



(12)发明专利申请

(10)申请公布号 CN 107624229 A

(43)申请公布日 2018.01.23

(21)申请号 201680029361.6

(22)申请日 2016.04.13

(30)优先权数据

102015209496.0 2015.05.22 DE

(85)PCT国际申请进入国家阶段日

2017.11.21

(86)PCT国际申请的申请数据

PCT/EP2016/058103 2016.04.13

(87)PCT国际申请的公布数据

W02016/188667 DE 2016.12.01

(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 T.洛特施派希 A.米勒

(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)

权利要求书2页 说明书11页 附图4页

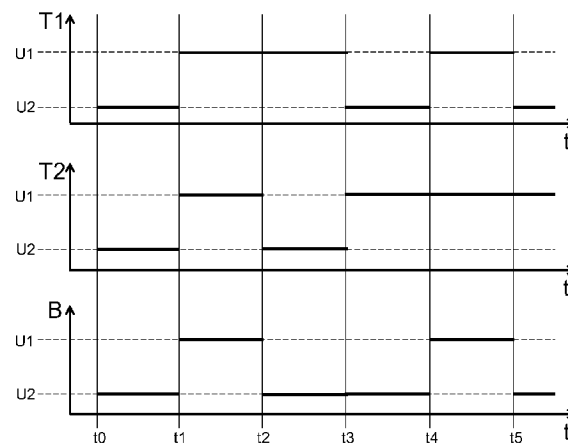
(54)发明名称

用于在网络中产生机密或密钥的方法

(57)摘要

提出一种用于在网络中生成机密或密钥的方法。在此所述网络具有至少一个第一和第二用户与在至少所述第一和第二用户之间的共同的传输通道。第一用户能够将至少一个第一和第二值提供到所述传输通道上并且第二用户能够将至少所述第一值和第二值提供到所述传输通道上,其中第一用户促使第一用户值序列并且第二用户促使第二用户值序列彼此尽可能同步地在所述传输通道上传输,并且第一用户基于关于第一用户值序列的信息以及基于由第一用户值序列与第二用户值序列在所述传输通道上的叠加所产生的叠加值序列并且第二用户基于关于第二用户值序列的信息以及基于由第一用户值序列与第二用户值序列在所述传输通道上的叠加所产生的叠加值序列分别生成共同的机密或共同的密钥。至少第一用户在第一用户值序列之外或第二用户在第二用户值序列之外以确定的间隔或根据所探测的叠加值序列来将至少一个填

充值提供到所述传输通道上,使得实现在所述传输通道上的边沿变换或值变换。



1. 用于在网络(20)中生成机密或密钥的方法,其中所述网络(30)具有至少一个第一用户(21)和第二用户(22)与在所述至少一个第一用户(21)和第二用户(22)之间的共同的传输通道(30),其中第一用户(21)能够将至少一个第一值(1)和第二值(0)提供到所述传输通道(30)上并且第二用户(22)能够将至少所述第一值(1)和第二值(0)提供到所述传输通道(30)上,其中第一用户(21)促使第一用户值序列并且第二用户(22)促使第二用户值序列彼此尽可能同步地在所述传输通道(30)上传输,并且第一用户(21)基于关于第一用户值序列的信息以及基于由第一用户值序列与第二用户值序列在所述传输通道(30)上的叠加所产生的叠加值序列并且第二用户(22)基于关于第二用户值序列的信息以及基于由第一用户值序列与第二用户值序列在所述传输通道(30)上的叠加所产生的叠加值序列分别生成共同的机密或共同的密钥,其特征在于,至少第一用户(21)在第一用户值序列之外或第二用户(22)在第二用户值序列之外以确定的间隔或根据所探测的叠加值序列来将至少一个填充值提供到所述传输通道(30)上,使得实现在所述传输通道(30)上的边沿变换或值变换。

2. 根据权利要求1所述的方法,其特征在于,第一用户(21)和第二用户(22)中的仅仅一个将所述填充值提供到所述传输通道(30)上并且第一用户(21)和第二用户(22)中的另外的用户探测所述填充值。

3. 根据权利要求2所述的方法,其特征在于,所述另外的用户借助所探测的填充值确定同步信息。

4. 根据权利要求1所述的方法,其特征在于,第一用户(21)在第一用户值序列之外将至少一个第一填充值提供到所述传输通道上并且第二用户(22)对此在第二用户值序列之外尽可能同步地将至少一个第二填充值提供到所述传输通道上,使得通过所述至少一个第一填充值和所述至少一个第二填充值的叠加实现所述传输通道上的边沿变换或值变换。

5. 根据前述权利要求之一所述的方法,其特征在于,如果由至少第一用户(21)或第二用户(22)探测到具有预先确定数量的相同值的叠加值序列,则至少第一用户(21)或第二用户(22)将所述填充值提供到所述传输通道(33)上。

6. 根据权利要求5所述的方法,其特征在于,如果探测到具有预先确定数量的相同值的叠加值序列,就将所述填充值直接作为下个值提供到所述传输通道(30)上。

7. 根据权利要求5所述的方法,其特征在于,在探测到具有预先确定数量的相同值的叠加值序列之后,延迟确实数量个值地将所述填充值提供到所述传输通道(30)上。

8. 根据权利要求5至7之一所述的方法,其特征在于,所述填充值与所探测的相同的值逆反。

9. 根据权利要求7所述的方法,其特征在于,所述填充值以固定的预先给定的间隔、特别是分别在提供到通道上的用户值序列的预先确定数量的值之后被提供到所述传输通道(30)上。

10. 根据前述权利要求之一所述的方法,其特征在于,至少两个填充值被提供到所述传输通道(30)上。

11. 根据权利要求10所述的方法,其特征在于,所述两个填充值包含值变换。

12. 根据前述权利要求之一所述的方法,其特征在于,如果不仅第一用户(21)而且第二用户(22)促使第一值(0)在所述传输通道(30)上的传输,则在所述传输通道(30)上出现对应于第一值(0)的状态,并且如果第一用户(21)或第二用户(22)或者如果两个用户(21、22)

促使第二值在所述传输通道(30)上的传输,则在所述传输通道(30)上出现对应于第二值(1)的状态。

13.根据前述权利要求之一所述的方法,其特征在于,第一用户值序列在第一用户(21)中并且第二用户值序列在第二用户(22)中本地地特别是借助随机发生器或伪随机发生器来产生。

