Overview of Emerging IEEE 802.11 Protocols for MAC and Above

Sunghyun Choi
Seoul National University

CONTENTS

Overview of Emerging IEEE 802.11 Protocols for MAC and Above

Sunghyun Choi

During the last few years, the IEEE 802.11 Wireless LAN (WLAN) has become a dominant technology for the (indoor) broadband wireless networking. Along with its success, there have been demands to enhance the performance of the 802.11. To meet such needs, the IEEE 802.11 Working Group (WG) has been developing new protocols to amend the existing protocols. In this paper, we overview the emerging protocols of the IEEE 802.11 WLAN for the medium access control (MAC) layers and above. These include 802.11e for quality-of-service (QoS), 802.11f for Inter-Access Point Protocol (IAPP), 802.11h for spectrum management at 5GHz, 802.11i for security enhancement, 802.11k for radio resource measurement, and finally 802.11m for higher throughput.

Keyword: IEEE 802.11, WLAN, MAC

I. INTRODUCTION

IEEE 802.11 Wireless LANs (WLANs) have been extensively deployed in the recent years in many different environments for enterprise, home, and public networking. The state-of-the-art 802.11 devices provide the Ethernet-like best-effort service with the transmission rate up to 54 Mbps at 2.4GHz and 5GHz unlicensed bands.

The 802.11 standard specifies the protocols for both the medium access control (MAC) sub-layer and physical (PHY) layer. The IEEE 802.11 Working Group (WG) [1] started its standardization activities in 1991, and published the first standard specification in 1997. The 802.11 devices currently available in the market are based on the following specifications:

- 802.11 MAC specified in [2], and
- 802.11a PHY specified in [3] supporting up to 54 Mbps transmission rate at 5GHz, and/or
- 802.11b PHY specified in [4] supporting up to 11 Mbps transmission rate at 2.4GHz, and/or
- 802.11g PHY specified in [7] supporting up to 54 Mbps transmission rate at 2.4GHz; 802.11g is a super set of 802.11b PHY.

Sunghyun Choi: Seoul National University

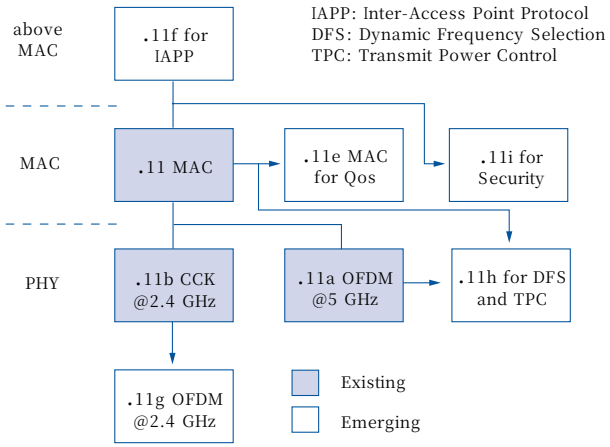


Figure 1. Current and emerging 802.11 specification

As found in the reference, all the specifications other than IEEE 802.11-1999 in [2] are amendments of the original specification.

During the last few years, the 802.11 WG has been working on the standardization of new specifications to enhance the performance of the 802.11 WLAN. Out of new and emerging specifications, the followings are related to the layers of the MAC and above:

- 802.11e for Quality-of-Service (QoS) support [5]
- 802.11f for Inter-Access Point Protocol (IAPP) [6]
- 802.11h for spectrum and transmit power management [8]
- 802.11i for security enhancement [9]
- 802.11k for radio resource measurement enhancement [10]
- 802.11n for higher throughput [1]

Figure 1 illustrates the relationship among the existing and emerging specifications, where the direction of each arrow specifies the original and amended standards. For example, the 802.11e MAC is an amendment of the 802.11-1999 MAC. Note that some specifications like 802.11h (and 802.11n, not shown in the figure) involve both MAC and PHY amendments. The figure represents the status of the 802.11 standard families as of late year 2003 or as late as early 2004; the standardization activities for 802.11f, 802.11g, and 802.11h have been finalized already, and the activities for 802.11e and 802.11i are expected to be finished by the end of 2003 or early 2004. The 802.11k and 802.11n are not shown since the standardization of these two protocols has recently started.

In this paper, we overview the characteristics of these emerging specifications of the 802.11 related to the MAC and above. The rest of the paper is organized as follows. We first briefly review the current MAC of the 802.11 in Section II. Then, Sections III, IV, V, and VI present the 802.11e for QoS, 802.11f for IAPP, 802.11h for spectrum and transmit power management, and 802.11i for security enhancement, respectively. After briefing the 802.11k and 802.11n in Section VII, we conclude this paper in Section VIII.

II. LEGACY 802.11 MAC [2]

The IEEE 802.11 legacy MAC [2] is based on the logical functions, called the coordination functions, which determine when a station (STA) operating within a Basic Service Set (BSS) is permitted to transmit and may be able to receive frames via the wireless medium. There are two types of BSSs. An infrastructure BSS is composed of an access point (AP) and multiple STAs associated with the AP, where the AP works as a bridge between the wireless and wired domains, and an independent BSS (IBSS) is composed of multiple STAs. Within an infrastructure BSS, a STA should be associated with an AP in order to perform a normal data transfer. A frame arriving from the higher layer to the MAC is referred to as MAC Service Data Unit (MSDU), and the frame, which carries the MSDU or its fragment along with the MAC header and Frame Check Sequence (FCS) based on CRC-32, is referred to as MAC Protocol Data Unit (MPDU). The MPDU is the frame which is being transferred between STAs in the MAC's perspective.

Two coordination functions are defined, namely, the mandatory distributed coordination function (DCF), for a distributed, contention-based channel access, based on carrier-sense multiple access with collision avoidance (CSMA/CA), and the optional point coordination function (PCF), for a centralized, contention-free channel access, based on poll-and-response mechanism. Most of today's 802.11 devices operate in the DCF mode only.

1. Distributed Coordination Function (DCF)

The 802.11 DCF works with a single first-in-first-out (FIFO) transmission queue. The CSMA/CA constitutes a distributed MAC based on a local assessment of the channel status, i.e., whether the channel is busy (i.e., somebody transmitting a frame) or idle (i.e., no transmission). Basically, the CSMA/CA of the DCF works as follows:

When a frame arrives at the head of the transmission queue, if the channel is busy, the MAC waits until the medium becomes idle, then defers for an extra time interval, called the DCF Interframe Space (DIFS). If the channel stays idle during the DIFS deference, the MAC then starts the backoff process by selecting a random backoff count. For each slot time interval, during which the medium stays idle, the random backoff counter (or BC) is decremented. When the counter reaches zero, the frame is transmitted. On the other hand, when a frame arrives at the head of the queue, if the MAC is in either the DIFS deference or the random backoff process[2], the processes described above are applied again. That is, the frame is transmitted only when the random backoff has finished successfully. When a frame arrives at an empty queue and the medium has been idle longer than the DIFS time interval, the frame is transmitted immediately.

Each STA maintains a contention window (CW), which is used to select the random backoff count. The backoff count is determined as a pseudo-random integer drawn from a uniform distribution over the interval [0,CW]. How to determine the CW value is further detailed below. If the channel becomes busy during a backoff process, the backoff is suspended. When the channel becomes idle again, and stays idle for an extra DIFS time interval, the backoff process resumes with the latest backoff counter value. The timing of DCF channel access is illustrated in Figure 2.

1) An MAC Service Data Unit (MSDU) is the unit of data arriving at the MAC from the higher layer.
2) This situation is possible due to the "post" backoff requirement as described below.

