(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 101305539 B
(45)授权公告日 2013.04.24

(21)申请号 200680042058.6
(22)申请日 2006.10.26
(30)优先权数据
05256974.6 2005.11.11 EP
(85)PCT申请进入国家阶段日
2008.05.12
(86)PCT申请的申请数据
PCT/GB2006/003995 2006.10.26
(87)PCT申请的公布数据
WO2007/054665 EN 2007.05.18
(73)专利权人 英国电讯有限公司
地址 英国伦敦
(72)发明人 维韦卡南德·科尔高昂卡尔本·斯特鲁
(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 李辉
(51)Int.Cl.
H04K 3/00(2006.01)
G06K 19/07(2006.01)

(56)对比文件
EP 1303069 A1,2003.04.16,
JP 62257236 A,1987.11.09,
JP 1768052 C,1993.06.11,
Ronald L. Rivest.Chaffing and Winnowing: Confidentiality without Encryption.《CRYPTOBYTES》.1998,第4卷(第1期),

审查员 喻文芳

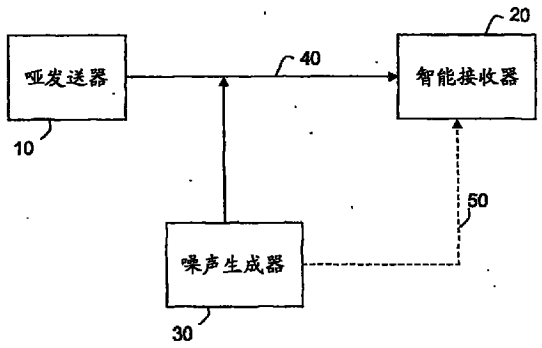
权利要求书2页 说明书7页 附图6页

(54)发明名称

用于安全通信的方法和系统

(57)摘要

一种通信系统,该通信系统包括接收器和第一发送器,其中第一发送器在该接收器所使用的一系列通信信道上发送多个噪声信号,该接收器适于在所述一系列通信信道的一个或更多个通信信道上接收第二发送器所发送的发送,并且适于利用来自第一发送器的与这些噪声信号有关的信息,从这些噪声信号中辨别出第二发送器的发送。



CN 101305539 B

1. 一种通信系统，该通信系统包括接收器和第一发送器，其中：

第一发送器能够操作以在该接收器所使用的一系列通信信道上发送多个噪声信号，其中所述第一发送器还能够操作以向所述接收器发送与这些噪声信号有关的信息；

该接收器适于在所述一系列通信信道的一个或更多个通信信道上接收第二发送器所发送的发送，所述发送与所述噪声信号相交织，并且该接收器适于利用来自第一发送器的与这些噪声信号有关的所述信息，从这些噪声信号中辨别出第二发送器的发送。

2. 根据权利要求 1 所述的通信系统，其中，该接收器和该第一发送器是同一装置的一部分。

3. 根据权利要求 1 或权利要求 2 所述的通信系统，其中，那些噪声信号的格式与该第二发送器的发送是相同的。

4. 根据权利要求 1 所述的通信系统，其中，那一系列通信信道包括不同时隙、不同频带、不同正交码中的一种或更多种。

5. 根据权利要求 1 所述的通信系统，该通信系统还包括所述第二发送器，该第二发送器在所述通信信道中的一个或更多个上进行发送。

6. 根据权利要求 5 所述的通信系统，该通信系统包括多个所述第二发送器。

7. 根据权利要求 5 或权利要求 6 所述的通信系统，其中，该第二发送器或每个第二发送器都是简单装置，所述简单装置在它们的计算功率、它们的电池功率或寿命或者它们的存储器能力的一个或更多个方面是受限的。

8. 根据权利要求 5 或权利要求 6 所述的通信系统，其中，该第二发送器或每个第二发送器都是仅能在一个通信信道上发送其自身标识符的装置。

9. 根据权利要求 5 或权利要求 6 所述的通信系统，其中，该第二发送器或每个第二发送器都不能进行加密发送。

10. 根据权利要求 7 所述的通信系统，其中，该第二发送器或每个第二发送器都是 RFID 标签，而该接收器是 RFID 读取器或监督标签。

11. 根据权利要求 1 所述的通信系统，其中，该接收器、该第二发送器或它们两者适于检测在特定信道上何时发生冲突，并且重新发送在该冲突中丢失的数据。

12. 一种保护第一发送器与接收器之间的通信的方法，该方法包括以下步骤：

在一系列通信信道的一个或更多个通信信道上从该第一发送器发送消息；

在所述一系列通信信道上从第二发送器发送噪声；

将所述消息与所述噪声相交织；

将有关来自该第二发送器的噪声的信息传递给该接收器；

利用来自该第二发送器的信息，从所述一系列通信信道上的发送中获取所发送的消息。

13. 根据权利要求 12 所述的方法，其中，获取步骤包括以下步骤：在该接收器中接收所发送的消息和所发送的噪声的组合；以及利用所述信息从该组合中分离出所发送的消息。

14. 根据权利要求 12 所述的方法，其中，获取步骤包括以下步骤：仅在所述一系列通信信道的一部分上选择性地接收，从而仅接收该消息，所述部分是利用所述信息来确定的。

15. 根据权利要求 12 到 14 中任意一项所述的方法，其中，该第二发送器和该接收器是同一装置的一部分。

16. 根据权利要求 12 到 14 中任意一项所述的方法，其中，那些噪声信号的格式与该第一发送器的发送相同。

17. 根据权利要求 12 到 14 中任意一项所述的方法，其中，那一系列通信信道包括不同时隙、不同频带、不同正交码中的一种或更多种。

18. 根据权利要求 12 到 14 中任意一项所述的方法，该方法还包括以下步骤：检测该第一发送器发送的消息的一部分与该第二发送器发送的噪声之间何时出现冲突；以及重新发送该消息的受影响部分。

