(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107395339 A
(43)申请公布日 2017.11.24

(21)申请号 201710342827.4

(22)申请日 2017.05.16

(30)优先权数据
102016208453.4 2016.05.17 DE

(71)申请人 罗伯特·博世有限公司
地址 德国斯图加特

(72)发明人 A.穆特

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 卢江 杜荔南

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 12/40(2006.01)
H04L 29/06(2006.01)

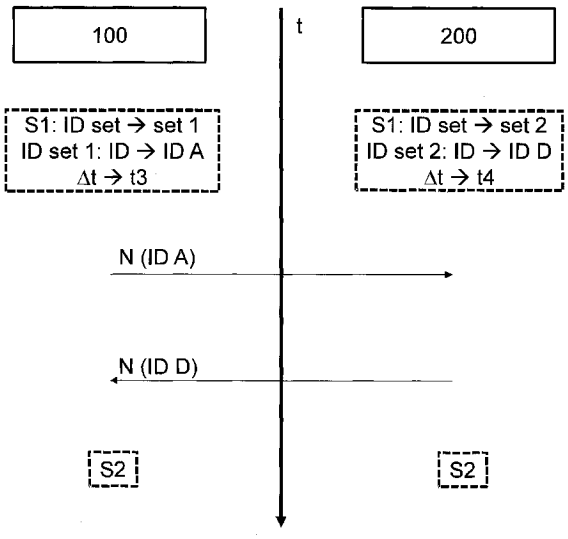
权利要求书2页 说明书7页 附图2页

(54)发明名称

用于在网络中生成秘密或密钥的方法

(57)摘要

本发明涉及用于在网络中生成秘密或密钥的方法。提出一种用于在网络中生成秘密的方法，其中网络至少具有第一用户(100)和第二用户(200)。第一用户(100)和第二用户(200)分别在网络的共同的传输介质上利用分别所选择的消息标识进行消息传输，并且第一用户(100)和第二用户(200)分别在不同消息标识的情况下根据第一用户(100)或第二用户(20)中的哪个已经使用了所述消息标识中的哪个来生成在第一用户(100)与第二用户(200)之间分享的秘密。第一用户(100)和第二用户(200)针对其相应消息传输从多于两个标识中随机地选择标识。



CN 107395339 A

1.一种用于在网络中生成秘密的方法，其中所述网络至少具有第一用户(100)和第二用户(200)，其中所述第一用户(100)和所述第二用户(200)分别在所述网络的共同的传输介质上利用分别所选择的消息标识进行消息传输，并且其中所述第一用户(100)和所述第二用户(200)分别在不同消息标识的情况下根据所述第一用户(100)或所述第二用户(20)中的哪个已经使用了所述消息标识中的哪个来生成在所述第一用户(100)与所述第二用户(200)之间分享的秘密，其特征在于，所述第一用户(100)和所述第二用户(200)针对其相应消息传输从多于两个标识中随机地选择标识。

2.根据权利要求1所述的方法，其特征在于，所述第一用户(100)和所述第二用户(200)为了选择分别具有一个包括至少四个标识的组，其中所述第一用户(100)和所述第二用户(200)尤其是具有相同的标识。

3.根据权利要求1所述的方法，其特征在于，所述第一用户(100)和所述第二用户(200)为了选择分别具有至少两个组，所述至少两个组分别包括至少两个标识，其中所述第一用户(100)和所述第二用户(200)尤其是具有相同的标识组。

4.根据权利要求3所述的方法，其特征在于，所述第一用户(100)和所述第二用户(200)为了选择首先分别选择所述组之一并且然后随机地选择所选择的组的一个标识。

5.根据权利要求4所述的方法，其特征在于，所述组之一的相应选择在所述第一用户(100)与所述第二用户(200)之间协调地进行。

6.根据权利要求5所述的方法，其特征在于，所述第一用户(100)和所述第二用户(200)选择彼此不同的组。

7.根据权利要求3至6之一所述的方法，其特征在于，所述第一用户(100)和所述第二用户(200)分别根据至少一个已经相互之间所生成的秘密为稍后的秘密生成选择标识组。

8.根据权利要求7所述的方法，其特征在于，所述第一用户(100)和所述第二用户(200)在所述秘密生成的第一阶段中分别利用预定的或所协商的标识组生成秘密，并且在所述秘密生成的第二阶段中分别根据至少已经相互之间所生成的秘密利用标识组生成秘密。

9.根据权利要求6所述的方法，其特征在于，所述第一用户(100)和所述第二用户(200)交替地设置用于秘密生成的消息传输，并且两个或更多个秘密生成直接彼此连接，其中所述第一用户(100)和所述第二用户(200)尤其是分别在没有等候时间的情况下基于通过时间窗的限制或者基于预定时间间隔或者基于要等待的确认消息而传输。