14.根据前述权利要求之一所述的方法,其特征在于,所述至少一个第一填充值和所述至少一个第二填充值不被考虑用来生成共同的机密或共同的密钥。

15.用于在网络(20)的第一用户(21)中生成机密或密钥的方法,其中第一用户(21)被设立用于通过传输通道(30)从网络(20)的至少一个第二用户(22)接收信息以及将信息传输到所述第二用户(22),其中第一用户(21)被设立用于能够将至少一个第一值和第二值提供到所述传输通道(30)上并且能够在所述传输通道上对其进行探测,其中第一用户(21)促使第一用户值序列与由第二用户(22)传输第二用户值序列尽可能同步地在所述传输通道(30)上进行传输,并且其中第一用户(21)基于关于第一用户值序列的信息以及基于在所述传输通道(30)上由第一用户值序列与第二用户值序列的叠加所产生的叠加值序列来生成机密或密钥,其特征在于,第一用户(21)在第一用户值序列之外以确定的间隔或根据所探测的叠加值序列来将至少一个第一填充值提供到所述传输通道(30)上,使得实现在所述传输通道上的边沿变换或值变换。

16.根据前述权利要求之一所述的方法,其特征在于,所述网络(20)是CAN、TTCAN、CAN-FD、LIN或I2C总线系统,第一值(1)是隐性总线电平并且第二值(0)是显性总线电平。

17.根据权利要求1至15之一所述的方法,其特征在于,在所述网络(20)中设置二进制振幅键控来进行数据传输。

18.具有至少一个第一用户(21)和第二用户(22)和传输通道(30)的网络(20),通过所述传输通道(30),第一用户(21)与第二用户(22)能够进行通信,其特征在于,所述网络(20)包括用于执行根据权利要求1至17之一所述的方法的所有步骤的机构。

19.一种设备,其被设立用于作为网络(20)上的用户(21)来执行根据权利要求15所述的方法的所有步骤。

20.一种计算机程序,其被设立用于执行根据权利要求1至17之一所述的方法之一的所有步骤。

21.一种机器可读的存储介质,具有在其上存储的根据权利要求20所述的计算机程序。

用于在网络中产生机密或密钥的方法

技术领域

[0001] 本发明涉及一种用于在网络中产生机密或机密的加密密钥的方法,特别是在网络的两个用户中产生共同的机密密钥。点对点的连接通常也属于网络并且在此应该同样利用该概念来寻址。在此,两个用户通过共同使用的传输介质来进行通信。在这种情况下,逻辑位序列(或一般:值序列)通过相应的传输方法作为信号或信号序列物理传输。所基于的通信系统例如可以是CAN总线。该CAN总线规定显性位和隐性位或者相应显性信号和隐性信号的传输,其中网络的用户的显性信号或位相对于隐性信号或位得以贯彻。相应于隐性信号的状态仅当所有参与的用户都规定隐性信号来进行传输或当所有同时进行发送的用户传输隐性信号电平时才在传输介质上出现。

背景技术

[0002] 不同设备之间的安全通信在增多联网的世界中越来越重要并且在多个应用领域中是用于接受的重要前提并且因此也是相应应用的经济成果。这根据应用包括不同的保护目标、诸如待传输的数据的机密的保持、所参与的节点的相互认证或数据完整性的确保。

[0003] 为了实现这些保护目标,通常使用合适的加密方法,所述加密方法通常可以细分成两个不同的类别:一方面对称方法,其中发送方和接收方具有相同的加密密钥,另一方面非对称方法,其中发送方利用接收方的公开(即也可能为潜在的攻击方所知)密钥来加密待传输的数据,但是仅利用所属的私钥才能进行解密,该私钥理想情况下仅为接收方已知。

[0004] 非对称方法特别是具有以下缺点,即非对称方法通常具有很高的计算复杂度。因此,非对称方法仅有条件地适用于资源受限的节点、诸如传感器、执行器或诸如此类的,所述节点通常仅具有相应小的计算功率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该能量高效地工作。此外,通常仅仅受限的带宽可用于数据传输,这使得具有2048位或还更多位的长度的非对称密钥的交换不具有吸引力。

[0005] 而在对称方法中必须保证,不仅接收方而且发送方具有相同的密钥。所属的密钥管理在此通常是要求很高的任务。在移动无线电的领域中,密钥例如借助SIM卡引入到移动电话中并且所属的网络然后可以将相应密钥分配给SIM卡的明确标记。而在无线LAN的情况下,通常在网络的装置中进行待使用的密钥的手动输入(通常通过输入密码)。然而,当例如在传感器网络或其他机器对机器通信系统、例如还有基于CAN的车辆网络中具有非常大量的节点时,这样的密钥管理快速变得非常耗费的和不适用的。此外,待使用的密钥的变化通常根本是不可能的或仅仅以很大的耗费而可行。

[0006] 用于相对于操纵来保护传感器数据的方法和例如在机动车网络中借助常见的加密方法来确保交易认证例如在DE 102009002396 A1中和在DE 102009045133 A1中公开。

[0007] 此外,自从一段时间以来,在关键词“物理层安全”下研究和开发新型方案,借助所述新型方案可以自动地基于所参与的节点之间的传输通道的物理特性来产生用于对称方法的密钥。在此充分利用这些传输通道的交互性和固有的随机性。然而,特别是在线连接的或光学系统中,该方案通常仅仅有条件地适合,因为相应的通道通常仅仅具有非常受限的

时间变化性并且攻击方例如可以借助建模相对好地推断出发送方和接收方之间的通道参数。在分布式系统中基于所连接的单元的通道特性的受保护的通信的这样的方法例如在未预先公开的申请DE 10 2014 208975 A1以及DE 10 2014 209042 A1中予以描述。

[0008] 用于在控制器局域网络(CAN)中和在CAN-FD中进行位填充的方法例如从DE 10 2011 080476 A1中可知。

[0009] 未预先公开的DE 10 2015 207220 A1公开了一种用于借助两个通信用户之间的公开讨论来产生共同的机密或机密的对称密钥的方法。

发明内容

[0010] 根据独立权利要求的用于生成机密或加密密钥的方法绝对不要求手动干预并且因此能够实现两个节点之间的安全通信关系或连接的自动建立。此外,所述方法具有很低的复杂度,特别是关于所需要的硬件设计、诸如所需的存储器资源和计算功率,并且所述方法伴随着少的能量和时间需求。此外,所述方法在同时很小的错误概率的情况下提供很高的密钥生成率。

[0011] 在此,所述方法从以下出发,即网络中的用户通过通信通道彼此通信。所述方法在此借助传输通道上的物理信号传输特别是逻辑值序列(如果涉及二进制逻辑,则是位序列)。即使通过信号、即在物理层面上进行传输通道上的可能的叠加,在本说明书中在下文中首先考虑逻辑层面。因此考虑所传输的逻辑值序列以及其逻辑叠加。

[0012] 因此,网络的用户可以将第一信号(其例如分配给逻辑位“1”)和第二信号(其例如分配给逻辑位“0”)提供到通信通道上并且在通信通道上探测到所产生的信号。如果现在两个用户(尽可能)同时分别传输一个信号序列,则用户可以在通信通道上探测到由此产生的叠加。通信通道上的由两个(无关)信号的(尽可能)同时传输而有效产生的信号然后又可以分配给一个(或多个)确定的逻辑值。

