(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 102546184 B
(45)授权公告日 2015.05.27

(21)申请号 201210037995.X

(22)申请日 2012.02.17

(73)专利权人 北京海联捷讯科技股份有限公司
地址 100176 北京市大兴区北京经济技术开发区经海二路29号院7号楼二层202-1

(72)发明人 陈春丽 孙岩

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 蒋雅洁 王黎延

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 9/06(2006.01)

(56)对比文件
CN 101547132 A,2009.09.30,
CN 102355356 A,2012.02.15,
CN 101080896 A,2007.11.28,
CN 1667999 A,2005.09.14,

审查员 万沙沙

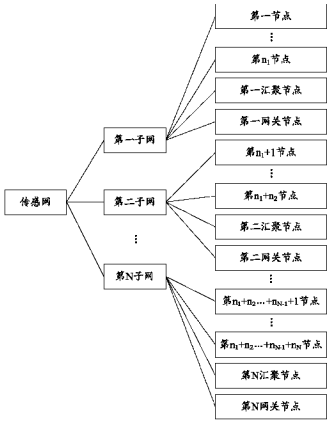
权利要求书4页 说明书12页 附图9页

(54)发明名称

传感网内消息安全传输或密钥分发的方法和系统

(57)摘要

本发明提供了一种传感网内的消息安全传输的方法，属于传感网的同一子网的所有节点均使用一个相同的安全密钥进行消息的加密传输与安全认证，并且属于不同的子网的节点所使用的安全密钥互不相同，不同的子网之间通过各个子网的网关节点进行消息传输，以及一种安全密钥分发方法，对将要被分发的安全密钥进行加密和认证，本发明还提供了一种传感网内的消息安全传输的系统和一种安全密钥分发系统，本发明提供的方法和系统解决了传感网的连通性和安全性无法共存以及在安全密钥的更新的过程中存在瞬间弱点的问题。



CN 102546184 B

1. 一种传感网内的消息安全传输的方法，其特征在于，包括：

属于传感网的同一子网的所有节点均使用一个相同的安全密钥进行消息的加密传输与安全认证；

属于不同子网的节点所使用的安全密钥互不相同，并且不同的子网之间通过各个子网的网关节点进行消息传输；

为各子网的信任中心及与其所属同一子网的所有节点都分别分配一个相同的加密校验密钥和一个相同的解密校验密钥，其中，能够根据所述加密校验密钥使用 RSA 算法对一个原始密钥进行加密得到加密后的密钥，然后根据所述解密校验密钥使用 RSA 算法对所述加密后的密钥进行解密，从而将所述加密后的密钥恢复为原始密钥；

所述信任中心根据其加密校验密钥，使用 RSA 算法，对待分发的安全密钥进行加密，然后将加密后的安全密钥发送至所述子网的所有节点；

所述子网的任一节点在接收到加密后的安全密钥后，根据其解密安全密钥，使用 RSA 算法对加密后的安全密钥进行解密，得到解密后的安全密钥，并根据其加密校验密钥对解密后的安全密钥进行加密并得到认证密钥，如果认证密钥与解密后的安全密钥相同，则将其安全密钥替换为解密后的安全密钥。

2. 根据权利要求 1 所述的方法，其特征在于，具体包括：属于传感网的同一子网的所有节点均使用一种对称密钥加密算法进行所述同一子网内节点的消息加密传输与安全认证操作；属于不同子网的节点，采用传统互联网的加密方式，进行所述子网之间的消息传输操作。

3. 根据权利要求 2 所述的方法，其特征在于，所述对称密钥加密算法为高级加密标准 AES 算法，则同一子网中的两个节点之间进行消息的加密传输与安全认证的操作包括：

消息源节点根据其安全密钥使用高级加密标准 AES 算法，对将要被发送的原始消息进行计算并得到原始认证码，并根据其安全密钥使用 AES 算法对原始认证码和原始消息分别进行加密并得到加密后的消息和加密后的认证码，然后将加密后的消息和加密后的认证码发送至消息目的节点；

消息目的节点接收到加密后的消息和加密后的认证码之后，根据其安全密钥使用 AES 算法对加密后的消息和加密后的认证码进行解密，得到解密后的消息和解密后的认证码，然后根据其安全密钥使用 AES 算法对解密后的消息进行计算并得到校验认证码，并判断校验认证码与解密后的认证码是否相同，如果相同，则保存解密后的数据。

4. 根据权利要求 1 所述的方法，其特征在于，入网申请节点申请进入所述传感网的一个子网时，该方法还包括：

入网节点根据其安全密钥使用 AES 算法，对入网申请消息进行计算并得到原始入网申请认证码，以及根据其安全密钥使用 AES 算法对入网申请消息和原始入网申请认证码分别进行加密，从而得到加密后的入网申请消息和加密后的入网申请认证码，并将加密后的入网申请消息和加密后的入网申请认证码发送至该入网节点要进入的子网的信任中心；

所述信任中心在接收到加密后的入网申请消息和加密后的入网申请认证码后，根据其安全密钥，使用 AES 算法对接收到的加密后的入网申请消息和加密后的入网申请认证码分别进行解密，得到解密后的入网申请消息和解密后的入网申请认证码，并判断接收到的加密后的入网申请消息是否有效，如果有效，则向所述入网节点发送允许入网命令。

5. 根据权利要求 4 所述的方法，其特征在于，所述信任中心向所述入网节点发送允许入网命令包括：

信任中心根据其安全密钥，使用 AES 算法，对其所述允许入网命令进行计算并得到命令认证码，以及根据其安全密钥使用 AES 算法对所述允许入网命令和所述命令认证码分别进行加密，从而得到加密后的允许入网命令和加密后的命令认证码，并将它们发送至入网节点；

入网节点在接收到加密后的允许入网命令和加密后的命令认证码后，根据其安全密钥，使用 AES 算法，对接收到的加密后的允许入网命令和加密后的命令认证码分别进行解密，得到解密后的允许入网命令和解密后的命令认证码，并判断接收到的加密后的允许入网命令是否有效，如果有效，则入网节点接下来进行入网操作。

6. 根据权利要求 1 至 5 任一所述的方法，其特征在于，还包括：

所述信任中心在将加密后的安全密钥发送至所述子网的所有节点之前、同时或之后还需要将其安全密钥替换为被分发的安全密钥。

7. 一种安全密钥分发方法，其特征在于，包括：

为分发密钥的信任中心和所有密钥接收节点都分别分配一个相同的加密校验密钥和一个相同的解密校验密钥，其中，能够根据所述加密校验密钥使用 RSA 算法对一个原始密钥进行加密得到加密后的密钥，然后根据所述解密校验密钥使用 RSA 算法对所述加密后的密钥进行解密，从而将所述加密后的密钥恢复为原始密钥；

所述信任中心根据其加密校验密钥，使用 RSA 算法，对待分发的安全密钥进行加密，然后将加密后的安全密钥发送至所有密钥接收节点；

所述密钥接收节点在接收到加密后的安全密钥后，根据其解密安全密钥，使用 RSA 算法对加密后的安全密钥进行解密，得到解密后的安全密钥，并根据其加密校验密钥对解密后的安全密钥进行加密并得到认证密钥，如果认证密钥与解密后的安全密钥相同，则将其安全密钥替换为解密后的安全密钥。

8. 一种传感网内消息安全传输系统，其特征在于，包括：

一个或多个子网，其中，每个子网都包括一个或多个节点、一个汇聚节点、一个网关节点以及一个信任中心；

属于传感网的同一子网的所有节点均具有一个相同的安全密钥，基于该安全密钥进行子网内消息的加密传输与安全认证；

属于不同子网的节点具有不同的安全密钥；所述网关节点用于所述子网之间的消息传输；

所有除信任中心以外的节点均分别包括一个密钥接收模块，每一个信任中心都包括一个密钥发送模块，其中，

每一个密钥发送模块和密钥接收模块都具有一个相同的加密校验密钥和一个相同的解密校验密钥，并且能够根据所述加密校验密钥使用 RSA 算法对一个原始密钥进行加密得到加密后的密钥，然后根据所述解密校验密钥使用 RSA 算法对这个加密后的密钥进行解密，从而将这个加密后的密钥恢复为原始密钥；

密钥发送模块，用于根据其加密校验密钥，使用 RSA 算法，对将要被分发的安全密钥进行加密，并将加密后的安全密钥发送至与其所属节点同在一个子网的除信任中心以外的所

有节点的密钥接收模块；

密钥接收模块，用于在接收到加密后的安全密钥后，根据其解密安全密钥，使用 RSA 算法对加密后的安全密钥进行解密，得到解密后的安全密钥，并根据其加密校验密钥对解密后的安全密钥进行加密并得到认证密钥，如果认证密钥与所述解密后的安全密钥相同，则将其所属节点的安全密钥替换为解密后的安全密钥。

9. 根据权利要求 8 所述的系统，其特征在于，所有的节点都还包含一个消息发送模块和一个消息接收模块，其中，

消息发送模块，用于根据其所属节点的安全密钥，使用 AES 算法对将要被发送的消息进行计算并得到原始认证码，以及根据其所属节点的安全密钥，使用 AES 算法对将要被发送的消息和原始认证码分别进行加密，从而得到加密后的消息和加密后的认证码，然后将加密后的消息和加密后的认证码发送至与该消息发送模块所属的节点同在一个子网的接收所述消息的节点的消息接收模块；

消息接收模块，用于在接收到加密后的消息和加密后的认证码后，根据其所属节点的安全密钥，使用 AES 算法对接收到的加密后的消息和加密后的认证码进行解密，得到解密后的消息和解密后的认证码，并判断接收到的加密后的消息的有效性，如果有效，则保存解密后的消息。

10. 根据权利要求 8 或 9 所述的系统，其特征在于，所述系统还包括一个或多个入网节点，其中，

每一个入网节点都包含一个入网申请模块，每一个信任中心都包含一个入网认证模块；

入网申请模块，用于根据其所属的入网节点的安全密钥，使用 AES 算法，对入网申请消息进行计算并得到原始入网申请认证码，以及根据其所属的入网节点的安全密钥，使用 AES 算法对入网申请消息和原始入网申请认证码分别进行加密，从而得到加密后的入网申请消息和加密后的入网申请认证码，并将加密后的入网申请消息和加密后的入网申请认证码发送至与其所属节点同在一个子网的信任中心的入网认证模块；

入网认证模块，用于在接收到加密后的入网申请消息和加密后的入网申请认证码后，根据其所属的信任中心的安全密钥，使用 AES 算法对接收到的加密后的入网申请消息和加密后的入网申请认证码分别进行解密，得到解密后的入网申请消息和解密后的入网申请认证码，并判断接收到的加密后的入网申请消息是否有效，如果有效，则向所述入网申请模块发送允许入网命令，否则，拒绝所述入网申请模块所属的入网节点进入该入网认证模块所属的信任中心所在的子网。

