[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/28 (2006.01)
H04Q 7/38 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510116986.X

[43] 公开日 2006 年 6 月 28 日

[11] 公开号 CN 1794682A

[22] 申请日 2005.10.28
[21] 申请号 200510116986.X
[30] 优先权
[32] 2005.7.11 [33] CN [31] 200510082882.1
[71] 申请人 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 肖正飞

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 王 琦 程殿军

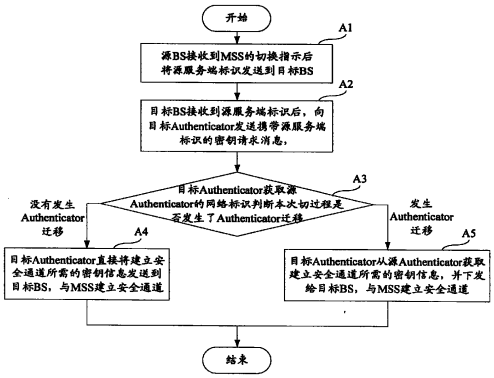
权利要求书 3 页 说明书 13 页 附图 6 页

[54] 发明名称

一种在无线接入网中建立安全通道的方法

[57] 摘要

本发明公开了一种在无线接入网中建立安全通道的方法，在移动用户站发生切换时包括：目标基站获得源服务端标识；目标基站根据所获得的源服务器端标识请求密钥信息；目标基站根据所述密钥信息与发生切换的移动用户站建立安全通道。可以在移动用户站和目标基站之间迅速建立安全通道，而不需要触发鉴权服务器发起重鉴权过程，既节省了空中接口上数据和信令的开销，又大大减少了建立安全通道的时间，提高了用户的业务质量。



1、一种在无线接入网中建立安全通道的方法，其特征在于，所述方法在移动用户站发生切换时包括:

A、目标基站获得源服务端标识;

B、目标基站根据所获得的源服务器端标识请求密钥信息;

C、目标基站根据所述的密钥信息与发生切换的移动用户站建立安全通道。

2、如权利要求 1 所述的方法，其特征在于，所述步骤 B 包括:

B11、目标基站将获得的源服务端标识上传给目标鉴权者;

B12、目标鉴权者根据所述源服务端标识确定源鉴权者的网络标识;

B13、目标鉴权者根据源鉴权者的网络标识向源鉴权者请求密钥信息，并将从源鉴权者获取的密钥信息下发给目标基站。

3、如权利要求 2 所述的方法，其特征在于，步骤 A 所述目标基站获得源服务端标识包括: 在源基站接收到移动用户站发送的切换指示后，将源服务端标识发送到目标基站; 目标基站接收所述源服务端标识。

4、如权利要求 3 所述的方法，其特征在于，所述源服务端标识为源基站的网络标识。

5、如权利要求 3 所述的方法，其特征在于，所述源服务端标识为源鉴权者的网络标识。

6、如权利要求 2 所述的方法，其特征在于，所述源服务端标识为源基站的网络标识;

步骤 A 所述目标基站获得源服务端标识为: 目标基站从切换进入的移动用户站发送的接入消息中获得源基站的网络标识。

7、如权利要求 2 所述的方法，其特征在于，所述源服务端标识为源鉴权者的网络标识;

步骤 A 所述目标基站获得源服务端标识为: 目标基站从切换进入的移动用户站发送的接入消息中获得源基站的网络标识; 目标基站根据源基站的网络标

识向源基站请求源鉴权者的网络标识；源基站将控制自身的源鉴权者的网络标识发送给目标基站。

8、如权利要求 4 或 6 所述的方法，其特征在于，步骤 B12 所述的根据所述源服务端标识确定源鉴权者的网络标识为：目标鉴权者根据源基站的网络标识以及预先配置的基站与鉴权者控制关系对应表查找得到控制源基站的源鉴权者的网络标识。

9、如权利要求 5 或 7 所述的方法，其特征在于，步骤 B12 所述的根据所述源服务端标识确定源鉴权者的网络标识为：目标鉴权者将接收的源鉴权者的网络标识直接确定为源鉴权者的网络标识。

10、如权利要求 2 所述的方法，其特征在于，所述方法在步骤 B12 之后进一步包括：目标鉴权者根据确定的源鉴权者的网络标识判断在所述移动用户站的切换过程中是否发生了鉴权者迁移，如果是，则继续执行步骤 B13；否则，目标鉴权者直接下发与发生切换的移动用户站对应的密钥信息到目标基站，目标基站根据接收的密钥信息与所述发生切换的移动用户站建立安全通道。

11、如权利要求 1 所述的方法，其特征在于，所述源服务端标识为源鉴权者的网络标识；

步骤 A 所述目标基站获得源服务端标识为：目标基站从切换进入的移动用户站发送的接入消息中获得源基站的网络标识；目标基站根据源基站的网络标识向源基站请求源鉴权者的网络标识；源基站将控制自身的源鉴权者的网络标识发送给目标基站；或者为

在源基站接收到移动用户站发送的切换指示后，将源鉴权者的网络标识发送到目标基站；目标基站接收所述源鉴权者的网络标识。

12、如权利要求 11 所述的方法，其特征在于，所述步骤 B 包括：

B21、目标基站根据源鉴权者的网络标识直接向源鉴权者请求密钥信息；

B22、源鉴权者直接将建立安全通道所需的密钥下发给目标基站。

13、如权利要求 1 所述的方法，其特征在于，所述方法在步骤 A 之后进一步包括：目标基站根据获得的源服务端标识判断在所述移动用户站的切换过程

中是否发生了鉴权者迁移，如果是，则继续执行步骤 B；否则，目标基站向目标鉴权者请求所述移动用户站对应的密钥信息，目标鉴权者将所述密钥信息直接下发给目标基站，目标基站根据接收的密钥信息与所述移动用户站建立安全通道。

14、如权利要求 13 所述的方法，其特征在于，所述源服务端标识为源基站的网络标识；

所述判断为：目标基站查找自身存储的、预先配置的、控制自身鉴权者所能控制的所有基站的网络标识列表，判断所获得的源基站网络标识是否在此列表中，如果在，则没有发生鉴权者迁移；否则，就发生了鉴权者迁移。

15、如权利要求 13 所述的方法，其特征在于，所述源服务端标识为源鉴权者的网络标识；

所述判断包括：目标基站根据自身存储的、预先配置的、控制自身鉴权者的网络标识得到目标鉴权者的网络标识；判断所获得的源鉴权者的网络标识与所述目标鉴权者的网络标识是否相同，如果相同，则没有发生鉴权者迁移；否则，发生了鉴权者迁移。

16、如权利要求 1 所述的方法，其特征在于，所述密钥信息至少包括：鉴权密钥、该鉴权密钥的标识以及该鉴权密钥的生命周期。

17、如权利要求 1、10 或 13 所述的方法，其特征在于，所述建立安全通道为：目标基站与移动用户站根据相同的密钥信息派生出用于加密空中接口数据以及对管理消息进行一致性检验的密钥，使用派生出的密钥加密空中接口数据，并对管理消息进行一致性检验。

