(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 101335621 B
(45)授权公告日 2011.03.16

(21)申请号 200710117956.X

(22)申请日 2007.06.26

(73)专利权人 中国科学院声学研究所
地址 100080 北京市海淀区北四环西路 21 号

(72)发明人 唐鼎 唐晖 林涛 赵志军 谭红艳

(74)专利代理机构 北京泛华伟业知识产权代理有限公司 11280
代理人 高存秀

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 12/28(2006.01)

审查员 张琦

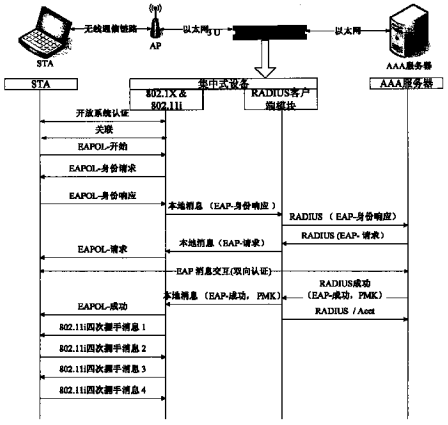
权利要求书 1 页 说明书 5 页 附图 3 页

(54)发明名称

一种 802.11i 密钥管理方法

(57)摘要

本发明涉及一种 802.11i 密钥管理方法，基于采用 802.11 分离 MAC 方案的系统构架实现，STA 通过分离 MAC 构架中的集中式设备完成主密钥协商；在获得主密钥后，STA 与所述集中式设备进一步协商，获得用于业务流加密的密钥；STA 利用用于业务流加密的密钥给数据加密。本发明基于分离 MAC 的 802.11i 密钥管理方案简化了 STA 发生二层切换时的接入认证和密钥协商过程，从而减少了整个二层切换的时延。本发明的认证处理以及数据加密的两个端点位于 STA 与集中设备上，可以有效的防止黑客通过替换 AP 等物理手段达到访问网络的目的。另外，本发明还便于升级，并减少了升级的成本。



CN 101335621 B

1. 一种 802.11i 密钥管理方法，基于采用 802.11 分离 MAC 方案的系统构架实现，STA 通过分离 MAC 构架中的集中式设备完成主密钥协商；在获得主密钥后，STA 与所述集中式设备进一步协商，获得用于业务流加密的密钥；STA 利用用于业务流加密的密钥给数据加密；

所述密钥管理方法包括如下步骤：

1) 安全能力协商阶段：STA 与集中式设备之间完成安全能力协商；

2) IEEE 802.1X 认证阶段：STA 通过集中式设备与认证服务器进行消息交互，完成双向认证和主密钥的协商；

3) 密钥协商阶段：集中式设备获得主密钥后，与 STA 进一步协商，得到用于业务流加密的密钥；

4) 传输数据转发保护：STA 利用用于业务流加密的密钥给数据加密，然后将加密数据发送给集中式设备，集中式设备将其解密并转发给目的地址；

STA 发生二层切换时，密钥管理方法包括如下步骤：

21) STA 切换到新的 AP 上时，与集中式设备进行重新关联，关联请求帧携带着前一次认证协商得到的主密钥标识；

22) 集中式设备按 STA 发送的主密钥标识查找本地的主密钥索引表；如果在主密钥索引表中找到相应的匹配项目，则发起 802.11i 四次握手过程，得到新的用于业务流加密的密钥；

23) STA 利用新的用于业务流加密的密钥给数据加密，然后将加密数据发送给集中式设备，集中式设备将其解密并转发给目的地址。

2. 按权利要求 1 所述的密钥管理方法，其特征在于，所述步骤 3) 中，所述集中式设备与 STA 的进一步协商是通过四次握手过程实现。

3. 按权利要求 2 所述的密钥管理方法，其特征在于，所述步骤 3) 中，所述集中式设备获得主密钥后，还将该主密钥缓存到一个数据结构变量中，该数据结构变量存储有每个 STA 的 MAC 地址、主密钥和主密钥标识，形成主密钥索引表。