[0013] 在此,传输就以下这点而言必须是尽可能同步的,即在传输介质上进行信号序列的各个信号的叠加,特别是相应于第一用户的第n逻辑值或位的信号与相应于第二用户的第n逻辑值或位的信号至少部分地叠加。为此,该叠加应该分别是足够长的,使得用户能够检测到叠加或确定相应的叠加值。

[0014] 叠加在此可以通过仲裁机制或通过物理信号叠加来确定。仲裁机制例如指的是以下情况,即一个节点想要施加隐性电平,但是在总线上探测到显性电平并且因此搁置传输。在该情况下不发生两个信号的物理传输,而是仅显性信号在传输通道上可见。

[0015] 然后用户可以由叠加的所产生的值序列和自身的值序列生成相对于外部攻击方是机密的密钥。其原因在于,例如可以窃听在共同使用的传输介质上施加的有效的总信号的外部攻击方仅仅看到值序列的叠加,但是不具有关于用户的各个值序列的信息。因此用户具有更多的信息,所述用户可以使用所述信息相对于攻击方来产生机密密钥。

[0016] 如果所描述的方法在没有附加措施的情况下用在确定的系统、诸如CAN中,则可能发生,相同位或信号电平的相对长的序列施加在共同使用的传输介质(例如CAN总线)上。然后,这又可以导致位填充错误和/或同步损失,这必要时促使其他节点来发送特定的错误消息(“错误帧”)并且中断过程。为了避免这,但却尽可能与当今已经可用的收发机和控制器兼容而提出,扩展所描述的用于密钥生成的方法,使得防止位填充错误和/或同步损失并且

因此提高所述密钥建立方法与当今已经可用的标准部件的兼容性。

[0017] 对此提出,参与密钥生成的用户站在其用户值序列之外、即除了其用户值序列之外还将至少一个填充值提供到共同的传输通道上,使得产生边沿变换或值变换(例如在二进制系统中0到1或1到0的位变换)。这可以通过用户站中的仅仅一个来进行。但是,在一种优选的设计方案中,由两个用户站尽可能同步地将填充值提供到传输通道上,使得由填充值的叠加信号产生边沿变换或值变换。

[0018] 在此,填充值以确定的间隔(即特别是在值序列的确定数量的单个值之后)或根据所探测的叠加值序列而被提供到传输通道上。

[0019] 在一种优选的实施方案中,如果用户分别探测到具有预先确定数量的相同值的叠加值序列,则所述用户将填充值提供到传输通道上。在此,填充值优选地与所探测的相同值逆反。因为填充位或填充值通常提高通信协议的管理费用并且因此降低密钥建立的效率,所以有利的是,仅仅当实际上超过确定数量的值重复时才设置这样的填充值,这在此借助叠加序列来探测。

[0020] 如果用户能够是属于此类的,则填充值与叠加值序列中的所探测数量的相同值直接相邻地提供到传输通道上。在该变型中,待探测的数量可以恰好被置于相同值的允许的最大数量上,使得确实仅仅在填充值是必需的情况下插入填充值。在其他情况下,也可以以用于探测值重复的数量的预先确定的间隔来插入填充值,其中所述数量于是应该相应地低于最大数量地来选择。由此尽管产生更高的管理费用,但是该方法是要求没那么高的(特别是关于用户的硬件要求)并且能够是更可靠的。

[0021] 为了还更简单地执行并且因此与现有的通信系统和用户硬件特别兼容,有一种替代的实施方式,其中填充值始终由用户以固定的预先确定的间隔插入,特别是在传输通道上的预先确定数量的所探测的值之后插入,而不必是相同的值。在此,优选地插入两个填充值,所述两个填充值已经包含值变换或边沿变换(例如由两个用户插入位序列01或由两个用户插入位序列10)。

[0022] 特别有利地,该方法可以用在以下网络中,在该网络中存在显性值(物理上:显性信号)和隐性值(物理上:隐性信号),当仅仅一个用户将该显性值施加在传输通道上时该显性值得以贯彻,仅仅当两个或所有用户传输隐性值时才在传输通道上产生该隐性值。基于就此清楚设置的叠加规则,这样的网络的用户可以从所产生的叠加序列特别简单地导出用于密钥生成的信息。替代地,用户站中至少一个用户站的隐性值的传输也可以通过以下方式代替,即在值序列的该位置处或作为至少两个可能的值之一什么都不传输。

[0023] 由用户尽可能同时地提供到传输通道上的用户值序列在相应的用户本身中在前字段中借助随机发生器或伪随机发生器来产生。因为传输通道上的所产生的叠加序列能够对于潜在的攻击方是可得到的,所以对于之后通信的安全性特别有利的是,使攻击方尽可能困难地推断出用户的各个值序列,即这些值序列在用户中本地地以及随机地或至少伪随机地产生。

[0024] 所描述的方法可以特别好地在CAN、TTCAN或CAN-FD总线系统中实现。在此,隐性总线电平由显性总线电平来抑制。因此,用户的值或信号的叠加遵循确定的规则,用户可以使用所述规则来从叠加的值或信号和由用户传输的值或信号导出信息。所述方法也良好地适用于其他通信系统、如LIN和I2C。

[0025] 替代地,但是该方法例如也可以用在具有二进制振幅键控的网络中。在此,同样通过以下方式确定叠加,即当用户之一或用户中的两个进行传输时用户作为信号“传输”和“无传输”来供选择并且叠加信号对应于信号“传输”,并且当两个用户不进行传输时,叠加信号对应于信号“无传输”。

[0026] 在该方法针对网络中的两个用户进行描述时,也已经可以通过网络的一个用户从自身的信号序列和从自身的信号序列与第二用户的信号序列的叠加导出机密密钥。对此,网络或网络的用户通过其具有电子存储器资源和计算资源的方式而被设立用于实施相应方法的步骤。在这样的用户的存储介质上或在网络的分布式存储器资源上也可以保存计算机程序,该计算机程序被设立用于当其在用户中或在网络中处理时实施相应方法的所有步骤。

附图说明

[0027] 随后参考附图并且借助实施例详细描述本发明。在此:

图1示意性示出示例性的所基于的通信系统的构造,

图2示意性示出线性总线作为所基于的通信系统的示例,

图3示意性示出网络的两个用户的示例性的信号序列以及在用户之间的传输通道上的所产生的叠加值序列,以及

图4示意性示出用于在网络的两个用户之间生成密钥的示例性方法的流程。

具体实施方式

[0028] 本发明涉及一种用于在通信系统的两个节点(网络的用户)之间生成共同的机密或(机密的)对称加密密钥的方法,所述两个节点通过共同使用的介质(网络的传输通道)来相互通信。加密密钥的生成或协定在此基于两个用户之间的公开数据交换,其中但是尽管如此作为攻击方的可能的进行窃听的第三方不能或仅能很困难地推断出所生成的密钥。因此利用本发明能够在网络的两个不同用户之间完全自动地并且安全地建立相应的对称加密密钥,以便然后基于所述密钥实现确定的安全功能、诸如数据加密。如细节上还要描述的那样,对此首先建立共同的机密,该共同的机密可以被考虑用于密钥生成。但是,这样的共同的机密原则上也可以为了其他目的而用作较窄意义上的加密密钥,例如用作一次性密钥。