用于安全通信的方法和系统

技术领域

[0001] 本发明涉及用于通信的方法和系统，具体地但不排他地涉及一种在不使用加密的情况下提供安全通信的方法和系统。

背景技术

[0002] 在通信领域中，长期以来人们已经接受了有两种可以在双方之间安全传送消息的主要方式：加密和掩密术 (steganography)。

[0003] 加密通常涉及用仅可以（希望）被期望接收方解码的代码来替换原始消息的“明文 (plain text)”。当前的加密技术（如 DES 和 RSA) 通常使用交换密钥或公有 / 私有密钥系统。

[0004] 掩密术涉及将原始消息的明文“隐藏”在双方之间所传送的另一项 (item) 中。这种途径包括诸如将明文放置在“掩护 (cover)”消息内的商定位置处或者将明文作为图片的一部分像素来传送的方法。在所有情况下，原始消息的明文仍呈现在其原始的未编码形式，但是只有期望接收方知道怎样从“掩护”中获取它。

[0005] 近来，在 Ronald L. Rivest 的 Chaffing and Winnowing：Confidentialitywithout Encryption，CryptoBytes(RSA Laboratories)，volume 4，number 1(summer 1998)，12-17 中提出了安全通信的第三种方法。这种技术被称为“掺麦壳 (chaffing)”，因为其原理是提供足够的“麦壳 (chaff)”从而只有期望接收方可以选出原始消息的“小麦 (wheat)”。因为原始消息在双方之间传送而不加密，而只有期望接收方能够获取该原始消息，所以掺麦壳在许多方面类似于掩密术。

[0006] 在所有领域中对于安全通信的需求都在不断增长。这种需求在为其中用来发送消息的装置相对简单且需要低成本的领域（如射频识别 (RFID)）中产生了问题。这种装置通常不能够执行对它们的消息进行加密所需的复杂例程或者不能够构造和发送掩密术所需的掩护消息。

[0007] 上述 Rivest 描述的掺麦壳方法仍需要两个通信方，以便为了使接收方能够辨别可靠的消息认证码 (MAC) 而预先交换信息。

发明内容

[0008] 因此，按其最广泛的方面来说，本发明提供了一种通信系统，其中，在一系列通信信道上发送噪声，并且接收器能够利用与该噪声有关的信息来辨别原始消息。不知道与该噪声有关的信息的接收器不能够辨别原始消息。

[0009] 本发明的第一方面提供了一种通信系统，该通信系统包括接收器和第一发送器，其中：

[0010] 第一发送器在该接收器所使用的一系列通信信道上发送多个噪声信号；

[0011] 该接收器适于在所述一系列通信信道的一个或更多个通信信道上接收第二发送器所发送的发送 (transmission)，并且适于利用来自第一发送器的与这些噪声信号有关的

信息，从这些噪声信号中辨别出第二发送器的发送。

[0012] 利用上述系统，因为从第一发送器发送的噪声提供了那些发送的安全性，所以第二发送器不需要具备任何加密或伪装其发送以将它们安全发送至该接收器的能力。因此，第二发送器可以被造得相对简单且廉价。

[0013] 优选的是，从第一发送器向该接收器传送与这些噪声信号有关的信息。该信息可以是这些噪声信号的完整内容，其可以包含时间戳，从而可以将这些信号与接收信号进行比较。另选或另外的是，该信息可以是在特定时刻发送噪声的那些信道。

[0014] 在第一方面的特定实施方式中，该接收器和第一发送器是同一装置的一部分。在这个实施方式中，与噪声信号有关的信息的传送可以由具有借以向接收器传递噪声的内部输出的第一发送器，或者共享公用存储器或处理器的该接收器和该发送器来实现。在一个具体实施方式中，第一发送器可以接收来自处理器的多个驱动器信号，并且该处理器可以将这些驱动器信号提供给该接收器。

[0015] 术语“噪声信号”用于描述不是来自第二发送器的发送的一部分的任何信号。这种信号在整个随机信号的含义中不一定是“噪声”，而优选的是，这些噪声信号使得它们可以容易地被接收器（例如，根据发送它们的信道）从来自第二发送器的发送中分离出来。

[0016] 实际上，优选的是，这些噪声信号的内容基本上与第二发送器的发送相同。如果是这种情况，则第三方或闯入方（interloper）可能更加难于通过分析发送的内容而简单地辨别来自第二发送器的发送。

[0017] 这一系列通信信道可以包括不同时隙、不同频带、不同正交码中的一个或更多个。这些通信信道还可以是其中没有限定时隙并且发送器在异步发送之前等待介质变为空闲的以太网型信道。

[0018] 本发明的另一方面提供了一种根据上述第一方面的通信系统，该通信系统还包括所述第二发送器，该第二发送器在所述通信信道的一个或更多个上进行发送。

[0019] 就此而言，可以存在多个所述第二发送器。

[0020] 该第二发送器或每个第二发送器都可以是简单装置。简单装置（有时被称为“哑”装置或标签）在它们的计算功率、它们的电池功率或寿命，或者它们的存储器能力的一个或更多个方面是受限的，由此不能够执行就那些因素而言非常昂贵的诸如加密的技术。例如，该简单装置可以是在预先选定的通信信道上简单地发送其自身 ID 的装置，或者是仅可以读取一个频率和一个协议的装置。因此它不能够过滤读数、存储标签数据等等。