4. 按权利要求 3 所述的密钥管理方法，其特征在于，所述数据结构变量是链表。

5. 按权利要求 1 所述的密钥管理方法，其特征在于，所述认证服务器是 RADIUS 服务器。

6. 按权利要求 1 所述的密钥管理方法，其特征在于，所述步骤 4) 中采用 TKIP 或 CCMP 加密算法对数据进行加密。

7. 按权利要求 1 所述的密钥管理方法，其特征在于，当 STA 发生二层切换时，集中式设备根据 STA 提供的主密钥标识查找主密钥索引表，如果在主密钥索引表中找到相应的匹配项目，则集中式设备直接与 STA 进一步协商，得到用于业务流加密的密钥。

8. 按权利要求 1 所述的密钥管理方法，其特征在于，所述主密钥是 PMK 密钥，所述用于业务流加密的密钥是 PTK 密钥。

一种 802.11i 密钥管理方法

技术领域

[0001] 本发明无线局域网接入领域，具体地说，本发明涉及一种 802.11i 密钥管理方法。

背景技术

[0002] 由于 IEEE802.11-1999 中 WEP 已被业界证明存在重大的缺陷，而且并没有提供安全的认证机制。因此在 2004 年 IEEE 标准组提出 IEEE802.11i 标准，标准中提出了 RSN 以增强无线局域网接入的安全性。

[0003] RSN 使用 IEEE802.1X 标准完成对 STA 的接入认证，并使用 TKIP 或 CCMP 加密算法对传输数据进行加密和完整性保护。由于 IEEE802.1X 认证信息是通过 802.11 的数据帧传送的，因此 RSN 在 STA 与 AP 完成关联后发生作用。对于支持 RSN 的 STA 接入过程可以分为以下几个阶段：安全能力协商阶段，IEEE802.1X 认证阶段，密钥协商阶段，传输数据转发保护。在安全能力协商阶段中，STA 完成 AP 的探测，与 AP 进行开放系统认证以及关联过程；在此阶段中双方通过在信标帧，探询帧，关联帧等管理帧中增加 RSN IE(RSN 信息元素）来确定并选择 RSN 中双方共同支持的认证、加密方式。在 IEEE802.1X 认证阶段，STA 通过 AP 与 AAA 服务器进行双向认证，AP 只对认证成功的 STA 进行数据转发；在密钥协商阶段，STA 与 AP 协商出用于数据加密的密钥。最后在传输数据转发保护阶段，STA 通过无线链路发送加密数据给 AP，AP 将其解密并转发给目的地址。

[0004] 802.11i 标准中 STA 的接入认证和密钥管理定义在 AP 实体上，这种网络结构在大规模布设无线网络时显现了它的不足：

[0005] STA 也不可能根据支持话音之类的实时应用的需求执行快速切换；

[0006] 如果某个接入点遭遇盗窃或破坏，安全将得不到保证。

[0007] 由于无线接入点的数量较多，当运营商需要升级认证控制功能时，需要替换大量的接入点，不易于升级。

[0008] 每个无线接入点都需要与 AAA 服务器建立连接并维持相互之间的安全的关联，这将增加 AAA 服务器的负担。

[0009] STA 在发生二层切换时，在 802.11i 协商过程中需要花费大量的时间进行认证，因此不适合实时业务的开展。

[0010] 另一方面，在 IETF RFC4118 中，根据 IEEE802.11MAC 功能实现的不同，将 WLAN 结构划分为本地 MAC 方式、分离 MAC 方式和远程 MAC 方式。其中，分离 MAC 方式是将 MAC 功能中的非实时部分实现在集中式设备上，而将和物理层联系比较紧密或实时性要求比较强的部分实现在 AP 上。控制了 AP 成本，利于开展话音业务和实现无线资源管理等高级管理功能。

