



(12) 发明专利申请

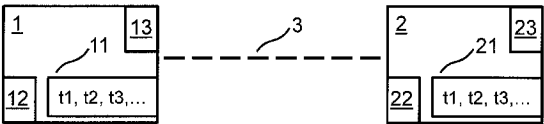
(10) 申请公布号 CN 105099667 A
(43) 申请公布日 2015. 11. 25

(21) 申请号 201510238149. 8
(22) 申请日 2015. 05. 12
(30) 优先权数据
102014208964. 6 2014. 05. 13 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 H. 魏勒
(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 胡莉莉
(51) Int. Cl.
H04L 9/08(2006. 01)
H04L 29/06(2006. 01)
H04J 3/06(2006. 01)

权利要求书1页 说明书4页 附图1页

(54) 发明名称
用于在网络中生成密钥的方法以及为此设立的网络用户

(57) 摘要
本发明涉及用于在网络中生成密钥的方法以及为此设立的网络用户。本发明以一种用于在网络的两个用户之间生成共同的密钥的方法为出发点。在此,两个用户分别拥有至少一个时钟以及用于检测确定的环境参量的装置。两个用户分别在预给定的时间点同步地检测确定的环境参量或者开始环境参量的变化的检测。最后两个用户分别在这样检测的环境参量的值被包括在内的情况下生成共同的密钥。



1. 用于在网络的两个用户(1,2)之间生成共同的密钥的方法,其中两个用户(1,2)分别拥有至少一个时钟(13,23)以及用于检测确定的环境参量(12,22)的装置,其特征在于,两个用户(1,2)分别在预给定的时间点(t_1 , t_2 , t_3)同步地检测确定的环境参量或者开始环境参量的变化的检测,并且两个用户(1,2)分别在这样检测的环境参量的值被包括在内的情况下生成共同的密钥。

2. 根据权利要求1所述的方法,其特征在于,所述共同的密钥代替在前的共同密钥。

3. 根据权利要求2所述的方法,其特征在于,在先前的共同的密钥被包括在内的情况下生成所述共同的密钥。

4. 根据前述权利要求之一所述的方法,其特征在于,这两个用户(1,2)的各自的时钟(13,23)首先被相互同步。

5. 根据权利要求4所述的方法,其特征在于,所述各自的时钟(13,23)的同步未经加密地进行。

6. 根据前述权利要求之一所述的方法,其特征在于,所述用户(1,2)经由已经受保护的通信连接从相同用户或不同的另外的用户接收所述预给定的时间点(t_1 , t_2 , t_3)。

7. 用于在网络的用户(1)中生成密钥的方法,其中所述用户(1)拥有时钟(13)以及用于检测确定的环境参量(12)的装置,其特征在于,所述用户(1)在预给定的时间点(t_1 , t_2 , t_3)检测确定的环境参量或开始环境参量的变化的检测,所述用户(1)在这样检测的环境参量的值被包括在内的情况下生成密钥,并且所述用户(1)将所述密钥用于与该网络的至少一个第二用户(2)的受保护的通信。

8. 在网络上的用户(1),所述用户拥有时钟(13)以及用于检测确定的环境参量(12)的装置,其特征在于,所述用户(1)拥有如下装置,所述装置用于:在预给定的时间点(t_1 , t_2 , t_3)检测确定的环境参量或开始确定的环境参量的变化的检测,在这样检测的环境参量的值被包括在内的情况下生成密钥,并且将所述密钥用于与该网络的至少一个第二用户(2)的受保护的通信。

9. 具有至少两个用户(1,2)的网络,所述用户分别拥有至少一个时钟(13,23)以及用于检测确定的环境参量(12,22)的装置,其特征在于,所述用户(1,2)拥有如下装置,所述装置用于:在预给定的时间点彼此同步地检测确定的环境参量或开始环境参量的变化的检测,分别在这样检测的环境参量的值被包括在内的情况下生成共同的密钥。

10. 计算机程序,其被设立用于执行根据权利要求1至7之一所述的方法的所有步骤。

11. 机器可读的存储介质,具有根据权利要求10所述的计算机程序。

用于在网络中生成密钥的方法以及为此设立的网络用户

技术领域

[0001] 本发明涉及在网络的用户之间的数据传输的保护。

背景技术

[0002] 在不同的设备之间的安全通信在增长地联网的世界中变得越发重要并且在许多应用领域中是对于可接受性和因此也对于相应应用的经济成功的重要前提。这(根据应用)包括不同的保护目标,例如要传输的数据的机密的维护、参与节点的相互认证或者数据完整的确保。

