(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118592018 A
(43)申请公布日 2024.09.03

(21)申请号 202280090009.9
(22)申请日 2022.12.16
(30)优先权数据
2022-065792 2022.04.12 JP
(85)PCT国际申请进入国家阶段日
2024.07.24
(86)PCT国际申请的申请数据
PCT/JP2022/046331 2022.12.16
(87)PCT国际申请的公布数据
WO2023/199552 JA 2023.10.19
(71)申请人 住友电气工业株式会社
地址 日本大阪
申请人 住友电装株式会社
株式会社自动网络技术研究所
(72)发明人 增川京佑 塚本博之 三好孝典 上田浩史
(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
专利代理师 田喜庆
(51)Int.Cl.
H04L 43/0852(2006.01)

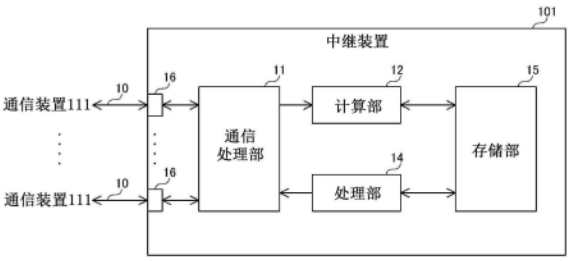
权利要求书1页 说明书16页 附图7页

(54)发明名称

检测装置及检测方法

(57)摘要

一种检测装置,具备:计算部,计算对象消息的接收间隔;检测部,基于所述接收间隔进行检测处理;以及计数部,对多个突发消息进行计数,所述多个突发消息包括所述接收间隔比所述发送周期大规定值以上的所述对象消息即延迟消息以及继所述延迟消息之后被接收且所述接收间隔为规定值以下的一个或多个所述对象消息,所述检测部基于所述计数部的计数值,确定是否对所述多个突发消息中的至少任一个所述突发消息进行基于所述接收间隔的所述检测处理。



CN 118592018 A

1.一种检测装置,检测网络中的异常,包括以规定的发送周期收发的周期消息的多个对象消息在所述网络中进行收发,所述检测装置具备:

计算部,计算所述对象消息的接收间隔;

检测部,基于由所述计算部计算出的所述接收间隔,进行检测所述网络中的异常的检测处理;以及

计数部,对多个突发消息进行计数,所述多个突发消息包括所述接收间隔比所述发送周期大规定值以上的所述对象消息即延迟消息以及继所述延迟消息之后被接收且所述接收间隔为规定值以下的一个或多个所述对象消息,

所述检测部基于所述计数部的计数值,确定是否对所述多个突发消息中的至少任一个所述突发消息进行基于所述接收间隔的所述检测处理。

2.根据权利要求1所述的检测装置,其中,

在所述计数值为阈值以下的情况下,所述检测部不进行基于所述多个突发消息中的至少任一个所述突发消息的所述接收间隔的所述检测处理。

3.根据权利要求1或2所述的检测装置,其中,

在所述计数值比所述阈值大的情况下,所述检测部基于所述多个突发消息的所述接收间隔进行所述检测处理。

4.根据权利要求1至3中任一项所述的检测装置,其中,

所述检测部根据作为所述延迟消息的所述对象消息的所述接收间隔来确定所述阈值。

5.根据权利要求1至4中任一项所述的检测装置,其中,

所述检测部计算根据所述接收间隔与关于所述接收间隔的参照信息的关系而增减的检测指标,并基于计算出的所述检测指标进行所述检测处理,

在所述计数值为所述阈值以下的情况下,所述检测部不进行针对所述多个突发消息中的至少任一个所述突发消息的所述检测指标的计算。

6.根据权利要求1至5中任一项所述的检测装置,其中,

在从作为所述突发消息的所述对象消息的接收时刻起规定时间以内未接收下一个所述对象消息的情况下,所述计数部结束计数,

所述检测部暂停所述检测处理,直到所述计数部的计数结束,并在所述计数部的计数结束后重启所述检测处理。

7.一种检测方法,是检测网络中的异常的检测装置中的检测方法,包括以规定的发送周期收发的周期消息的多个对象消息在所述网络中进行收发,所述检测方法包括以下步骤:

计算所述对象消息的接收间隔;

基于计算出的所述接收间隔,进行检测所述网络中的异常的检测处理;以及

对多个突发消息进行计数,所述多个突发消息包括所述接收间隔比所述发送周期大规定值以上的所述对象消息即延迟消息以及继所述延迟消息之后被接收且所述接收间隔为规定值以下的一个或多个所述对象消息,

在进行所述检测处理的步骤中,基于所述多个突发消息的计数值,确定是否对所述多个突发消息中的至少任一个所述突发消息进行基于所述接收间隔的所述检测处理。

检测装置及检测方法

技术领域

[0001] 本公开涉及检测装置及检测方法。

[0002] 本申请要求以2022年4月12日申请的日本申请特愿2022-65792号为基础的优先权,在此引入其公开的所有内容。

背景技术

[0003] 专利文献1(国际公开第2021/111685号)中公开了如下的检测装置。即,检测装置检测车载网络中的非法消息,所述检测装置具备:获取部,获取对象分布,所述对象分布是在所述车载网络中发送的周期消息的接收间隔的分布;提取部,按照规定的基准提取由所述获取部所获取的所述对象分布的一部分;以及检测部,基于由所述提取部所提取的所述对象分布的一部分,进行检测所述非法消息的检测处理。

[0004] 现有技术文献

[0005] 专利文献

[0006] 专利文献1:国际公开第2021/111685号

发明内容

[0007] 本公开的检测装置检测网络中的异常,包括以规定的发送周期收发的周期消息的多个对象消息在所述网络中进行收发,所述检测装置具备:计算部,计算所述对象消息的接收间隔;检测部,基于由所述计算部计算出的所述接收间隔,进行检测所述网络中的异常的检测处理;以及计数部,对多个突发消息进行计数,所述多个突发消息包括所述接收间隔比所述发送周期大规定值以上的所述对象消息即延迟消息以及继所述延迟消息之后被接收且所述接收间隔为规定值以下的一个或多个所述对象消息,所述检测部基于所述计数部的计数值,确定是否对所述多个突发消息中的至少任一个所述突发消息进行基于所述接收间隔的所述检测处理。

[0008] 本公开的检测方法是检测网络中的异常的检测装置中的检测方法,包括以规定的发送周期收发的周期消息的多个对象消息在所述网络中进行收发,所述检测方法包括以下步骤:计算所述对象消息的接收间隔;基于计算出的所述接收间隔,进行检测所述网络中的异常的检测处理;以及对多个突发消息进行计数,所述多个突发消息包括所述接收间隔比所述发送周期大规定值以上的所述对象消息即延迟消息以及继所述延迟消息之后被接收且所述接收间隔为规定值以下的一个或多个所述对象消息,在进行所述检测处理的步骤中,基于所述多个突发消息的计数值,确定是否对所述多个突发消息中的至少任一个所述突发消息进行基于所述接收间隔的所述检测处理。

[0009] 本公开的一方面不仅可以作为具备这样的特征性的处理部的检测装置而实现,而且还可以作为用于使计算机执行这样的特征性的处理的步骤的程序而实现,或者还可以作为实现检测装置的一部分或全部的半导体集成电路而实现,或者还可以作为包括检测装置的系统而实现。

附图说明

[0010] 图1是示出本公开的实施方式所涉及的通信系统的结构的图。

[0011] 图2是示出本公开的实施方式所涉及的中继装置的结构的图。

[0012] 图3是示出由本公开的实施方式所涉及的中继装置接收的对象消息及接收时刻的分布的一例的图。

[0013] 图4是示出在本公开的实施方式所涉及的中继装置中用于检测处理的统计值的一例的图。

[0014] 图5是示出由本公开的实施方式所涉及的中继装置接收的对象消息及接收时刻的分布的另一例的图。

[0015] 图6是示出在本公开的实施方式的比较例所涉及的中继装置中用于检测处理的统计值的一例的图。

[0016] 图7是示出由本公开的实施方式所涉及的中继装置接收的对象消息的接收时刻的一例的图。

[0017] 图8是示出由本公开的实施方式所涉及的中继装置接收的对象消息的接收时刻的另一例的图。

[0018] 图9是示出由本公开的实施方式所涉及的中继装置接收的对象消息的接收时刻的一例的图。

[0019] 图10是示出由本公开的实施方式所涉及的中继装置接收的对象消息的接收时刻的另一例的图。

[0020] 图11是示出由本公开的实施方式所涉及的中继装置接收的对象消息的接收时刻的一例的图。

[0021] 图12是示出本公开的实施方式所涉及的中继装置中的存储部所存储的对应表的一例的图。

[0022] 图13是规定本公开的实施方式所涉及的中继装置进行检测处理时的动作过程的一例的流程图。

[0023] 图14是规定本公开的实施方式所涉及的中继装置进行对突发消息进行计数的处理时的动作过程的一例的流程图。

[0024] 图15是示出本公开的实施方式所涉及的网络的连接拓扑的一例的图。

[0025] 图16是示出本公开的实施方式所涉及的中继装置中的存储部所存储的对应表的另一例的图。

具体实施方式

[0026] 以往,已提议一种用于提高网络中的安全性的技术。

[0027] [本公开要解决的技术问题]

[0028] 期望有一种能够超过专利文献1所记载的技术而更正确地检测网络中的异常的技术。

[0029] 本公开是为了解决上述技术问题而完成的,其目的在于提供能够更正确地检测网络中的异常的检测装置及检测方法。

[0030] [本公开的效果]

[0031] 根据本公开,能够更正确地检测网络中的异常。

[0032] [本公开的实施方式的说明]

[0033] 首先,列出本公开的实施方式的内容进行说明。

[0034] (1)本公开的实施方式所涉及的检测装置检测网络中的异常,包括以规定的发送周期收发的周期消息的多个对象消息在所述网络中进行收发,所述检测装置具备:计算部,计算所述对象消息的接收间隔;检测部,基于由所述计算部计算出的所述接收间隔,进行检测所述网络中的异常的检测处理;以及计数部,对多个突发消息进行计数,所述多个突发消息包括所述接收间隔比所述发送周期大规定值以上的所述对象消息即延迟消息以及继所述延迟消息之后被接收且所述接收间隔为规定值以下的一个或多个所述对象消息,所述检测部基于所述计数部的计数值,确定是否对所述多个突发消息中的至少任一个所述突发消息进行基于所述接收间隔的所述检测处理。

[0035] 这样,在基于对象消息的接收间隔进行检测处理的检测装置中,通过基于突发消息的计数值确定是否进行基于突发消息的接收间隔的检测处理的结构,能够根据多个突发消息中包括非法的对象消息的可能性的高低,确定是否将多个突发消息作为检测处理的对象,因此,例如能够在抑制由于发生突发现象而导致的误检测的同时,抑制漏掉多个突发消息中包括的非法消息。因此,能够更正确地检测网络中的异常。

