(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 109863732 B
(45)授权公告日 2022.02.25

(21)申请号 201780066155.7
(22)申请日 2017.11.17
(65)同一申请的已公布的文献号
申请公布号 CN 109863732 A
(43)申请公布日 2019.06.07
(30)优先权数据
102016222740.8 2016.11.18 DE
(85)PCT国际申请进入国家阶段日
2019.04.25
(86)PCT国际申请的申请数据
PCT/EP2017/079584 2017.11.17
(87)PCT国际申请的公布数据
WO2018/099736 DE 2018.06.07
(73)专利权人 大陆汽车有限公司
地址 德国汉诺威瓦伦沃德街9号
(72)发明人 H·青纳
(74)专利代理机构 上海华诚知识产权代理有限公司 31300
代理人 汤国华
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/10(2022.01)
H04L 67/12(2022.01)
(56)对比文件
EP 2892199 A1,2015.07.08
EP 2892199 A1,2015.07.08
JP 2000330897 A,2000.11.30
JP 2014520441 A,2014.08.21
US 2015089236 A1,2015.03.26
CN 104908781 A,2015.09.16
CN 1666477 A,2005.09.07
CN 101300807 A,2008.11.05
CN 103139184 A,2013.06.05
审查员 张宁

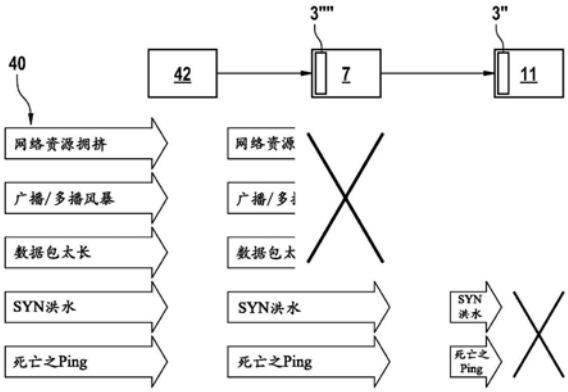
权利要求书1页 说明书8页 附图7页

(54)发明名称

用于通信网络的方法、和电子监测单元

(57)摘要

本发明涉及一种用于机动车辆中通信网络(1)的方法,其中,该通信网络(1)中的通信涉及执行数据传输并且该通信网络(1)提供用于至少两个通信用户(5,5”,7,9,11)。并且,本发明涉及用于机动车辆控制装置的电子监测单元。



CN 109863732 B

1.一种用于机动车辆中通信网络的方法,其中,该通信网络中的通信涉及进行数据传输并且该通信网络提供用于至少两个通信用户,所述通信用户被组合以产生通信路径,通信发生在与通信用户相关的所述通信路径中,其特征在于,

该方法包括以下方法步骤:

-将抵抗该通信网络上的攻击的安全措施的性能的至少一部分分配到多个通信用户上,

-查明每个通信用户的最大可能安全辅助,其中,

基于所述通信用户的最大可能安全辅助来分配所述安全措施的性能,

其中,安全辅助与所述通信用户为执行安全措施的辅助相关。

2.如权利要求1所述的方法,其特征在于,该方法包括以下进一步的方法步骤:

-查明这些通信用户的最大可能搜索深度,其中,

该最大可能搜索深度用于查明这些通信用户的最大可能安全辅助。

3.如权利要求1或2所述的方法,其特征在于,所提供的这些安全措施是过滤规则。

4.如权利要求2所述的方法,其特征在于,该通信是借助于具有多层的数据传输协议进行的,其中,对于最大可能搜索深度,查明了可由各通信用户分析的最大层和/或可由各通信用户分析的每个层的最大字节深度。

5.如权利要求1或2所述的方法,其特征在于,所提供的该通信用户是至少一个控制装置和/或至少一个交换机。

6.如权利要求1或2所述的方法,其中,该通信网络具有用于抵御该通信网络上的攻击的至少一个防火墙,其特征在于,该方法具有以下进一步的步骤:

-使得该防火墙的配置与这些安全措施的分配相匹配。

7.如权利要求1或2所述的方法,其特征在于,该方法在生产结束时、在软件更新之后、在发现安全缺陷之后或当替换或更新通信用户时执行一次。

8.一种用于机动车辆控制装置的电子监测单元,其特征在于,该机动车辆控制装置被设计成用于执行如权利要求1至7之一所述的方法。

用于通信网络的方法、和电子监测单元

[0001] 本发明涉及一种用于根据权利要求1的前序部分所述的通信网络的方法、并且涉及一种电子监测单元。

[0002] 基于以太网物理层以及在其上面的互联网协议(IP)，正在寻找信息技术系统的范围内已经广泛使用的技术进入到车辆的通信网络中的方式。尤其鉴于以太网和互联网协议越来越多的使用，需要另外的安全机制以便能够防止外部访问。由于越来越多的使用无线电技术以及相关联的开放和标准化协议，因此，基本上第一次可以在汽车行业通过远程访问车辆的通信网络。例如，已知的是在攻击者设法经由无线电获得访问车辆的权利并且因此影响重要的车辆功能期间访问车辆。其他工业领域具有不能应用至汽车的问题和解决方案，因为，例如在工作站级计算机的情况下，防火墙已经用已经存在在系统中的数据运行，而不是如车辆所需的实时数据。另外，工作站级计算机的安全软件可以用比汽车中的软件明显更容易的方式更新。

[0003] 根据现有技术的通信数据包通常包括传输装置的协议栈的上位层的报头。接收装置的协议栈将在接收此通信数据包时逐渐发展并且将借助于预先定义的过滤器来检验该通信数据包，以例如将传输数据运传送至相应的软件应用。通信数据包(例如以太网消息)通过例如控制装置中的TCP/IP栈运行并且基于对内容的分析而被传送至相应的应用。

[0004] 协议栈的复杂度随着所使用协议的数量而相当程度地增加。例如，用于传输和复现音频和视频数据的音频/视频桥接(AVB)包括四个子协议，并且时间敏感网络(TSN)甚至包括11个子协议和综合规范。这存在的缺点在于，因为由于所使用协议的多样性而存在非常大数量的不能简单表示的分支可能性，因此对于确定性协议栈不存在简单的可追踪性。因此，确定协议栈中存在的安全缺陷有相当大的问题。问题是，例如，如果有意或无意地使用了新的以太网类型那么该如何进行，这在有所怀疑的情况下将被送至中央计算单元，这可能导致严峻的系统状态、并且可能显著限制底层系统的功能并且可能危及道路使用者的安全。这样的故意的未经授权的访问可能使用先前未曾发现的安全缺陷，通过有意地在协议栈中寻找安全缺陷的阻断服务攻击(DoS)而发生。

[0005] 根据OSI模型，数据包可以具有七层。在这种情况下，该数据包由有用的数据和用于这些层中的每一层的报头构成。这些报头中的每个报头存储相关层的处理信息。这些层因此各自包含有用的数据、它们自身的报头以及下方层的报头。在这种情况下，这些层依赖于下方层的正确处理并且利用其工作。第三层形成例如所谓的“IP层”，其包含发送方和接收方的IP地址。

