(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 103096307 A
(43)申请公布日 2013.05.08

(21)申请号 201110331974.4

(22)申请日 2011.10.27

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区科技南路55号

(72)发明人 冯成燕

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 余刚 梁丽超

(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/06(2009.01)
H04W 84/12(2009.01)

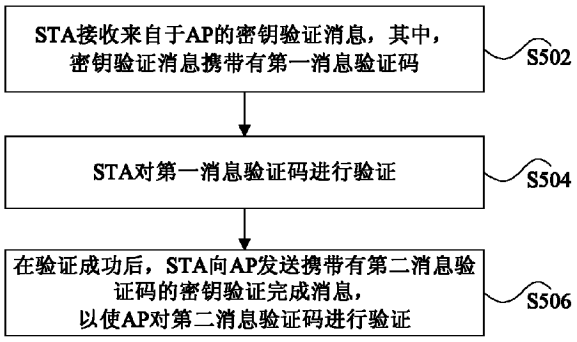
权利要求书3页 说明书13页 附图5页

(54)发明名称

密钥验证方法及装置

(57)摘要

本发明公开了一种密钥验证方法及装置，该方法包括：STA接收来自于AP的密钥验证消息，其中，密钥验证消息携带有第一消息验证码；STA对第一消息验证码进行验证；在验证成功后，STA向AP发送携带有第二消息验证码的密钥验证完成消息，以使AP对第二消息验证码进行验证。通过本方法提供的技术方案，减少了现有技术中安全验证的繁琐步骤，且达到了缩短了入网时延的效果，从整体上提升了系统的性能，同时也提高了用户体验。



CN 103096307 A

1. 一种密钥验证方法，其特征在于，包括：

工作站 STA 接收来自于接入点 AP 的密钥验证消息，其中，所述密钥验证消息携带有第一消息验证码；

所述 STA 对所述第一消息验证码进行验证；

在验证成功后，所述 STA 向所述 AP 发送携带有第二消息验证码的密钥验证完成消息，以使所述 AP 对所述第二消息验证码进行验证。

2. 根据权利要求 1 所述的方法，其特征在于，所述 STA 接收来自于所述 AP 的密钥验证消息之前，还包括以下之一：所述 STA 和所述 AP 认证成功；所述 STA 和所述 AP 开始进行认证。

3. 根据权利要求 1 所述的方法，其特征在于，所述密钥验证消息还携带有以下至少之一：所述第一随机数、所述第二随机数、计数器值、关联标识。

4. 根据权利要求 1 所述的方法，其特征在于，在所述 STA 接收来自于所述 AP 的密钥验证消息之前，还包括：

所述 AP 生成第一随机数或计数器值；

所述 AP 按照预定的密钥衍生算法对认证过程中生成的成对主密钥 PMK、所述 STA 生成的第二随机数以及所述 AP 生成的第一随机数计算获取成对临时密钥 PTK，或者对所述 PMK 和计数器值计算获取所述 PTK，并截取所述 PTK 获得密钥确认密钥 KCK；

所述 AP 根据所述 KCK 计算获取所述第一消息验证码，并将所述第一消息验证码携带在所述密钥验证消息中发送。

5. 根据权利要求 4 所述的方法，其特征在于，所述 AP 截取所述 PTK 获得所述 KCK 时，还包括：所述 AP 截取所述 PTK 获得所述密钥加密密钥 KEK 和 / 或临时密钥 TK。

6. 根据权利要求 5 所述的方法，其特征在于，在将所述第一消息验证码携带在所述密钥验证消息中发送之前，还包括：所述 AP 将所述第一随机数发送至所述 STA；

则所述 AP 将所述第一消息验证码携带在所述密钥验证消息中发送包括：所述 AP 采用所述 KEK 或所述 TK 对所述密钥验证消息进行加密后发送。

7. 根据权利要求 5 所述的方法，其特征在于，在所述 STA 接收来自于所述 AP 的密钥验证消息之前，还包括：

所述 AP 随机选取组临时密钥 GTK，采用所述 KEK 加密所述 GTK；

所述 AP 将加密的所述 GTK 携带在密钥验证消息中向所述 STA 发送。

8. 根据权利要求 7 所述的方法，其特征在于，在所述 AP 将加密的所述 GTK 和 / 或所述第三随机数携带在所述密钥验证消息中向所述 STA 发送之后，还包括：

所述 STA 接收来自于所述 AP 的所述密钥验证消息；

所述 STA 采用所述 KEK 解密所述密钥验证消息获得所述 GTK。

9. 根据权利要求 1 所述的方法，其特征在于，所述 STA 对所述第一消息验证码进行验证包括：

所述 STA 按照所述预定的密钥衍生算法对认证过程中生成的 PMK、所述 AP 生成的第一随机数、以及所述 STA 生成的第二随机数计算获取 PTK，或者对所述 PMK 和计数器值计算获取所述 PTK，并截取所述 PTK 获得所述 KCK；

所述 STA 采用所述 KCK 对所述第一消息验证码进行验证。

10. 根据权利要求 9 所述的方法，其特征在于，所述 STA 截取所述 PTK 获得所述 KCK 时，还包括：所述 STA 截取所述 PTK 获得 KEK 和 / 或 TK。

11. 根据权利要求 1 所述的方法，其特征在于，所述密钥验证完成消息还携带有以下至少之一：第一随机数、第二随机数。

12. 根据权利要求 1 至 11 中任一项所述的方法，其特征在于，

所述密钥验证消息还携带有以下至少之一：第一 EAP 相关消息和 / 或第一 DHCP 相关消息；

所述密钥验证完成消息还携带有以下至少之一：第二 EAP 相关消息和 / 或第二 DHCP 相关消息。

13. 根据权利要求 12 所述的方法，其特征在于，

所述第一 EAP 相关消息包括：EAP 成功消息；

所述第一 DHCP 相关消息包括：DHCP 提供消息、DHCP 确认消息；

所述第二 DHCP 相关消息包括：DHCP 发现消息、DHCP 请求消息。

14. 根据权利要求 12 所述的方法，其特征在于，所述 STA 向所述 AP 发送所述密钥验证完成消息包括以下之一：

当所述密钥验证完成消息包括所述第二 DHCP 相关消息时，所述 STA 采用所述 KEK 或所述 TK 加密所述第二 DHCP 相关消息后，将加密后的所述第二 DHCP 相关消息封装在密钥验证完成消息中向所述 AP 发送；

所述 STA 采用所述 KEK 或所述 TK 加密所述密钥验证完成消息后向所述 AP 发送。

15. 根据权利要求 1 所述的方法，其特征在于，在所述 STA 与所述 AP 进行认证之前，还包括：所述 AP 向所述 STA 发送网络发现消息，其中，所述网络发现消息包括：第三 EAP 相关消息。

16. 根据权利要求 1 所述的方法，其特征在于，在所述 STA 与所述 AP 进行认证时，还包括：

所述 STA 和 DHCP 服务器进行部分或者全部 DHCP 过程。

17. 根据权利要求 1 所述的方法，其特征在于，在所述 STA 与所述 AP 进行认证之前，还包括：所述 STA 向所述 AP 发送第一消息，其中，所述第一消息携带有以下至少之一：所述 STA 生成的所述第二随机数，计数器值、第四 EAP 相关消息、第三 DHCP 相关消息。

18. 根据权利要求 17 所述的方法，其特征在于，所述第一消息为以下之一：关联请求消息；802.1X 消息。

19. 根据权利要求 1 所述的方法，其特征在于，在所述 AP 对所述第二消息验证码验证成功后，还包括：所述 AP 向所述 STA 发送第二消息，其中，所述第二消息包括：第四 DHCP 相关消息。

20. 根据权利要求 19 所述的方法，其特征在于，所述第二消息为以下之一：关联响应消息；密钥信息帧 EAPOL-Key；802.1X 消息。

21. 根据权利要求 1 至 11、15 至 20 中任一项所述的方法，其特征在于，所述密钥验证消息和所述密钥验证完成消息为密钥信息帧 EAPOL-Key 消息。

22. 一种密钥验证装置，其特征在于，包括：

第一接收模块，用于接收来自于接入点 AP 的密钥验证消息，其中，所述密钥验证消息

携带有第一消息验证码；

第一验证模块，用于对所述第一消息验证码进行验证；

第一发送模块，用于在验证成功后，向所述 AP 发送携带有第二消息验证码的密钥验证完成消息，以使所述 AP 对所述第二消息验证码进行验证。

23. 根据权利要求 22 所述的装置，其特征在于，所述第一验证模块包括：

获取单元，用于按照所述预定的密钥衍生算法对认证过程中生成的成对主密钥 PMK、所述密钥验证装置生成的所述第二随机数和所述 AP 生成的第一随机数计算获取成对临时密钥 PTK，或者对所述 PMK 和计数器值计算获取所述 PTK，并截取所述 PTK 获得密钥确认密钥 KCK；

