Security of Wireless Networks

{thgoebel}@ethz.ch

ETH Zürich, HS 2020

This documents is a summary for the course *Security of Wirless Networks (SOWN)* at ETH Zurich.

This summary is created during the autumn semester 2020. But due to the few changes in syllabus content in the past we have reason to believe that it is also relevant beyond that very semester.

We do not guarantee correctness or completeness, nor is this document endorsed by the lecturers. Feel free to point out any erratas.

Contents

1. Wireless Basics

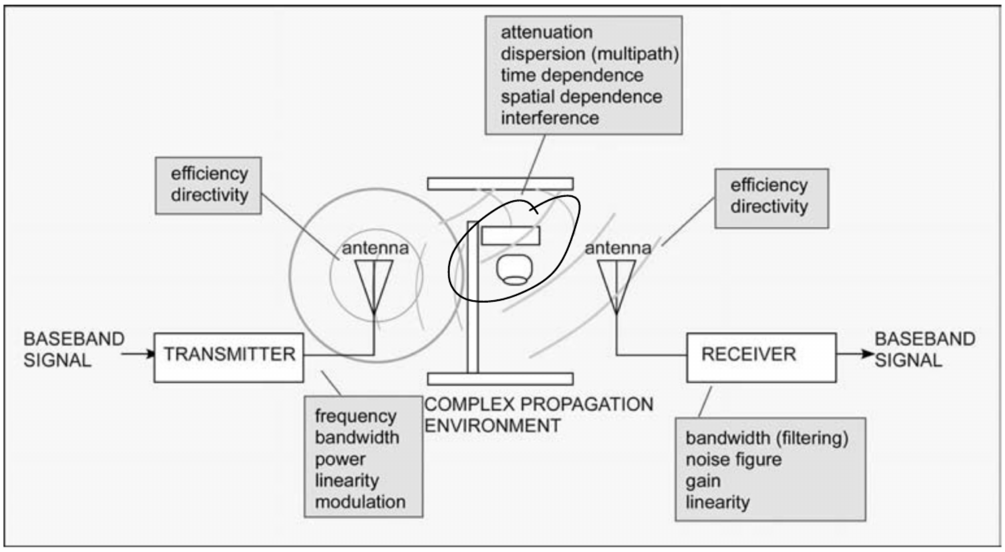

Figure 1: A wireless system, its basic components and characteristic measures

Radio Frequency Signal Electromagnetic radiation, with waves being created in the antenna by an alternating current at the desired frequency. Mathematically described as a function of the time t:

$$v(t) = A\sin(2\pi ft + \phi)$$

with amplitude A, frequency f and phase ϕ. Also recall that the period is $T = \frac{1}{f}$ and the wavelength (distance travelled during one period) is $\lambda = \frac{v}{f}$ (usually $v = c$ speed of light).

Bandwidth The capacity of a communications link to transmit the maximum amount of data from one point to another over a connection in a given amount of time (in bits per second bps). An analogy: The amount of water that can flow through a water pipe.

In other words, the measure of frequency content of the signal. E.g. the human voice contains frequencies in the range from 30 Hz to 10 kHz, and the bandwidth of a single 802.11 channel is 22 MHz.

Note that often the bandwidth of the baseband and that of the carrier (and thus that of the modulated signal) differ! E.g. see spread spectrum techniques.

Baseband An original transmission signal that has not been modulated or has been demodulated to its original frequency. I.e. the actual **information signal**. Most telecommunication protocols require baseband signals to be converted, or modulated, to a higher frequency in order to be transmitted over long distances.

Carrier A transmitted electromagnetic pulse or wave at a steady base frequency of alternation on which information can be imposed. Typically a pure sinusoid of a particular frequency and phase that carries the information. Usually the frequency of the carrier is much higher than that of the baseband.

Modulated Signal A carrier that has been loaded or modulated with the information signal.

