(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115803737 A
(43)申请公布日 2023.03.14

(21)申请号 202180048919.6
(22)申请日 2021.06.03
(30)优先权数据
2020-120721 2020.07.14 JP
(85)PCT国际申请进入国家阶段日
2023.01.09
(86)PCT国际申请的申请数据
PCT/JP2021/021285 2021.06.03
(87)PCT国际申请的公布数据
WO2022/014193 JA 2022.01.20
(71)申请人 株式会社电装
地址 日本爱知县
(72)发明人 菅岛健司 江川万寿三
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 郜琳琳
(51)Int.Cl.
G06F 21/55(2006.01)

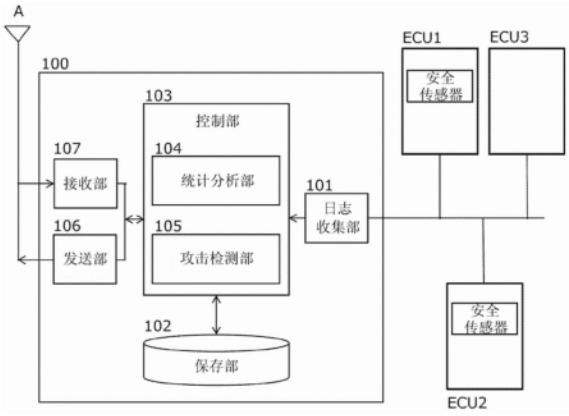
权利要求书2页 说明书10页 附图6页

(54)发明名称

日志管理装置以及安全攻击检测/分析系统

(57)摘要

本发明提供一种日志管理装置以及安全攻击检测/分析系统。日志管理装置(100)具有:日志收集部(101),接收安全传感器生成的日志;保存部(102),保存上述日志;统计分析部(104),通过进行多个上述日志的统计分析来求出统计计算结果;以及发送部(106),根据规定条件来发送上述日志或者上述统计计算结果。



CN 115803737 A

1.一种日志管理装置(100),具有:

日志收集部(101),接收安全传感器生成的日志;

保存部(102),保存上述日志;

统计分析部(104),通过进行多个上述日志的统计分析来求出统计计算结果;以及

发送部(106),根据规定条件来发送上述日志或者上述统计计算结果。

2.根据权利要求1所述的日志管理装置,其中,

还具有攻击检测部(105),上述攻击检测部基于上述日志来进行攻击检测,

在攻击检测为规定次数以上的情况下,上述统计分析部通过进行统计分析来求出统计计算结果。

3.根据权利要求1所述的日志管理装置,其中,

还具有攻击检测部(105),上述攻击检测部基于上述日志来进行攻击检测,

上述规定条件为攻击检测的次数。

4.根据权利要求3所述的日志管理装置,其中,

在上述攻击检测为规定次数以下的情况下,上述发送部将上述日志发送至中心装置,

在上述攻击检测为规定次数以上的情况下,上述发送部等待来自上述中心装置的上传请求而将上述统计计算结果发送至上述中心装置。

5.根据权利要求3所述的日志管理装置,其中,

能够根据上述安全传感器的设置场所或者连接有上述安全传感器的通信总线的重要度,来设定作为规定条件的攻击检测的次数。

6.根据权利要求1所述的日志管理装置,其中,

还具有接收部(107),上述接收部从上述中心装置接收上传请求,其中,上述上传请求是请求上传上述日志或者上述统计计算结果的请求,

上述规定条件为上述上传请求。

7.根据权利要求6所述的日志管理装置,其中,

上述规定条件除了上述上传请求外,还为上述日志的量。

8.根据权利要求7所述的日志管理装置,其中,

在上述日志的量为规定量以下的情况下,上述发送部将上述日志发送至中心装置,

在上述日志的量为规定量以上的情况下,上述发送部将上述统计计算结果发送至上述中心装置。

9.根据权利要求6所述的日志管理装置,其中,

在经过无法发送上述日志或者上述统计计算结果的情况而成为能够发送的情况下,上述发送部根据最新的上述上传请求来发送上述日志或者上述统计计算结果。

10.根据权利要求1～9中任一项所述的日志管理装置,其中,

该日志管理装置搭载于移动体。

11.一种日志管理方法,是由日志管理装置执行的日志管理方法,

接收安全传感器生成的日志,

保存上述日志,

通过进行多个上述日志的统计分析来求出统计计算结果,

根据规定条件来发送上述日志或者上述统计计算结果。

12.一种日志管理程序,是能够由日志管理装置执行的日志管理程序,

接收安全传感器生成的日志,

保存上述日志,

通过进行多个上述日志的统计分析来求出统计计算结果,

根据规定条件来发送上述日志或者上述统计计算结果。

13.一种安全攻击检测/分析系统(1),是包含日志管理装置(100)和中心装置(200)的安全攻击检测/分析系统(1),

上述日志管理装置具有:

日志收集部(101),接收安全传感器生成的日志;

保存部(102),保存上述日志;

统计分析部(104),通过进行多个上述日志的统计分析来求出统计计算结果;以及

发送部(106),根据规定条件来发送上述日志或者上述统计计算结果,

上述中心装置具有:

接收部(201),接收上述日志或者上述统计计算结果;

分析部(203),分析上述日志或者上述统计计算结果,并且基于分析结果来生成上传请求,其中,上述上传请求是请求上传追加的日志或者追加的统计计算结果的请求;

发送部(205),对上述日志管理装置发送上述上传请求。

14.根据权利要求13所述的安全攻击检测/分析系统,其中,

上述日志管理装置搭载于移动体,

上述中心装置的发送部对上述移动体的上述日志管理装置和/或搭载于同类型的其他移动体的日志管理装置发送上述上传请求。

日志管理装置以及安全攻击检测/分析系统

[0001] 相关申请的交叉引用

[0002] 本申请基于2020年7月14日申请的日本专利申请号2020－120721号，在此引用其记载内容。

技术领域

[0003] 本申请涉及检测/分析网络(cyber)攻击的系统，主要涉及包含搭载于移动体的日志管理装置和设置于移动体的外部的中心装置的安全攻击检测/分析系统。

背景技术

[0004] 近年来，以车间通信、路车间通信那样的V2X为首，进行驾驶辅助、自动驾驶控制的技术受到瞩目。伴随于此，车辆具备通信功能，所谓的车辆的联网化不断发展。其结果是，车辆受到网络攻击的可能性增加。由于车辆高速移动，因此存在伴随着网络攻击而失去车辆的控制的可能性，因此对于网络攻击需要更稳固的防御手段。

