(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 103797830 B
(45)授权公告日 2015.12.23

(21)申请号 201280044277.3
(22)申请日 2012.09.12
(30)优先权数据
61/533,627 2011.09.12 US
61/535,234 2011.09.15 US
61/583,052 2012.01.04 US
61/606,794 2012.03.05 US
61/611,553 2012.03.15 US
61/645,987 2012.05.11 US
13/610,738 2012.09.11 US
(85)PCT国际申请进入国家阶段日
2014.03.12
(86)PCT国际申请的申请数据
PCT/US2012/054879 2012.09.12
(87)PCT国际申请的公布数据
WO2013/040046 EN 2013.03.21
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 P·M·霍克斯 G·谢里安
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英
(51)Int.Cl.
H04L 9/08(2006.01)
H04W 12/04(2009.01)
(56)对比文件
CN 1719795 A,2006.01.11,
CN 1973495 A,2007.05.30,
US 6144744 A,2000.11.07,
审查员 王玉婧

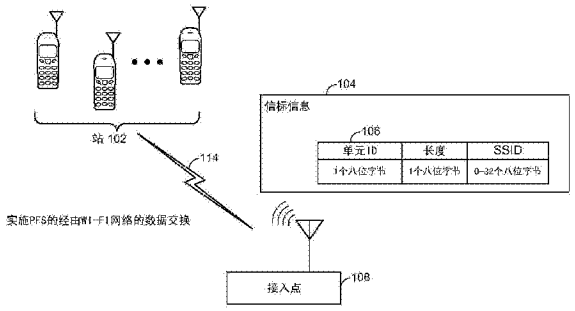
权利要求书3页 说明书12页 附图6页

(54)发明名称

用于对与一组共享临时密钥数据的交换进行编码的系统和方法

(57)摘要

一种方法包括:生成共享主秘密。该方法还包括:生成一组共享临时密钥数据。该组共享临时密钥数据是独立于共享主秘密而生成的。与共享主秘密的有效期相比,该组共享临时密钥数据的有效期较短。该方法还包括:至少基于共享主秘密和该组共享临时密钥数据,对要发送到至少一个站的至少一个消息进行加密。



CN 103797830 B

1. 一种通信方法，其包括：

生成共享主秘密；

生成成对临时密钥 PTK 和一组共享临时密钥数据，其中，所述 PTK 是基于所述共享主秘密而生成的，其中，所述一组共享临时密钥数据是独立于所述共享主秘密而生成的，并且其中，与所述共享主秘密的有效期相比，所述一组共享临时密钥数据的有效期较短；以及

至少基于所述共享主秘密、所述 PTK 和所述一组共享临时密钥数据，对要发送到至少一个站的至少一个消息进行加密。

2. 根据权利要求 1 所述的方法，其中，所述共享主秘密包括成对主密钥 PMK。

3. 根据权利要求 1 所述的方法，其中，所述一组共享临时密钥数据启用与接入点和所述至少一个站相关联的 Diffie-Hellman DH 密钥交换。

4. 根据权利要求 3 所述的方法，其中，所述 DH 密钥交换使用从由所述接入点规定的 DH 群组列表中选择的一组密钥。

5. 根据权利要求 4 所述的方法，其中，所述一组共享临时密钥数据的第一私有密钥、第二私有密钥、第一公共密钥和第二公共密钥是在所述 DH 密钥交换之前被计算的，其中，所述第一私有密钥和所述第一公共密钥存储在所述接入点处，其中所述第二私有密钥和所述第二公共密钥存储在所述至少一个站处，并且其中，所述第一公共密钥和所述第二公共密钥是在所述 DH 密钥交换期间交换的。

6. 根据权利要求 3 所述的方法，其中，所述 DH 密钥交换使用基于有限域算法而生成的一组密钥。

7. 根据权利要求 3 所述的方法，其中，所述 DH 密钥交换使用基于椭圆曲线算法而生成的一组密钥。

8. 根据权利要求 1 所述的方法，其中，所述一组共享临时密钥数据关联于与接入点以及所述至少一个站相关联的握手交换，执行所述握手交换以便对与所述接入点以及所述至少一个站相关联的通信进行认证。

9. 根据权利要求 8 所述的方法，其中，与所述接入点以及所述至少一个站相关联的所述握手交换包括：使用 Wi-Fi 协议的握手交换。

10. 根据权利要求 8 所述的方法，其中，所述握手交换包括可扩展认证协议 EAP 交换。

11. 根据权利要求 10 所述的方法，其中，与所述握手交换相关联的接入点随机数是经由与信标消息不同的消息发送的。

12. 根据权利要求 8 所述的方法，其中，所述握手交换包括四路握手。

13. 根据权利要求 1 所述的方法，其中，所述一组共享临时密钥数据包括基于 Diffie-Hellman DH 密钥交换而生成的一组公共密钥和基于所述 DH 密钥交换的一组私有密钥。

14. 根据权利要求 13 所述的方法，还包括：在生成所述一组共享临时密钥数据之后，删除所述一组私有密钥。

15. 根据权利要求 13 所述的方法，还包括：生成多组共享临时密钥数据以便对与接入点和多个站相关联的通信进行加密，其中，每一组共享临时密钥数据启用与所述接入点和所述多个站中的相应一个站相关联的相应握手交换，并且其中，与和所述接入点以及所述多个站中的相应一个站相关联的对应共享主秘密的有效期相比，每一组共享临时密钥数据

的有效期较短。

16. 根据权利要求 1 所述的方法，其中，与接入点和所述至少一个站相关联的所述至少一个消息的加密实现完美前向保密 PFS。

17. 根据权利要求 1 所述的方法，还包括 ：基于所述共享主秘密、所述 PTK 和所述一组共享临时密钥数据，生成完美前向保密 - 成对临时密钥 PFS-PTK。

18. 根据权利要求 2 所述的方法，所述 PMK 是基于序列 SEQ 消息、重新认证主密钥 rMSK、接入点随机数、站随机数、或者它们的组合而生成的。

19. 一种通信装置，其包括 ：

针对至少一个站的无线网络接口 ；以及

处理器，其被配置为经由所述无线网络接口与所述至少一个站进行通信，所述处理器被配置为 ：

生成共享主秘密 ；

生成成对临时密钥 PTK 和一组共享临时密钥数据，其中，所述 PTK 是基于所述共享主秘密而生成的，其中，所述一组共享临时密钥数据是独立于所述共享主秘密而生成的，并且其中，与所述共享主秘密的有效期相比，所述一组共享临时密钥数据的有效期较短 ；以及

至少使用所述共享主秘密、所述 PTK 和所述一组共享临时密钥数据，对要发送到所述至少一个站的至少一个消息进行加密。

20. 根据权利要求 19 所述的装置，其中，所述共享主秘密包括成对主密钥。

21. 根据权利要求 19 所述的装置，其中，所述一组共享临时密钥数据启用 Diffie-Hellman DH 密钥交换。

22. 根据权利要求 21 所述的装置，其中，所述 DH 密钥交换使用从由接入点规定的 DH 群组列表中选择的一组密钥。

23. 根据权利要求 22 所述的装置，其中，所述一组共享临时密钥数据的第一私有密钥、第二私有密钥、第一公共密钥和第二公共密钥是在所述 DH 密钥交换之前被计算的，其中，所述第一私有密钥和所述第一公共密钥存储在所述接入点处，其中所述第二私有密钥和所述第二公共密钥存储在所述至少一个站处，并且其中，所述第一公共密钥和所述第二公共密钥是在所述 DH 密钥交换期间交换的。

24. 根据权利要求 21 所述的装置，其中，所述 DH 密钥交换使用基于有限域算法或者基于椭圆曲线算法而生成的一组密钥。

25. 根据权利要求 19 所述的装置，其中，所述一组共享临时密钥数据关联于与接入点以及所述至少一个站相关联的握手交换，执行所述握手交换以便对与所述接入点和所述至少一个站相关联的通信进行认证。

26. 根据权利要求 25 所述的装置，其中，所述握手交换与接入点系统以及所述至少一个站相关联，并且所述握手交换使用 Wi-Fi 协议。

27. 根据权利要求 25 所述的装置，其中，所述握手交换包括 EAP 交换，并且其中，与所述握手交换相关联的接入点随机数是通过与信标消息不同的消息发送的。

28. 根据权利要求 25 所述的装置，其中，所述握手交换包括四路握手。

29. 根据权利要求 19 所述的装置，其中，所述一组共享临时密钥数据包括基于 Diffie-Hellman DH 密钥交换而生成的一组公共密钥和基于所述 DH 密钥交换而生成的一

组私有密钥。

30. 根据权利要求 29 所述的装置，其中，所述处理器被配置为：在生成所述一组共享临时密钥数据之后，删除所述一组私有密钥。

31. 根据权利要求 29 所述的装置，其中，所述处理器被配置为：生成多组共享临时密钥数据以便对与接入点和多个站相关联的通信进行加密，其中，每一组共享临时密钥数据启用与所述接入点和所述多个站中的相应一个站相关联的握手交换，并且其中，与和所述接入点以及所述多个站中的所述相应一个站相关联的对应共享主秘密的有效期相比，每一组共享临时密钥数据的有效期较短。

32. 根据权利要求 19 所述的装置，其中，与所述至少一个站相关联的所述至少一个消息的加密实现完美前向保密 PFS。

33. 一种通信装置，包括：

用于经由无线网络接口与至少一个站进行通信的模块；以及

用于生成共享主秘密、成对临时密钥 PTK 和一组共享临时密钥数据的模块，其中，所述 PTK 是基于所述共享主秘密而生成的，其中，所述一组共享临时密钥数据是独立于所述共享主秘密而生成的，其中，与所述共享主秘密的有效期相比，所述一组共享临时密钥数据的有效期较短；并且其中，至少基于所述共享主秘密、所述 PTK 和所述一组共享临时密钥数据，对要发送到所述至少一个站的至少一个消息进行加密。

