(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114616800 B
(45)授权公告日 2024.12.27

(21)申请号 202180005900.3
(22)申请日 2021.01.18
(65)同一申请的已公布的文献号
申请公布号 CN 114616800 A
(43)申请公布日 2022.06.10
(30)优先权数据
2020-007070 2020.01.20 JP
(85)PCT国际申请进入国家阶段日
2022.04.15
(86)PCT国际申请的申请数据
PCT/JP2021/001545 2021.01.18
(87)PCT国际申请的公布数据
WO2021/149651 JA 2021.07.29

(73)专利权人 松下电器(美国)知识产权公司
地址 美国加利福尼亚州
(72)发明人 牛尾贵志 佐佐木崇光
(74)专利代理机构 北京市中咨律师事务所 11247
专利代理师 林娜 段承恩

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/12(2022.01)
H04Q 9/00(2006.01)

(56)对比文件
CN 109076016 A,2018.12.21
CN 110168551 A,2019.08.23

审查员 许婵

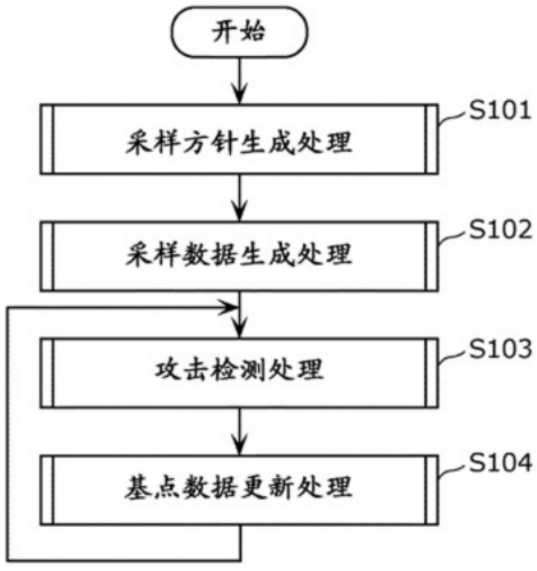
权利要求书3页 说明书27页 附图15页

(54)发明名称

攻击检测方法、攻击检测系统、以及程序记录介质

(57)摘要

攻击检测方法是检测对在移动体内部收发的传感器数据的攻击的攻击检测方法,包括:基于表示传感器数据的传感器值的偏差的统计值、以及表示传感器值的变化的时机的移动体的事件信息中的至少一方,决定包含采样间隔和采样时间的采样方针的步骤(S101);基于采样间隔和采样时间生成包含从传感器数据提取出的2个以上的传感器值、和第一以及第二顺序信息的采样数据的步骤(S102);算出表示评价对象数据的异常的程度的第一异常得分、以及、表示评价对象数据的异常的程度的第二异常得分,基于所算出的第一异常得分和第二异常得分,判定评价对象数据是否是受到攻击的数据,输出判定结果的步骤(S103)。



CN 114616800 B

1.一种攻击检测方法,是检测对在移动体内部为了进行移动体的控制而收发的传感器数据的攻击的攻击检测方法,包括:

采样方针决定步骤,按所述传感器数据所包含的传感器值的每个标识符,基于表示所述传感器数据的所述传感器值的偏差的统计值、以及表示所述传感器值的变化的时机的所述移动体的事件信息中的至少一方,决定包含从所述传感器数据中提取用于检测所述攻击的所述传感器值的采样间隔和每个该采样间隔的采样时间的采样方针;

采样数据生成步骤,基于所述采样间隔和所述采样时间,生成采样数据,所述采样数据包含:从所述传感器数据中提取出的2个以上的传感器值、表示所述采样时间中的所述2个以上的传感器值的时间上的顺序的第一顺序信息、以及表示每个所述采样间隔的所述2个以上的传感器值的时间上的顺序的第二顺序信息;

攻击判定步骤,基于所述采样数据所包含的评价对象数据的传感器值、所述第一顺序信息、以及表示取得了所述评价对象数据的所述采样时间中的与所述评价对象数据相比过去的传感器值的时序数据的短期传感器流,算出表示所述评价对象数据的异常的程度的第一异常得分,基于所述评价对象数据的传感器值、所述第二顺序信息、以及表示以与取得了所述评价对象数据的所述采样间隔相比过去的所述采样间隔取得了的传感器值的变化的长期传感器流,算出表示所述评价对象数据的异常的程度的第二异常得分,基于所算出的所述第一异常得分和所述第二异常得分,判定所述评价对象数据是否是受到所述攻击的数据,并输出判定结果。

2.根据权利要求1所述的攻击检测方法,

所述统计值包含表示每个所述标识符的传感器值的偏差的方差值,

所述事件信息包含表示是否发生了所述传感器值的变化的标记信息,

在所述采样方针决定步骤中,基于所述方差值和所述标记信息,决定所述采样间隔和所述采样时间。

3.根据权利要求2所述的攻击检测方法,

在所述采样方针决定步骤中,根据所述方差值是否为第一阈值以上的判定结果、和表示所述标记信息是否表示没有发生所述传感器值的变化这一情况的组合,决定所述采样时间和所述采样间隔。

4.根据权利要求2或3所述的攻击检测方法,

所述标记信息包含表示是否发生了所述移动体的驱动部的ON和OFF的切换、换挡杆的切换、以及自动驾驶模式的ON和OFF的切换中的至少1个的信息。

5.根据权利要求1~3中任一项所述的攻击检测方法,

在所述采样数据生成步骤中,基于在所述采样时间中应观测的正常接收数据数,决定在所述采样时间内提取的传感器数据的提取数,并提取所决定了的所述提取数的传感器数据。

6.根据权利要求5所述的攻击检测方法,

在所述采样数据生成步骤中,判定所述采样时间中所观测到的所述传感器值数是否为所述正常接收数据数以上,在为所述正常接收数据数以上的情况下,提取预定数的所述传感器值,在不为所述正常接收数据数以上的情况下,将所述传感器数据所包含的所述传感器值全数提取。

7.根据权利要求1～3、6中任一项所述的攻击检测方法，

所述第一顺序信息是表示在所述采样时间中所述2个以上的传感器值被取得的顺序的第一索引，

所述第二顺序信息是表示所述2个以上的传感器值被取得的所述采样间隔的顺序的第二索引，

在所述攻击判定步骤中，在所述评价对象数据所关联的所述第一索引低于第三阈值、且所述评价对象数据所关联的所述第二索引低于第四阈值的情况下，判定为不清楚所述评价对象数据是否是受到所述攻击的数据，在基于所述第一异常得分以及所述第二异常得分的第三异常得分为第五阈值以上的情况下，判定为所述评价对象数据是受到所述攻击的数据，在所述第三异常得分低于所述第五阈值的情况下，判定为所述评价对象数据是正常的，将表示所判定出的结果的所述评价对象数据所关联的所述判定结果输出。

8.根据权利要求1～3、6中任一项所述的攻击检测方法，

还包括更新步骤，所述更新步骤中，

基于所述评价对象数据所关联的所述判定结果、所述第一顺序信息、以及所述第二顺序信息，更新所述短期传感器流和所述长期传感器流。

9.根据权利要求8所述的攻击检测方法，

在所述更新步骤中，在所述评价对象数据所关联的所述判定结果是攻击的情况下，使用所述短期传感器流和所述长期传感器流中的至少1个推定所述评价对象数据应该能取的传感器值，基于所推定出的推定传感器值、所述第一顺序信息、以及所述第二顺序信息，更新所述短期传感器流和所述长期传感器流，在所述评价对象数据所关联的所述判定结果是正常或者不清楚的情况下，基于所述评价对象数据的传感器值、所述第一顺序信息、以及所述第二顺序信息，更新所述短期传感器流和所述长期传感器流。

10.根据权利要求1～3、6、9中任一项所述的攻击检测方法，

所述传感器数据存储于搭载于所述移动体的设备，并且是遵循CAN即控制器局域网络、CAN FD即具有灵活数据速率的控制器局域网络、FlexRay、以及EtherNet即以太网中的至少1个协议，对以任意的行驶时间间隔收发的以字节表现的网络数据进行解码而得到的结果。

11.根据权利要求1～3、6、9中任一项所述的攻击检测方法，

所述移动体是车辆。

12.一种攻击检测系统，是检测对在移动体内部用于进行移动体的控制而收发的传感器数据的攻击的攻击检测系统，具备：

采样方针决定部，按所述传感器数据所包含的传感器值的每个标识符，基于表示所述传感器数据的所述传感器值的偏差的统计值、以及表示所述传感器值的变化的时机的所述移动体的事件信息中的至少一方，决定包含从所述传感器数据中提取用于检测所述攻击的所述传感器值的采样间隔和每个该采样间隔的采样时间的采样方针；

采样数据生成部，基于所述采样间隔和所述采样时间，生成采样数据，所述采样数据包含：从所述传感器数据中提取出的2个以上的传感器值、表示所述采样时间中的所述2个以上的传感器值的时间上的顺序的第一顺序信息、以及表示每个所述采样间隔的所述2个以上的传感器值的时间上的顺序的第二顺序信息；

攻击判定部，基于所述采样数据所包含的评价对象数据的传感器值、所述第一顺序信

息、以及表示取得了所述评价对象数据的所述采样时间中的与所述评价对象数据相比过去的传感器值的时序数据的短期传感器流，算出表示所述评价对象数据的异常的程度的第一异常得分，基于所述评价对象数据的传感器值、所述第二顺序信息、以及表示以与取得了所述评价对象数据的所述采样间隔相比过去的所述采样间隔取得了的传感器值的变化的长期传感器流，算出表示所述评价对象数据的异常的程度的第二异常得分，基于所算出的所述第一异常得分和所述第二异常得分，判定所述评价对象数据是否是受到所述攻击的数据，并输出判定结果。

13.一种用于使计算机执行权利要求1～11中任一项所述的攻击检测方法的程序记录介质。

14.一种计算机程序产品，包括计算机程序，该计算机程序用于使计算机执行权利要求1～11中任一项所述的攻击检测方法。

攻击检测方法、攻击检测系统、以及程序记录介质

技术领域

[0001] 本公开涉及检测对传感器数据的攻击的攻击检测方法、攻击检测系统、以及程序记录介质。

背景技术

[0002] 要求监视汽车的系统(监视系统)检测对以车辆控制为目的而收发的车辆传感器数据的攻击(攻击检测)。监视系统也具有监视对象是大规模的这一特征。因此,需要抑制汽车与系统之间的通信成本或攻击检测的运算成本这样的监视成本。作为运算成本得以抑制的监视系统,公开了如下技术,即,通过根据频率解析的结果对于作为监视对象的传感器数据提取峰值等特征量,从而将削减了数据量的采样日志向监视系统发送(例如,参照专利文献1)。

[0003] 现有技术文献

[0004] 专利文献1:日本特开2018—164159号公报

[0005] 专利文献2:国际公开第2019/187350号

[0006] 非专利文献1:P.Malhotra,“Long Short Term Memory Networks for Anomaly Detection in Time Series”,23rd European Symposium on Artificial Neural Networks,Computational Intelligence and Machine Learning,ESANN 2015.

发明内容

[0007] 发明要解决的问题

[0008] 然而,在专利文献1所记载的技术中,进行采样的数据是为了削减数据量而由监视系统确定的唯一的时间间隔的数据。因此,有可能所采样的数据中不包含攻击消息而错过攻击。

[0009] 另外,已知利用传感器数据从正常周期的背离来从所采样的消息中检测攻击(攻击消息)的技术(例如,参照专利文献2)。然而,即使在这样的技术中,也很难根据攻击消息的取得间隔准确地检测攻击。

[0010] 因此,期望兼顾数据量削减和攻击检测性能,但是如上所述在现有技术中,很难兼顾数据量削减和攻击检测性能。

[0011] 因此,本公开提供一种能够兼顾数据量削减和攻击检测性能的攻击检测方法、攻击检测系统、以及程序记录介质。

[0012] 用于解决问题的手段

[0013] 本公开的一技术方案的攻击检测方法,是检测对在移动体(mobility)内部为了进行移动体的控制而收发的传感器数据的攻击的攻击检测方法,包括:采样方针决定步骤,按所述传感器数据所包含的传感器值的每个标识符,基于表示所述传感器数据的所述传感器值的偏差的统计值、以及表示所述传感器值的变化的时机的所述移动体的事件信息中的至少一方,决定包含从所述传感器数据中提取用于检测所述攻击的所述传感器值的采样间隔

和每个该采样间隔的采样时间的采样方针;采样数据生成步骤,基于所述采样间隔和所述采样时间,生成采样数据,所述采样数据包含:从所述传感器数据中提取出的2个以上的传感器值、表示所述采样时间中的所述2个以上的传感器值的时间上的顺序的第一顺序信息、以及表示每个所述采样间隔的所述2个以上的传感器值的时间上的顺序的第二顺序信息;攻击判定步骤,基于所述采样数据所包含的评价对象数据的传感器值、所述第一顺序信息、以及表示取得了所述评价对象数据的所述采样时间中的与所述评价对象数据相比过去的传感器值的时序数据的短期传感器流,算出表示所述评价对象数据的异常的程度的第一异常得分,基于所述评价对象数据的传感器值、所述第二顺序信息、以及表示以与取得了所述评价对象数据的所述采样间隔相比过去的所述采样间隔取得了的传感器值的变化的长期传感器流,算出表示所述评价对象数据的异常的程度的第二异常得分,基于所算出的所述第一异常得分和所述第二异常得分,判定所述评价对象数据是否是受到所述攻击的数据,并输出判定结果。

[0014] 另外,本公开的一技术方案的攻击检测系统,是检测对在移动体内部用于进行移动体的控制而收发的传感器数据的攻击的攻击检测系统,具备:采样方针决定部,按所述传感器数据所包含的传感器值的每个标识符,基于表示所述传感器数据的所述传感器值的偏差的统计值、以及表示所述传感器值的变化的时机的所述移动体的事件信息中的至少一方,决定包含从所述传感器数据中提取用于检测所述攻击的所述传感器值的采样间隔和每个该采样间隔的采样时间的采样方针;采样数据生成部,基于所述采样间隔和所述采样时间,生成采样数据,所述采样数据包含:从所述传感器数据中提取出的2个以上的传感器值、表示所述采样时间中的所述2个以上的传感器值的时间上的顺序的第一顺序信息、以及表示每个所述采样间隔的所述2个以上的传感器值的时间上的顺序的第二顺序信息;攻击判定部,基于所述采样数据所包含的评价对象数据的传感器值、所述第一顺序信息、以及表示取得了所述评价对象数据的所述采样时间中的与所述评价对象数据相比过去的传感器值的时序数据的短期传感器流,算出表示所述评价对象数据的异常的程度的第一异常得分,基于所述评价对象数据的传感器值、所述第二顺序信息、以及表示以与取得了所述评价对象数据的所述采样间隔相比过去的所述采样间隔取得了的传感器值的变化的长期传感器流,算出表示所述评价对象数据的异常的程度的第二异常得分,基于所算出的所述第一异常得分和所述第二异常得分,判定所述评价对象数据是否是受到所述攻击的数据,并输出判定结果。

[0015] 另外,本公开的一技术方案的程序记录介质是用于使计算机执行上述的攻击检测方法的程序记录介质。

[0016] 发明效果

[0017] 根据本公开的一技术方案,能够提供一种可兼顾数据量削减和攻击检测性能的攻击检测方法、攻击检测系统、以及程序记录介质。

附图说明

[0018] 图1是表示实施方式的监视系统的构成的框图。

[0019] 图2是表示实施方式的监视系统的动作的概要的流程图。

[0020] 图3是表示实施方式的采样方针生成部的构成的框图。

[0021] 图4是表示实施方式的采样方针生成处理的流程图。

[0022] 图5是表示实施方式的车辆传感器数据的一例的图。

[0023] 图6是说明实施方式的采样的图。

[0024] 图7是表示实施方式的采样方针数据的一例的图。

[0025] 图8是表示实施方式的采样数据生成部的构成的框图。

[0026] 图9是表示实施方式的采样数据生成处理的流程图。

[0027] 图10是表示实施方式的采样数据的一例的图。

[0028] 图11是表示实施方式的攻击检测部的构成的框图。

[0029] 图12是表示实施方式的攻击检测处理的流程图。

[0030] 图13是表示实施方式的基点数据的一例的图。

[0031] 图14是表示实施方式的检测结果的一例的图。

[0032] 图15是表示实施方式的基点数据更新部的构成的框图。

[0033] 图16是表示实施方式的基点数据更新处理的流程图。

[0034] 图17是表示实施方式的监视系统的构成的示意图。

[0035] 图18是表示实施方式的车载装置的构成的示意图。

具体实施方式

[0036] (成为本公开的基础的见解)

