(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 101436931 B
(45)授权公告日 2013.07.10

(21)申请号 200810212911.5
(22)申请日 2008.09.04
(30)优先权数据
12/203,652 2008.09.03 US
60/985,538 2007.11.05 US
60/981,767 2007.10.22 US
12/203,671 2008.09.03 US
60/969,773 2007.09.04 US
(73)专利权人 财团法人工业技术研究院
地址 中国台湾新竹县
(72)发明人 王瑞堂
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 蒲迈文
(51)Int.Cl.
H04W 12/06(2009.01)
H04W 12/04(2009.01)
H04L 29/06(2006.01)

(56)对比文件
CN 1251717 A,2000.04.26, 全文.
WO 2007046630 A2,2007.04.26, 说明书第第7页第16行-第22页第4行、附图4-6.
CN 1946019 A,2007.04.11, 全文.
CN 1682487 A,2005.10.12, 全文.

审查员 刘子菡

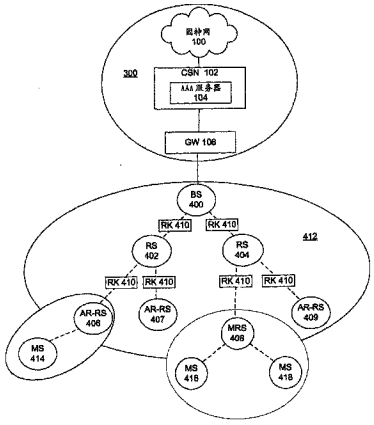
权利要求书3页 说明书10页 附图9页

(54)发明名称

无线通信系统中提供安全通信的方法、系统、基站与中继站

(57)摘要

本发明的一实施例提供一种在无线通信系统中提供安全通信的方法，适用于一通信网络中的一基站、一中继站以及一移动终端之间，该方法包括：通过该通信网络认证该移动终端；由该基站产生一安全数据，其中该安全数据包括至少一个交易加密密钥以及一信息确认码密钥；该基站传送该安全数据至该移动终端；该基站传送该安全数据至该中继站。



CN 101436931 B

1. 一种在无线通信系统中提供安全通信的方法，适用于一通信网络中的一基站、一中继站以及一移动终端之间，该方法包括：

通过该通信网络认证该移动终端；

由该基站产生一安全数据 (security material)，其中该安全数据包括至少一个交易加密密钥以及一信息确认码密钥；

该基站传送该安全数据至该移动终端；以及

该基站传送该安全数据至该中继站，

其中认证该移动终端的步骤还包括：

该基站接收来自一通信网络认证器的一认证密钥，其中该安全数据使用该认证密钥产生，且该安全数据不包含该认证密钥。

2. 如权利要求 1 所述的在无线通信系统中提供安全通信的方法，还包括：

该基站使用该安全数据传送多个安全的通信至该移动终端。

3. 如权利要求 1 所述的在无线通信系统中提供安全通信的方法，其中认证该移动终端的步骤还包括：

执行完整认证。

4. 如权利要求 3 所述的在无线通信系统中提供安全通信的方法，其中认证该移动终端的步骤还包括：

执行 IEEE802.1X 认证。

5. 如权利要求 1 所述的在无线通信系统中提供安全通信的方法，其中认证该移动终端的步骤还包括：

该基站接收来自该移动终端的一安全数据辨识码，该安全数据辨识码对应储存在该移动终端的一认证密钥；

当该基站认证该移动终端成功时，该基站传送一认证成功信息至该移动终端；以及

当该基站认证该移动终端失败时，该基站要求该移动终端执行一 IEEE802.1X 完整认证程序。

6. 如权利要求 1 所述的在无线通信系统中提供安全通信的方法，还包括：

在该基站与该中继站之间建立一安全通信路径，其中该基站通过该安全通信路径传送至少一个该安全数据至该中继站。

7. 如权利要求 1 所述的在无线通信系统中提供安全通信的方法，其中该基站与该中继站之间的通信方式为无线通信。

8. 一种在无线通信系统中提供安全通信的基站，适用于一通信网络，该基站包括：

至少一个存储器，用以储存数据与多个指令；

以及

至少一个处理器，用以存取该存储器并执行这些指令以执行一认证方法，该认证方法包括：

通过该通信网络认证一移动终端；

产生一安全数据，其中该安全数据包括至少一个交易加密密钥以及一信息确认码密钥；

传送该安全数据至该移动终端；以及

传送该安全数据至一中继站，

其中该认证方法还包括：

该基站接收来自一通信网络认证器的一认证密钥，其中该安全数据使用该认证密钥产生，且该安全数据不包含该认证密钥。

9. 如权利要求 8 所述的在无线通信系统中提供安全通信的基站，其中该认证方法还包括：

执行完整认证。

10. 如权利要求 8 所述的在无线通信系统中提供安全通信的基站，其中该认证方法还包括：

执行 IEEE802.1X 认证。

11. 如权利要求 8 所述的在无线通信系统中提供安全通信的基站，其中该认证方法还包括：

该基站接收来自该移动终端的一安全数据辨识码，该安全数据辨识码对应储存在该移动终端的一认证密钥；

当该基站认证该移动终端成功时，该基站传送一认证成功信息至该移动终端；以及

当该基站认证该移动终端失败时，该基站要求该移动终端执行一 IEEE802.1X 完整认证程序。

12. 如权利要求 8 所述的在无线通信系统中提供安全通信的基站，其中还包括一第一处理器，用以在该基站与该中继站之间建立一安全通信路径，其中该基站通过该安全通信路径传送至少一个该安全数据至该中继站。

13. 如权利要求 8 所述的在无线通信系统中提供安全通信的基站，其中该基站与该中继站之间的通信方式为无线通信。

14. 一种在无线通信系统中提供安全通信的中继站，适用于一通信网络，该中继站包括：

至少一个存储器，用以储存数据与多个指令；

一第一处理器，用以传送一安全数据更新信息至一移动终端，以通知该移动终端更新其安全数据；以及

至少一个处理器，用以存取该存储器并执行这些指令以执行一认证方法，该认证方法包括：

回应来自该移动终端的一量测距离请求，传送该移动终端的一认证请求至一基站；以及

使用由该基站产生并从该基站接收到的一安全数据，执行与该移动终端之间的一安全数据传输，其中该安全数据包括至少一个交易加密密钥以及一信息确认码密钥。

15. 如权利要求 14 所述的在无线通信系统中提供安全通信的中继站，其中该第一处理器还用以在该基站与该中继站之间建立一安全通信路径，其中该中继站通过该安全通信路径传送该认证请求至该基站。

16. 如权利要求 14 所述的在无线通信系统中提供安全通信的中继站，其中该中继站为一移动中继站。

17. 如权利要求 14 所述的在无线通信系统中提供安全通信的中继站，其中传送该安全

数据更新信息至该移动终端的传输方式为一多播传输方式。

18. 如权利要求 14 所述的在无线通信系统中提供安全通信的中继站，其中该基站与该中继站之间的通信方式为无线通信。

19. 一种提供安全通信的系统，该系统包括：

一基站，用以提供至一通信网络的接入，通过该通信网络认证至少一个移动终端，产生并传送一安全数据；以及

一中继站，与该基站通信，用以接收该安全数据并使用该安全数据以提供与至少一个该移动终端之间的多个安全数据传输，其中该安全数据包括至少一个交易加密密钥以及一信息确认码密钥，

其中该中继站使用该安全数据以提供与至少一个该移动终端之间的这些安全数据传输且不对该移动终端执行一认证程序。

20. 如权利要求 19 所述的提供安全通信的系统，其中该中继站为一移动中继站。

21. 如权利要求 20 所述的提供安全通信的系统，其中该基站聚集并传送该安全数据至该中继站。

22. 如权利要求 20 所述的提供安全通信的系统，其中该中继站使用该安全数据以提供与至少一个该移动终端之间的这些安全数据传输，但不改变该移动终端所持有的该交易加密密钥。

23. 如权利要求 19 所述的提供安全通信的系统，其中该基站与该中继站之间的通信方式为无线通信。

无线通信系统中提供安全通信的方法、系统、基站与中继站

技术领域

[0001] 本发明关于无线通讯，特别是在一无线通信环境中建立安全关联的系统与方法。

背景技术

[0002] 习知的无线网络环境连结移动电子装置至服务供应商。更具体的来说，全球互通微波接入(Worldwide Interoperability for Microwave Access,WiMAX)的网络环境通过中介连接(intermediate connections)连结一用户装置至一网络。WiMAX是一种无线网络科技，可以提供通信到相当远的无线装置。验证与再验证(reauthentication)造成的延迟，会使得与客户端装置(clientdevice)通信的速度变慢，而且降低了WiMAX无线环境的效率。

[0003] 图1为使用IEEE802.16d/802.16e WiMAX无线通信系统的一习知无线通信系统的方块图。网络100提供给至少一个连线服务网络(Connectivity ServiceNetwork，CSN)102，连线服务网络102则使用至少一个认证、授权以及计费(Authentication、Authorization、Accounting，以下简称AAA)服务器104。CSN102连结到网关(gateway)106与108。网关106与108为一种通信网络认证者(authenticator)，通常是被连结到数个基站(base station，BS)110至115，基站的数量是取决于在一定区域内的网络需求，虽然一个网关可能只能连结到单一的基站，但一个网关仍可连结到多个基站。在图1中只以网关106与108为例说明，但仍可视实际基站的数量来决定使用更多或更少的网关。

[0004] 在图1中，是以六个基站为例说明WiMAX环境，但仍可视实际可使用的网关以及WiMAX网络需求来增加或减少基站的数量。基站，如基站110与104，用以与一个或多个客户端装置通信。客户端装置包括移动终端(mobilestation,MS)，如移动终端120、122以及124，以及用户终端(subscriber station,SS)，其中基站提供无线网络服务给移动终端，且提供有线或无线网络服务给用户终端。数个客户端装置的网络需求可能可以藉由单一基站满足，而单 一基站可能可以同时满足移动终端与用户终端的需求。

