



(12) 发明专利

(10) 授权公告号 CN 102143491 B

(45) 授权公告日 2013. 10. 09

(21) 申请号 201010104936. 0

(22) 申请日 2010. 01. 29

(73) 专利权人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

(72) 发明人 刘晓寒 许怡娴 黄迎新 张丽佳

(74) 专利代理机构 深圳市深佳知识产权代理事
务所(普通合伙) 44285

代理人 彭愿洁 李文红

(51) Int. Cl.

H04W 12/06 (2009. 01)

H04W 88/14 (2009. 01)

H04W 88/16 (2009. 01)

(56) 对比文件

CN 101198148 A, 2008. 06. 11,

CN 101094065 A, 2007. 12. 26,

US 2008285749 A1, 2008. 11. 20,

3GPP, 3GPP TSG SA WG2 Meeting #76,

S2-097391, Proposal on MTC Architectual
Baseline for GPRS system and EPS. 《3GPP TSG
SA WG2 Meeting #76, S2-097391》. 2009,

审查员 邱德洁

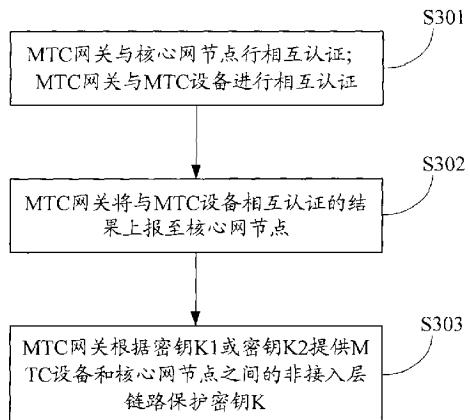
权利要求书5页 说明书13页 附图14页

(54) 发明名称

对MTC设备的认证方法、MTC网关及相关设备

(57) 摘要

本发明实施例提供一种对MTC设备的认证方法、MTC网关及相关设备，用于解决现有技术在对MTC设备认证时大量MTC设备与网络侧直接交互给网络带来沉重负荷的问题。所述方法包括：MTC网关与核心网节点进行相互认证；MTC网关与MTC设备进行相互认证；所述MTC网关将与所述MTC设备相互认证的结果上报至所述核心网节点；所述MTC网关根据密钥K1或密钥K2提供MTC设备和核心网节点之间的非接入层链路保护密钥K。本发明减轻了网络侧的链路负荷，而MTC设备与RAN节点之间的接入层功能通过MTC网关实现，MTC设备只实现与核心网节点之间的非接入层功能，这样也降低了MTC设备的成本。



1. 一种对 MTC 设备的认证方法, 其特征在于, 包括 :

MTC 网关与核心网节点进行相互认证 ;

所述 MTC 网关与 MTC 设备进行相互认证 ;

所述 MTC 网关将与所述 MTC 设备相互认证的结果上报至所述核心网节点 ;

所述 MTC 网关根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K ;

其中, 所述密钥 K1 为所述 MTC 网关与所述核心网节点进行相互认证过程中生成的密钥, 所述密钥 K2 为所述 MTC 网关根据密钥算法 A1 以及所述密钥 K1 推衍出的非接入层密钥。

2. 如权利要求 1 所述的方法, 其特征在于, 所述 MTC 网关根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 包括 :

所述 MTC 网关以所述密钥 K2 作为 MTC 设备和所述核心网节点之间的非接入层链路保护密钥 K 下发至所述 MTC 设备。

3. 如权利要求 1 所述的方法, 其特征在于, 所述 MTC 网关根据所述密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 包括 :

所述 MTC 网关根据密钥算法 A2 和所述密钥 K1, 或者根据密钥算法 A2 和所述密钥 K2 推衍非接入层密钥 K3 ;

所述 MTC 网关以所述非接入层密钥 K3 作为 MTC 设备和所述核心网节点之间的非接入层链路保护密钥 K 下发至所述 MTC 设备 ;

其中, 所述密钥算法 A2 是所述核心网节点接收所述 MTC 网关与所述 MTC 设备相互认证的认证结果后为所述 MTC 设备选择的一种密钥算法。

4. 如权利要求 1 至 3 任意一项所述的方法, 其特征在于, 所述 MTC 网关根据所述密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 之后进一步包括 :

所述 MTC 网关根据所述密钥 K1 提供 MTC 网关和无线接入网络节点之间的接入层链路保护密钥。

5. 如权利要求 4 所述的方法, 其特征在于, 所述 MTC 网关根据所述密钥 K1 提供 MTC 网关和无线接入网络节点之间的接入层链路保护密钥包括 :

所述 MTC 网关获取 MTC 设备提供的消息计数器计数值 Ncount1, 所述消息计数器计数值 Ncount1 是在所述 MTC 设备与所述核心网节点进行交互过程中对交互的消息进行计数所得的值 ;

所述 MTC 网关根据所述消息计数器计数值 Ncount1 和所述密钥 K1 推衍密钥 KeNB ;

所述 MTC 网关根据所述密钥 KeNB 推衍 MTC 网关和无线接入网络节点之间的接入层链路保护密钥。

6. 如权利要求 4 所述的方法, 其特征在于, 所述 MTC 网关根据所述密钥 K1 提供 MTC 网关和无线接入网络节点之间的接入层链路保护密钥包括 :

所述 MTC 网关获取 MTC 设备提供的消息计数器计数值 Ncount1, 所述计数值 Ncount1 是在所述 MTC 设备与所述核心网节点进行交互过程中对交互的消息进行计数所得的值 ;

所述 MTC 网关获取 MTC 设备的设备标识 ;

所述 MTC 网关根据所述消息计数器计数值 Ncount1、所述密钥 K1 和所述 MTC 设备的设备标识推衍密钥 KeNB ;

所述 MTC 网关根据所述密钥 KeNB 推衍 MTC 网关和无线接入网络节点之间的接入层链路保护密钥。

7. 如权利要求 4 所述的方法,其特征在于,所述 MTC 网关根据所述密钥 K1 提供 MTC 网关和无线接入网络节点之间的接入层链路保护密钥包括 :

所述 MTC 网关根据消息计数器计数值 Ncount2 和所述密钥 K1 推衍密钥 KeNB,所述消息计数器计数值 Ncount2 是在所述 MTC 网关与所述核心网节点进行交互过程中对交互的消息进行计数所得的值 ;

所述 MTC 网关根据所述密钥 KeNB 推衍 MTC 网关和无线接入网络节点之间的接入层链路保护密钥。

8. 一种对 MTC 设备的认证方法,其特征在于,包括 :

核心网节点与 MTC 网关进行相互认证 ;

所述核心网节点接收所述 MTC 网关发送的所述 MTC 网关与 MTC 设备相互认证的结果 ;

所述核心网节点根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K ;

其中,所述密钥 K1 是由所述核心网节点与所述 MTC 网关进行相互认证过程中生成,所述密钥 K2 为所述核心网节点根据密钥算法 A1 以及所述密钥 K1 推衍出的非接入层密钥。

9. 如权利要求 8 所述的方法,其特征在于,所述核心网节点根据所述密钥 K1 或所述密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 包括 :

所述核心网节点根据密钥算法 A2 和所述密钥 K1,或者根据密钥算法 A2 和所述密钥 K2 推衍所述 MTC 设备和所述核心网节点之间的非接入层链路保护密钥 K ;

所述核心网节点将所述密钥算法 A2 下发至所述 MTC 网关或 MTC 设备以使所述 MTC 网关或 MTC 设备根据所述密钥算法 A2 生成 MTC 设备和所述核心网节点之间的非接入层链路保护密钥 K ;

其中,所述密钥算法 A2 是所述核心网节点接收所述 MTC 网关与所述 MTC 设备相互认证的认证结果后为所述 MTC 设备选择的一种密钥算法。

10. 一种对 MTC 设备的认证方法,其特征在于,包括 :

MTC 设备与 MTC 网关进行相互认证 ;

在所述 MTC 网关与核心网节点进行相互认证并将与所述 MTC 设备进行相互认证的结果上报至所述核心网节点后,所述 MTC 设备获取所述 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 。

11. 如权利要求 10 所述的方法,其特征在于,所述 MTC 设备获取所述 MTC 设备和核心网节点之间的保护密钥 K 包括 :

所述 MTC 设备接收 MTC 网关下发的密钥 K2 ;

所述 MTC 设备以所述密钥 K2 为 MTC 设备和核心网节点之间的非接入层链路保护密钥 K ;

其中,所述密钥 K2 是所述 MTC 网关与所述核心网节点相互进行认证时根据所述密钥 K1 推衍所得的非接入层密钥,所述密钥 K1 是由所述 MTC 网关与核心网节点相互认证过程中生成。

12. 如权利要求 10 所述的方法,其特征在于,所述 MTC 设备获取所述 MTC 设备和核心网

节点之间的非接入层链路保护密钥 K 包括：

所述 MTC 设备接收所述 MTC 网关下发的密钥 K1 或所述 MTC 网关下发的密钥 K2；

所述 MTC 设备接收密钥算法 A2；

所述 MTC 设备根据所述密钥算法 A2 和所述密钥 K1，或者根据所述密钥算法 A2 和所述密钥 K2 生成 MTC 设备和核心网节点之间的非接入层链路保护密钥 K；

其中：

所述密钥算法 A2 是所述核心网节点接收所述 MTC 网关与所述 MTC 设备相互认证的认证结果后为所述 MTC 设备选择的一种密钥算法；

所述密钥 K2 是所述 MTC 网关与所述核心网节点进行相互认证时根据所述密钥 K1 推衍所得的非接入层密钥，所述密钥 K1 是由所述 MTC 网关与核心网节点相互认证过程中生成。

13. 如权利要求 10 所述的方法，其特征在于，所述 MTC 设备获取所述 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 包括：

所述 MTC 设备接收密钥算法 A2；

所述 MTC 设备将密钥算法 A2 发送至所述 MTC 网关；

所述 MTC 设备接收所述 MTC 网关下发的密钥 K3 并以所述密钥 K3 为 MTC 设备和核心网节点之间的非接入层链路保护密钥 K；

其中，所述密钥 K3 是所述 MTC 网关根据所述密钥算法 A2 和所述密钥 K1，或者根据所述密钥算法 A2 和所述密钥 K2 推衍所得，所述密钥 K2 是所述 MTC 网关与所述核心网节点相互进行认证时根据所述密钥 K1 推衍所得的非接入层密钥，所述密钥 K1 是由所述 MTC 网关与核心网节点相互认证过程中生成。

14. 如权利要求 10 所述的方法，其特征在于，所述 MTC 设备获取所述 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 包括：

所述 MTC 设备接收所述 MTC 网关下发的密钥 K3；

所述 MTC 设备以所述密钥 K3 为 MTC 设备和核心网节点之间的非接入层链路保护密钥 K；

其中，所述密钥 K3 是所述 MTC 网关根据密钥算法 A2 和密钥 K1，或者根据密钥算法 A2 和密钥 K2 推衍所得的非接入层密钥，所述密钥 K2 是所述 MTC 网关与所述核心网节点相互进行认证时根据所述密钥 K1 推衍所得，所述密钥 K1 是由所述 MTC 网关与核心网节点相互认证过程中生成。

15. 一种网关，其特征在于，包括：

认证模块，用于与核心网节点进行相互认证以及与 MTC 设备进行相互认证；

上报模块，用于将所述认证模块与所述 MTC 设备相互认证的结果上报至所述核心网节点；

密钥提供模块，用于根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K；

其中，所述密钥 K1 为所述认证模块与所述核心网节点进行相互认证过程中生成的密钥，所述密钥 K2 为所述 MTC 网关根据密钥算法 A1 和所述密钥 K1 推衍出的非接入层密钥。

16. 如权利要求 15 所述网关，其特征在于，所述密钥提供模块包括第一密钥下发单元；

所述第一密钥下发单元，用于以所述密钥 K2 作为 MTC 设备和所述核心网节点之间的非

接入层链路保护密钥 K 下发至所述 MTC 设备；

或者密钥提供模块包括密钥推衍单元和第二密钥下发单元；

所述密钥推衍单元，用于根据密钥算法 A2 和所述密钥 K1，或者根据密钥算法 A2 和所述密钥 K2 推衍非接入层密钥 K3，所述密钥算法 A2 是所述核心网节点接收所述 MTC 网关与所述 MTC 设备相互认证的认证结果后为所述 MTC 设备选择的一种密钥算法；

所述第二密钥下发单元，用于将所述密钥推衍单元推衍的非接入层密钥 K3 作为 MTC 设备和所述核心网节点之间的非接入层链路保护密钥 K 下发至所述 MTC 设备。

17. 一种核心网节点，其特征在于，包括：

认证模块，用于与 MTC 网关进行相互认证；

接收模块，用于接收所述 MTC 网关与 MTC 设备相互认证的结果；

密钥提供模块，用于根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K；

其中，所述密钥 K1 为所述 MTC 网关与所述核心网节点进行相互认证过程中生成的密钥，所述密钥 K2 为所述 MTC 网关根据密钥算法 A1 以及所述密钥 K1 推衍出的非接入层密钥。