11. 根据权利要求 10 所述的系统，其特征在于，每一个信任中心都还具有一个命令发送模块，每一个入网节点都还具有一个命令接收模块，

命令发送模块用于向其所属的信任中心的入网认证模块获取所述允许入网命令，然后根据其所属的信任中心的安全密钥，使用 AES 算法，对所述允许入网命令进行计算并得到命令认证码，以及根据其所属的信任中心的安全密钥，使用 AES 算法对所述允许入网命令和所述命令认证码分别进行加密，并将得到的加密后的允许入网命令和加密后的命令认证码发送至发送入网申请的入网节点的命令接收模块；

命令接收模块用于在接收到加密后的允许入网命令和加密后的命令认证码后，根据其

所属节点的安全密钥，使用 AES 算法，对接收到的加密后的允许入网命令和加密后的命令认证码分别进行解密，得到解密后的允许入网命令和解密后的命令认证码，并判断接收到的加密后的允许入网命令是否有效，如果有效，则该命令接收模块所属的入网节点接下来进行入网操作。

12. 根据权利要求 8 或 9 所述的系统，其特征在于，密钥发送模块，在发送所述加密后的安全密钥的同时、之前或之后还需要将其所属的信任中心的安全密钥替换为将要被分发的安全密钥。

13. 一种安全密钥分发系统，其特征在于，包括 ：一个或多个节点，以及一个信任中心，其中，

各个除信任中心以外的节点均分别具有一个密钥接收模块，所述信任中心具有一个密钥发送模块 ；

所述密钥发送模块都具有一个相同的加密校验密钥和一个相同的解密校验密钥，并且能够根据所述加密校验密钥使用 RSA 算法对一个原始密钥进行加密得到加密后的密钥，然后根据所述解密校验密钥使用 RSA 算法对这个加密后的密钥进行解密，从而将这个加密后的密钥恢复为原始密钥 ；

所述密钥发送模块，用于根据其加密校验密钥，使用 RSA 算法，对将要被分发的安全密钥进行加密，并将加密后的安全密钥发送至所有的密钥接收模块，并且在将加密后的安全密钥发送至所有密钥接收模块的之前、同时或之后还需要将其所述的信任中心的安全密钥替换为将要被分发的安全密钥 ；

所述密钥接收模块，用于在接收到加密后的安全密钥后，根据其解密安全密钥，使用 RSA 算法对加密后的安全密钥进行解密，得到解密后的安全密钥，并根据其加密校验密钥对解密后的安全密钥进行加密并得到认证密钥，如果认证密钥与解密后的安全密钥相同，则将其所属节点的安全密钥替换为解密后的安全密钥。

传感网内消息安全传输或密钥分发的方法和系统

技术领域

[0001] 本发明涉及物联网中的传感网，尤其涉及传感网内消息安全传输或密钥分发的方法和系统。

背景技术

[0002] 物联网 (IOT, Internet of Things)，是通过射频识别、红外感应器、全球定位系统、激光扫描器等信息传感设备，把物品与互联网相连接，以实现对物品的智能化识别、定位、跟踪、监控和管理的一种网络。物联网的推广可以给人们的生活带来便利，提高工作效率，改变人们的生活方式。但是，因为在物联网中传输的消息具有种类繁多和消息量大的特点，使得网络攻击者可以采用多种攻击方式对物联网进行网络攻击，所以物联网存在较多的安全问题，并且，由于在物联网中传输的消息的私密性需要受到保护，因此要想以信息化和商业化的方式使用物联网，就需要解决物联网的安全问题。

[0003] 物联网体系架构通常包含三个层次，由下至上依次为感知层、网络层和应用层。其中，物联网的网络层和应用层分别与互联网的网络层和应用层类似，特别地，当前的物联网的网络层和应用层的功能主要就是分别由互联网的网络层和应用层来实现的。由于当前互联网的各个层次的安全问题已经得到了很好的解决，因此，目前需要解决的是物联网的感知层存在的安全问题。

[0004] 传感网是物联网的一部分，位于物联网的感知层，图 1 为现有技术的传感网网络结构示意图，如图 1 所示，传感网由多个传感网子网（以下简称子网）组成，其中每一个子网都是由多个普通节点、至少一个汇聚 (Sink) 节点以及至少一个网关节点组成的，传感网的基本工作方式包括：普通节点之间通过紫蜂 (Zigbee) 协议进行消息传输；普通节点与汇聚节点之间直接或者以多跳转发的方式进行消息传输；汇聚节点与网关节点之间通过 Zigbee 协议进行消息传输；各个网关节点之间以及网关节点与传感网网络服务器（以下简称服务器）之间以有线的方式进行消息传输。

[0005] 如图 1 所示，由于各个子网之间存在信息交互，即属于不同子网的普通节点之间存在信息交互，所以，如果一个子网的连通性变差，例如，一个子网由于受到了网络攻击而关闭，使得这个子网的普通节点无法与属于其他子网的普通节点进行信息交互，则在与这个子网存在信息交互的其他子网中进行的消息传输就会受到阻碍，进而导致传感网的连通性变差。此外，如果一个子网由于受到了网络攻击，而使得在这个子网中传输的消息的安全性降低，则在与这个子网存在信息交互的子网中传输的消息的安全性就会降低，导致传感网的安全性降低，例如，如果网络攻击者获得了一个子网的消息接收的权限，则可以利用该权限获得与这个子网存在信息交互的子网发送来的消息。

[0006] 目前，没有能够保证传感网的连通性和安全性共存的有效的解决方案，其中传感网的连通性和安全性共存是指：在传感网中进行的消息传输不受到阻碍，并且在传感网中传输的消息是安全的。

[0007] 此外，在传感网中，通常使用安全密钥来保护在传感网中传输的消息，即为传感网

的每一个节点都分配一个安全密钥，在消息传输的过程中使用这个安全密钥对所传输的消息进行加密和解密，并且还需要对安全密钥进行更新，此时，传感网还需要具有至少一个信任中心节点（以下简称信任中心）；其中，信任中心通常为 Zigbee 网络协调器，更新安全密钥指的是：由传感网的信任中心向传感网中需要进行安全密钥更新的节点发送新的安全密钥，需要进行安全密钥更新的节点接收到新的安全密钥后，替换其旧的安全密钥的过程。但是在更新安全密钥的过程中会存在瞬间弱点，即在传感网的信任中心向需要更新安全密钥的节点发送新的安全密钥的过程中，这个安全密钥会被网络攻击者监听到并且截获，进而导致在传感网中传输的消息失去安全密钥的保护。

发明内容

[0008] 有鉴于此，本发明的主要目的在于提供传感网内消息安全传输的方法和系统，用于保证传感网的连通性与安全性的共存，以及提供安全密钥分发方法和系统，用于解决在进行安全密钥更新的过程中存在瞬间弱点的问题。

[0009] 为达到上述目的，本发明的技术方案是这样实现的：

[0010] 根据本发明的实施例，提供了一种传感网内的消息安全传输的方法，所述方法包括：

[0011] 属于传感网的同一子网的所有节点均使用一个相同的安全密钥进行消息的加密传输与安全认证；

[0012] 属于不同子网的节点所使用的安全密钥互不相同，并且不同的子网之间通过各个子网的网关节点进行消息传输。

[0013] 根据本发明的实施例，提供了一种安全密钥分发方法，所述方法包括：

[0014] 为分发密钥的信任中心和所有密钥接收节点都分别分配一个相同的加密校验密钥和一个相同的解密校验密钥，其中，能够根据所述加密校验密钥使用 RSA 算法对一个原始密钥进行加密得到加密后的密钥，然后根据所述解密校验密钥使用 RSA 算法对所述加密后的密钥进行解密，从而将所述加密后的密钥恢复为原始密钥；

[0015] 所述信任中心根据其加密校验密钥，使用 RSA 算法，对待分发的安全密钥进行加密，然后将加密后的安全密钥发送至所有密钥接收节点；

[0016] 所述密钥接收节点在接收到加密后的安全密钥后，根据其解密安全密钥，使用 RSA 算法对加密后的安全密钥进行解密，得到解密后的安全密钥，并根据其加密校验密钥对解密后的安全密钥进行加密并得到认证密钥，如果认证密钥与解密后的安全密钥相同，则将其安全密钥替换为解密后的安全密钥。

[0017] 根据本发明的实施例，提供了一种传感网内消息安全传输系统，所述系统包括：

[0018] 一个或多个子网，其中，每个子网都包括一个或多个节点、一个汇聚节点、以及一个网关节点；

[0019] 属于传感网的同一子网的所有节点均具有一个相同的安全密钥，基于该安全密钥进行子网内消息的加密传输与安全认证；

[0020] 属于不同子网的节点具有不同的安全密钥；所述网关节点用于所述子网之间的消息传输。

[0021] 根据本发明的实施例，提供了一种安全密钥分发系统，所述系统包括：一个或多个

节点，以及一个信任中心，其中，

[0022] 各个除信任中心以外的节点均分别具有一个密钥接收模块，所述信任中心具有一个密钥发送模块；

[0023] 所述密钥发送模块都具有一个相同的加密校验密钥和一个相同的解密校验密钥，并且能够根据所述加密校验密钥使用 RSA 算法对一个原始密钥进行加密得到加密后的密钥，然后根据所述解密校验密钥使用 RSA 算法对这个加密后的密钥进行解密，从而将这个加密后的密钥恢复为原始密钥；

[0024] 所述密钥发送模块，用于根据其加密校验密钥，使用 RSA 算法，对将要被分发的安全密钥进行加密，并将加密后的安全密钥发送至所有的密钥接收模块，并且在将加密后的安全密钥发送至所有密钥接收模块的之前、同时或之后还需要将其所述的信任中心的安全密钥替换为将要被分发的安全密钥；

[0025] 所述密钥接收模块，用于在接收到加密后的安全密钥后，根据其解密安全密钥，使用 RSA 算法对加密后的安全密钥进行解密，得到解密后的安全密钥，并根据其加密校验密钥对解密后的安全密钥进行加密并得到认证密钥，如果认证密钥与解密后的安全密钥相同，则将其所属节点的安全密钥替换为解密后的安全密钥。

[0026] 通过使用本发明的方法和系统，将传感网分成一个或多个子网，并且同一子网的所有节点均使用一个相同的安全密钥进行消息的加密传输与安全认证。由于采用上述方法和系统避免了各个子网的普通节点之间的直接信息交互，因此保证了传感网的连通性。同时，属于不同子网的节点所使用的安全密钥互不相同，并且不同的子网之间通过各个子网的网关节点进行消息传输，优选地，采用本发明的安全密钥更新方法进行安全密钥的更新，这样保证了传感网的安全性并且避免了，例如，通过传感网的一个子网的权限获得其他子网中的消息的问题，以及在更新安全密钥的过程中会存在瞬间弱点的问题，进而增强了传感网的安全性。

附图说明

[0027] 图 1 为现有技术的传感网网络结构示意图；

[0028] 图 2 为根据本发明的传感网内消息安全传输的方法的网络拓扑结构示意图；

[0029] 图 3 为根据本发明的传感网内消息安全传输的方法，在属于传感网的同一子网的两个节点之间进行消息的加密传输与安全认证的流程示意图；

[0030] 图 4 为根据本发明的传感网内消息安全传输的方法，在一个节点申请进入传感网的一个子网时，所述子网的信任中心对由该节点发送的入网申请消息进行安全认证的流程示意图；

