EE228a - Lecture 4 - Spring 2006 WiFi Operations

Scribed by Xiaoyi Tang (xiaoyi@eecs)

Abstract

This lecture covers the fundamentals of IEEE standards for wireless LAN, with emphasis on the physical layer and MAC.

I. References

References for this lecture include the following.

- 802.11 Wireless Networks: The Definitive Guide, M. Gast, O'Reilly 2002. Many drawings used in this lecture are from here.
- IEEE Std 802.11, 1999 Edition
- IEEE Std 802.11b-1999
- IEEE Std 802.11a-1999
- IEEE 802.11e-2005

II. Overview of Standards

Fig. 1 shows the IEEE 802 standards and their positions in the OSI model. As shown, 802.11 MAC is common to all 802.11 Physical Layer (PHY) standards. 802.11 PHY is split into Physical Layer Convergence Procedure (PLCP) and Physical Medium Dependent (PMD) sublayers.

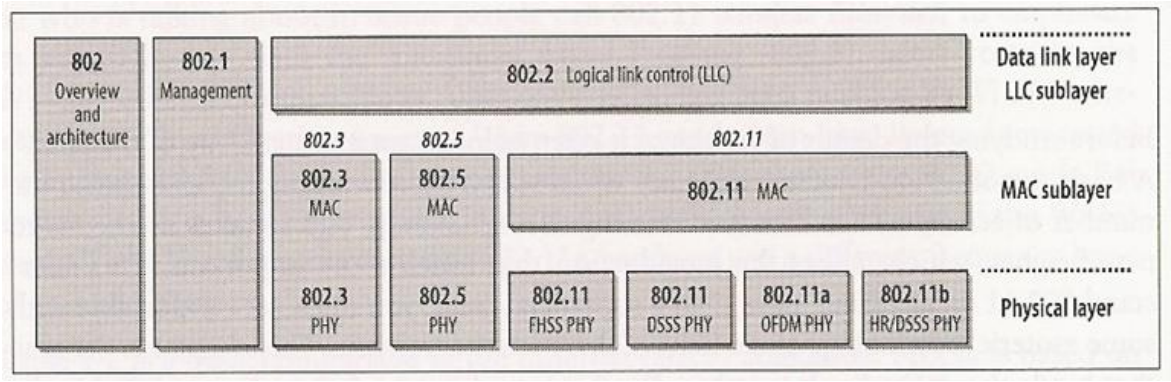

Fig. 1. IEEE 802 Standards & OSI Model.

There are several related standards.

- Bluetooth is originally intended for interconnecting computing, communication and entertainment devices.
- HIPERLAN is an European standard for wireless LANs.
- IEEE 802.16 is for broadband wireless MAN. 802.16-2004 addresses needs of fixed broadband wireless access replacing fibers, cables, DSL and etc. 802.16-2005, approved in Dec 2005, provides broadband access at vehicular speed.

Table I lists key 802.11 standards and their spectrum usage. The 2.4-2.5 GHz spectrum is referred to as S-Band

TABLE I
Key specifications of 802.11 standards

Key Standards	Max Rate	Spectrum (U.S.)	Year
802.11	2 Mbps	2.4 GHz	1997
802.11a	54 Mbps	5 GHz	1999
802.11b	11 Mbps	2.4 GHz	1999
802.11g	54 Mbps	2.4 GHz	2003
802.11e	N/A	N/A	2005

Industrial, Scientific, and Medical (ISM). Microwave ovens and some cordless phones operate in the same band. 802.11a uses Unlicensed National Information Infrastructure bands, including 5.15-5.25 GHz, 5.25-5.35 GHz, and 5.725-5.825 GHz. 802.11e provides QoS enhancements at the MAC layer, so there is no rate or spectrum specification. 802.11n has a draft specification approved in Jan 2006. It's based on multiple-input multiple-output (MIMO) technology which employs multiple antennas to increase throughput up to 600 Mbps. The MIMO technique embedded in 802.11n for which multi-path wireless diversity is provided can be introductorily understood by the originated paper, S. M. Alamouti, "A simple transmit diversity technique for wireless communications", IEEE Journal on Selected Areas in Communications, Vol.16, No.8, pp. 1451-1458, October 1998.