[0005] 在习知的WiMAX网络环境中，如图1所示，每一次移动终端120被一网关，如网关106，通过一相关的基站，如基站110，初始服务时，都必需要对移动终端120进行认证。藉由这样的认证动作，只要移动终端120移动的区域范围内都能够通过由原来认证的网关来使用服务的话，就不用对移动终端作更多的认证。但是，一但移动终端移到一个区域，是由另一个网关提供服务，如网关108，则网关在对移动终端120提供服务前，必须要先进行再认证动作。当一客户端装置被认证或在认证之后，安全关联(securityassociations)或是两个网络实体，如移动终端120与基站110，之间的安全信息会被建立，以确保两者之间的通信安全。

[0006] 认证协议标准(Authentication protocol standard)已经事先在认证技术上被标准化。这些标准化的协议可能包括，如IEEE802.IX认证、GSM用户身份模组延伸式认证协议法(extensible authentication protocol method for GSM(global system for mobile communications)subscriber identity modules(EAP-SIM))，UMTS用户身

份模组延伸式认证协议法与密钥协定(extensibleauthentication protocol method for universal mobile telecommunications systems(UMTS)authentication and key agreement(EAP-AKA))以及/或延伸式认证协议法与远端认证拨接使用者服务协定(Remote Authentication Dial-in UserService,RADIUS)的一种组合。此外,标准化的握手协议,如安全关联相关协议,可被使用来在一通信连结上建立多个安全关联,标准化的握手协议如安全关联与交易加密密钥三次握手程序(security association and trafficencryption key(SA-TEK)3-way handshake procedure)与TEK三次握手程序。

[0007] 在IEEE802.16d/802.16e WiMAX无线通信系统,这些标准化的技术在一基站与一移动终端之间执行。每一种标准化的认证技术需要多个传输(multiple transmissions),这会增加认证的时间以及处理所需的资源。

[0008] 图2为IEEE802.16d/802.16e WiMAX无线通信系统中习知的认证与授权运作的信号流程图。一初始化程序200被执行以确保移动终端的请求网络服务的请求被授权,使移动终端可以接入网络,且提供移动终端与基站之间的一安全关联(security association),用以允许移动终端与基站之间的的安全信息传输。举例来说,当移动终端120从原先基站110覆盖的范围移动到基站111所覆盖的范围时,初始化程序200可能被使用以提供移动终端与基站之间的一安全关联。

[0009] 在初始化程序200的第1步中,移动端120是通过连接程序(link upprocess)202无线连接基站111,举例来说连接程序202包括一量测距离请求(ranging request)与一量测距离回应(ranging response)。移动终端120接着继续认证程序的多个步骤,认证程序可能如IEEE 802.1X完整认证程序(fullauthentication)206。AAA服务器104计算一主会话密钥(master session key,MSK)208给移动终端120,并将主会话密钥208传送给网关106,并储存在网关106的快取中。这些认证程序的目的,如EAP认证方法或其他认证方法,就是要传送已经传送被AAA服务器104、网关106以及移动终端120认证的MSK 208。网关106会产生一成偶密钥(Pairwise master Key,PMK)210以及一认证密钥(authentication key,AK)212给移动终端120,并传送AK 212至基站111。

[0010] 移动终端120可能会独立的储存与保留AK 212在自己的存储器中,并且可能会产生AK 212。接着基站111可能执行SA-TEK三次握手程序(SA-TEK 3-way handshake procedure)214去认证移动终端212保留的AK是与基站111中的AK 212是相同的。使用AK 212,一般是保留在基站111与移动终端120中,可能可以分别的计算一共有的信息确认码密钥(messageauthentication code key,MACK)224以及一共有的密钥加密密钥(keyencryption key,KEK)220。MACK224可以分辨由移动终端120与基站111产生的一认证信息(authenticated message)。KEK 220可以保护由移动终端120到基站111的一交易加密密钥(traffic encryption key,TEK)。基站111以及移动终端120可以使用MACK 224来执行SA-TEK三次握手程序214以便互相认证。当SA-TEK三次握手程序214被成功的执行完毕,基站111产生TEK 22并且与KEK 220进行一TEK三次握手程序216,以建立与移动终端120的一安全关联。TEK 222一般来说是由基站111随机产生,且在移动终端120已经被认证且授权接入网络后,被使用来对传输在基站111与移动终端120之间的数据加密。SA-TEK三次握手程序214与TEK三次握手程序216为本领域普通技术人员所熟知,在此不赘述。

[0011] 在使用在如图 2 的 IEEE 802.16d/802.16e WiMAX 无线通信系统中的初始化程序 200 中，基站 111 控制基站 111 与移动终端 120 之间是否有数据传输，这是因为基站 111 与移动终端 120 都握有相同的 TEK 222、KEK 220 与 AK 212，而这些都是用来产生 MACK224。当移动终端 120 已经建立与基站 111 的安全关联后，换言之，移动终端 120 已经得到允许来通过网络通信，使用 TEK222 的加密的数据传输也因此产生在移动终端 120 与基站 111 之间。

[0012] 请参考图 1。当图 1 的系统运作时，信号的强度以及传输的品质可能会衰退，这是因为网络信号经过网关 106 或 108 至基站 110-115 再到客户端装置所造成的。此外，当移动终端由原先提供服务的基站移动到其他基站的服务时，信号的强度以及传输的品质亦可能衰退。信号品质与覆盖范围可能会受到其他因素影响，如实体建筑物、信号干扰、天气以及传输条件与格式。因此，覆盖间隙 (gap) 区域或漏洞 (hole) 区域可能会发生，而且当使用者位于这些区域时可能只有有限的或是根本没有网络接入服务。

[0013] 其中一个解决覆盖间隙区域的方法就是提供更多的基站，但这可能造成大量的成本花费。另外，为了避免这样的问题，亦可以采用中继站 (relaystation)，如 IEEE802.16j 中提到的多节点跳跃中继网络协议技术 (multi-hoprelaying，MR)。基站与中继站之间的沟通只有在中继站对来自基站或移动终端的信号增强或中继，并不会牵涉到认证程序或是建立安全关联。

[0014] 图 3 为使用 IEEE802.16j WiMAX 且具有 MR 架构的通信系统的一习知通信系统的方块图。与 IEEE802.16d 与 802.16e WiMAX 无线通信系统相似，通过至少一个 AAA 服务器，如 AAA 服务器 104，以及至少一个网关，如网关 106，来接入网络 100。为了方便起见，网络 100、CSN102、AAA 服务器 104 与网关 106 被以核心网络 (core network)300 表示。核心网络 300，或更精确的来说是网关 106，通过一有线连结来与基站 310 至 313 通信。

[0015] 在图 3 中，是以四个基站为例说明，但是亦可以使用更多或更少数量的基站。基站，如基站 310，一般是可以通过无线传输直接与一个或多个移动终端直接通信，如移动终端 320。基站，如基站 311 与 312，亦可间接与一个或多个移动终端通信。如移动终端 322、324、326。基站一般可通过无线通信来与一个或多个中继站通信，如中继站 328、330 与 332，但也可以通过有线连接通信。中继站 328、330 与 332 对于通过无线传输的方式，对于接收到来自或传送到移动终端 322 的信号增强或中继。如图所示，中继站 328、330 与 332 是固定的中继站。但是，基站亦可以与移动中继站 (mobile relay station，MRS) 通信，如移动中继站 334。移动中继站可以驻在火车，飞机或其他机动运输工具，用以提供拥有移动终端的乘客可以去通过移动中继站来连结基 站或其他中继来。如图 3 所示，移动中继站 334 提供无线服务给移动终端 324 与 326，但单一移动终端或数个移动终端的网络需求可能可以通过单一移动中继站得到满足。虽然图 3 未表示，但是基站，如基站 310 至 313，可以与一个或多个用户终端通信。因此，多个客户端装置的网络需求便可以直接由单一基站或是通过一个或多个中继站来满足。更进一步来说，中继站 328、330 与 332 可以提供无线服务给其他的中继站、移动中继站且 / 或移动终端。

[0016] 在一些应用上，中继站的使用可能会造成中继站与基站之间的站与站 (station-to-station) 切换 (handoff) 需求的增加，而且因为每个中继站 (包括移动中继站) 有限的覆盖区域，可能需要更多的处理资源来处理上述的台与台间的服务。此外，当进行安全通信相关运作时，来自一中继站或基站到另一中继站或基站的切换程序

(handoffprocess) 会消耗额外的资源，造成通信连接的效能、频宽或品质降低。

[0017] 本案公开的实施例就是为了解决上述这些问题。

发明内容

[0018] 本发明的一实施例提供一种在无线通信系统中提供安全通信的方法，适用于一通信网络中的一基站、一中继站以及一移动终端之间，该方法包括：通过该通信网络认证该移动终端；由该基站产生一安全数据，其中该安全数据包括至少一个交易加密密钥以及一信息确认码密钥；该基站传送该安全数据至该移动终端；该基站传送该安全数据至该中继站。

[0019] 本发明的另一实施例提供一种在无线通信系统中提供安全通信的基站，适用于一通信网络，该基站包括至少一个存储器，用以储存数据与多个指令，以及至少一个处理器，用以存取该存储器并执行这些指令以执行一认证方法。该认证方法包括：通过该通信网络认证一移动终端；产生一安全数据，其中该安全数据包括至少一个交易加密密钥以及一信息确认码密钥；传送该安全数据至该移动终端；传送该安全数据至一中继站。

[0020] 本发明的另一实施例提供一种在无线通信系统中提供安全通信的中继站，适用于一通信网络，该中继站包括至少一个存储器，用以储存数据与多个指令，以及至少一个处理器，用以存取该存储器并执行这些指令以执行一认证方法。该认证方法包括：回应来自一移动终端的一量测距离请求，传送该移动终端的一认证请求至一基站；使用该基站接收到的一安全数据，执行 与该移动终端之间的一安全数据传输，其中该安全数据包括至少一个交易加密密钥以及一信息确认码密钥。