18. 如权利要求 17 所述的核心网节点，其特征在于，所述密钥提供模块包括：

密钥推衍单元，用于根据密钥算法 A2 和所述密钥 K1，或者根据密钥算法 A2 和所述密钥 K2 推衍所述 MTC 设备和所述核心网节点之间的非接入层链路保护密钥 K；

下发单元，用于将所述密钥算法 A2 下发至所述 MTC 网关或 MTC 设备以使所述 MTC 网关或 MTC 设备根据所述密钥算法 A2 生成 MTC 设备和所述核心网节点之间的非接入层链路保护密钥 K，所述密钥算法 A2 是所述核心网节点接收所述 MTC 网关与所述 MTC 设备相互认证的认证结果后为所述 MTC 设备选择的一种密钥算法。

19. 一种 MTC 设备，其特征在于，包括：

认证模块，用于与 MTC 网关进行相互认证；

密钥获取模块，用于在所述 MTC 网关与核心网节点进行相互认证并将与所述认证模块进行相互认证的结果上报至所述核心网节点后，根据密钥 K1 或密钥 K2 获取所述 MTC 设备和核心网节点之间的非接入层链路保护密钥 K；

其中，所述密钥 K2 是所述 MTC 网关与所述核心网节点相互进行认证时根据所述密钥 K1 推衍所得的非接入层密钥，所述密钥 K1 是由所述 MTC 网关与核心网节点相互认证过程中生成。

20. 如权利要求 19 所述的 MTC 设备，其特征在于，所述密钥获取模块包括第一接收单元；

所述第一接收单元，用于接收 MTC 网关下发的密钥 K2，所述密钥 K2 是所述 MTC 网关与所述核心网节点相互进行认证时根据所述密钥 K1 推衍所得的非接入层密钥；

或者所述密钥获取模块包括第二接收单和密钥推衍单元；

所述第二接收单元，用于接收密钥算法 A2 和所述 MTC 网关下发的密钥 K1 或所述 MTC 网关下发的密钥 K2；

所述密钥推衍单元，用于根据所述第二接收单元接收的密钥算法 A2 和所述密钥 K1，或者根据所述第二接收单元接收的密钥算法 A2 和所述密钥 K2 生成 MTC 设备和核心网节点之间的非接入层链路保护密钥 K；

或者所述密钥获取模块包括第三接收单元、发送单元和第四接收单元；

所述第三接收单元，用于接收密钥算法 A2；

所述发送单元，用于将密钥算法 A2 发送至所述 MTC 网关；

所述第四接收单元，用于接收所述 MTC 网关下发的密钥 K3；

或者所述密钥获取模块包括第五接收单元；

所述第五接收单元，用于接收所述 MTC 网关下发的密钥 K3；

所述密钥算法 A2 是所述核心网节点接收所述 MTC 网关与所述 MTC 设备相互认证的认证结果后为所述 MTC 设备选择的一种密钥算法，所述密钥 K2 是所述 MTC 网关与所述核心网节点进行相互认证时根据所述密钥 K1 推衍所得的非接入层密钥，所述密钥 K1 是由所述 MTC 网关与核心网节点相互认证过程中生成，所述密钥 K3 是所述 MTC 网关根据密钥算法 A2 和密钥 K1，或者根据密钥算法 A2 和密钥 K2 推衍所得。

对 MTC 设备的认证方法、MTC 网关及相关设备

技术领域

[0001] 本发明涉及无线通信领域,具体涉及对 MTC 设备的认证方法、MTC 设备网关及相关设备。

背景技术

[0002] 机器对机器(M2M, Machine to Machine)技术是无线通信和信息技术的整合,用于双向通信,适用于安全监测、自动售货机、货物跟踪等领域。根据通信的对象可以将 M2M 分为机器对机器、机器对移动终端(如用户远程监视)和移动终端对机器(如用户远程控制)等三种通信模式。在 M2M 通信中,接入至网络的 M2M 设备也被称作机器类型通信(MTC, Machine Type Communication)设备。

[0003] 一般而言,支撑 M2M 通信的系统中,MTC 设备数量巨大。如果按照现有技术的认证方法直接对每一个 MTC 设备进行认证,那么每个 MTC 设备在与网络侧的认证过程中都会有大量的信令交互。这种大量 MTC 设备接入网络进行认证时产生的信令流量对网络侧而言是不可忽略的,并且,大量的认证过程会消耗网络侧的处理能力,这些都会给网络带来沉重的负荷。

发明内容

[0004] 本发明实施例提供一种对 MTC 设备的认证方法、MTC 网关及相关设备,用于解决现有技术在对 MTC 设备认证时大量 MTC 设备与网络侧直接交互给网络带来沉重负荷的问题。

[0005] 一种对 MTC 设备的认证方法,包括:MTC 网关与核心网节点进行相互认证;所述 MTC 网关与 MTC 设备进行相互认证;所述 MTC 网关将与所述 MTC 设备相互认证的结果上报至所述核心网节点;所述 MTC 网关根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K;其中,所述密钥 K1 为所述 MTC 网关与所述核心网节点进行相互认证过程中生成的密钥,所述密钥 K2 为所述 MTC 网关根据密钥算法 A1 以及所述密钥 K1 推衍出的非接入层密钥。

[0006] 一种对 MTC 设备的认证方法,包括:核心网节点与 MTC 网关进行相互认证;所述核心网节点接收所述 MTC 网关发送的所述 MTC 网关与 MTC 设备相互认证的结果;所述核心网节点根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K;其中,所述密钥 K1 是由所述核心网节点与所述 MTC 网关进行相互认证过程中生成,所述密钥 K2 为所述核心网节点根据密钥算法 A1 以及所述密钥 K1 推衍出的非接入层密钥。

[0007] 一种对 MTC 设备的认证方法,包括:MTC 设备与 MTC 网关进行相互认证;在所述 MTC 网关与核心网节点进行相互认证并将与所述 MTC 设备进行相互认证的结果上报至所述核心网节点后,所述 MTC 设备获取所述 MTC 设备和核心网节点之间的非接入层链路保护密钥 K。

[0008] 一种网关,包括:认证模块,用于与核心网节点进行相互认证以及与 MTC 设备进行相互认证;上报模块,用于将所述认证模块与所述 MTC 设备相互认证的结果上报至所述核

心网节点；密钥提供模块，用于根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K；其中，所述密钥 K1 为所述认证模块与所述核心网节点进行相互认证过程中生成的密钥，所述密钥 K2 为所述 MTC 网关根据密钥算法 A1 和所述密钥 K1 推衍出的非接入层密钥。

[0009] 一种核心网节点，包括：认证模块，用于与 MTC 网关进行相互认证；接收模块，用于接收所述 MTC 网关与 MTC 设备相互认证的结果；密钥提供模块，用于根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K。

[0010] 一种 MTC 设备，包括：认证模块，用于与 MTC 网关进行相互认证；密钥获取模块，用于在所述 MTC 网关与核心网节点进行相互认证并将与所述认证模块进行相互认证的结果上报至所述核心网节点后，根据密钥 K1 或密钥 K2 获取所述 MTC 设备和核心网节点之间的非接入层链路保护密钥 K；其中，所述密钥 K2 是所述 MTC 网关与所述核心网节点相互进行认证时根据所述密钥 K1 推衍所得的非接入层密钥，所述密钥 K1 是由所述 MTC 网关与核心网节点相互认证过程中生成。

[0011] 本发明实施例通过核心网节点与 MTC 网关直接相互认证，再由 MTC 网关与其连接的 MTC 设备组进行相互认证并将认证结果上报至核心网节点。由于核心网节点只与 MTC 网关直接相互认证，实际上是由 MTC 网关代理完成核心网节点与 MTC 设备的相互认证，因此，这种方式客观上减少了核心网节点与 MTC 设备直接相互认证时产生的信令流量，与现有技术相比，实际上减轻了网络侧的链路负荷，而 MTC 设备与无线接入网络（RAN, Radio Access Network）节点之间的接入层功能通过 MTC 网关实现，MTC 设备只实现与核心网节点之间的非接入层功能，这样也降低了 MTC 设备的成本。

附图说明

- [0012] 图 1 是本发明实施例提供的 MTC 设备接入核心网的示意图；
- [0013] 图 2 是本发明实施例提供的 MTC 设备与网络侧相互认证的方法基本流程示意图；
- [0014] 图 3 是本发明实施例一提供的对 MTC 设备的认证方法基本流程示意图；
- [0015] 图 4 是本发明实施例一提供的 MTC 网关、MTC 设备和核心网节点交互的流程示意图；
- [0016] 图 5 是本发明实施例二提供的 MTC 网关、MTC 设备和核心网节点交互的流程示意图；
- [0017] 图 6 是本发明实施例三提供的 MTC 网关、MTC 设备和核心网节点交互的流程示意图；
- [0018] 图 7 是本发明实施例提供的 MTC 设备、MTC 网关、RAN 节点（基站（NB）或演进基站（eNB））和核心网节点之间的交互流程示意图；
- [0019] 图 8 是本发明实施例二提供的对 MTC 设备的认证方法基本流程示意图；
- [0020] 图 9 是本发明实施例三提供的对 MTC 设备的认证方法基本流程示意图；
- [0021] 图 10 是本发明实施例四提供的 MTC 网关、MTC 设备和核心网节点交互的流程示意图；
- [0022] 图 11 是本发明实施例一提供的一种网关基本逻辑结构示意图；
- [0023] 图 12 是本发明实施例二提供的一种网关基本逻辑结构示意图；

- [0024] 图 13 是本发明实施例三提供的一种网关基本逻辑结构示意图；
- [0025] 图 14 是本发明实施例四提供的一种网关基本逻辑结构示意图；
- [0026] 图 15 是本发明实施例五提供的一种网关基本逻辑结构示意图；
- [0027] 图 16 是本发明实施例六提供的一种网关基本逻辑结构示意图；
- [0028] 图 17 是本发明实施例七提供的一种网关基本逻辑结构示意图；
- [0029] 图 18 是本发明实施例一提供的一种核心网节点基本逻辑结构示意图；
- [0030] 图 19 是本发明实施例二提供的一种核心网节点基本逻辑结构示意图；
- [0031] 图 20 是本发明实施例一提供的一种 MTC 设备基本逻辑结构示意图；
- [0032] 图 21 是本发明实施例二提供的一种 MTC 设备基本逻辑结构示意图；
- [0033] 图 22 是本发明实施例三提供的一种 MTC 设备基本逻辑结构示意图；
- [0034] 图 23 是本发明实施例四提供的一种 MTC 设备基本逻辑结构示意图；
- [0035] 图 24 是本发明实施例五提供的一种 MTC 设备基本逻辑结构示意图。

具体实施方式

[0036] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0037] 如图 1 所示，是本发明实施例一提供的 MTC 设备接入核心网的示意图。在本实施例中，MTC 设备 1 至 MTC 设备 N 构成一个 MTC 设备组 (Group)，MTC 设备组与 MTC 网关连接，MTC 网关再通过无线接入网络 (RAN, Radio Access Network) 节点接入核心网，本发明所有实施例即是基于这种组网结构对本发明技术方案进行说明。

[0038] 在实施例一中，MTC 网关与 MTC 设备组中的 MTC 设备不同，它可以是一种特殊的 MTC 设备，用于管理与其连接的 MTC 设备组中的 MTC 设备，具有与 RAN 节点之间的接入层 (AS, Access Stratum) 功能。而 MTC 设备组中的 MTC 设备只具有与核心网节点之间的非接入层 (NAS, Non Access Stratum) 功能，可以不具有与 RAN 节点之间的 AS 层功能。这种分层模式可以使得本发明与现有技术提供的认证方式不同，例如，本发明可以是分段认证、NAS 层和 AS 层的密钥分开生成以及 NAS 层和 AS 层链路保护分别实现等等，以下逐一说明。

[0039] 图 2 是本发明实施例一提供的网络侧与 MTC 设备相互认证的方法基本流程示意图，主要包括步骤：

[0040] S201，MTC 网关接受核心网节点对其进行认证并对该核心网节点进行认证。

[0041] 在本发明实施例中，核心网节点是指移动性管理实体 (MME, Mobile Management Entity) 或服务 GPRS 支持节点 (SGSN, Serving GPRS Support Node) 等，位于网络侧。MTC 网关和核心网节点之间进行相互认证，认证方式可以是认证和密钥协商 (Authentication and Key Agreement, AKA) 或证书。考虑到与现有系统的兼容性，可以优先使用 AKA 方式进行相互认证。若使用 AKA 方式认证，则认证过程中使用的标识可以是 MTC 网关管理的 MTC 设备组的组标识或者 MTC 网关的国际移动用户标识 (IMSI, International Mobile Subscriber Identity)，使用的密钥是该标识对应的基本密钥。由于核心网节点不直接与 MTC 设备相互认证，因此，若 MTC 网关与核心网节点之间的相互认证失败，则 MTC 网关需要通知与其连接

的 MTC 设备组会话密钥已经失效。至于相互认证的触发条件,在本实施例中,可以按照现有协议中的所有触发条件触发认证过程,也可以是在 MTC 设备组更新(例如,增加 MTC 设备或减少 MTC 设备等)时触发 MTC 网关与核心网节点之间的相互认证。