[0011] 为方便理解，下面列出本发明中出现的一些术语的中英文对照：

[0012] CCMP :Counter mode with CBC-MAC Protocol

[0013] PMK :Pairwise Master Key，对等主密钥

[0014] PMKID :Pairwise Master Key Identity，对等主密钥标识

[0015] AP :Access Point,接入点

[0016] STA :Station 客户端

[0017] EAP :Extensible Authentication Protocol,可扩展认证协议

[0018] EAPOL :EAP Over LAN,局域网帧承载的 EAP 消息

[0019] RADIUS :Remote Authentication Dial-In User Service,远程用户拨号认证系统

[0020] TKIP :Temporal Key Integrity Protocol,瞬时密钥完整性协议

[0021] GRE :Generic Routing Encapsulation,通用路由封装协议

[0022] AAA :Authentication、Authorization、Accounting,认证、授权、计费

[0023] RSN :Robust Security Network,增强性安全网络

[0024] RSN IE :RSN Information Element,增强性安全网络信息元素

[0025] PTK :Pairwi se Transient Key 成对瞬时密钥

发明内容

[0026] 本发明的目的是利用 802.11 分离 MAC 技术,提出一种集中式的 802.11i 认证密钥管理方法。

[0027] 为实现上述发明目的,本发明提供的 802.11i 密钥管理方法,基于采用 802.11 分离 MAC 方案的系统构架实现,包括如下步骤 :

[0028] 1) 安全能力协商阶段 :STA 与集中式设备之间完成安全能力协商 ;

[0029] 2)IEEE802.1X 认证阶段 :STA 通过集中式设备与认证服务器进行消息交互,完成双向认证和主密钥的协商 ;

[0030] 3) 密钥协商阶段 : 集中式设备获得主密钥后,与 STA 进一步协商,得到用于业务流加密的密钥 ;

[0031] 4) 传输数据转发保护 :STA 利用用于业务流加密的密钥给数据加密,然后将加密数据发送给集中式设备,集中式设备将其解密并转发给目的地址。

[0032] 上述技术方案中,所述步骤 3) 中,所述集中式设备与 STA 的进一步协商是通过四次握手过程实现。

[0033] 上述技术方案中,所述步骤 3) 中,所述集中式设备获得主密钥后,还将该主密钥缓存到一个数据结构变量中,该数据结构变量存储有每个 STA 的 MAC 地址、主密钥和主密钥标识,形成主密钥索引表。

[0034] 上述技术方案中,所述数据结构变量是链表。

[0035] 上述技术方案中,所述认证服务器是 RADIUS 服务器。

[0036] 上述技术方案中,所述步骤 4) 中采用 TKIP 或 CCMP 加密算法对数据进行加密。

[0037] 上述技术方案中,当 STA 发生二层切换时,集中式设备根据 STA 提供的主密钥标识查找主密钥索引表,如果在主密钥索引表中找到相应的匹配项目,则集中式设备直接与 STA 进一步协商,得到用于业务流加密的密钥。

[0038] 上述技术方案中,当 STA 发生二层切换时,密钥管理方法包括如下步骤 :

[0039] 21)STA 切换到新的 AP 上时,与集中式设备进行重新关联,关联请求帧携带着前一次认证协商得到的主密钥标识 ;

[0040] 22) 集中式设备按 STA 发送的主密钥标识查找本地的主密钥索引表 ;如果在主密

钥索引表中找到相应的匹配项目，则发起 802.11i 四次握手过程，得到新的用于业务流加密的密钥；

[0041] 23)STA 利用新的用于业务流加密的密钥给数据加密，然后将加密数据发送给集中式设备，集中式设备将其解密并转发给目的地址。

[0042] 上述技术方案中，所述主密钥是 PMK 密钥。

[0043] 上述技术方案中，所述用于业务流加密的密钥是 PTK 密钥。

[0044] 基于分离 MAC 的 802.11i 密钥管理方案简化了 STA 发生二层切换时的接入认证和密钥协商过程，从而减少了整个二层切换的时延。而且集中式密钥管理方案也解决了背景技术中提到的传统密钥管理的缺陷。例如：1、本发明的认证处理以及数据加密的两个端点位于 STA 与集中设备上，可以有效的防止黑客通过替换 AP 等物理手段达到访问网络的目的。2、相对无线接入点 AP 来说，集中设备的数量较少，当运营商需要升级认证控制功能时，仅需要升级集中设备即可，因此便于升级，减少了升级的成本。