III. Basics

Basic service set (BSS) is a set of mobile stations. There are two types of BSS depending on how stations communicate.
Independent BSS In an independent BSS (also called ad-hoc BSS), stations communicate with each other directly without hops in a peer-to-peer fashion. It's possible that two stations in the same BSS cannot talk due to range limit.
Infrastructure BSS In an infrastructure BSS, stations communicate via a component named Access Point (AP), which is the centralized coordinator and could be the bottleneck. All packets must be sent twice, between sender and AP, and between AP and receiver.
Fig. 2 is an illustration of the two types of BSS.

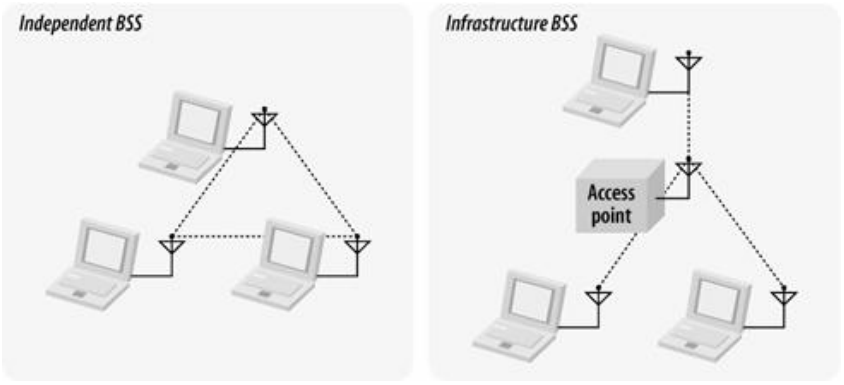

Fig. 2. Independent BSS and Infrastructure BSS.

Extended service set (ESS) is a set of infrastructure BSS. APs in an ESS communicate via distribution system (DS) to keep track of stations within an ESS and forward packets. Inter Access Point protocol (IAPP) is standardized by 802.11f-2003. Fig. 3 shows a diagram of an ESS.

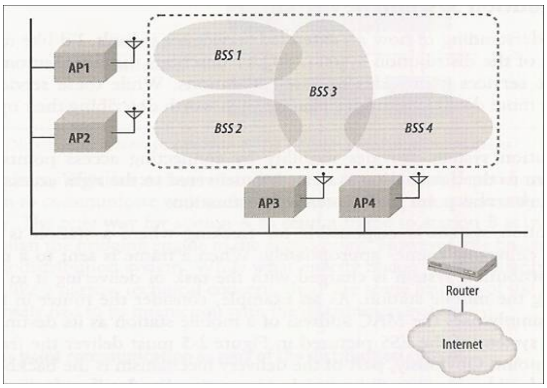

Fig. 3. Diagram of an extended service set.

Network services provided in a WLAN include the followings.
Distribution Communication through the DS.
Integration Integration with other WLAN or wired LAN.
Association A station must be associated with an AP before it can send data through the AP.
Reassociation Change association to a new AP. It's needed when a station moves around an ESS to a new BSS.
Disassociation Cancel an association. It can be initiated by an AP for various reasons (e.g. resource constraints) or a station if it leaves the network.
Authentication Provide security control to allow only authorized access.
Deauthentication Disable a previously authenticated station to access the network.

Privacy Offer data encryption based on the 802.11 Wired Equivalent Privacy (WEP) algorithm.
MAC Service Data Unit (MSDU) delivery Provide reliable delivery of data frames the MAC in one station to the MAC in one or more other stations.

WLAN provides seamless transition between two BSSs within an ESS. The IP address of a station doesn't change in this case. However, transitions are not supported between ESSs.

IV. Physical Layer

A. 802.11b

The physical layer of 802.11b is based on High Rate Direct-Sequence Spread Spectrum (HR/DSSS). It uses Complementary Code Keying (CCK) instead of Differential Quadrature Phase Shift Keying (DQPSK) used at lower rates. 4-bit (for 5.5 Mbps) or 8-bit (for 11 Mbps) symbols from MAC layer arrive at 1.375 million symbols per second. Each symbol is encoded using CCK code word, which provides both modulation and error correction. The code word is from the set $\{e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_4)}, -e^{j(\phi_1+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_3)}, e^{j(\phi_1+\phi_3)}, -e^{j(\phi_1+\phi_2)}, e^{j\phi_1}\}$ where $\phi_1, \phi_2, \phi_3, \phi_4$ are decided by symbol bits. It uses same channels as by the low rate DS. In US, channels 1-11 (with center frequencies at 2.412-2.462 GHz and 5 MHz distance) are available. For 11 Mbps, Channels 1, 6, and 11 give maximum number of channels with minimum interference. Fig. 4 illustrates the case. Fig. 5 shows the PLCP format.

