(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 107820283 B
(45)授权公告日 2021.04.09

(21)申请号 201610822515.9
(22)申请日 2016.09.13
(65)同一申请的已公布的文献号
申请公布号 CN 107820283 A
(43)申请公布日 2018.03.20
(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 吴荣 张博 甘露
(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫 熊永强
(51)Int.Cl.
H04W 36/00(2009.01)
H04W 12/041(2021.01)

(56)对比文件
US 2007060127 A1,2007.03.15
US 2013058308 A1,2013.03.07
CN 101946535 A,2011.01.12
CN 101340708 A,2009.01.07
CN 101841413 A,2010.09.22

审查员 杨雪

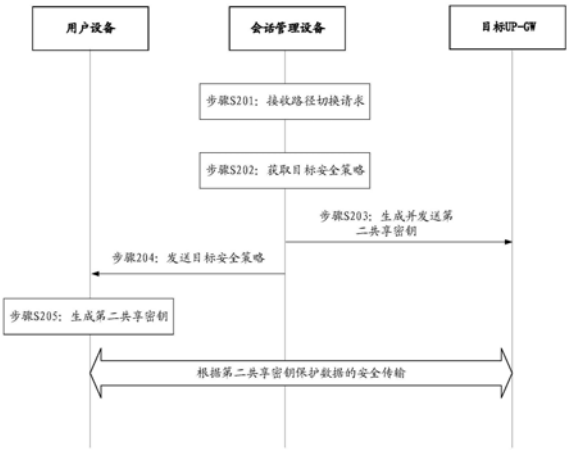
权利要求书9页 说明书36页 附图13页

(54)发明名称

一种网络切换保护方法、相关设备及系统

(57)摘要

本发明实施例公开了一种网络切换保护方法、相关设备及系统，该方法包括：会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求；会话管理设备根据路径切换请求获取目标安全策略；会话管理设备获取基于第一共享密钥和目标安全策略生成的第二共享密钥并将第二共享密钥发送给目标网关，或者将目标安全策略和预先获取的第一共享密钥发送给目标网关；会话管理设备将第二共享密钥发送给UE或者将目标安全策略发送给UE，以使UE根据第一共享密钥和目标安全策略生成第二共享密钥，第二共享密钥用于在UE与目标网关之间端到端地保护数据的安全传输。采用本发明，使得该UE在切换网络后依旧能够安全地传输数据。



CN 107820283 B

1.一种网络切换保护方法,其特征在于,包括:

会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求,所述源网络为所述UE当前驻留的网络;

所述会话管理设备根据所述路径切换请求获取目标安全策略,所述目标安全策略为初始安全策略或者为基于预设规则对所述初始安全策略处理得到的安全策略,所述初始安全策略定义了生成参考共享密钥的方式,所述参考共享密钥为根据基础密钥生成的用于所述UE在所述源网络中端到端地保护数据安全传输的密钥,所述基础密钥为所述UE与所述源网络双向认证生成的密钥或者基于所述UE与所述源网络双向认证生成的密钥推衍的密钥;

所述会话管理设备获取基于第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给目标网关,或者将所述目标安全策略和预先获取的所述第一共享密钥发送给所述目标网关,以使所述目标网关基于所述第一共享密钥和所述目标安全策略生成所述第二共享密钥,所述第一共享密钥为所述参考共享密钥或所述基础密钥,所述目标网关为所述目标网络的用户面网关;

所述会话管理设备将所述第二共享密钥发送给所述UE或者将所述目标安全策略发送给所述UE,以使所述UE根据所述第一共享密钥和所述目标安全策略生成所述第二共享密钥,所述第二共享密钥用于在所述UE与所述目标网关之间端到端地保护数据的安全传输。

2.根据权利要求1所述的方法,其特征在于,所述会话管理设备根据所述路径切换请求获取目标安全策略,包括:

所述会话管理设备向安全策略控制器发送安全策略请求消息,所述安全策略控制用于管理与所述源网络和/或所述目标网络中的设备相关的安全策略;

所述会话管理设备接收所述安全策略控制器发送的目标安全策略。

3.根据权利要求1所述的方法,其特征在于,所述会话管理设备包括源会话管理设备和目标会话管理设备;所述源会话管理设备用于管理所述源网络中的各个用户设备的会话,所述目标会话管理设备用于管理所述目标网络中的各个用户设备的会话;

所述会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求,包括:所述源会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求;

所述会话管理设备根据所述路径切换请求获取目标安全策略,包括:所述源会话管理设备获取初始安全策略并将所述初始安全策略发送给所述目标会话管理设备;所述目标会话管理设备根据所述初始安全策略获取目标安全策略;

所述会话管理设备获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给目标网关,包括:所述目标会话管理设备获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给目标网关;

所述会话管理设备将所述目标安全策略发送给所述UE,包括:所述目标会话管理设备将所述目标安全策略发送给所述UE。

4.根据权利要求3所述的方法,其特征在于,所述源会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求之后,所述目标会话管理设备获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给

目标网关之前，所述方法还包括：

所述源会话管理设备向源密钥管理设备发送密钥请求消息，所述源密钥管理设备用于管理接入到所述源网络中的各个用户设备的用于端到端地保护数据安全传输的共享密钥；

所述源会话管理设备接收所述源密钥管理设备根据所述密钥请求消息发送的第一共享密钥，并将所述第一共享密钥发送给所述目标会话管理设备。

5.根据权利要求1～4任一项所述的方法，其特征在于，所述会话管理设备获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥，包括：

向目标密钥管理设备发送所述目标安全策略，所述目标密钥管理设备用于管理接入到所述目标网络的各个用户设备的用于端到端地保护数据安全传输的共享密钥；

接收所述目标密钥管理设备根据所述目标安全策略和预先获取的所述第一共享密钥生成的第二共享密钥。

6.根据权利要求1～4任一项所述的方法，其特征在于，所述会话管理设备获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥，包括：

根据所述目标安全策略和预先获取的所述第一共享密钥生成第二共享密钥。

7.根据权利要求1～4任一项所述的方法，其特征在于，所述初始安全策略和所述目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

8.根据权利要求1～4任一项所述的方法，其特征在于，所述目标安全策略为根据所述用户设备的安全需求和/或所述目标网关的安全需求得到的，所述用户设备的安全需求表征了所述用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；所述目标网关的安全需求表征了所述目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

9.一种网络切换保护方法，其特征在于，包括：

密钥管理设备接收会话管理设备在接收到路径切换请求后发送的目标安全策略，所述路径切换请求用于请求将用户设备UE从源网络切换到目标网络，所述目标安全策略为初始安全策略或者为基于预设规则对所述初始安全策略处理得到的安全策略，所述初始安全策略定义了生成参考共享密钥的方式，所述参考共享密钥为根据基础密钥生成的用于所述UE在所述源网络中端到端地保护数据安全传输的密钥，所述基础密钥为所述UE与所述源网络双向认证生成的密钥或者基于所述UE与所述源网络双向认证生成的密钥推衍的密钥；

所述密钥管理设备根据所述目标安全策略和预先获取的第一共享密钥生成第二共享密钥，所述第一共享密钥为所述参考共享密钥或所述基础密钥；

所述密钥管理设备将所述第二共享密钥发送给所述会话管理设备，以使所述会话管理设备将所述第二共享密钥发送给目标网关，所述目标网关为所述目标网络的用户面网关，所述第二共享密钥用于所述UE与所述目标网关之间端到端地保护数据的安全传输。

10.根据权利要求9所述的方法，其特征在于，所述密钥管理设备根据所述目标安全策略和预先获取的所述第一共享密钥生成第二共享密钥之前，所述方法还包括：

所述密钥管理设备接收所述会话管理设备在接收到路径切换请求后发送的第一共享密钥，所述会话管理设备中预存了所述第一共享密钥或者所述会话管理设备预先向所述源网络中的管理密钥的设备获取了所述第一共享密钥。

11.根据权利要求9所述的方法，其特征在于，所述密钥管理设备根据所述目标安全策

略和预先获取的所述第一共享密钥生成第二共享密钥之前，所述方法还包括：

所述密钥管理设备向所述源网络中的管理密钥的设备发送密钥查询请求，所述密钥查询请求用于请求查询所述UE在所述源网络中用于端到端地保护数据安全传输的共享密钥；

所述密钥管理设备接收所述管理密钥的设备发送的所述第一共享密钥。

12.根据权利要求9所述的方法，其特征在于，所述密钥管理设备用于管理所述源网络中和所述目标网络中的各个用户设备的密钥，所述密钥管理设备中存储了所述第一共享密钥。

13.根据权利要求9～12任一项所述的方法，其特征在于，所述初始安全策略和所述目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

14.根据权利要求9～12任一项所述的方法，其特征在于，所述目标安全策略为根据所述用户设备的安全需求和/或所述目标网关的安全需求得到的，所述用户设备的安全需求表征了所述用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；所述目标网关的安全需求表征了所述目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

15.一种网络切换保护方法，其特征在于，包括：

用户设备向目标网络发送会话重建请求，所述会话重建请求用于触发向所述目标网络中的会话管理设备重建会话；

所述用户设备接收所述会话管理设备在接收到路径切换请求后发送的目标安全策略，所述路径切换请求用于请求将用户设备UE从源网络切换到目标网络，所述目标安全策略为初始安全策略或者为基于预设规则对所述初始安全策略处理得到的安全策略，所述初始安全策略定义了生成参考共享密钥的方式，所述参考共享密钥为根据基础密钥生成的用于所述UE在所述源网络中端到端地保护数据安全传输密钥，所述基础密钥为所述UE与所述源网络双向认证生成的密钥或者基于所述UE与所述源网络双向认证生成的密钥推衍的密钥；

所述用户设备根据所述目标安全策略和自身的第一共享密钥生成第二共享密钥；所述第二共享密钥用于所述UE与目标网关之间端到端地保护数据的安全传输，所述目标网关为所述目标网络的用户面网关，所述第一共享密钥为所述参考共享密钥或所述基础密钥。

16.根据权利要求15所述的方法，其特征在于，所述初始安全策略和所述目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

17.根据权利要求15或16所述的方法，其特征在于，所述目标安全策略为根据所述用户设备的安全需求和/或所述目标网关的安全需求得到的，所述用户设备的安全需求表征了所述用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；所述目标网关的安全需求表征了所述目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

18.一种会话管理设备，其特征在于，包括：

第一接收单元，用于接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求，所述源网络为所述UE当前驻留的网络；

第一获取单元，用于根据所述路径切换请求获取目标安全策略，所述目标安全策略为初始安全策略或者为基于预设规则对所述初始安全策略处理得到的安全策略，所述初始安全策略定义了生成参考共享密钥的方式，所述参考共享密钥为根据基础密钥生成的用于所

述UE在所述源网络中端到端地保护数据安全传输的密钥，所述基础密钥为所述UE与所述源网络双向认证生成的密钥或者基于所述UE与所述源网络双向认证生成的密钥推衍的密钥；

第二获取单元，用于获取基于第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给目标网关，或者将所述目标安全策略和预先获取的所述第一共享密钥发送给所述目标网关，以使所述目标网关基于所述第一共享密钥和所述目标安全策略生成所述第二共享密钥，所述第一共享密钥为所述参考共享密钥或所述基础密钥，所述目标网关为所述目标网络的用户面网关；

第一发送单元，用于将所述第二共享密钥发送给所述UE或者将所述目标安全策略发送给所述UE，以使所述UE根据所述第一共享密钥和所述目标安全策略生成所述第二共享密钥，所述第二共享密钥用于在所述UE与所述目标网关之间端到端地保护数据的安全传输。

19.根据权利要求18所述的会话管理设备，其特征在于，所述第一获取单元具体用于向安全策略控制器发送安全策略请求消息，所述安全策略控制用于管理与所述源网络和/或所述目标网络中的设备相关的安全策略；接收所述安全策略控制器发送的目标安全策略。

20.根据权利要求18所述的会话管理设备，其特征在于，所述会话管理设备包括源会话管理设备和目标会话管理设备；所述源会话管理设备用于管理所述源网络中的各个用户设备的会话，所述目标会话管理设备用于管理所述目标网络中的各个用户设备的会话；所述源会话管理设备包括所述第一接收单元和所述第一获取单元，所述目标会话管理设备包括所述第二获取单元和所述第一发送单元；

所述第一获取单元具体用于获取初始安全策略并将所述初始安全策略发送给所述目标会话管理设备；所述目标会话管理设备根据所述初始安全策略获取目标安全策略；

所述第二获取单元具体用于获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给目标网关。

21.根据权利要求20所述的会话管理设备，其特征在于，所述源会话管理设备还包括第二发送单元和第二接收单元：

所述第二发送单元用于在所述接收单元接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求之后，所述第二获取单元获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给目标网关之前，向源密钥管理设备发送密钥请求消息，所述源密钥管理设备用于管理接入到所述源网络中的各个用户设备的用于端到端地保护数据安全传输的共享密钥；

所述第二接收单元，用于接收所述源密钥管理设备根据所述密钥请求消息发送的第一共享密钥，并将所述第一共享密钥发送给所述目标会话管理设备。

22.根据权利要求18～21任一项所述的会话管理设备，其特征在于，所述第二获取单元具体用于向目标密钥管理设备发送所述目标安全策略，所述目标密钥管理设备用于管理接入到所述目标网络的各个用户设备的用于端到端地保护数据安全传输的共享密钥；接收所述目标密钥管理设备根据所述目标安全策略和预先获取的所述第一共享密钥生成的第二共享密钥。

23.根据权利要求18～21任一项所述的会话管理设备，其特征在于，所述第二获取单元具体用于根据所述目标安全策略和预先获取的所述第一共享密钥生成第二共享密钥。

24.根据权利要求18～21任一项所述的会话管理设备，其特征在于，所述初始安全策略

和所述目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

25.根据权利要求18～21任一项所述的会话管理设备，其特征在于，所述目标安全策略为根据所述用户设备的安全需求和/或所述目标网关的安全需求得到的，所述用户设备的安全需求表征了所述用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；所述目标网关的安全需求表征了所述目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

26.一种密钥管理设备，其特征在于，包括：

第一接收单元，用于接收会话管理设备在接收到路径切换请求后发送的目标安全策略，所述路径切换请求用于请求将用户设备UE从源网络切换到目标网络，所述目标安全策略为初始安全策略或者为基于预设规则对所述初始安全策略处理得到的安全策略，所述初始安全策略定义了生成参考共享密钥的方式，所述参考共享密钥为根据基础密钥生成的用于所述UE在所述源网络中端到端地保护数据安全传输的密钥，所述基础密钥为所述UE与所述源网络双向认证生成的密钥或者基于所述UE与所述源网络双向认证生成的密钥推衍的密钥；

生成单元，用于根据所述目标安全策略和预先获取的第一共享密钥生成第二共享密钥，所述第一共享密钥为所述参考共享密钥或所述基础密钥；

第一发送单元，用于将所述第二共享密钥发送给所述会话管理设备，以使所述会话管理设备将所述第二共享密钥发送给目标网关，所述目标网关为所述目标网络的用户面网关，所述第二共享密钥用于所述UE与所述目标网关之间端到端地保护数据的安全传输。

27.根据权利要求26所述的密钥管理设备，其特征在于，还包括：

第二接收单元，用于在所述密钥管理设备根据所述目标安全策略和预先获取的所述第一共享密钥生成第二共享密钥之前，接收所述会话管理设备在接收到路径切换请求后发送的第一共享密钥，所述会话管理设备中预存了所述第一共享密钥或者所述会话管理设备预先向所述源网络中的管理密钥的设备获取了所述第一共享密钥。

28.根据权利要求26所述的密钥管理设备，其特征在于，还包括：

第二发送单元，用于在所述密钥管理设备根据所述目标安全策略和预先获取的所述第一共享密钥生成第二共享密钥之前，向所述源网络中的管理密钥的设备发送密钥查询请求，所述密钥查询请求用于请求查询所述UE在所述源网络中用于端到端地保护数据安全传输的共享密钥；

第三接收单元，用于接收所述管理密钥的设备发送的所述第一共享密钥。

29.根据权利要求26所述的密钥管理设备，其特征在于，所述密钥管理设备用于管理所述源网络中和所述目标网络中的各个用户设备的密钥，所述密钥管理设备中存储了所述第一共享密钥。

30.根据权利要求26～29任一项所述的密钥管理设备，其特征在于，所述初始安全策略和所述目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

31.根据权利要求26～29任一项所述的密钥管理设备，其特征在于，所述目标安全策略为根据所述用户设备的安全需求和/或所述目标网关的安全需求得到的，所述用户设备的安全需求表征了所述用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；所述目标网关的安全需求表征了所述目标网关可接受的密钥算法、可接

受的密钥长度和可接受的密钥更新周期中至少一项。

32.一种用户设备，其特征在于，包括：

发送单元，用于向目标网络发送会话重建请求，所述会话重建请求用于触发向所述目标网络中的会话管理设备重建会话；

接收单元，用于接收所述会话管理设备在接收到路径切换请求后发送的目标安全策略，所述路径切换请求用于请求将用户设备UE从源网络切换到目标网络，所述目标安全策略为初始安全策略或者为基于预设规则对所述初始安全策略处理得到的安全策略，所述初始安全策略定义了生成参考共享密钥的方式，所述参考共享密钥为根据基础密钥生成的用于所述UE在所述源网络中端到端地保护数据安全传输密钥，所述基础密钥为所述UE与所述源网络双向认证生成的密钥或者基于所述UE与所述源网络双向认证生成的密钥推衍的密钥；

生成单元，用于根据所述目标安全策略和自身的第一共享密钥生成第二共享密钥；所述第二共享密钥用于所述UE与目标网关之间端到端地保护数据的安全传输，所述目标网关为所述目标网络的用户面网关，所述第一共享密钥为所述参考共享密钥或所述基础密钥。

33.根据权利要求32所述的用户设备，其特征在于，所述初始安全策略和所述目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

34.根据权利要求32或33所述的用户设备，其特征在于，所述目标安全策略为根据所述用户设备的安全需求和/或所述目标网关的安全需求得到的，所述用户设备的安全需求表征了所述用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；所述目标网关的安全需求表征了所述目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

35.一种会话管理设备，其特征在于，所述会话管理设备包括处理器、存储器和收发器，其中：

所述存储器用于存储数据和程序；

所述处理器调用所述存储器中的程序用于执行如下操作：

通过所述收发器接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求，所述源网络为所述UE当前驻留的网络；

根据所述路径切换请求获取目标安全策略，所述目标安全策略为初始安全策略或者为基于预设规则对所述初始安全策略处理得到的安全策略，所述初始安全策略定义了生成参考共享密钥的方式，所述参考共享密钥为根据基础密钥生成的用于所述UE在所述源网络中端到端地保护数据安全传输的密钥，所述基础密钥为所述UE与所述源网络双向认证生成的密钥或者基于所述UE与所述源网络双向认证生成的密钥推衍的密钥；

获取基于第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给目标网关，或者将所述目标安全策略和预先获取的所述第一共享密钥发送给所述目标网关，以使所述目标网关基于所述第一共享密钥和所述目标安全策略生成的所述第二共享密钥，所述第一共享密钥为所述参考共享密钥或所述基础密钥，所述目标网关为所述目标网络的用户面网关；

通过所述收发器将所述第二共享密钥发送给所述UE或者将所述目标安全策略发送给所述UE，以使所述UE根据所述第一共享密钥和所述目标安全策略生成所述第二共享密钥，

所述第二共享密钥用于在所述UE与所述目标网关之间端到端地保护数据的安全传输。

36.根据权利要求35所述的会话管理设备，其特征在于，所述处理器根据所述路径切换请求获取目标安全策略，具体为：

通过所述收发器向安全策略控制器发送安全策略请求消息，所述安全策略控制用于管理与所述源网络和/或所述目标网络中的设备相关的安全策略；

通过所述收发器接收所述安全策略控制器发送的目标安全策略。

37.根据权利要求35所述的会话管理设备，其特征在于，所述会话管理设备包括源会话管理设备和目标会话管理设备；所述源会话管理设备用于管理所述源网络中的各个用户设备的会话，所述目标会话管理设备用于管理所述目标网络中的各个用户设备的会话；所述源会话管理设备包括第一处理器和第一收发器，所述目标会话管理设备包括第二处理器和第二收发器，其中：

所述处理器通过所述收发器接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求，具体为：所述第一处理器通过所述第一收发器接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求；

所述处理器根据所述路径切换请求获取目标安全策略，包括：所述第一处理器获取初始安全策略并将所述初始安全策略发送给所述目标会话管理设备；根据所述初始安全策略获取目标安全策略；

所述处理器获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给目标网关，包括：所述第二处理器获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给目标网关；

所述处理器通过所述收发器将所述目标安全策略发送给所述UE，包括：第二处理器通过所述第二收发器将所述目标安全策略发送给所述UE。

38.根据权利要求37所述的会话管理设备，其特征在于，所述第一处理器通过所述第一收发器接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求之后，所述第二处理器获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥并将所述第二共享密钥发送给目标网关之前，所述第一处理器还用于：

通过所述第一收发器向源密钥管理设备发送密钥请求消息，所述源密钥管理设备用于管理接入到所述源网络中的各个用户设备的用于端到端地保护数据安全传输的共享密钥；

通过所述第一收发器接收所述源密钥管理设备根据所述密钥请求消息发送的第一共享密钥，并将所述第一共享密钥发送给所述目标会话管理设备。

39.根据权利要求35～38任一项所述的会话管理设备，其特征在于，所述处理器获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥，具体为：

向目标密钥管理设备发送所述目标安全策略，所述目标密钥管理设备用于管理接入到所述目标网络的各个用户设备的用于端到端地保护数据安全传输的共享密钥；

接收所述目标密钥管理设备根据所述目标安全策略和预先获取的所述第一共享密钥生成的第二共享密钥。

40.根据权利要求35～38任一项所述的会话管理设备，其特征在于，所述处理器获取基于所述第一共享密钥和所述目标安全策略生成的第二共享密钥，具体为：

根据所述目标安全策略和预先获取的所述第一共享密钥生成第二共享密钥。

41.根据权利要求35～38任一项所述的会话管理设备，其特征在于，所述初始安全策略和所述目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

42.根据权利要求35～38任一项所述的会话管理设备，其特征在于，所述目标安全策略为根据所述用户设备的安全需求和/或所述目标网关的安全需求得到的，所述用户设备的安全需求表征了所述用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；所述目标网关的安全需求表征了所述目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