[0037] 为了实现能够以低监视成本实现的监视系统,需要构筑适当的采样方法和攻击检测方法这两方。

[0038] 在专利文献1中,为了抑制监视系统中的监视成本,基于周期性的传感器数据的频率解析的结果,以采样间隔提取峰值等代表值,由此生成低密度的数据。因此,以能够周期性取得传感器值或具有规则性的值为前提。

[0039] 然而,有时取得周期或传感器值的规则性会被攻击者严重破坏。在专利文献1中,由于简单地提取代表值,所以会导致在周期性的传感器数据的采样时有时欠缺由攻击者注入的攻击值,难以进行攻击的检测。也就是说,在采样时有时由攻击者注入的攻击值没有被采样。因此,谋求构筑与攻击检测相适的、更进一步的采样方法。

[0040] 在专利文献2中,作为攻击检测方法,事先算出传感器数据的正常周期,在实际观测到的周期不在正常周期加上容限(margin)后的范围内的情况下,判定为攻击消息。容限是容许由正常消息与攻击消息的冲突产生的延迟的范围。本方法作为能够检测所追加的攻击消息等方法而具有鲁棒性。

[0041] 然而,在专利文献2中,由于基于消息的取得时间进行有无攻击的判定,所以难以适用于通过传感器数据的采样使1个传感器值的取得间隔成为采样间隔的数据。

[0042] 另外,在非专利文献1中,作为攻击检测方法,公开了如下技术,即,事先学习传感器值的正常的举止,在基于实际观测到的传感器值的列表来预测接下来的传感器值的结果背离了正常的举止的情况下,判定为攻击消息。本方法也能够适用于与采样间隔等周期相比较长的时间间隔的时序数据。

[0043] 然而,为了预测接下来的传感器值而实际观测到的传感器值的列表必须以攻击消息不会混入的方式而充足。

[0044] 因此,为了解决上述技术问题,与采样方法的构筑相配合地,攻击检测方法也需要进一步的改良。也就是说,期望能够兼顾数据量削减和攻击检测性能。因此,本申请的发明人对能够兼顾数据量削减和攻击检测性能的攻击检测方法等进行了锐意研究,并提出了以下说明的攻击检测方法等。

[0045] 本公开的一技术方案的攻击检测方法,是检测在对移动体(mobility)内部为了进行移动体的控制而收发的传感器数据的攻击的攻击检测方法,包括:采样方针决定步骤,按所述传感器数据所包含的传感器值的每个标识符,基于表示所述传感器数据的所述传感器值的偏差的统计值、以及表示所述传感器值的变化的时机的所述移动体的事件信息中的至少一方,决定包含从所述传感器数据中提取用于检测所述攻击的所述传感器值的采样间隔和每个该采样间隔的采样时间的采样方针;采样数据生成步骤,基于所述采样间隔和所述采样时间,生成采样数据,所述采样数据包含:从所述传感器数据中提取出的2个以上的传感器值、表示所述采样时间中的所述2个以上的传感器值的时间上的顺序的第一顺序信息、以及表示每个所述采样间隔的所述2个以上的传感器值的时间上的顺序的第二顺序信息;攻击判定步骤,基于所述采样数据所包含的评价对象数据的传感器值、所述第一顺序信息、以及表示取得了所述评价对象数据的所述采样时间中的与所述评价对象数据相比过去的传感器值的时序数据的短期传感器流,算出表示所述评价对象数据的异常的程度的第一异常得分,基于所述评价对象数据的传感器值、所述第二顺序信息、以及表示以与取得了所述评价对象数据的所述采样间隔相比过去的所述采样间隔取得了的传感器值的变化的长期传感器流,算出表示所述评价对象数据的异常的程度的第二异常得分,基于所算出的所述第一异常得分和所述第二异常得分,判定所述评价对象数据是否是受到所述攻击的数据,并输出判定结果。

[0046] 由此,与成为攻击检测处理的对象的传感器数据的特征相配合地,调整采样间隔和采样时间,进行采样数据的生成。进而,基于包含表示采样时间(短期)和采样间隔(长期)中的传感器值的时间上的顺序的2种顺序信息(例如,索引)在内的采样数据,算出2种异常得分,由此进行攻击的判定。例如,通过将采样间隔以及采样时间中的至少一方设定得长,能够削减数据量。另外,通过算出2种异常得分,与仅算出1种异常得分的情况相比,能够高精度地检测攻击。由此,能够在抑制监视成本的同时高精度进行攻击检测。由此,能够兼顾数据量削减和攻击检测性能。

[0047] 另外,例如也可以是,所述统计值包含表示每个所述标识符的传感器值的偏差的方差值,所述事件信息包含表示是否发生了所述传感器值的变化的标记信息,在所述采样方针决定步骤中,基于所述方差值和所述标记信息,决定所述采样间隔和所述采样时间。

[0048] 由此,由于使用传感器值的方差值以及标记信息这两方,所以能够更准确地决定采样间隔和采样时间。

[0049] 另外,例如也可以是,在所述采样方针决定步骤中,根据所述方差值是否为第一阈值以上的判定结果、和表示所述标记信息是否表示没有发生所述传感器值的变化这一情况的组合,决定所述采样时间和所述采样间隔。

[0050] 由此,通过传感器数据的方差值的判定结果和事件信息的内容的组合,能够决定采样间隔和采样时间。由此,能够通过判定结果决定适当的采样间隔和采样时间。例如,在方差值不为第一阈值以上的情况下,由于传感器值是稳定的,所以能够将采样间隔以及采

样时间中的至少一方决定为长的时间。由此,能够适当削减所提取的传感器数据的数据量。

[0051] 另外,例如也可以是,所述标记信息包含表示是否发生了所述移动体的驱动部的ON和OFF的切换、换挡杆的切换、以及自动驾驶模式的ON和OFF的切换中的至少1个的信息。

[0052] 由此,能够决定与移动体的驱动部、换挡杆、以及自动驾驶模式的切换相应的采样间隔和采样时间。例如,能够将从发生切换起预定时间经过后的采样间隔以及采样时间的至少一方决定为长的时间。由此,能够更加适当地削减传感器数据的数据量。

[0053] 另外,例如也可以是,在所述采样数据生成步骤中,基于在所述采样时间中应观测的正常接收数据数,决定在所述采样时间内提取的传感器数据的提取数,并提取所决定了的所述提取数的传感器数据。

[0054] 由此,能够基于所观测到的传感器数据数,更加适当地削减传感器数据的数据量。

[0055] 另外,例如也可以是,在所述采样数据生成步骤中,判定所述采样时间中所观测到的所述传感器值数是否为所述正常接收数据数以上,在为所述正常接收数据数以上的情况下,提取预定数的所述传感器值,在不为所述正常接收数据数以上的情况下,将所述传感器数据所包含的所述传感器值全数提取。

[0056] 由此,在传感器数据包含攻击数据的情况下,能够抑制攻击数据的欠缺并进行采样。由此,能够对采样数据高精度地进行攻击检测。

[0057] 另外,例如也可以是,所述第一顺序信息是表示在所述采样时间中所述2个以上的传感器值被取得的顺序的第一索引,所述第二顺序信息是表示所述2个以上的传感器值被取得的所述采样间隔的顺序的第二索引,在所述攻击判定步骤中,在所述评价对象数据所关联的所述第一索引低于第三阈值、且所述评价对象数据所关联的所述第二索引低于第四阈值的情况下,判定为不清楚所述评价对象数据是否是受到所述攻击的数据,在基于所述第一异常得分以及所述第二异常得分的第三异常得分为第五阈值以上的情况下,判定为所述评价对象数据是受到所述攻击的数据,在所述第三异常得分低于所述第五阈值的情况下,判定为所述评价对象数据是正常的,将表示所判定出的结果的所述评价对象数据所关联的所述判定结果输出。

[0058] 由此,能够削减采样数据中的攻击检测困难的评价对象数据,并能够进行基于短期的以及长期的传感器值的变化的统合性的判定。由此,能够对采样数据高精度地进行攻击检测。

[0059] 另外,例如,还可以包括更新步骤,所述更新步骤中,基于所述评价对象数据所关联的所述判定结果、所述第一顺序信息、以及所述第二顺序信息,更新所述短期传感器流和所述长期传感器流。

[0060] 由此,能够更新在攻击检测的判定中使用的短期传感器流和长期传感器流。通过使用更新后的短期传感器流和长期传感器流,能够提高攻击检测性能。

[0061] 另外,例如也可以是,在所述更新步骤中,在所述评价对象数据所关联的所述判定结果是攻击的情况下,使用所述短期传感器流和所述长期传感器流中的至少1个推定所述评价对象数据应该能取的传感器值,基于所推定出的推定传感器值、所述第一顺序信息、以及所述第二顺序信息,更新所述短期传感器流和所述长期传感器流,在所述评价对象数据所关联的所述判定结果是正常或者不清楚的情况下,基于所述评价对象数据的传感器值、所述第一顺序信息、以及所述第二顺序信息,更新所述短期传感器流和所述长期传感器流。

[0062] 由此,即使在采样数据中包含攻击数据的情况下,也能够除去攻击数据,更新为适当的短期传感器流以及长期传感器流。也就是说,能够抑制在短期传感器流以及长期传感器流中包含攻击数据这一情况。由此,能够对采样数据进行更高精度的攻击检测。

[0063] 另外,例如,所述传感器数据也可以存储于搭载于所述移动体的设备,并且是遵从CAN(Controller Area Network:注册商标),CAN FD(CAN with Flexible Data—rate),FlexRay(注册商标),以及EtherNet(注册商标)中的至少1个协议对以任意的行驶时间间隔所收发的以字节表现的网络数据进行了解码而得到的结果。

[0064] 由此,在遵从CAN、CAN FD、FlexRay、以及EtherNet中的至少1个协议进行通信的网络中,能够兼顾数据量削减和攻击检测性能。

[0065] 另外,例如,所述移动体也可以是车辆。

[0066] 由此,能够削减计算资源有限的车辆中的数据量,并能够抑制对该车辆的攻击的攻击检测性能的降低。

[0067] 另外,本公开的一技术方案的攻击检测系统,是检测对在移动体内部用于进行移动体的控制而收发的传感器数据的攻击的攻击检测系统,具备:采样方针决定部,按所述传感器数据所包含的传感器值的每个标识符,基于表示所述传感器数据的所述传感器值的偏差的统计值、以及表示所述传感器值的变化的时机的所述移动体的事件信息中的至少一方,决定包含从所述传感器数据中提取用于检测所述攻击的所述传感器值的采样间隔和每个该采样间隔的采样时间的采样方针;采样数据生成部,基于所述采样间隔和所述采样时间,生成采样数据,所述采样数据包含:从所述传感器数据中提取出的2个以上的传感器值、表示所述采样时间中的所述2个以上的传感器值的时间上的顺序的第一顺序信息、以及表示每个所述采样间隔的所述2个以上的传感器值的时间上的顺序的第二顺序信息;攻击判定部,基于所述采样数据所包含的评价对象数据的传感器值、所述第一顺序信息、以及表示取得了所述评价对象数据的所述采样时间中的与所述评价对象数据相比过去的传感器值的时序数据的短期传感器流,算出表示所述评价对象数据的异常的程度的第一异常得分,基于所述评价对象数据的传感器值、所述第二顺序信息、以及表示以与取得了所述评价对象数据的所述采样间隔相比过去的所述采样间隔取得了的传感器值的变化的长期传感器流,算出表示所述评价对象数据的异常的程度的第二异常得分,基于所算出的所述第一异常得分和所述第二异常得分,判定所述评价对象数据是否是受到所述攻击的数据,并输出判定结果。另外,本公开的一技术方案的程序记录介质是用于使计算机执行上述的攻击检测方法的程序记录介质。

[0068] 由此,实现与上述的攻击检测方法同样的效果。

[0069] 此外,这些整体或具体的技术方案也可以由系统、方法、集成电路、计算机程序或计算机可读取CD—ROM等记录介质而实现,也可以由系统、方法、集成电路、计算机程序或记录介质的任意组合而实现。

[0070] 以下,针对实施方式的监视方法(攻击检测方法的一例)等,一边参照附图一边说明。在此示出的实施方式均表示总括的或具体的例子。因此,以下的实施方式中示出的数值、构成要素、构成要素的配置以及连接方式、以及步骤和步骤的顺序等是一例,并非限定本公开的发明。另外,以下的实施方式的构成要素中独立权利要求没有记载的构成要素是能够任意附加的构成要素。另外,各图是示意图,并非进行了严格的图示。

[0071] (实施方式)

[0072] 首先,说明本实施方式的监视系统的构成。在本实施方式中,对监视系统100是用于检测对在车辆内部为了进行车辆控制而收发的传感器数据(车辆传感器数据)的攻击的信息处理系统的例子进行说明。车辆是作为监视系统100检测攻击的对象的移动体(mobility)的一例。另外,监视系统100是攻击检测系统的一例。

[0073] [1—1.监视系统的构成]

[0074] 图1是表示本实施方式的监视系统100的构成的框图。

[0075] 监视系统100是用于按照车辆传感器数据(参照图5)中的评价对象数据判定是否(受到)攻击的系统。监视系统100判定该评价对象数据是否是受到攻击的数据。此外,也将判定该评价对象数据是否是受到攻击的数据记载为是否是攻击数据。评价对象数据也可以说是判定是否是攻击数据的对象的传感器值。

[0076] 另外,车辆传感器数据存储于搭载于车辆的设备,是例如遵循CAN(Controller Area Network:注册商标),CAN FD(CAN with Flexible Data—rate),FlexRay(注册商标),以及EtherNet(注册商标)中的至少1个协议,按任意的行驶时间间隔(移动时间间隔的一例)收发的以字节表现的网络数据被解码得到的结果。

[0077] 监视系统100具备采样部101和采样数据监视部102。采样部101例如搭载于车辆,采样数据监视部102例如配置于与车辆不同的场所(例如,位于远程位置的监视中心)。采样部101以及采样数据监视部102以能够彼此通信(例如,能够进行无线通信)的方式连接。

[0078] 采样部101蓄积为了进行车辆的车辆控制而收发的车辆传感器数据,基于采样方针从所蓄积的多个传感器值(车辆传感器数据)中提取在采样数据监视部102的监视中所使用的传感器值,将包含所提取出的传感器值的采样数据向采样数据监视部102发送。采样方针由采样部101动态决定。采样部101例如按车辆传感器数据所包含的传感器值的每个标识符(以后,也记载为传感器标识符),基于表示车辆传感器数据的传感器值的偏差的统计值、以及表示传感器值的特征的变化(例如,传感器值的变化)的时机的车辆事件信息中的至少一方,决定采样方针。采样数据例如包含2个以上的传感器值。此外,针对传感器标识符稍后说明,但是是用于唯一确定“车速”、“挡位”等车辆传感器数据的信息。

[0079] 车辆传感器数据包含搭载于车辆的各种传感器的传感器值(例如,车速、加速度、操舵角等感测结果)。此外,针对采样方针稍后说明(参照图6),但是采样方针包含采样间隔、以及每个该采样间隔的采样时间。

[0080] 车辆事件信息包含与非周期性的车辆事件相关的信息,例如包含表示是否发生了传感器值的变化的标记信息。标记信息例如包含表示是否发生了车辆的发动机(移动体的驱动部的一例)的ON以及OFF的切换、换挡杆的切换、自动驾驶模式的ON以及OFF的切换中的至少1个信息。例如也可以是,标记信息在发生了车辆事件的情况下,包含表示“有”的“1”,在没有发生车辆事件的情况下,包含表示“无”的“0”。另外,监视包含向车辆的网络(cyber)攻击的检测处理。此外,车辆的发动机的ON以及OFF的切换例如也可以是发动机进行了再起动。

[0081] 采样部101具备:采样方针生成部110、采样数据生成部111、车辆传感器数据存储部112、采样方针存储部113、车辆信息存储部114、以及通信部115。

[0082] 采样方针生成部110是基于车辆传感器数据以及车辆事件中的至少一方,决定用

于生成采样数据的采样方针的处理部。在本实施方式中,采样方针生成部110基于车辆传感器数据以及车辆事件这两方决定采样方针。采样方针生成部110例如基于表示车辆传感器数据的传感器值的偏差的统计值和车辆事件的发生的时机(timing),决定采样方针。采样方针生成部110是采样方针决定部的一例。

[0083] 此外,传感器值的统计值也可以使用表示传感器值的偏差的任意指标。在本实施方式中,传感器值的统计值使用表示每个标识符的传感器值的偏差的方差值(数据方差)。方差值是表示传感器值的分散程度的值,并通过对偏差(各个传感器值与平均值之差)进行平方并取平均而算出。方差值例如是标准偏差。

[0084] 车辆事件的发生的时机(timing)表示车辆事件发生时的时机,例如,也可以说表示传感器值的特征的变化的时机。另外,车辆事件的发生的时机也可以说表示有无发生车辆事件。