[0005] 在这里，在计算机系统领域，以往就采取针对网络攻击的对策。

[0006] 例如，在专利文献1中，记载有决定是否需要输出安全日志的日志输出装置等。

[0007] 专利文献1：日本特开2020－38439号公报

[0008] 在这里，本发明人发现了以下的课题。

[0009] 在搭载于作为移动体的车辆的电子控制装置(ECU)中搭载有安全传感器，安全传感器监视ECU本身、ECU的通信并输出安全日志。在通过中心装置进行该安全日志的分析的情况下，若将所有的安全日志上传至中心装置，则通信量增大。

[0010] 另外，一般而言，中心装置的处理能力高于搭载于车辆的电子控制装置的处理能力。因此，存在即使搭载于车辆的电子控制装置无法进行异常检测，但若是中心装置则能够进行异常检测的情况。

[0011] 进一步，即使在通过中心装置进行异常检测的情况下，也存在安全日志等信息不充分的情况。在该情况下，若能够从该车辆、同类型的车辆得到追加的信息，则能够进行更正确的异常检测，并且能够进行针对多个车辆的分析。

发明内容

[0012] 本公开的目的在于实现能够削减与中心装置的通信量，并且削减中心装置的处理量的日志管理装置。

[0013] 另外，本公开的目的在于实现能够通过中心装置进行攻击分析，并且收集必要的信息的中心装置。

[0014] 此外，上述课题举出将日志管理装置搭载于车辆的情况为例，但这作为课题的一个例子记载。在日志管理装置未搭载于车辆的情况下，也可能产生通信量的增大、各单元、实体中的处理量的适当的分配这样的课题。

[0015] 本公开的一个方式的日志管理装置具有：日志收集部，接收安全传感器生成的日

志;保存部,保存上述日志;统计分析部,通过进行多个上述日志的统计分析来求出统计计算结果;以及发送部,根据规定条件来发送上述日志或者上述统计计算结果。

[0016] 本公开的另一个方式的日志管理方法是由日志管理装置执行的日志管理方法,接收安全传感器生成的日志,保存上述日志,通过进行多个上述日志的统计分析来求出统计计算结果,根据规定条件来发送上述日志或者上述统计计算结果。

[0017] 本公开的另一个方式的日志管理程序是能够由日志管理装置执行的日志管理程序,接收安全传感器生成的日志,保存上述日志,通过进行多个上述日志的统计分析来求出统计计算结果,根据规定条件来发送上述日志或者上述统计计算结果。

[0018] 本公开的另一个方式的安全攻击检测/分析系统是包含日志管理装置和中心装置的安全攻击检测/分析系统,上述日志管理装置具有:日志收集部,接收安全传感器生成的日志;保存部,保存上述日志;统计分析部,通过进行多个上述日志的统计分析来求出统计计算结果;以及发送部,根据规定条件来发送上述日志或者上述统计计算结果,上述中心装置具有:接收部,接收上述日志或者上述统计计算结果;分析部,分析上述日志或者上述统计计算结果,并且基于分析结果来生成上传请求,其中,上述上传请求是请求上传追加的日志或者追加的统计计算结果的请求;以及发送部,对上述日志管理装置发送上述上传请求。

[0019] 此外,权利请求书中记载的对发明的构成要件标记的括弧内的编号表示权利请求书所记载的发明与后述的实施方式的对应关系,并不旨在限定权利请求书所记载的发明。

[0020] 通过上述那样的结构,能够削减与中心装置的通信量,并且削减中心装置的处理量。

[0021] 另外,能够通过中心装置进行攻击分析,并且收集必要的信息。

附图说明

[0022] 图1是表示本公开的实施方式的安全攻击检测/分析系统的结构例的图。

[0023] 图2是表示本公开的实施方式的日志管理装置的结构例的框图。

[0024] 图3是表示本公开的实施方式的中心装置的结构例的框图。

[0025] 图4是表示本公开的实施方式的日志管理装置的动作的流程图。

[0026] 图5是表示本公开的实施方式的日志管理装置的动作的流程图。

[0027] 图6是表示本公开的实施方式的中心装置的动作的流程图。

[0028] 图7是表示本公开的实施方式的中心装置的动作的流程图。

具体实施方式

[0029] 以下,参照附图对本公开的实施方式进行说明。

[0030] 此外,以下所示的本发明是指权利请求书所记载的发明,并不限定于以下的实施方式。另外,至少双引号内的语句是指权利请求书所记载的语句,而相同地并不限定于以下的实施方式。

[0031] 权利请求书的从属权利请求所记载的结构以及方法是权利请求书的独立权利请求所记载的发明中任意的结构以及方法。从属权利请求所记载的结构以及方法所对应的实施方式的结构和方法、以及在权利请求书中没有记载而仅记载于实施方式的结构和方法是在本发明中任意的结构和方法。权利请求书的记载比实施方式的记载宽泛的情况下的实施

方式所记载的结构以及方法从是本发明的结构以及方法的例示的意义上讲，也是本发明中任意的结构以及方法。在任意的情况下，通过记载于权利请求书的独立权利请求，而成为本发明的必须的结构以及方法。

[0032] 实施方式中记载的效果是具有作为本发明的例示的实施方式的结构的情况的效果，并不一定是本发明所具有的效果。

[0033] 在存在多个实施方式的情况下，各实施方式所公开的结构并不仅封闭在各实施方式，也能够跨实施方式地组合。例如，也可以将一个实施方式所公开的结构与其他实施方式组合。另外，也可以将多个实施方式分别公开的结构集中起来进行组合。

[0034] 本公开中记载的课题并不是公知的课题，而是本发明人独自发现的，是与本公开的结构以及方法一起肯定发明的创造性的事实。

[0035] 1.第一实施方式

[0036] (1)安全攻击检测/分析系统的整体结构

[0037] 首先，使用图1对本实施方式的安全攻击检测/分析系统的整体结构进行说明。

[0038] 安全攻击检测/分析系统1包含日志管理装置100和中心装置200。

[0039] 日志管理装置100经由通信网络2与中心装置200连接。

[0040] 在本实施方式的情况下，日志管理装置100“搭载”于作为“移动体”的车辆。然而，也可以不搭载于移动体而搭载于固定物。

[0041] 在这里，所谓的“移动体”是指能够移动的物体，移动速度为任意的。另外，当然也包含移动体停止的情况。例如，包含汽车、两轮摩托车、自行车、行人、船舶、飞机以及搭载于它们的物体，另外，不限于这些。

[0042] 另外，所谓的“搭载”，除了直接固定于移动体的情况以外，也包含虽然未固定于移动体但与移动体一起移动的情况。例如，可举出由乘坐移动体的人持有的情况、搭载于载置于移动体的载荷的情况。

[0043] 在通信网络2为无线通信方式的情况下，例如能够使用IEEE802.11(WiFi(注册商标))、IEEE802.16(WiMAX(注册商标))、W－CDMA(Wideband Code Division Multiple Access:宽带码分多址)、HSPA(High Speed Packet Access:高速包接入)、LTE(Long Term Evolution:长期演进)、LTE－A(Long Term Evolution Advanced:长期演进技术升级版)、4G、5G等。或者，能够使用DSRC(Dedicated Short Range Communication:专用短程通信)。