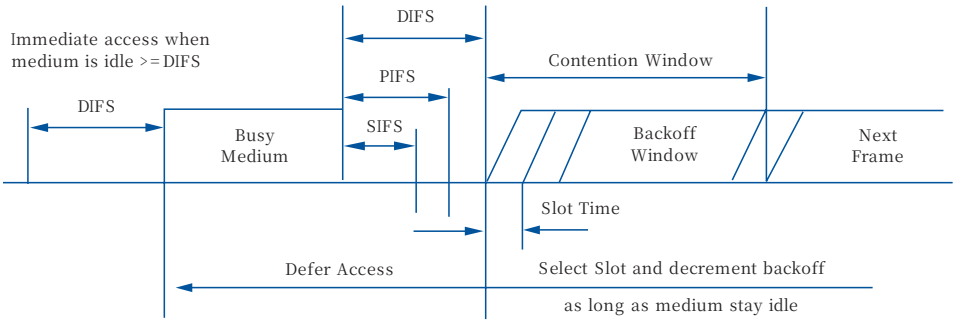


Figure 2. IEEE 802.11 DCF Channel Access

For each successful reception of a frame, the receiving STA immediately acknowledges the frame reception by sending an acknowledgement (ACK) frame. The ACK frame is transmitted after a short IFS (SIFS), which is shorter than the DIFS. Other STAs resume the backoff process after the DIFS idle time. Thanks to the SIFS interval between the data and ACK frames, the ACK frame transmission is protected from other STAs' contention. If an ACK frame is not received after the data transmission, the frame is retransmitted after another random backoff.

The CW size is initially assigned CWmin, and increases when a transmission fails, i.e., the transmitted data frame has not been acknowledged. After any unsuccessful transmission attempt, another backoff is performed using a new CW value updated by

$$CW := 2(CW + 1) - 1,$$

with an upper bound of CWmax. This reduces the collision probability in case there are multiple STAs attempting to access the channel. After each successful transmission, the CW value is reset to CWmin, and the transmission-completing STA performs the DIFS deference and a random backoff even if there is no other pending frame in the queue. This is often referred to as "post" backoff, as this backoff is done after, not before, a transmission. This post backoff ensures there is at least one backoff interval between two consecutive MSDU transmissions.

In the WLAN environments, there may be hidden STAs. Two STAs, which can transmit to and receive from a common STA while they cannot see each other, are hidden STAs each other. Since the DCF operates based on the carrier sensing, the existence of such hidden STAs can degrade the network performance severely. To reduce the hidden STA problem, the 802.11 defines a Request-to-Send/Clear-to-Send (RTS/CTS) mechanism. That is, if the transmitting STA opts to use the RTS/CTS mechanisms, before transmitting a data frame, the STA transmits a short RTS frame, followed by a CTS frame transmitted by the receiving STA. The RTS and CTS frames include the information of how long it does take to transmit the subsequent data frame and the corresponding ACK response. Thus, other STAs hearing the transmitting STA and hidden STAs close to the receiving STA will not start any transmissions; their timer called Network Allocation Vector (NAV) is set, and as long as the NAV value is non-zero, a STA does not contend for the

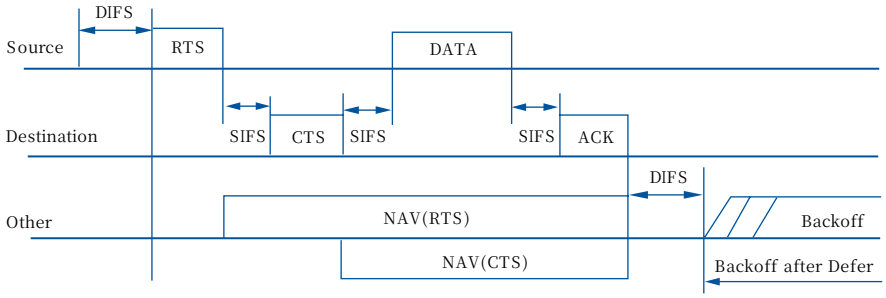


Figure. 3. RTS/CTS frame exchange

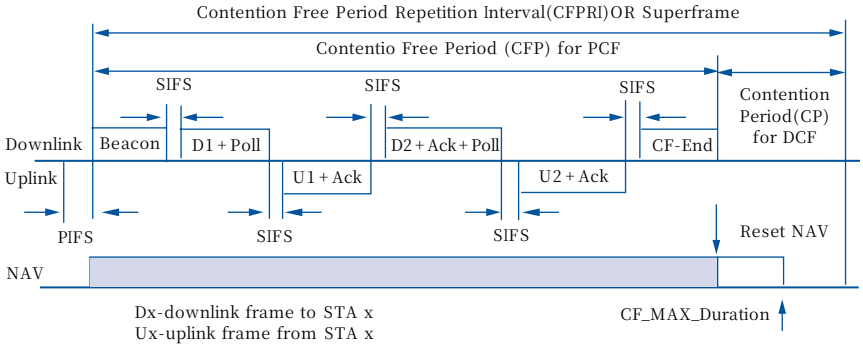


Figure 4. IEEE 802.11 PCF channel access during a CFP

medium. Between two consecutive frames in the sequence of RTS, CTS, data, and ACK frames, a SIFS is used. Figure 3 shows the timing diagram involved with an RTS/CTS frame exchange.

All of the MAC parameters including SIFS, DIFS, Slot Time, CWmin, and CWmax are dependent on the underlying physical layer (PHY). Irrespective of the PHY, DIFS is determined by SIFS+2 · SlotTime, and another important IFS, called PCF IFS (PIFS), is determined by SIFS+SlotTime.

2. Point Coordination Function (PCF)

To support time-bounded services, the IEEE 802.11 standard also optionally defines the Point Coordination Function (PCF) to let STAs have contention-free access to the wireless medium, coordinated by a Point Coordinator (PC), which is co-located within the AP. The PCF has higher priority than the DCF, because the period during which the PCF is used is protected from the DCF contention via the NAV set. Under the PCF, time axis is divided into repeated periods, called superframes, where each superframe is composed of a Contention Free Period (CFP) and a subsequent Contention Period (CP). During a CFP, the PCF is used for accessing the medium, while the DCF is used during a CP. It is mandatory that a superframe includes a CP of a minimum length that allows at least one MSDU delivery under the DCF at the lowest PHY rate. See Figure 4 for the CFP and CP co-existence.

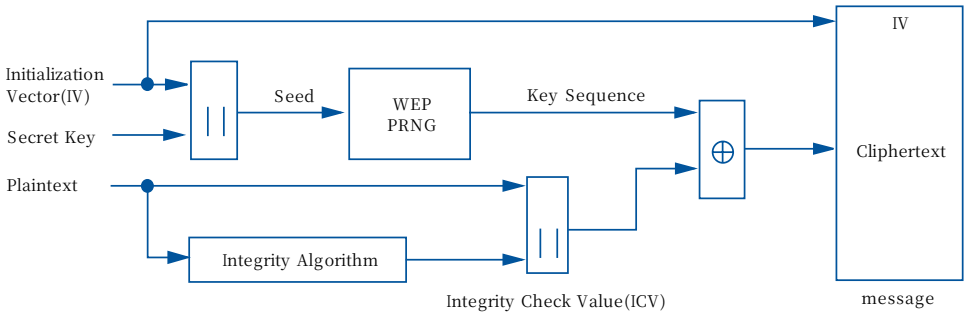


Figure 5. WEP encapsulation block diagram

A superframe starts with a beacon frame, which is a management frame that maintains the synchronization of the local timers in the STAs and delivers protocol related parameters. The AP generates beacon frames at regular beacon frame intervals, thus every STA knows when the next beacon frame will arrive; this instance is called target beacon transition time (TBTT), and is announced in every beacon frame. During a CFP, there is no contention among STAs; instead, STAs are polled. See Figure 4 for typical frame exchange sequences during a CFP. The PC polls a STA asking for a pending frame. If the PC itself has pending data for this STA, it uses a combined date and poll frame by piggybacking the CF-Poll frame into the data frame.

Upon being polled, the polled STA acknowledges the successful reception along with data. If the PC receives no response from a polled STA after waiting for a PIFS interval, it polls the next STA, or ends the CFP. Therefore, no idle period longer than PIFS occurs during CFP. The PC continues with polling other STAs until the CFP expires. A specific control frame, called CF-End, is transmitted by the PC as the last frame within the CFP to signal the end of the CFP.

