



(12)发明专利申请

(10)申请公布号 CN 107453863 A

(43)申请公布日 2017. 12. 08

(21)申请号 201710343331.9

(22)申请日 2017.05.16

(30)优先权数据

102016208451.8 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)

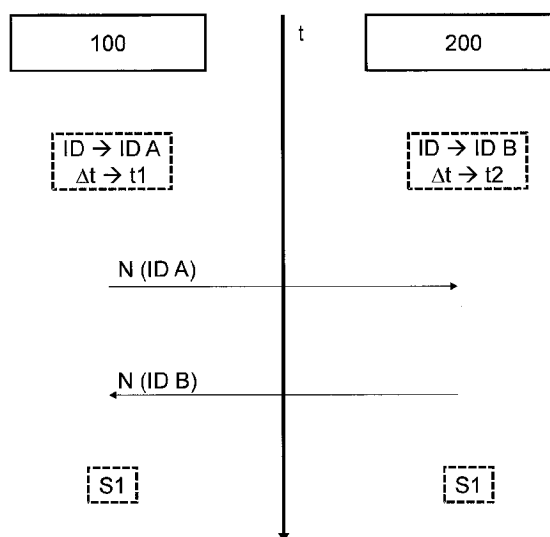
权利要求书2页 说明书6页 附图1页

(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/或第二用户(200)处理具有被提高的优先级的任务,所述任务与秘密生成相关联或是为了秘密生成所需的步骤。



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)分别在不同的消息标识的情况下根据所述第一用户(100)或所述第二用户(200)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/或所述第二用户(200)处理具有被提高的优先级的任务,所述任务与秘密生成相关联或者是为了所述秘密生成所需的步骤。

2. 根据权利要求1所述的方法,其特征在于,所述具有被提高的优先级的任务包括计算过程、存储过程、接收过程或发送过程。

3. 根据前述权利要求之一所述的方法,其特征在于,所述第一用户(100)和所述第二用户(200)中的至少一个用户具有调度器,所述调度器为所述任务指定与其它任务相比、尤其是与非安全性相关的任务相比更高的优先级。

4. 根据前述权利要求之一所述的方法,其特征在于,所述具有被提高的优先级的任务包括软件功能,所述软件功能针对具有被提高的优先级的处理被封装和/或用对被提高的优先级的指示来表征。

5. 根据前述权利要求之一所述的方法,其特征在于,与所述秘密生成相关联的消息或者为了所述秘密生成所需的所接收的消息以更高的优先级被处理。

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/或所述第二用户(200)具有通信控制器,并且与所述秘密生成相关联的消息或者为了所述秘密生成所需的消息从所述通信控制器中的提取以被提高的优先级进行。

7. 根据权利要求6所述的方法,其特征在于,为此将与所述秘密生成相关联的消息或者为了所述秘密生成所需的消息存放在接收存储器中,与另外的接收存储器相比以被提高的优先级从所述接收存储器中提取消息。

8. 根据前述权利要求之一所述的方法,其特征在于,与所述秘密生成相关联的消息或者为了所述秘密生成所需的消息尤其是在所述通信控制器中以更高的优先级被提供用于发送。

9. 根据权利要求8所述的方法,其特征在于,所述第一用户(100)和/或所述第二用户(200)具有通信控制器,并且与所述秘密生成相关联的消息或者为了所述秘密生成所需的消息被预加载在所述通信控制器中。

10. 根据权利要求9所述的方法,其特征在于,与所述秘密生成相关联的消息或者为了所述秘密生成所需的消息被加载在为此保留的输出存储器中。

11. 根据权利要求9或10之一所述的方法,其特征在于,由所述第一用户(100)和/或所述第二用户(200)尤其是根据随机数生成多个与所述秘密生成相关联的消息或者为了所述秘密生成所需的消息,并且将所述多个消息预加载到所述通信控制器中。

12. 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。

13. 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)中产生共同的密码密钥。

14. 根据权利要求13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。

15. 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。

16. 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)以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)在不同的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)处理具有被提高的优先级的任务, 所述任务与秘密生成相关联或者是为了所述秘密生成所需的步骤。

17. 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16之一所述的方法的所有步骤。

18. 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16所述的方法的所有步骤。

19. 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16之一所述的方法之一的所有步骤。

20. 一种机器可读存储介质, 具有存储在其上的根据权利要求19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,双方优选地确定随机延迟,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。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。根据哪方发送了哪个ID,这被双方解释和规定为预定密钥位(“1”或“0”)。在此,在一致的ID的情况下,不生成秘密或密钥位,并且仅仅在不一致的ID的情况下根据谁发送了两个ID中的哪个来生成秘密。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,因为该方法即使在最佳情况下针对每个所协商的位也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。