验证单元，用于采用所述 KCK 对所述第一消息验证码进行验证。

24. 一种密钥验证装置，其特征在于，包括：

第二发送模块，用于向工作站 STA 发送密钥验证消息，其中，所述密钥验证消息携带有第一消息验证码；

第二接收模块，用于在所述 STA 对所述第一消息验证码验证成功后，接收来自于所述 STA 的密钥验证完成消息，其中，所述密钥验证完成消息携带有第二消息验证码；

第二验证模块，用于对所述第二消息验证码进行验证。

25. 根据权利要求 24 所述的装置，其特征在于，还包括：

生成模块，用于生成第一随机数；

获取模块，用于按照预定的密钥衍生算法对认证过程中生成的成对主密钥 PMK、所述 STA 生成的第二随机数、以及所述生成模块生成的第一随机数计算获取成对临时密钥 PTK，或者对所述 PMK 和计数器值计算获取所述 PTK，并截取所述 PTK 获得密钥确认密钥 KCK；

计算模块，用于根据所述 KCK 计算获取所述第一消息验证码；

则所述第二发送模块，用于根据所述 KCK 计算获取所述第一消息验证码，并将所述第一消息验证码携带在所述密钥验证消息中发送。

26. 根据权利要求 25 所述的装置，其特征在于，还包括：

第三发送模块，用于将所述第一随机数发送至所述 STA。

密钥验证方法及装置

技术领域

[0001] 本发明涉及通信领域，具体而言，涉及一种密钥验证方法及装置。

背景技术

[0002] IEEE 802.11 是第一代无线局域网 (Wireless Local Area Networks，简称为 WLAN) 标准之一。该标准定义了物理层 (Physical Layer，简称为 PHY) 和媒体访问控制层 (Medium Access Control，简称为 MAC) 协议的规范，该规范允许无线局域网及无线设备制造商在一定范围内建立互操作网络设备。经过二十年的发展，IEEE 802.11 WLAN 标准工作组发展完善了一系列标准家族，其中具有较大影响力以及应用较为广泛的是 802.11a，802.11b，802.11g，802.11n，802.11ac 等标准。

[0003] 与 IEEE 802.11 相对应的 Wi-Fi 联盟是 1999 年成立的非营利性国际组织，用来检验以 IEEE802.11 规格为基础的 WLAN 产品的互操作性。Wi-Fi 联盟成员的目标是通过产品的互操作性来提高使用者的经验。

[0004] 如图 1 所示，一个 IEEE 802.11 网络包括 :工作站 (Station，简称为 STA)、无线接入点 (Access Point，AP)。其中，STA 是任何具备 IEEE 802.11 的 MAC 层和 PHY 层接口的设备，通常由一台 PC 机或笔记本计算机加上一块无线网卡构成，此外无线的终端还可以是非计算机终端上的能提供无线连接的嵌入式设备 (例如 802.11 手机)。AP 可以看成是一个无线的 Hub，用于提供 STA 和现有骨干网络之间的桥接，该骨干网络可以是有线的，也可以是无线的。一个 AP 和在其覆盖范围的一个或多个 STA 组成一个基本服务集 (Basic Service Set，简称为 BSS)。BSS 通过基本服务集标识 BSSID 来进行唯一标识，BSSID 即是 AP 的 MAC 地址。终端在一个 BSS 内可以互相通信。采用相同的服务集标识 SSID 的多个 BSS 形成的更大规模的虚拟 BSS，则定义为扩展服务集 (Extended Service Set，简称为 ESS)。终端在同一 ESS 内可以通信并且可以在下属的多个 BSS 间移动。在 ESS 内连接多个 BSS 的网络以及有线网络称为分布式系统 (Distribution System，简称为 DS)。DS 可以采用无线或有线技术，通常采用以太网技术。

[0005] 为了完成认证以及 IP 地址分配功能，WLAN 网络还包括认证服务器 (Authentication Server，简称为 AS) 和动态主机配置协议服务器 (Dynamic Host Configuration protocol Server，简称为 DHCP 服务器)，如图 2 所示。AS 是为 STA 提供认证服务的实体，仅有通过认证的 STA 才能被授权接入 802.11 网络。AS 也可以嵌入在 AP 中。DHCP 服务器则为 STA 分配 IP 地址。STA 通过该 WLAN 网络可以接入 Internet。

[0006] 如图 3 所示为 IEEE 802.11i 所引入的安全的密钥体系架构。其中，成对主密钥 (Pairwise Master Key，简称为 PMK) 是 STA 和 AS 在 EAP 认证过程中各自生成的密钥，长度为 256 位。成对临时密钥 (Pairwise Transient Key，简称为 PTK) 是 STA 和 AP 分别根据 PMK，以及 STA 生成的随机数 SNonce 和 AP 生成的随机数 ANonce，各自推导出的密钥。PTK 的低 128 位为密钥确认密钥 (Key Confirmation Key，KCK)，中间 128 位为密钥加密密钥 (Key Encryption Key，简称为 KEK)，剩下的高位 MSB 为临时密钥 (Temporal Key，简

称为 TK)。其中，KCK 用于为 4 次握手过程和组密钥握手过程中的 EAPOL-KEY(Extensible Authentication Protocol OVER LAN KEY) 消息提供数据源认证；KEK 用于为 4 次握手和组密钥握手的密钥信息帧 EAPOL-KEY 消息提供机密性保护；TK 用户保护 STA 和 AP 之间的数据报文的传输。

[0007] 此外，IEEE 802.11 还定义了组临时密钥 (Group Temporal Key，简称为 GTK)。GTK 是 AP 生成的一个随机数，在组密钥握手过程中，AP 将 GTK 用 KEK 加密后，传输给 STA。

[0008] 图 4 示出了 STA 初始接入 IEEE 802.11 网络时安全建立的流程图，具体步骤如下：

[0009] 步骤 1-2：通过 AP 广播信标 (Beacon) 消息，或者 STA 向 AP 主动发送探测请求 (Probe Request) 消息，AP 向 STA 响应探测响应 (Probe Response) 消息，告知 STA 关于 AP 的能力、参数和安全参数等信息。

[0010] 步骤 3-4：STA 和 AP 之间进行开放系统认证。该过程并没有建立真正的安全。

[0011] 步骤 5-6：STA 和 AP 之间进行关联。通过该步骤，STA 和 AP 之间建立了一个 IEEE 802.11 信道。

[0012] 步骤 7：STA 和 AS 之间进行 EAP 认证。在该过程完成后，STA 和 IEEE 802.11 网络完成了双向认证，并分别生成了 PMK。

[0013] 步骤 8：AS 通过远程用户拨号认证系统 (Remote Authentication Dial In User Service，简称为 RADIUS) 接入接受 (Access Accept) 消息，告知 AP 认证成功，并将 EAP 过程中生成的 PMK 发送给 AP。

[0014] 步骤 9：AP 向 STA 发送 802.1X 消息，其中封装有 EAP 成功 (EAP-Success) 消息。

[0015] 步骤 10：AP 和 STA 之间开始进行四次握手过程，验证双方生成的密钥。AP 生成随机数第一随机数 ANonce，并将其携带于密钥信息帧 (EAPOL-Key) 消息中，发送给 STA。

[0016] 步骤 11：STA 生成第二随机数 SNonce，并根据 SNonce 和接收到的 ANonce，以及 EAP 过程中生成的 PMK 生成 PTK，并截取 PTK 获取密钥确认密钥 KCK、KEK 和临时密钥 TK；STA 向 AP 发送 EAPOL-Key 消息，其中携带第二随机数 SNonce。该消息携带用 KCK 计算的消息验证码 (Message Integrity Code，简称为 MIC)。

[0017] 步骤 12：AP 根据接收到的 SNonce，和自己生成的 ANonce 以及 EAP 过程中生成的 PMK，按照和 STA 同样的算法，推导出 PTK，并截取 PTK 获取 KCK、KEK 和 TK。AP 用生成的 KCK 对接收到的 EAPOL-Key 消息进行验证。如果验证成功，AP 向 STA 发送 EAPOL-Key 消息，该消息携带随机数 ANonce，并携带用 KCK 计算的消息验证码 MIC。

[0018] 步骤 13：STA 对接收到的 EAPOL-Key 消息进行验证。如果验证成功，STA 安装根据截取 PTK 获得的临时密钥 TK，并向 AP 发送 EAPOL-Key 消息。该消息携带用 KCK 计算的消息验证码 MIC。至此，STA 和 AP 之间的 4 次握手过程结束。

[0019] 步骤 14：STA 和 AP 之间进行组密钥握手过程。AP 可选地生成第三随机数 GNonce，并随机选择组临时密钥 GTK，用 KEK 加密 GTK，将加密的 GTK 和 / 或随机数 GNonce 携带于 EAPOL-Key 消息中，发送给 STA。该消息同样也携带用 KCK 计算的消息验证码 MIC。

[0020] 步骤 15：STA 对接收到的 EAPOL-Key 消息进行验证，如果成功，用 KCK 解密获得 GTK；STA 向 AP 发送 EAPOL-Key 消息，携带用 KCK 计算的消息验证码 MIC。AP 对接收到的消息进行验证。至此，STA 完成了初始连接的建立，可以进行数据包的收发了。

[0021] 步骤 16：STA 和 WLAN 网络会进行 DHCP 过程，获取 IP 地址。

[0022] 移动用户不断地进入或离开一个 ESS 的覆盖区域。每次当移动设备进入一个 ESS 时，移动设备必须进行如图 4 所示的 STA 初始入网建立初始链路的过程。而在该初始链路建立的过程中，安全的步骤较多，从而导致初始入网的时延较长。当大量用户同时在较短时间内需要接入 WLAN 网络时（例如在地铁站，大量用户下了地铁后需要连接 WLAN 网络获取相关的路线信息），入网时延较长的问题会更严重。

