(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102932783 A
(43)申请公布日 2013.02.13

(21)申请号 201210468977.7
(22)申请日 2007.09.24
(30)优先权数据
60/847,195 2006.09.25 US
11/858,714 2007.09.20 US
(62)分案原申请数据
200780035404.2 2007.09.24
(71)申请人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 A·C·马亨德兰 徐大生
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英

(51)Int.Cl.
H04W 12/02(2009.01)

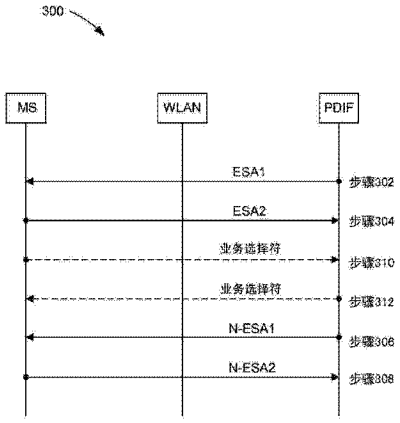
权利要求书 4 页 说明书 7 页 附图 4 页

(54)发明名称

具有用于移动台和安全网关之间的信令和媒体分组的空加密的方法和装置

(57)摘要

公开了一种用于通过无线局域网在移动台和安全网关之间高效传输分组以访问归属地服务的方法。在该方法中，建立第一加密安全关联以用于将第一类型分组从安全网关传输到移动台，并且建立第二加密安全关联以用于将第一类型分组从移动台传输到安全网关。接下来，建立第一空加密安全关联以用于将第二类型分组从安全网关传输到移动台，并且建立第二空加密安全关联以用于将第二类型分组从移动台传输到安全网关。基于业务选择符来选择用于使用第二空加密安全关联来传输的第二类型分组。而且，可以基于业务选择符来选择用于使用第一空加密安全关联来传输的第二类型分组。该业务选择符可以是预配置的。



CN 102932783 A

1. 一种用于传输分组的方法，包括：

建立针对移动台和安全网关之间的分组业务的加密安全关联；

建立针对所述移动台和所述安全网关之间的分组业务的空加密安全关联；以及

基于业务选择符来选择使用所述空加密安全关联进行传输的分组，其中，所述空加密安全关联应用于一个或多个 IMS 分组流，并且其中，所述加密安全关联至少应用于非 IMS 分组流。

2. 根据权利要求 1 所述的方法，其中，所述空加密安全关联应用于 SIP 信令消息。

3. 根据权利要求 2 所述的方法，其中，所述选择包括将所述 SIP 信令消息映射到被空加密的子安全关联。

4. 根据权利要求 1-3 中任意一项所述的方法，其中，所述空加密安全关联应用于 VoIP 分组。

5. 根据权利要求 1-4 中任意一项所述的方法，其中，所述加密安全关联包括 IPsec SA。

6. 根据权利要求 1-5 中任意一项所述的方法，其中，所述安全网关包括分组数据互通功能体。

7. 根据权利要求 1-6 中任意一项所述的方法，其中，所述加密安全关联或所述空加密安全关联包括 IP 隧道。

8. 根据权利要求 7 所述的方法，其中，所述选择包括将所述分组引导到所述 IP 隧道。

9. 根据权利要求 1-8 中任意一项所述的方法，其中，所述加密安全关联或所述空加密安全关联是使用 IKEv2 来建立的。

10. 根据权利要求 1-9 中任意一项所述的方法，还包括使用 IKEv2 来配置所述业务选择符。

11. 根据权利要求 1-10 中任意一项所述的方法，其中，所述业务选择符包括 IP 地址或端口号。

12. 根据权利要求 1-11 中任意一项所述的方法，其中，建立所述加密安全关联包括建立第一加密安全关联以用于将分组业务通过无线局域网从所述安全网关传输到所述移动台，所述方法还包括建立第二加密安全关联以用于将分组业务通过所述无线局域网从所述移动台传输到所述安全网关。

13. 根据权利要求 1-12 中任意一项所述的方法，其中，建立所述空加密安全关联包括建立第一空加密安全关联以用于将分组业务通过无线局域网从所述安全网关传输到所述移动台，所述方法还包括建立第二空加密安全关联以用于将分组业务通过所述无线局域网从所述移动台传输到所述安全网关。

14. 一种移动台，包括：

用于建立针对所述移动台和安全网关之间的分组业务的加密安全关联的模块；

用于建立针对所述移动台和所述安全网关之间的分组业务的空加密安全关联的模块；以及

用于基于业务选择符来选择使用所述空加密安全关联进行传输的分组的模块，其中，所述空加密安全关联应用于一个或多个 IMS 分组流，并且其中，所述加密安全关联至少应用于非 IMS 分组流。

15. 根据权利要求 14 所述的移动台，其中，所述空加密安全关联应用于 SIP 信令消息。

16. 根据权利要求 15 所述的移动台，其中，所述用于基于业务选择符来选择使用所述空加密安全关联进行传输的分组的模块包括用于将所述 SIP 信令消息映射到被空加密的子安全关联的模块。

17. 根据权利要求 14-16 中任意一项所述的移动台，其中，所述空加密安全关联应用于 VoIP 分组。

18. 根据权利要求 14-17 中任意一项所述的移动台，其中，所述加密安全关联包括 IPsec SA。

19. 根据权利要求 14-18 中任意一项所述的移动台，其中，所述安全网关包括分组数据互通功能体。

20. 根据权利要求 14-19 中任意一项所述的移动台，其中，所述加密安全关联或所述空加密安全关联包括 IP 隧道。

21. 根据权利要求 20 所述的移动台，其中，所述用于基于业务选择符来选择使用所述空加密安全关联进行传输的分组的模块包括用于将所述分组引导到所述 IP 隧道的模块。

