CW 16/17 Summary

Alexander Pastor

23.04.2017

Contents

1 Wireless Network Fundamentals

1.1 Why wireless?

Wireless networks have a number of potential advantages over wired networks.

These include mobility hence flexibility, ease of deployment, potential cost reduction.

Disadvantages include exposition to malevolent intrusion and at times lower speed.

1.2 Basic Terminology

A (802.11) network consits of *stations, the wireless medium, access points and the distribution system.*

stations
Defining aspect: devices used for data transfer among them. Devices with wireless interfaces, mostly, but not limited to handheld devices or laptops.

wireless medium
In our case two radio frequency layers (2.4 GHz and 5GHz).

access points
The points through which stations can access the network. Their main purpose is acting as a wireless-to-wired bridge, i.e. translating wireless frames to wired frames to communicate with the rest of the world.

distribution system
The logical network component that forwards (possibly "translated") frames from the access points to their destination. 802.11 does not specify a technology, but Ethernet is dominant.
From this fact one can derive that wireless technology is not meant to be a substitute for wired technology, but as a supplement to provide more mobility to users.

There are different two different basic types of networks, which gives rise to the next set of terminology.

basic service set (BSS)
A basic service set is the basic unit of a wireless network and simply comprises of a set of communicating computers. The covered area is called basic service area. These basic service sets come in two flavors. One is independent basic service set (IBSS), the other is infrastructure basic set service. Infrastructure basic service sets include access points, while independent basic service sets have no access points.

This means IBSSs have no connection to the outer world, hence the name "independent". Useful for short-ranged, short-lived ad-hoc networks for the purpose of data exchange during a conference.

service set identifier (SSID)
Serves as a name for the service set.

extended service set (ESS)
Created by linking several BSSs together with a backbone network. All linked sets share the same SSID, thus are not distinguishable from the viewpoint of the user.

virtual access points
Multiple virtual access points on the same physical access point make it possible to have several virtual ESSs with only one set of physical hardware. Particularly useful if you want to have networks with different levels of security or want to restrict access to certain resources.

atomic operation
Set of operations that is individable, i.e. if one operation out of the set fails the whole atomic operation fails.

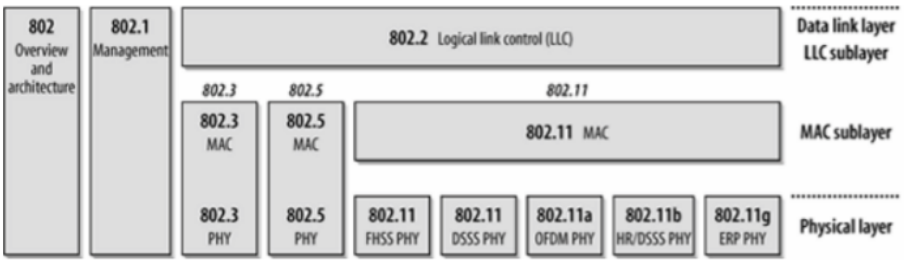
fragment
Large (management or higher-layer) frames would sometimes exceed a certain maximum length. If that would happen they are instead split into several smaller fragments. The point is this way they are less susceptible to interference, because the likelihood of an atomic operation succeeds increases. This may increase throughput. However, this comes at a price of additional management and frame overhead.

2 WLAN, LTE-U and LAA

To make network devices beautifully compatible industrial standards are needed. This is what the following section will discuss.

2.1 802 and 802.11

The following is a picture of the IEEE 802 norm family. 802 deals with *local area networks* (LANs) and *metropolitan area networks* (MANs). The specified protocols reside in the physical and data link layer. 802.11 is about *wireless LAN* (WLAN). As of now only the working groups of 802.1 (higher layer LAN protocols), 802.3 (Ethernet) and 802.11 are active.
A way of defining network technology is to define the services it provides, much like defining an API for software.



802.11 provides the following: distribution, integration, association, reassociation, disassociation, authentication, deauthentication, confidentiality, MAC SDU (MSDU) delivery, Transmit Power Control (TPC), Dynamic Frequency Selection (DFS).

A detailed description is omitted.

Note: It is worth to mention that while 802.11 supports seamless BSS transition within an ESS, it does not support seamless ESS transition, as higher layer connections are interrupted.

2.2 The LTE Unlicensed Family

LTE stands for Long-Term Evolution. It is a wireless communication standard for mobile devices. Despite not meeting the criteria defined by the ITU-R (the radio division of a specialized United Nations agency) to be labeled as 4G service it is marketed as such and has achieved an almost global presence. It is an improvement over preceding generations in terms of speed and other technical aspects such as spectral efficiency (measures transmission rate per bandwidth).

Note: LTE Advanced has been formally acknowledged to meet 4G's criteria and is a candidate 4G technology. The other candidate is 802.16m better known as "WiMax" (*Worldwide Interoperability for Microwave Access*) and is currently available in more than 150 countries.

LTE-U stands for LTE Unlicensed and is a proposal originally made by Qualcomm for the use of LTE technology in the unlicensed 5GHz band. However, the "indigenous" dual-band WiFi equipment vendors fear performance losses for their technology if LTE-U was to share a part in the band. LAA which expands to *License Assisted Access* is a term used by Ericsson to describe a similar technology. LAA uses a LBT contention protocol.

