Security of Wireless Networks

{thgoebel}@ethz.ch

ETH Zürich, HS 2020

This 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

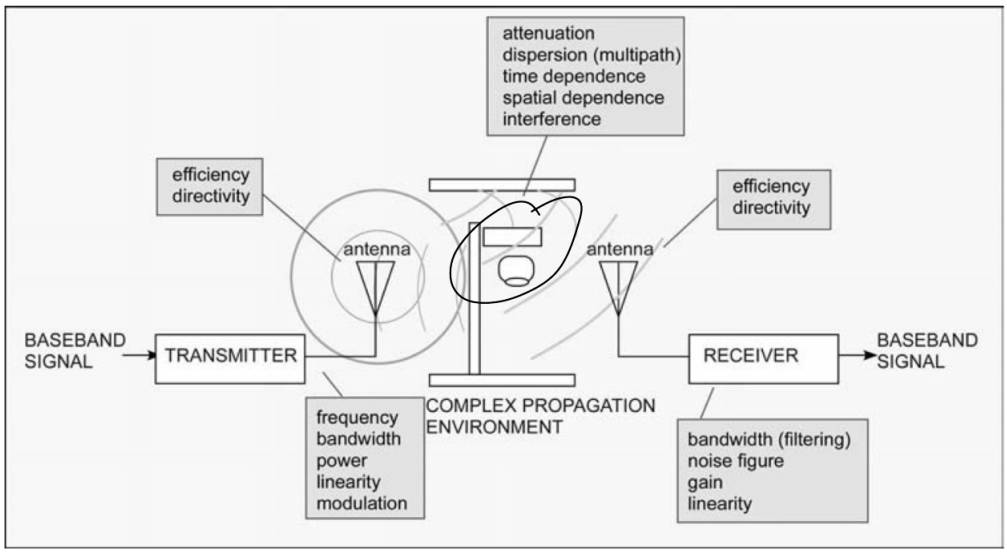

Figure 1: A wireless system, its basic components and characteristic measures

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 (subsection 2.1).

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.

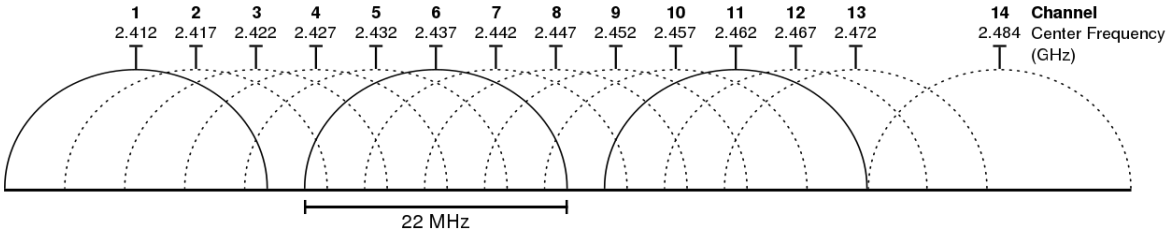

Figure 2: 2.4 GHz WiFi Channels [Source]

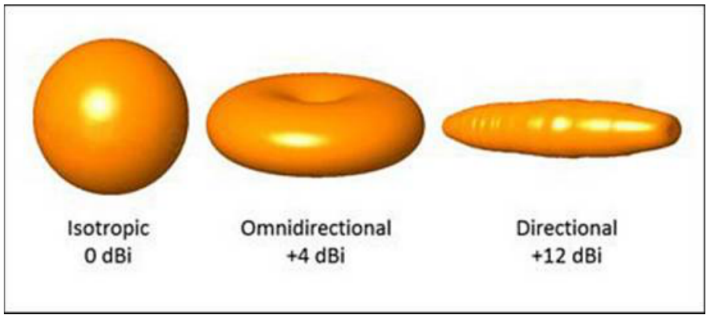

Figure 3: Antenna directionality

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.

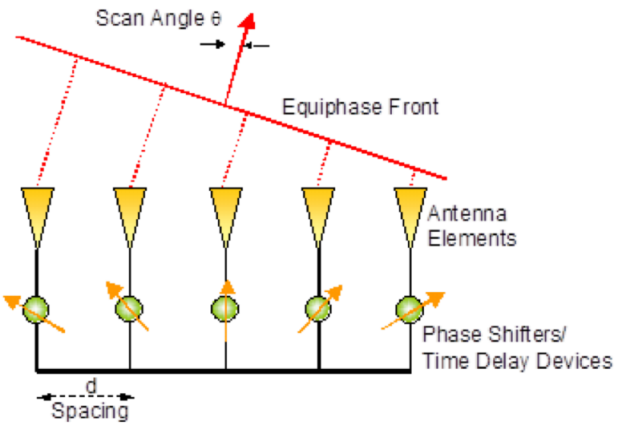

Figure 4: Beam steering

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:

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

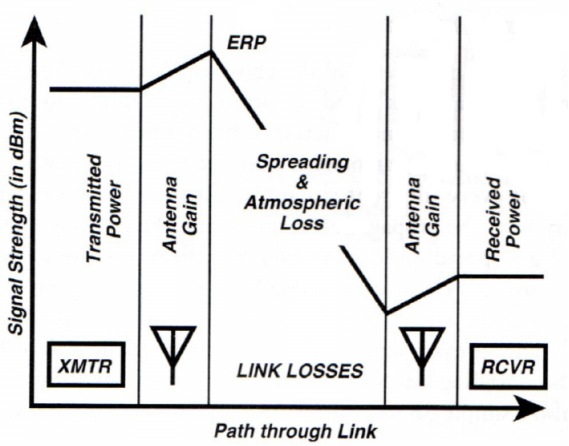

Figure 5: Signal strength across the channel (ERP = Effective Radiated Power)

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.

Attacker model
Types: responsive, sweep, random
Actions: jam, insert, modify (= overshadow)
Power to jam/insert/modify: P_j, P_t, P_o
channels to jam/insert/modify: c_j, c_t, c_o
Total strength/power P_T

$$c_j P_j + c_t P_t + c_o P_o \leq P_T$$

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.

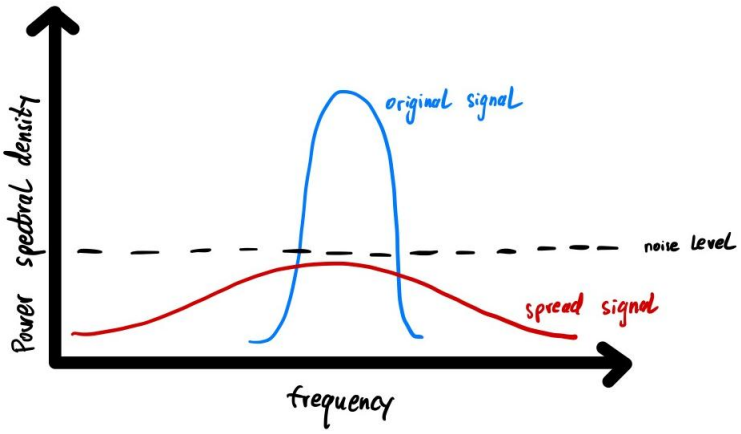

Figure 6: DSSS – hiding under the noise

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).

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.

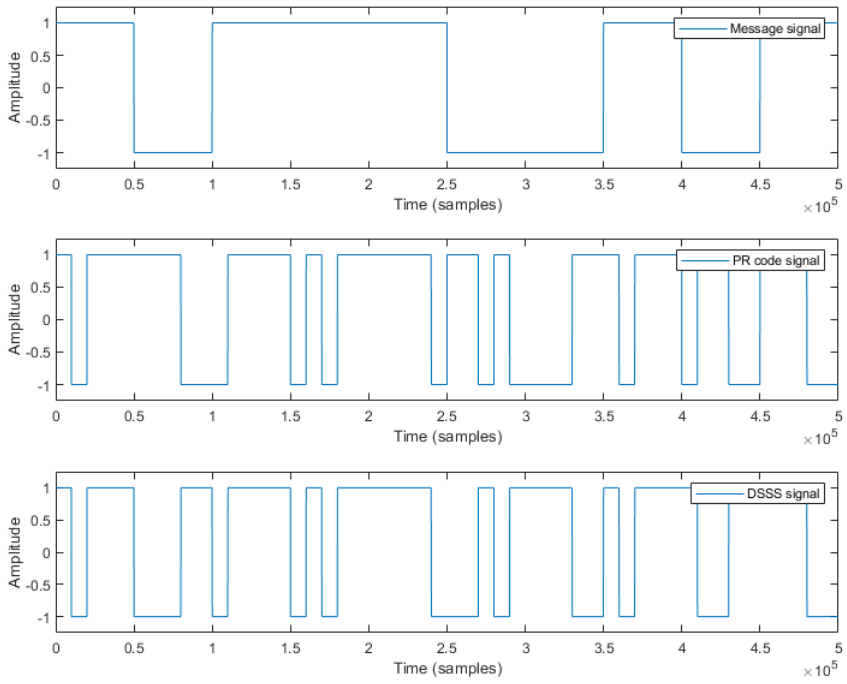

Figure 7: DSSS – baseband signal, spreading code, spread signal (top to bottom)

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

Code-Division Multiple Access CDMA Multiple transmitters sending in the same area simultaneously, but using different spreading codes. Allows sharing of the same frequencies/bandwidth without interference.

