(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 101800982 A
(43)申请公布日 2010.08.11

(21)申请号 201010013725.6

(22)申请日 2010.01.15

(71)申请人 西安电子科技大学
地址 710071 陕西省西安市太白南路 2 号

(72)发明人 姜奇 杨超 马建峰 芦翔 杨凯

(74)专利代理机构 陕西电子工业专利中心 61205
代理人 王品华 朱红星

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

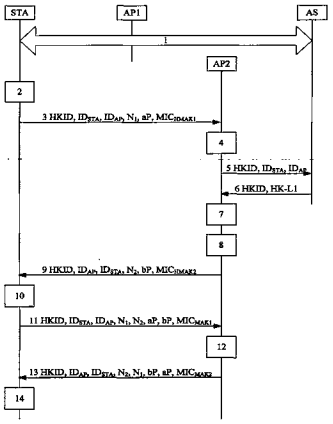
权利要求书 2 页 说明书 5 页 附图 1 页

(54)发明名称

无线局域网切换快速认证安全性增强方法

(57)摘要

本发明提供一种无线局域网切换快速认证安全性增强方法，主要解决现有标准无法满足军事应用高安全性需求的问题。其实现过程是：终端与认证服务器在初始接入认证阶段协商切换密钥；认证服务器在接收到接入点发送的切换子密钥请求时，计算相应的切换子密钥，并将该切换子密钥发送给该接入点；在切换过程中终端与接入点利用切换子密钥进行快速认证，并采用基于椭圆曲线的Diffie-Hellman交换生成会话密钥。本发明所提供方法具有前向保密性，能够抵抗部分拒绝服务攻击，简化了密钥管理，并降低了密钥泄露风险的优点，可用于紧急通信、指挥所的内部互联网，城市作战网络以及野战环境下快速网络部署。



CN 101800982 A

1. 一种无线局域网切换快速认证安全性增强方法，包括如下步骤：

(1) 协商切换密钥步骤：终端 STA 与认证服务器 AS 在初始接入认证阶段，预先协商切换密钥 HK；

(2) 切换认证请求步骤：

2a) 当终端 STA 决定关联到目标接入点 AP 时，利用切换密钥 HK 计算切换子密钥 HK-L1，并利用切换子密钥 HK-L1 计算切换消息认证密钥 HMAK；生成用于基于椭圆曲线的 Diffie-HellmanECDH 交换的终端 STA 的临时私钥与公钥对 (a,aP)，以及终端 STA 的一次性随机数 N_1；

2b) 将切换密钥标识 HKID、终端 STA 身份标识 ID_{STA}、接入点 AP 身份标识 ID_{AP}、终端 STA 的一次性随机数 N_1 和终端 STA 的临时公钥 aP 进行串联连接，利用切换消息认证密钥 HMAK 计算该连接结果的消息完整性验证码 MIC_{HMAK1}；

2c) 将所述的 HKID、ID_{STA}、ID_{AP}、N_1、aP 和 MIC_{HMAK1} 作为切换认证请求消息发送给接入点 AP；

(3) 切换认证响应步骤：

3a) 接入点 AP 接收到切换认证请求消息后，检查是否缓存有 HKID 对应的切换子密钥 HK-L1，若已缓存，转入步骤 3b)，否则，接入点 AP 向认证服务器 AS 请求对应的切换子密钥 HK-L1；

3b) 检查缓冲区中是否已缓存终端 STA 的一次性随机数 N_1，若已缓存，则该一次性随机数 N_1 有效性验证失败，否则，验证通过；接入点 AP 利用切换子密钥 HK-L1 计算切换消息认证密钥 HMAK，并对消息完整性验证码 MIC_{HMAK1} 进行验证；若验证通过，生成用于 ECDH 交换的接入点 AP 的临时私钥与公钥对 (b,bP)，以及接入点 AP 的一次性随机数 N_2；