3. Security Mechanisms

The 802.11 MAC provides two different forms of the security mechanisms, namely, authentication and frame encryption. The authentication can be performed between two STAs in either an IBSS or an infrastructure BSS. In case of the infrastructure BSS, the authentication is between a STA and an AP, and only after a successful authentication, an association between the STA and the AP can be made established. There are two forms of the authentication, namely, open system and shared key authentications. The open system is virtually equivalent with no authentication since two STAs just exchange authentication request and response frames under this type of authentication. On the other hand, with the share key type, two STAs exchange four frames to check if they have the same security key. Unless they have the same key, the authentication process is supposed to fail.

For the normal data frame transmissions after the authentication (and association in case of the infrastructure BSS), the transmitting STA can encrypt the frame frame using the mechanism called Wired Equivalent Privacy (WEP). The WEP scheme uses the RC4 pseudo-random number generator (PRNG) algorithm from RSA Data Security, Inc. based on 64-bit

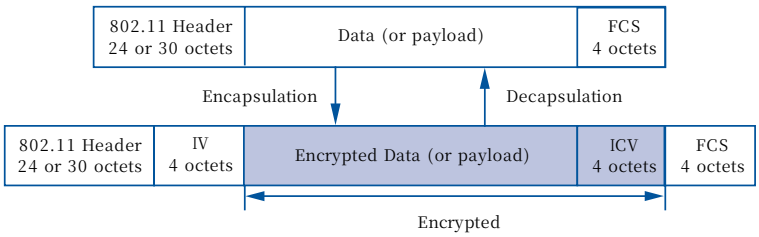


Figure 6. Original frame vs. WEP encapsulated MPDU

keys [2]. Figure 5 presents the block diagram of the WEP encapsulation. A 64-bit seed is actually generated by combining 40-bit secret key (which should be known to both the transmitter and the receiver off-line) and a 24-bit Initialization Vector (IV) chosen by the transmitting STA. On the other hand, an integrity algorithm, based on CRC-32, is applied to the plaintext, i.e., non-encrypted original data payload, to generate an Integrity Check Value (ICV). The ICV is intended for the receiver to check the integrity of the received frame. Then, the key sequence generated using the RC4 algorithm is XOR'ed with the plaintext and the ICV to generate a ciphertext. The ciphertext along with the IV value is transmitted in the 802.11 data frame body as shown in Figure 6. The receiving STA performs the reverse operation by decrypting the received frame body and checking if the decrypted frame is in tact.

4. MAC Management

There are basically three different MAC management functions: (1) synchronization; (2) power management; (3) association and reassociation; and (4) management information base (MIB) definitions.

First, the synchronization in the 802.11 WLAN is basically achieved via beacon frames. In the infrastructure BSS, the AP periodically transmits beacon frames, which include the Time Synchronization Function (TSF) timer value, and all the associated STA updates their local TSF timer upon the beacon reception. In the IBSS, STAs transmit beacon frames in a contentious manner.

Second, the power management allows a STA to stays in the doze state, in which the power consumption is minimal, and wakes up periodically without losing the traffic addressed to it. In the infrastructure BSS, the AP buffers all the frames addressed to a STA in the doze state, and announces the existence of the buffered frames via beacon frames. STAs wake up periodically in order to receive beacon frames, and if the buffered frames exist, the STA requests the delivery of its buffered frames by transmitting a special control frame called Power Save (PS)-Poll.

Third, in an infrastructure BSS, a STA first associates with an AP before starting any normal data transfer by exchanging associate request and response frames. As described in Section II.C, the authentication procedure should be preceded before the association procedure. When a STA moves out of the coverage of its associated AP, the STA performs the handoff procedures by finding new AP(s) and reassociating with the best AP. The detection of APs can be done via scanning processes (either passive or active scanning). The difference between the association and reassociation is basically the fact that a reassocaite request frame is used instead of an associate request

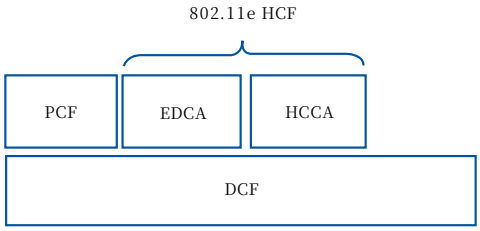


Figure 7. 802.11e MAC architecture

frame in the case of the reassociation, and the reassociate request frame includes the MAC address of the old AP. The new AP can utilize the old AP's MAC address in order to communicate with the old AP as described in Section IV.

Finally, the MIB comprises the managed objects, attributes, actions, and notifications required to manage a station. These MIB values can be used for the network management purpose by external entities, e.g., using Simple Network Management Protocol (SNMP) [28].

III. 802.11E MAC FOR QoS SUPPORT [5]

In this section, we present the 802.11e MAC for QoS provisioning. The IEEE 802.11e defines a single coordination function, called the hybrid coordination function (HCF). The HCF combines functions from the DCF and PCF with some enhanced QoS-specific mechanisms and QoS data frames in order to allow a uniform set of frame exchange sequences to be used for QoS data transfers during both the CP and CFP. Note that the 802.11e MAC is backward compatible with the legacy MAC, and hence it is a superset of the legacy MAC. The HCF is composed of two channel access mechanisms: (1) a contention-based channel access referred to as the enhanced distributed channel access (EDCA), and (2) a controlled channel access referred to as the HCF controlled channel access (HCCA). Figure 7 shows the logical relationship between the 802.11e HCF and the 802.11 DCF/PCF. As shown in the figure, the HCF sits on top of the DCF in the sense that the HCF utilizes and honors the CSMA/CA operation of the DCF.

One distinctive feature of the 802.11e HCF is the concept of transmission opportunity (TXOP), which is an interval of time when a particular STA has the right to initiate transmissions. During a TXOP, there can be a set of multiple frame exchange sequences, separated by SIFS, initiated by a single STA. A TXOP can be obtained either by a successful EDCA contention or by receiving a QoS CF-poll frame from the AP. It is called an EDCA TXOP for the former case while it is called a polled TXOP for the latter case. The new concept with TXOP is limiting the time interval during which a STA can transmit its frames. The limit of a the TXOP duration is determined by the AP, and is announced to STAs via the beacons (in case of EDCA TXOP) and the corresponding QoS CF-poll frame (in case of polled TXOP). On the other hand, the multiple consecutive frame transmissions during a TXOP can enhance the communication efficiency.

The readers, who are interested in the performance of the 802.11e WLAN, are referred to [13]~[15]. Even

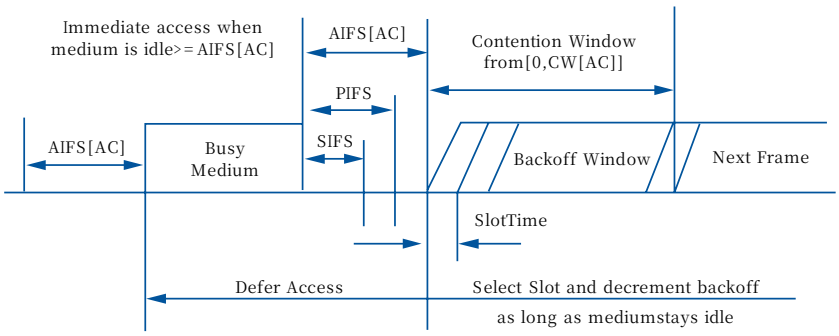


Figure 8. IEEE 802.11e EDCA channel access

though most of the existing 802.11e papers are based on some old versions of the draft, and hence the exact numbers may not be true, the general tendencies are still valid. The problems of the legacy 802.11 MAC and how the emerging 802.11e fixes those problems are discussed in [14],[15]. We briefly explain how the 802.11e HCF works below.

1. HCF Contention-Based Channel Access (EDCA)

The EDCA is designed to provide differentiated, distributed channel accesses for frames with 8 different user priorities (UPs) (from 0 to 7) by enhancing the DCF. Each frame from the higher layer arrives at the MAC along with a specific user priority value. Each QoS data frame also carries its user priority value in the MAC frame header. An 802.11e STA shall implement four channel access functions, where a channel access function is an enhanced variant of the DCF, as shown in Figure 9. Each frame arriving at the MAC with a user priority is mapped into an access category (AC) as shown in Table 1, where a channel access function is used for each AC. Note the relative priority of UP 0 is placed between 2 and 3. This relative priority is rooted from IEEE 802.1d bridge specification [11].