[0085] 采样方针生成部110例如是按车辆传感器数据所包含的传感器值的每个传感器标识符来决定采样方针的处理部。采样方针生成部110例如基于一个传感器标识符所对应的多个传感器值,决定该一个传感器标识符的采样方针。该采样方针是用于根据该一个传感器标识符所对应的多个传感器值来生成采样数据的采样方针。

[0086] 采样数据生成部111是基于采样方针生成部110所决定的采样方针,生成用于向采样数据监视部102发送的采样数据的处理部。采样数据生成部111例如基于所决定的采样方针,从车辆传感器数据存储部112所存储的多个传感器值中提取2个以上的传感器值,从而生成包含所提取的2个以上的传感器值的采样数据。

[0087] 采样数据生成部111例如基于采样间隔和采样时间,生成包含从多个传感器值(车辆传感器数据)中提取出的2个以上的传感器值、表示采样时间中的2个以上的传感器值的时间上的顺序的第一索引、以及表示每个采样间隔的2个以上的传感器值的时间上的顺序的第二索引的采样数据。按每个传感器值,赋予第一索引以及第二索引。

[0088] 第一索引表示在采样时间中取得(观测到)2个以上的传感器值的顺序,也可以说表示采样时间中的短期的传感器值的活动(变化)的顺序。第二索引表示取得(观测到)2个以上的传感器值的采样间隔的顺序,也可以说表示在采样间隔中的长期的传感器值的活动(变化)的顺序。第一索引是第一顺序信息的一例,第二索引是第二顺序信息的一例。

[0089] 车辆传感器数据存储部112是存储为了进行车辆的车辆控制而收发的多个传感器值(车辆传感器数据)的存储装置。车辆传感器数据存储部112蓄积多个传感器值。

[0090] 采样方针存储部113是存储采样方针生成部110决定了的采样方针的存储装置。

[0091] 车辆信息存储部114是存储车辆事件的存储装置。车辆信息存储部114例如存储车辆事件的内容、和与车辆事件发生的时刻相关联的车辆事件信息。

[0092] 通信部115是具有经由互联网等公共通信网络与采样数据监视部102通信的功能的处理部。通信部115例如包含通信回路(通信模块)而构成。

[0093] 接着,采样数据监视部102基于从采样部101取得的采样数据监视车辆。具体而言,采样数据监视部102基于采样数据,算出表示短期的异常的第一异常得分、以及表示长期的异常的第二异常得分,基于所算出的2个异常得分来判定成为评价对象的传感器值(以后,也记载为评价对象数据)是否是受到攻击的数据。也就是说,采样数据监视部102判定评价对象数据是否是攻击数据。采样数据监视部102也可以说判定车辆是否受到网络攻击。采样

数据监视部102具有基于2个异常得分进行攻击检测这一特征。

[0094] 此外,短期的异常表示基于短期间所取得的车辆传感器数据而检测的异常,例如,表示基于在1个采样时间内取得的车辆传感器数据而检测的异常。另外,长期的异常表示基于在比短期间长的长期间中所取得的车辆传感器数据而检测的异常,例如,表示基于按多个采样间隔的每一个而取得的车辆传感器数据而检测的异常。

[0095] 采样数据监视部102具备:攻击检测部120、基点数据更新部121、检测器存储部122、检测结果存储部123、基点数据存储部124、以及采样数据存储部125。

[0096] 攻击检测部120是基于从采样部101取得的采样数据,进行评价对象数据是否是攻击数据的判定的处理部。攻击检测部120算出第一异常得分和第二异常得分,基于所算出的第一异常得分和第二异常得分,判定评价对象数据是否受到攻击,输出判定结果。就第一异常得分以及第二异常得分的算出而言,稍后说明。

[0097] 基点数据更新部121是基于表示评价对象数据所关联的攻击检测部120的检测结果的检测结果信息、和所提取出的车辆传感器数据中的第一索引以及第二索引,对短期传感器流和长期传感器流进行更新的处理部。

[0098] 短期传感器流是为了检测短期的异常而使用的传感器值的时序数据,例如基于1个采样时间内取得的传感器值而生成。短期传感器流例如基于评价对象数据被取得的采样时间内的传感器值而生成。短期传感器流也可以说表示被判定为是正常的或被推定为是正常的、短期的传感器值的活动。

[0099] 长期传感器流是为了检测比短期传感器流长的长期的异常而使用的传感器值的时序数据,例如基于按多个采样间隔的每一个采用间隔的传感器值而生成。长期传感器流也可以说表示被判定为是正常的或被推定为正常的、长期的传感器值的活动。

[0100] 此外,也将包含短期传感器流以及长期传感器流的数据记载为基点数据。基点数据不包含攻击检测部120判定为是异常的(攻击的)传感器值。基点数据也可以说表示被判定为是正常的或被推定为是正常的传感器值的时序数据。

[0101] 检测器存储部122是存储用于算出表示短期传感器流与评价对象数据的背离程度的第一异常得分的第一检测器、以及算出长期传感器流与该评价对象数据的背离程度的第二异常得分的第二检测器的存储装置。第一检测器例如通过以将短期传感器流和评价对象数据作为输入,算出第一异常得分的方式进行了机器学习的学习完成模型而实现。另外,第二检测器例如通过以将长期传感器流和评价对象数据作为输入,算出第二异常得分的方式进行了机器学习的学习完成模型而实现。此外,存储学习完成模型意味着,将机器学习模型中的网络参数、运算的算法(机器学习算法)等信息进行存储。

[0102] 检测结果存储部123是存储攻击检测部120的检测结果的存储装置。

[0103] 基点数据存储部124是存储攻击检测部120用于进行有无攻击的判定的短期传感器流以及长期传感器流(基点数据)的存储装置。

[0104] 采样数据存储部125是存储从采样部101取得的采样数据的存储装置。

[0105] 通信部126是具有经由互联网等公共通信网络与采样部101通信的功能的处理部。通信部126例如包含通信回路(通信模块)而构成。

[0106] 车辆传感器数据存储部112、采样方针存储部113、车辆信息存储部114、检测器存储部122、检测结果存储部123、基点数据存储部124、以及采样数据存储部125例如由硬盘驱

动器或固态硬盘等可改写的非易失性存储器构成。

[0107] 采样方针生成部110、采样数据生成部111、通信部115、攻击检测部120、基点数据更新部121、以及通信部126例如由CPU、ASIC、或FPGA(Field Programmable Gate Array:现场可编程门阵列)等处理器构成。此外,监视系统100具备的各功能块通过CPU等处理器执行计算机所保持的计算机可读取程序而实现。

[0108] 此外,采样部101以及采样数据监视部102的通信方法没有特别限定。在通信方法是无线通信的情况下,采样部101以及采样数据监视部102的通信也可以通过红外线通信或电波通信进行。电波通信也可以是基于Wi—Fi(注册商标)(Wireless Fidelity),或Bluetooth(注册商标)的通信。另外,例如,采样部101以及采样数据监视部102的通信也可以通过有线通信进行。

[0109] 此外,在将采样部101和采样数据监视部102一体构成的情况下,采样部101和采样数据监视部102之间的通信各自不经由通信部115和通信部126也可。该情况下,无需通信部115以及通信部126的构成。

[0110] [1—2.监视系统的动作的概略]

[0111] 接着,说明如上所述构成的监视系统100的动作。图2是表示本实施方式的监视系统100的动作(攻击检测方法)的概要的流程图。图2所示的步骤S101以及S102例如是在采样部101中执行的处理,步骤S103以及S104例如是在采样数据监视部102中执行的处理。

[0112] 首先,监视系统100进行使用车辆传感器数据存储部112所存储的、车辆中的预定的行驶时间的车辆传感器数据,生成表示采样间隔以及采样时间的采样方针的采样方针生成处理(S101)。步骤S101的处理通过采样方针生成部110实施。预定的行驶时间例如也可以预先设定,也可以由通过监视系统100监视车辆的监视者设定。此外,步骤S101是采样方针决定步骤的一例。

[0113] 接着,监视系统100进行基于所决定的采样方针,根据车辆传感器数据生成采样数据的采样数据生成处理(S102)。步骤S102的处理通过采样数据生成部111实施。此外,步骤S102是采样数据生成步骤的一例。

[0114] 采样数据生成部111基于采样方针,从车辆传感器数据提取一部分车辆传感器数据(传感器值),对所提取出的各个车辆传感器数据(传感器值),附加第一索引和第二索引来生成采样数据。也就是说,采样数据包含所提取出的车辆传感器数据、第一索引以及第二索引。

[0115] 然后,采样数据生成部111将所生成的采样数据通过通信部115向通信部126发送。也就是说,采样数据生成部111将所生成的采样数据向采样数据监视部102发送。

[0116] 接着,监视系统100进行对采样数据的车辆传感器数据(评价对象数据)算出异常得分的攻击检测处理(S103)。步骤S103的处理通过攻击检测部120实施。步骤S103是攻击判定步骤的一例。

[0117] 攻击检测部120实施如下攻击判定处理,即,使用基点数据存储部124所存储的基点数据,以2种算出方法算出表示评价对象数据的传感器值的异常的程度的异常得分,使用所算出的2种异常得分,判定评价对象数据的传感器值是否(受到)攻击。

[0118] 接着,监视系统100实施如下基点数据更新处理,即,使用评价对象数据的第一索引、第二索引以及攻击检测处理的结果(判定结果),为了进行接下来的评价对象数据中的

攻击检测处理而更新基点数据(S104)。步骤S104的处理通过基点数据更新部121实施。步骤S104是更新步骤的一例。

[0119] 以后,对各处理部的详细构成以及流程图的各步骤的详细动作进行说明。

[0120] [2—1.采样方针生成部的构成]

[0121] 图3是表示本实施方式的采样方针生成部110的构成的框图。如图3所示,采样方针生成部110具备:车辆传感器数据取得部130、传感器数据稳定度算出部131、采样方针判定部132。

[0122] 车辆传感器数据取得部130是从车辆传感器数据存储部112取得车辆采样数据的处理部。车辆传感器数据取得部130读出车辆传感器数据存储部112所存储的车辆传感器数据。

[0123] 传感器数据稳定度算出部131是基于车辆传感器数据来算出用于在采样方针判定部132的采样方针的判定中使用的信息的处理部。例如,传感器数据稳定度算出部131按每个传感器标识符,算出传感器值的统计值。在本实施方式中,传感器数据稳定度算出部131按每个传感器标识符,算出传感器值的方差值。

[0124] 此外,传感器标识符包含车速等周期性收发的周期型的标识符、以及挡位的切换等根据驾驶员的操作等而发生的事件型的标识符。

[0125] 采样方针判定部132按车辆传感器数据所包含的每个传感器标识符,使用统计值以及车辆事件信息中的至少一方决定采样方针。在本实施方式中,采样方针判定部132使用统计值以及车辆事件信息这两方决定采样方针。

[0126] [2—2.采样方针生成部的动作]

[0127] 图4是表示本实施方式的采样方针生成处理(S101)的流程图。

[0128] 首先,采样方针生成部110取得车辆传感器数据存储部112所存储的车辆中的预定的行驶时间的车辆传感器数据(S111)。步骤S111的处理通过车辆传感器数据取得部130实施。车辆传感器数据取得部130例如从车辆传感器数据存储部112取得车辆传感器数据。

[0129] 在此,对车辆传感器数据进行说明。图5是表示本实施方式的车辆传感器数据的一例的图。车辆传感器数据是从以二进制表现的车辆网络数据中提取出可能成为攻击检测处理的输入的信息而得到的数据。如图5所示,车辆传感器数据包含:传感器标识符142、数据ID143、取得时刻144、传感器值145。

[0130] 传感器标识符142是用于唯一确定车辆传感器数据所包含的1个传感器数据的车辆控制对象的标识符。例如,作为传感器标识符142,包含“车速”、“挡位”等。

[0131] 数据ID143是用于根据车辆传感器数据所包含的上述的传感器标识符来唯一确定1个车辆传感器数据141的标识符。例如,作为数据ID143,包含从1起依次分配的数值。数据ID143例如根据传感器标识符被从1起依次分配。另外,数据ID143例如被分配为取得时刻的顺序。

[0132] 取得时刻144是表示从车辆网络接收到车辆传感器数据的时刻的时刻数据。取得时刻144例如在传感器标识符142是“车速”的情况下,表示周期性的时刻,在传感器标识符142是可能有“挡位”等事件发生的标识符的情况下,也可以取非周期性的时刻。取得时刻144例如能够根据发送车辆传感器数据的消息的时间戳而取得。

[0133] 此外,取得时刻144也可以是采样部101从车辆网络接收到车辆传感器数据的时

刻。另外,虽然示出了取得时刻144是从成为基准的时刻起的经过时间(相对时刻)的例子,但不限于此,也可以是绝对时刻。

[0134] 传感器值145是表示传感器标识符142所关联的车辆控制内容的数值数据。在车辆传感器数据中包含多个传感器值。

[0135] 在图5中,可知例如在传感器标识符142是“车速”的情况下,取得时刻144是“25.00ms”时传感器值145是“22.11km/h”,在接下来的取得时刻144是“50.01ms”时传感器值145是“22.50km/h”,车速的接收周期约为25ms。以下,对车速的接收周期约为25ms的例子进行说明,但接收周期不限定于此。

[0136] 再参照图4,返回采样方针生成处理的说明。采样方针生成部110按车辆传感器数据所包含的每个传感器标识符142,算出表示传感器值145的偏差的数据方差(例如,方差值),以及车辆传感器数据所包含的、表示事件型的传感器标识符142的车辆事件是否发生的车辆事件信息(例如,标记信息)(S112)。事件型的传感器标识符142例如包含发动机ON和OFF的切换以及挡位的切换等。步骤S112的处理通过传感器数据稳定度算出部131而实施。

[0137] 接着,采样方针生成部110判定车辆事件信息(标记信息)是否是“有”,或者数据方差是否为第一阈值以上(S113)。步骤S113的处理通过采样方针判定部132而实施。

[0138] 采样方针判定部132在数据方差为第一阈值以上的情况下,或者车辆事件标记信息是“有”、即,发生了车辆事件的情况下(S113中是),将采样方针设定为高密度的采样(高密度采样)(S114)。例如,在数据方差为第一阈值以上的情况下,由于车辆传感器数据的稳定度小(例如,偏差大),所以进行高密度采样。其原因在于,在数据方差为第一阈值以上的情况下,采样后的有无攻击的判定结果的再现率低。另外,例如,由于假设在车辆事件刚刚发生之后起一定时间,车辆传感器数据的稳定度小,所以进行高密度采样。其原因在于,通过车辆事件发生来初始化(reset:重置)长期传感器流的情况下,长期传感器流中的传感器值并不充分(足够)。

[0139] 另外,采样方针判定部132在除此以外的情况下(S113中为否),即,在数据方差低于第一阈值、且车辆事件信息是“无”的情况下,将采样方针设定为低密度的采样(低密度采样)(S115)。例如,在数据方差低于第一阈值的情况下,由于车辆传感器数据的稳定度大(例如,偏差小),所以进行低密度采样。其原因在于,在除此以外的情况下,采样后的有无攻击的判定结果的再现率高。另外,例如,假设在车辆事件刚刚发生之后起一定时间以外,车辆传感器数据的稳定度大,所以进行低密度采样。其原因在于,若为该一定时间以外,则长期传感器流中的传感器值是充分(足够)的。

[0140] 此外,在此的低密度以及高密度是相对的含义,高密度采样意味着采样密度比低密度采样要高。另外,采样密度通过采样时间以及采样间隔中的至少1个增减来实现。高密度采样例如与低密度采样相比,满足采样时间较长以及采样间隔较短中的至少1个。例如,也可以是,高密度采样与低密度采样相比,采样时间较长且采样间隔较短。

[0141] 接着,采样方针判定部132将所设定的采样方针存储于采样方针存储部113(S116)。

[0142] 如上所述,采样方针生成部110例如基于方差值和标记信息,决定采样间隔和所述采样时间。例如,采样方针生成部110也可以根据方差值是否为第一阈值以上的判定结果、和标记信息是否表示传感器值没有发生变化的组合,决定采样时间和采样间隔。

[0143] 在此,对采样的详情进行说明。图6是说明本实施方式的采样的图。图6所示的“○”表示取得了车辆传感器数据这一情况,图6的横轴表示时间。在图6中示出了,在采样间隔T秒中,取得了10个车辆传感器数据(传感器值)的例子。