10.根据前述权利要求之一所述的方法，其特征在于，仅仅在所述第一用户(100)的消息的标识和所述第二用户(200)的消息的标识的确定组合的情况下生成秘密。

11.根据权利要求10所述的方法，其特征在于，针对所述标识在所述第一用户(100)和所述第二用户(200)中定义如下组合，在所述组合的情况下生成秘密。

12.根据权利要求6所述的方法，其特征在于，所述第一用户(100)和所述第二用户(200)利用被设置用于秘密生成的消息传输来传输附加的有效数据或控制数据。

13.根据权利要求6所述的方法，其特征在于，所述第一用户(100)和所述第二用户(200)分别彼此独立地、尤其是尽可能快地执行用于多个秘密生成的多个消息传输。

14.根据权利要求13所述的方法，其特征在于，在所述用户之间为此规定时间窗，在所述时间窗中尤其是应当进行确定数目的秘密生成和相应的消息传输。

15.根据权利要求13或14之一所述的方法，其特征在于，分别针对消息传输，在所述第

一用户(100)和所述第二用户(200)中选择标识组。

16.根据前述权利要求之一所述的方法,其特征在于,作为秘密生成预定位或预定位序列。

17.根据前述权利要求之一所述的方法,其特征在于,从多个所生成的秘密中在所述第一用户(100)中和在所述第二用户(200)中生成共同的密码密钥。

18.根据权利要求17所述的方法,其特征在于,所述密钥被用于保护所述第一用户(100)与所述第二用户(200)之间的通信。

19.根据前述权利要求之一所述的方法,其特征在于,所述网络是CAN、TTCAN、CAN-FD、LIN或I2C总线系统。

20.一种用于在网络中生成秘密的方法,其中所述网络至少具有第一用户(100)和第二用户(200),其中所述第一用户(100)在所述网络的共同的传输介质上利用所选择的第一消息标识进行消息传输并且接收由所述第二用户(200)利用所选择的第二消息标识进行的消息传输,其中所述第一用户(100)在不同消息标识的情况下根据所述第一用户(100)或所述第二用户(20)中的哪个已经使用了所述消息标识中的哪个来生成在所述第一用户(100)与所述第二用户(200)之间分享的秘密,其特征在于,其特征在于,所述第一用户(100)针对其消息传输从多于两个标识中随机地选择标识。

21.一种网络,该网络至少具有第一用户(100)和第二用户(200)以及具有共同的传输介质,所述第一用户(100)能够通过所述传输介质与所述第二用户(200)通信,其特征在于,所述网络被设立用于执行根据权利要求1至20之一所述的方法的所有步骤。

22.一种设备,该设备被设立用于作为网络上的用户(100,200)执行根据权利要求20所述的方法的所有步骤。

23.一种计算机程序,该计算机程序被设立用于执行根据权利要求1至20之一所述的方法之一的所有步骤。

24.一种机器可读存储介质,具有存储在其上的根据权利要求23所述的计算机程序。

用于在网络中生成秘密或密钥的方法

技术领域

[0001] 本发明涉及一种用于在网络中生成秘密、如秘密的密码密钥的方法，尤其是在网络的两个用户中生成共同的秘密的密钥。点到点连接通常也被算作网络，并且这里应当同样用该术语来称呼。在此，两个用户通过共同使用的传输介质进行通信。在此情况下，逻辑位序列(或更一般地：值序列)通过相应传输方法作为信号或信号序列被物理地传输。作为基础的通信系统例如可以是CAN总线。该CAN总线设置显性和隐性位或相应地显性和隐性信号的传输，其中网络的用户的显性信号或位相对于隐性信号或位占优势。仅当所有参与的用户都设置用于传输的隐性信号时或者仅当所有同时发送的用户都传输隐性信号电平时，根据隐性信号的状态才出现在传输介质上。

背景技术

[0002] 不同设备之间的安全通信在越来越多地联网的世界中变得越来越重要，并且在许多应用领域中是接受度的重要前提，并且因此也是相应应用的经济成功。这视应用而定包括不同保护目标、诸如对要传输的数据的机密性的维护、参与的用户或节点的相互认证或者对数据完整性的确保。

[0003] 为了实现这些保护目标，通常使用合适的密码方法，一般可以将这些密码方法分为两个不同类别：一方面对称方法，在所述对称方法中发送方和接收方具有相同的密码密钥；另一方面非对称方法，在所述非对称方法中发送方利用接收方的公开(也就是说，也可能为潜在的攻击者所知)密钥对要传输的数据进行加密，但是解密仅能利用理想地仅为接收方所知的相关私有密钥来进行。

[0004] 非对称方法尤其具有如下缺点：非对称方法一般来说具有非常高的计算复杂度。因此，非对称方法仅仅有条件地适合于资源受限的用户或节点、诸如传感器、执行器等等，这些用户或节点通常仅仅具有相对小的计算能力以及小的存储器并且例如由于电池运行或使用能量采集而应当能量高效地工作。此外，常常仅仅有限的带宽可供用于数据传输，这使具有2048位或更多位的长度的非对称密钥的交换无吸引力。

