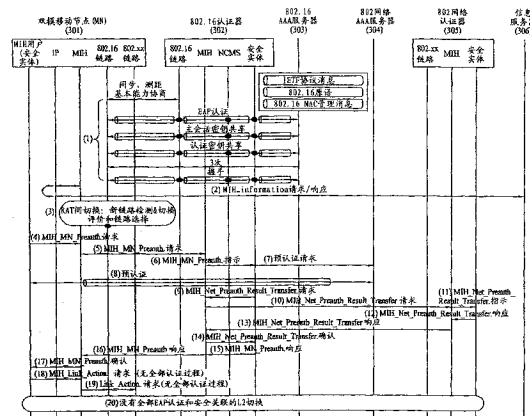




(45) 授权公告日 2014.04.02



1. 一种由多模移动台 MS 在异构无线接入网之间执行切换的方法,该方法包括以下步骤:

获取关于候选目标接入网以及连接到所述多模 MS 的当前接入网的信息;

确定每一个候选目标接入网的网络类型;

当从所述当前接入网接收到的信号电平低于规定的第一阈值时,直接或间接地向所述候选目标接入网中的所选择的目标接入网发送预认证请求消息;

从所选择的目标接入网直接或间接地接收响应于所述预认证请求消息的预认证结果信息;以及

当从所述当前接入网接收到的信号电平低于规定的第二阈值时,使用所述预认证结果信息来执行向所选择的目标接入网的切换而无需任何额外的认证处理,其中所述第一阈值被设置为高于所述第二阈值,

其中在第一类型目标网络的情况下,所述预认证结果信息包括从归属用户服务器 HSS 提取的所述多模 MS 的安全信息,以及在第二类型目标网络的情况下,所述预认证结果信息省略从 HSS 提取的所述多模 MS 的安全信息,

其中所述第一类型目标网络不把可扩展的认证协议 EAP 用作基本认证架构并且支持 EAP- 用户身份模块 SIM 或者 EAP- 认证密钥协议 AKA,而所述第二类型目标网络将 EAP 用作基本认证架构,

其中所述当前接入网的标识符 ID 和所述当前接入网的认证服务器的 ID 排除在所述预认证请求消息和所述预认证结果信息之外,并且

其中在执行所述方法时没有公开所述多模 MS 的 ID,并且所述多模 MS 的 ID 包括国际移动用户标识 IMSI、临时移动用户标识 TMSI 或媒体接入控制 MAC 地址。

2. 根据权利要求 1 所述的方法,其中,使用媒体无关切换 MIH 原语来执行获取信息、发送预认证请求消息、接收预认证结果信息、和执行切换中的至少一项。

3. 根据权利要求 2 所述的方法,其中,使用 MIH 预认证请求原语来执行发送预认证请求消息的步骤,并且其中所述 MIH 预认证请求原语包括以下中的至少一项:所选择的目标接入网的 ID、所选择的目标接入网的认证服务器的 ID、所述多模 MS 的 ID、以及预认证请求指示符。

4. 根据权利要求 2 所述的方法,其中,使用 MIH 预认证响应原语来执行接收预认证结果信息的步骤,并且其中所述 MIH 预认证响应原语包括以下中的至少一项:所述当前接入网的 ID、所述当前接入网的认证服务器的 ID、所选择的目标接入网的 ID、所选择的目标接入网的认证服务器的 ID、所选择的目标接入网的归属用户服务器 HSS 的 ID、预认证结果状态 ID、以及预认证结果传输状态 ID。

5. 根据权利要求 1 所述的方法,其中,如果间接地执行发送和接收,则经由所述当前接入网分别发送和接收所述预认证请求消息和所述预认证结果信息。

6. 根据权利要求 1 所述的方法,其中,由所述多模 MS 的 MIH 实体分别发送和接收所述预认证请求消息和所述预认证结果信息,并且该方法还包括以下步骤:

在所述多模 MS 的所述 MIH 实体发送所述预认证请求消息之前,由该 MIH 实体从所述多模 MS 的 MIH 用户实体接收所述预认证请求消息,以及

在所述 MIH 实体接收到所述预认证结果信息之后,由所述 MIH 实体向所述 MIH 用户实

体通知所述预认证结果信息。

7. 根据权利要求6所述的方法,其中,使用MIH预认证确认原语来执行向所述MIH用户实体通知所述预认证结果信息的步骤,并且其中所述MIH预认证确认原语包括以下中的至少一项:所选择的目标接入网的ID、所选择的目标接入网的认证服务器的ID、预认证结果状态ID、以及预认证结果传输状态ID。

8. 一种由特定接入网支持在异构无线接入网之间进行切换的方法,其中多模移动台MS执行向作为目标接入网的所述特定接入网的切换,该方法包括以下步骤:

从所述多模MS接收预认证请求消息,其中所述预认证请求消息是当多模MS从当前接入网接收到的信号电平低于规定的第一阈值时由所述多模MS发送的;

响应于所述预认证请求消息而向所述多模MS发送预认证结果信息;以及

通过使用所述预认证结果信息来支持所述多模MS执行向所述目标接入网的切换而无需任何额外的认证处理,其中当多模MS从所述当前接入网接收到的信号电平低于规定的第二阈值时,所述多模MS执行切换,其中所述第一阈值被设置为高于所述第二阈值,

其中在第一类型目标网络的情况下,所述预认证结果信息包括从归属用户服务器HSS提取的所述多模MS的安全信息,以及在第二类型目标网络的情况下,所述预认证结果信息省略从HSS提取的所述多模MS的安全信息,

其中所述第一类型目标网络不把可扩展的认证协议EAP用作基本认证架构并且支持EAP-用户身份模块SIM或者EAP-认证密钥协议AKA,而所述第二类型目标网络将EAP用作基本认证架构,

其中所述当前接入网的标识符ID和所述当前接入网的认证服务器的ID排除在所述预认证请求消息和所述预认证结果信息之外,并且

其中在执行所述方法时没有公开所述多模MS的ID,并且所述多模MS的ID包括国际移动用户标识IMSI、临时移动用户标识TMSI或媒体接入控制MAC地址。

9. 根据权利要求8所述的方法,其中,使用媒体无关切换MIH原语来执行接收预认证请求消息和发送预认证结果信息中的至少一项。

10. 根据权利要求9所述的方法,其中,通过所述特定接入网的MIH实体来分别接收和发送所述预认证请求消息和所述预认证结果信息,并且该方法还包括以下步骤:

在所述特定接入网的所述MIH实体接收到所述预认证请求消息之后,经由所述特定接入网的安全实体来将所述预认证请求消息发送至所述特定接入网的认证服务器;以及

在所述MIH实体发送所述预认证结果信息之前,从所述安全实体接收所述预认证结果信息。

用于异构无线接入网间切换的方法

技术领域

[0001] 本发明涉及用于异构无线接入网之间切换的方法,更具体地说,涉及使用预认证过程在异构无线接入网之间执行切换的方法。

背景技术

[0002] 当通信移动台从一个无线接入网移动到另一个无线接入网使得接入点发生改变时,由于切换操作可能会破坏服务的连续性。接入点的改变是指管理域的改变或子网的改变。尤其是,异构无线接入网之间的切换要求新的认证过程。由于执行认证过程而生成的延迟延缓了切换过程的结束,并且其结果是,影响了当前服务的多媒体会话。

[0003] 同时,在电气和电子工程师 (IEEE) 协会 802. 21 标准中,正在对异构网络之间的切换进行积极地讨论。在 IEEE 802. 21 标准中针对媒体无关切换 (MIH, media independent handover) 的范围是为了向链路层提供指令,以及建立将用于优化切换的有关网络信息发送至上位层的标准。其包括 IEEE 802 系列 (后面简称为“802 系列”) 的有线和无线网络,以及由第三代合作伙伴项目 (3GPP)/3GPP2 指定的链路。也就是说,IEEE802. 11 标准的目的在于:通过支持异构网之间的切换 (后面简称为“RAT 间切换”) 来提高用户的便利性,以及支持移动终端和网络中的可用信息的协作使用。为此,网络的接入点 (诸如移动终端或基站) 应该提供多模操作,这意味着支持多种无线标准,并且允许通过一个或更多个无线接口的同时连接。

[0004] 由 IEEE 802. 21 标准定义的 MIH 功能用于作为逻辑实体来确定切换。MIH 功能位于移动终端和网络两者中,并使得移动台和网络能够交换有关移动终端附近的接入网的设置或状态的信息。MIH 功能可以称作“MIH 实体”以与执行其它功能的其它实体进行区分。

[0005] 图 1 例示了移动终端、802 系列网络和 3GPP/3GPP2 网络的协议层结构。

[0006] 多模移动节点 101 可包括根据通信模式的接口。图 1 示出了包括 3GPP/3GPP2 接口 104 和 802 系列接口 105 的移动节点 101。将这些接口分成物理 (PHY) 层和媒体接入控制 (MAC) 层。图 1 中,802 系列网络 102 和 3GPP/3GPP2 网络 103 分别包括接口 106 和 107。

[0007] 同时,被表示为 MIH 功能 108、109 和 110 的 MIH 层位于包括网际协议 (IP) 层之下的上位层。MIH 层不仅定义了 802 系列接口之间的切换,还定义了 IEEE 802 系列接口与由 3GPP/3GPP2 定义的接口之间的切换。也就是说,MIH 功能通过从层 2 (例如,MAC 层) 获取有关其它网络的信息而容易地执行异构网之间的切换处理。

[0008] 图 1 例示了移动节点 101、802 系列网络 102 和 3GPP/3GPP2 网络 103 的上位层功能 111、112 和 113。就 MIH 来说,上位层功能 111、112 和 113 可以称作 MIH 用户或 MIH 用户实体。

[0009] 图 2 例示了基于 MIH 的多模移动终端在异构无线接入网之间的切换处理。

[0010] 图 2 中,当前接入网的多模移动终端 201 在由网络 X 202 提供服务的同时,执行向目标网络的网络 Y 的切换。假设在移动终端 201 中,MAC1201c 和 MAC2201d 是分别与网络 X202 和网络 Y 203 进行层 2 通信的实体。

[0011] 正在通信的多模移动终端 201 在保持与网络 X 202 的连接的同时,从网络 X 202 获得有关相邻网络(例如,网络 Y203)的信息(步骤 S201)。此时,可以通过在 MIH 功能中定义的信息服务来获得与层 2 的安全有关的信息(诸如,认证方法和加密算法)。移动终端 201 通过扫描从相邻网络接收信号并执行网络检测和选择过程(步骤 S202)。

[0012] 同时,如果从服务网络 X 202 接收的信号电平低于规定的电平,则接口 MAC1201c 通过本地事件触发器将该情况报告给上位层的 MIH201b,并通过远程事件触发器将该情况报告给网络 X 202 的 MIH 202b(步骤 S203)。网络 X 202 的 MIH 202b 请求要切换至的网络 Y 202 的 MIH 203b 发送 IP 信息(步骤 S204)。接收到 IP 信息请求的网络 Y 203 通过网络 X202 发送 IP 信息至移动终端 201(步骤 S205)。接收到网络 Y 203 的 IP 信息的移动终端 201 可以预先获得在向相应的网络切换期间要使用的 IP 地址。

