步骤S600、将异常终端在网络中的标识号添加至黑名单库。

[0058] 具体地，当完成步骤S300、将行为数据信息异常的车联网终端确定为异常终端之后，则将该异常终端在网络中的标识号添加至黑名单库中，即将行为数据信息异常的车联网终端在网络中的标识号添加至黑名单库中；当完成步骤S400、根据异常的行为数据信息的数据流向，追踪造成异常终端的行为数据信息异常的源头终端，确定源头终端为异常终端之后，则将该异常终端在网络中的标识号添加至黑名单库中，即将造成异常终端的行为数据信息异常的源头终端在网络中的标识号添加至黑名单库中。将异常终端在网络中的标识号添加至黑名单库，即将遭受过恶意攻击或入侵的车联网终端在网络中的标识号添加至黑名单库，在后续对车联网的入侵检测方法中，可以着重检测黑名单库中标识号对应的车联网终端，防止这些车联网终端再次遭受恶意攻击或入侵，并防止这些车联网终端再次成为攻击者的武器对网络或其它车联网终端造成恶意攻击或入侵。

[0059] 请参阅图5，本发明实施例还提供一种车联网的入侵检测系统，应用上述实施例所述的车联网的入侵检测方法，所述车联网的入侵检测系统包括处理器10，处理器用于获取连接在网络40中的车联网终端20的行为数据信息，并对车联网终端20的行为数据信息进行分析，将行为数据信息异常的车联网终端20确定为异常终端。

[0060] 具体地，请继续参阅图5，处理器10可以包括数据采集单元、数据分析单元12和异常确定单元13，其中，数据采集单元可以为安装在GGSN30上的分光器11，通过分光器11获取通过对应的GGSN30连接在网络40中的车联网终端20的行为数据信息，然后通过数据分析单元12对获取得到的连接在网络40中的车联网终端20的行为数据信息进行分析，通过异常确定单元13将行为数据信息异常的车联网终端20确定为异常终端。

[0061] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。

[0062] 在本发明实施例中，处理器10对车联网终端20的行为数据信息进行分析可以包括：处理器10分析行为数据信息中的数据流量，并判定行为数据信息的数据流量是否异常；当车联网终端20的行为数据信息中的数据流量异常时，处理器10分析行为数据信息的数据流向，并判定车联网终端的行为类型；处理器10根据恶意攻击类型情报库与车联网终端的行为类型，确定车联网终端遭受恶意攻击的类型。处理器10还用于建立攻击类型情报库。

[0063] 具体地，请参阅图5，处理器10中数据分析单元12可以包括数据流量判定模块121、行为类型判定模块122和恶意攻击类型确定模块123，处理器10还包括恶意攻击类型情报库建立单元14和存储器16。其中，恶意攻击类型情报库建立单元14用于建立恶意攻击类型情报库，恶意攻击类型情报库存储在存储器16中；当处理器10中数据分析单元12分析车联网终端的行为数据信息时，数据流量判定模块121则分析行为数据信息的数据流量，并判定行为数据信息的数据流量是否异常；当数据流量判定模块121判定得知行为数据信息的数据流量异常时，行为类型判定模块122则分析行为数据信息的数据流向，并判定车联网终端的行为类型，恶意攻击类型确定模块123则根据行为类型判定模块122判定得知的车联网终端的行为类型，以及由恶意攻击类型情报库建立单元14建立并存储在存储器16中的恶意攻击类型情报库，确定车联网终端遭受恶意攻击的类型。

[0064] 在本发明实施例中，处理器10还用于将异常终端在网络中的标识号添加至黑名单库。具体地，请参阅图5，处理器10还包括黑名单建立单元15，异常确定单元13将行为数据信息异常的车联网终端20确定为异常终端后，黑名单建立单元15将该异常终端在网络中的标识号添加至黑名单库，黑名单库存储在存储器16中。

[0065] 在本发明实施例中，处理器10还用于根据异常的行为数据信息的数据流向，追踪造成异常终端的行为数据信息异常的源头终端，确定源头终端为异常终端。具体地，请参阅图5，处理器10还包括恶意攻击源头追踪单元17，恶意攻击源头追踪单元17根据异常的行为数据信息的数据流向，追踪获得造成异常终端的行为数据信息异常的源头终端，异常确定单元13则确定该源头终端为异常终端，黑名单建立单元15将该异常终端在网络中的标识号添加至黑名单库。