[0005] 而在对称方法中必须保证：不仅接收方而且发送方都具有相同密钥。在此，相关密钥管理一般是要求非常高的任务。在移动无线电领域中，密钥例如借助于SIM卡被引入移动电话中并且相关网络于是可以给SIM卡的明确标识分配相应密钥。而在无线局域网(LAN)的情况下，在设立网络时通常进行要使用的密钥的人工输入(一般来说通过输入口令)。不过，当例如在传感器网络或者其它机器到机器通信系统、例如还有基于CAN的车辆网络中具有非常大数目的用户或节点时，这样的密钥管理快速地变为非常复杂并且不能实行。此外，要使用的密钥的改变常常是完全不可能的或者仅仅以非常大的花费是可能的。

[0006] 替代于用于为任意的多路访问系统、如总线系统、尤其是CAN系统生成对称密码密钥的常规密码方法，可以例如通过利用总线系统的物理特性在双方之间协商秘密信息作为共同的密钥的基础。在CAN总线的情况下的在此情况下所观察到的攻击者模型例如可以规定，攻击者仅仅通过传统CAN控制器具有对总线的访问。这尤其意味着，攻击者既不能测量

总线上的电压变化，也不能测量总线上的电流变化，或者完全不能在总线的两点之间测量这些电压或电流变化，也就是说，攻击者不具有对总线的直接的、任意物理的访问。

[0007] 当前，典型地不在CAN总线上使用密码方法。在其它总线系统中，在应用层中、但典型地不在处于该应用层之下的层中部分地使用常规密码方法。这样的方法大多需要公开密钥基础设施，以便中央地存储所有参与者的公开密钥(非对称方法)。在对称方法的情况下，各合法方将相同密钥用于加密和解密。对称密钥必须以替代的、安全的方式被协商或通知，例如通过在生产期间烧录(Einbrennen)到存储器中或者通过在受保护环境(车间等等)中进行调整。

[0008] 但是如所提到的那样对称密钥也可以通过相同通信信道来协商，其方式是，使用该信道的物理特性。这样的方法应当确保：即使整个通信在总线上被第三方窃听，也仅参与方知道该密钥。

[0009] 在DE 10 2015 207220中，网络、例如CAN总线的两个用户例如很大程度上同时通过共同的传输信道发送数据。该方法使用如下事实：在如下数据总线的情况下，该信号在有些情况下不允许推断出两个同时发送的信号，该数据总线在多路访问的情况下显示出所述信号的与运算(AND-Verknüpfung)。然而由于两个发送方知道其自己的所发送的信号，因此两个发送方可以从自该总线读回的总信号中“减去”该信号，并且这样确定对方站的发送信号。从该文献中同样可以得知，用户规定其传输的例如随机选择的时间延迟(抖动)，以便使从外部观察传输介质的攻击者从用户的传播时间差中获得关于该秘密的信息变得困难。

[0010] 不过，对于根据DE 10 2015 207220的方法，在CAN总线的情况下必须以如下形式改变总线控制器：尽管冲突被识别(这是，当双方或更多方同时发送并且因此相互干扰时)，但是该总线控制器继续发送并且不中断传输，如这否则在具有冲突探测的介质访问控制协议中是常见的。例如，在CAN总线的情况下，如下控制器通常暂时撤回其传输：该控制器的(隐性)位在仲裁阶段期间被其它发送方的显性位覆写了。如果在仲裁阶段之后发生冲突并且由此出现错误，则分组被总线用户解释为无效的。

[0011] 另一现有技术是应用在CAN总线上的所谓的“CANcrypt”方法(″CANcrypt technical functionality, February 26th, 2016, A summary of the technical features used by CANcrypt″, 在2016年4月26日以网址 http://www.esacademy.com/blog/2016/02/26/cancrypt-functionality/调用)。在此，双方确定随机延迟，根据该随机延迟，双方分别发送具有随机地来自两个可能的所选择的标识(ID)的一个标识的短数据分组或者将所述短数据分组设置用于发送。相应分组的发送不必直接彼此重叠地进行，不过在所定义的时间帧之内进行。在此，所述数据分组有意地不包含关于相应发送者的信息。在相同标识的情况下，传输不被用于秘密生成。在相应传输的不同标识的情况下，根据哪方已经首先发送了分组，这被双方解释和规定为预定密钥位(“1”或“0”)。尽管如此，(在发送时被战胜的)另一方此后仍然通过总线发送其所设置的分组。在双方随机地或有意地在码元持续时间/位持续时间内恰好同时发送的情况下，在CAN帧的仲裁阶段中在总线上看到如下方的ID：该方首先相对于另一方的隐性位发送显性位。另一方的CAN控制器识别到：其位被覆写为显性的，并且中断传输，使得第一方的分组无错误地处于总线上。紧接着，占优势方的CAN控制器不受干扰地发送其CAN帧。该方法与DE 10 2015 207220的方法相比具有如下优点：不需要CAN控制器中的改变。但是该方法为此与DE 10 2015 207220的方法相比明显