[0023] 针对相关技术中初始链路建立的过程中，安全验证的步骤较多，导致入网时延较长的问题，目前尚未提出有效的解决方案。

发明内容

[0024] 针对相关技术中初始链路建立的过程中，安全验证的步骤较多，导致入网时延较长的问题，本发明提供了一种密钥验证方法及装置，以至少解决该问题。

[0025] 根据本发明的一个方面，提供了一种密钥验证方法，包括：STA 接收来自于 AP 的密钥验证消息，其中，密钥验证消息携带有第一消息验证码；STA 对第一消息验证码进行验证；在验证成功后，STA 向 AP 发送携带有第二消息验证码的密钥验证完成消息，以使 AP 对第二消息验证码进行验证。

[0026] 上述 STA 接收来自于 AP 的密钥验证消息之前，还包括以下之一：STA 和 AP 认证成功；STA 和 AP 开始进行认证。

[0027] 上述密钥验证消息还携带有以下至少之一：第一随机数、第二随机数、计数器值、关联标识。

[0028] 在 STA 接收来自于 AP 的密钥验证消息之前，还包括：AP 生成第一随机数或计数器值；AP 按照预定的密钥衍生算法对认证过程中生成的成对主密钥 PMK、STA 生成的第二随机数以及 AP 生成的第一随机数计算获取成对临时密钥 PTK，或者对 PMK 和计数器值计算获取 PTK，并截取 PTK 获得密钥确认密钥 KCK；AP 根据 KCK 计算获取第一消息验证码，并将第一消息验证码携带在密钥验证消息中发送。

[0029] 上述 AP 截取 PTK 获得 KCK 时，还包括：AP 截取 PTK 获得密钥加密密钥 KEK 和 / 或临时密钥 TK。

[0030] 在将第一消息验证码携带在密钥验证消息中发送之前，还包括：AP 将第一随机数发送至 STA；则 AP 将第一消息验证码携带在密钥验证消息中发送包括：AP 采用 KEK 或 TK 对密钥验证消息进行加密后发送。

[0031] 在上述 STA 接收来自于 AP 的密钥验证消息之前，还包括：AP 随机选取组临时密钥 GTK，采用 KEK 加密 GTK；AP 将加密的 GTK 携带在密钥验证消息中向 STA 发送。

[0032] 在 AP 将加密的 GTK 和 / 或第三随机数携带在密钥验证消息中向 STA 发送之后，还包括：STA 接收来自于 AP 的密钥验证消息；STA 采用 KEK 解密密钥验证消息获得 GTK。

[0033] 上述 STA 对第一消息验证码进行验证包括：STA 按照预定的密钥衍生算法对认证过程中生成的 PMK、AP 生成的第一随机数、以及 STA 生成的第二随机数计算获取 PTK，或者对 PMK 和计数器值计算获取 PTK，并截取 PTK 获得 KCK；STA 采用 KCK 对第一消息验证码进行验证。

[0034] 上述 STA 截取 PTK 获得 KCK 时，还包括：STA 截取 PTK 获得 KEK 和 / 或 TK。

[0035] 上述密钥验证完成消息还携带有以下至少之一：第一随机数、第二随机数。

[0036] 上述密钥验证消息还携带有以下至少之一：第一 EAP 相关消息和 / 或第一 DHCP 相关消息；上述密钥验证完成消息还携带有以下至少之一：第二 EAP 相关消息和 / 或第二 DHCP 相关消息。

[0037] 第一 EAP 相关消息包括：EAP 成功消息；第一 DHCP 相关消息包括：DHCP 提供消息、DHCP 确认消息；第二 DHCP 相关消息包括：DHCP 发现消息、DHCP 请求消息。

[0038] 上述 STA 向 AP 发送密钥验证完成消息包括以下之一：当密钥验证完成消息包括第二 DHCP 相关消息时，STA 采用 KEK 或 TK 加密第二 DHCP 相关消息后，将加密后的第二 DHCP 相关消息封装在密钥验证完成消息中向 AP 发送；STA 采用 KEK 或 TK 加密密钥验证完成消息后向 AP 发送。

[0039] 在 STA 与 AP 进行认证之前，还包括：AP 向 STA 发送网络发现消息，其中，网络发现消息包括：第三 EAP 相关消息。

[0040] 在 STA 与 AP 进行认证时，还包括：STA 和 DHCP 服务器进行部分或者全部 DHCP 过程。

[0041] 在 STA 与 AP 进行认证之前，还包括：STA 向 AP 发送第一消息，其中，第一消息携带有以下至少之一：STA 生成的第二随机数，计数器值、第四 EAP 相关消息、第三 DHCP 相关消息。

[0042] 上述第一消息为以下之一：关联请求消息；802.1X 消息。

[0043] 在 AP 对第二消息验证码验证成功后，还包括：AP 向 STA 发送第二消息，其中，第二消息包括：第四 DHCP 相关消息。

[0044] 上述第二消息为以下之一：关联响应消息；密钥信息帧 EAPOL-Key；802.1X 消息。

[0045] 上述密钥验证消息和密钥验证完成消息为密钥信息帧 EAPOL-Key 消息。

[0046] 根据本发明的另一方面，提供了一种密钥验证装置，包括：第一接收模块，用于接收来自于 AP 的密钥验证消息，其中，密钥验证消息携带有第一消息验证码；第一验证模块，用于对第一消息验证码进行验证；第一发送模块，用于在验证成功后，向 AP 发送携带有第二消息验证码的密钥验证完成消息，以使 AP 对第二消息验证码进行验证。

[0047] 上述第一验证模块包括：获取单元，用于按照预定的密钥衍生算法对认证过程中生成的成对主密钥 PMK、密钥验证装置生成的第二随机数和 AP 生成的第一随机数计算获取成对临时密钥 PTK，或者对 PMK 和计数器值计算获取 PTK，并截取 PTK 获得密钥确认密钥 KCK；验证单元，用于采用 KCK 对第一消息验证码进行验证。

[0048] 根据本发明的又一方面，提供了一种密钥验证装置，包括：第二发送模块，用于向 STA 发送密钥验证消息，其中，密钥验证消息携带有第一消息验证码；第二接收模块，用于在 STA 对第一消息验证码验证成功后，接收来自于 STA 的密钥验证完成消息，其中，密钥验证完成消息携带有第二消息验证码；第二验证模块，用于对第二消息验证码进行验证。

[0049] 上述装置还包括：生成模块，用于生成第一随机数；获取模块，用于按照预定的密钥衍生算法对认证过程中生成的成对主密钥 PMK、STA 生成的第二随机数、以及生成模块生成的第一随机数计算获取成对临时密钥 PTK，或者对 PMK 和计数器值计算获取 PTK，并截取 PTK 获得密钥确认密钥 KCK；计算模块，用于根据 KCK 计算获取第一消息验证码；则第二发送模块，用于根据 KCK 计算获取第一消息验证码，并将第一消息验证码携带在密钥验证消息中发送。

[0050] 上述装置还包括：第三发送模块，用于将第一随机数发送至 STA。

[0051] 通过本发明，在 STA 与 AP 认证成功后，通过 STA 验证由 AP 发送的带有第一消息验证码的密钥验证消息，并在验证成功后，向 AP 发送带有第二消息验证码的密钥验证完成消息，使 AP 对第二消息验证码进行验证，解决了相关技术中初始链路建立的过程中，安全验证的步骤较多，导致入网时延较长的问题，进而减少了现有技术中安全验证的繁琐步骤，且达到了缩短了入网时延的效果，从整体上提升了系统的性能，同时也提高了用户体验。

附图说明

[0052] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0053] 图 1 是根据相关技术的一种 IEEE 802.11 网络结构示意图；

[0054] 图 2 是根据一种 WLAN 网络的结构示意图；

[0055] 图 3 是根据 IEEE 802.11i 引入的密钥架构的结构示意图；

[0056] 图 4 是根据目前 IEEE 802.11 定义的终端建立初始链路的流程图；

[0057] 图 5 是根据本发明实施例的密钥验证方法的流程图；

[0058] 图 6 是根据本发明优选实施例一的密钥验证方法的流程图；

[0059] 图 7 是根据本发明优选实施例二的密钥验证方法的流程图；

[0060] 图 8 是根据本发明实施例的一种密钥验证装置的结构框图；

[0061] 图 9 是根据本发明优选实施例的一种密钥验证装置的结构框图；

[0062] 图 10 是根据本发明实施例的另一种密钥验证装置的结构框图；

[0063] 图 11 是根据本发明优选实施例的另一种密钥验证装置的结构框图。

具体实施方式

[0064] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0065] 如图 5 所示，针对相关技术中初始链路建立的过程中，安全验证的步骤较多，且入网时延较长的问题，本实施例提供了一种密钥验证方法，包括以下步骤：