[0003] 为了实现这些保护目标,通常使用合适的密码的方法,其一般可以分成两种不同类型:对称方法,在其中发送器和接收器拥有相同的密码的密钥;以及非对称方法,在其中发送器利用公共的(即潜在攻击者也可能已知的)接收器密钥对要传输的数据进行加密,但是仅仅可以利用所属的私人密钥进行解密,所述私人密钥理想情况下仅仅对于接收器是已知的。

[0004] 非对称方法此外具有如下缺点:非对称方法通常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于资源受限的节点例如传感器、执行器等等,这些节点通常仅仅拥有相对较小的计算能力以及小的存储器并且应当高效地工作,例如基于电池运行或使用能量获得(Harvesting)。此外,经常仅仅可以利用有限的带宽来用于数据传输,这使得具有 2048 或者更多比特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:不仅接收器而且发送器拥有相同的密钥。在此,所属的密钥管理一般而言是非常高要求的任务。在移动无线电领域中,密钥例如借助 SIM 卡置入移动电话中并且所属的网络于是可以将相应的密钥分配给 SIM 卡的明确的标识。而在无线 LAN 的情况下,通常在网络配置时进行要使用的密钥的手动输入(通常通过输入口令)。但是,当例如在传感器网络或其他机器对机器的通信系统中有很大量节点时,这种密钥管理快速地变得非常昂贵并且不可实现。此外,要使用的密钥的改变经常是根本不可能的或者仅仅以非常大的花费才能实现。

[0006] 最近以来,因此在关键词“物理层安全”之下研究并且开发新型方案,借助所述新型方案可以自动基于在涉及的节点之间的传输信道产生用于对称方法的密钥。从信道参数中确定随机数或伪随机数例如可以从 WO 1996023376 A2 中得知,由信道参数产生机密密钥在 WO 2006081122 A2 中公开。在此,一般首先将(优选两侧都已知的)控制信号序列从第一节点发送至第二节点,然后将控制信号序列从第二节点发送至第一节点。相应的接收器可以从接收的导频信号序列中估计信道特性并且由此导出用于密码生成的合适参数。然而,在此当两个节点的测量之间的时间偏差太大时,可能得到不同的密钥并且因此提高了用于随后的密钥调整的花费或者共同的密钥生成甚至变得不可能。

发明内容

[0007] 本发明涉及按照独立的方法权利要求的方法以及在一个或多个网络上的用户,所

述用户被设立用于执行所述方法之一。此外,本发明还涉及计算机程序,该计算机程序被设立用于执行所述方法之一。

[0008] 在此提出:网络的用户在预先确定的时间检测环境参量并且从环境参量的值中导出用于受保护通信的密钥。拥有相应装置和关于预先确定的时间的信息的第二用户可以以相同的方式和方法来确定相同的密钥。因此,共同的、机密密钥是可能的,该密钥能够实现在这两个用户之间的受保护的通信。

[0009] 这种方法的优点由以下得出:受保护的通信所基于的机密是预先确定的时间点。该信息虽然也必须类似于对称密钥地被管理并且可供参与的网络用户使用。但是,潜在攻击者可能比以滥用获得的密钥更少地以滥用获得的时间点开始。除了关于时间点的信息之外,攻击者还必须具有用于检测所期望的环境参量的装置并且在预先给定的时间点处于所述用户的足够近处,以便检测环境参量的足够近似的值。

[0010] 如果该方法总是又被实施例如用于以新的密钥代替旧的密钥,则攻击者总是又必须在确定时间上在现场。因此,当在前的共同的密钥由此被代替时,该方法也是特别有利的。所述密钥或者可以是同样由这种方法产生的密钥、或者可以是另外的密钥。因此,知道旧密钥的攻击者也可以通过在预先确定时间基于环境参量测量的重新建立又从网络中被挤出或者至少从受保护的通信中被排除。为了该方法的进一步保护,也可以与在前密钥关联。