[0044] 在通信网络为有线通信方式的情况下，例如能够使用LAN(Local Area Network:局域网)、互联网、固定电话线路。作为使用有线通信方式的情况的例子，可举出车辆停放于停车场的情况、车辆被收容于修理厂的情况。

[0045] 无线通信网络也可以组合无线通信方式和有线通信方式。例如，也可以日志管理装置100与蜂窝系统中的基站装置之间通过无线通信方式连接，基站装置与中心装置200之间通过通信企业的主干线路、互联网等有线通信方式连接。

[0046] (2)日志管理装置的结构

[0047] 使用图2，对本实施方式的日志管理装置100的结构进行说明。

[0048] 日志管理装置100包含日志收集部101、保存部102、控制部103、发送部106以及接收部107。另外，控制部103实现统计分析部104和攻击检测部105。

[0049] 日志管理装置100能够包含通用的CPU(Central Processing Unit:中央处理器)、

RAM等易失性存储器、ROM、闪存、或者硬盘等非易失性存储器、各种接口、以及连接它们的内部总线。而且，能够构成为通过在这些硬件上执行软件，来发挥图2所记载的各功能模块的功能。在后述的图3所示的中心装置200中也相同。

[0050] 当然，也可以通过LSI等专用的硬件来实现日志管理装置100。

[0051] 在本实施方式中，日志管理装置100假定了作为半成品的电子控制装置(ECU(Electric Control Unit:电子控制单元)，以下简称为ECU。)的方式，但不限于此。例如，作为部件的方式，可举出半导体电路、半导体模块，作为成品的方式，可举出个人计算机(PC)、智能手机、移动电话、导航系统。

[0052] 此外，日志管理装置100除了由单一的ECU构成以外，也可以由多个ECU构成。例如，也可以由通信ECU负责与外部的通信。

[0053] 或者，也可以改变视点，将包含通信ECU的多个ECU理解为本实施方式的日志管理装置100。

[0054] 日志收集部101经由车载网络与连接于日志管理装置100的单个或者多个ECU连接，接收从设置于各ECU的安全传感器发送的安全日志。安全传感器监视各ECU自身、各ECU的通信，检测攻击等异常，并通过安全日志进行正常报告、异常报告。

[0055] 在图2中，日志收集部101经由车载网络与ECU1、ECU2以及ECU3连接。在ECU1、ECU2设置有监视各个ECU自身、各个ECU的通信的安全传感器。在ECU3未设置安全传感器。

[0056] 此外，除此之外，在ECU1、ECU2、ECU3中，除了安全传感器以外，还可以具备防御功能、生成通知各个ECU动作状态的日志的功能。而且，也可以代替安全日志或者与安全日志一起，将该日志作为本实施方式的处理对象。

[0057] ECU1、ECU2、ECU3为任意的ECU，例如，可举出进行发动机、方向盘、制动器等的控制的驱动系统电子控制装置；进行仪表、电动车窗等的控制的车身系统电子控制装置；导航装置等信息系统电子控制装置；或者进行用于防止与障碍物、行人的碰撞的控制的安全控制系统电子控制装置。另外，ECU彼此也可以不并列，而被分类为主设备和从设备。

[0058] 车载网络例如除了CAN(Controller Area Network:控制器域网)、LIN(Local Interconnect Network:本地互联网络)这样的通信方式以外，还能够使用Ethernet(注册商标)、Wi－Fi(注册商标)、Bluetooth(注册商标)等任意的通信方式。

[0059] 保存部102经由控制部103从日志收集部101、或者直接从日志收集部101保存由日志收集部101收集的安全日志。也可以也保存通过后述的统计分析部104求出的统计计算结果。

[0060] 保存部102由非易失性存储器或者易失性存储器构成。

[0061] 控制部103控制日志收集部101、保存部102、发送部106以及接收部107的动作。另外，控制部103通过其自身实现统计分析部104以及攻击检测部105。

[0062] 统计分析部104通过进行由日志收集部101收集的多个安全日志的统计分析，求出统计计算结果。作为统计分析的例子，例如可举出同一种类的安全日志的产生次数、频度、时间分布、或者相关性等。作为其他例子，可举出后述的攻击检测部105根据安全日志确定的攻击检测结果的次数、频度、时间分布、或者相关性等。这样，所谓的安全日志的统计分析包含对安全日志的直接或者间接的统计分析双方。

[0063] 攻击检测部105基于由日志收集部101收集的安全日志来进行攻击检测，求出攻击

检测结果。攻击检测存在多个阶段，如确定攻击、确定攻击路径、确定损害部位，攻击检测部105能够进行这些阶段中的至少一个阶段即可。

[0064] 所谓的确定攻击，是指确定为异常来自安全攻击。

[0065] 所谓的确定攻击路径，是指确定经由哪个ECU、哪个网络而被攻击。

[0066] 所谓的确定损害部位，是指确定哪个ECU、哪个网络受到损害。

[0067] 此外，如上述段落所述，也可以通过统计分析部104分析由攻击检测部105求出的攻击检测结果。在该情况下，间接地对安全日志进行统计分析。

[0068] 发送部106根据“规定条件”，将安全日志或者统计计算结果经由天线A发送至中心装置。作为具体例，根据“规定条件”，来发送安全日志或者统计计算结果中的任意一个。作为规定条件的例子，可举出攻击检测的次数、从中心装置接收到的上传请求、除了该上传请求外安全日志的量，这些在后述的日志管理装置的动作的部分中进行说明。能够通过控制部103判定是否满足规定条件。

[0069] 此处，所谓的“规定条件”，除与日志、统计计算结果有关的内部条件外，也可以是基于来自其他装置的指示、信息的外部条件。

[0070] 此外，在负责外部通信的通信ECU与日志管理装置分开设置的情况下，发送部106将安全日志、统计计算结果发送至通信ECU。但是，在该情况下，发送部106也经由通信ECU将安全日志、统计计算结果发送至中心装置，这一点没有不同。

[0071] 接收部107经由天线A从中心装置200接收请求安全日志、统计计算结果的上传的上传请求。

[0072] (3)中心装置的结构

[0073] 使用图3，对本实施方式的中心装置200的结构进行说明。

[0074] 中心装置200具有接收部201、控制部202、保存部204以及发送部205。另外，控制部202实现分析部203。

[0075] 在本实施方式中，中心装置200假定了作为成品的服务器装置的方式，但不限于此。例如，作为成品的方式，可举出工作站、个人计算机(PC)，作为半成品的方式可举出ECU，作为部件的方式可举出半导体电路元件。

