HW11

PB17111614

王嵘晟

1、(1).无线工作站搜寻无线接入点，发送认证请求

(2).无线接入点收到认证请求后，发回认证答复帧，其中包含一个明文文本。

(3).无线工作站点收到明文文本，用共享密钥加密，发回加密的密文。

(4).接入点用相同的密钥解密，结果与之前明文文本对比，相同则发送"成功"信息，否则发回"失败"。

2、(1).生成PN，保证每个MPDU有一个新的PN。

(2).用MAC头构造CCM的附加认证数据

(3).利用PN、MPDU自己发送地址和个人先级域计算CCM nonce

(4).把PN和key ID编入CCMP头部

(5).利用MPDU和Nonce构造CCM-MAC的IV。

(6).使用该IV，CCMP在CCM-MAC下使用AES计算出MIC，将MIC截为64位，添加在MPDU后面

(7).利用PN和MPDU TA构造CTR模式的counter

(8).利用该counter，CCMP在CTR模式下使用AES加密MPDU数据和MIC。

(9).由原MAC帧头、CCMP header和密文组合形成CCMP MPDU。

3、(1)连接到AS，STA向它的AP发送一个请求以连接到AS，AP记录并给AS发送一个访问请求。

(2).EAP交换：STA和AS相互授权

(3)密钥分发：一旦认证完成，AS和STA产生一个主会话密钥，称AAA密钥

4、用户身份认证、用户身份保密、用户数据保密、信令数据保密。

5、(1).网络接入安全：提供安全接入3G服务网的机制并抵御对无线链路的攻击。

(2).网络域安全：保证网内信令的安全传送并抵御对有线网络的攻击。

(3).用户域安全：主要保证对移动站的安全接入

(4).应用域安全：使用户域与服务提供商的应用保证能安全交换信息。

(5).安全特性的可适性及可配制能力：指用户能获知安全特性是否在使用以及安全服务提供商提供的服务是否需要以安全服务为基础。

以上五个部分与应用层、服务层、传输层构成3GPP安全的结构