[0013] 为了切换至网络 Y 203,移动终端 201 的 MIH201b 命令相应接口的 MAC(即,MAC2 201d)执行层 2 切换的过程(步骤 S206)。然后,移动终端 201 通过实施包括与认证及安全有关的过程的网络初始登记过程来执行向网络 Y 203 的层 2 切换过程(步骤 S207 和 S208)。

[0014] 如果移动终端 201 完成了与网络 Y 203 的层 2 切换(网络登记过程),则移动终端 201 的 MAC2201d 将该情况报告给用于层 3 切换的上位层 201a(步骤 S209)。移动终端 201 执行层 3 切换,该层 3 切换包括向本地代理登记从新的网络(网络 Y 203)获得的转交地址(CoA)的过程。如果完成了切换,则移动终端 201 开始与新的网络进行通信(步骤 S210)。接着,移动终端 201 断开与旧网络(网络 X 202)的连接(步骤 S211)。

[0015] 如上所述,在移动终端执行向新网络的层 2 切换时,IEEE 802.21 中定义的多模移动终端的 RAT 间切换重新执行认证和密钥获取过程。因此,可能出现很大的用户服务延迟,从而有可能损坏数据。

发明内容

[0016] 设计用于解决问题的本发明的目的在于:当多模移动终端执行 RAT 间切换时通过在与目标接入点的链路层切换过程之前执行认证来提供对当前服务的服务质量几乎没有影响的预认证方法以及使用该预认证方法来有效地执行切换的方法。

[0017] 本发明的另一个目的在于提供一种考虑到异构网之间的不同认证类型和不同认证能力而基于 MIH 执行预认证过程的方法。为此,定义了特定过程所需的各种 MIH 原语(primitive)以容易地执行由本发明提出的预认证方法。

[0018] 本发明的一个目的可以通过提供一种由多模移动台(MS)在异构无线接入网之间执行切换的方法来实现。该方法包括以下步骤:获取关于候选目标接入网以及连接到所述多模 MS 的当前接入网的信息;直接或间接地向所述候选目标接入网中的所选择的目标接入网发送预认证请求消息;从所选择的目标接入网直接或间接地接收响应于所述预认证请求消息的预认证结果信息;以及使用所述预认证结果信息来执行向所选择的目标接入网的切换而无需任何额外的认证处理。

[0019] 使用媒体无关切换(MIH)原语来执行获取信息、发送预认证请求消息、接收预认证结果信息、和执行切换步骤中的至少一项。

[0020] 当使用 MIH 预认证请求原语来执行发送预认证请求消息的步骤时,所述 MIH 预认证请求原语可以包括以下中的至少一项:所述当前接入网的标识符(ID)、所述当前接入网

的认证服务器的 ID、所选择的目标接入网的 ID、所选择的目标接入网的认证服务器的 ID、所述多模 MS 的 ID、以及预认证请求指示符。

[0021] 当使用 MIH 预认证响应原语来执行接收时,所述 MIH 预认证响应原语可以包括以下中的至少一项:所述当前接入网的 ID、所述当前接入网的认证服务器的 ID、所选择的目标接入网的 ID、所选择的目标接入网的认证服务器的 ID、所选择的目标接入网的归属用户服务器 (HSS) 的 ID、预认证结果状态 ID、以及预认证结果传输状态 ID。

[0022] 可以根据所述预认证原语和 / 或 MIH 预认证响应原语是否经由当前接入网络被发送至目标接入网络、还是被直接发送至目标接入网络、抑或根据所述目标接入网络的类型来确定参数的选择。

[0023] 如果间接地执行发送和接收,则可以经由所述当前接入网分别发送和接收所述预认证请求消息和所述预认证结果信息。

[0024] 可以由多模 MS 的 MIH 实体分别发送和接收所述预认证请求消息和所述预认证结果信息,并且该方法还包括以下步骤:在多模 MS 的所述 MIH 实体发送所述预认证请求消息之前,由该 MIH 实体从所述多模 MS 的 MIH 用户实体接收所述预认证请求消息,以及在所述 MIH 实体接收到所述预认证结果信息之后,由所述 MIH 实体向所述 MIH 用户实体通知所述预认证结果信息。

[0025] 可以使用 MIH 预认证确认原语来执行向所述 MIH 用户实体通知所述预认证结果信息的步骤,并且其中所述 MIH 预认证确认原语可以包括以下中的至少一项:所述当前接入网的 ID、所述当前接入网的认证服务器的 ID、所选择的目标接入网的 ID、所选择的目标接入网的认证服务器的 ID、预认证结果状态 ID、以及预认证结果传输状态 ID。

[0026] 在本发明的另一个方面,这里提供了一种由特定接入网支持在异构无线接入网之间进行切换的方法,其中多模移动台 (MS) 执行向作为目标接入网的所述特定接入网的切换,该方法包括以下步骤:从所述多模 MS 接收预认证请求消息;响应于所述预认证请求消息而向所述多模 MS 发送预认证结果信息;以及通过使用所述预认证结果信息来支持所述多模 MS 执行向所述目标接入网的切换而无需任何额外的认证处理。

[0027] 可以使用媒体无关切换 (MIH) 原语来执行接收预认证请求消息和发送预认证结果信息步骤中的至少一项。

[0028] 可以通过所述特定接入网的 MIH 实体来分别接收和发送所述预认证请求消息和所述预认证结果信息,并且该方法还可以包括以下步骤:在所述特定接入网的所述 MIH 实体接收到所述预认证请求消息之后,经由所述特定接入网的安全实体来将所述预认证请求消息发送至所述特定接入网的认证服务器;以及在所述 MIH 实体发送所述预认证结果信息之前,从所述安全实体接收所述预认证结果信息。

[0029] 在本发明的再一方面,这里提供了一种由特定接入网支持在异构无线接入网之间进行切换的方法,其中多模移动台 (MS) 执行向不同于该特定接入网的目标接入网的切换。该方法包括以下步骤:从所述多模 MS 接收预认证请求消息;响应于所述预认证请求消息而向所述目标接入网发送预认证结果信息;从所述目标接入网接收响应于所述预认证结果信息的响应消息,以及向所述多模 MS 发送预认证响应消息,其中,所述预认证响应消息包括所述预认证结果信息和关于所述目标接入网的响应消息的信息。

[0030] 可以使用媒体无关切换 (MIH) 原语来执行接收预认证请求消息、发送预认证结果

信息、接收响应消息、和发送预认证响应消息步骤中的至少一项。

[0031] 可以在所述特定接入网的 MIH 实体中执行接收预认证请求消息、发送预认证结果信息、接收响应消息和发送预认证响应消息的步骤，并且该方法还包括：在所述特定接入网的所述 MIH 实体接收到所述预认证请求消息之后，经由所述特定接入网的安全实体向所述目标接入网的认证服务器发送所述预认证请求消息；以及在所述 MIH 实体向所述目标接入网发送所述预认证结果信息之前，从所述安全实体接收所述预认证结果信息。

[0032] 所述特定接入网的所述 MIH 实体可以使用 MIH 预认证指示原语来将所述预认证请求消息发送至所述安全实体，并且所述 MIH 预认证指示原语可以包括以下中的至少一项：所述特定接入网的 ID、所述特定接入网的认证服务器的 ID、所述目标接入网的 ID、所述目标接入网的认证服务器的 ID、所述多模 MS 的 ID、以及预认证请求指示符。

[0033] 可以使用 MIH 预认证结果请求原语来执行接收所述预认证结果信息的步骤，并且所述 MIH 预认证结果传输请求原语可以包括以下中的至少一项：所述特定接入网的 ID、所述特定接入网的认证服务器的 ID、所述目标接入网的 ID、所述目标接入网的认证服务器的 ID、预认证结果状态信息、所述多模 MS 的 ID、针对重新认证的 ID、以及由所述目标接入网中的认证单元使用的安全上下文。

[0034] 可以使用 MIH 预认证结果传输响应原语来执行接收所述响应消息的步骤，并且所述 MIH 预认证结果传输响应原语可以包括以下中的至少一项：所述目标接入网的 ID、所述目标接入网的认证服务器的 ID、所述目标接入网的归属用户服务器 (HSS) 的 ID、所述多模 MS 的 ID、针对重新认证的 ID、预认证结果传输状态指示符、以及由所述目标接入网中的认证单元使用的安全上下文中的没有获得的信息列表。

[0035] 根据本发明的示例性实施方式，当多模移动终端执行 RAT 间切换时可以通过在与目标接入点的链路层切换过程之前执行认证来提供对当前服务的服务质量几乎没有影响的预认证方法以及使用该预认证方法来有效地执行切换的方法。

附图说明

[0036] 附图被包括进来以提供对本发明的进一步理解，附图例示了本发明的实施方式，并与说明书一起用于解释本发明的原理。

[0037] 在附图中：

[0038] 图 1 例示了移动终端、802 系列网络、和 3GPP/3GPP2 网络的协议层结构；

[0039] 图 2 例示了由基于 MIH 的多模移动终端在异构无线接入网之间进行的切换过程；

[0040] 图 3 例示了根据本发明的一个示例性实施方式的由 IEEE 802.16 网络服务的多模移动终端经由当前接入网来执行预认证接着执行向另一个 IEEE 802 系列网络的 RAT 间切换的处理；

[0041] 图 4 例示了根据本发明的另一个示例性实施方式，在未介入当前链路的情况下通过由 IEEE 802.16 网络服务的多模移动终端来直接执行与目标链路的预认证接着执行向 IEEE 802 系列网络的 RAT 间切换的处理；以及

[0042] 图 5 和图 6 例示了根据本发明的另一个示例性实施方式的当移动节点执行从 IEEE 802 系列网络向 3GPP 网络的切换时执行预认证的处理。

具体实施方式

[0043] 下面将参照附图具体介绍本发明的示例性实施方式。以下参照附图给出的详细描述旨在解释本发明的示例性实施方式,而不是示出根据本发明可以实施的仅有实施方式。以下详细描述包括具体细节以提供对本发明的彻底理解。但是,对本领域的技术人员来说很明显的是,可以在无需这些具体细节的情况下实现本发明。例如,以下描述是将 IEEE 802.16 系统作为当前接入网并将 802 系列系统或 3GPP/3GPPS 系统作为目标接入网进行的说明。但是,根据同样的原则,预认证方法和使用该预认证方法的切换方法可以应用于任何不同异构网之间的切换。

[0044] 同时,在一些示例中,为了不对本发明的概念造成模糊,省略了公知的结构和设备,或者将这些公知的结构和设备示出为框图的形式,而重点关注于结构和设备的重要特征。本说明书中通篇使用相同的参考标号来指代相同或类似的部分。

