CHAPTER 7

SCOPE FOR FUTURE WORK

7.1 IEEE 802.11i

802.11i includes standard known as Advanced Encryption Standard –Counter Mode Cipher Block Chaining –Message Authentication Code (AES-CCMP). AES is a much stronger encryption algorithm that the US National Institutes of Standards and Technology (NIST) chose AES to replace the aging Data Encryption Standard (DES). CCMP is the most advanced encryption available for wireless networks today and is central to the Robust Security Network (RSN) portion of 802.11i. 802.11i incorporates authentication, data integrity and data encryption mechanism to address security concerns for legacy (TKIP) and new wireless LANs (CCMP). However, AES-CCMP requires a hardware coprocessor to operate. Therefore, extra hardware is needed in the implementation of AES-CCMP.

TKIP targets at legacy equipment. To be backward compatible with WEP, TKIP uses RC4 stream cipher. TKIP is software-oriented whereas CCMP is hardware-oriented. CCMP is based on advanced encryption standard which requires new 802.11 hardware with great processing power. To overcome WEP problems permanently, it is required to design a new security protocol from scratch and to use a stronger ciphering technique than RC4 which will require new hardware in APs and wireless interface cards; this adds extra cost to wireless equipment.
7.2 IEEE802.1x

IEEE802.1x is a port-based network access control protocol used to achieve mutual authentication and efficient key exchange mechanism between clients and servers in wired and wireless LANs. IEEE 802.1x authentication requires three stations in place: the supplicant which is the user or client that wants to be authenticated, the Authentication Server (AS), and a device that will pass information between the supplicant and the authentication server called the authenticator.

Port-based authentication begins when the supplicant connects to a closed port or the authenticator recognizes a supplicant client on a closed port. It accomplishes this by utilizing the EAP protocol to pass authentication information over the network to the authentication system, which is usually a RADIUS server. The supplicant then sends an EAP-Response/Identity packet to the authenticator which passes it on to the authentication server. The authentication server responds with a challenge requiring the supplicant to supply identity information such as a password. If the returned information is correct then the authentication server instructs the authenticator to allow access of all network traffic to the supplicant.

EAP messages traveling between supplicants and the authenticator in wired or wireless LAN environment are encapsulated in an encapsulation technique called EAP over LAN or EAPoL, the terms EAPoL and EAP are used interchangeably when working in a LAN environment.
7.3 CCMP

Counter Mode with Cipher Block Chaining –Message Authentication Code (CCMP) is based on the Advanced Encryption Standard (AES), a FIPS-197 certified algorithm approved by NIST. AES operates in a counter mode (AES-128-CM) within 802.11i with CBC-MAC (CCM). Counter mode is used for data confidentiality and Cipher Block Chaining –Message Authentication Code (CBC-MAC) is used for data integrity and authentication.

CCMP is the most advanced encryption available for wireless networks today and is central to the Robust Security Network (RSN) portion of 802.11i. The protocol is capable of confidentiality with its Counter Mode and ensures data integrity based on the Cipher Block Chaining Message Authentication Codes (CBC-MAC). Although AES allows different values for key and block length, the CCMP protocol utilizes 128 bits for each of these [2][57].

**NONCE**: The nonce is constructed from the packet number (PN), MAC layer A2 Address field (A2) and MAC layer priority field. Since the nonce value can be pre-computed, the only thing required to predict the counter value is length of payload. The length of the payload can be obtained through a priori information.

**CCMP Security Mechanism**

CCMP requires a fresh temporal key for every session. CCMP also requires a unique nonce value for each frame protected by a given
temporal key, and CCMP uses a 48-bit packet number (PN). The CCMP headers concatenated with the MAC header, the encrypted payload, the encrypted MIC and the FCS field. These fields form the MPDU as illustrated in Figure 7-1.

![Figure 7-1 CCMP MPDU](image)

The CCMP encapsulation process is depicted in Figure 7-1. CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting cipher text using the following steps:
a) Increment the PN, to obtain a fresh PN for each MPDU, so that the PN never repeats for the same temporal key. Note that retransmitted MPDUs are not modified on retransmission.

b) Use the fields in the MPDU header to construct the additional authentication data (AAD) for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD. MPDU header fields that may change when retransmitted are muted by being masked to 0 when calculating the AAD.

c) Construct the CCM Nonce block from the PN, A2, and the Priority field of the MPDU where A2 is MPDU Address 2. The Priority field has a reserved value set to 0.
d) Place the new PN and the key identifier into the 8-octet CCMP header.

e) Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and MIC. This step is known as CCM originator processing.

f) Form the encrypted MPDU by combining the original MPDU header, the CCMP header, the encrypted data and MIC.

The CCMP decapsulation steps are depicted in the Figure 7-3.
The decryption steps are:

a) The encrypted MPDU is parsed to construct the AAD and nonce values.
b) The AAD is formed from the MPDU header of the encrypted MPDU.
c) The nonce value is constructed from the A2, PN, and Priority Octet fields (reserved and set to 0).
d) The MIC is extracted for use in the CCM integrity checking.
e) The CCM recipient processing uses the temporal key, AAD, nonce, MIC, and MPDU cipher text data to recover the MPDU plaintext data as well as to check the integrity of the AAD and MPDU plaintext data.
f) The received MPDU header and the MPDU plaintext data from the CCM recipient processing may be concatenated to form a plaintext MPDU.

Reconstruction of Nonce in CCMP protocol

The nonce block constitutes three fields. The first field is A2 address of MAC header (A2), second is priority field which is set to ‘0’ by default and the third field is PN field.

Priority Field || Address (A2) || Packet Number (PN) = Nonce

The construction of nonce has been devised in such a manner that its reconstruction by an adversary is possible[76]. The first 8 bits of nonce is the priority field which is presently kept as ‘0’, this field may be used in future for 802.11 frame prioritization. The A2 field, which is 48 bits, is extracted from the MAC header field and is concatenated with the priority field. The only dynamic field, which is monotonically increasing per MPDU, is the PN field. The Reserved octet can be assigned with signal rate from PLCP or the 48 bit PN field can be reduced to 40bit PN
field, an octet can be used to hold Signal field from PLCP header. The enhancement to nonce block is as follows:

Priority Field $|\,|\,\text{Address (A2)}\,|\,|\,\text{Packet Number (PN)}\,|\,|\,\text{signal rate from PLCP} = \text{Nonce}$

The nonce is reconstructed from the packet number (PN), MAC layer A2 Address field (A2), MAC layer priority field, and signal field value from physical layer convergence protocol. The Reserved octet can be assigned with signal rate from PLCP or the 48 bit PN field can be reduced to 40 bit PN field, an octet can be used to hold Signal field from PLCP header. Dynamic nonce can be generated because signal rate value is different for each transmission based on the channel condition.

IEEE 802.11i has been well analyzed and recently CCMP protocol has been incorporated providing encryption, integrity and authentication. The counter mode has been used with AES to provide the confidentiality services. The mechanism, devised, is using the PN, A2, priority field and length of payload length to compute the counter value. This weak construction of nonce renders the protocol vulnerable to attacks by intruders. The failure of the counter mode will result in the collapse of the whole security mechanism of 802.11 WLAN. The IEEE 802.11 standard provides multiple data rates at the physical layer (PHY). The Physical Layer Convergence Protocol (PLCP) header specifies the data rate of current transmission in SIGNAL field. Dynamic nonce can be generated because signal rate value is different for each transmission based on the channel condition.