[0076] 接收部201经由天线A接收从日志管理装置100发送的安全日志或者统计计算结果。

[0077] 控制部202控制接收部201、保存部204以及发送部205的动作。另外，控制部202通过其自身实现分析部203。

[0078] 分析部203对由接收部201接收到的安全日志或者统计计算结果进行分析。而且，基于分析结果，生成上传请求，其中，上述上传请求是对日志管理装置100请求上传追加的日志或者追加的统计计算结果的请求。

[0079] 上传请求的发送对象不限于由接收部201接收到的接收源的日志管理装置100。例如，搭载于“同类型”的其他车辆的日志管理装置100也可以是发送对象。

[0080] 在这里，所谓的“同类型”，除同一车型的情况外，搭载同一部件的情况、搭载同一平台的情况等具有某种共用性即可。

[0081] 保存部204保存由接收部201接收到的安全日志、统计计算结果。另外，也可以保存由分析部203生成的上传请求。

[0082] 发送部205对安全日志、统计计算结果的发送源的日志管理装置100、和/或对搭载于“同类型”的其他车辆的日志管理装置100发送上传请求。

[0083] (4)日志管理装置的动作

[0084] 使用图4和图5的流程图，对本实施方式的日志管理装置100的动作进行说明。

[0085] 此外，以下的动作不仅表示由日志管理装置100执行的日志管理方法，还表示能够由日志管理装置100执行的日志管理程序的处理步骤。

[0086] 而且，这些处理不限定于图4和图5所示的顺序。即，只要没有处于在某步骤中利用其前级的步骤的结果的关系等制约，也可以更换顺序。

[0087] 图4是与日志管理装置100的稳定的日志收集有关的动作。

[0088] 日志收集部101接收由ECU1以及ECU2的安全传感器生成以及发送的安全日志(S101)。然后，保存部102保存安全日志。

[0089] 攻击检测部105基于接收到的安全日志来进行攻击检测(S102)。

[0090] 攻击检测为确定攻击、确定攻击路径、确定损害部位中的至少任意一个即可。在未进行攻击检测的情况下(S102:“否”)，对正常日志进行统计分析，求出统计计算结果。在进行了攻击检测的情况下(S102:“是”)，将处理移至S104。

[0091] 在攻击检测部105的攻击检测为规定次数“以上”的情况下，统计分析部104通过进行统计分析来求出统计计算结果。

[0092] 另外，在将规定条件设为攻击检测的次数的情况下，在攻击检测为规定次数“以下”的情况下，控制部103向发送部106指示将安全日志发送至中心装置200，发送部106将安全日志发送至中心装置200。另外，在攻击检测为规定次数“以上”的情况下，控制部103等待来自中心装置200的上传请求，向发送部106指示将统计计算结果发送至中心装置200，发送部106将统计计算结果发送至中心装置200。

[0093] 在这里，所谓的“以上”也包括包含规定次数的情况、不包含规定次数的情况中的任意一种情况。

[0094] 所谓的“以下”也包括包含规定次数的情况、不包含规定次数的情况中的任意一种情况。

[0095] 在本实施方式中，在作为规定条件攻击检测为第一次的情况下(S104:“是”)，控制部103对发送部106进行指示，以使得将在进行攻击检测时使用的安全日志发送至中心装置200。然后，发送部106将安全日志发送至中心装置200(S105)。

[0096] 此外，除了安全日志以外，也可以一并发送未图示的车辆状态监视功能输出的表示车辆状态的车辆信息、车辆信息的统计计算结果。在下一段落中也相同。

[0097] 另外，在本实施方式中，在作为规定条件攻击检测为第二次以上的情况下(S104:“否”)，统计分析部104进行多个安全日志的统计分析，求出统计计算结果(S103)。例如，求出同一种类的安全日志的产生次数、频度、时间分布、或者相关性等。或者，攻击检测部105求出根据安全日志确定的攻击检测结果的次数、频度、时间分布、或者相关性等。

[0098] 求出的统计计算结果并不立即发送，而是控制部103等待来自中心装置200的上传请求而对发送部106指示发送统计计算结果，发送部106发送统计计算结果。在发送了统计计算结果的情况下，重置攻击次数。

[0099] 然而，也可以将求出的统计计算结果迅速地从发送部106发送。

[0100] 此外，在S104中，作为规定条件将规定次数设为一次，但也可以将规定次数设为2以上。例如，也可以在将规定次数设为3的情况下，发送安全日志直到异常检测为三次，在四次以上，通过进行统计分析求出统计计算结果，等待来自中心装置200的上传请求而发送统计计算结果。

[0101] 并且，作为规定条件，也可以设定攻击检测的次数以外的条件。例如，也可以为安全日志的接收次数、接收频度。

[0102] 规定条件也可以能够根据需要或者根据条件自动地变更。

[0103] 统计分析的内容也可以能够根据需要或者根据条件自动地变更。

[0104] 像这样，根据本实施方式，由于根据攻击的次数将发送对象作为安全日志或者统计计算结果中的任意一个，因此无需将所有的日志发送至中心装置，能够削减通信量。

[0105] 另外，根据本实施方式，由于等待来自中心装置200的请求而发送统计计算结果，因此在中心装置200判断为需要时发送统计计算结果即可，能够削减通信量。

[0106] 而且，根据本实施方式，由于中心装置200无需求出统计计算结果，因此能够削减处理量。

[0107] 图5是日志管理装置100从中心装置200接收到上传请求的情况的动作。也就是说，上传请求为规定条件的情况。

[0108] 接收部107从中心装置200接收上传请求(S111)。

[0109] 控制部103判定是否能够发送安全日志或者统计计算结果(S112)。在判定中，使用未图示的车辆状态监视功能输出的车辆信息。例如，由于车辆在睡眠时仅能够利用待机电源，因此判定为不能发送(S112:“否”)。在判定为能够发送的情况下(S112:“是”)，将处理移至S113。

[0110] 在作为规定条件设为接收到的安全日志的“量”的情况下，在安全日志的量为规定数量“以下”的情况下，控制部103对发送部106指示将安全日志发送至中心装置200，发送部106将安全日志发送至中心装置200。另外，在安全日志的量为规定数量“以上”的情况下，控制部103对发送部106指示将统计计算结果发送至中心装置200，发送部106将统计计算结果发送至中心装置200。

[0111] 在这里，所谓的“量”，除了日志的尺寸以外，还包含日志的数量、日志的接收频度等。

[0112] 所谓的“以上”，包括包含规定次数的情况、不包含规定次数的情况中的任意一种情况。

[0113] 所谓的“以下”，包括包含规定次数的情况、不包含规定次数的情况中的任意一种情况。

[0114] 在本实施方式中，在安全日志的数量为一个的情况下(S113:“是”)，控制部103对发送部106指示将安全日志发送至中心装置200。然后，发送部106将安全日志发送至中心装置200(S114)。