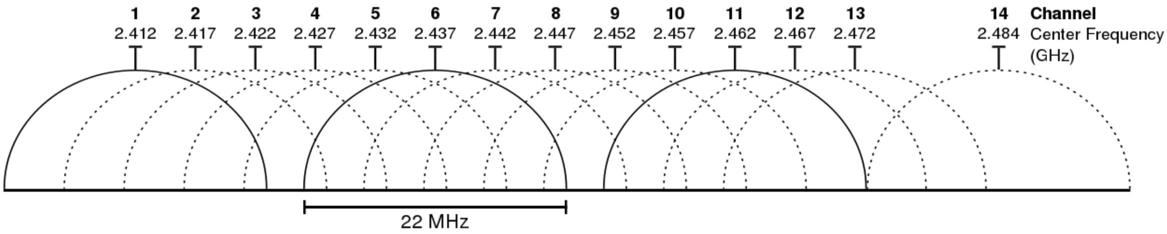

Figure 2: 2.4 GHz WiFi Channels [Source]

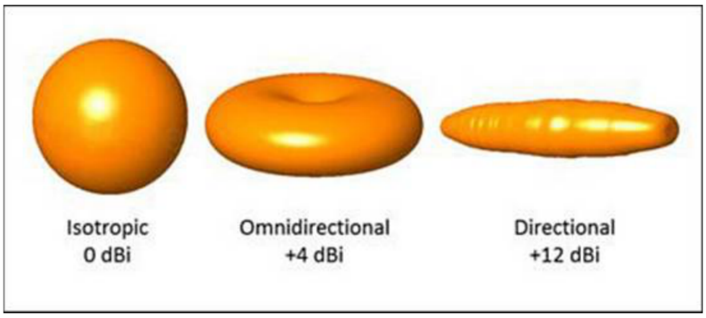

Figure 3: Antenna directionality

Modulation Process of imposing the baseband onto the carrier. The baseband is used to alter one aspect of the carrier, such as: signal strength (*amplitude modulation AM*), frequency (*frequency modulation FM*), phase (*phase modulation PM*). In other words, one of the values A, f, ϕ in the above equation of the signal is manipulated.

Phase-shift keying PSK Modulation technique varying the phase of the carrier. Used e.g. in WiFi, RFID, Bluetooth. Specific versions include Binary PSK, Quadrature PSK and Differential PSK. Simple example: if the baseband bit is 0 do nothing to the carrier, if it is 1 shift the carrier phase by π.

I-Q Signal Representation A pair of periodic signals are said to be in 'quadrature' when they differ in phase by 90 degrees (e.g. the sine and cosine wave). The 'in-phase' or reference signal is referred to as 'I' (conventionally cosine), and the signal that is shifted by 90 degrees (in quadrature) is called 'Q' (conventionally sine). Used to represent modulations.

Antenna Interface between radio waves in the air and electric alternating currents in a conductor. Types include: omni/dipole, yagi, horn, cantenna.

The directionality of an antenna described how well it transmits/receives into a particular direction.

- **isotropic** – Theoretical, radiates with the same intensity equally in all directions. Often used as a reference antenna when calculating the gain.
- **omni-directional** – Radiates equally well in all directions in a flat horizontal plane. Most common types in consumer devices.
- **directional** – Radiates best in a given direction by focussing its power. Can thus work with weaker signals than an omni-directional antenna of the same power.

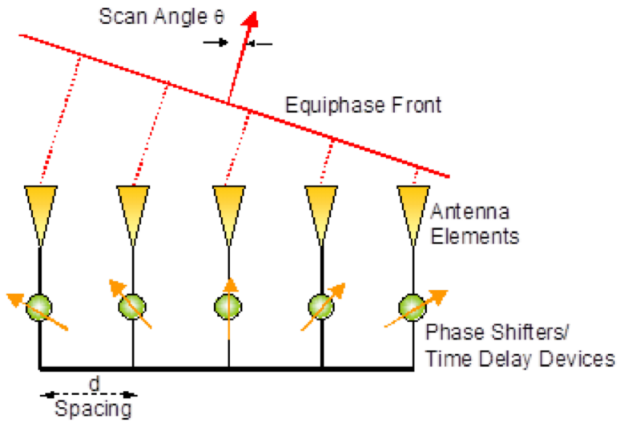

Figure 4: Beam steering

Phased Array Array of fixed antennas where the phase of each signal is dynamically adjusted so that the signal will be in phase for a given direction. Allows *beam steering* towards a specific direction. Possible applications? Can it be used to achieve security (e.g. confidentiality)?

Transmitter/Receiver Converts from digital to analogue, applies modulation and connects to the antenna (and vice versa). Properties: transmitted power, carrier frequency, information bandwidth, modulation type, receiver sensitivity.

Software Defined Radio SDR Flexible, low-cost transmitter/receiver. Implements components (mixer, amplifier, de-/modulator) in software rather than processing the signal in hardware.

Channel equation See Figure 5.

signal strength at the receiver = transm. power + transm. antenna gain − link loss + receiv. antenna gain

Note that in free space the power density of an EM wave obeys the inverse-square law:

$$p \propto \frac{1}{d^2}$$

Receiver sensitivity The weakest signal from which the receiver can still obtain the desired information signal. Depends not just on the antenna gain, but also on other factors such as the noise.