3c) 将切换密钥标识 HKID、接入点 AP 身份标识 ID_{AP}、终端 STA 身份标识 ID_{STA}、接入点 AP 一次性随机数 N_2 和接入点 AP 临时公钥 bP 进行串联连接，利用切换消息认证密钥 HMAK 计算该连接结果消息完整性验证码 MIC_{HMAK2}；

3d) 将所述的 HKID、ID_{AP}、ID_{STA}、N_2、bP 和 MIC_{HMAK2} 作为切换认证响应消息发送给接入点 AP；

(4) 切换认证确认步骤：

4a) 终端 STA 接收到切换认证响应消息后，检查缓冲区中是否已缓存接入点 AP 的一次性随机数 N_2，若已缓存，则该一次性随机数 N2 有效性验证失败，否则，验证通过；对消息完整性验证码 MIC_{HMAK2} 进行验证；若验证通过，终端 STA 利用切换子密钥 HK-L1 计算切换会话密钥 HSK；

4b) 将切换密钥标识 HKID、终端 STA 身份标识 ID_{STA}、接入点 AP 身份标识 ID_{AP}、终端 STA 的一次性随机数 N_1、接入点 AP 的一次性随机数 N_2、终端 STA 的临时公钥 aP 和接入点 AP 的临时公钥 bP 进行串联连接，利用消息认证密钥 MAK 计算该连接结果的消息完整性验证码 MIC_{MAK1}；

4c) 将所述的 HKID、ID_{STA}、ID_{AP}、N_1、N_2、aP、bP 和 MIC_{MAK1} 作为切换认证确认消息发送给接入点 AP；

(5) 切换认证通告步骤：

5a) 接入点 AP 接收到切换确认请求消息后，对消息完整性验证码 MIC_{MAK1} 进行验证，若

验证通过，接入点 AP 利用切换子密钥 HK-L1 计算切换会话密钥 HSK ；

5b) 将切换密钥标识 HKID、接入点 AP 身份标识 ID_{AP}、终端 STA 身份标识 ID_{STA}、接入点 AP 的一次性随机数 N_2、终端 STA 的一次性随机数 N_1、接入点 AP 的临时公钥 bP 和终端 STA 的临时公钥 aP 进行串联连接，利用消息认证密钥 MAK 计算该连接结果的消息完整性验证码 MIC_{MAK2} ；

5c) 将所述 HKID、ID_{AP}、ID_{STA}、N_2、N_1、bP、aP 和 MIC_{MAK2} 作为切换认证通告消息发送给接入点 AP ；

(6) 切换认证通告验证步骤 ：终端 STA 接收到切换认证通告消息后，对消息完整性验证码 MIC_{MAK2} 进行验证 ；若验证通过，则切换认证成功，终端 STA 使用切换会话密钥 HSK 进行安全数据通信。

2. 根据权利要求 1 所述的无线局域网切换快速认证安全性增强方法，其中步骤 3a) 所述的接入点 AP 向认证服务器 AS 请求对应的切换子密钥 HK-L1，按如下步骤进行 ：

A. 接入点 AP 将切换密钥标识 HKID、终端 STA 身份标识 ID_{STA} 和接入点 AP 的身份标识 ID_{AP}，作为切换密钥请求消息发送给认证服务器 AS ；

B. 认证服务器 AS 对接收到的切换密钥请求消息中的切换密钥标识 HKID 的有效性进行验证，若认证服务器 AS 未缓存切换密钥标识 HKID，则验证失败，并返回错误信息，否则，验证通过 ；认证服务器 AS 利用切换密钥 HK 计算对应于接入点 AP 的切换子密钥 HK-L1，并通过预先建立的安全信道将 HKID、切换子密钥 HK-L1 和有效期作为切换密钥响应消息发送给接入点 AP ；

C. 接入点 AP 接收到切换密钥响应消息后，将切换密钥标识 HKID、切换子密钥 HK-L1 和有效期保存起来。

3. 根据权利要求 1 所述的无线局域网切换快速认证安全性增强方法，其中步骤 4a) 和 5a) 所述的切换会话密钥，包括单播加密密钥 UEK、单播完整性校验密钥 UCK、消息认证密钥 MAK 和密钥加密密钥 KEK 四个部分。

