December 19, 2018

Fast WiFi scanning

Jiwoong Lee

Fast WiFi scanning

ABSTRACT

In some countries, unlicensed spectrum used by WiFi networks is shared with radar systems. WiFi networks that operate in such bands employ radar detection and avoidance. A WiFi transceiver spends a certain channel sojourn (dwell) time scanning a channel prior to starting communication on it. A full scan takes about seven seconds, a user-perceptible delay.

This disclosure describes techniques to reduce scan time by leveraging radar detection procedures that have already been completed by nearby access points. If a nearby access point has recently transmitted a frame or emits a wide-band transmission, it is an indication that the nearby access point has confirmed that the channel is clear of radar. Therefore, a device that is about to initiate a full scan can abbreviate its scan duration substantially. With implementation of the techniques of this disclosure, scan times drop from seven seconds to under two seconds.

KEYWORDS

- WiFi scanning
- channel sojourn time
- dynamic frequency selection (DFS)
- U-NII band
- spectrum sharing
- cognitive radio

BACKGROUND

In some countries, unlicensed spectrum used by WiFi networks is shared with weather radar. Radar being a higher-priority service, WiFi networks that operate in such bands, e.g., the UNII bands, employ radar detection and avoidance. A WiFi transceiver spends a certain channel

sojourn (dwell) time scanning a channel to confirm absence of radar signals prior to starting communication on it. A full scan, which is required whenever a new connection is established in a new RF environment, takes about seven seconds, a user-perceptible delay. A scan time as long as seven seconds has many disadvantages, e.g., poorer user experience, greater power consumption, inability to quickly move to a better network, slower roaming, etc.

In the United States and several other countries, there are eleven channels in the 2.4 GHz band and twenty channels in the 5 GHz band. In the 5 GHz band, there are four channels in the UNII-1 band, four channels in the UNII--2A band, twelve channels in the UNII--2B band, and five channels in the UNII--3 band. Dynamic frequency selection (DFS) channels, e.g., those in the UNII--2A and UNII--2B bands, require the detection of weather radar before starting transmission.

DESCRIPTION

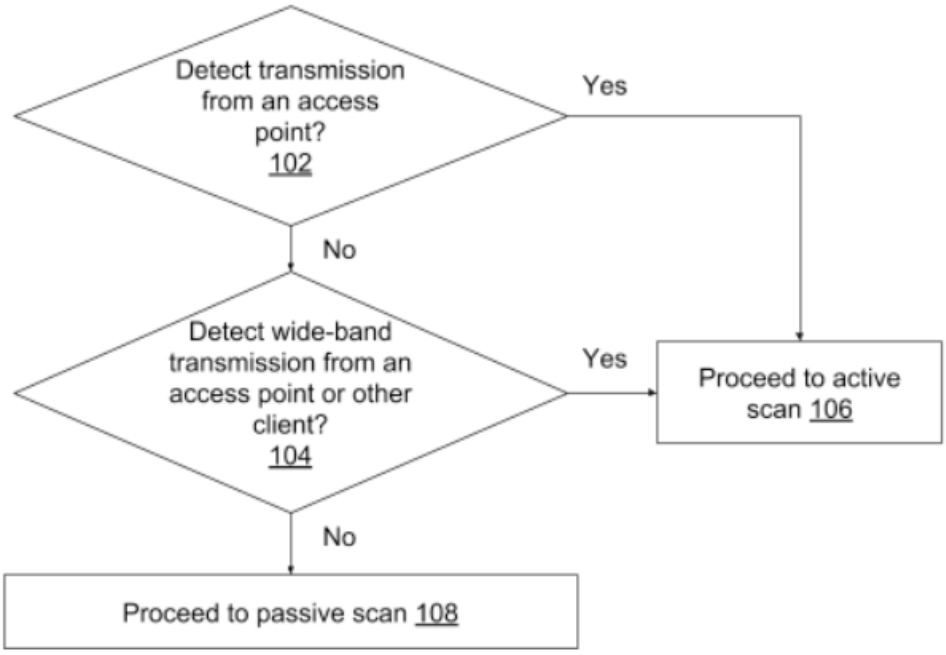

Fig. 1: Reducing scan time while conforming to standards requirements

Fig. 1 illustrates an example process that results in reduced WiFi scan time in DFS channels while conforming to standards requirements. A client, e.g., mobile device, that is about to start transmission on a DFS channel senses the presence of transmissions from a nearby access point (102). If a transmission is detected, such detection implies that the access point has already performed a radar detection test and has confirmed the absence of radar signals (or at least failed to detect radar). In such a case, the client proceeds to active scanning (106).