[0021] 尽管本发明也涵盖了更复杂的第二发送器，实际上可能具有相当大的处理功率的发送器，但在本发明的这个方面中，由于第一发送器的噪声发送所以不需要该处理功率来伪装或加密该安全发送。

[0022] 在一个典型例中，该第二发送器或每个第二发送器是 RFID 标签，而接收器是 RFID 读取器或监督（overseer）标签。

[0023] 优选的是，该接收器、第二发送器或者这两者适于检测在特定信道上何时出现冲突，并且重新发送在该冲突中丢失的数据。如果该系统具有这种能力，则第一发送器可以在所有可能的通信信道上进行发送，而不必知道（多个）第二发送器正在使用的信道，因为会检测到任何冲突并且重新发送丢失的数据。

[0024] 在本说明书中，引用“冲突”是指对于正被用于装置之间通信的介质同时存在一

个以上需求的情况。在 www.wikipedia.org 上该术语的定义写道：“在数据传输系统中，对于在任何指定时刻仅能处理一个需求的设备上同时作出两个或更多个需求时所发生的情况”。

[0025] 在媒体访问控制 (MAC) 协议的描述中“冲突”是标准技术术语。针对以太网的 MAC 和针对无线系统的 MAC 本质上是基于避免和 / 或检测并修正冲突，而这个意义上的冲突通常表现在这些协议的名称上，举例来说，CSMA/CA 是指载波检测多址 / 冲突避免。

[0026] 本发明的另一方面提供了一种保护第一发送器与接收器之间的通信的方法，该方法包括以下步骤：

[0027] 在一系列通信信道的一个或更多个通信信道上从该第一发送器发送消息；

[0028] 在所述一系列通信信道上从第二发送器发送噪声；

[0029] 将有关来自该第二发送器的噪声的信息传递给该接收器；

[0030] 利用来自该第二发送器的信息，从所述一系列通信信道上的发送内容中获取所发送的消息。

[0031] 获取步骤可以包括以下步骤：在该接收器中接收所发送的消息和所发送的噪声的组合；以及利用所述信息从该组合中分离出所发送的消息。

[0032] 另选或另外的是，获取步骤可以包括以下步骤：仅在所述一系列通信信道的一部分上选择性地接收，从而仅接收该消息，所述部分是利用所述信息来确定的。

[0033] 在这个方面的该方法的一个实施方式中，该第二发送器和该接收器是同一装置的一部分。

[0034] 优选的是，这些噪声信号的内容基本上与该第一发送器或每个第一发送器的发送相同。这个特征的优点已经结合上述第一方面进行了说明。

[0035] 这一系列通信信道可以包括不同时隙、不同频带、不同正交码中的一个或更多个。

[0036] 优选的是，该方法还包括以下步骤：检测该第一接收器发送的消息的一部分与该第二接收器发送的噪声之间何时出现冲突；以及重新发送该消息的受影响部分。

[0037] 本方面的方法可以在头两个方面中的任一方面（包括那些方面的可选或优选特征的任何组合）所述的系统中实现。

附图说明

[0038] 下面参照附图，对本发明的实施方式进行说明，附图中：

[0039] 图 1 是本发明第一实施方式的示意图；

[0040] 图 2 是本发明第二实施方式的示意图；

[0041] 图 3 是本发明第三实施方式的示意图；

[0042] 图 4 例示了本发明的实施方式的原理；

[0043] 图 5 是示出针对 EPCGlobal Gen2 RFID 标签中的标签单一化 (singulation) 的 Q 算法的流程图；

[0044] 图 6 是示出利用本发明实施方式的针对标签单一化的修正 Q 算法的流程图；

[0045] 图 7 是示出利用本发明实施方式的针对标签单一化的修正 Q 算法的另一部分的流程图。

具体实施方式

[0046] 图 1 以示意图的形式示出了本发明的第一实施方式。哑发送器 10 在从一系列这种信道 40 中预先选定的通信信道上进行发送。同时，噪声发送器 30 在包括该预先选定的通信信道在内的一系列通信信道 40 上发送噪声信号。噪声发送器 30 在安全通信链路 50 上将与其正在发送或已经发送的噪声有关的数据传递给智能接收器 20。

[0047] 智能接收器 20 接收在一系列通信信道 40 上发送的所有数据，包括哑发送器 10 在预先选定的通信信道上发送的数据。接收器 20 利用在安全通信链路 50 上从噪声发送器 30 接收到的数据，来辨别由哑发送器 10 发送的数据。

[0048] 在另选构造中，接收器 20 不接收在整个一系列通信信道 40 上发送的全部数据，而是根据有关噪声的数据来选择性地接收在那些通信信道 40 的特定通信信道上发送的数据。

[0049] 第三方或非友方侦听 (hear) 在一系列通信信道 40 上发送的全部数据，在不知道与这些数据的哪些部分是噪声发送器 30 所生成的噪声有关的信息的情况下不能辨别哑发送器 10 所发送的数据。

[0050] 图 2 示出了本发明的另选实施方式，其中，噪声发送器并入在接收器 21 中。这里，关于噪声的数据不需在安全通信信道上传递，因为它可以在接收器 21 内进行内部传递。除此之外，该系统按照上面结合图 1 所讨论地进行运行，包括其中接收器根据关于噪声的信息来选择性地接收来自通信信道 40 的数据的另选构成。

[0051] 在一种可能的构成中，处理器向并入接收器 21 的噪声发送器提供决定了噪声发送器将在哪个信道上进行发送的驱动器信号，并且将同一驱动器信号提供给使用该信息来接收该消息的接收器部分。