[0006] 通信网络上的攻击可以具有非常多样的形式。在这种情况下攻击可以攻击各个层并且利用在那里所获得的对信息进行访问。通过举例的方式，首先，第二层上所谓的“嗅探”可以查明用户的IP地址，并且然后所谓的“欺骗”可以改变服务用户的MAC表，使得不再正确传输服务提供方的请求。这然后导致所谓的“阻断服务攻击”(DoS)，这限制了服务和/或资源的可用性。为此根本不必攻击较高的层。

[0007] 然而，为了及时地检测所有的攻击，应当不仅搜索较低的层的报头还应该搜索较高的层的报头以及有用的数据，以搜索可能的错误或改变。而且，层的深度分析是有用的。

在各层上进行的分析越深，需要搜索的层的字节就越多并且可能发现的错误或潜在攻击越多。有待分析的最大可能层和层的最大可搜索字节的组合可以被称为“搜索深度”。以整个数据进行数据搜索(层五至层七的报头以及有用的数据和/或在层内的深度查看)被称为“深度数据包检查”。然而，通过分析检验的层越高，并且查看各层的内部越深，硬件和软件就需要越强大。相应地，深度分析和较高的层中的分析也变得更昂贵。

[0008] 防火墙可以分析例如所有的层并且因此尽可能全面的检测攻击。然而，随着以太网和100Mbit/s、或者将来甚至是1000Mbit/s或最高达10Gbit/s的速度的出现，数据流不再可以使用以前的控制器进行管理。如果DoS攻击以这种数据率发生，则所使用的防火墙(或者控制器)将过载，使得控制装置可能发生停顿。

[0009] 然而，出于成本原因，难以想象的是，可以在每个控制装置上实施附加的防火墙。如果这在各自情况下都需要附加的控制器芯，则控制装置的成本几乎会猛增。

[0010] E/E构架(电气/电子构架：在E/E系统的交互和网络连接、接口、环境、E/E系统中数据流和能量流、数据和软件构架方面为车辆创建某种结构，从而将在硬件、软件、车辆电子系统、线束和拓扑级产生一种用于所有E/E系统和E/E部件的连续的并且全车范围的架构)的一个技术问题将是大数据率的处理。在失效的情况下，在这种情况下可能出现可以不再由防火墙管理的大量数据。只是由于控制器具有100Mbit/s的接口绝不是意味着软件(防火墙)也可以处理这些大量数据(实时)。在这种情况下，技术是必要的，以便使车辆电子系统更安全，同时不会使成本以指数上升。

[0011] 本发明的目的因此是提供一种方法和一种设备，该方法和该设备可以用来使得车辆网络就外部访问而言更安全并且可以同时减轻防火墙上的负载。

[0012] 所述目的是借助于权利要求1、并且借助于另外的独立权利要求所述的方法来实现的。

[0013] 根据本发明的方法涉及用于机动车辆的通信网络，其中，通信网络中的通信涉及正在进行的数据传输。在这种情况下，通信网络提供用于至少两个通信用户。提供的是使得安全措施抵抗通信网络上的攻击。根据本发明，安全措施的性能被分到多个通信用户上。

[0014] 在此背景下，通信网络上的攻击旨在被理解为利用安全缺陷攻击网络。换言之，其涉及第三方的攻击(网络攻击(cyber attack)/黑客攻击)，借助于其攻击，该第三方获得访问车辆中控制机构/管理机构上的信息或对其的控制。在汽车中，被第三方这样接管控制可能尤其对车辆乘坐者的安全有影响，并且因此必须避免。这可以借助于本发明得以实现。

[0015] 这些安全措施例如可以追踪和抵御特定的攻击类型(例如DoS攻击)。分配安全措施的性能使得例如不同通信用户过滤、或抵御不同类型的攻击，从而有利地提供对许多不同可能的攻击的全覆盖或抵御而无需配备具有附加的硬件的防火墙和/或使所述防火墙过负载。因此，有利地节省了成本。并且，因此可以实时抵御攻击。进一步，本发明允许甚至在有害的数据包到达防火墙之前由其他通信用户拦截攻击。

[0016] 可以单独在通信用户之间或在通信用户与防火墙之间执行安全机制的分配。通过举例的方式，由防火墙特别优选地执行某一安全措施，同时使得其他安全措施由通信用户中的一个或多个通信用户执行、或使其分到一个或多个通信用户上。

[0017] 优选地，通信用户被组合以产生通信路径。通信发生在与通信用户相关的通信路径中。在本发明的另一个优选的发展中，安全机制的分配发生在为通信提供相应通信路径

的通信用户上。通信用户特别优选地至少包括传输方和接收方，在传输方与接收方之间通信以数据传输的形式进行。根据此发展，通信用户中的至少一个通信用户(也就是说传输方或接收方)被安排在汽车中。相应的其他通信用户可以类似地是安排在汽车中的，或其是被定位在外部的外部用户。外部用户可以例如是外部安排的控制装置或云。

[0018] 在本发明的优选的发展中，该方法还包括查明每个通信用户的最大可能安全辅助。换句话说，查明各通信用户可以提供的最大安全辅助。安全辅助在这种情况下与通信用户为执行安全措施的辅助相关。特别优选地，将查明的信息存储在数据库中。

[0019] 该发展允许查明可用于辅助防火墙的资源并且相应地进行安全措施的分配。因此，可以以最优的形式利用可利用的资源，以用于防止网攻击络。

[0020] 在本发明的优选的发展中，该方法包括查明每个通信用户的最大可能搜索深度。最大可能搜索深度特别优选地涉及通信用户可以搜索的协议层的最大复杂性。在这种情况下，协议层的“复杂性”旨在被理解成“复杂性”随着协议层数量的增加而增加。在层1(物理层)中，例如仅可获得报头和有用的数据，有用的数据是实际传输的数据并且报头包含关于由相应的相关层(在此情况下是层1)处理这些数据的信息。这是最低、最小复杂度的层并且需要最低的能力(计算花费)。在另一方面，在层7中，额外地需要搜索另外六个层，这需要更高的能力(计算花费)。对每个通信用户来说，因此优选地查明上至哪一层通信用户可以搜索数据包。

[0021] 可替代地或附加地，最大搜索深度还涉及各个层的分析深度，即各个层被搜索到多深(字节深度)，也就是说可以查看相应层内的多少字节“深度”。

[0022] 该信息然后优选地用于查明通信用户的最大可能安全辅助，因为搜索深度支配哪些攻击可以被通信用户检测到。这还允许最优地分配资源。

[0023] 在本发明的优选的发展中，安全机制是过滤规则的形式，或所使用的安全机制是过滤规则。在这种情况下，过滤规则优选地是规则，基于这些规则确定相应数据包会发生什么。过滤规则特别优选地可用作数据包过滤器、或网络过滤器，并且以此形式实施在通信用户和/或防火墙中。

[0024] 在本发明的优选的发展中，借助于数据传输协议进行用于通信的数据传输。数据传输协议具有多层。有利地，为该方法提供了具有已知数据传输协议和其相关联的所需分析资源的数据库。因此，对每个已知数据传输协议提供有应当分析哪些层并且以什么字节深度分析来使得可以可靠地检测攻击。当对通信用户查询可利用的资源时和/或当分配安全措施时，优选地使用了数据库。在未知数据传输协议的情况下，特别优选地阐述了，最大资源是必要的，因为在未知协议的情况下，不清楚攻击可能隐藏在哪里。在这种情况下，因此规定应当以最大字节深度搜索所有的层。