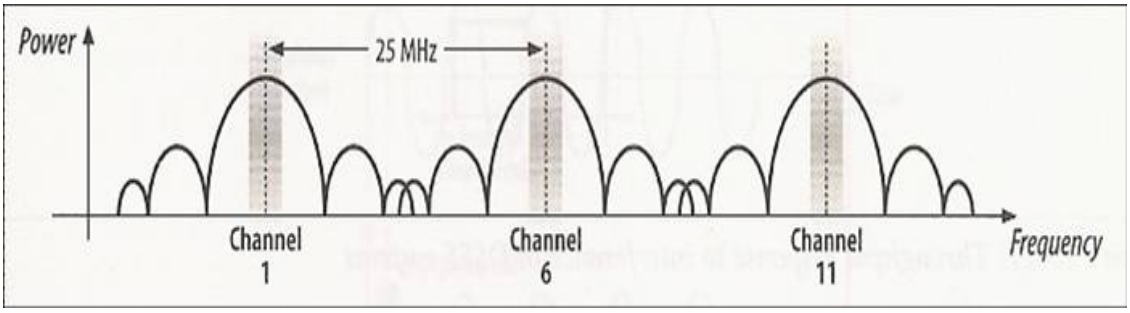

Fig. 4. Spectrum of 802.11b

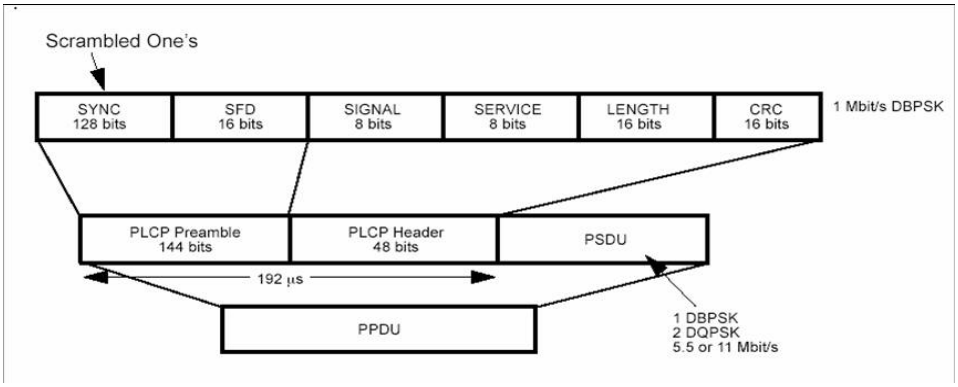

Fig. 5. 802.11b long PLCP format. Optional Short PLCP format is offered for better efficiency.

B. 802.11a

The physical layer of 802.11a is based on Orthogonal Frequency Division Multiplexing (OFDM). Fundamental OFDM work was done in 1960s, and a patent was issued in 1970. Basic idea is to use a number of subchannels in parallel for higher throughput. OFDM is similar to Frequency Division Multiplexing except it does not need guard bands. But it need guard times to minimize inter-symbol and inter-carrier interference. It relies on "orthogonality" in the frequency domain. Fig. 6 shows an example of OFDM spectrum.

It remains to be seen if 802.11a will be a success because there are still unanswered questions. For example, is denser access point deployment needed due to higher path loss? Will higher power need be a hindrance?