用于对与一组共享临时密钥数据的交换进行编码的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求享有下列共同拥有的美国临时专利申请的优先权：2011 年 9 月 12 日提交的美国临时专利申请 No.61/533,627（高通案卷号 113346P1）、2011 年 9 月 15 日提交的美国临时专利申请 No.61/535,234（高通案卷号 113346P2）、2012 年 1 月 4 日提交的美国临时专利申请 No.61/583,052（高通案卷号 113346P3）、2012 年 3 月 5 日提交的美国临时专利申请 No.61/606,794（高通案卷号 121585P1）、以及 2012 年 5 月 11 日提交的美国临时专利申请 No.61/645,987（高通案卷号 121585P2）、以及 2012 年 3 月 15 日提交的美国临时专利申请 No.61/611,553（高通案卷号 121602P1），以引用方式将上述美国临时专利申请的内容全部明确地并入本文。此外，以引用方式将下列非临时申请的内容并入本文：2012 年 9 月 11 日提交的、标题为 WIRELESS COMMUNICATION USING CONCURRENT RE-AUTHENTICATION AND CONNECTION SETUP 的高通案卷号为 113346 的非临时申请，以及 2012 年 9 月 11 日提交的、标题为 SYSTEMS AND METHODS OF PERFORMING LINK SETUP AND AUTHENTICATION 的高通案卷号为 121585 的非临时申请。

技术领域

[0003] 本申请涉及用于对与一组共享临时密钥数据的交换进行编码的系统和方法。

背景技术

[0004] 在 Wi-Fi 网络连接应用中，安全特征逐步演变以提供更稳健和更好集成的安全工具。在由电气和电子工程师协会（IEEE）发布的 EAP（可扩展认证协议）标准 802.11i 中，可以使用包括被称为“四路握手”机制的认证技术。在四路握手机制中，客户端设备（诸如膝上型计算机、智能电话或其它客户端设备）通常被称为“站”，其与无线路由器或其它设备（通常被称为“接入点”）进行协商，以便建立安全的网络连接会话。在会话期间，站可以寻找与互联网或其它网络的连接。

[0005] 在四路握手方式中，站和接入点基于可以执行的相互认证来交换一系列 4 个定义消息。接入点可以与用户服务（RADIUS）服务器或其它认证服务器、平台或服务中的远程认证拨号进行交互，以便建立由站和接入点执行四路握手过程所使用的一组共享秘密和 / 或公共密钥和私有密钥。作为四路握手过程的一部分，站和接入点可以访问共享秘密，所述共享秘密可以包括成对的主密钥（PMK）。可以使用公共密钥和私有密钥（包括临时成对密钥（PTK））的其它集合来对在站与接入点之间交换的消息进行编码，可以使用成对的主密钥作为其它加密密钥层的生成器来构建所述临时成对密钥（PTK）。

[0006] 然而，在现有的四路握手实施例中，能够成功截获并解码成对主密钥的攻击者可能随后能够使用该高级密钥来生成并且有可能通过生成或推导出相应的成对临时密钥或其它密码信息来截获和解码在接入点与一个或多个站之间的业务，这是因为一旦确立了成对主密钥，只要原始的成对主密钥保持有效，从该成对主密钥推导出的其它会话密钥就保

持有效并且可操作。从而，捕获了成对主密钥的成功的攻击者也许能够在该成对主密钥的有效寿命期间对接入点和与该接入点进行通信的任何一个或多个站之间的流进行解密。

发明内容

[0007] 本申请公开了用于在 Wi-Fi 网络会话中提供完美前向保密的系统和方法。完美前向保密 (PFS) 是一种实现安全的方法。PFS 可以指代密钥推导的属性，从而使得如果攻击者暴露了父秘密，那么该攻击者可能无法确定从该父秘密推导出的过去或未来的密钥。

[0008] 当客户端设备正在执行与接入点 (AP) 的四路握手时，生成成对主密钥 (PMK)，并且从该 PMK 推导出额外的密钥 (例如，成对临时密钥 (PTK))。只要 PMK 保持有效，PTK 就保持有效；因此，在没有增加的安全 (诸如 PFS) 的情况下，攻击者可以从被破解的 PMK 推导出 PTK，以便在被破解的 PMK 的有效寿命期间来对客户端设备与 AP 之间的传输进行解码。所描述的技术通过在四路握手中实施 PFS 来提供增强的安全性，而不是依赖于在只要 PMK 可以保持有效的期间就可以保持有效的推导出的密钥。

[0009] 当客户端设备执行与 AP 的四路握手时，AP 可以生成接入点随机数 (Anonce) 消息并发送给客户端设备。客户端设备可以获得 PMK 并且生成站随机数 (Snonce) 消息。客户端可以基于 PMK、Anonce、Snonce 和 / 或其它信息来推导出 PTK、密钥确认密钥 (KCK)、以及密钥加密密钥 (KEK)。

[0010] 为了在四路握手中实现 PFS，客户端设备可以向 AP 发送关联请求，该关联请求可以包括站 (STA)Diffie-Hellman 临时公共密钥 (SDHEPubKey)。AP 可以获得 PMK 并且根据 PMT 来推导 PTK。

[0011] 为了在四路握手中实现 PFS，AP 可以从 SDHEPubKey 和 AP 已知的接入点 Diffie-Hellman 临时私有密钥 (ADHEPrivKey) 推导出共享 Diffie-Hellman 临时密钥 (SharedDHEKey)。SDHEPubKey 和 ADHEPrivKey 可以分别由客户端设备和 AP 在参与四路握手之前预先生成。此外，AP 可以基于 SharedDHEKey 和 PTK 推导出完美前向保密 - 成对临时密钥 (PFS-PTK)、完美前向保密 - 密钥确认密钥 (PFS-KCK)、和完美前向保密 - 密钥加密密钥 (PFS-KEK)。AP 可以向客户端设备发送接入点 Diffie-Hellman 临时公共密钥 (ADHEPubKey)。客户端设备可以基于客户端设备已知的站 Diffie-Hellman 临时私有密钥 (SDHEPrivKey) 和 ADHEPubKey 推导出 SharedDHEKey。ADHEPubKey 和 SDHEPrivKey 可以分别由 AP 和客户端设备在参与四路握手之前预先生成。客户端设备可以基于 PTK 和 SharedDHEKey 推导出 PFS-PTK、PFS-KCK 和 PFS-KEK。

[0012] AP 和客户端设备在推导出 SharedDHEKey 之后可以分别删除 ADHEPrivKey 和 SDHEPrivKey。客户端设备和 AP 可以基于 PFS-KEK、PFS-KCK、SharedDHEKey 和 / 或从 PMK 推导出的另一个密钥来对各个接收到的传输进行解密。

[0013] 在特定的实施例中，一种方法包括生成共享主秘密。所述方法还包括 :生成一组共享临时密钥数据。该组共享临时密钥数据是独立于所述共享主秘密而生成的。与所述共享主秘密的有效期相比，该组共享临时密钥数据的有效期较短。所述方法还包括 :至少基于所述共享主秘密和所述一组共享临时密钥数据，对要发送到至少一个站的至少一个消息进行加密。

[0014] 在另一个特定的实施例中，一种装置包括针对至少一个站的无线网络接口。所述

装置还包括处理器，所述处理器被配置为：经由所述网络接口与所述至少一个站进行通信。所述处理器被配置为：生成共享主秘密并且生成一组共享临时密钥数据。该组临时密钥数据是独立于所述共享主秘密而生成的。与所述共享主秘密的有效期相比，该组共享临时密钥数据的有效期较短。所述处理器还被配置为：至少使用所述共享主秘密和所述一组共享临时密钥数据，对要发送到所述至少一个站的至少一个消息进行加密。

[0015] 由所公开的实施例中的至少一个实施例提供的一个特定的优点是：在 Wi-Fi 网络中，第一设备（例如，移动站）实现与第二设备（例如，接入点）的 PFS 的能力。

[0016] 在回顾整个申请文件（包括以下部分：附图说明、具体实施方式和权利要求书）之后，本申请的其它方面、优点和特征将变得清楚。

附图说明

[0017] 被纳入本说明书并且构成本说明书的一部分的附图示出了本发明的实施例，并且连同本说明书一起用于解释本发明的原理。在这些附图中：

[0018] 图 1 示出了根据各个实施例的整体网络，该整体网络可以在用于在 Wi-Fi 网络会话中提供完美前向保密的系统和方法中使用；

[0019] 图 2 示出了根据各个实施例，可以在被配置为使用用于在 Wi-Fi 网络会话中提供完美前向保密的系统和方法的接入点中使用的硬件、软件和其它资源；

[0020] 图 3A 和图 3B 示出了根据本发明的各个实施例，用于执行接入点与站之间的加密布置的配置和操作的示例性呼叫流序列；

[0021] 图 4 示出了根据本发明的各个实施例，用于执行接入点与站之间的加密布置的配置和操作的另一个示例性呼叫流序列；以及

[0022] 图 5 示出了根据各个实施例，可以用于在 Wi-Fi 网络会话中提供完美前向保密的示例性硬件、软件和其它资源。

具体实施方式

[0023] 本发明的实施例涉及用于在 Wi-Fi 网络会话中提供完美前向保密的系统和方法。更具体地说，实施例涉及：用于插入机制以便创建或允许完美前向保密 (PFS) 应用于 Wi-Fi 会话的平台和技术，所述 Wi-Fi 会话使用四路握手来建立接入点与站之间的通信。接入点和站可以执行四路握手操作，使用成对主密钥、认证服务器、消息完整性校验 (MIC) 以及由 802.11i 标准和 / 或其它协议规定的其它过程和资源。在用于在 Wi-Fi 网络会话中提供完美前向保密的系统和方法中，接入点和站可以应用其它级别的加密保护，包括插入到四路握手结构中的自组织密钥的额外集合的生成。该自组织密钥的额外集合可以包括使用 Diffie-Hellman(DH) 运算而生成的一组公共密钥和私有密钥数据，所述 Diffie-Hellman(DH) 运算可以是或者可以包括使用有限域、椭圆和 / 或其它算法的公共密钥和私有密钥对的生成。可以基于或使用随机数字生成器来生成 Diffie-Hellman 密钥和相关信息。

[0024] 当在接入点侧和站侧两者上生成和 / 或检索到相应的 Diffie-Hellman 共享密钥之后，接入点和站单元二者可以删除或销毁该 Diffie-Hellman 共享密钥的私有部分。由于那些私有密钥（例如，ADHEPrivKey 和 SDHEPrivKey）已经被删除或销毁，因此捕获到接入

点与站之间的消息流的攻击者不能破解当前会话之前或之后的其它流，即使该攻击者稍后能够恢复在当前会话期间所使用的成对主密钥。该攻击者不能够破解其它流，因为根据用于在 Wi-Fi 网络会话中提供完美前向保密的系统和方法编码的单独的会话将具有在每个会话期间单独生成的不同的 Diffie-Hellman 密钥数据，这些 Diffie-Hellman 密钥数据的解码需要获取其它 Diffie-Hellman 私有密钥和公共密钥信息。根据这些和其它方面，可以提高 Wi-Fi 会话的安全性，并且可以将完美前向保密 (PFS) 纳入四路握手安全方案中。

