(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 111316602 B
(45)授权公告日 2022.04.19

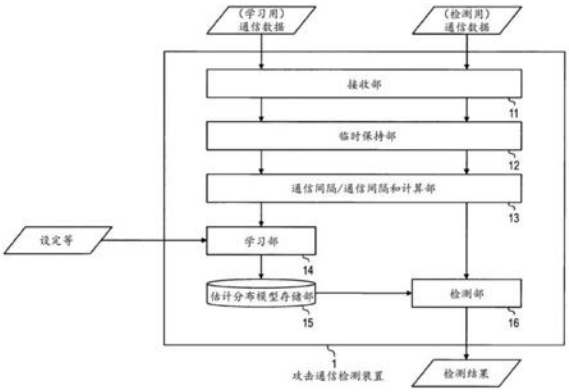
(21)申请号 201880070434.5
(22)申请日 2018.10.23
(65)同一申请的已公布的文献号
申请公布号 CN 111316602 A
(43)申请公布日 2020.06.19
(30)优先权数据
2017-208801 2017.10.30 JP
(85)PCT国际申请进入国家阶段日
2020.04.28
(86)PCT国际申请的申请数据
PCT/JP2018/039296 2018.10.23
(87)PCT国际申请的公布数据
WO2019/087858 JA 2019.05.09
(73)专利权人 日本电信电话株式会社
地址 日本东京都
(72)发明人 冈野靖 小山卓麻
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 金兰
(51)Int.Cl.
H04L 12/28(2006.01)
(56)对比文件
CN 104660594 A,2015.05.27
CN 101316266 A,2008.12.03
CN 105871833 A,2016.08.17
CN 1894661 A,2007.01.10
US 2006139835 A1,2006.06.29
胡彬.《基于机器学习的移动终端高级持续性威胁检测技术研究》.《计算机工程》.2017,第43卷(第1期),全文.
审查员 徐灿
权利要求书2页 说明书9页 附图11页

(54)发明名称

攻击通信检测装置及其方法、计算机可读取的记录介质

(57)摘要

提供对从通信间隔的设计值起的偏离坚强的攻击通信检测装置。从通信网络中的各电子控制装置的通信中检测攻击通信的攻击通信检测装置,其包含:接收部,接收不知道是否包含攻击通信的检测用通信数据;通信间隔和计算部,计算作为检测用通信数据的相邻二个通信间隔之和的通信间隔和;估计分布模型存储部,预先存储不包含攻击通信的学习用通信数据的通信间隔以及通信间隔和的估计分布模型;以及检测部,基于估计分布模型和检测用通信数据的通信间隔和,对检测用通信数据是否包含攻击通信进行检测。



CN 111316602 B

1.一种攻击通信检测装置,从通信网络中的各电子控制装置的通信中检测攻击通信,包含:

接收部,接收不知道是否包含所述攻击通信的检测用通信数据;

通信间隔和计算部,计算作为所述检测用通信数据的相邻二个通信间隔之和的通信间隔和;

估计分布模型存储部,预先存储不包含所述攻击通信的学习用通信数据的所述通信间隔以及所述通信间隔和的估计分布模型;以及

检测部,基于所述估计分布模型以及所述检测用通信数据的所述通信间隔和,检测所述检测用通信数据是否包含所述攻击通信。

2.如权利要求1所述的攻击通信检测装置,

所述估计分布模型包含:

所述学习用通信数据的所述通信间隔的估计分布、所述学习用通信数据的所述通信间隔和的估计分布、以及对于这些估计分布的阈值。

3.如权利要求2所述的攻击通信检测装置,

所述检测部在所述检测用通信数据的任意时刻下的所述通信间隔和成为所述阈值以下的情况下,判断为所述检测用通信数据中包含所述攻击通信。

4.一种攻击通信检测装置,从通信网络中的各电子控制装置的通信中检测攻击通信,包含

接收部,接收不包含所述攻击通信的学习用通信数据和不知道是否包含所述攻击通信的检测用通信数据;

通信间隔/通信间隔和计算部,计算所述学习用通信数据的通信间隔、以及作为所述检测用通信数据的相邻二个所述通信间隔之和的通信间隔和;

学习部,学习所述学习用通信数据的所述通信间隔以及所述通信间隔和的估计分布模型;以及

检测部,基于所述估计分布模型和所述检测用通信数据的所述通信间隔和,检测所述检测用通信数据是否包含所述攻击通信。

5.如权利要求4所述的攻击通信检测装置,

所述估计分布模型包含:

所述学习用通信数据的所述通信间隔的估计分布、所述学习用通信数据的所述通信间隔和的估计分布、以及对于这些估计分布的阈值。

6.如权利要求5所述的攻击通信检测装置,

所述检测部在所述检测用通信数据的任意时刻下的所述通信间隔和成为所述阈值以下的情况下,判断为所述检测用通信数据中包含所述攻击通信。

7.如权利要求5所述的攻击通信检测装置,

所述学习部将所述阈值决定为所述学习用通信数据的所述通信间隔的平均值a以上,且小于作为所述平均值a和预先确定的短间隔a'的和的a+a'。

8.如权利要求6所述的攻击通信检测装置,

所述学习部将所述阈值决定为所述学习用通信数据的所述通信间隔的平均值a以上,且小于作为所述平均值a和预先确定的短间隔a'的和的a+a'。

9.如权利要求4至8中任一项所述的攻击通信检测装置，

所述学习部按所述电子控制装置的每个设备状态，学习所述估计分布模型。

10.一种攻击通信检测方法，从通信网络中的各电子控制装置的通信中检测攻击通信，包含：

接收不知道是否包含所述攻击通信的检测用通信数据的步骤；

计算作为所述检测用通信数据的相邻二个通信间隔之和的通信间隔和的步骤；以及

基于不包含所述攻击通信的学习用通信数据的所述通信间隔以及所述通信间隔和的估计分布模型、和所述检测用通信数据的所述通信间隔和，检测所述检测用通信数据是否包含所述攻击通信的步骤。

11.一种计算机可读取的记录介质，

其记录了使计算机作为权利要求1至9中任一项所述的攻击通信检测装置而发挥功能的程序。

攻击通信检测装置及其方法、计算机可读取的记录介质

技术领域

[0001] 本发明涉及在例如搭载于车辆、机床、建设设备、农业设备等设备类上的网络、连接至该网络的通信装置、以及由他们构成的通信系统中，进行攻击通信的检测的攻击通信检测装置、攻击通信检测方法、以及程序。

背景技术

[0002] 在车辆(汽车，特殊车辆，摩托车，自行车等)、机床、建设设备、农业设备等设备类中，有搭载多个电子控制装置(ECU:Electronic Control Unit)的设备，用于这些ECU间的通信网络的，代表性的有控制器局域网(CAN:Controller Area Network)。CAN的网络结采用共享各ECU的通信线的、所谓的总线型结构。对ECU的总线中的通信过程，利用CSMA/CR(载波侦听多路访问/冲突解决(Carrier Sense Multiple Access/Collision Resolution))，即在通信冲突的情况下，优先级高的通信不受冲突影响，并重发优先级低的通信。在CAN上的各ECU的通信中包含ID，ID用于通信调解的优先级、数据内容或发送节点等的识别。

[0003] 暗示对于这些设备控制信息通信网络的网络攻击的危险性。已知通过对网络的不正当(unauthorized)的ECU的连接或对于现有ECU的不正当的操作改写等手段，插入与攻击对象功能关联的ID的攻击发送，有可能诱发该对象功能的不正当的操作。

[0004] 作为检测这些攻击通信的方法，存在检测各同一ID通信的通信间隔的异常的方法(例如非专利文献1)。在CAN中，设计为周期性地发出与重要的功能有关的通信，与该功能关联的ID的通信的间隔按照设计值而大体上固定。在被插入对某重要功能的攻击通信时，与该攻击对象功能有关的ID的通信间隔成为比设计值短的间隔，因此通过检测该间隔异常，能够实现攻击通信检测。但是，通过CSMA/CR的通信过程等，通信间隔常常在一定的允许值范围内偏离设计值，因此需要考虑偏离的允许值而进行通信间隔异常的检测。

[0005] 现有技术文献

[0006] 非专利文献

[0007] 非专利文献1:大冢、石乡冈，“无需变更现有ECU的面向车载LAN的侵入检测方法”，信息处理学会研究报告，Vol.2013-EMB-28,No.6,pp.31-35,2013.