22. 根据权利要求 14-21 中任意一项所述的移动台，其中，所述加密安全关联或所述空加密安全关联是使用 IKEv2 来建立的。

23. 根据权利要求 14-22 中任意一项所述的移动台，还包括用于使用 IKEv2 来配置所述业务选择符的模块。

24. 根据权利要求 14-23 中任意一项所述的移动台，其中，所述业务选择符包括 IP 地址或端口号。

25. 根据权利要求 14-24 中任意一项所述的移动台，其中，用于建立针对所述移动台和安全网关之间的分组业务的加密安全关联的模块包括用于建立第一加密安全关联以用于将分组业务通过无线局域网从所述安全网关传输到所述移动台的模块，所述移动台还包括用于建立第二加密安全关联以用于将分组业务通过所述无线局域网从所述移动台传输到所述安全网关的模块。

26. 根据权利要求 14-25 中任意一项所述的移动台，其中，用于建立针对所述移动台和所述安全网关之间的分组业务的空加密安全关联的模块包括用于建立第一空加密安全关联以用于将分组业务通过无线局域网从所述安全网关传输到所述移动台的模块，所述移动台还包括用于建立第二空加密安全关联以用于将分组业务通过所述无线局域网从所述移动台传输到所述安全网关的模块。

27. 一种计算机可读介质，包括：

用于建立针对移动台和安全网关之间的分组业务的加密安全关联的代码；

用于建立针对所述移动台和所述安全网关之间的分组业务的空加密安全关联的代码；以及

用于基于业务选择符来选择使用所述空加密安全关联进行传输的分组的代码，其中，所述空加密安全关联应用于一个或多个 IMS 分组流，并且其中，所述加密安全关联至少应用于非 IMS 分组流。

28. 根据权利要求 27 所述的计算机可读介质，其中，所述空加密安全关联应用于 SIP 信令消息。

29. 根据权利要求 28 所述的计算机可读介质，其中，所述用于基于业务选择符来选择

使用所述空加密安全关联进行传输的分组的代码包括用于将所述 SIP 信令消息映射到被空加密的子安全关联的代码。

30. 根据权利要求 27-29 中任意一项所述的计算机可读介质，其中，所述空加密安全关联应用于 VoIP 分组。

31. 根据权利要求 27-30 中任意一项所述的计算机可读介质，其中，所述加密安全关联包括 IPsec SA。

32. 根据权利要求 27-31 中任意一项所述的计算机可读介质，其中，所述安全网关包括分组数据互通功能体。

33. 根据权利要求 27-32 中任意一项所述的计算机可读介质，其中，所述加密安全关联或所述空加密安全关联包括 IP 隧道。

34. 根据权利要求 33 所述的计算机可读介质，其中，所述用于基于业务选择符来选择使用所述空加密安全关联进行传输的分组的代码包括用于将所述分组引导到所述 IP 隧道的代码。

35. 根据权利要求 27-34 中任意一项所述的计算机可读介质，其中，所述加密安全关联或所述空加密安全关联是使用 IKEv2 来建立的。

36. 根据权利要求 27-35 中任意一项所述的计算机可读介质，还包括用于使用 IKEv2 来配置所述业务选择符的代码。

37. 根据权利要求 27-36 中任意一项所述的计算机可读介质，其中，所述业务选择符包括 IP 地址或端口号。

38. 根据权利要求 27-37 中任意一项所述的计算机可读介质，其中，用于建立针对移动台和安全网关之间的分组业务的加密安全关联的代码包括用于建立第一加密安全关联以用于将分组业务通过无线局域网从所述安全网关传输到所述移动台的代码，所述计算机可读介质还包括用于建立第二加密安全关联以用于将分组业务通过所述无线局域网从所述移动台传输到所述安全网关的代码。

39. 根据权利要求 27-38 中任意一项所述的计算机可读介质，其中，用于建立针对所述移动台和所述安全网关之间的分组业务的空加密安全关联的代码包括用于建立第一空加密安全关联以用于将分组业务通过无线局域网从所述安全网关传输到所述移动台的代码，所述计算机可读介质还包括用于建立第二空加密安全关联以用于将分组业务通过所述无线局域网从所述移动台传输到所述安全网关的代码。

40. 一种装置，包括：

存储器；以及

处理器，用于建立针对移动台和安全网关之间的分组业务的加密安全关联，建立针对所述移动台和所述安全网关之间的分组业务的空加密安全关联，以及基于业务选择符来选择使用所述空加密安全关联进行传输的分组，其中，所述空加密安全关联应用于一个或多个 IMS 分组流，并且其中，所述加密安全关联至少应用于非 IMS 分组流。

41. 根据权利要求 40 所述的装置，其中，所述空加密安全关联应用于 SIP 信令消息。

42. 根据权利要求 41 所述的装置，其中，所述选择包括将所述 SIP 信令消息映射到被空加密的子安全关联。

43. 根据权利要求 40-42 中任意一项所述的装置，其中，所述空加密安全关联应用于

VoIP 分组。

44. 根据权利要求 40-43 中任意一项所述的装置，其中，所述加密安全关联包括 IPsec SA。

45. 根据权利要求 40-44 中任意一项所述的装置，其中，所述安全网关包括分组数据互通功能体。

46. 根据权利要求 40-45 中任意一项所述的装置，其中，所述加密安全关联或所述空加密安全关联包括 IP 隧道。

47. 根据权利要求 46 所述的装置，其中，所述选择包括将所述分组引导到所述 IP 隧道。

48. 根据权利要求 40-47 中任意一项所述的装置，其中，所述加密安全关联或所述空加密安全关联是使用 IKEv2 来建立的。

49. 根据权利要求 40-48 中任意一项所述的装置，其中，所述处理器还用于使用 IKEv2 来配置所述业务选择符。

50. 根据权利要求 40-49 中任意一项所述的装置，其中，所述业务选择符包括 IP 地址或端口号。

51. 根据权利要求 40-50 中任意一项所述的装置，其中，建立所述加密安全关联包括建立第一加密安全关联以用于将分组业务通过无线局域网从所述安全网关传输到所述移动台，所述处理器还用于建立第二加密安全关联以用于将分组业务通过所述无线局域网从所述移动台传输到所述安全网关。

