Assignment 1: Setting up a framework for the evaluation of the second capture effect in generic 802.11 hardware

1. Goals

Students must implement a framework for evaluating the ability of generic 802.11 hardware to handle "Second Capture". This feature, which manufacturers started implementing a few years ago, allows a chipset to stop the decoding of a frame when it detects a new preamble as reported in Figure 1. This implicitly requires that the intensity of the new frame (frame 2) is much higher than that of the current one being decoded (frame 1) so that the new preamble can be effectively decoded.

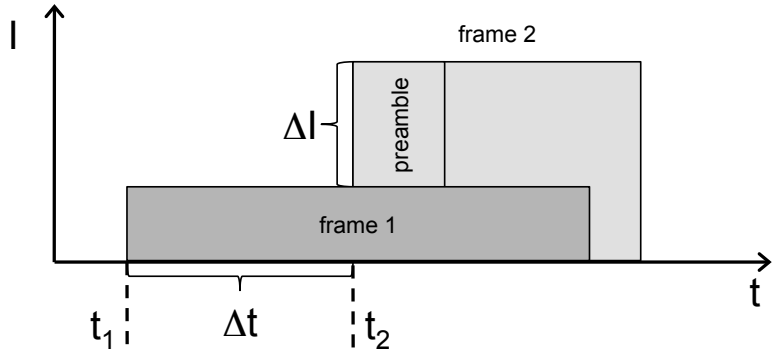

Figure 1 Second frame can be decoded if its intensity is high enough.

The rationale behind second capture is that if the intensity gap ΔI between the two frames is high enough, then

- Decoding of the frame 1 will fail, no capture effect might help;
- Decoding of the new frame 2 could be possible.

This clearly poses a condition on gap ΔI and on the time delay ΔT between the two frames.

The goal of this project is to design and implement a flexible firmware that allows a couple of transmitters to keep perfect synchronization and to start transmitting frames with configurable delay ΔT and power gap ΔP (this setting reflects into ΔI) as sketched in the reference scenario in Figure 2. This will allow to study the second capture behavior of general 802.11 devices and express it as a function of the two parameters (ΔT, ΔI) for different combinations of the data-rates of the two overlapping frames.

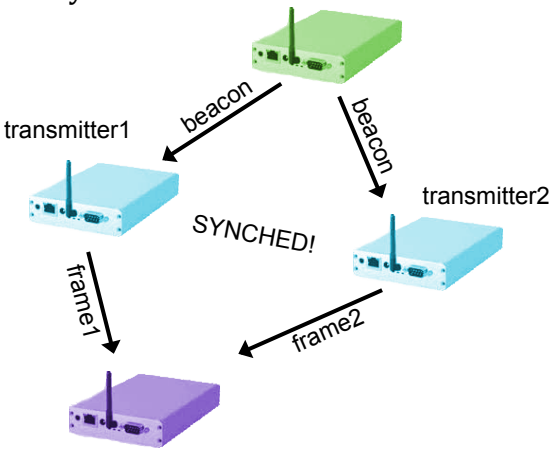

Figure 2 Reference scenario.

To implement the framework the following requirements and modifications are needed:

1) Transmitters should be able to transmit frames according to two different styles:
   a. TDMA-like: specific frames generated in the user-space like those to UDP port 3939 should be transmitted following a TDMA approach (refer to document "2016-nomadic-3-tutorial5.pdf"). Transmission times should almost match apart the small delay ΔT: to avoid to implement complex synchronization techniques, students should compute the transmission time by extracting it from the least N significant bit of the internal clock. In the example in Figure 3 N is set to 10: each node transmits at every slot whose duration is set to 2^10μs (=1024μs) with a specific delay since the beginning of the slot.

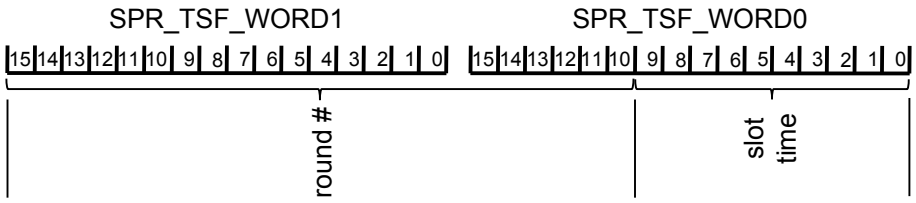

Figure 3 Transmission times are computed from the least significant bit of the clock.

   b. DCF: this channel access is required for transmitting all the other frames. Among such, the probes that are necessary to keep the nodes associated to an AP which in turn allows to keep the clocks synchronized and to transmit frames.