一种在无线接入网中建立安全通道的方法

技术领域

本发明涉及到保证无线接入网安全性的技术，特别涉及到在无线接入网中建立安全通道的方法。

背景技术

随着因特网业务的蓬勃发展和无线网络的广泛应用，已经对无线接入网提出了越来越多的安全性要求，除采用目前广泛使用的设备鉴权、用户鉴权和服务授权等等方法来提高无线通信的安全性之外，移动用户站（MSS）与基站（BS）之间安全通道的建立，保密信息的交换，以及 BS 和鉴权者（Authenticator）、Authenticator 和鉴权服务器（Authentication Server）之间的安全通道的建立，保密信息的交换等等都是目前需要特别关注的问题。

图 1 显示了现阶段无线接入网的安全网络架构体系。如图 1 所示，在无线接入网的安全网络架构中主要涉及到以下网元：MSS、BS、Authenticator 以及 Authentication Server。其中，MSS 在所述安全架构中的主要功能是发起认证、鉴权，与 Authentication Server 交换产生根密钥所需的信息，生成根密钥，根据根密钥产生对空中接口数据加密所需要的鉴权密钥（AK，Authorization Key）以及根据 AK 派生出用于加密数据及管理消息一致性检验的其他密钥信息等；BS 在上述安全架构中的功能是为 BS 和 MSS 提供安全体系通道，对空中接口数据进行压缩与加密，交换 BS 和 MSS 之间的保密信息，为 MSS 提供从 BS 到 Authenticator 的安全通道等；Authenticator 在上述安全架构中的主要功能是为 MSS 认证、授权和计费提供代理功能，根据 Authentication Server 提供的与 MSS 之间对等的根密钥信息，产生 BS 和 MSS 之间建立安全通道所需的 AK，并将 AK 分发到相应的 BS；Authentication

Server 的主要功能包括：为 MSS 进行认证、授权和计费，产生并分发根密钥信息到 Authenticator，在用户信息产生变化时及时通知 Authenticator 和其他网元用户信息改变所产生的后果。

在 MSS 初次接入无线接入网时，MSS 的鉴权、认证以及与 BS 之间安全通道的建立过程如下：

a、MSS 通过 BS 和 Authenticator，发送与鉴权有关的信息到 Authentication Server;

在这里所述的与鉴权有关的信息与 MSS 和 Authentication Server 选择的鉴权算法有关，通常包括：MSS 的网络标志符（NAI），所使用鉴权算法的标识，用户识别模块（SIM）卡号码或者随机产生的随机数等等，Authentication Server 可以根据这些信息对 MSS 进行鉴权;

b、Authentication Server 根据接收的鉴权信息对该 MSS 进行鉴权，并在鉴权通过后，与 MSS 同时按照约定的算法各自建立用于产生根密钥的鉴权认证计费密钥（AAA-Key）;

c、Authentication 服务器将 AAA-Key 下发给 Authenticator，Authenticator 与 MSS 根据 AAA-Key 使用相同的算法各自生成根密钥，Authenticator 与 MSS 再根据根密钥生成 AK，Authenticator 进一步将 AK 下发给 BS;

d、BS 和 MSS 根据 AK，按照 IEEE 802.16e 中的密钥管理协议（PKM）机制协商产生对 MSS 和 BS 之间空中接口数据进行加密以及对管理信息进行一致性检验所需的相关密钥，在空中接口上建立安全通道。

这样，空中接口上传输的数据都能够通过加密实现安全传输，而空中接口上传输的管理消息也可以通过使用用于一致性检验的消息认证码（MAC，Message Authentication Code）实现安全传输。

由于 MSS 是可移动的，因此，在移动过程中，MSS 很可能从一个 BS 覆盖的范围移动到另一个 BS 覆盖的范围，在这种情况下，MSS 就需要从一个称为源 BS 的 BS，切换到另一个称为目标 BS 的 BS。在上述切换过程中，如果源 BS 和目标 BS 受到同一个 Authenticator 的控制，则在切换后，该

Authenticator 仅需要把当前 MSS 的 AK 下发到目标 BS，MSS 和目标 BS 就可以根据该 AK 建立安全通道了。但是，如果控制源 BS 和目标 BS 的 Authenticator 不同，即在 MSS 的切换过程中发生了 Authenticator 迁移，则根据协议规定，管理目标 BS 的 Authenticator，称为目标 Authenticator 就会向 Authentication Server 申请新的根密钥，这将导致 Authentication Server 重新对 MSS 进行如上述步骤 A 至 D 所述的鉴权、授权和密钥协商的完整过程，以便在 MSS 和目标 BS 之间建立新的安全通道。

这样，不仅仅会增加 BS 与 Authenticator 及 Authenticator 与 Authentication Server 之间数据和信令的开销，还将占用较多的空中接口资源，增加安全通道建立所需的时间。特别是在 Authenticator 与 BS 在物理上存在于一个网元中的情况下，MSS 在 BS 间的切换必然引起 Authenticator 的迁移，使得 Authenticator 的迁移过于频繁，最终导致用户会话的中断及业务质量的下降。

发明内容

为了解决上述技术问题，本发明提供了一种在无线接入网中建立安全通道的方法，使得在由 MSS 切换引发 Authenticator 迁移时，目标 BS 可以及时获得建立安全通道所需的密钥信息，迅速在 MSS 和目标 BS 之间建立安全通道，而不需要触发 Authentication Server 的重鉴权过程，保证用户会话的业务质量。

本发明所述在无线接入网中建立安全通道的方法在移动用户站发生切换时包括:

A、目标基站获得源服务端标识;

B、目标基站根据所获得的源服务器端标识请求密钥信息;

C、目标基站根据所述密钥信息与发生切换的移动用户站建立安全通道。

本发明所述步骤 B 包括:

B11、目标基站将获得的源服务端标识上传给目标鉴权者；

B12、目标鉴权者根据所述源服务端标识确定源鉴权者的网络标识；

B13、目标鉴权者根据源鉴权者的网络标识向源鉴权者请求密钥信息，并将从源鉴权者获取的密钥信息下发给目标基站。

步骤 A 所述目标基站获得源服务端标识包括：在源基站接收到移动用户站发送的切换指示后，将源服务端标识发送到目标基站；目标基站接收所述源服务端标识。

本发明所述源服务端标识为源基站的网络标识。

本发明所述源服务端标识为源鉴权者的网络标识。

本发明所述源服务端标识为源基站的网络标识；

步骤 A 所述目标基站获得源服务端标识为：目标基站从切换进入的移动用户站发送的接入消息中获得源基站的网络标识。

本发明所述源服务端标识为源鉴权者的网络标识；

步骤 A 所述目标基站获得源服务端标识为：目标基站从切换进入的移动用户站发送的接入消息中获得源基站的网络标识；目标基站根据源基站的网络标识向源基站请求源鉴权者的网络标识；源基站将控制自身的源鉴权者的网络标识发送给目标基站。

步骤 B12 所述的根据所述源服务端标识确定源鉴权者的网络标识为：目标鉴权者根据源基站的网络标识以及预先配置的基站与鉴权者控制关系对应表查找得到控制源基站的源鉴权者的网络标识。