[0066] 在本发明实施例中，处理器10还用于对异常终端进行处理，并通知异常终端；其

中，对异常终端的处理为：对异常终端的安全软件中的恶意程序特征库进行更新、对异常终端警告、限制异常终端的数据流量或终止对异常终端的服务。具体地，请参阅图5，处理器10还包括异常处置单元18，异常处置单元18对异常确定单元13确定的异常终端进行处理，并通知异常终端，其中，对异常终端的处理可以为：对异常终端的固件进行更新，或者，对异常终端进行警告，或者，结合防火墙、网络管理平台50限制异常终端的数据流量，或者，结合防火墙、网络管理平台50终止对异常终端的服务。

[0067] 以上所述，仅为本发明的具体实施方式，但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内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

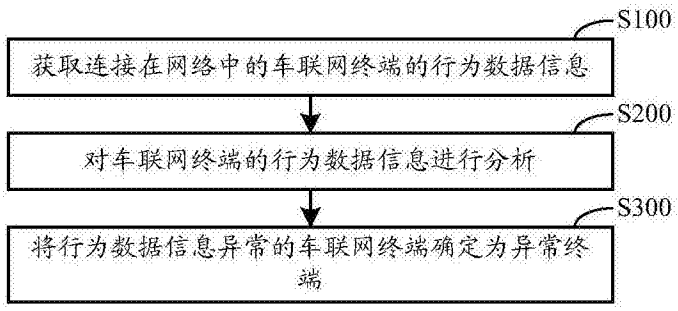

S100
获取连接在网络中的车联网终端的行为数据信息
S200
对车联网终端的行为数据信息进行分析
S300
将行为数据信息异常的车联网终端确定为异常终端

图1

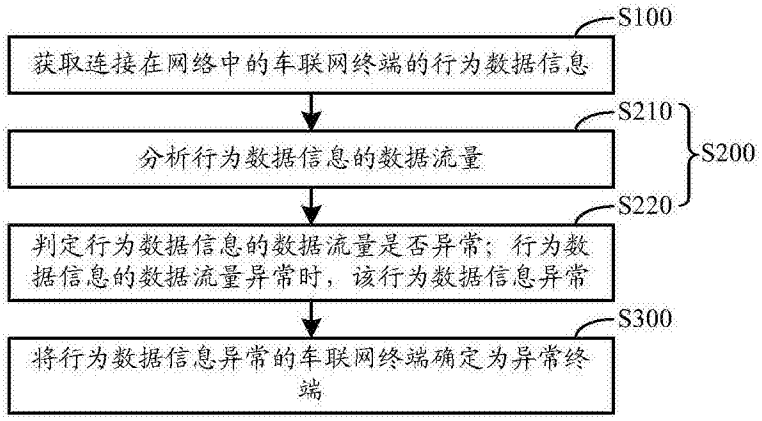

S100
获取连接在网络中的车联网终端的行为数据信息
S210
分析行为数据信息的数据流量
S200
S220
判定行为数据信息的数据流量是否异常；行为数据信息的数据流量异常时，该行为数据信息异常
S300
将行为数据信息异常的车联网终端确定为异常终端