[0066] 步骤 S502，STA 接收来自于 AP 的密钥验证消息，其中，密钥验证消息携带有第一消息验证码；

[0067] 步骤 S504，STA 对第一消息验证码进行验证；

[0068] 步骤 S506，在验证成功后，STA 向 AP 发送携带有第二消息验证码的密钥验证完成消息，以使 AP 对第二消息验证码进行验证。

[0069] 在本实施例中，由于相关技术中初始链路建立的过程中，安全验证的步骤较多，导致入网时延较长，采用图 5 所示的通过 STA 验证由 AP 发送的带有第一消息验证码的密钥验证消息，并在验证成功后，向 AP 发送带有第二消息验证码的密钥验证完成消息，使 AP 对第二消息验证码进行验证的方法，从而可以减少现有技术中安全验证的繁琐步骤，达到了缩短了入网时延的效果，从整体上提升了系统的性能，同时也提高了用户体验。

[0070] 优选地，STA 接收来自于 AP 的密钥验证消息之前，还包括以下之一的处理：

[0071] (1)STA 和 AP 认证成功；

[0072] (2)STA 和 AP 开始进行认证。

[0073] 即步骤 S502 的触发条件包括 :STA 与 AP 认证成功,或者 STA 与 AP 开始进行相互认证。

[0074] 优选地,上述密钥验证消息还可以携带有以下至少之一 :第一随机数 (如 ANonce)、第二随机数 (如 SNonce)、关联标识 (AID)。

[0075] 在步骤 S502 中,在 STA 接收来自于 AP 的密钥验证消息之前,还可以包括以下处理 :

[0076] (1)AP 生成第一随机数或者计数器值 ;

[0077] (2)AP 按照预定的密钥衍生算法对认证过程中生成的 PMK、STA 生成的第二随机数和 AP 生成的第一随机数计算获取 PTK,并截取 PTK 获得密钥确认密钥 KCK ;或者,AP 按照预定的密钥衍生算法对认证过程中生成的成对主密钥 PMK、计数器值 COUNT 计算获取成对临时密钥 PTK,并截取 PTK 获得密钥确认密钥 KCK ;

[0078] 其中,如果采用计数器值的话,STA 和 AP 各自维护一个计数器。初始入网时或每次认证成功后计数器进行初始化,在每一次推导 PTK 之前或之后 STA 和 AP 各自递增自己维护的计数器。STA 和 AP 各自维护的计数器值需要进行同步。

[0079] (3)AP 根据 KCK 计算获取第一消息验证码,并将第一消息验证码携带在密钥验证消息中发送。

[0080] 优选地,当 AP 截取 PTK 获得 KCK 时,还可以获得以下之一 :密钥加密密钥 (KEK) ;临时密钥 (TK) ;临时密钥 (TK) 和密钥加密密钥 (KEK) 的组合。

[0081] 在步骤 S502 中,将第一消息验证码携带在密钥验证消息中发送之前,还可以包括以下处理 :AP 将第一随机数发送至 STA。

[0082] 则当 AP 在发送携带有第一消息验证码的密钥验证消息时,还可以采用上述 KEK 或 TK 对密钥验证消息或密钥验证消息的部分信息元进行加密后发送。

[0083] 在优选实施过程中,在 STA 接收来自于 AP 的密钥验证消息之前,还可以包括以下处理 :

[0084] (1)AP 随机选取组临时密钥 GTK,采用 KEK 加密 GTK ;

[0085] (2)AP 将加密的 GTK 携带在密钥验证消息中向 STA 发送。

[0086] 可选地,在 AP 将 GTK 和 / 或第三随机数携带在密钥验证消息中向 STA 发送之前,还可以包括以下处理 :AP 生成第三随机数。

[0087] 其中,在 AP 将加密的 GTK 和 / 或第三随机数携带在密钥验证消息中向 STA 发送之后,还可以包括以下处理 :STA 接收来自于 AP 的密钥验证消息,之后采用 KEK 解密上述密钥验证消息获得 GTK。

[0088] 优选地,上述步骤 S504 中, STA 对第一消息验证码进行验证可以进一步包括以下处理 :STA 按照预定的密钥衍生算法对认证过程中生成的 PMK、STA 生成的第二随机数和 AP 生成的第一随机数计算获取 PTK,并截取 PTK 获得 KCK ;STA 采用 KCK 对第一消息验证码进行验证 ;或者,STA 按照预定的密钥衍生算法对认证过程中生成的 PMK、计数器值 COUNT 计算获取上述 PTK,并截取上述 PTK 获得 KCK ;

[0089] 其中,上述密钥验证完成消息还可以携带有以下至少之一 :第一随机数、第二随机数、计数器值 COUNT。

[0090] 优选地，当 STA 截取 PTK 获得 KCK 时，还可以包括 ：STA 截取 PTK 获得 KEK 和 / 或 TK。

[0091] 优选地，密钥验证消息还可以携带有以下至少之一 ：第一 EAP 相关消息和 / 或第一 DHCP 相关消息。

[0092] 优选地，密钥验证完成消息还可以携带有以下至少之一 ：第二 EAP 相关消息和 / 或第二 DHCP 相关消息。

[0093] 在具体实施过程中，如果的密钥验证消息携带有第一 EAP 相关消息和 / 或第一 DHCP 相关消息，密钥验证完成消息携带有第二 EAP 相关消息和 / 或第二 DHCP 相关消息，则 STA 在成功完成对接收到的消息的验证后，将封装的第一 EAP 相关消息和 / 或第一 DHCP 相关消息发送给上层处理，若还存在后续消息，则继续接收上层返回的相应后续消息。

[0094] 例如，上述第一 EAP 相关消息可以为 ：EAP-Success 消息 ；上述第一 DHCP 相关消息可以为 ：DHCP 提供消息、DHCP 确认消息 ；上述第二 DHCP 相关消息可以为 ：DHCP 发现消息、DHCP 请求消息。

[0095] 优选地，上述步骤 S506 中，STA 向 AP 发送密钥验证完成消息可以进一步包括以下之一的处理 ：

[0096] 处理一 ：当密钥验证完成消息包括 DHCP 相关消息时，STA 采用 KEK 或 TK 加密 DHCP 相关消息后，将加密后的 DHCP 相关消息封装在密钥验证完成消息中向 AP 发送 ；

[0097] 处理二 ：STA 采用 KEK 或 TK 加密密钥验证完成消息后向 AP 发送。

[0098] 优选地，在 STA 与 AP 进行认证之前，还可以包括以下处理 ：AP 向 STA 发送网络发现消息，其中，网络发现消息包括 ：第三 EAP 相关消息。

[0099] 例如，上述第二 EAP 相关消息可以为 EAP-Request/Identity 消息。上述网络发现消息可以为 ：Beacon 消息或者 Probe Response 消息。

[0100] 优选地，在 STA 与 AP 进行认证之前，还可以包括以下处理 ：STA 向 AP 发送第一消息，其中，第一消息携带有以下至少之一 ：STA 生成的第二随机数、计数器值 COUNT、第四 EAP 相关消息、第三 DHCP 相关消息。

[0101] 其中，上述第一消息可以为以下之一 ：关联请求消息 ；802.1X 消息。

[0102] 例如，上述第四 EAP 相关消息可以为 ：EAP-Response/Identity ；上述第三 DHCP 相关消息可以为 ：DHCP Discover 消息。

[0103] 在 AP 对第二消息验证码验证成功后，还可以包括以下处理 ：AP 向 STA 发送第二消息，其中，第二消息包括 ：第四 DHCP 相关消息。

[0104] 其中，上述第二消息可以为以下之一 ：关联响应消息 ；密钥信息帧 (EAPOL-Key) ；802.1X 消息。

[0105] 例如，上述第四 DHCP 相关消息可以为 ：DHCP Ack 消息。

[0106] 需要注意的是，上述第一 EAP 相关消息、第二 EAP 相关消息、第三 EAP 相关消息、第四 EAP 相关消息、第一 DHCP 相关消息、第二 DHCP 相关消息、第三 DHCP 相关消息、以及第四 DHCP 相关消息均为上层消息。

[0107] 优选地，在 STA 与 AP 进行认证时，包括 ：STA 和 DHCP 服务器进行部分或者全部 DHCP 过程。

[0108] 通过上述并行处理，可以进一步减少处理时间，降低用户接入网络的时延。

[0109] 需要注意的是，上述密钥验证方法可以应用于 IEEE 802.11 网络中，当然，还可以应用于其他网络中。对于 IEEE 802.11 网络而言，上述密钥验证消息和密钥验证完成消息可以为 EAPOL-Key 消息。

[0110] 以下结合图 6 和图 7 的两个示例进一步描述上述优选实施方式。

[0111] 优选实施例一

[0112] 图 6 是根据本发明优选实施例一的密钥验证方法的流程图。如图 6 所示，该密钥验证方法主要包括以下处理：

[0113] 步骤 S602，STA 和 AP 之间进行交互，STA 获知 AP 的安全能力。该过程可以通过 AP 广播的信标消息或者 STA 和 AP 之间进行的探测请求 / 探测响应消息交互进行；或者通过 AP 广播的信标消息或者 STA 和 AP 之间进行的探测请求 / 探测响应消息，以及 STA 与 AP 之间进行的关联请求 / 关联响应消息交互进行。

[0114] 优选地，在该过程中，STA 可以将生成的随机数 SNonce 发送给 AP。

[0115] 步骤 S604，STA 和 AP 之间进行认证。该认证过程可以基于 EAP 的双向认证。当成功完成认证后，STA 和 AP 各自生成密钥 PMK。

[0116] 优选地，在该过程中，STA 可以将生成的随机数 SNonce 或计数器值 COUNT 发送给 AP。其中，如果采用计数器值的话，STA 和 AP 各自维护一个计数器。初始入网时或每次认证成功后计数器进行初始化，在每一次密钥验证流程之前 STA 和 AP 各自递增自己维护的计数器。