52. 根据权利要求 40-51 中任意一项所述的装置，其中，建立所述空加密安全关联包括建立第一空加密安全关联以用于将分组业务通过无线局域网从所述安全网关传输到所述移动台，所述处理器还用于建立第二空加密安全关联以用于将分组业务通过所述无线局域网从所述移动台传输到所述安全网关。

具有用于移动台和安全网关之间的信令和媒体分组的空加密的方法和装置

[0001] 基于 35U.S.C. §119 要求优先权

[0002] 本申请是 2007 年 9 月 24 日提交的、申请号为 200780035404.2 的、发明名称为“具有用于移动台和安全网关之间的信令和媒体分组的空加密的方法和装置”的申请的分案申请。本申请要求享有 2006 年 9 月 25 日递交的名称为“NULL-ENCRYPTION FOR SIP SIGNALING AND MEDIA PACKETS BETWEEN MS AND PDIF”的临时申请 No.60/847,195 的优先权。该临时申请被转让给本受让人并通过引用明确地并入本文。

技术领域

[0003] 本发明概括地说涉及无线通信领域，更具体地涉及选择性内容保护。

背景技术

[0004] 通信技术具有许多应用领域，包括例如，寻呼、无线本地环路、因特网电话和卫星通信系统。一种示例性应用是用于移动用户的蜂窝电话系统。（如这里所使用的，术语“蜂窝”系统包括蜂窝和个人通信服务（PCS）系统频率。）已经针对这种蜂窝系统开发了被设计成允许多个用户访问公共通信介质的现代通信系统，比如无线通信系统。这些现代通信系统可以基于多址技术，比如码分多址（CDMA）、时分多址（TDMA）、频分多址（FDMA）、空分多址（SDMA）、极分多址（PDMA）或本领域公知的其它调制技术。这些调制技术对从通信系统的多个用户接收的信号进行解调，从而能够增加通信系统的容量。与此相关，已经建立了各种无线通信系统，包括例如，先进移动电话服务（AMPS）、全球移动通信系统（GSM）和其它无线系统。

[0005] 在 FDMA 系统中，将总频谱划分为多个更小的子带，并且给每个用户指定自己的子带以接入通信介质。可替换地，在 TDMA 系统中，将总频谱划分为多个更小的子带，每个子带在多个用户之间共享，并且允许每个用户在预定时隙中使用该子带进行发送。CDMA 系统相比其它类型的系统提供了潜在的优势，包括增加了系统容量。在 CDMA 系统中，给每个用户指定了所有时间内的整个频谱，但是通过使用唯一的编码来区分每个用户的传输。

[0006] CDMA 系统可以设计为支持一个或多个 CDMA 标准，比如（1）“用于双模宽带扩频蜂窝系统的 TIA/EIA-95-B 移动台 - 基站兼容标准”（IS-95 标准），（2）由名为“第 3 代合作伙伴项目”（3GPP）的组织提供的并且体现在一系列文档中的标准，这些文档包括文档 No.3G TS 25.211、No.3G TS25.212、No.3G TS 25.213 和 No.3G TS 25.214（W-CDMA 标准），以及（3）由名为“第 3 代合作伙伴项目 2”（3GPP2）的组织提供的并且体现在“用于 cdma2000 扩频系统的 TR-45.5 物理层标准”（IS-2000 标准）中的标准。

[0007] 在上述 CDMA 通信系统和标准中，在多个用户之间同时共享可用频谱，并且可以利用适当技术来提供服务，比如语音和数据服务。

[0008] 典型移动用户使用诸如移动电话或膝上型计算机的移动台或终端来接入无线通信系统。除语音通信外，移动台可以访问由归属地 3G 系统提供的其它网络数据服务，比如

即时消息服务(IMS)。

[0009] 移动台可以接入无线本地接入网(WLAN),其可以提供可选择的通信信道,用于访问由归属地 3G 系统提供的网络数据服务,而不使用归属地 3G 系统的“蜂窝”容量。图 1 示出了 3G-WLAN 交互架构。移动台(MS)经由无线局域网(WLAN)系统可以访问 MS 归属地网络中的服务。分组数据互通功能体(PDIF)作为安全网关,保护网络服务(例如,即时消息服务(IMS)),防止未授权的访问。IMS 是基于 SIP 的系统,其允许 MS 建立因特网语音协议(VoIP)呼叫。

[0010] 为了从 WLAN 系统访问 IMS 服务,MS 使用因特网密钥加密版本 2 (IKEv2)来与分组数据互通功能体(PDIF)建立安全 IP 隧道。由归属地鉴权认证计费(H-AAA)对该隧道的建立进行鉴权和认证。虚线是用于鉴权、认证、计费(AAA)信息的路径。实线是用户数据业务的承载路径,管道是保护 MS 和 PDIF 之间的用户数据业务的安全 IP 隧道。在建立安全 IP 隧道之后,MS 可以在 3G 归属地网络中注册 IMS。MS 使用会话启动协议(SIP)来与 IMS 中的控制实体(例如,代理呼叫会话控制功能(P-CSCF))进行通信。

[0011] 然而,该安全 IP 隧道对于特定业务类型来说效率低下。因此,在本领域中,对于移动台和 3G 网络来说,需要允许该移动台高效地访问由该 3G 网络提供的网络数据服务,而不使用该 3G 系统的“蜂窝”容量。