发明内容

[0008] 发明所要解决的课题

[0009] 在对于以往的通信间隔的异常检测中，需要预先掌握通信间隔的设计值以及偏离的允许值。但是，存在没有按照通信间隔的设计值安装ECU的情况、使用了不知道其设计值本身的ECU(例如第三方提供的ECU)的情况等，有时难以事先掌握。关于偏离的允许值，由于通信过程本身包括不确定要素，因此预计即使是如设计值安装的ECU，多数也难以预先掌握。这样，在不能够预先掌握通信间隔的设计值或偏离的允许值的情况下，必须按每个ID掌握间隔值，实施与偏离对应的调整，要费很大的工夫。

[0010] 此外，偏离的允许值的值越大大，则检测精度越差。例如，在比较偏离的允许值为

设计值的±10％的情况和±50％的情况时，如果进行检测以使不会将正常通信误检测，则就前者而言，如果其间隔成为相较于通常的间隔值的90％以下则能够检测为异常通信，相对于此，就后者而言，如果其间隔不成为相较于通常的间隔值的50％以下就检测不到，漏看增多。为了进一步提高检测精度，需要对偏离允许值花费更适当的工夫。

[0011] 因此在本发明中，其目的在于，提供对相对于通信间隔的设计值的偏离具有鲁棒性的攻击通信检测装置。

[0012] 用于解决课题的手段

[0013] 本发明的攻击通信检测装置是从通信网络中的各电子控制装置的通信中检测攻击通信的装置，包含接收部、通信间隔和计算部、估计分布模型存储部、以及检测部。

[0014] 接收部接收不知道是否包含攻击通信的检测用通信数据。通信间隔和计算部计算作为检测用通信数据的相邻二个通信间隔之和的通信间隔和。估计分布模型存储部预先存储不包含攻击通信的学习用通信数据的通信间隔以及通信间隔和的估计分布模型。检测部基于估计分布模型和检测用通信数据的通信间隔和，对检测用通信数据是否包含攻击通信进行检测。

[0015] 本发明的攻击通信检测装置对相对于通信间隔的设计值的偏离具有鲁棒性。

附图说明

[0016] 图1是表示被插入了攻击通信的情况下的通信间隔、通信间隔和的例子的图。

[0017] 图2是表示以任意的时刻为基准的情况下的通信间隔和的推移的图。

[0018] 图3是表示实施例1的攻击通信检测装置的结构的框图。

[0019] 图4是表示实施例1的攻击通信检测装置的学习操作的流程图。

[0020] 图5是表示实施例1的攻击通信检测装置的检测操作的流程图。

[0021] 图6是表示存在偏置偏离的情况下的通信间隔、通信间隔和的例子的图。

[0022] 图7是表示实施例2的攻击通信检测装置的结构的框图。

[0023] 图8是表示实施例2的攻击通信检测装置的学习操作的流程图。

[0024] 图9是表示实施例3的攻击通信检测装置的结构的框图。

[0025] 图10是表示实施例3的攻击通信检测装置的学习操作的流程图。

[0026] 图11是表示变形例1的攻击通信检测装置的结构的框图。

具体实施方式

[0027] 以下详细说明本发明的实施方式。另外，对具有相同功能的结构部附加相同的编号，并省略重复说明。

[0028] 在以下，设想使用CAN(控制器局域网(Controller Area Network))来作为通信网络的协议而进行说明，但本发明的攻击通信检测装置执行攻击通信检测的通信网络的协议并不限定于CAN。本发明的攻击通信检测装置也可以将CAN以外的通信网络的协议(例如，以太网(Ethernet))作为攻击通信检测对象。

[0029] 以下的实施例的攻击通信检测装置通过不仅使用通信间隔，还使用将相邻的二个通信间隔相加的和(以下，称为通信间隔和)，并基于设备控制信息通信网络上的通信的监听或者通过监听得到的数据而进行学习，从而适当地估计通信间隔以及通信间隔和的设计

值以及偏离允许值，并通过基于这些估计，检测通信间隔和(或者除此之外还有通信间隔)的异常，从而进行被插入的攻击通信的检测。

[0030] ＜通信间隔和＞

[0031] 首先说明使用了通信间隔和的异常检测(攻击检测)。如图1所示，通信间隔在正常通信中是大体固定的间隔a(通信间隔的设计值)，但正常通信-攻击通信的间隔成为更短的d(该图中的时刻S_1和时刻S_A之间)。d可以根据插入攻击的定时而在0≤d≤a的范围中任意改变。另一方面，关于通信间隔和，在持续正常通信的情况下成为通信间隔的倍数即2a(例如，同图中的时刻S_2和S_4之间)，但在正常通信-攻击通信-正常通信的模式中的通信间隔和与攻击插入定时无关，一定成为a(同图中的时刻S_1和时刻S_2之间)。在频繁地插入攻击通信的情况下，例如在正常通信-攻击通信-攻击通信中，其通信间隔和成为比a小的值。另一方面，在正常通信-正常通信-攻击通信的部分中的通信间隔和为a+d(该图中的时刻S_0和S_A之间)，在攻击通信-正常通信-正常通信的部分中的通信间隔和为2a-d(同图中的时刻S_A和S_3之间)。

[0032] 因此在不包含攻击通信的情况下的通信间隔和成为2a附近，正常通信-攻击通信-正常通信模式或正常通信-攻击通信-攻击通信的模式的通信间隔和成为a附近或比其小的值，因此这些值能够有较大的差异(参照图2)，能够实现更高精度的检测。记载为附近是因为需要将偏离允许值计算在内，对此将在后面叙述。

[0033] ＜学习＞

[0034] 接下来描述学习。关于与通信间隔以及通信间隔和有关的设计值以及偏离允许值，通过如下的学习(参数化估计)来估计：即，假设通信间隔以及通信间隔和的值的分布，并使用通过观察正常通信而得到的通信间隔以及通信间隔和的值的样本，估计该分布的参数。在以下以将正态分布作为假设的分布的情况为例进行说明。正态分布能够通过计算样本的算数平均和标准差这2个参数来估计。设计值能够将该算数平均作为估计值来使用。偏离允许值能够基于通信间隔以及通信间隔和的估计分布而调整/决定，其细节将在后面叙述。假设的分布不限于正态分布，也可以使用三角分布、连续均匀分布、伽马分布等适当的分布。

[0035] ＜阈值＞

[0036] 最后说明对于偏离的适当的调整。根据上述的内容，认为如果通信间隔和小于2a，则可以检测为包含攻击通信。但是，若考虑偏离允许值，则最好在适当的阈值T以下判定为异常(例如图2的阈值T)，所述阈值T为了抑制误检测而比2a小，且为了提高检测率而比a大。此时，也可以说是阈值T：＝通信间隔和的设计值-通信间隔和的偏离允许值。

[0037] ＜估计分布＞

[0038] 如前所述，在使用了通信间隔和的异常检测中，在包含攻击通信的情况，且其模式为正常通信-攻击通信-正常通信的情况下，其通信间隔和与正常时的通信间隔的值成为相同的值(图1中的时刻S_1和S_2之间)。因此，在是正常通信-攻击通信-正常通信的情况下的通信间隔和的估计分布能够由正常通信中的通信间隔的估计分布来代用。即，只需要学习正常通信，就能够得到正常时的通信间隔的估计分布和正常通信-攻击通信-正常通信模式中的攻击时的通信间隔和的估计分布双方。

[0039] 此时，若使用适当的概率密度函数(整个区间的积分结果为1)来作为估计分布，并将能够允许的最大误检测率(误检测率：＝误检测为异常的正常通信数÷全部正常通信数)

设定为p_-，则能够根据正常时的估计分布来决定满足下式的最大的阈值T。这里L_-是正常时的通信间隔和的估计分布。

[0040] $\int^{T}L_-(x)dx \leqq p_-$

[0041] 此外，如果设定了阈值T，则能够根据攻击时的估计分布，通过下式来预想检测率(检测率：＝正确地检测为异常的攻击通信数÷全部攻击通信数)。这里L_+是(由正常时的通信间隔的估计分布来代替的)攻击时的通信间隔和的估计分布。

[0042] 预想检测率＝$\int^{T}L_+(x)dx$

[0043] 能够使用数值计算等来求得积分值。另一方面，例如，在使用正太分布作为估计分布的情况下，也可以使用通信间隔和的平均值μ、标准差σ、以及z值来如下所示地决定阈值T。

[0044] $T=\mu-z\times\sigma$

[0045] 在正态分布中，积分值(概率)和z值的关系已经作为标准正态分布表而被总结，参照该表而使用接近$1-p_-\times2$的概率的z值即可。在将最大误检测率设为0.15％的情况下，标准正态分布表中的概率为100％-0.15％×2＝99.7％，能够参照表而将对应的z值决定为z＝3。z值是仅根据指定的最大误检测率而决定的值，也可以不按照每个ID来逐个调整。能够利用像这样能够根据使用的分布而容易地计算阈值T的方法。

[0046] 由此，能够机械地进行满足能够允许的最大误检测率且能够预测此时的检测率的、对于偏离的调整，而不需要对于每个ID的手动调整。另一方面，在特定的ID中要求特别低的误检测率的情况等存在个别的要求的情况下，也可以进行按每个该特定ID而指定最大误检测率等的个别设定。

[0047] 此外，也可以如下所示，指定能够允许的最小检测率p_+，求取阈值T或其预想误检测率，同样能够机械地进行调整。

[0048] $\int^{T}L_+(x)dx \leqq p_+$

[0049] 预想误检测率＝$\int^{T}L_-(x)dx$

[0050] 作为将通信间隔和用于异常检测的优点，还能够举出与利用通信间隔的情况相比，偏离较小这一点。多数ECU是使用内部时钟来计量周期发送的定时。因此，由于因等待冲突而延迟了的通信的紧随其后的通信，(由于不是在隔开了设计值的间隔的量之后发送，而是根据时钟定时而被发送)可以视为是缩短在紧前延迟了的量的间隔而提前被发送。另一方面，通信间隔和成为使该延迟量和提前发送量进行了抵消的结果。因此，通信间隔和的偏离采用比根据通信间隔的偏离而预想的更小的值，甚至根据情况而成为比通信间隔的偏离更小的值。偏离小有利于检测精度的提高。

[0051] 【实施例1】

[0052] 以下，参照图3说明实施例1的攻击通信检测装置的结构。如该图所示，本实施例的攻击通信检测装置1包含接收部11、临时保持部12、通信间隔/通信间隔和计算部13、学习部14、估计分布模型存储部15、以及检测部16。以下，参照图4来说明学习时的各结构要件的操作。

[0053] ＜接收部11(学习时)＞

[0054] 接收部11接收作为设备控制信息通信网络的通信或者通过通信的加工等而生成的通信数据的、不包含攻击通信的学习用通信数据(S11-1)。接收部11对学习用通信数据的