更低效，因为该方法针对每个所协商的位通过总线发送至少两个有效的分组。

发明内容

[0012] 提出方法，利用所述方法可以高效地在网络的两个或更多个用户之间生成秘密，而跟踪网络中的通信的第三方不能以简单的方式获悉该秘密。

[0013] 为此提出，为了在至少具有第一用户和第二用户的网络中生成秘密，第一用户和第二用户分别在网络的共同的传输介质上设置消息传输，并且第一用户和第二用户分别根据所述用户中的哪个在消息传输中已经使用了从至少两个消息标识中选择的哪个消息标识来生成在第一用户与第二用户之间分享的秘密。第一用户和第二用户为其相应消息传输从多于两个消息标识中随机地选择消息标识(ID)。

[0014] 虽然在网络中节约地分派消息标识是广泛流行的基本原理并且针对用于秘密生成的方法建议尽可能小的数目的所使用的标识。所描述的方法利用两个标识是可能的并且根据该基本原理实际上以该数目也应当够用。

[0015] 不过认识到了，在这样减小的数量的标识的情况下，可能发生在实践中干扰性地高数目的冲突或仅能以花费来解决的状况。因此，提出使用多于两个标识、尤其是仅仅一个标识组中的四个或更多个标识、或者分别具有至少两个标识的两组标识。通过方法的这样被提高的复杂度，也使干扰该方法或者导出秘密对于攻击者来说变得困难。

[0016] 在一个优选设计方案中，用户分别使用分别具有至少两个标识的至少两个标识组，首先选择要使用的组，然后随机地从中选择要使用的标识。标识组的选择优选地在用户之间协调地进行，尤其是协调地进行，使得每个用户分别使用一个或多个与其它用户不同的标识组。在该设计方案的一个特别优选的变型方案中，标识组的选择在用户中根据一个或多个已经在用户之间生成的秘密来进行。这例如可以通过如下方式来进行：用户在第一阶段中分别利用预定的或所协商的标识组来生成秘密，直到在用户之间生成了一个秘密或确定数目的秘密，并且在第二阶段中基于至少一个共同的秘密来确定：所述至少两组中的哪组在相应用户中被用于下一秘密生成。

[0017] 在所描述的、用户协调地使用彼此不同的标识组(并且因此不同的标识)的变型方案中，这些组有利地在用户中被选择，使得尽管所述标识组在两个用户中是相同的，但用户不再能够随机地选择相同的标识。用户优选地定期地重新、例如针对每个时间窗选择所使用的组。在一时间窗中，每个用户例如传输用于秘密生成的消息。在两个用户都已经发送了消息之后，时间窗也可以在实际时间期满之前结束。如果一时间窗的时间期满并且用户中的至少一个还未发送消息，则可以确定错误情况并且通过例如发送控制消息进行错误处理。

[0018] 因此，攻击者不能基于标识进一步推断出发送方，因为两个用户原则上都有具有相同标识的相同组可供使用。由于在用户之间对不同标识组的协调选择优选地基于用户之间的先前的共同的秘密进行，因此攻击者也不能从中导出：哪个用户使用哪组标识。

[0019] 但是由此使两个用户能够不仅特别安全地、而且此外还特别高效地构成秘密生成。为此，两个用户可以分别进行其消息传输以用于秘密生成，必要时不考虑固定的时间栅格(Zeitraster)或固定的时间窗。通过由于明确地不同的标识而不再能够发生冲突，节点不必等待确定时间段的期满或者对方的冲突或确认消息，而是可以在先前的秘密生成的两

个消息传输结束时分别进行用于秘密生成的消息传输。各两个相继的消息传输(第一用户的一个和第二用户的一个)被用于秘密生成。

[0020] 为了秘密生成本身可以规定,在确定的标识组合的情况下生成秘密(对应于在使用仅仅两个标识时不同标识的情况)或者不生成秘密(对应于在使用仅仅两个标识时相同标识的情况)。为此,可以将一个组的标识指派给确定的值。例如,在两个具有各两个标识的组的情况下分别将每组的一个标识指派给逻辑“0”,并且将每组的一个标识指派给逻辑“1”。如果相同逻辑值的两个标识相遇(“0”,“0”或“1”,“1”),则不生成秘密。这尤其是进行,以便知道标识的含义的攻击者不能利用该知识。如果不同逻辑值的两个标识相遇(“0”,“1”或“1”,“0”),则根据哪个用户已经发送了标识中的哪个来生成秘密。

[0021] 在不同标识的这样的设计方案中,用于秘密生成的消息传输也可以一起传输附加的有效数据或控制信息,因为不必担心冲突。控制信息尤其是也可以又加速进一步的秘密生成。