[0045] 本发明提供了基于 MIH 的预认证方法,该方法通过在 RAT 间切换期间,在多模移动终端与目标接入点执行链路层切换过程之前执行认证而对当前服务的服务质量 (QoS) 的影响尽可能的小。在考虑单个管理域的异构环境中,可以支持切换而无需认证服务器。但是,在由多个管理域运行的异构环境中,因为认证服务器根据认证类型和能力而生成不同的认证结果,因此,应当定义灵活且有效的安全机制。例如,当在使用基于可扩展的认证协议 (EAP) 认证的 IEEE 802.11 网络与 IEEE 802.16 网络之间发生切换时,如果由单个服务供应商运行两个接入网,则不存在与切换有关的问题。但是,如果由多个服务供应商来运行异构无线接入网,由于不能使用没有通过认证服务器的切换机制,则必须解决这种问题。

[0046] 本发明提出了以下方法:当将 EAP 用作认证架构的 IEEE 802.16 无线接入网的多模移动终端执行向另一个 IEEE 802 系列无线接入网(诸如,使用基于 EAP 认证架构的无线 LAN) 的切换时,或者,当移动终端执行向不将 EAP 用作基本认证架构的非 IEEE 系列无线接入网(例如,3GPP 网络)的切换时,在移动终端执行向目标网络接入点的链路层切换之前执行预认证,并设置用于通信的密钥材料。因为多模移动终端在接入新的接入点之前提前执行了耗时的针对相应移动终端的认证过程,因此建立了快速的安全关联且减少了 QoS 的恶化。在下面的说明书中,虽然将 IEEE 802.16 网络作为开始切换的接入网的示例进行描述,但是也可以采用其它的 IEEE 802 系列(例如,802.11) 网络。

[0047] 本发明提出的方法适于应用于 IEEE 802.21 标准。也就是说,到目前为止,IEEE 802.21 标准没有提及有关安全的问题,因此本发明可作为改进该标准的技术。但是,下面介绍的基于 MIH 的预认证方法和使用该方法的 RAT 间切换方法不但可应用于 IEEE 802.21 标准,而且还可以应用于其它标准。

[0048] 根据本发明提出的预认证用于提前通过请求相邻接入点以及当前接入点允许认证来从至少一个接入点中获得认证。也就是说,作为常规预认证的概念的扩展,预认证用于在发生 RAT 间切换时提前获得不是来自当前接入网而是来自相邻目标接入网的认证。接着,目标接入网的认证器在预认证的最终步骤中可以获得与相应的移动终端有关的密钥材料,并且移动终端提前从目标接入网获得认证,同时获得密钥材料。

[0049] 为了提高切换的能力,设计本发明用于提供接入技术中的通用技术,在该技术中安全机制的优化不同,为此,考虑使用上述的 MIH。

[0050] 本发明的预认证方法不处理由单个服务供应商(管理域)运营的网络之间的 RAT

间切换,而是处理由不同服务供应商(管理域)运营的网络之间的 RAT 间切换。也就是说,假设打算切换的服务认证器和目标认证器是基于不同服务供应商网络的不同接入技术。在这种情况下,本发明使得移动终端能够在连接目标接入点之间提前获得认证,并设置用于通信的安全密钥。因为预认证过程假设使用 MIH 功能,因此可以与接入技术无关地应用于各种情况。

[0051] 在本发明中,因为在由不同管理域运营的不同网络之间进行 RAT 间切换期间通过多模移动终端的 MIH 来执行预认证的过程,所以减小了在常规技术中当重新执行认证时出现的负载延迟,并且可以执行快速切换过程。因此,本发明定义了用于减小服务连续性损害或 QoS 的恶化的方法。这包括以下方法:在链路层切换结束之前,向目标网络的认证器以及移动终端发送在 RAT 间切换期间要在目标网络中使用的用于通信的密钥材料。

[0052] 如上所述,本发明适于应用于 IEEE 802.21 标准。也就是说,由于 IEEE 802.21 标准没有介绍用于 MIH 的认证和安全关联设置方法,因此如果通过经由 IEEE 802.21 的 MIH 执行预认证来执行不同网络之间的 RAT 间切换,能够提供在 QoS 方面具有最少的影响的连续服务。本发明可以应用于由不同服务供应商运营的网络之间进行 RAT 间切换的情况,而不是由相同服务供应商运营的 RAT 间切换的情况。但是,所提出的方法可以应用于除 IEEE 802.21 之外的其它标准以获得相同的效果。

[0053] 所提出的预认证方法基本上基于使用 IEEE 802.21 的信息服务以获得诸如相邻网络的检测或相邻网络间的漫游协议的信息。也就是说,移动终端可以从 IEEE 802.21 信息服务器获得关于在移动终端的附近存在哪些候选网络的信息。移动终端在连接到目标接入点之前,通过从信息服务器获得的信息而结束预认证过程,并且可以提前设置密钥材料。因此,可以减少在切换期间生成的延迟。

[0054] 理想的是,IEEE 802.21 标准在 RAT 间的 MIH 期间考虑到了安全(诸如,认证和密钥交换方法)。也就是说,需要一种向执行 RAT 间切换的移动终端提供连续服务而不对网络造成严重负载的方法。

[0055] 下面,对本发明提出的各种 MIH 原语进行说明以提供用于执行以下操作方法:按照移动终端来执行预认证、使用该预认证来执行切换、以及根据服务网络和/或目标网络来支持移动终端的 RAT 间切换。虽然 MIH 原语包括具体细节以使本领域的技术人员容易地实施本发明,但是可以按照与以下描述不同的方式来定义这些原语名称中的选择信息以及原语的说明。

[0056] 本发明考虑使用 IEEE 802.21 标准中提供的以下原语来获得移动终端要执行切换到至少一个相邻候选接入网的类型、或者其它有关信息。

[0057] 【表 1】

[0058]

原语	描述
MIH_information 请求	1) 在 IEEE 802.21 标准中定义的远程 MIH 原语。从移动终端的 MIH 传输到当前服务网络的 MIH。用于移动终端请求关于切换的网络的信息,并且可以用于辨别对应网络支持的认证类型。 2) 原语的结构 MIH_information 请求{ InfoQueryFilter:信息请求网络的类型(例如, 802、GSM、CDMA 等) InforQueryParameters:请求信息的特定参数(例如, 链路层信息、上位层信息、安全有关的信息等)}
MIH_information 响应	1) 对 MIH_information 请求原语的响应。由 MIH 用于向移动终端提供网络信息。包括: 可用网络的列表、地理位置信息、传输技术信息、网络供应商标识符、网络供应商名称、IP 版本、漫游伙伴列表、服务等级列表、相邻网络的信息、链路层安全信息、链路层 QoS 参数、路由器信息等。 2) 通过从移动终端接收 MIH_information 请求并发送 MIH_information 响应来提供服务网络的相邻网络信息,并且即使在移动终端正常地与服务网络通信时,

[0059]

	通过以广播的形式周期性地发送 MIH_information 响应至移动终端来获得有关相邻网络的信息。 3) 原语的结构 MIH_information 响应{ InfoQueryFilter:网络的类型(例如, 802、GSM、CDMA 等) MIH_REPORT:信息的特定参数(例如, 相邻信息、支持链路层安全、链路 QoS 参数等) Status:信息传输状态(例如, 成功, 失败) }
--	---

[0060] 也就是说,为了在保持与当前链路的连接同时获得有关相邻网络的信息,通信移动终端可以通过表 1 所示的 MIH 功能中定义的 MIH_information 请求/响应原语来获得与层 2 安全有关的信息(诸如认证方法和加密算法)。

[0061] 同时,本发明提出了通过指定以下的 MIH 原语来请求希望切换的、且由另一个服务供应商运营的目标无线接入网执行预认证,并且当成功地实施了预认证时获得要在相应网络中使用的密钥材料。

[0062] 【表 2】

[0063]

原语	说明
MIH_MN_Preauth 请求	1) 由移动终端的 MIH 用户 (安全实体) 传输到 MIH 功能的原语, 用于请求目标认证服务器执行预认证。接收到该原语的 MIH 功能生成包括该原语内的参数的远程消息的 MIH_MN_Preauth 请求并将该 MIH_MN_Preauth 请求发送至当前链路的认证器的 MIH 功能。 2) 原语结构 MIH_MN_Preauth 请求 { 当前链路标识符 当前认证服务器标识符 目标链路标识符 目标认证服务器标识符 移动终端标识符 (例如, MAC 地址、IMSI 等) 预认证请求指示 }
MIH_MN_Preauth 指示	1) 原语通过当前链路的认证器的 MIH 功能向 MIH 用户通知从移动终端接收到了 MIH_MN_Preauth 请求消息。接收到该原语的 MIH 用户发送预认证请求消息至当前链路的 AAA 服务器, 该预认证请求消息被发送至目标链路的 AAA 服务器。 3) 原语结构 MIH_MN_Preauth 指示 { 当前链路标识符

[0064]

	当前认证服务器标识符 目标链路标识符 目标认证服务器标识符 移动终端标识符 (例如, MAC 地址、IMSI 等) 预认证请求指示 }
--	--

[0065] 【表 3】

[0066]

原语	说明
MIH_MN_Preauth 响应	1) 为了针对移动终端请求的预认证过程而向 MIH 功能通知从目标链路的认证服务器生成的预认证, 由当前链路的认证器的 MIH 用户发送至 MIH 功能的原语。接收到该原语的 MIH 功能生成包括该原语内的参数的远程消息的 MIH_MN_Preauth 响应并向移动终端的 MIH 功能发送该 MIH_MN_Preauth 响应。该原语可包括与网络唯一安全有关的上下文。 2) 原语结构 <pre> MIH_MN_Preauth 响应{ 当前链路标识符 当前认证服务器标识符 目标链路标识符 目标认证服务器标识符 目标 HSS 标识符 预认证结果指示 (例如, 成功, 失败) 受保护的化名 (pseudonym) (例如, TMSI、针对重新认证的 ID 等) }</pre>
MIH_MN_Preauth 确认	1) 由移动终端的 MIH 功能用于向 MIH 用户通知已经接收到 MIH_MN_Preauth 响应的原语。该原语包括 MIH_MN_Preauth 响应中包含的参数, 用于向移动终端的 MIH 用户提供来自目标链路的认证服务器的认证是否成功的结果。该原语可包括与网络唯一安全有关的上下文。 2) 原语结构 <pre> MIH_MN_Preauth 确认 { 当前链路标识符 当前认证服务器标识符 目标链路标识符 目标认证服务器标识符 预认证结果指示 (例如, 成功, 失败) 受保护的化名 (pseudonym) (例如, TMSI、针对重新认证的 ID 等) }</pre>

[0067] 也就是说, 移动终端可使用表 2 中的 MIH_MN_Preauth 请求和 MIH_MN_Preauth 指示原语来请求由不同管理域运营的目标链路的认证服务器执行预认证, 并且这些原语被传输至目标链路的 AAA 服务器以针对移动终端执行预认证。具体而言, 可以通过 IETF 协议来执行对移动终端的预认证过程。在各个示例性实施方式中将介绍各个参数的使用。