4. 根据权利要求 1 所述的无线局域网切换快速认证安全性增强方法，其中步骤 4a) 所述的终端 STA 利用切换子密钥 HK-L1 计算切换会话密钥 HSK，是终端 STA 将自己的临时私钥 a 与接入点 AP 的临时公钥 bP 相乘得到乘积 abP，将切换子密钥 HK-L1 和乘积 abP 作为参数代入密钥推导函数中，得到切换会话密钥 HSK，并在计算完成之后安全擦除终端 STA 的临时私钥 a。

5. 根据权利要求 1 所述的无线局域网切换快速认证安全性增强方法，其中步骤 5a) 所述的接入点 AP 利用切换子密钥 HK-L1 计算切换会话密钥 HSK，是接入点 AP 将自己的临时私钥 b 与终端 STA 的临时公钥 aP 相乘得到乘积 baP，将切换子密钥 HK-L1 和乘积 baP 作为参数代入密钥推导函数，得到切换会话密钥 HSK，并在计算完成之后安全擦除接入点 AP 的临时私钥 b。

无线局域网切换快速认证安全性增强方法

技术领域

[0001] 本发明属于网络安全技术领域，涉及无线局域网的安全性增强方法，可用于紧急通信、指挥所的内部互联网，城市作战网络以及野战环境下快速网络部署。

背景技术

[0002] 无线局域网WLAN(Wireless Local Area Network)通过无线电波作为媒介来传输信息，是计算机网络与无线通信技术相结合的产物。近年来，无线局域网凭借其高速传输能力和灵活性，在民用领域取得了广泛应用。目前已应用于公司内部、政府部门、学校、医院和住宅小区。无线局域网不但面临着传统有线网络的攻击方式的挑战，还要面临无线网络的特殊性所带来的挑战。无线信道的广播特性，使得信息的窃听，截获，插入，删除十分容易。无线局域网安全问题受到了广泛关注，国内外均制定了一系列相应安全标准。

[0003] 从无线局域网诞生之初，美国 IEEE 802.11 工作组便制定了有线等效保密 WEP 安全机制，但 WEP 早在 2001 年就被国际安全专家发现存在严重安全漏洞。IEEE 802.11 工作组于 2004 年提出 IEEE 802.11i 弥补 WEP 存在的安全问题。为了解决终端快速安全切换问题，该工作组又于 2008 年通过了 IEEE 802.11r，通过重用初始接入认证过程中建立的信任关系，并将认证交互信息叠加到认证和关联帧来减小切换过程的认证时延，从而实现快速安全切换。但是，该方法存在如下问题：切换认证过程中所协商的会话密钥不具有前向保密性；由于切换认证过程的前两条消息未采取任何安全保护机制，易受到拒绝服务攻击；密钥管理非常复杂，密钥管理开销大，使网络规模受限；此外，由于接入点 AP 的物理安全通常难以保障，因而将根密钥下推给 AP 存在风险，如果根密钥因 AP 被攻陷而泄露，则所有派生密钥均会泄露。

[0004] 中国在无线局域网领域的第一个国家标准 GB 15629.11-2003 于 2003 年 11 月 1 日正式实施，其中的安全解决方案称为 WLAN 鉴别和保密基础设施 WAPI。2004 年 3 月，中国 IT 标准化技术委员会的国家宽带无线 IP 标准工作组 BWIPS 发布了 WAPI 的实施方案，对原国家标准 WAPI 的一些安全缺陷进行了修正。中国宽带无线 IP 标准工作组于 2006 年 7 月 31 日公布了新的国家标准GB 15629.11-2003/XG1-2006WAPI-XG1。WAPI-XG1 是为了与 IEEE 802.11i 兼容并存，在 WAPI 及其实施方案的基础上提出的新的 WLAN 安全解决方案。到目前为止，中国还没有制定快速安全切换相关的安全标准，因此，无法满足军事应用的高安全性需求。