[0025] 在特定的实施例中，一种方法包括生成共享主秘密。该方法还包括生成一组共享临时密钥数据来对与接入点和至少一个站相关联的交换进行编码，其中，所述一组共享临时密钥数据是基于与用于执行对与接入点和至少一个站相关联的通信进行认证的接入点和至少一个站相关联的握手交换的内容。所述一组共享临时密钥数据是独立于共享主秘密生成的，并且与共享主秘密的有效期相比，所述一组共享临时密钥数据的有效期较短。该方法还包括：至少基于所述共享主秘密和所述一组共享临时密钥数据，对至少一个消息进行编码。

[0026] 在另一个特定的实施例中，一种装置包括针对至少一个站的无线网络接口。该装置还包括被配置为经由网络接口与至少一个站进行通信的处理器，处理器被配置为：生成共享主秘密并且生成一组共享临时密钥数据，来对与接入点系统和至少一个站相关联的交换进行编码。所述一组共享临时密钥数据是基于用于与执行对与接入点系统和至少一个站相关联的通信进行认证的接入点系统和至少一个站相关联的握手交换的内容。所述一组临时密钥数据是独立于所述共享主秘密生成的，并且与共享主秘密的有效期相比，所述一组共享临时密钥数据的有效期较短。处理器还被配置为：至少使用共享主秘密和所述一组共享临时密钥数据，对与接入点系统和至少一个站相关联的至少一个消息进行编码。

[0027] 参考附图中所示的本发明的示例性实施例。其中，在整个附图中可能使用相同的附图标记来指代相同或相似的部分。

[0028] 图 1 示出了其中用于在 Wi-Fi 网络会话中提供完美前向保密的系统和方法可以操作的整体网络 100。如图所示，接入点 108 可以向范围内的一组站 102 广播无线网络信号。接入点 108 可以包括无线路由器和 / 或其它网络接入点，并且接入点 108 可以被配置为：使用由 IEEE 规范 802.11b、802.11g、802.11n 和 / 或其它标准中规定的 Wi-Fi 无线标准来进行操作。当作为 Wi-Fi 接入点进行操作时，接入点 108 可以例如操作在 2.4GHz 频带中。然而，将明白的是，在其它实施例中，可以使用其它无线接入标准、信道和 / 或频率。如下面更详细讨论的，该组站 102 中的至少一个站可以参与数据交换 114，数据交换 114 经由 Wi-Fi 网络来实现对接入点 108 的完美前向保密 (PFS)。

[0029] 该组站 102 中的每一个设备或站可以包括任何具有无线网络功能的设备，诸如配备 Wi-Fi 的智能电话、触摸板设备和 / 或另一种设备或平台。如图 2 中所示，可以使用一个或多个硬件、软件和 / 或其它资源来对该组站 102 中的各个站 118 进行配置。站 118 可以包括各种硬件、软件和其它资源，包括操作系统 112、例如可以显示操作系统 112 的图形用户界面 (GUI) 的显示器 110 和射频天线 150（或多个天线）。操作系统 112 可以包括诸如可从美国加利福尼亚州山景城的谷歌公司 (Google Inc.，Mountain View，California，U.S.) 获得的安卓 (Android™) 操作系统或其它操作系统之类的移动设备操作系统。如同所指出的，操作系统 112 可以包括用于对站 118 进行操作的图形用户接口 (GUI) 以及文件管理、功率

管理、通信和/或其它逻辑、服务和/或资源。操作系统112可以包括计算机指令116。计算机指令116可以使得处理器经由Wi-Fi网络来实现针对数据交换的PFS。站118可以托管应用、服务、逻辑和/或其它逻辑、服务和/或模块，这些应用、服务、逻辑和/或其它逻辑、服务和/或模块可以用于建立与接入点和/或其它信道的连接。该组站102中的任意一个或多个站可以在同一时间连接到接入点108。如图2中所示，接入点108可以向该组站102广播信标信息104。信标信息104可以包括用于指示名称、连接类型、可用信道以及其它网络信息和由接入点108向其无线连接范围内的任何站提供的服务的服务集合标识(SSID)信息单元(IE)。图3示出了可以用于根据Wi-Fi标准，建立具有根据用于在Wi-Fi网络会话中提供完美前向保密(包括在各个网络会话中提供完美前向保密(PFS))的系统和方法的增强、特征、扩展和/或优点的连接的呼叫序列。概括地说，可以在两个或更多个平台、系统、节点、设备和/或其它硬件(包括如图所示的站120、第一接入点122、第二接入点124、认证服务器126和动态主机配置协议(DHCP)服务器128)之间执行呼叫流序列。虽然示出了那些单个的平台、系统、节点、设备和/或硬件，但是应当明白的是：在其它实施例中可以使用替代或额外的硬件平台、系统、节点、设备和/或硬件。如0002处所示，站120可以接近并进入诸如Wi-Fi无线路由器和/或其它接入设备、平台或站点的第一接入点122(被标记为AP1)的无线范围。在1002处，站120可以移出第一接入点122的范围并且进入第二接入点124(被标记为AP2)的无线范围。类似地，第二接入点124可以包括Wi-Fi无线路由器和/或另一个接入设备或站点。在2002处，第二接入点124可以生成接入点随机数(Anonce)消息，所述接入点随机数消息可以包括用于公布第二接入点124的存在并且可以在密钥码的生成中使用的一次性消息、字符串、数据和/或代码。接入点随机数(Anonce)可以包括随机或伪随机地生成的数字和/或其它数据。可以将接入点随机数(Anonce)消息插入到第二接入点124广播的信标消息中。

[0030] 在3002处，站120可以获得用于与第二接入点124建立安全通信的成对主密钥(PMK)。为了获得PMK，站120可以生成包括例如，SEQ消息或数据、rMSK消息或数据，以及站随机数(Snonce)消息或数据的信息。如果使用了预先建立的成对主密钥，那么站120可以检索该成对主密钥。在3004处，站120可以使用成对主密钥、接入点随机数(Anonce)、站随机数(Snonce)和/或其它信息来推导额外信息，所述额外信息包括：例如，成对临时密钥(PTK)、LAN上的扩展认证协议(EAPOL)-密钥确认密钥(KCK)和EAPOL-密钥加密密钥(KEK)。

[0031] 在4002处，站120可以生成关联请求(Assoc Req)并且向第二接入点124发送该请求。结合该请求，站120可以执行运算来生成额外的密钥和相关数据，其包括Diffie-Hellman临时私有密钥(SDHEPrivKey)和Diffie-Hellman临时公共密钥(SDHEPubKey)。可以使用Diffie-Hellman加密方法来生成站Diffie-Hellman临时私有密钥(SDHEPrivKey)和站Diffie-Hellman临时公共密钥(SDHEPubKey)，所述Diffie-Hellman加密方法可以包括椭圆算法或其它算法。

[0032] 可能要注意的是：站120和第二接入点124中的一个或该二者可以访问、存储和/或预先计算相同的Diffie-Hellman数据并在需要时检索该数据，这可以减少在执行修改后的4路握手协议期间的计算负担。站Diffie-Hellman临时公共密钥(SDHEPubKey)可以并入关联请求(Assoc Req)的参数或字段中，并且可以发送到第二接入点124。在4004处，

第二接入点 124 可以接收关联请求 (Assoc Req)，但是如果接入点随机数 (Anonce) 消息不是当前的、有效的或新鲜的，那么可以忽略该请求。

[0033] 在 5002 处，第二接入点 124 可以向认证服务器 126 发送 AAA EAP 请求。如图所示，AAA EAP 请求可以包括多个参数或字段，这些参数或字段中的一些或全部可以用于对站 120 和 / 或与站 120 相关联的数据或证书进行认证。在 6002 处，认证服务器 126 可以验证认证标签 (Auth 标签) 并且推导出 rMSK 密钥或数据。在 7002 处，认证服务器 126 可以向第二接入点 124 发送 AAA EAP- 应答，如图所示，该应答可以包括多个参数或字段。在 8002 处，第二接入点 124 可以指派与 AAA EAP- 应答中返回的 rMSK 相等的成对主密钥。在使用存储的成对主密钥的其它实施例中，取代地，第二接入点 124 可以从储存器中检索成对主密钥。

[0034] 在 9002 处，第二接入点 124 可以从成对主密钥、站随机数 (Snonce) 和接入点随机数 (Anonce) 推导出成对临时密钥 (PTK)。在 10002 处，第二接入点 124 可以使用 KCK 和 KEK 数据和 / 或其它信息来验证具有快速分配 (Rapid commit) 消息和 EAPOL-KEY_F 消息的 DHCP- 发现。在 11002 处，第二接入点 124 可以向 DHCP 服务器 128 发送具有快速分配 () 消息的 DHCP- 发现。在 12002 处，第二接入点 124 可以从 ADHEPrivKey 和 SDHEPubKey 和 / 或其它信息或数据推导出自组织或共享 Diffie-Hellman 临时密钥 (SharedDHEKey)。在 12004 处，第二接入点 124 可以推导出完美前向保密 - 成对临时密钥 (PFS-PTK) 以及其它信息或数据，包括 :完美前向保密密钥确认密钥 (PFS-KCK) 以及使用成对临时密钥的完美前向保密 -EAPOL- 密钥加密密钥 (PFS-KEK)、共享 Diffie-Hellman 临时密钥 (SharedDHEKey) 和 / 或其它信息。

[0035] 在 13002 处，第二接入点 124 可以根据需要来生成群组临时密钥 (GTK) 和完整性群组临时密钥 (IGTK)。可能要注意的是 :在生成共享 Diffie-Hellman 临时密钥 (SharedDHEKey) 之后和 / 或在其它时刻，站 120 和第二接入点 124 可以分别删除、丢弃、重写和 / 或以其它方式抹去或销毁它们各自的 Diffie-Hellman 临时私有密钥 (也就是说，相应的 SDHEPrivKey 和 ADHEPrivKey)。通过删除、重写和 / 或以其它方式抹去或销毁属于站 120 和第二接入点 124 的 Diffie-Hellman 临时私有密钥，站 120 和第二接入点 124 可以确保没有攻击者能够破解所存储的消息业务。即使攻击者能够获得成对主密钥和没有被改变的成对临时密钥也是如此，这是因为仍然需要共享 Diffie-Hellman 临时密钥 (SharedDHEKey) 来对该业务进行解密，但是一旦相应的私有 Diffie-Hellman 密钥 (SDHEPrivKey 和 ADHEPrivKey) 被删除，则该共享 Diffie-Hellman 临时密钥 (SharedDHEKey) 就不可恢复。在 14002 处，DHCP 服务器 128 可以生成具有快速分配 (IP-addr) 消息的 DHCP-Ack，并且向第二接入点 124 发送该消息。该消息可以包括针对站 120 所分配的 IP 地址。可能要注意的是 :虽然 11002 至 14002 被示为以特定的次序发生，但是那些处理步骤、消息、判决逻辑和 / 或其它动作以及图 3A 和图 3B 中以及别处所示出的其它元素可以以各种其它顺序或次序发生，这取决于站 120 和第二接入点 124 的配置和 / 或其它因素。