[0029] 本发明适合于大量线连接的或无线的以及还有光学的网络或通信系统、特别是还有这样的,其中不同的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按位的总线仲裁来实现。该原理例如是广泛流行的CAN总线的基础。本发明的可能的应用领域特别是也相应地包括基于CAN的车辆网络以及自动化技术中的基于CAN的网络。

[0030] 本发明描述一种方案,利用该方案可以在网络中或特别是在网络的两个节点之间自动生成对称的加密密钥。该生成在此在充分利用相应传输层的特性的情况下实现。但是,不同于在“物理层安全”的常见方案中那样,为此不分析传输通道的物理参数、如传输强度等。更确切地说,对此在所参与的节点之间存在公开的数据交换,该数据交换由于通信系统的和/或所使用的调制方法的特性不能或不充分地作为可能的进行窃听的攻击方实现对由此协定的密钥的推断。

[0031] 在下文中考虑如在图1中抽象示出的装置。在此,不同的用户2、3和4可以通过所谓的共享的传输介质(“共享介质”)10彼此通信。在本发明的一种有利的构型中,该共享的传输介质对应于如例如在图2中示出的线性总线(线连接的或光学的)30。图2中的网络20由作为共享传输介质(例如作为线连接的传输通道)的恰好该线性总线30、用户或节点21、22和23以及(可选的)总线终端31和32构成。

[0032] 在下文中针对不同节点21、22和23之间的通信而假设:所述通信的特征在于显性值和隐性值的区分。在该示例中,作为可能的值而采用位“0”和“1”。在此,显性位(例如逻辑位‘0’)可以一定程度上抑制或覆写同时传输的隐性位(例如逻辑位‘1’)。

[0033] 针对这样的传输方法的示例是所谓的二进制键控(二进制振幅键控),其中恰好区分两个传输状态:在第一情况(值‘0n’或“0”)下传输例如简单的载波信号形式的信号,在另外的情况(值‘0ff’或“1”)下不传输信号。状态‘0n’在此是显性的,而状态‘0ff’是隐性的。

[0034] 支持显性位和隐性位的所述区分的相应的通信系统的另一示例是基于按位的如例如在CAN总线中所使用的总线仲裁的(线连接的或光学的)系统。基础理念在此同样在于,如果例如两个节点想要同时传输信号并且一个节点传输‘1’,而第二节点发送‘0’,则‘0’“获胜”(即显性位),即能够在总线上测量到的信号电平对应于逻辑‘0’。在CAN中,该机制特别是用于解决可能的冲突。在此,首先传输较高优先级的消息(即具有较早的显性信号电平的消息),其方式是,每个节点在传输其CAN标识符时同时按位地监视总线上的信号电平。如果节点自身传输隐性位,但是在总线上探测到显性位,则相应的节点在有利于较高优先级的消息(具有较早的显性位的消息)的情况下中断其传输企图。

[0035] 显性位与隐性位的区分允许将共享传输介质理解成一种二进制运算器,该二进制运算器借助逻辑与函数相互连接不同的输入位(=所有同时传输的位)。

[0036] 在图3中例如示出用户1(T1)如何准备好位序列0,1,1,0,1来通过传输通道在时间点t0和t5之间进行发送。用户2(T2)准备好位序列0,1,0,1,1来通过传输通道在时间点t0和t5之间进行发送。利用通信系统的上述特性和假设在该示例中位电平“0”是显性位的情况下,在总线(B)上可见位序列0,1,0,0,1。仅在时间点t1和t2之间以及在t4和t5之间,不仅用户1(T1)而且用户2(T2)设置隐性位“1”,使得仅在这里逻辑与连接导致总线(B)上的为“1”的位电平。

[0037] 在充分利用通信系统的传输方法的该特性的情况下,现在可以通过以下方式在相应网络的两个用户之间进行密钥生成,即用户在传输介质上探测两个用户的位序列的叠加并且由该信息与关于自身发送的位序列的信息一起来产生共同的(对称的)机密密钥。

[0038] 在下文中借助图4来解释示例性的特别优选的实现方案。

[0039] 用于生成对称密钥对的过程在步骤41中从在该示例中两个参与的节点(用户1和用户2)之一开始。这例如可以通过发送特定的消息或特定的消息头来实现。

[0040] 不仅用户1而且用户2在步骤42中首先本地(即内部地并且彼此无关地)生成位序列。优选地,该位序列是作为该方法的结果所期望的共同密钥的至少两倍长、特别是至少三倍长。位序列优选地分别作为随机的或伪随机的位序列例如借助合适的随机数发生器或伪随机数发生器来产生。

[0041] 针对20位长度的本地位序列的示例:

-用户1的所产生的位序列: $S_{11} = 01001101110010110010$

- 用户2的所产生的位序列: $S_{T2} = 10010001101101001011$ 。

[0042] 在步骤43中,用户1和用户2彼此(尽可能)同步地通过共享传输介质传输其分别产生的位序列(在使用具有显性位和隐性位的传输方法的情况下,如之前已经解释的那样)。在此可以设想用于同步相应传输的不同可能性。因此,例如或者用户1或者用户2可以首先将合适的同步消息发送到分别另外的节点并且在紧接着该消息的完全传输的确定的持续时间之后然后开始真正的位序列的传输。但是同样也可以设想的是,由两个节点之一仅传输合适的消息头(例如由仲裁字段和控制字段构成的CAN头)并且在所属的有效载荷阶段期间于是两个节点同时(尽可能)同步地传递其生成的位序列。在方法的一种变型中,用户的在步骤42中生成的位序列也可以在步骤43中分布到多个消息上来传输,例如当这使相应消息的(最大)长度必需时如此。也在该变型中,又(尽可能)同步地进行另外的用户的分布到相应多个、相应长的消息上的位序列的传输。

[0043] 然后,在共享传输介质上,两个位序列叠加,其中基于具有显性位和隐性位的区分的系统的之前所要求的特性,用户1和用户2的各个位得出叠加,在所提及的示例中实际上是连接。因此在传输通道上得出相应的叠加,例如进行窃听的第三方用户可以探测到该叠加。

[0044] 针对上面本地位序列的叠加位序列的示例:

- 传输通道上的有效位序列: $S_{eff} = S_{T1}$ 与 $S_{T2} = 000000001100000000010$ 。

[0045] 不仅用户1而且用户2在传输其步骤43的位序列期间在并行的步骤44中探测共享传输介质上的有效的(叠加的)位序列 S_{eff} 。对于CAN总线的示例,这即使在常规系统中在仲裁阶段期间本来通常也这样做。