[0144] 如图6所示,采样间隔是进行车辆传感器数据的采样的间隔,采样时间是在该采样间隔中持续采样的时间。采样时间是时间上连续的时间,例如,不包含离散的时间。也就是说,在采样时间中被采样的车辆传感器数据成为时间上连续的数据。采样开始时刻是开始车辆传感器数据的采样的时刻,例如也可以是采样时间的公开(开始)时刻。此外,采样开始时刻不限定于采样间隔的开始时刻(例如,开始计测采样间隔的时间的时刻),只要是从采样间隔的开始时刻起经过(T－S)秒之前即可。也就是说,若将采样开始时刻设为N,则N可以被决定为满足以下式。

[0145] $0 \leqq N < T - S$ (式1)

[0146] 车辆传感器数据的采样在采样间隔T秒之中、从采样开始时刻第N秒起采样时间S秒之间的范围内进行。

[0147] 将采样间隔T秒之中、从采样开始时刻第N秒起采样时间S秒之间的车辆传感器数据作为采样数据。也就是说,在图6中,示出了在采样间隔T秒中取得了10个车辆传感器数据,但是将其中3个车辆传感器数据提取为采样数据的例子。换言之,在采样间隔T秒中所取得的10个车辆传感器数据之中、7个车辆传感器数据没有被发送至采样数据监视部102。在此,通过调整采样间隔以及采样时间,实现高密度的采样和低密度的采样。采样的具体例稍后说明。

[0148] 图7是表示本实施方式的采样方针数据的一例的图。在图7的例子中,高密度采样中的采样间隔是200.00ms,采样时间是75.00ms,低密度采样中的采样间隔是1000.00ms,采样时间是55.00ms。这样,例如,高密度采样中的采样间隔比低密度采样中的采样间隔要短,例如,是低密度采样中的采样间隔的1/5左右。另外,例如,高密度采样中的采样时间比低密度采样中的采样时间要长,例如,是低密度采样中的采样间隔的1.35倍左右。此外,高密度采样中的采样间隔以及采样时间、和低密度采样中的采样间隔以及采样时间不限定于上述。

[0149] 如图7所示,采样方针数据包含:传感器标识符152、文件编号153、数据方差154、车辆事件标记155、采样间隔156、采样时间157。采样方针数据存储于采样方针存储部113,是将传感器标识符152、在采样方针判定部132的判定中使用的信息(数据方差154以及车辆事件标记155)、以及采样方针(采样间隔156以及采样时间157)进行了关联得到的历史记录。

[0150] 传感器标识符152与车辆传感器数据的传感器标识符142关联,并且是用于唯一确定车辆控制对象的标识符。

[0151] 文件编号153是用于识别由通信部115发送的1个文件单位的文件标识符。例如,按照根据每预定的行驶时间所取得的车辆传感器数据,增加(increment)文件编号,算出不同的采样方针。

[0152] 数据方差154是以文件单位表示按每个传感器标识符152算出的预定行驶时间内的传感器值的偏差的数值数据。

[0153] 车辆事件标记155是表示,与传感器标识符152不同地表示发动机ON和OFF的切换以及挡位的切换等事件型的传感器标识符142的车辆事件是否发生的标记信息。

[0154] 采样间隔156表示以文件单位按每个传感器标识符152算出的采样的密度。

[0155] 采样时间157表示文件内按每个传感器标识符152算出的采样的密度。

[0156] 另外,采样方针生成部110在每当更新成为处理对象的车辆传感器数据时反复执行步骤S111～S115的处理。

[0157] 例如,在图7的文件编号是“2”、传感器标识符152是“车速”的情况下,数据方差是0.22、车辆事件标记是“无”。在将数据方差的阈值定为10时,0.22为阈值以下。因此,在上述情况下,成为进行低密度的采样的方针,例如,以相对于上述的周期“约25ms”变长的方式,将采样间隔设为“1000ms”,以成为上述周期的约2倍的方式,将采样时间设为“55ms”,从而能够大幅削减将发送的数据量。

[0158] 此外,采样方针判定部132也可以设定在数据方差为第一阈值以上的情况下和车辆事件标记信息是“有”的情况下彼此不同的采样密度。也就是说,也可以在高密度采样中设定多个采样密度。

[0159] [3—1.采样数据生成部的构成]

[0160] 图8是表示本实施方式的采样数据生成部111的构成的框图。如图8所示,采样数据生成部111具备:车辆传感器数据取得部130、采样信息取得部160、数据提取部161、索引赋予部162。

[0161] 车辆传感器数据取得部130是从车辆传感器数据存储部112取得车辆采样数据的处理部。车辆传感器数据取得部130读出车辆传感器数据存储部112所存储的车辆采样数据。此外,车辆传感器数据取得部130既可以是与采样方针生成部110具有的车辆传感器数据取得部130共同的构成要素,也可以是彼此不同的构成要素。

[0162] 采样信息取得部160是将采样方针生成部110决定了的采样方针从采样方针存储部113取得的处理部。

[0163] 数据提取部161是从车辆传感器数据取得部130取得的车辆传感器数据中提取基于采样方针存储部113取得的采样方针得到的车辆传感器数据的处理部。

[0164] 索引赋予部162是对于数据提取部161提取出的车辆传感器数据,将表示时间上的顺序的索引与传感器值进行关联而赋予的处理部。索引赋予部162按每个车辆传感器数据(传感器值),赋予第一索引以及第二索引这两方。

[0165] [3—2.采样数据生成部的动作]

[0166] 图9是表示本实施方式的采样数据生成处理(S102)的流程图。

[0167] 首先,采样数据生成部111按每个传感器标识符,取得包含采样间隔和采样时间的采样方针数据151以及车辆信息(S121)。步骤S121的处理通过采样信息取得部160实施。采样信息取得部160例如从采样方针存储部113取得采样方针数据151,从车辆信息存储部114取得车辆信息。

[0168] 采样方针数据151包含唯一表示车辆的体系结构(architecture)的车辆编号(未图示)、和表示车辆传感器数据所包含的各个传感器标识符的取得周期的周期(采样间隔以及采样时间)。另外,车辆信息例如包含车辆事件信息。

[0169] 接着,采样数据生成部111取得车辆传感器数据存储部112所包含的预定的行驶时间的车辆传感器数据(S122)。步骤S121的处理通过车辆传感器数据取得部130实施。车辆传感器数据取得部130例如取得图5所示的车辆传感器数据。

[0170] 接着,采样数据生成部111基于车辆传感器数据、和采样方针数据所包含的采样时间,按每1个采样间隔计算采样时间中的接收数据数(S123)。步骤S123的处理通过数据提取部161实施。步骤S123以后,按每个采样时间执行。

[0171] 接着,采样数据生成部111判定接收数据数是否比第二阈值多(S124)。步骤S124的处理通过数据提取部161实施。数据提取部161在上述的接收数据数比采样时间中的正常接收数据数加上预定的容限而得到的值(第二阈值的一例)大的情况下(在S124中为“是”),提取采样时间内的预定数据数的、时间上连续的车辆传感器数据。在步骤S124中为“是”的情况下,有可能在接收数据(传感器值)中包含很多受到攻击的数据。在这样的情况下,若提取全部数据则数据数变多,导致数据量的增加。因此,数据提取部161在步骤S124中为“是”的情况下,仅提取预定数据数的接收数据(S125)。由此,由于能够提取包含受到攻击的数据的预定数据数的接收数据,所以能够削减数据量,并生成能进行攻击检测的采样数据。

[0172] 此外,预定数据数例如是比正常接收数据数大的数。另外,第二阈值不限定于是正常接收数据数加上预定的容限而得到的值,也可以是正常接收数据数,还可以是根据各个传感器标识符而预先设定的固定值。另外,预定的容限例如既可以根据正常接收数据数而设定,也可以是固定值。

[0173] 另外,数据提取部161在上述的接收数据数为采样时间中的正常接收数据数加上预定的容限而得到的值以下的情况下(S124中为“否”),提取正常接收数据数(S126)。数据提取部161例如提取采样时间中的全部接收数据(传感器值)。

[0174] 这样,在步骤S124～S126中,基于采样时间中应观测的正常接收数据数,决定在采样时间内将提取的车辆传感器数据的提取数,并提取所决定的提取数的传感器数据。例如,判定采样时间中观测到的传感器值数是否为正常接收数据数以上,在为正常接收数据数以上的情况下,提取预定数的传感器值,在不为正常接收数据数以上的情况下,提取车辆传感器数据所包含的全部传感器值。

[0175] 在此,正常接收数据数表示上述的采样时间内的正常的接收数据数,基于按每个传感器标识符的上述周期而被事先算出。例如,如图7所示那样,将传感器标识符为“车速”的情况下的采样时间设为“55ms”时,周期是“约25ms”,因此正常接收数据数为“2”。

[0176] 接着,采样数据生成部111对上述的提取数据,赋予表示采样时间中的短期的传感器值的活动的数据顺序的第一索引、和表示按采样间隔的长期的传感器值的活动的顺序的第二索引。也就是说,采样数据生成部111对提取数据所包含的传感器值的每一个,赋予2种索引(S127)。步骤S127的处理通过索引赋予部162而实施。

[0177] 索引赋予部162例如在将采样时间设为了“55ms”的情况下,将采样时间“55ms”中提取出的多个数据从开头起按顺序将第一索引赋予为1、2、3・・・。例如,索引赋予部162从取得时刻旧的数据开始依次对所提取出的多个数据赋予第一索引。

[0178] 索引赋予部162例如还进行,每当执行上述步骤S125或者S126时赋予唯一确定的第二索引。例如,索引赋予部162按采样时间旧的数据开始依次对所提取出的多个数据赋予第二索引。在此,在将采样间隔设为“1000ms”的情况下,第二索引发生变化这一情况是对约“1000ms”后的数据进行处理时。

[0179] 接着,采样数据生成部111判定是否对所提取出的各个传感器值赋予了索引(S128)。步骤S128的处理通过索引赋予部162实施。索引赋予部162例如在预定的行驶时间

所包含的2个以上的采样间隔各自的全部采样时间中,判定是否进行了步骤S123～S127的处理。

[0180] 索引赋予部162在没有对所提取出的各个传感器值赋予索引的情况下(S128中为“否”),返回步骤S123,对接下来的采样时间执行步骤S123以后的处理。也就是说,对成为处理对象的车辆传感器数据,按每个采样间隔反复执行步骤S123～S127的处理。

[0181] 采样数据生成部111在对索引赋予部162提取出的各个传感器值赋予了索引的情况下(S128中为“是”),将提取数据作为采样数据,通过通信部115向通信部126发送。也就是说,采样数据生成部111向采样数据监视部102发送赋予了索引的提取数据(采样数据)(S129)。

[0182] 在此,对采样数据生成部111发送的采样数据(提取数据),参照图10进行说明。图10是表示本实施方式的采样数据的一例的图。

[0183] 如图10所示,采样数据包含:传感器标识符172、评价ID173、传感器值174、第一索引175、第二索引176。

[0184] 传感器标识符172以及传感器值174与车辆传感器数据中的传感器标识符142以及传感器值145(参照图5)同样。评价ID173是用于根据采样数据所包含的各传感器标识符172唯一确定1个传感器数据171的标识符。

[0185] 如上所述,第一索引175表示短期的传感器值的活动的顺序,第二索引176表示长期的传感器值的活动的顺序。

[0186] 例如,评价ID“1”以及“2”表示的传感器值,由于第二索引均是“1”,所以是在相同采样时间所取得的传感器值。另外,由于评价ID“1”表示的传感器值,第一索引是“1”,评价ID“2”表示的传感器值,第一索引是“2”,所以表示在取得了评价ID“1”表示的传感器值之后接着取得了评价ID“2”表示的传感器值。

[0187] 另外,虽然第二索引是“1”以及“2”时的传感器值数是2个,但是第二索引时“3”时的传感器值数为3以上。由于根据各采样时间决定采样方针,所以传感器值数能够根据各采样时间,也即是根据各第二索引而变化。

[0188] 例如,将图10所示的采样数据向采样数据监视部102发送。

[0189] [4—1.攻击检测部的构成]

[0190] 图11是表示本实施方式的攻击检测部120的构成的框图。如图11所示,攻击检测部120具备:采样数据取得部181、基点数据取得部182、第一异常得分算出部183、第二异常得分算出部184、攻击判定部185。

[0191] 采样数据取得部181是从采样数据存储部125取得采样数据的处理部。采样数据取得部181例如取得图10所示的采样数据。

[0192] 基点数据取得部182是从基点数据存储部124取得在攻击判定部185的判定中使用的基点数据的处理部。基点数据取得部182取得短期传感器流以及长期传感器流来作为基点数据。

[0193] 第一异常得分算出部183是基于评价对象数据191以及短期传感器流算出表示评价对象数据191与短期传感器流的背离程度的第一异常得分的处理部。也就是说,第一异常得分算出部183使用在评价对象数据191被取得的采样时间所取得的其他数据,算出对该评价对象数据191的第一异常得分。第一异常得分算出部183算出对1个采样时间内这样的短

期间内的传感器值的变化的异常得分。短期间例如是指,1个采样间隔以下的时间(例如,1个采样时间)。

[0194] 第一异常得分算出部183也可以说,例如基于采样数据所包含的评价对象数据的传感器值、第一索引、表示评价对象数据被取得的采样时间中的比该评价对象数据更靠过去的传感器值的时序数据的短期传感器流,算出表示评价对象数据的异常的程度的第一异常得分。

[0195] 第二异常得分算出部184是基于评价对象数据191以及长期传感器流,算出表示评价对象数据191与长期传感器流的背离程度的第二异常得分的处理部。也就是说,第二异常得分算出部184使用包含评价对象数据191被取得的采样间隔的多个采样间隔的数据,算出对该评价对象数据191的第二异常得分。第二异常得分算出部184算出对多个采样间隔这样的长期间的传感器值的变化的异常得分。长期间是指比短期间长的时间,例如比1个采样间隔长。

[0196] 第二异常得分算出部184也可以说,例如,基于评价对象数据的传感器值、第二索引、表示在比评价对象数据被取得的采样间隔靠过去的采样间隔取得的传感器值的变化的长期传感器流,算出表示评价对象数据的异常的程度的第二异常得分。

[0197] 攻击判定部185是基于所算出的第一异常得分以及第二异常得分,判定评价对象数据191是否是受到攻击的数据,也即是车辆是否受到网络攻击,并输出判定结果的处理部。在本实施方式中,攻击判定部185基于第一异常得分以及第二异常得分算出第三异常得分,将所算出的第三异常得分与预定的阈值(第五阈值)进行比较,基于比较结果判定评价对象数据191是否是受到攻击的数据。此外,攻击判定部185也可以不限定于算出第三异常得分,针对第一异常得分以及第二异常得分的每一个与对应的阈值进行比较,基于比较结果来判定评价对象数据191是否是受到攻击的数据。

[0198] [4—2.攻击检测部的动作]

[0199] 图12是表示本实施方式的攻击检测处理(S103)的流程图。此外,图12所示的攻击检测处理例如既可以对采样数据所包含的任意的传感器值进行,也可以对采样数据所包含的全部传感器值进行。在对全部传感器值进行攻击检测处理的情况下,例如,也可以从取得时刻旧的传感器值开始依次进行图12所示的处理。

[0200] 首先,攻击检测部120取得采样数据,取出作为采样数据中的1个数据的评价对象数据(参照图13所示的评价对象数据191)(S131)。步骤S131的处理通过采样数据取得部181实施。

[0201] 接着,攻击检测部120取得评价对象数据191所关联的基点数据(S132)。步骤S132的处理通过基点数据取得部182而实施。

[0202] 图13是表示本实施方式的基点数据的一例的图。

[0203] 如图13所示,基点数据包含:传感器标识符192、评价ID193、传感器值194、第一索引195、第二索引196、短期传感器流197、长期传感器流198。

[0204] 传感器标识符192、评价ID193、传感器值194、第一索引195、以及第二索引196与采样数据中的传感器标识符172、评价ID173、传感器值174、第一索引175、以及第二索引176(参照图10)同样。

[0205] 短期传感器流197是具有与评价对象数据191相同的第二索引,将评价对象数据

191的第一索引之前的索引作为参照键,唯一的传感器值被确定的过去的传感器值的列表。

[0206] 例如,在图13中,在评价ID是“82”的评价对象数据的情况下,第二索引具有“3”,将第一索引为“2”之前的“1”作为参照键,将评价ID为81的评价对象数据的传感器值的代表值作为短期传感器流而保存。另外,关于上述的代表值的算出方法,稍后说明。

[0207] 另一方面,长期传感器流198是将评价对象数据191的第二索引之前的索引作为参照键,具有唯一值的过去的传感器值的代表值列表。

[0208] 例如,在图13中,在评价ID是“82”的评价对象数据的情况下,将第二索引为“3”之前的“1”和“2”作为参照键,将评价对象数据的传感器值的代表值作为长期传感器流而保存。另外,关于上述的代表值的算出方法,稍后说明。