步骤 B12 所述的根据所述源服务端标识确定源鉴权者的网络标识为：目标鉴权者将接收的源鉴权者的网络标识直接确定为源鉴权者的网络标识。

本发明所述方法在步骤 B12 之后进一步包括：目标鉴权者根据确定的源鉴权者的网络标识判断在所述移动用户站的切换过程中是否发生了鉴权者迁移，如果是，则继续执行步骤 B13；否则，目标鉴权者直接下发与发生切换的移动用户站对应的密钥信息到目标基站，目标基站根据接收的密钥信息与所述发生切换的移动用户站建立安全通道。

本发明所述源服务端标识为源鉴权者的网络标识；

步骤 A 所述目标基站获得源服务端标识为：目标基站从切换进入的移动用户站发送的接入消息中获得源基站的网络标识；目标基站根据源基站的网络标识向源基站请求源鉴权者的网络标识；源基站将控制自身的源鉴权者的网络标识发送给目标基站；

或在源基站接收到移动用户站发送的切换指示后，将源鉴权者的网络标识发送到目标基站；目标基站接收所述源鉴权者的网络标识。

本发明所述步骤 B 包括：

B21、目标基站根据源鉴权者的网络标识直接向源鉴权者请求密钥信息；

B22、源鉴权者直接将建立安全通道所需的密钥下发给目标基站。

本发明所述方法在步骤 A 之后进一步包括：目标基站根据获得的源服务端标识判断在所述移动用户站的切换过程中是否发生了鉴权者迁移，如果是，则继续执行步骤 B；否则，目标基站向目标鉴权者请求所述移动用户站对应的密钥信息，目标鉴权者将所述密钥信息直接下发给目标基站，目标基站根据接收的密钥信息与所述移动用户站建立安全通道。

本发明所述源服务端标识为源基站的网络标识；

所述判断为：目标基站查找自身存储的、预先配置的、控制自身鉴权者所能控制的所有基站的网络标识列表，判断所获得的源基站网络标识是否在此列表中，如果在，则没有发生鉴权者迁移；否则，就发生了鉴权者迁移。

本发明所述源服务端标识为源鉴权者的网络标识；

所述判断包括：目标基站根据自身存储的、预先配置的、控制自身鉴权者的网络标识得到目标鉴权者的网络标识；判断所获得的源鉴权者的网络标识与所述目标鉴权者的网络标识是否相同，如果相同，则没有发生鉴权者迁移；否则，发生了鉴权者迁移。

本发明所述密钥信息至少包括：鉴权密钥、该鉴权密钥的标识以及该鉴权密钥的生命周期。

本发明所述建立安全通道为：目标基站与移动用户站根据相同的密钥信息派生出用于加密空中接口数据以及对管理消息进行一致性检验的密钥，使用派生出的密钥加密空中接口数据，并对管理消息进行一致性检验。

由此可以看出，本发明所述的方法在由 MSS 切换导致 Authenticator 发生迁移的情况下，通过在源 Authenticator 和目标 Authenticator 之间传递建立安全通道所需的密钥信息，可以在 MSS 和目标 BS 之间迅速建立安全通道，而不需要触发 Authentication Server 发起重鉴权过程，这一方面节省了空中接口上数据和信令的开销，另一方面，大大减少了建立安全通道的时间，提高了用户的业务质量。

附图说明

图 1 显示了现阶段无线接入网的安全网络架构体系；

图 2 显示了实施例 1 所述的在无线接入网中建立安全通道的方法；

图 3 显示了实施例 2 所述的在无线接入网中建立安全通道的方法；

图 4 显示了实施例 3 所述的在无线接入网中建立安全通道的方法；

图 5 显示了实施例 4 所述的在无线接入网中建立安全通道的方法；

图 6 显示了实施例 5 所述的在无线接入网中建立安全通道的方法。

具体实施方式

为了在 MSS 切换引发 Authenticator 迁移时，目标 BS 可以及时获得建立安全通道所需的密钥信息，本发明提供了在无线接入网中建立安全通道的方法，可以在不触发 Authentication Server 进行重鉴权过程的情况下，令目标 BS 及时获得建立安全通道所需的密钥信息，迅速在 MSS 和目标 BS 之间建立安全通道。

本发明所述的方法适用于图 1 所示的无线接入网的安全网络架构体系。

为使发明的目的、技术方案及优点更加清楚明白，以下参照附图并举实施例，对本发明作进一步详细说明。

实施例 1:

图 2 显示了实施例 1 所述的在无线接入网中建立安全通道的方法。如图 2 所示，该方法主要包括以下步骤:

A1、源 BS 接收到 MSS 的切换指示后，将源服务端标识发送到目标 BS;所述源服务端标识为源 BS 的网络标识或源 Authenticator 的网络标识;

在该步骤中，源 BS 可以通过 BS 之间的接口直接将源服务端标识发送到所述 BS，还可以通过诸如基站控制器或接入服务网络网关（ASN GW）等控制网元之间的接口将所述源服务端标识间接转发到所述目标 BS;

A2、目标 BS 接收到来自源 BS 的源服务端标识后，向控制自身的 Authenticator，即目标 Authenticator，发送一密钥请求消息，申请该 MSS 对应的密钥信息，并在该密钥请求消息中携带接收到的源服务端标识;

由于在每个 BS 中都存储有预先配置的控制自身的 Authenticator 的网络标识，因此，任何一个 BS 都能够寻址到控制自身的 Authenticator，向该 Authenticator 申请建立安全通道所需的密钥信息;

A3、目标 Authenticator 根据密钥请求消息中的源服务端标识获得源 Authenticator 的网络标识，再根据源 Authenticator 的网络标识判断本次切换过程是否发生了 Authenticator 迁移，即判断自身的网络标识是否与接收到的源 Authenticator 的网络标识相同，如果没有发生 Authenticator 迁移，则执行步骤 A4；否则，执行步骤 A5;

在该步骤中，目标 Authenticator 可以根据所接收源服务端标识的不同采用两种方式获得源 Authenticator 的网络标识：若所述源服务端标识为源 Authenticator 的网络标识，则目标 Authenticator 可以直接获得源 Authenticator 的网络标识;若所述源服务端标识为源 BS 的网络标识，则目标 Authenticator 要根据自身预先配置的 BS 与 Authenticator 的控制关系对应表查找出控制所述源 BS 的源 Authenticator 的网络标识;

在得到源 Authenticator 的网络标识后，目标 Authenticator 将比较源 Authenticator 的网络标识与自身的网络标识是否相同，如果相同，则没有发

生 Authenticator 迁移；否则，就发生了 Authenticator 迁移；

A4、目标 Authenticator 直接将建立安全通道所需的密钥信息发送到目标 BS，目标 BS 根据接收的密钥信息与 MSS 建立安全通道，然后结束；

A5、目标 Authenticator 从源 Authenticator 获取建立安全通道所需的密钥信息，并将获取的密钥信息下发给目标 BS，目标 BS 根据接收的密钥信息与 MSS 建立安全通道，然后结束。