发明内容

[0005] 本发明目的在于解决现有标准所存在的问题，提出一种无线局域网切换快速认证安全性增强方法，以完善 WLAN 的切换认证过程，满足军事应用对 WLAN 系统的高安全性需求。

[0006] 为实现上述目的，本发明的无线局域网切换快速认证安全性增强方法，包括以下步骤：

[0007] (1) 协商切换密钥步骤：终端 STA 与认证服务器 AS 在初始接入认证阶段，预先协商切换密钥 HK；

[0008] (2) 切换认证请求步骤：

[0009] 2a) 当终端 STA 决定关联到目标接入点 AP 时，利用切换密钥 HK 计算切换子密钥 HK-L1，并利用切换子密钥 HK-L1 计算切换消息认证密钥 HMAK；生成用于基于椭圆曲线的 Diffie-Hellman ECDH 交换的终端 STA 的临时私钥与公钥对 (a，aP)，以及终端 STA 的一次性随机数 N_1；

[0010] 2b) 将切换密钥标识 HKID、终端 STA 身份标识 ID_{STA}、接入点 AP 身份标识 ID_{AP}、终端 STA 的一次性随机数 N_1 和终端 STA 的临时公钥 aP 进行串联连接，利用切换消息认证密钥 HMAK 计算该连接结果的消息完整性验证码 MIC_{HMAK1}；

[0011] 2c) 将所述的 HKID、ID_{STA}、ID_{AP}、N_1、aP 和 MIC_{HMAK1} 作为切换认证请求消息发送给接入点 AP；

[0012] (3) 切换认证响应步骤：

[0013] 3a) 接入点 AP 接收到切换认证请求消息后，检查是否缓存有 HKID 对应的切换子密钥 HK-L1，若已缓存，转入步骤 3b)，否则，接入点 AP 向认证服务器 AS 请求对应的切换子密钥 HK-L1；

[0014] 3b) 检查缓冲区中是否已缓存终端 STA 的一次性随机数 N_1，若已缓存，则该一次性随机数 N_1 有效性验证失败，否则，验证通过；接入点 AP 利用切换子密钥 HK-L1 计算切换消息认证密钥 HMAK，并对消息完整性验证码 MIC_{HMAK1} 进行验证；若验证通过，生成用于 ECDH 交换的接入点 AP 的临时私钥与公钥对 (b，bP)，以及接入点 AP 的一次性随机数 N_2；

[0015] 3c) 将切换密钥标识 HKID、接入点 AP 身份标识 ID_{AP}、终端 STA 身份标识 ID_{STA}、接入点 AP 一次性随机数 N_2 和接入点 AP 临时公钥 bP 进行串联连接，利用切换消息认证密钥 HMAK 计算该连接结果消息完整性验证码 MIC_{HMAK2}；

[0016] 3d) 将所述的 HKID、ID_{AP}、ID_{STA}、N_2、bP 和 MIC_{HMAK2} 作为切换认证响应消息发送给接入点 AP；

[0017] (4) 切换认证确认步骤：

[0018] 4a) 终端 STA 接收到切换认证响应消息后，检查缓冲区中是否已缓存接入点 AP 的一次性随机数 N_2，若已缓存，则该一次性随机数 N_2 有效性验证失败，否则，验证通过；对消息完整性验证码 MIC_{HMAK2} 进行验证；若验证通过，终端 STA 利用切换子密钥 HK-L1 计算切换会话密钥 HSK；

[0019] 4b) 将切换密钥标识 HKID、终端 STA 身份标识 ID_{STA}、接入点 AP 身份标识 ID_{AP}、终端 STA 的一次性随机数 N_1、接入点 AP 的一次性随机数 N_2、终端 STA 的临时公钥 aP 和接入点 AP 的临时公钥 bP 进行串联连接，利用消息认证密钥 MAK 计算该连接结果的消息完整性验证码 MIC_{MAK1}；

