(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 102355356 A
(43)申请公布日 2012.02.15

(21)申请号 201110309726.X

(22)申请日 2011.10.13

(71)申请人 国电南京自动化股份有限公司
地址 210009 江苏省南京市鼓楼区新模范马路 38 号

(72)发明人 杨春瑜 徐大可 张雷

(74)专利代理机构 南京纵横知识产权代理有限公司 32224
代理人 董建林 许婉静

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04W 12/02(2009.01)

权利要求书 1 页 说明书 3 页

(54)发明名称

一种适用于 ZIGBEE 无线抄表的非对称加密方法

(57)摘要

本发明公开了一种适用于 ZIGBEE 无线抄表的非对称加密方法，包括以下步骤：步骤一：中心节点和终端节点在硬件初始化时，使用 RSA 算法中特定的 p、q 和 e 生成相同的公钥和密钥，这样中心节点和终端节点都保存了一份公钥和密钥，公钥用来给消息加密，私钥用来给消息解密；步骤二：当中心节点发送消息给终端节点时，先使用公钥给数据加密，然后发送给终端节点；步骤三：当终端节点收到数据后，使用私钥解密数据并还原成原始消息；当终端节点给中心节点发送消息时，也采用步骤二至步骤三的步骤。本发明将 RSA 非对称加密方法的可靠性的优点与 ZIGBEE 无线传输每帧数据量少的特点相结合，有效的提高无线传输的安全性。

CN 102355356 A

1. 一种适用于 ZIGBEE 无线抄表的非对称加密方法，包括以下步骤：

步骤一：中心节点和终端节点在硬件初始化时，使用 RSA 算法中特定的 p、q 和 e 生成相同的公钥和密钥，这样中心节点和终端节点都保存了一份公钥和密钥，公钥用来给消息加密，私钥用来给消息解密；

步骤二：当中心节点发送消息给终端节点时，先使用公钥给数据加密，然后发送给终端节点；

步骤三：当终端节点收到数据后，使用私钥解密数据并还原成原始消息；

当终端节点给中心节点发送消息时，也采用步骤二至步骤三的步骤。

一种适用于 ZIGBEE 无线抄表的非对称加密方法

技术领域

[0001] 本发明涉及一种无线通信以及传输加密方法。具体涉及到一种适用于 ZIGBEE 无线抄表的非对称加密方法。

背景技术

[0002] ZIGBEE 技术是近几年兴起的一种面向自动化和无线控制的双向无线通信技术。它具有近距离、低数据速率、低复杂度、低功耗、低成本的特点。ZIGBEE 无线可使用的频段有 3 个，分别是 2.4GHz 的 ISM(Industrial Scientific Medical) 频段、美国的 915MHz 频段、以及欧洲的 868MHz 频段。在中国采用 2.4GHz 频段，是免申请和免使用费的频率。它的传输速率为 20kb/s~250kb/s，传输距离为 10m~75m。它依据 802.15.4 标准，在数千个微小的传感器之间相互协调实现通信。这些传感器只需要很少的能量，以接力的方式通过无线电波将数据从一个传感器传到另一个传感器，所以通信效率非常高。而较低数据速率以及较小通信范围的特点决定了它适合于承载数据流量较小的业务，主要应用领域包括无线数据采集、无线工业控制、消费性电子设备、汽车自动化、家庭和楼宇自动化、医用设备控制、远程网络控制等场合。此外，ZIGBEE 采取了 IEEE 802.15.4 强有力的无线物理层所具有的全部优点：省电、简单、成本低的规格，增加了逻辑网络、网络安全和应用层。

[0003] ZIGBEE 安全技术是基于一组 128 位的密钥实现的，使用 AES-128 分块加密。在数据加密过程中，可以使用三种基本密钥。分别是主密钥、链接密钥和网络密钥。主密钥可以在设备制造时安装，也可以通过信任中心设置，或者是基于用户访问的数据，例如，个人识别码 (PIN)、口令和密码等。主密钥是两个设备长期安全通信的基础，也可以作为一般的链接密钥使用。所以，必须维护主密钥的保密性和正确性。当在网络传输过程中，采用主密钥可以阻止窃听。链接密钥是在一个 PAN 网络中被两个设备共享的，它可以通过主密钥建立，也可以在设备制造时安装。网络密钥可以通过信任中心设置，也可以在设备制造时安装。它可应用在数据链路层、网络层和应用层。链接密钥和网络密钥不断地进行周期性的更新。当两个设备都拥有这两种密钥时，采用链接密钥进行通信。由于安全机制是基于共享密钥，网络的安全保障主要依赖于初始化安全和所有密钥的存储安全。