由于 Authenticator 之间存在接入服务网络的内部接口——R6 接口，因此，目标 Authenticator 通过自定义的密钥申请消息向源 Authenticator 请求并获取所述的密钥信息。另外，在源 Authenticator 和目标 Authenticator 之间传递的密钥信息的安全性可以通过传输层/网络层的安全机制来保证，例如，使用因特网协议安全（IPSec）或虚拟专网（VPN）等技术来保证。

在上述步骤 A4 和步骤 A5 中，所述密钥信息至少包括 MSS 的 AK、该 AK 的标识（AKID）以及该 AK 的生命周期。所述密钥信息还可以包括诸如 EAP 完整性密钥（EIK，EAP Integrity Key）等其他密钥信息。

在目标 BS 得到了与 MSS 相同的 AK 后，就可以使用与 MSS 相同的算法派生出用于加密空中接口数据及对管理消息进行一致性检验的其他相关密钥，使用派生出的密钥加密空中接口数据，并对管理消息进行一致性检验，从而建立安全通道实现空中接口上数据和管理消息的安全传输。

从上述实施例 1 的步骤 A3 可以看出，在本实施例中，本次切换过程是否发生了 Authenticator 迁移是由目标 Authenticator 来判断的，在实际的应用中，还可以由目标 BS 判断是否发生了 Authenticator 迁移，参见实施例 2 所述的方法。

实施例 2:

图 3 显示了实施例 2 所述的在无线接入网中建立安全通道的方法。如图 3 所示，该方法主要包括以下步骤:

B1、源 BS 接收到 MSS 的切换指示后，将源服务端标识发送到目标 BS;

所述源服务端标识为源 BS 的网络标识或源 Authenticator 的网络标识;

在本步骤中，源 BS 也可以采用与步骤 A1 相同的方法直接或间接的将源服务端标识发送到目标 BS;

B2、目标 BS 根据接收到的源服务端标识判断是否发生了 Authenticator 迁移，如果发生了 Authenticator 迁移，则执行步骤 B3；否则，执行步骤 B5;

在该步骤中，若所述源服务端标识为源 Authenticator 的网络标识，则目标 BS 直接将自身存储的、预先配置的、控制自身的 Authenticator 网络标识与所述源 Authenticator 的网络标识进行比较，如果相同，则没有发生 Authenticator 迁移，否则，就发生了 Authenticator 迁移;

若所述源服务端标识为源 BS 的网络标识，则目标 BS 必须存储有预先配置的、控制自身的 Authenticator 所能控制的所有 BS 网络标识的列表，目标 BS 通过查找源 BS 的网络标识是否在此列表中来判断是否发生了 Authenticator 迁移，如果在此列表中，则没有发生 Authenticator 迁移，否则，就发生了 Authenticator 迁移;

B3、目标 BS 将接收的源服务端标识通过密钥请求消息发送到控制自身的 Authenticator，即目标 Authenticator，向目标 Authenticator 申请该 MSS 对应的密钥信息;

B4、目标 Authenticator 根据密钥请求消息中的源服务端标识获得源 Authenticator 的网络标识，然后从源 Authenticator 获取建立安全通道所需的密钥信息，并将获取的密钥信息下发给目标 BS，目标 BS 根据接收的密钥信息与 MSS 建立安全通道，然后结束;

本步骤所述获得源 Authenticator 的网络标识的方法与上述步骤 A3 所述的方法相同；所述从源 Authenticator 获取密钥信息的方法与步骤 A5 所述的方法相同;

B5、目标 BS 向目标 Authenticator，即源 Authenticator，申请该 MSS 对应的密钥信息，目标 Authenticator 将该 MSS 的密钥信息直接下发给目标 BS，目标 BS 根据接收的密钥信息与 MSS 建立安全通道，然后结束。

在上述步骤 B4 和步骤 B5 中，所述的密钥信息也至少包括 MSS 的 AK。

在目标 BS 得到了与 MSS 相同的 AK 后，就可以使用与 MSS 相同的算法派生出用于加密空中接口数据及对管理消息进行一致性检验的其他密钥，使用派生出的密钥加密空中接口数据，并对管理消息进行一致性检验，从而建立安全通道实现空中接口上数据和管理消息的安全传输。

从上述过程可以看出，在上述两个实施例中，目标 BS 是从来自源 BS 的切换消息中获得源服务端标识的，但是在某些时候，可能出现在 MSS 已经切换进入目标 BS 时，目标 BS 仍无法从源 BS 获得源服务端标识的情况，例如，由于 MSS 已经离开源 BS 的覆盖区域，使得源 BS 无法收到 MSS 发送的切换指示，从而导致源 BS 不会将源服务端标识发送到目标 BS。在这种情况下，目标 BS 无法得知源服务端标识，从而无法通过目标 Authenticator 快速获得原来使用的密钥信息。

下面将要描述的本发明的优选实施例可以解决上述问题。

实施例 3:

图 4 显示了实施例 3 所述的在无线接入网中建立安全通道的方法。如图 4 所示，所述方法在 MSS 切换进入目标 BS 后，包括以下步骤:

C1、目标 BS 从 MSS 的接入消息中获取源 BS 的网络标识;

C2、目标 BS 根据源 BS 的网络标识向源 BS 发送包含 MSS 标识的切换指示请求，要求源 BS 提供源 Authenticator 的网络标识;

在该步骤中，目标 BS 可以通过 BS 之间的接口直接向源 BS 请求源服务端标识，还可以通过诸如基站控制器或 ASN GW 等控制网元之间的接口间接向源 BS 请求源 Authenticator 的网络标识;

C3、获得源 Authenticator 的网络标识后，目标 BS 将源 Authenticator 的网络标识通过密钥请求消息发送到控制自身的 Authenticator，即目标 Authenticator，向目标 Authenticator 申请该 MSS 对应的密钥信息;

C4、目标 Authenticator 根据密钥请求消息中的源 Authenticator 的网络标识判断在本次切换过程中是否发生了 Authenticator 迁移，如果没有发生 Authenticator 迁移，则执行步骤 C5，否则执行步骤 C6;

C5、目标 Authenticator 直接将建立安全通道所需的密钥下发给目标 BS，目标 BS 根据接收的密钥信息与 MSS 建立安全通道，然后结束；

C6、目标 Authenticator 从源 Authenticator 获取建立安全通道所需的密钥信息，并将获取的密钥信息下发给目标 BS，目标 BS 根据接收的密钥信息与 MSS 建立安全通道，然后结束。

本步骤所述从源 Authenticator 获取密钥信息的方法与实施例 1 步骤 A5 所述的方法相同。

上述步骤 C5 和 C6 所述的密钥信息也至少包括源 MSS 的 AK。在目标 BS 得到了与 MSS 相同的 AK 后，就可以与 MSS 派生出其他密钥实现空中接口上数据和管理消息的安全传输。