[0036] 在 15002 处，第二接入点 124 可以形成具有各个字段或分量的关联响应 (Assoc Resp)。各个字段或分量可以包括与 EAP 认证有关的消息，即，在 7002 处从认证服务器接收的 EAP- 结束消息或数据。EAP- 结束消息或数据可以是 EAP- 结束 Re-Auth 消息或数据。Assoc 响应还可以包括与具有各种选项的 DHCP 有关的消息，如图所示，这些消息可以包括 :

具有在 14002 处从 DHCP 服务器接收的快速分配消息或数据的 DHCP-Ack、和 / 或其它消息或数据。AP2 可以将加密和 / 或完整性保护应用于这些消息或数据。加密可以使用 KEK 或 PFS-KEK 或者根据 PMK 和 / 或 PTK 和 / 或 SharedDHEKey 推导出的另一个密钥。完整性保护可以使用 KCK 或 PFS-KCK 或者根据 PMK 和 / 或 PTK 和 / 或 SharedDHEKey 推导出的另一个密钥。Assoc 响应还可以包括与 EAPOL- 密钥消息有关的消息，如图所示，这些消息可以包括使用完美前向保密 - 成对临时密钥 (PFS-PTK) 和 / 或其它密钥或数据的、针对加密、认证和 / 或完整性校验的选项。该 EAPOL- 密钥有关的消息可以包括 ADHEPubKey。该 EAPOL- 密钥有关的消息可以包括使用 KCK 在 EAPOL- 密钥有关的消息或数据上计算出的消息完整性校验 (MIC)。AP2122 可以使用 PFS KCK 和 / 或其它数据、消息或信息来计算完美前向保密 - 消息完整性校验 (PFS-MIC)。PFS-MIC 可以提供对 Assoc Req4002 和 Assoc Resp15002 的组合中的一部分或全部的完整保护。受完整保护的部分可以与 Assoc Resp15002 中的 EAPOL- 密钥有关的消息或数据相对应。可以在 EAP- 结束 Re-Auth 或 DHCP 或 EAPOL- 密钥有关的消息或数据的内部发送 PFS-MIC。PFS-MIC 可以是 Assoc Resp 的一部分，但是位于 EAP- 结束 Re-Auth 或 DHCP 或 EAPOL- 密钥有关的消息或数据的外部。

[0037] 在 16002 处，站 120 可以使用 rIK 和 / 或其它信息来验证 EAP- 结束 Re-Auth 消息。在 17002 处，站 120 可以使用 KCK 来验证 EAPOL- 密钥消息完整性校验 (MIC)。在 18002 中，站 120 可以根据位于如同在 15002 处产生或给出的 EAPOL- 密钥消息中的 SDHEPrivKey 和 ADHEPubKey，和 / 或其它数据或信息来生成共享 Diffie-Hellman 临时密钥 (SharedDHEKey)。在 18004 处，站 120 可以使用成对临时密钥和共享 Diffie-Hellman 临时密钥 (SharedDHEKey) 和 / 或其它数据或信息来推导出 PFS-PTK、PFS-KCK 和 PFS-KEK 信息。在 18006 处，站 120 可以使用 PFS-KCK 和 / 或其它数据、消息或信息来对 PFS-MIC 进行验证。

[0038] 在 19002 处，站 120 可以对 DHCP-Ack 消息进行验证和 / 或解密。解密可以使用 KEK 或 PFS-KEK 或从 PMK 和 / 或 PTK 和 / 或 SharedDHEKey 推导出的另一个密钥。验证可以使用 KCK 或 PFS-KCK 或从 PMK 和 / 或 PTK 和 / 或 SharedDHEKey 推导出的另一个密钥。在 20002 中，站 120 可以向第二接入点 124 发送授权确认 (Auth-Confirm) 消息，如图所示，所述 Auth-Confirm 消息包括一组参数或字段。Auth-Confim 消息可以包括与 EAPOL- 密钥消息有关的消息或数据。该 EAPOL- 密钥有关的消息或数据可以包括使用 KCK 在 EAPOL- 密钥有关的消息或数据上计算出的消息完整性校验 (MIC)。当根据本发明使用完美前向保密 (PFS) 时，完美前向保密 - 消息完整性校验 (PFS-MIC) 可以并入授权 (Auth-Confirm) 消息中。可以使用 PFS、KCK、和 / 或其它数据、消息或信息来计算 PFS-MIC。PFS-MIC 可以提供对 AssocReq4002 和 Assoc Resp15002 和 Auth- 确认 20002 的组合中的一部分或全部的完整保护。受完整保护的部分可以与 Auth 确认 20002 中的 EAPOL- 密钥有关的消息或数据相对应。PFS-MIC 可以位于 EAP- 结束 Re-Auth 或 DHCP 或 EAPOL- 密钥有关的消息或数据的内部。PFS-MIC 可以是 Auth-Confirm 的一部分，但是位于 EAP- 结束 Re-Auth 或 DHCP 或 EAPOL- 密钥有关的消息或数据的外部。

[0039] 在 21002 处，站 120 可以安装包括 PFS-TK、GTK 和 IGTK 的密钥或数据。在 21004 处，站 120 可以安装由动态主机配置协议 (DHCP)128 通过认证过程而生成的 IP(互联网协议) 地址。

[0040] 在 22002 处，第二接入点 124 可以使用密钥确认密钥来验证消息完整性校验

(MIC)。在 2302 处，第二接入点 124 可以使用 PFS-KCK 数据和 / 或其它数据、消息或信息对 PFS-MIC 进行验证。在 2402 处，第二接入点 124 可以安装包括 PFS-TK、GTK 和 IGTK 的密钥或数据。在 24004 处，第二接入点 124 可以安装站 120 的 IP（互联网协议）地址。在 24004 处，站 120 可以使用所分配的 IP（互联网协议）地址，通过第二接入点 124 来访问互联网和 / 或其它公共网络或私有网络。可能要注意的是 :虽然图 3A 和 3B 中示出的加密和有关处理描绘了站 120 与该站 120 正在前往的第二接入点 124 之间的交换，但是相同或相似的处理可以应用于 :站 120 与第一接入点 122 之间、站 120 与第三接入点（没有示出）之间和 / 或其它网络配置。

[0041] 可能同样要注意的是 :在图 2 中所示的增强型认证过程完成之后，站 120 与第二接入点 124 之间进行的会话受到成对主密钥 (PMK)、成对临时密钥 (PTK) 和 / 或可扩展认证协议 (EAP) 的其它安全特征（包括四路握手）的保护。然而，根据本发明的一些方面，与“裸”四路握手相比，与完美前向保密 (PFS) 有关的特征的添加以及基于 Diffie-Hellman 发生器的公 / 私有密钥集合的使用提供了增加的安全性。根据本发明的一些方面，捕获并存储站 120 与第二接入点 124（或者任何相当的接入点）之间的消息流（包括成对主密钥 (PMK) 和成对临时密钥 (PTK)）的攻击者仍然不能够破坏那些流的完整性，因为完成该破坏所需的共享 Diffie-Hellman 临时密钥 (SharedDHEKey) 的再创建在没有属于该站的私有 Diffie-Hellman 临时密钥 (SDHEPrivKey) 和 / 或属于接入点的私有 Diffie-Hellman 临时密钥 (ADHEPrivKey) 情况下是不可能的，而所述 SDHEPrivKey 和 ADHEPrivKey 在建立该会话之后相对较短的命令中已经被丢弃了。

[0042] 可以在各种网络连接环境（包括，例如，其中并入了快速初始链路建立 (FILS) 能力的 Wi-Fi 网络连接环境）中实现根据用于在 Wi-Fi 网络会话中提供完美前向保密的系统和方法的安全性处理。快速初始链路建立 (FILS) 包括由电气和电子工程师协会 (IEEE) 标准 802.11ai 发布的一套通信协议，其旨在应当站向接入点的接近和注册以瞬间方式发生的情况，诸如经过公共机场、公共汽车终点站和 / 或其它环境的智能电话或具有无线功能的膝上型计算机，在这些情况下，可以建立无线连接的速度是很高的。然而，应当明白的是，不管是否使用快速初始链路建立 (FILS)，可以将根据本发明的平台和技术整合到其它网络配置中。

[0043] 在进一步的考虑中，根据本发明的一些方面，站 120 和第二接入点 124（或者其它接入点或节点）可以分别存储在会话期间生成的共享 Diffie-Hellman 临时密钥 (SharedDHEKey)，以便在以后相同的两个设备之间的第二次会话中重新使用。当检索到而不是生成共享 Diffie-Hellman 临时密钥 (SharedDHEKey) 时，在两端都可以节省大量的运算。根据这些实施例，例如，站 120 和第二接入点 124（或者其它接入点或节点）中的每一个可以将标识符与共享 Diffie-Hellman 临时密钥 (SharedDHEKey) 相关联，例如，通过基于它们各自的公有 Diffie-Hellman 临时密钥 (SDHEPubKey 和 ADHEPubKey) 中的一个或这二者来生成哈希 (hash) 函数输出、或者通过其它方式。在其它实施例中，站 120 和接入点 124 不需要为共享 Diffie-Hellman 临时密钥 (SharedDHEKey) 创建明确的标识符，取代地，而是可以被配置为 :当遇到或者识别出与先前会话中的站或接入点相同的站或接入点时，自动关联和检索该密钥。

[0044] 图 4 示出了用于使用延迟的 Anonce 来执行图 3A 和 3B 的加密布置的配置和操作

的特定的呼叫流序列，一般将该呼叫流序列标示为 400。

[0045] 例如，第二接入点 124 不是像图 3A 中所示的经由信标消息从第二接入点 124 向站 120 发送 Anonce，而是可以在其它消息中发送 Anonce。在特定的实施例中，第二接入点 124 在第二接入点 124 处生成 PTK 之后发送 Anonce。为了说明，在向站 120 发送 Anonce 之前，在 402 处，第二接入点 124 可以从站 120 接收授权消息。授权消息可以包括 Snonce、SDHEPubKey 和 EAP-Re-auth- 发起消息。在 404 处，第二接入点 124 可以生成 SharedDHEKey 并且根据 rMSK、Snonce 和 Anonce 推导出 PTK。此外，在 404 处，第二站 124 还可以生成 GTK 和 IGTK。