发明内容

[0012] 本发明的一方面在于一种用于通过无线局域网在移动台和安全网关之间高效传输分组以访问归属地服务的方法。在该方法中,建立第一加密安全关联以用于将第一类型分组从安全网关传输到移动台,并且建立第二加密安全关联以用于将第一类型分组从移动台传输到安全网关。接下来,建立第一空加密安全关联以用于将第二类型分组从安全网关传输到移动台,并且建立第二空加密安全关联以用于将第二类型分组从移动台传输到安全网关。基于业务选择符来选择用于使用第二空加密安全关联来传输的第二类型分组。而且,可以基于业务选择符来选择使用第一空加密安全关联来传输的第二类型分组。

[0013] 在本发明的更多具体方面中,业务选择符可以是预配置的并且为移动台和安全网关所已知。业务选择符可以是目的和 / 或源 IP 地址和端口号。

[0014] 此外,可以在建立第一和第二加密安全关联之前产生业务选择符,或者可以在建立第一和第二加密安全关联之后产生业务选择符。此外,移动台可以产生业务选择符并使用第二加密安全关联将该业务选择符转发给安全网关,或者安全网关可以产生业务选择符并使用第一加密安全关联转发该业务选择符。

[0015] 在本发明的其它更多具体方面中,第一和第二空加密安全关联均可以是子安全关联。每个安全关联可以是安全 IP 隧道。可以由第三代移动电话归属地网络来提供归属地服务。安全网关可以是分组数据互通功能体。所选择的用于使用第二空加密安全关联来传输的第二类型分组可以是先前加密的语音 IP 分组,或者其可以是先前加密的会话启动协议分组。

[0016] 本发明的另一方面可以在于一种移动台,其包括用于建立第一加密安全关联以用于将第一类型分组通过无线局域网从安全网关传输到移动台的模块,用于建立第二加密安全关联以用于将第一类型分组通过无线局域网从移动台传输到安全网关的模块,用于建立

第一空加密安全关联以用于将第二类型分组通过无线局域网从安全网关传输到移动台的模块，用于建立第二空加密安全关联以用于将第二类型分组通过无线局域网从移动台传输到安全网关的模块，以及用于基于业务选择符来选择使用第二空加密安全关联来传输的第二类型分组的模块。

[0017] 本发明的另一方面可以在于一种包括计算机可读介质的计算机程序产品，该计算机可读介质包括用于使计算机执行以下操作的代码：建立第一加密安全关联以用于将第一类型分组通过无线局域网从安全网关传输到移动台，建立第二加密安全关联以用于将第一类型分组通过无线局域网从移动台传输到安全网关，建立第一空加密安全关联以用于将第二类型分组通过无线局域网从安全网关传输到移动台，建立第二空加密安全关联以用于将第二类型分组通过无线局域网从移动台传输到安全网关，以及基于业务选择符来选择使用第二空加密安全关联来传输的第二类型分组。

附图说明

[0018] 图 1 是通过无线局域网与归属地 3G 系统进行通信的移动台的方框图。

[0019] 图 2 是无线通信系统的实例。

[0020] 图 3 是用于在移动台和安全网关之间建立安全关联的方法的流程图。

[0021] 图 4 是移动台的方框图。

具体实施方式

[0022] 词语“示例性”在这里用于表示“作为实例、例子或图示”。没有必要将这里描述为“示例性”的任何实施例均视为比其它实施例更优选或有利。

[0023] 也称为移动台（MS）、接入终端（AT）、用户设备或用户单元的远程站可以是移动的或固定的，并且可以与也称为收发基站（BTS）或节点 B 的一个或多个基站进行通信。远程站通过一个或多个基站向也称为无线网络控制器（RNC）的基站控制器发送和接收数据分组。基站和基站控制器是被称为接入网的网络的一部分。接入网在多个远程站之间传送数据分组。接入网还可以连接到接入网外部的附加网络，比如企业内部网或因特网，并且接入网可以在每个远程站和这种外部网络之间传送数据分组。已经与一个或多个基站建立活动业务信道连接的远程站，称为活动远程站并且被称为处于业务状态中。在与一个或多个基站建立活动业务信道连接过程中的远程站被称为处于连接建立状态。远程站可以是通过无线信道进行通信的任何数据设备。远程站还可以是多种类型设备中的任何设备，包括但不局限于 PC 卡、压缩闪存、外部或内部调制解调器或无线电话。远程站向基站发送信号所通过的通信链路称为上行链路，也称为反向链路。基站向远程终端发送信号所通过的通信链路称为下行链路，也称为前向链路。

[0024] 参照图 2，无线通信系统 100 包括一个或多个无线移动台（MS）102、一个或多个基站（BS）104、一个或多个基站控制器（BSC）106 以及核心网 108。核心网可以经由适当回程连接到因特网 110 和公共交换电话网（PSTN）112。典型的无线移动台可以包括手持电话或膝上型计算机。无线通信系统 100 可以采用多个多址技术中的任意一种技术，比如码分多址（CDMA）、时分多址（TDMA）、频分多址（FDMA）、空分多址（SDMA）、极分多址（PDMA）或本领域公知的其它调制技术。

[0025] 再次参照图 1,MS 可以访问由该 MS 的归属地第三代(3G)网络 18 提供的服务。分组数据互通功能体(PDIF)20 用作防止未授权使用 3G 网络服务的安全网关。因为已经经由 IPsec 传输模式对在 MS 和 P-CSCF 之间交换的会话启动协议(SIP)信令进行了加密,所以该方法和装置可以对 MS 和 PDIF 之间传输的 SIP 信令消息禁用 IPsec 加密。该目的是为了避免在 MS 处对 SIP 信令消息的嵌套 IPsec 加密 / 解密。