Table 1. User priofity to access category mappings

Priority	User Priority (UP)	Access Category (AC)	Designation (Informative)
Lowest	1	AC_BK	Background
	2	AC_BK	Background
·	0	AC_BE	Best Effort
·	3	AC_VI	Video
·	4	AC_VI	Video
	5	AC_VI	Video
	6	AC_VO	Voice
Highest	7	AC_VO	Voice

Basically, a channel access function uses AIFS[AC], CWmin[AC], and CWmax[AC] instead of DIFS, CWmin, and CWmax, of the DCF, respectively, for the contention to transmit a frame belonging to access category AC. AIFS[AC] is determined by

$$AIFS[AC] = SIFS + AIFSN[AC] \cdot SlotTime,$$

where AIFSN[AC] is an integer greater than one. Figure 8 shows the timing diagram of the EDCA channel access. One big difference between the DCF

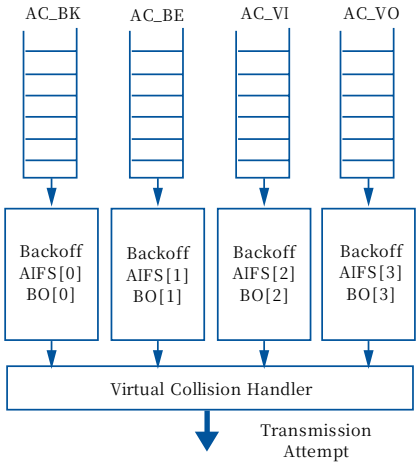


Figure 9. Four channel access functions for EDCA

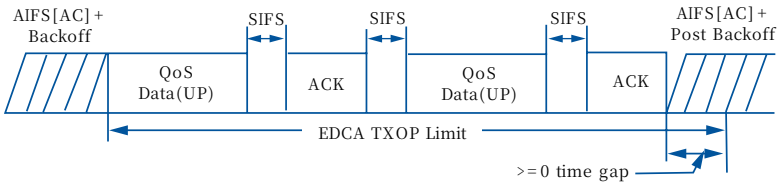


Figure 10. EDCA TXOP operation timing structure

and EDCA in terms of the backoff countdown rule is as follows: the first countdown occurs at the end of the AIFS[AC] interval. Moreover, at the end of each idle slot interval, either a backoff countdown or a frame transmission occurs, but not both. Note that according to the legacy DCF, a STA countdown a backoff counter, and if the counter becomes zero, it transmits a frame at that moment.

Figure 9 shows the 802.11e MAC with four channel access functions, where each functions behaves as a single enhanced DCF contending entity, where each queue has its own AIFS and maintains its own backoff counter. When there is more than one channel access function finishing the backoff at the same time, the collision is handled in a virtual manner. That is, the highest priority frame among the colliding frames is chosen and transmitted, and the others perform a backoff with increased CW values.

The values of AIFS [AC], CWmin [AC], and CWmax [AC], which are referred to as the EDCA parameters, are announced by the AP via beacon frames. The AP can adapt these parameters dynamically depending on network conditions even though frequent adaptation is not desired due to the network stability. Basically, the smaller AIFS [AC] and CWmin [AC], the shorter the channel access delay for user priority UP, and hence the more bandwidth share for a given traffic condition. These parameters can be used in order to differentiate the channel access among different user priority (or AC more accurately speaking) traffic.

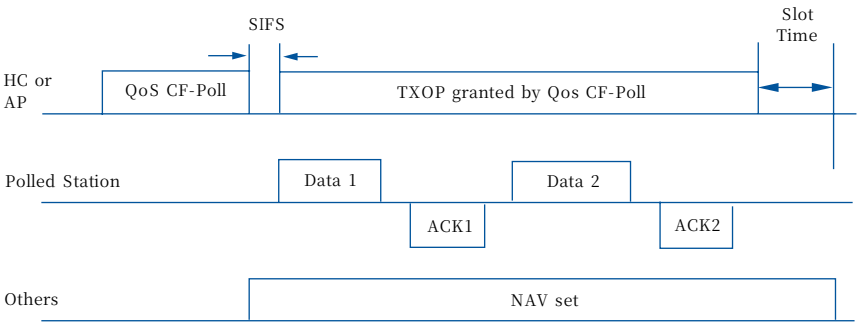


Figure 11. Polled TXOP timing

As mentioned above, the IEEE 802.11e defines a TXOP as the interval of time when a particular STA has the right to initiate transmissions. Along with the EDCA parameters of AIFS [AC], CWmin [AC], and CWmax [AP], the AP also determines and announces the limit of an EDCA TXOP interval for each AC, i.e., TXOPLimit [AC], in beacon frames. During an EDCA TXOP, a STA is allowed to transmit multiple MSDUs of the same AC with a SIFS time gap between an ACK and the subsequent frame transmission.

Figure 10 shows the transmission of two QoS data frames of user priority UP during an EDCA TXOP, where the whole transmission time for two data and ACK frames is less than the EDCA TXOP limit determined by the AP. As multiple MSDU transmission honors the TXOP limit, the worst-case delay performance is not be affected by allowing the EDCA TXOP operation.

2. HCF Controlled Channel Access (HCCA)

If the EDCA is for the prioritized QoS, which supports differentiated channel accesses to 8 different user priority traffic, the HCCA is mainly for the parameterized QoS, which provides the QoS based on the contract between the AP and the corresponding QSTA(s). Before commencing the transfer of any frame requiring the parameterized QoS, a virtual connection, called traffic stream, is established first. A traffic stream could be either uplink, or downlink, or directlink, which are QSTA-to-AP, and AP-to-QSTA, and QSTA-to-QSTA, respectively. In order to set up a traffic stream, a set of traffic characteristics (such as nominal MSDU size, mean data rate, and maximum burst size) and QoS requirement parameters (such as delay bound) are exchanged and negotiated between the AP and the corresponding QSTA(s), and the traffic stream should be admitted by the AP. Accordingly, the AP should implement an admission control algorithm to determine whether to admit a specific traffic stream into its BSS or not.

Once a traffic stream is set up, the hybrid coordinator (HC) co-located within the AP endeavors to provide the contracted QoS by allocating the required bandwidth to the traffic stream using the HCCA. Under the HCCA, the HC has the full control over the medium during a CFP, and during a CP it can also grab the medium after a PIFS idle time whenever it wants. The channel grabbing is done by initiating its downlink frame transfer or by transmitting a polling frame, i.e., QoS CF-poll frame, in order to grant a polled TXOP to a QSTA.

By receiving a QoS CF-poll, the polled STA, called a TXOP holder, assumes the control over the medium up to the TXOP limit specified in the QoS CF-poll frame, and transmits multiple MSDUs during the limited time, where the transmitted frames and their transmission order are determined by the TXOP holder according to its scheduling algorithm. All the other STAs, which receive the QoS CF-poll, set the NAV with the TXOP limit plus an extra slot time such that they will not contend for the medium during that time period. The timing diagram of a polled TXOP operation is shown in Figure 11.

As is clear from the above explanation, in order to meet the contracted QoS requirements, the HC needs to schedule its downlink frame transmissions as well as the QoS CF-poll frame transmissions properly. Since the wireless medium involves the time-varying and location-dependent channel conditions, developing a good scheduling algorithm is a challenging problem. Note that an intelligent scheduling algorithm can result in better system performance, e.g., not violating the QoS contract, while admitting more traffic streams.

3. Other Features of 802.11e MAC

There are some more features defined as part of the 802.11e MAC. They are not directly related to the QoS provisioning, but can increase the efficiency of the 802.11 WLAN. We just briefly summarize a couple of such new features here.

The first one is the block acknowledgement (BlockAck) mechanism, which allows a group of QoS data frames to be transmitted, each separated by a SIFS period, and then a single BlockAck frame acknowledges the group of QoS data frames. The legacy MAC is based on a stop-and-wait automatic retransmission request (ARQ) scheme, which involves a lot of overheads due to the immediate ACK transmissions. The newly-introduced Block Ack allows the selective-repeat ARQ, and can enhance the system efficiency significantly.