[0031] 图 5 为根据本发明的传感网内消息安全传输的方法，在一个节点进入传感网的一个子网时，所述子网的信任中心对由该节点发送的入网申请消息进行安全认证的另一个流程示意图；

[0032] 图 6 为根据本发明的安全密钥分发方法，对传感网的密钥接收节点的安全密钥进行更新的流程示意图；

[0033] 图 7 为根据本发明的传感网内消息安全传输的方法的另一网络拓扑结构示意图；

[0034] 图 8 为本发明的传感网内消息安全传输系统的结构示意图；

[0035] 图 9 为本发明的一种安全密钥分发系统的结构示意图。

具体实施方式

[0036] 本发明的核心思想是：属于传感网的同一子网的所有节点均使用一个相同的安全密钥进行消息的加密传输与安全认证；属于不同子网的节点所使用的安全密钥互不相同，并且不同的子网之间通过各个子网的网关节点进行消息传输；以及使用一种安全密钥分发方法对传感网中的节点的安全密钥进行更新。

[0037] 需要说明的是，在不冲突的情况下，本发明中的实施例及实施例中的特征可以相互组合。下面将结合附图来详细说明本发明。

[0038] 本发明提供了一种传感网内消息安全传输的方法，具体包括：在同一子网中，所有的节点均使用一个相同的安全密钥进行消息的加密传输与安全认证；属于不同子网的节点所使用的安全密钥互不相同，并且不同的子网之间通过各个子网的网关节点进行消息传输。

[0039] 具体地，属于传感网的同一子网的所有节点均使用一种对称密钥加密算法进行所述同一子网内节点的消息加密传输与安全认证操作；属于不同子网的节点，采用传统互联网的加密方式，进行所述子网之间的消息传输操作。

[0040] 实施例 1

[0041] 图 2 为根据本发明的传感网内消息安全传输的方法的网络拓扑结构示意图，如图 2 所示，传感网由 N 个子网组成，包括第一子网、第二子网 ..... 和第 N 子网。第一节点 .....、第 n_1 节点、第一汇聚节点、第一网关节点均为第一子网的节点，第 n_1+1 节点 .....、第 n_1+n_2 节点、第二汇聚节点、第二网关节点均为第二子网的节点 .....，第 $n_1+n_2...+n_{N-1}+1$ 节点 .....、第 $n_1+n_2...+n_{N-1}+n_N$ 节点、第 N 汇聚节点、第 N 网关节点均为第 N 子网的节点，并且，n_1、$n_2...$、n_{N-1}、n_N 和 N 均为自然数，

[0042] 其中，在第一子网内，第一节点 .....、第 n_1 节点、第一汇聚节点、第一网关节点均使用一个相同的安全密钥 K_1，在第二子网内，第 n_1+1 节点 .....、第 n_1+n_2 节点、第二汇聚节点、第二网关节点均使用一个相同的安全密钥 K_2.....，在第 N 子网内，第 $n_1+n_2...+n_{N-1}+1$ 节点 .....、第 $n_1+n_2...+n_{N-1}+n_N$ 节点、第 N 汇聚节点、第 N 网关节点均使用一个相同的安全密钥 K_N，安全密钥 K_1、K_2.....、K_N 互不相同；属于第一子网的节点之间使用安全密钥 K_1 进行消息的加密传输与安全认证，属于第二子网的节点之间使用 K_2 进行消息的加密传输与安全认证 .....，属于第 N 子网的节点之间使用 K_n 进行消息的加密传输与安全认证。

[0043] 为了使传感网的子网之间可以进行数据传输，每一个子网都还包括了一个或多个汇聚节点以及一个或多个网关节点，优选地为每个子网设置一个汇聚节点和一个网关节点，如图 2 所示，第一子网具有第一汇聚节点和第一网关节点，第二子网具有第二汇聚节点和第二网关节点 .....，第 N 子网具有第 N 汇聚节点和第 N 网关节点，同时，第一子网、第二子网 .....、第 N 子网之间通过第一网关节点、第二网关节点 ..... 和第 N 网关节点进行消息传输。此外，上述汇聚节点和网关节点还用于子网与服务器之间的消息传输。其中，由于第一网关节点、第二网关节点 ..... 和第 N 网关节点之间，以及这些节点与服务器之间的消息传输是在物联网的网络层进行的，所以可以采用传统的加密方式对传输的消息进行加密，例如，使用安全套接层 (SSL，Security Socket Layer) 协议中规定的公开密钥的加密

技术进行加密，使这些消息能更安全地传输。

[0044] 实施例 2

[0045] 图 3 为根据本发明的传感网内消息安全传输的方法，在属于传感网的同一子网的两个节点之间进行消息的加密传输与安全认证的流程示意图，为了方便说明，将上述两个节点分别称为消息源节点和消息目的节点，如图 3 所示，所述流程包括如下步骤：

[0046] 步骤 101：消息源节点根据其安全密钥使用高级加密标准 (AES，Advanced Encryption Standard) 算法对原始消息 D_0 进行加密和计算，得到加密后的消息 D_1 和加密后的认证码 T_1，

[0047] 具体地，消息源节点根据其安全密钥使用 AES 算法对原始消息 D_0 进行计算得到原始认证码 T_0，之后再根据其安全密钥使用 AES 算法对原始认证码 T_0 和原始消息 D_0 分别进行加密，得到加密后的认证码 T_1 和加密后的消息 D_1；加密后的认证码 T_1 用来在接收消息的时候判断加密后的消息 D_1 的有效性；

[0048] 在本实施例中的使用 AES 算法对原始消息进行计算并得到原始认证码，以及使用 AES 算法进行加密和解密的操作都可以是由整合了 AES 算法的芯片来完成的；消息源节点的安全密钥可以是预先设置的，在本实施例中，消息源节点的安全密钥为 K_1；AES 算法是一种对称密钥加密算法，即在对数据进行加密和解密的过程中使用的密钥是相同的，使用 AES 算法进行加密和计算的具体实现过程是本领域所公知的，这里将不再赘述；另外，

[0049] 使用 AES 算法对原始消息进行计算并得到原始认证码，以及对原始消息或原始认证码进行加密的操作都是与安全密钥密切相关的，根据不同的安全密钥使用 AES 算法对同一消息进行加密后得到的加密后的消息是不同的，同样根据不同的安全密钥使用 AES 算法对同一消息进行计算得到的认证码也是不同的；

[0050] 步骤 102：消息源节点以 Zigbee 无线传输的方式将加密后的消息 D_1 和加密后的认证码 T_1 发送至消息目的节点，该消息目的节点与消息源节点属于同一子网；

[0051] 步骤 103：消息目的节点接收到由消息源节点发送的加密后的消息 D_1 和加密后的认证码 T_1 后，使用 AES 算法对接收到的加密后的消息 D_1 和加密后的认证码 T_1 分别进行解密得到解密后的消息 D_2 和解密后的认证码 T_2，其中，

[0052] 在进行解密时使用的安全密钥为消息目的节点的安全密钥，消息目的节点的安全密钥也是预先设置的，在本实施例中，由于消息目的节点和消息源节点在同一子网中，所以消息目的节点的安全密钥也为 K_1；

[0053] 步骤 104：消息目的节点根据解密后的认证码 T_2 对接收到的加密后的消息 D_1 的有效性进行判断，如果 D_1 是有效的，则执行步骤 105，否则，执行步骤 106，其中，

[0054] 根据解密后的认证码 T_2 判断接收到的加密后的消息 D_1 是否有效包括：消息目的节点根据其安全密钥 K_1 使用 AES 算法对解密后的消息 D_2 进行计算并且得到认证码 T_2'；如果 T_2 与 T_2' 相同，则表示接收到的加密后的消息 D_1 有效，否则，表示接收到的加密后的消息 D_1 是无效的；

[0055] 步骤 105：消息目的节点保存解密后的消息 D_2；

[0056] 步骤 106：当前流程结束。

[0057] 实施例 3

[0058] 图 4 为根据本发明的传感网内消息安全传输的方法，在一个节点申请进入传感网

的一个子网时，所述子网的信任中心对由该节点发送的入网申请消息进行安全认证的流程示意图，本实施例的传感网的每个子网中都至少有一个信任中心，所述信任中心用于对其接收到的入网申请消息进行安全认证。

[0059] 这里，为了方便说明，将上述申请入网的节点称为入网节点，本实施例是在接收入网申请消息的一个子网内进行的，在该子网中，包括信任中心在内的所有节点都具有一个相同的安全密钥，该安全密钥为 K_2，并且所述入网节点具有安全密钥 k_2。如图 4 所示，所述流程包括如下的步骤：

[0060] 步骤 201：入网节点生成一个入网申请消息 M_0，并根据其安全密钥 k_2 使用 AES 算法对入网申请消息 M_0 进行计算和加密，得到加密后的入网申请消息 M_1 和加密后的认证码 P_1，

[0061] 具体地，入网节点根据其安全密钥 k_2 使用 AES 算法对入网申请消息 M_0 进行计算并得到原始认证码 P_0，之后再根据其安全密钥使用 AES 算法对入网申请消息 M_0 和原始认证码 P_0 分别进行加密，得到加密后的入网申请消息 M_1 和加密后的认证码 P_1；加密后的认证码 P_1 用来在信任中心接收到加密后的入网申请消息 M_1 之后判断加密后的入网申请消息 M_1 的有效性；

[0062] 在本实施例中的使用 AES 算法对入网申请消息进行计算并得到原始认证码，对入网申请消息或原始认证码进行加密以及对加密后的入网申请消息或认证码进行解密的操作也都可以是由上述整合了 AES 算法的芯片来完成的；入网节点的安全密钥可以是管理员预先设置的，合法的入网节点与信任中心的安全密钥应该是相同的，即 K_2 与 k_2 相同；此外，在本实施例中关于 AES 算法的描述与实施例 2 中描述的相关内容相同，这里将不再赘述；

[0063] 步骤 202：入网节点以 Zigbee 无线传输的方式将加密后的入网申请消息 M_1 和加密后的认证码 P_1 进行全网广播，其中，

[0064] 入网节点将加密后的入网申请消息 M_1 和加密后的认证码 P_1 进行全网广播具体包括：入网节点将加密后的入网申请消息 M_1 和加密后的认证码 P_1 发送至所述入网节点申请加入的子网中的所有节点；

[0065] 步骤 203：信任中心以监听的方式接收到加密后的入网申请消息 M_1 和加密后的认证码 P_1 后，使用 AES 解密算法对加密后的入网申请消息 M_1 和加密后的认证码 P_1 进行解密，得到解密后的入网申请 M_2 和解密后的认证码 P_2，其中，在解密的过程中使用的安全密钥为信任中心的安全密钥 K_2；

[0066] 步骤 204：信任中心对接收到的加密后的入网申请消息 M_1 的有效性进行判断，如果 M_1 是有效的，则执行步骤 205，否则，拒绝所述入网节点进入所述信任中心所在的子网，其中，