[0026] 因为 VoIP 媒体分组的加密 / 解密(每 20ms 一次)可能会引起 PDIF 和 MS 中的显著处理负荷,所以应当对在 MS 和 PDIF 之间传输的 VoIP 媒体分组禁用 IPsec 加密。下面描述的方法和装置节省了 MS 中的处理资源,更具体地节省了支持许多 MS 的 PDIF 中的处理资源。

[0027] 尽管需要对 SIP 信令和 VoIP 媒体分组禁用 IPsec 加密,但是优选地对其它非 IMS 分组流(例如,emial 消息、IM 等)应用 IPsec 加密。

[0028] 该方法的目的是为 MS 和 PDIF 沿每个方向建立两个 IPsec SA。(沿每个方向均需要两个 IPsec SA 是因为每个 IPsec SA 均是单方向的。)一个 IPsec SA 用于加密,另一个 IPsec SA 用于空加密。MS 配置安全策略数据库(SPD)中的业务选择符,使得将该空加密 IPsec SA 应用于 SIP 信令消息以及可选地应用于 VoIP 媒体分组,并且将加密 IPsec SA 应用于其它业务。

[0029] 在初始 IKEv2 协商期间,MS 和 PDIF 建立默认 IPsec SA 以用于对发往该 MS 和源于该 MS 的所有业务(初始的非 IMS 业务)进行加密。在该 IPsec SA 的建立期间,MS 和 PDIF 使用 IKEv2 来配置 SPD 中的业务选择符,使得该加密 IPsec SA 应用于发往该 MS 的 IP 地址的所有分组和源于该 MS 的 IP 地址的所有分组。

[0030] 当 MS 需要 IMS 业务时,MS 执行 SIP 注册。经由与 P-CSCF 的 SIP REGISTER/200OK 交换,MS 获得客户 / 服务器端口号,该端口号将用于携带后续 SIP 信令消息,并且这些消息将通过 MS 和 P-CSCF 之间的 IPsec 加密来保护。在 MS 获得客户 / 服务器端口号之后,MS 使用创建子 SA (Create-Child-SA)交换来建立用于 SIP 信令和可选地用于 VoIP 媒体分组的空加密 IPsec SA。在空加密 IPsec SA 的建立期间,MS 和 PDIF 使用 IKEv2 来配置 SPD 中的业务选择符,使得该空加密 IPsec SA 应用于具有该客户 / 服务器端口号的分组(指示该分组携带已加密的 SIP 信令消息)。

[0031] 此外,MS 和 PDIF 可以配置 SPD 中的附加业务选择符,使得该空加密 IPsec SA 应用于 VoIP 媒体分组。有两种方法来进行该操作 :

[0032] 1)如果将 MS 静态地配置为总是利用源端口 x 发送 VoIP 媒体分组并利用目的端口 y 接收 VoIP 媒体分组,则在空加密 IPsec SA 的建立期间,MS 可以配置 SPD 中的附加业务选择符(针对端口 x 和 y),使得该空加密 IPsec SA 应用于具有端口 x 的源于 MS 的分组和具有端口 y 的终止于 MS 的分组。

[0033] 2)如果为每个 VoIP 会话动态地选择端口号,则在每个 VoIP 会话的开始,MS 知道其将使用哪个端口(例如,端口 u)来发送 VoIP 媒体分组以及其将使用哪个端口(例如,端口 v)来接收 VoIP 媒体分组。MS 可以使用 IKEv2 信息交换(Informational Exchange)来更新 SPD 中的业务选择符(针对端口 u 和 v),使得该空加密 IPsec SA 应用于具有端口 u 的源于 MS 的分组和具有端口 v 的终止于 MS 的分组。

[0034] MS 具有以下性能 :在 MS 通过 SIP 交换获得客户 / 服务器端口号之后,MS 使用

IKEv2 来为具有这些客户 / 服务器端口号的分组(这些分组将携带已加密的 SIP 信令消息，并且不需要在 MS 和 PDIF 之间再次加密)建立空加密 IPsec SA ;并且 MS 可以使用 IKEv2 来配置 SPD 中的业务选择符，以便对 VoIP 媒体分组应用空加密 IPsec SA。PDIF 具有以下性能 :支持 SIP 信令消息的空加密 IPsec SA ;以及支持用于 VoIP 媒体分组的空 IPsec SA。

[0035] 参照图 1 和 3，本发明的一方面在于一种用于通过无线局域网 WLAN 22 在移动台 MS 102 和安全网关 20 (例如，PDIF) 之间高效传输分组以访问归属地服务的方法 300。在该方法中，建立第一加密安全关联 ESA1 以用于将第一类型分组从安全网关传输到移动台(步骤 302)，并且建立第二加密安全关联 ESA2 以用于将第一类型分组从移动台传输到安全网关(步骤 304)。接下来，建立第一空加密安全关联 N-ESA1 以用于将第二类型分组从安全网关传输到移动台(步骤 306)，并且建立第二空加密安全关联 N-ESA2 以用于将第二类型分组从移动台传输到安全网关(步骤 308)。基于业务选择符来选择用于使用第二空加密安全关联来传输的第二类型分组。而且，可以基于业务选择符来选择用于使用第一空加密安全关联来传输的第二类型分组。

[0036] 第一类型分组是那些需要加密的分组，并且使用第一和第二加密安全关联来传输。第二类型分组是那些已加密的分组(例如，SIP 信令、VoIP 等)，并且使用第一和第二空加密安全关联来传输。

[0037] 业务选择符可以是预配置的并且为移动台和安全网关所已知。业务选择符可以是目的和 / 或源 IP 地址和端口号。分组的类型可以通过关联的 IP 地址和 / 或端口号来确定。

[0038] 可替换地，可以在建立第一和第二加密安全关联之前产生业务选择符，或者可以在建立第一和第二加密安全关联之后产生业务选择符。例如，移动台可以产生业务选择符并使用第二加密安全关联将该业务选择符转发到安全网关(步骤 310)，或者安全网关可以产生业务选择符并使用第一加密安全关联转发该业务选择符(步骤 312)。