[0022] 在该方法的一个变型方案中,用户在使用明确地不同的标识的情况下也可以彼此独立地、优选地分别如其目前可能的那样快地进行其消息传输。由此该方法再次变得更快和更高效。于是,秘密生成在用户中最大限度地进行到如下程度,即用户中的较慢者已经促使了相应的消息传输(因为为了秘密生成,第一用户的第x个消息传输被分配给第二用户的第x个消息传输)。

[0023] 在该方法的一个优选设计方案中,在用户之间将预定的或所协商的时间窗用于秘密生成,在所述时间窗中用户交换确定数目的消息帧。在该变型方案中,相应秘密优选地在时间窗结束时在用户中生成,其方式是,分别将第一用户的第x个消息传输分配给第二用户的第x个消息传输。在交换数目为2xN的消息的情况下,于是从中可以最大限度地生成N个秘密。为了将该方法构成为尽可能安全的,用户为此可以分别针对每个消息传输使用不同标识组。标识(组)的选择优选地再次在用户之间例如基于用户之间的先前的共同的秘密协调地进行。如果两个用户的所约定的消息传输结束了,则为此设置的时间窗优选地被视为结束(即使在实际时间期满之前),并且必要时可以设置用于秘密生成的下一时间窗的自动开始。如果时间窗的时间期满并且用户中的至少一个还未发送所约定的数目的消息,则优选地确定错误情况并且通过例如发送控制消息来执行错误处理。

[0024] 所描述的方法可以特别良好地在CAN、TTCAN或CAN-FD总线系统中实施。这里,隐性总线电平被显性总线电平排挤。用户的值或信号的叠加因此遵循所规定的规则,用户可以将所述规则用于从叠加的值或信号以及由其所传输的值或信号中导出信息。其它通信系统、如LIN和I2C也良好地适合于使用这些方法。

[0025] 网络或网络的用户为此被设立,其方式是,其具有执行相应方法的步骤的电子存储和计算资源。在这样的用户的存储介质上或者在网络的分布式存储资源上,也可以存放计算机程序,该计算机程序被设立用于在该计算机程序在用户中或者在网络中被处理时执行相应方法的所有步骤。

附图说明

[0026] 随后参考附图并按照实施例进一步描述本发明。在此,图1和图2示例性地示出用于在第一和第二阶段中在网络的两个用户之间进行秘密或密钥生成的示例性方法的流程。

具体实施方式

[0027] 本发明涉及一种用于在通信系统的两个节点(网络的用户)之间生成秘密、如(秘密的)对称密码密钥的方法,所述节点通过共同使用的介质(网络的传输信道)彼此通信。在此,秘密、尤其是密码密钥的生成或协商基于两个用户之间的公开数据交换,其中但是可能的窃听的第三方作为攻击者还是不能或仅能非常困难地推断出所生成的密钥。

[0028] 利用本发明因此可以在网络的两个不同用户之间完全自动化地并且安全地建立相应对称密码密钥,以便在此基础上于是实现确定的安全功能、诸如数据加密。如还要详细描述的,为此首先建立共同的秘密,该秘密可以被用于密钥生成。但是这样的共同的秘密原则上也可以被用于与用于较窄意义上的密码密钥相比、例如与一次性密码本(One-Time-Pad)相比不同的目的。

[0029] 本发明适合于大量有线或无线以及光网络或通信系统、尤其是还适合于如下网络或通信系统:在所述网络或通信系统的情况下,不同用户通过线性总线彼此通信并且对该总线的介质访问借助于逐位总线仲裁来进行。该原理例如是广泛流行的CAN总线的基础。本发明的可能的使用领域与此相应地尤其是还包括基于CAN的车辆网络以及自动化技术中的基于CAN的网络。

[0030] 在图1和图2中示出了所提出的方法的示例性流程。图1尤其是示出该方法的第一阶段,在该第一阶段中用户分别使用相同的标识组或ID组。图2尤其是示出该方法的第二阶段,在该第二阶段中用户针对一个或多个时间窗排他地使用ID组。哪个用户使用哪些ID组从迄今为止的秘密中导出。这里,该方法示例性地按照CAN总线通信来解释。

[0031] 网络的第一用户100发起密钥生成(未在图1中示出),例如其方式是,第一用户将消息(分组、例如CAN帧)发送给网络的第二用户200并且必要时将参数通知该第二用户,所述参数可以由第二用户200保存。该消息的结束例如同时是一时间窗的开始,该时间窗的长度例如在初始分组中被通知了。该时间窗的开始也可以被通知给第二用户,或者由该第二用户根据所得到的消息来确定。替代地,也可以在用户之间协商用于执行该方法的时间窗。

[0032] 两个用户100和200现在在第一步骤中分别随机地从例如$n>2$种可能性(ID A,ID B,ID 1,ID 2)中确定CAN ID以及根据设计方案分别确定处于该时间帧之内的随机延迟(Δt)。在此,CAN ID被选择,使得所述CAN ID不允许推断出使用所述CAN ID的用户。原则上双方在其相应的延迟期满之后打算发送CAN帧。在一个优选的设计方案中,在此涉及具有除了标识(CAN ID)之外相同的内容和相同的类型的CAN帧。