[0067] 信任中心判断接收到的加密后的入网申请消息 M_1 是否有效包括：信任中心根据其安全密钥 K_2 使用 AES 算法对解密后的入网申请 M_2 进行计算，得到认证码 P_2'，如果 P_2 与 P_2' 相同，则表示加密后的入网申请消息 M_1 有效，否则，表示加密后的入网申请消息 M_1 是无效的；

[0068] 步骤 205：信任中心以无线单播传输的方式，向入网节点发送入网许可命令；

[0069] 步骤 206：入网节点收到入网许可命令后，进行入网操作，进入子网。

[0070] 实施例 4

[0071] 在实施例 3 的步骤 205 中，由于信任中心向入网节点发送的入网许可命令本质上

也是一种类型的消息，因此信任中心向入网节点发送入网许可命令的操作，也可以采用与实施例 2 的消息传输与安全认证的流程相类似的步骤来进行。

[0072] 图 5 为根据本发明的传感网内消息安全传输的方法，在一个节点进入传感网的一个子网时，所述子网的信任中心对由该节点发送的入网申请消息进行安全认证的另一个流程示意图，为了方便说明，也将上述申请入网的节点称为入网节点，其中入网节点和信任中心的安全密钥的设置以及使用 AES 算法进行计算、加密和解密的操作与实施例 3 中描述的相同，这里将不再赘述，如图 5 所示，所述流程包括如下的步骤：

[0073] 步骤 301 至步骤 304 与实施例 2 中的步骤 201 至步骤 204 相同；

[0074] 步骤 305：信任中心使用 AES 算法对入网许可命令进行计算，得到入网许可认证码，之后使用 AES 算法对入网许可命令和入网许可认证码分别进行加密，并将加密后得到的加密后的入网许可命令和加密后的入网许可认证码以无线单播传输的方式发送给入网节点，其中，使用 AES 算法进行计算和加密时所使用的安全密钥均为信任中心的安全密钥；

[0075] 步骤 306：入网节点接收到加密后的入网许可命令和加密后的入网许可认证码后，根据其安全密钥，使用 AES 算法对接收到的加密后的入网许可命令和加密后的入网许可认证码分别进行解密，得到解密后的入网许可命令和解密后的入网许可认证码；

[0076] 步骤 307：入网节点对接收到的加密后的入网许可命令的有效性进行判断，如果有效，则入网节点进行入网操作，否则，流程结束，其中，

[0077] 入网节点对接收到的加密后的入网许可命令的有效性进行判断包括：入网节点根据其安全密钥使用 AES 算法对解密后的入网许可命令进行计算得到一个比较认证码，如果这个比较认证码与解密后的入网许可认证码相同，则表示加密后的入网许可命令是有效的，否则，表示加密后的入网许可命令是无效的。

[0078] 实施例 5

[0079] 本发明还提供了一种安全密钥分发方法来对传感网中的节点的安全密钥进行更新，具体包括：在传感网中，使用信任中心进行安全密钥的分发，为信任中心以及所有需要更新安全密钥的节点（以下简称为密钥接收节点）都分别分配一对相同的校验密钥，所述校验密钥对包括一个加密校验密钥和一个解密校验密钥，并且这对校验密钥是相互关联的，即可以根据加密校验密钥使用一种加密算法对一个原始安全密钥进行加密得到加密后的安全密钥，然后可以根据解密校验密钥使用该加密算法对这个加密后的安全密钥进行解密，从而将这个加密后的安全密钥恢复为原始安全密钥；分发密钥的信任中心，根据其加密校验密钥，使用一种加密算法，对将要分发给密钥接收节点的安全密钥（以下简称为新密钥）进行加密得到加密后的新密钥，并将加密后的新密钥以 Zigbee 无线传输的方式发送至所有密钥接收节点；密钥接收节点接收到加密后的新密钥后，根据其解密校验密钥对加密后的新密钥进行解密和有效性的判断，如果加密后的新密钥有效，则将其安全密钥替换为解密后的新密钥。

[0080] 图 6 为根据本发明的安全密钥分发方法，对传感网的密钥接收节点的安全密钥进行更新的流程示意图，如图 6 所示，所述流程的步骤如下：

[0081] 步骤 401：为信任中心和所有密钥接收节点都分别分配一对相同的校验密钥，所述校验密钥对包括一个加密校验密钥 Key_1 和一个解密校验密钥 Key_2，其中，

[0082] 能够根据加密校验密钥 Key_1 使用一种加密算法，本实例优选为 RSA(Ron Rivest，

Adi Shamirh,LenAdleman）算法，对一个原始密钥进行加密得到加密后的密钥，然后根据解密校验密钥 Key_2 使用 RSA 算法对加密后的密钥进行解密，从而将加密后的密钥恢复为原始密钥；

[0083] 进行网络规划时，由管理员为信任中心和所有密钥接收节点分别分配一对相同的校验密钥；

[0084] 步骤 402：设置新密钥为 k_1，分发密钥的信任中心根据加密校验密钥 Key_1 使用 RSA 算法对新密钥 k_1 进行加密，从而得到加密后的新密钥 k_1'；

[0085] 步骤 403：分发密钥的信任中心将加密后的新密钥 k_1' 以 Zigbee 无线传输的方式发送至密钥接收节点；

[0086] 步骤 404：密钥接收节点接收到加密后的新密钥 k_1' 后，根据其解密校验密钥 Key_2 使用 RSA 算法进行解密，从而得到解密后的新密钥 k_1"；

[0087] 步骤 405：密钥接收节点判断解密后的新密钥 k_1" 的有效性，如果有效则执行步骤 406，否则，密钥更新的流程结束，

[0088] 具体地，密钥接收节点根据其加密校验密钥 Key_1 使用 RSA 算法对解密后的新密钥 k_1" 进行加密，得到认证密钥 k，如果 k 与 k_1' 相同则表示解密后的新密钥 k_1" 是有效的，则执行步骤 406，否则，表示解密后的新密钥 k_1" 是无效的，则密钥更新的流程结束；

[0089] 步骤 406：密钥接收节点将其安全密钥替换为解密后的新密钥 k_1"。

[0090] 实施例 6

[0091] 在实施例 1 的基础上，采用实施例 5 中的安全密钥分发方法，对实施例 1 中的安全密钥 K_1.....、K_n 进行更新，以进一步提高传感网的消息传输的安全性，并且避免在进行安全密钥更新的过程存在的瞬间弱点。

[0092] 图 7 为根据本发明的传感网内消息安全传输的方法的另一网络拓扑结构示意图，如图 7 所示，与图 2 描述的传感网类似，传感网也是由 N 个子网组成，包括第一子网、第二子网 ..... 和第 N 子网，另外，每一个子网还包括一个信任中心，

[0093] 其中，第一子网内，第一节点.....、第 n_1 节点、第一汇聚节点、第一网关节点和第一信任中心均使用一个相同的安全密钥 K_1.....，在第 N 子网内，第 $n_1+n_2.....+n_{N-1}+1$ 节点.....、第 $n_1+n_2.....+n_{N-1}+n_N$ 节点、第 N 汇聚节点、第 N 网关节点和第 N 信任中心均使用一个相同的安全密钥 K_N，安全密钥 K_1、K_2.....、K_N 互不相同，下面以第一子网为例，对传感网的安全密钥的更新过程进行说明。

[0094] 在第一子网中，为所有节点都分配一对校验密钥 Key_1、Key_2，所述校验密钥对的说明与实施例 5 中的相关描述相同，这里将不再赘述。将安全密钥 k_1 作为新密钥，第一信任中心将第一节点、第二节点.....、第 n_1 节点、第一汇聚节点、第一网关节点的安全密钥更新为新密钥 k_1，具体的更新流程与实施例 5 的安全密钥更新流程相似，这里将不再赘述；

[0095] 此外，在上述操作过程中，第一信任中心还需要将安全密钥 K_1 更新为 k_1，这个操作可在第一信任中心向第一节点、第二节点.....、第 n_1 节点、第一汇聚节点、第一网关节点发送加密后的新的安全密钥之前、同时或之后进行。

[0096] 实施例 7

[0097] 图 8 为本发明的传感网内消息安全传输系统的结构示意图，如图 8 所示，所述系统包括：第一子网、第二子网.....、第 N 子网，其中，

[0098] 第一节点……、第 n_1 节点、第一汇聚节点、第一网关节点均为第一子网的节点，第 n_1+1 节点……、第 n_1+n_2 节点、第二汇聚节点、第二网关节点均为第二子网的节点……，第 n_1+n_2...+n_{N-1}+1 节点……、第 n_1+n_2...+n_{N-1}+n_N 节点、第 N 汇聚节点、第 N 网关节点均为第 N 子网的节点；第一节点……、第 n_1 节点、第一汇聚节点、第一网关节点均具有一个相同的安全密钥 K_1、第 n_1+1 节点……、第 n_1+n_2 节点、第二汇聚节点、第二网关节点均具有一个相同的安全密钥 K_2……，第 n_1+n_2...+n_{N-1}+1 节点……、第 n_1+n_2...+n_{N-1}+n_N 节点、第 N 汇聚节点、第 N 网关节点均具有一个相同的安全密钥 K_N，安全密钥 K_1，K_2……，K_N 互不相同；并且，第一子网、第二子网……、第 N 子网之间通过第一网关节点、第二网关节点…… 和第 N 网关节点进行消息传输。其中，n_1、n_2...、n_{N-1}、n_N、N 均为自然数。此外，上述汇聚节点和网关节点还用于子网与服务器之间的消息传输。

[0099] 实施例 8

[0100] 在图 8 描述的消息安全传输的系统中，所有的节点都可包含一个消息发送模块和一个消息接收模块，其中，

[0101] 消息发送模块，用于根据其所属节点的安全密钥，使用 AES 算法对将要被发送的消息进行计算并得到原始认证码，以及根据其所属节点的安全密钥，使用 AES 算法对将要被发送的消息和原始认证码分别进行加密，从而得到加密后的消息和加密后的认证码，然后将加密后的消息和加密后的认证码发送至与该消息发送模块所属的节点同在一个子网的接收所述消息的另一节点的消息接收模块；

[0102] 消息接收模块，用于在接收到加密后的消息和加密后的认证码后，根据其所属节点的安全密钥，使用 AES 算法对接收到的加密后的消息和加密后的认证码进行解密，得到解密后的消息和解密后的认证码，并判断接收到的加密后的消息的有效性，如果有效，则保存解密后的消息，否则，不保存解密后的消息，其中，

[0103] 判断加密后的消息是否有效包括：消息接收模块根据其所属节点的安全密钥，使用 AES 算法对解密后的消息进行计算得到消息校验认证码，如果消息校验认证码与解密后的认证码相同，则表示接收到的加密后的数据是有效的，否则，表示接收到的加密后的数据是无效的；