附图说明

[0045] 图 1 是基于 802.11 分离 MAC 的密钥管理示意及模块图

[0046] 图 2 是基于分离 MAC 的密钥管理信令时序图

[0047] 图 3 是切换过程中密钥管理示意图

[0048] 图 4 是将密钥下发给内核 High MAC 模块的处理图

具体实施方式

[0049] 本发明由集中式设备负责对 STA 的认证，集中式设备维护着所有 AP 下接入的 STA 认证、密钥等信息。由于这些信息并不维护在每个 AP 上，当 STA 从一个 AP 切换到另一个 AP 时，集中式设备并不需要对 STA 重新进行整个认证过程，而是根据 STA 在接入时提供的主密钥索引，找到以前认证时获得的主密钥，并直接进入密钥协商中的四次握手过程，从而减少整个二层切换的时延。

[0050] 下面结合附图和具体实施例对本发明作进一步地描述。

[0051] 实施例 1

[0052] 本实施例的系统构架基于分离 MAC 方案，将 MAC 层拆分为两部分，即 HighMAC 部分和 Low MAC 部分。其中，High MAC 部分实现在集中式设备上，以支持无线资源的管理、优化移动性管理；Low MAC 部分实现在接入点上，主要是处理对实时性要求比较高以及和物理层关系比较紧密的功能。

[0053] High MAC 部分实现的功能：管理帧的处理；能够保证 STA 与 AC 之间的管理帧交互；数据帧的处理，包括分组和重组；能够将 STA 发送的数据帧转换成以太网帧；或将发送给 STA 的以太网帧转换为 802.11 数据帧，发送给 STA；转发功能；数据报文的加密、解密。

[0054] Low MAC 部分实现的功能：控制帧的处理；速率调整；信标帧的产生；探询帧的处理；节电模式的处理。

[0055] 如附图 1 所示，本实施例的集中式设备具有基于分离 MAC 的密钥管理系统主要涉及到以下几个功能模块：认证和密钥协商模块、RADIUS 客户端模块、内核中的 High MAC 模块。其中认证和密钥协商模块主要完成与用户端进行认证以及密钥握手通信，其它模块给

予辅助。

[0056] 如图 2 所示，本实施例中，STA 第一次接入时密钥管理流程如下：

[0057] (1) 认证和密钥协商模块在程序启动时，初始化认证和加密的方式，以及网络套接口、Netlink 套接口和本地套接口，然后进入无限循环，等待接收消息。

[0058] (2) 当 AP 启动后，向集中式设备发送注册信息，在成功注册之后，集中式设备的内核通过 Netlink 套接口将 AP 信息发送至认证和密钥协商模块。

[0059] (3)STA 接入网络，与集中设备先后进行开放系统认证、关联，关联过程中 STA 与集中设备完成认证和加密方式的协商，即安全能力协商。该过程 AP 需要将关联请求帧通过 GRE 隧道转发给集中设备，成功之后内核通过 netlink 套接口将 STA 的 MAC 地址、认证和加密方式等信息发送至认证和密钥协商模块。此时在认证和密钥协商模块中已经维护一张与 AP 相关的链表，里面存放了 AP 的 MAC、及其 RSN 参数等相关信息。同时也有了一张与其关联的 STA 相关的链表，其中存放了 STA 的 MAC，及其 RSN 参数等相关信息。至此安全能力协商阶段完成。