Decibel

- dBm – signal strength in dB / 1 milliwatt mW
- dBW – signal strength in dB / 1 watt W
- dBi – antenna gain in dB / antenna gain of isotopic antenna in dB

Calculating a value in dB:

$$dB(n) = 10\log_{10}(n) \quad \text{and} \quad dBm(n) = 10\log_{10}(n/1mW)$$

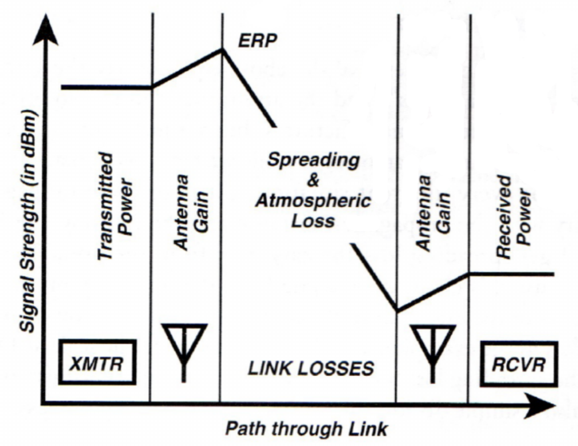

Figure 5: Signal strength across the channel (ERP = Effective Radiated Power)

Power Spectral Density diagram Depicts the power density (in dB) for a range of frequencies. In simple terms, it shows how strong the signal is at a given frequency.

Security Goals Reasons: *security* (integrity, confidentiality, authentication), *regulatory* (personal liability for misuse of one's network access), *safety* (RF-enabled implants).

Just reducing transmission power, hoping that the attacker will be too far away to listen on / send / modify messages, is NOT a solution. In fact, WiFi signals can be received 10 km away, and similarly Bluetooth at 1 km distance (with good, directed equipment).

Example: *passive keyless entry and start systems (PKES)*, i.e. wireless car keys. Wrongly assume communication implies physical proximity (relay attack). Needs: Authenticated proximity verification, message authentication.

2. Jamming Basics

Jamming Entirely preventing or reducing the ability of communicating parties to pass information, either intentionally or unintentionally.

The jamming signal needs to have the same frequency as the modulated signal. If the latter is unknown to the attacker, they thus need to jam a wide bandwidth of frequencies to be successful.

Effectively, jamming is always a power play.

Symbol Carries one or more bit of information, depending on the modulation scheme.

Symbol Jamming Corrupts symbols such that the receiver can EITHER no interpret them OR interprets them incorrectly.
Targeted, low-power jamming of specific symbols is hard!

Communication Jamming Corrupts enough bits that the information cannot be reconstructed any more, despite error correction.

Jamming-to-Signal Ratio J/S $= J - S$, i.e. the difference between the jamming signal and the modulated signal in dB. A ratio ≥ 0 usually results in successful jamming.

Burn-through range Range in which communication still succeeds, despite jamming.

2.1. Jamming Resistant Communication

Basic principle If you cannot fight (i.e. have too little power), RUN, HIDE or WAIT. And get ad advantage over the attacker: use a shared secret.

Frequency Hopping Spread Spectrum FHSS Regularly change transmission frequency. The pseudo-random frequency sequence is derived from a shared secret. Sender and receiver **must** be synchronised.

Note that frequency hoppers can be detected and located, simply by looking over time from which direction someone is sending on changing frequencies.

Possible attacks:

- **Partial band jammer:** Distribute jamming power over a subset of all hopping frequencies to achieve $J/S = 0$ at least on that range.
- **Follower jammer:** Detects on which frequency communication occurs and then jams it. Can be protected against by using error codes (since only the final bits will be corrupted).