[0025] 特别地，数据传输协议例如是以太网、FlexRay、VLAN(虚拟局域网)、IP(互联网协议)、AVB(音频/视频桥接)、TSN(时间敏感网络)或SOME/IP(基于IP的可扩展的基于服务的中间件)形式的。

[0026] 在本发明的另一个优选的发展中，通信用户是控制装置(ECU-电子控制单元)和/或交换机的形式。存在在车辆中的多种不同的装置因此无论如何都可用于分配安全措施。因此，不必提供另外的、附加的硬件。

[0027] 在本发明优选的发展中，通信网络具有防火墙，并且防火墙的配置与安全措施的

分配匹配。如果有通信用户承担安全措施，则防火墙的配置可以被改变成使得防火墙不再执行这些被承担的安全措施。这减轻了防火墙上的负载。替代性地，防火墙还可以继续执行这些安全机制，使得有利地存在冗余。

[0028] 根据本发明的方法优选地在生产结束时(在汽车的生产已经完成之后)、在软件更新之后、在发现安全缺陷之后或当替换或更新通信路径的用户时实施一次。因此还可以在交付给终端消费者(例如如果替换控制装置或如果已经提供了软件更新)之后有利地检测安全缺陷。因此，终端消费者还提供在操作车辆期间抵抗攻击的增加的安全性。

[0029] 在本发明优选的发展中，针对安全辅助的查询和/或安全机制的分配使用了与不同攻击情形相关的信息。该信息优选地以类似的方式存储在数据库中，该数据库尤其存储在存储器中并且不会被连续更新。该信息特别优选地涉及不同可能的攻击类型并且涉及所需要的安全机制。一种可能的攻击类型例如是DoS(拒绝服务)，其中由第三方导致过负载并且导致防火墙或ECU的功能或服务或其他方面的失效。

[0030] 在本发明优选的发展中，数据库存储在安全存储区中。特别地，此安全存储区提供有加密并且因此受保护而免受攻击。在这种情况下，安全存储区可以例如被安排在中心控制装置上。

[0031] 在优选的发展中，借助于算法执行对通信用户关于其最大可能安全辅助的评级。算法可以优选地使用最大可能搜索深度以便同样创建资源等级并且可以对通信用户指定资源等级。为此目的，算法尤其包含与最大可能搜索深度相关的、与数据传输协议相关的和/或与在评定中还同不同攻击情形相关的信息相关的一个或多个数据库。

[0032] 本发明还涉及一种被设计成用于执行该方法的、用于机动车辆控制装置的电子监测单元或控制单元。

[0033] 本发明可以有利地增加了车辆网络的安全性，特别是在没有额外财务支出的情况下。通过在汽车中使用以太网或其他数据传输系统(例如FlexRay)，尤其需要利用简单技术和给定的技术特征的机制，以便能够省却昂贵的实施以及进一步附加的硬件。

[0034] 进一步优选的实施例基于附图从以下对示例性实施例的描述中显现。

[0035] 在示意性描绘中：

[0036] 图1示出了通信数据包或栈的结构，

[0037] 图2示出了经由连接单元和中心防火墙将车辆网络网络连接到因特网的说明性实例，

[0038] 图3示出了经由多个连接单元和多个中心防火墙将车辆网络网络连接到因特网的说明性实例，

[0039] 图4示出了作为图3发展的本发明的示例实施例，

[0040] 图5示出了根据本发明用于查明最大可能搜索深度的方法的示例性构型，

[0041] 图6示出了用于所查明的搜索深度的数据库的示例性构型，

[0042] 图7示出了用于根据安全辅助分配控制装置的方法的示例性构型，

[0043] 图8示出了以太网交换机与防火墙的搜索深度的比较，

[0044] 图9示出了用于分配搜索深度的方法的示例性实施例，

[0045] 图10示出用于分配安全机制的示例性序列。

[0046] 为了允许简短地描述示例实施例，完全相同的元件提供有相同的附图标记。

[0047] 图1示以展示的方式示出了通信栈的结构。根据该实例，该通信栈可以具有基于OSI模型的七层。对用于保护网络的防火墙的需求是取决于通信层的。发生通信的层越高，帧深度越深-就需要保留越多的存储器并且需要越强的计算能力。此外，计算能力随着在每层中分析的深度的增加而增加。在这种情况下，分析的深度是指用来查看层内部的字节深度。

[0048] 图1因此示出了与所检查的通信层有关的复杂性、计算能力和存储器需求的改变。随着层增加(层的数量增加)，数据包的帧大小也增加。因此，在检查期间缓冲存储数据所需要的缓冲存储器也增加。同样地，所需要的计算能力也因此增加。为了能够搜索具有所有层的未来数据包，将需要提供带有更好或附加的硬件的防火墙，这产生成本。

[0049] 图2示出了将车辆网络1网络连接到因特网的说明性实例。在这种情况下，车辆网络1具有连接单元5和车辆网络9的具有(中央)防火墙3的剩余部分。车辆网络的剩余部分可以例如是控制装置或者可以具有多个控制装置和经由CAN、LIN、FlexRay、MOST、LVDS、WLAN、蓝牙或以太网连接至彼此(未描绘)的网关。网络1经由连接单元5(“连通性单元”)连接至因特网。根据该实例，网络9的剩余部分与连接单元5之间的连接是有线连接形式，并且在连接单元5与因特网之间的连接是无线(无线电)连接形式。

[0050] 图3示出了图2的更复杂的变体，其中，车辆网络1包含多个防火墙3’、3”和多个以太网交换机7。连接单元5’和另一个连接单元5”类似地安排在车辆网络1中。在车辆网络的剩余部分9中可以提供另外的单元，该车辆网络被描绘为块。车辆网络的剩余部分9和两个连接单元5’、5”各自具有它们自己的防火墙3’、3”、3”’。防火墙3’、3”、3”’可以例如是被配置成用于承担合适任务(例如执行安全措施)的控制器形式。

[0051] 图4示出了图3的发展，其中，车辆网络的剩余部分9是具有防火墙3”的控制装置(ECU)11形式。此外，以太网交换机7各自额外具有防火墙3””。这可以例如通过相应地配置交换机7的微控制器单元(尤其是ASIC)来提供，也就是说承担防火墙的任务。根据该实例，防火墙3””可以执行数据包的预分选，这些数据包然后被防火墙3”和3”’(并且可能是3’)针对攻击进行过滤，或它们可以承担防火墙3”、3”’(并且可能是3’)的一些任务并且因此减轻它们上的负载。防火墙3’和3”在这种情况下可以是更简单和/或冗余的防火墙的形式。由于多个单元(5”，7，11)在分析时合作并且因此分担检验的计算负载，不再需要单一防火墙执行分析。

[0052] 网络1中的各个单元可以是通信用户。虽然连接单元5”不再是主要通信路径的一部分，但是也可能涉及安全机制的执行。在执行安全措施之后，然后需要将数据或结果返还至通信路径。