各数据单位(例如各分组、各帧)附加通信时刻。设为按通信的每个ID来区分学习用通信数据,以下的步骤中,设为对各ID的学习用通信数据,按每个ID分别地执行。

[0055] 接收部11可以通过对网络或网关进行监听而获得通信,另一方面,也可以从其他监控设备获得通信数据而作为日志等数据。对通过监听而获得的通信附加其接收时刻(通信时刻),但在获得通信数据作为日志等数据的情况下,并且是已经附加了接收时刻(通信时刻)的情况下,也可以省略时刻附加。在接收部11中,也可以根据通信的ID而仅选择并接受检测对象。

[0056] <临时保持部12(学习时)>

[0057] 临时保持部12从最新的学习用通信数据的通信时刻起保持多个(例如3个)学习用通信数据的通信时刻(S12-1)。

[0058] <通信间隔/通信间隔和计算部13(学习时)>

[0059] 通信间隔/通信间隔和计算部13使用在步骤S12-1中被保持的学习用通信数据的通信时刻,计算学习用通信数据的通信间隔(S13-1)。此外,通信间隔/通信间隔和计算部13为了计算前述的阈值T,也一并计算学习用通信数据的通信间隔和。

[0060] <学习部14>

[0061] 学习部14以通过设定而指定的假设分布或最大误检测率(或者最小检测率)为条件,使用在步骤S13-1中计算的通信间隔、通信间隔和,来对学习用通信数据的通信间隔的估计分布、学习用通信数据的通信间隔和的估计分布、以及对于这些估计分布的阈值T等进行学习(S14)。这些估计分布、阈值T等作为估计分布模型而被存储于估计分布模型存储部15。

[0062] 例如,学习部14将在步骤S13-1中计算的通信间隔、通信间隔和作为样本数据,以通过设定(装置的管理者等输入)而指定的假设的分布或最大误检测率(或者最小检测率)等作为条件,按每个ID来确定估计分布或阈值T,将它们作为估计分布模型来进行学习并存储于估计分布模型存储部15中。

[0063] 学习部14汇总一定程度的量的样本数据,在实施预处理后进行估计分布的确定。作为样本数据的预处理的例子,存在去除值大的以及值小的百分之几的数据,抑制例外值的影响等。另一方面,如果可以的话,学习部14也可以不汇总样本数据,而以一件件地逐次处理,更新估计分布模型的方法来实施学习。例如在使用正态分布的情况下,能够使用动差(moment)来进行逐次处理。

[0064] <估计分布模型存储部15>

[0065] 如上所述,存储在估计分布模型存储部15中的估计分布模型可以包含学习用通信数据的通信间隔的估计分布、学习用通信数据的通信间隔和的估计分布、以及对于这些估计分布的阈值T,也可以包含除此以外的估计分布的参数。在估计分布模型存储部15中按每个ID保存估计分布模型。若以正态分布为例,则估计分布模型中包含它们的平均值、标准差、阈值T等。模型也可以根据要件而仅适当地存储必要的内容。例如,也可以仅保管用于检测时的阈值T。此外,也可以仅将平均值、标准差存储在估计分布模型存储部15中,阈值T每次由检测部16来计算。

[0066] 以下,参照图5来说明检测时的各结构要件的操作。

[0067] <接收部11(检测时)>

[0068] 接收部11接收作为设备控制信息通信网络的通信或者通过通信的加工等而生成的通信数据的、不知道是否包含攻击通信的检测用通信数据(S11-2)。

[0069] ＜临时保持部12(检测时)＞

[0070] 临时保持部12从最新的检测用通信数据的通信时刻起保持多个(至少3个以上)检测用通信数据的通信时刻(S12-2)。为了计算通信间隔和,需要相同ID的通信的最近3个以上的通信时刻,因此临时保持部12按每个ID保持最近3个以上的通信时刻。

[0071] 在通信新到达的情况下,临时保持部12调查其ID,丢弃对应的ID的最早的通信时刻,并追加新的通信时刻(快进快出(First in First out)缓冲器)。

[0072] ＜通信间隔/通信间隔和计算部13(检测时)＞

[0073] 通信间隔/通信间隔和计算部13使用在步骤S12-2中被保持的检测用通信数据的通信时刻,计算作为检测用通信数据的相邻二个通信间隔之和的通信间隔和(S13-2)。若使用图1的例子来说明步骤S13-2,则例如在该图的例子中,在接收时刻S_1的通信数据的通信单位(例如分组或者帧),并新记录了通信时刻S_1的情况下,使用时刻S_1和早于时刻S_1的二个通信时刻来计算通信间隔和2a。同样地,在接收时刻S_A的通信数据的通信单位(例如分组或者帧),并新记录了通信时刻S_A的情况下,使用时刻S_A、时刻S_1、时刻S_0来计算通信间隔和a+d。同样地,在接收时刻S_2的通信数据的通信单位(例如分组或者帧),并新记录了通信时刻S_2的情况下,使用时刻S_2、时刻S_A、时刻S_1来计算通信间隔和a。因此,在该图的例子的情况下,伴随着通信数据的接收,以2a、a+d、a、2a-d、2a的顺序来依次计算其通信间隔和。

[0074] ＜检测部16＞

[0075] 检测部16基于估计分布模型和检测用通信数据的通信间隔和,对检测用通信数据是否包含攻击通信进行检测(S16)。

[0076] 更具体而言,检测部16将在步骤S13-2中被依次计算的通信间隔和与存储在估计分布模型存储部15中的估计分布模型进行比较,并在检测用通信数据的任意的时刻中的通信间隔和成为对于估计分布的阈值T以下的情况下,判断为检测用通信数据中包含攻击通信,并输出检测结果(S16)。如前所述,阈值T可以预先在学习时进行计算,也可以每次由检测部16来计算。检测处理可以在每次接收通信时进行,也可以在汇总了一定程度的通信之后进行。

[0077] 检测结果可以是输出异常或正常的形式,也可以仅在异常时输出检测结果。也可以对检测结果附加用于确定检测用通信数据的信息,例如接收时刻或ID等。在连续检测到对于同一ID的异常的情况下,可以将它们汇总,或者除此以外还附加异常检测开始时刻、结束时刻、ID等而输出。检测部16可以通过网络发送检测结果,也可以经由其他装置而发送/通知检测结果。

[0078] 另外,在频繁地被插入攻击通信的情况下,有时与正常通信冲突,其中一方的通信没有被发送。此时,接收部11也可以接收在CAN中发送的错误帧,通过错误帧而估计没有被发送的通信,将该通信与通常的通信同样地进行处理。在攻击通信与正常通信冲突,且仅发送了攻击通信的情况下,其通信间隔/通信间隔和不能够与正常时区分。但是,如前所述,通过还加入错误帧,能够将在同时刻被发送的正常通信和攻击通信作为2个通信来处理,能够实现通信间隔/通信间隔上的区分。

[0079] 攻击通信检测装置1也可以设为去除了检测部16的仅进行学习的装置,也可以设

为去除了学习部14的仅进行检测的装置。仅进行学习的装置将估计分布模型作为其学习的结果而存储在估计分布模型存储部15中。如果将所存储的估计分布模型存储在仅进行检测的装置的估计分布模型存储部15中，则能够在该装置中无需学习就进行检测。关于仅进行检测的装置，将在后面的变形例1中叙述。

[0080] 【实施例2】

[0081] 在周期型发送中存在变形，通常以固定的通信间隔而发送通信，但有时在某个契机下，仅在该时刻超过偏离允许值而以短间隔(或者长间隔)来发送，并在其之后以原来的固定间隔来发送。以下描述关于作为这种变形的存在偏置偏离的周期型的异常检测。

[0082] 在图6中示出存在偏置偏离的周期型的通信间隔以及通信间隔和。如该图所示，存在正常通信的间隔缩短为a’(＜a)的地方，因此在将比设计值a短间隔的通信间隔检测为由攻击通信引起的通信间隔算法中，误检测a’。另一方面，正常时的通信间隔和在a+a’到2a之间分布，且异常时的通信间隔和在正常-攻击-正常模式中成为a附近，因此在将阈值T设为a附近，且通信间隔和与阈值T相等或比阈值T小的情况下，能够将该通信检测为异常。如果阈值T考虑偏离允许值而被设为从a到a+a’之间的适当的值，且决定了阈值，则可以适用通信间隔和来与实施例1同样地进行检测。

[0083] 参照图7来说明实施例2的攻击通信检测装置的结构。如该图所示，本实施例的攻击通信检测装置2包含接收部11、临时保持部12、通信间隔/通信间隔和计算部13、学习部24、估计分布模型存储部15、以及检测部16，学习部24以外的各结构要件与实施例1相同。

[0084] ＜学习部24＞

[0085] 参照图8说明学习部24的操作。如前所述，学习部24将阈值T决定为学习用通信数据的通信间隔的平均值a以上、且小于作为平均值a和预先确定的短间隔a’的和的a+a’，并学习估计分布模型(S24)。

[0086] 学习部24如以下求取估计分布。首先，学习部24基于学习用通信数据的各通信时刻，求取将短间隔a’除外了的通信间隔的估计分布和将短间隔和a+a’除外了的通信间隔和的估计分布。在该除外中，存在通过去除值大的和值小的百分之几的数据而求取估计分布的方法或进行使用了似然度的分布估计的方法。

[0087] 接下来，学习部24分别求取仅短间隔a’的估计分布、仅短间隔和a+a’的估计分布。短间隔的估计分布也可以使用与前述的将短间隔除外了的估计分布不同的分布。学习部24例如能够在前者中使用正态分布，在后者中使用均匀连续分布。如果这样求取估计分布，则能够与实施例1同样地求取阈值。