[0033] 对总线线路的电流或电压不具有直接访问的第三方不能基于介质的总线特性来区分:哪个用户已经发送了CAN帧,因为在CAN帧中未包含关于此的信息。由于即使在最坏情况下在总线上的信号传播时间也明显短于一个位/码元的持续时间,因此在该方法中尤其是可能出现三种情况:

1. 两个用户之一首先利用第一消息标识进行发送,并且另一用户稍后利用第二消息标识进行发送。在图1中,用户100已经随机地确定了时间延迟t1,以及从第一标识组ID set 1中随机地选择了标识ID A。用户200已经随机地确定了时间延迟t2,以及从该标识组ID set 1中随机地选择了标识ID B。为此,用户100和200例如可以已经同意选用确定的标识组,或者首先使用的标识组是预定的。该组ID set 1例如仅仅包括标识ID A和ID B。

[0034] 用户100由于较小的时间延迟t1在图1中首先发送。基于事先规定的协定，由用户根据哪个用户已经发送了哪个消息标识这一事实来确定秘密、尤其是密钥位。例如，当第一用户100已经使用了第一标识ID A并且第二用户200已经使用了第二标识ID B时，在两个用户中生成的秘密是密钥位‘1’，并且当第一用户100已经使用了ID B并且第二用户已经使用了ID A时，秘密是密钥位‘0’。因此，在图1的情况下，在消息传输之后在两个用户中生成相同的秘密S1、即密钥位‘1’。在相同标识的情况下，不生成秘密。因此，该第一秘密的生成结束。

[0035] 根据该第一秘密S1，现在可以如图2中所示的那样确定：哪个标识组在下一时间窗中被使用。这样，为用户100又选择第一标识组ID set 1(ID A，ID B)，不过为用户200选择第二标识组ID set 2(具有标识ID C，ID D)，其中所述组分别包含不同标识。针对下一秘密生成，用户100现在选择来自组ID set 1的标识ID A和延迟t3，并且用户200选择来自组ID set 2的标识ID D和延迟t4。根据哪个用户已经发送了哪些标识，现在在两个用户中产生秘密S2。该秘密或者S1和S2的组合现在可以然后再次被用于在用户中选择标识组。

[0036] 2．两个用户100和200想要同时发送。两个用户附加地已经随机地选择了不同的标识。同时的发送愿望因此可能由于未曾使用随机延迟或者因为发送时刻随机地为相同的或者因为总线曾被占用而引起。在发送时，用户之一100或200将基于CAN协议和其中已知的仲裁规则而实现传输。另一用户紧接着发送。在不同标识(IDA，ID B)的情况下，秘密又根据哪个用户已经发送了哪个标识来生成。针对紧接着的时间窗对标识组的选择可以如在情况1下那样进行。

[0037] 3．两个用户100和200设置在相同时刻的传输，并且也相应地同时执行所述传输。两个用户附加地已经随机地选择了相同的标识。用户100和200的相同CAN帧将重叠。用户从中什么也没有领会。这种情况尤其是仅仅在该方法的阶段1中出现，在该阶段1中用户使用相同的标识。这种情况尤其是在显性/隐性地起作用的多路访问系统、如CAN总线中出现。这种情况现在优选地通过如下方式被捕获：在该时间帧之内在总线上读取了仅仅一个分组。两个用户都探测到这一点，并且不生成密钥位。由此，在下一秘密生成时不能根据之前生成的秘密从不同标识组中进行选择。因此，继续使用商定或预定的标识组(图1中的ID set 1)。因此，该方法优选地一直停留在阶段1中，直到至少一个秘密被生成了。

[0038] 在一个优选的变型方案中，在从一组的多于两个、尤其是至少四个标识中进行选择时，情况2的概率与不期望的情况3相比被明显提高。附加地使攻击者对该方法的可观察性变得困难。

[0039] 如果用户的标识如在上面描述的示例中那样在第一个成功的秘密生成之后从不同标识组中被选择，使得在两个用户之间不可能出现相同的标识，则从该时刻起仅情况1和2可能存在，但是不期望的情况3不可能存在。

[0040] 在一个替代的变型方案中，在用户之间对不同标识组的选择还实现放弃用于各个秘密生成的时间窗或时间栅格，所述选择导致用户之间的明确地不同的标识。用户于是可以交替地在没有所规定的时间窗的情况下或者彼此独立地在用于生成多个秘密的时间窗中设置其消息传输。

[0041] 因此，在所描述的设计方案中，首先在用户之间生成秘密(例如在使用预定标识组的情况下)。然后根据该秘密在用户中间协调地确定：哪个用户在下一秘密生成时使用(来