[0104] 此外，在上述系统中，关于 AES 算法的说明与实施例 2 中的相关描述的相同，这里将不再赘述。

[0105] 实施例 9

[0106] 在图 8 描述的消息安全传输的系统中，所有的子网都还可以包含一个信任中心，所述系统还包括一个或多个入网节点，其中，

[0107] 每一个入网节点都包含一个入网申请模块，每一个信任中心都包含一个入网认证模块；

[0108] 入网申请模块，用于根据其所属的入网节点的安全密钥，使用 AES 算法，对所述入网申请消息进行计算并得到原始入网申请认证码，以及根据其所属的入网节点的安全密钥，使用 AES 算法对入网申请消息和原始入网申请认证码分别进行加密，从而得到加密后的入网申请消息和加密后的入网申请认证码，并将加密后的入网申请消息和加密后的入网申请认证码发送至与其所属节点同在一个子网的信任中心的入网认证模块；

[0109] 入网认证模块，用于在接收到加密后的入网申请消息和加密后的入网认证码后，

根据其所属的信任中心的安全密钥，使用 AES 算法对接收到的加密后的入网申请消息和加密后的入网认证码分别进行解密，得到解密后的入网申请消息和解密后的入网认证码，并判断接收到的加密后的入网申请消息是否有效，如果有效，则向所述入网申请模块发送允许入网命令，否则，拒绝所述入网申请模块所属的入网节点进入该入网认证模块所属的信任中心所在的子网，其中，

[0110] 判断接收到的加密后的入网申请是否有效包括：所述入网认证模块根据其所属的信任中心的安全密钥，使用 AES 算法对解密后的入网申请消息进行计算得到入网校验认证码，如果入网校验认证码与解密后的认证码相同则表示接收到的加密后的入网申请消息是有效的，否则，表示接收到的加密后的入网申请消息是无效的；

[0111] 此外，在上述系统中，关于使用 AES 算法的说明与实施例 2 中描述的相同，这里将不再赘述。

[0112] 实施例 10

[0113] 在根据实施例 9 所述的系统中，每一个信任中心都还具有一个命令发送模块，每一个入网节点都还具有一个命令接收模块，

[0114] 命令发送模块，用于向其所属的信任中心的入网认证模块获取所述允许入网命令，然后根据其所属的信任中心的安全密钥，使用 AES 算法，对所述允许入网命令进行计算并得到命令认证码，以及根据其所属的信任中心的安全密钥，使用 AES 算法对所述允许入网命令和所述命令认证码分别进行加密，从而得到加密后的允许入网命令和加密后的命令认证码，并将它们发送至发送入网申请的所述入网节点的命令接收模块；

[0115] 命令接收模块，用于在接收到加密后的允许入网命令和加密后的命令认证码后，根据其所属节点的安全密钥，使用 AES 算法，对接收到的加密后的允许入网命令和加密后的命令认证码分别进行解密，得到解密后的允许入网命令和解密后的命令认证码，并判断接收到的加密后的允许入网命令是否有效，如果有效，则该命令接收模块所属的入网节点接下来进行入网操作，否则，命令接收模块所属的入网节点不进行入网操作，其中，

[0116] 判断接收到的加密后的允许入网命令是否有效的操作包括：命令接收模块根据其所属的入网节点的安全密钥，使用 AES 算法对解密后的允许入网命令进行计算得到命令校验认证码，如果命令校验认证码与解密后的命令认证码相同则表示接收到的加密后的允许入网命令是有效的，否则，表示接收到的加密后的允许入网命令是无效的；

[0117] 此外，在上述系统中，关于使用 AES 算法的说明与实施例 2 中的相关描述相同，这里将不再赘述。

[0118] 实施例 11

[0119] 图 9 为本发明的一种安全密钥分发系统的结构示意图，如图 9 所示，包括：第一节点、第二节点 ..... 第 n_1 节点、第一信任中心，其中，

[0120] 第一节点、第二节点 ..... 第 n_1 节点分别具有第一密钥接收模块、第二密钥接收模块 ..... 第 n_1 密钥接收模块，第一信任中心具有第一密钥发送模块；

[0121] 第一密钥接收模块、第二密钥接收模块 ..... 第 n_1 密钥接收模块和第一密钥发送模块都具有一个相同的加密校验密钥和一个相同的解密校验密钥，并且能够根据所述加密校验密钥使用 RSA 算法对一个原始密钥进行加密得到加密后的密钥，然后根据所述解密校验密钥使用 RSA 算法对这个加密后的密钥进行解密，从而将这个加密后的密钥恢复为原

始密钥；

[0122] 第一密钥发送模块，用于根据其加密校验密钥，使用 RSA 算法，对将要被分发的安全密钥进行加密，并将加密后的安全密钥发送至所有的密钥接收模块，并且在将加密后的安全密钥发送至所有密钥接收模块的之前、同时或之后还需要将其所述的信任中心的安全密钥替换为将要被分发的安全密钥；

[0123] 第一密钥接收模块、第二密钥接收模块 ..... 或第 n_1 密钥接收模块，用于在接收到加密后的安全密钥后，根据其解密安全密钥，使用 RSA 算法对加密后的安全密钥进行解密，得到解密后的安全密钥，并根据其加密校验密钥对解密后的安全密钥进行加密并得到认证密钥，如果认证密钥与解密后的安全密钥相同，则将其所属节点的安全密钥替换为解密后的安全密钥；其中，

[0124] RSA 算法是本领域所公知的，这里将不再赘述。

[0125] 实施例 12

[0126] 图 9 所示的安全密钥分发系统还可以应用在图 8 所示的消息安全传输系统中。在图 8 所示的系统的基础上，为第一子网、第二子网 ..... 和第 N 子网都分别设置一个信任中心，第一节点 .....、第 n_1 节点 .....、第 $n_1+n_2...+n_{N-1}+n_N$ 节点、第一汇聚节点 .....、第 N 汇聚节点、第一网关节点 ..... 和第 N 网关节点都分别包括一个密钥接收模块，每一个信任中心都还包括一个密钥发送模块，其中，

[0127] 每一个密钥发送模块和密钥接收模块都具有一个相同的加密校验密钥和一个相同的解密校验密钥，并且能够根据所述加密校验密钥使用 RSA 算法对一个原始密钥进行加密得到加密后的密钥，然后根据所述解密校验密钥使用 RSA 算法对这个加密后的密钥进行解密，从而将这个加密后的密钥恢复为原始密钥；

[0128] 密钥发送模块，用于根据其加密校验密钥，使用 RSA 算法，对将要被分发的安全密钥进行加密，并将加密后的安全密钥发送至与其所属节点同在一个子网的除信任中心以外的所有节点的密钥接收模块，在密钥发送模块发送所述加密后的安全密钥的同时、之前或之后还需要将其所属的信任中心的安全密钥替换为将要被分发的安全密钥；

[0129] 密钥接收模块，用于在接收到加密后的安全密钥后，根据其解密安全密钥，使用 RSA 算法对加密后的安全密钥进行解密，得到解密后的安全密钥，并根据其加密校验密钥对解密后的安全密钥进行加密并得到认证密钥，如果认证密钥与所述解密后的安全密钥相同，则将其所属节点的安全密钥替换为解密后的安全密钥；其中，

[0130] RSA 算法是本领域所公知的，这里将不再赘述。

[0131] 本发明提供的传感网内的消息安全传输的方法和系统，在传感网的同一子网中，所有的节点均使用一个相同的安全密钥进行消息的加密传输与安全认证，提高了在传感网中传输的消息的安全性，同时属于不同的子网的节点所使用的安全密钥互不相同，并且不同的子网之间通过各个子网的网关节点进行消息传输，降低了在消息传输过程中不同子网之间的互相干扰，这样同时保证了传感网的连通性和安全性。此外，本发明提供的安全密钥分发方法和系统，对被分发的安全密钥进行加密，这保证了被分发的安全密钥的安全性，从而解决了在安全密钥的更新的过程中存在瞬间弱点的问题。

[0132] 以上所述，仅为本发明的较佳实施例而已，并非用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。在不违背本发明精神实质和原则的基础上，所