[0115] 另外，在本实施方式中，在安全日志的数量为两个以上的情况下(S113:“否”)，控制部103对发送部106指示将统计计算结果发送至中心装置200。然后，发送部106将统计计算结果发送至中心装置200(S115)。

[0116] 在S112中为“否”的情况下，统计分析部104为了进行无法发送安全日志的重要因

素的分析，而进行无法发送的理由的统计分析(S116)。然后，在成为能够发送的情况下(S117：“是”)，根据此前接收到的上传请求中最新的上传请求，将处理移至S113。作为成为能够发送的情况的例子，可举出下次的IG－ON(点火接通)时。在成为能够发送的情况下(S117：“是”)，也可以进一步发送无法发送的理由的统计分析的统计计算结果。

[0117] 此外，在S113中，作为规定条件将安全日志的数量设为1，但也可以设为2以上。例如，也可以在将安全日志的数量设为3的情况下，发送安全日志直到安全日志的数量为3，在4以上的情况下发送统计计算结果。

[0118] 并且，作为规定条件，也可以设定安全日志的数量以外的条件。

[0119] 规定条件也可以能够根据需要或者根据条件自动地变更。

[0120] 统计分析的内容也可以能够根据需要或者根据条件自动地变更。

[0121] 像这样，根据本实施方式，由于根据安全日志的数量将发送对象设为安全日志或统计计算结果中的任意一个，因此无需将所有的日志发送至中心装置，能够削减通信量。

[0122] 另外，根据本实施方式，由于等待来自中心装置200的请求而发送统计计算结果，因此在中心装置200判断为需要时发送统计计算结果即可，能够削减通信量。

[0123] 而且，根据本实施方式，由于中心装置200无需求出需要在分析的过程中进行的统计计算结果，因此能够削减处理量。即，能够不使中心装置200中的分析精度降低地削减与中心装置200的通信量。

[0124] (5)中心装置的动作

[0125] 使用图6和图7的流程图，对本实施方式的中心装置200的动作进行说明。

[0126] 此外，以下的动作不仅表示由中心装置200执行的安全攻击/分析方法，还表示能够由中心装置200执行的安全攻击/分析程序的处理步骤。

[0127] 而且，这些处理不限定于图6和图7所示的顺序。即，只要没有处于在某步骤中利用其前级的步骤的结果的关系等制约，也可以更换顺序。

[0128] 图6是从车辆的日志管理装置100接收到安全日志或者统计计算结果的情况的动作。

[0129] 中心装置200的接收部201接收从特定的车辆发送的安全日志或者统计计算结果(S201)。这里接收的安全日志或者统计计算结果既可以是如图4所示的基于特定的车辆的日志管理装置100的稳定的日志收集的安全日志(S105)或者统计计算结果(S103)，也可以是如图5所示的针对来自中心装置200的上传请求发送的安全日志(S114)或者统计计算结果(S115)。即，图6的流程图连接于图4、图5而执行。

[0130] 分析部203使用在S201中接收到的安全日志或者统计计算结果进行攻击分析(S202)。攻击分析也可以是与车辆的日志管理装置100的攻击检测部105相同的算法，但也可以进行更细致的攻击分析。攻击分析的方法能够使用公知的方法。

[0131] 在判定为对特定的车辆有攻击的情况、或者无法判定有无攻击而判定为需要追加分析的情况下(S203：“是”)，分析部203将处理移至S204。此时，也可以进一步判定追加分析所需的信息是仅需要来自该特定的车辆、或者存在安全漏洞等给同一车型带来危险的情况、还是需要广泛收集信息的情况。在判定为对特定的车辆无攻击的情况下，分析部203结束处理。

[0132] 分析部203为了从特定的车辆、或者与特定的车辆同一车型的一部分或者全部车

辆收集信息，而对发送部205指示发送上传请求(S204)。然后，发送部205对特定的车辆、或者与特定的车辆同一车型的一部分或者全部车辆发送上传请求。同一车型的发送目的地能够通过使用保存于中心装置200的保存部204的车辆注册数据来确定。

[0133] 接收部201从作为特定的车辆的单个车辆、或者作为与特定的车辆同一车型的一部分或者全部的多个车辆接收安全日志或者统计计算结果。然后，分析部203使用这些信息进行攻击分析(S205)。在多个车辆中，既可以包含特定的车辆，也可以不包含特定的车辆。

[0134] 这样，根据本实施方式，能够通过中心装置200进行攻击分析，并且广泛收集所需的信息来进行攻击分析。

[0135] 图7与图6相同地，是从车辆的日志管理装置100接收到安全日志或者统计计算结果的情况的动作。与图6相同的步骤引用图6的说明而省略说明。

[0136] 在S201中从特定的车辆接收到安全日志的情况下，分析部203对保存部204确认是否在过去从该特定的车辆接收/保存了统计计算结果(S211)。若在过去未接收(S211：“否”)，则分析部203对发送部205指示对该特定的车辆发送统计计算结果的追加上传请求。然后，发送部205发送追加上传请求(S212)。若在过去接收了(S211：“是”)，则将处理移至S202。

[0137] 这样，根据本实施方式，在通过中心装置200进行攻击分析时，通过充分地收集来自特定的车辆的信息，能够提高攻击分析的精度。

[0138] 3.其他

[0139] (1)对象日志发送和统计计算结果的发送条件的变更

[0140] 在图4的S103、图5的S113中，将规定条件设为攻击检测次数、安全日志的数量，但也可以根据安全传感器的设置场所(例如特定的ECU)、连接有安全传感器的通信总线的重要度，自动或者手动地设定规定条件。例如，也可以能够设定作为规定条件的攻击检测的次数。

[0141] 另外，对于与安全有关的信息、与位置信息等隐私有关的信息，也可以变更其他日志和规定条件。例如，对于与安全有关的信息而言，通过增大作为规定条件的攻击检测次数、安全日志的数量，能够增大未加工的原始数据量。另外，对于与隐私有关的信息而言，通过作为规定条件减小攻击检测次数、安全日志的数量，能够减少直接明确隐私的内容的原始数据量。

[0142] (2)对象日志、统计计算结果的优先顺序

[0143] 在发送对象日志时，例如，也可以提高与安全有关的信息、与位置信息等隐私有关的信息的优先度，而优先于其他日志地发送。

[0144] (3)从其他观点理解发明

[0145] 本公开也能够作为以下的发明来理解。

[0146] 一种日志管理装置(100)，具有：

[0147] 日志收集部(101)，收集安全传感器生成的日志；

[0148] 保存部(102)，保存上述日志；

[0149] 发送部(106)，向外部发送上述日志；以及

[0150] 统计分析部(104)，通过进行多个上述日志的统计分析来求出统计计算结果，

[0151] 在满足规定条件的情况下，上述发送部代替上述日志而将上述统计计算结果向外

部发送。

[0152] 4.总结

[0153] 以上,对本公开的各实施方式中的日志管理装置、中心装置、以及安全攻击检测/分析系统的特征进行了说明。

[0154] 由于各实施方式中使用的术语是例示,所以也可以置换为同义的术语、或者包含同义的功能的术语。

[0155] 实施方式的说明所使用的框图按功能分类以及整理装置的结构。表示各个功能的模块由硬件或者软件的任意的组合来实现。另外,因为是表示功能的模块,所以这样的框图也能够作为方法的发明、以及实现该方法的程序的发明的公开来理解。