[0117] 优选地，在进行 EAP 的过程中，STA、AP 和 DHCP 服务器可以同时进行部分或者全部 DHCP 过程。

[0118] 步骤 S606，AS 向 AP 发送 EAP-Success 消息，该消息封装于 RADIUS 消息中，携带密钥 PMK。

[0119] 步骤 S608，密钥验证。若 AP 还未生成随机数 ANonce，则 AP 生成随机数 ANonce；AP 根据接收到的 PMK，以及 SNonce 和 ANonce，按照 IEEE 802.11 协议规定的密钥衍生算法，推导密钥 PTK；或者，AP 根据接收到的 PMK，以及 COUNT 值，按照 IEEE 802.11 协议规定的密钥衍生算法，推导密钥 PTK。AP 依据推导出的 PTK，截取获得 KCK 和 / 或 KEK 和 / 或 TK；AP 向 STA 发送密钥验证消息。该消息携带参数：随机数 ANonce，和 / 或随机数 SNonce，和 / 或 AP 为该 STA 分配的关联标识 AID，用 KCK 计算得到的该消息的消息验证码 MIC。

[0120] 可选地，若 STA 和 AP 使用计数器值 COUNT 生成密钥 PTK，则 AP 收到 STA 发送的 COUNT 值后，与自己维护的计数器值进行比较。若接收到的 COUNT 值大于自己维护的计数器值，则令自己维护的计数器值等于接收到的 COUNT 值，并使用该 COUNT 值推导 PMK；若接收到的 COUNT 值等于自己维护的计数器值，则使用该 COUNT 值推导 PMK；接收到的 COUNT 值小于自己维护的计数器值，则判定为无效消息，进入异常处理流程。

[0121] 优选地，该密钥验证消息携带封装的上层消息：EAP-Success 消息，和 / 或 DHCP 相关消息。DHCP 相关消息可以为：DHCP Offer 消息，或 DHPC Ack 消息。

[0122] 优选地，AP 将 DHCP 相关消息用 KEK 加密后，封装于密钥验证消息中。

[0123] 优选地，若 AP 在前面的步骤中，已经将 ANonce 发送给 STA，则该步骤中 AP 可以对密钥验证消息进行加密后再发送。加密使用的密钥可以为 KEK，或 TK。

[0124] 优选地，AP 可以和 STA 同时进行组密钥握手。AP 可选生成随机数 GNonce，并随机

选择组临时密钥 GTK，用密钥加密密钥 KEK 加密 GTK，将加密的 GTK 和 / 或随机数 GNonce 携带于密钥验证消息中，发送给 STA。其中，该密钥验证消息可以为 :EAPOL-Key 消息。

[0125] 步骤 S610，密钥验证完成。STA 根据 EAP 过程中生成的密钥 PMK，以及接收到的随机数 ANonce，和自己生成的随机数 SNonce，按照和 AP 同样的密钥衍生算法，推导出密钥 PTK，并截取 PTK 获取 KCK 和 / 或 KEK 和 / 或 TK ；或者，STA 根据接收到的 PMK，以及 COUNT 值，按照 IEEE 802.11 协议规定的密钥衍生算法，推导密钥 PTK。STA 根据推导出的 KCK 对接收到的密钥验证消息的 MIC 进行验证 ；若验证通过，STA 向 AP 发送密钥验证完成消息，其中携带随机数 SNonce，和 / 或随机数 ANonce。该消息携带用 KCK 计算的消息验证码 MIC。

[0126] 优选地，若该密钥验证完成消息携带有上层消息如 DHCP 相关消息，则 STA 在成功完成对接收到的消息的验证后，将封装的上层消息发送给上层处理，接收上层返回的相应后续消息。DHCP 相关消息可以为 :DHCP Discover 消息或 DHCP Offer 消息。

[0127] 优选地，STA 将 DHCP 相关消息用 KEK 加密后，封装于密钥验证完成消息中 ；或 STA 将整个密钥验证完成消息进行加密后发送给 AP，加密使用的密钥可以为 KEK，或 TK。

[0128] 若接收到的密钥验证消息中包括加密的组密钥 GTK，STA 用 KEK 解密获得 GTK。该密钥验证完成消息可以为 :EAPOL-Key 消息。

[0129] 步骤 S612，STA 和 AP 之间进行余下的 DHCP 或全部 DHCP 过程。如果在步骤 S602 中，还未成功完成关联过程，则该 DHCP 消息可以承载在关联过程的消息中发送。如果在步骤 S602 中，已经完成了关联过程，则此处的 DHCP 过程可以承载于密钥信息帧 (EAPOL-KEY) 消息中发送，或者在用户数据报文中发送。

[0130] 至此，STA 和 AP 之间成功完成初始链路的建立，可以安全地收发数据报文了。

[0131] 优选实施例二

[0132] 如图 7 所示，该实施例示出了一种快速建立 WLAN 初始链路的方法，具体包括步骤 S702 至 S720。

[0133] 步骤 S702，AP 与 STA 进行安全能力发现流程，在该流程中，AP 告知 STA 关于 AP 的能力、参数和安全参数等信息。可选地，该过程包括关联请求 / 关联响应消息交互。

[0134] 优选地，在该过程的下行链路消息中，封装有 EAP-Request/Identity 消息。可选地，该下行链路消息还可以携带参数 :AP 生成的随机数 ANonce（即上述第一随机数）。此处的下行链路消息可以为 :信标消息，或探测响应消息，或关联响应消息。

[0135] 步骤 S704，STA 向 AP 发送第一消息，该消息封装有 EAP-Response/Identity 消息。

[0136] 优选地，STA 生成随机数 SNonce（即上述第二随机数），并在第一消息中携带该随机数 SNonce。

[0137] 优选地，该第一消息中携带封装的 DHCP Discover 消息。

[0138] 此处的第一消息可以为 :关联请求消息，或 802.1X 消息。

[0139] 步骤 S706，AP 将 EAP-Response/Identity 消息封装于 RADIUS 消息中，发送给 AS。

[0140] 步骤 S708，可选地，AP 将第一消息中封装的 DHCP Discover 消息转发给 DHCP 服务器 ；DHCP 服务器向 AP 发送 DHCP Offer 消息，携带网络的配置参数和 IP 地址信息。步骤 S706、步骤 S708、步骤 S710、步骤 S712 没有严格的时间顺序。

[0141] 步骤 S710，STA 和 AS 之间进行基于 EAP 的认证。在双方成功完成认证后，STA 和 AS 分别生成密钥 PMK。

[0142] 步骤 S712，AS 向 AP 发送 EAP-Success 消息，该消息封装于 RADIUS 消息中，携带密钥 PMK。

[0143] 步骤 S714，若 AP 还未生成随机数 ANonce，则 AP 生成随机数 ANonce ；AP 根据接收到的 PMK，以及 SNonce 和 ANonce，按照 IEEE 802.11 协议规定的密钥衍生算法，推导密钥 PTK ；或者，AP 根据接收到的 PMK，以及 COUNT 值，按照 IEEE 802.11 协议规定的密钥衍生算法，推导密钥 PTK。AP 依据推导出的 PTK，截取获得 KCK 和 / 或 KEK 和 / 或 TK ；AP 向 STA 发送密钥验证消息，该消息携带参数 ：随机数 ANonce，和 / 或随机数 SNonce，或计数器值 COUNT，和 / 或 AP 为该 STA 分配的关联标识 AID，用 KCK 计算得到的该消息的消息验证码 MIC。

[0144] 其中，如果采用计数器值的话，STA 和 AP 各自维护一个计数器。初始入网时或每次认证成功后计数器进行初始化，在每一次密钥验证流程之前 STA 和 AP 各自递增自己维护的计数器。STA 和 AP 各自维护的计数器值需要进行同步。

[0145] 优选地，该密钥验证消息携带封装的上层消息 ：EAP-Success 消息，和 / 或 DHCP Offer 消息。

[0146] 优选地，AP 将 DHCP Offer 消息用 KEK 加密后，封装于密钥验证消息中。

[0147] 可选地，若 AP 在前面的步骤中，已经将 ANonce 发送给 STA，则该步骤中 AP 可以对密钥验证消息进行加密后再发送。加密使用的密钥可以为 KEK，或 TK。

[0148] 优选地，AP 可以和 STA 同时进行组密钥握手。AP 可选地生成随机数 GNonce，并随机选择组临时密钥 GTK(Group Temporal Key)，用密钥加密密钥 KEK(Key Encryption Key) 加密 GTK，将加密的 GTK 和 / 或随机数 GNonce 携带于密钥验证消息中，发送给 STA。