43.一种密钥管理设备，其特征在于，所述密钥管理设备包括处理器、存储器和收发器，其中：

所述存储器用于存储数据和程序；

所述处理器调用所述存储器中的程序用于执行如下操作：

通过所述收发器接收会话管理设备在接收到路径切换请求后发送的目标安全策略，所述路径切换请求用于请求将用户设备UE从源网络切换到目标网络，所述目标安全策略为初始安全策略或者为基于预设规则对所述初始安全策略处理得到的安全策略，所述初始安全策略定义了生成参考共享密钥的方式，所述参考共享密钥为根据基础密钥生成的用于所述UE在所述源网络中端到端地保护数据安全传输的密钥，所述基础密钥为所述UE与所述源网络双向认证生成的密钥或者基于所述UE与所述源网络双向认证生成的密钥推衍的密钥；

根据所述目标安全策略和预先获取的第一共享密钥生成第二共享密钥，所述第一共享密钥为所述参考共享密钥或所述基础密钥；

通过所述收发器将所述第二共享密钥发送给所述会话管理设备，以使所述会话管理设备将所述第二共享密钥发送给目标网关，所述目标网关为所述目标网络的用户面网关，所述第二共享密钥用于所述UE与所述目标网关之间端到端地保护数据的安全传输。

44.根据权利要求43所述的密钥管理设备，其特征在于，所述处理器根据所述目标安全策略和预先获取的所述第一共享密钥生成第二共享密钥之前，还用于：

通过所述收发器接收所述会话管理设备在接收到路径切换请求后发送的第一共享密钥，所述会话管理设备中预存了所述第一共享密钥或者所述会话管理设备预先向所述源网络中的管理密钥的设备获取了所述第一共享密钥。

45.根据权利要求43所述的密钥管理设备，其特征在于，所述处理器根据所述目标安全策略和预先获取的所述第一共享密钥生成第二共享密钥之前，还用于：

通过所述收发器向所述源网络中的管理密钥的设备发送密钥查询请求，所述密钥查询请求用于请求查询所述UE在所述源网络中用于端到端地保护数据安全传输的共享密钥；

通过所述收发器接收所述管理密钥的设备发送的所述第一共享密钥。

46.根据权利要求43所述的密钥管理设备，其特征在于，所述密钥管理设备用于管理所述源网络中和所述目标网络中的各个用户设备的密钥，所述密钥管理设备中存储了所述第一共享密钥。

47.根据权利要求43～46任一项所述的密钥管理设备，其特征在于，所述初始安全策略和所述目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

48.根据权利要求43～46任一项所述的密钥管理设备，其特征在于，所述目标安全策略为根据所述用户设备的安全需求和/或所述目标网关的安全需求得到的，所述用户设备的

安全需求表征了所述用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项;所述目标网关的安全需求表征了所述目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

49.一种用户设备,其特征在于,所述用户设备包括处理器、存储器和收发器,其中:

所述存储器用于存储数据和程序;

所述处理器调用所述存储器中的程序用于执行如下操作:

通过所述收发器向目标网络发送会话重建请求,所述会话重建请求用于触发向所述目标网络中的会话管理设备重建会话;

通过所述收发器接收所述会话管理设备在接收到路径切换请求后发送的目标安全策略,所述路径切换请求用于请求将用户设备UE从源网络切换到目标网络,所述目标安全策略为初始安全策略或者为基于预设规则对所述初始安全策略处理得到的安全策略,所述初始安全策略定义了生成参考共享密钥的方式,所述参考共享密钥为根据基础密钥生成的用于所述UE在所述源网络中端到端地保护数据安全传输密钥,所述基础密钥为所述UE与所述源网络双向认证生成的密钥或者基于所述UE与所述源网络双向认证生成的密钥推衍的密钥;

根据所述目标安全策略和自身的第一共享密钥生成第二共享密钥;所述第二共享密钥用于所述UE与目标网关之间端到端地保护数据的安全传输,所述目标网关为所述目标网络的用户面网关,所述第一共享密钥为所述参考共享密钥或所述基础密钥。

50.根据权利要求49所述的用户设备,其特征在于,所述初始安全策略和所述目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

51.根据权利要求49或50所述的用户设备,其特征在于,所述目标安全策略为根据所述用户设备的安全需求和/或所述目标网关的安全需求得到的,所述用户设备的安全需求表征了所述用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项;所述目标网关的安全需求表征了所述目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

52.一种通信系统,其特征在于,所述通信系统包括会话管理设备、密钥管理设备和用户设备,其中:

所述会话管理设备为权利要求18～25任一项所述的会话管理设备,或者为权利要求35～42任一项所述的会话管理设备;

所述密钥管理设备为权利要求26～31任一项所述的密钥管理设备,或者为权利要求43～48任一项所述的密钥管理设备;

所述用户设备为权利要求32～34任一项所述的用户设备,或者为权利要求49～51任一项所述的用户设备。

一种网络切换保护方法、相关设备及系统

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种网络切换保护方法、相关设备及系统。

背景技术

[0002] 未来第五代移动通信技术(5th-Generation，简称：5G)网络正朝着网络多元化、宽带化、综合化、智能化的方向发展。随着各种用户设备(英文：User Equipment，简称：UE)的普及，移动数据流量将呈现爆炸式增长。为了提高流量的传输效率，5G网络在交互流程上也会做相应的改进，例如，5G技术中UE在网络中传输数据时，无需与无线接入网设备(英文：Radio Access Network，简称：RAN)之间验证数据的安全性，该RAN用来转发该UE与UP-GW之间的数据即可，验证数据安全性任务的工作由该UE与该网络中的用户面网关(英文：User Plane-Gateway，简称：UP-GW)来进行，即UE与UP-GW之间端到端地保护数据的安全传输。

[0003] 图1为目前正在研究的一种5G网络的流程示意图，该流程的执行需要的网元包括UE、RAN、UP-GW等，执行流程大致如下：

[0004] 步骤1：UE在当前驻留的网络(当前驻留的网络可以称为“源网络”)中进行数据的传输，该UE与该UP-GW预先协商出共享密钥来保护数据的安全传输。

[0005] 步骤2：该UE执行由源网络到新网络的切换，未来5G中可以根据网络当前的负载、该UE的地理位置变化、当前网络的信号强度等信息来触发该UE发生切换。新网络中的用户面网关可以称为目标UP-GW。

[0006] 步骤3：该UE与该目标UP-GW建立新会话。

[0007] 步骤4：该UE基于该新会话在该新网络中进行数据传输，且该UE与该UP-GW共同保护数据的安全传输。

[0008] 步骤5：该UE与切换之前的网络中的UP-GW进行协商，释放该之前的网络中的会话。可以理解的是，步骤4和5的执行顺序可以交换，或者同时进行。

[0009] 在上述流程中，UE与目标UP-GW建立新会话时需要生成新的共享密钥，后续该UE与该目标UP-GW使用该共享密钥来保护数据在新网络中安全传输；如何生成该UE在新网络中的共享密钥是本领域的技术人员正在研究的问题。

发明内容

[0010] 本发明实施例公开了一种网络切换保护方法、相关设备及系统，使得该UE在切换网络后依旧能够安全地传输数据。

[0011] 第一方面，本发明实施例提供一种网络切换保护方法，该方法包括：会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求，该源网络为该UE当前驻留的网络；该会话管理设备根据该路径切换请求获取目标安全策略，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输的密钥，该基础密钥为该UE与该源网络双向认证生

成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥;该会话管理设备获取基于第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关,或者将该目标安全策略和预先获取的该第一共享密钥发送给该目标网关,以使该目标网关基于该第一共享密钥和该目标安全策略生成的该第二共享密钥,该第一共享密钥为该参考共享密钥或该基础密钥,该目标网关为该目标网络的用户面网关;该会话管理设备将该第二共享密钥发送给该UE或者将该目标安全策略发送给该UE,以使该UE根据该第一共享密钥和该目标安全策略生成该第二共享密钥,该第二共享密钥用于在该UE与该目标网关之间端到端地保护数据的安全传输。

[0012] 通过执行上述步骤,该UE切换到目标网络时,通过源网络或者目标网络中的网元生成目标安全策略,然后基于该目标安全策略和第一共享密钥生成第二共享密钥,最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥,使得该UE在切换网络后依旧能够安全地传输数据。

[0013] 结合第一方面,在第一方面的第一种可能的实现方式中,该会话管理设备根据该路径切换请求获取目标安全策略,包括:该会话管理设备向安全策略控制器发送安全策略请求消息,该安全策略控制用于管理与该源网络和/或该目标网络中的设备相关的安全策略;该会话管理设备接收该安全策略控制器发送的目标安全策略。

[0014] 结合第一方面,在第一方面的第二种可能的实现方式中,该会话管理设备包括源会话管理设备和目标会话管理设备;该源会话管理设备用于管理该源网络中的各个用户设备的会话,该目标会话管理设备用于管理该目标网络中的各个用户设备的会话;该会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求,包括:该源会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求;该会话管理设备根据该路径切换请求获取目标安全策略,包括:该源会话管理设备获取初始安全策略并将该初始安全策略发送给该目标会话管理设备;该目标会话管理设备根据该初始安全策略获取目标安全策略;该会话管理设备获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关,包括:该目标会话管理设备获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关;该会话管理设备将该目标安全策略发送给该UE,包括:该目标会话管理设备将该目标安全策略发送给该UE。

[0015] 结合第一方面的第二种可能的实现方式,在第一方面的第三种可能的实现方式中,该源会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求之后,该目标会话管理设备获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关之前,该方法还包括:该源会话管理设备向源密钥管理设备发送密钥请求消息,该源密钥管理设备用于管理接入到该源网络中的各个用户设备的用于端到端地保护数据安全传输的共享密钥;该源会话管理设备接收该源密钥管理设备根据该密钥请求消息发送的第一共享密钥,并将该第一共享密钥发送给该目标会话管理设备。

[0016] 结合第一方面,或者第一方面的第一种可能的实现方式,或者第一方面的第二种可能的实现方式,或者第一方面的第三种可能的实现方式,在第一方面的第四种可能的实现方式中,该会话管理设备获取基于该第一共享密钥和该目标安全策略生成的第二共享密

钥，包括：向目标密钥管理设备发送该目标安全策略，该目标密钥管理设备用于管理接入到该目标网络的各个用户设备的用于端到端地保护数据安全传输的共享密钥；接收该目标密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成的第二共享密钥。

[0017] 结合第一方面，或者第一方面的第一种可能的实现方式，或者第一方面的第二种可能的实现方式，或者第一方面的第三种可能的实现方式，在第一方面的第五种可能的实现方式中，该会话管理设备获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥，包括：根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥。

[0018] 结合第一方面，或者第一方面的第一种可能的实现方式，或者第一方面的第二种可能的实现方式，或者第一方面的第三种可能的实现方式，或者第一方面的第四种可能的实现方式，或者第一方面的第五种可能的实现方式，在第一方面的第六种可能的实现方式中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0019] 结合第一方面，或者第一方面的第一种可能的实现方式，或者第一方面的第二种可能的实现方式，或者第一方面的第三种可能的实现方式，或者第一方面的第四种可能的实现方式，或者第一方面的第六种可能的实现方式，在第一方面的第七种可能的实现方式中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0020] 第二方面，本发明实施例提供一种网络切换保护方法，该方法包括：

[0021] 密钥管理设备接收会话管理设备在接收到路径切换请求后发送的目标安全策略，该路径切换请求用于请求将用户设备UE从源网络切换到目标网络，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输的密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；该密钥管理设备根据该目标安全策略和预先获取的第一共享密钥生成第二共享密钥，该第一共享密钥为该参考共享密钥或该基础密钥；该密钥管理设备将该第二共享密钥发送给该会话管理设备，以使该会话管理设备将该第二共享密钥发送给目标网关，该目标网关为该目标网络的用户面网关，该第二共享密钥用于该UE与该目标网关之间端到端地保护数据的安全传输。

[0022] 通过执行上述步骤，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0023] 结合第二方面，在第二方面的第一种可能的实现方式中，该密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥之前，该方法还包括：该密钥管理设备接收该会话管理设备在接收到路径切换请求后发送的第一共享密钥，该会话管理设备中预存了该第一共享密钥或者该会话管理设备预先向该源网络中的管理密钥的设备获取了该第一共享密钥。

[0024] 结合第二方面，在第二方面的第二种可能的实现方式中，该密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥之前，该方法还包括：该密钥管理设备向该源网络中的管理密钥的设备发送密钥查询请求，该密钥查询请求用于请求查询该UE在该源网络中用于端到端地保护数据安全传输的共享密钥；该密钥管理设备接收该管理密钥的设备发送的该第一共享密钥。

[0025] 结合第二方面，在第二方面的第三种可能的实现方式中，该密钥管理设备用于管理该源网络中和该目标网络中的各个用户设备的密钥，该密钥管理设备中存储了该第一共享密钥。

[0026] 结合第二方面，或者第二方面的第一种可能的实现方式，或者第二方面的第二种可能的实现方式，或者第二方面的第三种可能的实现方式，在第二方面的第四种可能的实现方式中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0027] 结合第二方面，或者第二方面的第一种可能的实现方式，或者第二方面的第二种可能的实现方式，或者第二方面的第三种可能的实现方式，或者第二方面的第四种可能的实现方式，在第二方面的第五种可能的实现方式中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0028] 第三方面，本发明实施例提供一种网络切换保护方法，该方法包括：用户设备向目标网络发送会话重建请求，该会话重建请求用于触发向该目标网络中的会话管理设备重建会话。该用户设备接收该会话管理设备在接收到路径切换请求后发送的目标安全策略，该路径切换请求用于请求将用户设备UE从源网络切换到目标网络，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；该用户设备根据该目标安全策略和自身的第一共享密钥生成第二共享密钥；该第二共享密钥用于该UE与目标网关之间端到端地保护数据的安全传输，该目标网关为该目标网络的用户面网关，该第一共享密钥为该参考共享密钥或该基础密钥。

[0029] 通过执行上述操作，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0030] 结合第三方面，在第三方面的第一种可能的实现方式中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0031] 结合第三方面，或者第三方面的第一种可能的实现方式，在第三方面的第二种可能的实现方式中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥

长度和可接受的密钥更新周期中至少一项;该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0032] 第四方面,本发明实施例提供一种会话管理设备,该会话管理设备包括:第一接收单元,用于接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求,该源网络为该UE当前驻留的网络;第一获取单元,用于根据该路径切换请求获取目标安全策略,该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略,该初始安全策略定义了生成参考共享密钥的方式,该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输的密钥,该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥;第二获取单元,用于获取基于第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关,或者将该目标安全策略和预先获取的该第一共享密钥发送给该目标网关,以使该目标网关基于该第一共享密钥和该目标安全策略生成的该第二共享密钥,该第一共享密钥为该参考共享密钥或该基础密钥,该目标网关为该目标网络的用户面网关;第一发送单元,用于将该第二共享密钥发送给该UE或者将该目标安全策略发送给该UE,以使该UE根据该第一共享密钥和该目标安全策略生成该第二共享密钥,该第二共享密钥用于在该UE与该目标网关之间端到端地保护数据的安全传输。

[0033] 通过执行上述操作,该UE切换到目标网络时,通过源网络或者目标网络中的网元生成目标安全策略,然后基于该目标安全策略和第一共享密钥生成第二共享密钥,最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥,使得该UE在切换网络后依旧能够安全地传输数据。

[0034] 结合第四方面,在第四方面的第一种可能的实现方式中,该第一获取单元具体用于向安全策略控制器发送安全策略请求消息,该安全策略控制用于管理与该源网络和/或该目标网络中的设备相关的安全策略;接收该安全策略控制器发送的目标安全策略。

[0035] 结合第四方面,在第四方面的第二种可能的实现方式中,该会话管理设备包括源会话管理设备和目标会话管理设备;该源会话管理设备用于管理该源网络中的各个用户设备的会话,该目标会话管理设备用于管理该目标网络中的各个用户设备的会话;该源会话管理设备包括该第一接收单元和该第一获取单元,该目标会话管理设备包括该第二获取单元和该第一发送单元;该第一获取单元具体用于获取初始安全策略并将该初始安全策略发送给该目标会话管理设备;该目标会话管理设备根据该初始安全策略获取目标安全策略;该第二获取单元具体用于获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关。

[0036] 结合第四方面的第二种可能的实现方式,在第四方面的第三种可能的实现方式中,该源会话管理设备还包括第二发送单元和第二接收单元:该第二发送单元用于在该接收单元接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求之后,该第二获取单元获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关之前,向源密钥管理设备发送密钥请求消息,该源密钥管理设备用于管理接入到该源网络中的各个用户设备的用于端到端地保护数据安全传输的共享密钥;该第二接收单元,用于接收该源密钥管理设备根据该密钥请求消息发送的第一共享密钥,并将该第一共享密钥发送给该目标会话管理设备。

[0037] 结合第四方面，或者第四方面的第一种可能的实现方式，或者第四方面的第二种可能的实现方式，或者第四方面的第三种可能的实现方式，在第四方面的第四种可能的实现方式中，该第二获取单元具体用于向目标密钥管理设备发送该目标安全策略，该目标密钥管理设备用于管理接入到该目标网络的各个用户设备的用于端到端地保护数据安全传输的共享密钥；接收该目标密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成的第二共享密钥。

[0038] 结合第四方面，或者第四方面的第一种可能的实现方式，或者第四方面的第二种可能的实现方式，或者第四方面的第三种可能的实现方式，在第四方面的第五种可能的实现方式中，该第二获取单元具体用于根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥。

[0039] 结合第四方面，或者第四方面的第一种可能的实现方式，或者第四方面的第二种可能的实现方式，或者第四方面的第三种可能的实现方式，或者第四方面的第四种可能的实现方式，或者第四方面的第五种可能的实现方式，在第四方面的第六种可能的实现方式中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0040] 结合第四方面，或者第四方面的第一种可能的实现方式，或者第四方面的第二种可能的实现方式，或者第四方面的第三种可能的实现方式，或者第四方面的第四种可能的实现方式，或者第四方面的第六种可能的实现方式，在第四方面的第七种可能的实现方式中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0041] 第五方面，本发明实施例提供一种密钥管理设备，该密钥管理设备包括：第一接收单元，用于接收会话管理设备在接收到路径切换请求后发送的目标安全策略，该路径切换请求用于请求将用户设备UE从源网络切换到目标网络，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输的密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；生成单元，用于根据该目标安全策略和预先获取的第一共享密钥生成第二共享密钥，该第一共享密钥为该参考共享密钥或该基础密钥；第一发送单元，用于将该第二共享密钥发送给该会话管理设备，以使该会话管理设备将该第二共享密钥发送给目标网关，该目标网关为该目标网络的用户面网关，该第二共享密钥用于该UE与该目标网关之间端到端地保护数据的安全传输。

[0042] 通过运行上述单元，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0043] 结合第五方面，在第五方面的第一种可能的实现方式中，还包括：第二接收单元，用于在该密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成第二共享

密钥之前，接收该会话管理设备在接收到路径切换请求后发送的第一共享密钥，该会话管理设备中预存了该第一共享密钥或者该会话管理设备预先向该源网络中的管理密钥的设备获取了该第一共享密钥。

[0044] 结合第五方面，在第五方面的第二种可能的实现方式中，还包括：第二发送单元，用于在该密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥之前，向该源网络中的管理密钥的设备发送密钥查询请求，该密钥查询请求用于请求查询该UE在该源网络中用于端到端地保护数据安全传输的共享密钥；第三接收单元，用于接收该管理密钥的设备发送的该第一共享密钥。

[0045] 结合第五方面，在第五方面的第三种可能的实现方式中，该密钥管理设备用于管理该源网络中和该目标网络中的各个用户设备的密钥，该密钥管理设备中存储了该第一共享密钥。

[0046] 结合第五方面，或者第五方面的第一种可能的实现方式，或者第五方面的第二种可能的实现方式，或者第五方面的第三种可能的实现方式，在第五方面的第四种可能的实现方式中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0047] 结合第五方面，或者第五方面的第一种可能的实现方式，或者第五方面的第二种可能的实现方式，或者第五方面的第三种可能的实现方式，或者第五方面的第四种可能的实现方式，在第五方面的第五种可能的实现方式中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0048] 第六方面，本发明实施例提供一种用户设备，该用户设备包括：发送单元，用于向目标网络发送会话重建请求，该会话重建请求用于触发向该目标网络中的会话管理设备重建会话。接收单元，用于接收该会话管理设备在接收到路径切换请求后发送的目标安全策略，该路径切换请求用于请求将用户设备UE从源网络切换到目标网络，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；生成单元，用于根据该目标安全策略和自身的第一共享密钥生成第二共享密钥；该第二共享密钥用于该UE与目标网关之间端到端地保护数据的安全传输，该目标网关为该目标网络的用户面网关，该第一共享密钥为该参考共享密钥或该基础密钥。

[0049] 通过运行上述单元，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0050] 结合第六方面，在第六方面的第一种可能的实现方式中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0051] 结合第六方面，或者第六方面的第一种可能的实现方式，在第六方面的第二种可能的实现方式中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0052] 第七方面，本发明实施例提供一种会话管理设备，该会话管理设备包括处理器、存储器和收发器，其中：该存储器用于存储数据和程序；该处理器调用该存储器中的程序用于执行如下操作：

[0053] 通过该收发器接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求，该源网络为该UE当前驻留的网络；根据该路径切换请求获取目标安全策略，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输的密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；获取基于第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关，或者将该目标安全策略和预先获取的该第一共享密钥发送给该目标网关，以使该目标网关基于该第一共享密钥和该目标安全策略生成的该第二共享密钥，该第一共享密钥为该参考共享密钥或该基础密钥，该目标网关为该目标网络的用户面网关；通过该收发器将该第二共享密钥发送给该UE或者将该目标安全策略发送给该UE，以使该UE根据该第一共享密钥和该目标安全策略生成该第二共享密钥，该第二共享密钥用于在该UE与该目标网关之间端到端地保护数据的安全传输。

[0054] 通过执行上述操作，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0055] 结合第七方面，在第七方面的第一种可能的实现方式中，该处理器根据该路径切换请求获取目标安全策略，具体为：通过该收发器向安全策略控制器发送安全策略请求消息，该安全策略控制用于管理与该源网络和/或该目标网络中的设备相关的安全策略；通过该收发器接收该安全策略控制器发送的目标安全策略。