做的各种修改、等同替换以及改进等，均在包含在本发明的保护范围之内。

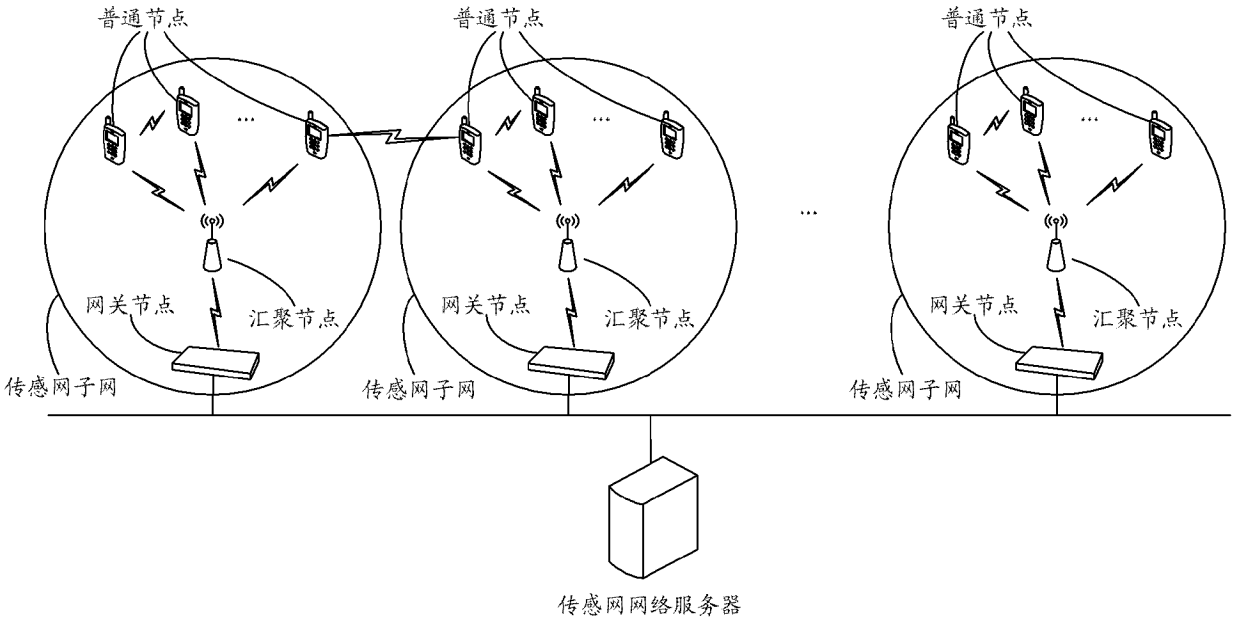

普通节点
普通节点
普通节点
网关节点
汇聚节点
网关节点
汇聚节点
网关节点
汇聚节点
传感网子网
传感网子网
传感网子网
传感网网络服务器

图 1

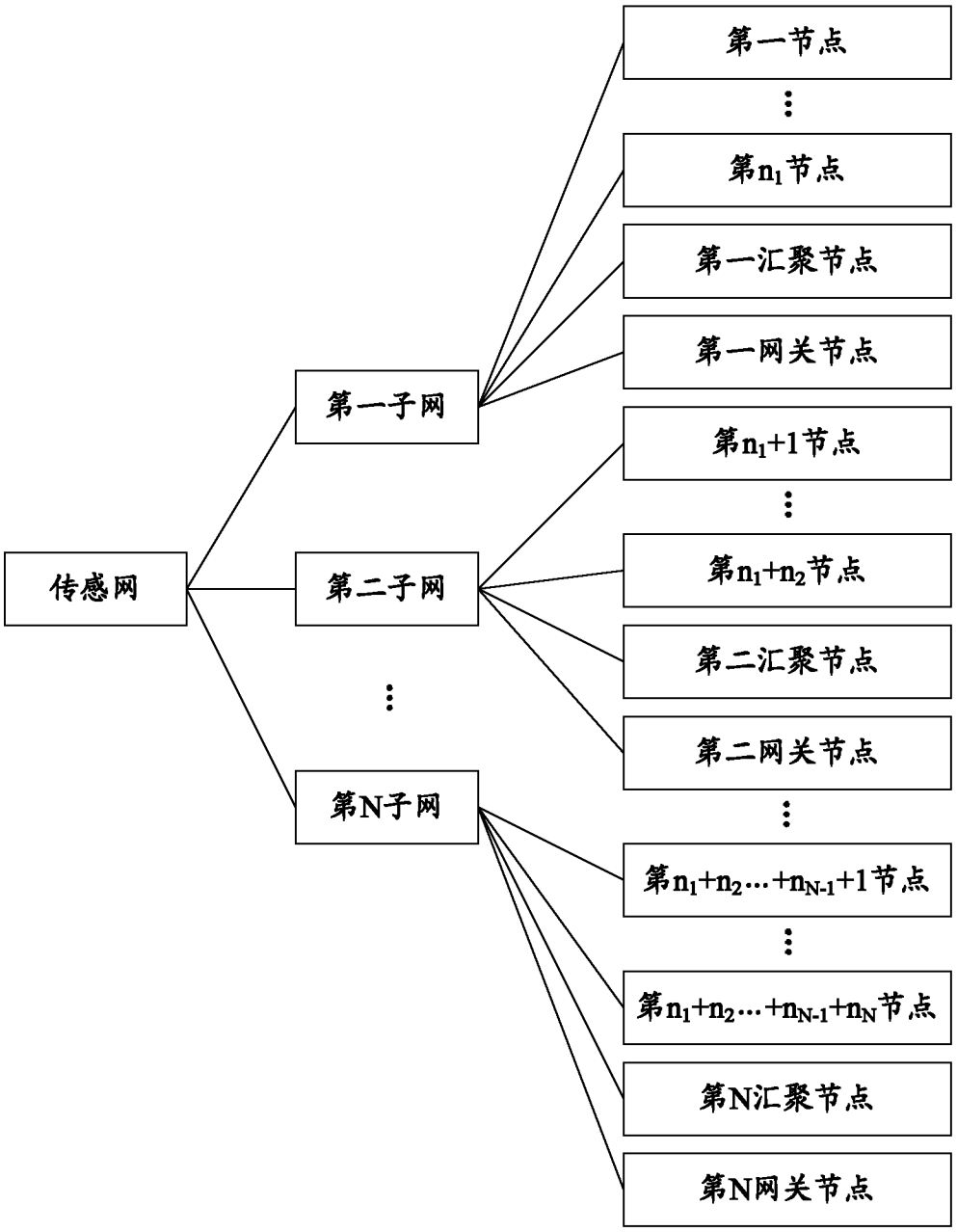

传感网
第一子网
第二子网
第N子网
第一节点
第n_1节点
第一汇聚节点
第一网关节点
第n_1+1节点
第n_1+n_2节点
第二汇聚节点
第二网关节点
第n_1+n_2…+n_{N-1}+1节点
第n_1+n_2…+n_{N-1}+n_N节点
第N汇聚节点
第N网关节点

图 2

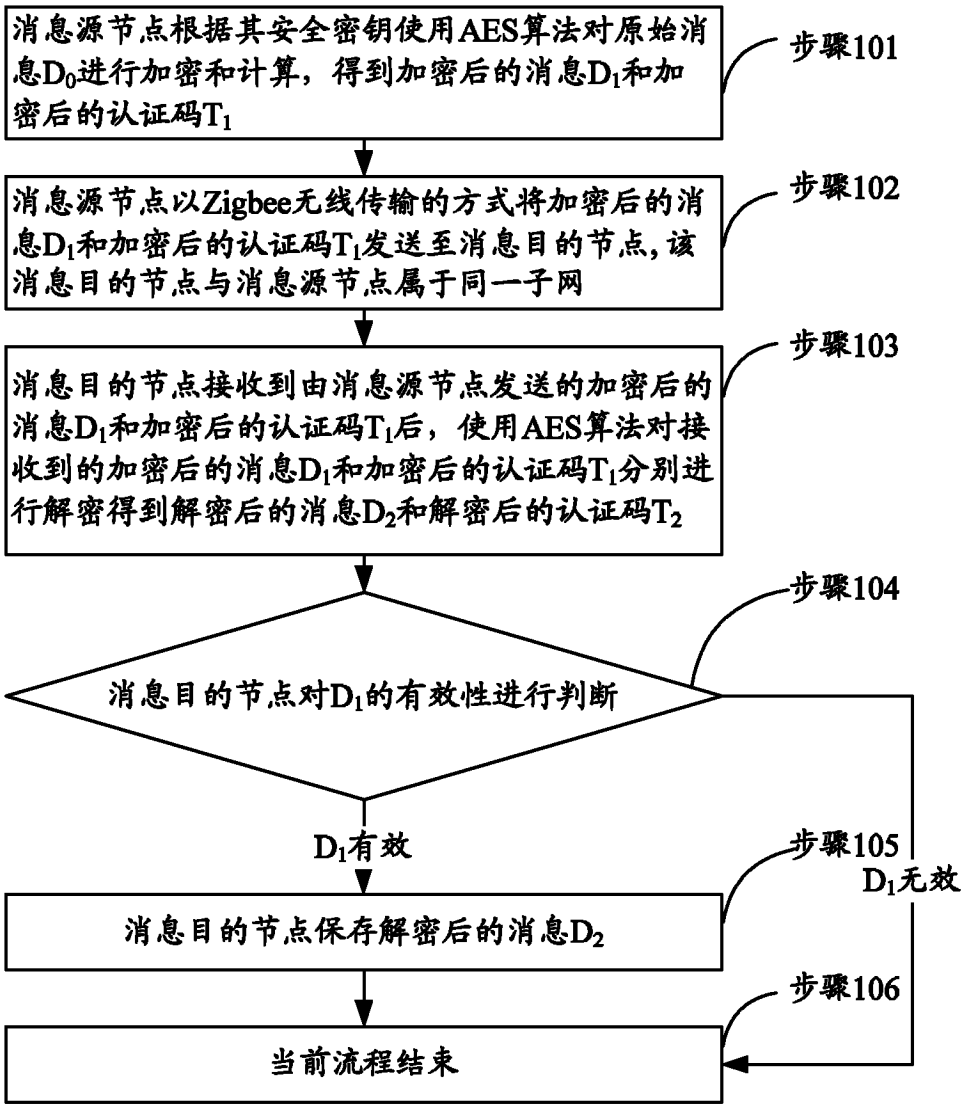

消息源节点根据其安全密钥使用AES算法对原始消息D_0进行加密和计算，得到加密后的消息D_1和加密后的认证码T_1
步骤101
消息源节点以Zigbee无线传输的方式将加密后的消息D_1和加密后的认证码T_1发送至消息目的节点，该消息目的节点与消息源节点属于同一子网
步骤102
消息目的节点接收到由消息源节点发送的加密后的消息D_1和加密后的认证码T_1后，使用AES算法对接收到的加密后的消息D_1和加密后的认证码T_1分别进行解密得到解密后的消息D_2和解密后的认证码T_2
步骤103
消息目的节点对D_1的有效性进行判断
步骤104
D_1有效
D_1无效
消息目的节点保存解密后的消息D_2
步骤105
当前流程结束
步骤106

图 3

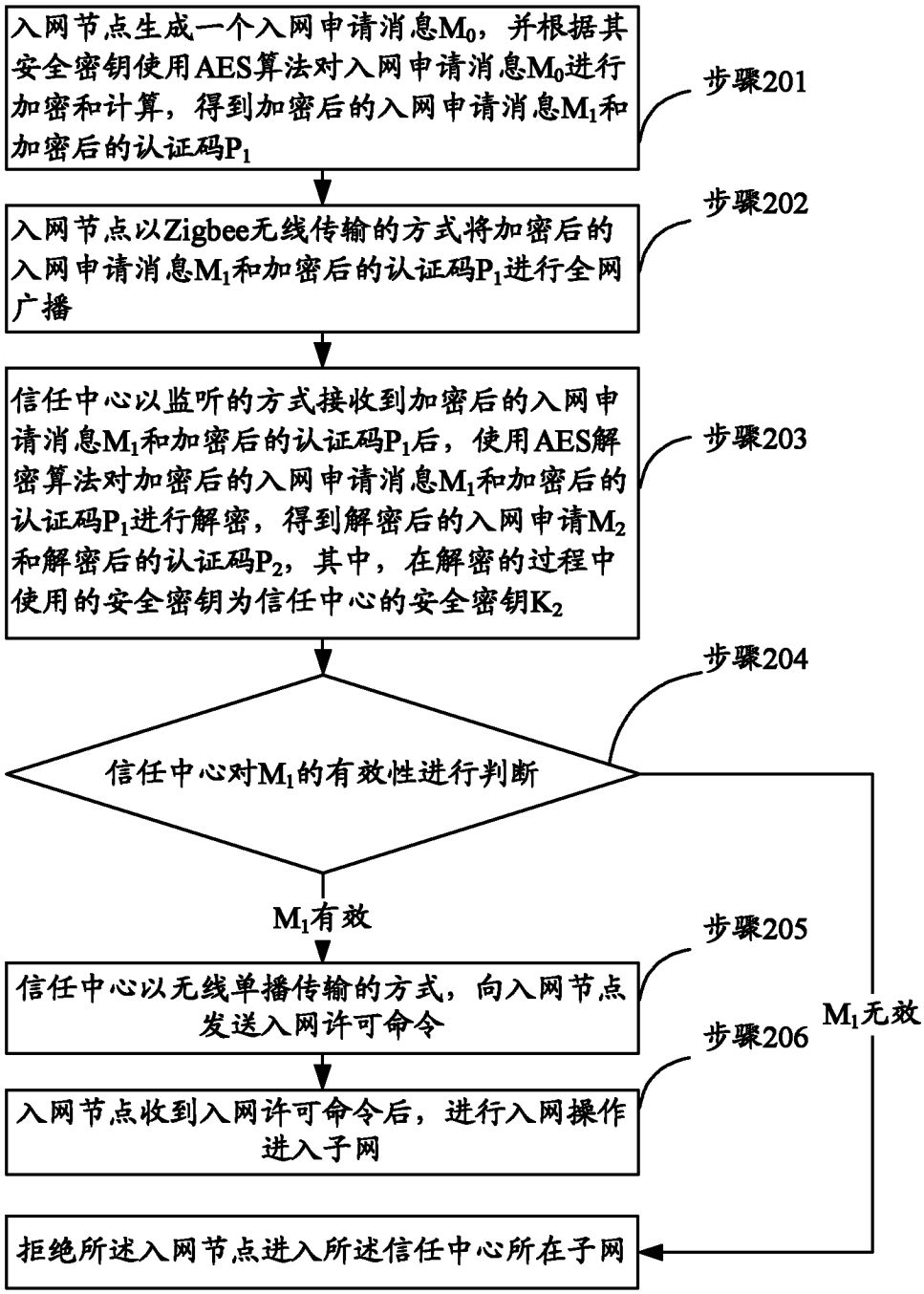

入网节点生成一个入网申请消息M_0，并根据其安全密钥使用AES算法对入网申请消息M_0进行加密和计算，得到加密后的入网申请消息M_1和加密后的认证码P_1
步骤201
入网节点以Zigbee无线传输的方式将加密后的入网申请消息M_1和加密后的认证码P_1进行全网广播
步骤202
信任中心以监听的方式接收到加密后的入网申请消息M_1和加密后的认证码P_1后，使用AES解密算法对加密后的入网申请消息M_1和加密后的认证码P_1进行解密，得到解密后的入网申请M_2和解密后的认证码P_2，其中，在解密的过程中使用的安全密钥为信任中心的安全密钥K_2
步骤203
信任中心对M_1的有效性进行判断
步骤204
M_1有效
M_1无效
信任中心以无线单播传输的方式，向入网节点发送入网许可命令
步骤205
入网节点收到入网许可命令后，进行入网操作进入子网
步骤206
拒绝所述入网节点进入所述信任中心所在子网