[0052] 图 3 示出了本发明的另一实施方式，其中，具体噪声发送器 31 作用于从哑发送器 10 接收到的消息，在一系列通信信道 40 上同时发送该消息和噪声。噪声发送器 31 还在专用通信信道 51 上发送关于噪声的信息。智能接收器 35 接收在一系列通信信道 40 上发送的所有信号，以及在专用通信信道 51 上发送的有关噪声的信息，并且利用该信息来确定传递给哑接收器 22 进行处理的消息的内容。此外，智能接收器 35 可以利用关于噪声的信息，如上所述选择性地接收来自一系列通信信道 40 的数据。

[0053] 在图 3 的实施方式的另选构成中，预先排列信道序列可用于噪声，该预先排列的序列在噪声发送器 31 与智能接收器 51 之间是已知的。在这种情况下，关于噪声的信息不需要在信道 51 上传递，尽管这个信道可以被用于发送初始预先排列的序列，或该序列的变更。

[0054] 下面，对可以在本发明中使用的通信信道的一些例子进行阐述。

[0055] 时间 :装置通过许多不同的时隙进行通信。假定需要发送消息，该消息被分解成许多比特（或者更大的块 (chunk)，例如，字节、16 比特字，或任何预定数量的比特）。通信信道是时隙且发送方以随机选定的时隙来发送消息。由于其它装置（特别是噪声发送器）是以不同的时隙进行发送，所以数据与来自其它装置的数据进行交织，从而使其不易辨别。噪声发送器可以在认证了对关于噪声信号的信息感兴趣的任一方之后向该方发送该信息。

[0056] 频率 :装置通过许多不同的频率进行通信。消息同样被分解成许多比特（或比特的组合），而且在这种情况下，在随机选定的频率信道上进行发送。噪声发送器基本上是同

样运行的。从而，接收器在许多不同的频率上接收信息，并基于关于噪声发送器所用频率的信息来提取信息。

[0057] 正交码：装置通过不同的正交码进行通信。消息同样被分解成许多比特（或比特的组合），而且在这种情况下，用随机选定的正交码进行编码并在该信道上进行发送。噪声发送器对噪声数据进行同样的处理。接收器利用噪声发送器发送的信息来提取信息。

[0058] 在本发明的一个具体实施方式中，与 RFID 标签相关联地使用该系统和方法。

[0059] 在其最简单的方面，该构成考虑了两个发送装置 A 和 B。每个装置发送的信息都是典型的 1 或 0 的比特流，例如，如图 4 所示。在通信期间，两个装置都获知通信和发生的冲突，由此可以识别彼此的比特（参见图 4 中的最终比特流）。但偷听方不能分辨该比特来自哪个装置。由此，如果仅两个装置 A 和 B 进行发送，则它们将获知彼此的输出。它们还可以获知共享秘密，这种共享秘密例如可以根据任一方的输出或一起 XOR 后的输出，或者根据彼此的数据的偏差或这个组合流的其它功能来构造。

[0060] 然而，第三方或闯入方装置 C 可以接收上述数据，而却不能获知输出或共享秘密。

[0061] 然而，如果希望将新的装置引入安全网络中，则噪声发送装置 B 可以对 C 执行认证步骤。接着，如果 B 对于 C 的证件 (credential) 感到满意，它就可以向 C 通告使其理解 A 的输出的必要信息。这样，B 就代表可能是本身不能进行认证的这种简单装置的 A 来执行认证。

[0062] 一个示例系统是其中 RFID 标签在被 RFID 读取器查询时发送产品标识信息的系统。RFID 中关注的保密性或安全性主要存在于 RFID 标签与 RFID 读取器之间的无线链路上，因为这通常是不加密的，由此易受电子欺骗 (spoofing) 和偷听。根据本发明的实施方式，在 RFID 标签向 RFID 读取器发送信息时在数据中添加已知噪声。

[0063] 存在几种可能情况，其中的两个例子是：

[0064] a、受信 RFDI 读取器通过发送噪声信号来保护 RFID 标签所发送的信息，这样防止了非受信读取器偷听该信息。这种情况可能有助于在团体场景下来防止间谍。

[0065] b、特殊噪声生成器标签可以在由标签发送的信息中添加噪声信号 -RFID 标签仍可以是低成本的，并且 RFID 读取器不需要改动。噪声生成器标签由个人携带，以向该人的标签所发送的信息中添加噪声信号。

[0066] 读取器标签通信协议对于这两种情况是相同的。标签使用与分时隙 ALOHA 类似的随机接入防冲突协议来防止争用。分时隙 ALOHA 是其中将时间分成任何装置可用于进行发送的多个时隙的同步协议。每个装置都可以随机选择一时隙，但在发送之前不检查时隙是否空闲。如果仅一个装置进行发送，则数据被发送，而如果两个（或更多个）装置在同一时隙中进行发送，则所有数据都会丢失。接着，两个装置都重新发送，但是随机重新选择它们的时隙，从而使发生再次冲突的可能性很小。

[0067] 考虑单个标签在被读取器查询时生成信息的情况。生成的信息可以是如 1 或 0 的比特，例如，如图 4 所示并参照上述说明。读取器接收复合数据。如果噪声生成器标签被用于伪装消息，则读取器将在噪声生成器标签发送与消息中的噪声信号有关的信息之前向噪声生成器标签认证自己。

[0068] 噪声生成器标签是与 RFID 标签距离很近的装置，从而它可以在标签向读取器发送数据时插入噪声比特。噪声生成器标签实质上是将无关数据添加至信道中，以使对方难