[0046] 对于具有‘二进制键控’的系统(无线的、线连接的或光学的),这相应地同样可能。在这种情况下,特别是以下对实践可实现性有好处,即在这样的系统中状态‘On’是显性的并且状态‘Off’是隐性的(如之前已经解释的那样)。因此,节点即使在没有测量的情况下也知道,只要该节点本身已经发送显性位,在“共享介质”上的有效状态就是显性的。而如果节点已经发送隐性位,则该节点首先并非毫无困难地识别共享传输介质上的状态,然而该节点在该情况下可以通过合适的测量来确定,该状态看起来如何。因为节点本身在该情况下不进行发送,所以也就是不存在具有所谓的自干扰的问题,否则该自干扰特别在无线系统的情况下将使耗费的回声补偿必需。

[0047] 在下一步骤45中,不仅用户1而且用户2同样又(尽可能)同步地传输其初始位序列 S_{T1} 和 S_{T2} ,然而这次进行逆反。相应传输的同步在此又可以恰好与上面描述的相同的方式来实现。在共享通信介质上,两个序列然后又彼此进行与连接。用户1和用户2又确定共享传输介质上的有效的叠加的位序列 S_{eff} 。

[0048] 针对上面位序列的示例:

- 用户1的逆反的位序列: $S_{T1}' = 10110010001101001101$

- 用户2的逆反的位序列: $S_{T2}' = 01101110010010110100$

- 通道上的有效的叠加的位序列: $S_{eff}' = S_{T1}'$ 与 $S_{T2}' = 00100010000000000100$ 。

[0049] 不仅用户1而且用户2在传输其现在逆反的位序列期间于是又确定共享传输介质上的有效的叠加的位序列。因此,在该时间点,两个节点(用户1和用户2)以及还有可能的对共享传输介质上的通信进行窃听的攻击方(例如用户3)了解有效的叠加的位序列 S_{eff} 和

S_{eff}' 。但是与攻击方或第三用户相对,用户1还了解其初始产生的本地位序列 S_{T1} 并且用户2了解其初始产生的本地位序列 S_{T2} 。但是,用户1又不了解用户2的初始产生的本地位序列并且用户2不了解用户1的初始产生的本地位序列。又在传输期间在步骤46中进行叠加位序列的探测。

[0050] 替代于所述示例性的实施变型,用户1和用户2也可以将其逆反的本地位序列直接与其原始的本地位序列一起或直接在其原始的本地位序列之后进行发送,即步骤45和46与步骤43和44一起进行。原始的和逆反的位序列在此可以在一个消息中,但是也可以在作为部分位序列的分开的消息中传递。

[0051] 在步骤47中,用户1和用户2现在分别本地地(即内部地)特别是利用逻辑或函数来连接有效的叠加的位序列(S_{eff} 和 S_{eff}')。

[0052] 针对上面位序列的示例: $S_{ges} = S_{eff}$ 或 $S_{eff}' = 00100011100000000110$ 。

[0053] 由或连接产生的位序列(S_{ges})中的各个位现在说明, S_{T1} 和 S_{T2} 的相应位是相同的还是不同的。如果 S_{ges} 内的第n位例如是‘0’,则这意味着, S_{T1} 内的第n位与 S_{T2} 内的相应位是逆反的。一样地适用:如果 S_{ges} 内的第n位是‘1’,则 S_{Alice} 和 S_{Bob} 内的相应位是相同的。

[0054] 然后,用户1和用户2在步骤48中基于从或连接获得的位序列 S_{ges} 在其原始的初始位序列 S_{T1} 和 S_{T2} 中删去在两个序列中相同的所有位。因此,这导致相应缩短的位序列。

[0055] 针对上面位序列的示例:

- 用户1的缩短的位序列: $S_{T1,v} = 01011100101100$
- 用户2的缩短的位序列: $S_{T2,v} = 10100011010011$ 。

[0056] 所产生的缩短的位序列 $S_{T1,v}$ 和 $S_{T2,v}$ 现在恰好是彼此逆反的。因此,两个用户之一可以通过逆反其缩短的位序列而精确地确定那个如在另外的用户中已经存在的缩短的位序列。

[0057] 这样共同存在的缩短的位序列现在由用户1和用户2在步骤49中分别本地地以合适的方式进行整理,以便生成所期望长度N的实际期望的密钥。在这种情况下又存在能够如何进行该整理的多种可能性。一种可能性是从共同存在的缩短的位序列中选择N位,其中必须清楚定义哪N个位可以选取,例如其方式是,总是简单地选择序列的前N位。同样可能的是关于共同存在的缩短的位序列的哈希函数的计算,其提供长度N的哈希值。相当普遍地,可以利用每个任意的线性和非线性函数来进行整理,该函数在应用于共同存在的缩短的位序列的情况下返回长度N位的位序列。由共同存在的缩短的位序列来产生密钥的机制优选地在两个用户1和2中相同地存在并且相应地以相同的方式来执行。

[0058] 接着密钥生成必要时还可以进行校验,由用户1和2生成的密钥实际上是相同的。对此,例如可以计算关于所生成的密钥的检验和并且在用户1和2之间进行交换。如果两个检验和是不同的,则某些东西明显是失败的。在该情况下可以重复所描述的方法来进行密钥生成。

[0059] 在用于密钥生成的方法的一种优选的变型中,在不同的遍历中也可以首先产生所得的在用户1和2中分别存在的缩短的位序列的一个完整系列,然后该完整系列在实际的密钥由此导出之前被组合成唯一的长的序列。如果在所描述的的程序的一次遍历之后例如共同的缩短的位序列的长度例如应该小于所期望的密钥长度N,则可以在实际的密钥导出之前

通过重新遍历来生成例如另外的位。

[0060] 所生成的对称密钥对现在可以仅仅由用户1和用户2结合所建立的(对称的)加密方法、诸如用于数据加密的密码来使用。

[0061] 特别是借助逻辑或函数连接两个叠加部分值序列的目标是可以进行以下那些位的删除,被动的对通信进行观察的攻击方也可以毫无困难地基于其观察来确定所述位。一种对此的替代方案是保留这些位,但是为此首先生成比所期望的明显更多的位(即如果例如期望128位的机密或密钥,则首先产生300位)并且所述位于是最后例如借助哈希函数或诸如此类的来减小到所期望的长度。

[0062] 可能的攻击方(例如用户3)可以窃听用户1和用户2之间的公开的数据传输并且因此如所描述那样获得有效的叠加的位序列(S_{eff} 和 S_{eff}')的知识。然而,攻击方于是因此仅仅知道用户1和2的本地生成的位序列中的哪些位是相同的和哪些位是不同的。此外,在相同的位的情况下,攻击方甚至还能够确定在此是‘1’还是‘0’。但是,对于所产生的缩短的位序列(和因此用于密钥生成的基础)的完整知识,攻击方缺少关于不同的位的信息。为了进一步加难攻击方的可能的攻击,在一种优选的变型中在用户1和2的原始的本地产生的位序列中附加地删除相同的位值。因此用户3仅仅具有根本不用于密钥生成的信息。尽管用户3知道相应缩短的位序列从用户1和2的本地位序列之间的不同的位来产生。但是用户3不知道用户1和用户2分别已经发送哪些位。