[0053] 安全措施的执行分布于通信用户。在这种情况下，不是所有的防火墙或所有的通信用户都需要承担安全措施。优选地，分配被实施成使得存在最佳资源利用。特别地，通信用户和/或防火墙还可以作为冗余件运行并且因此承担安全措施，该安全措施同样可以由另一个防火墙或另一个通信用户执行。这提供更高水平的安全性，这是由于可以减小检测攻击中的错误。

[0054] 图5示出了一种用于查明各个通信用户的最大可能搜索深度的方法。在这种情况下，在该方法开始20之后，所选择的通信路径或通信与所涉及的控制装置所需要的通信需求首先被传输22至所选择的防火墙(例如3-3””)。通信需求可以包括例如消息频率、数据包

类型、或协议类型、以及安全级别。防火墙3-3""(或可替代地另一个控制单元)计算通信24所需的资源并且将它们存储在通信矩阵中。特别地,基于所使用的协议类型对所需要的资源进行分类。已知协议和所需要的相关资源可以提供为可以诉诸的数据库。尤其是使用了新的协议类型的外部通信优选地被分类成使得进行最大分析。即优选地以最大字节分析深度检验所有的协议层,因为在未知协议的情况下,并不清楚攻击可能隐藏在协议的什么地方。

[0055] 在查明所需要的资源之后,对控制装置5、5'、5"、7、11发出信息请求26、30。例如,查明上至哪个数据包层存在由控制装置5、5'、5"、7、11辅助的可能性26并且上至什么字节深度存在辅助的可能性30。因此,查明了控制装置5、5'、5"、7、11的最大可能搜索深度看起来是什么样子。控制装置5、5'、5"、7、11向防火墙3-3""提供对请求的适当响应28、32。所查明的信息优选地存储在数据库中、特别优选地存储在安全存储区中,并且查明对工作负载的经资源优化的分配。随后,可以通过控制装置5、5'、5"、7、11启用分析34。在这种情况下,控制装置5、5'、5"、7、11和防火墙3-3""被配置成按照查明的分配抵御攻击。

[0056] 例如在步骤中可以由控制装置5、5'、5"、7、11进行关于受辅助的层26的查询。在这种情况下,可以相继查询对第一层到最大层的辅助。通过举例的方式,首先查询是否辅助了第一层。如果是,则查询是否辅助了第二层等。在这种情况下,应当注意的是,在实践中可以省略对第一层的查询,因为第一层作为物理基础必须始终是可分析的。如果在逐步查询的过程中查明特定的层可能不再被分析,则可以由此得出最初检验的层(仍被查明为受辅助层)是最大可能受辅助的层。然后此结果可以例如存储在与检验控制装置相关的数据库中。

[0057] 图6示出了具有与各个通信用户相关的查明的信息的数据库的可能矩阵,这些通信用户可以例如是控制装置5、5'、5"、7、11和/或防火墙3-3""。根据该实例,数据库可以存储控制装置5、5'、5"、7、11和防火墙3-3""是否可以识别并且抵御特别的攻击。每次攻击发生在特定的协议层上。给出了多种可能的攻击类型,因此,很可能影响不同层。每个控制装置具有对于数据协议的最大可能搜索深度。例如在第一控制装置仅可以搜索较低的层时,第二控制装置还例如能够搜索较高的层。例如,第二控制装置可以因此覆盖较高的层上的攻击,并且第一控制装置可以覆盖较低的层上的攻击。防火墙也具有最大搜索深度并且当安全机制分配在控制装置上时,可以配置成例如使得其覆盖控制装置不能承担的层的剩余部分。

[0058] 图7中也描绘了根据本发明的构思。图的左侧示出了可能的攻击40,这些攻击可以例如经由天线42到达网络。作为进一步通信用户,提供了交换机7和ECU 11,它们应该接收数据包。根据该实例,所描绘的可能的攻击40是DoS(阻断服务攻击)的不同变体,例如"死亡Ping(Ping of Death)"、"SYN洪水(SYN flood)"或"广播风暴(broadcast storm)"。根据该实例,这些攻击不通过天线42处理。一些攻击的第一识别由交换机7承担。攻击40因此可以被过滤出去、或过滤掉,使得仅有攻击40没有被交换机7承担的剩余部分留下。信息或数据包被传送到ECU 11,其承担对残留的攻击40的识别,或抵御攻击40。对击40的识别或抵御可以被称为安全措施。用于避免攻击网络1的安全措施40因此是以分布形式在网络1中进行的。为此目的,对可利用的资源的分析(例如通过交换机7和ECU 11)之后是执行的安全措施分配。有利地,可以因此抵御大带宽的攻击40而不需要提供检测所有攻击40所需的新硬件。安全措施的分配性能因此允许节约成本。

[0059] 图8以示例性形式示出了用来描绘以太网交换机7和防火墙3-3""的搜索深度的数据包。不同框是报头和有用的数据。虽然以太网交换机7只可以搜索数据(最左边的框)和前两个报头/层50,而防火墙3-3""可以搜索数据包的所有层(例如具有七层)52。如果交换机7和防火墙3-3""都开始搜索,将因此在前两层50的区域中存在冗余。这种冗余可以通过将该区域中的交换机7与防火墙3-3""的结果进行比较而用于错误分析,或防火墙3-3""仅搜索不被交换机7搜索的报头(图9)。在后面一种情况下,分析区域的移位54因此针对防火墙3-3""发生。因此不再需要搜索也可以由交换机7分析的层。在那种情况下,防火墙3-3""有利地具有可用于进一步任务的资源。有待分析的区域自然可以类似地拆分在另外的交换机7或控制装置11上,使得防火墙3-3""的份额变得更小。

[0060] 图10示出了图5所示的用于在使用特定的数据传输协议时分配安全措施的方法的整体视图的替代性描绘。在该方法开始20之后,例如通过控制单元或防火墙查明必要的分析资源22,这些必要的分析资源然后存储在通信矩阵中。然后查明控制单元或防火墙可以提供对哪些层和什么深度的分析。结果被存储在安全数据库62中。随后,确定安全措施的分配是如何发生的33。此后,可以在实践中实施查明的分配,为此,相应地配置控制单元和防火墙34。为此目的,实现了与控制单元和防火墙的通信35。匹配的构型用于以分布的方式成功地认出和阻止攻击36。

[0061] 关于本发明的进一步信息:

[0062] 本发明提出一种新颖方法以便在网络中分配和透露过滤规则(防火墙的基本原则)。此外,本发明提供一种方法,以便就所述规则而言查询汽车网络及其部件并且根据所述规则配置它们。在这种情况下,本发明限定机制,以便适时选择针对可能攻击功能的正确安全平台;关于这点,见图5的说明性实例。

[0063] 本发明提出一种方法,该方法配置安全能力和选项,并且经由接口使它们在网络中有用。因此,变得明白的是,哪个安全机制可以被重复覆盖,哪个安全机制根本不能被覆盖以及哪个安全机制可以被省略。以此方式获得的安全矩阵允许首先简单地描绘可以实施哪种类型的安全保障,并且其次还简单地描绘借助于相应控制装置所可提供的安全水平。本发明的方法首次阐明了防火墙可以如何减轻负载并且计算能力可以重新定位到哪里。