[0056] 结合第七方面，在第七方面的第二种可能的实现方式中，该会话管理设备包括源会话管理设备和目标会话管理设备；该源会话管理设备用于管理该源网络中的各个用户设备的会话，该目标会话管理设备用于管理该目标网络中的各个用户设备的会话；该源会话管理设备包括第一处理器和第一收发器，该目标会话管理设备包括第二处理器和第二收发器，其中：该处理器通过该收发器接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求，具体为：该第一处理器通过该第一收发器接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求；该处理器根据该路径切换请求获取目标安全策略，包括：该第一处理器获取初始安全策略并将该初始安全策略发送给该目标会话管理设备；根据该初始安全策略获取目标安全策略；该处理器获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关，包括：该第二处理器获取

基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关;该处理器通过该收发器将该目标安全策略发送给该UE,包括:第二处理器通过该第二收发器将该目标安全策略发送给该UE。

[0057] 结合第七方面的第二种可能的实现方式,在第七方面的第三种可能的实现方式中,该第一处理器通过该第一收发器接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求之后,该第二处理器获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关之前,该第一处理器还用于:通过该第一收发器向源密钥管理设备发送密钥请求消息,该源密钥管理设备用于管理接入到该源网络中的各个用户设备的用于端到端地保护数据安全传输的共享密钥;通过该第一收发器接收该源密钥管理设备根据该密钥请求消息发送的第一共享密钥,并将该第一共享密钥发送给该目标会话管理设备。

[0058] 结合第七方面,或者第七方面的第一种可能的实现方式,或者第七方面的第二种可能的实现方式,或者第七方面的第三种可能的实现方式,在第七方面的第四种可能的实现方式中,该处理器获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥,具体为:向目标密钥管理设备发送该目标安全策略,该目标密钥管理设备用于管理接入到该目标网络的各个用户设备的用于端到端地保护数据安全传输的共享密钥;接收该目标密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成的第二共享密钥。

[0059] 结合第七方面,或者第七方面的第一种可能的实现方式,或者第七方面的第二种可能的实现方式,或者第七方面的第三种可能的实现方式,在第七方面的第五种可能的实现方式中,该处理器获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥,具体为:根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥。

[0060] 结合第七方面,或者第七方面的第一种可能的实现方式,或者第七方面的第二种可能的实现方式,或者第七方面的第三种可能的实现方式,或者第七方面的第四种可能的实现方式,或者第七方面的第五种可能的实现方式,在第七方面的第六种可能的实现方式中,该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0061] 结合第七方面,或者第七方面的第一种可能的实现方式,或者第七方面的第二种可能的实现方式,或者第七方面的第三种可能的实现方式,或者第七方面的第四种可能的实现方式,或者第七方面的第六种可能的实现方式,在第七方面的第七种可能的实现方式中,该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的,该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项;该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0062] 第八方面,本发明实施例提供一种密钥管理设备,其特征在于,该密钥管理设备包括处理器、存储器和收发器,其中:该存储器用于存储数据和程序;该处理器调用该存储器中的程序用于执行如下操作:

[0063] 通过该收发器接收会话管理设备在接收到路径切换请求后发送的目标安全策略,该路径切换请求用于请求将用户设备UE从源网络切换到目标网络,该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略,该初始安全策略定

义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输的密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；根据该目标安全策略和预先获取的第一共享密钥生成第二共享密钥，该第一共享密钥为该参考共享密钥或该基础密钥；通过该收发器将该第二共享密钥发送给该会话管理设备，以使该会话管理设备将该第二共享密钥发送给目标网关，该目标网关为该目标网络的用户面网关，该第二共享密钥用于该UE与该目标网关之间端到端地保护数据的安全传输。

[0064] 通过执行上述操作，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0065] 结合第八方面，在第八方面的第一种可能的实现方式中，该处理器根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥之前，还用于：通过该收发器接收该会话管理设备在接收到路径切换请求后发送的第一共享密钥，该会话管理设备中预存了该第一共享密钥或者该会话管理设备预先向该源网络中的管理密钥的设备获取了该第一共享密钥。

[0066] 结合第八方面，在第八方面的第二种可能的实现方式中，该处理器根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥之前，还用于：通过该收发器向该源网络中的管理密钥的设备发送密钥查询请求，该密钥查询请求用于请求查询该UE在该源网络中用于端到端地保护数据安全传输的共享密钥；通过该收发器接收该管理密钥的设备发送的该第一共享密钥。

[0067] 结合第八方面，在第八方面的第三种可能的实现方式中，该密钥管理设备用于管理该源网络中和该目标网络中的各个用户设备的密钥，该密钥管理设备中存储了该第一共享密钥。

[0068] 结合第八方面，或者第八方面的第一种可能的实现方式，或者第八方面的第二种可能的实现方式，或者第八方面的第三种可能的实现方式，在第八方面的第四种可能的实现方式中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0069] 结合第八方面，或者第八方面的第一种可能的实现方式，或者第八方面的第二种可能的实现方式，或者第八方面的第三种可能的实现方式，或者第八方面的第四种可能的实现方式，在第八方面的第五种可能的实现方式中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0070] 第九方面，本发明实施例提供一种用户设备，该用户设备包括处理器、存储器和收发器，其中：该存储器用于存储数据和程序；该处理器调用该存储器中的程序用于执行如下操作：

[0071] 通过该收发器向目标网络发送会话重建请求，该会话重建请求用于触发向该目标

网络中的会话管理设备重建会话。通过该收发器接收该会话管理设备在接收到路径切换请求后发送的目标安全策略，该路径切换请求用于请求将用户设备UE从源网络切换到目标网络，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；根据该目标安全策略和自身的第一共享密钥生成第二共享密钥；该第二共享密钥用于该UE与目标网关之间端到端地保护数据的安全传输，该目标网关为该目标网络的用户面网关，该第一共享密钥为该参考共享密钥或该基础密钥。

[0072] 通过执行上述操作，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0073] 结合第九方面，在第九方面的第一种可能的实现方式中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0074] 结合第九方面，或者第九方面的第一种可能的实现方式，在第九方面的第二种可能的实现方式中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0075] 第十方面，本发明实施例提供一种通信系统，该通信系统包括会话管理设备、密钥管理设备和用户设备，其中：该会话管理设备为第四方面的任意可能实现方式中的会话管理设备，或者第七方面任意可能实现方式中的会话管理设备；该密钥管理设备为第五方面的任意可能实现方式中的密钥管理设备，或者第八方面任意可能实现方式中的密钥管理设备；该用户设备为第六方面的任意可能实现方式中的用户设备，或者第九方面任意可能实现方式中的用户设备。

[0076] 通过实施本发明实施例，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

附图说明

[0077] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍。

[0078] 图1是现有技术中的一种网络切换方法的流程示意图；

[0079] 图2A是本发明实施例提供的一种网络切换保护系统的结构示意图；

[0080] 图2B是本发明实施例提供的一种网络切换保护方法的流程示意图；

[0081] 图3A是本发明实施例提供的又一种网络切换保护方法的流程示意图；

[0082] 图3B是本发明实施例提供的又一种网络切换保护方法的流程示意图；

[0083] 图3C是本发明实施例提供的又一种网络切换保护方法的流程示意图；

[0084] 图3D是本发明实施例提供的又一种网络切换保护方法的流程示意图；

[0085] 图3E是本发明实施例提供的又一种网络切换保护方法的流程示意图；

[0086] 图3F是本发明实施例提供的又一种网络切换保护方法的流程示意图；

[0087] 图3G是本发明实施例提供的又一种网络切换保护方法的流程示意图；

[0088] 图3H是本发明实施例提供的又一种网络切换保护方法的流程示意图；

[0089] 图4是本发明实施例提供的一种会话管理设备的结构示意图；

[0090] 图5是本发明实施例提供的一种密钥管理设备的结构示意图；

[0091] 图6是本发明实施例提供的用户设备的结构示意图；

[0092] 图7是本发明实施例提供的又一种会话管理设备的结构示意图；

[0093] 图8是本发明实施例提供的又一种密钥管理设备的结构示意图；

[0094] 图9是本发明实施例提供的又一种用户设备的结构示意图；

[0095] 图10是本发明实施例提供的一种通信系统的结构示意图。

具体实施方式

[0096] 下面将结合附图对本发明实施例中的技术方案进行清楚、详细地描述，首先介绍本发明实施例可能涉及到的相关术语和网元。

[0097] 本发明涉及用户设备从一个网络切换到另一个网络，该用户设备切换前的网络可以称为“源网络”，切换后的网络可以称为“目标网络”。

[0098] 用户设备(英文:User Equipment，简称:UE)：该UE可以为手机、智能手表等智能终端，还可以为服务器、网关、基站、控制器等通信设备，还可以为传感器、电表、水表等物联网(英文:Internet of thing，简称:IoT)设备，还可以为其他能够接入到蜂窝网的设备。

[0099] 移动性管理(英文:Mobility Management，简称:MM)网元:后续可以直接称执行该移动性管理网元的功能的物理实体为移动性管理设备或者MM。

[0100] 会话管理网元(英文:Session Management，简称:SM)：该会话管理网元用于执行会话、切片、流flow或者承载bearer的建立和管理，后续可以称执行该会话管理网元的功能的物理实体为会话管理设备或者SM。为了便于区分，如果该源网络和该目标网络各自有自己的会话管理设备，则可称该源网络中的会话管理设备为源会话管理设备，称该目标网络中的会话管理设备为目标会话管理设备。

[0101] 密钥管理中心(英文:Key Management System，简称:KMS)，负责密钥的生成、管理和协商，支持合法监听。KMS可以作为一个独立的逻辑功能实体单独部署，也可以集合在MM、SM等设备中。后续可以称执行该密钥管理中心的功能的物理实体为密钥管理设备。通常情况下，该KMS为网络中的认证单元(英文:Control Plane-Authentication Unit，简称:CP-AU)，后续可以称执行该认证单元的功能的物理实体为密钥管理设备或者CP-AU。为了便于区分，还可以称该源网络中的密钥管理设备为源密钥管理设备，可以称该目标网络中的密钥管理设备为目标密钥管理设备。

[0102] 安全策略控制器(英文:Security Policy Function，简称:PCF)：安全策略控制器用于管理网络中的安全策略，源网络和目标网络中可以各自具有自身的安全策略控制器也可以具有同一个安全策略控制器。

[0103] 用户面网关(英文:User Plane-Gateway,UP-GW):用户面网关用于连接运营商网络和数据网络(英文:Data Network,DN),UE通过该用户面网关接入到网络;本发明实施例中可以称该UE接入到源网络时用到的网关为源网关(可表示为“源UP-GW”或者“源GW”),称该UE接入到目标网络时用到的网关为目标网关(可表示为“目标UP-GW”或者“目标GW”)。

[0104] 请参见图2A,图2A是本发明实施例提供的一种网络切换保护系统20的结构示意图,该系统20包括用户设备UE 201、会话管理设备SM202、源网关GW203和目标网关GW 204。该系统20还可以包括其他网元,例如,接入网(英文:Access Network,简称:AN)设备、安全策略控制器、密钥管理设备等;需要说明的是,此处的会话管理设备202未明确是源会话管理设备还是目标设备,因此存在如下两种情况:一、该系统20中包括源会话管理设备和目标会话管理设备这两个设备,由于该源会话管理设备和该目标会话管理设备按照功能作用来区分均属于会话管理设备,因此通过会话管理设备202来统一描述。情况二、该源会话管理设备和该目标会话管理设备为同一个设备,该同一设备描述为会话管理设备202。可以理解的是,本发明实施例中的密钥管理设备KMS、CP-AU等设备在描述的时候也可能存在与该会话管理设备20类似的两种情况。

[0105] 请参见图2B,图2B是本发明实施例提供的一种网络切换保护方法,该方法可以基于图2A所示的系统架构来实现,该方法包括但不限于如下步骤。

[0106] 步骤S201:会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求。

[0107] 具体地,当UE从原来驻留的源网络切换到目标网络时,该UE与该源网络中的移动性管理MM设备、该目标网络中的移动性管理MM设备、相关接入网AN之间会进行交互,完成网络切换的准备工作。

[0108] 可选的,向该会话管理设备发送该路径切换请求的设备除MM外还可以为UE、目标UP-GW、提供业务的业务服务器(APP Server)、业务服务控制器(APP server controller)等设备,向该会话管理设备发送的消息还可以称为路径更新请求、会话重建请求、或者其他与UE发生路径切换相关的请求。

[0109] 该路径切换请求(也可以称为UE位置变换请求)可以由该目标网络中的移动性管理MM设备发送给会话管理设备,该路径切换请求中可以包含该UE的身份标识UEID、该目标网络中的接入网AN设备的身份标识ANID等信息。该UEID为在一定范围内区分该UE与其他设备的信息,例如:该UE的媒体访问控制(英文:Media Access Control,简称:MAC)地址、网络协议(英文:Internet Protocol,简称:IP)地址、手机号码、国际移动设备标识(英文:International Mobile Equipment Identity,简称:IMEI)、国际移动用户识别码(英文:International Mobile Subscriber Identity,简称:IMSI)、IP多媒体私有标识(英文:IP Multimedia Private Identity,简称:IMPI)、临时移动用户标识符(英文:Temporary Mobile Subscriber Identity,简称:TMSI)、IP多媒体公共标识(英文:IP Multimedia Public Identity,简称:IMPU)、全球唯一临时UE标识(英文:Globally Unique Temporary UE Identity,简称:GUTI)等;该ANID为在一定范围内区分该目标网络中的AN设备与其他设备的信息,例如,该AN设备的MAC地址、IP地址等信息。

[0110] 步骤S202:该会话管理设备根据该路径切换请求获取目标安全策略。

[0111] 具体地,UE接入到网络中均需要有共享密钥来端到端地保护数据安全传输,该端

到端具体指该UE到该UE所驻留的网络中的用户面网关UP-GW,UE处于不同的网络中时由于会话的变换导致需要的用来保护数据的安全传输的共享密钥基本上是不同的,本发明实施例中称该UE在源网络中用来保护数据安全传输的共享密钥为第一共享密钥。该UE与该源网络进行双向认证生成的共享密钥可以称为基础密钥,基于该基础密钥进一步生成的端到端的会话保护密钥可以称为参考共享密钥,该第一共享密钥为该基础密钥或者该参考共享密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥。

[0112] 该参考共享密钥的生成需要参照初始安全策略来进行。如果该UE要切换到目标网络,那么该UE同样需要在该目标网络中用来端到端地保护数据安全传输的共享密钥,为了方便描述可以称之为第二共享密钥,该第二共享密钥同样需要参照一种安全策略来生成(不排除该第二共享密钥就为该第一共享密钥),该安全策略可以为该初始安全策略也可以为通过预先设定的某个算法对该初始安全策略进行处理的得到的新的安全策略,为了方便描述可以称之为目标安全策略。

[0113] 该初始安全策略和该目标安全策略均属于安全策略,安全策略包含密钥算法、密钥长度、密钥更新周期等信息,例如,常用的密钥算法有null、Snow 3G、ZUC、AES等,常用密钥长度为64bit、128bit、256bit等,常用的密钥更新时间有6小时、12小时、1天、2天等。在本发明实施例中,每个网元都可能具有自身的安全需求,该安全需求表征了该网元可以接受的密钥算法有哪些、可以接受的密钥长度有哪些,可以接受的密钥更新周期是哪些等等,根据相关网元的安全需求得到的能够满足该相关网元中各个网元所要求的密钥算法、密钥长度、密钥更新周期的方案为本发明实施例所描述的安全策略,该相关网元(例如,密钥管理网元、移动性管理网元等)具体指与该UE在网络中传输数据所涉及到的至少一个网元。当该UE从源网络切换到目标网络时,该UE接入网络所需要的用户面网关也会由源UP-GW变为目标UP-GW,因此最好能够新生成一份安全策略来涵盖该目标UP-GW的安全需求,当涉及其他网元时还可能涵盖其他网元的安全需求。

[0114] 本发明实施例中,基于预设规则对该初始安全策略处理得到的安全策略过程通常为,对该初始安全策略进行处理使得该处理后得到的安全策略能够满足新的相关网元的安全需求。该初始安全策略可能预先存储在该会话管理设备中也可能预先存储在其他设备(如,目标UP-GW、安全部策略控制器等)中,当该原始会话管理设备存储在其他设备中时,该会话管理设备可以向该其他设备发送请求该初始安全策略的请求消息,该请求消息可以包含该UE的身份标识UEID,以便该其他设备根据该请求消息中的UEID查找该UE(该UE与该第一共享密钥存也在对应关系)对应的初始安全策略。例如,上述网络切换系统中还包括安全策略控制器(Security Policy Function),该安全策略控制器存储了一些设备对应的安全策略。该会话管理设备可以向该安全策略控制器发送请求消息来请求该UE对应的初始安全策略。

[0115] 当该目标安全策略为通过预先设定的规则对该初始安全策略进行处理得到时,该会话管理设备获取目标安全策略的方式有很多,在一种可选的方案中,该会话管理设备根据预设规则对该初始安全策略进行处理得到该目标安全策略;在又一种可选的方案中,该会话管理设备将该初始安全策略发送给其他设备(例如,安全策略控制器(Security Policy Function)),由其他设备基于预设规则对该初始安全策略进行处理得到该目标安全策略,然后接收该其他设备发送的该目标安全策略。

[0116] 步骤S203:该会话管理设备获取基于该第一共享密钥和该目标安全策略生成的第共享密钥并将该第二共享密钥发送给目标网关,或者将该目标安全策略和预先获取的该第一共享密钥发送给该目标网关,以使该目标网关基于该第一共享密钥和该目标安全策略生成的该第二共享密钥,该目标网关为该目标网络的网关。

[0117] 具体地,本发明实施例中的第二共享密钥用于该UE在该目标网络中保护数据的安全传输,因此该UE与该目标网络中的网关(即目标网关)之间需要共享该第二共享密钥。该目标网关可以自己生成该第二共享密钥也可以接收该会话管理设备发送的第二共享密钥。该第二共享密钥的生成需要参考上述第一共享密钥和目标安全策略。当该第二共享密钥由该目标网关自己生成时,该目标网关用到的第一共享密钥和目标安全策略可以由该会话管理设备发送给该目标网关。当该目标网关的第二共享密钥来自该会话管理设备发送时,该会话管理设备中的第二共享密钥可能由该会话管理设备自己生成也可能由该目标网络中的密钥管理设备(可称为"目标密钥管理设备"以方便描述)生成后发送给该会话管理设备,该目标密钥管理设备用于管理接入到该目标网络中的各个用户设备的用于端到端地保护数据安全传输的共享密钥,可以为目标网络中的CP-AU。

[0118] 当该第二共享密钥由该会话管理设备生成时,该会话管理设备可以预先向源网络中的密钥管理设备发送请求来请求该UE的第一共享密钥,该源网络中的密钥管理设备(即该源网络中的管理密钥的设备)可以称为源密钥管理设备,也可能该会话管理设备自身存储了该第一共享密钥。该源密钥管理设备用于管理接入到该源网络中的各个用户设备的用于端到端地保护数据安全传输的共享密钥,可以为源网络中的CP-AU。

[0119] 当该第二共享密钥由该目标密钥管理设备生成再发送给该会话管理设备时,该目标密钥管理设备用到的目标安全策略可以由该会话管理设备发送,用到的第一共享密钥可能由该会话管理设备发送给该目标密钥管理设备,也可能由上述源密钥管理设备发送给该目标密钥管理设备。

[0120] 需要说明的是,本发明实施例中的源密钥管理设备和目标密钥管理设备可以为同一个设备,即该源网络和该目标网络共用同一个密钥管理设备。在这种情况下,如果上述第二共享密钥由该目标密钥管理设备来生成,那么,该源密钥管理设备可以不将第一共享密钥发送给该会话管理设备来转发给该目标密钥管理设备。

[0121] 步骤S204:该会话管理设备将该目标安全策略发送给该UE。

[0122] 步骤S205:该UE接收该目标安全策略并根据第一共享密钥和该目标安全策略生成该第二共享密钥;也可能步骤S204中已发送第二共享密钥,在这种情况下,步骤S205中不需要再生成第二共享密钥。

[0123] 具体地,由于该第一共享密钥用于该UE在源网络中保护数据的安全传输,因此该UE中已经存在了该第一共享密钥,该UE接收到该目标安全策略后即可基于该第一共享密钥和目标安全策略生成该第二共享密钥。举例来说,该目标共享密钥K_sup2=KDF(K_up,New E2E Policy Set,(UE ID,加密标识,切片标识,网络标识,业务参数,time1,nonce1,序列号的至少一项)),其中,K_up为第一共享密钥,New E2E Policy Set为目标安全策略,该式子表明生成该第二共享密钥K_sup2需要考虑第一共享密钥K_up、目标安全策略New E2E Policy Set,除此之外还要考虑UEID、切片标识、网络标识、业务参数、time1、nonce1和序列号中至少一项。另外,加密标识可以为一个字符串,用于标识此推衍的结果为加密密钥。

Nonce1为随机参数，可以由密钥管理设备发送给UE，使用随机数nonce1计算的目的在于，提高密钥的安全性和随机性。也可能密钥推衍中包含两个nonce的至少一项，其中一个nonce由密钥管理设备KMS或其他设备发送至UE，另一个nonce来自UE自己生成。最后，该UE和该目标网关均具备了该第二共享密钥，因此该UE可以将该第二共享密钥作为该UE与该目标网关之间端到端地保护数据安全传输的共享密钥。执行完上述流程后，该源网关和该目标网关进行数据反传，保证该UE上的业务的连续性。通常情况下，该UE生成第二共享密钥除了要用到该目标安全策略和第一共享密钥外，还可能会用到其他参数，例如，新鲜参数nonce、密钥算法标识、会话标识等，那么这些参数均可以由该会话管理设备或者相关网元发送给该UE。

[0124] 上述方案中的会话管理设备可以为一个设备也可以为一类设备，当为一类设备时该会话管理设备包括源会话管理设备和目标会话管理设备，该源会话管理设备用于管理该源网络中的各个用户设备的会话，该目标会话管理设备用于管理该目标网络中的各个用户设备的会话；上述各个步骤的描述可以细化如下：