In U.S., there are 12 channels, each 20 MHz wide. Fig. 7 shows the specifications of the 12 channels. Fig. 8 shows the spectrum layout of 802.11a. Each channel is divided into 52 subchannels; 48 are used for data and the other 4 are pilot subchannels used to minimize frequency and phase shifts. Fig. 9 is a diagram of the PLCP Protocol Data Unit (PPDU) format. PHY uses rate of 250K symbols per second with each symbol spanning all 48 channels. Convolution code is used by all subchannels. Fig. 10 lists rate dependent parameters in 802.11a. Take 54 Mbits/s as an example for rate

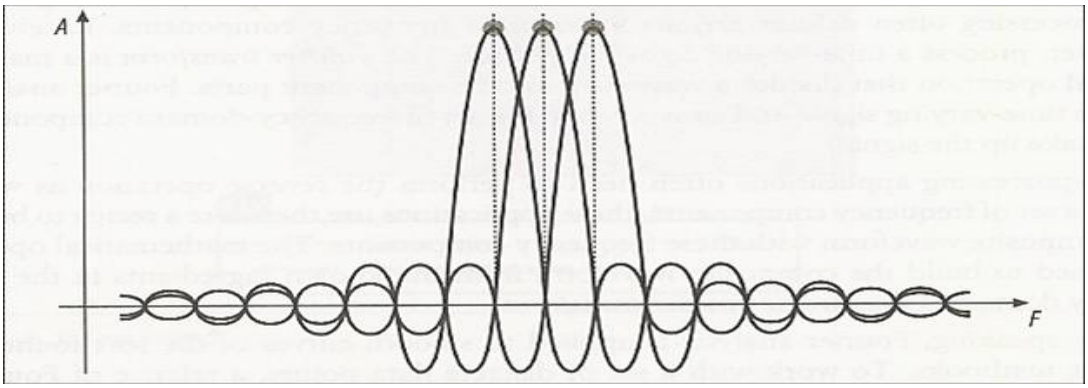

Fig. 6. Spectrum of OFDM.

calculation. It uses 64-QAM which is 6 coded bits per symbol per subchannel or 288 coded bits across all 48 channels per symbol. At a coding rate of 3/4, there are 216 data bits per symbol. Therefore, data rate is 250K symbols/sec × 216 bits/symbol or 54 Mbits/s.

In 802.11 standards, dynamic rate adaptation is utilized to achieve the best throughput between mobile station and AP. When there is packet loss, the data rate is reduced (while keeping PLCP rate same) and the rate is increased after timer expires.

Regulatory domain	Band (GHz)	Operating channel numbers	Channel center frequencies (MHz)
United States	U-NII lower band (5.15–5.25)	36 40 44 48	5180 5200 5220 5240
United States	U-NII middle band (5.25–5.35)	52 56 60 64	5260 5280 5300 5320
United States	U-NII upper band (5.725–5.825)	149 153 157 161	5745 5765 5785 5805

Fig. 7. Channel specifications in 802.11a.

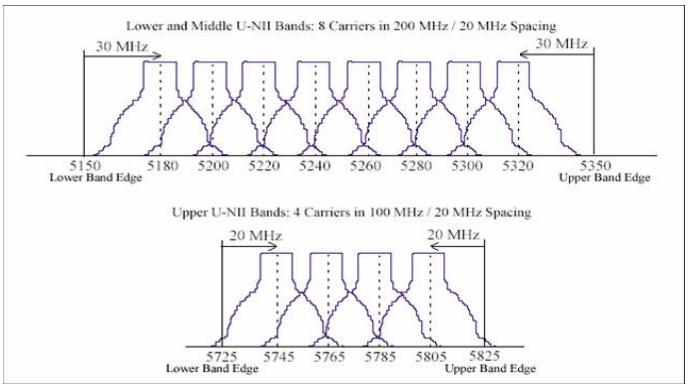

Fig. 8. Spectrum layout of OFDM in 802.11a.

V. MAC

MAC in WiFi has the following access modes.

Distributed Coordination Function (DCF) DCF is based on Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).

Point Coordination Function (PCF) PCF is restricted to Infrastructure BSSs and not widely implemented. In PCF mode, an access point polls stations for medium access.

The usage of the two modes are shown in Fig. 11.

In DCF, various Interframe Spacing (IFS) are defined as follows.