[0064] 该方法允许就安全性方面(来自外部的攻击)更容易地检查和测试整个网络。

[0065] 本发明提出为了车辆安全的目的使用以太网TSN标准并且在这种情况下具体地使用IEEE802.1Qci入口流量监管(Ingress Policing)和过滤标准。其标准和性能可能对汽车行业变得特别重要,首先因为这些功能实施在硬件中,并且因此在软件中不需要计算能力,其次这种部件未来将可能包括在每个汽车中。

[0066] 本发明的本质和新颖性首先在于车辆网络的安全性有所增加(对于相同成本来说),其次对安全机制提供了冗余。随着以太网的出现,尤其还需要利用简单技术和给定的技术特征的机制,以便能够省却昂贵的实施以及进一步附加的硬件。

[0067] 本发明具有的优点在于,可以更好地管理新技术(例如以太网或IP)。新技术必须不再在汽车中受到绑架。来自IT的典型技术并非所有都可以被采用。例如,加密不可能具有限定的深度(128bits),因为必要计算时间典型地在几秒的范围内。在这种情况下,不能满足汽车中的需求。

[0068] 在CAN或LIN上发生错误的情况下,控制器(包括防火墙)目前公认地能够管理数据

包的洪水攻击(如果它们100％运行的话)。在100Mbit/s以太网或甚至1000Mbit/s以太网的情况下,这不再是可能的(不管控制器是否具有这种接口)。作为本发明的结果防火墙可以可靠地操作并且不承受过负载。

[0069] 因此不必增加防火墙上的硬件需求。如果符合使得安全性能保持恒定就可以因此省略附加的控制器。这导致由于防火墙所必需的计算能力减小使得成本节约。

[0070] 安全机制的分配和某些机制的冗余执行或计算还允许避免简单的错误。车辆电子系统中安全功能的重复集成因此允许在实际防火墙之前检测攻击/错误,并且更快速地发起应对措施。

[0071] 这表明,没有部件可以独自管理车辆电子系统的安全(考虑到合理的总成本)。虽然原则上防火墙可以几乎覆盖所有事物,但是为了实时进行此任务结果就需要非常高水平的性能。交换机已经可以在较低的层覆盖这些功能的许多功能并且可以在没有附加的部件(例如存储器或CPU)的情况下进行管理,这是由于其内置的HW辅助方法。针对系统实现的辅助至此不仅使得整体构思更具冗余性并且更加安全,还使得(多个)防火墙的复杂性更简单。

[0072] 根据通信路径的传输(在系统中动态地传输,在使用DBC、Fibex文件实施防火墙、或生产结束编程(end-of-production programming)时),防火墙计算用于保护传入消息的必要资源。数据包类型、数据包长度、协议和消息频率直接影响因此所需要的计算能力和存储器。即使今天,为了深度数据包检查也仅提供单一CPU。本发明提出防火墙使得网络中的安全机制重新定位或冗余地提供它们。为此目的,在系统设计、更新期间或在实施期间,使用服务发现方法就以太网交换机的功能查询它们。查询的目的是深刻理解深度数据包检查的重新定位,这种重新定位需要高水平的计算能力并且已经可以部分地重新定位。

[0073] 因此,这些不同的攻击技术有利地并不首先被防火墙阻止,而是可以已经被控制装置在实际防火墙和接收方之前部分地消除。根据安全辅助的分类,系统(防火墙)能够保护(多个)通信路径并且分配安全机制。

[0074] 本发明提供的另一个选项是优化防火墙。ECU的或交换机的搜索深度的检测允许防火墙使用针对其他检验的计算能力并且由此执行实时检验。由于不再需要搜索整个帧,这节省了存储器和计算能力。