[0156] 对于能够作为各实施方式所记载的处理、流程、以及方法来理解的功能模块,只要没有处于在一个步骤中利用其前级的其他步骤的结果的关系等限制,也可以更换顺序。

[0157] 在各实施方式、以及权利请求书中使用的第一、第二、或第N(N为整数)的用语用于区分同类型的两个以上的结构、方法,并不限定顺序、优劣。

[0158] 各实施方式以搭载于车辆的车辆用的日志管理装置作为前提,但本发明除了在权利请求书中特别限定的情况以外,也包含车辆用以外的专用或者通用的日志管理装置。

[0159] 在各实施方式中,以将各实施方式所公开的日志管理装置搭载于车辆的前提进行了说明,但也可以为行人持有的前提。

[0160] 另外,作为本公开的日志管理装置、中心装置的方式的例子,可举出以下的例子。

[0161] 作为部件的方式,可举出半导体元件、电子电路、模块、微型计算机。

[0162] 作为半成品的方式,可举出电子控制装置(ECU(Electric Control Unit))、系统板。

[0163] 作为成品的方式,可举出移动电话、智能手机、平板电脑、个人计算机(PC)、工作站、服务器。

[0164] 另外,包含具有通信功能的设备等,例如可举出摄像机、静态相机、汽车导航系统。

[0165] 另外,也可以向日志管理装置、中心装置追加天线、通信用接口等所需的功能。

[0166] 假定本公开的中心装置以提供各种服务为目的而使用。伴随着提供这样的服务,使用本公开的中心装置、使用本公开的方法或/和执行本公开的程序。

[0167] 此外,本公开不仅能够通过具有在各实施方式中说明的结构以及功能的专用的硬件实现,也能够作为记录于存储器、硬盘等记录介质的用于实现本公开的程序、以及具有能够执行该程序的专用或者通用CPU以及存储器等的通用的硬件的组合来实现。

[0168] 储存于专用、通用的硬件的非过渡性实体记录介质(例如,外部存储装置(硬盘、USB存储器、CD/BD等)、或者内部存储装置(RAM、ROM等))的程序也能够经由记录介质、或者不经由记录介质而从服务器经由通信线路提供至专用或者通用的硬件。由此,能够通过程序的升级始终提供最新的功能。

[0169] 本公开的日志管理装置主要作为搭载于汽车的车辆用的电子控制装置进行了说明,但不仅能够应用于两轮摩托车、带电动机的自行车、铁路,也能够应用于行人、船舶、飞机等所有移动的移动体。