[0068] 同时, 当前链路的认证器使用表 3 中示出的 MIH_MN_Preauth 响应 / 确认原语来向移动终端发送由目标链路的认证服务器传输来的、针对特定移动终端的预认证结果。也就是说, 通过当前链路的认证器和认证服务器来将移动终端的预认证请求发送至其它服务供应商的目标认证服务器, 或者, 直接通过目标链路的认证器将移动终端的预认证请求发送

至其它服务供应商的认证服务器。接收到预认证请求的目标链路的认证服务器执行预认证并将预认证的结果发送至服务链路的认证服务器。预认证的结果最终由服务链路的认证服务器经由当前链路的认证器发送至移动终端,或者被直接发送至移动终端。

[0069] 同时,本发明还提出将以下原语作为用于发送特定移动终端的预认证结果以及由于根据网络的预认证而生成的密钥材料的 MIH 原语。

[0070] 【表 4】

[0071]

原语	说明
MIH_Net_Preauth_Result_Transfer 请求	1) 由当前链路的认证器的 MIH 用户发送至 MIH 功能的原语,用于向目标链路的认证器发送特定移动终端的认证结果以及密钥材料以由移动终端执行预认证。接收到该原语的 MIH 功能生成远程 MIH 协议消息的 MIH_Net_Preauth_Result_Transfer 请求并将该远程 MIH 协议消息的 MIH_Net_Preauth_Result_Transfer 请求发送至目标链路的认证器。 2) 原语结构 MIH_Net_Preauth_Result_Transfer 请求{ 当前链路标识符 当前认证服务器标识符 目标认证服务器标识符 预认证结果状态(例如,成功,失败) 移动终端标识符(例如,MAC 地址,IMSI 等) 受保护的化名(例如,TMSI、重新认证 ID) 密钥材料:由目标链路的认证器使用并且可以用于对移动终端与网络之间的安全关联进行设置的安全上下文。

[0072]

MIH_Net_Preauth_Result_Transfer 指示	1) 用于由目标链路的认证器的 MIH 功能向 MIH 用户通知已经从当前链路的认证器的 MIH 中接收到 MIH_Net_Preauth_Result_Transfer 请求的原语。接收到该原语的 MIH 用户生成作为用于向 MIH 功能通知预认证结果的原语的 MIH_Net_Preauth_Result_Transfer 响应并发送该 MIH_Net_Preauth_Result_Transfer 响应。 2) 原语结构 MIH_Net_Preauth_Result_Transfer 指示 { 目标认证服务器标识符 目标 HSS 标识符 预认证结果状态 (例如, 成功, 失败) 移动终端标识符 (例如, MAC 地址, IMSI 等) 受保护的化名 (例如, TMSI、重新认证 ID) 密钥材料: 由目标链路的认证器使用并且可以用于对移动终端与网络之间的安全关联进行设置的安全上下文。 }
---	---

[0073] 【表 5】

[0074]

原语	说明
MIH_Net_Preauth_Result_Transfer 响应	1) 由目标链路的认证器的 MIH 用户传输至 MIH 功能的原语, 并且该原语用于通知是否已经正常发送了特定移动终端的认证结果以及密钥材料。通过该参数发送的参数包括用于预认证结果的传输请求的状态以及相关的密钥材料, 并且包括没有被正常发送的密钥材料的列表。接收到该原语的 MIH 功能生成 MIH_Net_Preauth_Result_Transfer 响应并向服务链路的认证器的 MIH 发送该 MIH_Net_Preauth_Result_Transfer 响应。 2) 原语结构 MIH_Net_Preauth_Result_Transfer 响应 { 目标链路标识符 目标认证服务器标识符 目标 HSS 标识符 移动终端标识符 (例如, MAC 地址, IMSI 等) 受保护的化名 (例如, TMSI, 重新认证 ID) 没有获得的密钥材料的列表 预认证结果传输状态 (例如, 成功, 失败) }
MIH_Net_Preauth_Result_Transfer 确认	1) 用于由服务链路的认证器的 MIH 向 MIH 用户通知已经接收到 MIH_Net_Preauth_Result_Transfer 响应的原语。该原语中包含的参数如下: 2) 原语结构

[0075]

	MIH_Net_Preauth_Result_Transfer 确认{ 目标链路标识符 移动终端标识符 (例如, MAC 地址, IMSI 等) 没有获得的密钥材料的列表 预认证结果传输状态 (例如, 成功, 失败) }
--	---

[0076] 具体而言,表 4 例示了用于发送特定移动终端的预认证结果以及由于预认证而生成的密钥材料的原语。表 5 例示了目标链路的认证器用来向当前链路的认证器通知是否已经通过表 4 所示的原语发送了相应移动终端的预认证结果和密钥材料的原语。

[0077] 同时,示例性的实施方式提出要实现根据本发明所提出的方法可以满足以下条件。

[0078] 1) 由无线接入技术 (诸如,3GPP/3GPP2) 中的移动终端和网络长期共享的安全凭证可以保存在多模移动终端的用户身份模块 (SIM) 卡或通用集成电路卡 (UICC :universal integrated circuit card) 中。

[0079] 2) 可以提供针对服务网络与目标网络之间交换的有关预认证的信令或针对密钥材料的保护。

[0080] 3) IEEE 802.16 网络可以签订与 3GPP 网络或其它异构网络互联的漫游协议。

[0081] 4) 为了保护用户标识符 (例如, IMSI, TMSI 和 MAC 地址),可以不公开这些标识符。

[0082] 如上所述,服务接入网的移动终端在执行到目标接入网的切换之前,使用 MIH 信息服务经由服务接入网与目标接入网执行预认证,或者经由目标接入网直接执行预认证。移动终端可以与一个或更多个接入网执行预认证。各个接入网运行不同的认证、授权和计费 (AAA :Authentication, Authorization, and Accounting) 服务器。在 AAA 服务器中包括用于认证的 EAP 服务器功能。可以通过远程认证拨入用户服务 (RADIUS :RemoteAuthentication Dial-In User Service) 或对 RADIUS 的改进的 AAA 协议 (诸如 diameter) 来实现认证器与认证服务器之间的通信。

[0083] 如果目标认证器使用基于 EAP 的主会话密钥 (MSK :master sessionkey) 来生成链路层 (诸如, IEEE 802.16 或 IEEE 802.11 网络) 的密钥,则预认证过程可以通过生成目标认证器的 MSK 来在移动终端与网络 (基站或接入点) 之间设置安全关联。

[0084] 本发明提出在移动终端、服务认证器、目标认证器和认证服务器之间的两种形式的预认证方法。根据服务认证器如何与预认证信令相关,预认证的方法有所不同。也就是说,本发明提出了以下直接的预认证方法和间接的预认证方法。

[0085] 首先,在直接预认证方法中,在移动终端与目标认证器之间透明地交换预认证信令,并且经由目标认证器将该信令传输到目标认证服务器。接着,在间接的预认证方法中,服务认证器与预认证信令相关,并且此方法是作为当出于安全的原因不允许目标认证器与移动终端之间的 IP 通信时的必要技术而提出的。也就是说,间接预认证信令被分成移动终端与服务认证器之间的信令以及服务认证器与目标认证器之间的信令。服务认证器与目标认证器之间的信令包括服务接入网的认证服务器以及目标接入网的认证服务器。

[0086] 下面将参照附图具体说明使用上述示例的间接预认证的示例性实施方式。

[0087] 图 3 例示了根据本发明的一个示例性实施方式的由 IEEE 802.16 网络服务的多模移动终端经由当前接入网来执行预认证接着执行向另一个 IEEE 802 系列网络的 RAT 间切换的处理。

[0088] 图 3 中,当前链路的认证器经由当前链路的认证服务器发送移动终端的预认证请求至目标链路的认证服务器。接收到该请求的目标链路的认证服务器针对相应移动终端执行预认证,并经由当前链路的认证器发送预认证的结果给目标链路的认证器。接着,目标链路的认证器将对预认证结果的响应报告给当前链路的认证器。当前链路的认证器将目标链路中要使用的密钥材料作为预认证的结果发送至移动终端。

[0089] 在该示例性实施方式中,由于很难通过修改由当前 IETF 定义的 AAA 架构来增加 MIH 功能,因此假设认证服务器不支持 MIH 功能。但是,本发明不排除通过由认证服务器支持 MIH 功能来直接交换对应的 MIH 原语的概念。

[0090] 在执行预认证的两种形式中,图 3 例示了通过服务链路的认证器来发送预认证请求,并且在这种情况下,可以有选择地使用表 2 和表 3 中定义的 MIH 原语。也就是说,不是始终使用表 2 中的原语,可以排除当前链路标识符和当前认证服务器标识符的参数。类似地,可以排除表 3 中提出的原语中的以上两个参数。

[0091] 将基于以上说明来介绍图 3 中例示的各个过程。

[0092] (1) 首先,步骤 (1) 例示了这样的处理,即,通过基于 EAP 的认证来共享主会话密钥 (MSK) 和认证密钥 (AK),以及通过将多模移动节点 301 接入 IEEE 802.16 网络经由 3 次握手来共享业务加密密钥 (TEK:traffic encryption key)。如果使用除 IEEE 802.16 网络以外的其它 IEEE 802 系列,则可以实施类似形式的基于 EAP 的初始认证过程。

[0093] (2) 正在通信的多模移动节点 301 在保持与 IEEE 802.16 网络的连接的同时,从信息服务器 306 获得有关至少一个相邻候选网络的信息 (步骤 (2))。可以通过之前说明的 MIH 中定义的信息服务 (例如,通过诸如表 1 所示的 MIH_Information 请求 / 响应原语的 MIH 信息请求 / 响应原语) 来获得有关相邻网络的信息。移动节点可以使用这些原语来接收链路层安全有关的参数 (诸如,相邻网络的认证方法 / 加密算法)。例如,由当前管理域运营的 IEEE 802.16 网络 302 的 MIH 可以请求期望切换到的 802 系列网络 305 的 MIH 发送 IP 信息,并且可以发送该 IP 信息至移动节点 301。可以在移动节点的切换期间使用 IP 地址。

[0094] (3) 移动节点 301 通过扫描从相邻网络中接收信号,并执行链路检测 / 选择过程 (步骤 (3))。作为步骤 (3) 的结果,假设作为潜在的切换目标链路的 802 系列网络 305 由不同的管理域来运营。802 系列网络假设包括 IEEE 802.16 网络、IEEE 802.11 网络等。

[0095] (4) 当识别到从 IEEE 802.16 网络接收到的信号电平低于规定的电平时,移动节点 301 发送 MIH 预认证请求原语 (诸如表 2 中提出的 MIH_MN_Preauth 请求) 至该移动节点 301 的 MIH 实体以命令 MIH 实体执行预认证过程 (步骤 (4))。如表 2 所例示的 MIH_MN_Preauth 请求原语,MIH 预认证请求原语可包括:当前链路 302 的标识符、当前认证服务器 303 的标识符、目标链路 305 的标识符、目标认证服务器 304 的标识符、多模移动节点 301 的标识符、以及预认证请求指示符。