[0020] 4c) 将所述的 HKID、ID_{STA}、ID_{AP}、N_1、N_2、aP、bP 和 MIC_{MAK1} 作为切换认证确认消息发送给接入点 AP；

[0021] (5) 切换认证通告步骤：

[0022] 5a) 接入点 AP 接收到切换确认请求消息后，对消息完整性验证码 MIC_{MAK1} 进行验证，若验证通过，接入点 AP 利用切换子密钥 HK-L1 计算切换会话密钥 HSK；

[0023] 5b) 将切换密钥标识 HKID、接入点 AP 身份标识 ID_{AP}、终端 STA 身份标识 ID_{STA}、接入点 AP 的一次性随机数 N_2、终端 STA 的一次性随机数 N_1、接入点 AP 的临时公钥 bP 和终端 STA 的临时公钥 aP 进行串联连接，利用消息认证密钥 MAK 计算该连接结果的消息完整性验证码 MIC_{MAK2}；

[0024] 5c) 将所述 HKID、ID_{AP}、ID_{STA}、N_2、N_1、bP、aP 和 MIC_{MAK2} 作为切换认证通告消息发送给接入点 AP；

[0025] (6) 切换认证通告验证步骤：终端 STA 接收到切换认证通告消息后，对消息完整性验证码 MIC_{MAK2} 进行验证；若验证通过，则切换认证成功，终端 STA 使用切换会话密钥 HSK 进行安全数据通信。

[0026] 本发明由于采用了基于椭圆曲线的 Diffie-Hellman ECDH 交换协商切换会话密钥，对切换认证请求消息和切换认证响应消息进行了消息完整性保护，密钥层次中增加了切换子密钥层，增强了切换认证的安全性，因而具有如下优点：

[0027] 1) 切换会话密钥具有前向保密性，在切换密钥和切换子密钥泄露时，切换会话密钥依然是安全的；

[0028] 2) 能够抵抗部分拒绝服务攻击；

[0029] 3) 简化了密钥管理，接入点 AP 只需要维护与认证服务器 AS 的安全关联；

[0030] 4) 降低了密钥泄露的风险，在接入点 AP 被攻陷时，只会泄露自己的切换子密钥，不会对切换密钥和其他 AP 的切换子密钥的安全性造成影响。

附图说明

[0031] 图 1 是本发明切换快速认证流程。

具体实施方式

[0032] 结合上述附图，对本发明作进一步详述：

[0033] 步骤 1、终端 STA 初始接入 WLAN 网络时，假定该 STA 与接入点 AP1 发生关联，该 STA 与认证服务器 AS 在初始接入认证阶段预先协商切换密钥 HK 和切换密钥标识 HKID，预先协商方法包括 IEEE 802.1X 和改进的 WAPI。

[0034] 步骤 2、当 STA 决定关联到接入点 AP2 时，STA 利用切换密钥 HK 计算对应于 AP2 的切换子密钥 HK-L1，并利用 HK-L1 计算切换消息认证密钥 HMAK。

[0035] STA 利用切换密钥 HK 计算对应于 AP2 的切换子密钥 HK-L1 的方式如下，但不限于如下方式：

[0036] $HK\text{-}L1 = KD\text{-}HMAC\text{-}SHA256(HK, \text{“Handover key level 1”} | ADD_{AP2} | ADD_{STA})$；

[0037] 其中，KD-HMAC-SHA256 为密钥推导算法，ADD_{AP} 为 AP2 的媒体访问控制地址，ADD_{STA} 为 STA 的媒体访问控制地址。

[0038] STA 利用 HK-L1 计算切换消息认证密钥 HMAK 的方式如下，但不限于如下方式：

[0039] $HMAK = KD\text{-}HMAC\text{-}SHA256(HK\text{-}L1, \text{“Handover MAK”} | ADD_{AP} | ADD_{STA})$。