[0170] 另外,能够适用于移动电话、平板电脑、游戏机等用于各种用途的装置。

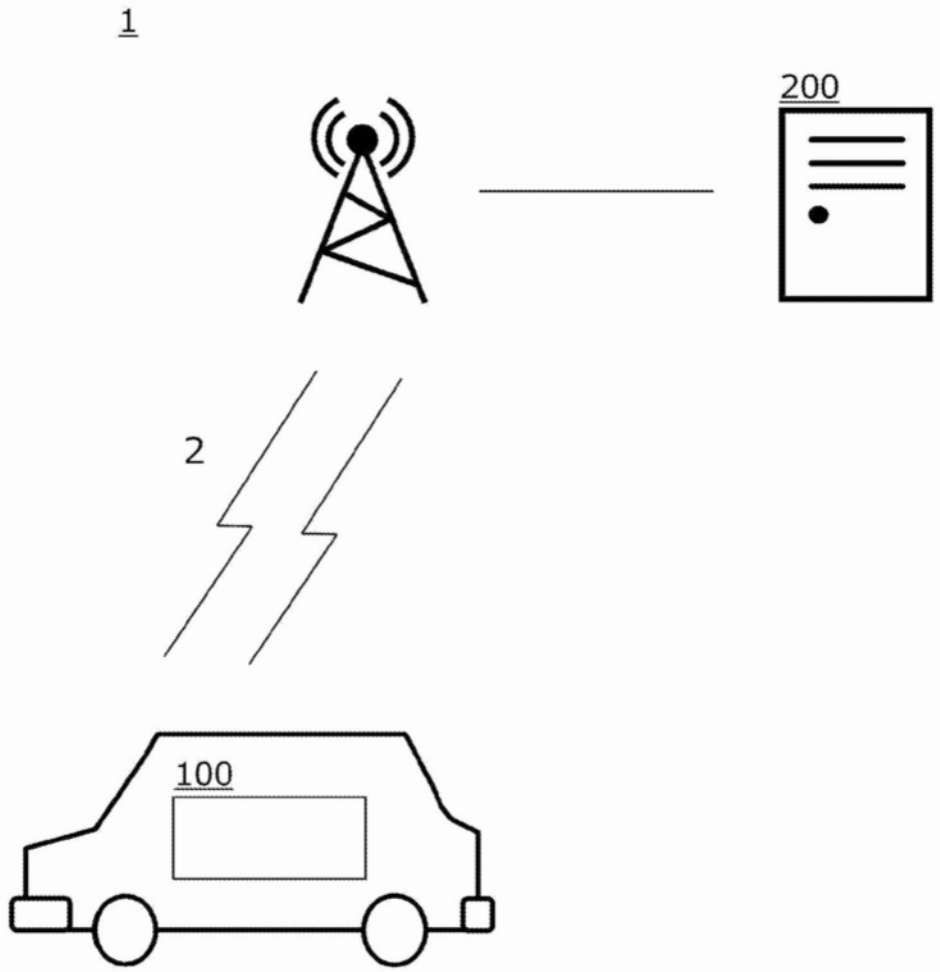


图1

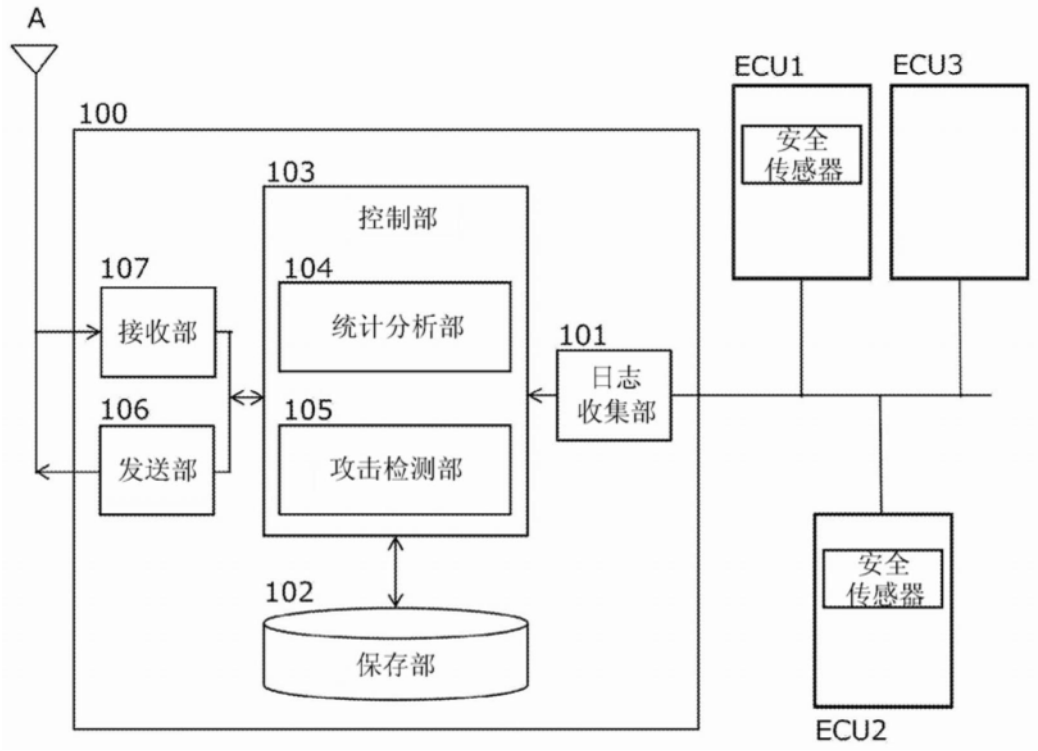

A
100
103
控制部
107
接收部
104
统计分析部
101
日志
收集部
106
发送部
105
攻击检测部
102
保存部
ECU1
安全
传感器
ECU3
安全
传感器
ECU2