[0096] 因此,移动节点 301 的 MIH 用户 (即,MIH 的上位层) 可以请求移动节点 301 的 MIH

发送预认证过程请求至目标链路的 802 系列网络认证服务器 304。可以经由 802.16 网络认证器 302 和 802.16 网络认证服务器 303 来发送预认证过程请求至 802 系列网络认证服务器 304。虽然该实施方式例示了包括 EAP 功能的 AAA 服务器不支持 MIH 的情况,但是本发明不限于此。

[0097] 此外,因为假设在步骤 (4) 中,在实施层 2 切换之前执行预认证过程,所以将在确定从当前链路接收到的信号电平是否低于规定的电平时使用的规定的阈值理想地设置为比用于确定发起层 2 切换的阈值更高的电平。但是,在发起实质的切换过程之前,还可以使用除了用于执行预认证的上述方法之外的各种方法。

[0098] (5) 在步骤 (5) 中,接收到 MIH 预认证请求原语 (诸如 MIH_MN_Preauth 请求原语) 的移动节点 301 的 MIH 生成 MIH 远程协议消息的 MIH_MN_Preauth 请求协议消息并将该消息发送至服务网络的 IEEE 802.16 网络认证器 302 的 MIH (步骤 (5))。该消息可包括步骤 (4) 中的 MIH 预认证请求原语内的参数。

[0099] (6) 接着,IEEE 802.16 网络认证器 302 的 MIH 生成并发送 MIH 预认证指示原语 (诸如表 2 所示的 MIH_MN_Preauth 指示原语) 以向认证器 302 的 MIH 用户通知远程协议消息的接收结果 (步骤 (6))。如表 2 所例示的,MIH 预认证指示原语可包括:当前链路 302 的标识符、当前认证服务器 303 的标识符、目标链路 305 的标识符、目标认证服务器 304 的标识符、多模移动节点 301 的标识符、和预认证请求指示符。

[0100] (7) 在步骤 (7) 中,在步骤 (6) 中接收到 MIH 预认证指示原语的、负责管理认证器 302 的安全的安全实体通过与 IEEE 802.16 网络 302 连接的 AAA 服务器 303 发送预认证请求消息至与目标 802 系列网络 305 连接的 AAA 服务器 304。

[0101] (8) 接着,在移动节点 301 与目标链路的 AAA 服务器 304 之间执行预认证过程 (步骤 (8))。该预认证过程与移动节点 301、服务认证器 302、服务认证服务器 303、以及目标认证服务器 304 相关联。此外,预认证结果被发送至服务认证器 302 的 MIH 用户。在此实施方式中,虽然在服务链路中使用的认证凭证 (credential) 可能与目标链路中使用的认证凭证不完全相同,但是可以通过获得由步骤 (2) 中的 MIH 信息服务所提供的信息来解决这个问题。也就是说,因为移动节点 301 可以通过 MIH 信息请求 / 响应原语来获得有关目标链路中考虑的凭证的信息,所以可以执行预认证过程。

[0102] (9) 目标链路的 IEEE 802 系列 AAA 服务器 304 生成包括预认证过程结果和要在目标链路中使用的密钥材料的预认证响应消息并通过 IEEE 802.16 网络的 AAA 服务器 303 将该响应消息发送至服务链路 302 的安全实体。接收到预认证过程结果和要在目标链路中使用的密钥材料的当前认证器 302 的 MIH 用户生成 MIH 预认证结果传输请求原语 (诸如表 4 中例示的 MIH_Net_Preauth_Result_Transfer 请求原语) 并将该 MIH 预认证结果传输请求原语发送至当前认证器 302 的 MIH (步骤 (9))。如表 4 所例示,MIH 预认证结果传输请求原语可包括:当前链路 302 的标识符、当前认证服务器 303 的标识符、目标链路 305 的标识符、目标认证服务器 304 的标识符 304、预认证结果状态信息 (预认证成功或失败)、多模移动节点 301 的标识符、受保护的安全信息、以及由目标链路的认证单元使用的安全上下文。

[0103] (10) 在步骤 (10) 中,接收到 MIH 预认证结果传输请求原语的当前认证器 302 的 MIH 生成远程协议消息的 MIH_Net_Preauth_Result_Transfer 请求并将该 MIH_Net_Preauth_Result_Transfer 请求发送至目标链路认证器 305 (步骤 (10))。该消息包括步骤

(9) 中的 MIH 预认证结果传输请求原语内的参数。

[0104] (11) 接着,接收到MIH预认证结果传输请求原语的目标认证器 305 的 MIH 生成 MIH 预认证结果传输指示原语(诸如表 4 中的 MIH_Net_Preauth_Result_Transfer 指示原语)以向 MIH 用户通知该消息,并将生成的原语发送至该 MIH 用户(步骤(11))。如表 4 所例示的,所生成的 MIH 预认证结果传输指示原语可包括:MIH 预认证结果传输请求原语中包含的参数的一部分,以及目标认证器 305 的 MIH 用户所需的部分参数。

[0105] (12) 接收到 MIH 预认证结果传输指示原语的目标认证器 305 的 MIH 用户生成 MIH 预认证结果传输响应原语(诸如表 5 中例示的 MIH_Net_Preauth_Result_Transfer 响应)并将该 MIH 预认证结果传输响应原语发送至 MIH,以发送移动节点 301 的预认证过程结果以及由目标链路认证服务器 304 生成的密钥材料的接收结果(步骤(12))。如图 5 所例示的,MIH 预认证结果传输响应原语可包括:目标链路 305 的标识符、目标认证服务器 304 的标识符、目标归属用户服务器(HSS)的标识符、多模移动节点 301 的标识符、预认证 ID、没有获得的密钥材料、以及预认证结果传输状态标识符。在这些参数中,可以省略 HSS 标识符。

[0106] (13) 接收到 MIH 预认证结果传输响应原语的目标认证器 305 的 MIH 生成远程 MIH 原语的 MIH_Net_Preauth_Result_Transfer 响应原语并将该 MIH_Net_Preauth_Result_Transfer 响应原语发送至服务认证器 302(步骤(13))。所生成的原语可包括步骤(12)中的 MIH 预认证结果传输响应原语中包含的参数。

[0107] (14) 作为步骤(13)中提及的接收到 MIH 预认证结果响应原语的结果,服务链路认证器 302 生成 MIH 预认证结果确认原语(诸如表 5 中例示的 MIH_Net_Preauth_Result_Transfer 确认原语)并将该 MIH 预认证结果确认原语发送至 MIH 用户(步骤(14))。

[0108] (15) 服务认证器 302 的 MIH 用户接收步骤(14)所述的 MIH_Net_Preauth_Result_Transfer 确认原语,并向服务认证器 302 的 MIH 发送 MIH 预认证响应原语(诸如表 3 中例示的 MIH_MN_Preauth 响应原语)(步骤(15))。

[0109] (16) 步骤(15)中提及的服务认证器 302 的 MIH 发送远程协议消息的 MIH_MN_Preauth 响应原语至移动节点 301 的 MIH(步骤(16))。该原语可包括步骤(15)中介绍的 MIH_MN_Preauth 响应原语中包含的参数。

[0110] (17) 接收到 MIH_MN_Preauth 响应原语消息的移动节点 301 的 MIH 生成 MIH 预认证确认原语(诸如表 3 中的例示的 MIH_MN_Preauth 确认原语)并将该 MIH 预认证确认原语发送至移动节点 301 的 MIH 用户(步骤(17))。

[0111] (18) 在预认证过程完成之后,与新的网络进行切换,也就是说,从更高管理实体发送发起链路动作过程的命令。在这种情况下,更高管理实体通知可以省略安全有关的过程,该安全有关的过程在诸如新的认证和安全密钥设定时需要大量的载荷,并且有可能导致延迟(步骤(18))。

[0112] (19) 然后,移动节点 301 的 MIH 发送链路动作命令至对应的链路(步骤(19))。

[0113] (20) 多模移动节点 301 执行层 2(L2) 切换(步骤(20))。此时,省略了新的认证过程,而作为步骤(4)至步骤(17)执行的预认证的结果,可以省略在基于服务链路和目标链路的网络实体(认证器和认证服务器)之间交换的信息向目标链路进行登记期间重新执行认证以及设置密钥的处理。

[0114] 如果层 2 切换完成,则移动节点 301 的 MAC 设置与目标链路的接入点的安全关联,

并且可以准备进行通信。

[0115] 参照图 3 解释的上述实施方式示出了当在 IEEE 802.16 网络中被提供的多模移动节点经由服务链路的认证器发送预认证请求并执行向 802 系列网络的切换的情况。但是,对于优化的过程可以省略步骤 (16) 至步骤 (18)。

[0116] 下面,将介绍多模移动节点直接发送到目标链路的认证器以使得目标链路的认证服务器执行预认证的过程的一个示例性实施方式。

[0117] 图 4 例示了根据本发明的另一个示例性实施方式,在未介入当前链路的情况下通过 IEEE 802.16 网络服务的多模移动终端来直接执行与目标链路的预认证,然后执行向另一个 IEEE 802 系列网络的 RAT 间切换的处理。

[0118] 与图 3 相比,图 4 的过程与图 3 的过程基本上相同,所不同的是:多模移动节点 401 直接请求目标认证器 405 和目标认证服务器 404 执行预认证并接收预认证的结果,以及当前认证器 402 和当前认证服务器 403 与目标认证器 405 及认证服务器 404 的预认证处理无关,并且仅实施中继功能。下面,将在当前认证器和当前认证服务器只对层 2 实施中继而不管预认证过程的情况下执行的预处理称作“直接预处理”,而将在当前认证器和认证服务器实质上与预认证过程有关(具体而言,要求层 3 或更多层的关系)的情况下执行的预处理称作“间接预认证”。为了省略重复说明,根据例示了直接预认证过程的图 4 的各个步骤,仅对与图 3 中例示间接预认证的部分不同的部分进行说明。

[0119] 图 4 中,将预认证请求直接发送至目标认证器 405。此时,因为预认证结果被从目标认证服务器 404 发送至目标认证器 405,所以与图 3 不同,可以不使用表 4 和表 5 中定义的原语。下面,根据图 4 的各个步骤,将重点介绍不同于图 3 的部分。

[0120] (1)-(4) 如图 3 的步骤 (1) 至 (4) 所示,多模移动节点 401 可以在与当前链路 402 进行通信的同时,从信息服务器 406 经由 MIH 信息请求/响应原语获得有关至少一个候选接入网的信息。如果从当前链路 402 接收的信号电平小于规定的阈值(例如,高于用于确定发起切换的值的阈值),移动节点 401 的上位层可以命令 MIH 发起预认证过程,并且可以利用结合图 3 介绍的 MIH_MN_Preauth 请求原语来执行预认证过程。

[0121] (5) 接收到 MIH_MN_Preauth 请求的移动节点 401 的 MIH 生成 MIH 远程协议消息的 MIH_MN_Preauth 请求原语并将该 MIH 远程协议消息的 MIH_MN_Preauth 请求原语发送至目标链路的 IEEE 802.16 网络认证器 405 的 MIH。与图 3 不同,假设在不介入服务认证器 402 和服务认证服务器 403 的情况下从移动节点 401 的 MIH 发送 MIH_MN_Preauth 请求原语至目标认证器 405 的 MIH。即,服务链路仅用于在移动节点 401 与目标认证器 405 之间进行中继。