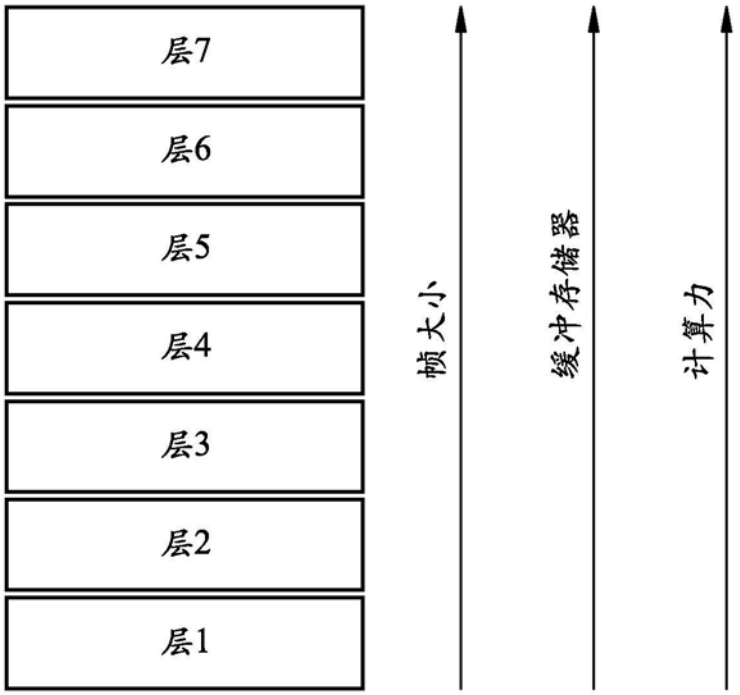


图1

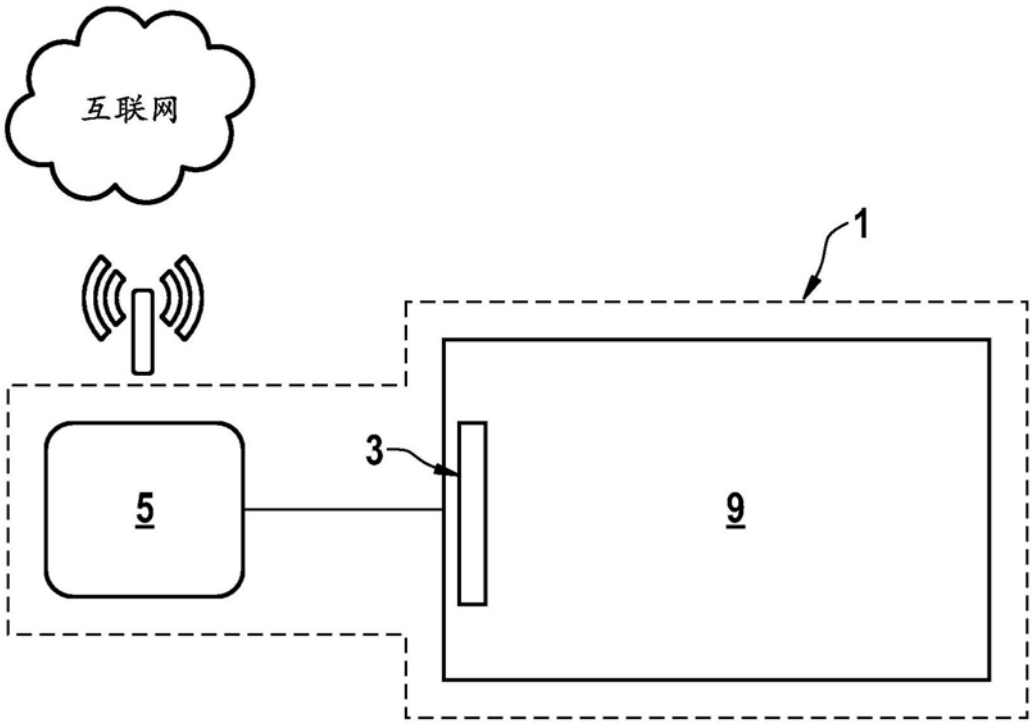


图2

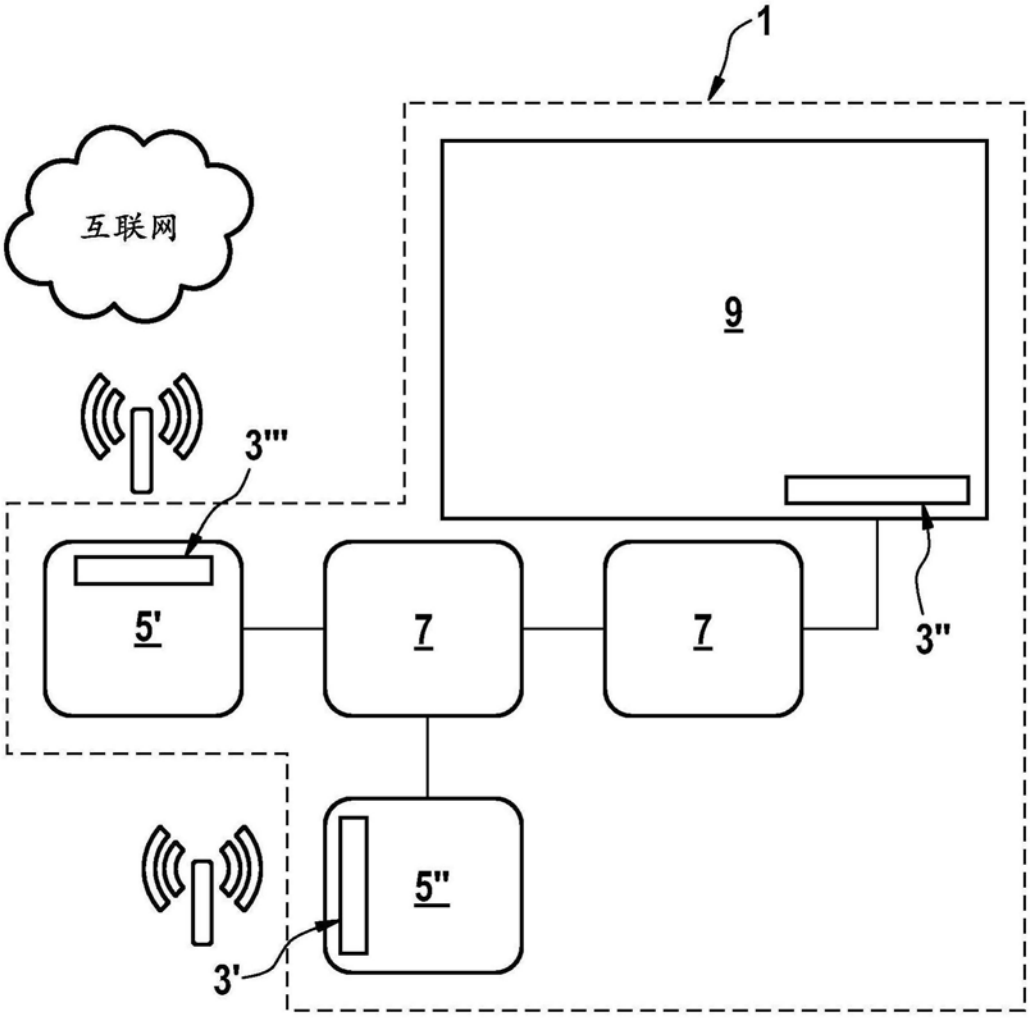


图3

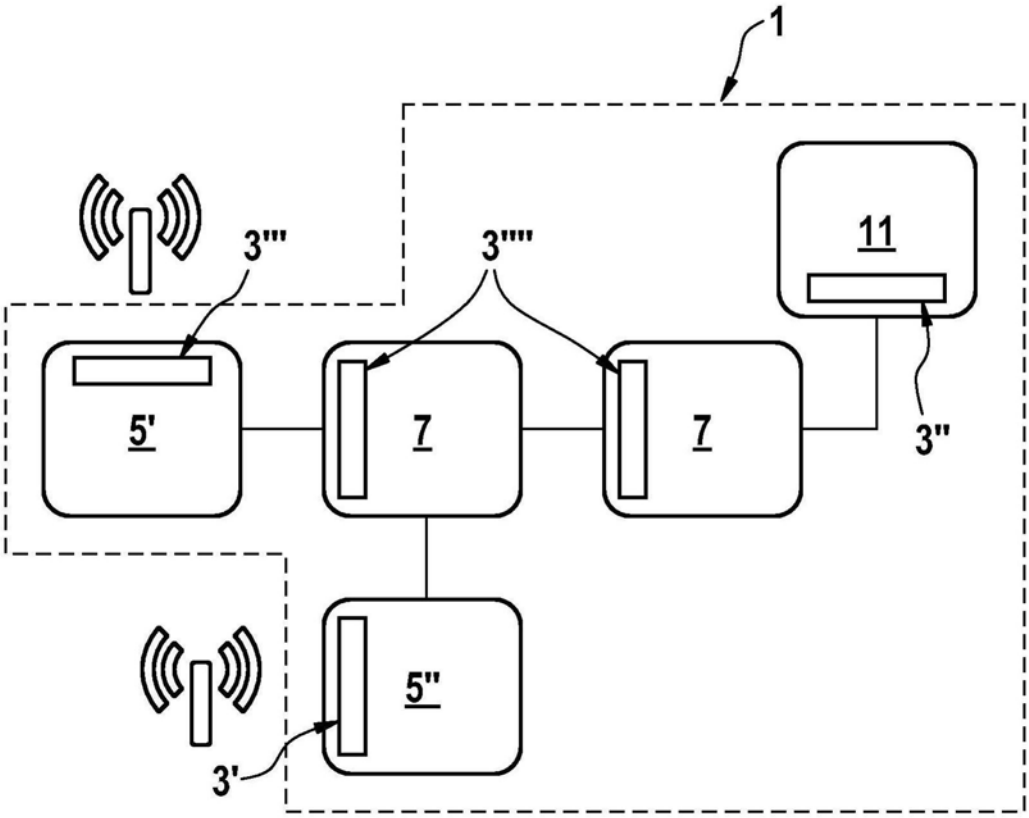


图4

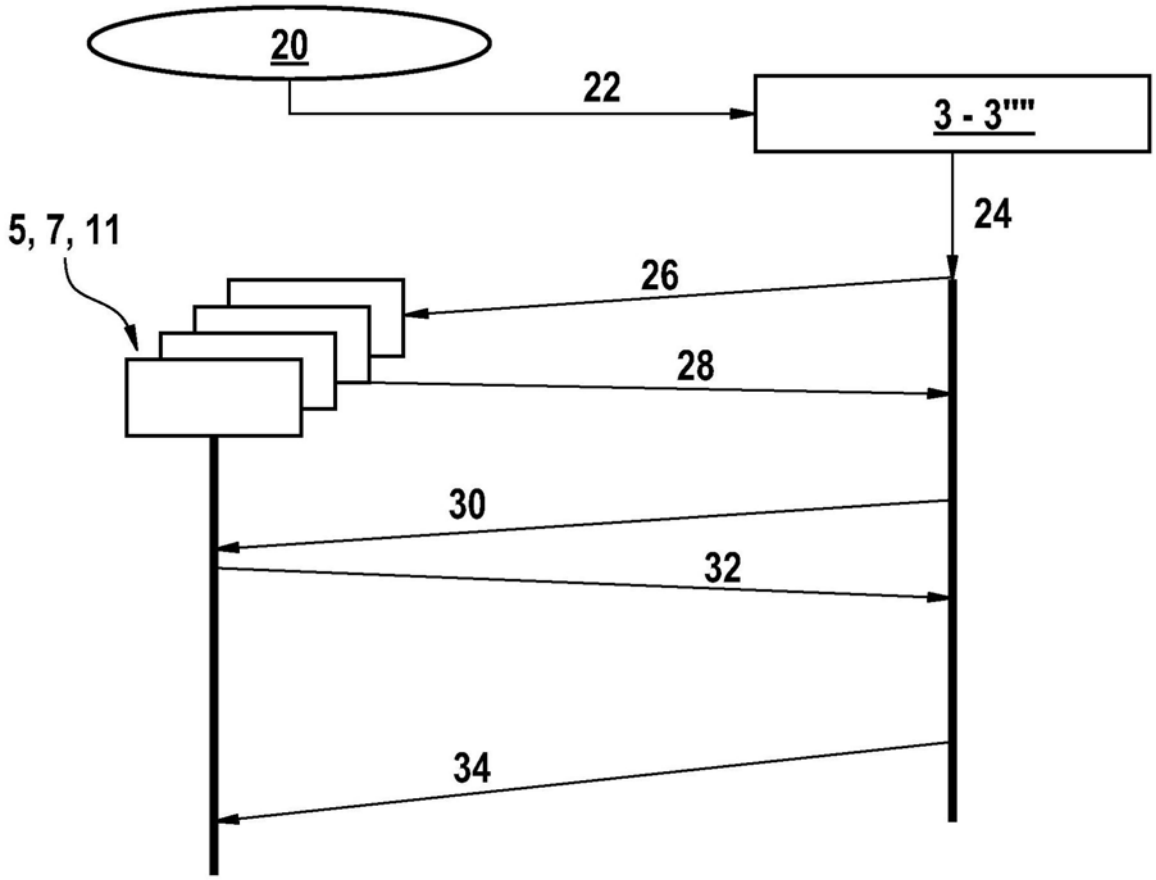


图5

攻击	ECU1	ECU2 包括开关	……	全防火墙
DoS攻击	不可能	辅助	……	完全覆盖
VLAN	不可能	完全覆盖	……	限制可能性