The other one is the Direct Link Protocol (DLP). The legacy MAC does not allow STAs within the same infrastructure BSS to transmit frames to each other directly, and instead the AP should relay the frames always. For certain applications, e.g., the bandwidth-intensive video streaming within a home, this limitation result in using the precious wireless bandwidth twice, and hence the 802.11e defines the mechanism to support the direct QSTA-to-QSTA transfer. Basically, before commencing any direct frame transfer, a direct link is set up between two QSTAs via the DLP, which involves the exchange of management frames between two QSTAs through the AP.

IV. IEEE 802.11F FOR INTER-ACCESS POINT PROTOCOL (IAPP)

As explained in Section II, within an infrastructure BSS, a STA is associated with an AP, and this STA communicates with any other nodes through this AP. A WLAN can be composed of multiple APs. In the 802.11 terms, the system, which connects the multiple APs, is called a distribution system (DS), and a set of BSSs and the DS connecting these BSSs is called extended service set (ESS). In today's WLANs, the DS is typically constructed with the Ethernet. One can easily imagine that this kind of WLAN structure is similar to that of the wide-area cellular systems, where multiple base STAs are connected via the wired links, and each base station serves an area called a *cell*.

A key function in this multi-AP WLAN is the handoff or roaming, i.e., a STA can switch from an AP

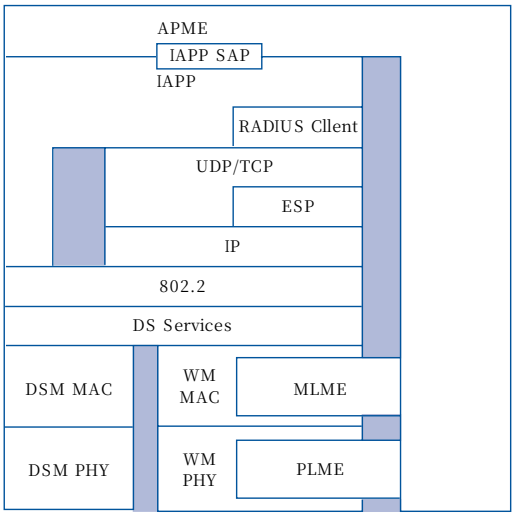


Figure 12. AP architecture with IAPP

to another as it moves. The handoff involves the communication between the APs, which relies on the DS. While the 802.11 defines the concept of the DS, it does not define how to implement the DS. The reasons behind include (1) the DS involves the protocols belonging to the above MAC, which is out of scope of the 802.11, dealing with the MAC and PHY only, and (2) it could be desirable to have the flexibility for the DS construction. Note that the DS can be constructed with any network link, e.g., even with the WLAN link, which is referred to as wireless distribution system (WDS).

However, the lack of the standardized DS construction caused APs from different vendors not to interoperate, especially, in the context of the handoff support. In the 802.11 WLAN (or more specifically, ESS), a STA should have only a single association, i.e., the association with a single AP. However, the enforcement of this restriction is unlikely to be achieved due to the lack of the communication among the APs within the ESS.

The 802.11f is a recommended practice, which specifies the information to be exchanged between APs amongst themselves and higher layer management entities to support the 802.11 DS functions. According to the IEEE standards terms, the recommended practice is defined as a document, in which procedures and positions preferred by the IEEE are presented. On the other hand, the standards like 802.11-1999 are defined as documents with mandatory requirements.[3] It should be noted that the 802.11f does not define anything related to the STA operation for the handoff. The 802.11 MAC management defines the AP scanning of the STAs and reassociation procedures for the basic handoff support as discussed in Section II.D. The readers, who are interested in the 802.11 handoff issues, are referred to other literature in [18]~[21].

3) Within a standard specification document, both mandatory requirements and recommended practice can exist. Mandatory requirements are generally characterized by use of the verb "shall," whereas recommended practices normally use the word "should."

1. Inter-AP Communication

The IAPP uses TCP/IP or UDP/IP to carry IAPP packets between APs, as well as describing the use of Remote Authentication Dial In User Service (RADIUS) protocol [27], so that APs may obtain information about one another. A proactive caching mechanism is also defined in order to provide faster roaming by sending the STA context to neighboring APs before the actual handoff event.

Figure 12 shows the architecture of the AP with IAPP. The AP management entity (APME) is a function that is external to the IAPP, and typically is the main operational program of the AP, implementing an AP manufacturer's proprietary features and algorithms. The 802.11-1999 defines an entity called STA management entity (SME), and the APME of the AP incorporates the SME functions. As shown in the figure, the APME can manage/control the IAPP, 802.11 MAC, and 802.11 PHY via the IAPP Service Access Point (SAP), MAC Layer Management Entity (MLME) SAP, and PHY Layer Management Entity (PLME) SAP, respectively.

Some functions of the IAPP rely on the RADIUS protocol for the correct and secure operation. In particular, the IAPP entity, i.e., the AP, should be able to find and use a RADIUS server to look up the IP addresses of other APs in the ESS when given the BSSIDs of those APs, and to obtain security information to protect the content of certain IAPP packets. Actually, the RADIUS server must provide extensions for IAPP-specific operations, and these operations are currently being defined by Internet Engineering Task Force (IETF) [28].

The IAPP sSupports (1) DDS services, (2) address mapping between AP's MAC and IP addresses, (3) forrmation of DS, (4) maintenance of DS, (5) enforcement of a single association of a STA at a given time, and (6) transfer of STA context information between APs.

2. IAPP Operations

There are basically three different IAPP operations: (1) STA ADD operation: (2) STA MOVE operation; and (3) proactive caching. These operations are briefly explained below.

First, the STA ADD operation is triggered when a STA is newly associated with an AP. When a STA is associated, the AP transmits two packets to the DS or the wired infrastructure: layer-2 update frame and IAPP ADD-notify packet. The layer-2 update frame is addressed at the broadcast address, and upon the reception of this frame, any layer-2 bridge devices, e.g., Ethernet switches connecting multiple APs within the ESS, update the routing table for the associating STA according to the IEEE 802.1d bridge table self-learning procedure [11]. The IAPP ADD-notify packet is an IP packet with a destination IP address of the IAPP IP multicast address so that any receiving APs within the ESS remove a stale association information with the associating STA.

Second, the STA MOVE operation is triggered when a STA reassociates with an AP, which happens when this STA hands off from an AP to another AP. The STA, which is handing off from an AP, transmits a reassociation request management frame to the new AP, where the reassocaition request frame includes the MAC address of the old AP. The new AP transmits two packets in this case as well: layer-2 update frame and IAPP MOVE-notify packet. The IAPP MOVE-notify packet is transmitted to the old AP, which in turn transmits an IAPP MOVE-response packet. The response packet carries the context block[4] for the STA's

association from the old AP to the new AP. Since the reassociation request frame from the STA contains the old AP's MAC address only, the new AP needs to look up the IP address of the old AP via the help by a RADIUS server within the ESS. The purpose of the layer-2 update frame is the same as with the STA ADD operation case. One important fact is that the layer-2 update frame is broadcasted only after the IAPP MOVE-response packet is received from the old AP, as the final step of the hand-off support procedure.

Third, the proactive caching is triggered when a STA (re)associate with an AP or the context of the STA changes. Basically, when the proactive caching is triggered by the APME of an AP, the AP (or the AP 's IAPP entity more specifically) transmits the IAPP CACHE-notify packets to its neighboring APs. The notify packet includes the context of the corresponding STA. This proactive caching can significant reduce the hand-off delay by broadcasting the layer-2 update frame without waiting for the IAPP MOVE-response packet upon a reassociation (or handoff) of a STA when the new AP has the context of the handing-off STA, where the context was received from the old AP via the IAPP CACHE-notify packet earlier. One may question about how to know the neighboring APs. This can be achieved via the dynamic learning. That is, an AP can learn that another AP is its neighbor when a STA hands off from this AP to itself. The neighboring AP list can grow over time as more and more STAs move around across the ESS. On the other hand, the network administrator can of course pre-configure the neighboring AP list.