[0036] (2)在上述(1)中,也可以是,在所述计数值为阈值以下的情况下,所述检测部不进行基于所述多个突发消息中的至少任一个所述突发消息的所述接收间隔的所述检测处理。

[0037] 通过这样的结构,能够从检测处理的对象中排除包括非法的对象消息的可能性低的多个突发消息,抑制由于发生突发现象而导致的误检测。

[0038] (3)在上述(1)或(2)中,也可以是,在所述计数值比所述阈值大的情况下,所述检测部基于所述多个突发消息的所述接收间隔进行所述检测处理。

[0039] 通过这样的结构,能够不从检测处理的对象中排除有可能包括非法的对象消息的多个突发消息地基于该多个突发消息的接收间隔进行检测处理,因此能够抑制漏掉非法消息。

[0040] (4)在上述(1)至(3)中的任一项中,也可以是,所述检测部根据作为所述延迟消息的所述对象消息的所述接收间隔来确定所述阈值。

[0041] 通过这样的结构,能够使用根据延迟消息的延迟程度而确定的阈值更适当地判断是否进行基于突发消息的接收间隔的检测处理。

[0042] (5)在上述(1)至(4)中的任一项中,也可以是如下结构:所述检测部计算根据所述接收间隔与关于所述接收间隔的参照信息的关系而增减的检测指标,并基于计算出的所述检测指标进行所述检测处理,在所述计数值为所述阈值以下的情况下,所述检测部不进行针对所述多个突发消息中的至少任一个所述突发消息的所述检测指标的计算。

[0043] 通过这样的结构,能够在抑制由于发生突发现象而导致的误检测的同时,基于表示消息的接收间隔偏离正常值的程度的检测指标,更准确地检测网络中的异常。

[0044] (6)在上述(1)至(5)中的任一项中,也可以是,在从作为所述突发消息的所述对象消息的接收时刻起规定时间以内未接收下一个所述对象消息的情况下,所述计数部结束计数,所述检测部暂停所述检测处理,直到所述计数部的计数结束,并在所述计数部的计数结束后重启所述检测处理。

[0045] 通过这样的结构,能够随着突发现象的结束而结束突发消息的计数,并在更适当的定时重启检测处理。

[0046] (7)本公开的实施方式所涉及的检测方法是检测网络中的异常的检测装置中的检测方法,包括以规定的发送周期收发的周期消息的多个对象消息在所述网络中进行收发,所述检测方法包括以下步骤:计算所述对象消息的接收间隔;基于计算出的所述接收间隔,进行检测所述网络中的异常的检测处理;以及对多个突发消息进行计数,所述多个突发消息包括所述接收间隔比所述发送周期大规定值以上的所述对象消息即延迟消息以及继所述延迟消息之后被接收且所述接收间隔为规定值以下的一个或多个所述对象消息,在进行所述检测处理的步骤中,基于所述多个突发消息的计数值,确定是否对所述多个突发消息中的至少任一个所述突发消息进行基于所述接收间隔的所述检测处理。

[0047] 这样,在基于对象消息的接收间隔进行检测处理的检测装置中,通过基于突发消息的计数值确定是否进行基于突发消息的接收间隔的检测处理的方法,能够根据多个突发消息中包括非法的对象消息的可能性的高低,确定是否将多个突发消息作为检测处理的对象,因此,例如能够在抑制由于发生突发现象而导致的误检测的同时,抑制漏掉多个突发消息中包括的非法消息。因此,能够更正确地检测网络中的异常。

[0048] 以下,使用附图对本公开的实施方式进行说明。需要说明的是,对图中相同或相当的部分标注相同的附图标记并省略其重复的说明。另外,也可以任意组合以下记载的实施方式的至少一部分。

[0049] [结构及基本动作]

[0050] 图1是示出本公开的实施方式所涉及的通信系统的结构的图。参照图1,通信系统301具备中继装置101和多个通信装置111。通信系统301例如搭载于车辆。在这种情况下,通信装置111例如是车载ECU(Electronic Control Unit:电子控制单元)。需要说明的是,通信系统301也可以是具备中继装置101以外的未图示的其他中继装置的结构。

[0051] 中继装置101及通信装置111构成网络201。更详细而言,中继装置101及通信装置111经由传输线10而相互连接。通信系统301可以是中继装置101如图1所示经由线型的传输线10而与通信装置111一对一地连接的结构,也可以是经由未图示的其他中继装置及传输线10而与通信装置111连接的结构,还可以是经由总线型的传输线10而与多个通信装置111一对多地连接的结构。传输线10例如是按照CAN(Controller Area Network:控制器局域网)(注册商标)、FlexRay(注册商标)、MOST(Media Oriented Systems Transport:媒体导向系统传输)(注册商标)、以太网(注册商标)以及LIN(Local Interconnect Network:本地互联网络)等标准的线缆。

[0052] 中继装置101能够与通信装置111进行通信。中继装置101例如进行对在与不同的传输线10连接的多个通信装置111间交换的信息进行中继的中继处理。

[0053] 包括周期性地发送的消息的多个消息在网络201中进行收发。

[0054] 更详细而言,在网络201中,例如,按照规定的约定,从通信装置111经由中继装置101周期性地向其他的通信装置111发送消息。以下,也将在网络201中周期性地发送的消息称为周期消息。需要说明的是,“周期消息”并不限于严格地周期性地发送的消息,而是意指应该周期性地发送的种类的消息。

[0055] 另外,在网络201中,除了周期消息以外,还存在从通信装置111经由中继装置101

不定期地向其他的通信装置111发送的消息。以下,也将在网络201中不定期地发送的消息称为事件消息。

[0056] 通信装置111对消息的发送可以通过广播进行,也可以通过单播进行,还可以通过多播进行。

[0057] 中继装置101作为检测装置发挥功能,检测网络201中的异常。

[0058] 〔中继装置〕

[0059] 图2是示出本公开的实施方式所涉及的中继装置的结构的图。参照图2,中继装置101具备通信处理部11、计算部12、处理部14、存储部15及多个通信端口16。处理部14是计数部的一例、且是检测部的一例。通信处理部11、计算部12及处理部14中的一部分或全部例如通过包括一个或多个处理器的处理电路(Circuitry)来实现。存储部15例如是上述处理电路中包括的闪存。通信端口16例如是连接器或端子。传输线10与各通信端口16连接。

[0060] 通信处理部11进行对在通信装置111间传输的消息进行中继的中继处理。例如,通信处理部11在经由对应的传输线10及对应的通信端口16从通信装置111接收到消息时,生成作为接收到的消息的副本的消息CP,并对所生成的消息CP赋予表示接收到的消息的接收时刻的时间戳。然后,通信处理部11经由对应的通信端口16及对应的传输线10将接收到的消息向其他的通信装置111发送,并向计算部12输出被赋予时间戳的消息CP。

[0061] (接收间隔的计算)

[0062] 计算部12计算成为中继装置101中的检测处理的对象的消息即对象消息的接收间隔。中继装置101可以是将从一个通信装置111发送的一种消息作为对象来进行检测处理的结构,也可以是将从多个通信装置111分别发送的多种消息作为对象而按消息的每个种类进行检测处理的结构。以下,对中继装置101将从某通信装置111发送的消息作为“对象消息M”来进行检测处理的例子进行说明。在网络201中发送的多个对象消息M中,包括按照规定的发送周期Cm从该通信装置111发送的周期消息。

[0063] 更详细而言,计算部12获取由通信处理部11中继的消息中的对象消息M的接收时刻t。

[0064] 例如,存储部15存储有对象消息的每个种类的ID。以下,也将对象消息的ID称为对象ID,也将对象消息M的ID称为对象ID_M。

[0065] 计算部12从通信处理部11接收消息CP,并确认收到的消息CP中包括的ID以及存储部15中的对象ID。

[0066] 然后,计算部12在从通信处理部11收到的消息CP中包括的ID与对象ID_M一致的情况下,识别为作为该消息CP的复制源的消息为对象消息M,并通过参照对该消息CP赋予的时间戳,来获取对象消息M的接收时刻t。

[0067] 计算部12在获取到对象消息M的接收时刻t时,计算该接收时刻t与前一个对象消息M的接收时刻t之差作为对象消息M的接收间隔x。更详细而言,计算部12通过从由通信处理部11接收到的第m个对象消息Mm的接收时刻tm减去由通信处理部11接收到的第(m-1)个对象消息M(m-1)的接收时刻t(m-1),来计算对象消息Mm的接收间隔xm。在此,m是正整数。计算部12将计算出的接收间隔xm及接收时刻tm保存在存储部15中。在存在多个对象消息的情况下,计算部12针对每个对象消息计算接收间隔xm及接收时刻tm,并按每个对象ID将计算出的接收间隔xm及接收时刻tm保存在存储部15中。

[0068] (检测处理)

[0069] 处理部14基于由计算部12计算出的接收间隔x,进行检测网络201中的异常的检测处理。

[0070] 例如,处理部14使用由计算部12计算出的接收间隔x的标准偏差σ来计算接收间隔x的统计值T,并基于计算出的统计值T进行检测处理。统计值T表示接收间隔x偏离正常状态的程度。统计值T是检测指标的一例。

[0071] 更详细而言,在由计算部12将对象消息Mm的接收间隔xm保存在了存储部15中时,处理部14按照以下的式(1)计算对象消息Mm的异常度Dm。

[0072] [数学式1]

[0073] $$Dm=\left(\frac{xm-\mu}{\sigma}\right)^2 \cdots (1)$$

[0074] 在此,μ是接收间隔x的平均值,是关于对象消息M的参照信息的一例。标准偏差σ及平均值μ保存在存储部15中。例如,标准偏差σ预先由通信系统301的制造商基于接收间隔x而计算出,并保存在存储部15中。另外,例如,平均值μ是预先由通信系统301的制造商基于网络201中的对象消息M的发送周期Cm的设计值而计算出的值,并预先保存在存储部15中。需要说明的是,处理部14也可以定期或不定期地基于与多个对象消息M对应的多个接收间隔x来计算标准偏差σ及平均值μ,并将存储部15中的标准偏差σ及平均值μ更新为计算出的标准偏差σ及平均值μ。

[0075] 处理部14在计算出对象消息Mm的异常度Dm时,按照以下的式(2)计算对象消息Mm的统计值Tm。

[0076] [数学式2]

[0077] $Tm=\max\{0,(T(m-1)+Dm-k)\} \cdots (2)$

[0078] 在此,k是限制参数。限制参数k是预先设定的常数。如式(2)所示,对象消息Mm的统计值Tm为从对象消息M(m-1)的统计值T(m-1)与异常度Dm之和减去限制参数k而得到的值以及零中更大一方的值。