熟悉本领域的技术人员可以理解，也可以在目标 BS 获得源 Authenticator 的网络标识后，由目标 BS 根据源 Authenticator 的网络标识判断在本次切换过程中是否发生了 Authenticator 迁移，其判断方法可以采用实施例 2 步骤 B2 所述的判断方法，如果发生了 Authenticator 迁移，则将源 Authenticator 的网络标识上报给目标 Authenticator，通过目标 Authenticator 从源 Authenticator 获取建立安全通道所需的密钥信息，从而建立安全通道；否则，直接从源 Authenticator 获取密钥信息建立安全通道。

实施例 4：

图 5 显示了实施例 4 所述的无线接入网中建立安全通道的方法。如图 5 所示，所述方法在 MSS 切换进入目标 BS 后，包括以下步骤：

D1、目标 BS 从 MSS 的接入消息中获取源 BS 的网络标识；

D2、目标 BS 将源 BS 的网络标识通过密钥请求消息发送到控制自身的 Authenticator，即目标 Authenticator，向目标 Authenticator 申请该 MSS 对应的密钥信息；

D3、目标 Authenticator 根据密钥请求消息中的源 BS 网络标识查找自身存储的 BS 与 Authenticator 控制关系对应表得到源 Authenticator 的网络标识，并根据源 Authenticator 的网络标识判断在本次切换过程中是否发生了

Authenticator 迁移，如果是，则执行步骤 D4，否则执行 D5;

D4、目标 Authenticator 直接将建立安全通道所需的密钥下发给目标 BS，目标 BS 根据接收的密钥信息与 MSS 建立安全通道，然后结束;

D5、目标 Authenticator 从源 Authenticator 获取建立安全通道所需的密钥信息，并将获取的密钥信息下发给目标 BS，目标 BS 根据接收的密钥信息与 MSS 建立安全通道，然后结束。

上述步骤 D4 和 D5 所述的密钥信息也至少包括该 MSS 的 AK。在目标 BS 得到了与 MSS 相同的 AK 后，就可以与 MSS 派生出其他密钥实现空中接口上数据和管理消息的安全传输。

与实施例 3 相同，在实施例 4 中也可以在目标 BS 获得源 BS 的网络标识后，由目标 BS 根据源 BS 的网络标识查找管理自身的 Authenticator 所管理所有 BS 列表，判断在本次切换过程中是否发生了 Authenticator 迁移，其判断方法可以采用实施例 2 步骤 B2 所述的判断方法，如果发生了 Authenticator 迁移，则将源 BS 的网络标识上报给目标 Authenticator，通过目标 Authenticator 从源 Authenticator 获取建立安全通道所需的密钥信息，从而建立安全通道;否则，直接从源 Authenticator 获取密钥信息建立安全通道。

实施例 5:

如果允许目标 BS 直接到源 Authenticator 请求密钥信息，而且目标 BS 可以获得源 Authenticator 的网络标识，就可以进一步简化上述实施例 1～4 的方法。

图 6 显示了实施例 5 所述的无线接入网中建立安全通道的方法。如图 6 所示，所述方法在 MSS 切换进入目标 BS 后，包括以下步骤:

E1、目标 BS 从 MSS 的接入消息中获取源 BS 的网络标识;

E2、目标 BS 根据源 BS 的网络标识向源 BS 发送包含 MSS 标识的切换指示请求，要求源 BS 提供源 Authenticator 的网络标识;

对应上述步骤 E1 和 E2，目标 BS 还可以通过如下方法获得源 Authenticator 的网络标识：在源基站接收到移动用户站发送的切换指示后，

将源 Authenticator 的网络标识发送到目标基站；目标基站接收所述源 Authenticator 的网络标识。

E3、源 BS 通过会话响应消息将源 Authenticator 的网络标识通知给目标 BS;

E4、在获得了源 Authenticator 的网络标识后，目标 BS 根据源 Authenticator 的网络标识直接向源 Authenticator 申请该 MSS 的密钥信息;

E5、源 Authenticator 直接将建立安全通道所需的密钥下发给目标 BS，目标 BS 根据接收的密钥信息与 MSS 建立安全通道，然后结束。

上述步骤 E5 所述的密钥信息至少包括该 MSS 的 AK。在目标 BS 得到了与 MSS 相同的 AK 后，就可以与 MSS 派生出其他密钥实现空中接口上数据和管理消息的安全传输。

从上述实施例 1 至实施例 5 所述的方法可以看出，在 MSS 切换导致 Authenticator 发生迁移的情况下，不需要触发 Authentication Server 发起重鉴权过程，就可以在 MSS 和目标 BS 之间迅速建立安全通道，节省了数据和信令的开销，大大减少了建立安全通道的时间，提高了用户的业务质量。

如果上述过程发生故障，出现目标 BS 或目标 Authenticator 无法得到建立安全通道所需的密钥信息，那么目标 Authenticator 就将重新启动现有技术中，由 MSS、目标 BS、目标 Authenticator 和 Authentication Server 共同参与的完整的重新鉴权、授权和密钥信息交换等过程，以在 MSS 和目标 BS 之间建立新的根密钥，新的 AK 以及其他相关密钥，达到建立新的安全通道的目的。