4) The 802.11f does not define what the context block could contain. The examples of the context include security and accounting information of the corresponding stationSTA.

V. IEEE 802.11H FOR SPECTRUM AND TRANSMIT POWER MANAGEMENT [8]

The 802.11h defines two mechanisms on top of the 802.11-1999 MAC and the 802.11a PHY, namely, dynamic frequency selection (DFS) and transmit power control (TPC).

In case of the 5GHz 802.11a PHY, a BSS occupies a channel of 20MHz. Today, in the US, there are 12 channels available for the 802.11a [3]. On the other hand, the 802.11h defines 19 channels for the operation in Europe. The DFS is used to switch the operational frequency channel of a BSS to another dynamically. There can be many reasons why a BSS may want to change its operational frequency channel. One interesting example is when the current channel condition is too bad due to the interference from the neighboring devices. In this context, the DFS can be used in order to enhance the QoS of the WLAN.

Most of today's 802.11 devices use a fixed transmit power for the frame transmissions. Note that the dynamic transmit power control is very critical in the popular code-division multiple access (CDMA) systems due to the near-far problem. On the other hand, the TPC is a desirable feature than a necessary feature. However, the TPC in the WLAN can be useful in many different ways: (1) to meet the regulatory requirements as discussed below, (2) to control the range of a BSS, (3) to control the inter-BSS interference, and (4) to minimize the energy consumption to save the battery energy [16],[17].

As the title found in [8] indicates, the 802.11h has been developed for the 5GHz in Europe. Many countries in Europe require that any WLAN devices have these two functions in order to co-exist with the primary users at the 5GHz bands, namely, the satellite

and radar systems [31]. For example, the WLAN devices are required to switch its operational frequency channel to another channel once a radar signal is detected in the operational frequency channel. On the other hand, when a satellite signal is detected, the WLAN devices are allowed to use the transmit power up to the regulatory maximum level minus 3dB while normally they can transmit at up to the regulatory maximum. Even though the 802.11h has been developed for the European regulation, it can be apparently used in any other countries for multiple purposes.

Note that both DFS and TPC involve implementation-dependent algorithms. For example, a TPC algorithm is needed in order to determine the transmit power level of a frame transfer. Basically, the 802.11h defines the mechanisms/protocols to enable a right decision of the power level, not the implementation itself. We briefly review the mechanisms/protocols defined by the 802.11h below. It should be noted that there is virtually no change in terms of the channel access functions. That is, the 802.11 DCF and/or PCF are used to transmit the new management frames as part of the 802.11h.

1. Dynamic Frequency Selection (DFS)

In the infrastructure BSS, it is the AP, which determines when and which channel to switch to. For this purpose, the AP should monitor the status of the current and other frequency channels. For this purpose, the AP is allowed to request other STAs to measure the current and other channels. After the channel status measurement, the requested STA can reports the measurement results. There are basically three different measurement types:

- Basic type includes whether the followings were detected in the measured channel, namely, another BSS, a non-802.11 OFDM signal, an unidentified signal, and a radar signal;
- Clear channel assessment (CCA) type measures the fractional duration of the channel busy periods during the total measurement interval; and
- Received power indication (RPI) histogram type measures the histogram of the quantized measures of the received energy power levels as seen at the antenna connector during the measurement interval.

Based on its own measurement as well as the reports from the associated STAs, the AP continues to monitor the channel status so that the channel switch can be conducted in a proper instance.

The channel switch occurs immediately before a TBTT, which the AP has specified, so that a normal communication operation can be conducted beginning the following beacon interval at the new operational frequency channel. Note that the beacon frames are transmitted periodically.[5] The channel quieting operation is also defined since the European regulation requires the STA to become silent (or not transmitting any) once a radar system is detected in the operational frequency channel.

Finally, it should be noted that a separate protocol is defined for the DFS operation in the independent BSS, where no AP exists. Basically, in such a network, the STA, which initiated the BSS, is called the *DFS owner*, and takes the responsibility of the channel status collection as well as the channel switch decision. How

5) The beacon transmission can be delayed due to the contention from the stations under the DCF rule. However, the target beacon transmission times at least repeat periodically.

to elect a new DFS owner when the old DFS owner disappears (due to the switch off or so) is also handled.

2. Transmit Power Control (TPC)

Basically, there are two main functions defined. First, the AP specifies the regulatory and local maximum power level as part of the beacon, where the local maximum specifies the actual maximum power level used within its BSS. The local maximum power should be smaller than or equal to the regulatory maximum. The STAs in the BSS can use the transmit power smaller than or equal to the local maximum value.

Second, in order to determine the proper (or best) transmit power level for a given frame, the transmitting STA needs to know the link condition between the receiving STA and itself. The 802.11h defines a mechanism to achieve it. A STA can transmit a management frame called TPC request frame to another STA when it desires. Upon receiving the TPC request frame, the receiving STA determines the link margin between the transmitting STA and itself, then responds with a TPC response frame, which includes the link margin as well as the transmit power level of the response frame. The link margin is defined by the ratio of the received signal power to the minimum desired by the receiving STA. The transmitting STA can utilize the received link margin and power level information in order to determine the best transmit power level in the future. The beacon from the AP also includes the transmit power level used for the beacon transmission, which can be used by the associated STAs to monitor the channel condition between the AP and hemselves.

VI. IEEE 802.11I FOR SECURITY ENHANCEMENT [9]

It turned out that the existing security mechanisms of the 802.11, i.e., authentication and WEP, are basically useless. The basic problems include:

- Cryptographic weakness of RC4
- BSS-wide security key usage, i.e., all STAs in a BSS can use the same key
- One-way authentication, i.e., STA is authenticated by an AP, but not the other way around
- Reuse of the IV by multiple frames
- Absence of Message Integrity Check (MIC) on frames, i.e., ICV based on CRC-32 is currently used.

The security flaws of the current 802.11 are discussed in detail in [22]~[24]. The emerging 802.11i is intended to address these security holes.

The IEEE 802.11i defines the Robust Security Network Associations (RSNA), which is established between two STAs, i.e., a STA and an AP in an infrastructure BSS or a pair of STAs in an IBSS, via the authentication/association using the 4-Way Handshake. A RSNA depends on IEEE 802.1X [12] to transport its authentication services and to deliver key management services. Therefore, all STAs and APs in an RSNA contain an 802.1X entity that handles these services, and the 802.11i defines how an RSNA utilizes the 802.1X to access these services.

The RSNA defines a number of security features on top of the WEP and IEEE 802.11 authentication including:

- Enhanced mutual authentication mechanisms for both APs and STAs
- Key management algorithms

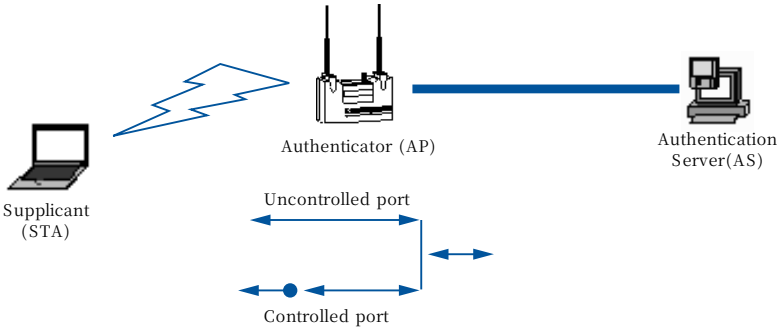


Figure 13. IEEE 802.1X architecture for 802.11i WLAN [23]

- Cryptographic key establishment
- An enhanced data encapsulation mechanism, called Counter mode with CBC-MAC[6] Protocol (CCMP) and, optionally, Temporal Key Integrity Protocol (TKIP)

We consider the ESS security in this section even though the 802.11i addresses the security mechanism in IBSSs as well since the ESSs are practically more important than the IBSSs.

1. RSNA and IEEE 802.1X

An RSNA relies on IEEE 802.1X [12] to provide authentication and key management services, where the 802.1X architecture is shown in. In the 802.1X terms, non-AP STA is the supplicant, and the AP is the authenticator. The Authentication Server (AS) is an entity residing in the wired infrastructure (or possibly the AP itself), which participates in the authentication (See Figure 13).