[0088] 【实施例3】

[0089] 某个ECU有时根据设备状态，例如车辆的停车、行驶、自动行驶等状态的不同，其发送定时发生变化。在这种情况下，在周期型发送中，根据设备状态而其通信间隔以及通信间隔和会发送变更。以下，说明进行与设备状态对应的异常检测的实施例3的攻击通信检测装置3。

[0090] 如图9所示，本实施例的攻击通信检测装置3包含接收部11、临时保持部12、通信间隔/通信间隔和计算部13、学习部34、估计分布模型存储部15、以及检测部16，学习部34以外的各结构要件与实施例1相同。

[0091] ＜学习部34＞

[0092] 参照图10说明学习部34的操作。学习部34按照电子控制装置的每个设备状态，学习估计分布模型(S34)。更详细而言，学习部34按每个设备状态确定估计分布模型，按每个设备状态以及每个ID而将其估计分布模型存储在估计分布模型存储部15中。接收部11接收表示设备状态的通信/信号，并根据该接收内容而判断设备状态，将估计分布模型存储部15切换为用于该设备状态。由此，在由于设备状态而发生变化的情况下也可以进行异常检测。表示设备状态的通信/信号可以在网络上发送，也可以在其他路径上发送。

[0093] [变形例1]

[0094] 参照图11，说明变形例1的攻击通信检测装置1A。本变形例的攻击通信检测装置1A是从实施例1的装置中去除了学习功能而仅进行检测的装置的例子。如该图所示，本变形例的攻击通信检测装置1A是包含接收部11、临时保持部12、通信间隔和计算部13A、估计分布模型存储部15、以及检测部16的结构。在估计分布模型存储部15中，预先存储了在实施例1的步骤S14等中学习完毕的估计分布模型。在本变形例中，检测用通信数据的通信间隔和的计算是必须的，但检测用通信数据的通信间隔的计算不是必须的，因此实施例1中的通信间隔/通信间隔和计算部13在本变形例中更名为通信间隔和计算部13A。

[0095] ＜效果＞

[0096] 根据上述的实施例、变形例的攻击通信检测装置，即使预先不知道设计值/偏离，也能够通过学习而掌握，从而能够容易地对各种车型或设备应用异常检测。此外，即使不按每个ID而手动地进行调整，也能够通过指定能够允许的最大误检测率等期望的精度，容易进行自动调整，实现高效化。通过利用通信间隔和，提高检测精度。

[0097] ＜附记＞

[0098] 本发明的装置作为单一的硬件实体，例如具有能够连接键盘等的输入部、能够连接液晶显示器等的输出部、能够连接可以和硬件实体的外部进行通信的通信装置(例如通信电缆)的通信部、CPU(中央处理单元(Central Processing Unit)，可以具备高速缓存或寄存器等)、作为存储器的RAM或ROM、作为硬盘的外部存储装置、以及以能够进行这些输入部、输出部、通信部、CPU、RAM、ROM、外部存储装置之间的数据交换的方式连接的总线。另外，根据需要，也可以在硬件实体中设置能够读写CD-ROM等存储介质的装置(驱动器)等。作为具备这样的硬件资源的物理性实体，有通用计算机、嵌入设备等。

[0099] 在硬件实体的外部存储装置中存储有实现上述功能所需的程序以及该程序的处理所需的数据等(不限于外部存储装置，例如也可以将程序预先存储在作为只读存储装置的ROM中)。此外，通过这些程序的处理得到的数据等，被适当地存储在RAM或外部存储装置等中。

[0100] 在硬件实体中，存储在外部存储装置(或者ROM等)中的各程序和处理该各程序所需的数据根据需要被读入存储器，适当地通过CPU进行解释执行/处理。其结果，CPU实现规定的功能(上述由……部、……手段等表示的各结构要件)。

[0101] 本发明不限于上述实施方式，能够在不脱离本发明主旨的范围内进行适当的变更。另外，上述实施方式中说明的处理不仅按照记载的顺序按时间顺序执行，也可以根据执行处理的装置的处理能力或根据需要并行地或单独地执行。

[0102] 如上所述，在上述实施方式中说明的硬件实体(本发明的装置)中的处理功能通过计算机、嵌入设备来实现的情况下，硬件实体应具有的功能的处理内容由程序来记述。然

后，通过在计算机、嵌入设备上执行该程序，在计算机、嵌入设备上实现上述硬件实体中的处理功能。

[0103] 记述了该处理内容的程序能够预先存储在计算机、嵌入设备可读取的存储介质上。作为计算机、嵌入设备可读取的存储介质，例如可以是磁存储装置、光盘、光磁存储介质、半导体存储器等。具体而言，例如，能够将硬盘装置、柔性盘、磁带等用作磁存储装置，将DVD(数字多用盘(Digital Versatile Disc))、DVD-RAM(随机存取存储器(Random Access Memory))、CD-ROM(紧凑盘只读存储器(Compact Disc Read Only Memory))、CD-R(可记录(Recordable))/RW(可重写(ReWritable))等用作光盘，将MO(磁光盘(Magneto-Optical disc))等用作光磁存储介质，将EEP-ROM(电子可擦可编程只读存储器(Electronically Erasable and Programmable-Read Only Memory)等)用作半导体存储器等。

[0104] 此外，该程序的流通例如通过销售、转让、借出存储了该程序的DVD、CD-ROM等便携式存储介质等来进行。进一步，也可以设为如下结构：将该程序预先存储在服务器计算机的存储装置中，通过网络，将该程序从服务器计算机转发到其他的计算机、嵌入设备，从而使该程序流通。

[0105] 执行这种程序的计算机、嵌入设备例如首先将记录在便携式存储介质中的程序或从服务器计算机转发的程序暂时存储在自己的存储装置中。然后，在执行处理时，该计算机、嵌入设备读取存储在自己的存储介质中的程序，执行根据读取的程序的处理。另外，作为该程序的另一执行方式，计算机、嵌入设备也可以从便携型存储介质直接读取程序，执行按照该程序的处理，而且，在从服务器计算机每次向该计算机、嵌入设备转发程序时，也可以按照所接受的程序依次执行处理。此外，也可以构成为如下结构：不从服务器计算机向该计算机、嵌入设备转发程序，而基于只通过该执行指示和结果获取来实现处理功能的、所谓的ASP(应用服务供应商(Application Service Provider))型服务来执行上述处理。另外，设为在本方式的程序中，包含供电子计算机处理用的、并且是基于程序的信息(不是对于计算机、嵌入设备的直接指令，但具有用于规定计算机、嵌入设备的处理的性质的数据等)。

[0106] 此外，在该方式中，设为通过在计算机、嵌入设备上执行规定的程序，构成硬件实体，但也可以设为在硬件上实现这些处理内容的至少一部分。

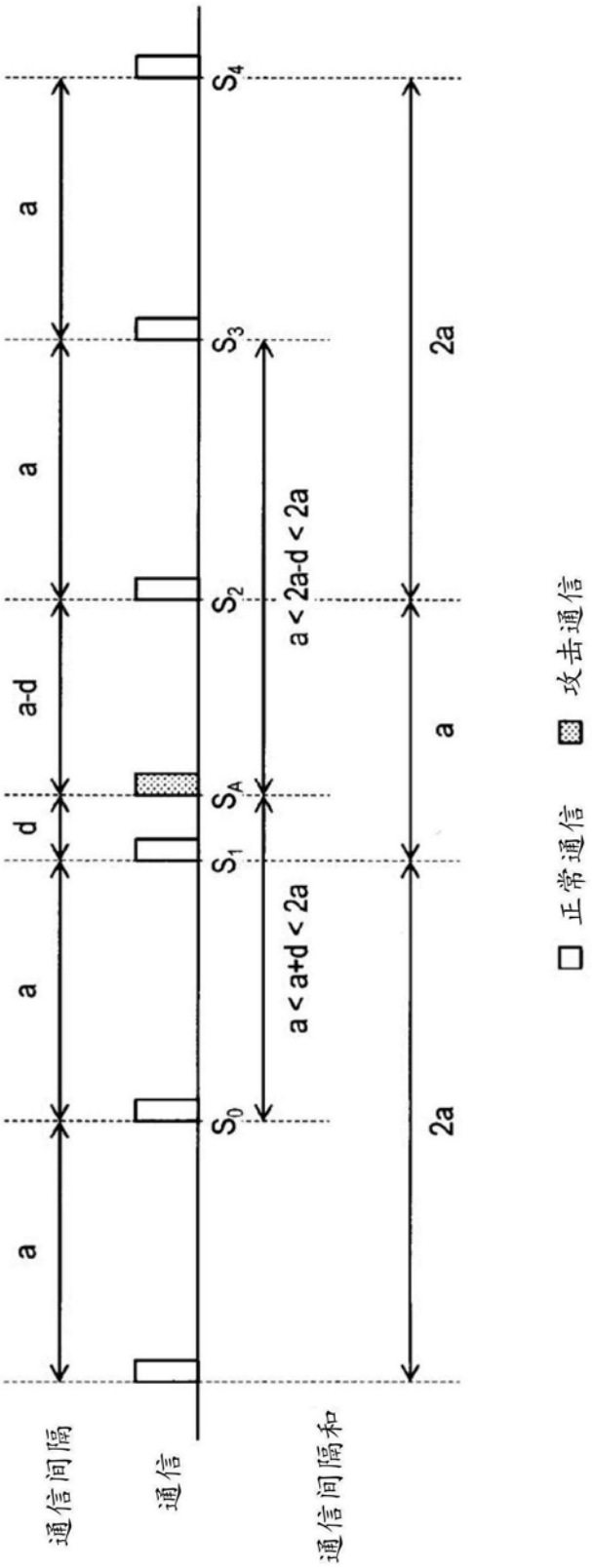

通信间隔
通信
通信间隔和
a
a
a-d
d
a
a
S_0
S_1
S_A
S_2
S_3
S_4
a < a+d < 2a
a < 2a-d < 2a
2a
a
2a
正常通信
攻击通信