[0060] (4) 进入 802.1X 认证阶段，STA 发送 EAPOL 开始消息，引发 802.1X 双向认证（也可以由集中式设备直接发送 EAPOL 身份请求消息引发认证）。此时集中式设备在 STA 与 RADIUS 服务器之间负责 EAP 消息的传递，STA 与集中式设备之间是 EAPOL 消息，集中式设备与 RADIUS 服务器之间是由 RADIUS 协议承载的 EAP 消息（在集中式设备上由认证和密钥协商模块解析、封装和处理 EAPOL 消息，RADIUS 客户端模块解析、封装和处理 RADIUS 消息，两个模块之间通过本地套接口发送内部消息）

[0061] (5) 当双向认证在 STA 与 RADIUS 服务器之间成功完成之后，服务器会将 EAP 认证成功消息以及 PMK 传递给集中式设备，集中式设备获得 PMK 后，将该 PMK 缓存到一个全局的的链表中，该链表是一个存储有 STA 的 MAC 地址、PMK 和 PMKID 三元组的链表。（这一缓存表也可采用链表以外的其它数据结构实现，如采用哈西表的方式实现，这是本领域技术人员容易理解的）此时无线认证结束，向 RADIUS 客户端模块发送计费消息给 RADIUS 服务器，并进入密钥协商阶段。

[0062] (6) 集中式设备将自己产生的随机数以及 MAC 地址通过 EAPOL-Key 发送给 STA（即 802.11i 四次握手消息 1）

[0063] (7)STA 发送四次握手消息 2（其中包括 STA 的 MAC 地址和 STA 产生的随机数），集中式设备利用消息中的信息产生 PTK，且由 PTK 推导出各种所需要的密钥。并发送包含组播密钥的消息 3

[0064] (8)STA 以消息 4 最终确认，四次握手至此完成。整个 802.1X 认证密钥协商过程结束。

[0065] (9) 集中式设备上的认证和密钥协商模块下发 PTK 等密钥材料给位于驱动层的 802.11High MAC 功能单元，以供内核驱动程序加密数据（图 4）。

[0066] (10) 最后，STA 发送加密数据给 AP，AP 使用 GRE 隧道直接将加密数据发送给集中设备，集中式设备中的 802.11High MAC 模块使用一定加密算法（如 TKIP 或 CCMP）和 PTK 对 STA 数据解密并转发至目的地址。

[0067] 上述过程为 STA 首次接入认证的过程，当 STA 已经完成首次接入并发生切换时的过程如下（图 3）：

[0068] (1) 当 STA 要从原始 AP 移动到新的 AP 的时候，与集中式设备上的 High MAC 功能单元进行重新关联，关联请求帧携带着前一次认证协商得到的 PMKID。集中式设备提取 PMKID 与本地的 PMKID 缓存表比较，发现对应的 PMK 已经存在，于是触发二层切换的密钥协商过程；

[0069] (2) 触发二层切换的集中式设备在与 STA 完成无线关联之后直接发送四次握手的第一个消息，收到四次握手消息的客户端于是也进入四次握手。客户端和集中式设备利用第一次协商的 PMK 协商出全新的 PTK；

[0070] (3) 集中式设备上的认证和密钥协商模块下发 PTK 等密钥材料给位于驱动层的 802.11High MAC 功能单元，以供内核驱动程序加密数据（图 4）。

[0071] (4) 最后，STA 发送加密数据给新的 AP，新的 AP 使用 GRE 隧道直接将加密数据发送给集中设备，集中式设备中的 802.11High MAC 模块使用一定加密算法（如 TKIP 或 CCMP）和新的 PTK 对 STA 数据解密并转发至目的地址。

[0072] 试验数据：

[0073] 按图 4 拓扑网络结构搭建试验床进行试验，结果如下：

[0074] 第一次整个认证和协商过程总共需要传输了 33 个报文，包括了 2 个设备认证，2 个无线关联帧，4 个密钥协商帧，剩下的全部为用户认证数据，经历了约 400 毫秒，这意味着只要客户接入网络就需要接近 400 毫秒的消耗。如果客户是第一次接入网络这个过程是必须的，然而如果客户通过认证后在网内移动还需要这种反复的认证，这样的延迟就是不能接受的，这 400 毫秒时间这对普通人虽然是转瞬即逝，但是对于 QoS 要求高的应用，如 VoIP 业务，用户就可以明显的感觉到语音的中断。