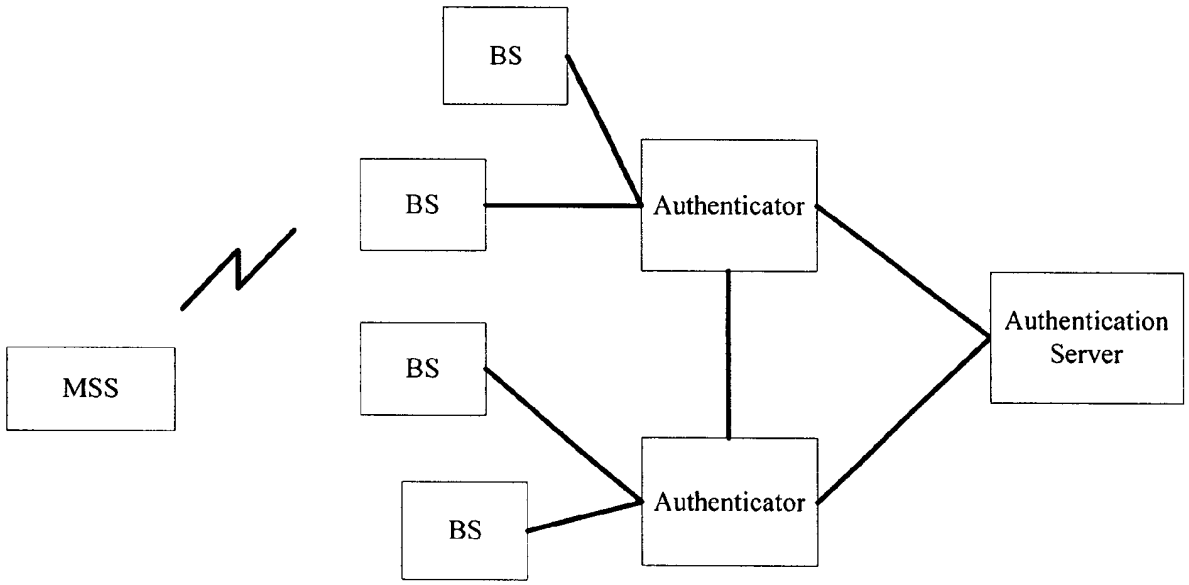

BS
BS
Authenticator
MSS
BS
Authentication Server
BS
Authenticator
BS

图 1

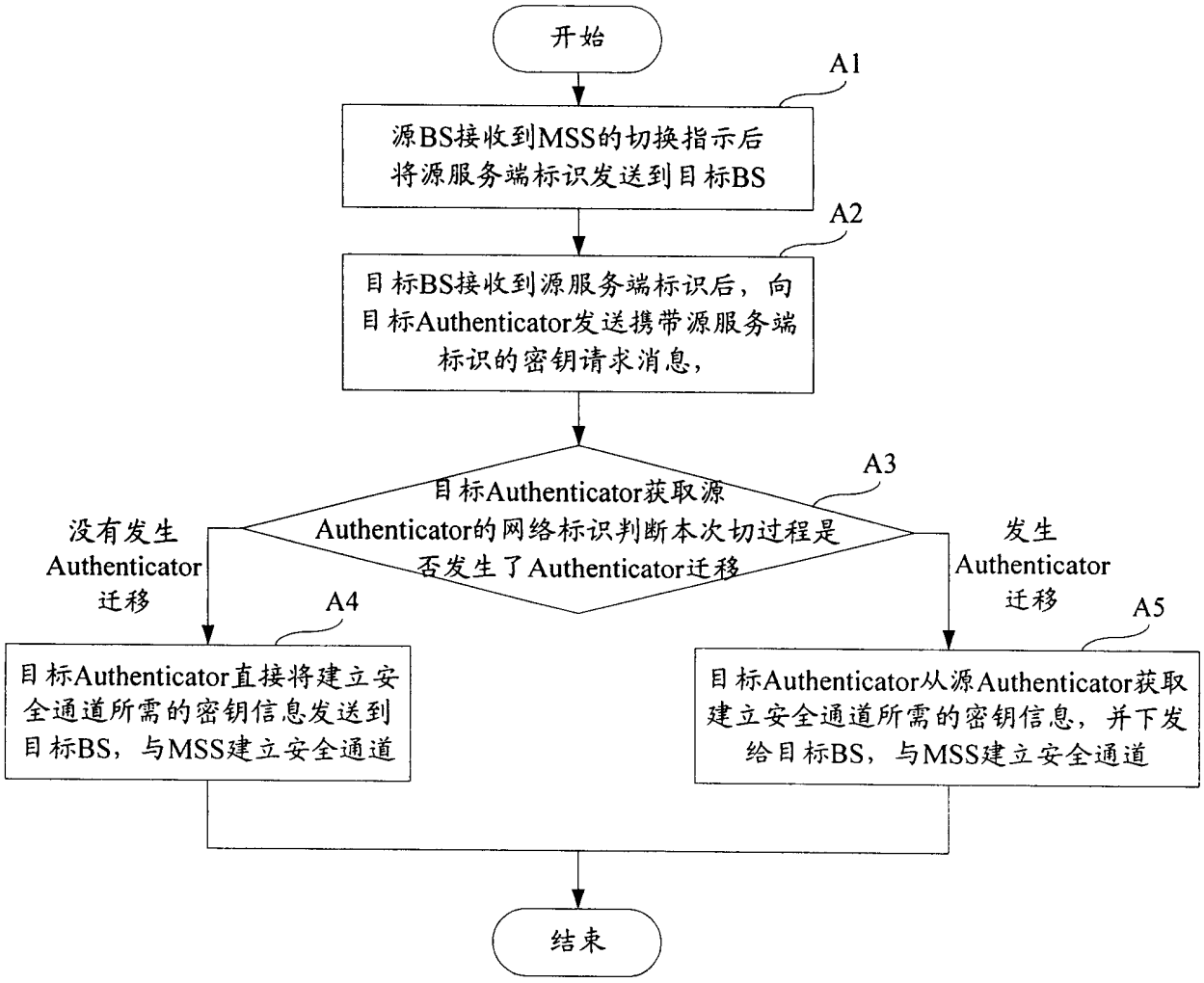

开始
A1
源BS接收到MSS的切换指示后将源服务端标识发送到目标BS
A2
目标BS接收到源服务端标识后，向目标Authenticator发送携带源服务端标识的密钥请求消息，
A3
目标Authenticator获取源Authenticator的网络标识判断本次切过程是否发生了Authenticator迁移
没有发生Authenticator迁移
发生Authenticator迁移
A4
目标Authenticator直接将建立安全通道所需的密钥信息发送到目标BS，与MSS建立安全通道
A5
目标Authenticator从源Authenticator获取建立安全通道所需的密钥信息，并下发给目标BS，与MSS建立安全通道
结束