图1

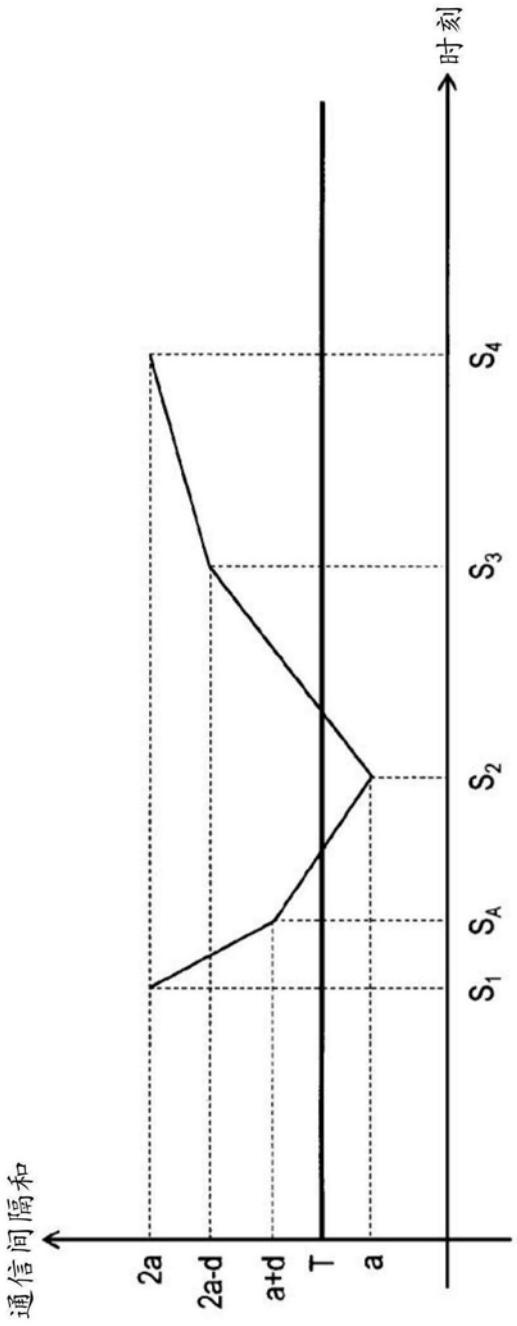


图2

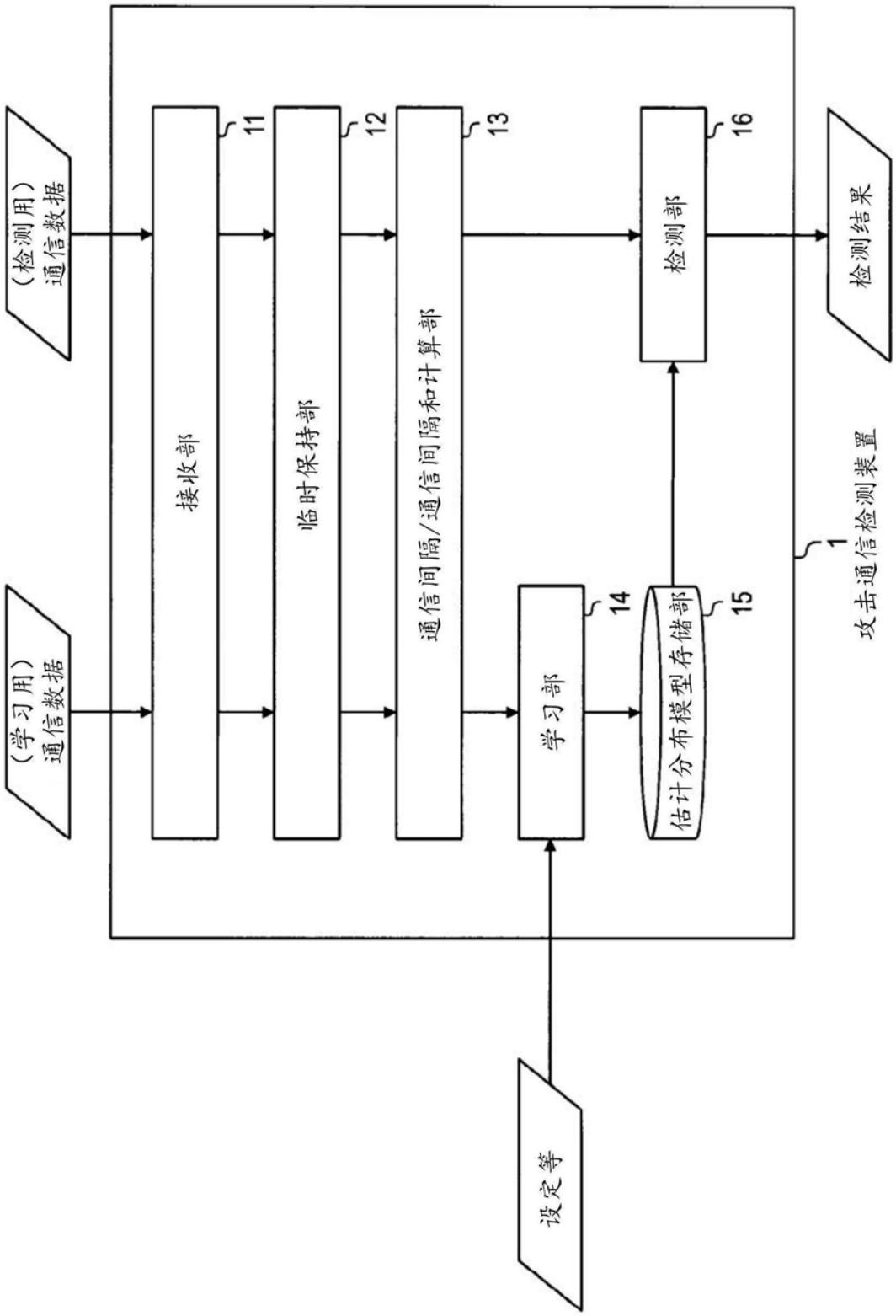

（检测用）
通信数据
（学习用）
通信数据
接收部
11
临时保持部
12
通信间隔/通信间隔和计算部
13
学习部
14
估计分布模型存储部
15
检测部
16
检测结果
1
攻击通信检测装置
设定等

图3

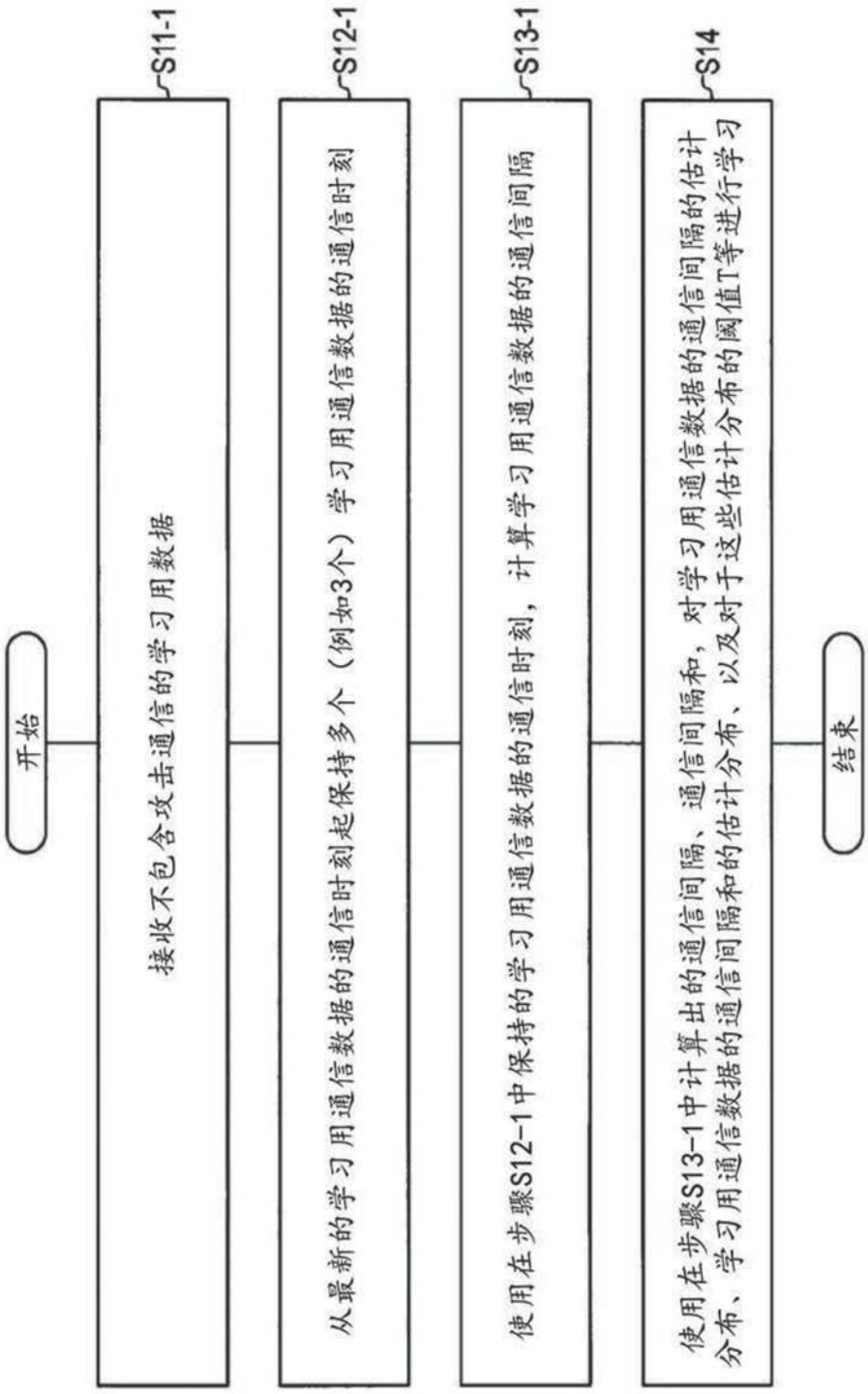

开始
S11-1
接收不包含攻击通信的学习用数据
S12-1
从最新的学习用通信数据的通信时刻起保持多个（例如3个）学习用通信数据的通信时刻
S13-1
使用在步骤S12-1中保持的学习用通信数据的通信时刻，计算学习用通信数据的通信间隔
S14
使用在步骤S13-1中计算出的通信间隔、通信间隔和，对学习用通信数据的通信间隔的估计分布、学习用通信数据的通信间隔和的估计分布、以及对于这些估计分布的阈值T等进行学习
结束