[0040] 步骤 3、STA 生成用于基于椭圆曲线的 Diffie-Hellman ECDH 交换的临时私钥与公钥对 (a, aP)，以及一次性随机数 N_1；将切换密钥标识 HKID、STA 身份标识 ID_{STA}、AP2 身份标识 ID_{AP}、N_1 和 aP 串联连接，利用 HMAK 计算该连接结果的消息完整性验证码 MIC_{HMAK1}；将 HKID、

ID_{STA}、ID_{AP}、N_1、aP 和 MIC_{HMAK1} 作为切换认证请求消息发送给 AP2。

[0041] STA 利用 HMAK 计算消息完整性验证码 MIC_{HMAK1} 的方式如下，但不限于如下方式：

[0042] MIC_{HMAK1} = HMAC-SHA256(HMAK, HKID|ADD_{STA}|ADD_{AP}|N_1|aP)；

[0043] 其中 HMAC-SHA256 为消息认证码算法。

[0044] 步骤 4、AP2 接收到切换认证请求消息后，检查是否缓存有 HKID 对应的切换密钥；若已缓存，则转入步骤 8，否则，AP2 向 AS 请求对应的切换子密钥。

[0045] 步骤 5、AP2 向 AS 发送 HKID，ID_{STA}，ID_{AP} 作为切换密钥请求消息。

[0046] 步骤 6、AS 接收到切换密钥请求消息后，验证 HKID 的有效性，若 AS 未缓存切换密钥标识 HKID，则验证失败，并返回错误信息，否则，验证通过，AS 利用切换密钥 HK 计算对应于该 AP 的切换子密钥 HK-L1，并通过预先建立的安全信道发送 HKID、HK-L1 和有效期作为切换密钥响应消息。AS 计算 HK-L1 的方式与 STA 计算 HK-L1 的方式相同。

[0047] 步骤 7、AP2 接收到切换密钥响应消息后，将 HKID、HK-L1 和有效期保存起来。

[0048] 步骤 8、AP2 检查缓冲区中是否已缓存终端 STA 的一次性随机数 N_1，若已缓存，则该一次性随机数 N_1 有效性验证失败，否则，验证通过；AP2 利用切换子密钥 HK-L1 计算切换消息认证密钥 HMAK，验证消息认证码 MIC_{HMAK1} 的有效性。AP2 计算 HMAK 的方式与 STA 计算 HMAK 的方式相同。

[0049] 步骤 9、验证通过后，AP2 生成用于 ECDH 交换的临时私钥与公钥对 (b,bP)，以及一次性随机数 N_2；将切换密钥标识 HKID、ID_{AP}、ID_{STA}、N_2 和 bP 串联连接，利用 HMAK 计算该连接结果的消息完整性验证码 MIC_{HMAK2}；将 HKID、ID_{AP}、ID_{STA}、N_2、bP 和 MIC_{HMAK2} 作为切换认证响应消息发送给 STA。

[0050] 步骤 10、STA 接收到切换认证响应消息后，检查缓冲区中是否已缓存接入点 AP2 的一次性随机数 N_2，若已缓存，则该一次性随机数 N_2 有效性验证失败，否则，验证通过；对消息完整性验证码 MIC_{HMAK2} 进行验证；若验证通过，STA 计算切换会话密钥 HSK，包括单播加密密钥 UEK、单播完整性校验密钥 UCK、消息认证密钥 MAK 和密钥加密密钥 KEK 四部分。

[0051] STA 将自己的临时私钥 a 与接入点 AP 的临时公钥 bP 相乘得到乘积 abP，利用 HK-L1 和 abP 计算切换会话密钥 HSK 的方式如下，但不限于如下方式：

[0052] HSK = KD-HMAC-SHA256(HK-L1，“Handover Session Key”|ADD_{AP}|ADD_{STA}|N_1|N_2|abP)，