图 4

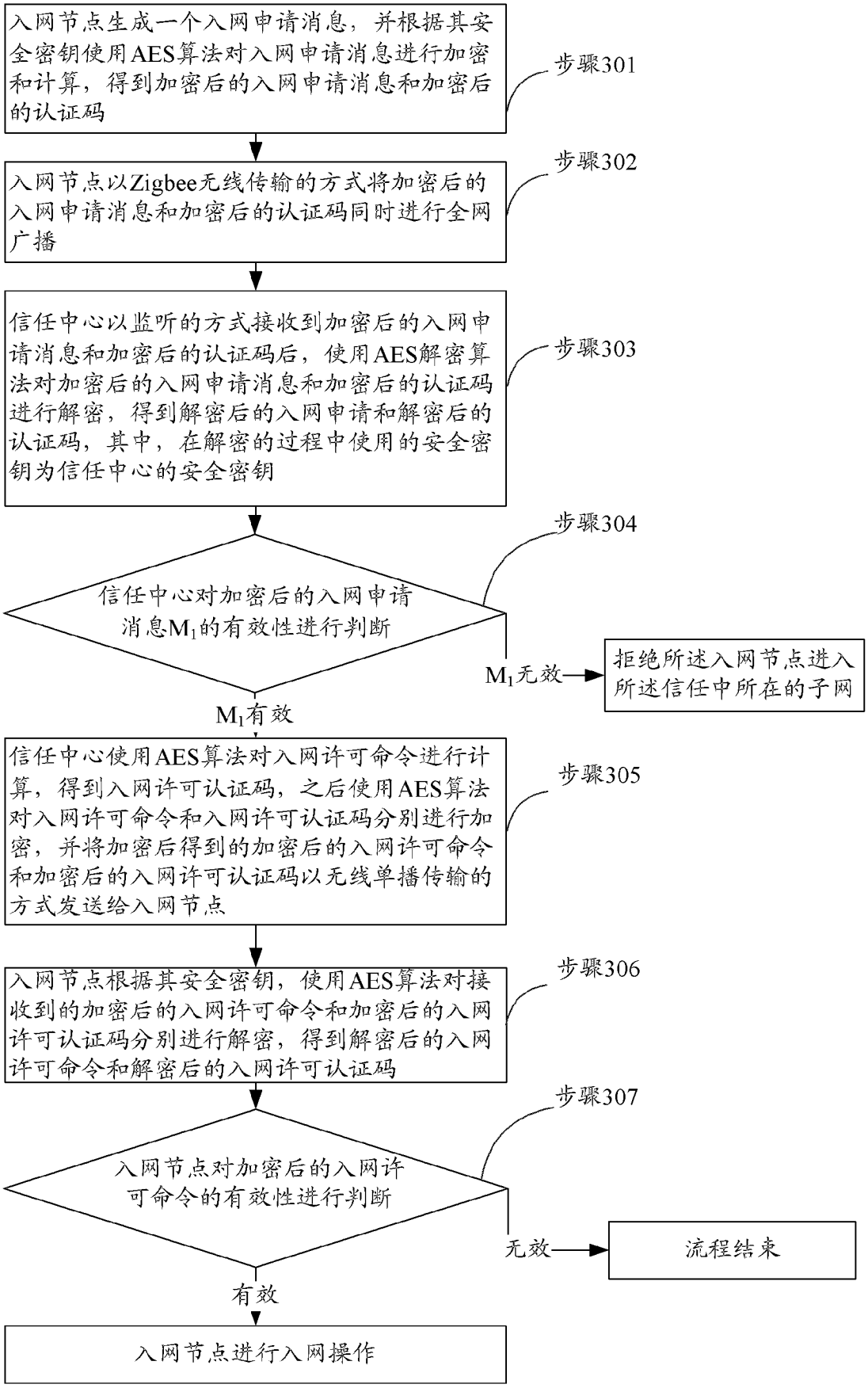

入网节点生成一个入网申请消息，并根据其安全密钥使用AES算法对入网申请消息进行加密和计算，得到加密后的入网申请消息和加密后的认证码
步骤301
入网节点以Zigbee无线传输的方式将加密后的入网申请消息和加密后的认证码同时进行全网广播
步骤302
信任中心以监听的方式接收到加密后的入网申请消息和加密后的认证码后，使用AES解密算法对加密后的入网申请消息和加密后的认证码进行解密，得到解密后的入网申请和解密后的认证码，其中，在解密的过程中使用的安全密钥为信任中心的安全密钥
步骤303
信任中心对加密后的入网申请消息M_1的有效性进行判断
步骤304
M_1无效
拒绝所述入网节点进入所述信任中所在的子网
M_1有效
信任中心使用AES算法对入网许可命令进行计算，得到入网许可认证码，之后使用AES算法对入网许可命令和入网许可认证码分别进行加密，并将加密后得到的加密后的入网许可命令和加密后的入网许可认证码以无线单播传输的方式发送给入网节点
步骤305
入网节点根据其安全密钥，使用AES算法对接收到的加密后的入网许可命令和加密后的入网许可认证码分别进行解密，得到解密后的入网许可命令和解密后的入网许可认证码
步骤306
入网节点对加密后的入网许可命令的有效性进行判断
步骤307
无效
流程结束
有效
入网节点进行入网操作

图 5

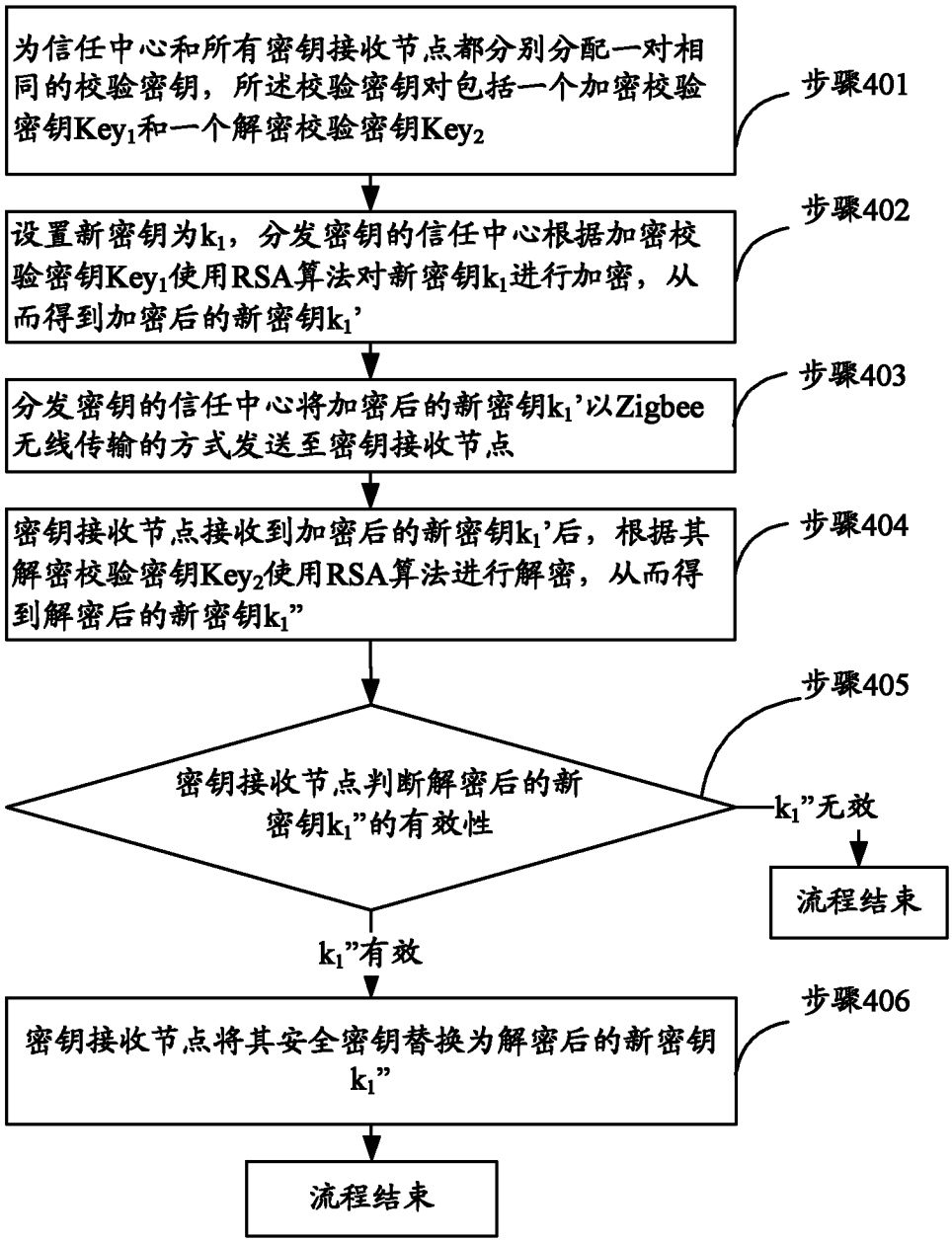

为信任中心和所有密钥接收节点都分别分配一对相同的校验密钥，所述校验密钥对包括一个加密校验密钥Key1和一个解密校验密钥Key2
步骤401
设置新密钥为k1，分发密钥的信任中心根据加密校验密钥Key1使用RSA算法对新密钥k1进行加密，从而得到加密后的新密钥k1'
步骤402
分发密钥的信任中心将加密后的新密钥k1'以Zigbee无线传输的方式发送至密钥接收节点
步骤403
密钥接收节点接收到加密后的新密钥k1'后，根据其解密校验密钥Key2使用RSA算法进行解密，从而得到解密后的新密钥k1"
步骤404
密钥接收节点判断解密后的新密钥k1"的有效性
步骤405
k1"无效
流程结束
k1"有效
密钥接收节点将其安全密钥替换为解密后的新密钥k1"
步骤406
流程结束