图4

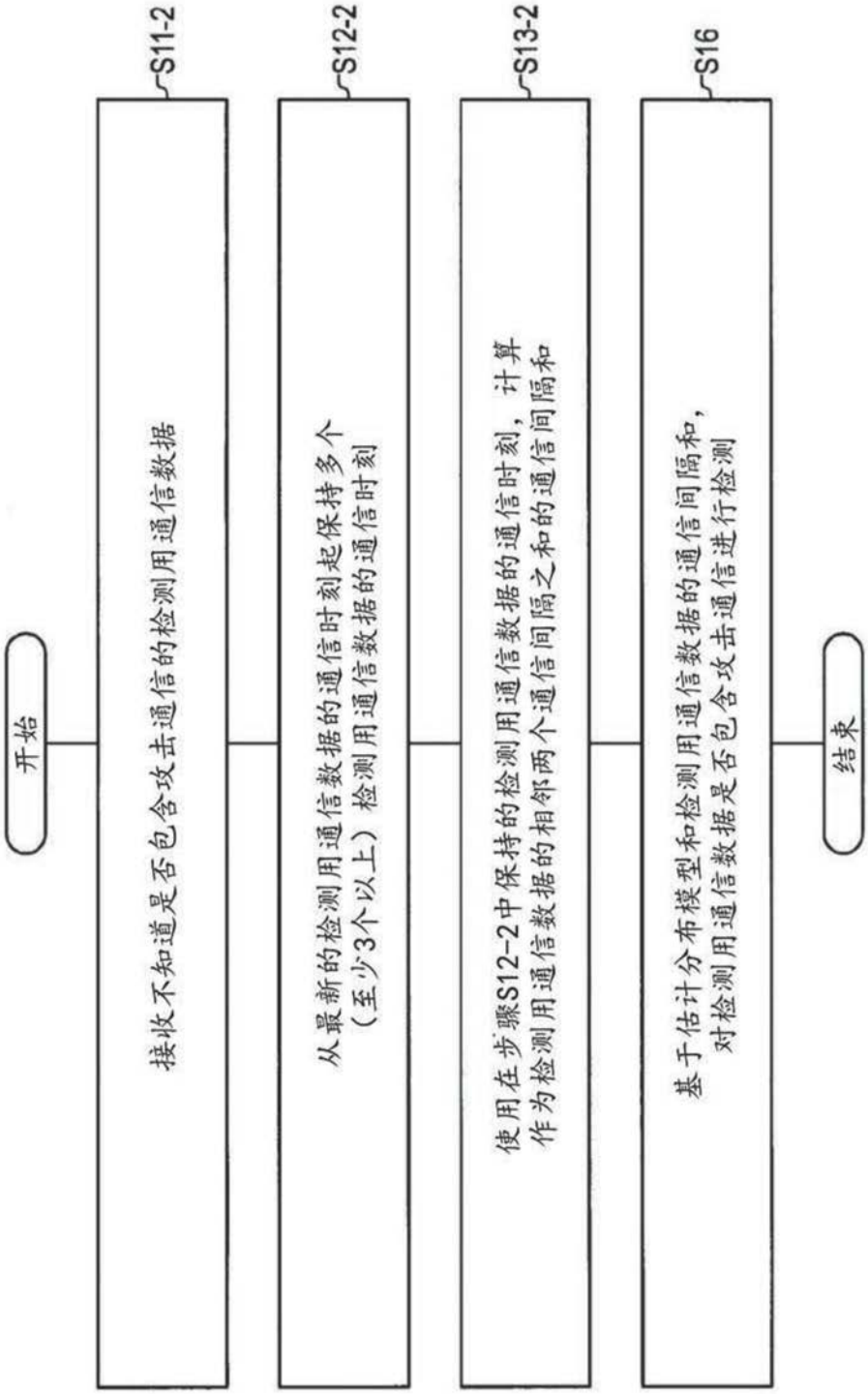

开始
S11-2
接收不知道是否包含攻击通信的检测用通信数据
S12-2
从最新的检测用通信数据的通信时刻起保持多个（至少3个以上）检测用通信数据的通信时刻
S13-2
使用在步骤S12-2中保持的检测用通信数据的通信时刻，计算作为检测用通信数据的相邻两个通信间隔之和的通信间隔和
S16
基于估计分布模型和检测用通信数据的通信间隔和，对检测用通信数据是否包含攻击通信进行检测
结束

图5

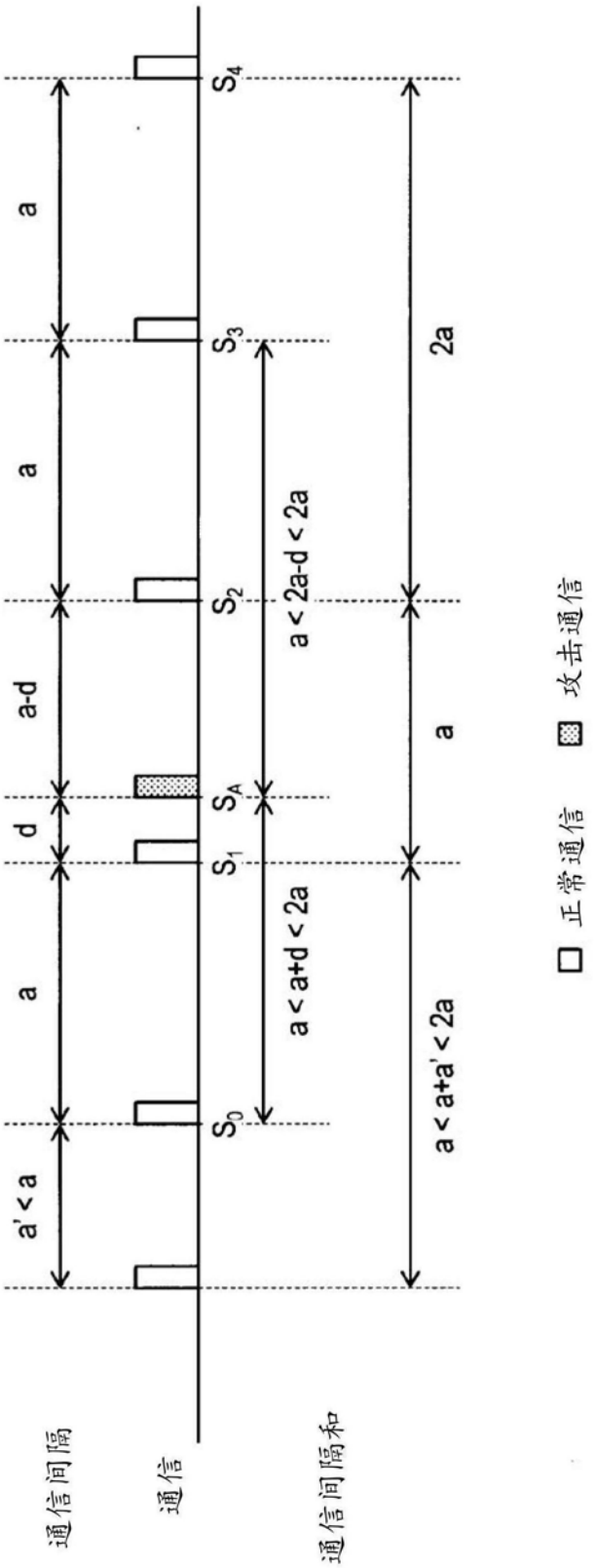

通信间隔
通信
通信间隔和
a' < a
a
d
a-d
a
a
S0
S1
SA
S2
S3
S4
a < a+d < 2a
a < 2a-d < 2a
a < a+a' < 2a
a
2a
正常通信
攻击通信