[0079] 如式(1)及式(2)所示,统计值Tm根据对象消息Mm的接收间隔xm与平均值μ的关系而增减。具体而言,在因接收间隔xm为大幅背离平均值μ的值而使异常度Dm成为比限制参数k大的值的情况下,对象消息Mm的统计值Tm成为比前一个对象消息M(m-1)的统计值T(m-1)大的值。另一方面,在因接收间隔xm为接近平均值μ的值而使异常度Dm成为比限制参数k小的值的情况下,对象消息Mm的统计值Tm成为零、或者成为比前一个对象消息M(m-1)的统计值T(m-1)小的值。

[0080] 处理部14基于计算出的统计值T,进行检测网络201中的异常的检测处理。例如,处理部14基于计算出的统计值T及规定的阈值Thx,检测网络201中的异常。

[0081] 更详细而言,处理部14对计算出的统计值T与阈值Thx进行比较。在统计值T为阈值Thx以下的情况下,处理部14判定为未发生网络201中的异常。另一方面,在统计值T比阈值Thx大的情况下,处理部14判定为发生网络201中的异常。

[0082] 图3是示出由本公开的实施方式所涉及的中继装置接收的对象消息及接收时刻的分布的一例的图。在图3中,横轴表示时刻。

[0083] 参照图3,由通信处理部11接收的多个对象消息M包括:对象消息M1～M4、M6、M8、

M10、M12,其是在从接收时刻t1到接收时刻t12为止的期间中在基于发送周期Cm的定时接收的合法的周期消息;以及对象消息M5、M7、M9、M11、M13,其是在从接收时刻t5到接收时刻t13为止的期间中例如在基于发送周期Cm的定时接收的非法消息BM。即,在从接收时刻t5到接收时刻t13为止的期间中,合法的周期消息和非法的周期消息交替地来到中继装置101。

[0084] 图4是示出在本公开的实施方式所涉及的中继装置中用于检测处理的统计值的一例的图。在图4中,横轴表示时刻,纵轴表示统计值。图4示出了由计算部12基于图3所示的对象消息M1～M13的接收时刻t1～t13而计算出的统计值T1～T13。

[0085] 参照图4,在从接收时刻t1到接收时刻t4为止的期间中,通过通信处理部11仅接收以一定的发送周期Cm发送的合法的对象消息M1～M4,接收间隔x1～x4成为与平均值μ大致相等的值,因此由处理部14计算出的统计值T1～T4为零。

[0086] 由于计算出的统计值T1～T4为阈值Thx以下,因此处理部14判定为在从接收时刻t1到接收时刻t4为止的期间中未发生网络201中的异常。

[0087] 另一方面,在从接收时刻t5到接收时刻t13为止的期间中,除了以发送周期Cm发送的对象消息M6、M8、M10、M12以外还有非法消息BM被通信处理部11接收,接收间隔x5～x13成为背离平均值μ的值,因此由处理部14计算出的统计值T5～T13逐渐增加。

[0088] 由于计算出的统计值T9超过阈值Thx,因此处理部14判定为在接收时刻t9发生网络201中的异常。处理部14在判定为发生网络201中的异常的情况下,将表示发生网络201中的异常的警报信息经由通信处理部11发送到通信系统301外的上层装置。上层装置例如是接收警报信息并进行规定的处理的服务器等装置。

[0089] 在此,阈值Thx能够由网络201的制造商任意地设定。例如,通过将阈值Thx设定为更小的值,能够在开始网络201中的非法消息的发送之后更早地判定为发生网络201中的异常。

[0090] 图5是示出由本公开的实施方式所涉及的中继装置接收的对象消息及接收时刻的分布的另一例的图。在图5中,横轴表示时刻。图5示出了作为合法的周期消息的对象消息M1～M9的接收时刻的分布。

[0091] 参照图5,对象消息M1、M2以发送周期Cm来到中继装置101,另一方面,由于作为对象消息M的发送源的通信装置111中的处理负荷及网络201中的通信量的增大或集中等的影响,本来应在从对象消息M2的接收时刻t2起经过发送周期Cm后来到中继装置101的对象消息M3有时会延迟。特别是,在中继装置101与多个通信装置111一对多地连接的网络201中,由于作为发送源的通信装置111等待访问权,容易产生来到中继装置101的对象消息M的延迟。另外,在中继装置101经由其他中继装置与通信装置111连接的网络201中,由于该其他中继装置中的拥塞,容易产生来到中继装置101的对象消息M的延迟。如图5所示,在对象消息M3延迟的情况下,例如,继对象消息M3之后的对象消息M4～M7随着对象消息M3的延迟而以非常短的间隔来到中继装置101。以下,也将多个对象消息M以短的间隔来到中继装置101的现象称为突发现象。

[0092] [技术问题]

[0093] 图6是示出在本公开的实施方式的比较例所涉及的中继装置中用于检测处理的统计值的一例的图。在图6中,横轴表示时刻,纵轴表示统计值。图6示出了由计算部12基于图5所示的对象消息M1～M9的接收时刻t1～t9而计算出的统计值T1～T9。

[0094] 参照图6,由于对象消息M3延迟而使接收间隔x3成为比平均值μ大的值,因此计算出的统计值T3增大。另外,由于对象消息M4～M7以非常短的间隔来到中继装置而使接收间隔x4～x7成为比平均值μ小的值,因此计算出的统计值T4～T7逐渐增大。

[0095] 在比较例所涉及的中继装置中,例如统计值T5超过阈值Thx,因此判定为发生网络201中的异常。即,比较例所涉及的中继装置在尽管非法消息未到来、但却由于突发现象而使对象消息M的接收间隔x变短的情况下,判定为发生网络201中的异常。

[0096] 为了抑制这样的误检测,考虑从检测处理的对象中排除在发生突发现象的期间中到来的对象消息M的接收间隔x的方法。然而,在该方法中,在非法消息在发生突发现象的期间中到来的情况下,无法检测出该非法消息。

[0097] 于是,本公开的实施方式所涉及的中继装置101通过如下的结构来解决上述技术问题。

[0098] (延迟消息DEM的检测)

[0099] 处理部14检测延迟消息DEM,该延迟消息DEM是接收间隔x比发送周期Cm大规定值以上的对象消息M。

[0100] 更详细而言,在由计算部12将对象消息M的接收间隔x及接收时刻t保存在了存储部15中时,处理部14通过对该接收间隔x与规定的阈值ThD进行比较,来判定该对象消息M是否是例如上述对象消息M3那样的延迟消息DEM。阈值ThD是用于检测延迟消息DEM的阈值,例如是周期消息的发送周期Cm的2倍。

[0101] 图7是示出由本公开的实施方式所涉及的中继装置接收的对象消息的接收时刻的一例的图。在图7中,横轴表示时刻。

[0102] 参照图7,在对象消息Mm的接收间隔xm小于阈值ThD的情况下,处理部14判定为该对象消息Mm不是延迟消息DEM。在这种情况下,处理部14计算该接收间隔xm的统计值Tm。然后,处理部14对计算出的统计值Tm与阈值Thx进行比较,并基于比较结果,判定是否发生网络201中的异常。

[0103] 图8是示出由本公开的实施方式所涉及的中继装置接收的对象消息的接收时刻的另一例的图。在图8中,横轴表示时刻。

[0104] 参照图8,在对象消息Mm的接收间隔xm为阈值ThD以上的情况下,处理部14判定为该对象消息Mm是延迟消息DEM。在这种情况下,处理部14暂停延迟消息DEM的接收间隔x的统计值T的计算,直到计算时刻tB为止,该计算时刻tB是对延迟消息DEM的接收时刻t加上阈值ThB而得到的时刻。即,处理部14暂停接收间隔xm的统计值Tm的计算,直到计算时刻tBm为止,该计算时刻tBm是对作为延迟消息DEM的对象消息Mm的接收时刻tm加上阈值ThB而得到的时刻。然后,处理部14等待由计算部12将对象消息Mm的下一个对象消息M(m+1)的接收间隔x(m+1)保存在存储部15中。

[0105] 例如,阈值ThB基于存储消息的帧的IFG(InterFrame Gap:帧间距)而预先设定。优选阈值ThB是对与最小的IFG相应的帧的传输时间加上基于帧的发送定时的波动所设定的规定的裕度而得到的值。需要说明的是,阈值ThB也可以是从发送周期Cm减去规定值而得到的值。

[0106] (突发现象的判定)

[0107] 处理部14在检测到延迟消息DEM的情况下,判定是否发生突发现象。

[0108] 更详细而言,处理部14根据在针对延迟消息DEM的计算时刻tB之前是否有新的对象消息M来到中继装置101,来判定是否发生突发现象。需要说明的是,处理部14在计算时刻tB之前有对象消息M以外的新的消息来到中继装置101的情况下,也可以将计算时刻tB更新为对该新的消息的接收时刻加上阈值ThB而得到的时刻。

[0109] 图9是示出由本公开的实施方式所涉及的中继装置接收的对象消息的接收时刻的一例的图。在图9中,横轴表示时刻。图9示出了在图8所示的接收时刻tm以后由通信处理部11接收的对象消息M(m+1)的接收时刻t(m+1)。

[0110] 参照图9,在针对对象消息Mm的计算时刻tBm在由通信处理部11接收作为延迟消息DEM的对象消息Mm的下一个对象消息M(m+1)之前到来的情况下,处理部14判定为未发生突发现象。即,在计算时刻tBm在由计算部12将对象消息M(m+1)的接收间隔x(m+1)及接收时刻t(m+1)保存在存储部15中之前到来的情况下,处理部14判定为未发生突发现象。在这种情况下,处理部14解除上述暂停,并按照上述式(1)及式(2)计算接收间隔xm的统计值Tm。然后,处理部14对计算出的统计值Tm与阈值Thx进行比较,并基于比较结果,判定是否发生网络201中的异常。

[0111] 图10是示出由本公开的实施方式所涉及的中继装置接收的对象消息的接收时刻的另一例的图。在图10中,横轴表示时刻。图10示出了在图8所示的接收时刻tm以后由通信处理部11接收的对象消息M(m+1)的接收时刻t(m+1)。

[0112] 参照图10,在针对对象消息Mm的计算时刻tBm之前由通信处理部11接收到作为延迟消息DEM的对象消息Mm的下一个对象消息M(m+1)的情况下,处理部14判定为在对象消息Mm的接收时刻tm发生突发现象。即,在计算时刻tBm到来之前由计算部12将对象消息M(m+1)的接收间隔x(m+1)及接收时刻t(m+1)保存在了存储部15中的情况下,处理部14判定为在对象消息Mm的接收时刻tm发生突发现象。