图2

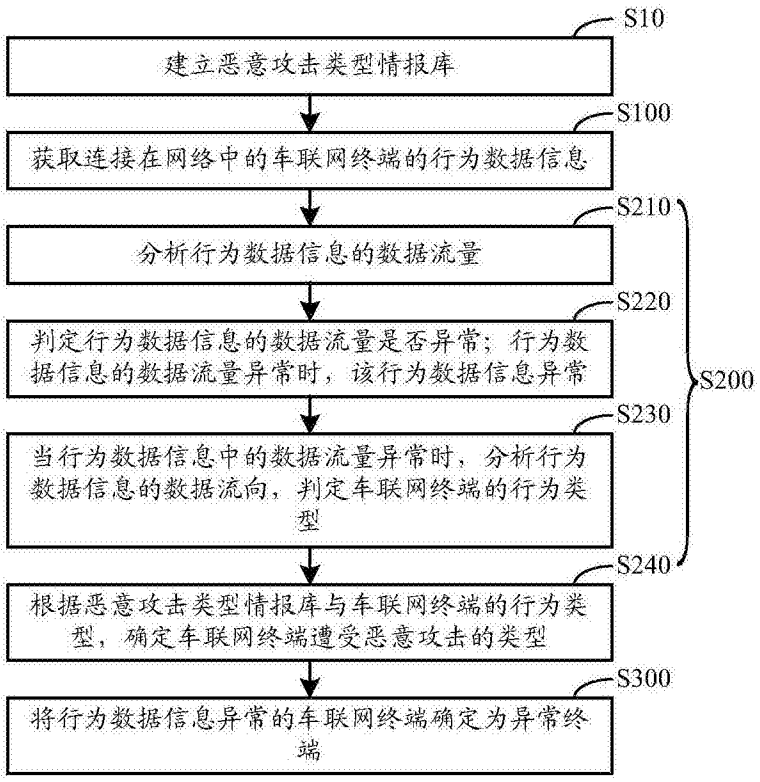

S10
建立恶意攻击类型情报库
S100
获取连接在网络中的车联网终端的行为数据信息
S210
分析行为数据信息的数据流量
S220
判定行为数据信息的数据流量是否异常；行为数据信息的数据流量异常时，该行为数据信息异常
S230
当行为数据信息中的数据流量异常时，分析行为数据信息的数据流向，判定车联网终端的行为类型
S240
根据恶意攻击类型情报库与车联网终端的行为类型，确定车联网终端遭受恶意攻击的类型
S300
将行为数据信息异常的车联网终端确定为异常终端
S200