[0042] S202, MTC 网关对 MTC 设备进行认证并接受该 MTC 设备对其进行认证。

[0043] 本实施例的方法都是基于图 1 所示实施例的 MTC 设备组网结构,即 MTC 设备与 MTC 网关连接。MTC 网关对 MTC 设备进行互相认证,该认证方式可以使用 AKA、扩展的认证协议 AKA (EAP-AKA, Extensible Authentication Protocol-AKA) AKA 或数字证书等,本发明对此并不加限制。

[0044] S203, MTC 网关将与 MTC 设备相互认证的结果上报至核心网节点。

[0045] 由于核心网节点不是直接与 MTC 设备相互认证,因此,MTC 网关必须将其与 MTC 设备相互认证的结果上报至核心网节点。只有获知 MTC 网关与某一或某些 MTC 设备相互认证是否成功后,核心网节点才可以进行后续的流程。

[0046] 需要说明的是,在本实施例中,MTC 网关除了其自身接入核心网的认证信任状外,还具有管理 MTC 设备组中每一个 MTC 设备的认证信任状和其他安全相关信息。MTC 网关可以通过一个可信的安全环境(例如, TrE 等)保存这些认证信任状或其他安全相关信息等安全管理相关数据。一旦 MTC 设备组发生改变,MTC 网关可以通过开放移动联盟设备管理(OMA DM, Open Mobile Alliance Device Management)或与网络侧网元(例如,HSS、EIR 和 OAM 服务器等)同步等方式对安全管理相关数据更新。

[0047] 在上述本发明实施例中,虽然核心网节点(网络侧)没有与 MTC 设备直接相互认证,但 MTC 网关作为代理完成了与核心网节点的相互认证和与组内 MTC 设备的互相认证,并将认证结果上报至核心网节点,从而间接完成核心网节点与 MTC 设备组的相互认证。由于核心网节点只与 MTC 网关直接相互认证,实际上是由 MTC 网关代理完成核心网节点与 MTC 设备的相互认证,因此,这种方式客观上减少了核心网节点与 MTC 设备直接相互认证时产生的信令流量,与现有技术相比,实际上减轻了网络侧的链路负荷。

[0048] 在本发明实施例中,无论是 MTC 设备与核心网节点之间 NAS 层链路的保护还是 MTC 设备与 RAN 节点之间 AS 层链路的保护都是通过密钥进行。以下通过实施例分别以 NAS 层和 AS 层为例说明这两种协议层链路保护密钥的生成方法。

[0049] 图 3 是本发明实施例一提供的对 MTC 设备的认证方法基本流程示意图,详述如下:

[0050] S301, MTC 网关与核心网节点进行相互认证以及 MTC 网关与 MTC 设备进行相互认证;

[0051] 在本发明实施例中, MTC 网关与核心网节点进行相互认证以及 MTC 网关与 MTC 设备进行相互认证可以同时进行,也可以分时进行,在分时进行时,本发明对先后顺序并不加限制。

[0052] S302, MTC 网关将与 MTC 设备相互认证的结果上报至核心网节点;

[0053] S303, MTC 网关根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K。

[0054] 在本实施例中,密钥 K1 是 MTC 网关和核心网节点之间进行相互认证过程中生成的,可以是 Kasme 密钥,而密钥 K2 可以是 MTC 网关选择一种密钥算法 A1 例如 NAS 算法并根

据该密钥算法和密钥 K1 推衍出来的 NAS 层密钥，其包括 NAS 完整性保护密钥和加密密钥。由于密钥 K1 是 MTC 网关和核心网节点之间进行相互认证过程中生成的，因此，可以理解的是，核心网节点也可以根据密钥 K1 而推衍上述密钥 K2。

[0055] 作为本发明一个实施例，MTC 网关可以将密钥 K2 下发至与其连接的所有 MTC 设备。

[0056] 由于 MTC 设备组中的各 MTC 设备保存 MTC 网关下发的密钥 K2，而核心网节点也推衍了该密钥 K2，因此，MTC 设备或核心网节点可以使用密钥 K2 保护 MTC 设备和核心网节点之间 NAS 链路上传送的数据，即，在本实施例中，MTC 设备可以直接以密钥 K2 作为其与核心网节点之间的非接入层链路保护密钥 K。

[0057] 图 4 示出了 MTC 网关以密钥 K2 作为 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 下发至 MTC 设备时，MTC 网关、MTC 设备和核心网节点交互的流程，简述如下：

[0058] S41，MTC 网关和核心网节点进行相互认证，MTC 网关和 MTC 设备之间进行相互认证，MTC 网关和核心网节点进行相互认证过程中生成密钥 K1 和密钥 K2；

[0059] S42，MTC 网关将与 MTC 设备进行相互认证的认证结果上报至核心网节点。

[0060] S43，MTC 网关向 MTC 设备组下发在 S41 中推衍的密钥 K2。

[0061] S44，MTC 设备保存 MTC 网关下发的密钥 K2。

[0062] 作为本发明另一个实施例，MTC 网关也可以采用如下方法提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K：

[0063] MTC 网关根据密钥算法 A2 和密钥 K1，或者根据密钥算法 A2 和密钥 K2 推衍非接入层密钥 K3；

[0064] MTC 网关以非接入层密钥 K3 作为 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 下发至 MTC 设备；

[0065] 其中，密钥算法 A2 是核心网节点接收到 MTC 网关与 MTC 设备相互认证的认证结果后为 MTC 设备选择的一种密钥算法。

[0066] 为了清楚地说明 MTC 网关提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 这一实施例，图 5 示出了 MTC 网关、MTC 设备和核心网节点之间的一种交互流程，简述如下：

[0067] S51，MTC 网关和核心网节点之间进行相互认证，MTC 网关和 MTC 设备之间进行相互认证，MTC 网关根据认证过程中生成的密钥 K1 和选择的某种密钥算法 A1 推衍密钥 K2；

[0068] S52，MTC 网关将与 MTC 设备进行相互认证的认证结果上报至核心网节点；

[0069] S53，核心网节点收到 MTC 网关上报的与某个 MTC 设备进行相互认证的认证结果后，为该某个 MTC 设备选择一种密钥算法 A2，并根据 S51 中的密钥 K1 和选择的密钥算法 A2，或者根据 S51 中的密钥 K2 和选择的密钥算法 A2 推衍非接入层密钥 K3；

[0070] S54，核心网节点将选择的密钥算法 A2 下发给该某个 MTC 设备；

[0071] S55，该某个 MTC 设备将核心网节点下发的密钥算法 A2 发送给 MTC 网关；

[0072] S56，MTC 网关根据 S51 中的密钥 K1 和选择的密钥算法 A2，或者根据 S51 中的密钥 K2 和选择的密钥算法 A2 推衍非接入层密钥 K3；

[0073] 需要说明的是，对于 S54 至 S56，一种可替代的方式是：核心网节点将选择的密钥算法 A2 直接下发给 MTC 网关，而由 MTC 网关根据 S51 中的密钥 K1 和选择的密钥算法 A2，或者根据 S51 中的密钥 K2 和选择的密钥算法 A2 推衍非接入层密钥 K3。

[0074] S57, MTC 网关将推衍出的非接入层密钥 K3 发送至某个 MTC 设备。

[0075] 显然,由于在 S53 中,核心网节点也推衍出了非接入层密钥 K3,而在 S57 中,MTC 网关将推衍出的非接入层密钥 K3 也发送至某个 MTC 设备,因此,该某个 MTC 设备就可以以非接入层密钥 K3 作为 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 对链路上的数据进行保护。

[0076] 图 6 示出了 MTC 网关提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 这一实施例中,MTC 网关、MTC 设备和核心网节点之间的另一种交互流程,包括:

[0077] S61, MTC 网关和核心网节点之间进行相互认证, MTC 网关和多个 MTC 设备之间进行相互认证, MTC 网关根据认证过程中生成的密钥 K1 和选择的某种密钥算法 A1 推衍密钥 K2;

[0078] MTC 网关和多个 MTC 设备之间进行相互认证可以是同时进行,也可以是分时进行,本实施例对此并不加限定。

[0079] S62, MTC 网关将与该多个 MTC 设备进行相互认证的认证结果上报至核心网节点;

[0080] S63,核心网节点收到 MTC 网关上报的与该多个 MTC 设备进行相互认证的认证结果后,为该多个 MTC 设备选择密钥算法 A2,并根据 S61 中的密钥 K1 和选择的密钥算法 A2,或者根据 S61 中的密钥 K2 和选择的密钥算法 A2 推衍非接入层密钥 K3;

[0081] S64,核心网节点将选择的密钥算法 A2 下发给 MTC 网关;

[0082] S65,MTC 网关根据 S61 中的密钥 K1 和选择的密钥算法 A2,或者根据 S61 中的密钥 K2 和选择的密钥算法 A2 推衍非接入层密钥 K3;

[0083] 同样需要说明的是,对于 S64 至 S65,一种可替代的方式是:核心网节点将选择的密钥算法 A2 下发给该多个 MTC 设备,MTC 设备将密钥算法 A2 发送给 MTC 网关,再由 MTC 网关根据 S61 中的密钥 K1 和选择的密钥算法 A2,或者根据 S61 中的密钥 K2 和选择的密钥算法 A2 推衍非接入层密钥 K3。

[0084] 在本实施例中,核心网节点为多个 MTC 设备选择的密钥算法 A2 可以是同一种密钥算法,也可以是根据不同的 MTC 设备选择不同的密钥算法,批量下发到 MTC 设备或 MTC 网关。

[0085] S66, MTC 网关将推衍出的非接入层密钥 K3 发送至该多个 MTC 设备。

[0086] 图 5 所示实施例和图 6 所示实施例的区别之一在于:在图 5 所示实施例中,由于核心网节点是根据每一个 MTC 设备选择密钥算法 A2,因此,密钥算法是逐个下发至 MTC 网关(或 MTC 设备),再由 MTC 网关为各个 MTC 设备推衍非接入层密钥 K3,而在图 6 所示实施例中,核心网节点为多个 MTC 设备选择密钥算法 A2 时,可以将密钥算法 A2 批量下发到 MTC 设备或 MTC 网关,再由 MTC 网关为多个 MTC 设备推衍非接入层密钥 K3。

[0087] 不难理解,当有一个新的 MTC 设备连接到 MTC 网关时,即 MTC 设备组更新时,可以按照图 5 所示实施例中的流程进行非接入层密钥 K3 推衍和更新。当然,若 MTC 网关和核心网节点上配置的策略是 MTC 设备组更新时触发 MTC 网关和核心网节点之间的认证,那么 MTC 网关和核心网节点之间会进行新的认证流程来更新密钥 K1 或密钥 K2。

[0088] MTC 设备和 RAN 节点例如基站(NodeB)或演进基站(eNodeB)之间接入层链路保护密钥的保护可以分段实现:MTC 设备和 MTC 网关之间的链路保护为前段链路保护, MTC 网关和 RAN 节点之间的链路保护为后段链路保护。对于前段链路保护,由于是短距离传输链路

(例如蓝牙、Zigbee 等) 的保护,因此不在 3GPP 考虑的范围之内,后段链路的保护可以通过在 MTC 网关和 RAN 节点上生成一个密钥 KeNB,再由该密钥 KeNB 推衍 MTC 网关和 RAN 节点之间的空口保护密钥。作为本发明一个实施例,MTC 网关可以根据密钥 K1 提供 MTC 网关和 RAN 节点之间的接入层链路保护密钥,包括如下步骤:

[0089] S061, MTC 网关获取 MTC 设备提供的消息计数器计数值 Ncount1;

[0090] 消息计数器计数值 Ncount1 是在 MTC 设备与核心网节点进行交互过程中对交互的消息进行计数所得的值,是 MTC 设备主动向 MTC 网关上报或根据 MTC 网关的请求向 MTC 网关上报。

[0091] S062, MTC 网关根据该消息计数器计数值 Ncount1 和密钥 K1 推衍密钥 KeNB;

[0092] S063, MTC 网关根据密钥 KeNB 推衍 MTC 网关和 RAN 节点之间的接入层链路保护密钥。

[0093] 为了使不同时刻推衍的 KeNB 不同,即为了保持 KeNB 最新,也可以除了密钥 K1 或消息计数器计数值 Ncount1 外,再加入其它密钥推衍参数来推衍 KeNB,例如 MTC 设备标识等,因此,作为本发明另一个实施例,MTC 网关根据密钥 K1 提供 MTC 网关和 RAN 节点之间的接入层链路保护密钥,包括如下步骤:

[0094] S' 061, MTC 网关获取 MTC 设备提供的消息计数器计数值 Ncount1;

[0095] 本实施例中消息计数器计数值 Ncount1 与前述实施例中消息计数器计数值 Ncount1 的含义相同。

[0096] S' 062, MTC 网关获取 MTC 设备的设备标识;

[0097] S' 063, MTC 网关根据消息计数器计数值 Ncount1、密钥 K1 和 MTC 设备的设备标识推衍密钥 KeNB;

[0098] S' 064, MTC 网关根据密钥 KeNB 推衍 MTC 网关和 RAN 节点之间的接入层链路保护密钥。

[0099] 由于 MTC 网关自身能够提供与所述核心网节点进行交互过程中对交互的消息进行计数所得的值,因此,下述步骤是 MTC 网关根据密钥 K1 提供 MTC 网关和 RAN 节点之间的接入层链路保护密钥的又一实施例,包括:

[0100] MTC 网关根据消息计数器计数值 Ncount2 和密钥 K1 推衍密钥 KeNB;

[0101] 消息计数器计数值 Ncount2 是在 MTC 网关与核心网节点进行交互过程中对交互的消息进行计数所得的值;

[0102] MTC 网关根据密钥 KeNB 推衍 MTC 网关和 RAN 节点之间的接入层链路保护密钥。

[0103] 为了清楚地说明 MTC 网关根据密钥 K1 提供 MTC 网关和 RAN 节点之间的接入层链路保护密钥这一实施例,图 7 示出了 MTC 设备、MTC 网关、RAN 节点(基站(NB)或演进基站(eNB))和核心网节点之间的交互流程,简述如下:

[0104] S71, MTC 网关和核心网节点之间进行相互认证,生成密钥 K1, MTC 网关和 MTC 设备之间进行相互认证;

[0105] S72, 第一个接入核心网的 MTC 设备发送密钥推衍参数至 MTC 网关;

[0106] MTC 设备组中,第一个通过 MTC 网关接入到核心网的 MTC 设备会帮助 MTC 网关建立 AS 层安全。帮助 MTC 网关建立 AS 层安全的 MTC 设备有能力提供推衍根密钥 KeNB 和空口保护密钥所需的密钥推衍参数,例如,消息计数器计数值(例如,Ncount1)等。在本实施例中,

还可以由 MTC 网关向 MTC 设备发送一个请求, MTC 设备接收到该请求后, 将密钥推衍参数发送给 MTC 网关, 如附图 7 虚线框中的流程 S' 72。

[0107] S73, MTC 网关根据接收的密钥推衍参数推衍密钥 KeNB 并由密钥 KeNB 进一步推衍 MTC 网关和 RAN 节点之间的空口保护密钥;

[0108] S74, 核心网节点根据和 MTC 网关进行相互认证时生成密钥 K1 推衍密钥 KeNB;

[0109] 由于多个 MTC 设备连接到 MTC 网关时, 多个 MTC 设备共享该 MTC 网关的 AS 层, 因此, 对于在第一个通过 MTC 网关接入到核心网并帮助 MTC 网关建立 AS 层安全的 MTC 设备之后, 核心网节点和 MTC 网关不再为其他接入网络的 MTC 设备推衍 KeNB 或者将之后推衍的 KeNB 忽略。

[0110] S75, 核心网节点将密钥 KeNB 发送至 RAN 节点;

[0111] S76, RAN 节点根据密钥 KeNB 推衍 RAN 节点和 MTC 网关之间的空口保护密钥。

[0112] 从上述实施例可知, 在 MTC 设备通过 MTC 网关接入核心网时, MTC 设备可以只实现其与网络侧核心网节点之间较高的协议层, 例如 GMM/SM 层或 NAS 层, MTC 设备与网络侧 RAN 节点之间较低的协议层(例如, AS 层)在 MTC 网关上实现, 因此, 无论从软件还是硬件角度, 都降低了 MTC 设备自身的成本。

[0113] 图 8 是本发明实施例二提供的对 MTC 设备的认证方法基本流程示意图, 主要包括步骤:

[0114] S801, 核心网节点与 MTC 网关进行相互认证;

[0115] S802, 核心网节点接收 MTC 网关发送的该 MTC 网关与 MTC 设备相互认证的结果;

[0116] S803, 核心网节点根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K。

[0117] 在本实施例中, 密钥 K1 或密钥 K2 与前述实施例中的相同, 核心网节点与 MTC 网关进行相互认证、核心网节点接收 MTC 网关发送的该 MTC 网关与 MTC 设备相互认证的结果已在前述实施例中详细说明, 此处不再赘述。核心网节点根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 可以通过以下方式实现:

[0118] S081, 核心网节点根据密钥算法 A2 和密钥 K1, 或者根据密钥算法 A2 和密钥 K2 推衍 MTC 设备和核心网节点之间的非接入层链路保护密钥 K;

[0119] 需要说明的是, 在本实施例中, 核心网节点根据密钥算法 A2 和密钥 K1, 或者根据密钥算法 A2 和密钥 K2 推衍 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 时, 可以为不同的 MTC 设备选择不同的密钥算法 A2, 从而为不同的 MTC 设备推衍不同的非接入层链路保护密钥 K, 如前述图 5 示例中的流程 S53 和 S54 所述或如前述图 6 示例中的流程 S63 和 S64 所述。

[0120] S082, 核心网节点将密钥算法 A2 下发至 MTC 网关或 MTC 设备。

[0121] 之后, MTC 网关或 MTC 设备可以根据密钥算法 A2 生成 MTC 设备和核心网节点之间的非接入层链路保护密钥 K。在本实施例中, 核心网节点、MTC 网关和 MTC 设备之间的交互如图 5 或图 6 所示, 请参阅图 5 或图 6 及其文字说明, 此处不再赘述。

[0122] 图 9 是本发明实施例三提供的对 MTC 设备的认证方法基本流程示意图, 主要包括步骤:

[0123] S901, MTC 设备与 MTC 网关进行相互认证;

[0124] S902,在MTC网关与核心网节点进行相互认证并将与MTC设备进行相互认证的结果上报至核心网节点后,该MTC设备获取MTC设备和核心网节点之间的非接入层链路保护密钥K。

[0125] MTC设备与MTC网关进行相互认证、MTC网关将其与MTC设备进行相互认证的结果上报至核心网节点已在前述实施例中详细说明,此处不再赘述。

[0126] 在本实施例中,MTC设备获取MTC设备和核心网节点之间的非接入层链路保护密钥K可以是:MTC设备接收MTC网关下发的密钥K2;MTC设备直接以密钥K2为MTC设备和核心网节点之间的非接入层链路保护密钥K,例如,在图4示例流程S41至S43中,MTC网关推衍密钥K2,在S44中将推衍的密钥K2下发至MTC设备组。或者,MTC设备直接接收MTC网关下发的密钥K3;MTC设备以密钥K3为MTC设备和核心网节点之间的非接入层链路保护密钥K,例如,在图5或图6示例流程S55至S57或S65至S67的可替代方式中,核心网节点将选择的密钥算法A2直接下发给MTC网关,而由MTC网关根据S51或S61中的密钥K1和选择的密钥算法A2,或者根据S51或S61中的密钥K2和选择的密钥算法A2推衍密钥K3,然后,MTC网关将推衍出的非接入层密钥K3发送至某个MTC设备或多个设备,如此,MTC设备以密钥K3为MTC设备和核心网节点之间的非接入层链路保护密钥K。

[0127] 本实施例中,密钥K2和非接入层链路保护密钥K的含义与图4示例相同,MTC设备能够直接以密钥K2作为MTC设备和核心网节点之间的非接入层链路保护密钥K的原因也在图4示例中说明。

[0128] 以下分别给出MTC设备获取MTC设备和核心网节点之间的非接入层链路保护密钥K的另两种方式。

[0129] 方式一:

[0130] S911,MTC设备接收密钥算法A2;

[0131] S912,MTC设备将密钥算法A2发送至MTC网关;

[0132] S913,MTC设备接收MTC网关下发的密钥K3并以所述密钥K3为MTC设备和核心网节点之间的非接入层链路保护密钥K。

[0133] 对于上述S912、S913,示例可以参阅图5或图6。在图5或图6示例的流程S55或流程S64中,核心网节点下发的密钥算法A2被发送给MTC网关后,MTC网关根据图5或图6示例的流程S51或流程S61中的密钥K1和选择的密钥算法A2,或者根据流程S51或流程S61中的密钥K2和选择的密钥算法A2推衍非接入层密钥K3;MTC网关推衍出的密钥K3被某个或多个MTC设备接收后,MTC设备可以以该密钥K3为MTC设备和核心网节点之间的非接入层链路保护密钥K。

[0134] 方式二:

[0135] S921,MTC设备接收MTC网关下发的密钥K1或MTC网关下发的密钥K2;

[0136] S922,MTC设备接收密钥算法A2;

[0137] S923,MTC设备根据密钥算法A2和密钥K1,或者根据密钥算法A2和密钥K2生成MTC设备和核心网节点之间的非接入层链路保护密钥K;

[0138] 上述实施方式中,密钥算法A2、密钥K1或密钥K2均与前述实施例中的相同,不另行说明。

[0139] 为了清楚地说明上述方式二这一实施例,图10示出了MTC网关、MTC设备和核心

网节点之间的一种交互流程，简述如下：

[0140] S101, MTC 网关和核心网节点之间进行相互认证, MTC 网关和 MTC 设备之间进行相互认证, MTC 网关根据认证过程中生成的密钥 K1 和选择的某种密钥算法 A1 推衍密钥 K2；

[0141] S102, MTC 网关将与某个 MTC 设备进行相互认证的认证结果上报至核心网节点；

[0142] S103, MTC 网关将其与核心网节点之间进行相互认证过程中生成的密钥 K1 或根据密钥 K1 和选择的某种密钥算法 A1 推衍出的密钥 K2 下发至 MTC 设备；

[0143] S104, 核心网节点为某个 MTC 设备选择一种密钥算法 A2, 并根据 S101 中的密钥 K1 和选择的密钥算法 A2 或者根据 S101 中的密钥 K2 和选择的密钥算法 A2 推衍非接入层密钥 K3；

[0144] S105, 核心网节点将选择的密钥算法 A2 下发给该某个 MTC 设备；

[0145] S106, 该某个 MTC 设备根据密钥 K1 和密钥算法 A2, 或者根据密钥 K2 和密钥算法 A2 推衍非接入层密钥 K3。

[0146] K3 即是 MTC 设备和核心网节点之间的非接入层链路保护密钥 K。

[0147] 在本发明实施例中, 由于密钥 K1 是在 MTC 网关和核心网节点之间进行相互认证时推衍出, 这里有必要对 MTC 网关和核心网节点之间进行相互认证的触发条件加以说明。在本发明实施例中, MTC 网关和核心网节点之间进行相互认证的触发条件可以是: MTC 设备组发生更新时、在某个定时器到期时或 MTC 设备组中某个 MTC 设备的 NAS 消息计数器达到计数最大值时 MTC 网关和核心网节点就进行相互认证。

[0148] 为了避免频繁触发 MTC 网关和核心网节点之间的认证从而频繁更新 MTC 设备和核心网节点之间的密钥 K1, 也可以设置密钥 K1 的生存期(Lifetime), 在生存期完结时 MTC 网关和核心网节点就进行相互认证, 开始生成密钥 K1。

[0149] 需要说明的是, 为了减少认证时产生的信令流量, 应该保证核心网节点只对 MTC 网关触发认证而禁止对与 MTC 网关直接相连的 MTC 设备触发认证。在本发明实施例中, 可以采用下述方式达到上述目的。

[0150] 方式一: 核心网节点通过识别设备标识或设备标志位来区分 MTC 网关和 MTC 设备, 从而保证只对 MTC 网关触发认证而不对与 MTC 网关直接相连的 MTC 设备触发认证。例如, 可以在核心网节点的用户设备上下文(Context) 字段中增加设备标志位, 使用不同的设备标志位(例如, 比特“0”或比特“1”)来区分 MTC 网关和 MTC 设备, 或者, 将 MTC 网关和 MTC 设备采用不同的 IMSI 范围作为设备标识进行区分。

[0151] 方式二: 禁止 MTC 设备在发起初始层三消息是触发认证, 即消息中增加一个 IE, 核心网节点根据此 IE 判断禁止对与 MTC 网关直接相连的 MTC 设备触发认证；

[0152] 方式三: MTC 网关将自身的密钥标识符(Key Set Identifier, KSI)发送至与其连接的每个 MTC 设备, MTC 设备在发起初始层三消息时携带该 KSI, 核心网节点根据此 KSI 区分 MTC 网关和 MTC 设备。

[0153] 从上述本发明实施例可知, 在 MTC 设备通过 MTC 网关接入核心网时, MTC 设备可以只实现其与网络侧核心网节点之间的较高的协议层, 例如 GMM/SM 层或 NAS 层, 而不需要实现与网络侧 RAN 节点之间的较低的协议层, 例如, AS 层, 因此, 无论从软件还是硬件角度, 降低了 MTC 设备自身的成本。

[0154] 图 11 是本发明实施例一提供的一种网关基本逻辑结构示意图。为了便于说明, 仅

仅示出了与本发明实施例相关的部分，其中的功能模块 / 单元可以是硬件模块 / 单元、软件模块 / 单元或软硬件相结合的模块 / 单元。该网关包括认证模块 111、上报模块 112 和密钥提供模块 113。

[0155] 认证模块 111，用于与核心网节点进行相互认证以及与 MTC 设备进行相互认证；
[0156] 上报模块 112，用于将认证模块 111 与 MTC 设备相互认证的结果上报至核心网节点；

[0157] 密钥提供模块 113，用于根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K，其中，密钥 K1 为认证模块 111 与核心网节点进行相互认证过程中生成的密钥，密钥 K2 为 MTC 网关根据密钥算法 A1 和密钥 K1 推衍出的非接入层密钥。

[0158] 密钥提供模块 113 可以包括第一密钥下发单元 121，如图 12 所示，用于以密钥 K2 作为 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 下发至 MTC 设备。