[0021] 本发明的另一实施例提供一种提供安全通信的系统，该系统包括一基站以及一中继站。该基站，用以提供至一通信网络的接入，通过该通信网络认证至少一个移动终端，产生并传送一安全数据。该中继站，与该基站通信，用以接收该安全数据并使用该安全数据以提供与至少一个该移动终端之间的多个安全数据传输，其中该安全数据包括至少一个交易加密密钥以及一信息确认码密钥。

附图说明

[0022] 图 1 为使用 IEEE802.16d/802.16e WiMAX 无线通信系统的一习知无线通信系统的方块图。

[0023] 图 2 为 IEEE802.16d/802.16e WiMAX 无线通信系统中习知的认证与授权运作的信号流程图。

[0024] 图 3 为使用 IEEE802.16j WiMAX 且具有 MR 架构的通信系统的一习知通信系统的方块图。

[0025] 图 4 为根据本发明的使用在 IEEE802.16jWiMAX 无线通信系统的一无线通信系统的一实施例的方块图。

[0026] 图 5A 为一基站的一实施例的方块示意图。

[0027] 图 5B 为一移动终端的一实施例的方块示意图。

[0028] 图 5C 为中继站或移动中继站的一实施例的方块示意图。

[0029] 图 6 为根据本发明的一 IEEE802.16d/802.16e WiMAX 无线通信系统中的认证与授

权运作的一实施例的信号流程图。

[0030] 图 7 为根据本发明的一切换程序的一实施例的信号流程图。

[0031] 图 8 为根据本发明的一切换程序的另一实施例的信号流程图。

[0032] 图 9 为根据本发明的一切换程序的另一实施例的信号流程图。

具体实施方式

[0033] 本案说明书中提及的实施例提供在 IEEE802.16jWiMAX 无线通信环境或其他无线通信使用中继站的网络系统内的多个安全关联。藉由提供可建立与一移动终端之间的安全连结以及可提供多个移动终端接入网络 300 的中继站，额外开销 (processing overhead) 可以被显著的减少。特别是藉由提供具有 TEK 或 MAC 的中继站，该中继站可建立与移动终端的一安全关联并且执行对移动终端的认证与授权，其中该 TEK 与 MAC 为对应想接入网络 300 的一移动终端。

[0034] 图 4 为根据本发明的使用在 IEEE 802.16j WiMAX 无线通信系统的一无线通信系统的一实施例的方块图，其中该无线通信系统选择使用中继站作为认证中继站 (authenticator relay-relay station，AR-RS)。在图 4 中，一基站 400 通过一有线线路连结到网络 300，并且比无线通信方式与一个或多个中继站 402 与 404 通信，中继站用以增强或中继接收到的信号并传送到多个 AR-RS406 至 409。如图 4 所示，AR-RS(MRS)408 为一移动中继站。安全区域密钥 (security zone key)，又称中继密钥 (relay key，RK)，410 被基站 400 散布到中继站 402 与 404 以及在中继站 402 与 404 之后的 AR-RS 406 至 409，且 AR-RS 406 至 409 在对网络 300 的个别的初始化程序中被认证。安全区域密钥被使用在 IEEE 802.116j 网络中的中继站以及 / 或中继站以及基站之间的多个通信通道 (communication channels) 的数据与信号的保护。中继站 402 与 404 且 / 或基站 400 可以使用中继密钥 410 来执行数据与信号的加密、解密与信息认证。由基站 400、中继站 402 与 404 以及 AR-RS 406 至 409 提供的网络覆盖区域被称为安全中继区 (security relay zone，SRZ)412。图 4 以由 AR-RS 406 提供服务的一移动终端 414 以及由 AR-RS(MRS)408 提供服务的移动终端 416 与 418 为例说明，但多个移动终端的网络需求是可以由单一 AR-RS 所提供。此外，虽然图上只有 AR-RS 408 表示为移动中继站，在 SRZ412 内额外的多个 AR-RS 仍以作为移动中继站。

[0035] 每一次当移动终端 414 被初始化由基站 400 提供服务时，都必需建立与网络 300 的一安全关联。只要移动终端 414 在 SRZ 412 内移动，就可以绕过 (bypass) 进一步的安全关联建立与认证。但是，一但移动终端 414 移到由另一个基站提供服务的区域时，移动终端 414 就由其他基站提供服务，如此一来就必需针对不同的基站建立基站与移动终端 414 之间的安全关联，且取决于是否有其他的基站被连结到网关 106。对移动终端 414 的认证也是切换 (handoff) 程序中的一部分。这样的再认证且 / 或安全关联建立程序，就造成对移动终端 414 提供服务的延迟。

[0036] 图 5A 为一基站的一实施例的方块示意图。基站 400 可以为任何形式的通信装置，用以在一无线通信系统中与一个或多个移动终端、中继站以及 / 或 AR-RS，之间传送且 / 或接收信号且 / 或通信，其中移动终端可能为移动终端 414，中继站可能为中继站 402 与 404，AR-RS 可能如 AR-RS406 至 409。如图 5A 所示，每一个基站 400 可能包过一个或多个下列元件 :至少一个中央处理单元 500、随机存取存储器 (RAM)502、随机只读存储器 (ROM)504、存

储器506、数据库508、输入/输出(I/O)装置510、接口512、天线514等。中央处理单元500用以执行电脑程序指令,以执行不同的程序与方法。RAM502与ROM504用以存取并储存信息与电脑程序指令。存储器506用以储存数据与信息。数据库508用以储存多个表(table)、目录(list)或其他数据结构。上述元件为本领域普通技术人员所熟知,在此不赘述。

[0037] 图5B为一移动终端的一实施例的方块示意图。如图所示,每一移动终端414可能包含一个或多个下列元件:至少一个中央处理单元520、随机存取存储器(RAM)522、随机只读存储器(ROM)524、存储器526、数据库528、输入/输出(I/O)装置520、接口522、天线524等。中央处理单元520用以执行电脑程序指令,以执行不同的程序与方法。RAM522与ROM524用以存取并储存信息与电脑程序指令。存储器526用以储存数据与信息。数据库528用以储存多个表(table)、目录(list)或其他数据结构。上述元件为本领域普通技术人员所熟知,在此不赘述。

[0038] 图5C为中继站或移动中继站的一实施例的方块示意图。如图5c所示,每一中继站或移动中继站406可能包含一个或多个下列元件:至少一个中央处理单元540、随机存取存储器(RAM)542、随机只读存储器(ROM)544、存储器546、数据库548、输入/输出(I/O)装置540、接口542、天线544等。中央处理单元540用以执行电脑程序指令,以执行不同的程序与方法。RAM542与ROM544用以存取并储存信息与电脑程序指令。存储器546用以储存数据与信息。数据库548用以储存多个表(table)、目录(list)或其他数据结构。上述元件为本领域普通技术人员所熟知,在此不赘述。

[0039] 图6为根据本发明之一IEEE802.16d/802.16e WiMAX无线通信系统中的认证与授权运作的一实施例的信号流程图,其中该无线通信系统选择使用中继站作为认证中继站(authenticator relay-relay station,AR-RS)。一初始化程序600被执行以确保移动终端的请求网络服务的请求被授权,使移动终端可以接入网络,且提供一安全关联(security association)于移动终端、中继站与认证中继站之间,用以允许移动终端与基站之间的的安全信息传输。举例来说,当移动终端414刚开机(turned on)或是在移动终端414由通过连接网关108的一基站提供的覆盖范围进入AR-RS 406提供服务的覆盖范围时,初始化程序600可能被用以认证并建立与移动终端414之间的一安全关联。

[0040] 在一初始连接程序602中,移动终端414传送一量测距离请求给AR-RS406。AR-RS406则回应一量测距离回应给移动终端414,用以确认目前移动终端是否在AR-RS 406覆盖范围。AR-RS 406接着传送受到中继密钥(relaykey)410保护的一认证请求604至基站400。认证请求604会告知由AR-RS 406提供服务的移动终端414的识别数据给基站500。因为移动终端414前次或最近并没有通过基站400与网关106连结网络300,因此移动终端414利用使用IEEE 802.1X完整认证程序206的AAA服务器104来进行认证。

[0041] 当IEEE 802.1X完整认证程序206被成功的执行完毕后,AAA服务器104与移动终端414会计算一主会话密钥(master session key,MSK)606。接着AAA服务器104将MSK 606传送给网关106。当网关106接收到MSK 606时,网关106会根据MSK 606计算PMK 608,并将PMK 608储存在网关106的快取。网关106接着根据PMK 608计算AK 610,并且将AK 610传送给基站400。当基站400接收到AK 610时,基站400开始根据AK 610来产生安全数据(security material),安全数据包括了KEK 612与MACK 616。MSK 606是已经为AAA服务器104、网关106以及一客户端装置,如移动终端414,所知道的。移动终端因此

独立的持有MSK 606，且可能得到PMK 608与AK610，并且得到相同的MACK 616与KEK 612。一客户端装置，如移动终端414，在一成功的认证使用后，如EAP认证方法，将PMK 608暂存在其存储器中。此时，基站400与移动终端414根据MACK 616执行一SA-TEK三次握手程序214来互相认证。当SA-TEK三次握手程序214被成功的完成时，基站400会产生并传送安全数据至移动终端414，其中该安全数据包括TEK614，且受到KEK 612的保护。在一实施例中，TEK 614是由基站400随机产生，而且用以提供在基站400与AR-RS 406之间的数据机密性。同时，基站400会传送安全数据至AR-RS 406，其中该安全数据包括TEK 614，且受到KEK 612的保护。中继站406可能接收MACK 615用以直接认证移动终端414并接收TEK 614用以加密或解密要传送到移动终端414或是来自移动终端414的已加密的信息。一个或多个安全密钥，如MK、MSK 606、PMK 608、AK610、KEK612、TEK614、MACK615，都可能可以用来作为安全数据。