[0046] 在 406 处，第二接入点 124 可以在授权回复消息中向站 120 发送 Anonce。授权回复消息可以包括 Anonce、EAP- 结束 Re-auth 信息单元以及 ADHEPubKey。在 408 处，站 120 可以在接收授权回复消息之后生成 SharedDHEKey 和 PTK。在 410 处，站 120 可以向第二接入点 124 发送关联请求。关联请求可以包括具有快速分配消息和密钥确认的 DHCP- 发现。在 412 处，第二接入点 124 可以向站 120 发送关联响应。关联响应可以包括具有快速分配 (IP-addr) 消息的 DHCP-Ack、GTK 和 IGTK。

[0047] 图 5 示出了根据实施例，可以用于在 Wi-Fi 网络会话中提供完美前向保密的实施例中的各种硬件、软件和其它资源。在如图所示的实施例中，接入点 108 可以包括与存储器 144（诸如电子随机存取存储器），以及与网络接口（诸如以太网和 / 或与互联网和 / 或其它网络的其它有线或无线连接）进行通信的处理器 142 的特征。处理器 140 可以被编程或者配置为 :执行根据本发明对操作、网络连接性操作和其它操作进行编码的字符集。处理器 140 还可以与本地数据储存器 146（诸如本地硬盘和 / 或其它存储）以及可以连接到射频天线 152（或多个天线）的无线接口 148（诸如 Wi-Fi 可兼容芯片组，包括射频芯片组和相关联的硬件和软件）进行通信。存储器 144 可以包括指令 154。指令 154 可以使得处理器 (例如，处理器 140) 经由 Wi-Fi 网络来实施用于数据交换的 PFS。

[0048] 结合所描述的实施例，一种装置可以包括 :用于经由无线网络接口与至少一个站进行通信的模块。例如，用于进行通信的模块可以包括 :图 1 的站 102 的一个或多个组件 (例如，发射机、接收机、天线）、图 1 的接入点 108 的一个或多个组件（例如，发射机、接收机、天线）、图 2 的射频天线 150、图 3A、图 3B 和图 4 的站 120 的一个或多个组件（例如，发射机、接收机、天线）、图 3A、图 3B 和图 4 的第一接入点 120 的一个或多个组件（例如，发射机、接收机、天线）、图 3A、图 3B 和图 4 的第二接入点 124 的一个或多个组件（例如，发射机、接收机、天线）、图 5 的无线接口 148、图 5 的射频天线 152、被配置为无线地传送数据的一个或多个其它设备、或者它们的任意组合。该装置还可以包括用于进行处理的模块，该用于进行处理的模块被配置为 :生成共享主秘密并且生成一组共享临时密钥数据。该组共享临时密钥数据是独立于共享主秘密而生成的。与共享主秘密的有效期相比，该组共享临时密钥数据的有效期较短。用于处理的模块还被配置为 :至少基于共享主秘密和一组共享临时密钥数据，对要发送到至少一个站的至少一个消息进行加密。例如，用于处理的模块可以包括 :图 1 的站 102 的一个或多个组件（例如，处理器）、图 1 的接入点 108 的一个或多个组件（例如，处理器）、图 2 的操作系统 112 和指令 116、图 3A、图 3B 和图 4 的站 120 的一个或多个组件（例如，处理器）、图 3A、图 3B 和图 4 的第一接入点 120 的一个或多个组件（例如，处理器）、图 3A、图 3B 和图 4 的第二接入点 124 的一个或多个组件（例如，处理器）、图

5 的处理器 142 和指令 154、被配置为处理传送数据的一个或多个其它设备、或者它们的任意组合。

[0049] 前面的描述是说明性的，并且对本领域的技术人员来说，可以出现配置和实现的变型。例如，虽然已经描述和示出了站 120 接近第二接入点 124 来进行注册和应用完美前向保密 (PFS) 的实施例，但是，在其它实施例中，例如，可能有使用群组主密钥、群组共享 Diffie-Hellman 临时密钥 (DHESharedKey) 和 / 或其它密钥或数据的、连接到一个接入点的多个站。或者，在其它实施例中，接近接入点并且向接入点注册的每个站可以与该站分别交换单独的自组织或共享 Diffie-Hellman 临时密钥 (DHESharedKey)。

[0050] 虽然已经描述和示出了可以在也使用按照 IEEE802.11ai 的快速初始链路建立 (FILS) 标准的网络连接情景中使用完美前向保密 (PFS) 的实施例，但是根据本发明的完美前向保密 (PFS) 可以应用于不包含快速初始链路建立 (FILS) 的环境中。类似地，虽然已经描述了在其中一个认证服务器 126 操作以支持提供密钥和建立经加密的消息流的实施例，但是在其它实施例中，可以使用多个认证服务器和 / 或服务。被描述为单数或集成式的其它资源在其它实施例中可以是复数或分布式的，并且被描述为多个或分布式的资源在其它实施例中可以是组合的。另外，虽然已经描述了在接入点 / 站布置中配置的 Wi-Fi 网络中进行操作的实施例，但是，在其它实施例中，也可以应用这些教导将完美前向保密 (PFS) 和其它特征合并入 Wi-Fi 网络的对等或其它配置中。还有，虽然已经描绘了使用 Wi-Fi 无线网络连接标准的实施例，但是根据本发明提供的完美前向保密 (PFS) 也可以应用于与 Wi-Fi 网络不同的其它网络。

[0051] 所公开的实施例中的一个或多个实施例可以在可以包括通信设备、固定位置数据单元、移动位置数据单元、移动电话、蜂窝电话、计算机、平板电脑、便携式计算机或台式计算机的系统或装置中实现。此外，系统或装置可以包括机顶盒、娱乐单元、导航设备、个人数字助理 (PDA)、监视器、计算机显示器、电视、调谐器，无线电、卫星无线电、音乐播放器、数字音乐播放器、便携式音乐播放器、视频播放器、数字视频播放器、数字视频光盘 (DVD) 播放器、便携式数字视频播放器、存储或检索数据或计算机指令的任何其它设备，或它们的组合。作为另一个说明性而非限制性的示例，系统或装置可以包括诸如移动电话、手持式个人通信系统 (PCS) 单元的远程单元、诸如个人数据助理的便携式数据单元、具有全球定位系统 (GPS) 功能的设备、导航设备、诸如仪表读取装置的固定位置数据单元、或者存储或检索数据或计算机指令的任何其它设备、或者它们的任意组合。尽管图 1-5 中的一个或多个图可能示出了根据本申请的教导的系统、装置和 / 或方法，但本申请并不局限于这些示出的系统、装置和 / 或方法。可以在包括集成电路 (其包括存储器、处理器和片上电路) 的任何设备中适当地采用本申请的实施例。

[0052] 应当理解的是，对本文元素的任何引用使用诸如“第一”、“第二”等指定，通常并不限制那些元素的数量或顺序。相反，本文中可以将这些指定用作区分两个或更多个元素或者一个元素的实例的简便方法。因此，对于第一元素和第二元素的引用并不意味着 :仅可以使用两个元素，或者第一元素必须以某种方式位于第二元素之前。此外，除非另行声明，否则元素的集合可以包括一个或多个元素。此外，本说明书或权利要求书中使用的“A、B 或 C 中的至少一个”的术语形式是指“A 或 B 或 C 或这些元素的任意组合”。

[0053] 如本文所使用的，术语“确定”涵盖多种多样的动作。例如，“确定”可以包括计算、

运算、处理、推导、研究、查询（例如，在表格、数据库或其它数据结构中进行查询）、查明等。此外，“确定”可以包括接收（例如，接收信息）、访问（例如，访问存储器中的数据）等。此外，“确定”可以包括解析、选定、选择、建立等。此外，本文中使用的“信道宽度”在某些方面中可以涵盖带宽或者也可以被称为带宽。

[0054] 如本文所使用的，指代一列条目“中的至少一个”的短语是指这些条目的任意组合，包括单数成员。举例说明，“a、b、或 c 中的至少一个”旨在覆盖 :a、b、c、a-b、a-c、b-c 和 a-b-c。

[0055] 上面已经对各种示例性的部件、框、模块、电路以及步骤围绕其功能进行了总体描述。至于这种功能是实现成硬件还是实现成处理器可执行的软件，取决于具体应用和向整个系统施加的设计约束。此外，上述方法的各种操作可以由能够执行这些操作的任何适当的单元来执行，诸如各种硬件和 / 或软件组件、电路和 / 或模块。通常，在图 1 至图 5 中示出的任何操作可以由能够执行这些操作的相应功能单元来执行。熟练的技术人员可以针对每个特定应用，以变通的方式实现所描述的功能，但是，这种实现决策不应解释为导致背离本申请的保护范围。

[0056] 本领域技术人员会进一步明白，被设计为执行本文所描述的功能的通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列信号 (FPGA) 或其它可编程逻辑器件 (PLD)、分立门或者晶体管逻辑、分立硬件组件（例如，电子硬件）、处理器执行的计算机软件、或者它们的任意组合，可以实现或执行结合本申请所描述的各种示例性的逻辑框、模块、电路和算法步骤。通用处理器可以是微处理器，或者，该处理器也可以是任何市售的处理器、控制器、微控制器或者状态机。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、与 DSP 核相结合的一个或多个微处理器、或者任何其它这类结构。

[0057] 在一个或多个方面中，可以使用硬件、软件、固件或它们的任意组合来实现所描述的功能。如果用软件实现，则可以将功能存储为计算机可读介质上的一条或多条指令或代码。计算机可读介质包括计算机可读存储介质和通信介质，所述通信介质包括有助于计算机程序从一个地点向另一个地点传输的任何介质。存储介质可以是计算机能够访问的任何可用介质。举例说明而非限制，这种计算机可读存储介质可以包括随机存取存储器 (RAM)、只读存储器 (ROM)、可编程只读存储器 (PROM)、可擦除 PROM(EPROM)、电可擦除 PROM(EEPROM)、寄存器、硬盘，可移动磁盘、压缩光盘只读存储器 (CD-ROM)、其它光盘存储器、磁盘存储器、磁性存储设备、或可以用于存储具有指令或数据结构形式的所期望的程序代码并且可由计算机访问的任何其它介质。替代地，计算机可读介质（例如，存储介质）可以是处理器的组成部分。处理器和存储介质可以位于专用集成电路 (ASIC) 中。该 ASIC 可以位于计算设备或用户终端中。或者，处理器和存储介质可以作为分立组件位于计算设备或用户终端中。