[0063] 用户1和用户2除了关于叠加的总位序列的信息之外还具有关于分别由其发送的本地产生的位序列的信息。由相对于仅仅跟踪公开的数据传输的用户3的所述信息优势而造成以下事实,即在用户1和2中生成的密钥尽管公开的数据传输作为基础仍保持机密。

[0064] 利用用于密钥生成的所描述的方法而能够发生,相同的位或信号电平的相对长的序列在由用户1和2同时传输时有效地施加在传输通道上。这建立在以下基础上,即两个用户首先彼此无关地生成随机的位序列,但是在通道上分别仅仅有效地存在所述位序列的叠加。在假设显性位为0并且隐性位为1的情况下,这例如可以是利用与连接组合的位序列。因为两个用户不了解分别另外的用户的随机产生的位序列,所以首先可能总是出现,有效的位序列具有近似任意长的子序列,所述子序列具有相同的依次的位。这可能在确定的通信系统中在使用标准硬件和软件的情况下又是有问题的,这在下文中应该示例性地以CAN为例来详细解释。

[0065] CAN协议规定,在N=5个依次的相同值的位之后必须将具有互补值的所谓的‘填充位’插入到实际待传输的位序列中,该填充位在接收方处又自动被去除。因此,所述‘填充位’不是信息位,而是具有以下背景:

1) 具有大于N=5个依次的相同值的位的位序列被用于控制目的(例如作为“帧结束”指示或作为“错误帧”)并且因此必须被保证,使得这样的序列不出现在实际的信息部分中。

2) CAN使用不归零编码来传输CAN消息。然而这由于不同节点中的不完美同步的时钟而有利于同步损失,因此在传输或接收CAN消息期间必须执行时间上的再同步,以便能够将对硬件的要求保持地少(例如对本地振荡器的要求)。通过引入‘填充位’,最晚在N=5个依次的位之后进行边沿变换,该边沿变换于是可以用于这样的再同步。

[0066] 如果‘位填充规则’在CAN中被违背,则发现该违背的所有用户立即传输‘错误标识’(=6或更多个依次的显性位)并且因此尝试中断过程。于是,这又防止利用上面简短概述

的方法来成功建立对称的加密密钥。

[0067] 因此,在下文中提出所描述方法的扩展,借助所述扩展能够避免位填充错误,使得例如在CAN的情况下不由于这样的错误而从另外的节点发送‘错误标识’。因此同时可以保证,定期的时间再同步通过通信系统的用户是可能的并且因此可以减少同步错误的概率。根据通信系统的种类和类型,两个方面可能是重要的或其中仅仅一个方面是重要的。

[0068] 通过引入合适的‘填充位’应该防止,多于N个依次的位具有相同的值。然而,这不能通过针对各个用户的传输调节而与其用户无关地实现,因为在所描述的方法中视叠加值序列的相应边沿变换或值变换而定。对此提出不同的可能性。

[0069] 在第一优选的设计方案中充分利用:第一和第二用户在用于密钥生成的所描述的方法中在步骤43中在同步传输随机的位序列期间本来总是在并行步骤44中探测在共同使用的传输介质上的有效的信号电平(或有效的位序列)。在这种情况下,如果节点确定传输介质上的有效的位值N个依次的总是相同,则两个节点发送填充位作为下一位,该填充位于N个依次存在的有效位逆反。因此,与常规位填充的主要区别是,是否必须插入填充位的决定不最初取决于自身的消息或位序列,而是仅仅取决于共同使用的传输介质上的有效的位序列。相同的适用于填充位的应该被发送的值。

[0070] 示例:

用户1的随机的初始的(本地产生的)位序列: 011010110110101

用户2的随机的初始的(本地产生的)位序列: 010100001111011

传输介质上的在单个序列的逻辑与连接的情况下的在没有填充位下的有效位序列:
010000000110001

如果N=5(诸如在CAN中),则因此存在一个填充错误,因为在传输介质上存在7个依次的有效位值‘0’。

[0071] 而利用根据第一实施例的上面提出的方案,下面的位序列实际上将存在于传输介质上: 01000000100110001

带下划线的位在此是附加引入的位,该位在用户1和用户2五次探测到共同的传输介质上的位‘0’之后由用户1和用户2来插入和发送。因此,针对该示例,Alice和Bob的实际发送的位序列看起来如下:

用户1的实际发送的位序列: 0110101110110101

用户2的实际发送的位序列: 0101000101111011

因此,相较于用户1和2的上面的随机和本地产生的初始的位序列,相应的填充位(在此:1)插入在位置8处。

[0072] 在第二优选的设计方案中考虑:在一些通信系统中对于用户必要时可能困难(例如由于使用成本适宜的简单的硬件)的是,在探测到传输介质上的N个相同的依次的位的序列之后立即插入填充位(如上所示),因为不仅位的探测而且下个位的传输的准备根据实施需要一点时间并且因此可能不能足够快地进行反应。在这样的情况下可以调整第一实施例的方案,使得在探测到共同使用的传输介质上的N-M($1 \leq M \leq N-2$)个相同的依次的有效位之后已经准备填充位的引入,但是实际上从探测到(至少)N-M个相同的依次位的序列的第一位起计算着在传输N个位之后才发送该填充位。

[0073] 在一种特别鲁棒的变型中,只有当在N-M个相同的位之后并且在传输填充位之前在共同的传输介质上进行(有效的)位变换并且因此实际上不存在填充错误时,才发送该准备的填充位(因为在该情况下即使没有填充位在传输介质上也将不存在多于N个的相同的位)。这也导致有效的位序列(没有填充错误),然而在该情况下由于(在此实际上不必需的)填充位而具有较大的管理费用。

[0074] 示例(N=5,M=2):

首先假设:用户1和2的初始的生成的位序列与第一实施变型的示例相同,即:

用户1的随机的初始的(本地产生的)位序列:011010110110101

用户2的随机的初始的(本地产生的)位序列:010100001111011

传输介质上的在单个序列的逻辑与连接的情况下的在没有填充位下的有效位序列:
010000000110001

但是在传输中,不仅Alice而且Bob在传输位5之后将探测到在共同使用的传输介质上形成N-M=3个依次的相同的位并且然后准备在位置8处插入填充位(具有值‘1’)。

[0075] 因此,实际上由Alice和Bob传输的位序列对应于(类似于之前):