[0122] MIH_MN_Preauth 请求原语可包括步骤 (4) 中接收到的原语内的参数。

[0123] (6) 目标认证器 405 的 MIH 生成 MIH 预认证指示原语(诸如表 2 中例示的 MIH_MN_Preauth 指示)并将该 MIH 预认证指示原语发送至目标认证器 405 的 MIH 用户以向认证器 405 的 MIH 用户通知远程协议消息的接收结果。如表 2 所例示的,MIH 预认证指示原语可包括:当前链路 402 的标识符、当前认证服务器 403 的标识符、目标链路 405 的标识符、目标认证服务器 404 的标识符、多模移动节点 401 的标识符、以及预认证请求指示符。但是,当 MIH 原语被与当前链路无关地直接发送至目标链路时,可以省略当前链路 402 的标识符和当前认证服务器 403 的标识符。

[0124] (7) 接收到 MIH_MN_Preauth 指示原语的认证器 403 的安全实体发送预认证请求消息至与目标 802 系列网络链接的 AAA 服务器 404 (步骤 (7))。

[0125] (8) 接着,除了预认证过程是在没有介入当前认证器 402 和当前认证服务器 403 的情况下移动节点 401、目标认证器 405、和目标认证服务器 404 之间实现的以外,预认证过程基本上与图 3 的预认证过程相同。此外,预认证结果没有被发送至图 3 的当前认证器的 MIH 用户,而是被发送至目标认证器 405 的 MIH 用户。

[0126] (9) 目标认证服务器 404 生成包括预认证过程结果的预认证响应消息并将该响应消息发送至目标 IEEE 802 系列网络认证器 405 的安全实体。接收到预认证过程结果以及要在目标链路中使用的密钥材料的目标认证器 405 的 MIH 用户生成 MIH 预认证响应原语 (诸如表 3 中例示的 MIH_MN_Preauth 响应原语) 并将该响应原语发送至认证器 405 的 MIH。

[0127] (10) 接收到 MIH_MN_Preauth 响应原语的目标认证器 405 的 MIH 生成远程协议消息的 MIH_MN_Preauth_Response 原语并将该远程协议消息的 MIH_MN_Preauth_Response 原语发送至服务认证服务器 402 的 MIH。该消息可包括 MIH_MN_Preauth 响应原语内的参数。服务认证器 402 的 MIH 接收远程 MIH_MN_Preauth 响应原语消息并将该消息发送至移动节点 401 的 MIH。

[0128] (11)-(14) 接收到 MIH_MN_Preauth 响应原语的多模移动节点 401 的 MIH 生成 MIH 预认证确认原语 (诸如表 3 中例示的 MIH_MN_Preauth 确认) 并将该 MIH 预认证确认原语发送至 MIH 用户。预认证过程结束之后,从更高管理实体发送与新网络进行切换的命令 (即发起链路动作过程)。此时,更高管理实体通知可以省略安全有关的过程,该安全有关的过程在诸如新的认证和安全密钥设定时需要大量的载荷,并且有可能导致延迟。因此,移动节点 401 可以容易地执行切换过程。

[0129] 上述实施方式示出了当在 IEEE 802.16 网络中被提供的多模移动节点经由目标链路的认证器发送预认证请求并执行向 802 系列网络切换的情况。但是,对于优化的过程可以省略步骤 (9) 至步骤 (11)。

[0130] 结合图 3 和图 4 介绍的以上两个实施方式提供了当移动节点使用基于 EAP 的认证架构时在接入网之间的切换。但是,根据本发明的预认证方法和使用该预认证方法的切换方法可以等同地应用于切换到不使用基于 EAP 的认证架构的非 IEEE 802 系列网络 (即,可以应用于 3GPP 网络)。

[0131] 图 5 和图 6 例示了根据本发明的另外示例性实施方式的当移动节点执行从 IEEE 802 系列网络向 3GPP 网络的切换时所执行的预认证的处理。

[0132] 图 5 和图 6 的示例性实施方式示出了当移动节点执行从 IEEE 802.16 网络向诸如 3GPP 网络的非 IEEE 802 系列网络的切换时所执行的预认证过程的处理。也就是说,当存在用于互通的 3GPP AAA 服务器 504 或 604 并且支持基于 EAP 的认证架构时,通过诸如 EAP-AKA 或 SIM 的认证方法来实现预认证。

[0133] 基本的预认证方法和使用该预认证方法的切换方法与图 3 和图 4 中的方法相同。因此,虽然将逐个步骤地介绍图 5 和图 6 的实施方式,但是,将重点介绍与图 3 和图 4 的实施方式的不同之处。

[0134] 图 5 中,移动节点 501 通过图 3 所示的当前链路 502 请求目标链路 506 来执行预认证。

[0135] 多模移动节点 501 接入 IEEE 802.16 网络以执行基于 EAP 的认证（步骤 (1)），并在保持与 IEEE 802.16 网络 502 的连接的同时检测一个或多个候选网络（步骤 (2)）。其后，移动节点 501 如在上述实施方式中那样选择目标链路并通过 MIH 信息请求 / 响应原语从信息服务器 507 获得关于目标链路的信息（步骤 (3)）。假设由不同管理域通过这些原语操作的 非 802 系列网络是切换的目标链路。具体而言，在图 5 中，非 802 系列网络的 3GPP 网络 506 被选择作为目标链路。

[0136] 同时，如果多模移动节点 501 识别出从 IEEE 802.16 网络接收到的信号电平低于规定的电平（例如，该规定的电平高于用来确定切换发起的电平），移动节点 501 的 MIH 用户通过 MIH_MN_Preauth 请求原语来请求移动节点 501 的 MIH 发送预认证过程请求至目标链路的非 802 系列网络认证服务器 504（步骤 (4)）。可以通过 802.16 网络认证器 502 和认证服务器 503 来将预认证过程请求发送至目标链路的非 802 系列网络认证服务器 504。在此实施方式中还假设，与图 3 和图 4 的实施方式一样，包括 EAP 功能的 AAA 服务器 503 不支持 MIH。

[0137] 接收到 MIH_MN_Preauth 请求原语的移动节点 501 经由服务链路的 IEEE 802.16 网络认证器 502 的 MIH 和 MIH 用户（步骤 (5) 和 (6)）来将相应的信息发送至目标链路的 3GPPAAA 服务器 504（步骤 (7)）。在图 5 中例示了在各步骤中使用的原语的示例。

[0138] 如果目标认证服务器 504 接收到预认证请求信息，则执行预认证过程（步骤 (8)）。归属用户服务器 (HSS)、以及移动节点 501、服务认证器 502、服务认证服务器 503、目标认证服务器 504 和目标认证器 506 与预认证过程相关联。预认证过程的结果被发送至服务认证器 502 的安全实体。包括 3GPP 网络认证服务器 504 的预认证过程假设含有从 HSS 提取与用户有关的安全上下文的过程。

[0139] 可以与图 3 的步骤 (9) 至 (20) 相同地执行步骤 (9) 至 (20)。但是，与省略了 HSS 标识符信息的图 3 的实施方式不同，假设包含关于预认证结果的信息的 MIH 预认证结果传输请求 / 响应原语包括与预认证有关的 HSS 标识符信息。对于优化的过程可以省略步骤 (15) 至步骤 (17)。

[0140] 可以有选择地使用诸如 MIH_MN_Preauth 请求 / 指示原语和 MIH_MN_Preauth 响应 / 确认原语的原语。

[0141] 因此，因为在执行实质的层 2 切换之前执行了预认证，因此，减小了由于 RAT 间切换处理中的认证而带来的延迟。

[0142] 同时，图 6 中，移动节点 601 直接请求目标网络 606 执行预认证而 不像图 4 中那样考虑到与当前网络 602 的关系。

[0143] 多模移动节点 601 接入当前服务链路的 IEEE 802.16 网络 602 以执行基于 EAP 的认证（步骤 (1)）并在保持与 IEEE 802.16 网络 602 的连接的同时检测一个或多个候选网络（步骤 (2)）。其后，移动节点 601 如上述实施方式那样选择目标链路并通过 MIH_Information 请求 / 响应原语从信息服务器 607 获得关于目标链路的信息（步骤 (3)）。假设由不同管理域通过这些原语操作的 非 802 系列网络是切换的目标链路。具体而言，在图 6 中，非 802 系列网络的 3GPP 网络 606 被选择作为目标链路。

[0144] 同时，如果多模移动节点 601 识别出从 IEEE 802.16 网络接收到的信号电平低于规定的电平（例如，该规定的电平高于用来确定切换发起的电平），移动节点 601 的 MIH 用

户通过 MIH_MN_Preauth 请求原语请求移动节点 601 的 MIH 发送预认证过程请求至目标链路的非 802 系列网络认证服务器 604(步骤 (4))。尽管可以通过与图 5 的实施方式中的 802.16 网络认证器 502 和认证服务器 503 的预认证过程的关系来将预认证过程请求发送至目标链路的非 802 系列网络认证服务器 604,但是在图 6 的实施方式中通过 802.16 网络认证器 602 和认证服务器 603 的简单中继来将预认证请求发送至目标认证器 606(步骤 (5) 和 (6))。此外,在此实施方式中,发送的 MIH_MN_Preauth 指示原语可额外的包括 MIH 用户所需的参数(例如,HSS 标识符)。

[0145] 接收到 MIH_MN_Preauth 指示原语的认证器 606 的安全实体发送预认证请求消息至与目标 3GPP 网络连接的 AAA 服务器 604。

[0146] 在移动节点 601 与目标 AAA 服务器 604 之间通过 IETF 协议来执行预认证过程(步骤 (8))。移动节点 601、目标认证器 606、目标认证服务器 604、和目标 HSS 605 可与预认证过程相关联。预认证过程的结果被发送至目标认证器 606 的 MIH 用户。包括 3GPP 网络的认证服务器 604 的预认证过程包括从 HSS 605 提取与用户有关的安全上下文的过程。

[0147] 可以与图 4 的实施方式相同地执行步骤 (9) 至 (16)。但是,与图 4 的实施方式不同的是,假设发送预认证结果的 MIH 预认证响应原语可包括 HSS 605 的标识符。

[0148] 同时,对于优化的过程可以省略步骤 (9) 至步骤 (13)。

[0149] 如上所述,因为在切换之前执行了预认证的过程,所以可以减少在实际的切换处理期间由于认证而导致的延迟。

[0150] 已经给出了本发明的示例性实施方式的详细说明以使得本领域的技术人员能够实现并实施本发明。虽然已经参照示例性的实施方式介绍了本发明,但是本领域的技术人员应了解,在不脱离由所附权利要求所描述的本发明的精神或范围的情况下,可以对本发明进行各种变型和修改。因此,本发明不应当限于此处说明的具体实施方式,而应当符合与此处公开的原则和特征一致的最广泛的范围。