[0075] 切换过程的认证和密钥协商试验。对于非集中式架构的方案，切换过程的接入与第一次接入一样需要花费 400 毫秒。而使用本发明的方案，切换过程只需要传输 8 个报文，消耗大约 80 毫秒，极大的提高了切换速度。

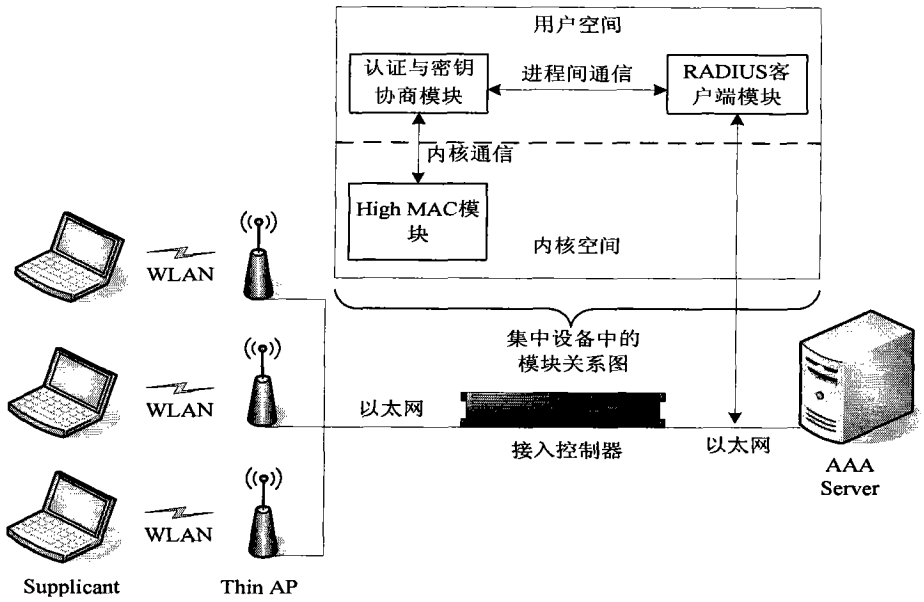

用户空间
认证与密钥协商模块
进程间通信
RADIUS客户端模块
内核通信
High MAC模块
内核空间
集中设备中的模块关系图
WLAN
WLAN
WLAN
以太网
接入控制器
以太网
AAA Server
Supplicant
Thin AP