图 2

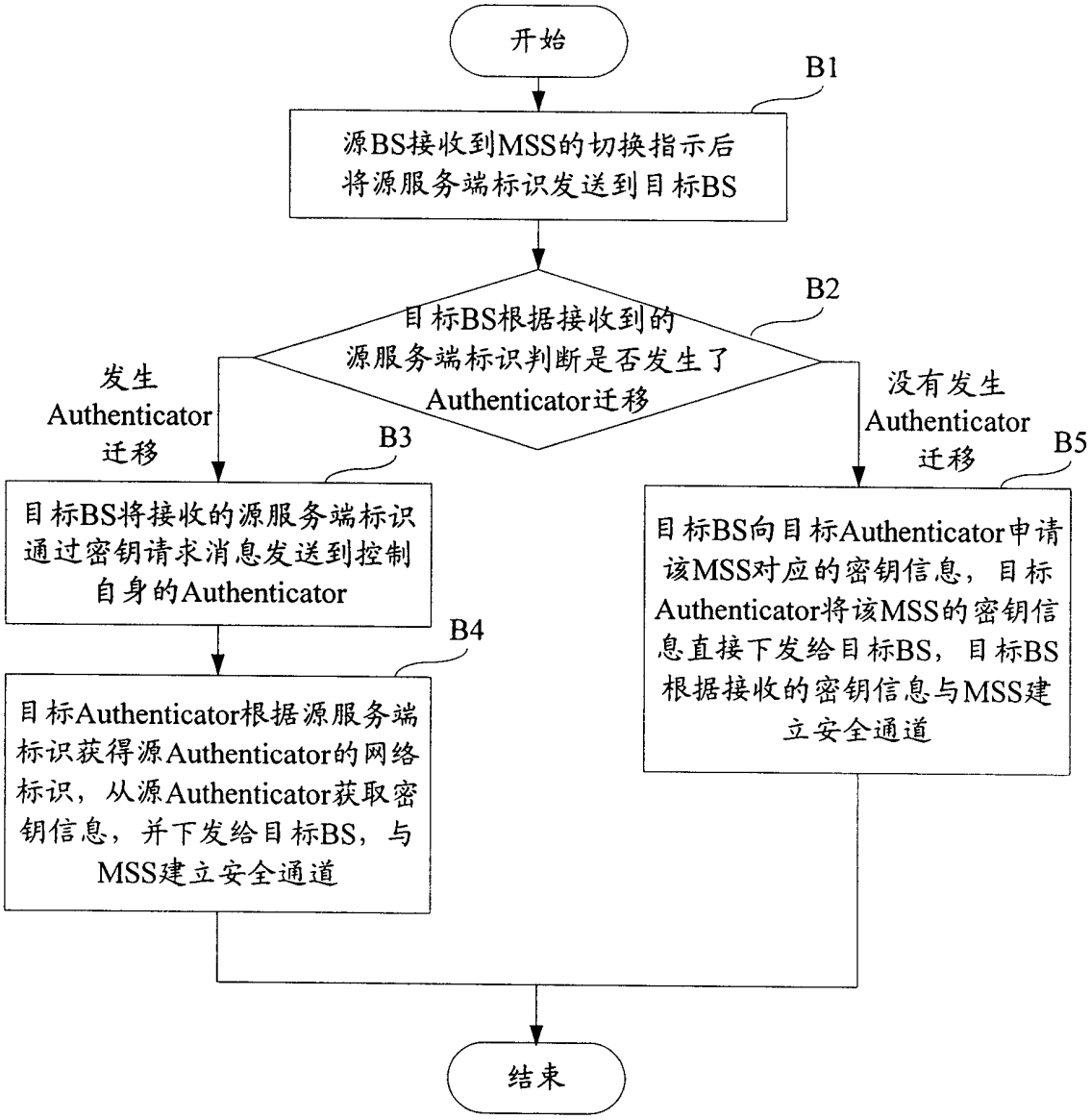

开始
B1
源BS接收到MSS的切换指示后将源服务端标识发送到目标BS
B2
目标BS根据接收到的源服务端标识判断是否发生了Authenticator迁移
发生Authenticator迁移
没有发生Authenticator迁移
B3
目标BS将接收的源服务端标识通过密钥请求消息发送到控制自身的Authenticator
B4
目标Authenticator根据源服务端标识获得源Authenticator的网络标识，从源Authenticator获取密钥信息，并下发给目标BS，与MSS建立安全通道
B5
目标BS向目标Authenticator申请该MSS对应的密钥信息，目标Authenticator将该MSS的密钥信息直接下发给目标BS，目标BS根据接收的密钥信息与MSS建立安全通道
结束

图 3

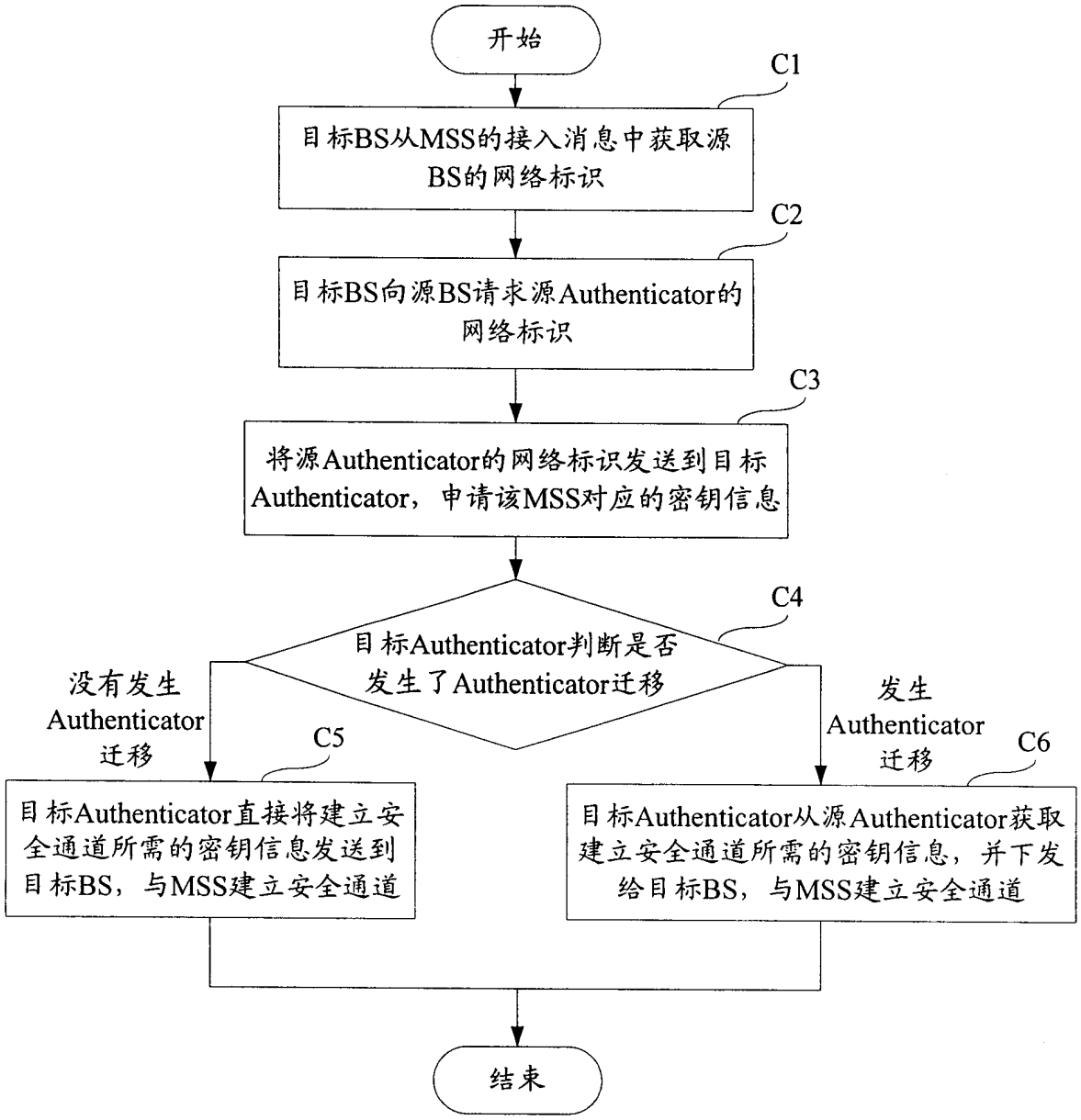

开始
C1
目标BS从MSS的接入消息中获取源BS的网络标识
C2
目标BS向源BS请求源Authenticator的网络标识
C3
将源Authenticator的网络标识发送到目标Authenticator，申请该MSS对应的密钥信息
C4
目标Authenticator判断是否发生了Authenticator迁移
没有发生Authenticator迁移
发生Authenticator迁移
C5
目标Authenticator直接将建立安全通道所需的密钥信息发送到目标BS，与MSS建立安全通道
C6
目标Authenticator从源Authenticator获取建立安全通道所需的密钥信息，并下发给目标BS，与MSS建立安全通道
结束