[0209] 图14是表示本实施方式的检测结果信息的一例的图。

[0210] 如图14所示,检测结果信息包含:传感器标识符202、评价ID203、传感器值204、第一异常得分205、第二异常得分206、第三异常得分207、检测结果208。检测结果208是评价对象数据所关联的判定结果的一例。

[0211] 传感器标识符202、评价ID203、传感器值204与采样数据中的传感器标识符172、评价ID173、传感器值174(参照图10)同样。

[0212] 第一异常得分205、第二异常得分206、第三异常得分207、检测结果208稍后说明。

[0213] 再参照图12,接着,攻击检测部120判定第一索引以及第二索引中的至少一方是否为预定值以上(S133)。预定值被预先设定并存储于存储部。第一索引中的预定值和第二索引中的预定值既可以是相同值,也可以是彼此不同的值。

[0214] 攻击检测部120在对于评价对象数据的第一索引以及第二索引中的至少一方为预定值以上的情况下(S133中为“是”),算出稍后说明的异常得分(第一异常得分以及第二异常得分中的至少一方),在第一索引以及第二索引各自均低于预定值的情况下(S133中为“否”),将检测结果设为“不明”(S134)。攻击检测部120在步骤S133中为“是”的情况下,判定第一索引是否是预定值以上(S135)。预定值被预先设定,并存储于存储部。在步骤S135中使用的预定值是第三阈值的一例。第三阈值例如被设定为能够准确地算出第一异常得分的值。

[0215] 例如,在图13中,在评价ID“1”的数据是评价对象数据的情况下,第一索引是“1”,第二索引是“1”。因此,例如,在预定值是2的情况下,如图14所示,上述该数据的检测结果成为“不明”。此外,在判定为“不明”的情况下,第一异常得分、第二异常得分以及第三异常得分也可以是“0”。

[0216] 接着,攻击检测部120在对于评价对象数据的第一索引以及第二索引中的至少一方为预定值以上(S133中为“是”)、且第一索引为预定值以上的情况下(S135中为“是”),将算出表示评价对象数据与短期的传感器值的正常流(短期传感器流)的背离程度的第一异常得分的第一检测器进行读出,基于上述的评价对象数据191和短期传感器流,算出第一异常得分(S136)。步骤S136的处理通过第一异常得分算出部183而实施。

[0217] 第一异常得分算出部183在步骤S133以及S135中为“是”的情况下,将第一检测器从检测器存储部122中读出。第一检测器也可以通过以将评价对象数据191和短期传感器流作为输入,输出表示评价对象数据191与短期传感器流的背离程度的第一异常得分的方式进行了学习的学习完成模型而实现。第一检测器以背离的程度越大,则输出越大值的第一

异常得分的方式进行学习,但不限定于此。另外,第一异常得分例如是0～100的值(例如,标准化的值),但也可以是等级(“高”、“中”、“低”等)。

[0218] 例如,在图13中,在评价ID是“82”的评价对象数据的情况下,第一索引是“2”,在短期传感器流中包含“35.11”,传感器值是“100.50”。该情况下,如图14所示,第一检测器输出的第一异常得分例如是“95”。第一异常得分为95这一情况通过第一异常得分算出部183而算出。

[0219] 此外,第一检测器也可以使用由基于评价对象数据的传感器值与短期传感器流之间的传感器值的差分的、OC－SVM(One Class－Support Vector Machine)等机器学习模型实现的偏离值检测器。另外,第一检测器也可以使用如下检测器,即,取代传感器值而使用取得时间,以短期传感器流与评价对象数据之间的取得时间的差分是否基于周期来进行判定。此外,也可以统合使用前述的检测器。

[0220] 此外,第一异常得分算出部183并不限定于使用机器学习模型算出第一异常得分。第一异常得分算出部183例如也可以使用与评价对象数据191以及短期传感器流、和第一异常得分进行了关联的表(查找表)算出第一异常得分,也可以使用评价对象数据191以及短期传感器流进行预定的运算由此算出第一异常得分。

[0221] 另外,攻击检测部120在对评价对象数据的第一索引以及第二索引中的至少一方为预定值以上(S133中为“是”)、且第一索引低于预定值的情况下(S135中为“否”),进入步骤S137。在步骤S135为“否”的情况下,评价对象数据被取得的采样时间内的、在该评价对象数据以前取得的车辆传感器数据数少,难以准确地判定该评价对象数据是否异常。由此,攻击检测部120在步骤S135中为“否”的情况下,也可以不算出第一异常得分。此外,攻击检测部120在步骤S135中为“否”的情况下,也可以将第一异常得分设为“0”。

[0222] 接着,攻击检测部120判定第二索引是否为预定值以上(S137)。预定值被预先设定并存储于存储部。在步骤S137中使用的预定值既可以是与在步骤S133中使用的预定值相同的值,也可以不同。在步骤S137中使用的预定值是第四阈值的一例。第四阈值例如被设定为能够准确地算出第二异常得分的值。

[0223] 接着,攻击检测部120在第二索引为预定值以上的情况下(S137中为“是”),将算出表示评价对象数据与长期的传感器值的正常流(长期传感器流)的背离的程度的第二异常得分的第二检测器读出,基于上述的评价对象数据191和长期传感器流,算出第二异常得分(S138)。步骤S138的处理通过第二异常得分算出部184实施。

[0224] 第二异常得分算出部184在步骤S137中为“是”的情况下,从检测器存储部122读出第二检测器。第二检测器也可以通过以将评价对象数据191和长期传感器流作为输入,输出表示评价对象数据191与长期传感器流的背离程度的第二异常得分的方式进行了学习的学习完成模型而实现。第二检测器以背离的程度越大,则输出越大的值的第二异常得分的方式进行学习,但不限定于此。另外,第二异常得分例如是0～100的值(例如,标准化的值),但是也可以是等级(“高”、“中”、“低”等)。

[0225] 例如,在图13中,在评价ID“82”的数据是评价对象数据的情况下,第二索引是“3”,在长期传感器流中包含“22.50”以及“33.50”,传感器值是“100.50”。该情况下,如图14所示,第二检测器输出的第二异常得分是“80”。第二异常得分是80这一情况通过第二异常得分算出部184算出。

[0226] 此外,第二检测器也可以使用如下变化点检测器,即,使用递归神经网络模型(RNN:Recurrent Neural Network)或自回归移动平均模型(ARIMA:Auto Regressive Integrated Moving Average),预测正常的传感器值的举止,基于与实测值的误差判定为异常。

[0227] 另外,攻击检测部120在对于评价对象数据的第二索引低于预定值的情况下(S137中为“否”),进入步骤S139。在步骤S137为“否”的情况下,评价对象数据被取得的采样间隔中的、在该评价对象数据以前取得的车辆传感器数据少,难以准确地判定该评价对象数据是否异常。由此,攻击检测部120在步骤S137中为“否”的情况下,不算出第二异常得分也可。此外,攻击检测部120也可以在步骤S137中为“否”的情况下,将第二异常得分设为“0”。

[0228] 此外,第一检测器以及第二检测器既可以是彼此不同的检测器,也可以是1个检测器。

[0229] 接着,攻击检测部120根据第一异常得分和第二异常得分,算出第三异常得分(S139)。步骤S139的处理通过攻击判定部185实施。

[0230] 此外,第三异常得分是基于第一异常得分以及第二异常得分的异常得分。第三异常得分例如也可以是第一异常得分,也可以是第二异常得分,也可以是基于第一异常得分和第二异常得分的统计值。统计值例如是平均值(例如,加权平均),但也可以是中央值、频度最高值、最大值、最小值中的任一个。

[0231] 此外,算出第三异常得分并不是必须的。

[0232] 接着,攻击检测部120使用第三异常得分,判定有无攻击(S140)。步骤S139的处理通过攻击判定部185实施。攻击判定部185也可以说,判定评价对象数据是否是受到攻击的数据。攻击判定部185例如在第三异常得分为第五阈值以上的情况下,判定为“攻击”(有攻击),在低于第五阈值的情况下,判定为“正常”(无攻击)。

[0233] 例如,在图14中,在评价ID是“82”的情况下,该数据的第一异常得分的“95”、以及第二异常得分的“80”均被算出(在S135为“是”、且S137为“是”的情况下),作为第三异常得分算出平均值为“87”。该情况下,攻击判定部185在将第五阈值设为“60”时,将评价ID为“82”的传感器值判定为“攻击”。也就是说,攻击判定部185将传感器值“100.50”判定为是受到攻击的数据。

[0234] 另外,在图14中,在评价ID为“81”的情况下,仅算出该数据的第二异常得分的“6”(在S135为“否”、S137为“是”的情况下),作为第三异常得分算出“6”。该情况下,攻击判定部185在将第五阈值设定为“60”时,判定为“正常”。也就是说,攻击判定部185将传感器值“35.11”判定为没有受到攻击。

[0235] 步骤S135为“否”、且在步骤S137为“是”的情况例如假设为是在第二索引为预定值以上时的紧接着采样间隔的开始时刻之后等的情况。该情况下,虽然是尚未取得该采样间隔中的采样时间内的全部车辆传感器数据的状态(例如,作为采样时间的开头的时机的状态),但是是每个采样间隔的车辆传感器数据仅具有能够判定有无攻击的数量的状态。换言之,步骤S135为“否”、且步骤S137为“是”的情况是指,无法进行使用了第一检测器进行的攻击的检测、且能够进行使用了第二检测器进行的攻击的检测的情况。

[0236] 此时,攻击检测部120能够使用由第二检测器得到的第二异常得分判定评价对象数据是否是受到攻击的数据。

[0237] 另外,步骤S135为“是”、且步骤S137为“否”的情况是指,例如,想定虽然经过的采样间隔少,但是经过的采样间隔中的采样时间内的车辆传感器数据全部取得完毕的情况。该情况下,虽然按每个采样间隔的车辆传感器数据数少,但是是采样时间内的车辆传感器数据仅具有能够判定有无攻击的数量的状态。换言之,步骤S135为“是”、且步骤S137为“否”的情况下是指,能够进行使用了第一检测器进行的攻击的检测、且无法进行使用了第二检测器进行的攻击的检测的情况。

[0238] 此时,攻击检测部120能够使用由第一检测器得到的第一异常得分判定评价对象数据是否是受到攻击的数据。

[0239] 这样,第一检测器以及第二检测器能够补充在彼此无法检测的时间内的攻击检测。也就是说,攻击检测部120能够减少无法进行攻击的检测的时间。由此,能够提高攻击检测部120中的攻击的检测性能。

[0240] 接着,攻击检测部120将步骤S134或S140的判定结果存储于检测结果存储部123(S141)。攻击检测部120也可以说将判定结果向检测结果存储部123输出。

[0241] 这样,攻击检测部120在评价对象数据所关联的第一索引低于第三阈值、且该评价对象数据所关联的第二索引低于第四阈值的情况下,判定为不清楚该评价对象数据是否是受到攻击的数据(S134)。另外,攻击检测部120在基于第一异常得分以及第二异常得分的第三异常得分为第五阈值以上的情况下,判定为评价对象数据是受到攻击的数据,在第三异常得分低于第五阈值的情况下,判定为评价对象数据是正常的(S140),将表示所判定出的结果的检测结果进行输出。

[0242] 此外,在图12中,攻击检测部120还可以使用车辆事件信息,算出异常得分。攻击检测部120例如也可以在车辆事件信息表示发生了车辆的发动机的ON以及OFF的切换、换挡杆的切换、自动驾驶模式的ON以及OFF的切换中的至少1个的情况下,对长期传感器流所包含的传感器值进行初始化(重置)。也就是说,攻击检测部120也可以在发生了该至少1个的情况下,基于在该时刻之后所取得的传感器值算出第二异常得分。该情况下,由于需要蓄积长期传感器流所包含的传感器值,所以蓄积的期间(例如,与2个以上的采样间隔相当的期间)中,虽然无法算出第二异常得分,但是在第一索引为预定值以上的情况下,能够算出第一异常得分。

[0243] 这样,攻击检测部120在发生了该至少1个的情况下,基于第一异常得分进行攻击的检测,由此能够减少无法进行攻击的检测的时间。由此,能够进一步提高攻击检测部120中的攻击的检测性能。

[0244] [5—1.基点数据更新部的构成]

[0245] 图15是表示本实施方式的基点数据更新部121的构成的框图。如图15所示,基点数据更新部121具备:基点数据取得部182、检测结果取得部201、以及基点数据追加部302。

[0246] 基点数据取得部182是从基点数据存储部124取得基点数据的处理部。

[0247] 检测结果取得部201是从检测结果存储部123取得攻击检测部120的检测结果的处理部。

[0248] 基点数据追加部302是向基点数据取得部182取得的基点数据追加与检测结果取得部201取得的检测结果相应的数据的处理部。基点数据追加部302也可以说对基点数据进行更新。

[0249] [5—2.基点数据更新部的动作]

[0250] 图16是表示本实施方式的基点数据更新处理(S104)的流程图。基点数据更新处理通过基点数据更新部121而实施。

[0251] 首先,基点数据更新部121根据通过基点数据取得部182取得的评价对象数据,对基点数据进行初始化(S151)。基点数据更新部121取得评价对象数据191所关联的基点数据,在评价对象数据191的第一索引是1的情况下,对基点数据中的短期传感器流进行初始化,在评价对象数据191的第二索引是1的情况下,对基点数据中的长期传感器流进行初始化。此外,在此的初始化意味着,成为在短期传感器流或长期传感器流中不包含传感器值的状态。例如,图13的评价ID是“1”时的短期传感器流197以及长期传感器流、以及评价ID是“81”时的短期传感器流197(图13所示的[ ])表示被进行了初始化。

[0252] 接着,基点数据更新部121取得评价对象数据所关联的检测结果S152)。步骤S152的处理通过检测结果取得部201而实施。检测结果取得部201将评价对象数据191所关联的检测结果从检测结果存储部123读出。检测结果取得部201例如读出图14所示的检测结果。

[0253] 接着,基点数据更新部121判定所取得的检测结果是否是“攻击”(S153)。步骤S153～S157的处理通过基点数据追加部302而实施。基点数据追加部302例如基于评价对象数据的评价ID203所对应的检测结果208,进行步骤S153的判定。

[0254] 接着,基点数据追加部302在检测结果是“攻击”的情况下(在S153中为“是”),作为用于补全传感器值的值,将推定传感器值设定为追加数据(S154),在检测结果是“正常”或者“不明”的情况下(S153中为“否”),将评价对象数据的传感器值(实测值)设定为追加数据(S155)。

[0255] 此外,推定传感器值可以是在评价对象数据所关联的短期传感器流的最后被追加的值,也可以是短期传感器流的平均值。另外,推定传感器值也可以是基于上述的长期传感器流,由第二检测器算出的评价对象数据的传感器值的预测值。

[0256] 基点数据追加部302,例如在图13中,在评价ID是“82”的情况下,由于检测结果是“攻击”,所以作为将推定传感器值作为在评价对象数据所关联的短期传感器流的最后被追加的值而设定“35.11”。

[0257] 接着,基点数据追加部302按照下述(数2),对在接下来的评价对象数据的判定中使用的短期传感器流(数1)进行更新(S156)。

[0258] 【数1】

[0259] $S=\{s_1,s_2,s_3,s_i,\cdots\cdots\}$ (式2)

[0260] 【数2】

[0261] $$s_i=\begin{cases}p_i^j, & (label_i^j=\text{“Attack”})\\ x_i^j, & (otherwise)\end{cases}$$ (式3)

[0262] 在此,si表示短期传感器流所包含的1个传感器值,i表示评价对象数据的第一索引,j表示评价对象数据的第二索引。基点数据追加部302在上述的检测结果labeli—j是“攻击”(“Attack”)的情况下,用上述的推定传感器值pi—j来更新si。另外,基点数据追加

部302在labeli－j是“正常”(“Normal”)或者“不明”(“Unknown”)的情况下,用上述的评价对象数据的传感器值xi－j来更新si。此外,si是代表值的一例。

[0263] 接着,基点数据追加部302按下述(数4),更新长期传感器流(数3)(S157)。

[0264] 【数3】

[0265] $H=\{h_1,h_2,h_3,h_j,.....\}$ (式4)

[0266] 【数4】

[0267] $$h_j=\begin{cases}p_i^j, & (label_i^j=\text{“}Attack\text{”})\\ x_i^j, & (otherwise)\end{cases}$$ (式5)

[0268] 在此,hj表示长期传感器流所包含的1个传感器值。基点数据追加部302在上述的检测结果labeli－j是“攻击”(“Attack”)的情况下,用上述的推定传感器值pi－j更新hj。另外,基点数据追加部302在labeli－j是“正常”或者“不明”的情况下,用上述的评价对象数据的传感器值xi－j更新hj。此外,hj是代表值的一例。