图 1

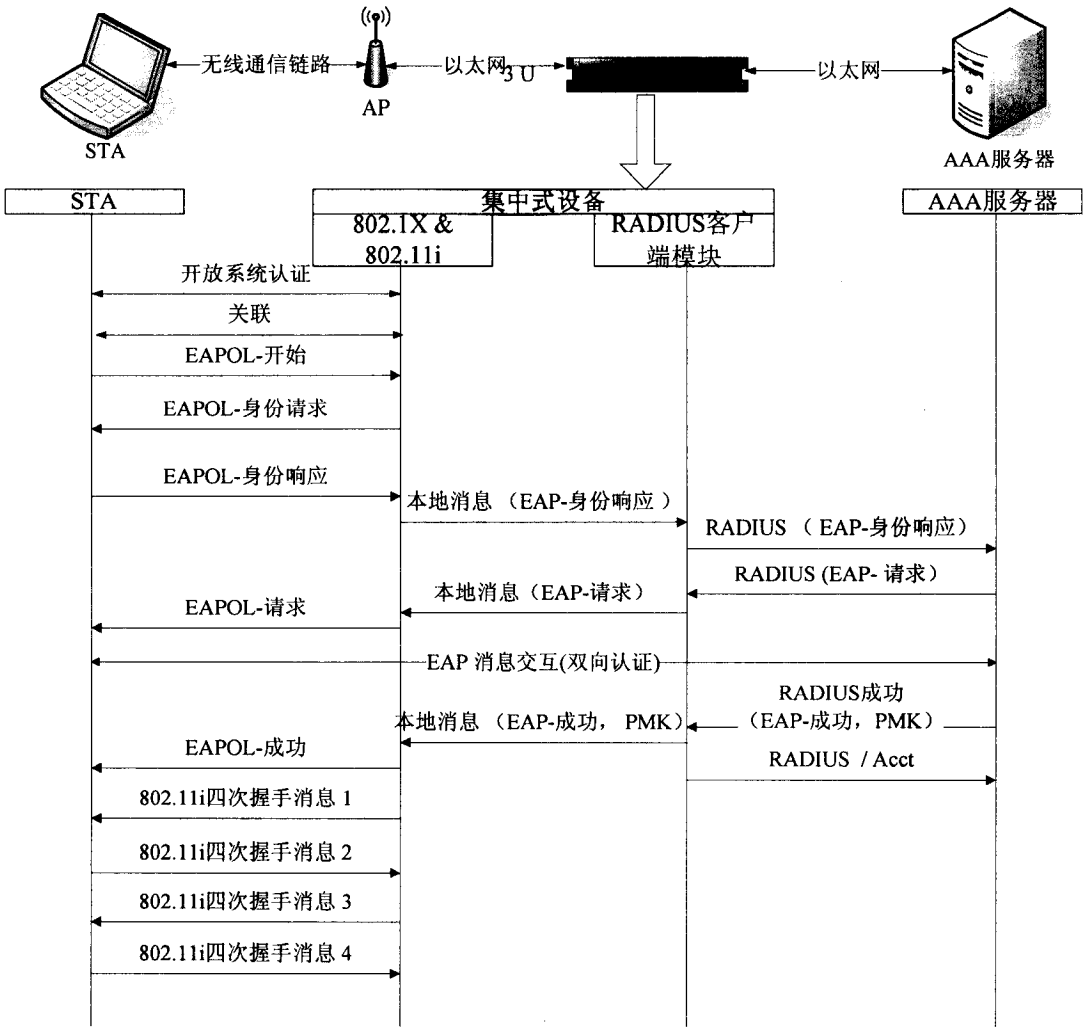

无线通信链路
以太网
以太网
STA
AP
AAA服务器
STA
集中式设备
802.1X & 802.11i
RADIUS客户端模块
AAA服务器
开放系统认证
关联
EAPOL-开始
EAPOL-身份请求
EAPOL-身份响应
本地消息 （EAP-身份响应 ）
RADIUS （ EAP-身份响应）
RADIUS (EAP- 请求）
本地消息（EAP-请求）
EAPOL-请求
EAP 消息交互(双向认证)
RADIUS成功
（EAP-成功，PMK）
本地消息 （EAP-成功， PMK）
EAPOL-成功
RADIUS / Acct
802.11i四次握手消息 1
802.11i四次握手消息 2
802.11i四次握手消息 3
802.11i四次握手消息 4