[0004] 然而，在应用中对称密钥的使用需要分发到上百个设备节点上，这存在很大的安全隐患，而且 AES 加密方法的更多缺陷会在以后日益显现。对数据加密和交换密钥都使用单一的对称加密方法或许会成为 ZIGBEE 安全结构中的薄弱点。基于这个原因，使用非对称加密方法来分发密钥期待能有所扩展。

发明内容

[0005] 本发明的目的在于解决对称加密方法密钥单一的缺点，提出一种在 ZIGBEE 中使用的非对称加密方法。

[0006] 本发明采用的技术方案为：利用 RSA 非对称方法，在发送端用公钥对发出的数据进行加密，在接收端用私钥对接收的数据进行解密。方法包括以下内容：

一种适用于 ZIGBEE 无线抄表的非对称加密方法，包括以下步骤：

步骤一：中心节点和终端节点在硬件初始化时，使用 RSA 算法中特定的 p、q 和 e 生成相同的公钥和密钥，这样中心节点和终端节点都保存了一份公钥和密钥，公钥用来给消息加密，私钥用来给消息解密；

步骤二：当中心节点发送消息给终端节点时，先使用公钥给数据加密，然后发送给终端节点；

步骤三：当终端节点收到数据后，使用私钥解密数据并还原成原始消息。

[0007] 当终端节点给中心节点发送消息时，也将采用相同的步骤。

[0008] 本发明技术方案的显著性进步和特点主要体现在：将 RSA 非对称加密方法的可靠性的优点与 ZIGBEE 无线传输每帧数据量少的特点相结合，有效的提高无线传输的安全性。由于 ZIGBEE 网络的 20-250kb/s 整体传输速率，当网络中的节点数量为 100 个节点时，每个节点的速率小于 2kb/s。而 RSA 加密的密钥长度需要至少 1024 bits，此时受到图像数据比较大的限制，ZIGBEE 网络将承载不了这种传输需求。因此本发明采用 ZIGBEE 网络传输极小数据量的抄表数据（小于 kb 级），网络容量可以达到 100 个节点的规模，RSA 的密钥长度可以达到 2048 bits，增强了安全性。

具体实施方式

[0009] 所谓非对称，是指该方法需要一对密钥，使用其中一个加密，则需要用另一个才能解密。RSA 方法是其中一种非对称密码方法。

[0010] 一：生成公钥和私钥

1. 取两个随机大的质数 p 和 q，p 不等于 q，计算 N=p*q；
2. 根据欧拉函数，不大于 N 且与 N 互质的整数个数为 (p-1)*(q-1)；
3. 随机选取一个整数 e 与 (p-1)*(q-1) 互质，并且 e 小于 (p-1)*(q-1)；
4. 用以下公式计算 d：d*e ≡ 1 (mod (p-1)*(q-1))；
5. 将 p 和 q 的记录销毁。

[0011] 由此，(N, e) 是公钥，(N, d) 是私钥，(N, d) 是秘密的。发送方用公钥 (N, e) 加密发送的数据，用私钥 (N, d) 解密接收到的数据。

[0012] 二：加密消息

假设中心节点想给终端节点发送消息 m，它知道公钥 (N, e)。它使用预先与终端节点约定的格式将 m 转换为一个小于 N 的整数 n，比如将 m 表示十六进制码，然后将这些十六进制码连在一起组成一个数字。然后用下面这个公式将 n 加密为 c：

$$n^e \equiv c \pmod{N}$$

中心节点计算出 c 后就可以将 c 发送给终端节点。

[0013] 三：解密消息

终端节点接收到消息 c 后就可以利用私钥 (N, d) 来解码。可以用以下公式来将 c 转换为 n：

$$n^e \equiv c \pmod{N}$$

得到 n 后，终端节点可以将 n 还原成原始消息 m。

[0014] RSA 方法历史悠久容易说明，且同时可用作加解密。而 RSA 的速度决定了它一般用于少量数据加密。

[0015] 综上所述，结合 RSA 非对称加密方法后，能够更加安全地在 ZIGBEE 无线网络中传输数据。

[0016] 以上所述，仅是本发明的较佳实施例子而已，并非对本发明作任何形式上的限制，凡是依据本发明的技术实质对以上实施例所作的任何简单修改、等同变化与装饰，均仍属于本发明技术方案的范围内。