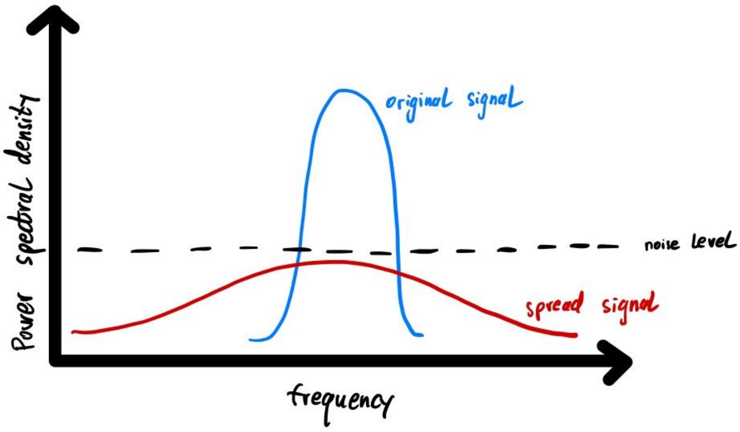

Figure 6: DSSS – hiding under the noise

Direct Sequence Spread Spectrum DSSS Spreads the baseband over a larger bandwidth using a shared secret (narrowband to broadband).
Since the transmission power remains the same, the power density at any given frequency decreases. Thus the spread signal can effectively "hide under the noise" (Figure 6).

To spread over more frequencies, we need a higher symbol/bit rate. To achieve this the information signal is multiplied with a high-frequency pseudorandom sequence called **chips** or **spreading code**. The result resembles **white noise**. See Figure 7.

During de-spreading, the signal is again multiplied with the same spreading code. De-spreading thus converts the wideband signal into a narrowband one (this works due to the autocorrelation properties of the spreading code). At the same time, any narrowband interference is spread out.
Thus DSSS is more robust against (un)intentional interference and multipath effects, and narrowband jamming requires much more power. Broadband jamming is possible, but inherently requires much power.

Detecting DSSS signals is difficult, but not impossible (energy detection of strong signals, signal characteristics such as constant chip rate). Interception and modification is hard.

Example usages: GPS, 802.11b WiFi, CDMA (used in 3G). Non-military applications mainly use DSSS for interference-resistance and use public spreading codes. They are thus still vulnerable to malicious jamming as DoS.

Processing Gain PG Ratio of the spread bandwidth to the baseband bandwidth, in dB.

Chirp Signal / Sweep Signal Signal in which the frequency increases and decreases over time ("sweeping" over a bandwidth much wider than the baseband bandwidth). Narrowband and partial-band jamming are prevented, follower jamming not so much

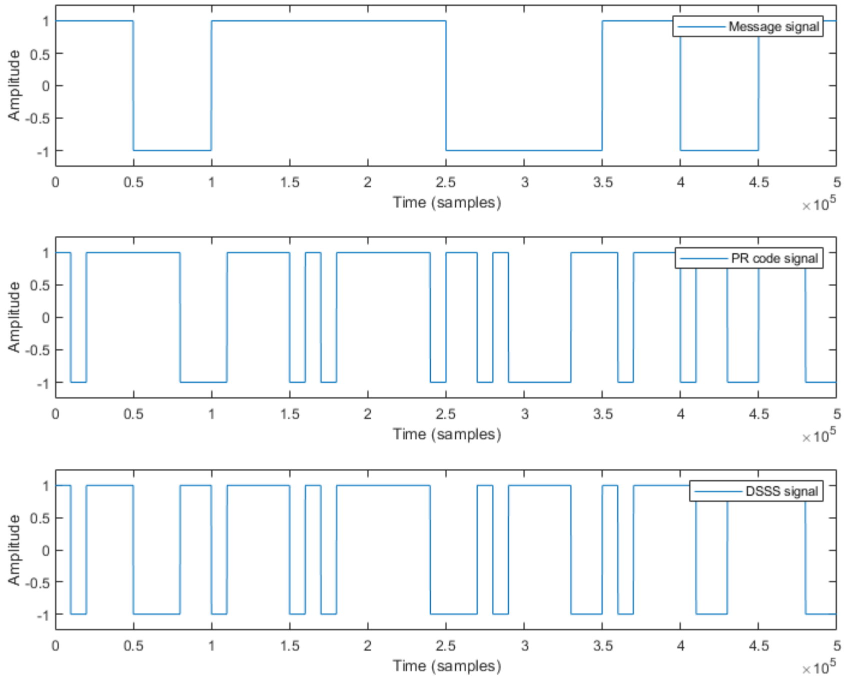

Figure 7: DSSS – baseband signal, spreading code, spread signal (top to bottom)

A. Imprint

This document closely follows the lecture slides of the *Security of Wireless Networks* lecture in the spring semester 2020 at ETH Zurich. Our contribution to this is editing the whole lot and refactoring even more so that it may fit the "lecture summary" style. However, basically all graphics are copy & pasted from the slides. If you don't want yours here, please contact us and we will remove them.

In addition, it is based on another summary by Sarah Kamp.

Otherwise, our part of the work is published as CC BY-NC-SA.