于读取标签信息。

[0069] 图5示出了针对EPCGlobal Gen2 RFID标签中的标签单一化(singulation)的标准Q算法的简化形式。这种算法被RFID读取器/接收器用于协调一组标签,从而它可以使每个标签单独发送并由此可以被读取器依次读取。在当前情况下,信道是时隙。

[0070] 在步骤S1,读取器广播查询(Q)(其可以根据标签所处环境和用途定期地生成,例如,每分钟一次、每十分钟一次等)。作为响应,所有标签都"醒来"并基于0与2^Q之间的数来选择一个标识符(ID)。

[0071] 接着,在步骤S2,读取器向ID为0的标签发送查询。如果不存在ID为0的标签,致使读取器不能获得响应("静默"),则在步骤S7中所有标签都将它们的ID减少1,重复步骤S2和S3直到获得响应为止。如果在步骤S2中一个以上的标签对读取器作出了响应("冲突"),则在步骤S6忽略所有标签,直到生成下一个查询为止。随后在步骤S7中,ID大于0的所有标签都减去1。

[0072] 如果仅有一个ID为0的标签("选定1个标签"),则在步骤S4中,它对接收器作出响应。接着,发送标签和接收器可以进行进一步的通信;典型地,标签会把它的密钥信息发送给接收器。接着,发送标签入睡,直到下一个查询为止(步骤S5),而其它标签将它们的ID减去1并且重复该处理直到所有标签都被延缓或被接收器识别为止(步骤S7)。图6示出了被调整成考虑本发明的实施方式的保护处理的图5的Q算法。因为算法的步骤相同,所以使用了相同的编号,并且不再进一步说明这些步骤。

[0073] 在图5的算法中插入了三个额外步骤,从而考虑噪声生成器(或这里假定为类似的RFID标签,并且称为"噪声生成器标签")的存在。

[0074] 首先,在查询阶段之前,读取器查询周围的噪声生成器标签(步骤S0)。噪声生成器标签和读取器利用加密认证协议来相互认证它们自身。因此,在认证之后,噪声生成器标签和读取器将共享有关噪声信号的信息。

[0075] 在该算法中,一旦确认了与选定标签的通信(步骤S40),就开始图7所示的噪声保护发送序列。

[0076] 选定标签和噪声生成器利用经修订的分时隙ALOHA(如上所述)来生成经修订数据。步骤S40中的这个子例程替换了图5的Q算法中的步骤S4,其中选定标签将其信息发送给接收器。相反,选定标签与噪声生成器标签争用该信道来发送其信息。对于该例的目的,我们假定在该处理过程中仅有一个选定RFID标签和一个噪声生成器标签可用(active)。

[0077] 如图7所示,读取器启动一轮(round)并确定一轮中的时隙数(步骤S42)。在步骤S43,噪声生成器和选定标签都在选定时隙(通信信道)中发送比特。优选的是,噪声生成器标签所发送的比特模式无法与选定标签所发送的比特模式区别开。

[0078] 一轮中的时隙数越大,该时隙出现冲突的概率越小。一轮期间冲突的概率由1/n给定,其中,n为一轮中的时隙数。发送特定比特的概率由1/n给定,其中,n为一轮中的时隙数。例如,一轮中四个时隙,噪声生成器标签和选定标签决定用概率1/4在特定时隙中进行发送。一轮期间冲突的概率由1/4给定。

[0079] 该处理将被重复进行n+m轮,直到正确地接收到n个RFID标签比特和m次冲突为止。

[0080] 接收器检测在噪声生成器与选定标签所发送的比特之间是否存在冲突(步骤

S44)。如果发生了冲突，则读取器在该轮的结尾发送“重复”信号（步骤 S45)，请求标签和噪声生成器标签重新发送自发生冲突起的最后一个比特。否则，它将发生“下一个”信号，告诉它们已经接收到了最后一个比特，并请求它们发送下一个比特（步骤 S42)，直到完成标签发送为止，在该时点，接收器发信号通知其它标签发送结束（步骤 S46)，并且该算法如图 6 中所示继续进行（步骤 S41)。

[0081] 尽管上述说明针对的是单个比特的发送，但是也可以在每个时隙中发送任意数量（例如，字节、16 比特字等）的比特组。

[0082] 一旦完成了标签发送，噪声生成器标签就向接收器（如果噪声生成器标签和接收器是同一装置的一部分，则其可以是内部链路）发送噪声比特序列（步骤 S41)，以使接收器可以确定从选定标签发送来的数据。当然，噪声生成器标签可以与发送并行地向接收器连续传递噪声比特序列，而非等待发送完成再传递。

[0083] 这样，不能对数据进行直接或信号分析的第三方或闯入方无法在来自选定标签的数据比特与噪声生成器标签所生成的数据比特之间加以区分，由此实现了针对标签发送的数据安全性。

[0084] 实现本发明的实施方式的另一个例子是在以太网中。

[0085] 在该例中，第一计算机通过出于某些原因被认为不安全的以太网段而连接至路由器。通过将路由器设置为只要计算机试图进行发送就发送“噪声”帧，无需改动第一计算机就可以保护以太网链路。为此，路由器将可觉察到但无意义的帧插入到以太网中，这些帧携带了作为发送器的第一计算机的 MAC，以及作为接收器的路由器的 MAC，因此第三方或闯入方无法将其与第一计算机所发送的真实帧区别开。

[0086] 当然，上述例子可以扩展为连接至该以太网段的大量第一计算机，在该情况下，路由器同样插入与那些计算机相对应的帧。而且，可以由与路由器分离但是与其有安全连接的装置将“噪声”帧插入到以太网中。