图2

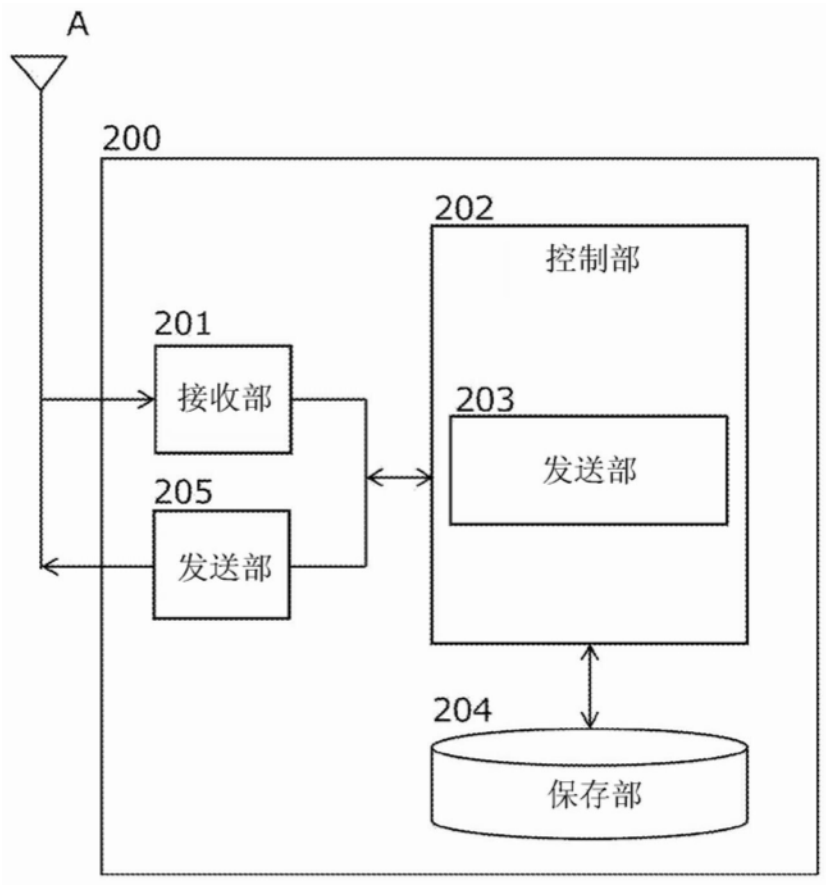

A
200
202
控制部
201
接收部
203
发送部
205
发送部
204
保存部

图3

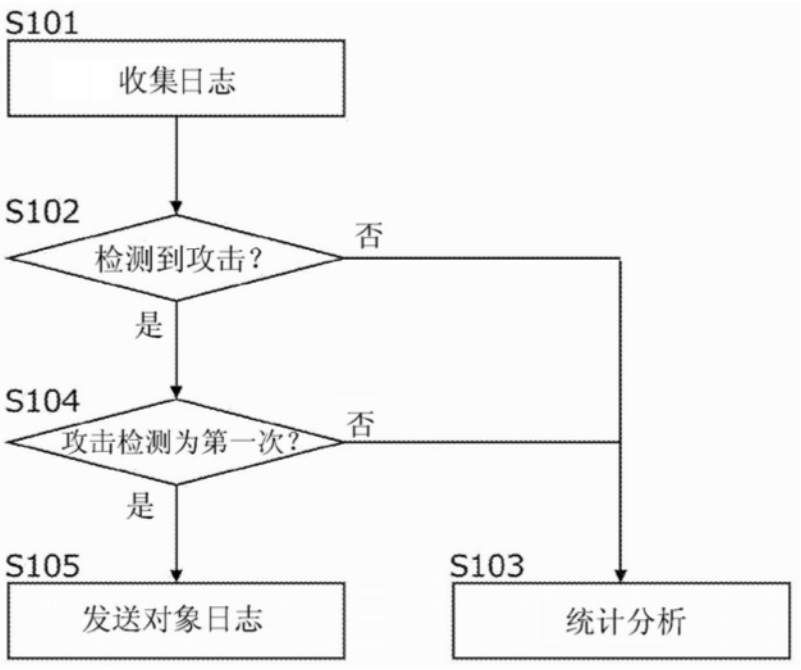

S101
收集日志
S102
检测到攻击？
否
是
S104
攻击检测为第一次？
否
是
S105
发送对象日志
S103
统计分析

图4

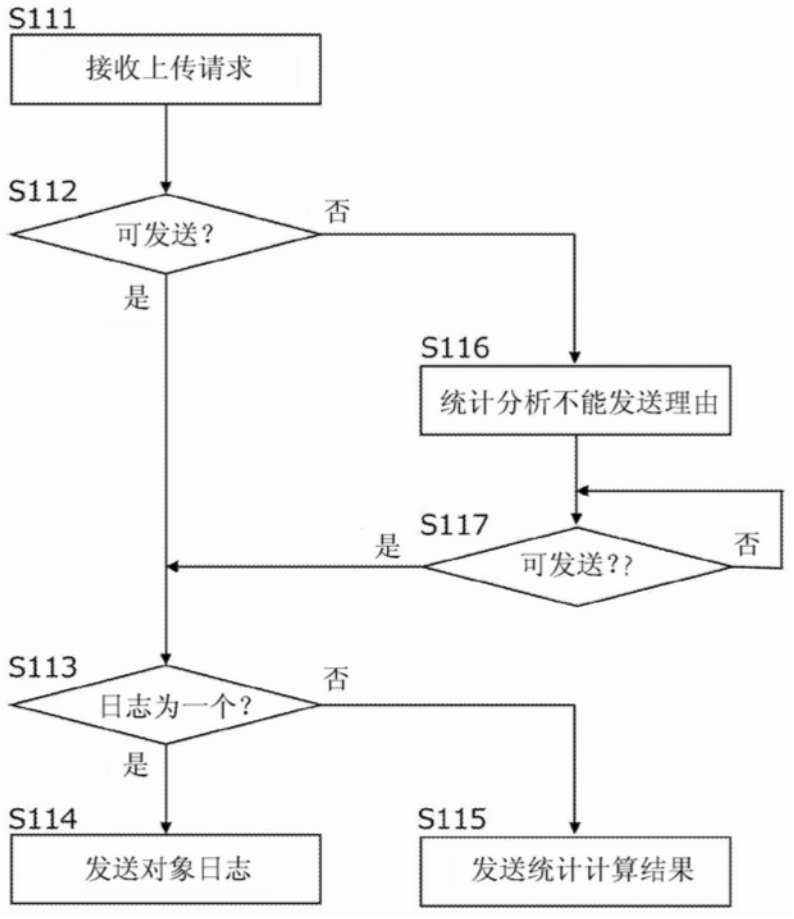

S111
接收上传请求
S112
可发送?
否
是
S116
统计分析不能发送理由
S117
可发送??
是
否
S113
日志为一个?
否
是
S114
发送对象日志
S115
发送统计计算结果

图5

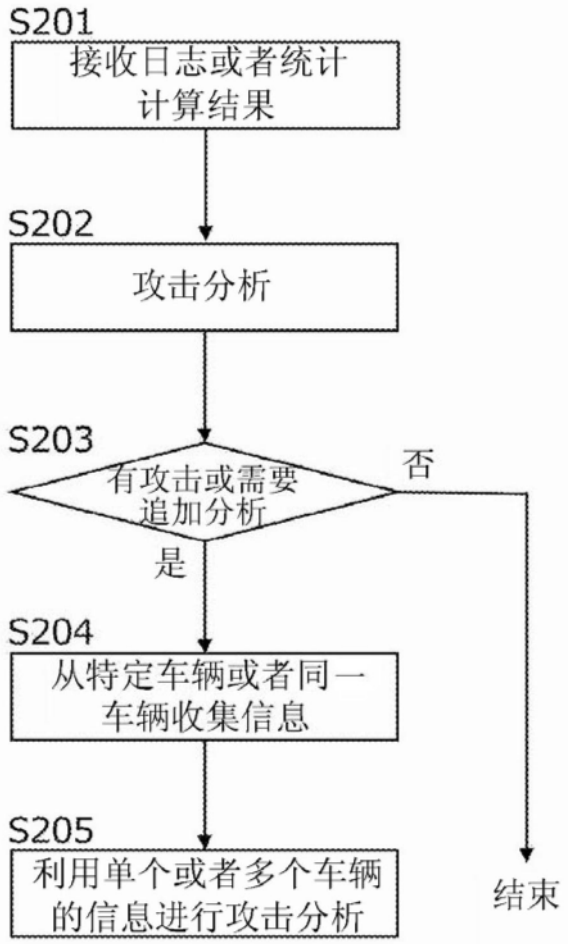

S201
接收日志或者统计计算结果
S202
攻击分析
S203
有攻击或需要追加分析
否
是
S204
从特定车辆或者同一车辆收集信息
S205
利用单个或者多个车辆的信息进行攻击分析
结束

图6

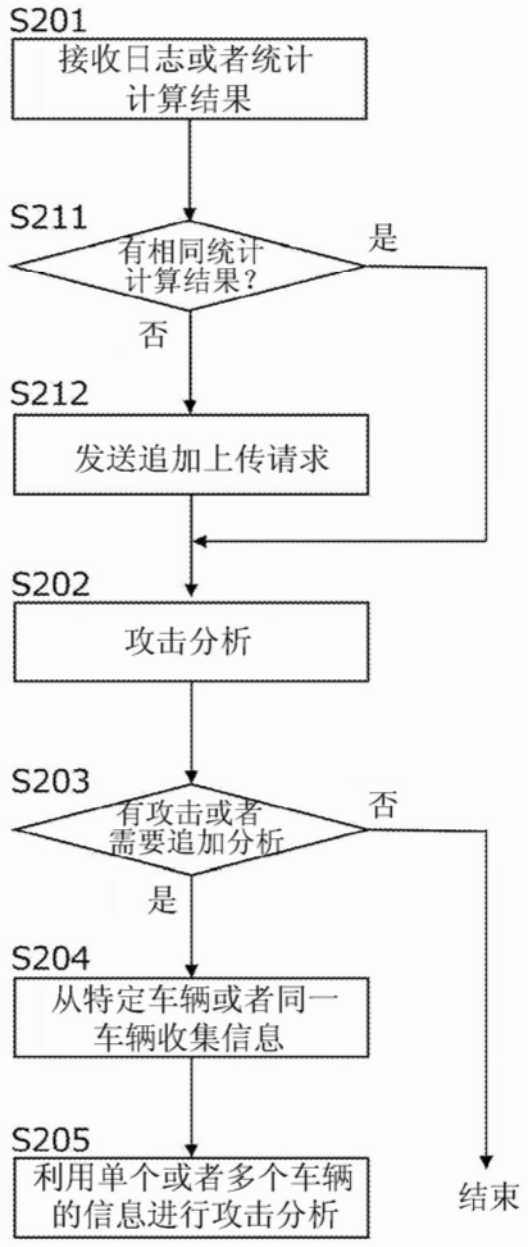

S201
接收日志或者统计计算结果
S211
有相同统计计算结果?
是
否
S212
发送追加上传请求
S202
攻击分析
S203
有攻击或者需要追加分析
否
是
S204
从特定车辆或者同一车辆收集信息
S205
利用单个或者多个车辆的信息进行攻击分析
结束

图7