[0053] 在计算完成之后，STA 安全擦除自己的临时私钥 a。

[0054] 步骤 11、STA 将切换密钥标识 HKID、ID_{STA}、ID_{AP}、N_1、N_2、aP 和 bP 串联连接，利用 MAK 计算该连接结果的消息完整性验证码 MIC_{MAK1}；将 HKID、ID_{STA}、ID_{AP}、N_1、N_2、aP、bP 和 MIC_{MAK1} 作为切换认证确认消息发送给 AP2。

[0055] STA 利用 MAK 计算消息完整性验证码 MIC_{MAK1} 的方式如下，但不限于如下方式：

[0056] MIC_{MAK1} = HMAC-SHA256(MAK, HKID|ADD_{STA} |ADD_{AP}|N_1|N_2|aP|bP)；

[0057] 步骤 12、AP2 接收到切换确认请求消息后，验证切换确认请求消息中 MIC_{MAK1} 的有效性；若验证通过，AP2 将自己的临时私钥 b 与终端 STA 的临时公钥 aP 相乘得到乘积 baP，利用 HK-L1 和乘积 baP 计算切换会话密钥 HSK，并在计算完成之后安全擦除 AP2 的临时私钥 b，AP2 计算 HSK 的方式与 STA 计算 HSK 的方式相同。

[0058] 步骤 13、AP2 将切换密钥标识 HKID、ID_{AP}、ID_{STA}、N_2、N_1、bP 和 aP 串联连接，利用 MAK

计算该连接结果的消息完整性验证码 MIC_{MAK2} ;将 HKID、ID_{AP}、ID_{STA}、N_2、N_1、bP、aP 和 MIC_{MAK2} 作为切换认证通告消息发送给 AP2。

[0059] 步骤 14、STA 接收到切换认证通告消息后,验证切换认证通告消息中 MIC_{MAK2} 的有效性 ;若验证通过,认证成功,将使用 HSK 进行安全数据通信。