[0159] 密钥提供模块 113 还可以包括密钥推衍单元 131 和第二密钥下发单元 132，如图 13 所示，其中：

[0160] 密钥推衍单元 131，用于根据密钥算法 A2 和认证模块 111 与核心网节点进行相互认证过程中生成的密钥 K1，或者根据密钥算法 A2 和密钥 K2 推衍非接入层密钥 K3；

[0161] 第二密钥下发单元 132，用于将密钥推衍单元 131 推衍的非接入层密钥 K3 作为 MTC 设备和核心网节点之间的非接入层链路保护密钥 K 下发至 MTC 设备。

[0162] 图 11 至图 13 所示实施例的网关还可以进一步包括接入层链路保护密钥提供模块 141，如图 14 所示。接入层链路保护密钥提供模块 141 用于根据认证模块 111 与核心网节点进行相互认证过程中生成的密钥 K1，提供 MTC 网关和无线接入网络节点之间的接入层链路保护密钥。

[0163] 图 14 所示接入层链路保护密钥提供模块 141 可以包括计数值获取单元 151、密钥 KeNB 第一推衍单元 152 和接入层链路保护密钥推衍单元 153，如图 15 所示，其中：

[0164] 计数值获取单元 151，用于获取 MTC 设备提供的消息计数器计数值 Ncount1，该消息计数器计数值 Ncount1 是在 MTC 设备与核心网节点进行交互过程中对交互的消息进行计数所得的值；

[0165] 密钥 KeNB 第一推衍单元 152，用于根据密钥 K1 和计数值获取单元 151 获取的消息计数器计数值 Ncount1 推衍密钥 KeNB；

[0166] 接入层链路保护密钥第推衍单元 153，用于根据密钥 KeNB 第一推衍单元 152 推衍的密钥 KeNB 推衍 MTC 网关和无线接入网络节点之间的接入层链路保护密钥。

[0167] 图 14 所示接入层链路保护密钥提供模块 141 可以包括计数值获取单元 151、设备标识获取单元 161、密钥 KeNB 第二推衍单元 162 和接入层链路保护密钥推衍单元 153，如图 16 所示，其中：

[0168] 计数值获取单元 151，用于获取 MTC 设备提供的消息计数器计数值 Ncount1，该消息计数器计数值 Ncount1 是在 MTC 设备与核心网节点进行交互过程中对交互的消息进行计数所得的值

[0169] 设备标识获取单元 161，用于获取 MTC 设备的设备标识；

[0170] 密钥 KeNB 第二推衍单元 162，用于根据消息计数器计数值 Ncount1、密钥 K1 和设备标识推衍密钥 KeNB；

[0171] 接入层链路保护密钥第推衍单元 153,用于根据密钥 KeNB 第二推衍单元 162 推衍的密钥 KeNB 推衍 MTC 网关和无线接入网络节点之间的接入层链路保护密钥。

[0172] 图 14 所示接入层链路保护密钥提供模块 141 可以包括密钥 KeNB 第三推衍单元 171 和接入层链路保护密钥推衍单元 153,如图 17 所示,其中,密钥 KeNB 第三推衍单元 171 用于根据消息计数器计数值 Ncount2 和密钥 K1 推衍密钥 KeNB,消息计数器计数值 Ncount2 是在 MTC 网关与核心网节点进行交互过程中对交互的消息进行计数所得的值。

[0173] 图 18 是本发明实施例一提供的一种核心网节点基本逻辑结构示意图。为了便于说明,仅仅示出了与本发明实施例相关的部分,其中的功能模块 / 单元可以是硬件模块 / 单元、软件模块 / 单元或软硬件相结合的模块 / 单元。该核心网节点包括认证模块 181、接收模块 182 和密钥提供模块 183,其中 :

[0174] 认证模块 181,用于与 MTC 网关进行相互认证;

[0175] 接收模块 182,用于接收 MTC 网关与 MTC 设备相互认证的结果;

[0176] 密钥提供模块 183,用于根据密钥 K1 或密钥 K2 提供 MTC 设备和核心网节点之间的非接入层链路保护密钥 K。

[0177] 密钥提供模块 183 可以进一步包括密钥推衍单元 1931 和下发单元 1932,如图 19 所示,其中 :

[0178] 密钥推衍单元 1931,用于根据密钥算法 A2 和密钥 K1,或者根据密钥算法 A2 和密钥 K2 推衍 MTC 设备和核心网节点之间的非接入层链路保护密钥 K;

[0179] 下发单元 1932,用于将密钥算法 A2 下发至 MTC 网关或 MTC 设备以使 MTC 网关或 MTC 设备根据密钥算法 A2 生成 MTC 设备和核心网节点之间的非接入层链路保护密钥 K。

[0180] 在图 18 和图 19 所示实施例中,密钥算法 A2 是核心网节点接收 MTC 网关与 MTC 设备相互认证的认证结果后为 MTC 设备选择的一种密钥算法。

[0181] 图 20 是本发明实施例一提供的一种 MTC 设备基本逻辑结构示意图。为了便于说明,仅仅示出了与本发明实施例相关的部分,其中的功能模块 / 单元可以是硬件模块 / 单元、软件模块 / 单元或软硬件相结合的模块 / 单元。该 MTC 设备包括认证模块 201 和密钥获取模块 202,其中 :

[0182] 认证模块 201,用于与 MTC 网关进行相互认证;

[0183] 密钥获取模块 202,用于在 MTC 网关与核心网节点进行相互认证并将与认证模块 201 进行相互认证的结果上报至核心网节点后,根据密钥 K1 或密钥 K2 获取 MTC 设备和核心网节点之间的非接入层链路保护密钥 K。

[0184] 图 20 所示实施例中密钥获取模块 202 可以包括第一接收单元 211,如图 21 所示,用于接收 MTC 网关下发的密钥 K2。

[0185] 图 20 所示实施例中密钥获取模块 202 可以包括第二接收单元 221 和密钥推衍单元 222,如图 22 所示,其中 :

[0186] 第二接收单元 221,用于接收密钥算法 A2 和 MTC 网关下发的密钥 K1 或 MTC 网关下发的密钥 K2;

[0187] 密钥推衍单元 222,用于根据第二接收单元 221 接收的密钥算法 A2 和密钥 K1,或者根据第二接收单元 221 接收的密钥算法 A2 和密钥 K2 生成 MTC 设备和核心网节点之间的非接入层链路保护密钥 K。

[0188] 图 20 所示实施例中密钥获取模块 202 可以包括第三接收单元 231、发送单元 232 和第四接收单元 233，如图 23 所示，其中：

[0189] 第三接收单元 231，用于接收密钥算法 A2；

[0190] 发送单元 232，用于将第三接收单元 231 接收的密钥算法 A2 发送至 MTC 网关；

[0191] 第四接收单元 233，用于接收 MTC 网关下发的密钥 K3。

[0192] 图 20 所示实施例中密钥获取模块 202 可以包括第五接收单元 241，如图 24 所示，用于接收 MTC 网关下发的密钥 K3。

[0193] 在图 20 至图 24 所示实施例中，密钥算法 A2 是核心网节点接收 MTC 网关与 MTC 设备相互认证的认证结果后为 MTC 设备选择的密钥算法，密钥 K2 是 MTC 网关与核心网节点进行相互认证时根据密钥 K1 推衍所得的非接入层密钥，密钥 K1 是由 MTC 网关与核心网节点相互认证过程中生成，密钥 K3 是 MTC 网关根据密钥算法 A2 和密钥 K1，或者根据密钥算法 A2 和密钥 K2 推衍所得。

[0194] 需要说明的是，上述设备各模块 / 单元之间的信息交互、执行过程以及技术效果等内容，由于与本发明方法实施例基于同一构思，具体内容可参见本发明方法实施例中的说明，此处不再赘述。

[0195] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：只读存储器(ROM, Read Only Memory)、随机存取存储器(RAM, Random Access Memory)、磁盘或光盘等。

[0196] 以上对本发明实施例所提供的对 MTC 设备的认证方法、MTC 网关及相关设备进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