[0125] 该会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求具体为：该源会话管理设备接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求。该会话管理设备根据该路径切换请求获取目标安全策略具体为：该源会话管理设备获取初始安全策略并将该初始安全策略发送给该目标会话管理设备；该目标会话管理设备根据该初始安全策略获取目标安全策略。该会话管理设备获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关具体为：该目标会话管理设备获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关。该会话管理设备将该目标安全策略发送给该UE具体为：该目标会话管理设备将该目标安全策略发送给该UE。执行完上述流程后，该源会话管理设备可以进行用户面安全上下文重配，删除掉该UE在源网络中的相关信息。

[0126] 可选的，该会话管理设备获取初始安全策略并将该初始安全策略发送给该目标会话管理设备具体为：向源密钥管理设备发送密钥请求消息，该源密钥管理设备用于管理接入到该源网络中的各个用户设备的用于保护数据安全传输的共享密钥；接收该源密钥管理设备根据该密钥请求消息发送的第一共享密钥，并将该初始安全策略发送给该目标会话管理设备。

[0127] 需要说明的是，可以基于该第一共享密钥、目标安全策略、加密算法标识等信息生成加密密钥，也可以基于该第一共享密钥、目标安全策略、完整性保护算法标识等信息生成完整性保护密钥，该加密密钥和该完整性保护密钥均属于该第二共享密钥。

[0128] 也可能基于该第二共享密钥进一步计算后得到加密和完保密钥。例如，加密密钥K_SID1_enc＝KDF(K_sup2,(安全策略，加密算法标识，UE ID，会话标识中至少一项))，即生成该加密密钥需要考虑该第二共享密钥K_sup2，除此之外还可以考虑安全策略、加密算法标识、UEID、会话标识等信息，该加密算法标识指示了生成该K_SID1_enc所需要用到的加密算法。完保密钥K_SID1_int＝KDF(K_sup2,(安全策略，完整性保护算法标识，UE ID，会话标识中至少一项))，即生成该完保密钥需要考虑该第二共享密钥K_sup2，除此之外还可以考虑完整性保护算法标识、UEID、会话标识等信息，该完整性保护算法标识指示了生成该K_SID1_enc所需要用到的完整性保护算法。切片标识，承载(bearer)ID，服务质量(英文：Quality of Service，简称：QoS)和流(flow)ID等

[0129] 以上使用到的参数承载(bearer)标识,流(flow)标识、切片标识、会话标识(session ID)都可能与上述目标安全需求一起携带在相同的消息中。另外加密算法的算法标识和完整性保护算法的算法标识可以为目标安全策略的内容。

[0130] 为了更好地理解本发明实施例的方案,下面结合图3A～3H所示的具体场景来展开描述。

[0131] 请参见图3A,图3A是本发明实施例提供的又一种网络切换保护方法的流程示意图;上述图2A所示的系统20包括用户设备UE、源会话管理设备SM、目标会话管理设备SM、源移动性管理设备MM、目标移动性管理设备MM、源CP-AU、目标CP-AU、源UP-GW、目标UP-GW和安全策略控制器,图3A所示的流程需要基于该系统20来实现,该流程如下:

[0132] 步骤S3101:目标MM向源SM发送路径切换请求,该路径切换请求用于请求将该UE从源网络切换到目标网络;该路径切换请求包含该UE的身份标识UEID、目标网络的地址等信息。

[0133] 步骤S3102:该源SM接收该路径切换请求并响应该路径切换请求,响应的方式包括向该安全策略控制器发送包含上述UEID的策略查询请求,该策略查询请求用于请求该安全策略控制器根据该UEID查询该UE对应的安全策略并将查询到的安全策略反馈给该源SM,然后执行后续步骤,该UE对应的安全策略为初始安全策略。当然,该源SM自身可能存储了该UE对应的初始安全策略,这种情况下该就可以直接从自身获取该初始安全策略而不是向该安全策略控制器获取。可选的,该源SM可以判断是否要执行SM的更新,若是才执行后续步骤。

[0134] 步骤S3103:该源SM接收该安全策略控制器发送的初始安全策略。

[0135] 步骤S3104:该源SM向源CP-AU发送密钥查询请求,该密钥查询请求用于请求查询该UE在该源网络中用于保护数据安全传输的共享密钥。当然,该源SM也有可能存储了该UE在该源网络中用于端到端地保护数据安全传输的共享密钥。

[0136] 步骤S3105:该源CP-AU接收该密钥查询请求并响应该密钥查询请求查询该UE在该源网络中用于保护数据安全传输的共享密钥,即第一共享密钥。然后,该源CP-AU将该第一共享密钥发送给该源SM,也可能该源CP-AU将该第一共享密钥发送给该目标CP-AU,再由该目标CP-AU转发给该源SM。

[0137] 步骤S3106:该源SM向该目标SM发送该初始安全策略和该第一共享密钥。可选的,该第一共享密钥还可以由该源CP-AU发送给该目标CP-AU,在由该目标CP-AU向该目标SM转发。

[0138] 步骤S3107:该目标SM接收该初始安全策略和该第一共享密钥;然后,向该安全策略控制器发送输入信息,该输入信息至少包括该初始安全策略。

[0139] 步骤S3108:该安全策略控制器接收该输入信息,并通过预设规则对该输入信息进行处理得到新的安全策略或者与其他设备进行协商得到该新的安全策略,该新的安全策略为目标安全策略。然后,该安全策略控制器将该目标安全策略发送给该目标SM。

[0140] 步骤S3109:该目标SM接收该目标安全策略,并向该目标CP-AU发送该目标安全策略。可以理解为,目标SM和目标CP-AU都可能需要存储该目标安全策略。

[0141] 步骤S3110:该目标CP-AU接收该目标安全策略,并根据该目标安全策略和该第一共享密钥生成第二共享密钥,需要说明的是,该目标CP-AU用到的第一共享密钥可以是该目标SM发送给的,也可以是上述源CP-AU发送的。

[0142] 步骤S3111:该目标CP-AU将该第二共享密钥发送给该目标SM。

[0143] 步骤S3112:该目标SM接收该第二共享密钥并将该第二共享密钥发送给目标GW。

[0144] 步骤S3113:该目标SM将该目标安全策略发送给该UE。当然,该目标SM也可以直接将该第二共享密钥发送给UE,这样UE就不用执行后续基于目标安全策略和第一共享密钥生成第二共享密钥的操作了。

[0145] 步骤S3114:该UE接收该目标安全策略,然后结合该目标安全策略和自身已有的第一共享密钥生成第二共享密钥。

[0146] 至此,UE与目标UP-GW之间均存在了该第二共享密钥,因此UE可以通过该第二共享密钥或者基于该第二共享密钥衍生的共享密钥来端到端地保护数据在目标网络中安全传输。需要说明的是,UE和该目标UP-GW均具有该第二共享密钥后,上述系统中的各个设备之间可能还存在一些交互,例如,目标SM通知源SM进行用户面安全上下文重配置,清除该UE之前驻留源网络时的相关信息;再如,目标UP-GW与源GW之间进行数据反传,保证该UE的业务从该源网络到该目标网络保持连续性。可选的,在开始执行上面会话建立的相关步骤前,可能由UE发起会话(session)重建的请求该触发该相关步骤。另外,各个步骤可以按照以上描述的先后顺序来执行,也可以不完全按照描述的顺序来执行,只要逻辑不存在问题即可。

[0147] 需要说明的是,该目标安全策略还可以为该初始安全策略,在这种情况下就不存在上述根据初始安全策略生成目标安全策略的步骤了。可选的,当该初始安全策略就是该目标安全策略时,生成该第二共享密钥所需要的目标安全策略和第一共享密钥在源网络中都有,因此步骤S3106中该源SM不需要向该目标SM发送第一共享密钥和初始安全策略,而是将该初始安全策略发送给源CP-AU以使该源CP-AU基于该第一共享密钥和该初始安全策略生成该第二共享密钥;之后源CP-AU将该第二共享密钥发送给该源SM由该源SM转发给该目标SM并最终转发给该目标UP-GW。也即是说,该可能性与步骤S3101～S3114该方案的区别在于,该目标UP-GW用到的第二共享密钥由源CP-AU生成而不是由该目标CP-AU生成。

[0148] 请参见图3B,图3B是本发明实施例提供的又一种网络切换保护方法的流程示意图;上述图2A所示的系统20包括用户设备UE、源会话管理设备SM、目标会话管理设备SM、源移动性管理设备MM、目标移动性管理设备MM、CP-AU、源UP-GW、目标UP-GW和安全策略控制器,该目标网络和该源网络中的CP-AU为同一个CP-AU,图3B所示的流程需要基于该系统20来实现,该流程如下:

[0149] 步骤S3201:目标MM向源SM发送路径切换请求,该路径切换请求用于请求将该UE从源网络切换到目标网络;该路径切换请求包含该UE的身份标识UEID、目标网络的地址等信息。

[0150] 步骤S3202:该源SM接收该路径切换请求并响应该路径切换请求,响应的方式包括向该安全策略控制器发送包含上述UEID的策略查询请求,该策略查询请求用于请求该安全策略控制器根据该UEID查询该UE对应的安全策略并将查询到的安全策略反馈给该源SM,然后执行后续步骤,该UE对应的安全策略为初始安全策略。当然,该源SM自身可能存储了该UE对应的初始安全策略,这种情况下该就可以直接从自身获取该初始安全策略而不是向该安全策略控制器获取。可选的,该源SM可以判断是否进行SM的更新,若是,若是则执行后续步骤。

[0151] 步骤S3203:该源SM接收该安全策略控制器发送的初始安全策略。

[0152] 步骤S3204：该源SM向CP-AU发送密钥查询请求，该密钥查询请求用于请求查询该UE在该源网络中用于保护数据安全传输的共享密钥。当然，该源SM也有可能存储了该UE在该源网络中用于端到端地保护数据安全传输的共享密钥。

[0153] 步骤S3205：该CP-AU接收该密钥查询请求并响应该密钥查询请求查询该UE在该源网络中用于保护数据安全传输的共享密钥，即第一共享密钥。

[0154] 步骤S3206：该源SM向该目标SM发送该初始安全策略。

[0155] 步骤S3207：该目标SM接收该初始安全策略；然后，向该安全策略控制器发送输入信息，该输入信息至少包括该初始安全策略。

[0156] 步骤S3208：该安全策略控制器接收该输入信息，并通过预设规则对该输入信息进行处理得到新的安全策略，该新的安全策略为目标安全策略。然后，该安全策略控制器将该目标安全策略发送给该目标SM。

[0157] 步骤S3209：该目标SM接收该目标安全策略，并向该CP-AU发送该目标安全策略。可以理解为，该目标SM和CP-AU都可能需要存储该目标安全策略。

[0158] 步骤S3210：该CP-AU接收该目标安全策略，并根据该目标安全策略和该第一共享密钥生成第二共享密钥。

[0159] 步骤S3211：该CP-AU将该第二共享密钥发送给该目标SM。

[0160] 步骤S3212：该目标SM接收该第二共享密钥并将该第二共享密钥发送给目标UP-GW。

[0161] 步骤S3213：该目标SM将该目标安全策略发送给该UE。当然，该目标SM也可以直接将该第二共享密钥发送给UE，这样UE就不用执行后续基于目标安全策略和第一共享密钥生成第二共享密钥的操作了。

[0162] 步骤S3214：该UE接收该目标安全策略，然后结合该目标安全策略和自身已有的第一共享密钥生成第二共享密钥。

[0163] 至此，UE与目标UP-GW之间均存在了该第二共享密钥，因此UE可以通过该第二共享密钥或者基于该第二共享密钥衍生的共享密钥来端到端地保护数据在目标网络中安全传输。需要说明的是，UE和该目标UP-GW均具有该第二共享密钥后，上述系统中的各个设备之间可能还存在一些交互，例如，目标SM通知源SM进行用户面安全上下文重配置，清除该UE之前驻留源网络时的相关信息；再如，目标UP-GW与源GW之间进行数据反传，保证该UE的业务从该源网络到该目标网络保持连续性。可选的，在开始执行上面会话建立的相关步骤前，可能由UE发起会话(session)重建的请求该触发该相关步骤。另外，各个步骤可以按照以上描述的先后顺序来执行，也可以不完全按照描述的顺序来执行，只要逻辑不存在问题即可。

[0164] 需要说明的是，该目标安全策略还可以为该初始安全策略，在这种情况下就不存在上述根据初始安全策略生成目标安全策略的步骤了。可选的，当该初始安全策略就是该目标安全策略时，生成该第二共享密钥所需要的目标安全策略和第一共享密钥在源网络中都有，因此步骤S3206中该源SM不需要向该目标SM发送初始安全策略，而是将该初始安全策略发送给CP-AU以使该CP-AU基于该第一共享密钥和该初始安全策略生成该第二共享密钥；之后由该CP-AU将该第二共享密钥发送给该目标SM并由该目标SM转发给该目标UP-GW。也即是说，该可能性与步骤S3201～S3214该方案的区别在于，该目标UP-GW用到的第二共享密钥由源SM触发该CP-AU生成，而不是由该目标SM触发该CP-AU生成。

[0165] 请参见图3C，图3C是本发明实施例提供的又一种网络切换保护方法的流程示意图；上述图2A所示的系统20包括用户设备UE、源会话管理设备SM、目标会话管理设备SM、源移动性管理设备MM、目标移动性管理MM设备、源CP-AU、目标CP-AU、源UP-GW、目标UP-GW和安全策略控制器，图3C所示的流程需要基于该系统20来实现，该流程如下：

[0166] 步骤S3301：目标MM向源SM发送路径切换请求，该路径切换请求用于请求将该UE从源网络切换到目标网络；该路径切换请求包含该UE的身份标识UEID、目标网络的地址等信息。

[0167] 步骤S3302：该源SM接收该路径切换请求并响应该路径切换请求，响应的方式包括向该安全策略控制器发送包含上述UEID的策略查询请求，该策略查询请求用于请求该安全策略控制器根据该UEID查询该UE对应的安全策略并将查询到的安全策略反馈给该源SM，然后执行后续步骤，该UE对应的安全策略为初始安全策略。当然，该源SM自身可能存储了该UE对应的初始安全策略，这种情况下该就可以直接从自身获取该初始安全策略而不是向该安全策略控制器获取。可选的，该源SM可以判断是否要执行SM的更新，若是才执行后续步骤。

[0168] 步骤S3303：该源SM接收该安全策略控制器发送的初始安全策略。

[0169] 步骤S3304：该源SM向源CP-AU发送密钥查询请求，该密钥查询请求用于请求查询该UE在该源网络中用于保护数据安全传输的共享密钥。当然，该源SM也有可能存储了该UE在该源网络中用于端到端地保护数据安全传输的共享密钥。

[0170] 步骤S3305：该源CP-AU接收该密钥查询请求并响应该密钥查询请求查询该UE在该源网络中用于保护数据安全传输的共享密钥，即第一共享密钥。然后，该CP-AU将该第一共享密钥发送给该源SM，也可能该源CP-AU将该第一共享密钥发送给该目标CP-AU，再由该目标CP-AU转发给该源SM。

[0171] 步骤S3306：该源SM向该目标SM发送该初始安全策略和该第一共享密钥。可选的，该第一共享密钥还可以由该源CP-AU发送给该目标CP-AU，再由该目标CP-AU向该目标SM转发。可选的，该源SM发送的该第一共享密钥可能为该源SM基于随机数、序列号等信息衍生过的。

[0172] 步骤S3307：该目标SM接收该初始安全策略和该第一共享密钥；然后，向该安全策略控制器发送输入信息，该输入信息至少包括该初始安全策略。

[0173] 步骤S3308：该安全策略控制器接收该输入信息，并通过预设规则对该输入信息进行处理得到新的安全策略，该新的安全策略为目标安全策略。然后，该安全策略控制器将该目标安全策略发送给该目标SM。

[0174] 步骤S3309：该目标SM接收该目标安全策略，并根据该目标安全策略和该第一共享密钥生成第二共享密钥。

[0175] 步骤S3310：该目标SM将该第二共享密钥发送给目标UP-GW。

[0176] 步骤S3311：该目标SM将该目标安全策略发送给该UE。当然，该目标SM也可以直接将该第二共享密钥发送给UE，这样UE就不用执行后续基于目标安全策略和第一共享密钥生成第二共享密钥的操作了。

[0177] 步骤S3312：该UE接收该目标安全策略，然后结合该目标安全策略和自身已有的第一共享密钥生成第二共享密钥。

[0178] 至此，UE与目标UP-GW之间均存在了该第二共享密钥，因此UE可以通过该第二共享

密钥或者基于该第二共享密钥衍生的共享密钥来端到端地保护数据在目标网络中安全传输。需要说明的是,UE和该目标UP-GW均具有该第二共享密钥后,上述系统中的各个设备之间可能还存在一些交互,例如,目标SM通知源SM进行用户面安全上下文重配置,清除该UE之前驻留源网络时的相关信息;再如,目标UP-GW与源GW之间进行数据反传,保证该UE的业务从该源网络到该目标网络保持连续性。可选的,在开始执行上面会话建立的相关步骤前,可能由UE发起会话(session)重建的请求该触发该相关步骤。另外,各个步骤可以按照以上描述的先后顺序来执行,也可以不完全按照描述的顺序来执行,只要逻辑不存在问题即可。

[0179] 需要说明的是,该目标安全策略还可以为该初始安全策略,在这种情况下就不存在上述根据初始安全策略生成目标安全策略的步骤了。可选的,当该初始安全策略就是该目标安全策略时,生成该第二共享密钥所需要的目标安全策略和第一共享密钥在源网络中都有,因此步骤S3306中该源SM不需要向该目标SM发送初始安全策略和第一共享密钥,而是直接基于该第一共享密钥和该初始安全策略生成该第二共享密钥;之后将第二共享密钥发送给该目标UP-GW。也即是说,该可能性与步骤S3301～S3314该方案的区别在于,该目标UP-GW用到的第二共享密钥由源SM生成,而不是由该目标SM生成。

[0180] 请参见图3D,图3D是本发明实施例提供的又一种网络切换保护方法的流程示意图;上述图2A所示的系统20包括用户设备UE、源会话管理设备SM、目标会话管理设备SM、源移动性管理设备MM、目标移动性管理设备MM、源CP-AU、目标CP-AU、源UP-GW、目标UP-GW和安全策略控制器,图3D所示的流程需要基于该系统20来实现,该流程如下:

[0181] 步骤S3401:目标MM向源SM发送路径切换请求,该路径切换请求用于请求将该UE从源网络切换到目标网络;该路径切换请求包含该UE的身份标识UEID、目标网络的地址等信息。

[0182] 步骤S3402:该源SM接收该路径切换请求并响应该路径切换请求,响应的方式包括向该安全策略控制器发送包含上述UEID的策略查询请求,该策略查询请求用于请求该安全策略控制器根据该UEID查询该UE对应的安全策略并将查询到的安全策略反馈给该源SM,然后执行后续步骤,该UE对应的安全策略为初始安全策略。当然,该源SM自身可能存储了该UE对应的初始安全策略,这种情况下该就可以直接从自身获取该初始安全策略而不是向该安全策略控制器获取。可选的,该源SM可以判断是否要执行SM的更新,若是才执行后续步骤。

[0183] 步骤S3403:该源SM接收该安全策略控制器发送的初始安全策略。

[0184] 步骤S3404:该源SM向源CP-AU发送密钥查询请求,该密钥查询请求用于请求查询该UE在该源网络中用于保护数据安全传输的共享密钥。当然,该源SM也有可能存储了该UE在该源网络中用于端到端地保护数据安全传输的共享密钥。

[0185] 步骤S3405:该源CP-AU接收该密钥查询请求并响应该密钥查询请求查询该UE在该源网络中用于保护数据安全传输的共享密钥,即第一共享密钥。然后,该CP-AU将该第一共享密钥发送给该源SM,也可能该源CP-AU将该第一共享密钥发送给该目标CP-AU,再由该目标CP-AU转发给该源SM。

[0186] 步骤S3406:该源SM向该目标SM发送该初始安全策略和该第一共享密钥。可选的,该第一共享密钥还可以由该源CP-AU发送给该目标CP-AU,在由该目标CP-AU向该目标SM转发。需要说明的是,该源SM发送的该第一共享密钥可能为该源SM基于随机数、序列号等信息衍生过的。

[0187] 步骤S3407:该目标SM接收该初始安全策略和该第一共享密钥;然后,向该安全策略控制器发送输入信息,该输入信息至少包括该初始安全策略。

[0188] 步骤S3408:该安全策略控制器接收该输入信息,并通过预设规则对该输入信息进行处理得到新的安全策略,该新的安全策略为目标安全策略。然后,该安全策略控制器将该目标安全策略发送给该目标SM。

[0189] 步骤S3409:该目标SM接收该目标安全策略,并将该目标安全策略和该第一共享密钥发送给目标UP-GW。

[0190] 步骤S3410:该目标UP-GW接收该目标安全策略和第一共享密钥,并根据该目标安全策略和该第一共享密钥生成第二共享密钥,该目标UP-GW生成该第二共享密钥的时机此处不作限定,在一种可选的方案中,该目标UP-GW接收到该目标安全策略和第一共享密钥后马上生成该第二共享密钥,以便即将建立的会话(session)可以用上该第二共享密钥;在又一种可选的方案中,该目标UP-GW接收到该目标安全策略和第一共享密钥后先不生成该第二共享密钥,即将建立的会话(session)依旧沿用该UE在源网络中的第一共享密钥,即在极特别情况下,目标session的密钥无须更新,但依然需要更新并储存目标安全策略以便于在下一次UE发生切换时使用;在该第二共享密钥生成之后建的session可以使用该第二共享密钥。

[0191] 步骤S3411:该目标SM将该目标安全策略发送给该UE。当然,该SM也可以直接将该第二共享密钥发送给UE,这样UE就不用执行后续基于目标安全策略和第一共享密钥生成第二共享密钥的操作了。可选的,如果无须更新目标Session的端到端保护密钥,则目标SM发送的将是第一共享密钥。

[0192] 步骤S3412:该UE接收该目标安全策略,然后结合该目标安全策略和自身已有的第一共享密钥生成第二共享密钥。可以理解的是,如果步骤S3410中没有即时生成第二共享密钥供即将建立的会话session,那么UE也可以先不生成该第二共享密钥,而是在后续再有新的会话建立时才生成该第二共享密钥。