[0149] 该密钥验证消息可以为 ：EAPOL-Key 消息。

[0150] 步骤 S716，STA 根据 EAP 过程中生成的密钥 PMK，以及接收到的随机数 ANonce，和自己生成的随机数 SNonce，按照和 AP 同样的密钥衍生算法，推导出密钥 PTK，并截取 PTK 获取 KCK 和 / 或 KEK 和 / 或 TK ；或者，STA 根据 EAP 过程中生成的密钥 PMK，以及 COUNT 值，按照和 AP 同样的密钥衍生算法，推导出密钥 PTK，并截取 PTK 获取 KCK 和 / 或 KEK 和 / 或 TK ；STA 根据推导出的 KCK 对接收到的密钥验证消息的 MIC 进行验证 ；若验证通过，STA 向 AP 发送密钥验证完成消息，其中携带随机数 SNonce，和 / 或随机数 ANonce。该消息携带用 KCK 计算的消息验证码 MIC(Message Integrity Code)。

[0151] 优选地，若该密钥验证消息携带有上层消息 EAP-Success 消息和 / 或 DHCP Offer 消息，则 STA 在成功完成对接收到的消息的验证后，将封装的上层消息发送给上层处理，接收上层返回的相应后续消息。

[0152] 优选地，该密钥验证完成消息携带封装的上层消息 ：DHCP Request 消息。

[0153] 优选地，AP 将 DHCP Request 消息用 KEK 加密后，封装于密钥验证完成消息中 ；或 STA 将整个密钥验证完成消息进行加密后发送给 AP，加密使用的密钥可以为 KEK，或 TK。

[0154] 若接收到的密钥验证消息中包括加密的组密钥 GTK，STA 用 KEK 解密获得 GTK。

[0155] 该密钥验证完成消息可以为 ：EAPOL-Key 消息。

[0156] 步骤 S718，AP 用生成的 KCK 对接收到的密钥验证完成消息进行验证。如果验证成功，若密钥验证完成消息中携带上层消息 DHCP Request，可选地，AP 向 DHCP 服务器转发 DHCPRequest 消息，DHCP 服务器向 AP 返回 DHCP Ack 消息。

[0157] 步骤 S720，AP 向 STA 发送第二消息。可选地，该消息携带参数 ：AP 为该 STA 分配

的关联标识 AID，和 / 或上层消息 DHCP Ack 消息。

[0158] 该第二消息可以为：关联响应消息，或 802.1X 消息，或密钥信息帧 EAPOL-Key 消息。

[0159] 需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0160] 图 8 是根据本发明实施例的一种密钥验证装置的结构框图。如图 8 所示，该装置包括：第一接收模块 102，用于在 STA 与接入点 AP 认证时或认证成功后，接收来自于 AP 的密钥验证消息，其中，密钥验证消息携带有第一消息验证码；第一验证模块 104，用于对第一消息验证码进行验证；第一发送模块 106，用于在验证成功后，向 AP 发送携带有第二消息验证码的密钥验证完成消息，以使 AP 对第二消息验证码进行验证。

[0161] 优选地，上述密钥验证装置可以设置在 STA 中。

[0162] 其中，上述密钥验证消息还可以携带有以下至少之一：第一随机数、第二随机数、计数器值、关联标识。

[0163] 其中，上述密钥验证完成消息还携带有以下至少之一：第一随机数、第二随机数。

[0164] 优选地，如图 9 所示，第一验证模块 104 可以包括：获取单元 1042，用于按照预定的密钥衍生算法对认证过程中生成的 PMK、AP 生成的第一随机数和 STA 生成的第二随机数计算获取成对临时密钥 PTK，或者对 PMK 和计数器值计算获取 PTK，并截取 PTK 获得 KCK；验证单元 1044，用于采用 KCK 对第一消息验证码进行验证。获取单元 1042 和验证单元 1044 依次连接或耦合。

[0165] 优选地，获取单元 1042 截取 PTK 获得 KCK 时，还可以截取 PTK 获得 KEK 和 / 或 TK。

[0166] 上述密钥验证消息和密钥验证完成消息均可以携带上层消息。密钥验证消息携带的上层消息可以为第一 EAP 相关消息和第一 DHCP 相关消息，例如，第一 EAP 相关消息为 EAP 成功 EAP-Success 消息；第一 DHCP 相关消息为：DHCP 提供消息、DHCP 确认消息；密钥验证完成消息携带的上层消息可以为第二 EAP 相关消息和第二 DHCP 相关消息，例如，第二第二 DHCP 相关消息可以为 DHCP 请求消息或 DHCP 发现消息。

[0167] 优选地，第一发送模块 106 向 AP 发送密钥验证完成消息包括以下之一：

[0168] 当密钥验证完成消息包括第二 DHCP 相关消息时，第一发送模块 106 采用 KEK 或 TK 加密第二 DHCP 相关消息后，将加密后的第二 DHCP 相关消息封装在密钥验证完成消息中向 AP 发送；第一发送模块 106 采用 KEK 或 TK 加密密钥验证完成消息后向 AP 发送。

[0169] 需要说明的是，上述装置中的各模块，各单元相互结合的优选工作方式具体可以参见图 5 至图 7 的描述，此处不再赘述。

[0170] 图 10 是根据本发明实施例的另一种密钥验证装置的结构框图。如图 10 所示，该密钥验证装置包括：第二发送模块 202，用于向工作站 STA 发送密钥验证消息，其中，密钥验证消息携带有第一消息验证码；第二接收模块 204，用于在 STA 对第一消息验证码验证成功后，接收来自于 STA 的密钥验证完成消息，其中，密钥验证完成消息携带有第二消息验证码；第二验证模块 206，用于对第二消息验证码进行验证。

[0171] 优选地，上述密钥验证装置可以设置在 AP 中。

[0172] 其中，上述密钥验证消息还可以携带有以下至少之一：第一随机数、第二随机数、

计数器值、关联标识。

[0173] 其中，密钥验证完成消息还携带有以下至少之一：第一随机数、第二随机数。

[0174] 优选地，如图 11 所示，该密钥验证装置还可以包括：生成模块 208，用于生成第一随机数；获取模块 210，用于按照预定的密钥衍生算法对认证过程中生成的 PMK、STA10 生成的第二随机数和生成模块 208 生成的第一随机数计算获取 PTK，或者对 PMK 和计数器值计算获取 PTK，并截取该 PTK 获得密钥确认密钥 KCK；计算模块 212，用于根据 KCK 计算获取第一消息验证码；则第二发送模块 202，用于根据 KCK 计算获取第一消息验证码，并将该第一消息验证码携带在密钥验证消息中发送。其中，生成模块 208、获取模块 210、计算模块 212 和第二发送模块 202 依次连接或耦合。

[0175] 在优选实施过程中，获取模块 210 在截取该 PTK 获得 KCK 的同时，还可以获得 KEK 和 / 或 TK。

[0176] 优选地，如图 11 所示，上述密钥验证装置还包括：第三发送模块 214，用于将第一随机数发送至 STA。

[0177] 优选地，上述密钥验证装置在 STA 接收来自于上述密钥验证装置的密钥验证消息之前，还可以可选地生成第三随机数；随机选取 GTK，采用 KEK 加密 GTK；将加密的 GTK 和 / 或第三随机数携带在密钥验证消息中向 STA 发送。

[0178] 优选地，上述密钥验证装置将加密的 GTK 和 / 或第三随机数携带在密钥验证消息中向 STA 发送之后；STA 接收来自于上述密钥验证装置的密钥验证消息；STA 采用 KEK 解密密钥验证消息获得 GTK。

[0179] 在 STA 与上述密钥验证装置进行认证之前，上述密钥验证装置向 STA 发送网络发现消息，其中，网络发现消息包括：第三 EAP 相关消息。

[0180] STA 在与网络进行认证时，可以和 DHCP 服务器进行部分或者全部 DHCP 过程。

[0181] STA 向上述密钥验证装置发送第一消息，其中，第一消息携带有以下至少之一：STA 生成的第二随机数，计数器值。

[0182] 其中，第一消息还可以携带有：上层消息。包括：第四 EAP 相关消息和 / 或第三 DHCP 相关消息。

[0183] 例如，第一消息可以为以下之一：关联请求消息；802.1X 消息。

[0184] 上述密钥验证装置对第二消息验证码验证成功后，向 STA 发送第二消息，其中，第二消息包括：第四 DHCP 相关消息。

[0185] 例如，第二消息为以下之一：关联响应消息；密钥信息帧 EAPOL-Key；802.1X 消息。

[0186] 需要注意的是，上述密钥验证消息和密钥验证完成消息可以为 EAPOL-Key 消息。

[0187] 需要说明的是，上述装置中的各模块，各单元相互结合的优选工作方式具体可以参见图 5 至图 7 的描述，此处不再赘述。

[0188] 综上所述，借助本发明提供的上述实施例，可以大大加快终端建立初始链路的速度，减少终端初始接入 WLAN 网络的时延。特别是对于大量用户需要在极短时间内接入 WLAN 网络的场景，成功的减少了现有技术中安全验证的繁琐步骤，且缩短了入网时延的效果，从整体上提升了系统的性能，同时也提高了用户体验。

[0189] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成

的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0190] 以上仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