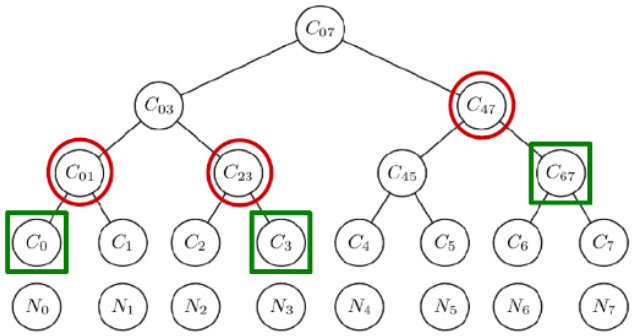

Figure 8: Dynamic Jamming Mitigation – cover codes (red circle), test code (green square)

3. Jamming-Resistant Broadcast

Broadcast Communication One sender, many receivers. Inherently open: receivers may join and leave at any time. All receivers listen (c.f. multicast). E.g. radio (FM/AM), GPS.

Challenges when securing broadcast:
many and unknown receivers, colluding receivers, internal + external attackers. In particular, plain spreading techniques (with group keys) do not work – an interal attacker can use their knowledge to jam other receivers.

Based on FHSS Broadcast Anti-Jamming System due to Desmedt et al.
Base station transmits on multiple frequencies simultaneously. Each receiver listens on a subset of frequencies at a given time. Protects against $j-1$ colluding receivers, ensuring that each receiver has at least one non-jammed channel.

- **[Public] Channel Allocation Table:** Defines which channels any receiver should listen on, such that $j-1$ receivers do not cover all channels of any other receiver (set coverage).
- **[Secret] Frequency Allocation Table:** Mapping from channel id to frequencies. Derived using a PRG. The complete table is only known to the base station.

Disadvantages: effectively a multicast solution since it requires a shared secret between the base station and each receiver.

Based on DSSS Dynamic Jamming Mitigation due to Chiang and Hu. Counteract jamming by using a balanced binary key tree.
Each node in the tree corresponds to a spreading code C_i. Each receiver N_i is assigned a leaf and knows all codes on the path from the root to that leaf.
The base station transmits on (a) a disjoint cover of codes (i.e. all users can decode exactly one code) and (b) a set of test codes. If a client receives a test code but not the detectable code, it reports jamming.
Splitting and reforming of the tree enables jamming mitigation.

Disadvantages: requires highly flexible, powerful base station. Requires a feedback channel. Requires a growing number of shared secrets (and receivers must be known).

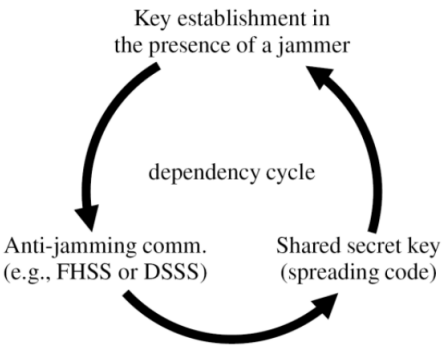

Figure 9: Circular dependency between anti-jamming and key establishment

Anti-Jamming—Key-Establishment Dependency Above techniques lead to a circular dependency. We need techniques without shared secrets! Idea: if we cannot coordinate sender and receiver, then don't even try (see next two techniques).

In addition, pre-loading shared keys in full of problems: requires a trusted party, key revocation, new clients joining, etc.

Uncoordinated Frequency Hopping Spread Spectrum UFH Neither attacker nor legitimate receivers can predict which channels are used. Equivalent to FH in terms of jamming protection (but not in throughput).

Transmitter steps:

1. Fragment message
2. Link fragments (against insertion)
3. Encode packets (ECC against jamming)
4. Repeated transmission while hopping on frequencies

Receiver steps: same process but reversed (plus packet ordering). Hops from one frequency to the other (sequentially is fine), in the hope of receiving a fragment.

Issue with fragment linking:
The signature is only verified at the end for the entire message.[1] Since there are exponentially many combinations for re-assembly, the attacker can now perform a DoS on a logical (rather than physical) level (pollution attack).
Solution: cryptographic linking of fragments (but without a shared key). E.g. hash linking, one-way accumulators, short signatures.

Disadvantages: Throughout up to 1000x less than FH. Higher latency (depending on attacker strengths, i.e. how high the chances are that the receiver gets a packet).

[1]The signature is based on public-keys and a mutually trusted – but potentially offline – certificate authority CA.