[0039] 在本发明的其它更多具体方面中，第一和第二空加密安全关联均可以是子安全关联。每个安全关联均可以是安全 IP 隧道 24。可以由第三代移动电话归属地网络 18 来提供归属地服务。安全网关可以是分组数据互通功能体 20。所选择的用于使用第二空加密安全关联来传输的第二类型分组可以是先前加密的语音 IP (VoIP) 分组，或者其可以是先前加密的会话启动协议(SIP) 分组。

[0040] 参照图 4，本发明的另一方面可以在于一种移动台 102，其包括用于建立第一加密安全关联以用于将第一类型分组通过无线局域网从安全网关传输到移动台的模块，用于建立第二加密安全关联以用于将第一类型分组通过无线局域网从移动台传输到安全网关的模块，用于建立第一空加密安全关联以用于将第二类型分组通过无线局域网从安全网关传输到移动台的模块，用于建立第二空加密安全关联以用于将第二类型分组通过无线局域网从移动台传输到安全网关的模块，以及用于基于业务选择符来选择用于使用第二空加密安全关联来传输的第二类型分组的模块。上述模块可以包括控制处理器 402。该移动台还可以包括如移动电话通常所具有的存储器件 404、键盘 406、麦克风 408、显示器 410、扬声器、天线等。

[0041] 本发明的另一方面可以在于一种包括计算机可读介质的计算机程序产品，该计算机可读介质，比如存储器件 404，包括用于使计算机执行以下操作的代码 :建立第一加密安全关联以用于将第一类型分组通过无线局域网从安全网关传输到移动台，建立第二加密安

全关联以用于将第一类型分组通过无线局域网从移动台传输到安全网关，建立第一空加密安全关联以用于将第二类型分组通过无线局域网从安全网关传输到移动台，建立第二空加密安全关联以用于将第二类型分组通过无线局域网从移动台传输到安全网关，以及基于业务选择符来选择用于使用第二空加密安全关联来传输的第二类型分组。

[0042] 本领域技术人员应当理解，可以使用各种不同的方法和技术中的任何一种来表示信息和信号。例如，在以上整个说明书中所提及的数据、指令、命令、信息、信号、比特、符号和码片可以用电压、电流、电磁波、磁场或磁性粒子、光场或光粒子或者其任何组合来表示。

[0043] 本领域技术人员还应当注意，结合这里公开的实施例所描述的各种示例性逻辑块、模块、电路和算法步骤可以实现为电子硬件、计算机软件或两者的组合。为了清楚地说明硬件和软件的这种可互换性，已经就各种示意性组件、方块、模块、电路和步骤的功能对其进行了整体描述。这种功能是实现为软件还是实现为硬件取决于具体应用以及施加给整个系统的设计约束。本领域技术人员可以针对每种具体应用以各种方式来实现所述的功能，但是这种实现决定不应被解释为导致脱离本发明的范围。

[0044] 结合这里公开的实施例所描述的各种示例性逻辑块、模块和电路可以利用被设计成用于执行这里所述功能的下列部件来实现或执行：通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现场可编程门阵列（FPGA）或其它可编程逻辑器件、离散门或晶体管逻辑、分立的硬件组件或者这些部件的任何组合。通用处理器可以是微处理器，但是可选地，处理器可以是任何传统处理器、控制器、微控制器或状态机。处理器也可以实现为计算设备的组合，例如，DSP 和微处理器的组合、多个微处理器、一个或多个微处理器结合 DSP 核、或任何其它这种配置。

[0045] 结合这里公开的实施例所描述的方法或算法的步骤可以直接包含在硬件中、由处理器执行的软件模块中或这两者的组合中。软件模块可以位于 RAM 存储器、闪速存储器、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动盘、CD-ROM、或本领域已知的任何其它存储介质形式。示例性的存储介质耦合到处理器，使得处理器能够从该存储介质中读取信息或向该存储介质写入信息。作为替换，所述存储介质可以与处理器集成在一起。处理器和存储介质可以位于 ASIC 中。ASIC 可以位于用户终端中。作为替换，处理器和存储介质可以作为分立的部件位于用户终端中。

[0046] 在一个或多个示例性实施例中，所述功能可以实现在硬件、软件、固件或其任意组合中。如果实现在作为计算机程序产品的软件中，则可以将这些功能作为一个或多个指令或代码来存储在计算机可读介质上或通过计算机可读介质来传送。计算机可读介质包括计算机存储介质和通信介质，该通信介质包括有助于将计算机程序从一个位置传送到另一个位置的任何介质。存储介质可以是能够由计算机访问的任何可用介质。举例而言而非限制性地，该计算机可读介质可以包括 RAM、ROM、EEPROM、CD-ROM 或其它光盘存储介质、磁盘存储介质或其它磁性存储设备，或者是可以用于携带或存储以指令或数据结构形式的所需程序代码并且能够由计算机访问的任何其它介质。此外，任何连接都可以适当地称为计算机可读介质。例如，如果使用同轴线缆、光纤线缆、双绞线、数字用户线路（DSL）或诸如红外、无线电和微波的无线技术来从网站、服务器或其它远程源发送软件，则上述同轴线缆、光纤线缆、双绞线、DSL 或诸如红外、无线电和微波的无线技术均包括在介质的定义。如这里所使用的，磁盘和光盘包括压缩盘（CD）、激光盘、光学盘、数字多功能盘（DVD）、软盘、蓝光盘，