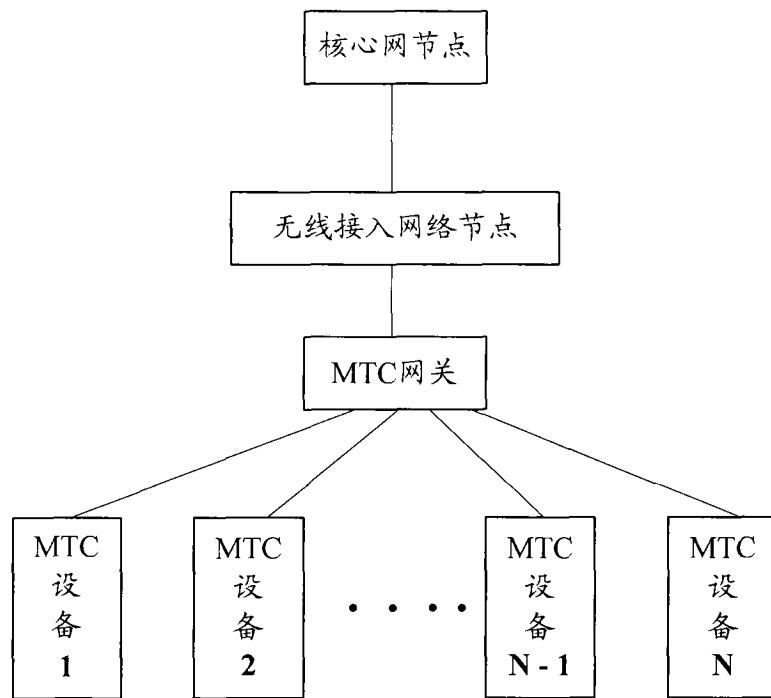


图 1

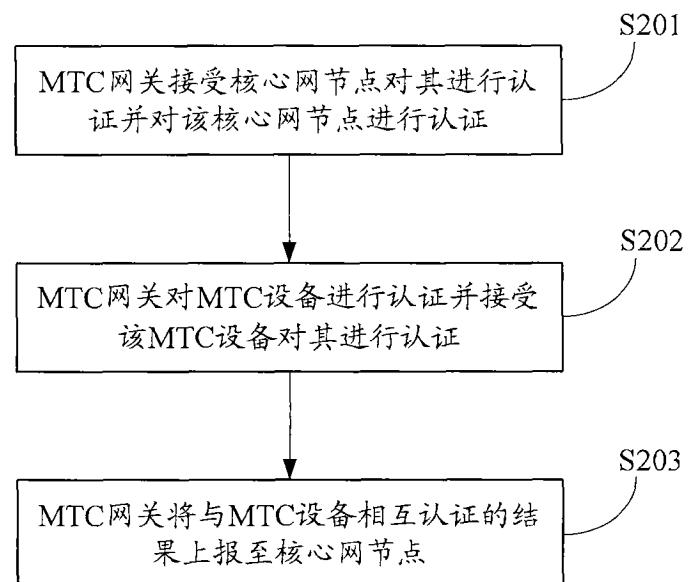


图 2

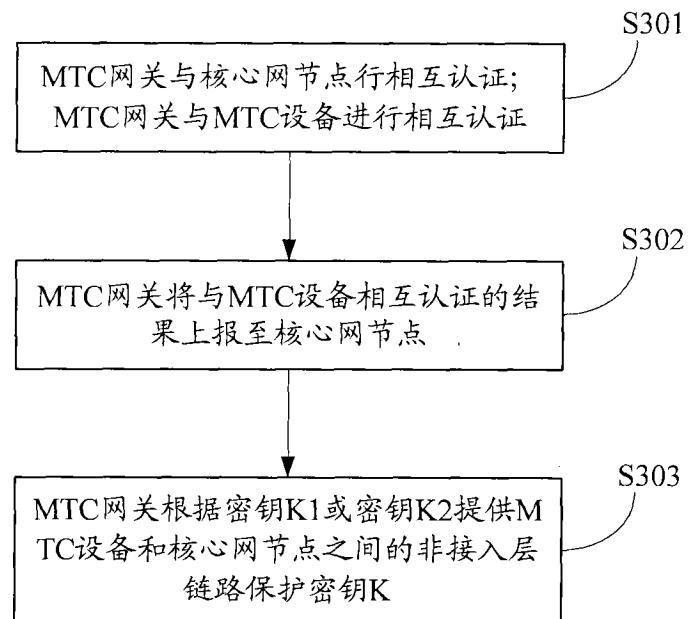


图 3

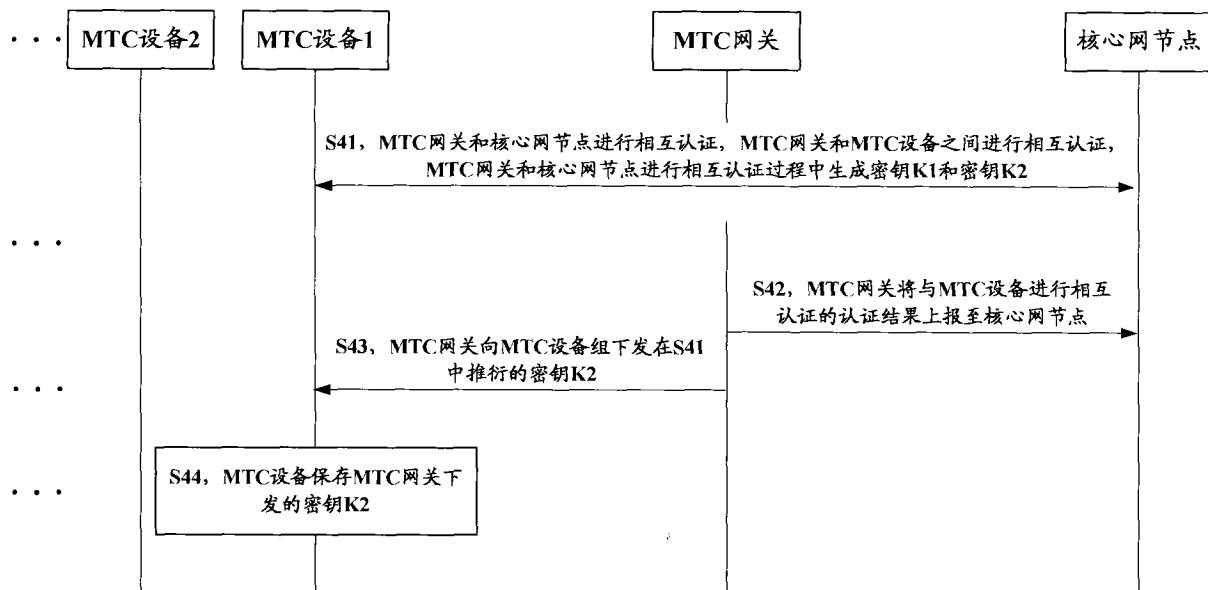


图 4

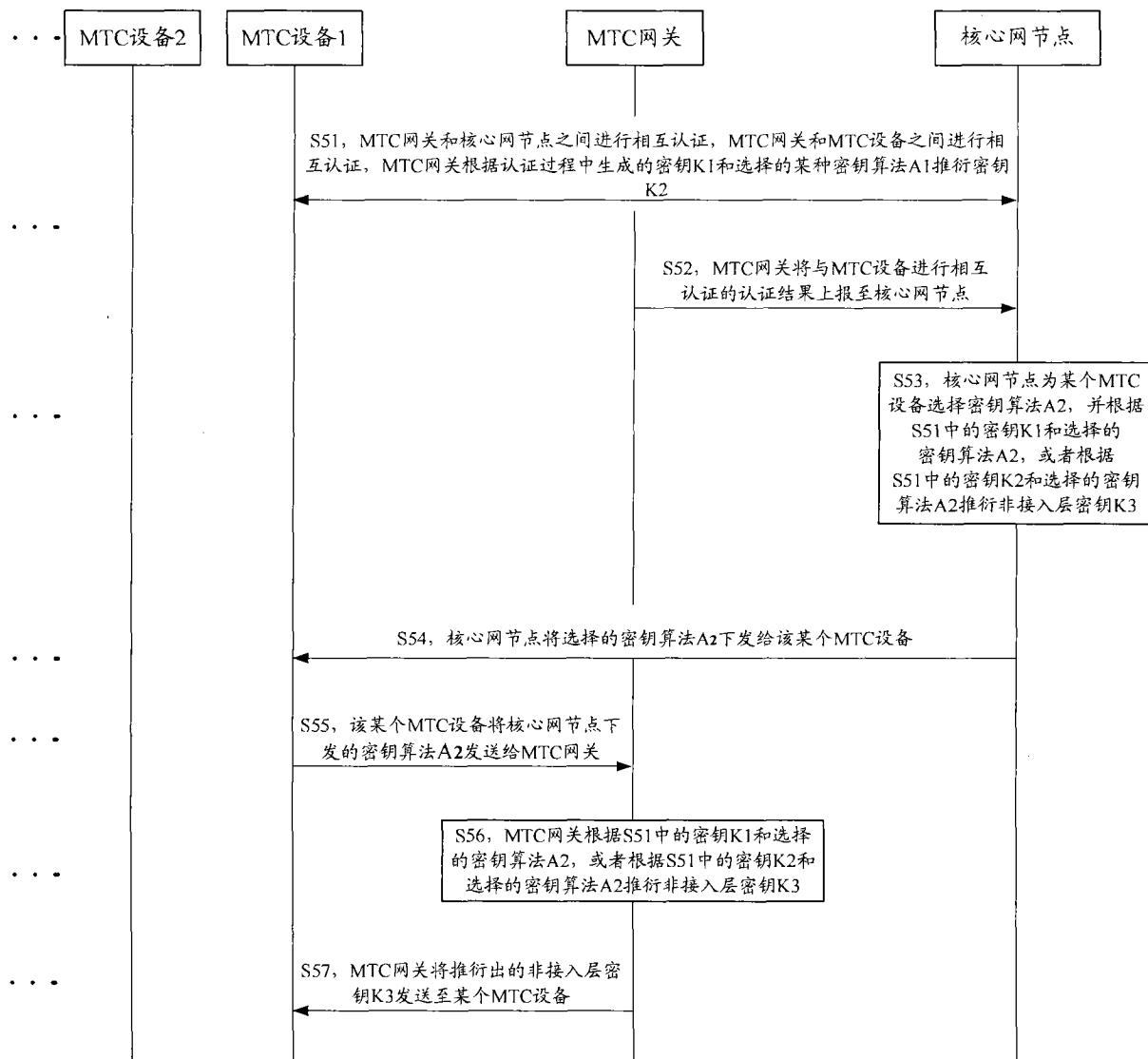


图 5

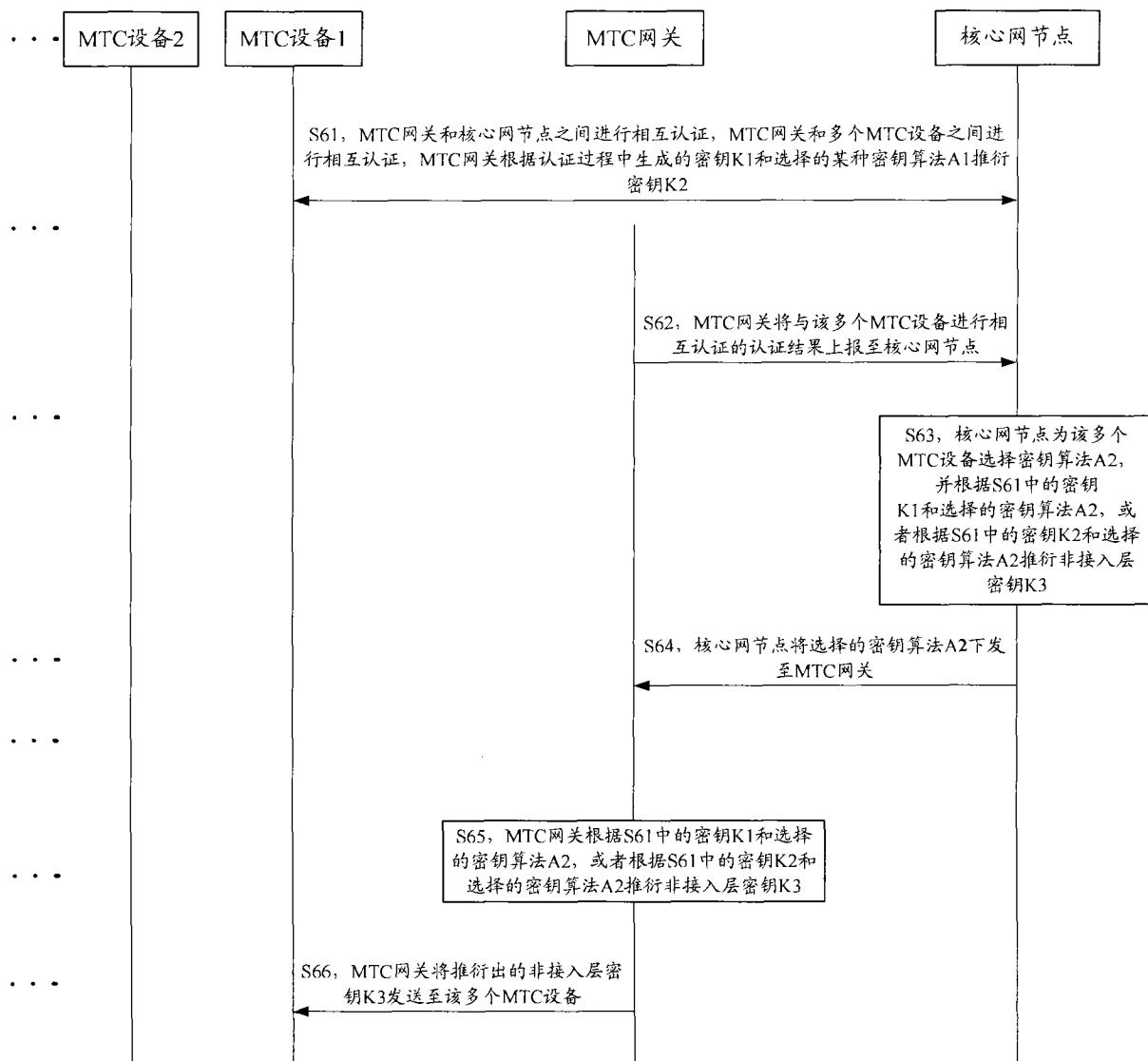


图 6

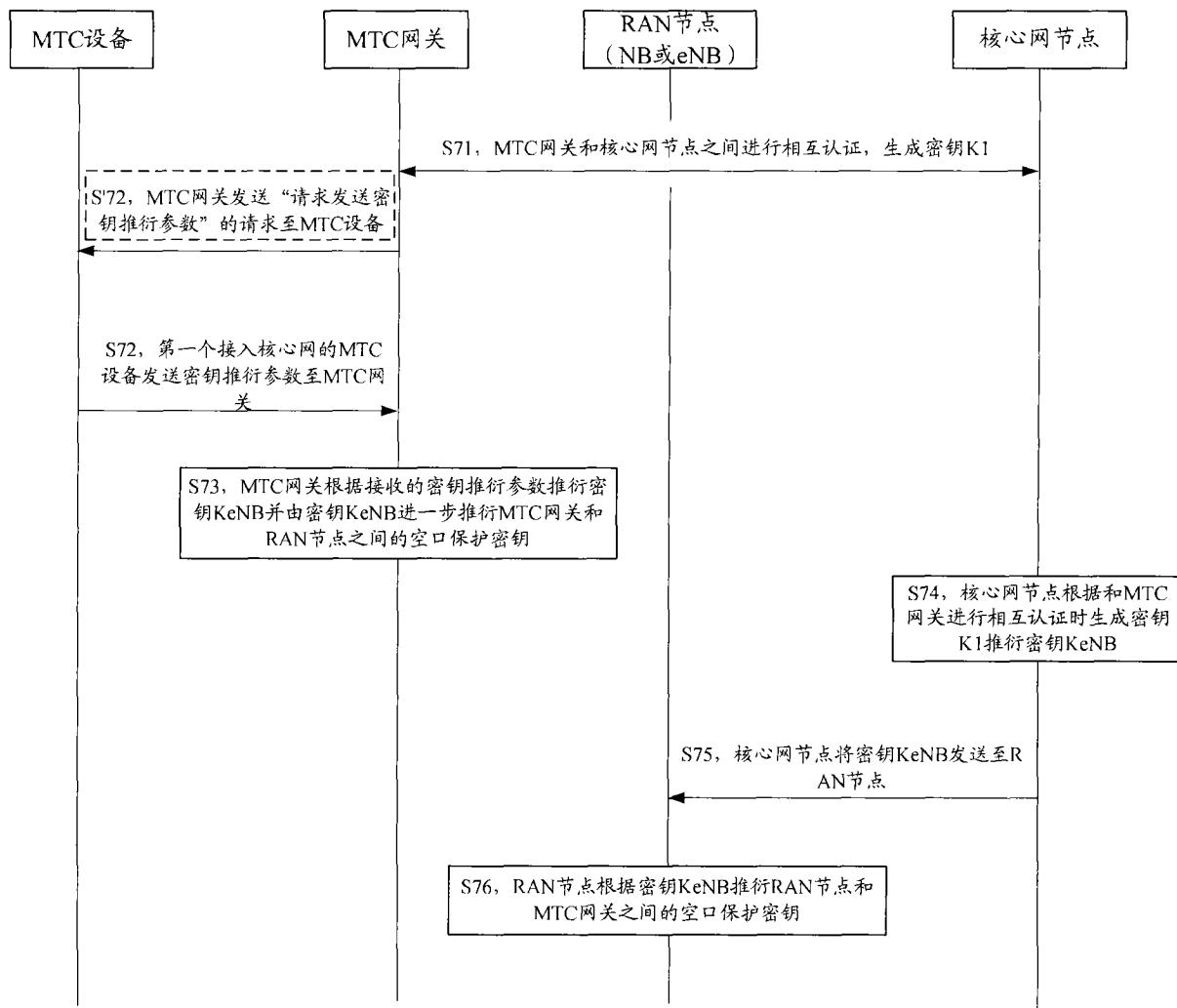


图 7

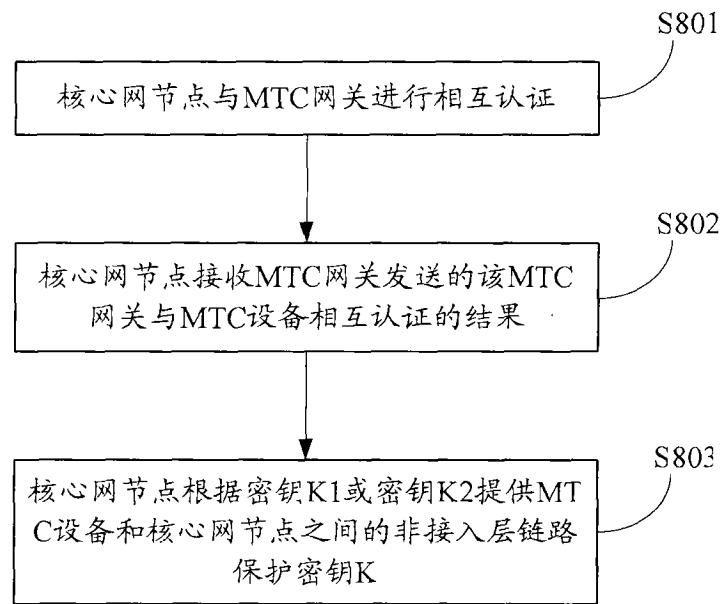