[0011] 为了保证预先确定的时间在所有用户中也保持相同,在用户之间的同步是有利的。对此,于是也可以使用更精确的环境参量值,因为更少的不安全性存在于准确的时间点中。在这种实施中,潜在的攻击者有另外的障碍:必要时也需要进行相应的同步。在此,所述同步可以还未经加密地进行,因为机密在于时间点。

[0012] 有利地,用户从网络的相同的中央机构接收预先确定的时间点,借助所述时间点所述用户例如分别已经建立受保护的通信。但是其他的选择也是可以的,例如这些用户采取不同源的时间。

附图说明

[0013] 下面参照附图并且借助实施例进一步描述本发明。在此,

图1示意性示出了具有两个用户的示例性网络,所述用户具有用于生成共同的机密密钥的装置。

具体实施方式

[0014] 本发明涉及用于基于无线或有线通信系统的节点、也即网络的用户的环境参量的物理特性自动生成对称的密码的密钥的方法。在使用在两个用户中的情况下,因此可以无高花费地使用对称加密方法以用于实现不同的安全目标,这尤其是针对在机器至机器通信范围中的应用、也即例如针对在不同的传感器节点和/或执行器节点之间的数据传输是令人感兴趣的。

[0015] 两个节点的相应环境参量对此必须具有足够的固有随机性、也即足够的时间变量,以便可以生成具有期望的熵的密钥。此外,在空间上在两个通常分离的节点之间的环境参量不允许太过分地波动,使得两个节点检测环境参量的足够一致的值,由所述值可以

生成一致的、共同的密钥。

[0016] 这例如可以如在下面描述的那样进行。两个节点利用合适的装置基于两侧存在的时间点彼此同步地确定确定的环境参量。节点对此应该可以采用彼此足够同步的时间装置(时钟),以及传感器,借助所述传感器这两个节点可以检测相同的确定的环境参量。必要时,这两个节点还拥有用于通过合适的计算方法从检测的数据中确定环境参量的值的装置,所述环境参量优选地在两个节点中以相同规格存在。

[0017] 由此确定的值由两个节点合适地量化。随后优选地跟随着用于噪声或错误减少的措施,例如通过相应的错误解码。于是借助合适的机制优选在使用公共协议的情况下进行在节点之间的量化值的调整。这是必需的,因为由于测量精度、噪声、干扰等等,两个节点一般首先通常没有确定相同的比特序列。在此调整应当被设计成,使得可以窃听交换的数据的潜在攻击者不能由此容易地推断出所确定的比特序列。对此例如可以在节点之间交换奇偶校验位。可选地,还可以执行密钥校验(例如熵估计)和密钥改进(例如通过经由哈希值形成的密钥压缩)。最后基于调整的、量化的值来生成相应的对称密钥。

[0018] 此外,可以借助该方案也无大花费地定期地执行密钥更新,也即重新计算要使用的密钥。此外也不必采用复杂的、计算强度大的非对称方法。

[0019] 在所描述的方法中,以以下为出发点:这两个节点的(物理)环境参量在时间上具有足够的值波动,以便能够由此导出合适的比特序列,所述比特序列适于在节点中作为用于密钥生成的基础(尤其是具有足够的随机特性)。

[0020] 通过在两个节点之间时间上同步值检测,尽管环境参量的在时间上的强烈变化,也可以确定相同的或者强相关的参量值。因此,也可以从这样检测的环境参量值中相应地、局部地导出共同密钥。在此假设:关于节点之间的距离的环境参量空间上足够恒定,使得相应的节点尽管空间上的距离仍然可以确定相同或者足够相关的环境参量值,以便得到足够类似的比特序列,由所述比特序列可以获得相同的密钥。

[0021] 所确定的相同的密钥于是可以被用于对称加密方法。

[0022] 优选地,在这两个节点中的时钟在该方法开始时彼此同步。这可以利用已知方法来进行,例如按照 IEEE 1588。同步数据的加密是可以的,但是原则上不是必需的。优化地,针对在两个节点中的该方法使用具有高运转稳定性的时钟,使得不必太经常地进行用户之间的同步。