其中磁盘通常通过磁性再现数据，而光盘利用激光通过光学技术再现数据。上述内容的组合也应当包括在计算机可读介质的范围内。

[0047] 上面描述了所公开的实施例，以使本领域的任何技术人员均能够实现或者使用本发明。对于本领域技术人员来说，对这些实施例的各种修改是显而易见的，并且本申请定义的一般性原理也可以在不脱离本发明的精神和范围的基础上应用于其它实施例。因此，本发明并不限于这里所给出的实施例，而是与本申请公开的原理和新颖性特征的最广范围相一致。

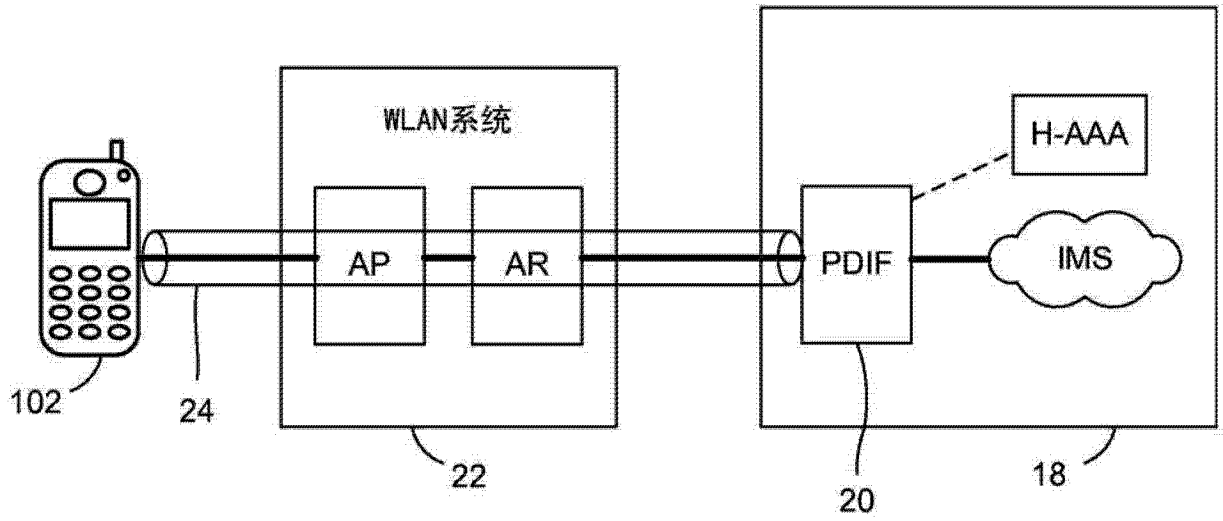


图 1