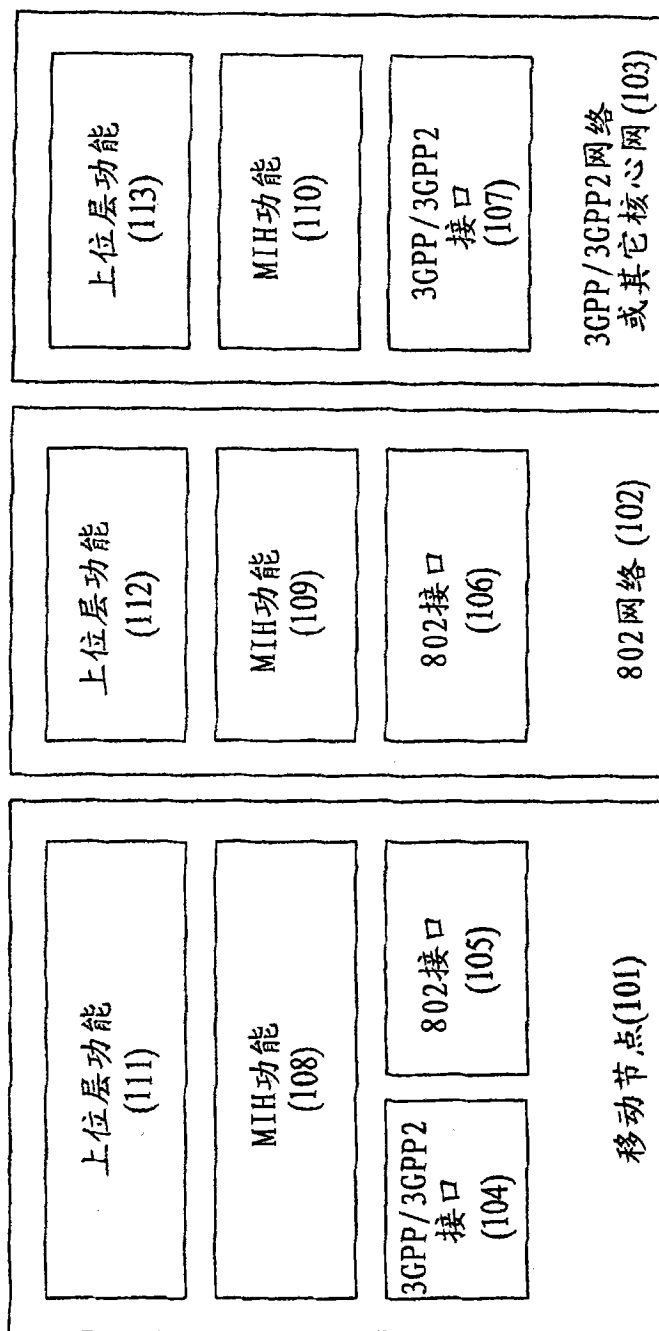


图 1

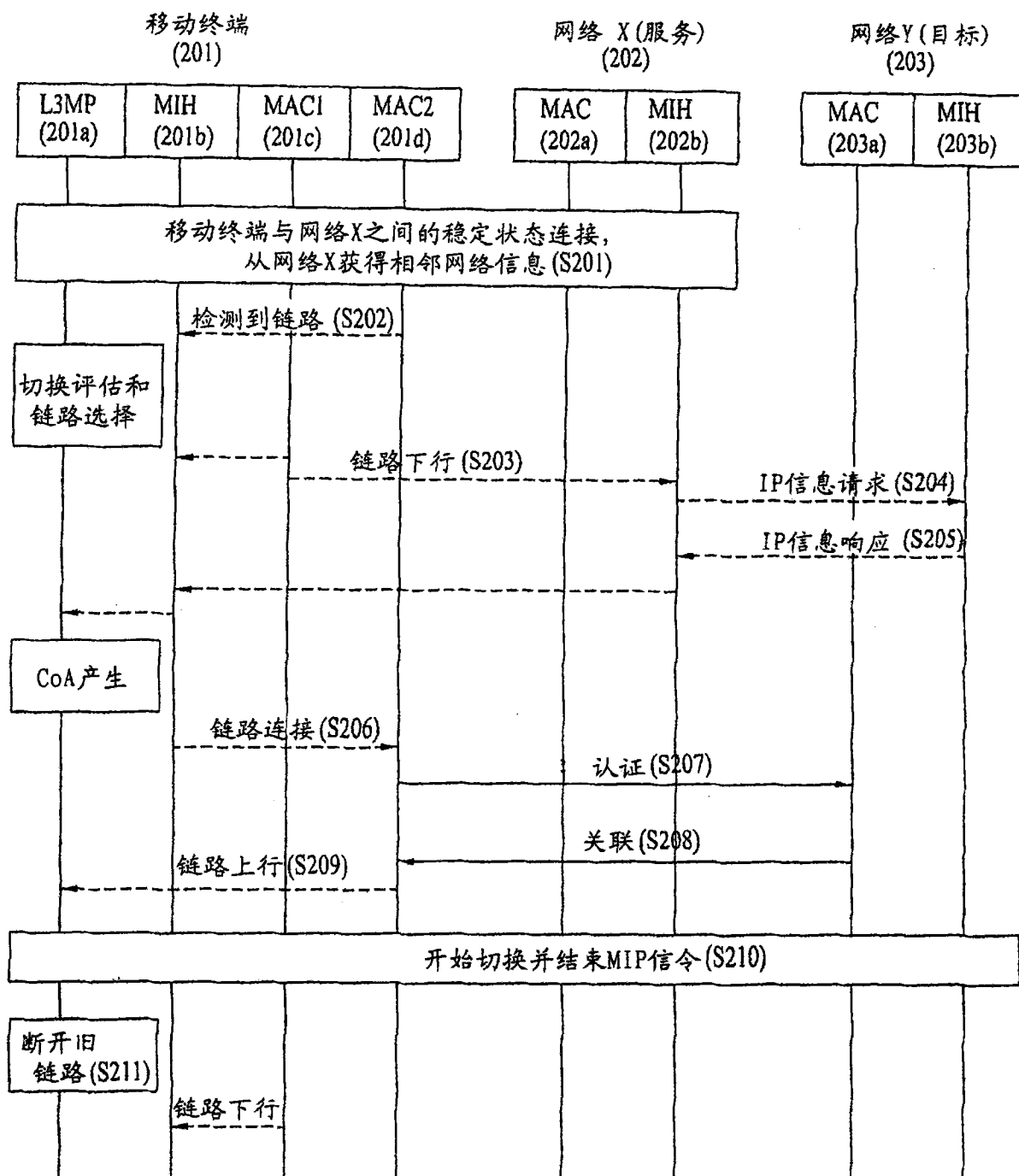


图 2

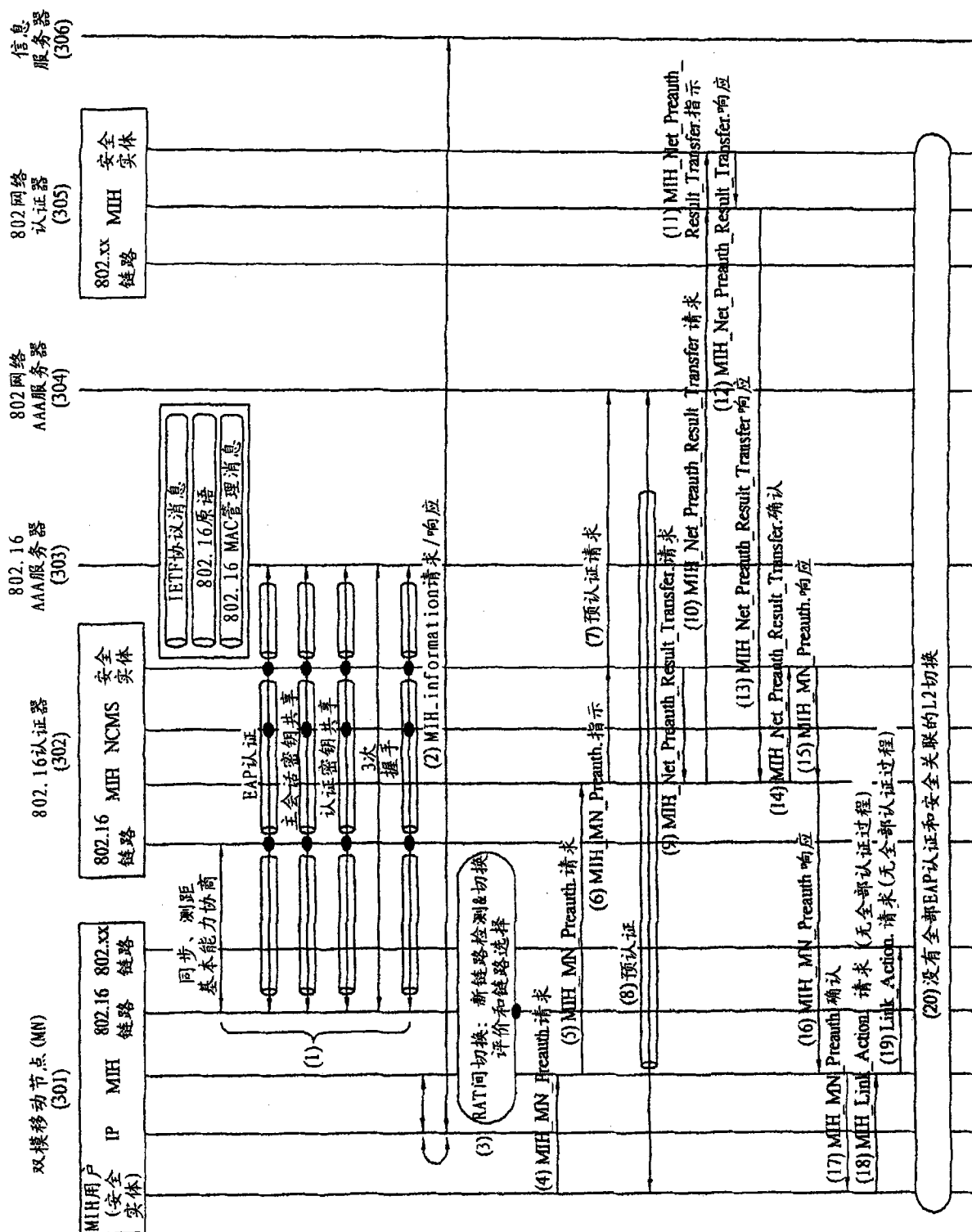


图 3