图 2

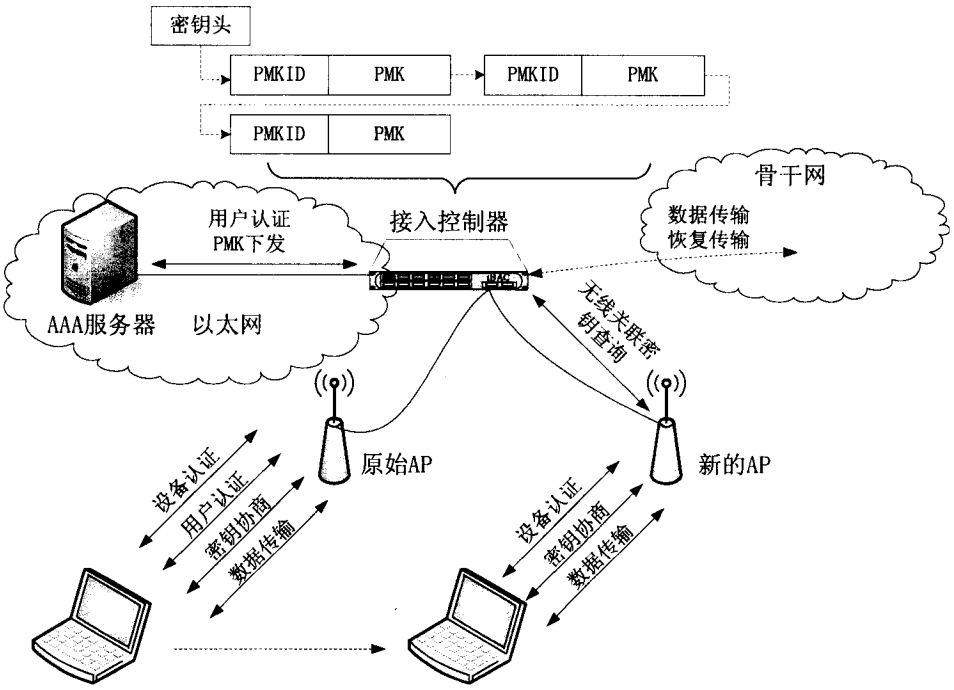

密钥头
PMKID
PMK
PMKID
PMK
PMKID
PMK
骨干网
数据传输
恢复传输
用户认证
PMK下发
接入控制器
AAA服务器
以太网
无线关联密钥查询
原始AP
新的AP
设备认证
用户认证
密钥协商
数据传输
设备认证
密钥协商
数据传输

图 3

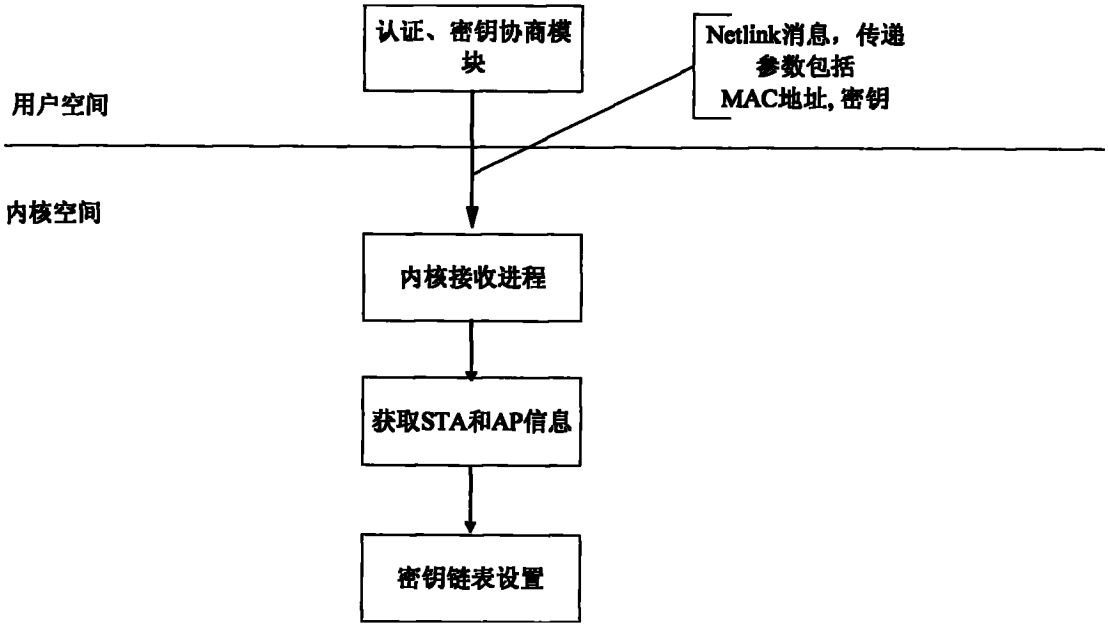

认证、密钥协商模块
Netlink消息，传递参数包括MAC地址,密钥
用户空间
内核空间
内核接收进程
获取STA和AP信息
密钥链表设置

图 4