If the client senses a wide-band transmission from an access point or another client (104), e.g., a 40 MHz transmission in 802.11n, or a 40/80/160 MHz transmission in 802.11ac, such detection implies that the access point or client has already performed a radar detection test and confirmed the absence of radar. In such a case, the client proceeds to active scanning (106).

If no transmission is detected from an access point, and no wide-band transmission is detected from either an access point or another client, then the client proceeds to passive scanning (108).

Example 1: A client changes its channel to DFS channel number 100 and is required to scan prior to transmission. A purely passive scan requires a passive scanning channel sojourn time of S_p seconds, during which time the client receives beacon frames. If the client detected at time T_f a frame of any type from a nearby access point, or any data frame from a nearby client, then the client cancels its passive scanning and switches to active scanning. Active scanning is initiated by sending out a probe request management frame, which solicits responses from nearby access points. An active scanning channel sojourn time of S_a seconds is spent before completing scanning. The client switches from passive to active scanning as long as $S_p > T_f + S_a$.

Example 2: A client changes its channel to DFS channel number 100 and is required to scan prior to transmission. The client detects an 80 MHz transmission, implying that no radar was detected

in channels 100, 104, 108, and 112. When these channels are ready for transmission by the client, the client skips passive scanning, and spends a smaller scanning time of S_a seconds for active scanning.

Comparison of scan times

In the UNII-2A and UNII-2B bands, there are four possible 80 MHz channel groups: 52-64, 100-112, 116-128, and 132-144. Per techniques of this disclosure, the average sojourn time in a DFS channel is $S_a + T_f/4$ seconds. Let N_{nd} and N_d denote respectively the number of non-DFS channels and DFS channels. Then the total scanning time $S_{o,1}$ is given by

$$S_{o,1} = S_a N_{nd} + (\frac{T_f}{4} + S_a) N_d$$

assuming channel switching time and software processing delays are negligible.

Under the baseline scheme, e.g., when the client uses passive channel for every channel, the total scanning time $S_{o,2}$ is S_p times the total number of channels:

$$S_{o,2} = S_p(N_{nd} + N_d)$$

Typical operating systems don't perform passive scanning for non-DFS channels, and do so only for DFS channels. The total scanning time $S_{0,3}$ for typical OS scan times is thus given by

$$S_{o,3} = S_p N_d + S_a N_{nd}.$$

Using typical values for parameters, e.g.,

$S_p = 400$ msec, in order to robustly collect beacons of at least 100 msec duration;

$S_a = 40$ msec, in order to account for the low data rate of management and probe request/response frames from up to 10 nearby access points that have the same channel as the primary 20 MHz bandwidth channel;

$T_f = 50$ msec, set to half the value of a typical beacon period;

$N_{nd} = 20$, set to the number of 2.4 GHz, UNII-1, and UNII-3 channels; and

$N_d = 16$, to include the UNII-2A and UN11-2N channels;

we obtain the following table:

	Lower bound	This disclosure ($S_{o,1}$)	Typical OS ($S_{o,3}$)	Baseline ($S_{o,2}$)
Full scanning time	1.44 sec	1.64 sec	7.2 sec	14.4 sec

The table shows that the techniques described in this document achieve a scanning time more than five seconds better than that of the typical OS, and nearly the same as the lower bound.

CONCLUSION

This disclosure describes techniques to reduce scan time by leveraging radar detection procedures that have already been completed by nearby access points. If a nearby access point has recently transmitted a frame or emits a wide-band transmission, it is an indication that the nearby access point has confirmed that the channel is clear of radar. Therefore, a device that is about to initiate a full scan can abbreviate its scan duration substantially. With implementation of the techniques of this disclosure, scan times drop from seven seconds to under two seconds.