[0113] 处理部14在判定为在对象消息Mm的接收时刻tm发生突发现象时,将包括对象消息M(m+1)的接收时刻t(m+1)的突发发生信息输出到计算部12。

[0114] 计算部12在从处理部14收到突发发生信息的情况下,基于对对象消息M的接收时刻t加上阈值ThB而得到的时刻即结束判定时刻tE,判定突发现象是否结束。

[0115] 更详细而言,在收到的突发发生信息所示的接收时刻t(m+1)以后、在针对对象消息M(m+q+1)的结束判定时刻tE(m+q+1)之前由通信处理部11接收到对象消息M(m+q+1)的下一个对象消息M(m+q+2)的情况下,计算部12判定为突发现象在继续。即,在结束判定时刻tE(m+q+1)到来之前由通信处理部11输出了包括表示接收时刻t(m+q+2)的时间戳的消息CP的情况下,计算部12判定为突发现象在继续。在此,q是正整数。

[0116] 另一方面,在收到的突发发生信息所示的接收时刻t(m+1)以后、针对对象消息M(m+q+1)的结束判定时刻tE(m+q+1)在由通信处理部11接收对象消息M(m+q+1)的下一个对象消息M(m+q+2)之前到来的情况下,计算部12判定为突发现象结束。即,在结束判定时刻tE(m+q+1)在由通信处理部11输出包括表示接收时刻t(m+q+2)的时间戳的消息CP之前到来的情况下,计算部12判定为突发现象结束。计算部12在判定为突发现象结束的情况下,将突发结束信息输出到处理部14。

[0117] 需要说明的是,在结束判定时刻tE之前有对象消息M以外的新的消息来到中继装置101的情况下,计算部12也可以将结束判定时刻tE更新为对该新的消息的接收时刻加上

阈值ThB而得到的时刻。即,计算部12也可以是如下结构:在突发发生信息所示的接收时刻t(m+1)以后,每当从通信处理部11收到消息CP时,都与收到的消息CP中包括的ID无关地,基于该消息CP中包括的时间戳更新结束判定时刻tE,并在结束判定时刻tE到来之前通信处理部11未输出下一个消息CP的情况下,判定为突发现象结束。

[0118] (突发消息的计数)

[0119] 处理部14对包括检测到的延迟消息DEM以及继该延迟消息DEM之后被接收且接收间隔x为阈值ThB以下的一个或多个对象消息M的多个突发消息Mbst进行计数。即,处理部14将由通信处理部11连续接收的作为延迟消息DEM的对象消息M以及继该对象消息M之后且接收间隔x为阈值ThB以下的一个或多个对象消息M作为突发消息Mbst进行计数。

[0120] 例如,处理部14对在发生突发现象的期间中由通信处理部11接收到的对象消息M即突发消息Mbst进行计数。

[0121] 更详细而言,处理部14在基于接收间隔x(m+1)与阈值ThB的比较结果判定为在对象消息Mm的接收时刻tm发生突发现象的情况下,判断为对象消息Mm是第一个突发消息Mbst,对象消息M(m+1)是第二个突发消息Mbst,并保持突发消息Mbst的计数值CNT即“2”。

[0122] 图11是示出由本公开的实施方式所涉及的中继装置接收的对象消息的接收时刻的一例的图。在图11中,横轴表示时刻。图11示出了在图10所示的接收时刻tm以后由通信处理部11接收的多个对象消息M的接收时刻t。

[0123] 参照图11,处理部14在判定为发生突发现象之后,每当由计算部12将对象消息M(m+n)的接收间隔x(m+n)及接收时刻t(m+n)保存在存储部15中时,都将计数值CNT递增更新。在此,n是2以上的整数。

[0124] 更详细而言,在由计算部12将对象消息M(m+2)的接收间隔x(m+2)及接收时刻t(m+2)保存在存储部15中,处理部14将计数值CNT更新为“3”。

[0125] 同样地,在由计算部12将对象消息M(m+N)的接收间隔x(m+N)及接收时刻t(m+N)保存在存储部15中时,处理部14将计数值CNT更新为“N+1”。

[0126] 例如,在从作为突发消息Mbst的对象消息M的接收时刻t起规定时间以内未由通信处理部11接收下一个对象消息M的情况下,处理部14结束计数。更详细而言,处理部14在从计算部12收到突发结束信息的情况下,结束突发消息Mbst的计数。

[0127] (突发消息的接收间隔的使用限制)

[0128] 处理部14基于计数值CNT,确定是否进行基于多个突发消息Mbst的接收间隔x的检测处理。

[0129] 例如,在计数值CNT为阈值ThC以下的情况下,处理部14不进行基于多个突发消息Mbst中的至少任一个突发消息Mbst的接收间隔x的检测处理。详细而言,在计数值CNT为阈值ThC以下的情况下,处理部14限制多个突发消息Mbst中的至少任一个突发消息Mbst的接收间隔x在检测处理中的使用。更详细而言,处理部14在结束了突发消息Mbst的计数时,对计数值CNT与阈值ThC进行比较。在计数值CNT为阈值ThC以下的情况下,处理部14将所有突发消息Mbst的接收间隔x废弃而不用于检测处理。

[0130] 例如,处理部14根据作为延迟消息DEM的对象消息M的接收间隔x,确定用于与计数值CNT进行比较的阈值ThC。

[0131] 图12是示出本公开的实施方式所涉及的中继装置中的存储部所存储的对应表的

一例的图。参照图12,存储部15存储有表示延迟消息DEM的接收间隔x与阈值ThC的对应关系的对应表Tb1。例如,在对应表Tb1中,在假设对象消息M在按照发送周期Cm的定时来到中继装置101的情况下,阈值ThC被设定为在从延迟消息DEM的前一个对象消息M的接收时刻t起到该延迟消息DEM的接收时刻t为止的期间中由通信处理部11接收的对象消息M的数量与规定的裕度相加而得到的值。

[0132] 例如,处理部14从存储部15中的对应表Tb1获取与判定为是延迟消息DEM的对象消息Mm的接收间隔xm对应的阈值ThC。作为一例,在判定为是延迟消息DEM的对象消息Mm的接收间隔xm为发送周期Cm的4倍以上且小于发送周期Cm的5倍的情况下,处理部14获取“5”作为阈值ThC。

[0133] 再次参照图11,处理部14对所获取的阈值ThC与计数值CNT进行比较,在计数值CNT为阈值ThC以下的情况下,不将作为突发消息Mbst的对象消息Mm、M(m+1)…、M(m+N)的接收间隔xm、x(m+1)…、x(m+N)用于检测处理而将其废弃。

[0134] 更详细而言,在计数值CNT为阈值ThC以下的情况下,不进行针对突发消息Mbst的统计值T的计算。即,处理部14不进行接收间隔xm、x(m+1)…、x(m+N)的统计值Tm、T(m+1)…、T(m+N)的计算,而从存储部15中删除接收间隔xm、x(m+1)…、x(m+N)。

[0135] 在计数值CNT为阈值ThC以下的情况下,由通信处理部11接收到的多个突发消息Mbst中包括非法消息的可能性低,因此通过不将突发消息Mbst的接收间隔x用于检测处理而将其废弃,能够抑制由于发生突发现象而导致的误检测。

[0136] 例如,处理部14在判定为发生突发现象的情况下,暂停检测处理,直到突发消息Mbst的计数结束,并在突发消息Mbst的计数结束后重启检测处理。

[0137] 更详细而言,在对象消息M(m+N+1)的接收间隔x(m+N+1)比阈值ThB大且小于阈值ThD的情况下,处理部14判定为突发现象在对象消息M(m+N)的接收时刻t(m+N)结束、且该对象消息M(m+N+1)不是延迟消息DEM,并计算接收间隔x(m+N+1)的统计值T(m+N+1)。更详细而言,处理部14使用突发消息Mbst的前一个对象消息M(m-1)的统计值T(m-1)取代接收间隔x(m+N)的统计值T(m+N),来按照上述式(1)计算统计值T(m+N+1)。

[0138] 然后,处理部14对计算出的统计值T(m+N+1)与阈值Thx进行比较,并基于比较结果,判定是否发生网络201中的异常。

[0139] 接着,在由计算部12将对象消息M(m+N+2)的接收间隔x(m+N+2)保存在存储部15中、且接收间隔x(m+N+2)小于阈值ThD的情况下,处理部14判定为该对象消息M(m+N+2)不是延迟消息DEM,并计算接收间隔x(m+N+2)的统计值T(m+N+2)。

[0140] 然后,处理部14对计算出的统计值T(m+N+2)与阈值Thx进行比较,并基于比较结果,判定是否发生网络201中的异常。

[0141] 需要说明的是,处理部14在判定为突发现象在对象消息M(m+N)的接收时刻t(m+N)结束的情况下,也可以不进行接收间隔x(m+N+1)的统计值T(m+N+1)的计算,而从存储部15中删除接收间隔x(m+N+1)。在这种情况下,处理部14等待由计算部12将接收间隔x(m+N+2)保存在存储部15中,并使用突发消息Mbst的前一个对象消息M(m-1)的统计值T(m-1)取代接收间隔x(m+N+1)的统计值T(m+N+1),来按照上述式(1)计算统计值T(m+N+2)。

[0142] (使用突发消息的接收间隔的检测处理)

[0143] 在计数值CNT比阈值ThC大的情况下,处理部14基于突发消息Mbst的接收间隔x进

行检测处理。

[0144] 更详细而言,处理部14对阈值ThC与计数值CNT进行比较,并在计数值CNT比阈值ThC大的情况下,计算作为突发消息Mbst的对象消息Mm、M(m+1)…、M(m+N)的接收间隔xm、x(m+1)…、x(m+N)的统计值Tm、T(m+1)…、T(m+N)。

[0145] 然后,处理部14对计算出的统计值Tm、T(m+1)…、T(m+N)与阈值Thx进行比较,并基于比较结果,判定是否发生网络201中的异常。

[0146] 在计数值CNT比阈值ThC大的情况下,由通信处理部11接收到的多个突发消息Mbst中有可能包括非法消息,因此通过基于突发消息Mbst的接收间隔x像通常那样进行检测处理,能够抑制漏掉非法消息。

[0147] <变形例>

[0148] 虽然处理部14采用了计算接收间隔x的统计值T、并基于计算出的统计值T进行检测处理的结构,但并不限定于此。处理部14也可以是不计算统计值T来进行检测处理的结构。作为一例,处理部14计算由通信处理部11接收到的最近的p个对象消息M的接收间隔x的移动平均值A,并基于计算出的移动平均值A进行检测处理。p是2以上的整数。移动平均值A是检测指标的一例。

[0149] 更详细而言,处理部14在计算出对象消息Mm的接收间隔xm时,计算接收间隔xm、x(m-1)、x(m-2)…、x(m-p+1)的移动平均值Am。在此,接收间隔x(m-1)、x(m-2)…、x(m-p+1)是关于对象消息M的参照信息的一例。以下,也将接收间隔x(m-1)、x(m-2)…、x(m-p+1)称为参照间隔rm。移动平均值Am根据对象消息Mm的接收间隔xm与参照间隔rm的关系而增减。