   It is also necessary to keep records of how many times one or the other method was chosen to extract statistics later.

2) Transmitters have to be associated to an AP: in this way
   a. their clocks are kept automatically synchronized;
   b. they can transmit frames to UDP port 3939.

3) Frames to port 3939 should be transmitted with TDMA access and with a fake receiver address that must be overwritten by the firmware, to avoid the receiving AP to transmit the reply frame (i.e., the acknowledgment). The firmware can detect these frames by checking the value of TXHDR_UNUSED in the transmission hardware header: this field is filled with a non-zero value for UDP frames to port 3939 by the b43.ko kernel driver that can be downloaded from the course website: remember to replace the module of the transmitters with this one. The module is also setting the frame in a way so that the firmware will not wait for any acknowledgment.

4) It should be possible to fix the transmission power spectrum and the antenna so that the frame is transmitted always with the same settings[1]. The modified b43 driver is able to fix

[1] Even though the transmission power spectrum should depend only on the power set by the user invoking "iwconfig wlan0 txpower N", the kernel keeps adjusting the real transmitted power following a closed loop approach where the feedback is computed by the firmware during the transmission. This might have bad effects on the stability of the transmission power monitored by a sniffer, and of course on the analysis of the second capture effects. To avoid troubles we prevent the kernel to adjust the transmit power.

them when a UDP transmission to UDP port 10000 is done from the user-space: the dmesg reports a message acknowledging the user request. Remember to always fix settings and check the dmesg. Sending a UDP transmission to UDP port 20000 reset to default behavior and allows to change the transmission power by invoking "iwconfig".

Firmware verification Before starting second capture tests, students should carefully verify that the implemented firmware works according to the aforementioned requirements/modifications. To this end a single transmitter should be active and its transmission times checked by using a classic sniffer: to this end students will extract transmission times reported in the radiotap header and check that they follow the rule as in Figure 3. Students should also verify that the RSSI reported by the sniffer is almost fixed.

Second capture characterization The device to test is provided by the facilitator for this assignment. It is based on an Atheros QCA 9882 chipset which is 802.11ac compliant. For the purpose of this test, only second capture of legacy DSSS and OFDM frames can be measured given the limitations of the transmitter's chipset.

In general, the characterization should be run for a specific choice of values ΔI (i.e., ΔP) and ΔT by performing a given number of transmissions from the two transmitters, i.e., N = 1000. The device under test should be configured in monitor mode on the same channel as the two transmitters and it should capture all frames, including those damaged (i.e., corrupt by errors). To avoid spurious traffic to affect the measurement, students should

- Use a traffic-free channel (i.e., channel 14);
- Filter the captured traffic and remove frames that appear to be transmitted by other nodes, in particular this applies to correctly received frames.

Once frames have been filtered, students should count how many frames have been received in total, and how many are correct. Then they should compare these numbers with the transmission statistics reported by the two transmitters and try to quantify the second capture effect.

Note, however, that trying all possible values ΔP and ΔT can be time consuming and we are not even sure about whether the capture effects depends on ΔP only or on ΔP and P1 (or equivalently on ΔP and P2). For this reason students are encouraged to follow this measurement campaign criteria:

1) Fix the modulation and data-rate of the two transmitter to OFDM 6Mb/s;
2) Fix the delay to something in the middle of the preamble, i.e., 10μs;
3) Fix the power of transmitter 1 so that the chipset under test receives its frames with an average power of -60dBm;
4) Evaluate the second capture effect when the power of transmitter 2 is reported by the chipset ranging from -60dBm to the maximum value that can be achieved.
5) Repeat the characterization by setting the transmitting power of transmitter 1 so that its frames are received at either -50dBM or -70dBm.

At the end of this phase it will be possible to state whether the second capture effect depends only on the difference of the transmitters' powers or not. If this is the case, then the following experiments can be done by setting the transmission power of transmitter 1 and changing the other one, otherwise the whole characterization must be repeated for different transmission power of transmitter 1.

Students should then test the dependency of the second capture effect on the delay, for different values of the transmission power gap (refer to the end of the previous paragraph). Analysis should be done with very fine granularity (i.e., 1μs) starting from 0 up to the internal of the data-frame: this maximum delay depends on the modulation, i.e., it could be 30μs for OFDM so that at least two symbols are considered, or 210μs for DSSS so that at least a few barker sequence after the PLCP are considered.

Finally it could be interesting to see how second capture works when the modulations of the two frames are different: to this end students should first experiment with the same modulation and different data-rates, and then with different modulations, i.e., OFDM comes first, then DSSS or the opposite.