图 4

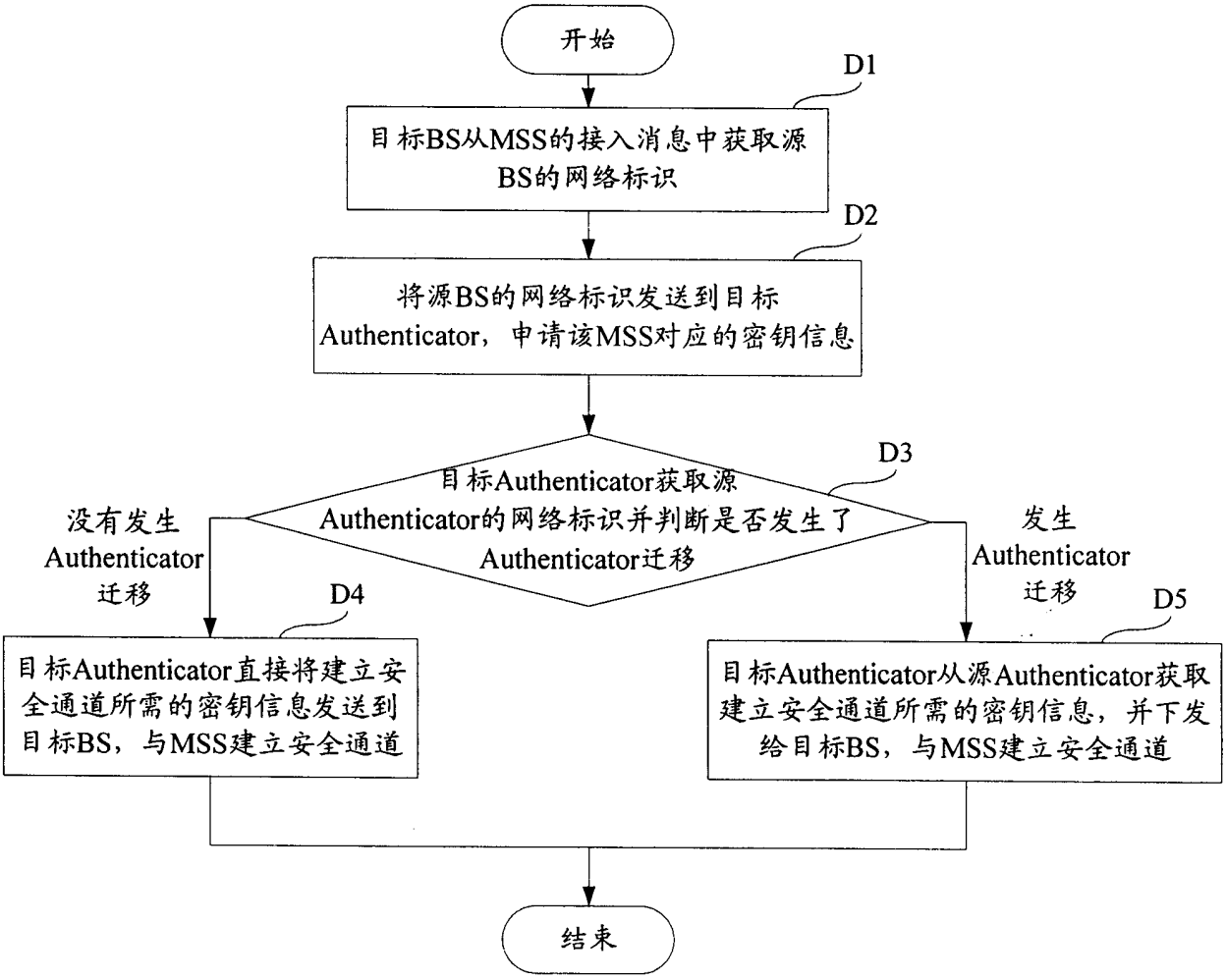

开始
D1
目标BS从MSS的接入消息中获取源BS的网络标识
D2
将源BS的网络标识发送到目标Authenticator，申请该MSS对应的密钥信息
D3
目标Authenticator获取源Authenticator的网络标识并判断是否发生了Authenticator迁移
没有发生Authenticator迁移
发生Authenticator迁移
D4
目标Authenticator直接将建立安全通道所需的密钥信息发送到目标BS，与MSS建立安全通道
D5
目标Authenticator从源Authenticator获取建立安全通道所需的密钥信息，并下发给目标BS，与MSS建立安全通道
结束

图 5

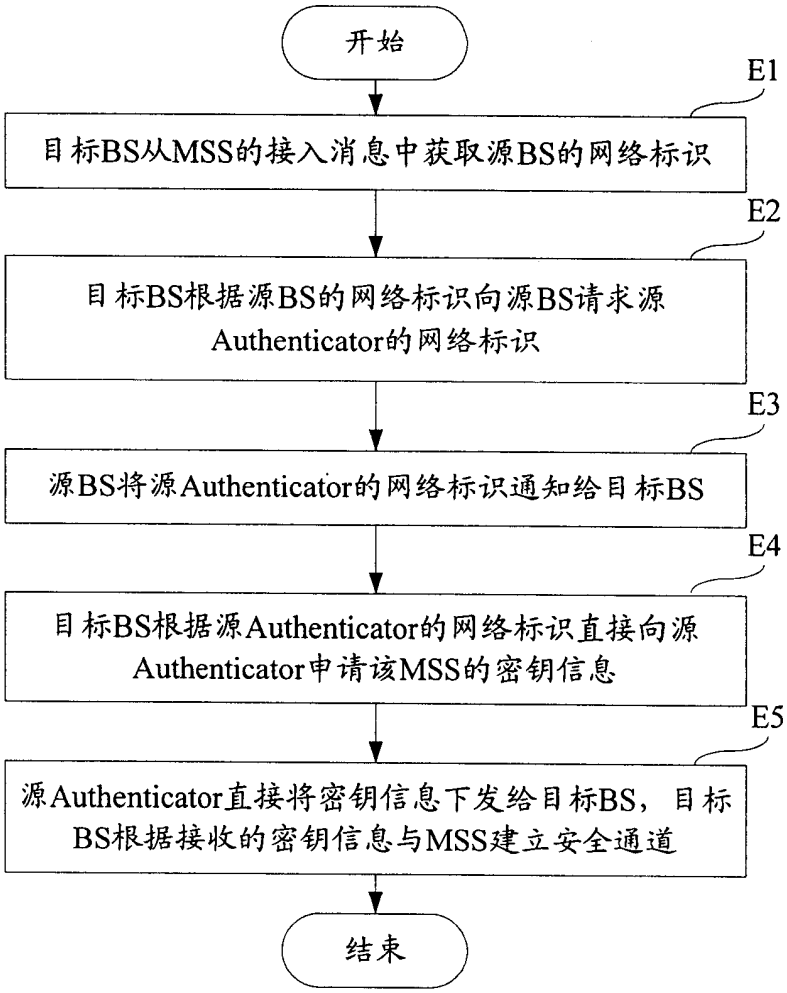

开始
E1
目标BS从MSS的接入消息中获取源BS的网络标识
E2
目标BS根据源BS的网络标识向源BS请求源Authenticator的网络标识
E3
源BS将源Authenticator的网络标识通知给目标BS
E4
目标BS根据源Authenticator的网络标识直接向源Authenticator申请该MSS的密钥信息
E5
源Authenticator直接将密钥信息下发给目标BS，目标BS根据接收的密钥信息与MSS建立安全通道
结束

图 6