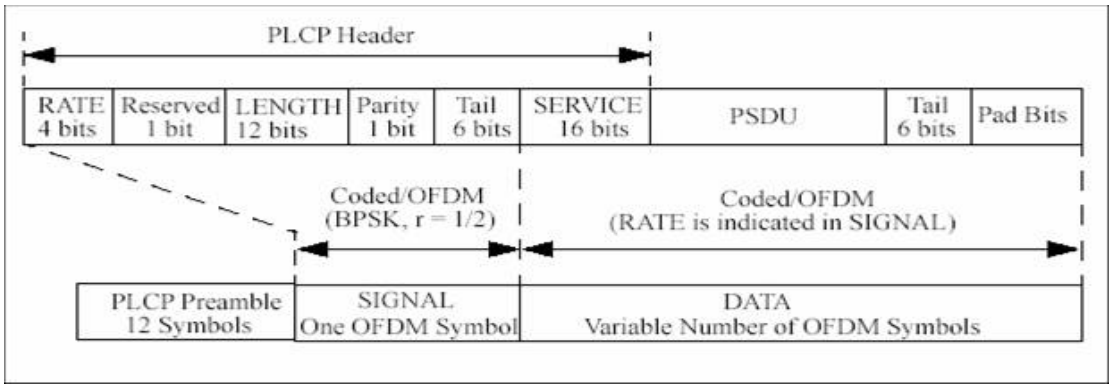

Fig. 9. PLCP Protocol Data Unit (PPDU) format in 802.11a.

Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Fig. 10. Rate dependent parameters in 802.11a.

- Short IFS: For atomic exchanges
- PCF IFS: For prioritized PCF access
- DCF IFS: For Normal DCF access
- Extended IFS: For access after error

Fig. 12 is a diagram of 802.11 MAC. The main ideas of MAC is CSMA/CA. A station must sense the medium first and proceeds with transmission if the medium is free. If medium is idle for DIFS interval after a correctly received frame and backoff time has expired, transmission can begin immediately. If previous frame contained errors, medium must be free for EIFS. If medium is busy, access is deferred until medium is idle for DIFS and exponential backoff. Backoff counter is decremented by one if a time slot is determined to be idle. Unicast data must be acknowledged as part of an atomic exchange, lack of acknowledgment triggers exponential backoff. A successful transmission triggers immediate backoff even if no frames are currently queued.

Interframe Spacing values are physical layer dependent. SIFS and Slot_Time are explicitly specified, and the others are derived.

- PIFS = SIFS + Slot_Time
- DIFS = SIFS + 2 Slot_Time
- EIFS = SIFS + DIFS + (Ack_Time @ 1 Mbps)

For 802.11a and 802.11b SIFS is 16 μs and 10 μs, respectively and Slot_Time is 9 μs and 20 μs, respectively.

Backoff is performed for R slots: R is randomly chosen integer in the interval [0, CW] where CWmin $\leq$ CW $\leq$ CWmax. CWmin = 31 slots and CWmax = 1023 slots (for 802.11b). Up to CWmax, $CW = (CW_{min} + 1) \times 2^n - 1$, where n = 0, 1, 2, ... is (re)transmission number.

Each frame is associated with a retry counter based on frame size as compared to RTS/CTS threshold. It can be either a short retry counter or a long retry counter. Fragments are given a maximum lifetime by MAC before discarding them.

Fig. 13 illustrates the hidden terminal and exposed terminal problems. As illustrated, hidden terminal problem happens when station A wants to send data to B, it does not know B is busy because C is transmitting and B is within

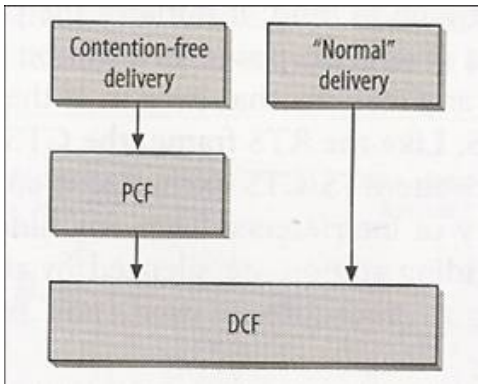

Fig. 11. MAC access modes.