[0058] 此外，任何连接可以被适当地称为计算机可读介质。例如，如果使用同轴电缆、光纤光缆、双绞线、数字用户线 (DSL) 或者诸如红外线、无线电和微波之类的无线技术从网站、服务器或其它远程源发送软件，那么介质的定义中包括同轴电缆、光纤光缆、双绞线、DSL 或者诸如红外线、无线电和微波之类的无线技术。如本文中所使用的，磁盘和光碟包括压缩光碟 (CD)、激光光碟、光碟、数字多功能光碟 (DVD)、软盘和蓝光®光碟，其中磁盘通常

磁性地复制数据，而光碟则使用激光来光学地复制数据。因此，在一些方面，计算机可读介质可以包括非临时性计算机可读介质（例如，有形介质）。此外，在一些方面，计算机可读介质可以包括临时性计算机可读介质（例如，信号）。上面的组合也应当包括在计算机可读介质的范围之内。

[0059] 本文所公开的方法包括用于实现所述方法的一个或多个步骤或动作。在不脱离权利要求的保护范围的前提下，方法步骤和／或动作可以相互交换。换言之，除非规定了特定顺序的步骤或动作，否则可以在不脱离权利要求的保护范围的前提下，修改特定步骤和／或动作的顺序和／或使用。

[0060] 因此，某些方面可以包括用于执行本文所展示的操作的计算机程序产品。例如，这样的计算机程序产品可以包括其上存储（和／或编码）有指令的计算机可读介质，所述指令可由一个或多个处理器执行以执行本文所描述的操作。对于某些方面，计算机程序产品可以包括封装材料。

[0061] 也可以在传输介质上发送软件或指令。例如，如果软件是使用同轴线缆、光纤线缆、双绞线、数字用户线 (DSL)、或者诸如红外线、无线电和微波之类的无线技术，从网站、服务器或其它远程源传输的，那么传输介质的定义中包括同轴线缆、光纤线缆、双绞线、DSL、或者诸如红外线、无线电和微波之类的无线技术。

[0062] 此外，应当明白，在适当的时候，用户终端和／或基站能够下载和／或以其它方式获得用于执行本文所描述的方法和技术的模块和／或其它适当的单元。或者，本文中描述的各种方法可经由存储模块（例如，RAM、ROM、诸如压缩光盘 (CD) 或软盘等物理存储介质）来提供。此外，可以使用用于向设备提供本文所描述的方法和技术的任何其它适当的技术。

[0063] 应该理解的是，权利要求不限于上面说明的精确的配置和组件。为了使本领域普通技术人员能够实施或者使用所公开的实施例，提供了对所公开的实施例的前述描述。尽管前文涉及本申请的一些方面，但在不背离本申请的基本范围的前提下，可以设计本申请的其它以及进一步的方面，并且范围是由后面的权利要求确定的。在不背离本申请或权利要求的范围的前提下，可以对本文中描述的布置、操作和实施例的细节进行各种修改、改变和变型。因此，本申请并不旨在限于本文中的这些实施例，而是符合与如后面的权利要求及其等价物所限定的原理和新颖特征相一致的可能的最宽范围。

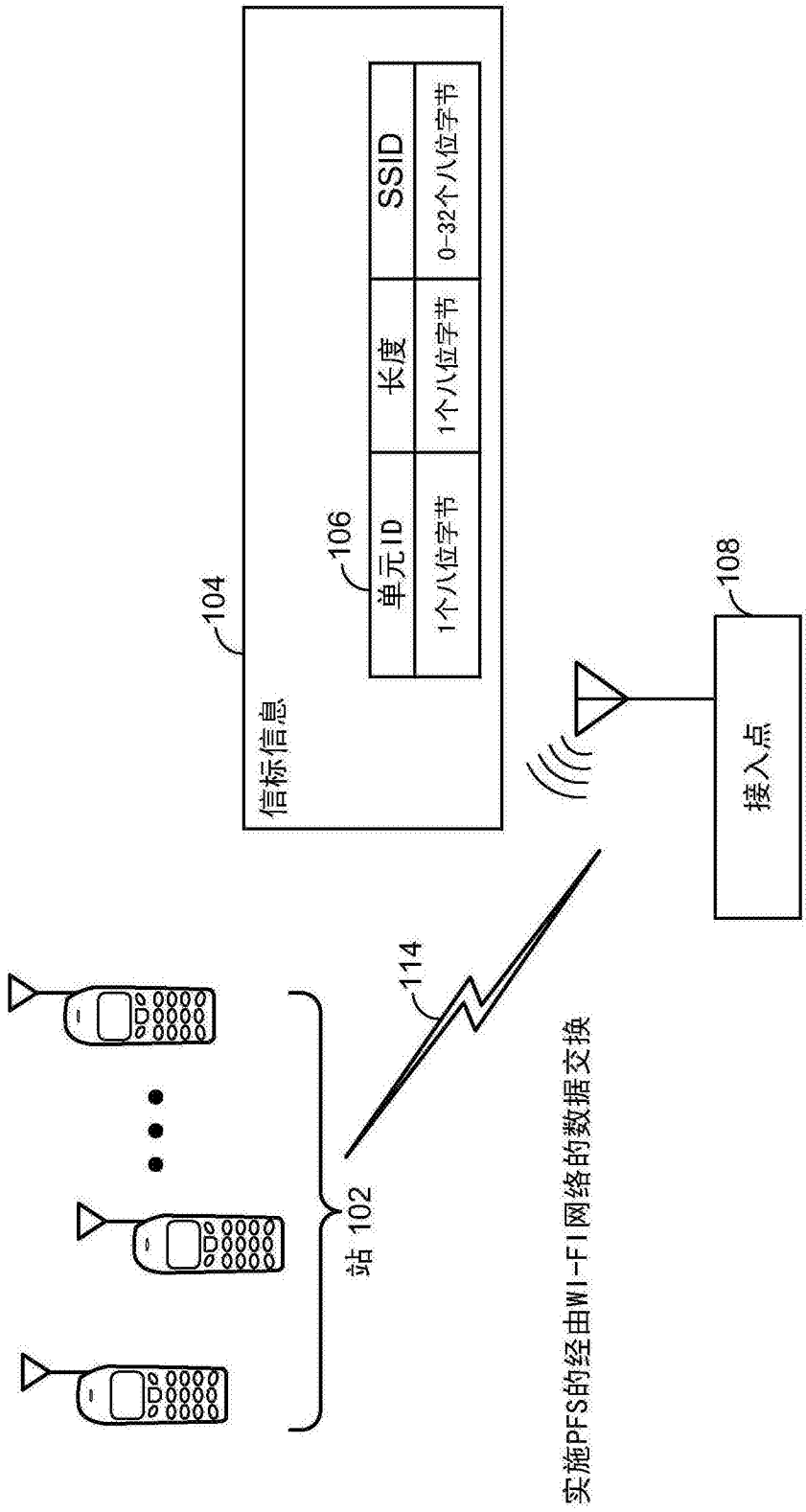

104
信标信息
106
单元ID
1个八位字节
长度
1个八位字节
SSID
0-32个八位字节
108
接入点
114
站 102
实施PFS的经由WI-FI网络的数据交换