[0087] 虽然结合上述实施方式示范了本发明，但这些实施方式不应被认为是对本发明的限制，而是应该理解，在本发明的范围内可以对上述实施方式做进一步的变化和修改。

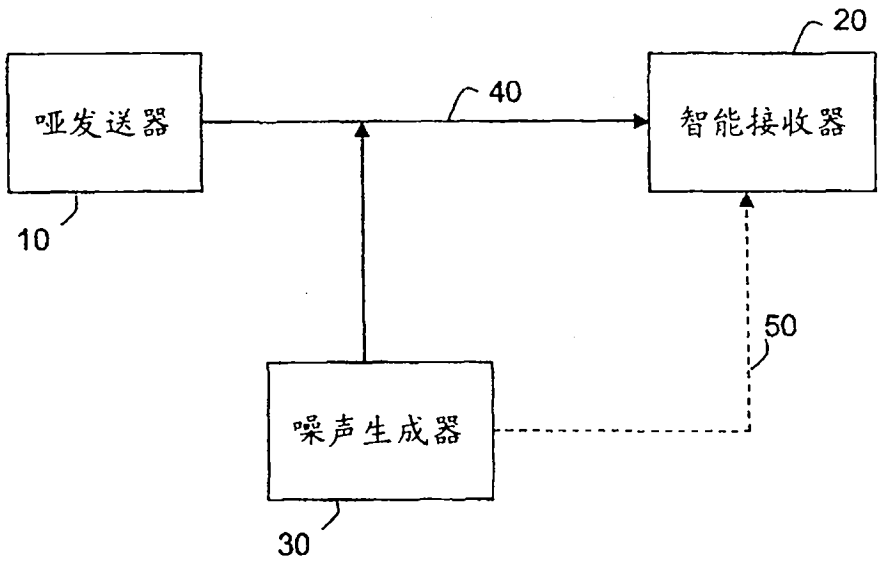


图 1

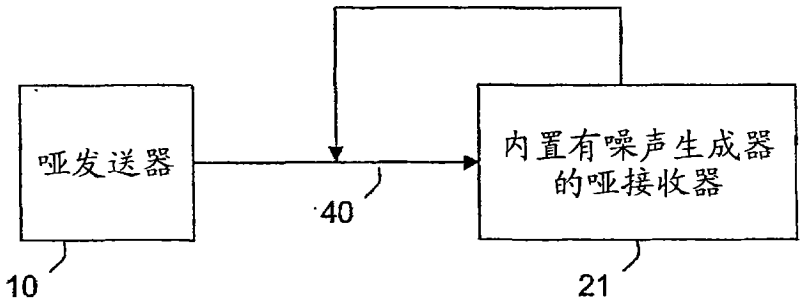


图 2

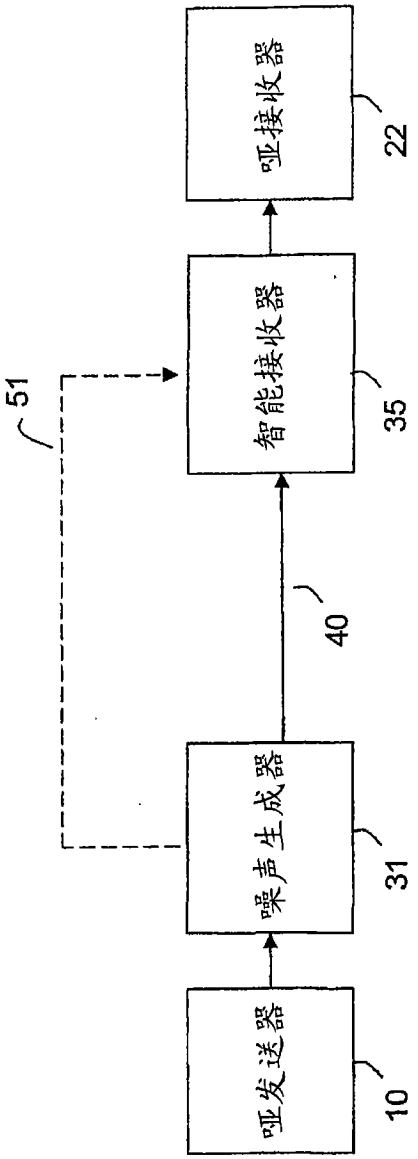


图 3

- RFID 标签输出

  101011100011010 1

  – RFID 标签输出可能会与噪声生成器标签所生成的输出相交织

- 全部输出可能看起来像下面这样

  1 1 0 0 1 1 0 1 0 1 1 1 1 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 0 0