[0193] 至此,UE与目标UP-GW之间均存在了该第二共享密钥,因此UE可以通过该第二共享密钥或者基于该第二共享密钥衍生的共享密钥来保护数据在目标网络中安全传输。需要说明的是,UE和该目标UP-GW均具有该第二共享密钥后,上述系统中的各个设备之间可能还存在一些交互,例如,目标SM通知源SM进行用户面安全上下文重配置,清除该UE之前驻留源网络时的相关信息;再如,目标UP-GW与源WG之间进行数据反传,保证该UE的业务从该源网络到该目标网络保持连续性。可选的,在开始执行上面会话建立的相关步骤前,可能由UE发起会话(session)重建的请求该触发该相关步骤。另外,各个步骤可以按照以上描述的先后顺序来执行,也可以不完全按照描述的顺序来执行,只要逻辑不存在问题即可。

[0194] 需要说明的是,该目标安全策略还可以为该初始安全策略,在这种情况下就不存在上述根据初始安全策略生成目标安全策略的步骤了。可选的,当该初始安全策略就是该目标安全策略时,生成该第二共享密钥所需要的目标安全策略和第一共享密钥在源网络中都有,因此步骤S3306中该源SM不需要向该目标SM发送初始安全策略和第一共享密钥,而是将该第一共享密钥和该初始安全策略发送给该源UP-GW由该源UP-GW根据该第一共享密钥和初始安全策略生成该第二共享密钥,之后将第二共享密钥发送给该目标UP-GW。也即是说,该可能性与步骤S3301～S3312该方案的区别在于,该目标UP-GW用到的第二共享密钥由

源UP-GW生成，而不是由该目标UP-GW生成。可选的，可以由该目标SM向该源UP-GW发送包含UEID的消息或者由该目标UP-GW转发由该SM发送的包含UEID的消息给该源UP-GW，从而触发该UP-GW根据该UEID获取该UE对应的第一共享密钥和初始安全策略并基于该第一共享密钥和初始安全策略生成该第二共享密钥。

[0195] 请参见图3E，图3E是本发明实施例提供的又一种网络切换保护方法的流程示意图；上述图2A所示的系统20包括用户设备UE、会话管理设备SM、源移动性管理设备MM、目标移动性管理设备MM、源CP-AU、目标CP-AU、源UP-GW、目标UP-GW和安全策略控制器，图3E所示的流程需要基于该系统20来实现，该流程如下：

[0196] 步骤S3501：目标MM向SM发送路径切换请求，该路径切换请求用于请求将该UE从源网络切换到目标网络；该路径切换请求包含该UE的身份标识UEID、目标网络的地址等信息。

[0197] 步骤S3502：该SM接收该路径切换请求并响应该路径切换请求，响应的方式包括向该安全策略控制器发送包含上述UEID的策略查询请求，该策略查询请求用于请求该安全策略控制器根据该UEID查询该UE对应的安全策略并将查询到的安全策略反馈给该SM，然后执行后续步骤，该UE对应的安全策略为初始安全策略。当然，该SM自身可能存储了该UE对应的初始安全策略，这种情况下该就可以直接从自身获取该初始安全策略而不是向该安全策略控制器获取。

[0198] 步骤S3503：该SM获取该目标安全策略，该目标安全策略为该初始安全策略或者根据该初始安全策略生成的安全策略；当该SM自身存储了该初始安全策略时该SM可以根据该初始安全策略以及其他信息来生成该目标安全策略，当该SM自身未存储该初始安全策略时，可以由该安全策略控制器根据该初始安全策略以及其他信息生成了该目标安全策略后将该目标安全策略发送给该SM，或者发送该初始安全策略给该SM由该SM自己来生成目标安全策略。

[0199] 步骤S3504：该SM向源CP-AU发送密钥查询请求，该密钥查询请求用于请求查询该UE在该源网络中用于保护数据安全传输的共享密钥。当然，该源SM也有可能存储了该UE在该源网络中用于端到端地保护数据安全传输的共享密钥。

[0200] 步骤S3505：该源CP-AU接收该密钥查询请求并响应该密钥查询请求查询该UE在该源网络中用于保护数据安全传输的共享密钥，即第一共享密钥。然后，该源CP-AU将该第一共享密钥发送给该SM，也可能该源CP-AU将该第一共享密钥发送给该目标CP-AU，再由该目标CP-AU转发给该SM。

[0201] 步骤S3506：该SM向该目标CP-AU发送该目标安全策略和第一共享密钥。可以理解为，SM和目标CP-AU都可能需要存储该目标安全策略。

[0202] 步骤S3507：该目标CP-AU接收该目标安全策略和第一共享密钥，并根据该目标安全策略和该第一共享密钥生成第二共享密钥，需要说明的是，该目标CP-AU用到的第一共享密钥可以是该SM发送给的，也可以是上述源CP-AU发送的。

[0203] 步骤S3508：该目标CP-AU将该第二共享密钥发送给该SM。

[0204] 步骤S3509：该SM接收该第二共享密钥并将该第二共享密钥发送给目标GW。

[0205] 步骤S3510：该SM将该目标安全策略发送给该UE。当然，该SM也可以直接将该第二共享密钥发送给UE，这样UE就不用执行后续基于目标安全策略和第一共享密钥生成第二共享密钥的操作了。

[0206] 步骤S3511:该UE接收该目标安全策略,然后结合该目标安全策略和自身已有的第一共享密钥生成第二共享密钥。

[0207] 至此,UE与目标UP-GW之间均存在了该第二共享密钥,因此UE可以通过该第二共享密钥或者基于该第二共享密钥衍生的共享密钥来端到端地保护数据在目标网络中安全传输。需要说明的是,UE和该目标UP-GW均具有该第二共享密钥后,上述系统中的各个设备之间可能还存在一些交互,例如,目标UP-GW与源GW之间进行数据反传,保证该UE的业务从该源网络到该目标网络保持连续性。可选的,在开始执行上面会话建立的相关步骤前,可能由UE发起会话(session)重建的请求该触发该相关步骤。另外,各个步骤可以按照以上描述的先后顺序来执行,也可以不完全按照描述的顺序来执行,只要逻辑不存在问题即可。

[0208] 需要说明的是,该目标安全策略还可以为该初始安全策略,在这种情况下就不存在上述根据初始安全策略生成目标安全策略的步骤了。可选的,当该初始安全策略就是该目标安全策略时,生成该第二共享密钥所需要的目标安全策略和第一共享密钥在源网络中都有,因此步骤S3506中该SM不需要将该目标安全策略发送给目标CP-AU,而是将该目标安全策略发送给源CP-AU以使该源CP-AU基于该第一共享密钥和该初始安全策略生成该第二共享密钥;之后源CP-AU将该第二共享密钥发送给该SM由该SM转发给该目标UP-GW。也即是说,该可能性与步骤S3501～S3511该方案的区别在于,该目标UP-GW用到的第二共享密钥由源CP-AU生成而不是由该目标CP-AU生成。

[0209] 请参见图3F,图3F是本发明实施例提供的又一种网络切换保护方法的流程示意图;上述图2A所示的系统20包括用户设备UE、会话管理设备SM、源移动性管理设备MM、目标移动性管理设备MM、CP-AU、源UP-GW、目标UP-GW和安全策略控制器,该目标网络和该源网络中的CP-AU为同一个CP-AU,图3F所示的流程需要基于该系统20来实现,该流程如下:

[0210] 步骤S3601:目标MM向SM发送路径切换请求,该路径切换请求用于请求将该UE从源网络切换到目标网络;该路径切换请求包含该UE的身份标识UEID、目标网络的地址等信息。

[0211] 步骤S3602:该SM接收该路径切换请求并响应该路径切换请求,响应的方式包括向该安全策略控制器发送包含上述UEID的策略查询请求,该策略查询请求用于请求该安全策略控制器根据该UEID查询该UE对应的安全策略并将查询到的安全策略反馈给该SM,然后执行后续步骤,该UE对应的安全策略为初始安全策略。当然,该SM自身可能存储了该UE对应的初始安全策略,这种情况下该就可以直接从自身获取该初始安全策略而不是向该安全策略控制器获取。

[0212] 步骤S3603:该SM获取该目标安全策略,该目标安全策略为该初始安全策略或者根据该初始安全策略生成的安全策略;当该SM自身存储了该初始安全策略时该SM可以根据该初始安全策略以及其他信息来生成该目标安全策略,当该SM自身未存储该初始安全策略时,可以由该安全策略控制器根据该初始安全策略以及其他信息生成了该目标安全策略后将该目标安全策略发送给该SM,或者发送该初始安全策略给该SM由该SM自己来生成目标安全策略。

[0213] 步骤S3604:该SM向CP-AU发送密钥查询请求,该密钥查询请求用于请求查询该UE在该源网络中用于保护数据安全传输的共享密钥。当然,该SM也有可能存储了该UE在该源网络中用于端到端地保护数据安全传输的共享密钥。

[0214] 步骤S3605:该CP-AU接收该密钥查询请求并响应该密钥查询请求查询该UE在该源

网络中用于保护数据安全传输的共享密钥,即第一共享密钥。

[0215] 步骤S3606:该SM向该CP-AU发送该目标安全策略。可以理解为,该SM和CP-AU都可能需要存储该目标安全策略。

[0216] 步骤S3607:该CP-AU接收该目标安全策略,并根据该目标安全策略和该第一共享密钥生成第二共享密钥。

[0217] 步骤S3608:该CP-AU将该第二共享密钥发送给该SM。

[0218] 步骤S3609:该SM接收该第二共享密钥并将该第二共享密钥发送给目标UP-GW。

[0219] 步骤S3610:该SM将该目标安全策略发送给该UE。当然,该SM也可以直接将该第二共享密钥发送给UE,这样UE就不用执行后续基于目标安全策略和第一共享密钥生成第二共享密钥的操作了。

[0220] 步骤S3611:该UE接收该目标安全策略,然后结合该目标安全策略和自身已有的第一共享密钥生成第二共享密钥。

[0221] 至此,UE与目标UP-GW之间均存在了该第二共享密钥,因此UE可以通过该第二共享密钥或者基于该第二共享密钥衍生的共享密钥来端到端地保护数据在目标网络中安全传输。需要说明的是,UE和该目标UP-GW均具有该第二共享密钥后,上述系统中的各个设备之间可能还存在一些交互,例如,目标UP-GW与源GW之间进行数据反传,保证该UE的业务从该源网络到该目标网络保持连续性。可选的,在开始执行上面会话建立的相关步骤前,可能由UE发起会话(session)重建的请求该触发该相关步骤。另外,各个步骤可以按照以上描述的先后顺序来执行,也可以不完全按照描述的顺序来执行,只要逻辑不存在问题即可。

[0222] 需要说明的是,该目标安全策略还可以为该初始安全策略,在这种情况下就不存在上述根据初始安全策略生成目标安全策略的步骤了。

[0223] 请参见图3G,图3G是本发明实施例提供的又一种网络切换保护方法的流程示意图;上述图2A所示的系统20包括用户设备UE、会话管理设备SM、源移动性管理设备MM、目标移动性管理MM设备、源CP-AU、目标CP-AU、源UP-GW、目标UP-GW和安全策略控制器,图3G所示的流程需要基于该系统20来实现,该流程如下:

[0224] 步骤S3701:目标MM向SM发送路径切换请求,该路径切换请求用于请求将该UE从源网络切换到目标网络;该路径切换请求包含该UE的身份标识UEID、目标网络的地址等信息。

[0225] 步骤S3702:该SM接收该路径切换请求并响应该路径切换请求,响应的方式包括向该安全策略控制器发送包含上述UEID的策略查询请求,该策略查询请求用于请求该安全策略控制器根据该UEID查询该UE对应的安全策略并将查询到的安全策略反馈给该SM,然后执行后续步骤,该UE对应的安全策略为初始安全策略。当然,该SM自身可能存储了该UE对应的初始安全策略,这种情况下该就可以直接从自身获取该初始安全策略而不是向该安全策略控制器获取。

[0226] 步骤S3703:该SM获取该目标安全策略,该目标安全策略为该初始安全策略或者根据该初始安全策略生成的安全策略;当该SM自身存储了该初始安全策略时该SM可以根据该初始安全策略以及其他信息来生成该目标安全策略,当该SM自身未存储该初始安全策略时,可以由该安全策略控制器根据该初始安全策略以及其他信息生成了该目标安全策略后将该目标安全策略发送给该SM,或者发送该初始安全策略给该SM由该SM自己来生成目标安全策略。

[0227] 步骤S3704:该SM向源CP-AU发送密钥查询请求,该密钥查询请求用于请求查询该UE在该源网络中用于保护数据安全传输的共享密钥。当然,该SM也有可能存储了该UE在该源网络中用于端到端地保护数据安全传输的共享密钥。

[0228] 步骤S3705:该源CP-AU接收该密钥查询请求并响应该密钥查询请求查询该UE在该源网络中用于保护数据安全传输的共享密钥,即第一共享密钥。然后,该源CP-AU将该第一共享密钥发送给该SM,也可能该源CP-AU将该第一共享密钥发送给该目标CP-AU,再由该目标CP-AU转发给该SM。

[0229] 步骤S3706:该SM根据该目标安全策略和该第一共享密钥生成第二共享密钥。

[0230] 步骤S3707:该SM将该第二共享密钥发送给目标UP-GW。

[0231] 步骤S3708:该SM将该目标安全策略发送给该UE。当然,该SM也可以直接将该第二共享密钥发送给UE,这样UE就不用执行后续基于目标安全策略和第一共享密钥生成第二共享密钥的操作了。

[0232] 步骤S3709:该UE接收该目标安全策略,然后结合该目标安全策略和自身已有的第一共享密钥生成第二共享密钥。

[0233] 至此,UE与目标UP-GW之间均存在了该第二共享密钥,因此UE可以通过该第二共享密钥或者基于该第二共享密钥衍生的共享密钥来端到端地保护数据在目标网络中安全传输。需要说明的是,UE和该目标UP-GW均具有该第二共享密钥后,上述系统中的各个设备之间可能还存在一些交互,例如,目标UP-GW与源WG之间进行数据反传,保证该UE的业务从该源网络到该目标网络保持连续性。可选的,在开始执行上面会话建立的相关步骤前,可能由UE发起会话(session)重建的请求该触发该相关步骤。另外,各个步骤可以按照以上描述的先后顺序来执行,也可以不完全按照描述的顺序来执行,只要逻辑不存在问题即可。

[0234] 需要说明的是,该目标安全策略还可以为该初始安全策略,在这种情况下就不存在上述根据初始安全策略生成目标安全策略的步骤了。

[0235] 请参见图3H,图3H是本发明实施例提供的又一种网络切换保护方法的流程示意图;上述图2A所示的系统20包括用户设备UE、会话管理设备SM、源移动性管理设备MM、目标移动性管理设备MM、源CP-AU、目标CP-AU、源UP-GW、目标UP-GW和安全策略控制器,图3H所示的流程需要基于该系统20来实现,该流程如下:

[0236] 步骤S3801:目标MM向SM发送路径切换请求,该路径切换请求用于请求将该UE从源网络切换到目标网络;该路径切换请求包含该UE的身份标识UEID、目标网络的地址等信息。

[0237] 步骤S3802:该SM接收该路径切换请求并响应该路径切换请求,响应的方式包括向该安全策略控制器发送包含上述UEID的策略查询请求,该策略查询请求用于请求该安全策略控制器根据该UEID查询该UE对应的安全策略并将查询到的安全策略反馈给该SM,然后执行后续步骤,该UE对应的安全策略为初始安全策略。当然,该SM自身可能存储了该UE对应的初始安全策略,这种情况下该就可以直接从自身获取该初始安全策略而不是向该安全策略控制器获取。

[0238] 步骤S3803:该SM获取该目标安全策略,该目标安全策略为该初始安全策略或者根据该初始安全策略生成的安全策略;当该SM自身存储了该初始安全策略时该SM可以根据该初始安全策略以及其他信息来生成该目标安全策略,当该SM自身未存储该初始安全策略时,可以由该安全策略控制器根据该初始安全策略以及其他信息生成了该目标安全策略后

将该目标安全策略发送给该SM,或者发送该初始安全策略给该SM由该SM自己来生成目标安全策略。

[0239] 步骤S3804:该SM向源CP-AU发送密钥查询请求,该密钥查询请求用于请求查询该UE在该源网络中用于保护数据安全传输的共享密钥。当然,该SM也有可能存储了该UE在该源网络中用于端到端地保护数据安全传输的共享密钥。

[0240] 步骤S3805:该源CP-AU接收该密钥查询请求并响应该密钥查询请求查询该UE在该源网络中用于保护数据安全传输的共享密钥,即第一共享密钥。然后,该CP-AU将该第一共享密钥发送给该SM,也可能该源CP-AU将该第一共享密钥发送给该目标CP-AU,再由该目标CP-AU转发给该SM。

[0241] 步骤S3806:该SM将该目标安全策略和该第一共享密钥发送给目标UP-GW。

[0242] 步骤S3807:该目标UP-GW接收该目标安全策略和第一共享密钥,并根据该目标安全策略和该第一共享密钥生成第二共享密钥,该目标UP-GW生成该第二共享密钥的时机此处不作限定,在一种可选的方案中,该目标UP-GW接收到该目标安全策略和第一共享密钥后马上生成该第二共享密钥,以便即将建立的会话(session)可以用上该第二共享密钥;在又一种可选的方案中,该目标UP-GW接收到该目标安全策略和第一共享密钥后先不生成该第二共享密钥,即将建立的会话(session)依旧沿用该UE在源网络中的第一共享密钥,即在极特别情况下,目标session的密钥无须更新,但依然需要更新并储存目标安全策略以便于在下一次UE发生切换时使用;在该第二共享密钥生成之后建的session可以使用该第二共享密钥。

[0243] 步骤S3808:该SM将该目标安全策略发送给该UE。当然,该SM也可以直接将该第二共享密钥发送给UE,这样UE就不用执行后续基于目标安全策略和第一共享密钥生成第二共享密钥的操作了。可选的,如果无须更新目标Session的端到端保护密钥,则SM发送的将是第一共享密钥。

[0244] 步骤S3809:该UE接收该目标安全策略,然后结合该目标安全策略和自身已有的第一共享密钥生成第二共享密钥。可以理解的是,如果步骤S3807中没有即时生成第二共享密钥供即将建立的会话session,那么UE也可以先不生成该第二共享密钥,而是在后续再有新的会话建立时才生成该第二共享密钥。

[0245] 至此,UE与目标UP-GW之间均存在了该第二共享密钥,因此UE可以通过该第二共享密钥或者基于该第二共享密钥衍生的共享密钥来保护数据在目标网络中安全传输。需要说明的是,UE和该目标UP-GW均具有该第二共享密钥后,上述系统中的各个设备之间可能还存在一些交互,例如,目标UP-GW与源WG之间进行数据反传,保证该UE的业务从该源网络到该目标网络保持连续性。可选的,在开始执行上面会话建立的相关步骤前,可能由UE发起会话(session)重建的请求该触发该相关步骤。另外,各个步骤可以按照以上描述的先后顺序来执行,也可以不完全按照描述的顺序来执行,只要逻辑不存在问题即可。

[0246] 需要说明的是,该目标安全策略还可以为该初始安全策略,在这种情况下就不存在上述根据初始安全策略生成目标安全策略的步骤了。可选的,当该初始安全策略就是该目标安全策略时,生成该第二共享密钥所需要的目标安全策略和第一共享密钥在源网络中都有,因此步骤S3806中该SM不需要将初始安全策略和第一共享密钥发送给目标UP-GW,而是将该第一共享密钥和该初始安全策略发送给该源UP-GW由该源UP-GW根据该第一共享密

钥和初始安全策略生成该第二共享密钥，之后将第二共享密钥发送给该目标UP-GW。也即是说，该可能性与步骤S3801～S3819该方案的区别在于，该目标UP-GW用到的第二共享密钥由源UP-GW生成，而不是由该目标UP-GW生成。可选的，可以由该SM向该源UP-GW发送包含UEID的消息或者由该目标UP-GW转发由该SM发送的包含UEID的消息给该源UP-GW，从而触发该UP-GW根据该UEID获取该UE对应的第一共享密钥和初始安全策略并基于该第一共享密钥和初始安全策略生成该第二共享密钥。

[0247] 在上述各个方法实施例中，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0248] 上述详细阐述了本发明实施例的方法，为了便于更好地实施本发明实施例的上述方案，相应地，下面提供了本发明实施例的装置。

[0249] 请参见图4，图4是本发明实施例提供的一种会话管理设备40的结构示意图，该会话管理设备40可以包括第一接收单元401、第一获取单元402、第二获取单元403和第一发送单元404，其中，各个单元的详细描述如下。

[0250] 第一接收单元401用于接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求，该源网络为该UE当前驻留的网络；

[0251] 第一获取单元402用于根据该路径切换请求获取目标安全策略，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输的密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；

[0252] 第二获取单元403用于获取基于第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关，或者将该目标安全策略和预先获取的该第一共享密钥发送给该目标网关，以使该目标网关基于该第一共享密钥和该目标安全策略生成的该第二共享密钥，该第一共享密钥为该参考共享密钥或该基础密钥，该目标网关为该目标网络的用户面网关；

[0253] 第一发送单元404用于将该第二共享密钥发送给该UE或者将该目标安全策略发送给该UE，以使该UE根据该第一共享密钥和该目标安全策略生成该第二共享密钥，该第二共享密钥用于在该UE与该目标网关之间端到端地保护数据的安全传输。

[0254] 通过运行上述单元，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0255] 在一种可选的方案中，该第一获取单元402具体用于向安全策略控制器发送安全策略请求消息，该安全策略控制用于管理与该源网络和/或该目标网络中的设备相关的安全策略；接收该安全策略控制器发送的目标安全策略。

[0256] 在又一种可选的方案中，该会话管理设备包括源会话管理设备和目标会话管理设备；该源会话管理设备用于管理该源网络中的各个用户设备的会话，该目标会话管理设备

用于管理该目标网络中的各个用户设备的会话;该源会话管理设备包括该第一接收单元401和该第一获取单元402,该目标会话管理设备包括该第二获取单元403和该第一发送单元403;

[0257] 该第一获取单元402具体用于获取初始安全策略并将该初始安全策略发送给该目标会话管理设备;该目标会话管理设备根据该初始安全策略获取目标安全策略;

[0258] 该第二获取单元403具体用于获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关。

[0259] 在又一种可选的方案中,该源会话管理设备还包括第二发送单元和第二接收单元:

[0260] 该第二发送单元用于在该接收单元接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求之后,该第二获取单元403获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关之前,向源密钥管理设备发送密钥请求消息,该源密钥管理设备用于管理接入到该源网络中的各个用户设备的用于端到端地保护数据安全传输的共享密钥;

[0261] 该第二接收单元,用于接收该源密钥管理设备根据该密钥请求消息发送的第一共享密钥,并将该第一共享密钥发送给该目标会话管理设备。

[0262] 在又一种可选的方案中,该第二获取单元403具体用于向目标密钥管理设备发送该目标安全策略,该目标密钥管理设备用于管理接入到该目标网络的各个用户设备的用于端到端地保护数据安全传输的共享密钥;接收该目标密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成的第二共享密钥。

[0263] 在又一种可选的方案中,该第二获取单元403具体用于根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥。

[0264] 在又一种可选的方案中,该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0265] 在又一种可选的方案中,该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的,该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项;该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0266] 需要说明的是,该会话管理设备40的具体实现还可以对应参照图2A、2B、3A～3H所示的方法实施例的相应描述。

[0267] 在图4所示的会话管理设备40中,该UE切换到目标网络时,通过源网络或者目标网络中的网元生成目标安全策略,然后基于该目标安全策略和第一共享密钥生成第二共享密钥,最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥,使得该UE在切换网络后依旧能够安全地传输数据。

[0268] 请参见图5,图5是本发明实施例提供的一种密钥管理设备50的结构示意图,该密钥管理设备50可以包括第一接收单元501、生成单元502和第一发送单元503,其中,各个单元的详细描述如下。

[0269] 第一接收单元501用于接收会话管理设备在接收到路径切换请求后发送的目标安

全策略，该路径切换请求用于请求将用户设备UE从源网络切换到目标网络，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输的密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；

[0270] 生成单元502用于根据该目标安全策略和预先获取的第一共享密钥生成第二共享密钥，该第一共享密钥为该参考共享密钥或该基础密钥；

[0271] 第一发送单元503用于将该第二共享密钥发送给该会话管理设备，以使该会话管理设备将该第二共享密钥发送给目标网关，该目标网关为该目标网络的用户面网关，该第二共享密钥用于该UE与该目标网关之间端到端地保护数据的安全传输。

[0272] 通过运行上述单元，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0273] 在一种可选的方案中，该密钥管理设备50还包括：

[0274] 第二接收单元，用于在该密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥之前，接收该会话管理设备在接收到路径切换请求后发送的第一共享密钥，该会话管理设备中预存了该第一共享密钥或者该会话管理设备预先向该源网络中的管理密钥的设备获取了该第一共享密钥。

[0275] 在又一种可选的方案中，上述密钥管理设备50还包括：

[0276] 第二发送单元，用于在该密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥之前，向该源网络中的管理密钥的设备发送密钥查询请求，该密钥查询请求用于请求查询该UE在该源网络中用于端到端地保护数据安全传输的共享密钥；

[0277] 第三接收单元，用于接收该管理密钥的设备发送的该第一共享密钥。

[0278] 在又一种可选的方案中，该密钥管理设备用于管理该源网络中和该目标网络中的各个用户设备的密钥，该密钥管理设备中存储了该第一共享密钥。

[0279] 在又一种可选的方案中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0280] 在又一种可选的方案中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0281] 需要说明的是，该密钥管理设备50的具体实现还可以对应参照图2A、2B、3A～3H所示的方法实施例的相应描述。

[0282] 在图5上述的密钥管理设备50中，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到

端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0283] 请参见图6，图6是本发明实施例提供的一种用户设备60的结构示意图，该用户设备60可以包括发送单元601、接收单元602和生成单元603，其中，各个单元的详细描述如下。

[0284] 发送单元601用于向目标网络发送会话重建请求，该会话重建请求用于触发向该目标网络中的会话管理设备重建会话；

[0285] 接收单元602用于接收该会话管理设备在接收到路径切换请求后发送的目标安全策略，该路径切换请求用于请求将用户设备UE从源网络切换到目标网络，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；

[0286] 生成单元603用于根据该目标安全策略和自身的第一共享密钥生成第二共享密钥；该第二共享密钥用于该UE与目标网关之间端到端地保护数据的安全传输，该目标网关为该目标网络的用户面网关，该第一共享密钥为该参考共享密钥或该基础密钥。

[0287] 通过运行上述单元，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0288] 在一种可选的方案中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0289] 在又一种可选的方案中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0290] 需要说明的是，该用户设备60的具体实现还可以对应参照图2A、2B、3A～3H所示的方法实施例的相应描述。

[0291] 在图6所述的用户设备6中，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0292] 请参见图7，图7是本发明实施例提供的一种会话管理设备70，该会话管理设备70包括处理器701、存储器702和收发器703，该处理器701、存储器702和收发器703通过总线相互连接。

[0293] 存储器702包括但不限于是随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或者快闪存储器)、或便携式只读存储器(CD-ROM)，该存储器702用于相关指令及数据。

[0294] 该收发器703可以包括一个接收器和一个发送器，例如，无线射频模块。

[0295] 处理器701可以是一个或多个中央处理器(英文:Central Processing Unit，简

称:CPU),在处理器701是一个CPU的情况下,该CPU可以是单核CPU,也可以是多核CPU。

[0296] 该会话管理设备70中的处理器701用于读取该存储器702中存储的程序代码,执行以下操作:

[0297] 通过该收发器703接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求,该源网络为该UE当前驻留的网络;

[0298] 根据该路径切换请求获取目标安全策略,该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略,该初始安全策略定义了生成参考共享密钥的方式,该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输的密钥,该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥;

[0299] 获取基于第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关,或者将该目标安全策略和预先获取的该第一共享密钥发送给该目标网关,以使该目标网关基于该第一共享密钥和该目标安全策略生成的该第二共享密钥,该第一共享密钥为该参考共享密钥或该基础密钥,该目标网关为该目标网络的用户面网关;

[0300] 通过该收发器703将该第二共享密钥发送给该UE或者将该目标安全策略发送给该UE,以使该UE根据该第一共享密钥和该目标安全策略生成该第二共享密钥,该第二共享密钥用于在该UE与该目标网关之间端到端地保护数据的安全传输。

[0301] 通过执行上述操作,该UE切换到目标网络时,通过源网络或者目标网络中的网元生成目标安全策略,然后基于该目标安全策略和第一共享密钥生成第二共享密钥,最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥,使得该UE在切换网络后依旧能够安全地传输数据。

[0302] 在一种可选的方案中,该处理器701根据该路径切换请求获取目标安全策略,具体为:

[0303] 通过该收发器703向安全策略控制器发送安全策略请求消息,该安全策略控制用于管理与该源网络和/或该目标网络中的设备相关的安全策略;

[0304] 通过该收发器703接收该安全策略控制器发送的目标安全策略。

[0305] 在又一种可选的方案中,该会话管理设备70包括源会话管理设备和目标会话管理设备;该源会话管理设备用于管理该源网络中的各个用户设备的会话,该目标会话管理设备用于管理该目标网络中的各个用户设备的会话;该源会话管理设备包括第一处理器和第一收发器,该目标会话管理设备包括第二处理器和第二收发器,其中:

[0306] 该处理器701通过该收发器703接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求,具体为:该第一处理器通过该第一收发器接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求;

[0307] 该处理器701根据该路径切换请求获取目标安全策略,包括:该第一处理器获取初始安全策略并将该初始安全策略发送给该目标会话管理设备;根据该初始安全策略获取目标安全策略;

[0308] 该处理器701获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关,包括:该第二处理器获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关;

[0309] 该处理器701通过该收发器703将该目标安全策略发送给该UE，包括：第二处理器通过该第二收发器将该目标安全策略发送给该UE。

[0310] 在又一种可选的方案中，该第一处理器701通过该第一收发器703接收用于请求将用户设备UE从源网络切换到目标网络的路径切换请求之后，该第二处理器701获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥并将该第二共享密钥发送给目标网关之前，该第一处理器701还用于：

[0311] 通过该第一收发器703向源密钥管理设备发送密钥请求消息，该源密钥管理设备用于管理接入到该源网络中的各个用户设备的用于端到端地保护数据安全传输的共享密钥；

[0312] 通过该第一收发器703接收该源密钥管理设备根据该密钥请求消息发送的第一共享密钥，并将该第一共享密钥发送给该目标会话管理设备。

[0313] 在又一种可选的方案中，该处理器701获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥，具体为：

[0314] 向目标密钥管理设备发送该目标安全策略，该目标密钥管理设备用于管理接入到该目标网络的各个用户设备的用于端到端地保护数据安全传输的共享密钥；

[0315] 接收该目标密钥管理设备根据该目标安全策略和预先获取的该第一共享密钥生成的第二共享密钥。

[0316] 在又一种可选的方案中，该处理器701获取基于该第一共享密钥和该目标安全策略生成的第二共享密钥，具体为：

[0317] 根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥。

[0318] 在又一种可选的方案中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0319] 在又一种可选的方案中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0320] 需要说明的是，该会话管理设备70的具体实现还可以对应参照图2A、2B、3A～3H所示的方法实施例的相应描述。

[0321] 在图7所述的会话管理设备70中，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0322] 请参见图8，图8是本发明实施例提供的一种密钥管理设备80，该密钥管理设备80包括处理器801、存储器802和收发器803，该处理器801、存储器802和收发器803通过总线相互连接。

[0323] 存储器802包括但不限于是随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或者快闪存储器)、或便携式只读存储器(CD-ROM)，该存储器802用于相关指令及数据。

[0324] 该收发器803可以包括一个接收器和一个发送器，例如，无线射频模块。

[0325] 处理器801可以是一个或多个中央处理器(英文:Central Processing Unit，简称:CPU)，在处理器801是一个CPU的情况下，该CPU可以是单核CPU，也可以是多核CPU。

[0326] 该密钥管理设备80中的处理器801用于读取该存储器802中存储的程序代码，执行以下操作：

[0327] 通过该收发器803接收会话管理设备在接收到路径切换请求后发送的目标安全策略，该路径切换请求用于请求将用户设备UE从源网络切换到目标网络，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输的密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；

[0328] 根据该目标安全策略和预先获取的第一共享密钥生成第二共享密钥，该第一共享密钥为该参考共享密钥或该基础密钥；

[0329] 通过该收发器803将该第二共享密钥发送给该会话管理设备，以使该会话管理设备将该第二共享密钥发送给目标网关，该目标网关为该目标网络的用户面网关，该第二共享密钥用于该UE与该目标网关之间端到端地保护数据的安全传输。

[0330] 通过执行上述操作，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0331] 在一种可选的方案中，该处理器801根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥之前，还用于：

[0332] 通过该收发器803接收该会话管理设备在接收到路径切换请求后发送的第一共享密钥，该会话管理设备中预存了该第一共享密钥或者该会话管理设备预先向该源网络中的管理密钥的设备获取了该第一共享密钥。

[0333] 在又一种可选的方案中，该处理器801根据该目标安全策略和预先获取的该第一共享密钥生成第二共享密钥之前，还用于：

[0334] 通过该收发器803向该源网络中的管理密钥的设备发送密钥查询请求，该密钥查询请求用于请求查询该UE在该源网络中用于端到端地保护数据安全传输的共享密钥；

[0335] 通过该收发器803接收该管理密钥的设备发送的该第一共享密钥。

[0336] 在又一种可选的方案中，该密钥管理设备用于管理该源网络中和该目标网络中的各个用户设备的密钥，该密钥管理设备中存储了该第一共享密钥。

[0337] 在又一种可选的方案中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0338] 在又一种可选的方案中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0339] 需要说明的是，该密钥管理设备80的具体实现还可以对应参照图2A、2B、3A～3H所示的方法实施例的相应描述。

[0340] 在图8所示的密钥管理设备80中，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0341] 请参见图9，图9是本发明实施例提供的一种用户设备90，该用户设备90包括处理器901、存储器902和收发器903，该处理器901、存储器902和收发器903通过总线相互连接。

[0342] 存储器902包括但不限于是随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或者快闪存储器)、或便携式只读存储器(CD-ROM)，该存储器902用于相关指令及数据。

[0343] 该收发器903可以包括一个接收器和一个发送器，例如，无线射频模块。

[0344] 处理器901可以是一个或多个中央处理器(英文:Central Processing Unit，简称:CPU)，在处理器901是一个CPU的情况下，该CPU可以是单核CPU，也可以是多核CPU。

[0345] 该用户设备90中的处理器901用于读取该存储器902中存储的程序代码，执行以下操作：

[0346] 通过该收发器903向目标网络发送会话重建请求，该会话重建请求用于触发向该目标网络中的会话管理设备重建会话；

[0347] 通过该收发器903接收该会话管理设备在接收到路径切换请求后发送的目标安全策略，该路径切换请求用于请求将用户设备UE从源网络切换到目标网络，该目标安全策略为初始安全策略或者为基于预设规则对该初始安全策略处理得到的安全策略，该初始安全策略定义了生成参考共享密钥的方式，该参考共享密钥为根据基础密钥生成的用于该UE在该源网络中端到端地保护数据安全传输密钥，该基础密钥为该UE与该源网络双向认证生成的密钥或者基于该UE与该源网络双向认证生成的密钥推衍的密钥；

[0348] 根据该目标安全策略和自身的第一共享密钥生成第二共享密钥；该第二共享密钥用于该UE与目标网关之间端到端地保护数据的安全传输，该目标网关为该目标网络的用户面网关，该第一共享密钥为该参考共享密钥或该基础密钥。

[0349] 通过执行上述操作，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0350] 在一种可选的方案中，该初始安全策略和该目标安全策略均定义了密钥算法、密钥长度和密钥更新周期中至少一项。

[0351] 在又一种可选的方案中，该目标安全策略为根据该用户设备的安全需求和/或该目标网关的安全需求得到的，该用户设备的安全需求表征了该用户设备可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项；该目标网关的安全需求表征了该目标网关可接受的密钥算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。

[0352] 需要说明的是，该用户设备90的具体实现还可以对应参照图2A、2B、3A～3H所示的

方法实施例的相应描述。

[0353] 在图9所述的用户设备90中，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0354] 请参见图10，图10是本发明实施例提供的一种通信系统100的结构示意图，该通信系统100包括会话管理设备1001、密钥管理设备1002和用户设备1003，其中：该会话管理设备1001为图4所示的会话管理设备40或者图7所述的会话管理设备70；密钥管理设备1002为图5所示的密钥管理设备50或者图8所述的密钥管理设备80；用户设备1003为图6所述的用户设备60或者图9所示的用户设备90。

[0355] 综上所述，通过实施本发明实施例，该UE切换到目标网络时，通过源网络或者目标网络中的网元生成目标安全策略，然后基于该目标安全策略和第一共享密钥生成第二共享密钥，最后该UE和该目标网络中的目标网关将该第二共享密钥作为UE与该目标网关之间端到端地保护数据安全传输的共享密钥，使得该UE在切换网络后依旧能够安全地传输数据。

[0356] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0357] 以上实施例仅揭露了本发明中较佳实施例，不能以此来限定本发明之权利范围，本领域普通技术人员可以理解实现上述实施例的全部或部分流程，并依本发明权利要求所作的等同变化，仍属于发明所涵盖的范围。

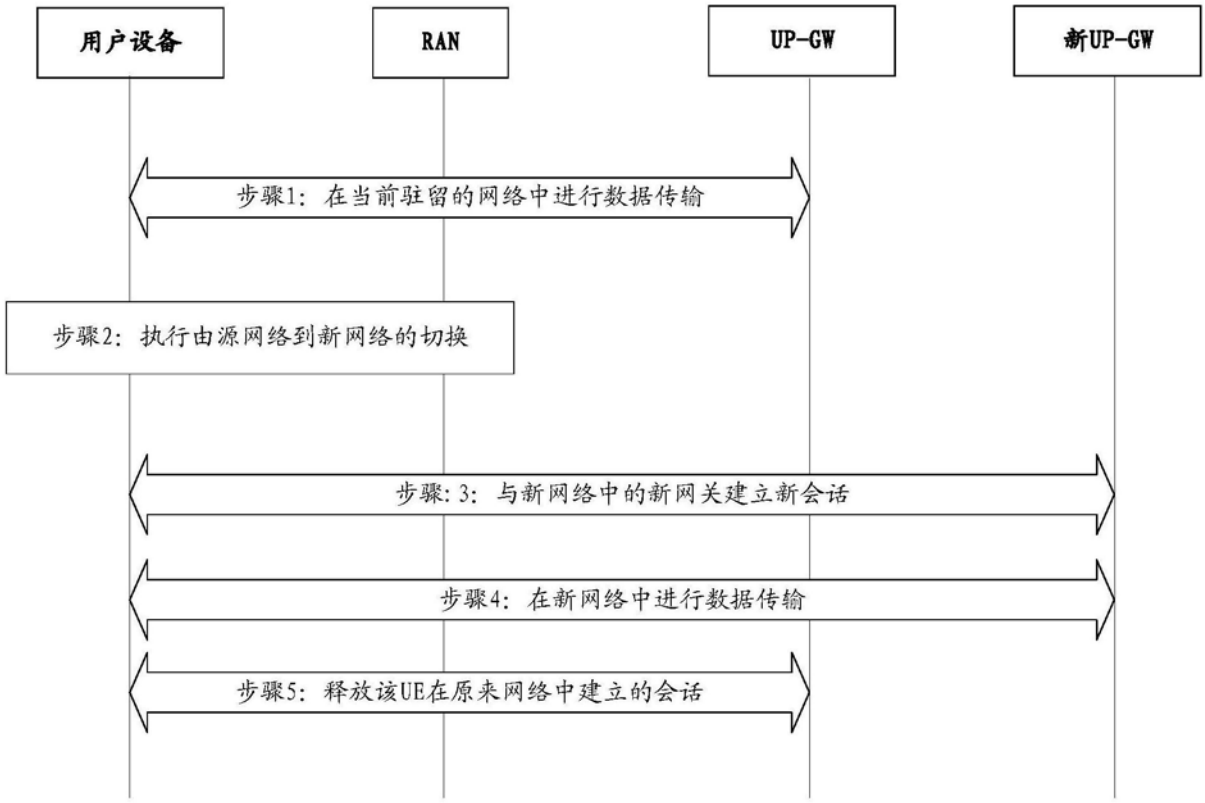

用户设备
RAN
UP-GW
新UP-GW
步骤1：在当前驻留的网络中进行数据传输
步骤2：执行由源网络到新网络的切换
步骤: 3：与新网络中的新网关建立新会话
步骤4：在新网络中进行数据传输
步骤5：释放该UE在原来网络中建立的会话

图1

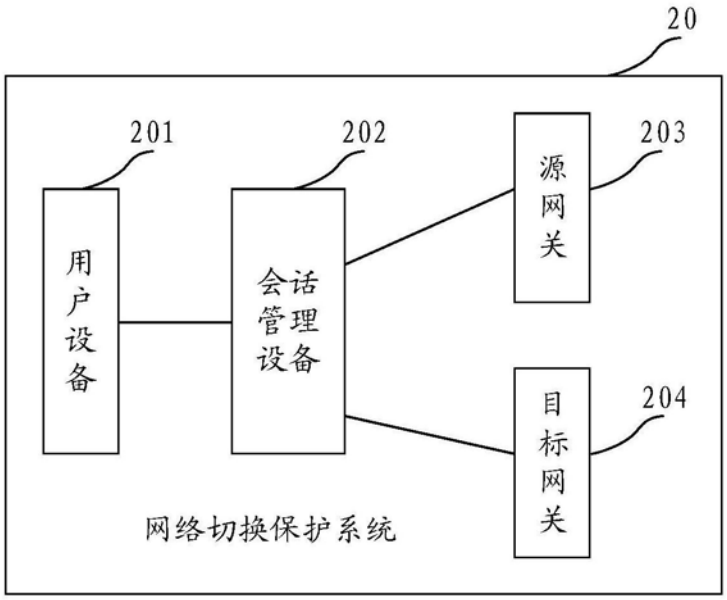

20
201
202
203
204
用户设备
会话管理设备
源网关
目标网关
网络切换保护系统

图2A

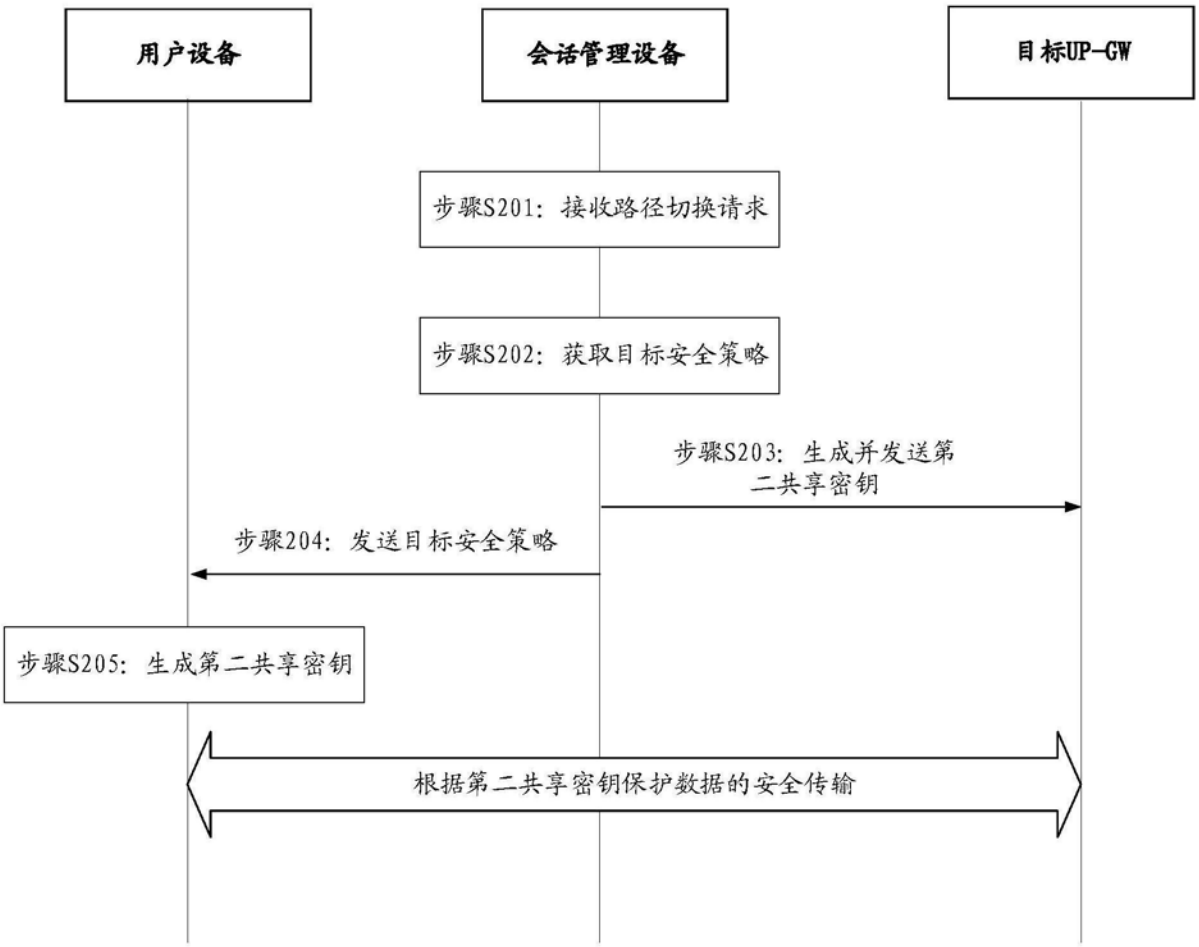

用户设备
会话管理设备
目标UP-GW
步骤S201：接收路径切换请求
步骤S202：获取目标安全策略
步骤S203：生成并发送第二共享密钥
步骤204：发送目标安全策略
步骤S205：生成第二共享密钥
根据第二共享密钥保护数据的安全传输