图 6

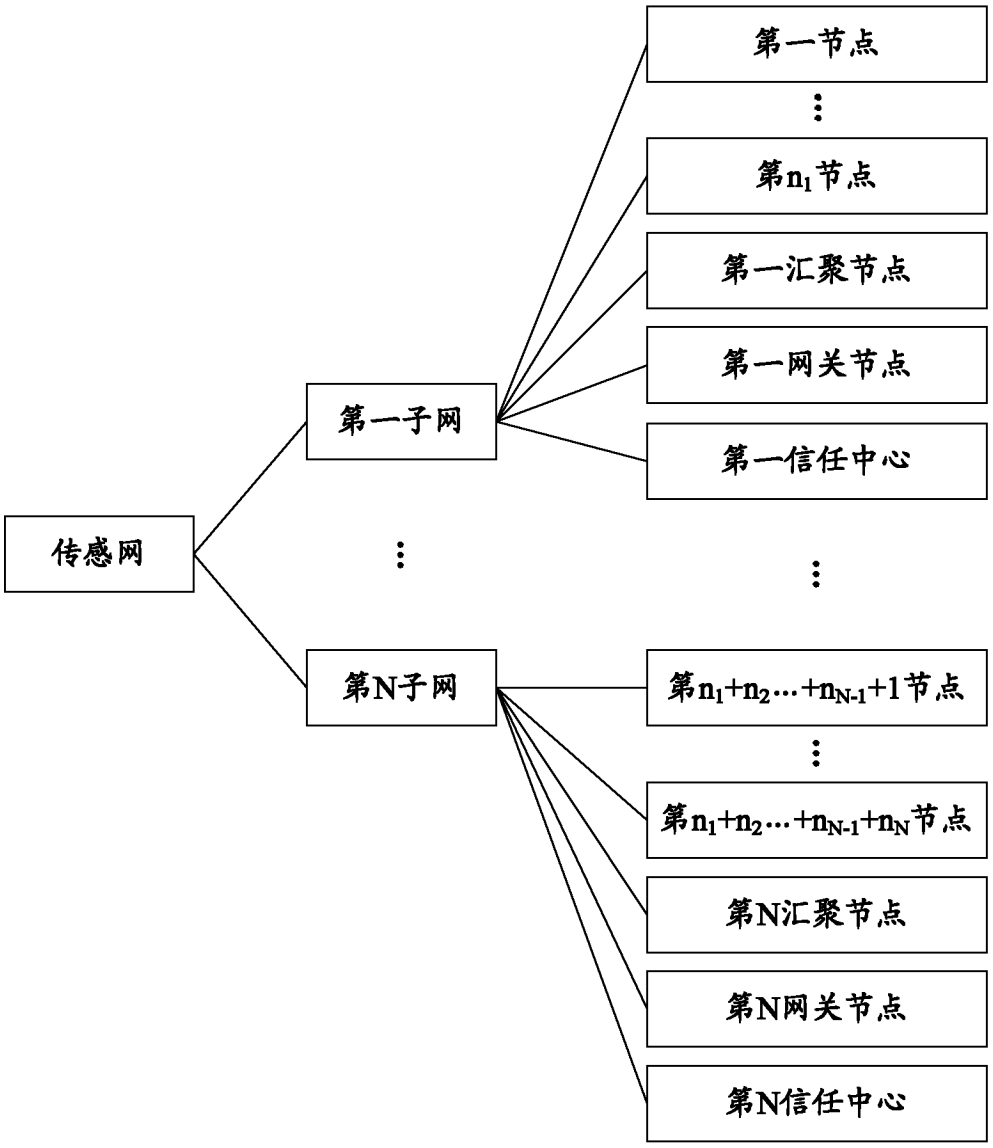

传感网
第一子网
第N子网
第一节点
第n_1节点
第一汇聚节点
第一网关节点
第一信任中心
第$n_1+n_2\cdots+n_{N-1}+1$节点
第$n_1+n_2\cdots+n_{N-1}+n_N$节点
第N汇聚节点
第N网关节点
第N信任中心

图 7

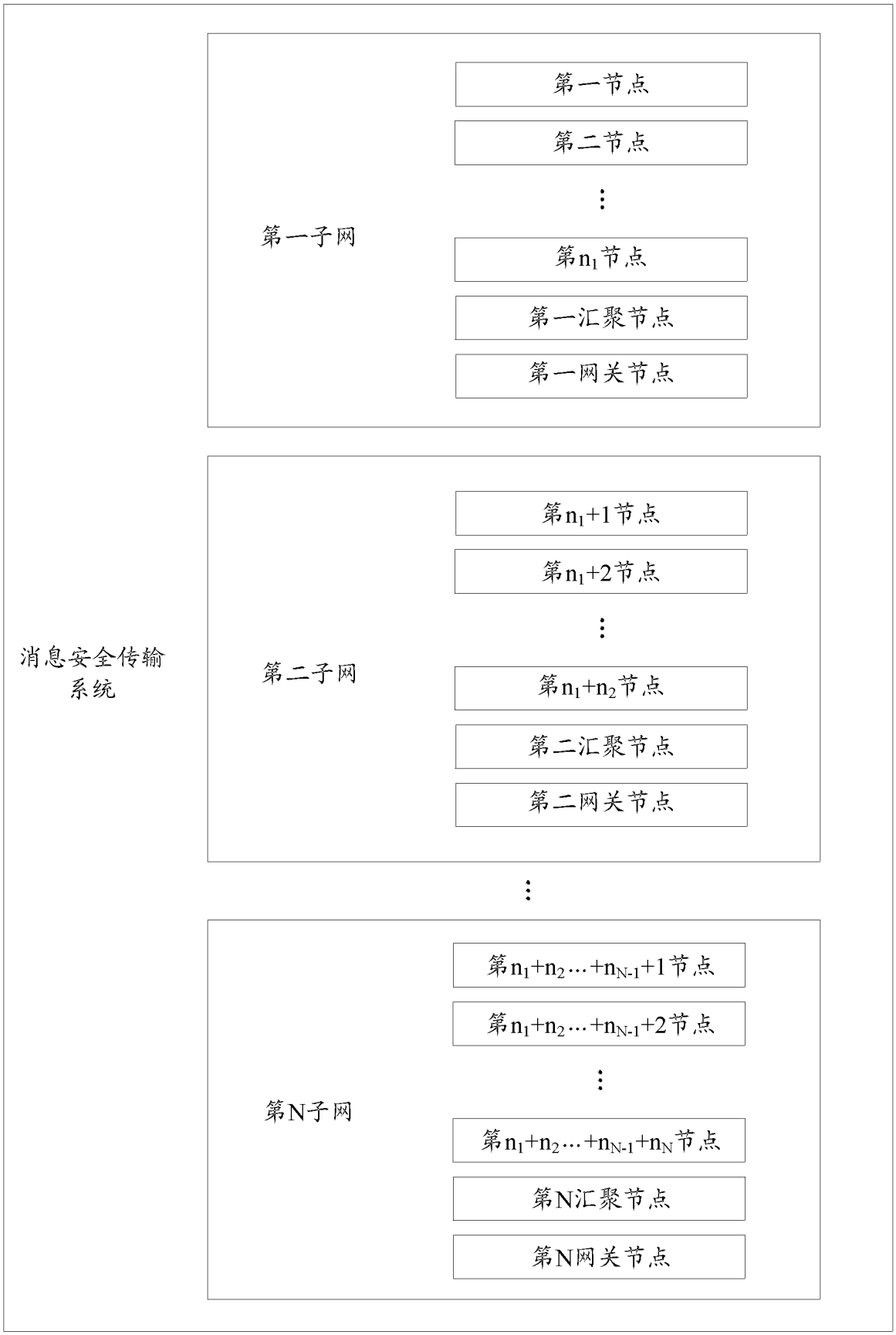

消息安全传输系统
第一子网
第一节点
第二节点
第n_1节点
第一汇聚节点
第一网关节点
第二子网
第n_1+1节点
第n_1+2节点
第n_1+n_2节点
第二汇聚节点
第二网关节点
第N子网
第n_1+n_2…+n_{N-1}+1节点
第n_1+n_2…+n_{N-1}+2节点
第n_1+n_2…+n_{N-1}+n_N节点
第N汇聚节点
第N网关节点

图 8

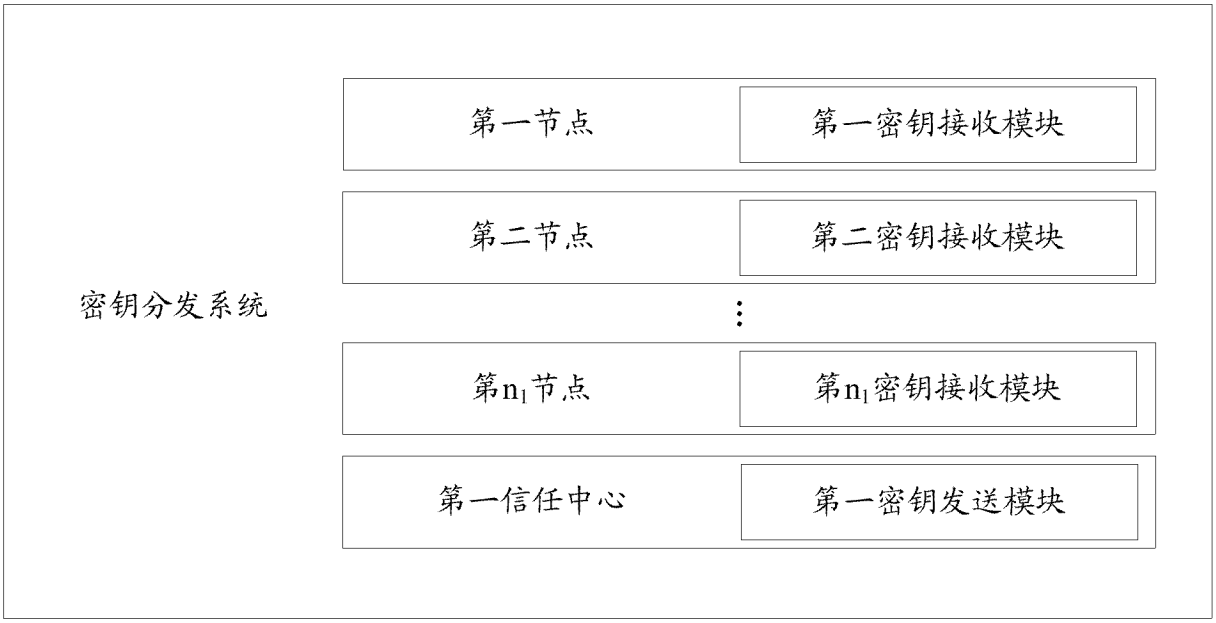

密钥分发系统
第一节点
第一密钥接收模块
第二节点
第二密钥接收模块
第n_1节点
第n_1密钥接收模块
第一信任中心
第一密钥发送模块

图 9