Qualcomm and their allies Verizon and Ericsson claim that LTE-U family technologies would better neighbors to WiFi in terms of joint AND individual throughput, than WiFi itself. Google and the WiFi-alliance claim WiFi performance losses of up to 40%. Both parties mutually accuse the other's studies, tests and allegations would be profoundly biased and unfair.

2.3 MAC Challenges

Wireless transmissions based on radio waves suffer from multiple physical problems wired transmissions don't have. Overcoming these obstacles is the challenge for designers of MAC protocols.

2.3.1 Link Quality

Noise, interference and multipath fading make wireless signals less reliable both in terms of bit error rate, establishing and keeping up a connection at all, in case a node moves into a dead spot.

Radio link quality is also influencing the possible maximum data transmission rates. As signal quality degrades one has to slow down the data transmission rate to make sure a useful (correctly demodulatable) signal arrives at the other side. The overall volatile nature of wireless transmission also forces the technology to be highly adaptive in terms of for instance speed regulation. The keyword here is *multirate support*.

2.3.2 The Hidden Node Problem

In Ethernet networks CSMA/CD is used to detect collisions. This is not the case for wireless networks.

Since the signal quality of every radio wave transmitter degrades over distance each station has a limited range.

Suppose node B was in range of nodes A and C, but A and C not in each other's range, then A is called hidden node from the viewpoint of C and vice versa.

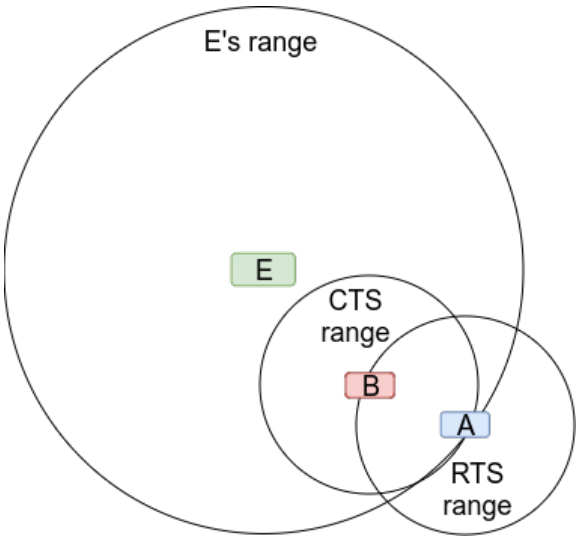
Collisions from hidden nodes are hard to detect, because wireless transceivers are *half-duplex*, i.e. able to transmit and receive packets, but not at the same time. The reason is that due to attenuation the magnitude of received waves can be several powers below those of the originally transmitted waves. If a node was to simultaneously send and receive the received signal would simply "drown in the sea of transmission noise".

Note: It is possible to receive and transmit at the same time, but this requires very intricate and thus costly signal processing hardware.

For networks of sufficient capacity (delay-bandwidth-product) so-called *Request-to-Send-Singnals* (RTS) as well as *Clear-To-Send-Signals* (CTS) can aid to achieve the goal of collision avoidance. However, this palpably increases the duration of an atomic operation, which then consits of RTS, CTS, the data frame and the ACK (and interframe spacing).

[thought experiment:] If I had nodes with very different power levels belonging to the same BSS (for instance let edge nodes have more "buzz" in order to cover

peripheral areas). Imagine now that an arbitrary node A wants to transmit and issues a RTS. A set of nodes {B} in vicinity of this node will subsequently respond with a CTS and shutdown nodes in their vicinity. Suppose the CTS doesn't reach an edge node E, but the edge node's power would be big enough to interfere with the original sender. Suppose that without loss of generality range A equals the range of each member of the set B. This implies that E's range is more than twice as big as A's. Is this possible scenario with 802.11? The question has come up once I read that 802.11 features energy regulation to adapt the nodes' respective ranges to prevent similar scenarios to what I described. Below a little sketch to illustrate what I'm asking.



2.4 How the MAC stuff is supposed to work

First let's discuss the difference between CSMA/CD and CSMA/CA.

A CSMA/CD-like protocol is used for the wired Ethernet. Since wired connections are full-duplex collisions can be detected. In case of a collision CSMA/CD shuts down transmission to minimize the damage dealt, i.e. minimize wasted transmission time (and also power).

As discussed earlier wireless transmissions are half-duplex and that is why collisions are not detected and we only try to avoid them. For this purpose we listen to the channel before we transmit (LBT) and optionally use the 802.11 RTS/CTS exchange.

The LBT procedure is implemented as a so-called *distributed coordination function* (DCF). In case contention-free service is required a function built on top, the so-called *point coordination function* can be used. A *quality of service* (QoS) compromise can be achieved with the *hybrid coordination function* (HCF).

[confirmation required] DCF is the only practically established MAC access function.

2.4.1 Virtual Carrier Sensing and the Network Allocation Vector

[question] Is the following statement correct: 802.11 only uses physical carrier sensing while receiving and just before sending?