[0269] 这样,基点数据追加部302在每当进行是否是攻击的判定时,更新2种基点数据,用于接下来的判定。

[0270] 此外,在上述说明中,示出了:在监视系统100中,采样处理和攻击检测处理由彼此不同的装置进行的例子,但是也可以由同一装置(例如,1个装置)进行。

[0271] 如以所述,与成为监视处理(例如,攻击检测处理)的对象的车辆传感器数据的特征相应地,调整采样间隔和采样时间,进行采样数据的生成。进而,基于包含表示短期以及长期的传感器值的活动的2种索引的采样数据,算出2种异常得分,由此进行攻击的判定。由此,能够抑制监视成本并高精度进行攻击检测。

[0272] 另外,基点数据更新部121在评价对象数据所关联的检测结果是攻击的情况下,使用短期传感器流以及长期传感器流中的至少1个来推定评价对象数据应该能取的传感器值,基于所推定出的推定传感器值、第一索引、和第二索引,更新短期传感器流和长期传感器流。另外,基点数据更新部121在评价对象数据所关联的检测结果是正常或者不明的情况下,基于评价对象数据的传感器值(实测值)、第一索引、以及第二索引,更新短期传感器流和长期传感器流。

[0273] 由此,能够抑制攻击等偏离值混合存在于基点列表这一情况。由此,通过使用这样的基点列表,能够抑制监视成本并高精度进行攻击检测。

[0274] 以下,对上述的监视系统100的利用方式进行说明。

[0275] 图17是表示本实施方式的监视系统100的构成的示意图。图17是表示具备采样部401以及采样数据监视部501的监视系统100的构成的框图。监视系统100具备存在于云上的服务器500、和车载装置400。监视系统100能够经由车载装置400,取得所提取出的车辆传感器数据(采样数据),基于所取得的车辆传感器数据来检测攻击。

[0276] 车载装置400以及服务器500例如能够经由互联网等公共通信网络以能够通信的方式连接。车载装置400是安全保护ECU(Electronic Control Unit)或汽车导航等。

[0277] 车载装置400具备:采样部401和攻击通知装置402。

[0278] 采样部401是将对车辆网络数据进行采样得到的结果(采样数据)向采样数据监视部501发送的装置。采样部401例如按每个预定的行驶时间,将以二进制表现的CAN数据变换为传感器值,进而变换为采样数据。而且,采样部401将采样数据向采样数据监视部501发送。

[0279] 攻击通知装置402是用于将从服务器500接收到的对车辆网络的攻击的发生向驾驶员通知的装置。攻击通知装置402例如通知攻击的发生,并通过指示在与网络断开的安全模式下进行驾驶这一情况的声音或者画面而进行输出。攻击通知装置402通过显示装置、扬声器装置等而实现。

[0280] 采样数据监视部501判定有无对从车载装置400接收到的车辆网络数据(例如,采样数据)的攻击,在有攻击的情况下向攻击通知装置402发送攻击检测的结果。

[0281] 此外,采样部401的构成也可以与采样部101同样。另外,采样数据监视部501的构成也可以与采样数据监视部102同样。

[0282] 图18是表示本实施方式的车载装置600的构成的示意图。图18是表示具备监视装置601的车载装置600的构成的框图。车载装置600具备监视装置601和攻击通知装置602。

[0283] 监视装置601仅在车辆内部,针对对车辆网络数据进行采样得到的结果判定有无攻击,在有攻击的情况下向攻击通知装置602发送攻击检测的结果。此外,监视装置601例如构成为具有采样部101以及采样数据监视部102所具有的功能。这样,采样部101以及采样数据监视部102所具有的功能也可以通过1个装置(例如,搭载于车辆的装置)而实现。监视装置601是攻击检测系统的一例。

[0284] 攻击通知装置602是用于向驾驶员通知对从监视装置601接收到的车辆网络的攻击的发生的装置。攻击通知装置602通过显示器装置、扬声器装置等而实现。

[0285] 这样,在图17的监视系统100以及图18的监视装置601中,针对对车辆网络进行了采样而得到的结果,适当地判定是否有攻击,由此能够以低监视成本实现攻击检测。另外,在监视系统100以及监视装置601中,进而,由于通过检测结果的通知能够将检测到攻击这一情况向驾驶员通知,所以能够减轻由攻击导致的事故发生。

[0286] (其他实施方式)

[0287] 以上,对实施方式的监视装置进行了说明,但本公开并不限定于该实施方式。

[0288] 例如,在上述实施方式中,对搭载于汽车等车辆的车载网络中的安全保护对策进行了说明,但是适用范围并不限定于此。例如,除了汽车等车辆以外,也可以适用于作为移动体的建机、农机、船舶、铁路以及飞机等的移动体(mobility)。即,能够作为移动体网络以及移动体网络系统中的网络安全保护对策而适用。

[0289] 另外,上述实施方式的监视装置所包含的各处理部典型地作为集成电路即LSI而实现。既可以将它们个别地单芯片化,也可以单芯片化为包含一部分或全部。

[0290] 另外,集成电路化并不限于LSI,也可以由专用电路或通用处理器实现。也可以利用能够在LSI制造后编程的FPGA、或能够再构成LSI内部的电路单元的连接和/或设定的可重构处理器。

[0291] 另外,本公开也可以作为通过监视系统执行的监视方法(例如,攻击检测方法)而实现。例如,本公开的一技术方案也可以是使计算机执行监视方法所包含的特征的各步骤的计算机程序。另外,本公开的一技术方案也可以是记录了这样的程序的DVD等计算机可读

取非瞬时性记录介质。例如,也可以使这样的程序记录于记录介质而发布或流通。例如,由这样的程序以及该程序构成的数字信号也可以经由以电通信线路、无线或有线通信线路、互联网为代表的网络、数据广播等而传送。例如,也可以通过将所发布的程序安装于具有其他处理器的装置,使该处理器执行该程序,从而能够使该装置进行上述各处理。

[0292] 另外,在上述实施方式中,对第一顺序信息是第一索引的例子进行了说明,但并不限定于此、第一顺序信息例如也可以是绝对时刻。另外,在上述实施方式中,对第二顺序信息是第二索引的例子进行了说明,但是并不限定于此,第二顺序信息例如也可以是采样间隔开始的绝对时刻。

[0293] 另外,在上述实施方式中,各构成要素可以通过专用的硬件构成,也可以通过执行与各构成要素相适的软件程序而实现。各构成要素也可以通过CPU或处理器等程序执行部将硬盘或半导体存储器等记录介质所记录的软件程序读出并执行而实现。

[0294] 另外,框图中的功能块的分割是一例,也可以将多个功能块实现为一个功能块,将一个功能块分割为多个,或者将一部分功能移至其他功能块。另外,也可以将具有类似功能的多个功能块的功能由单一的硬件或软件并行或分时进行处理。

[0295] 另外,在监视系统由多个装置实现的情况下,采样部具有的功能以及采样数据监视部具有的功能也可以在多个装置中任意分配。

[0296] 另外,流程图中的各步骤被执行的顺序是为了具体说明本公开而例示的顺序,也可以是上述以外的顺序。另外,上述步骤的一部分也可以与其他步骤同时(并行)执行。

[0297] 以上,对一个或多个技术方案的监视系统,基于实施方式进行了说明,但本公开并不限定于该实施方式。只要不脱离本公开的主旨,能够对本实施方式实施本领域技术人员能想到的各种变形,对不同实施方式中的构成要素进行组合而构筑的方式也可以包含在一个或多个技术方案的范围内。

[0298] 产业上的可利用性

[0299] 本公开能够适用于对车辆传感器数据的监视装置,例如,能够适当判定车辆传感器数据所包含的车辆控制用的数据是否受到攻击。例如,本公开能够利用于安全保护(security)用ECU等车载装置或者远程监视服务器中的SIEM(Security Information and Event Management:安全信息和事件管理)等监视装置或监视系统。

[0300] 标号说明

[0301] 100 监视系统

[0302] 101、401 采样部

[0303] 102、501 采样数据监视部

[0304] 110 采样方针生成部

[0305] 111 采样数据生成部

[0306] 112 车辆传感器数据存储部

[0307] 113 采样方针存储部

[0308] 114 车辆信息存储部

[0309] 115、126 通信部

[0310] 120 攻击检测部

[0311] 121 基点数据更新部

[0312] 122 检测器存储部

[0313] 123 检测结果存储部

[0314] 124 基点数据存储部

[0315] 125 采样数据存储部

[0316] 130 车辆传感器数据取得部

[0317] 131 传感器数据稳定度算出部

[0318] 132 采样方针判定部

[0319] 141 车辆传感器数据

[0320] 142、152、172、192、202 传感器标识符

[0321] 143 数据ID

[0322] 144 取得时刻

[0323] 145、174、194、204 传感器值

[0324] 151 采样方针数据

[0325] 153 文件编号

[0326] 154 数据方差

[0327] 155 车辆事件标记

[0328] 156 采样间隔

[0329] 157 采样时间

[0330] 160 采样信息取得部

[0331] 161 数据提取部

[0332] 162 索引赋予部

[0333] 173、193、203 评价ID

[0334] 175、195 第一索引

[0335] 176、196 第二索引

[0336] 181 采样数据取得部

[0337] 182 基点数据取得部

[0338] 183 第一异常得分算出部

[0339] 184 第二异常得分算出部

[0340] 185 攻击判定部

[0341] 191 评价对象数据

[0342] 197 短期传感器流

[0343] 198 长期传感器流

[0344] 201 检测结果取得部

[0345] 205 第一异常得分

[0346] 206 第二异常得分

[0347] 207 第三异常得分

[0348] 208 检测结果

[0349] 302 基点数据追加部

[0350] 400、600 车载装置

[0351] 402、602 攻击通知装置

[0352] 500 服务器

[0353] 601 监视装置。

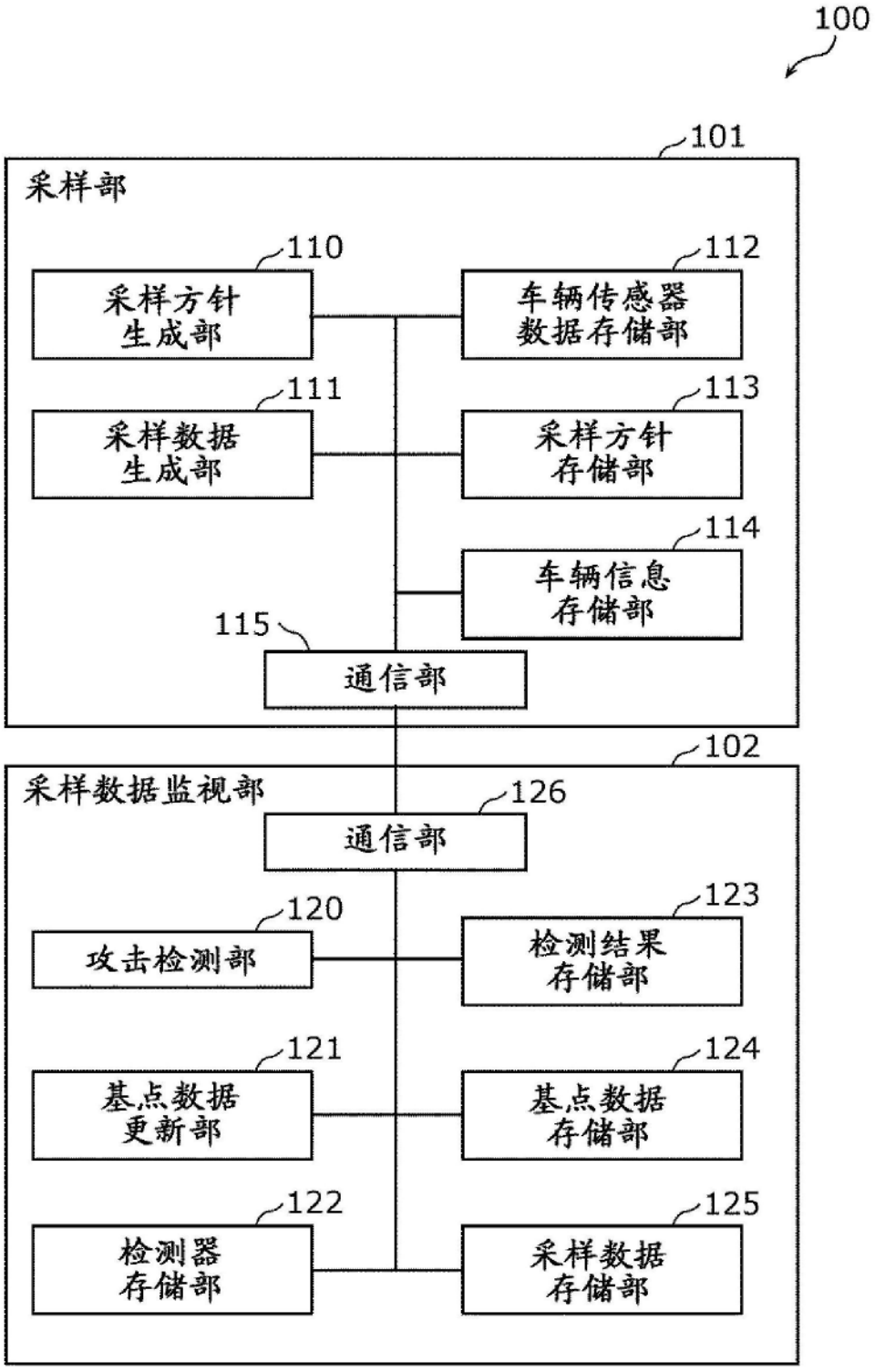

100
101
采样部
110
采样方针
生成部
112
车辆传感器
数据存储部
111
采样数据
生成部
113
采样方针
存储部
114
车辆信息
存储部
115
通信部
102
采样数据监视部
126
通信部
120
攻击检测部
123
检测结果
存储部
121
基点数据
更新部
124
基点数据
存储部
122
检测器
存储部
125
采样数据
存储部

图1

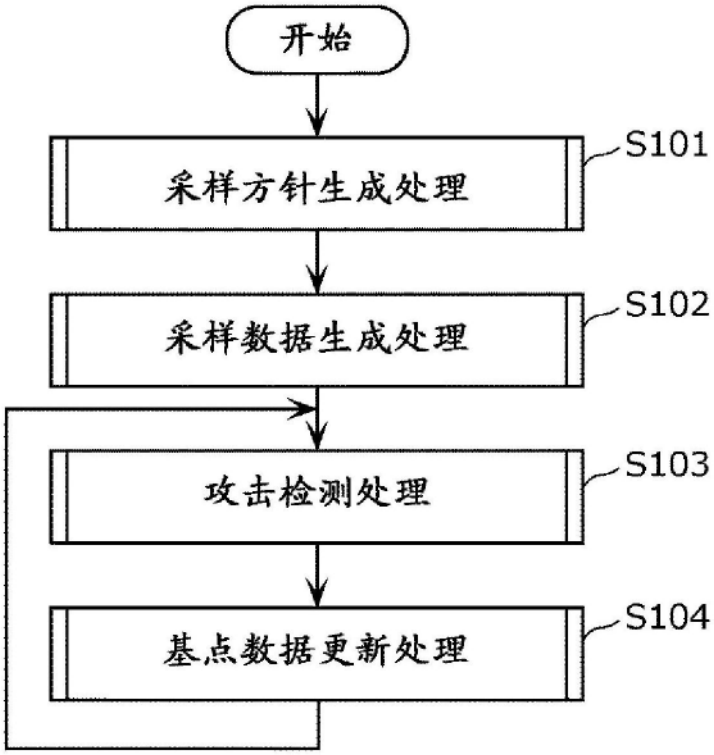

开始
采样方针生成处理
S101
采样数据生成处理
S102
攻击检测处理
S103
基点数据更新处理
S104

图2

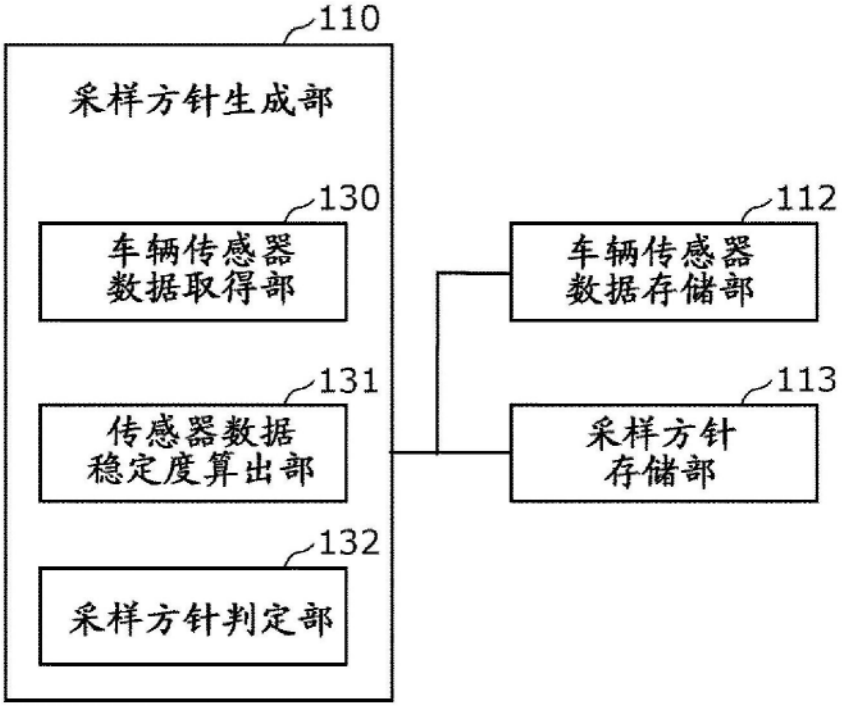

110
采样方针生成部
130
车辆传感器
数据取得部
131
传感器数据
稳定度算出部
132
采样方针判定部
112
车辆传感器
数据存储部
113
采样方针
存储部