[0042] AR-RS406可以切换在移动终端414与AR-RS406之间的通信通道为一已授权状态，以提供移动终端414接入网络300。更进一步来说，因为移动终端414与AR-RS406都有TEK614，因此双方都可以交换已加密的数据传输。更具体的来说，在移动终端414被认证之后，TEK614可以用来加密传输在移动终端414与AR-RS406之间的数据。如果一多播服务(multicastservice)是可用的，基站400可以散布一多播密钥(multicast key)给AR-RS406，以致能移动终端414来接收要传送给多个移动终端的多个传输，其中多播服务是一基站同时传送多个信息给多个用户端装置，且多播密钥是用来保护多个多播传输。

[0043] 图7为根据本发明的一切换程序的一实施例的信号流程图，该切换程序是当由一目前AR-RS，如AR-RS406，转换到一目标AR-RS，如AR-RS407，时发生的，且目前AR-RS与目标AR-RS是与相同的基站通信，如基站400。在图7中，当移动终端414传送一量测距离请求给AR-RS407时且AR-RS407回应一量测距离回应给移动终端414时，连结702因此被建议在移动终端414与AR-RS407之间，其中AR-RS407包括一安全数据识别，如认证密钥识别码(authentication key identification，AKID)。因为移动终端414对AR-RS406的优先认证，该认证密钥识别码辨识目前储存在移动终端414的一存储器，如存储器526、ROM524、RAM522或数据库528内的AK。AR-RS407在一AK确认信号要求(verification signal request)704内，传送AKID至基站400，用以确认储存在移动终端414的AK与储存在基站400的存储器，如存储器526、ROM524、RAM522或数据库528，内的AK是否符合。因为AR-RS406与AR-RS407都在SRZ412内，因此两者共享相同的中继密钥410。基于安全的目的，使用中继密钥410对确认信号要求704加密。在一实施例中，因为移动终端先前通过AR-RS406与基站400执行完一完整的认证程序，因此在基站400与移动终端414内的安全数据是符合的，在这安全数据是可以指AK610。如果AK符合，基站400传送一AK确认成功信息706至AR-RS407。在另一实施例中，基站414可能被程控用以传送一区域网络延伸认证协议(Extensible Authentication Protocol over Local Area Network，EAPOL)开始信息708，以触发IEEE802.1X完整验证程序206。当AR-RS407接收到EAPOL开始信息708时，AR-RS407可以传送一EAPOL成功信息710给移动终端414，以略过IEEE802.1X完整验证程序206，因此这也指出认证程序在不经历IEEE802.1X完整验证程序206亦可以成功。

[0044] 因为此时基站400与移动终端414可能持有相同的安全数据，如AK610。移动终端414与基站400可个别由AK610导出MACK616。移动终端414与基站400可能持有前次计

算到的 TEK614 且 / 或前次产生的 KEK612，而且可以直经执行 SA-TEK 三次握手程序来互相验证。此外，如图 6 所述的连结关系，基站 400 可以藉由 AK610 产生一新的 KEK72 并产生一新的 TEK714。基站 400 使用 KEK712（或 TEK612）对 TEK714（或 TEK612）加密，且为了数据机密性，基站 400 传送已加密的 TEK714（或 TEK614）至移动终端 414。

[0045] 基站 400 会使用中继密钥 410 保护并即时传送安全数据，如 TEK714（或 TEK614）以及 MACK616 至 AR-RS407。在 AR-RS407 得到 TEK714（或 TEK614）后，AR-RS407 切换在移动终端 414 与 AR-RS407 之间的通信通道为一已授权状态，以提供移动终端 414 接入网络 300。更进一步来说，因为移动终端 414 与 AR-RS407 都有 TEK714（或 TEK614），因此双方都可以交换已加密的数据传输。

[0046] 图 8 为根据本发明之一切换程序的另一实施例的信号流程图，该切换程序是由连结到一目前基站的一 AR-RS，如 AR-RS407 连结到基站 400，转换到连结到一相异的目标基站 804 的一目标 AR-RS802。在图 8 中，移动终端 414 传送一连结信息 702 至一目标 AR-RS802，其中连结信息 702 包括一安全数据辨识码，如 AKID。

[0047] 因为对 AR-RS407 的优先认证，AKID 辨识目前储存在移动终端 414 的一存储器内的 AK，该存储器可能是存储器 526、ROM524、RAM522 或数据库 528。在一 AK 确认信号要求 (verification signal request)704 内，目标 AR-RS802 传送 AKID 至基站 804，用以确认储存在移动终端 414 的 AK 与储存在目标基站 804 的存储器内的 AK 是否符合，该存储器可能是存储器 526、ROM524、RAM522 或数据库 528。AR-RS802 与 AR-RS407 并不是与相同的基站通信，因此并没有共享相同的中继密钥 401，但是 AR-RS802 与目标基站 804 共享一相同的中继密钥 802。如果在基站 804 内目前的 AK 与移动终端 414 存储器内的 AK 相符，基站 804 传送一认证成功信息 (VerificationSuccess message) 至 AR-RS802。如果在基站 804 内目前的 AK 与移动终端 414 存储器内的 AK 不相符或是移动终端并没有持有一 AK，基站 804 传送一认证失败信息 (Verification Failure message)808 至 AR-RS802。在图 8 的实施例中，因为移动终端 414 前一次是通过基站 400 认证，移动终端 414 目前持有的 AK 或 AK610 都与基站 804 持有的 AK 不符，或是基站 804 根本就没有对应到移动终端 414 的任何 AK，因此基站 804 传送一认证失败信息 808 至移动终端 414。当移动终端 414 接收到认证失败信息 808，移动终端 414 与 AAA 服务器 104 执行一 IEEE802.1X 完整验证程序 206，以从基站 804 获得新的 MSK810、PMK812 以及 AK414。

[0048] 当基站 804 与移动终端 414 都握有 AK814 时，两者可以从 AK814 中得到 MACK820 与 KEK816，并且执行一 SA-TEK 三次握手程序来互相认证。当 SA-TEK 三次握手程序 214 被成功的完成时，基站 804 会产生新的 TEK818 并传送新的 TEK818 或旧的 TEK712 至移动终端 414，以提供在中继站 407 与移动终端 407 之间的数据机密性，其中基站 804 传送的 TEK818 或 TEK712 是受到 KEK816 的保护。

[0049] 基站 804 也会传送 TEK818 与 MACK820 至 AR-RS802，其中 TEK818 与 MACK820 亦是受到 KEK816 的保护。在 AR-RS802 得到 TEK818 与 MACK820 后，AR-RS802 切换在移动终端 414 与 AR-RS407 之间的通信通道为一已授权状态，以提供移动终端 414 接入网络 300。更进一步来说，因为移动终端 414 与 AR-RS802 都有 TEK818 与 MACK820，因此双方都可以交换已加密的数据传输。

[0050] 虽然上述的初始化程序与切换程序也同样可以应用在移动中继站，移动中继站与

利用移动中继站接入网络的移动终端必需要准备好以应付基站的变动，其中 AR-RS，特别是移动中继站，并不会改变。

[0051] 图 9 为根据本发明之一切换程序的另一实施例的信号流程图，该切换程序是一移动中继站由一目前基站切换到另一基站。在图 9 中，当移动中继站 AR-RS408 移动到基站 900 覆盖的范围内时，移动中继站 AR-RS408 会与基站 900 产生关联。移动终端 416 与 418 被连接到 AR-RS408，且移动终端与 AR-RS408 之间的连接通过基站 900 是被更好的维持。当 AR-RS408 接近或在基站 900 覆盖的范围内时，为了更新移动终端 416 与 418 的 AK，AR-RS408 会优先传送一量测距离信息 (ranging message)902 至移动终端 416 与 418，以通知移动终端 416 与 418 必须更新其本身拥有的安全数据。当接受到量测 距离信息 902 的接收回应时，AR-RS408 必需接收一 AK，且接受与对一移动终端认证相类似的认证。网关 106 可能在一 AK 转传 (transfer)904 内，传送 AK 给移动中继站。

[0052] AR-RS408 传送一再认证触发信息 (re-authentication trigger message) 或安全数据更新信息 906 至移动终端 416 与 418。再认证触发信息 906 可能会被以多播的传送方式传送至移动终端 416 与 418。当接受到再认证触发信息 906 的接收回应时，移动终端 416 至 418 与 AAA 服务器 104 以及网关 106 进行一 IEEE802.1X 完整认证程序 206。网关 106 从网关中既有的 PMK 计算一新的 AK 给基站 900。在 AK 转传 908 中，网关 106 且 / 或 AAA 服务器 104 可能会传送所有与 AR-RS408 有关的移动终端的安全数据，如 AK，给基站 900，且可利用隧道模式 (tunnel mode)，一次性的同时传输所有与 AR-RS408 连结的移动终端的所有参数，如 AK，给基站 900。在隧道模式中，两点之间的逻辑连接，如 AR-RS408 与网关 106，是专用的，而且中介节点 (intermediatenode) 并不会处理隧道封包，而只是转递隧道封包。移动终端 416 与 418 接着与基站 900 执行一 SA-TEK 三次握手程序 214。基站 900 会在一 TEK 转传 910 中，将每一个移动终端的 TEK 与 MACK 传送给 AR-RS408，而且可利用隧道模式完成。在一实施例中，基站 900 会聚集每一个移动终端的安全数据，并在 TEK 转传 910 中，以一信息聚集模式 (message aggregation mode) 传送给 AR-RS408。在一实施例中，基站 900、移动终端 416 与 418 接收到的多个 TEK 与 MAC 会先优先使用在基站间切换 (inter-base station handoff)，以避免移动终端 416 与 418 内的服务断线。AR-RS408 接着会提供安全数据传输给移动终端 416 与 418，且可以无用对移动终端 416 与 418 执行认证程序。此外 AR-RS408 可以只更新移动终端 416 与 418 内的认证数据，且在另外的实施例中，AR-RS408 可不改变 416 与 / 或 418 所持有的 TEK。

[0053] 虽然图 9 表示的是基站 900 通过网关 106 来跟网络与 AAA 服务器 104 通信，但本领域普通技术人员当可根据图 9 所描述的方法，得知基站 900 如何过网关 108 来跟网络与 AAA 服务器 104 通信。