An 802.1X port is present on any STA in an RSNA, where the port determines when to allow general data traffic across an IEEE 802.11 link. That is, general data traffic between a STA and its AP is blocked by the controlled port until the 802.1 X authentication procedures complete successfully. RSNA depends upon the use of an Extensible Authentication Protocol (EAP) method that supports mutual authentication between the AS and the STA, not just authentication of the STA to an AP. The EAP authentication frames are transmitted in IEEE 802.11 data frames, rather than the 802.11 management frames, and passed via the uncontrolled port of the 802.1X authenticator, i.e., the AP.

2. RSNA Establishment

In an ESS, a STA establishes an RSNA using either IEEE 802.1X authentication and key management or using a pre-shared key (PSK). When the 802.1X is used, the STA establishes an RSNA via the following procedures:

1) It identifies the AP as RSNA-capable via AP scanning

6) CBC-MAC stands for Cipher-Block Chaining Message Authentication Code.

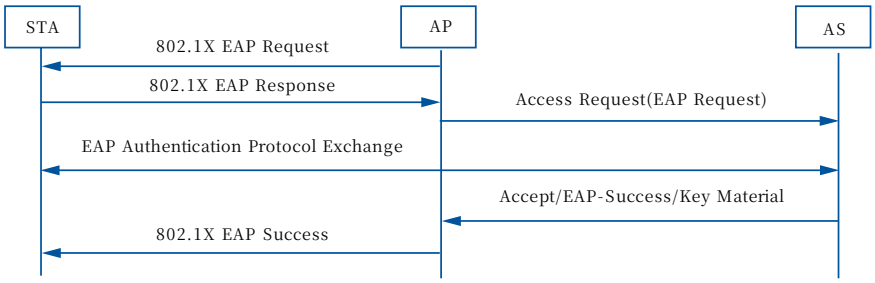


Figure 14. IEEE 802.1X EAP Authentication

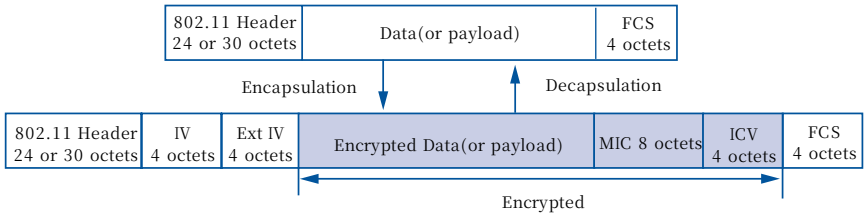


Figure 15. Expanded TKIP MPDU

2) It uses Open System Authentication (see Section II.C)
3) It negotiates cipher suites (e.g., either TKIP or CCMP) during association
4) It uses IEEE 802.1X to authenticate
5) It establishes temporal keys by executing a key exchange algorithm
6) It uses the agreed upon temporal keys and cipher suites to protect the link

Note that the Shared Key Authentication is deprecated as part of the 802.11i since the 802.11i relies on the 802.1X for the authentication after the association. Figure 14 illustrates the IEEE 802.1X EAP authentication procedure corresponding to step 4) above. The STA and AS authenticate each other (e.g., EAP-TLS [26]) and generates a pairwise master key (PMK) to seed the exchange in step 5) above. The PMK is sent from the AS to the authenticator (i.e., the AP) via a secure channel. When the PSK is used instead of the 802.1X, the step 4) above is skipped, and the PSK is used as the PMK.

Now, to establish temporal keys to be used for the frame encryption, the AP initiates a 4-Way Handshake utilizing EAP over LANs (EAPOL)-Key messages. Basically, four messages are exchanged between the STA and the AP in order to establish both pairwise transient key (PTK) for the unicast frame encryption and group transient key (GTK) for the broadcast/multicast frame encryption. The PTK is derived from the PMK. Upon completion of the 4-Way Handshake, the AP changes the state of the IEEE 802.1X access port, opening the controlled port to permit general data traffic to pass onto the DS. When the AP changes the GTK later, it sends the new GTK to the STA using the Group Key Handshake.

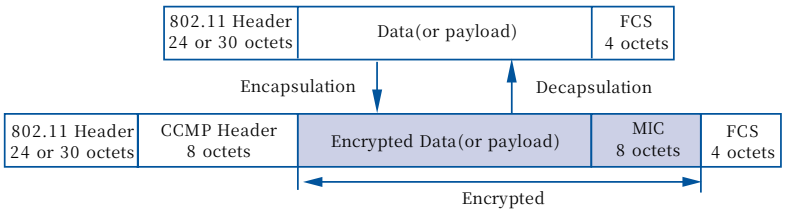


Figure 16. Expanded CCMP MPDU

3. Cryptographic Algorithms

The 802.11i defines two cryptographic algorithms on top of the WEP algorithm defined in the 802.11-1999, namely, optional TKIP and mandatory CCMP. The TKIP is based on the RC4 algorithm as the WEP is, and the CCMP is based on the Advanced Encryption Standard (AES).

The TKIP is a cipher suite enhancing the WEP protocol on pre-RSNA (i.e., legacy) hardware, and it uses WEP with the following modifications:

- A transmitter calculates a keyed cryptographic message integrity code (MIC), called Michael, over the frame source and destination addresses, the priority, and the plaintext data. Any frames with invalid MICs, i.e., possibly affected by forgery attacks, are discarded at the receiver.
- TKIP uses a packet TKIP sequence counter (TSC) to sequence the frames it sends, and this counter is encoded as a WEP IV and Extended IV. Any frames received out of order, i.e., possibly affected by replay attacks, are discarded at the receiver.
- TKIP uses a cryptographic mixing function to combine a temporal key, transmitter address, and the TSC into the WEP seed. This mixing function is designed to defeat weak-key attacks against the WEP key.

Figure 15 depicts the layout of the encrypted frame when using TKIP. The TSC occupies 6 octets across IV and Extended IV fields.

On the other hand, the CCMP employs the AES encryption algorithm using the CCM mode of operation. The CCM mode combines Counter Mode (CTR) for confidentiality and Cipher Block Chaining Message Authentication Code (CBC-MAC) for authentication and integrity. The CCM protects the integrity of both frame MPDU payload and selected portions of the MAC header. All AES processing used within CCMP uses AES with a 128 bit key and a 128 bit block size. Note that AES is a block cipher different from RC4, a stream cipher, used in WEP and TKIP. CCM requires a fresh temporal key for every session to ensure the security guarantees.

Figure 16 depicts the frame format using CCMP. The CCMP header includes the Packet Number (PN) and Key ID. The PN is basically the same as TSC defined for TKIP.

VII. TWO NEWLY-STARTED STANDARDIZATIONS

In this section, we briefly introduce two newly-started standardization activities, namely, IEEE 802.11k

for radio resource measurement and IEEE 802.11n for higher throughput.

1. IEEE 802.11k for Radio Resource Measurement

Task Group K (TGk) was established early 2003 within the 802.11 WG in order to define radio resource measurement enhancements to provide mechanisms to higher layers for radio and network measurements. Based on the current draft [10], the group is defining the followings:

- Addition of more MIB values on top of what the 802.11-1999 defined for more intelligent network management
- Defining various radio measurement types such received signal power, noise, hidden nodes and neighboring APs

Various types of radio measurements are expected to be used to enhance the WLAN performance. For example, the neighboring AP list measurement and announcement by the AP can aid in reducing the handoff delay.

2. IEEE 802.11n for Higher Throughput

Task Group N (TGn) was established in mid 2003 within the 802.11 WG in order to achieve a higher throughput by revising both the PHY and MAC of the 802.11. The group is basically targeting at a throughput of at least 100Mbps measured at the MAC SAP. Since the 802.11a and 802.11g WLANs achieve about 25 Mbps maximum throughput in practice, this represents at least 4 times faster WLAN.