用户1的实际发送的位序列:0110101110110101

用户2的实际发送的位序列:0101000010111011

由此得出在传输介质上实际存在的位序列:01000000100110001

带下划线的位在此又是附加引入的位,该位在用户1和用户2在位5之后三次探测到共同的传输介质上的位‘0’之后由用户1和用户2来插入和发送。因此,在此也将不再出现位填充错误(其中N=5)并且恰好具有与之前的示例中相同的结果。然而,不仅用户1而且用户2利用更多的时间来准备填充位的插入或传输。

[0076] 根据第三优选的实施例的用于避免填充错误和/或同步损失的方法是与实际的信息位无关地、即与用户序列无关并且与所探测的叠加序列无关地周期地强制进行位或边沿变换。这可以设计成,使得不仅用户1而且用户2总是在传输K(具有 $K < N$)个信息位(=初始随机产生的位)之后插入两个填充位,所述两个填充位在叠加时导致位或边沿变换。在确定的通信系统、如CAN中,对此两个填充位已经可以包含位变换,例如或者位序列‘01’或者‘10’,使得叠加同样产生位序列‘01’或‘10’。插入这两个可能的情况中的哪个,在该示例中不重要,只要保证不仅用户1而且用户2总是插入相同的序列。

[0077] 该实施变型导致相对高的管理费用,但是能够十分鲁棒并且不耗费地实现并且也可以特别好地利用现有的标准部件来执行。

[0078] 示例(N=5,K=4):

首先假设:用户1和2的初始的生成的位序列与第一和第二实施变型的示例中相同,即:

用户1的随机的初始的(本地产生的)位序列:011010110110101

用户2的随机的初始的(本地产生的)位序列:010100001111011

传输介质上的在单个序列的逻辑与连接的情况下的在没有填充位下的有效位序列:
010000000110001

然而,现在总是在K=4个位之后由用户1以及用户2与信息位无关地插入位序列‘01’。因此,用户1和用户2的实际待传输的位序列得出为:

用户1的实际待传输的位序列: 011001101101011001101

用户2的实际待传输的位序列: 0101010000001111101011

因此得出在共同的传输介质上的以下的有效位序列: 010001000001011001001

因此在该情况下也不出现填充错误(其中N=5)。

[0079] 与使用所描述的方案中的哪个无关地,填充位本身优选地在接收方侧被丢弃。填充位特别是不共同用作生成对称的加密密钥的基础,以便防止由于在密钥生成中考虑非随机的结构而减弱密钥。

[0080] 方法的所描述的实施方式也可以在一种替代的设计方案中被改型,使得填充值(填充位)不是由两个用户提供到共同的传输介质上,而是两个用户中的仅仅一个生成并且输出填充值。该方法具有以下优点,即用户可以通过该值序列彼此再同步。对于该替代方案,用户之一优选地被确定用于传输填充值。这例如可以是以下那个用户,该用户发起密钥生成,或者是(例如通过配置)预先确定的用户。另外的用户探测填充值并且例如可以根据该填充值获得同步信息。特别是可以借助至少一个填充值来探测到其时钟与另外的用户的时钟的可能的时间偏差并且基于该确定的偏差而进行其时钟的再同步。

[0081] 所提出的方法是一种用于在充分利用位传输层的特性的情况下来在两个节点之间生成对称的加密密钥的方案。该方案特别是适用于线连接的或光学的通信系统,只要所述通信系统支持‘二进制键控’或按位的总线仲裁(例如CAN、TTCAN、CAN-FD、LIN、I2C)。但是在无线的(基于无线电的)通信系统中也可以使用该方案,所述通信系统优选地具有在发送方和接收方之间的很短的距离和可能的直接的视线传播。

[0082] 原则上,(如上所述那样)能够实现显性位和隐性位区分的所有通信系统适合于使用。因此,在此描述的方法可以用在多种无线的、线连接的和光学的通信系统中。所描述的方案在此对于机器对机器通信、即对于在不同的传感器、执行器等之间的数据传输是特别有吸引力的,所述传感器、执行器等通常仅具有十分受限的资源并且可能不能利用可替代的耗费手动地在现场进行配置。

[0083] 例如在家庭和建筑物自动化、远距医疗、汽车对X系统或工业自动化技术中存在其他应用可能性。在今后的具有无线电接口的最小传感器中以及在CAN总线的所有应用领域中、即特别是在车辆联网或自动化技术中的使用也是特别有吸引力的。