[0054] 在此公开的系统及方法可实施在数字电子电路或在电脑硬件、固件、软件、或其结合。利用本发明的装置可实施在电脑程序产品，此电脑程序产品包含在关于可程序化处理器所执行的机械可读取储存装置。包含本发明的方法步骤可由可程序化处理器来执行，其实行指令程序，以藉由根据输入数据 的操作及产生输出信号来执行本发明的功能。包含本发明的实施例可实施在可程序化系统中可执行的一或多个电脑程序，其包括用来接收来自储存系统的数据以及传送数据至储存系统的至少一个可程序化处理器、至少一个输入装置、以及至少一个输出装置。电脑程序可实施在高阶或物件导向程序语言、以及 / 或组合或

机械编码。语言或编码可以示编译或翻译语言或编码。处理器可包括一般或专用定制微处理器。处理器接收来自存储器的指令或数据。包含电脑程序指令和数据的储存装置包括所有型态的非易失存储器，包括半导体存储装置，例如 EPROM、EEPROM、以及快闪存储装置；磁盘机，例如内部硬盘及卸除式硬盘；以及 CD-ROM。上述的任一种可由 ASIC 来补充或包含在 ASIC 内。

[0055] 本技术领域的人士可知，不同的修改和变化可应用于在无线通讯系统中建立安全关联的系统及方法。例如，本技术领域的人士可了解范围请求和回应是一种信号讯息类型，且其他信号讯息可被使用。此外，本技术领域的人士可了解，流量编码密钥是一种流量密钥的类型，而其他流量密钥可被使用，且 MACK 是一种认证密钥的类型，而其他认证密钥可被使用。本技术领域的人士也可了解，基站与中继站之间可以是无线通讯或有线通讯。本发明虽以优选实施例公开如上，然其并非用以限定本发明的范围，任何所属技术领域中具有通常知识者，在不脱离本发明的精神和范围内，当可做些许的更动与润饰，因此本发明的保护范围当视后附之权利要求书所界定者为准。

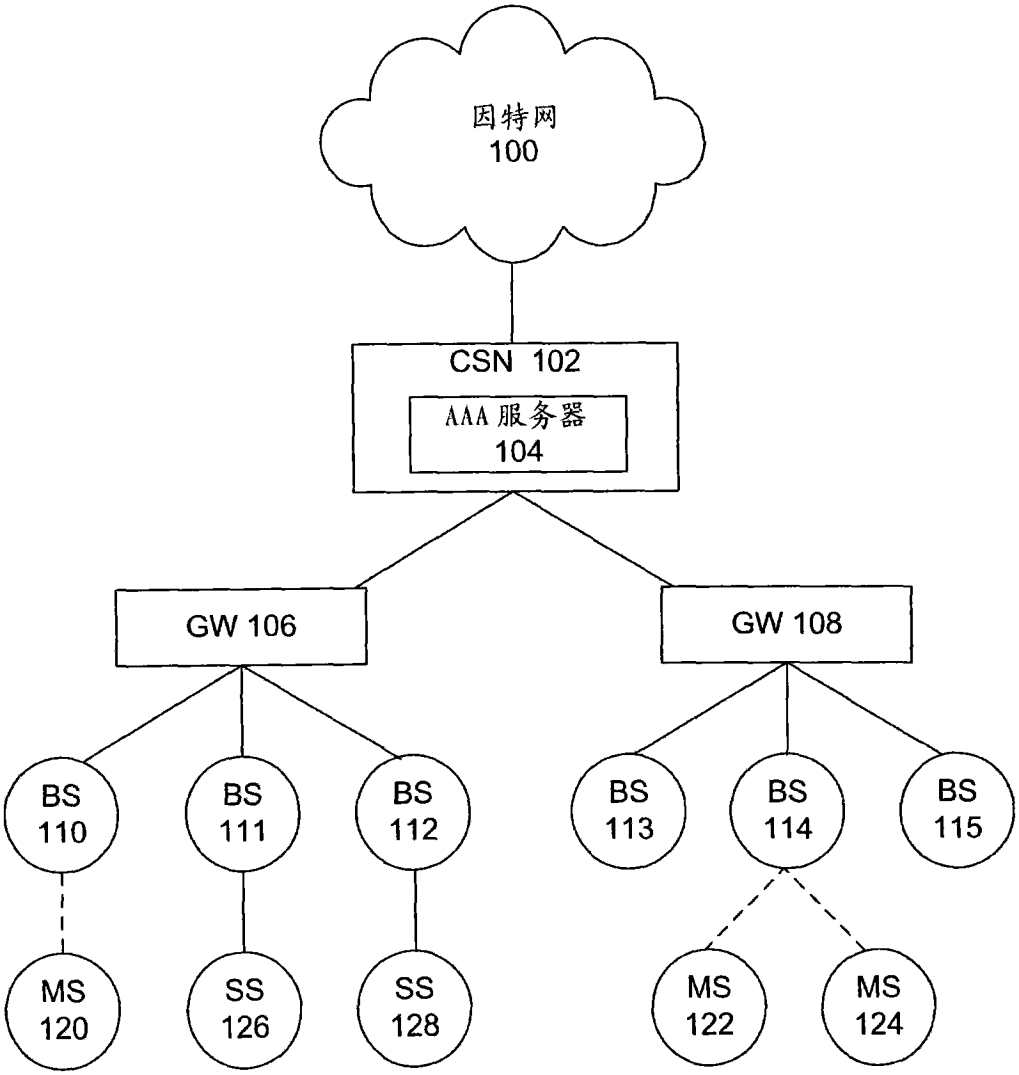

因特网
100
CSN 102
AAA 服务器
104
GW 106
GW 108
BS
110
BS
111
BS
112
BS
113
BS
114
BS
115
MS
120
SS
126
SS
128
MS
122
MS
124

图 1

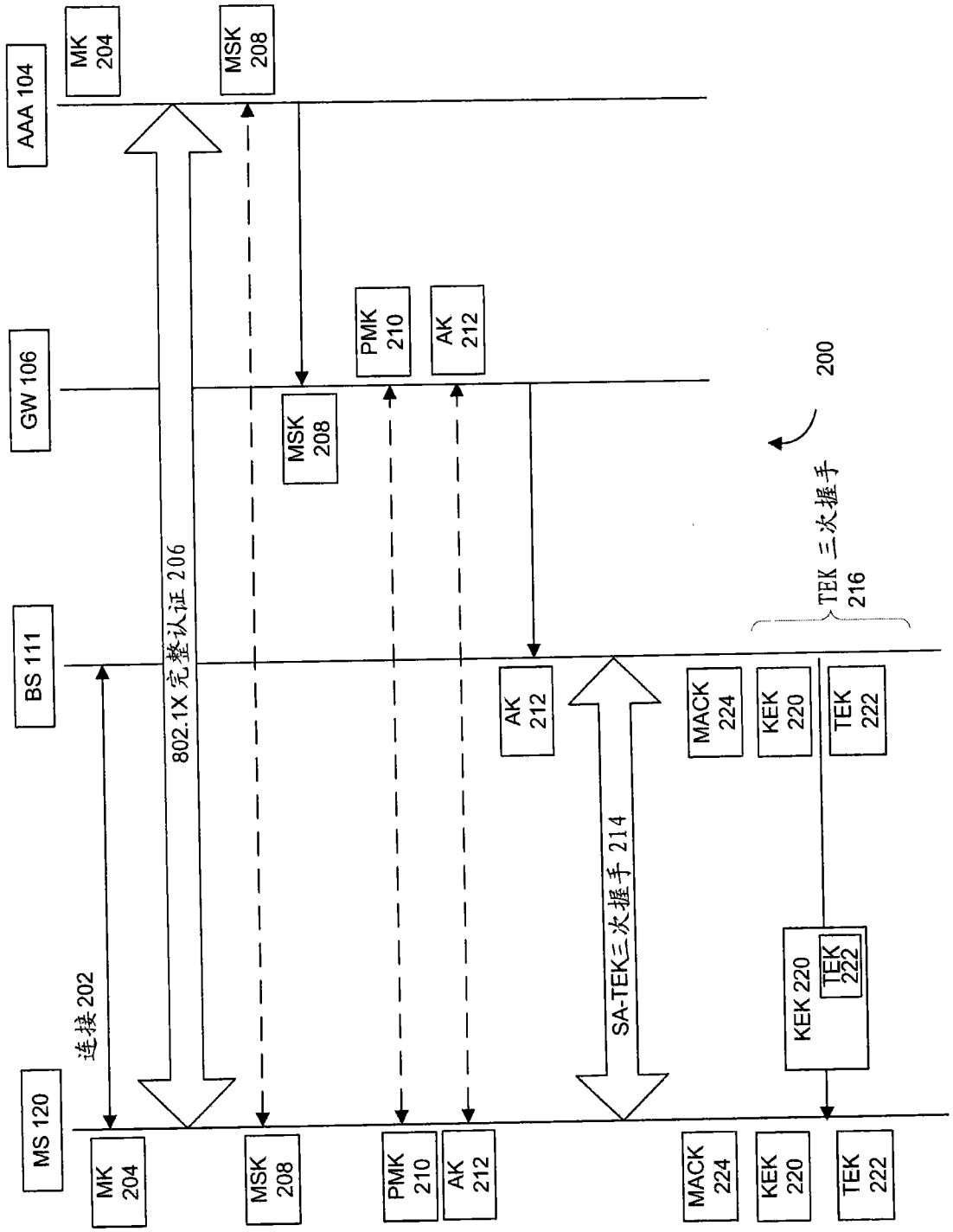

AAA 104
MK 204
MSK 208
GW 106
PMK 210
AK 212
MSK 208
200
TEK 三次握手 216
BS 111
802.1X完整认证 206
AK 212
MACK 224
KEK 220
TEK 222
SA-TEK三次握手 214
连接 202
KEK 220
TEK 222
MS 120
MK 204
MSK 208
PMK 210
AK 212
MACK 224
KEK 220
TEK 222