自多个标识组的)哪个组。这进行,使得即使在从所述组中随机选择的情况下在用户之间也不可能出现相同的标识。上面的示例中的标识ID A、ID B、ID C和ID D优选地是分别不同的标识。

[0042] 不仅在不同的具有标识的组的情况下而且在一组具有多于两个标识的变型方案中为两个用户所知的是,标识的哪个组合导致秘密生成,以及哪个组合不导致秘密生成。例如,在所提及的标识中ID A和ID C可以被分配给值“0”并且ID B和ID D可以被分配给值“1”,并且可以规定:仅仅不同值的标识的组合被用于秘密生成。

[0043] 为了生成密钥,可以多次重复用于生成秘密的该方法。

[0044] 下面解释对所描述的方法的进一步的补充和修改。

[0045] 所介绍的方法是一种用于在网络的两个用户或节点之间生成对称密码密钥的方案。该方案尤其是适合于无线、有线和光通信系统、尤其是适合于CAN、TTCAN、CAN-FD、LIN、I2C。

[0046] 原则上,实现(如上所述的)显性和隐性位的区分、但是不限于该区分的所有通信系统都特别适合于使用。这里所描述的方法因此可以在大量无线、有线和光通信系统的情况下被使用。在此,特别感兴趣的是所描述的方案用于机器到机器通信、即用于不同传感器、执行器等等之间的数据传输,所述传感器、执行器等等一般而言仅仅具有非常有限的资源并且可能不能以合理的花费人工地在现场进行配置。

[0047] 例如在家庭和楼宇自动化、远程医疗、车到X系统或工业自动化技术中存在另外的使用可能性。在具有无线电接口的未来最小传感器中以及在CAN总线的所有应用领域、即尤其是车辆联网或自动化技术中的使用也是特别感兴趣的。