图 8

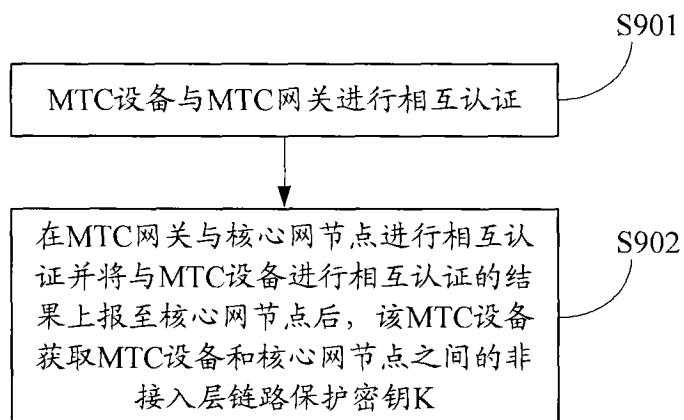


图 9

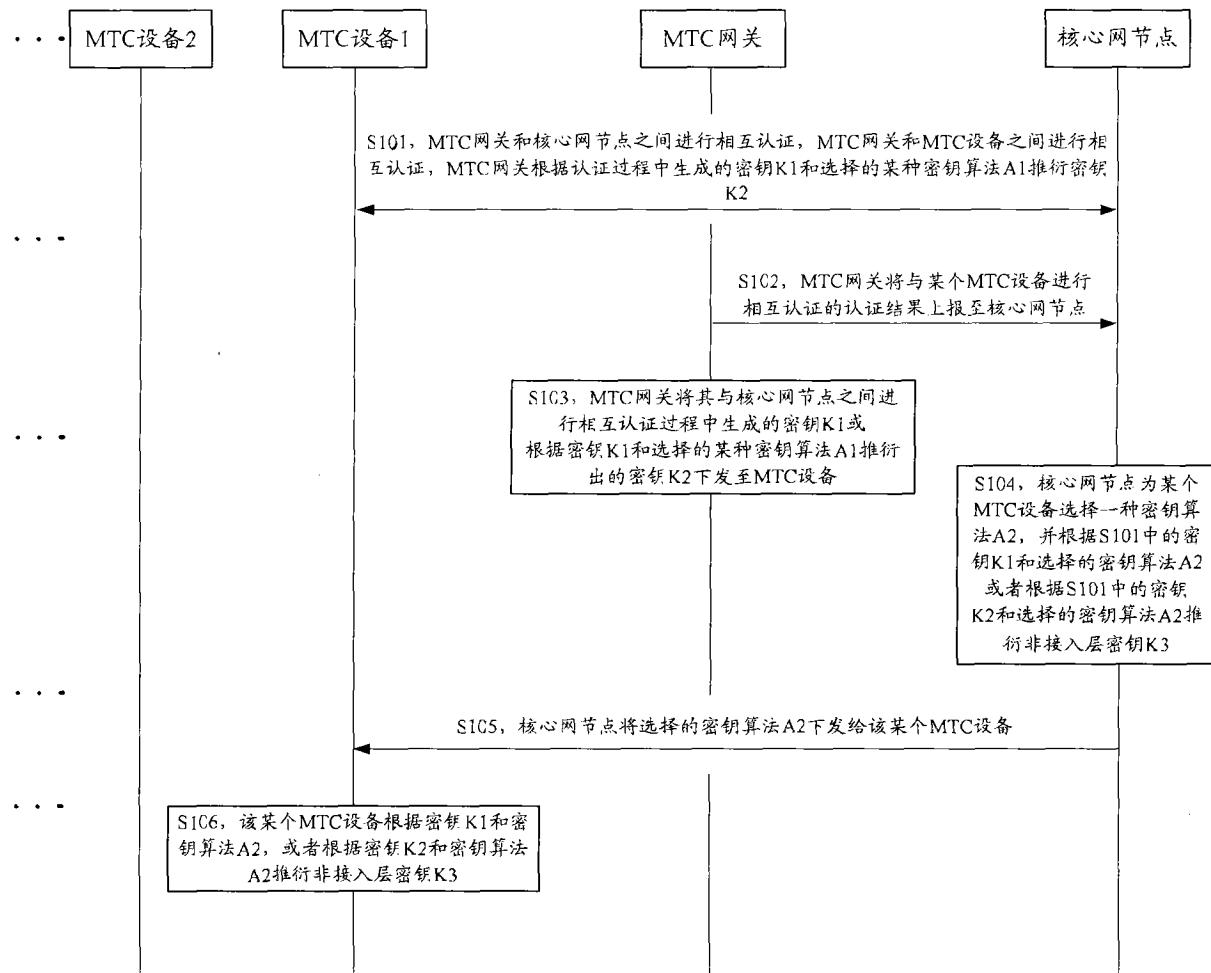


图 10

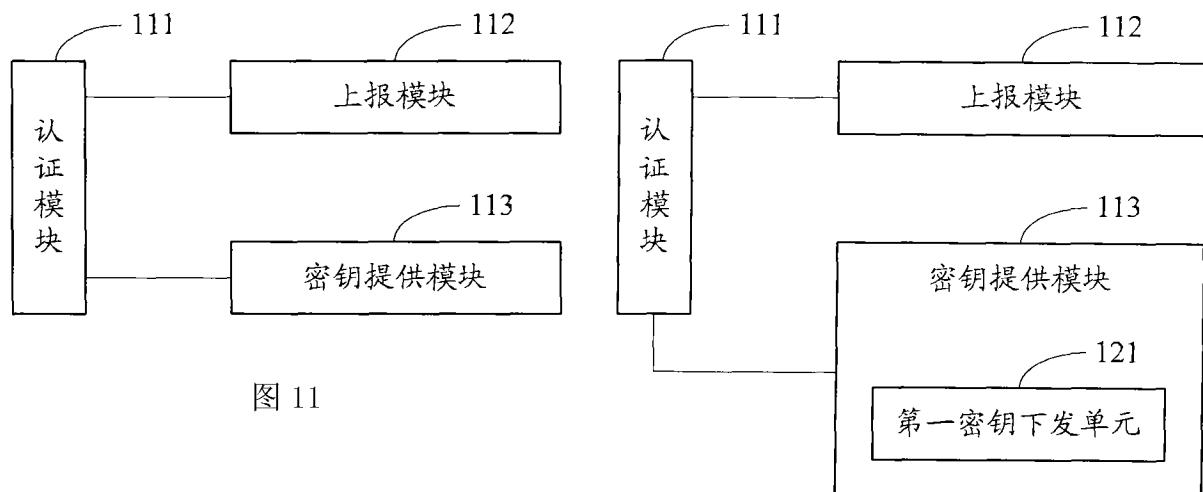


图 11

图 12

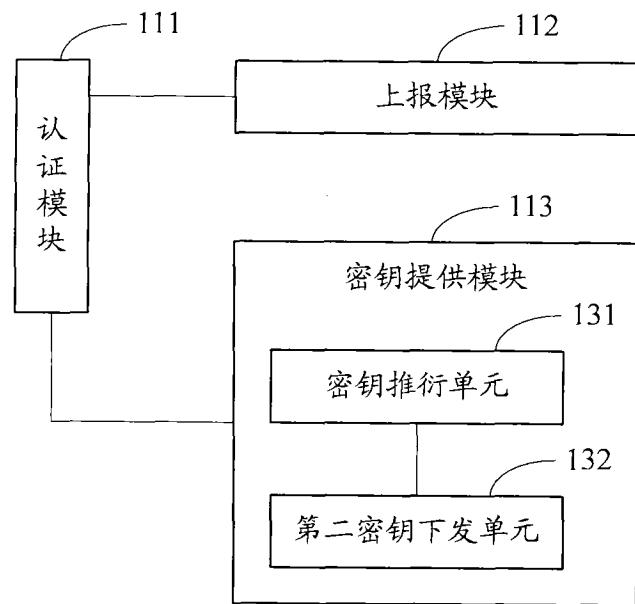


图 13

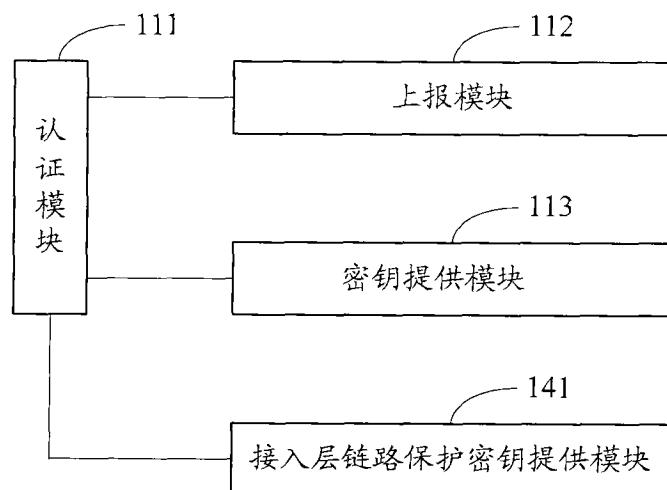


图 14

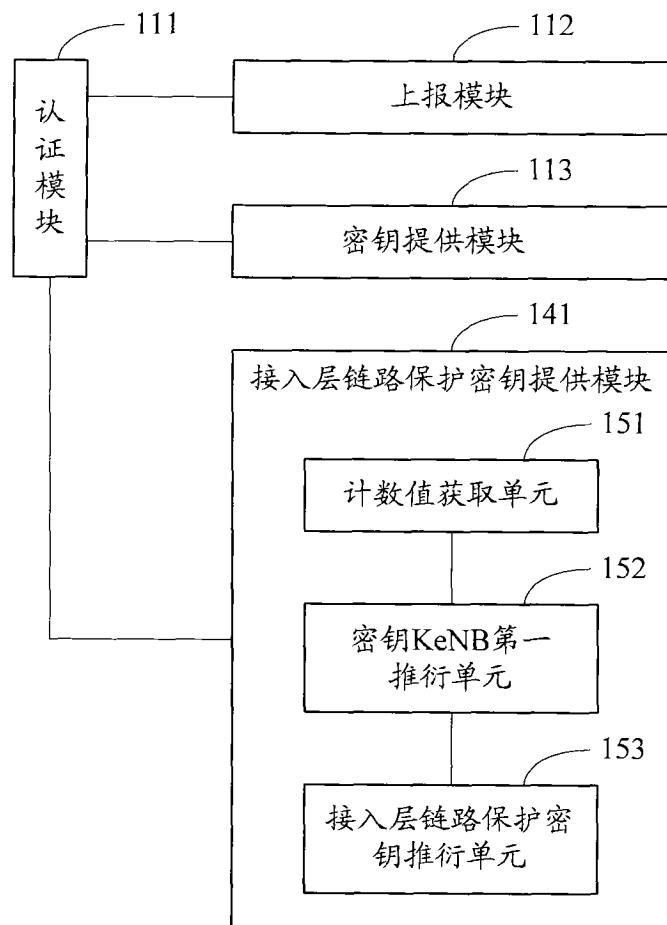


图 15

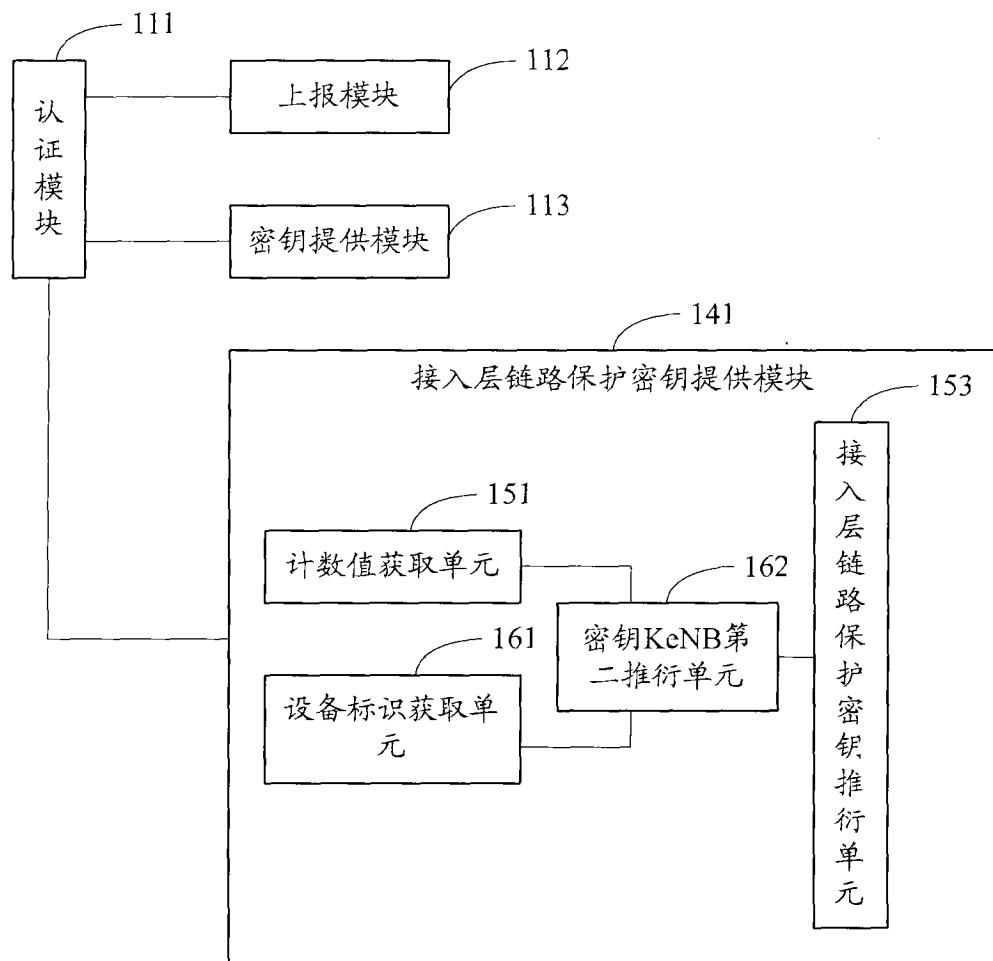


图 16