图 2

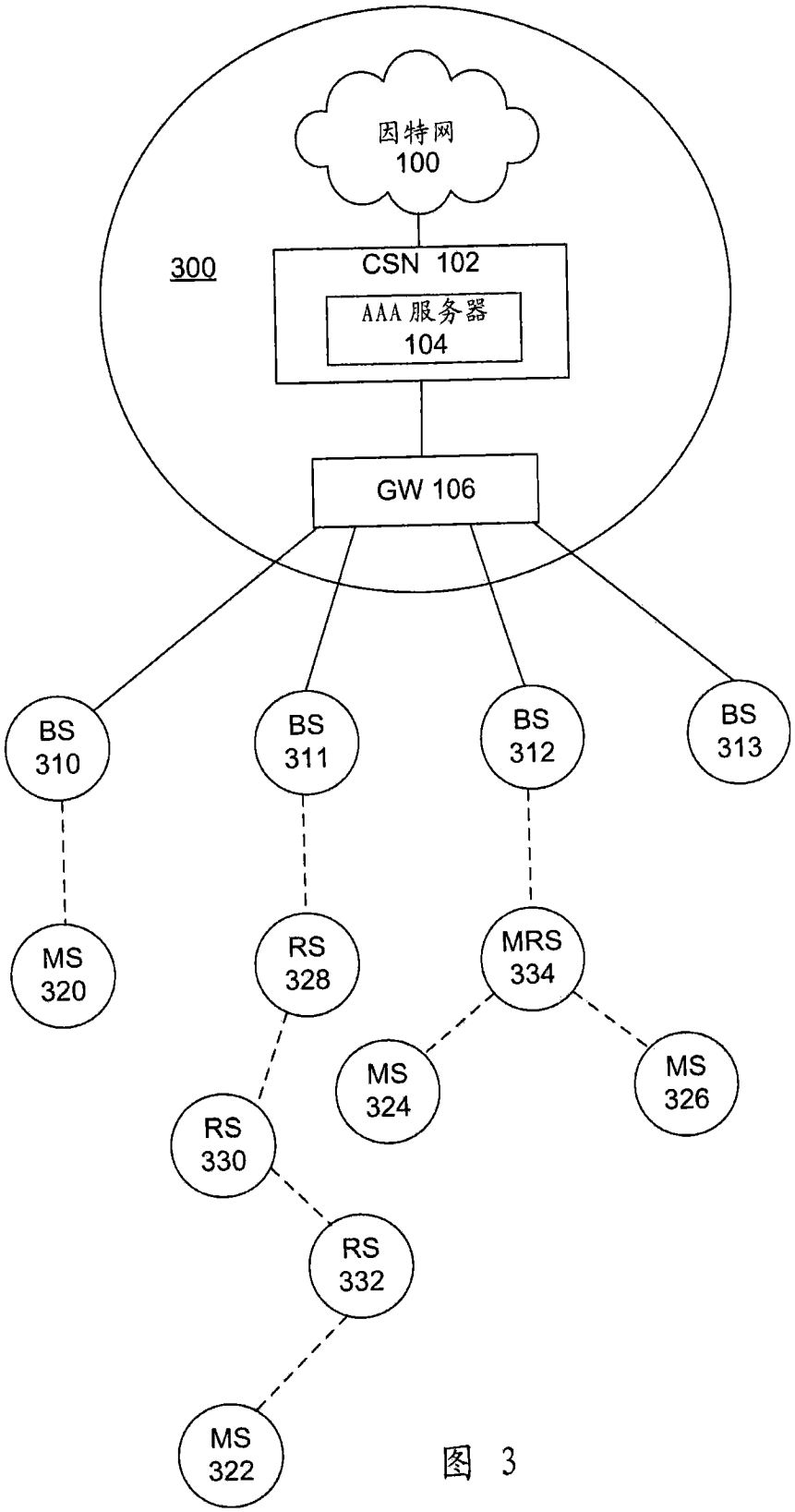

因特网
100
300
CSN 102
AAA 服务器
104
GW 106
BS
310
BS
311
BS
312
BS
313
MS
320
RS
328
MRS
334
MS
324
MS
326
RS
330
RS
332
MS
322

图 3

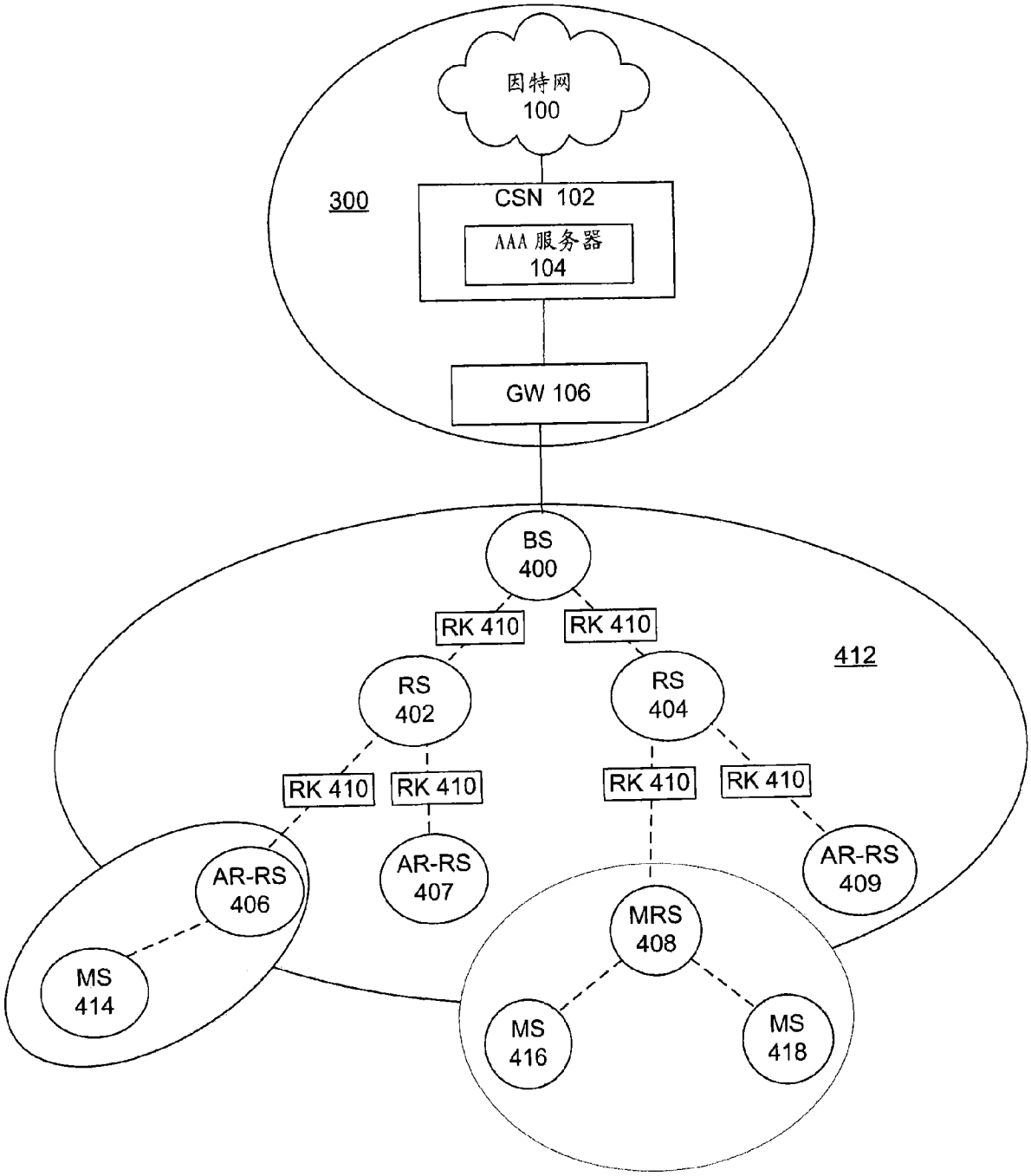

因特网
100
300
CSN 102
AAA 服务器
104
GW 106
BS
400
RK 410
RK 410
412
RS
402
RS
404
RK 410
RK 410
RK 410
RK 410
AR-RS
406
AR-RS
407
AR-RS
409
MRS
408
MS
414
MS
416
MS
418