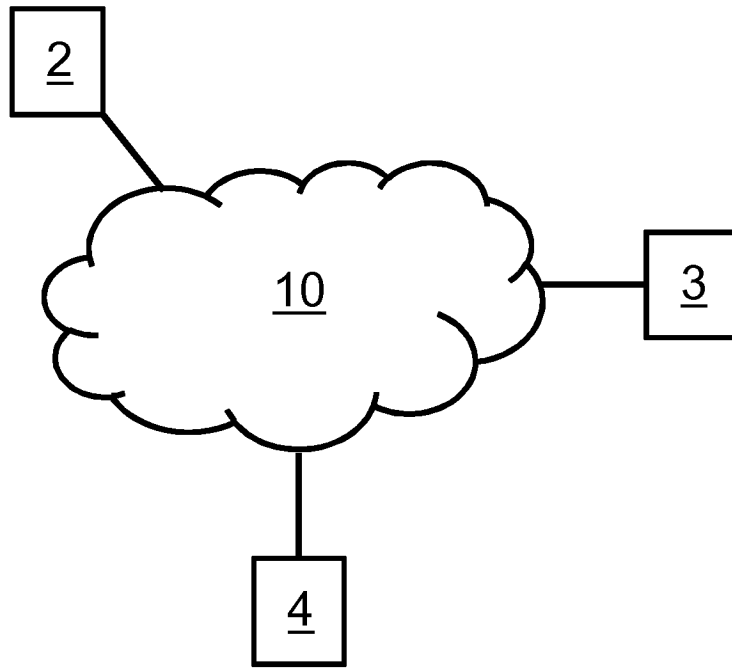


图 1

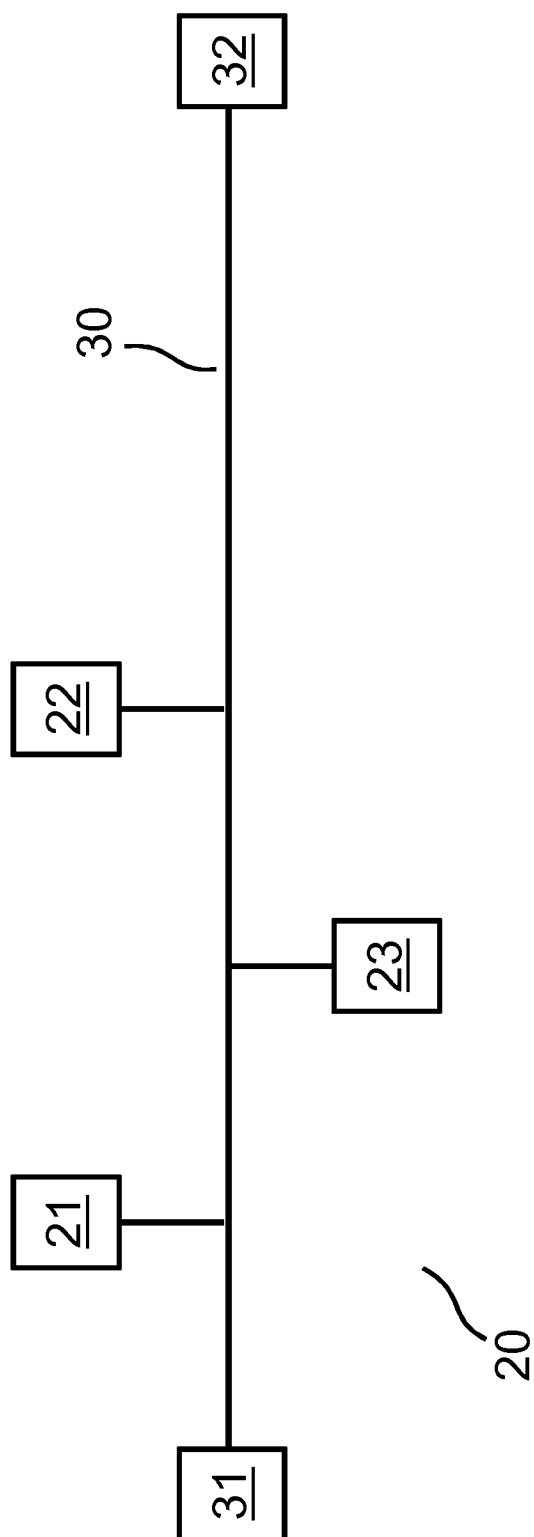


图 2

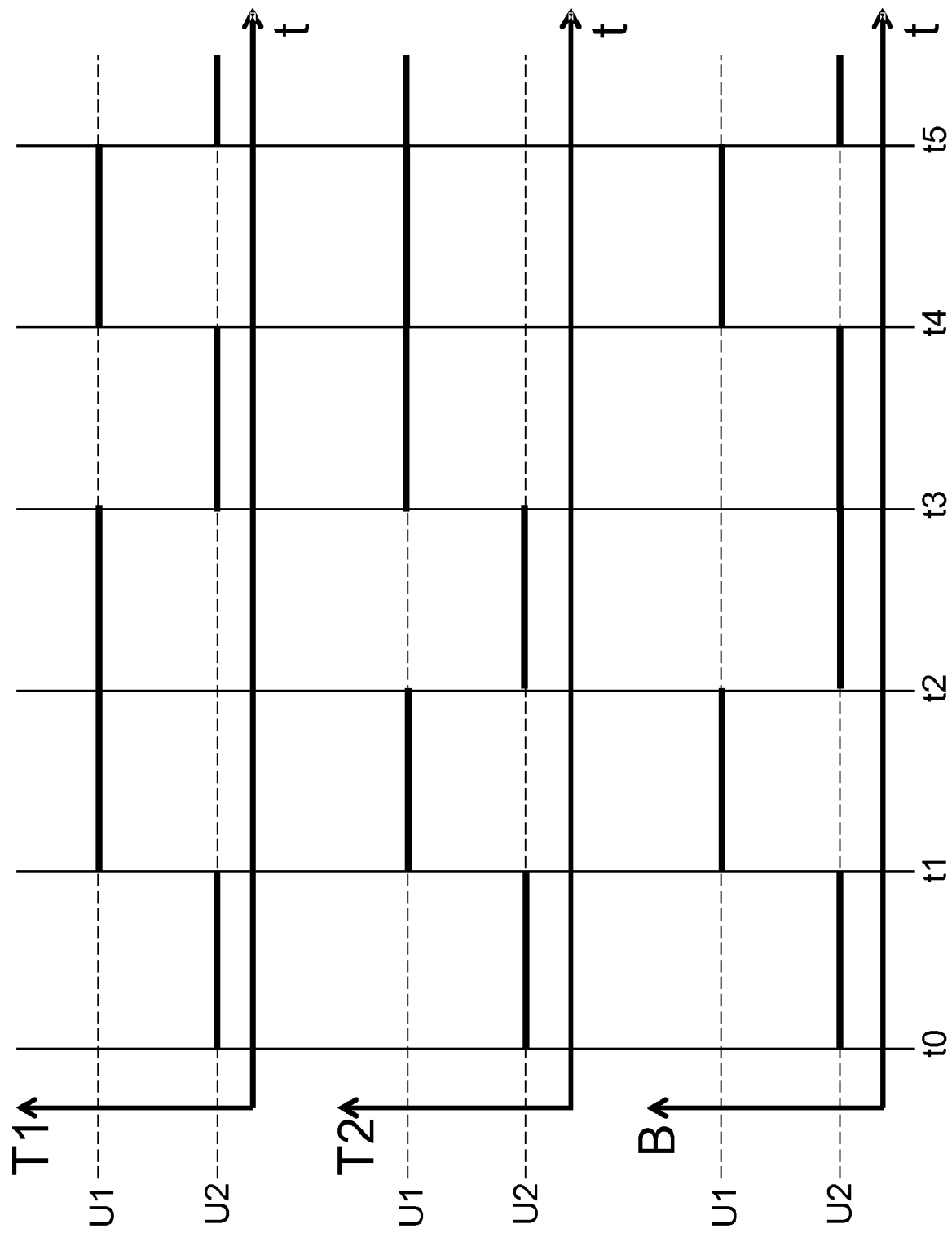


图 3

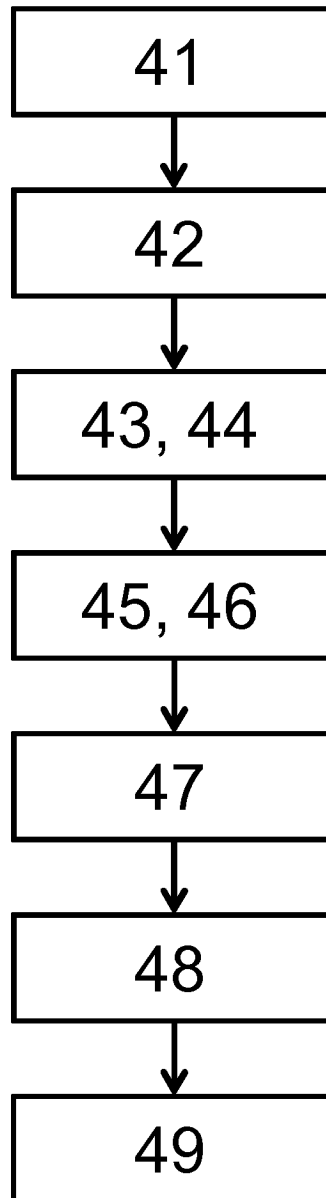


图 4