层2QoS	不可能	完全覆盖	……	限制可能性
TOS	不可能	完全覆盖	……	完全覆盖
数据包大小	不可能	完全覆盖	……	限制可能性
频率	不可能	完全覆盖	……	限制可能性
Syn洪水	不可能	不可能	……	完全覆盖
Smurf攻击	不可能	不可能	……	完全覆盖

图6

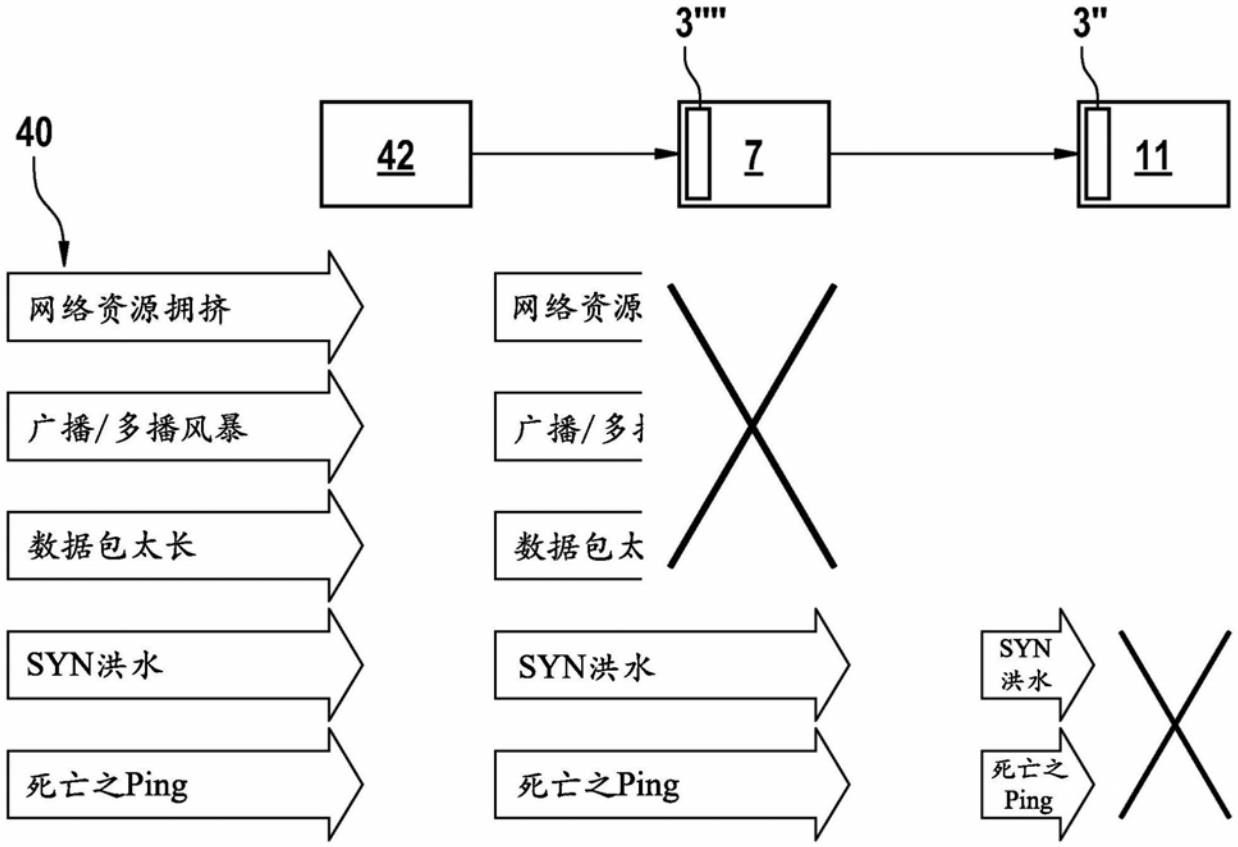

3''''
3''
40
42
7
11
网络资源拥挤
广播/多播风暴
数据包太长
SYN洪水
死亡之Ping
网络资源
广播/多
数据包太
SYN洪水
死亡之Ping
SYN
洪水
死亡之
Ping