图 4

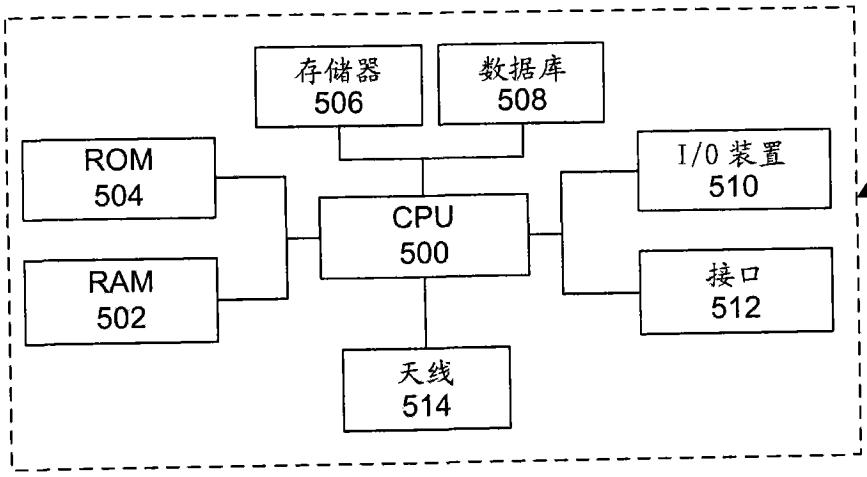

存储器
506
数据库
508
ROM
504
I/O 装置
510
400
CPU
500
RAM
502
接口
512
天线
514

图 5A

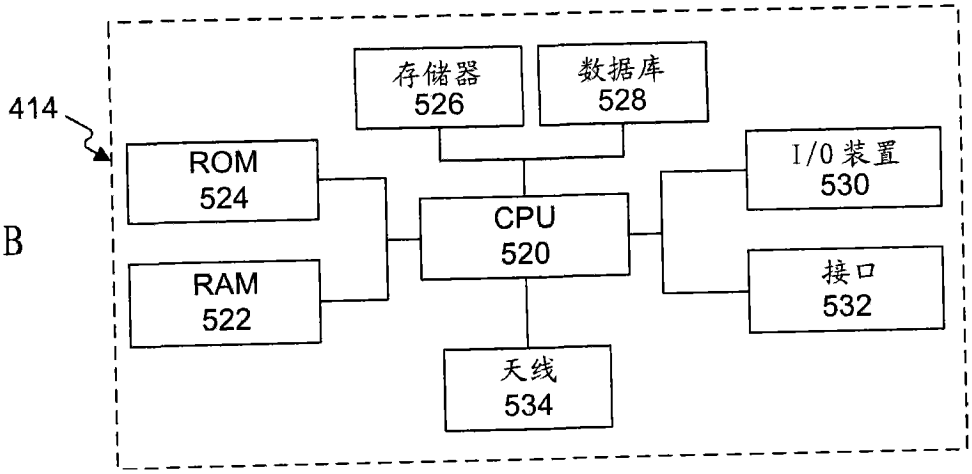

414
存储器
526
数据库
528
ROM
524
I/O 装置
530
CPU
520
RAM
522
接口
532
天线
534

图 5B

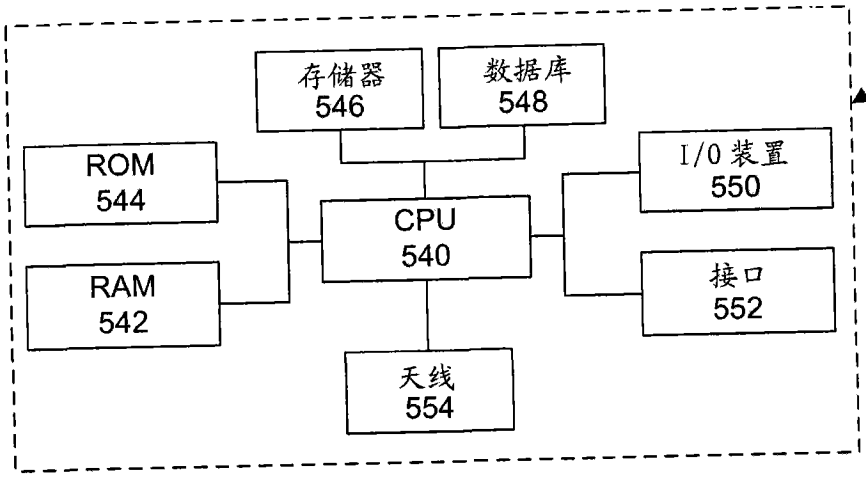

406 - 409
存储器
546
数据库
548
ROM
544
I/O 装置
550
CPU
540
RAM
542
接口
552
天线
554

图 5C

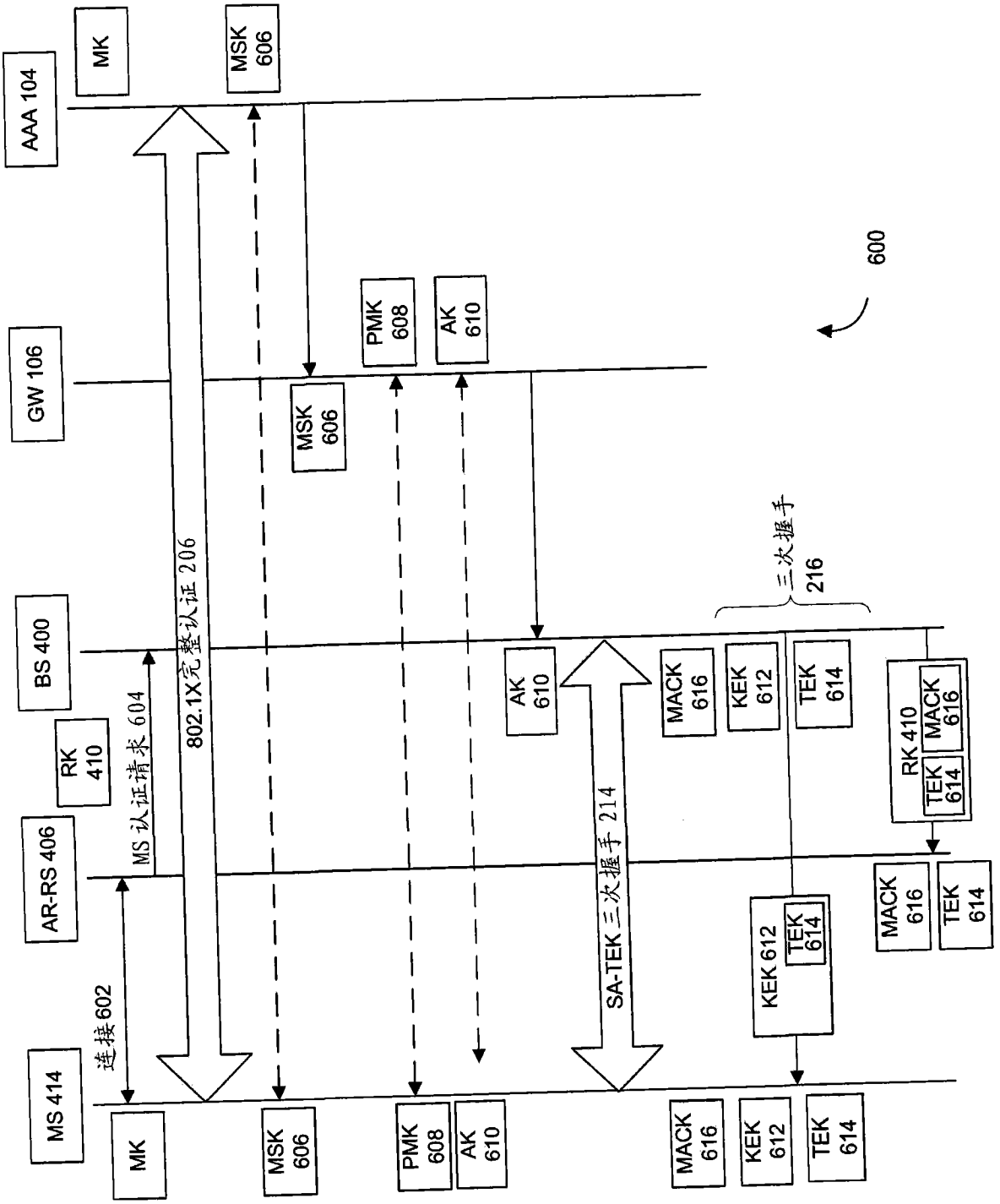

AAA 104
MK
MSK 606
GW 106
PMK 608
AK 610
600
802.1X完整认证 206
三次握手 216
BS 400
RK 410
MS认证请求 604
AR-RS 406
SA-TEK三次握手 214
MACK 616
KEK 612
TEK 614
连接 602
MS 414