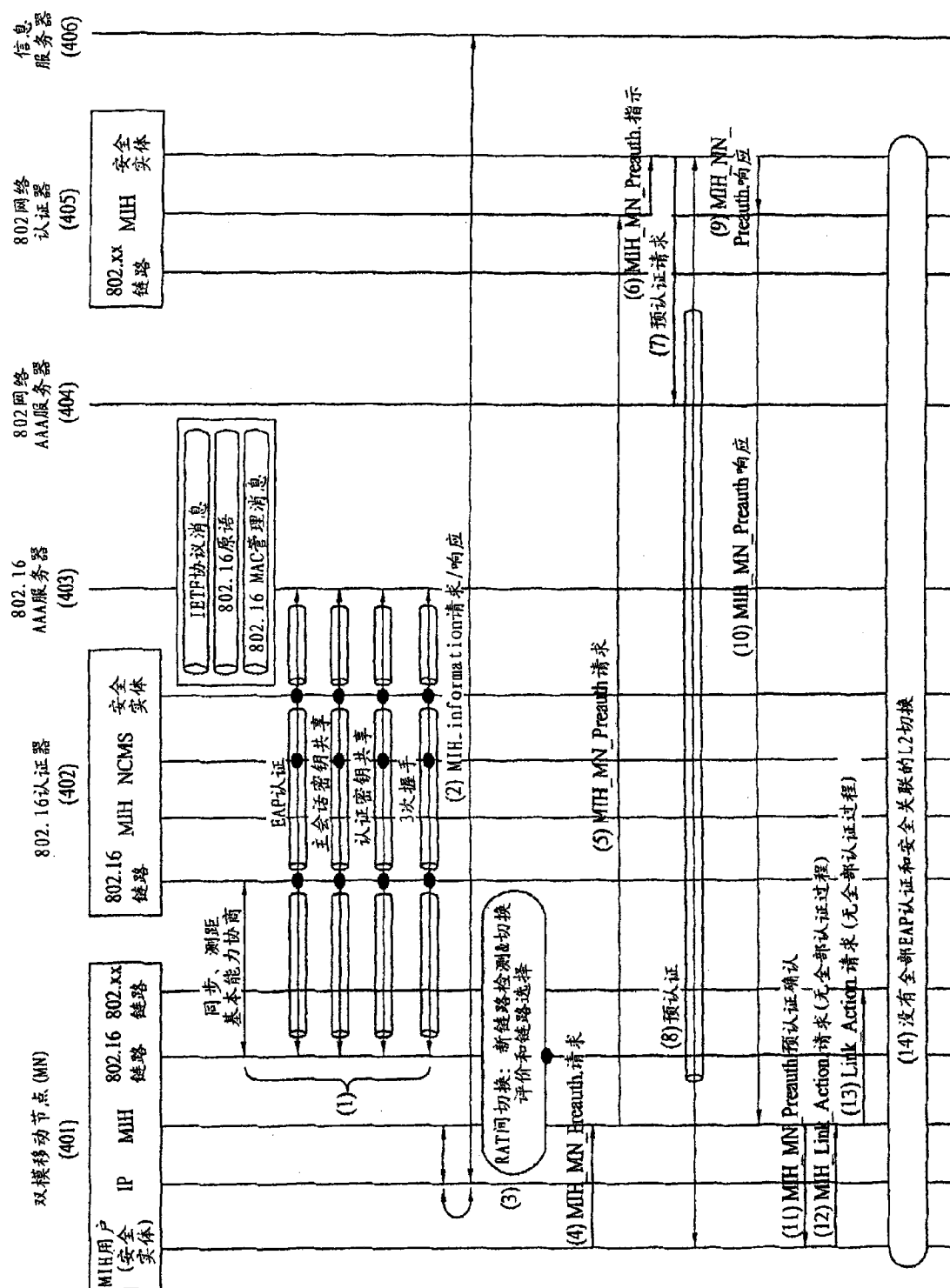


图 4

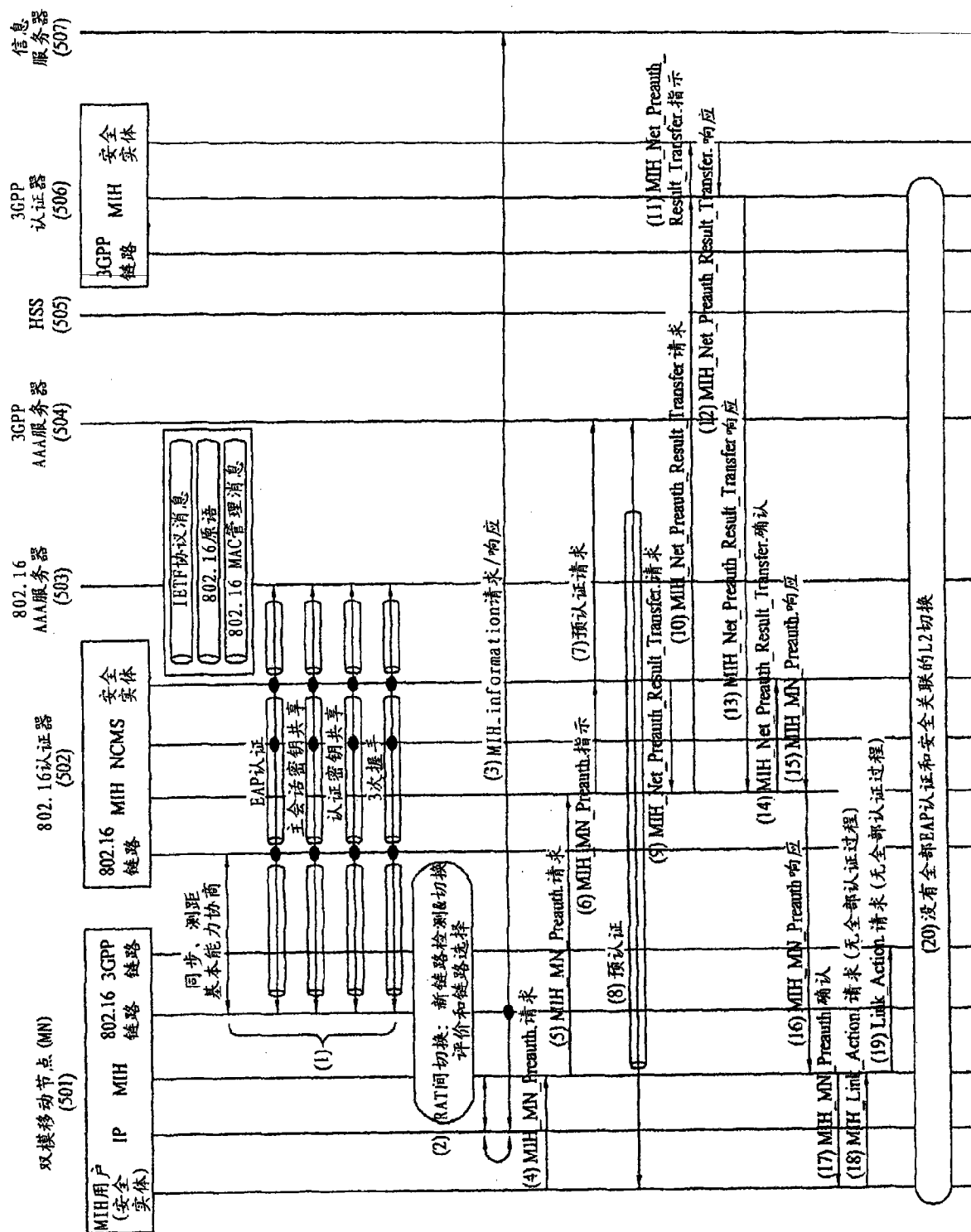


图 5

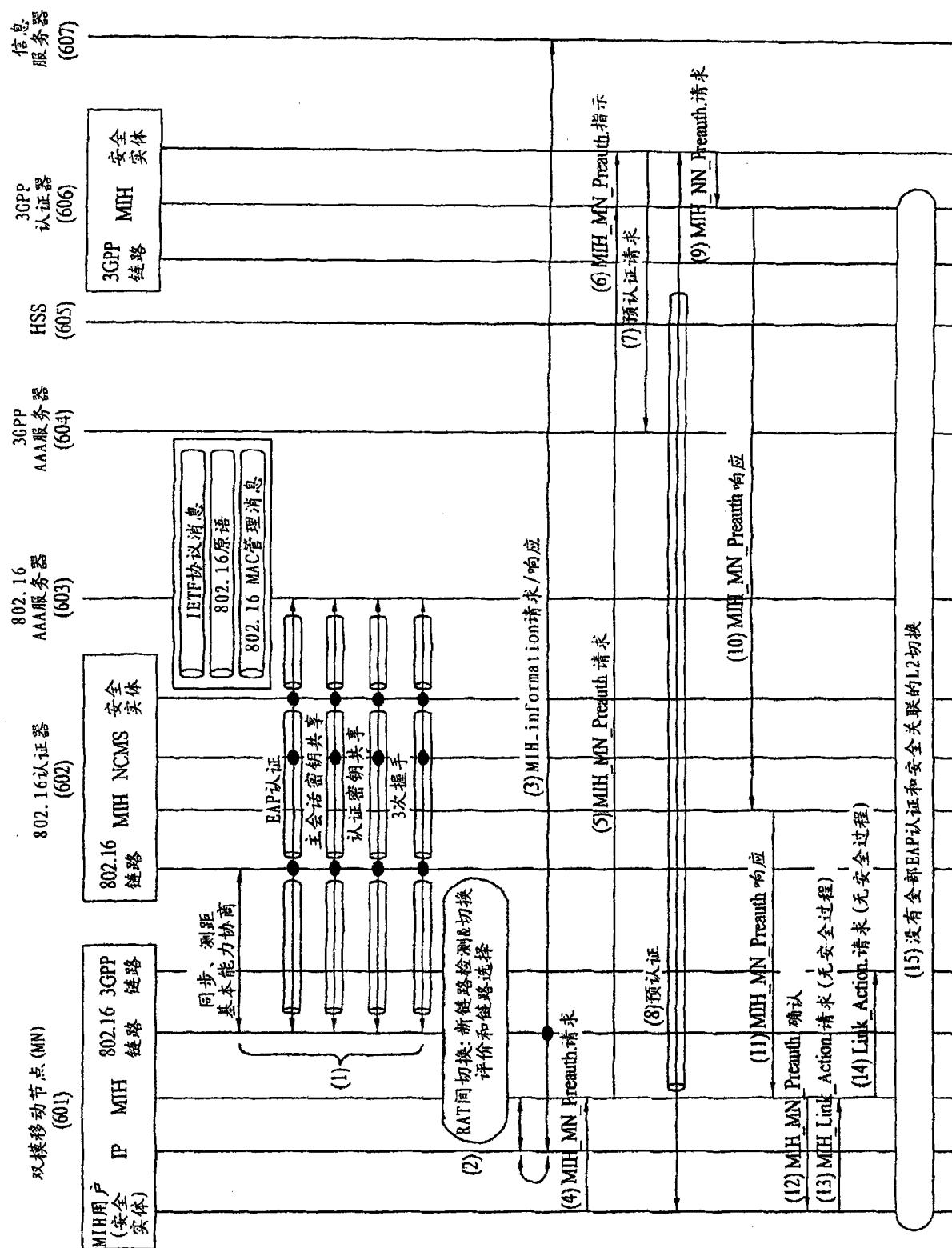


图 6