图3

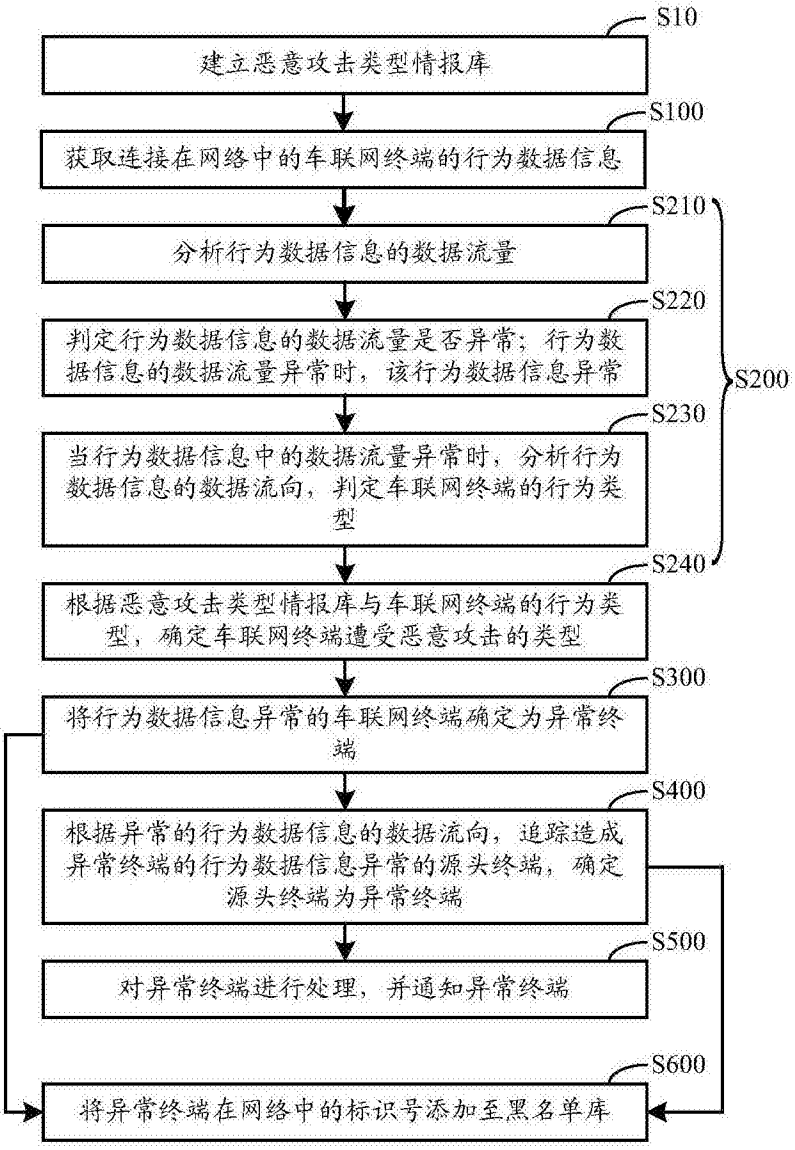

S10
建立恶意攻击类型情报库
S100
获取连接在网络中的车联网终端的行为数据信息
S210
分析行为数据信息的数据流量
S220
判定行为数据信息的数据流量是否异常；行为数据信息的数据流量异常时，该行为数据信息异常
S230
当行为数据信息中的数据流量异常时，分析行为数据信息的数据流向，判定车联网终端的行为类型
S200
S240
根据恶意攻击类型情报库与车联网终端的行为类型，确定车联网终端遭受恶意攻击的类型
S300
将行为数据信息异常的车联网终端确定为异常终端
S400
根据异常的行为数据信息的数据流向，追踪造成异常终端的行为数据信息异常的源头终端，确定源头终端为异常终端
S500
对异常终端进行处理，并通知异常终端
S600
将异常终端在网络中的标识号添加至黑名单库

图4

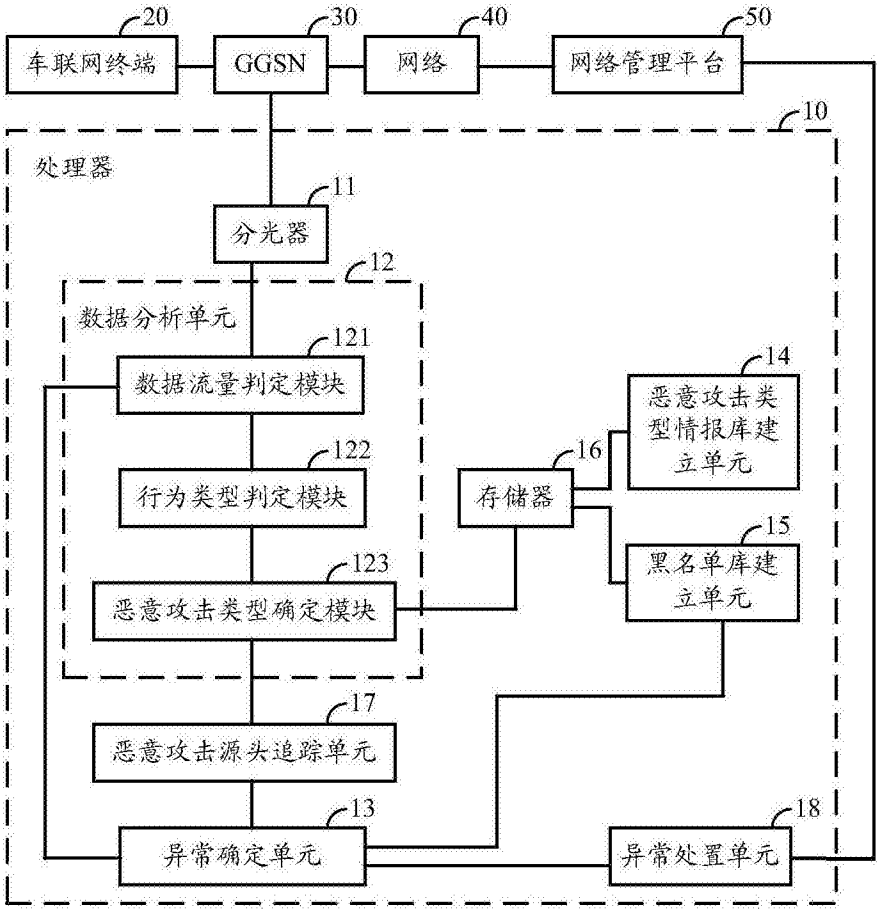

20
车联网终端
30
GGSN
40
网络
50
网络管理平台
10
处理器
11
分光器
12
数据分析单元
121
数据流量判定模块
122
行为类型判定模块
123
恶意攻击类型确定模块
14
恶意攻击类型情报库建立单元
16
存储器
15
黑名单库建立单元
17
恶意攻击源头追踪单元
13
异常确定单元
18
异常处置单元

图5