[0060] 符号说明

[0061] ‖ :串联连接

[0062] (a, aP)、(b, bP) :分别是 STA 和 AP 的临时私钥与公钥对

[0063] ADD_{AP}、ADD_{STA} :分别是 AP 和 STA 的媒体访问控制地址

[0064] AP :接入点

[0065] AS :认证服务器

[0066] ECDH :基于椭圆曲线的 Diffie-Hellman

[0067] HK :切换密钥

[0068] HKID :切换密钥标识

[0069] HK-L1 :切换子密钥

[0070] HMAK :切换消息认证密钥

[0071] HMAC-SHA256 :消息认证码算法

[0072] HSK :切换会话密钥

[0073] ID_{AP}、ID_{STA} :分别是 STA 和 AP 的身份标识

[0074] IEEE :电气电子工程师协会

[0075] IEEE 802.11i :IEEE 制定的无线局域网安全标准

[0076] IEEE 802.11r :IEEE 制定的无线局域网快速切换标准

[0077] IEEE 802.1X :IEEE 制定的认证框架标准

[0078] KD-HMAC-SHA256 :密钥推导算法

[0079] KEK :密钥加密密钥

[0080] MAK :消息认证密钥

[0081] MIC :消息完整性验证码

[0082] N_1、N_2 :分别是 STA 和 AP 的一次性随机数

[0083] STA :终端

[0084] UEK :单播加密密钥

[0085] UCK :单播完整性校验密钥

[0086] WAPI :WLAN 鉴别和保密基础设施,中国无线局域网安全标准

[0087] WAPI-XG1 :中国无线局域网安全标准第一号修改单

[0088] WEP :有线等效保密

[0089] WLAN :无线局域网。

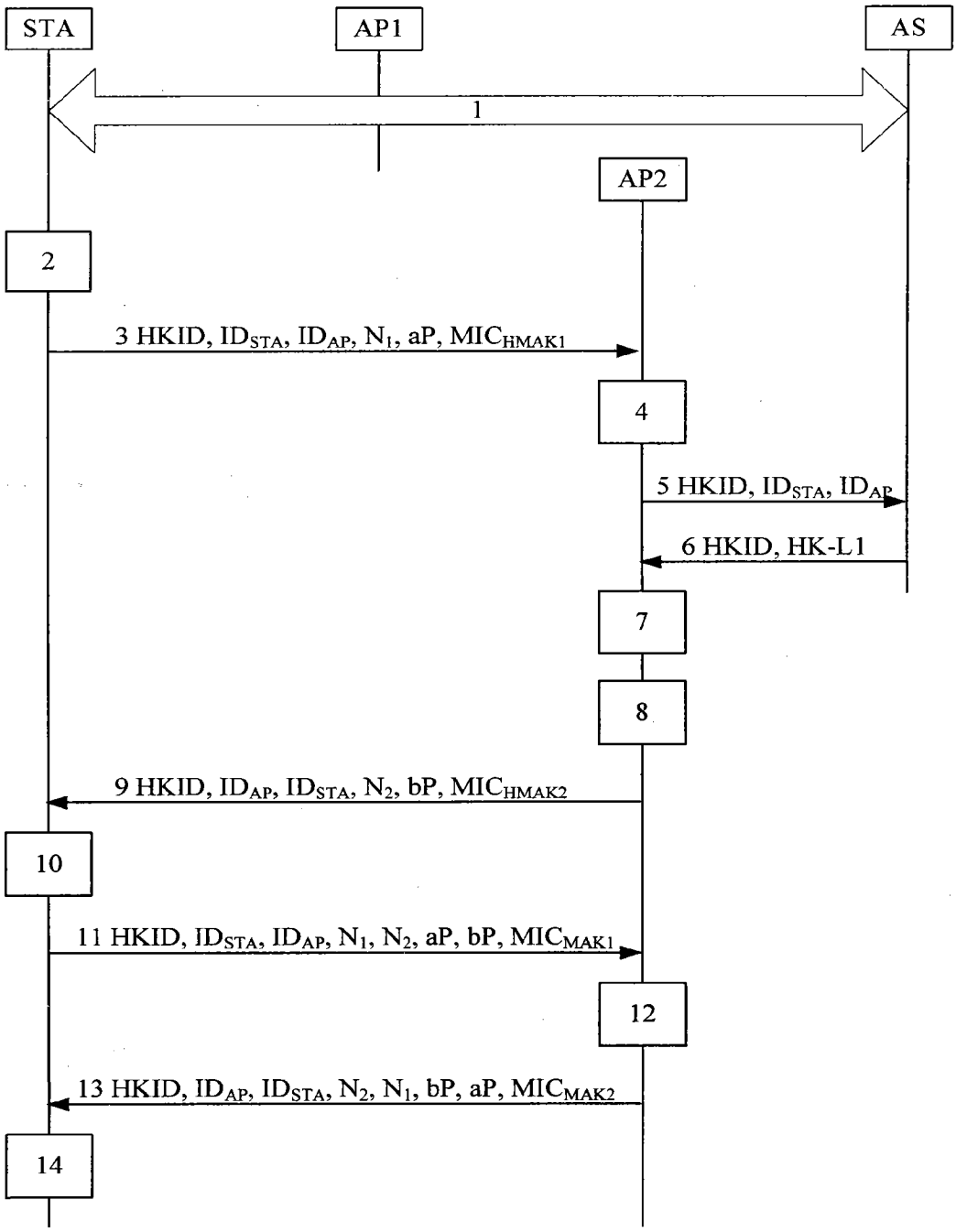

STA
AP1
AS
1
AP2
2
3 HKID, ID_{STA}, ID_{AP}, N_1, aP, MIC_{HMAK1}
4
5 HKID, ID_{STA}, ID_{AP}
6 HKID, HK-L1
7
8
9 HKID, ID_{AP}, ID_{STA}, N_2, bP, MIC_{HMAK2}
10
11 HKID, ID_{STA}, ID_{AP}, N_1, N_2, aP, bP, MIC_{MAK1}
12
13 HKID, ID_{AP}, ID_{STA}, N_2, N_1, bP, aP, MIC_{MAK2}
14

图 1