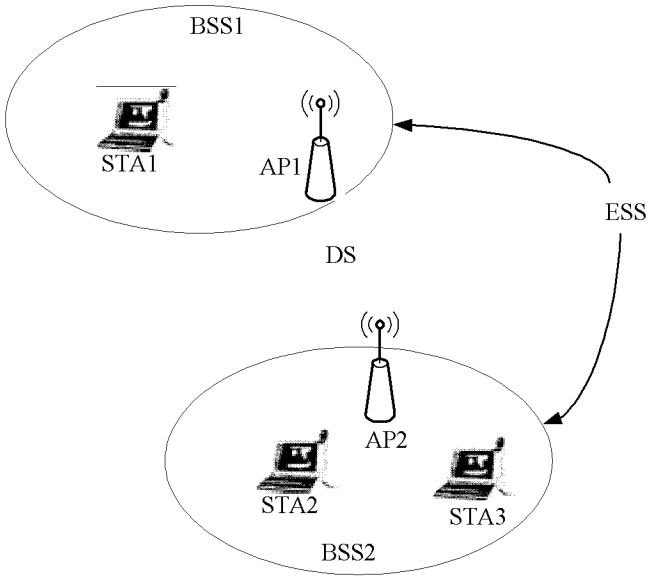

BSS1
STA1
AP1
ESS
DS
AP2
STA2
STA3
BSS2

图 1

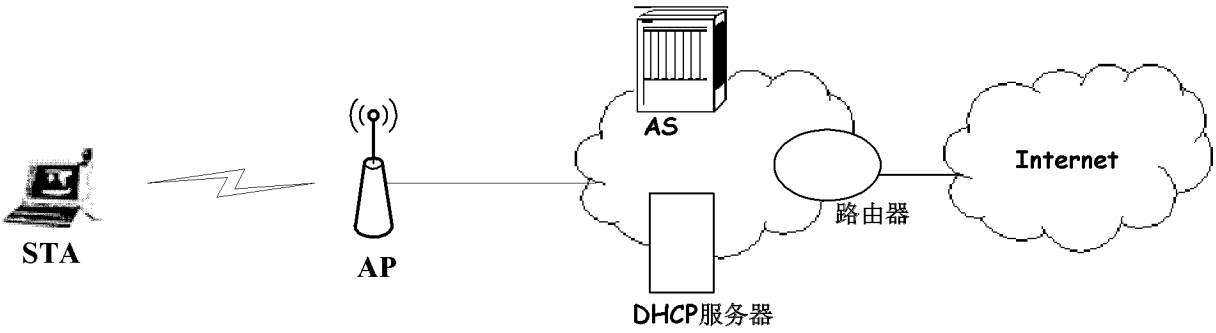

AS
Internet
STA
AP
路由器
DHCP服务器

图 2

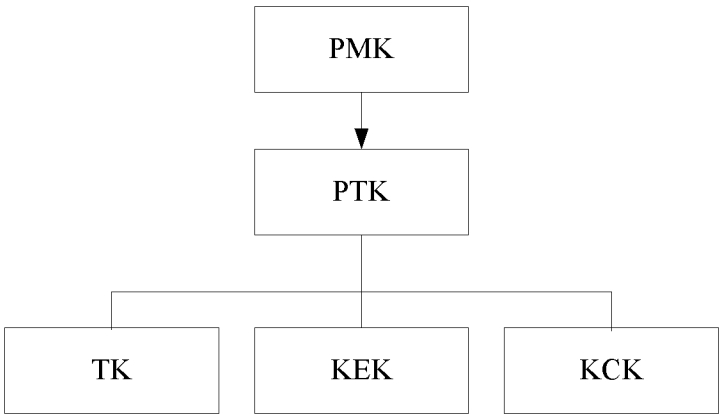

PMK
PTK
TK
KEK
KCK

图 3

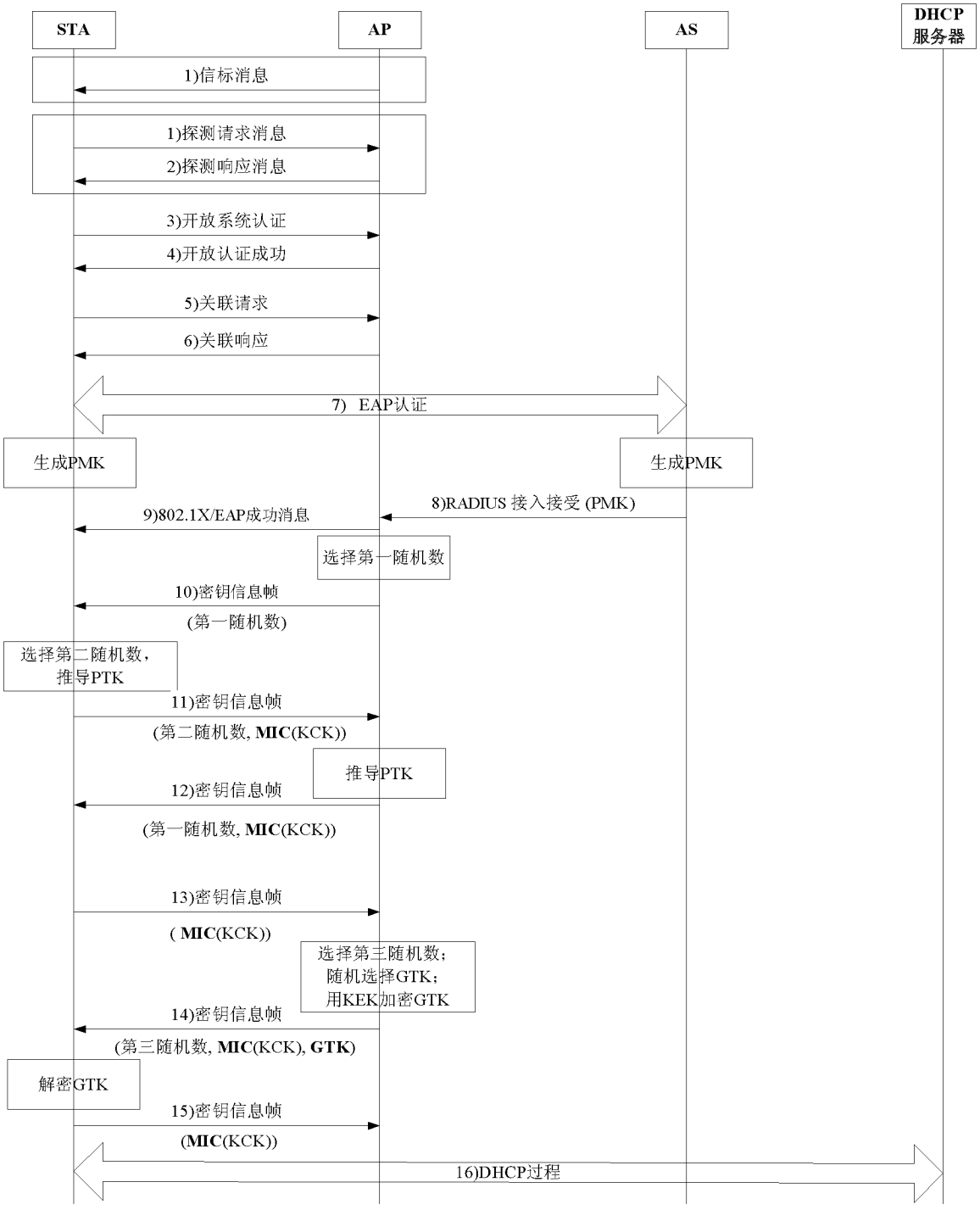

STA
AP
AS
DHCP
服务器
1)信标消息
1)探测请求消息
2)探测响应消息
3)开放系统认证
4)开放认证成功
5)关联请求
6)关联响应
7) EAP认证
生成PMK
生成PMK
8)RADIUS 接入接受 (PMK)
9)802.1X/EAP成功消息
选择第一随机数
10)密钥信息帧
(第一随机数)
选择第二随机数，
推导PTK
11)密钥信息帧
(第二随机数, MIC(KCK))
推导PTK
12)密钥信息帧
(第一随机数, MIC(KCK))
13)密钥信息帧
(MIC(KCK))
选择第三随机数；
随机选择GTK；
用KEK加密GTK
14)密钥信息帧
(第三随机数, MIC(KCK), GTK)
解密GTK
15)密钥信息帧
(MIC(KCK))
16)DHCP过程

图 4

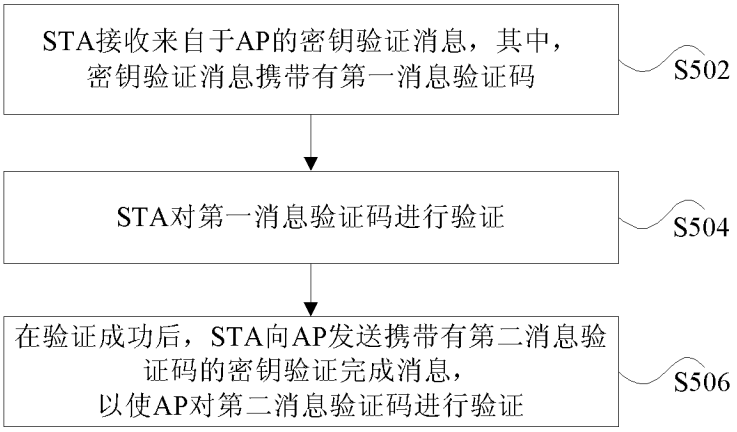

STA接收来自于AP的密钥验证消息，其中，
密钥验证消息携带有第一消息验证码
S502
STA对第一消息验证码进行验证
S504
在验证成功后，STA向AP发送携带有第二消息验
证码的密钥验证完成消息，
以使AP对第二消息验证码进行验证
S506