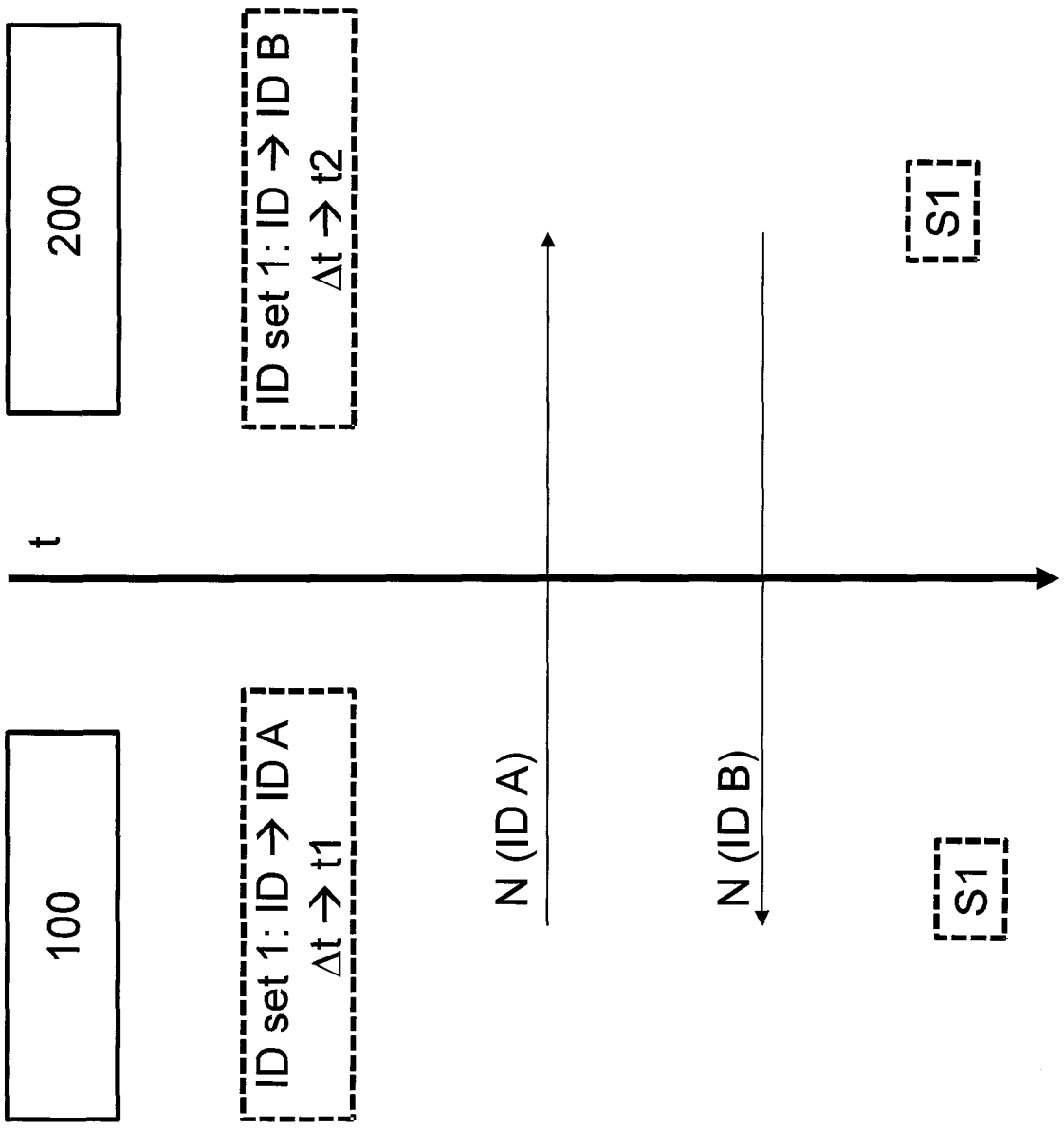


图 1

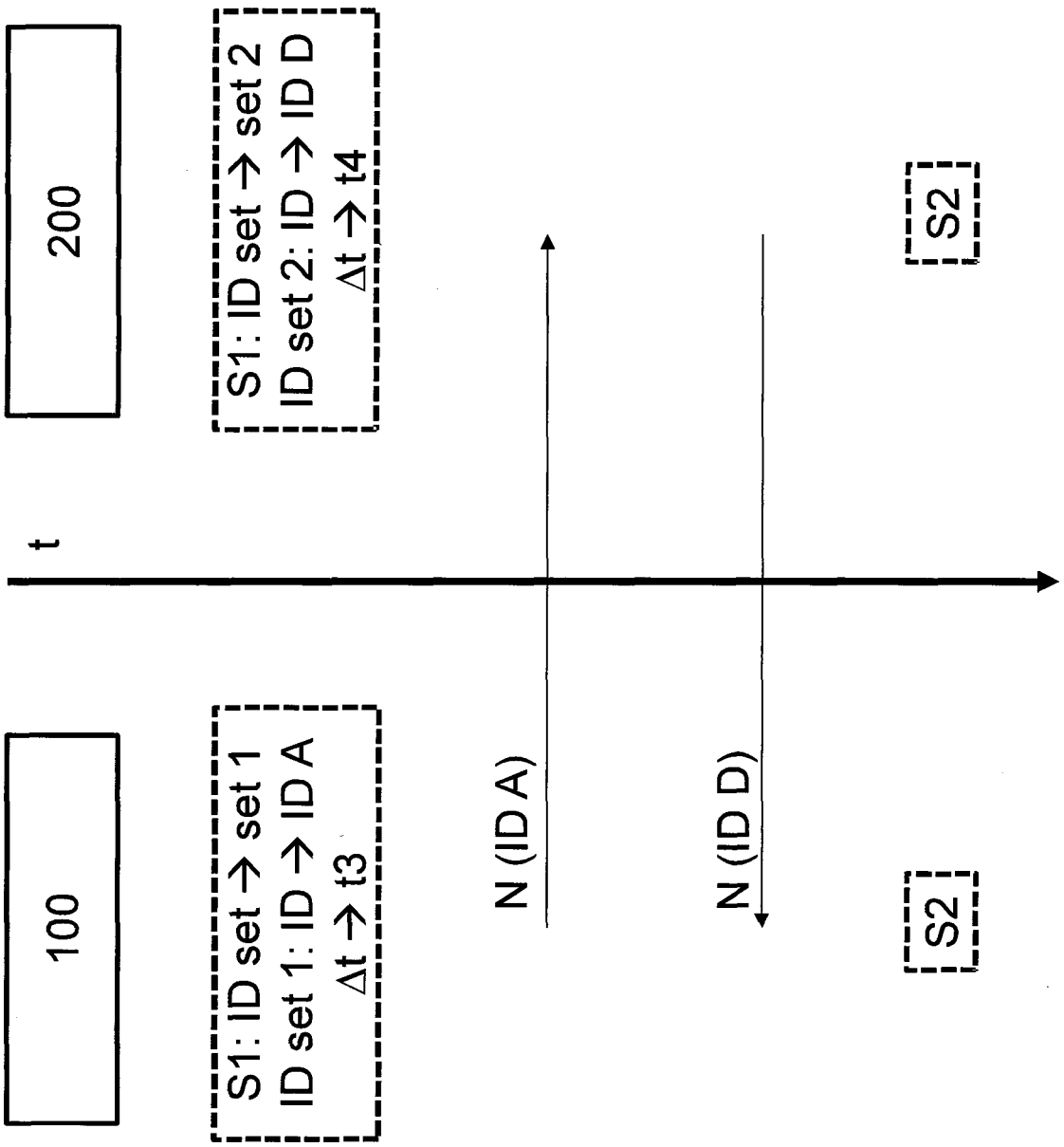

200
S1: ID set → set 2
ID set 2: ID → ID D
Δt → t4
S2
t
100
S1: ID set → set 1
ID set 1: ID → ID A
Δt → t3
N (ID A)
N (ID D)
S2

图 2