图3

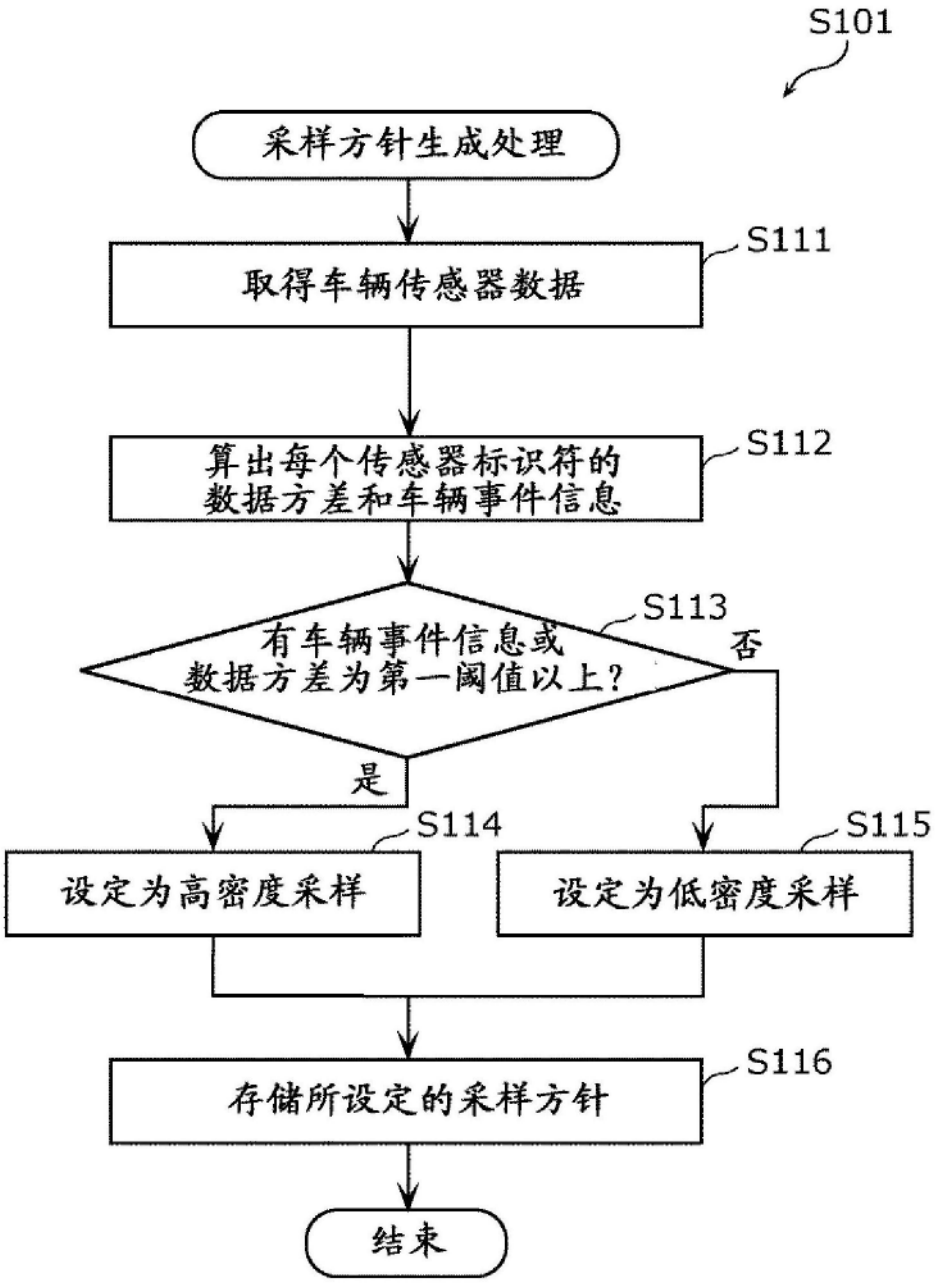

S101
采样方针生成处理
S111
取得车辆传感器数据
S112
算出每个传感器标识符的
数据方差和车辆事件信息
S113
有车辆事件信息或
数据方差为第一阈值以上?
否
是
S114
设定为高密度采样
S115
设定为低密度采样
S116
存储所设定的采样方针
结束

图4

141

142 传感器标识符	143 数据ID	144 取得时刻[ms]	145 传感器值
车速	1	25.00	22.11
车速	2	50.01	22.50
车速	3	75.15	23.11
…	…	…	…
车速	41	1025.00	30.11
车速	42	1050.00	33.50
车速	43	1075.00	33.50
…	…	…	…
车速	81	2025.00	35.11
车速	82	2048.00	100.50
车速	83	2050.00	35.50
…	…	…	…
车速	2401	60025.00	40.11
挡位	1	30.00	3.00(驱动)
…	…	…	…
挡位	2000	60010.00	0.00(驱动)
…	…	…	…

图5

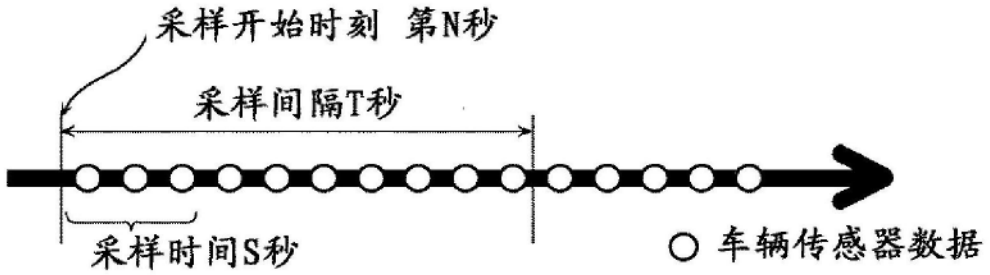


图6

传感器标识符	文件编号	数据方差	车辆事件标记	采样间隔 [ms]	采样时间 [ms]
车速	1	0.22	有	200.00	75.00
…	1	…		…	…
车速	2	0.22	无	1000.00	55.00
…	2	…		…	…
车速	3	10.22	无	200.00	75.00
…	3	…		…	…

152 153 154 155 156 157

151

图7

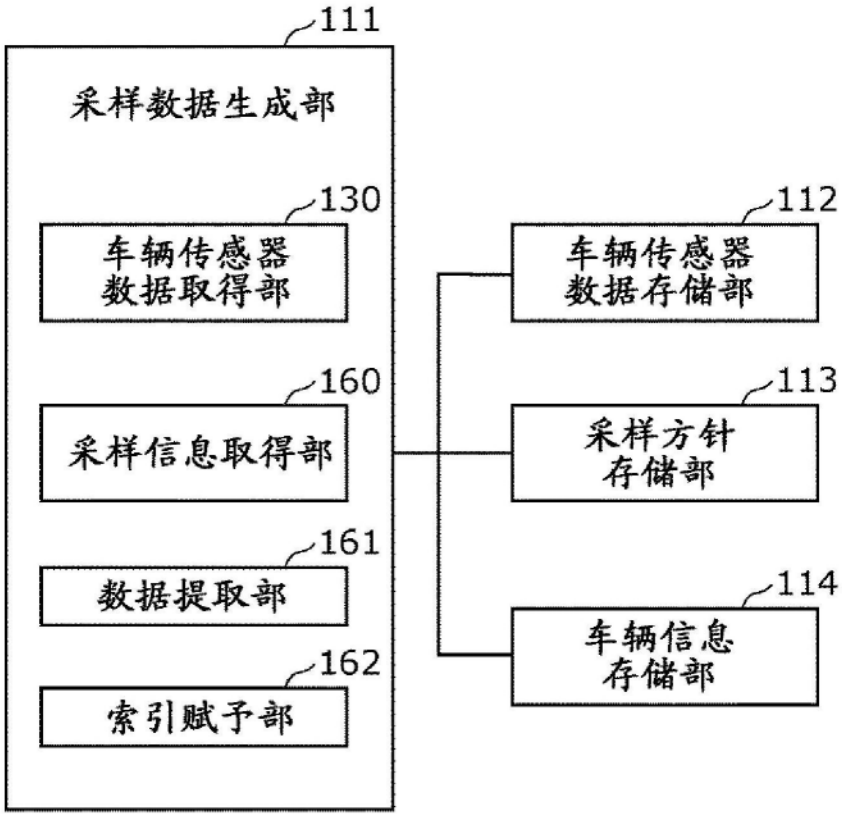

111
采样数据生成部
130
车辆传感器
数据取得部
160
采样信息取得部
161
数据提取部
162
索引赋予部
112
车辆传感器
数据存储部
113
采样方针
存储部
114
车辆信息
存储部

图8

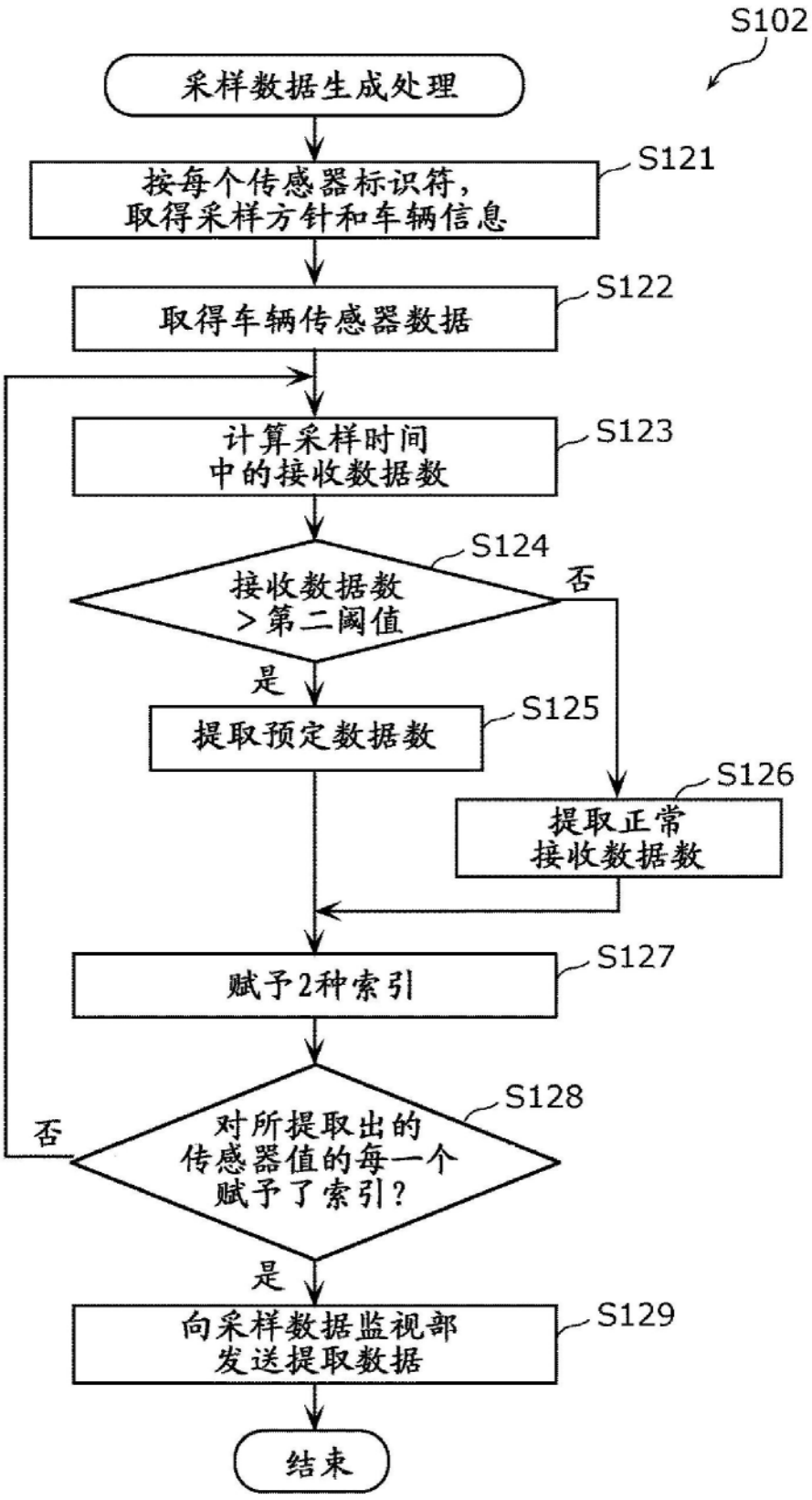

S102
采样数据生成处理
S121
按每个传感器标识符，
取得采样方针和车辆信息
S122
取得车辆传感器数据
S123
计算采样时间
中的接收数据数
S124
接收数据数
＞第二阈值
否
是
S125
提取预定数据数
S126
提取正常
接收数据数
S127
赋予2种索引
S128
对所提取出的
传感器值的每一个
赋予了索引？
否
是
S129
向采样数据监视部
发送提取数据
结束

图9

171

172 传感器标识符	173 评价ID	174 传感器值	175 第一索引	176 第二索引
车速	1	22.11	1	1
车速	2	22.50	2	1
车速	41	30.11	1	2
车速	42	33.50	2	2
车速	81	35.11	1	3
车速	82	100.50	2	3
车速	83	35.50	3	3
…	…	…	…	…
车速	2401	40.11	1	60
…	…	…	…	…

图10

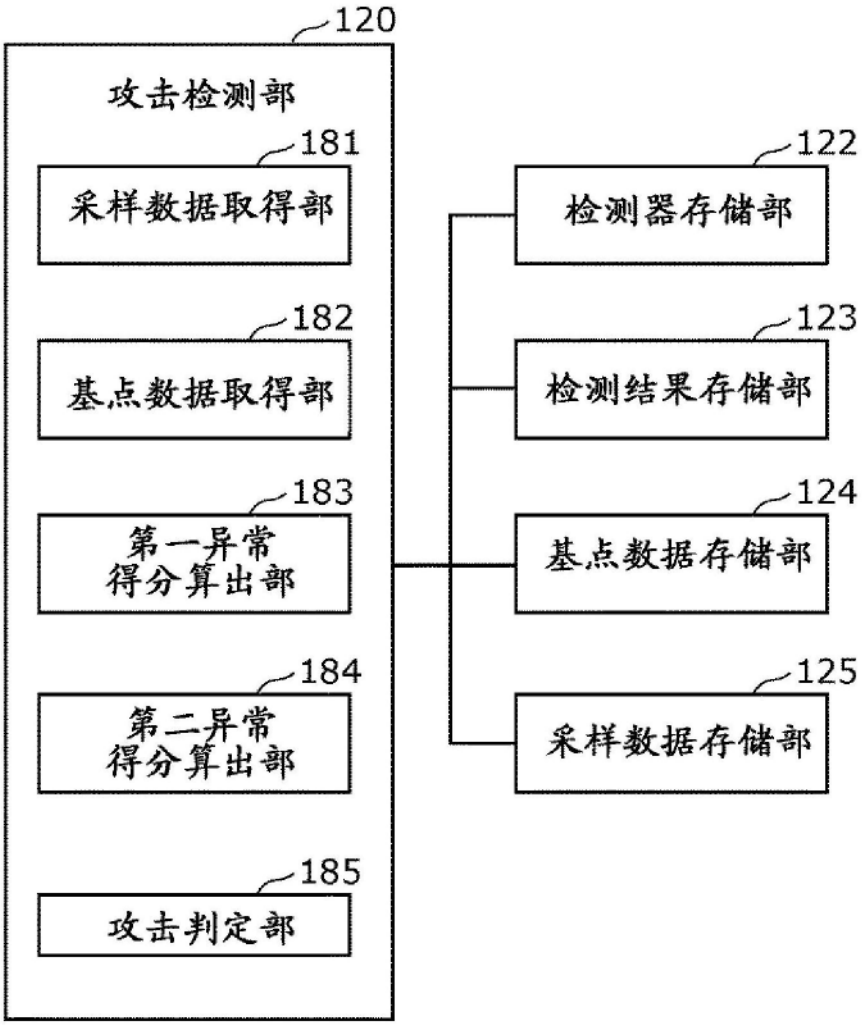

120
攻击检测部
181
采样数据取得部
182
基点数据取得部
183
第一异常
得分算出部
184
第二异常
得分算出部
185
攻击判定部
122
检测器存储部
123
检测结果存储部
124
基点数据存储部
125
采样数据存储部