[0023] 两个节点在预先确定的目标时间检测环境参量。这些目标时间应当是机密的、也即仅仅对于这两个节点和必要时值得信任的另外的机构是已知的。攻击者不应当拥有所述信息,所述信息于是也不应当未经加密地在这两个节点之间传送或者被传送给这两个节点。按照不同实施方式,时间点可以由一个或多个值得信任的机构加密地被传输给这两个节点,其中所述值得信任的机构拥有至这两个节点的受保护的传输路径。代替地,这两个节点可以在利用先前密钥加密的通信中协商时间点(或者节点之一向另外的节点传送相应时间点)。在另一不太安全、但是特别简单地实现的代替方案中,时间点至两个节点的传送或者在两个节点之间的传送可以在以下条件下手动地开始,即当前预料到没有攻击者。

[0024] 在共同的目标时间点,两个节点测量时间可变的环境参量。在此,例如涉及辐射强度、或辐射频谱、亮度、温度、噪声水平或噪声频谱、在空气中的物质浓度、电磁场强等等或者其组合。

[0025] 数据检测的过程可以周期地或者在预先确定时间点被重复,以便产生更安全的密钥或密钥序列。这种彼此相继的、从相互不相关的测量参量中获得的密钥是彼此无关的。该方法也可以被用来替换或者改变现有密钥(是否通过相应的方法来生成)。

[0026] 与已知方案、例如物理层安全(其中在两个节点之间测量信道特性)的不同之处在于,在那里潜在攻击者不像这两个通过信道相互通信的节点那样看到同样的信道特性,但是在这里的方案中该机密处于检测所述信息的预给定时间点中(通过同步化的时钟来实现)。

[0027] 在图 1 中,作为实施例示出了第一节点 1,其拥有存储器 11,在存储器中存放预先确定的时间点 t_1 、 t_2 、 t_3 、 $\dots$,在这些时间点应当利用节点 1 的传感器 12 检测确定的环境参量。节点 1 通过其时钟 13 确认所述预先确定的时间点的到达。节点 2 相应地拥有存储器 21,相同的预先确定的时间点 t_1 、 t_2 、 t_3 、 $\dots$ 存放在存储器 21 中,在这些时间点应当利用节点 2 的传感器 22 检测确定的环境参量。节点 2 通过其时钟 23 确认所述预先确定的时间点的到达。从同步检测的环境参量值中节点 1 和 2 现在分别导出共同的、也即对称的密钥。通过所述密钥,节点 1 和 2 现在使得其通过共同通信连接 3 的通信受到保护。通过该通信连接 3 可以在准备阶段也进行节点 1 和 2 的时钟 13 和 23 的同步。同样地,在相应的实施方式中,可以在节点之间进行预先确定时间点的协商或传送。

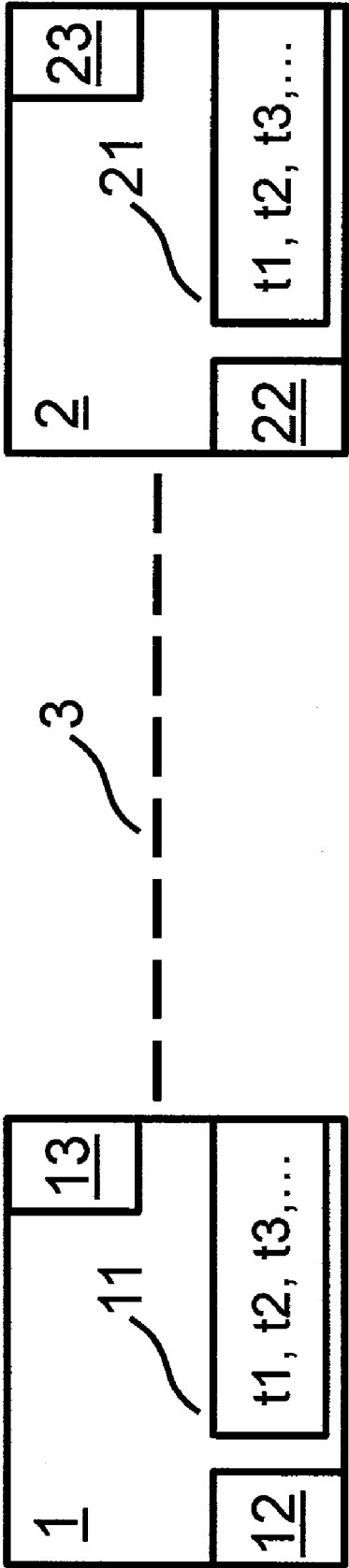


图 1