图 6

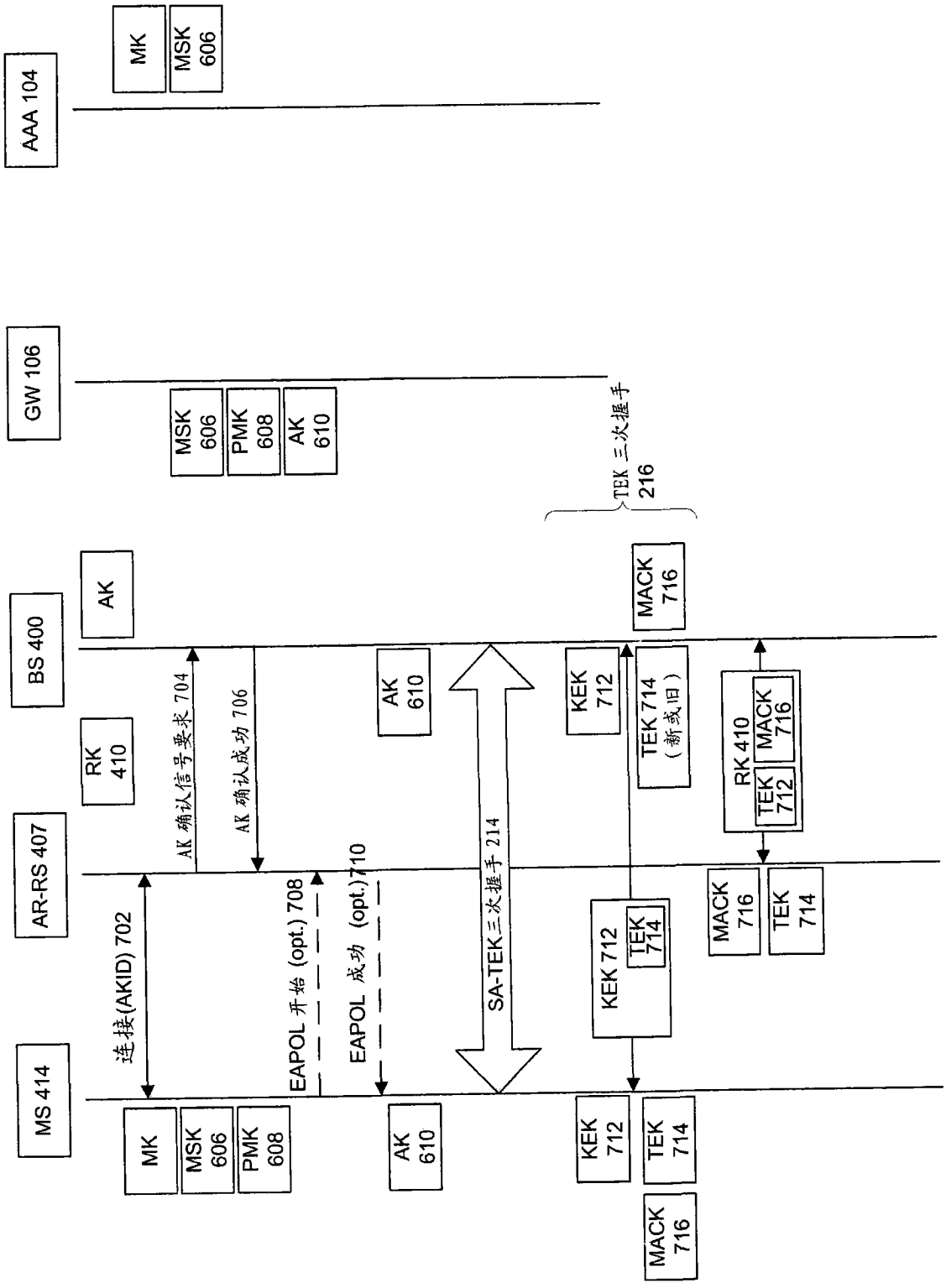

AAA 104
MK
MSK 606
GW 106
MSK 606
PMK 608
AK 610
TEK 三次握手 216
BS 400
AK
MACK 716
RK 410
AK 确认信号要求 704
AK 确认成功 706
AK 610
KEK 712
TEK 714 (新或旧)
RK 410
TEK 712
MACK 716
AR-RS 407
连接(AKID) 702
EAPOL 开始 (opt.) 708
EAPOL 成功 (opt.) 710
SA-TEK三次握手 214
KEK 712
TEK 714
MACK 716
TEK 714
MS 414
MK
MSK 606
PMK 608
AK 610
KEK 712
TEK 714
MACK 716

图 7

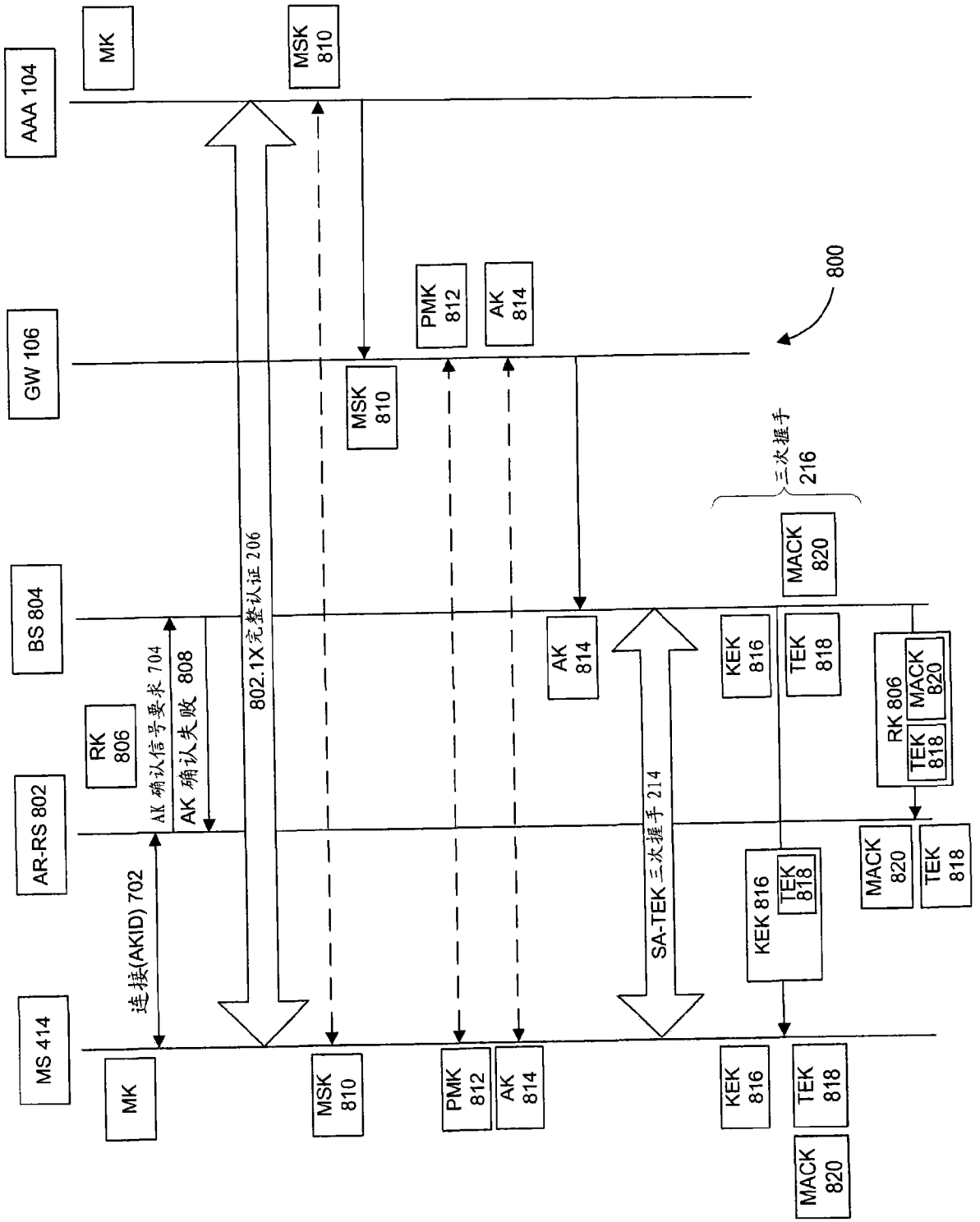

AAA 104
GW 106
BS 804
AR-RS 802
MS 414
MK
MSK 810
PMK 812
AK 814
800
三次握手 216
MACK 820
KEK 816
TEK 818
RK 806
802.1X完整认证 206
AK 确认信号要求 704
AK 确认失败 808
连接(AKID) 702
SA-TEK 三次握手 214

图 8

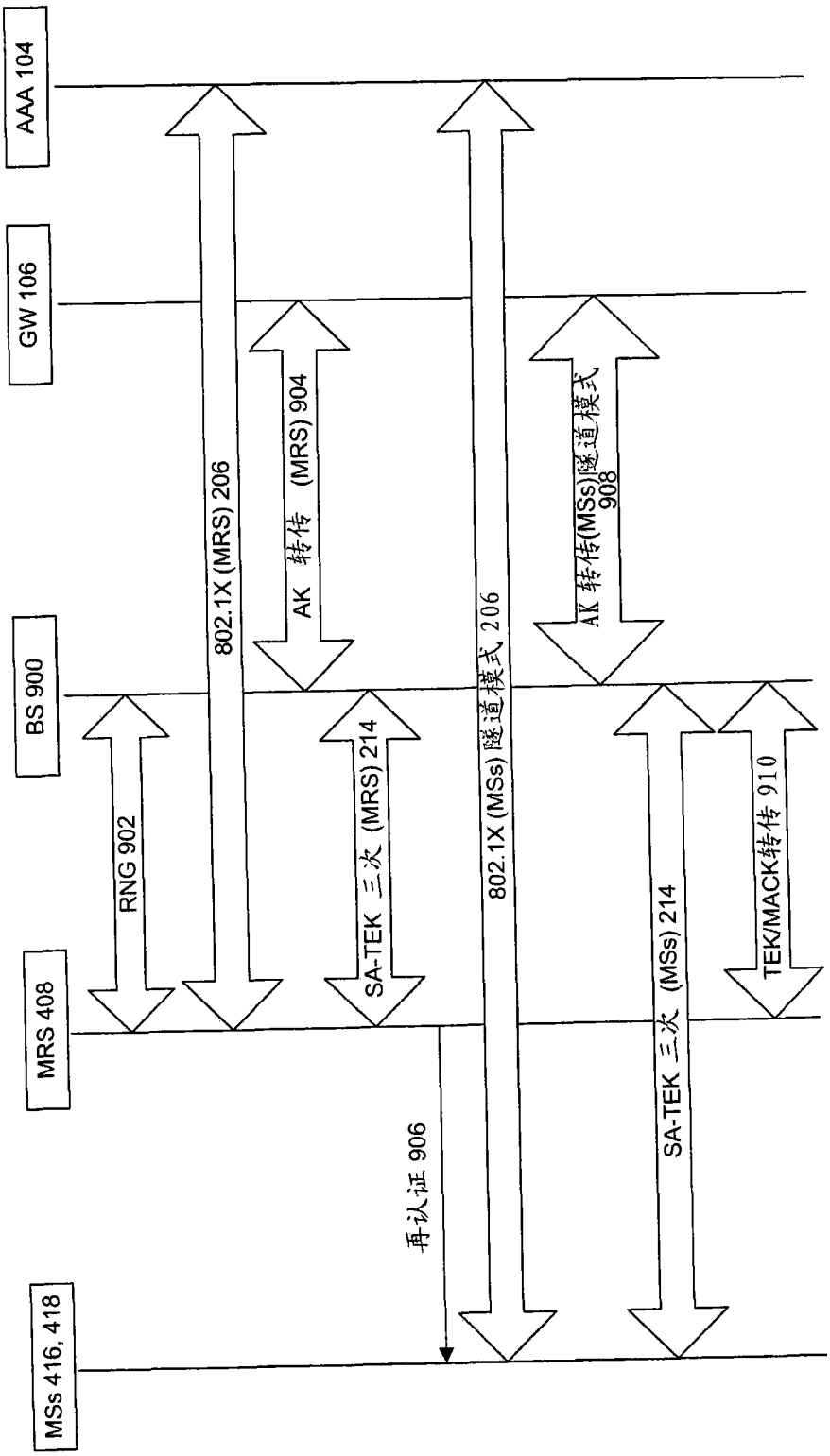

AAA 104
GW 106
BS 900
MRS 408
MSs 416, 418
802.1X (MRS) 206
AK 转传 (MRS) 904
AK 转传(MSs)隧道模式 908
RNG 902
SA-TEK 三次 (MRS) 214
802.1X (MSs) 隧道模式 206
SA-TEK 三次 (MSs) 214
TEK/MACK转传 910
再认证 906

图 9