[0014] 第一和第二用户中的至少一个、优选地二者现在处理具有被增高的优先级的内部任务,所述内部任务与秘密生成相关联或是为了秘密生成所需的步骤。这尤其是可以包括,有助于秘密生成的计算过程或存储过程或者接收过程或发送过程以与其它任务相比更高的优先级被执行。

[0015] 由此,可以避免或妨碍对秘密生成的潜在攻击,在所述潜在攻击的情况下攻击者有针对性地用任务(例如通过发送消息)使参与秘密生成的两个用户之一过载并且因此可以推断出:该用户是(至少以更高概率)稍后执行其消息传输的那个用户。但是这样的趋势可以使对在用户之间所协商的秘密的攻击变得容易,并且因此是对用于秘密生成的方法的安全性的降低。

[0016] 为此,在一个优选设计方案(尤其是作为软件实现)中,用户节点中的调度器例如可以设置如下任务:所述任务与其它不与秘密生成相关联的任务相比、尤其是与不是(特别)安全性相关(即安全(Safety)或安全性(Security)相关)的任务相比、或者与其它可(关于用户节点)从外部请求的任务相比具有更高优先级。用于在相应用户节点中生成秘密的软件功能为此尤其是可以被合适地封装,以便所述软件功能可以共同地以更高优先级被处理。用于秘密生成的任务也可以用对其被提高的优先级的指示来表征。

[0017] 在另一优选设计方案中,用户节点具有通信控制器(在CAN的情况下具有CAN控制器)。该通信控制器可以通过用户的共同的传输介质提供到达的信息(或消息帧)。为了在用户中进一步处理而从通信控制器中提取现在针对涉及秘密生成的信息(消息帧)同样与确定的其它信息、尤其是非安全性相关的信息的提取相比被指定更高优先级。为此,例如可以使用不同接收存储器(例如FIFO1和FIFO2),其中被指定更高优先级的信息(消息帧)总是被存放到接收存储器之一(例如FIFO1)中,从该接收存储器中相对于其它接收存储器优先地提取信息。

[0018] 在另一优选变型方案中,涉及秘密生成的信息(或消息帧)被设置用于更快的传输。为此,尤其是可以在所打算的发送时刻之前已经将这样的信息(或消息帧)预加载到通信控制器(在CAN网络的情况下到CAN控制器)中,而这些信息(或消息帧)没有已经被发送。这例如可以通过如下方式发生:信息(消息帧)已经被存放在通信控制器的发送存储器中,但是还未设置相应的发送请求。如果在用户之一中为了秘密生成而根据随机数确定消息内容、尤其是消息标识,则可以通过产生或使用较长随机数为未来马上要传输的多个消息产生消息内容或消息标识以用于秘密生成,并且这些多个消息可以相应地被预加载在通信控制器中。为了更快地传输用于秘密生成的信息(消息帧)或者为了预加载相应信息(消息帧),用户、尤其是其通信控制器可以具有单独的、为此保留的输出存储器(例如FIFO)。

[0019] 每个时间帧必然执行更少的为了秘密生成所需的任务。由此减轻用户的计算单元的负荷,并且其余的为了秘密生成所需的任务被更快地处理。因此,这样的系统更不易受如下攻击:所述攻击的目的在于使节点满载,以便该节点延迟地发送用于秘密生成的消息。

[0020] 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。

[0021] 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

[0022] 随后参考附图并按照实施例进一步描述本发明。在此,图1示意性地示出用于网络的两个用户之间的秘密或密钥生成的示例性方法的流程。

具体实施方式

[0023] 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。

[0024] 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,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。

[0025] 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。

[0026] 在图1中示出了所提出的方法的示例性流程。这里,该方法示例性地按照CAN总线通信来解释。

[0027] 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帧的开始,该时间帧的长度例如在初始分组中被通知了。该时间帧的开始也可以被通知给第二用户200,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段。

[0028] 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)中确定CAN ID以及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。两个用户持续地还从总线接收自己的信号。

[0029] 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. 两个用户之一首先发送,并且另一用户稍后发送。

1.1) 用户随机地选择不同标识(例如ID A, ID B)。在图1中,用户100已经随机地确定了时间延迟 t_1 以及已经随机地选择了标识ID A。用户200已经随机地确定了时间延迟 t_2 以及随机地选择了标识ID B。用户100由于较小的时间延迟 t_1 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’。

1.2) 在相同标识的情况下,不生成秘密。因此,第一秘密的生成结束。

[0030] 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(ID A, ID B)。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(ID A, 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。