  1– 噪声生成器装置 B 输出

  1– 装置 A 输出

图 4

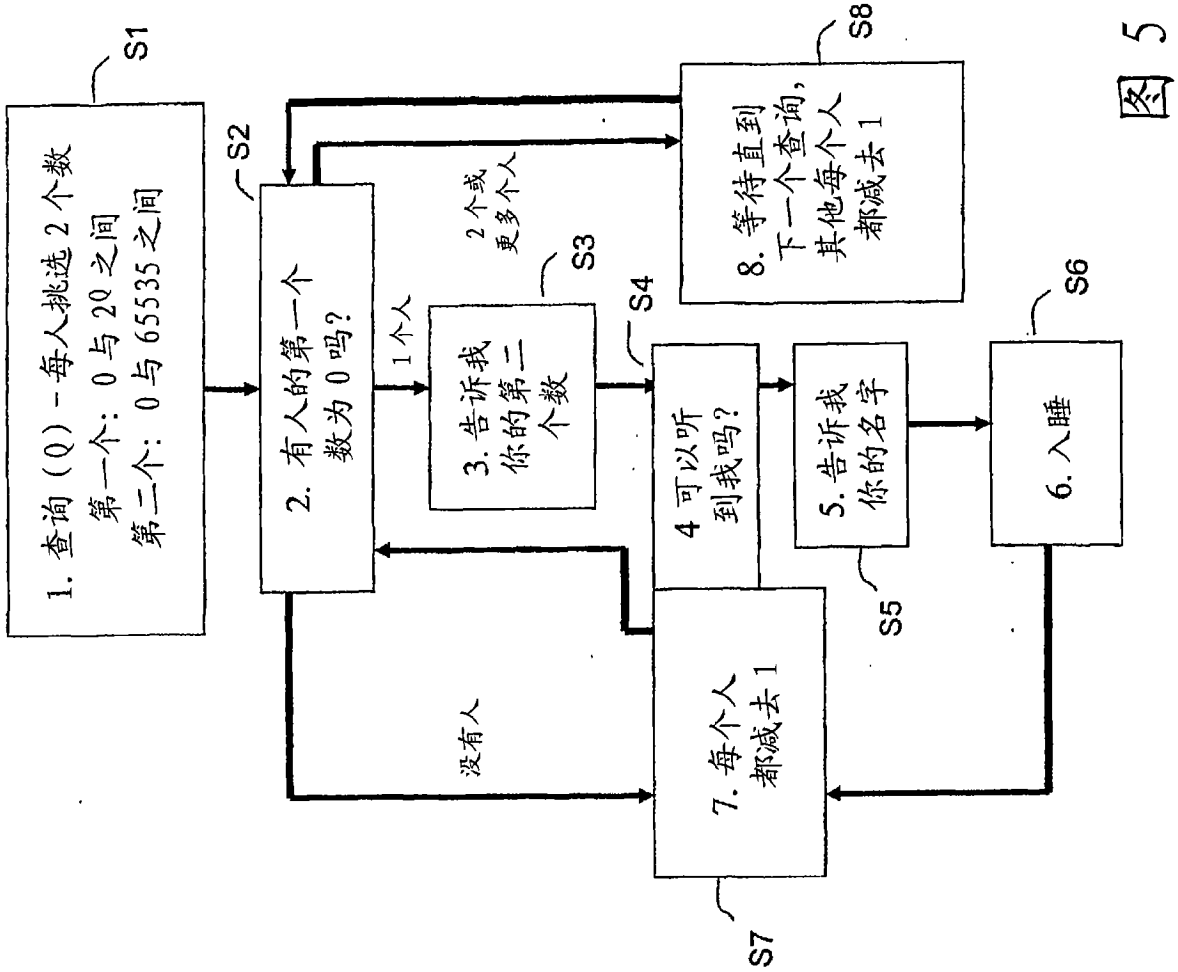

1. 查询（Q）- 每人挑选 2 个数
第一个：0 与 20 之间
第二个：0 与 65535 之间
S1
2. 有人的第一个数为 0 吗?
S2
1 个人
2 个或更多个人
3. 告诉我你的第二个数
S3
4 可以听到我吗?
S4
5. 告诉我你的名字
S5
6. 入睡
S6
7. 每个人都减去 1
S7
没有人
8. 等待直到下一个查询，其他每个人都减去 1
S8