[0150] 例如,在如图3所示由通信处理部11接收的多个对象消息M包括非法消息BM的情况下,由处理部14计算出的移动平均值A在从接收时刻t5到接收时刻t13为止的期间中逐渐减小。

[0151] 处理部14基于计算出的移动平均值A和规定的阈值Thy,检测网络201中的异常。更详细而言,处理部14对计算出的移动平均值A与阈值Thy进行比较。在移动平均值A为阈值Thy以上的情况下,处理部14判定为未发生网络201中的异常。另一方面,在移动平均值A小于阈值Thy的情况下,处理部14判定为发生网络201中的异常。

[0152] 在突发消息Mbst的计数值CNT为阈值ThC以下的情况下,处理部14不将突发消息Mbst的接收间隔x用于移动平均值A的计算而将其废弃。然后,在突发消息Mbst的下一个接收到的对象消息M的接收间隔x为规定值以上的情况下,处理部14计算除了突发消息Mbst以外的由通信处理部11接收到的最近的p个对象消息M的接收间隔x的移动平均值A,并基于计算出的移动平均值A进行检测处理。

[0153] [动作流程]

[0154] 图13是规定本公开的实施方式所涉及的中继装置进行检测处理时的动作过程的一例的流程图。

[0155] 参照图13,首先,中继装置101等待对象消息M的到来(在步骤S102中为“否”),在接收到对象消息M时(在步骤S102中为“是”),计算接收到的对象消息M的接收间隔x(步骤S104)。

[0156] 接着,在计算出的接收间隔x小于阈值ThD的情况下(在步骤S106中为“是”),中继装置101判定为接收到的对象消息M不是延迟消息DEM,并基于计算出的接收间隔x进行检测

处理。更详细而言,中继装置101计算接收间隔x的统计值T,对计算出的统计值T与阈值Thx进行比较,并基于比较结果,判定是否发生网络201中的异常。中继装置101在检测处理中判定为发生网络201中的异常的情况下,例如将警报信息发送到通信系统301外的上层装置(步骤S108)。

[0157] 接着,中继装置101等待新的对象消息M的到来(在步骤S102中为“否”)。

[0158] 另一方面,在计算出的接收间隔x为阈值ThD以上的情况下(在步骤S106中为“否”),中继装置101判定为接收到的对象消息M是延迟消息DEM,并判定是否发生突发现象。更详细而言,中继装置101等待延迟消息DEM的下一个对象消息M的到来或针对延迟消息DEM的计算时刻tB的到来,在计算时刻tB到来之前接收到延迟消息DEM的下一个对象消息M的情况下,判定为发生突发现象,在计算时刻tB在延迟消息DEM的下一个对象消息M到来之前已到来的情况下,判定为未发生突发现象(步骤S110)。

[0159] 接着,中继装置101在判定为未发生突发现象的情况下(在步骤S112中为“是”),进行检测处理。更详细而言,中继装置101计算延迟消息DEM的接收间隔x的统计值T以及延迟消息DEM的下一个对象消息M的接收间隔x的统计值T,对计算出的各统计值T与阈值Thx进行比较,并基于比较结果,判定是否发生网络201中的异常(步骤S108)。

[0160] 接着,中继装置101等待新的对象消息M的到来(在步骤S102中为“否”)。

[0161] 另一方面,中继装置101在判定为发生突发现象的情况下(在步骤S112中为“否”),对突发消息Mbst进行计数。更详细而言,中继装置101等待新的对象消息M的到来,并对在发生突发现象的期间中接收到的对象消息M即突发消息Mbst进行计数(步骤S114)。

[0162] 接着,在突发消息Mbst的计数值CNT比阈值ThC大的情况下(在步骤S116中为“是”),中继装置101基于突发消息Mbst的接收间隔x进行检测处理。更详细而言,中继装置101分别计算多个突发消息Mbst的接收间隔x的统计值T,对计算出的各统计值T与阈值Thx进行比较,并基于比较结果,判定是否发生网络201中的异常(步骤S108)。

[0163] 接着,中继装置101等待新的对象消息M的到来(在步骤S102中为“否”)。

[0164] 另一方面,在突发消息Mbst的计数值CNT为阈值ThC以下的情况下(在步骤S116中为“否”),中继装置101将突发消息Mbst的接收间隔x废弃(步骤S118)。

[0165] 接着,中继装置101等待新的对象消息M的到来(在步骤S102中为“否”)。

[0166] 图14是规定本公开的实施方式所涉及的中继装置进行对突发消息进行计数的处理时的动作过程的一例的流程图。图14示出了图13中的步骤S114的详情。

[0167] 参照图14,首先,中继装置101等待从突发消息Mbst的接收时刻t起经过阈值ThB以及接收新的对象消息M(在步骤S302中为“否”且在步骤S304中为“否”),在从突发消息Mbst的接收时刻t起经过阈值ThB之前接收到新的对象消息M的情况下(在步骤S302中为“否”且在步骤S304中为“是”),判断为接收到的对象消息M是突发消息Mbst,并将计数值CNT递增更新(步骤S306)。

[0168] 另一方面,在接收新的对象消息M之前从突发消息Mbst的接收时刻t起经过了阈值ThB的情况下(在步骤S302中为“是”且在步骤S304中为“否”),中继装置101判定为突发现象结束,并结束突发消息Mbst的计数(步骤S308)。

[0169] 需要说明的是,在本公开的实施方式所涉及的通信系统301中,采用了由中继装置101检测网络201中的异常的结构,但并不限定于此。在通信系统301中,也可以是中继装置

101以外的装置作为检测装置发挥功能而检测网络201中的异常的结构。例如,通信系统301具备经由传输线10与中继装置101连接的检测装置。中继装置101在从通信装置111接收到消息时,将作为接收到的消息的副本的镜像消息经由传输线10发送到该检测装置。该检测装置基于从中继装置101接收到的镜像消息在中继装置101中的接收时刻,进行接收间隔x的计算及检测处理。

[0170] 另外,在本公开的实施方式所涉及的通信系统301中,采用了作为检测装置发挥功能的中继装置101与传输线10直接连接的结构,但并不限定于此。

[0171] 图15是示出本公开的实施方式所涉及的网络的连接拓扑的一例的图。参照图15,也可以是检测装置151经由通信装置111与传输线10连接的结构。在这种情况下,检测装置151例如通过监视该通信装置111接收的消息来检测网络201中的异常。更详细而言,该通信装置111将接收到的消息输出到检测装置151。检测装置151具备计算部12、处理部14及存储部15。检测装置151中的计算部12获取由通信装置111接收到的对象消息M的接收时刻t,并基于所获取的接收时刻t计算接收间隔x。

[0172] 另外,在本公开的实施方式所涉及的中继装置101中,存储部15采用了存储有对应表Tb1的结构,但并不限定于此。

[0173] 图16是示出本公开的实施方式所涉及的中继装置中的存储部所存储的对应表的另一例的图。参照图16,存储部15也可以是存储有表示延迟消息DEM的接收间隔x与阈值ThC的对应关系的对应表Tb2来取代对应表Tb1的结构、或者是除了对应表Tb1以外还存储有表示延迟消息DEM的接收间隔x与阈值ThC的对应关系的对应表Tb2的结构。例如,在对应表Tb2中,在假设对象消息M在按照发送周期Cm的定时来到中继装置101的情况下,阈值ThC被设定为在从延迟消息DEM的前一个对象消息M的接收时刻t起到该延迟消息DEM的接收时刻t为止的期间中由通信处理部11接收的对象消息M的数量、基于该期间中的事件的发生频率推测由通信处理部11接收的事件消息的数量以及规定的裕度相加而得到的值。

[0174] 存储部15也可以是未存储有对应表Tb1、Tb2的结构。在这种情况下,例如,处理部14使用规定的计算式计算基于判定为是延迟消息DEM的对象消息M的接收间隔x及发送周期Cm的阈值ThC。

[0175] 另外,在本公开的实施方式所涉及的中继装置101中,处理部14采用了在计数值CNT为阈值ThC以下的情况下、将所有突发消息Mbst的接收间隔x废弃而不用于检测处理的结构,但并不限定于此。处理部14也可以是废弃一部分突发消息Mbst的接收间隔x、而将另一部分突发消息Mbst的接收间隔x用于检测处理的结构。例如,处理部14将多个突发消息Mbst中的延迟消息DEM的接收间隔x用于检测处理、而废弃除了延迟消息DEM以外的一个或多个突发消息Mbst的接收间隔x。

[0176] 另外,在本公开的实施方式所涉及的中继装置101中,处理部14采用了在计数值CNT比阈值ThC大的情况下、基于突发消息Mbst的接收间隔x进行检测处理的结构,但并不限定于此。处理部14也可以是在计数值CNT比阈值ThC大的情况下、不进行基于突发消息Mbst的接收间隔x的检测处理的结构。例如,在计数值CNT比阈值ThC大的情况下,处理部14不进行检测处理,而判定为发生网络201中的异常。

[0177] 另外,在本公开的实施方式所涉及的中继装置101中,处理部14采用了根据作为延迟消息DEM的对象消息M的接收间隔x来确定用于与计数值CNT进行比较的阈值ThC的结构,

但并不限定于此。处理部14也可以是与作为延迟消息DEM的对象消息M的接收间隔x无关地将预定的阈值ThC用于与计数值CNT的比较的结构。

[0178] 另外,在本公开的实施方式所涉及的中继装置101中,处理部14采用了在判定为发生突发现象的情况下暂停检测处理直到突发消息Mbst的计数结束、并在突发消息Mbst的计数结束后重启检测处理的结构,但并不限定于此。处理部14也可以基于由计算部12累积在存储部15中的规定数量的接收间隔x事后进行检测处理。处理部14也可以是在事后进行检测处理的情况下不进行检测处理的暂停及重启的结构。更详细而言,处理部14基于计数值CNT与阈值ThC的比较结果,废弃作为累积在存储部15中的接收间隔x的一部分的突发消息Mbst的接收间隔x,并基于剩余的接收间隔x进行检测处理。

[0179] 另外,在本公开的实施方式所涉及的中继装置101中,处理部14采用了从计算部12接收突发结束信息并结束突发消息Mbst的计数的结构,但并不限定于此。处理部14也可以是基于接收间隔x与阈值ThB的比较结果判定突发现象的结束并结束计数的结构。更详细而言,在对象消息M(m+N+1)的接收间隔x(m+N+1)比阈值ThB大的情况下,处理部14判定为突发现象在对象消息M(m+N)的接收时刻t(m+N)结束,并结束突发消息DM的计数。