图6

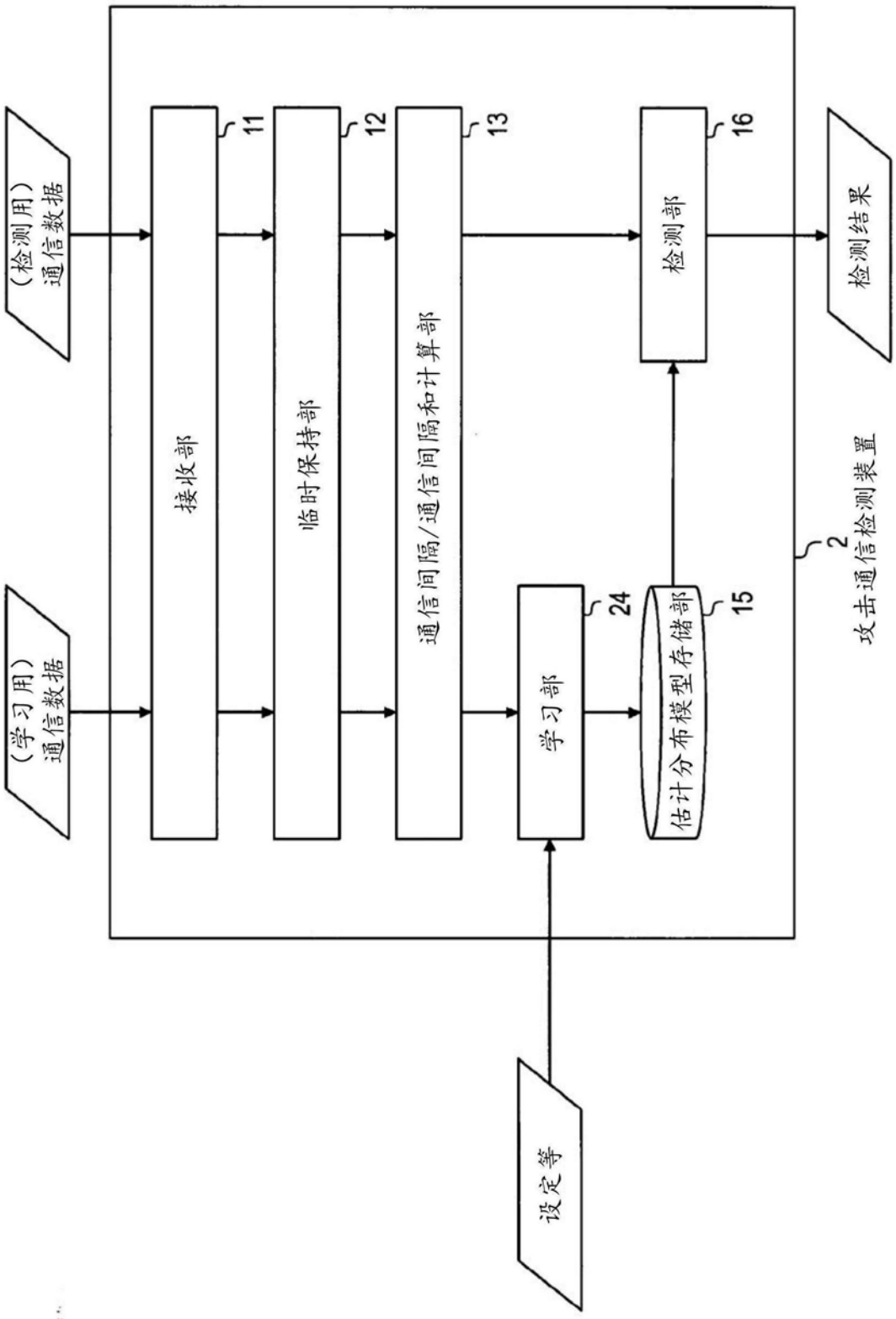

（检测用）
通信数据
（学习用）
通信数据
接收部
11
临时保持部
12
通信间隔/通信间隔和计算部
13
学习部
24
估计分布模型存储部
15
检测部
16
检测结果
2
攻击通信检测装置
设定等

图7

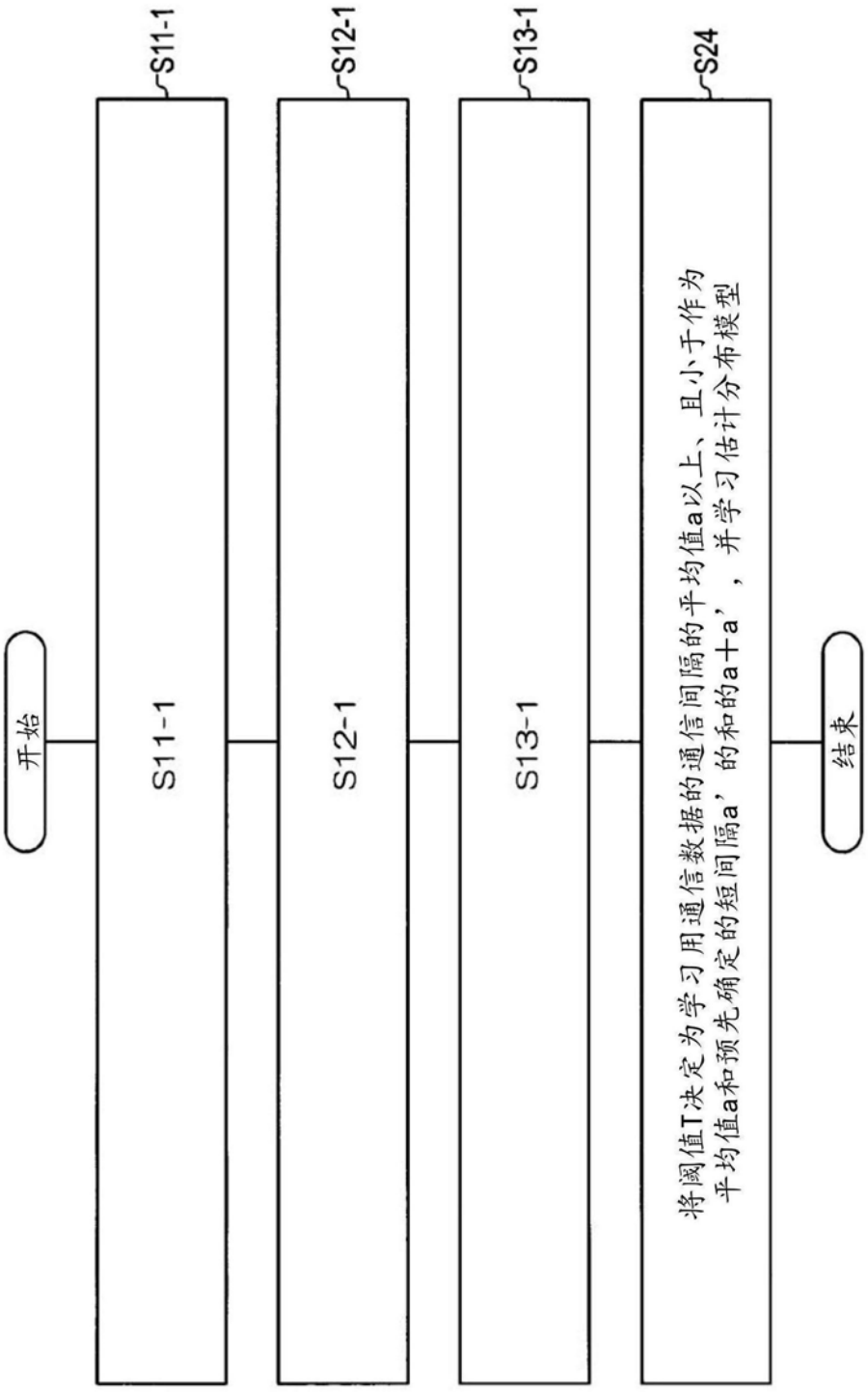

开始
S11-1
S11-1
S12-1
S12-1
S13-1
S13-1
S24
将阈值T决定为学习用通信数据的通信间隔的平均值a以上、且小于作为平均值a和预先确定的短间隔a'的和的a+a'，并学习估计分布模型
结束