图 5

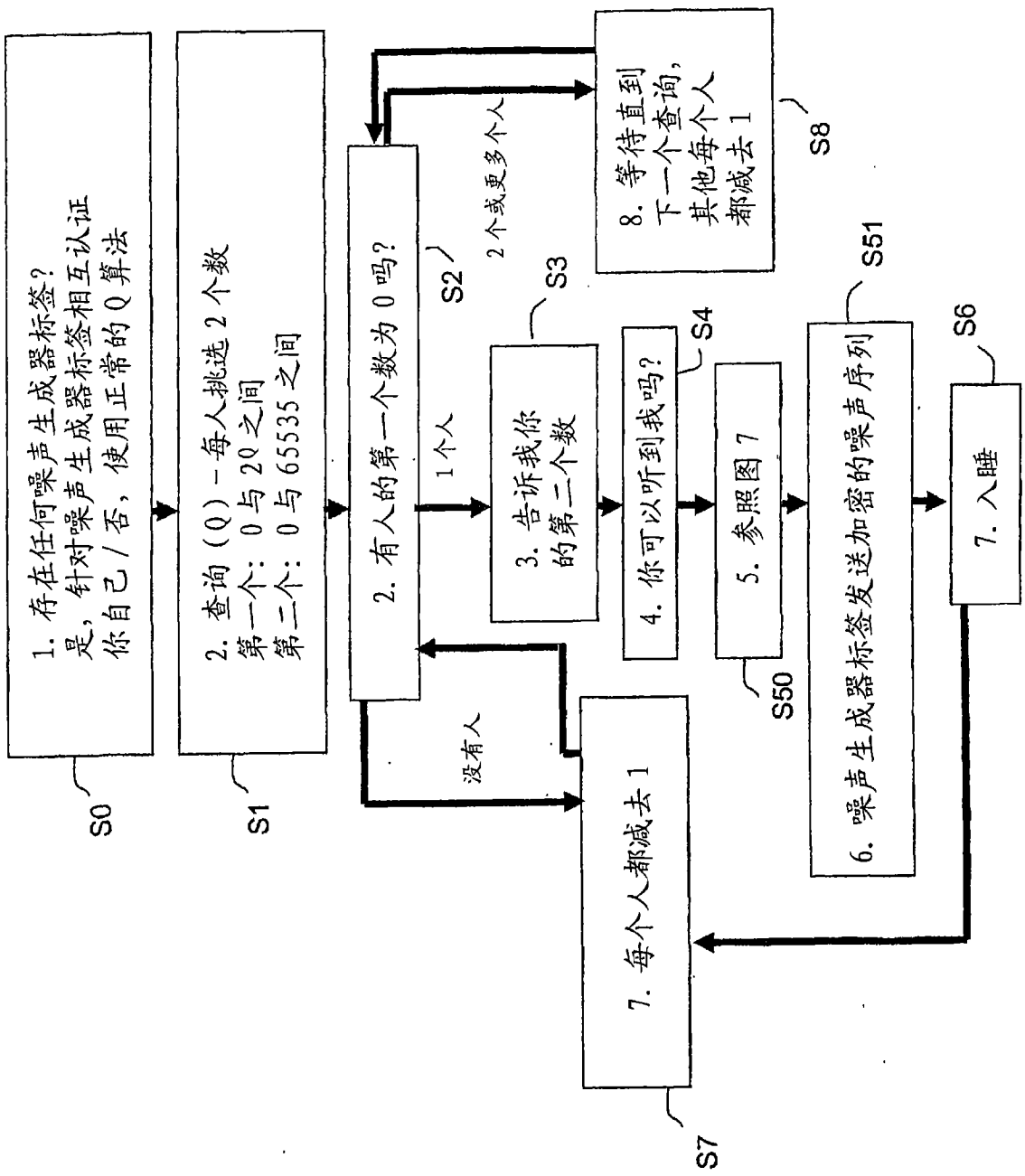

1. 存在任何噪声生成器标签？
是，针对噪声生成器标签相互认证
你自己 / 否，使用正常的 Q 算法
S0
2. 查询 (Q) - 每人挑选 2 个数
第一个：0 与 2^Q 之间
第二个：0 与 65535 之间
S1
2. 有人的第一个数为 0 吗？
S2
1 个人
2 个或更多个人
没有人
3. 告诉我你的第二个数
S3
4. 你可以听到我吗？
S4
5. 参照图 7
S50
6. 噪声生成器标签发送加密的噪声序列
S51
7. 入睡
S6
7. 每个人都减去 1
S7
8. 等待直到下一个查询，其他每个人都减去 1
S8

图 6

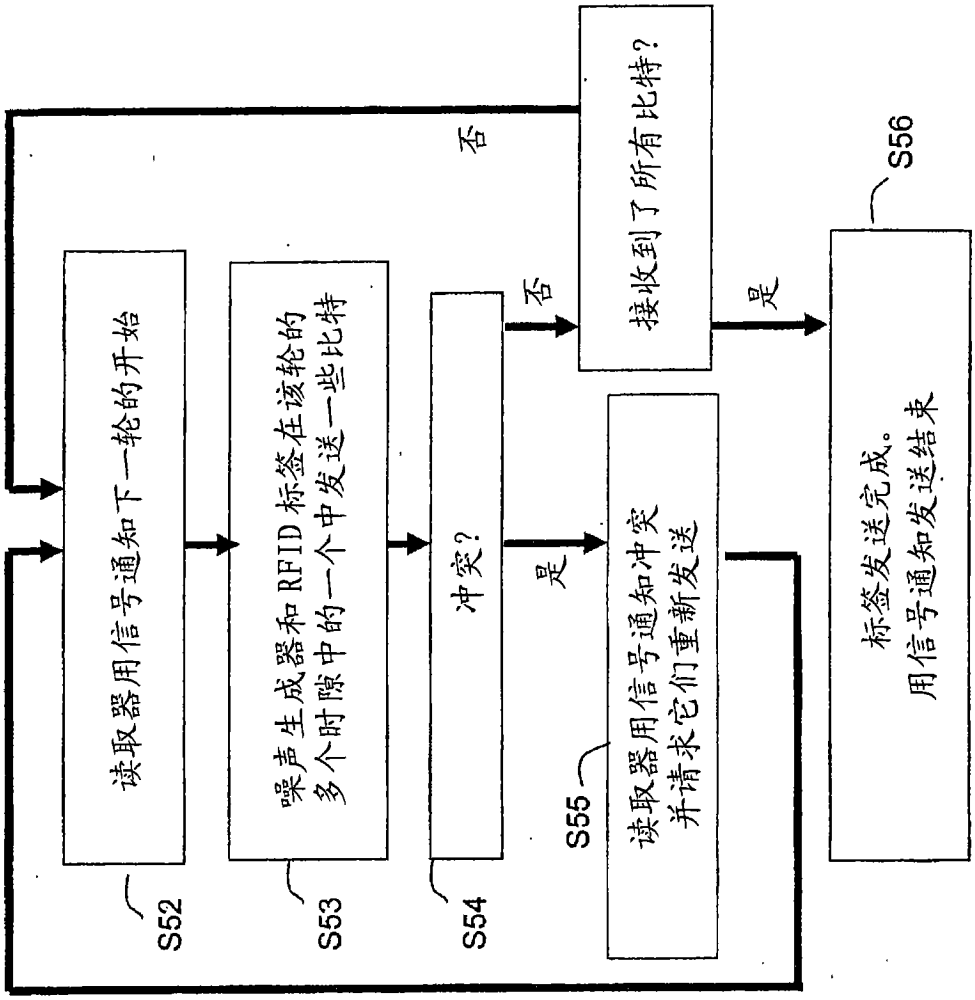

读取器用信号通知下一轮的开始
S52
噪声生成器和 RFID 标签在该轮的多个时隙中的一个中发送一些比特
S53
冲突?
S54
是
否
读取器用信号通知冲突并请求它们重新发送
S55
接收到了所有比特?
否
是
标签发送完成。用信号通知发送结束
S56

图 7