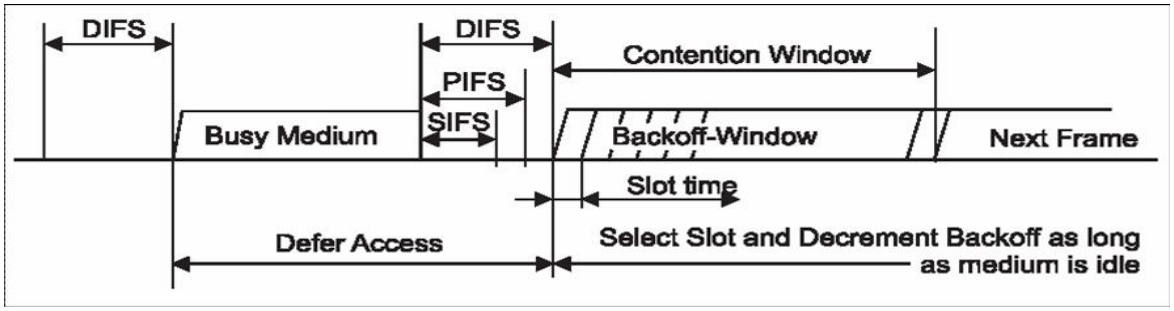

Fig. 12. 802.11 MAC

the transmission range of C while A is not. Thus, it leads A to falsely think it can transmit. Exposed terminal problem is similar. One solution is to use RTS/CTS Clearing as illustrated in Fig. 14. When a station needs to send data, it first sends a Request to Send (RTS) frame to the intended receiver. After receiving the RTS, the receiver replies with a Clear to Send (CTS) frame only if it is free. Afterwards, normal communication resumes. With RTS/CTS Clearing, station A wouldn't send data to B because no CTS would be received from B in the hidden terminal case. Of course, RTS frame itself might not be received. Therefore, it is used for frames larger than RTS/CTS threshold as a tradeoff between overhead and retransmission costs. In practice, most infrastructure WLANs don't use RTS/CTS.

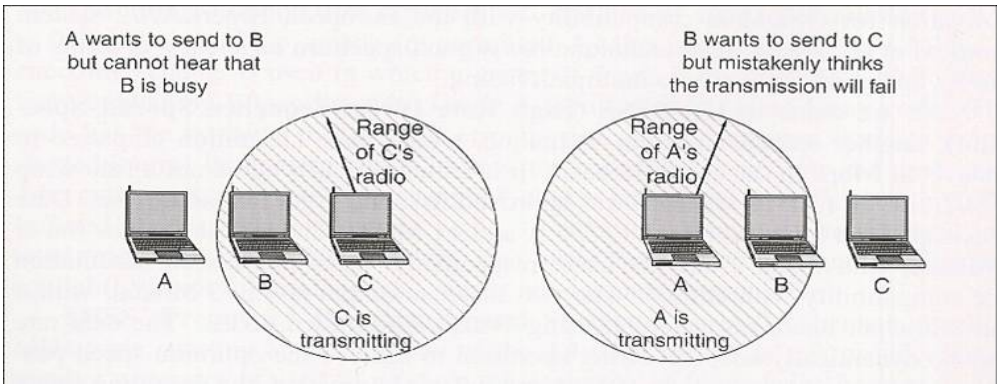

Fig. 13. Hidden Terminal and Exposed Terminal problems

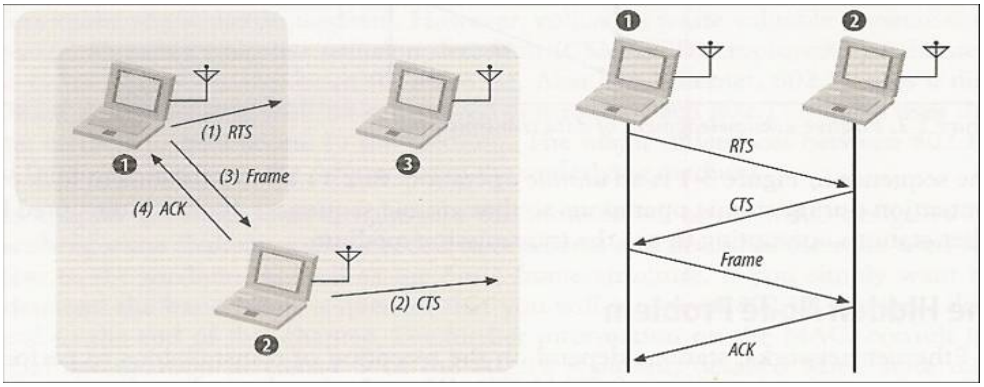

Fig. 14. RTS/CTS Clearing scheme.