图8

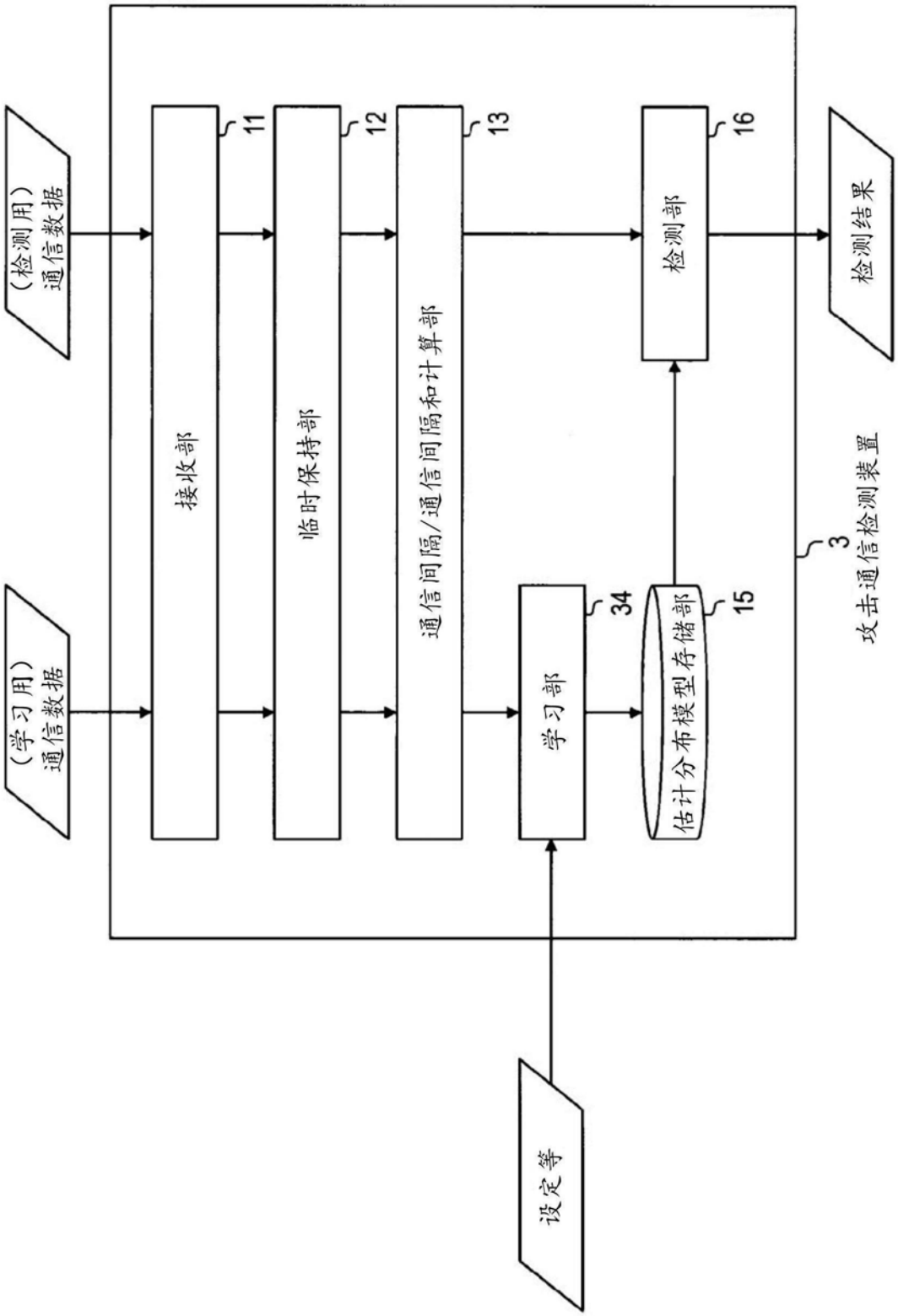

(检测用)
通信数据
(学习用)
通信数据
设定等
接收部
11
临时保持部
12
通信间隔/通信间隔和计算部
13
学习部
34
估计分布模型存储部
15
检测部
16
检测结果
3
攻击通信检测装置

图9

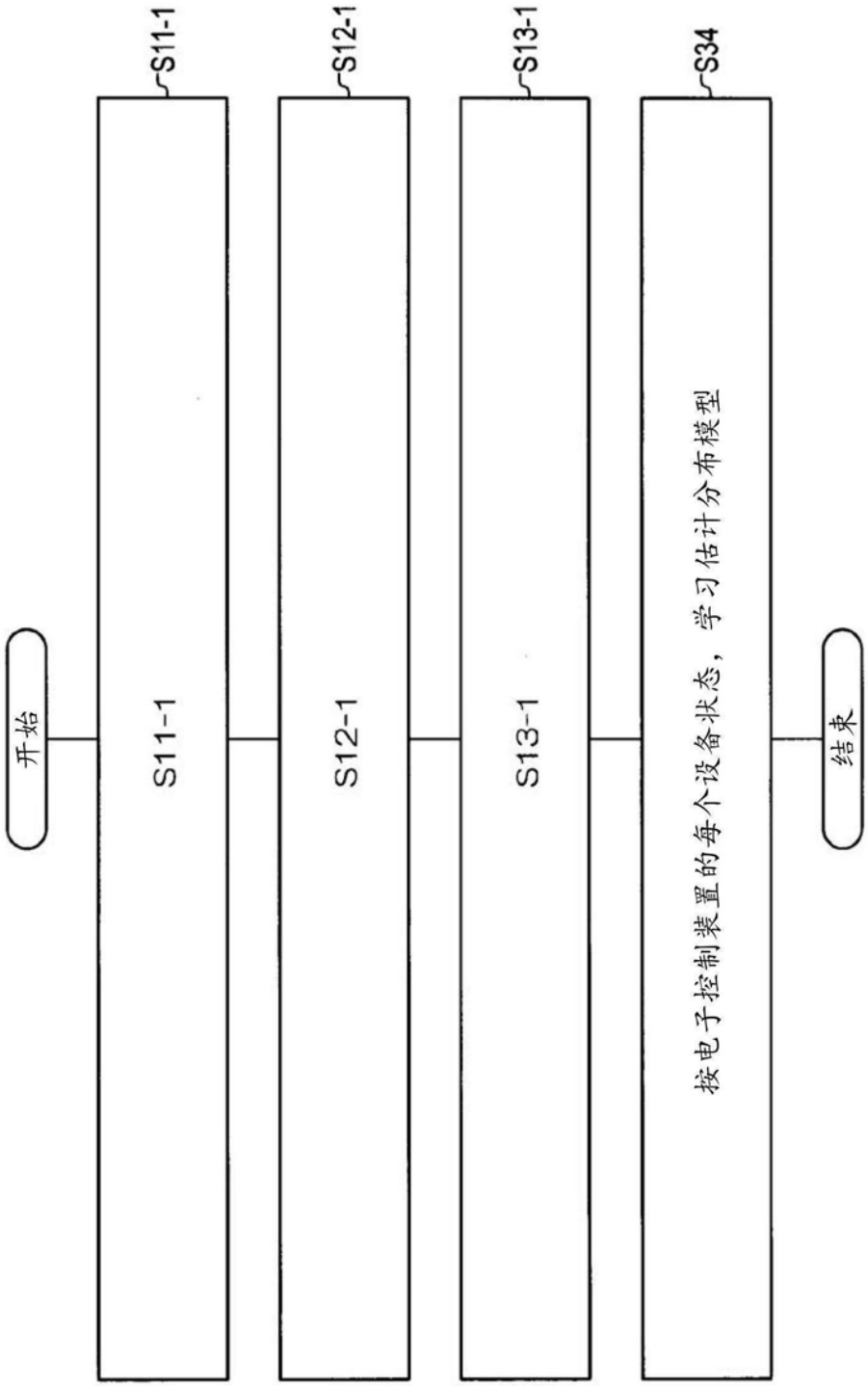


图10

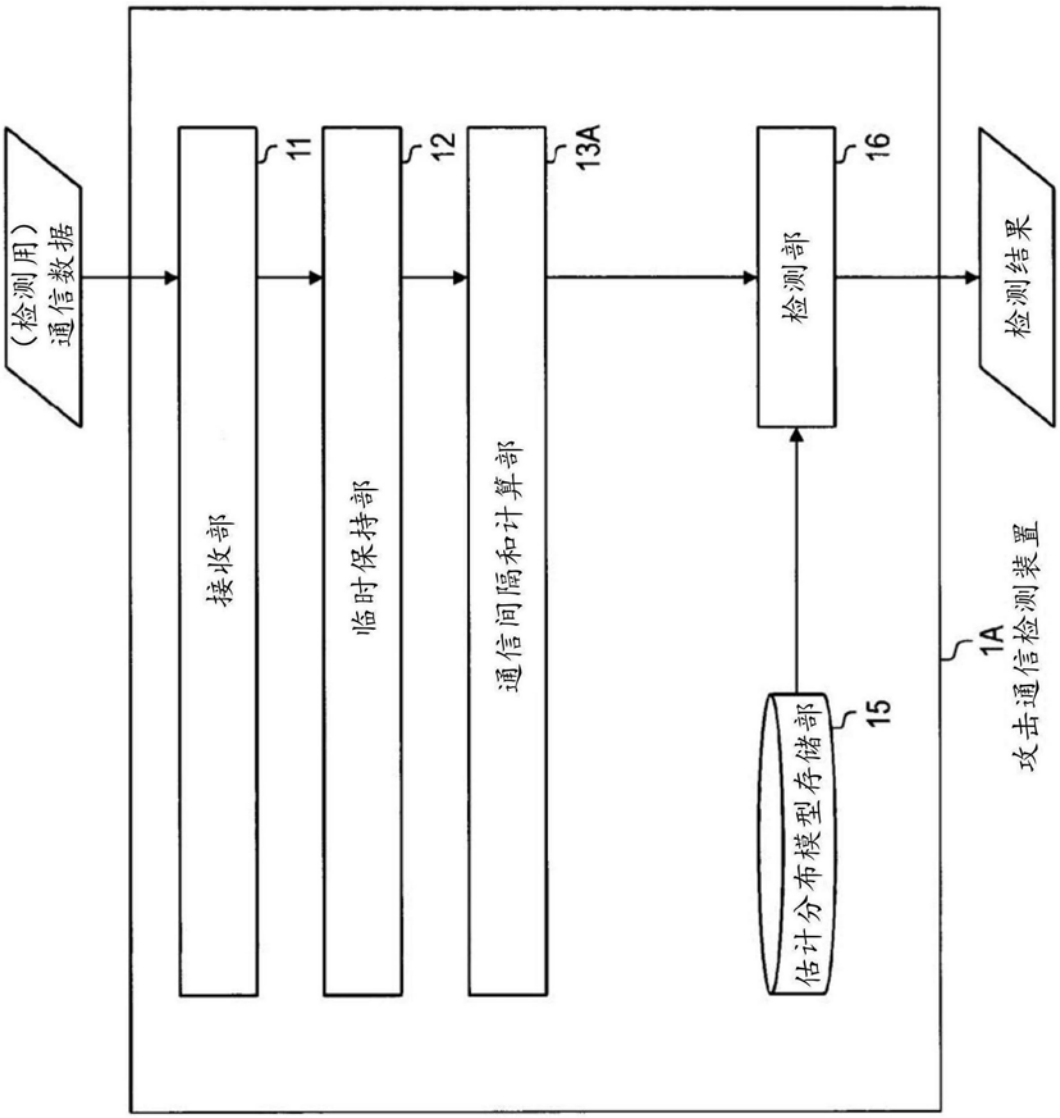

(检测用)
通信数据
接收部
11
临时保持部
12
通信间隔和计算部
13A
检测部
16
检测结果
估计分布模型存储部
15
1A
攻击通信检测装置

图11