802.11 uses to type of carrier sensing functions to determine, whether the channel is busy or not. One is physical carrier sensing and the other virtual carrier sensing. If either sense finds a busy channel, the MAC layer reports a busy channel to the above layer.

Needless to mention, but still: the physical carrier sense alone is insufficient, because radio transceivers cannot transmit and receive at the same time. Hidden nodes make matters worse.

The so-called *Network Allocation Vector* (NAV) is designed to solve this problem. Most 802.11 frames carry a duration field in which is filled in with the time in microseconds which a node expects to use the medium. Other stations can then count down from NAV to 0 before trying to transmit. This nifty trick is called *virtual carrier sensing*.

2.4.2 Interframe Spacing

Interframe spacing is yet another measure to coordinate traffic. According to the simple logic that higher priority frames should have to wait less than lower priority frames (in 802.11) there are four different fixed-duration interframe intervals (not a function of transmission rate, but dependent on physical layer protocol - "arbitrary" but fixed).

Important frames such as RTS/CTS and ACKs have the highest priority and the space between them is the *short interframe space* (SIFS).

Frames sent off "with the consent" of DCF and PCF respectively have interframe spaces of DIFS and PIFS.

In case of transmission errors there also exists the *extended interframe space* EIFS for retransmissions.

[question] What is meant by the following statement: "Once a station has transmitted the first frame in a sequence, it has gained control over the channel. Any additional frames and their ACKs can be sent using the SIFS, which locks any other stations"? (p.42, Gast) Does this imply after seizing control over the channel there are no frame intervals of length DIFS anymore? This wouldn't make sense, because after a break of DIFS follows the contention-phase. I think the following statement would be more concise: "Once a station has transmitted

the first FRAGMENT of a sequence (...) it sends any additional FRAGMENTS OF THAT ATOMIC SEQUENCE with an interframe (better interfragment) spacing of SIFS.

2.5 Error Recovery and Backoff with the DCF

When an error is detected a retransmission has to take place. Upon retransmission a station's retry counter (one for each frame) is incremented. We distinguish between short and long frames and also between short and long retry counts. Frames longer than a threshold (typically the RTS frame length) are considered to be long, otherwise short.

After a certain number of retries has been reached the MAC layer discards these frames. Higher layers may issue further retransmissions though. From the point of the MAC layer these retransmissions are completely new and independent though and hence the retry counter starts at 0.

The reason for having different maximum retry counts for long and short frames is that longer frames require more buffer space. If we have a lower maximum retry count for them we can (potentially) save buffer space.

Another feature added to frames is a lifetime. When the specified limit is reached the frame is simply discarded and no attempt is made to (re)transmit any associated fragments.

[confirmation required] I think the point of this is to catch some fairly rare errors, such as that frame still lingering around will be discarded instead of taken for a valid frame of a later transmission.

The DCF backoff works as follows: if two stations wanted to transmit a frame they would cause a "collision" in the contention phase. As a consequence, the number of coSPectrntention slots is roughly doubled (powers of 2 minus 1). In the subsequent contention phase they arbitrarily choose a slot. The station with the lowest slot number wins. This process is repeated until no slot collision occurs.

An exception in this concept is the *Spectralink Voice Priority* (SVP) which allows frames carrying voice data to get the 0^{th} contention slot, hence prioritizes speech over other data. The reason is to bolster the QoS of VoIP services which are inherently vulnerable to any delays. To ensure stability however, retransmissions of speech are subject to contention.

2.6 Frame Format

Specific frame formats are omitted here. However, here are some questions.

[question] (Gast p.51 footnote) "802.11 specifies that stations should ignore frames that do not have the same BSSID (...)." But what about ESS-based services then? I assume the following: since ESSs have the same SSID for all their BSSs one could say that all BSSs of an ESS have the same BSSID. Wouldn't it be more concise to generally speak of ESSID in that case or simply of SSID in a general case?

[question] (Gast p.53) "(...) There is no higher-level protocol tag in the 802.11 frame to distinguish between higher-layer protocol types. Higher-layer protocol types are tagged with a type field by an additional header (...)." What is a tag and how are they used? If a tag is something like a higher-layer header, doesn't the second contradict the first one then?

[question] (Gast p.53) "802.11 does not have negative ACKs for frames that fail the frame check sequence". Why not? Would this add, too much to the device complexity?

3 Getting to Know GNU Companion

I have built some simple block diagrams. Looking at more of this is the next top priority. A more detailed description is omitted in this summary for the sake of saving some time. More will follow in later write-ups.

4 Python

I bought a book and did some basic tasks. Not much more to say here, except that I'll put more effort into that during the next weeks.

5 LaTeX

I currently use TeX Live and TeXStudio as IDE. I have not faced any significant problems as of now.

I looked at basic functionality such as creating a title page, a structure, equation, align and other environments. Furthermore I looked at how to add pictures and text and to format these including virtual and horizontal spacing, floats, coloring, adding a text-style and more.

More features I need to look at: Generating a well-formatted table of contents, footnotes, bibliography, means to creates sketches and more.

I also acquired a LaTeX-reference book by Helmut Kopka.