[0031] 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(ID A或ID B)。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。

[0032] 用户100和200中的与密钥生成相关联的任务现在在所述用户中以提高的优先级被处理。这样,尤其是为了秘密生成所接收的信息(或消息帧)可以优先地从相应用户的通信控制器中被加载,为了秘密生成所需的计算和存储过程(例如分析随机数、创建消息等等)可以加速地被处理,或者为了秘密生成要发送的信息(或消息帧)可以被预先加载在相应用户的通信控制器中以用于更快地发送。

[0033] 为了生成密钥,可以多次重复用于生成秘密的该方法。

[0034] 下面解释对所描述的方法的进一步的补充和修改。

[0035] 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。

[0036] 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。

[0037] 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。

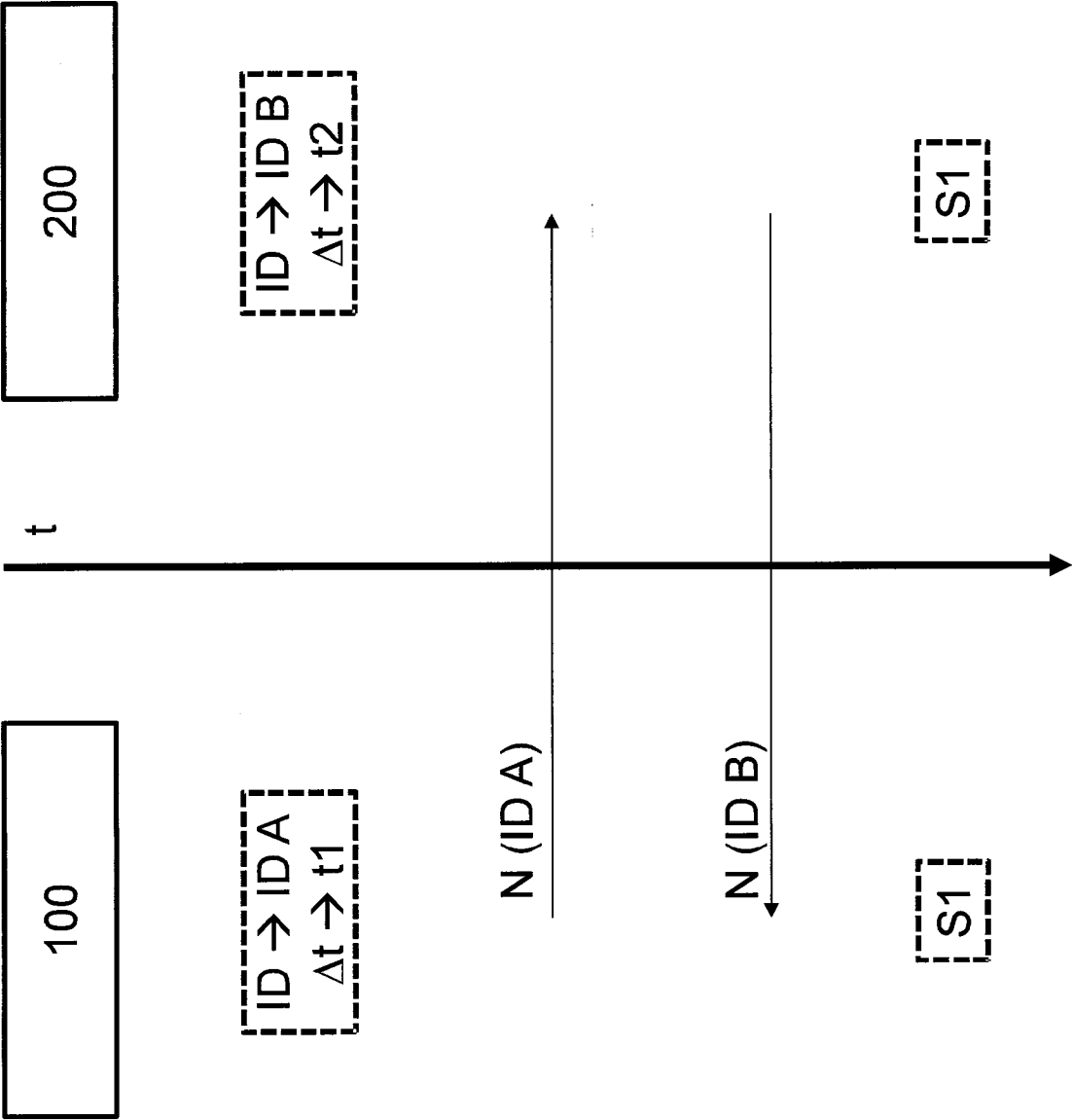


图 1