图 5

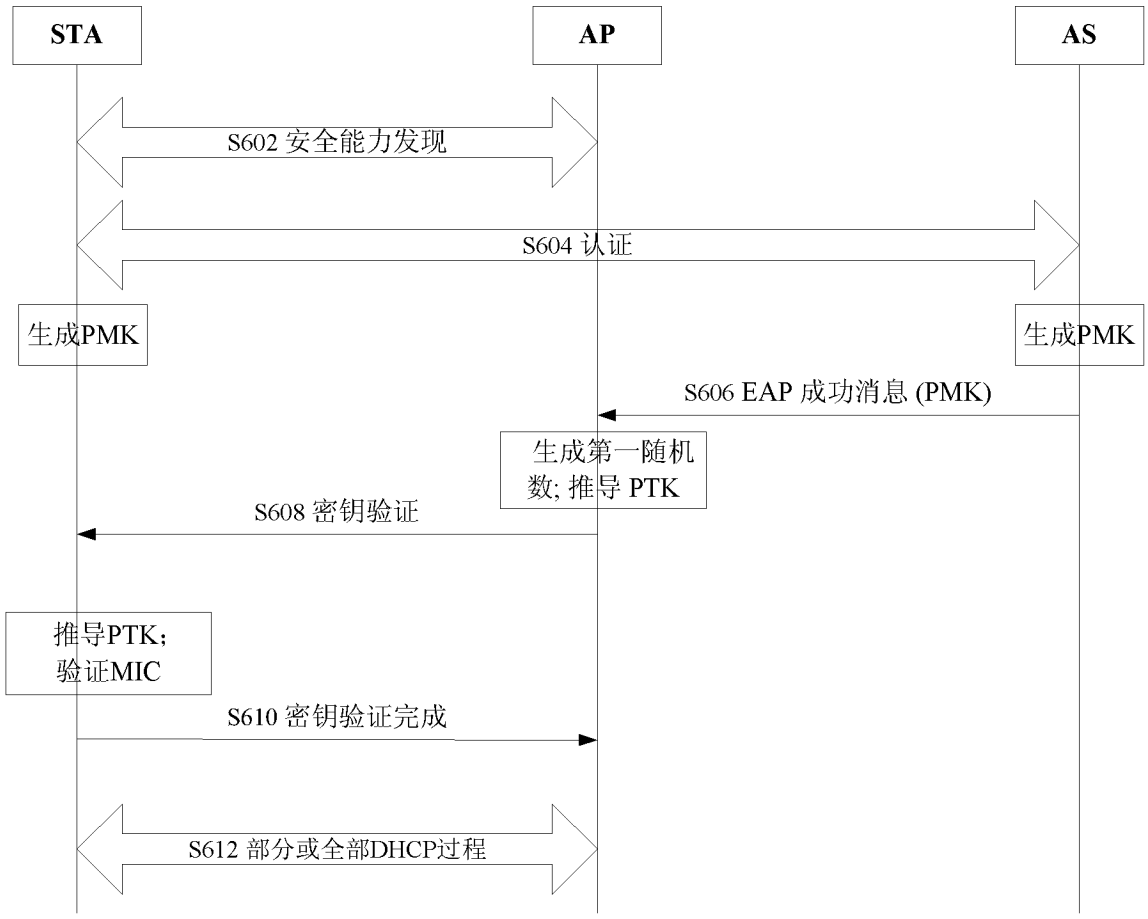

STA
AP
AS
S602 安全能力发现
S604 认证
生成PMK
生成PMK
S606 EAP 成功消息 (PMK)
生成第一随机
数; 推导 PTK
S608 密钥验证
推导PTK；
验证MIC
S610 密钥验证完成
S612 部分或全部DHCP过程

图 6

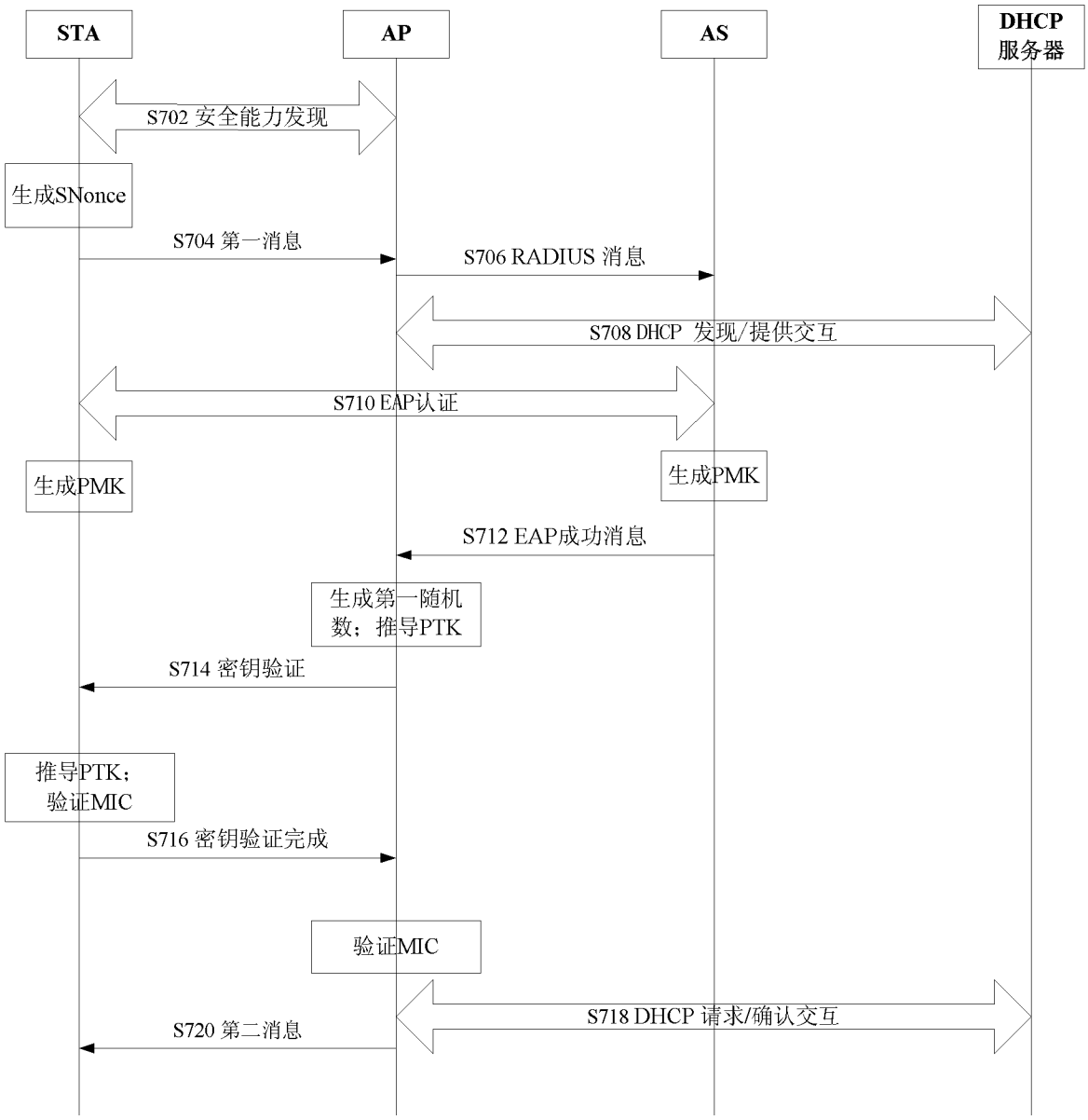

STA
AP
AS
DHCP 服务器
S702 安全能力发现
生成SNonce
S704 第一消息
S706 RADIUS 消息
S708 DHCP 发现/提供交互
S710 EAP认证
生成PMK
生成PMK
S712 EAP成功消息
生成第一随机数；推导PTK
S714 密钥验证
推导PTK；验证MIC
S716 密钥验证完成
验证MIC
S718 DHCP 请求/确认交互
S720 第二消息

图 7


第一接收模块102
第一验证模块104
第一发送模块106

图 8

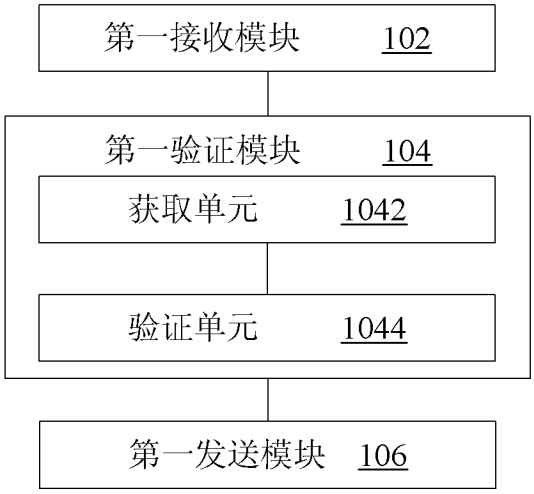

第一接收模块 102
第一验证模块 104
获取单元 1042
验证单元 1044
第一发送模块 106

图 9


第二发送模块202
第二接收模块204
第二验证模块206

图 10


第三发送模块 214
加密模块216
生成模块 208
获取模块 210
计算模块 212
第二发送模块 202
第二接收模块 204
第二验证模块 206

图 11