图11

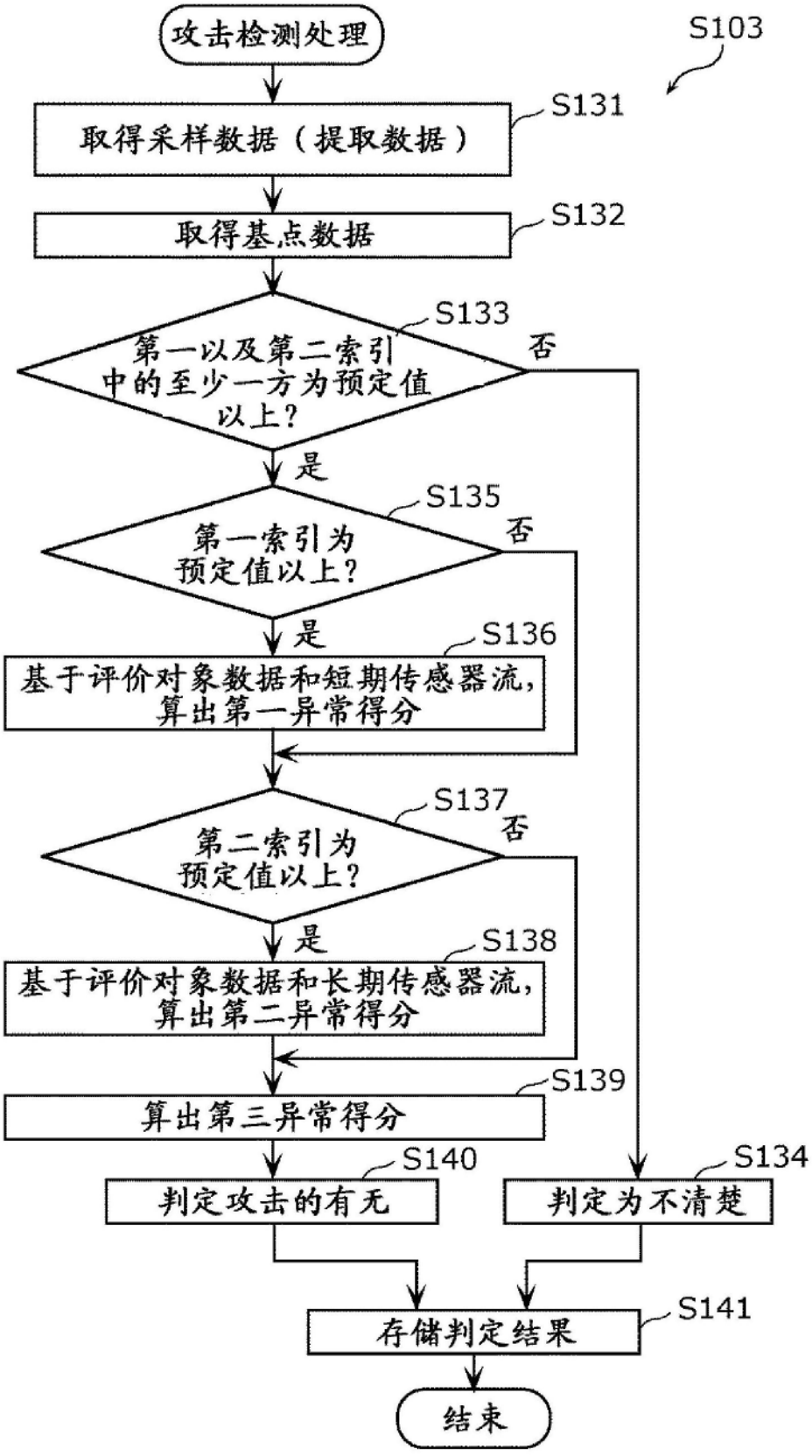

攻击检测处理
S103
取得采样数据（提取数据）
S131
取得基点数据
S132
第一以及第二索引中的至少一方为预定值以上？
S133
否
是
第一索引为预定值以上？
S135
否
是
基于评价对象数据和短期传感器流，算出第一异常得分
S136
第二索引为预定值以上？
S137
否
是
基于评价对象数据和长期传感器流，算出第二异常得分
S138
算出第三异常得分
S139
判定攻击的有无
S140
判定为不清楚
S134
存储判定结果
S141
结束

图12

191

192 传感器标识符	193 评价ID	194 传感器值	195 第一索引	196 第二索引	197 短期传感器流	198 长期传感器流
车速	1	22.11	1	1	[]	[]
…	…	…	…	…	…	…
车速	81	35.11	1	3	[]	[22.50, 33.50]
车速	82	100.50	2	3	[35.11]	[22.50, 33.50]
车速	83	35.50	3	3	[35.11, 35.11]	[22.50, 33.50, 35.11]
…	…	…	…	…	…	…

图13

202 传感器标识符	203 评价ID	204 传感器值	205 第一异常得分	206 第二异常得分	207 第三异常得分	208 检测结果
车速	1	22.11	0	0	0	“不清楚”
…	…	…	…	…	…	
车速	81	35.11	0	6	6	“正常”
车速	82	100.50	95	80	87	“攻击”
车速	83	35.50	2	0	1	“正常”
…	…	…	…	…	…	

图14

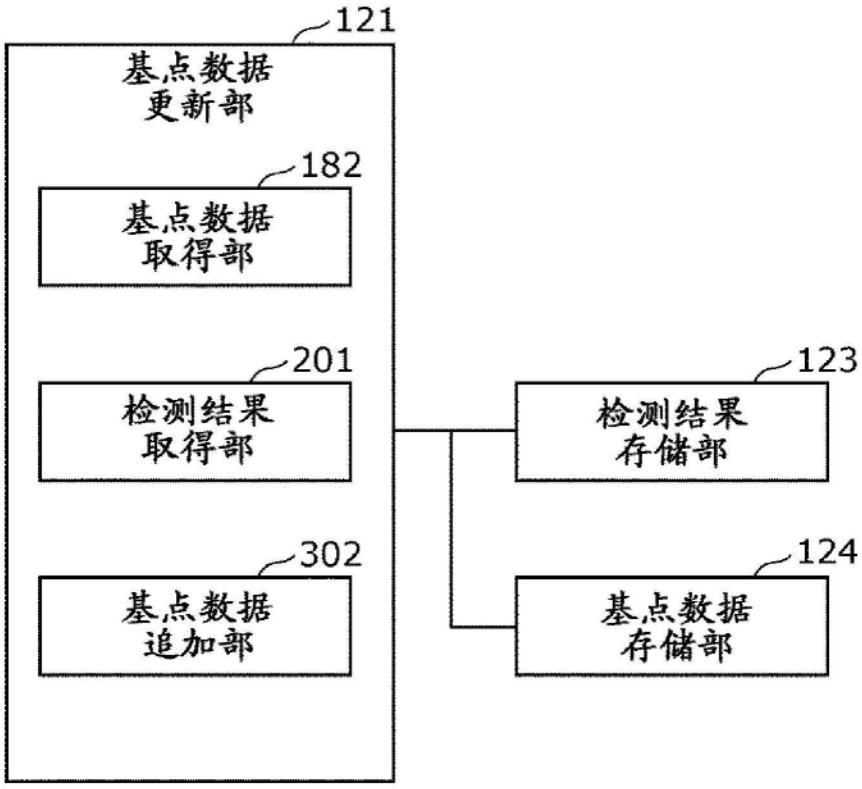

121
基点数据
更新部
182
基点数据
取得部
201
检测结果
取得部
302
基点数据
追加部
123
检测结果
存储部
124
基点数据
存储部

图15

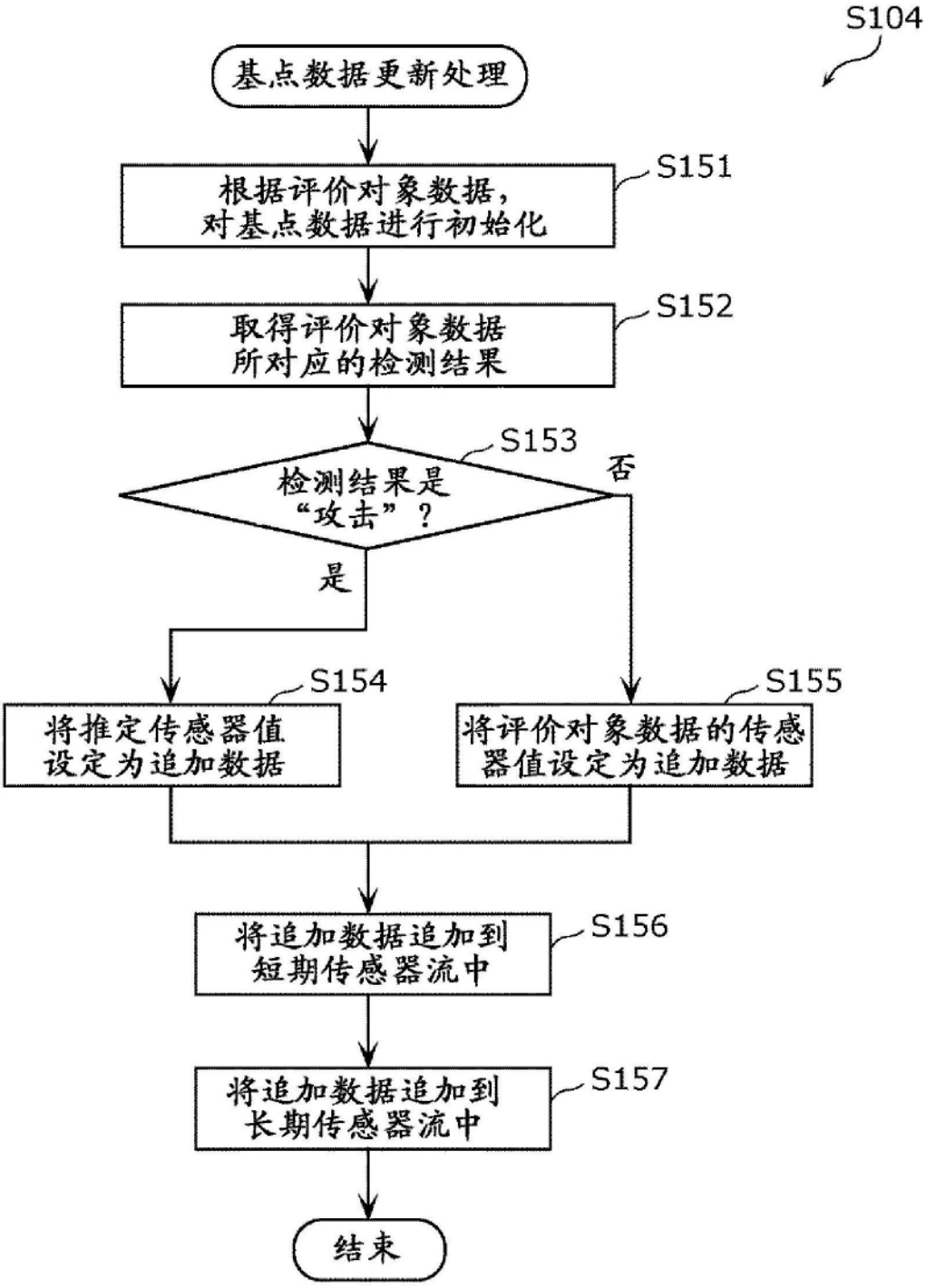

S104
基点数据更新处理
S151
根据评价对象数据，
对基点数据进行初始化
S152
取得评价对象数据
所对应的检测结果
S153
检测结果是
“攻击”？
否
是
S154
将推定传感器值
设定为追加数据
S155
将评价对象数据的传感
器值设定为追加数据
S156
将追加数据追加到
短期传感器流中
S157
将追加数据追加到
长期传感器流中
结束

图16

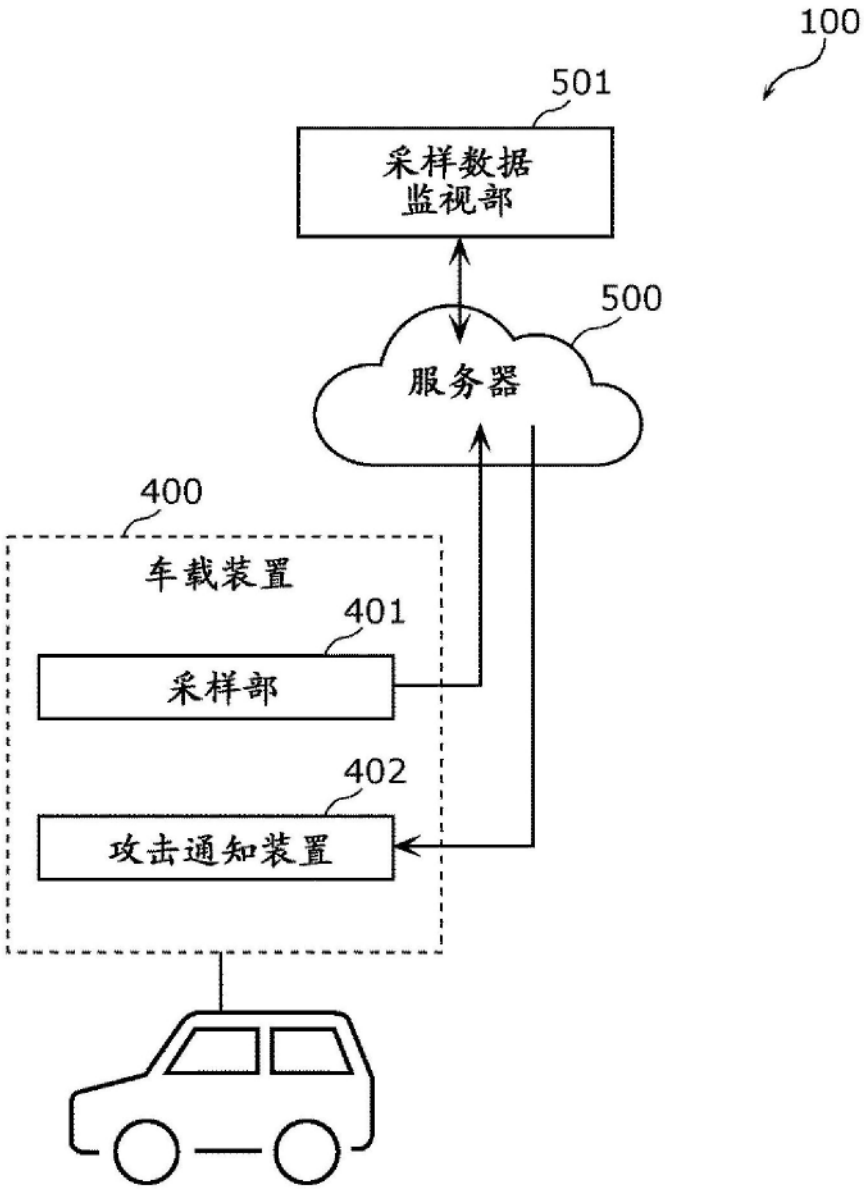


图17

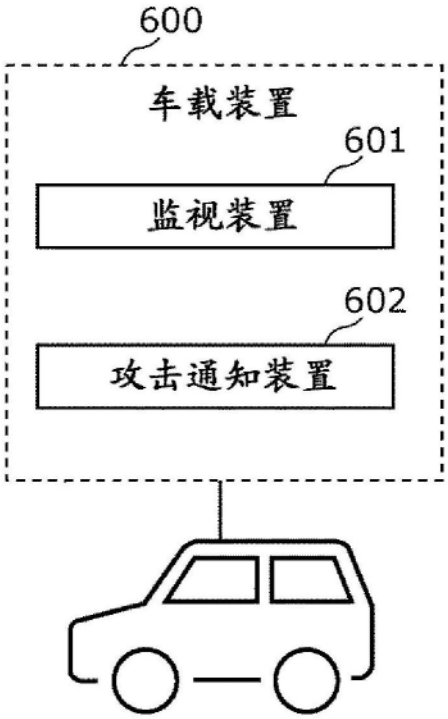


图18