It is too early to predict how the 802.11n will look like. However, the 802.11n PHY is expected to increase the PHY transmission rate by using multiple antennas or combining multiple frequency channels (of 20MHz in case of 5GHz bands). The MAC should be enhanced in order to reduce the MAC overheads. It is well known that the 802.11 MAC introduces remarkable overheads due to the backoff and ACK transmissions. It is the main reason why the maximum throughput of the 802.11a and 802.11g is under the half of the maximum PHY transmission rate, i.e., 54Mbps. The 802.11e block ACK is expected to enhance the MAC efficiency. Other techniques such as the frame aggregation [30] can also be also possible options.

VIII. CONCLUDING REMARKS

Recently, the IEEE 802.11 WLAN has become very successful in the market as the prevailing technology for the (indoor) broadband wireless networking. Along with its success, the demand on the evolution of the technology became evident. During the last few years, remarkable efforts to enhance the current 802.11 have been made.

In this paper, we have overviewed the emerging protocols of the 802.11 WLAN for the MAC and above, namely, 802.11e for QoS, 802.11f for IAPP, 802.11h for spectrum management, and 802.11i for security enhancement. We also briefly discussed newly-initiated standardization efforts for the 802.11k for radio resource measurements and 802.11n for enhancements for higher throughput. It is our belief that the usage of the 802.11 WLANs will be growing faster and more widely in the future.

[REFERENCES]

[1] IEEE Working Group (WG), http://www.ieee802.org/11, online link.

[2] IEEE, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Reference number ISO/IEC 8802-11:1999(E), IEEE Std 802.11, 1999 edition, 1999.

[3] IEEE, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5GHZ Band, IEEE Std. 802.11a-1999, 1999.

[4] IEEE, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-speed Physical Layer Extension in the 2.4 GHz Band, IEEE Std. 802.11b-1999, 1999.

[5] IEEE 802.11 WG, Draft Supplement to Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS), IEEE 802.11e/D5.0, Jul. 2003.

[6] IEEE 802.11 WG, Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution System Supporting IEEE 802.11 Operation, IEEE 802.11f/D5.0, Jan. 2003.

[7] IEEE 802.11 WG, Draft Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher-Speed Physical Layer Extension in the 2.4GHz Band, IEEE 802.11g/D8.2, Apr. 2003.

[8] IEEE 802.11 WG, Draft Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Spectrum and Transmit Power Management extensions in the 5GHz band in Europe, IEEE 802.11h/D3.3.4, Feb. 2003.

[9] IEEE 802.11 WG, Draft Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements, IEEE 802.11i/D5.0, Jul. 2003.

[10] IEEE 802.11 WG, Draft Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Specification for Radio Resource Measurement, IEEE WG 802.11k/D0.4, Jul. 2003.

[11] IEEE, Part 3: Media Access Control (MAC) bridges, ANSI/IEEE Std. 802.1D, IEEE 802.1d-1998, 1998 edition, 1998.

[12] IEEE Std. 802.1X, Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control, Jun. 14, 2001.

[13] Stefan Mangold, Sunghyun Choi, Guido R. Hiertz, Ole Klein, and Bernhard Walke, "Analysis of IEEE 802.11e for QoS Support in Wireless LANs," accepted to *IEEE Wireless Communications Magazine*, Special Issue on Evolution of Wireless LANs and PANs, Jul. 2003.

[14] Sunghyun Choi, Javier del Prado, Sai Shankar N, and Stefan Mangold, "IEEE 802.11e Contention-Based Channel Access (EDCF) Performance Evaluation," in *Proc. IEEE ICC '03*, Anchorage, Alaska, USA, May 2003.

[15] Sunghyun Choi, "Emerging IEEE 802.11e WLAN for Quality-of-Service (QoS) Provisioning," *SK Telecom Telecommunications Review*, Vol. 12, No. 6, Dec. 2002, pp. 894-906.

[16] Daji Qiao, Sunghyun Choi, Amit Jain, and Kang G. Shin, "MiSer: An Optimal Low-Energy Transmission Strategy for IEEE 802.11a/h," *in Proc. ACM MobiCom'03*, San Diego, CA, 14-19, 2003.

[17] Daji Qiao, Sunghyun Choi, Amjad Soomro, and Kang G. Shin, "Energy-Efficient PCF Operation of IEEE 802.11a WLAN via Transmit Power Control," *Elsevier Computer Networks (ComNet)*, Vol. 42,

No. 1, May 2003, pp. 39-54.

[18] Marc Portoles, Zhun Zhong, Sunghyun Choi, and Chun-Ting Chou, "IEEE 802.11 Link-Layer Forwarding For Smooth Handoff," *in Proc. IEEE PIMRC'03*, Beijing, China, Sep. 7-10, 2003.

[19] Marc Portoles, Zhun Zhong, and Sunghyun Choi, "IEEE 802.11 Downlink Traffic Shaping Scheme For Multi-User Service Enhancement," *in Proc. IEEE PIMRC'03*, Beijing, China, Sep. 7-10, 2003.

[20] Sangheon Pack and Yanghee Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN based on IEEE 802.1x Model, "in *Proc. IFIP TC6 Personal Wireless Communications (PWC2002),* Singapore, Oct. 2002.

[21] Sangheon Pack and Yanghee Choi, "Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN," in *Proc. IEEE Networks '2002 (Jointly with ICN'2002 and ICWLHN'2002)*, Atlanta, USA, Aug. 2002.

[22] W. A. Arbaugh, N. Shankar, J. Wang, and K. Zhang, "Your 802.11 network has no clothes," *IEEE Wireless Communications Magazine*, Dec. 2002.

[23] Jesse Walker, "Overview of 802.11 Security," http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3-Overview-of-802-11-Security.ppt, Mar. 2001.

[24] Nikita Borisov, Ian Goldberg, and David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," in *Proc. ACM MOBICOM'01*, Rome, Italy, Jul. 2001.

[25] RFC 2284, PPP Extensible Authentication Protocol (EAP), Mar. 1998.

[26] RFC 2716, PPP EAP TLS Authentication Protocol, Oct. 1999.

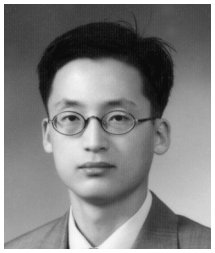
[27] RFC 2865, Remote Authentication Dial In User Service (RADIUS), Jun. 2000.

[28] RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, Dec. 2002.

[29] Robert Moskowitz, RADIUS Client Kickstart, draft-moskowitz-radius-client-kickstart-00.txt.

[30] Youngsoo Kim, Sunghyun Choi, Hyosun Hwang, and Kyunghun Jang, "Throughput Enhancement via Frame Aggregation - A Sequel," IEEE 802.11-03/567r0, http://grouper.ieee.org/groups/802/11/Documents/index.html, Jul. 2003.

[31] ERC/DEC/(99)23, ERC Decision of 29 November 1999 on the harmonized frequency bands to be designated for the introduction of High Performance Radio Local Area Networks (HIPERLANs).



최 성 현 Sunghyun Choi

Sunghyun Choi is an assistant professor at the School of Electrical Engineering, Seoul National University (SNU), Seoul, Korea. Before joining SNU in September 2002, he was with Philips Research USA, Briarcliff Manor, New York, USA as a Senior Member Research Staff and a project leader for three years. He received his B.S. (summa cum laude) and M.S. degrees in electrical engineering from Korea Advanced Institute of Science and Technology (KAIST) in 1992 and 1994, respectively, and received Ph.D. at the Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor in September, 1999.

His current research interests are in the area of wireless/mobile networks with emphasis on the QoS guarantee and adaptation, resource management, wireless LAN and PAN, next-generation mobile networks, data link layer protocols, and connection and mobility management. He authored/coauthored over 40 technical papers and book chapters in the areas of wireless/mobile networks and communications. He is currently serving on program committees of a number of leading wireless and networking conferences including IEEE INFOCOM, IEEE GLOBECOM, and IEEE VTC. He is also an active participant and contributor of the IEEE 802.11 WLAN standardization committee.

Dr. Choi was a recipient of the Korea Foundation for Advanced Studies Scholarship and the Korean Government Overseas Scholarship during 1997~1999 and 1994~1997, respectively.

• E-mail: schoi@snu.ac.kr
• Tel: +82-2-880-1753
• Fax: +82-2-877-1753