[0180] 顺便提及,期望有一种能够更正确地检测网络中的异常的技术。

[0181] 与此相对地,在本公开的实施方式所涉及的中继装置101中,计算部12计算对象消息M的接收间隔x。处理部14基于由计算部12计算出的接收间隔x,进行检测网络201中的异常的检测处理。处理部14对多个突发消息Mbst进行计数,该多个突发消息Mbst包括延迟消息DEM以及继延迟消息DEM之后被接收且接收间隔x为规定值以下的一个或多个对象消息M,该延迟消息DEM是接收间隔x比发送周期Cm大规定值以上的对象消息M。处理部14基于突发消息Mbst的计数值CNT,确定是否对多个突发消息Mbst中的至少任一个突发消息Mbst进行基于接收间隔x的检测处理。

[0182] 这样,在基于对象消息M的接收间隔x进行检测处理的中继装置101中,通过基于突发消息Mbst的计数值CNT来限制突发消息Mbst的接收间隔x在检测处理中的使用的结构,例如能够从检测处理的对象中排除包括非法的对象消息M的可能性低的多个突发消息Mbst,抑制由于发生突发现象而导致的误检测。因此,能够更正确地检测网络201中的异常。

[0183] 应该被认为的是,上述实施方式在所有方面都是例示性的,而非限制性的。本发明的范围并非由上面的说明而是由权利要求示出,旨在包括与权利要求等同的含义和范围内的所有变更。

[0184] 上述实施方式的各处理(各功能)通过包括一个或多个处理器的处理电路(Circuitry)实现。上述处理电路也可以由除了上述一个或多个处理器之外还组合有一个或多个存储器、各种模拟电路、各种数字电路的集成电路等构成。上述一个或多个存储器存储使上述一个或多个处理器执行上述各处理的程序(命令)。上述一个或多个处理器可以按照从上述一个或多个存储器中读出的上述程序执行上述各处理,也可以按照预先设计为执行上述各处理的逻辑电路执行上述各处理。上述处理器可以是CPU(Central Processing Unit:中央处理单元)、GPU(Graphics Processing Unit:图形处理单元)、DSP(Digital Signal Processor:数字信号处理器)、FPGA(Field Programmable Gate Array:现场可编程门阵列)以及ASIC(Application Specific Integrated Circuit:专用集成电路)等适合于计算机的控制的各种处理器。需要说明的是,物理上分离的上述多个处理器也可以相互

协作来执行上述各处理。例如,分别搭载于物理上分离的多个计算机的上述处理器也可以经由LAN(Local Area Network:局域网)、WAN(Wide Area Network:广域网)及因特网等网络相互协作地执行上述各处理。上述程序可以经由上述网络从外部的服务器装置等安装于上述存储器,也可以以存储在CD-ROM(Compact Disc Read Only Memory:光盘只读存储器)、DVD-ROM(Digital Versatile Disk Read Only Memory:数字通用光盘只读存储器)及半导体存储器等记录介质中的状态流通,并从上述记录介质安装于上述存储器。

[0185] 以上的说明包括以下附记的特征。

[0186] [附记1]

[0187] 一种检测装置,检测网络中的异常,包括以规定的发送周期收发的周期消息的多个对象消息在所述网络中进行收发,所述检测装置具备:

[0188] 计算部,计算所述对象消息的接收间隔;

[0189] 检测部,基于由所述计算部计算出的所述接收间隔,进行检测所述网络中的异常的检测处理;以及

[0190] 计数部,检测延迟消息,并对包括所述延迟消息以及继所述延迟消息之后被接收且所述接收间隔为规定值以下的一个或多个所述对象消息的多个突发消息进行计数,所述延迟消息是所述接收间隔比所述发送周期大规定值以上的所述对象消息,

[0191] 所述检测部基于所述计数部的计数值,确定是否对所述多个突发消息中的至少任一个所述突发消息进行基于所述接收间隔的所述检测处理,

[0192] 在所述计数部的计数值为阈值以下的情况下,所述检测部废弃所述多个突发消息的所述接收间隔,在所述计数值比所述阈值大的情况下,所述检测部基于所述多个突发消息的所述接收间隔进行所述检测处理。

[0193] [附记2]

[0194] 一种检测装置,检测网络中的异常,包括以规定的发送周期收发的周期消息的多个对象消息在所述网络中进行收发,

[0195] 所述检测装置具备处理电路,

[0196] 所述处理电路

[0197] 计算所述对象消息的接收间隔;

[0198] 基于计算出的所述接收间隔,进行检测所述网络中的异常的检测处理;

[0199] 检测所述接收间隔比所述发送周期大规定值以上的所述对象消息即延迟消息,并对包括所述延迟消息以及继所述延迟消息之后被接收且所述接收间隔为规定值以下的一个或多个所述对象消息的多个突发消息进行计数;以及

[0200] 基于所述计数值,确定是否对所述多个突发消息中的至少任一个所述突发消息进行基于所述接收间隔的所述检测处理。

[0201] 附图标记说明

[0202] 10传输线;11通信处理部;12计算部;14处理部(计数部、检测部);15存储部;16通信端口;101中继装置;111通信装置;151检测装置;201网络;301通信系统;Tb1、Tb2对应表。

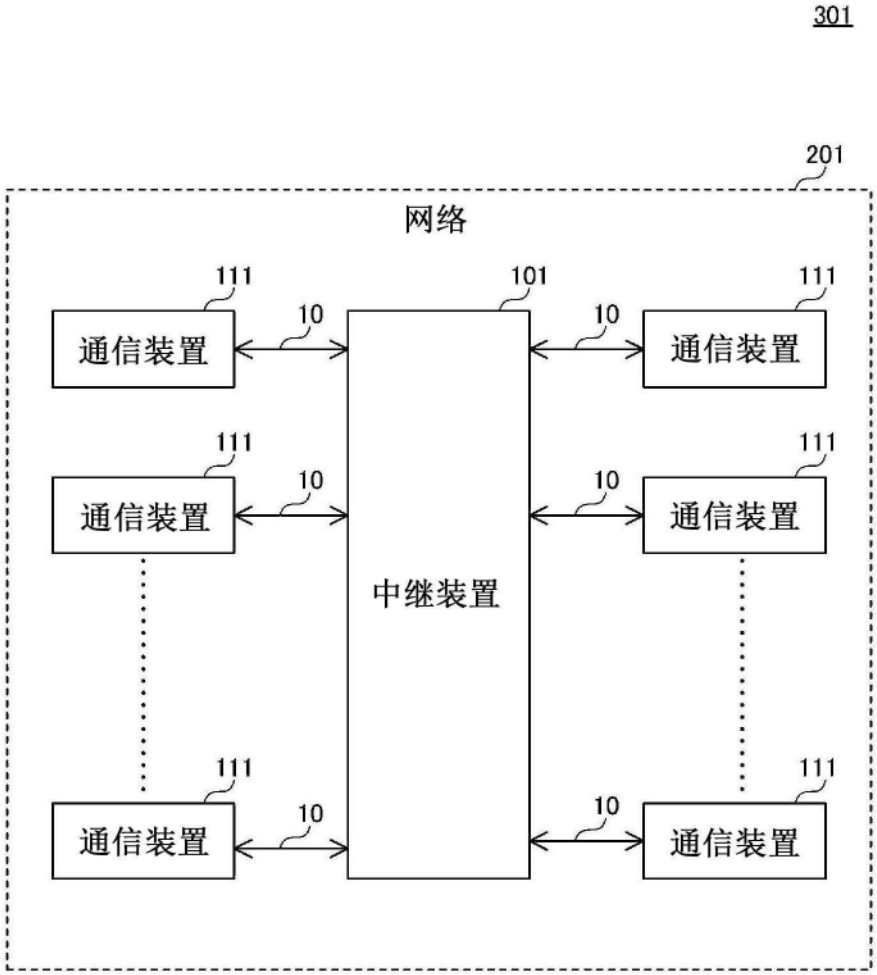

301
201
网络
111
101
111
10
10
通信装置
通信装置
111
111
10
10
通信装置
通信装置
中继装置
111
111
10
10
通信装置
通信装置

图1

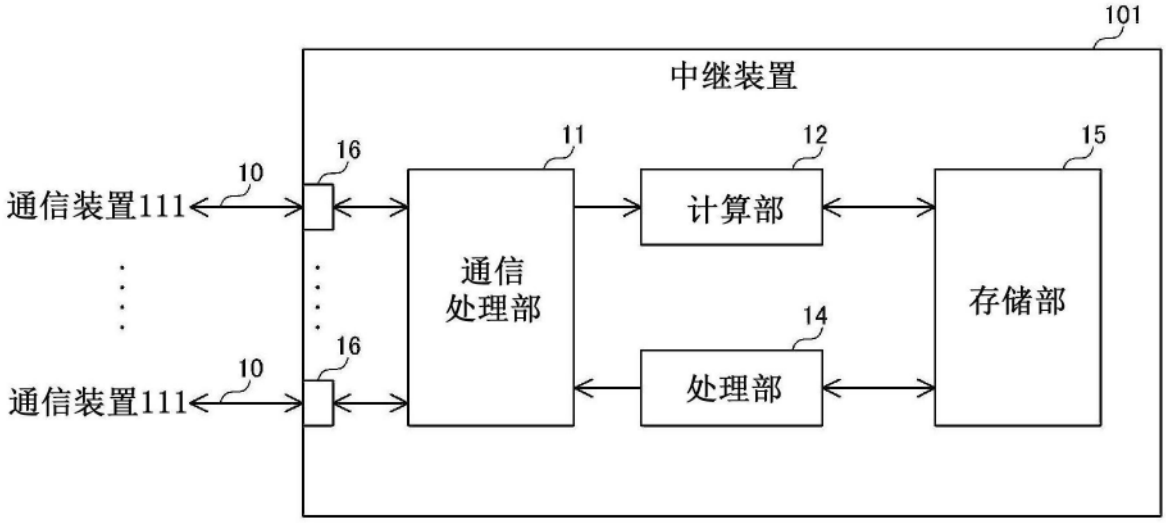

101
中继装置
16
11
12
15
10
通信装置111
通信
处理部
计算部
存储部
14
16
10
通信装置111
处理部

图2

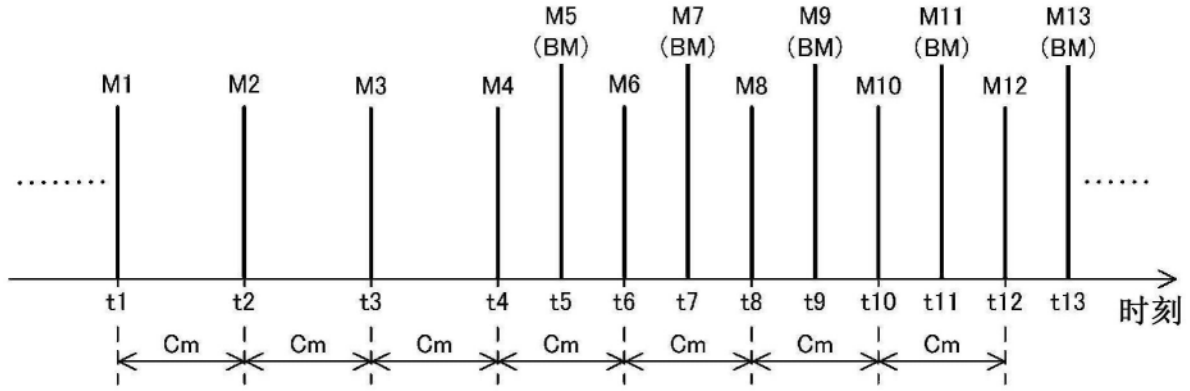

M1
M2
M3
M4
M5 (BM)
M6
M7 (BM)
M8
M9 (BM)
M10
M11 (BM)
M12
M13 (BM)
t1
t2
t3
t4
t5
t6
t7
t8
t9
t10
t11
t12
t13
时刻
Cm