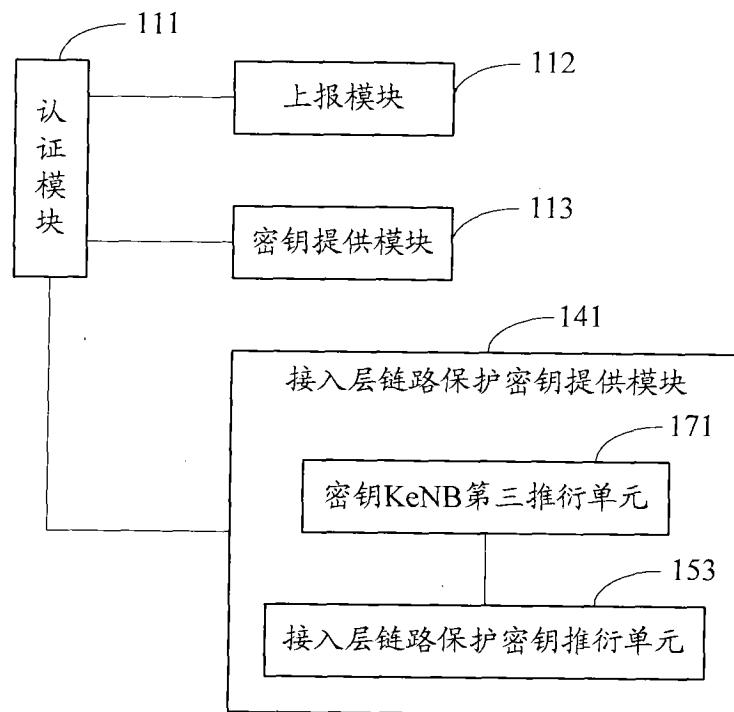


图 17

网关侧

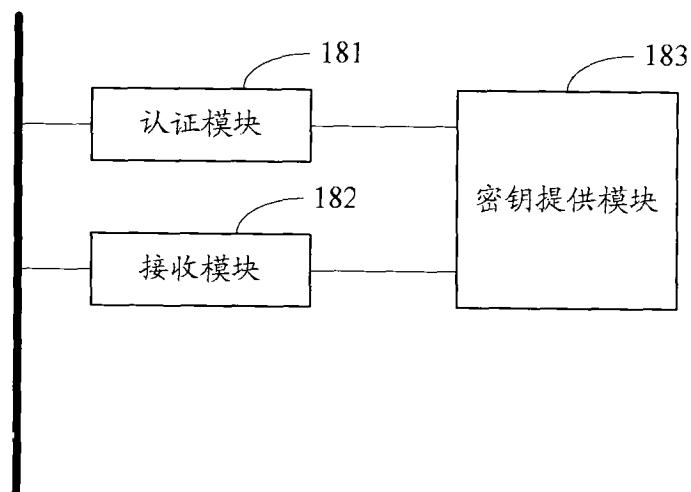


图 18

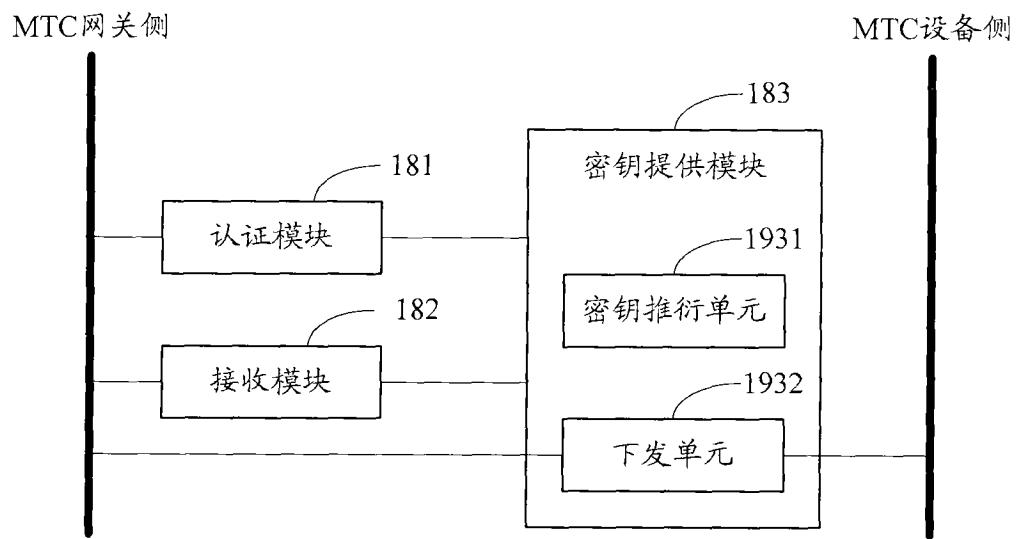


图 19

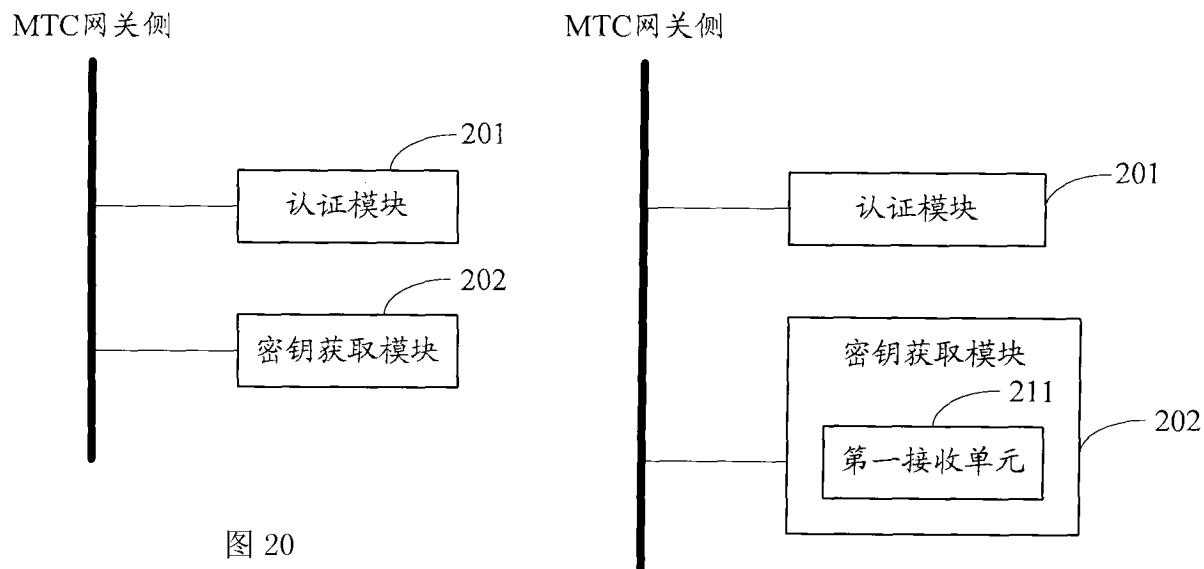


图 20

图 21

MTC网关侧

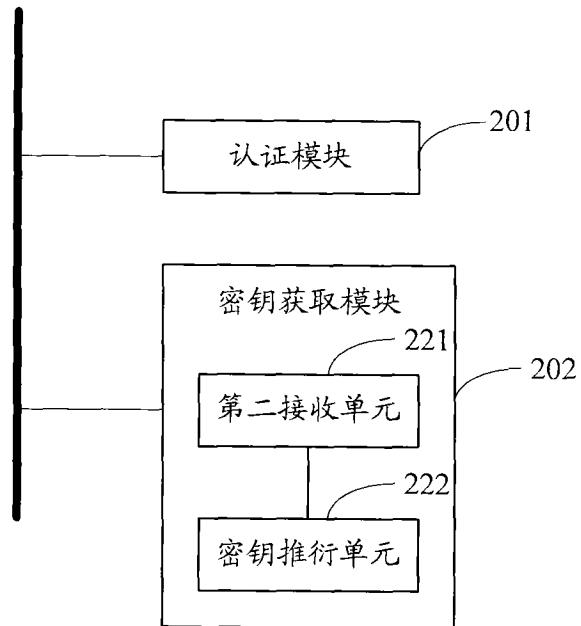


图 22

MTC网关侧

核心网节点侧

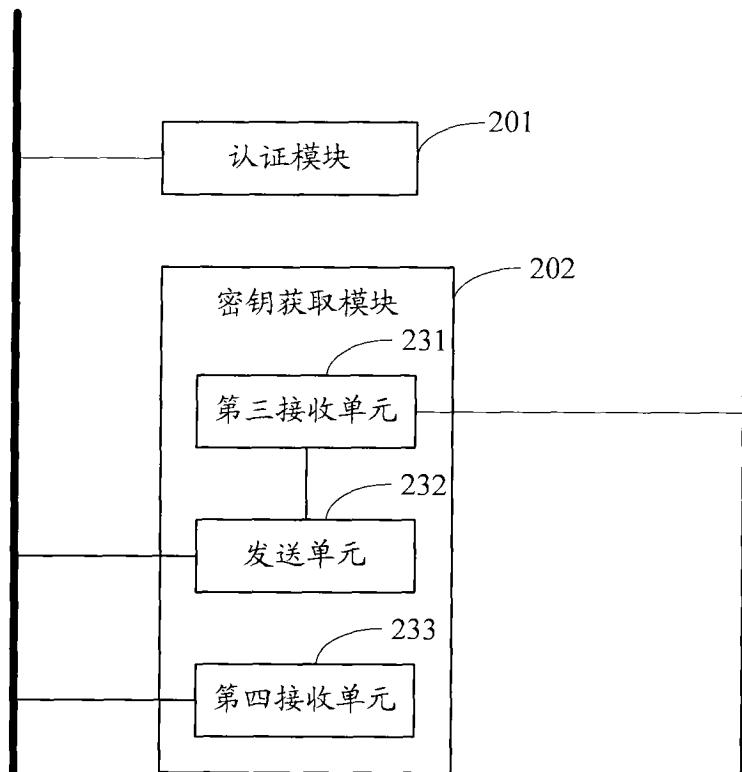


图 23

MTC网关侧

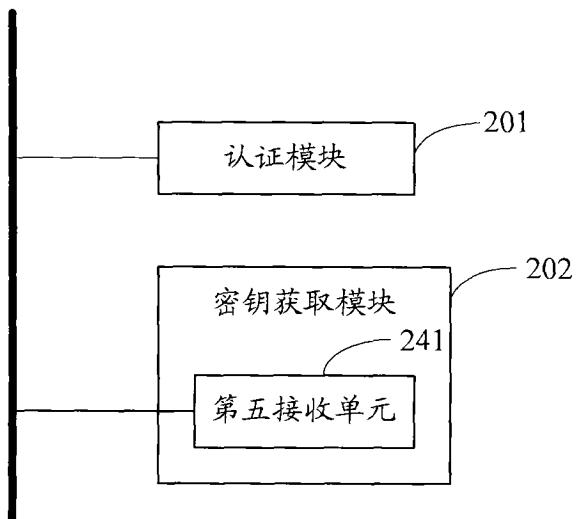


图 24