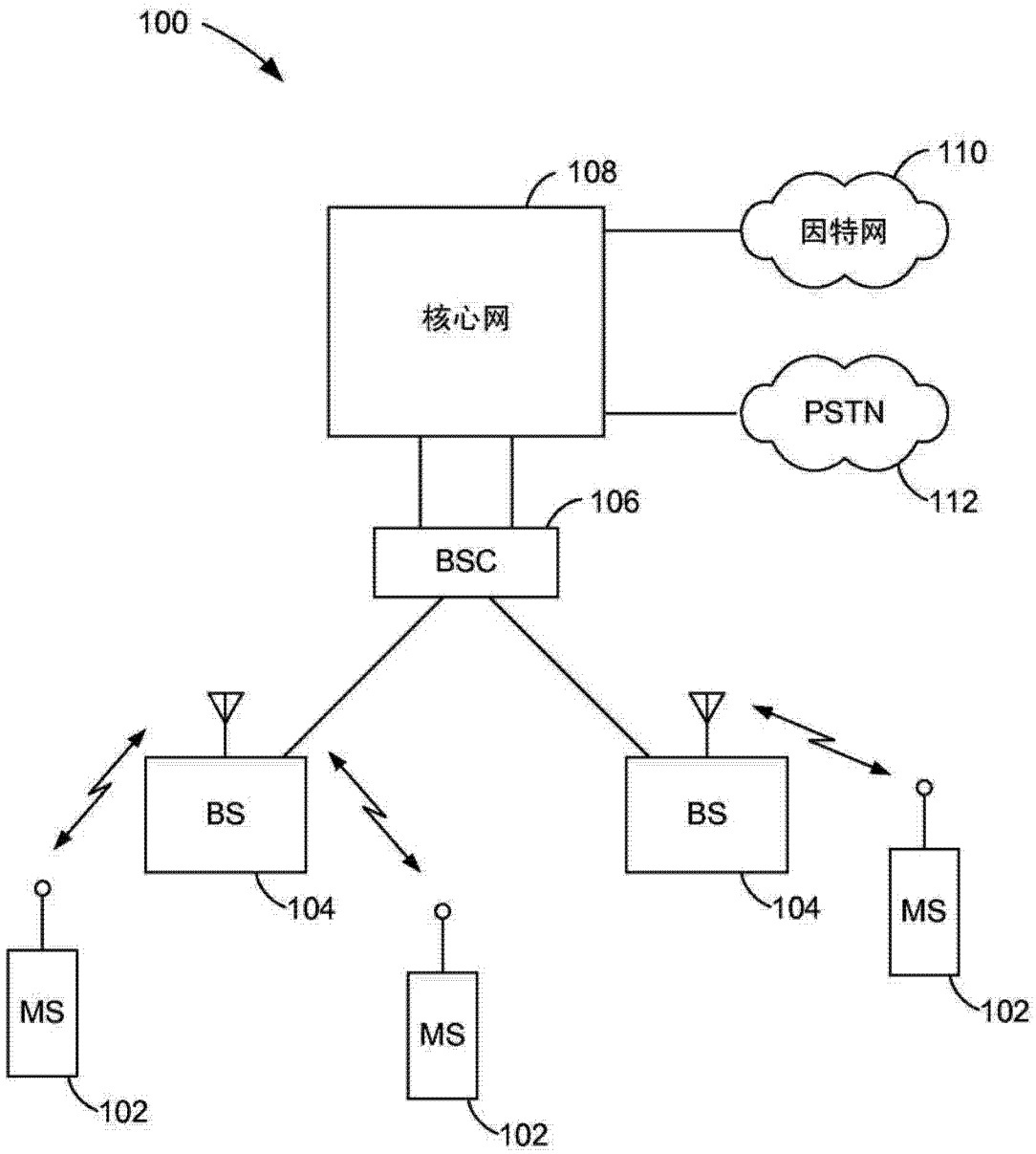

100
108
110
因特网
核心网
PSTN
112
106
BSC
BS
BS
104
104
MS
MS
MS
102
102
102

图 2

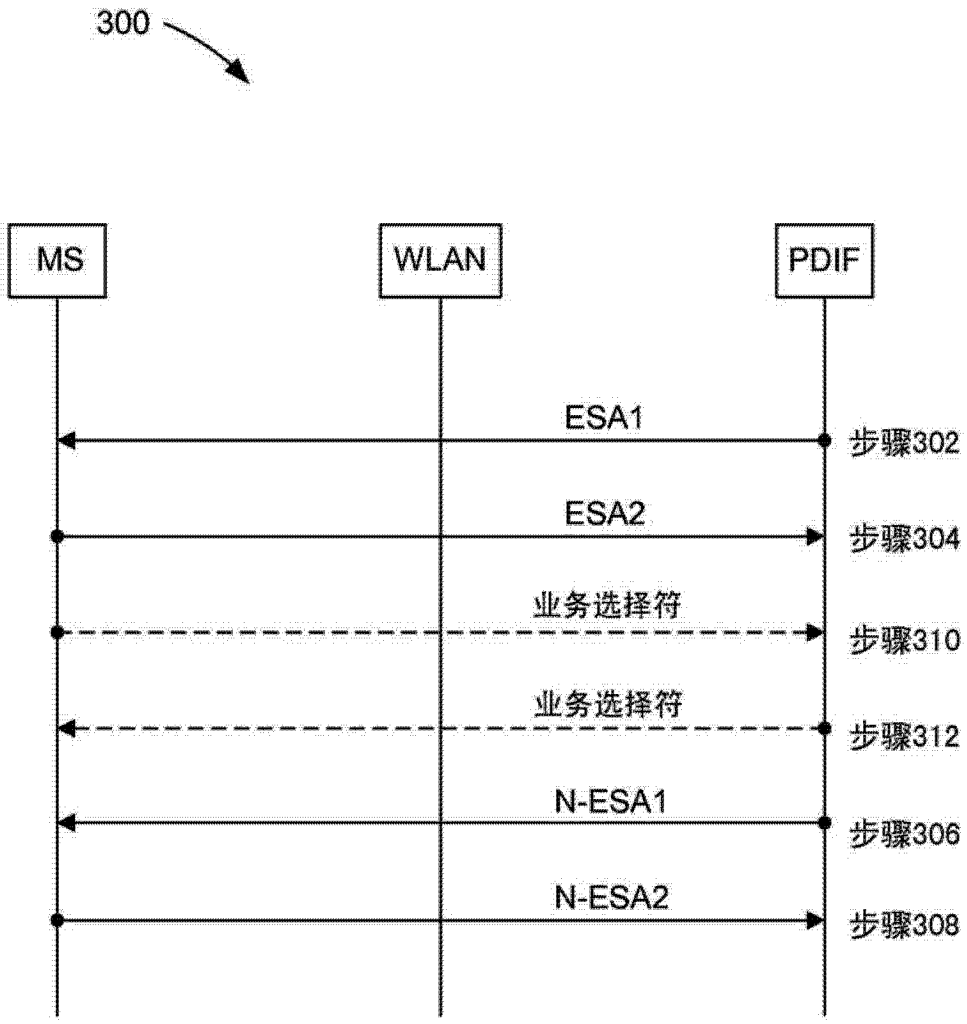

300
MS
WLAN
PDIF
ESA1
步骤302
ESA2
步骤304
业务选择符
步骤310
业务选择符
步骤312
N-ESA1
步骤306
N-ESA2
步骤308

图 3

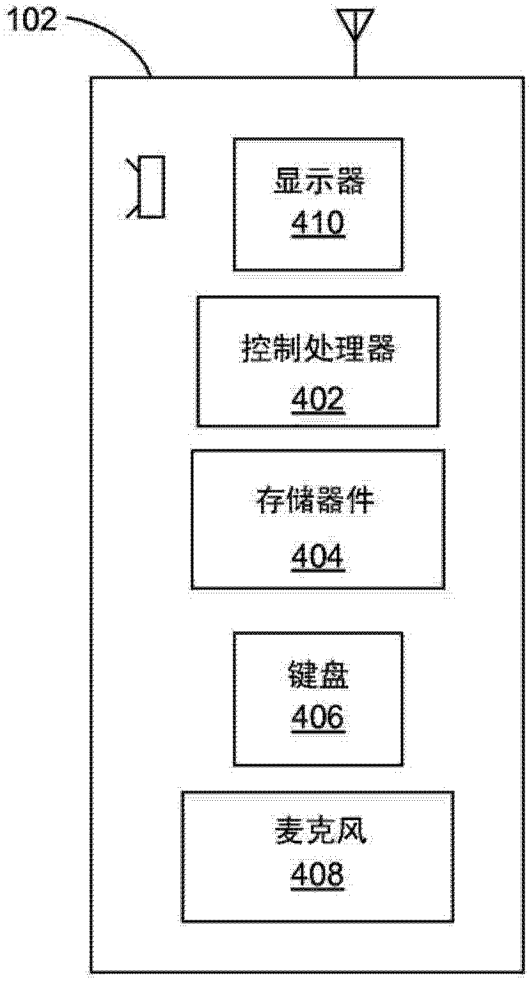


图 4