图3

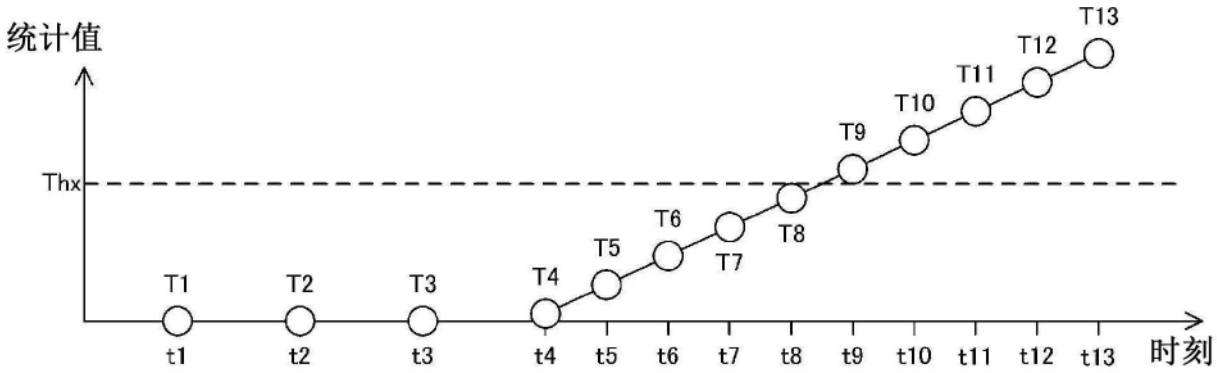

统计值
Thx
T1
T2
T3
T4
T5
T6
T7
T8
T9
T10
T11
T12
T13
时刻

图4

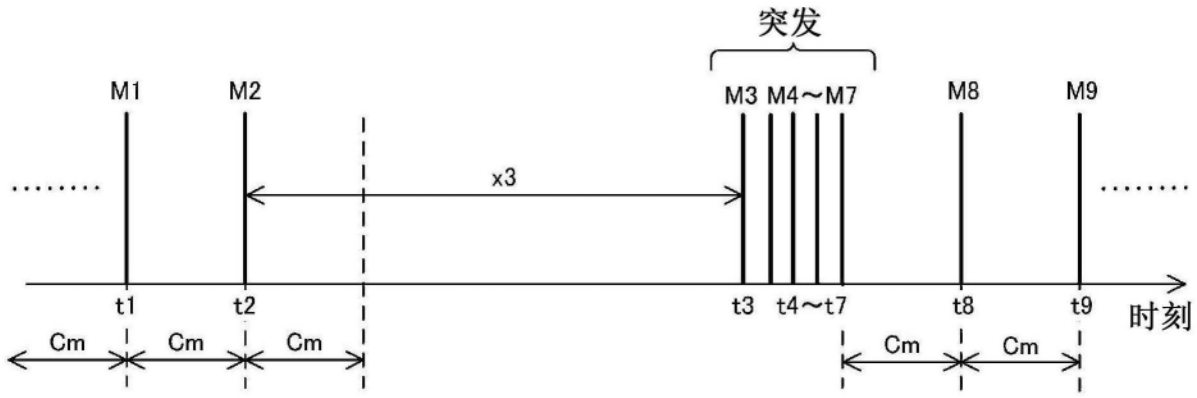

突发
M1
M2
M3 M4～M7
M8
M9
x3
t1
t2
t3
t4～t7
t8
t9
时刻
Cm

图5

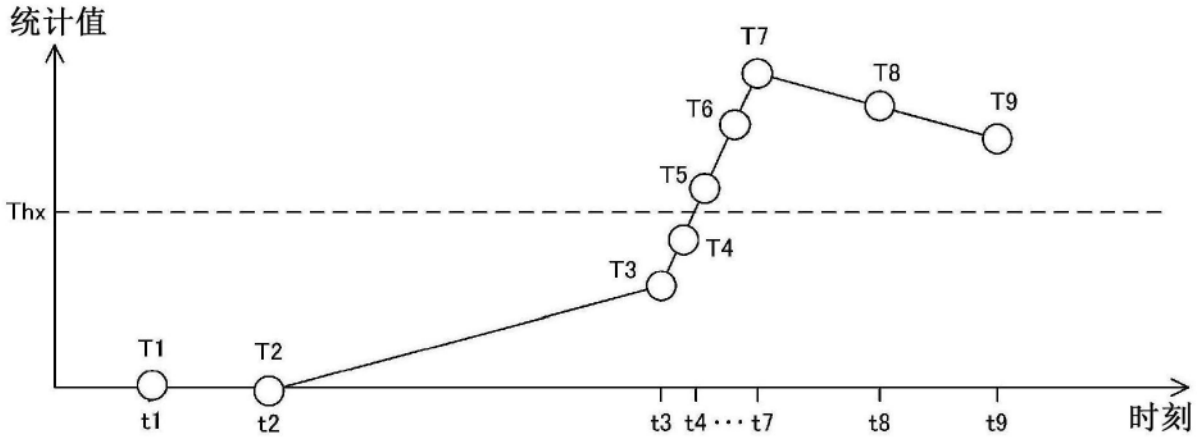

统计值
T7
T8
T9
T6
T5
Thx
T4
T3
T1
T2
t1
t2
t3 t4 ··· t7
t8
t9
时刻

图6

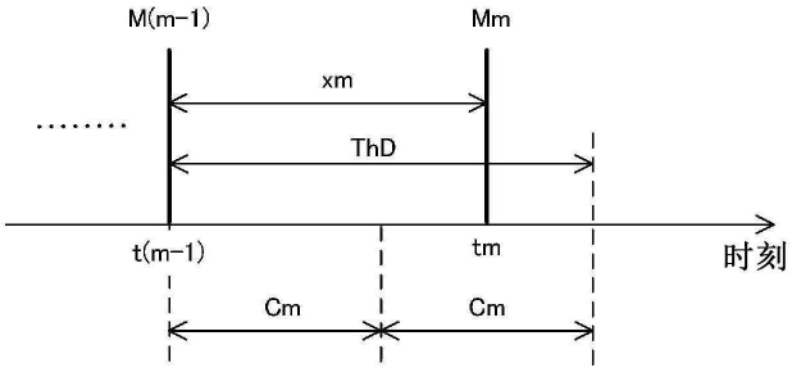

M(m-1)
Mm
xm
ThD
t(m-1)
tm
时刻
Cm
Cm

图7

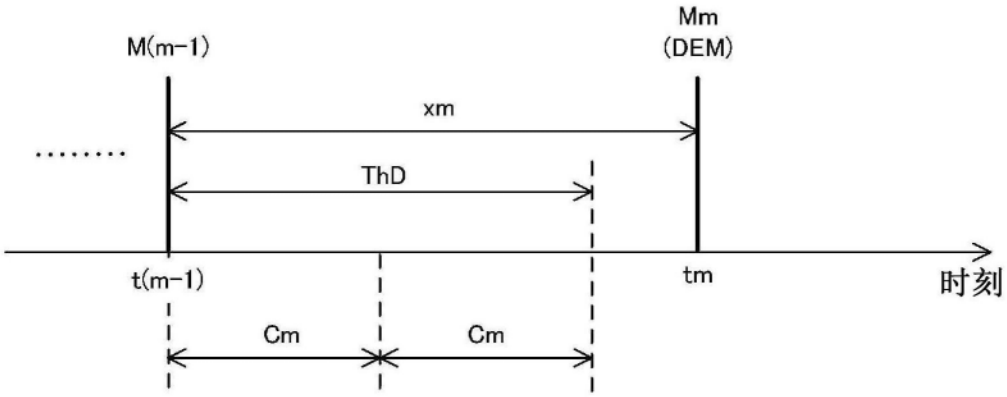

Mm
(DEM)
M(m-1)
xm
ThD
t(m-1)
tm
时刻
Cm
Cm

图8

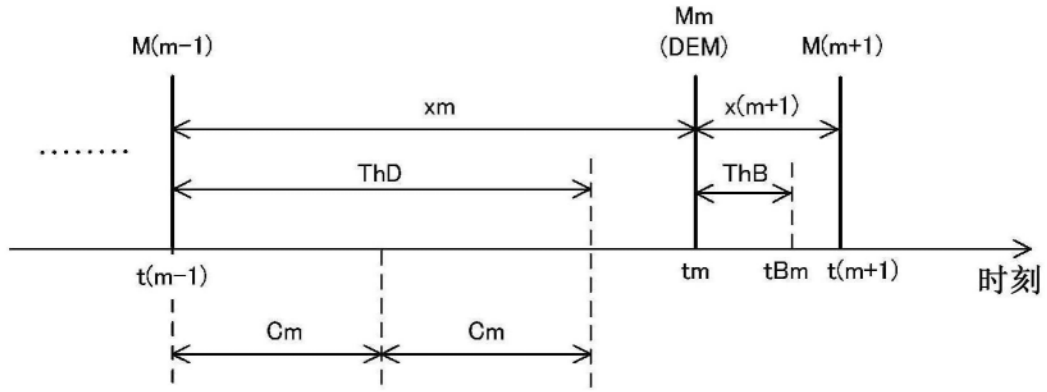

M(m-1)
Mm
(DEM)
M(m+1)
xm
x(m+1)
ThD
ThB
t(m-1)
tm
tBm
t(m+1)
时刻
Cm
Cm

图9

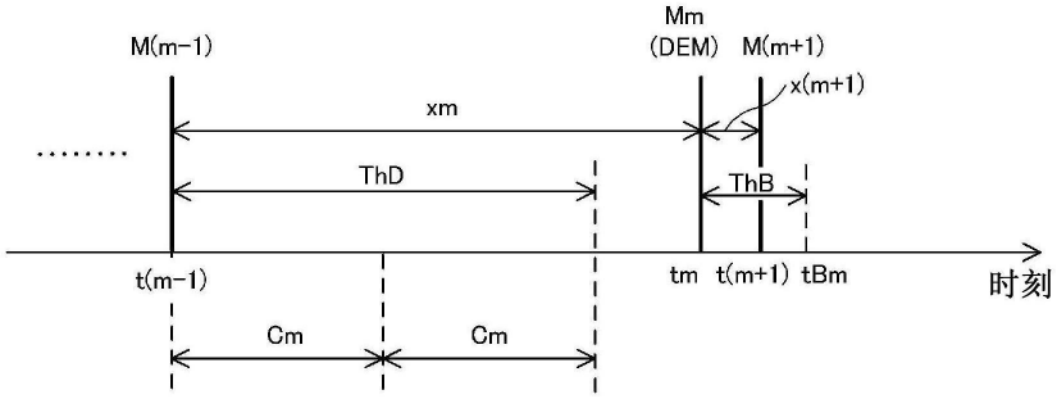

M(m-1)
Mm
(DEM)
M(m+1)
x(m+1)
xm