图2B

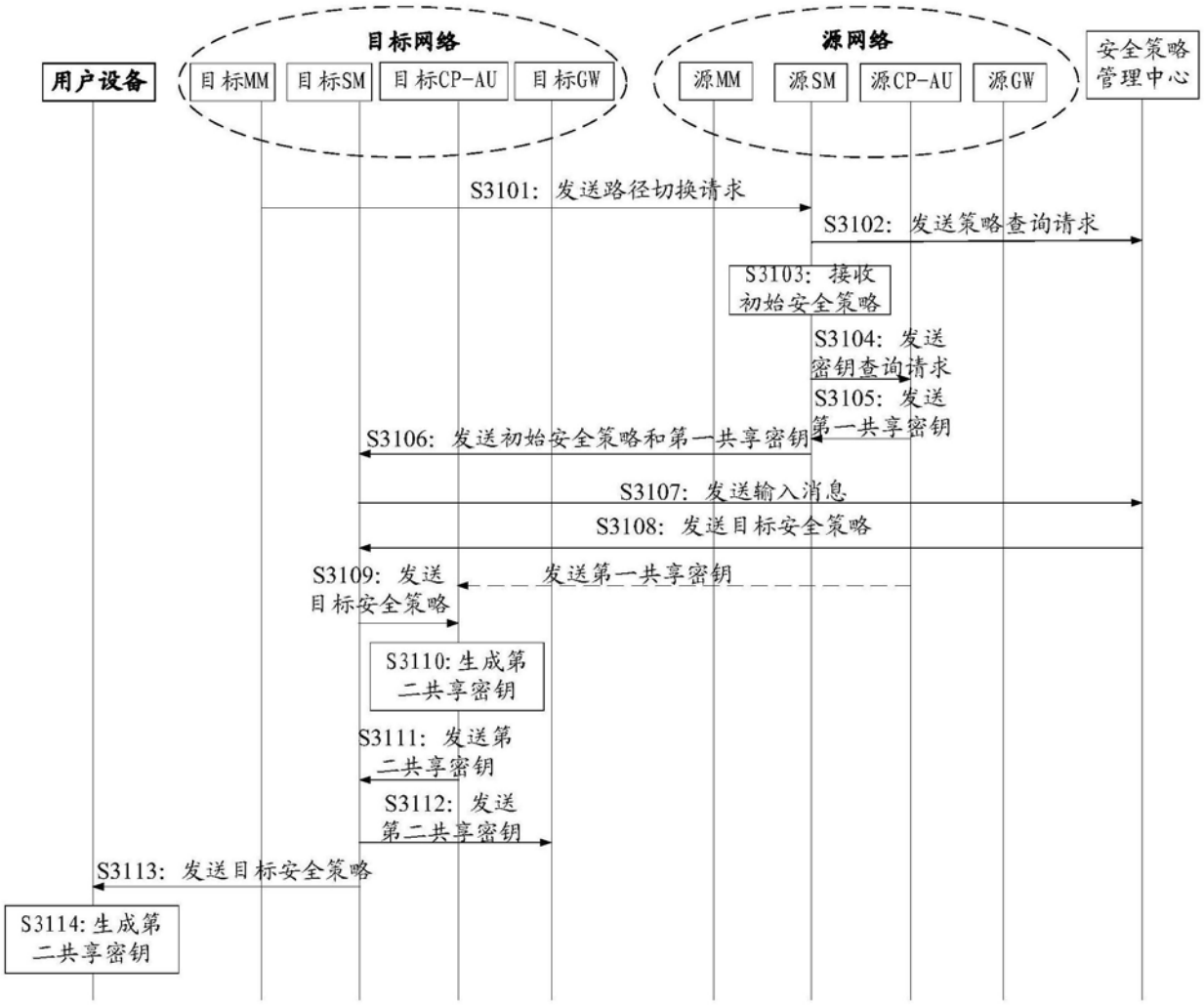

目标网络
源网络
用户设备
目标MM
目标SM
目标CP-AU
目标GW
源MM
源SM
源CP-AU
源GW
安全策略管理中心
S3101: 发送路径切换请求
S3102: 发送策略查询请求
S3103: 接收初始安全策略
S3104: 发送密钥查询请求
S3105: 发送第一共享密钥
S3106: 发送初始安全策略和第一共享密钥
S3107: 发送输入消息
S3108: 发送目标安全策略
S3109: 发送目标安全策略
发送第一共享密钥
S3110: 生成第二共享密钥
S3111: 发送第二共享密钥
S3112: 发送第二共享密钥
S3113: 发送目标安全策略
S3114: 生成第二共享密钥

图3A

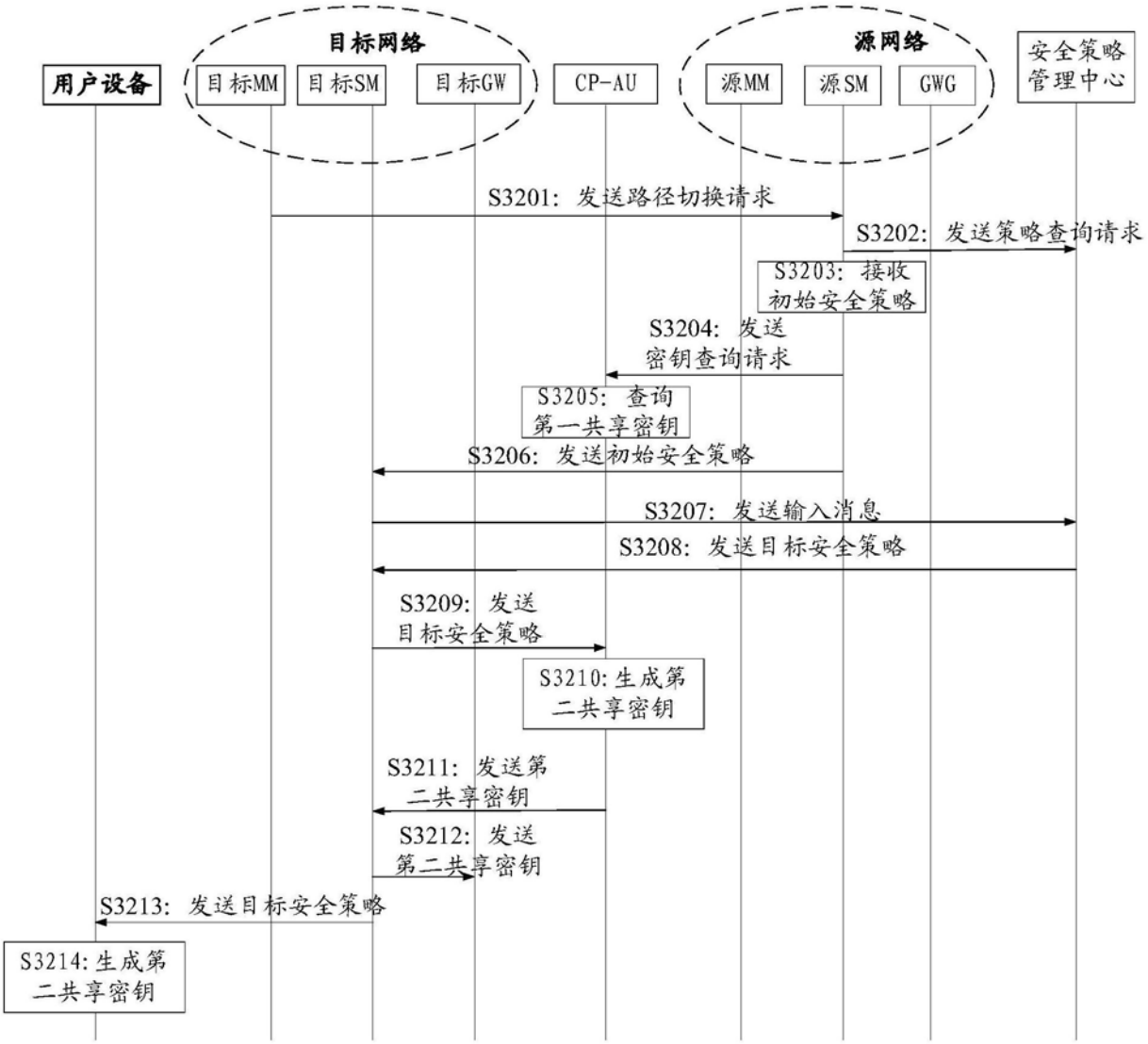

目标网络
源网络
用户设备
目标MM
目标SM
目标GW
CP-AU
源MM
源SM
GWG
安全策略管理中心
S3201：发送路径切换请求
S3202：发送策略查询请求
S3203：接收初始安全策略
S3204：发送密钥查询请求
S3205：查询第一共享密钥
S3206：发送初始安全策略
S3207：发送输入消息
S3208：发送目标安全策略
S3209：发送目标安全策略
S3210：生成第二共享密钥
S3211：发送第二共享密钥
S3212：发送第二共享密钥
S3213：发送目标安全策略
S3214：生成第二共享密钥

图3B

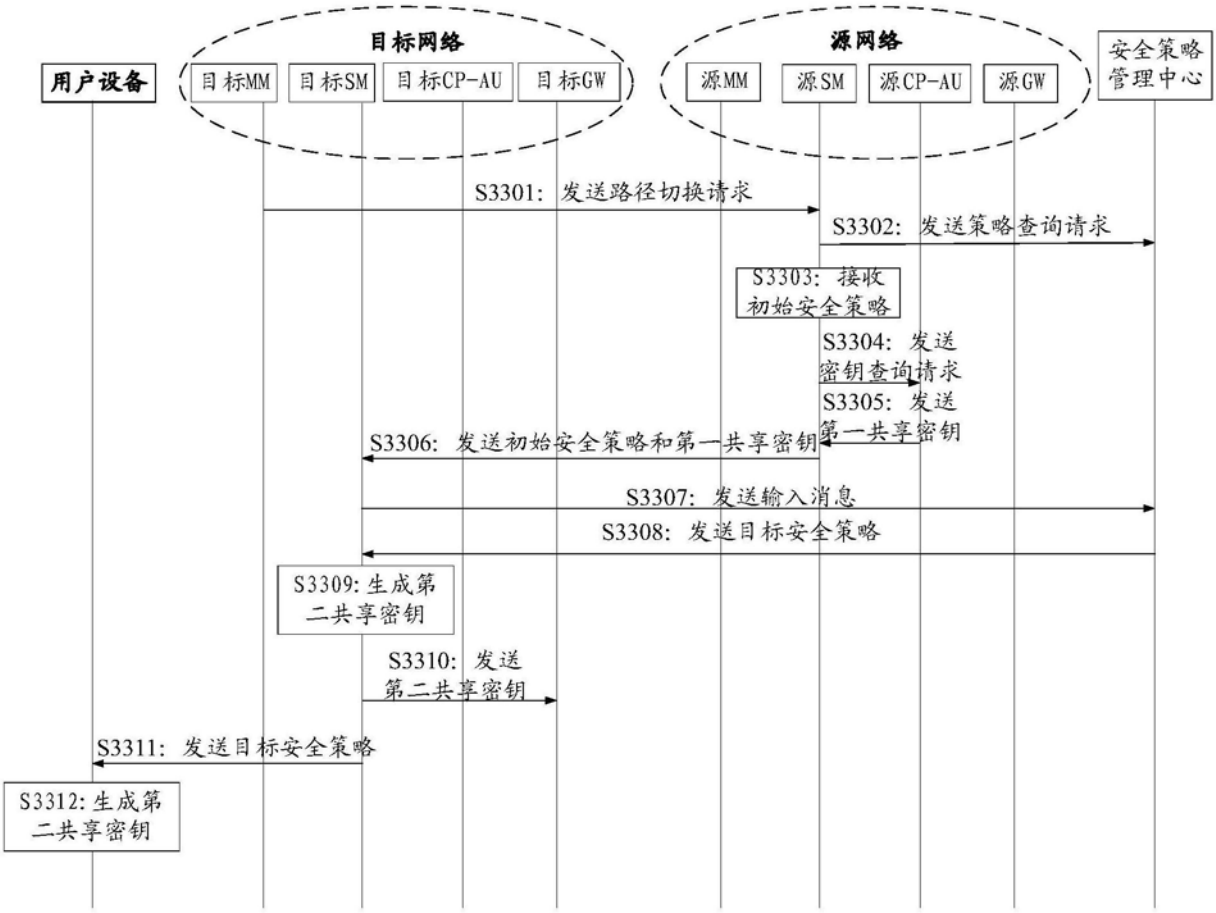

目标网络
源网络
用户设备
目标MM
目标SM
目标CP-AU
目标GW
源MM
源SM
源CP-AU
源GW
安全策略管理中心
S3301: 发送路径切换请求
S3302: 发送策略查询请求
S3303: 接收初始安全策略
S3304: 发送密钥查询请求
S3305: 发送第一共享密钥
S3306: 发送初始安全策略和第一共享密钥
S3307: 发送输入消息
S3308: 发送目标安全策略
S3309: 生成第二共享密钥
S3310: 发送第二共享密钥
S3311: 发送目标安全策略
S3312: 生成第二共享密钥

图3C

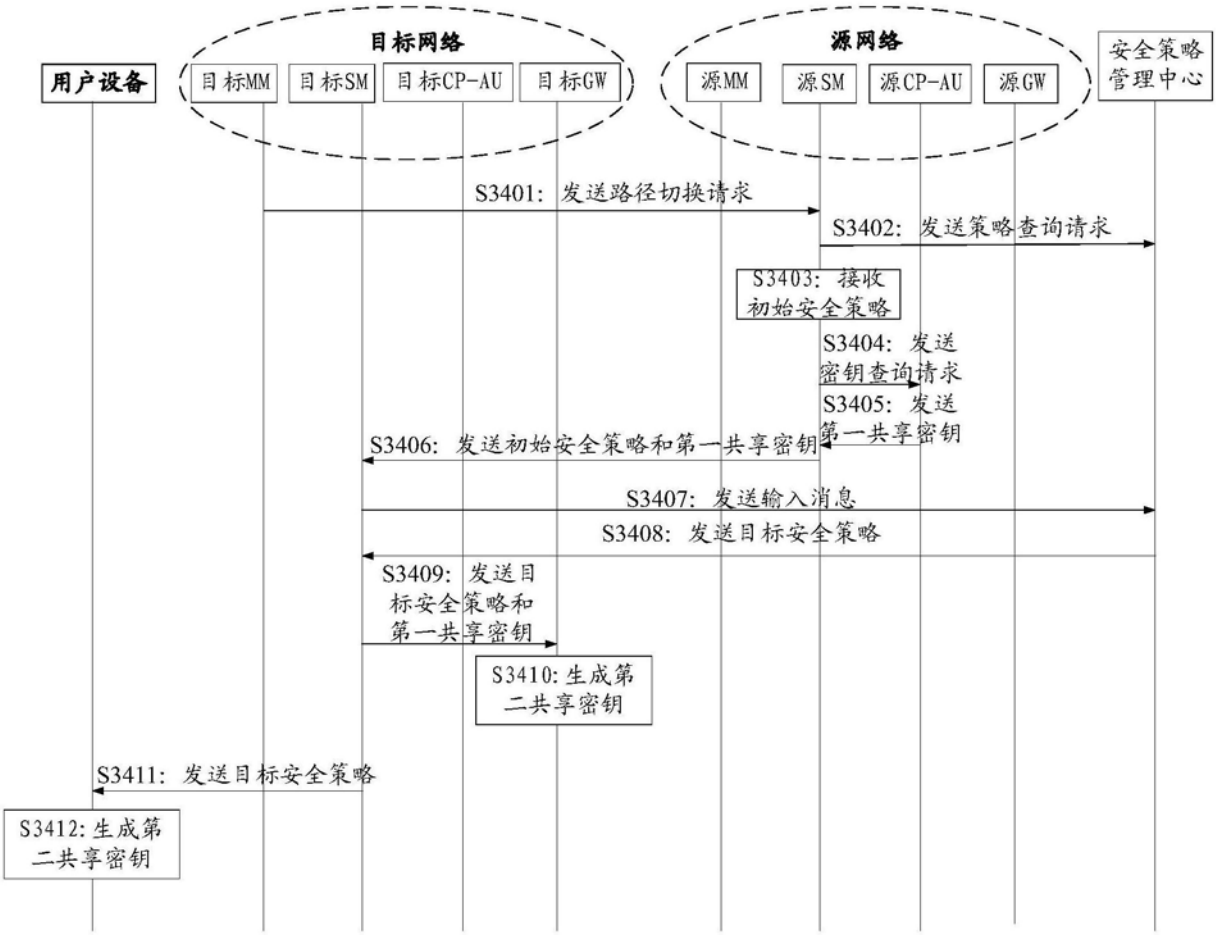

目标网络
源网络
用户设备
目标MM
目标SM
目标CP-AU
目标GW
源MM
源SM
源CP-AU
源GW
安全策略管理中心
S3401: 发送路径切换请求
S3402: 发送策略查询请求
S3403: 接收初始安全策略
S3404: 发送密钥查询请求
S3405: 发送第一共享密钥
S3406: 发送初始安全策略和第一共享密钥
S3407: 发送输入消息
S3408: 发送目标安全策略
S3409: 发送目标安全策略和第一共享密钥
S3410: 生成第二共享密钥
S3411: 发送目标安全策略
S3412: 生成第二共享密钥

图3D

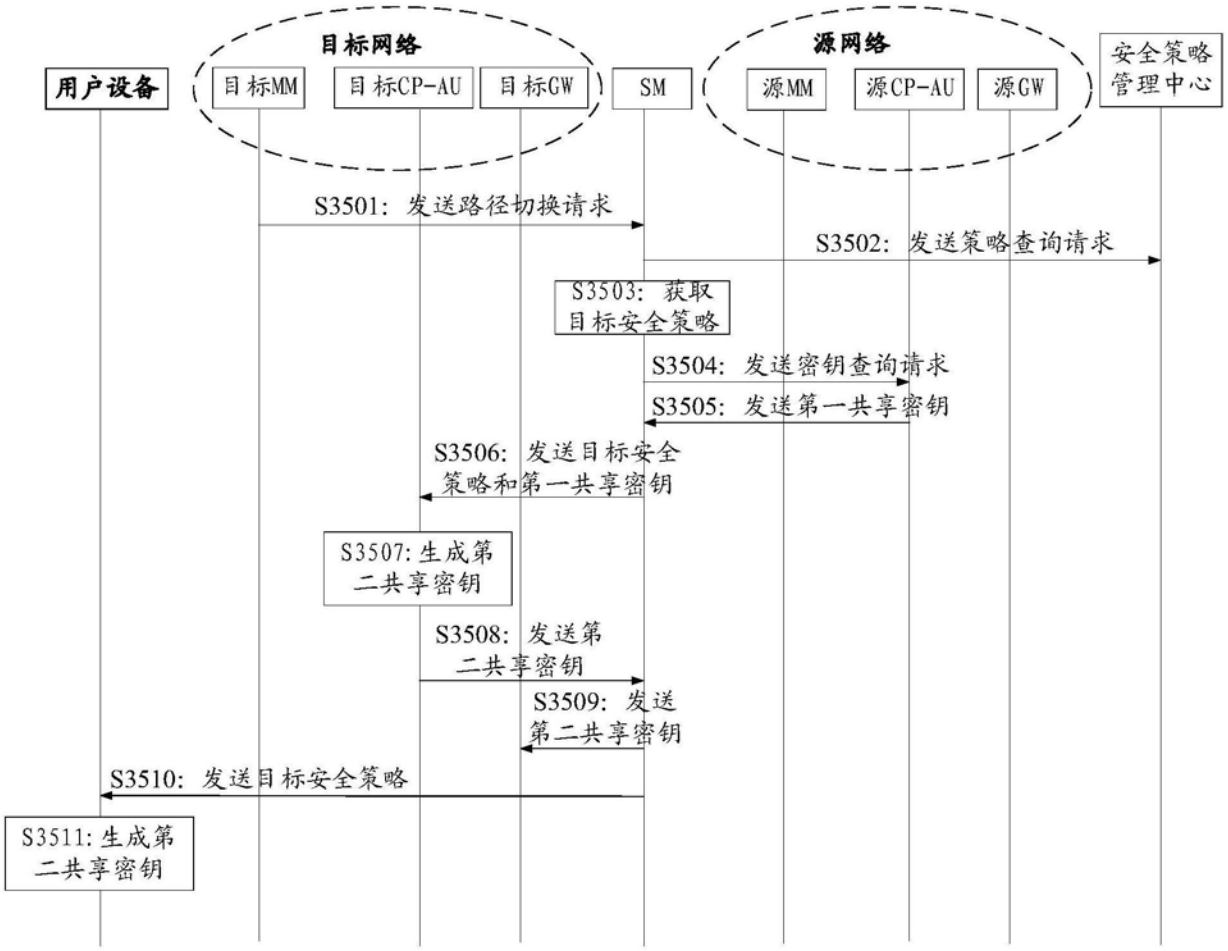

目标网络
源网络
用户设备
目标MM
目标CP-AU
目标GW
SM
源MM
源CP-AU
源GW
安全策略管理中心
S3501：发送路径切换请求
S3502：发送策略查询请求
S3503：获取目标安全策略
S3504：发送密钥查询请求
S3505：发送第一共享密钥
S3506：发送目标安全策略和第一共享密钥
S3507：生成第二共享密钥
S3508：发送第二共享密钥
S3509：发送第二共享密钥
S3510：发送目标安全策略
S3511：生成第二共享密钥