图 1

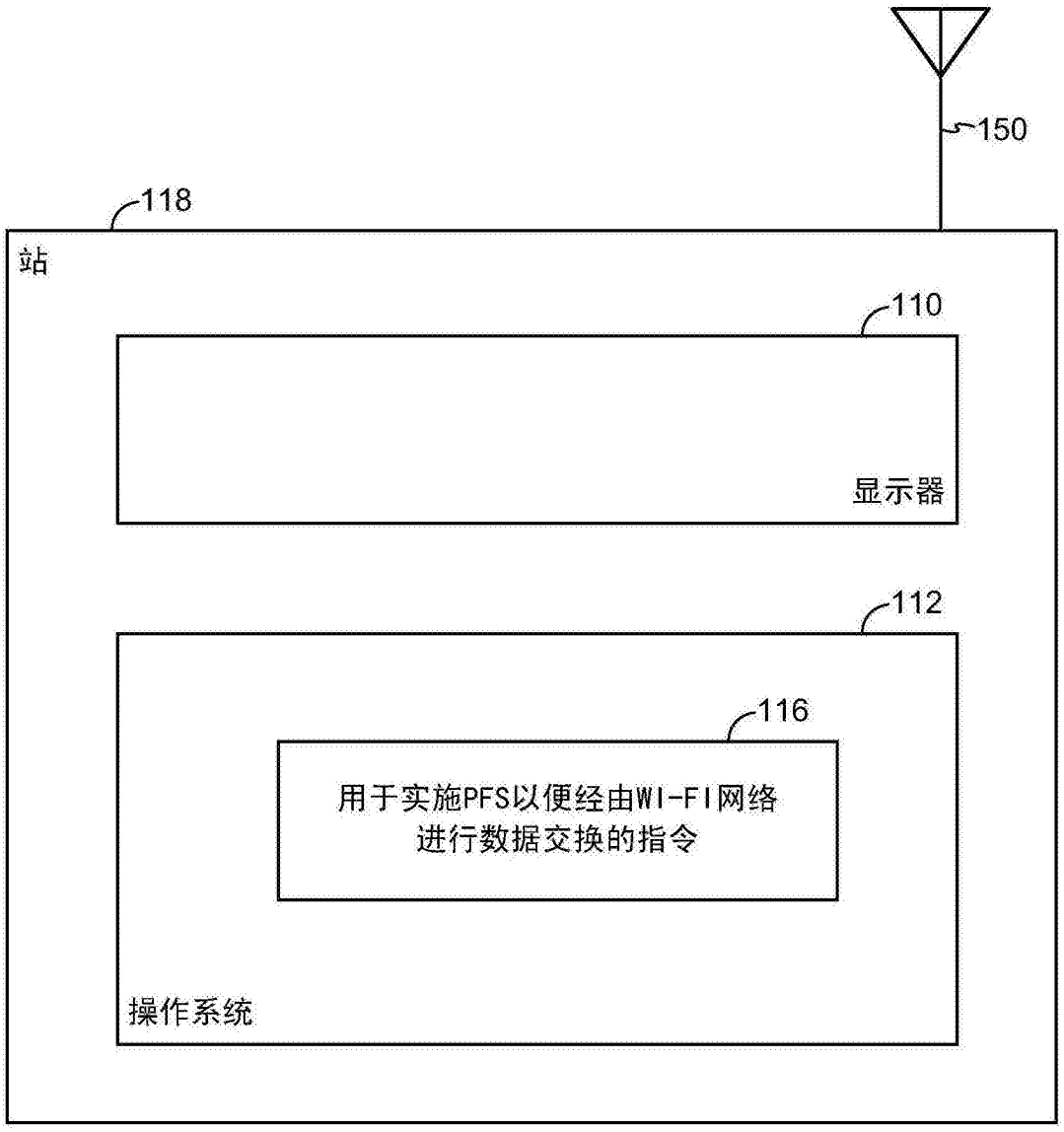


图 2

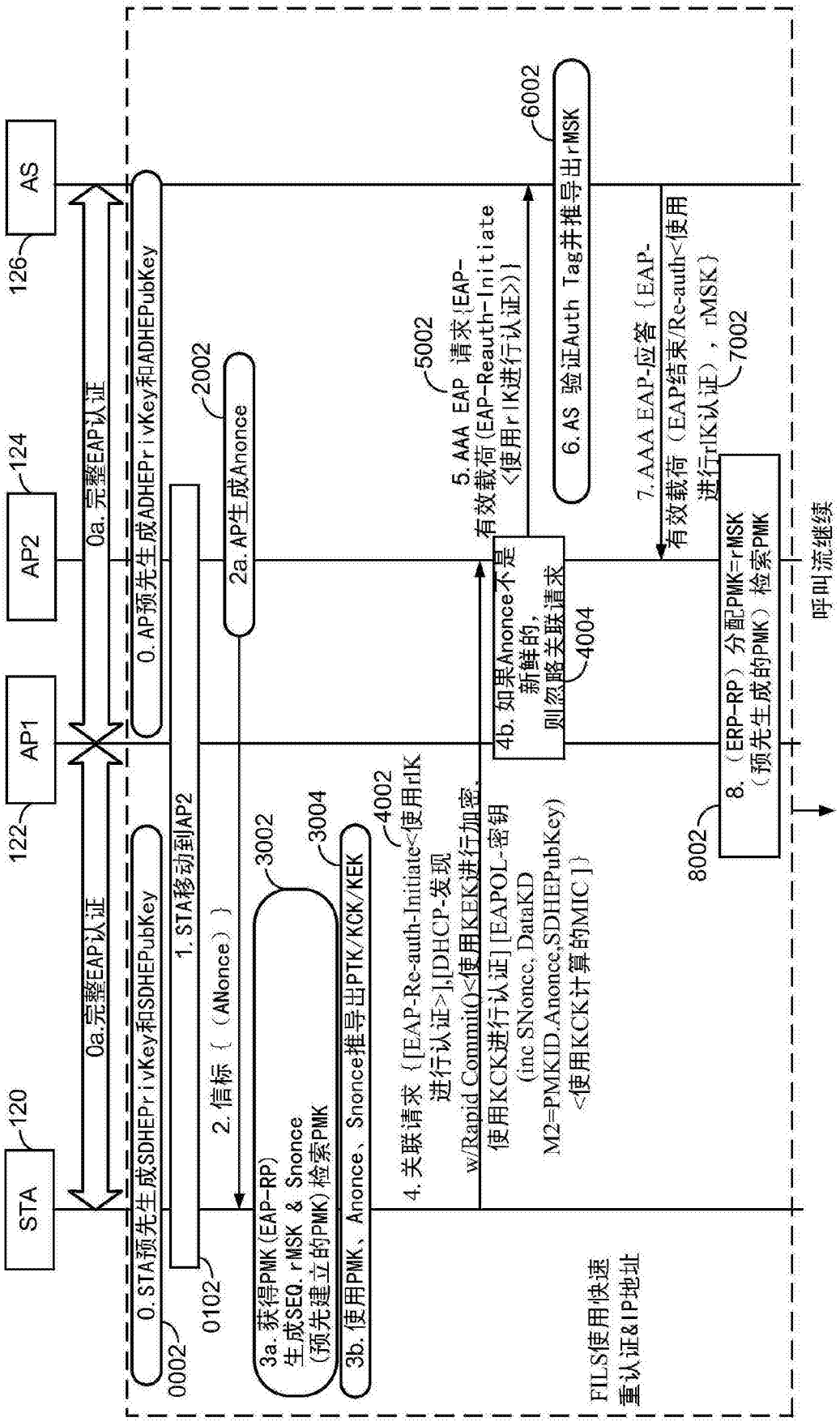

STA
AP1
AP2
AS
120
122
124
126
0a.完整EAP认证
0a.完整EAP认证
0. STA预先生成SDHEPrivKey和SDHEPubKey
0. AP预先生成ADHEPrivKey和ADHEPubKey
0002
1. STA移动到AP2
0102
2. 信标 {（ANonce）}
2002
2a. AP生成Anonce
3a. 获得PMK(EAP-RP)
生成SEQ. rMSK & Snonce
(预先建立的PMK)检索PMK
3002
3004
3b. 使用PMK、Anonce、Snonce推导出PTK/KCK/KEK
4002
4. 关联请求 {[EAP-Re-auth-Initiate<使用rIK进行认证>],[DHCP-发现
w/Rapid Commit()<使用KEK进行加密,
使用KCK进行认证] [EAPOL-密钥
(inc SNoncc, DataKD
M2=PMKID.Anonce,SDHEPubKey)
<使用KCK计算的MIC]}
4004
4b. 如果Anonce不是
新鲜的,
则忽略关联请求
5002
5. AAA EAP 请求{EAP-
有效载荷(EAP-Reauth-Initiate
<使用rIK进行认证>)}
6002
6. AS 验证Auth Tag并推导出rMSK
7. AAA EAP-应答 {EAP-
有效载荷 (EAP结束/Re-auth<使用
进行rIK认证），rMSK}
7002
8002
8. （ERP-RP）分配PMK=rMSK
（预先生成的PMK）检索PMK
呼叫流继续
FILS使用快速
重认证&IP地址

图 3A

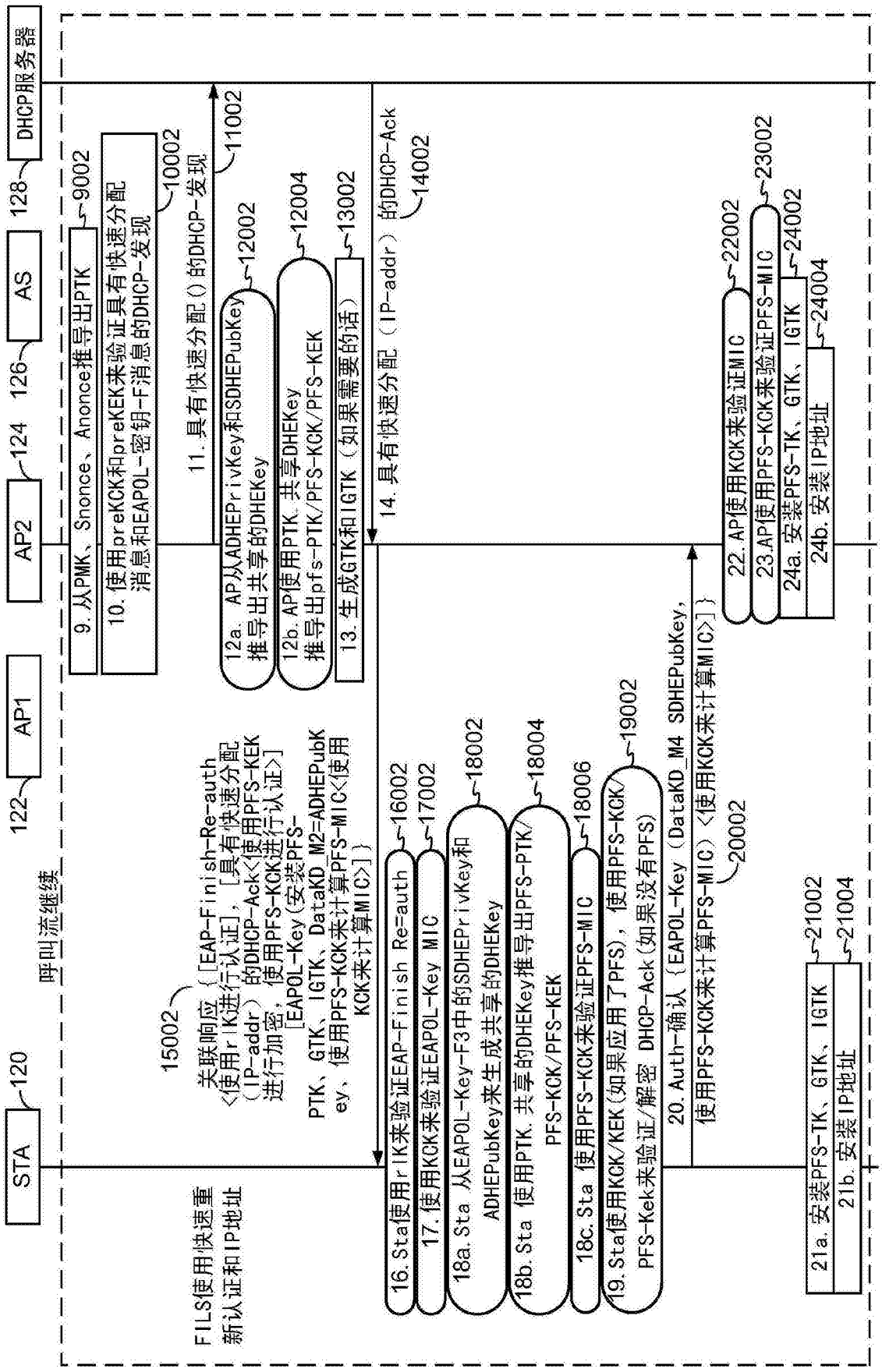

STA
120
AP1
122
AP2
124
AS
126
DHCP服务器
128
呼叫流继续
FILS使用快速重新认证和IP地址
9. 从PMK、Snonce、Anonce推导出PTK
9002
10. 使用preKCK和preKEK来验证具有快速分配消息和EAPOL-密钥-F消息的DHCP-发现
10002
11. 具有快速分配()的DHCP-发现
11002
12a. AP从ADHEPrivKey和SDHEPubKey推导出共享的DHEKey
12002
12b. AP使用PTK. 共享DHEKey推导出pfs-PTK/PFS-KCK/PFS-KEK
12004
13. 生成GTK和IGTK（如果需要的话）
13002
14. 具有快速分配（IP-addr）的DHCP-Ack
14002
15002
关联响应｛[EAP-Finish-Re-auth <使用rIK进行认证]，[具有快速分配（IP-addr）的DHCP-Ack<使用PFS-KEK进行加密，使用PFS-KCK进行认证>][EAPOL-Key(安装PFS-PTK、GTK、IGTK、DataKD_M2=ADHEPubKey，使用PFS-KCK来计算PFS-MIC<使用KCK来计算MIC>]｝
16. Sta使用rIK来验证EAP-Finish Re=auth
16002
17. 使用KCK来验证EAPOL-Key MIC
17002
18a. Sta 从EAPOL-Key-F3中的SDHEPrivKey和ADHEPubKey来生成共享的DHEKey
18002
18b. Sta 使用PTK. 共享的DHEKey推导出PFS-PTK/PFS-KCK/PFS-KEK
18004
18c. Sta 使用PFS-KCK来验证PFS-MIC
18006
19. Sta使用KCK/KEK(如果应用了PFS)，使用PFS-KCK/PFS-Kek来验证/解密 DHCP-Ack(如果没有PFS)
19002
20. Auth-确认｛EAPOL-Key（DataKD_M4 SDHEPubKey，使用PFS-KCK来计算PFS-MIC）<使用KCK来计算MIC>]｝
20002
22. AP使用KCK来验证MIC
22002
23. AP使用PFS-KCK来验证PFS-MIC
23002
24a. 安装PFS-TK、GTK、IGTK
24002
24b. 安装IP地址
24004
21a. 安装PFS-TK、GTK、IGTK
21002
21b. 安装IP地址
21004