图7

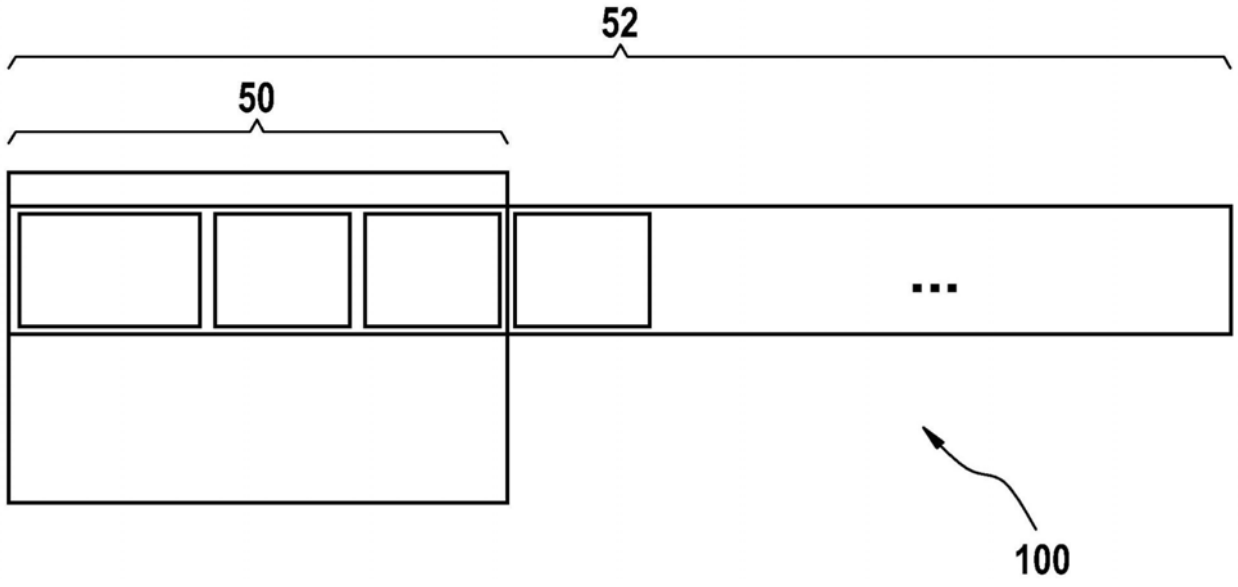

52
50
...
100

图8

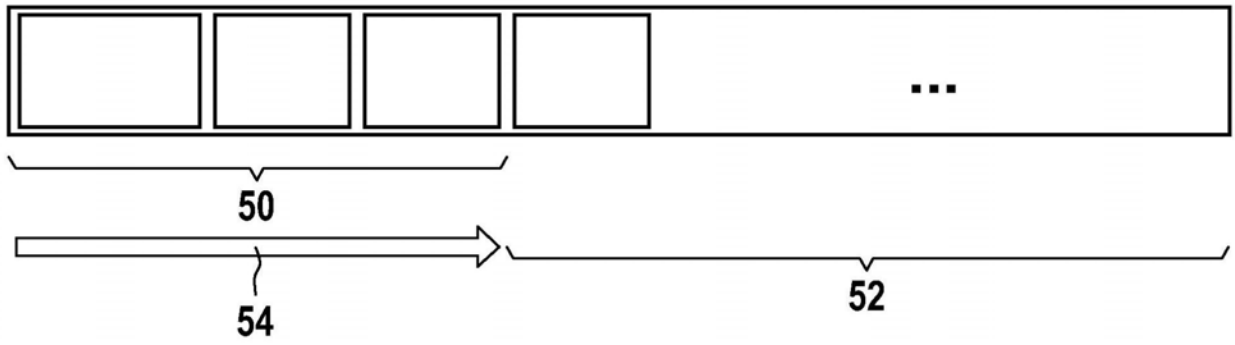


图9

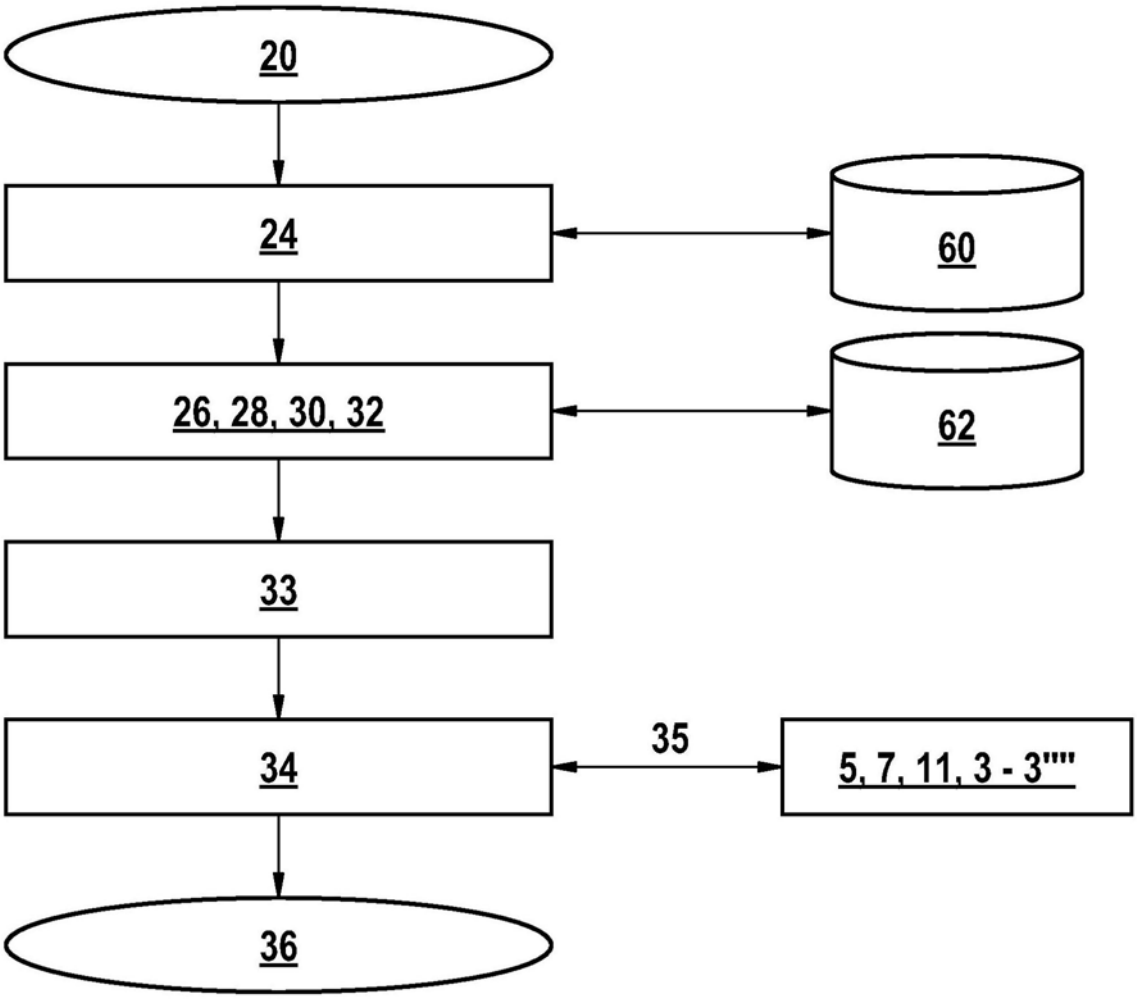


图10