图3E

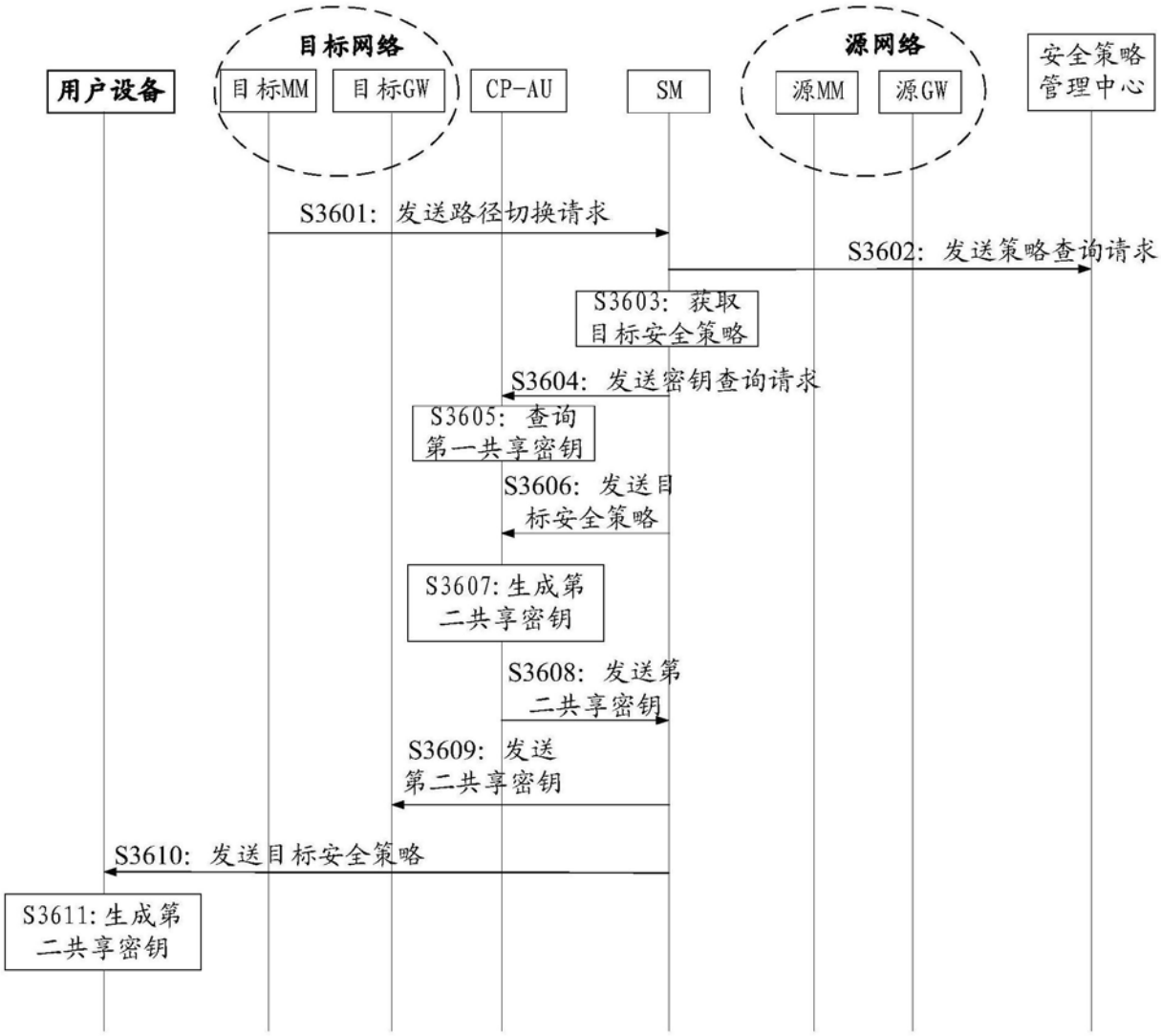

目标网络
源网络
用户设备
目标MM
目标GW
CP-AU
SM
源MM
源GW
安全策略管理中心
S3601: 发送路径切换请求
S3602: 发送策略查询请求
S3603: 获取目标安全策略
S3604: 发送密钥查询请求
S3605: 查询第一共享密钥
S3606: 发送目标安全策略
S3607: 生成第二共享密钥
S3608: 发送第二共享密钥
S3609: 发送第二共享密钥
S3610: 发送目标安全策略
S3611: 生成第二共享密钥

图3F

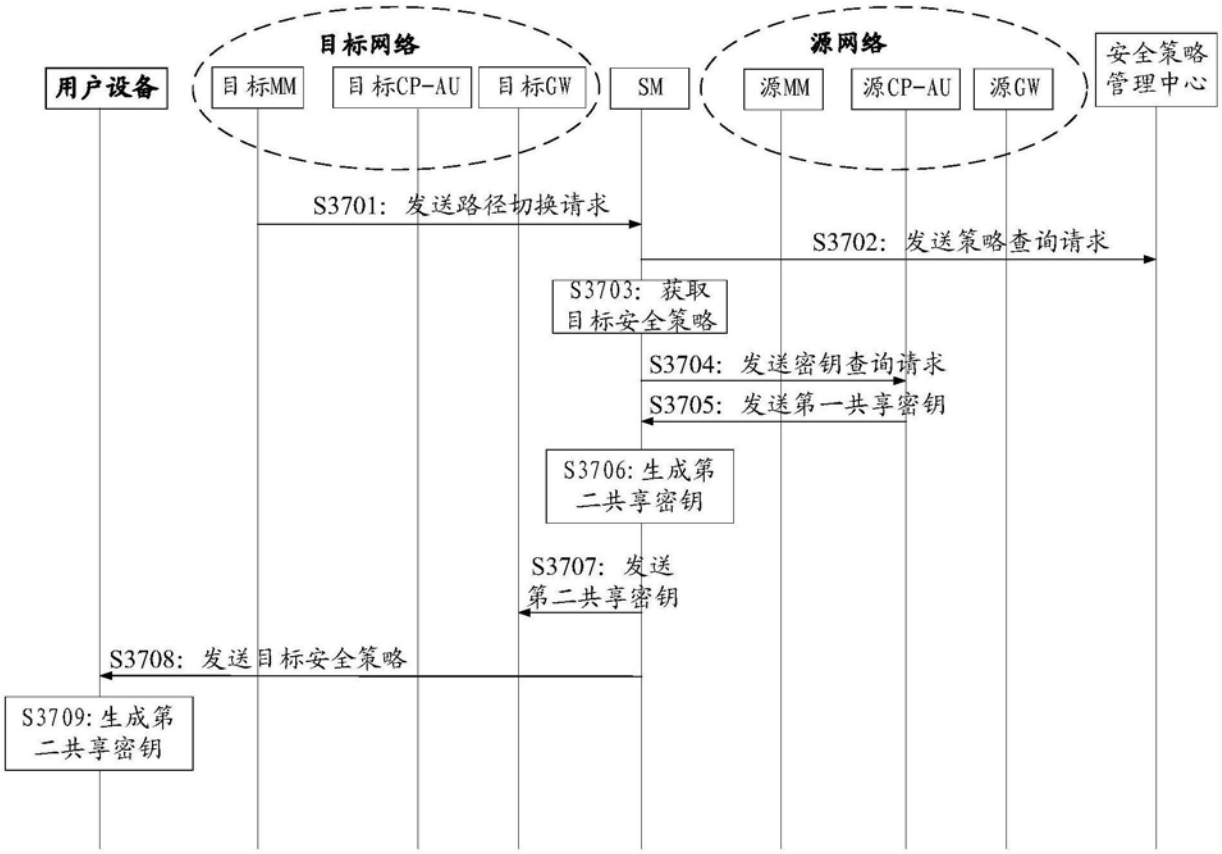

目标网络
源网络
用户设备
目标MM
目标CP-AU
目标GW
SM
源MM
源CP-AU
源GW
安全策略管理中心
S3701：发送路径切换请求
S3702：发送策略查询请求
S3703：获取目标安全策略
S3704：发送密钥查询请求
S3705：发送第一共享密钥
S3706：生成第二共享密钥
S3707：发送第二共享密钥
S3708：发送目标安全策略
S3709：生成第二共享密钥

图3G

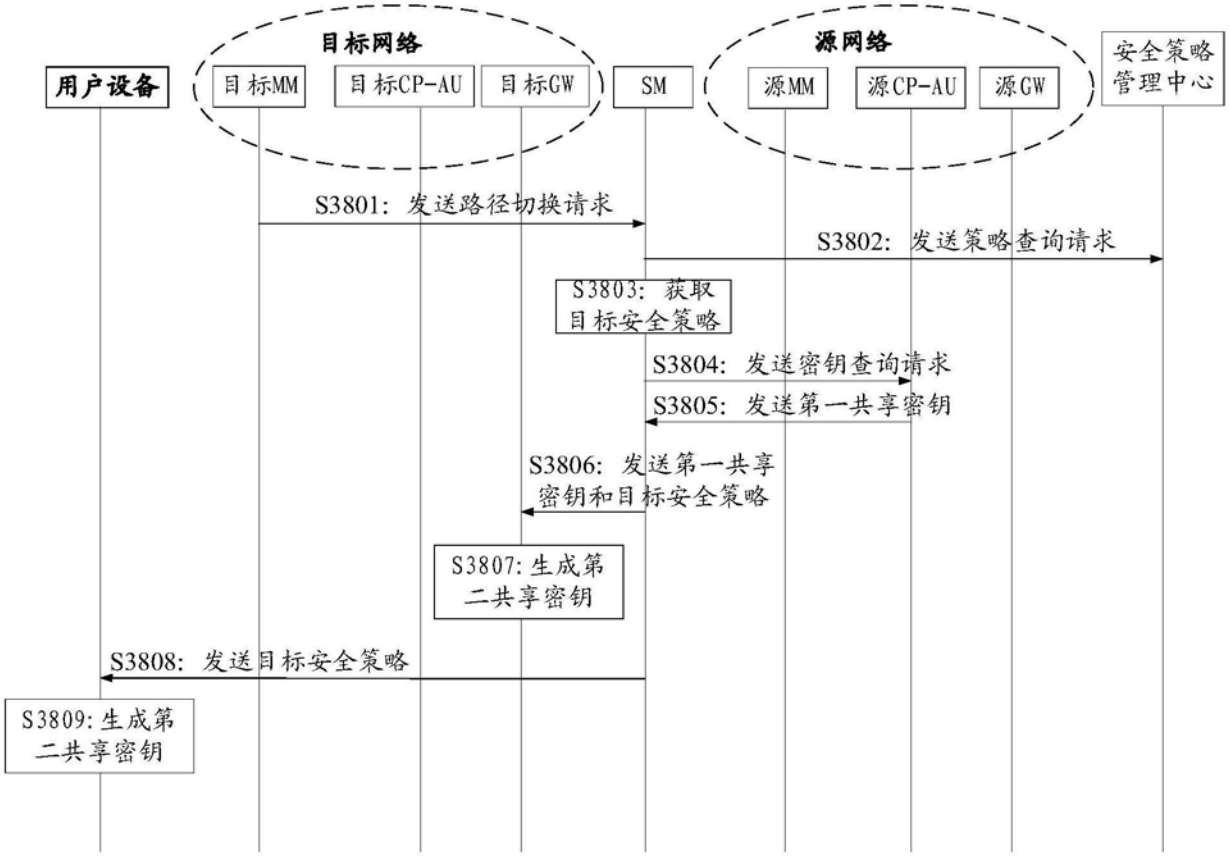

目标网络
源网络
用户设备
目标MM
目标CP-AU
目标GW
SM
源MM
源CP-AU
源GW
安全策略管理中心
S3801：发送路径切换请求
S3802：发送策略查询请求
S3803：获取目标安全策略
S3804：发送密钥查询请求
S3805：发送第一共享密钥
S3806：发送第一共享密钥和目标安全策略
S3807：生成第二共享密钥
S3808：发送目标安全策略
S3809：生成第二共享密钥

图3H

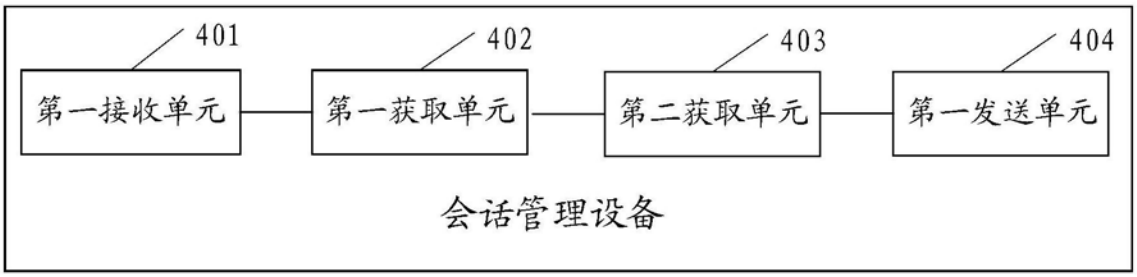

401
402
403
404
第一接收单元
第一获取单元
第二获取单元
第一发送单元
会话管理设备

图4

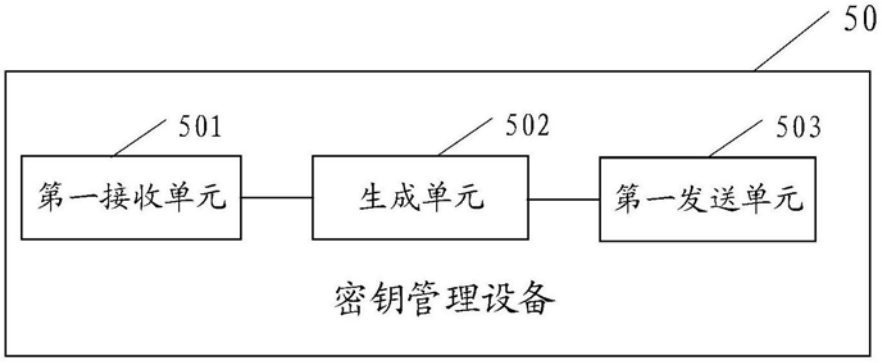

50
501
502
503
第一接收单元
生成单元
第一发送单元
密钥管理设备

图5

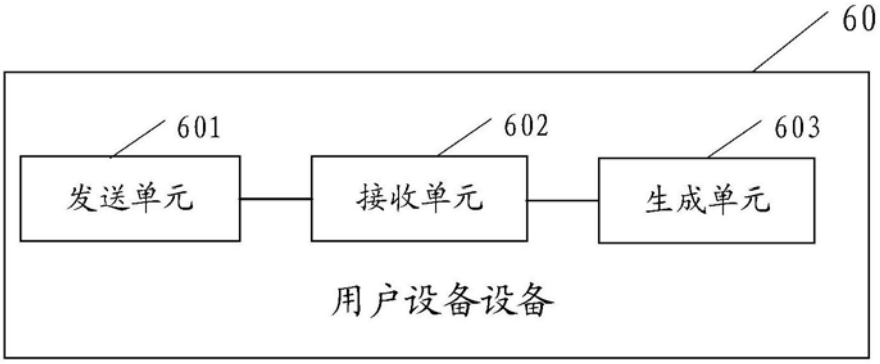

60
601
602
603
发送单元
接收单元
生成单元
用户设备设备

图6

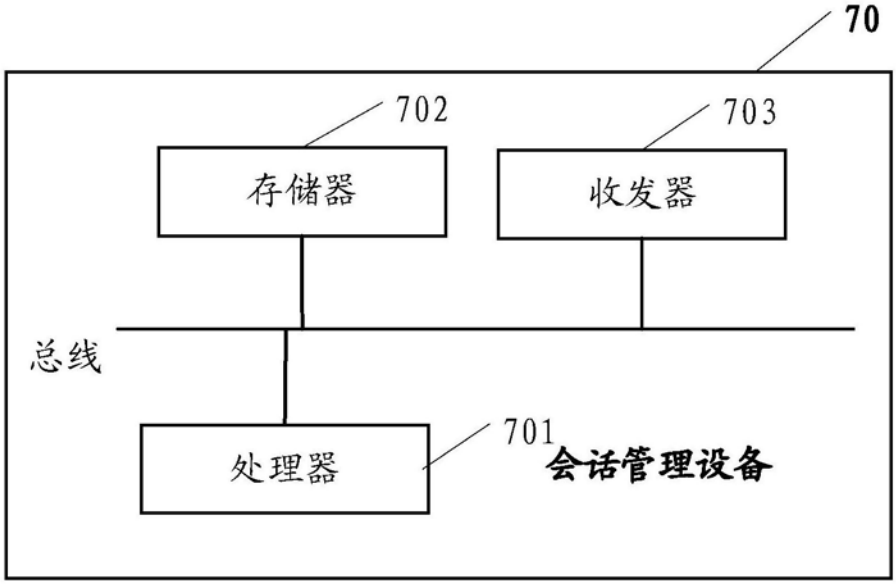

70
702
703
存储器
收发器
总线
处理器
701
会话管理设备

图7

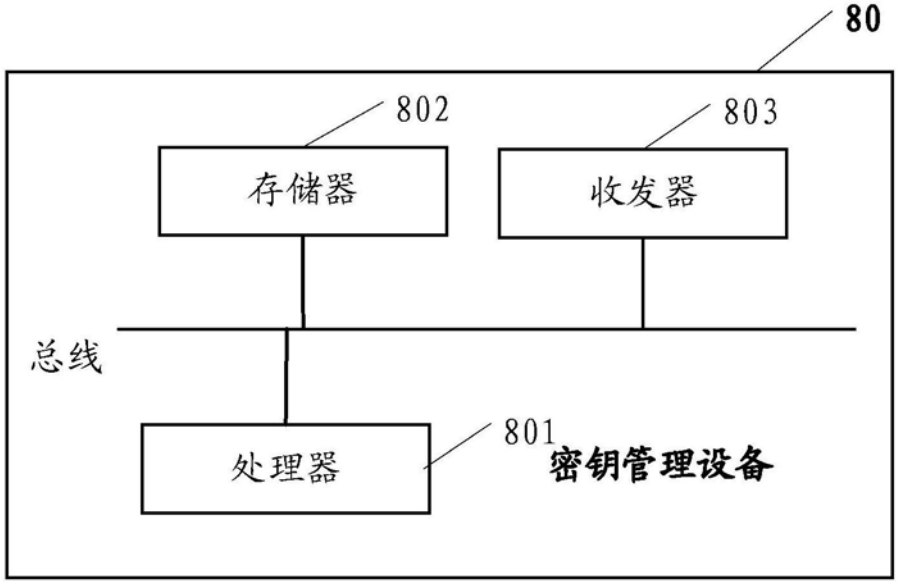

80
802
803
存储器
收发器
总线
处理器
801
密钥管理设备

图8

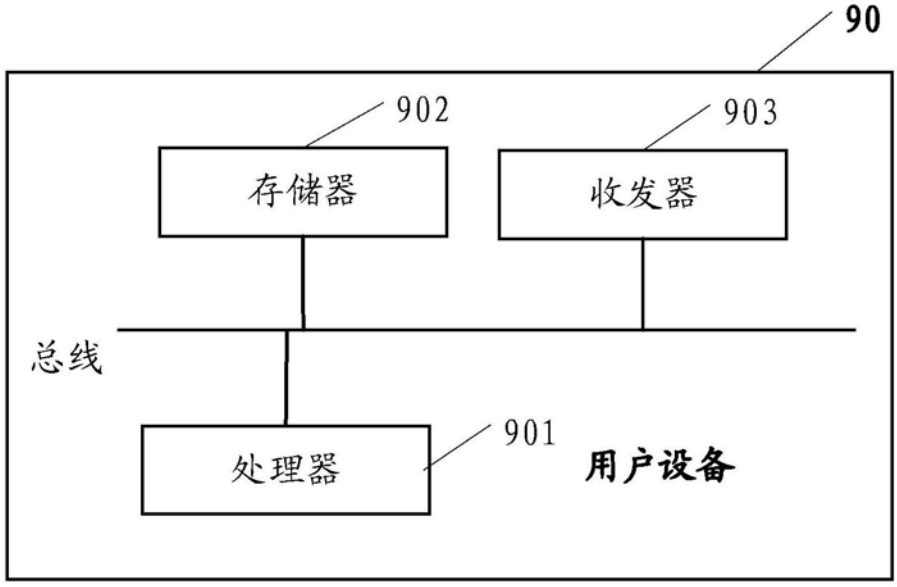

90
902
903
存储器
收发器
总线
处理器
901
用户设备

图9

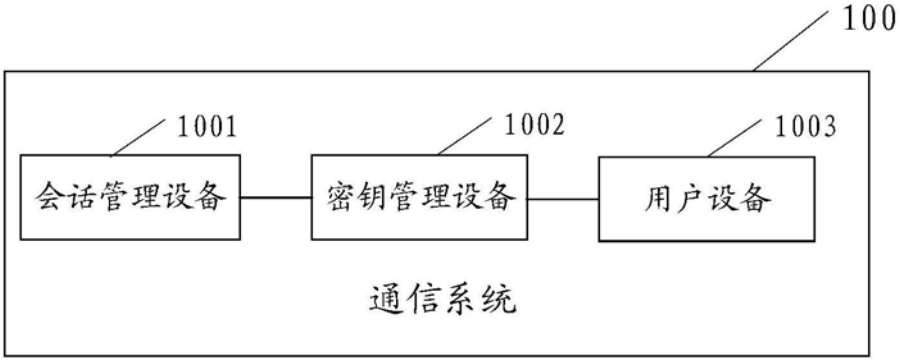


图10