图 3B

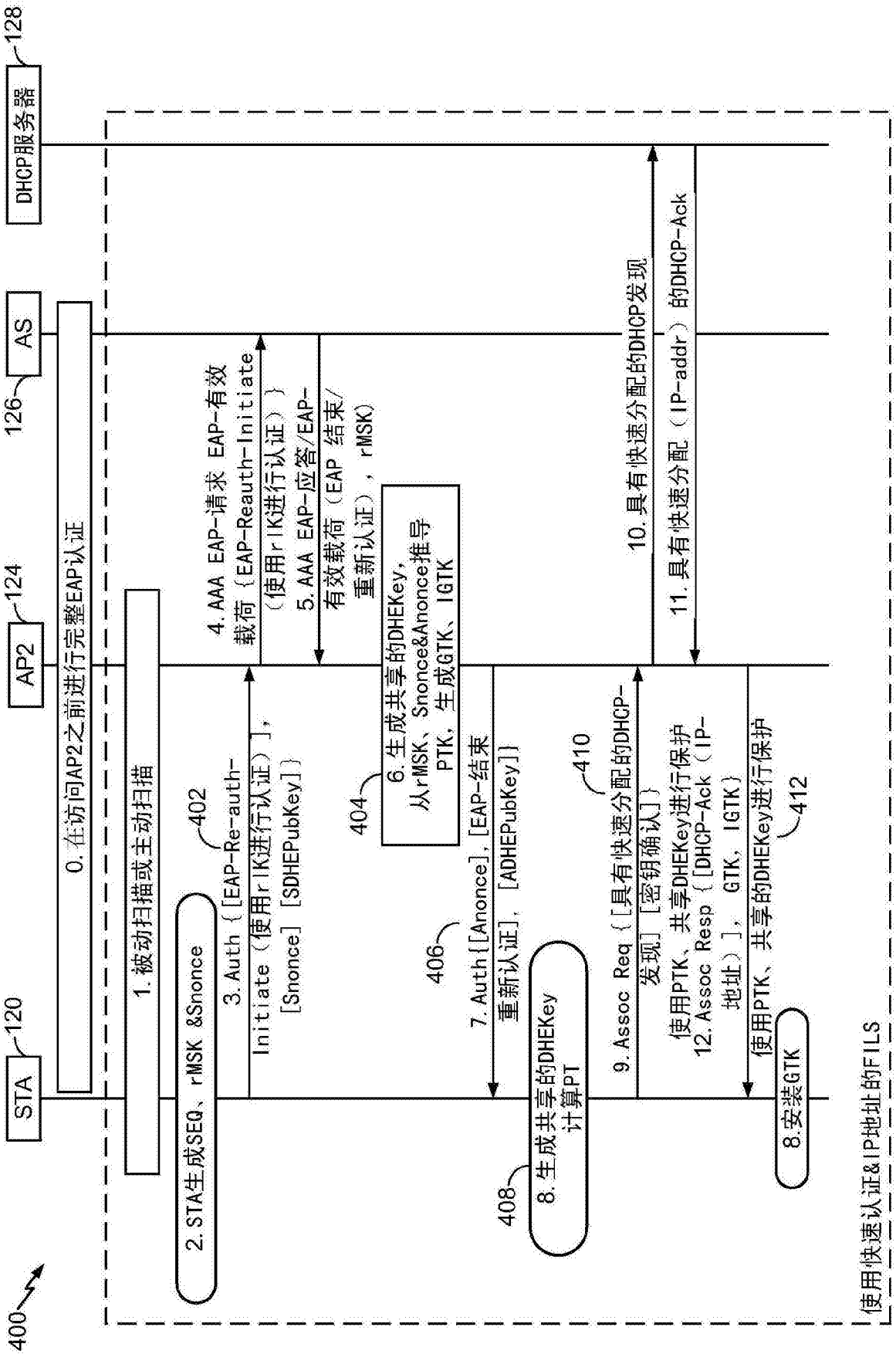

400
STA
120
AP2
124
AS
126
DHCP服务器
128
使用快速认证&IP地址的FILS
0. 在访问AP2之前进行完整EAP认证
1. 被动扫描或主动扫描
2. STA生成SEQ、rMSK &Snonce
402
3. Auth｛[EAP-Re-auth-Initiate（使用rIK进行认证）]，[Snonce] [SDHEPubKey]｝
4. AAA EAP-请求 EAP-有效载荷｛EAP-Reauth-Initiate（使用rIK进行认证）｝
5. AAA EAP-应答/EAP-有效载荷（EAP 结束/重新认证），rMSK)
404
6. 生成共享的DHEKey，从rMSK、Snonce&Anonce推导PTK，生成GTK、IGTK
406
7. Auth{[Anonce]，[EAP-结束重新认证]，[ADHEPubKey]}
408
8. 生成共享的DHEKey计算PT
410
9. Assoc Req｛[具有快速分配的DHCP-发现] [密钥确认]｝
10. 具有快速分配的DHCP发现
11. 具有快速分配（IP-addr）的DHCP-Ack
使用PTK、共享DHEKey进行保护
12. Assoc Resp｛[DHCP-Ack（IP-地址）]，GTK，IGTK｝
412
使用PTK、共享的DHEKey进行保护
8.安装GTK

图 4

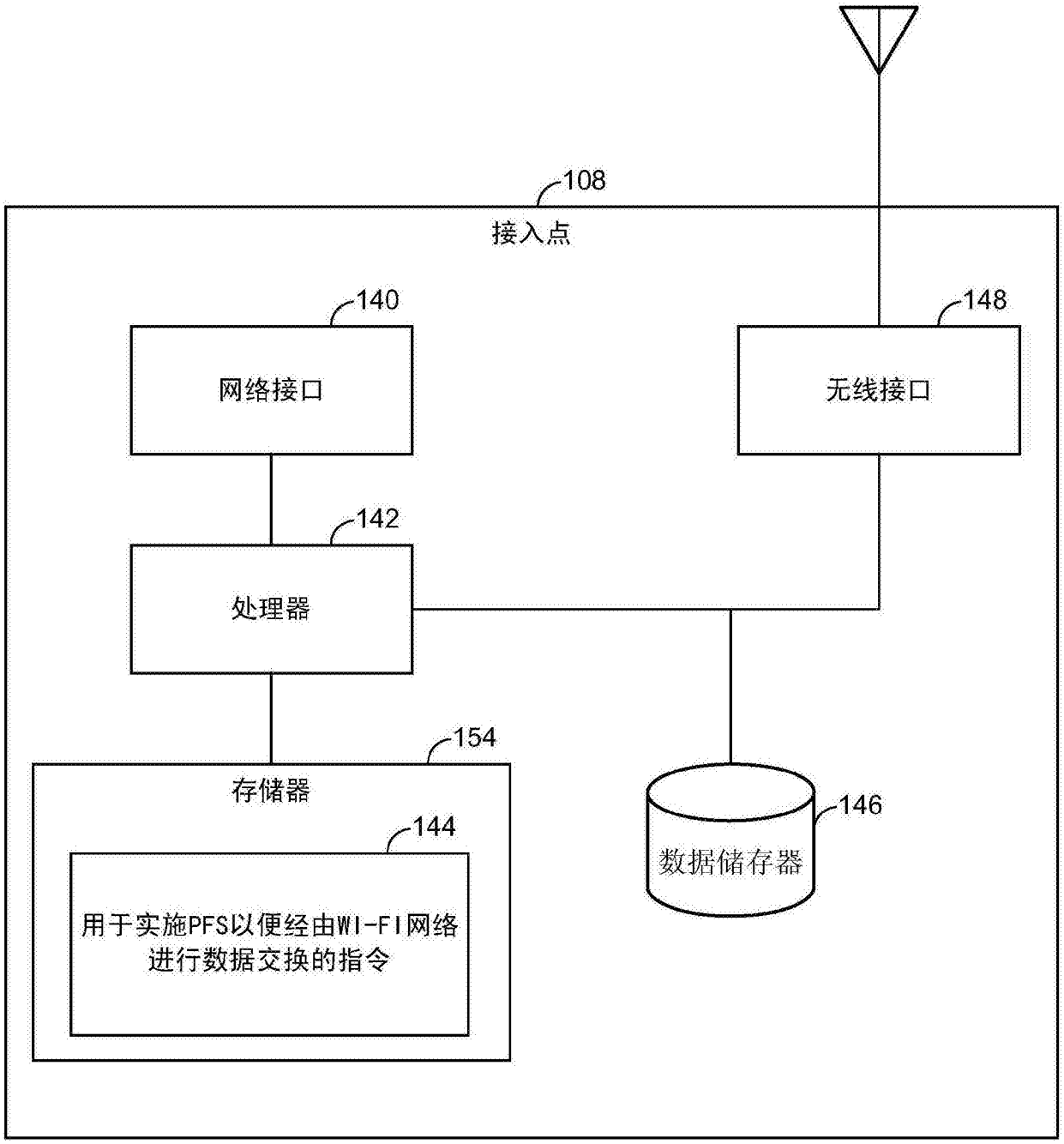

108
接入点
140
网络接口
148
无线接口
142
处理器
154
存储器
144
用于实施PFS以便经由WI-FI网络进行数据交换的指令
146
数据储存器

图 5