ThD
ThB
t(m-1)
tm
t(m+1)
tBm
时刻
Cm
Cm

图10

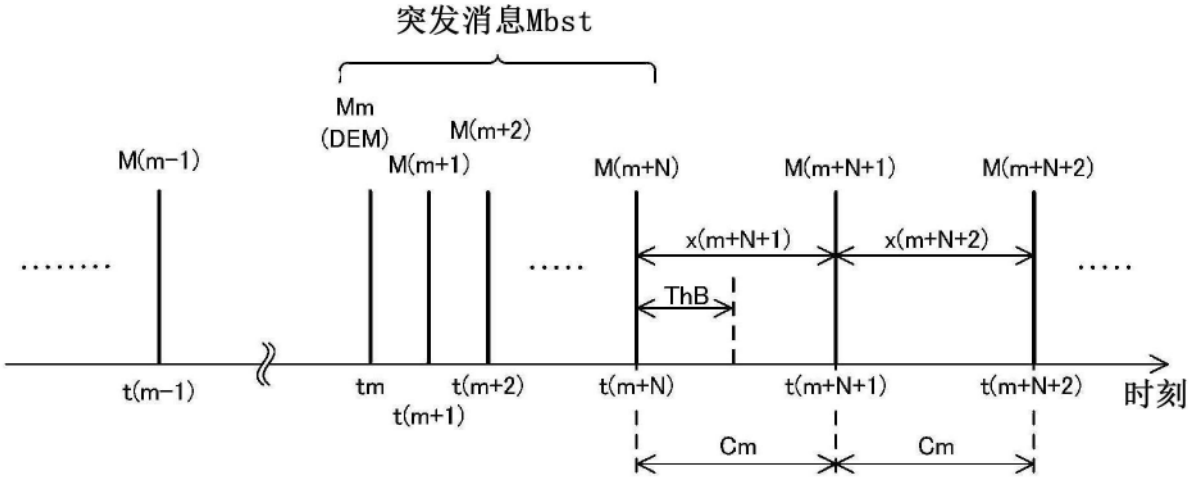

突发消息Mbst
Mm
(DEM)
M(m+2)
M(m-1)
M(m+1)
M(m+N)
M(m+N+1)
M(m+N+2)
x(m+N+1)
x(m+N+2)
ThB
t(m-1)
tm
t(m+2)
t(m+1)
t(m+N)
t(m+N+1)
t(m+N+2)
时刻
Cm
Cm

图11

Tb1

延迟消息DEM的接收间隔x	阈值ThC
2×Cm≤x<3×Cm	3
3×Cm≤x<4×Cm	4
4×Cm≤x<5×Cm	5
⋮	⋮

图12

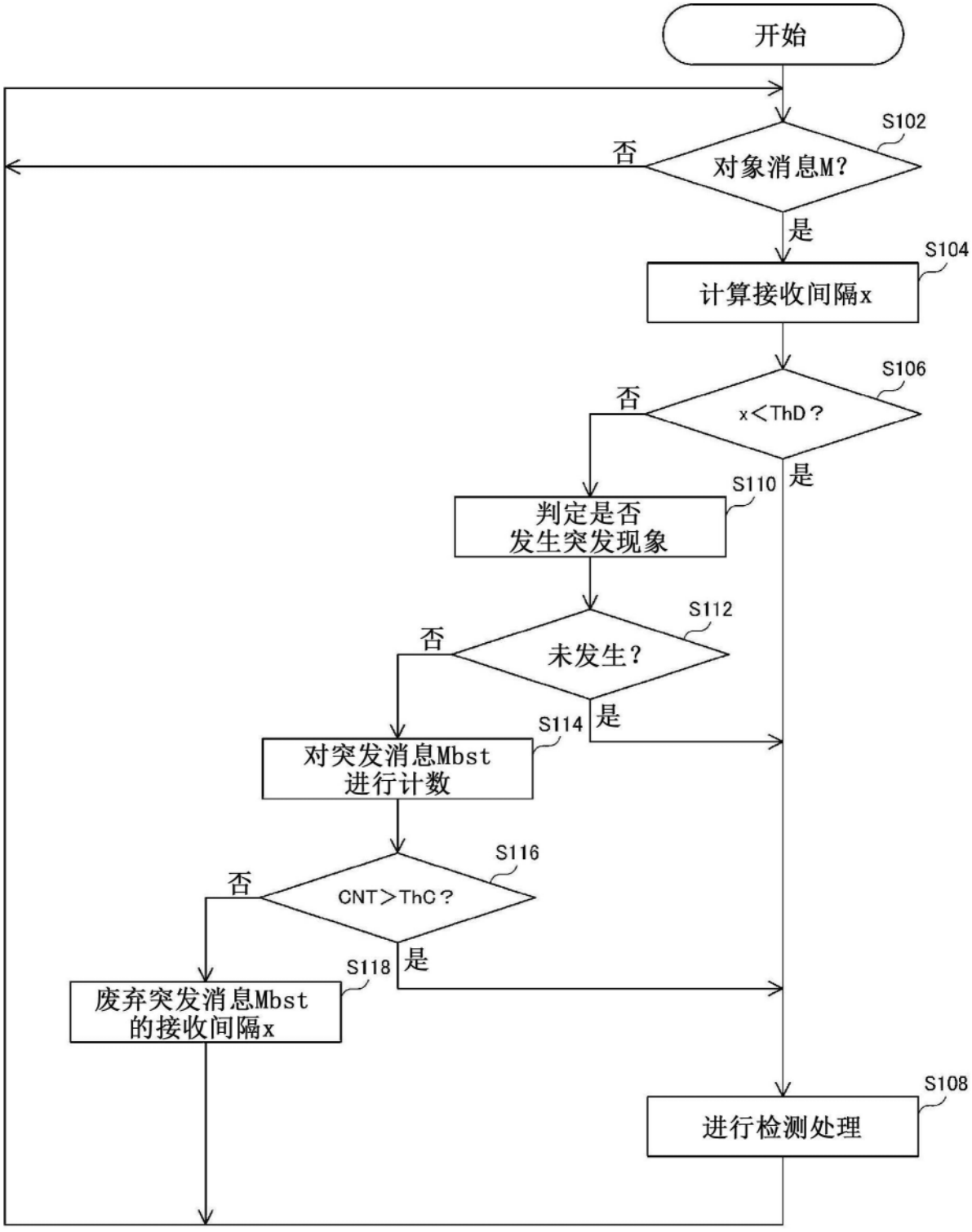

开始
S102
对象消息M?
否
是
S104
计算接收间隔x
S106
x＜ThD？
否
是
S110
判定是否
发生突发现象
S112
未发生？
否
是
S114
对突发消息Mbst
进行计数
S116
CNT＞ThC？
否
是
S118
废弃突发消息Mbst
的接收间隔x
S108
进行检测处理

图13

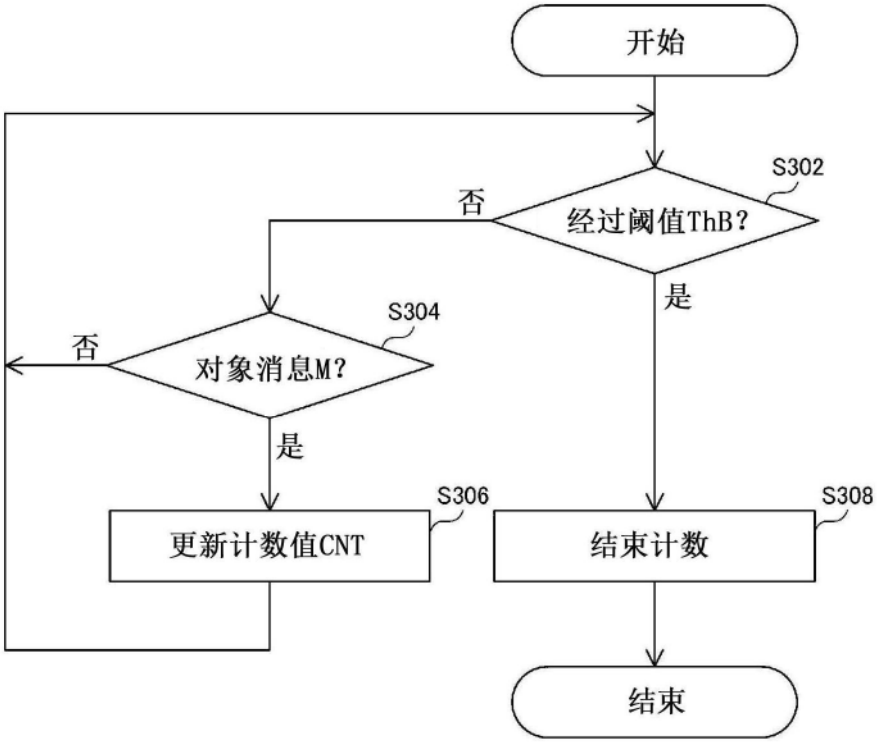


图14

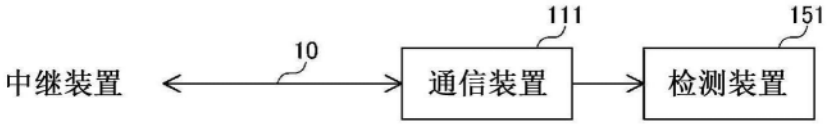


图15

Tb2

延迟消息DEM的接收间隔x	阈值ThC
2×Cm≤x<3×Cm	3
3×Cm≤x<4×Cm	5
4×Cm≤x<5×Cm	6
⋮	⋮

图16