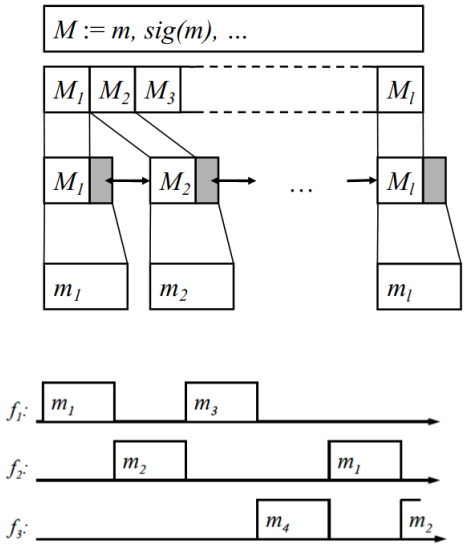

Figure 10: UFH transmitter steps

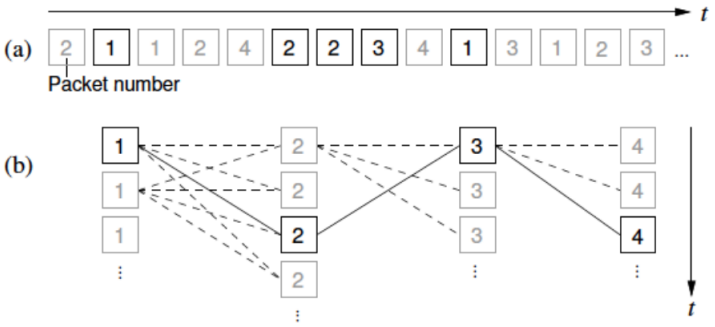

Figure 11: UFH fragment linking – exponentially many candidate messages

Uncoordinates Direct Sequence Spread Spectrum UDSSS Neither attacker nor legitimate receivers can predict which spreading codes are used. The public code set C is composed of n code sequences, each containing l spreading codes.[2] Despreading is done by trial-and-error: it requires the correct code sequence and correct synchronisation (which fragment are we at?). The message is also repeatedly sent because of possible jamming – possibly in parallel to improve throughput.

Optimisation: first transmit the message M with a secret spreading code K using DSSS. Then transmit the spreading code K using UDSSS.
Advantage: quicker decoding, longer messages, flexible security level.

[2]This allows a message to be fragmented into l pieces.

4. Security of Global Navigation Satellite Systems GNSS

Overview Orbiting satellites transmit their location and a precise timestamp. Receivers collect these navigation messages and their arrival time and use **triangulation** to calculate their own position. Satellites are positioned such that at least four are always in sight on any point on Earth.

Three segments: users, satellites, ground control.[3]

Signalling Each satellite modulates the navigation message with a spreading code (coarse acquisition C/A for civilians (public), precision P/Y for military (secret)). The spread signal is then modulated onto a carrier.
Individual satellites use individual spreading codes to allow distinction.
GPS sends on two carrier frequencies at the same time, L1 (1575.42 MHz = 10.23 MHz × 154) and L2 (1227.60 MHz = 10.23 MHz × 120).[4] Apart from jamming resistance and redundancy, this also allows to calculate the ionospheric delay error.
Due to atmospheric attenuation, down on Earth the GPS signal is well below the thermal noise.

Navigation message Each message consists of 25 frames. Each takes 30 sec to transmit, so the total time is 12.5 min.
Each frame contains: satellite clock + health data, 2x ephemeris (orbit details), other data + almanac (orbital + clock details).

Time of Arrival TOA Travel time of the signal from the satellite to the receiver. Used to calculate the distance and thus eventually the receiver position. Found by sliding the spreading code over the received message until a correlation peak.

Spoofing attacks Messages are unauthenticated (for practical reasons, else they would become too long).
By sending stronger signals, overshadowing the legitimate ones, an attacker can modify the *navigation message contents* (transmission time, satellite location) or their *time of arrival* (retransmitting captured signals with a temporal shift), resulting in a wrong location being calculated.
This is an issue in civilian GPS (messages can be generated and delayed) as well as in military GPS (messages can only be delayed since they are encrypted). Unfortunately, commercial GPS signal generators are becoming increasingly cheap.

4.1. Spoofing Detection and Mitigation

Types of countermeasures

- **Infrastructure/protocol:** e.g. cryptographic authentication of navigation messages
- **Receivers:** Use physical-layer characteristics of the signal to validate the signal as well as the calculated position/velocity/time. E.g. direction of arrival, carrier phase, signal strength, etc.

[3] There are of course issues with special and general relativity that mess with the time.
[4] This only applies to military. The civilian C/A is only transmitted on L1.

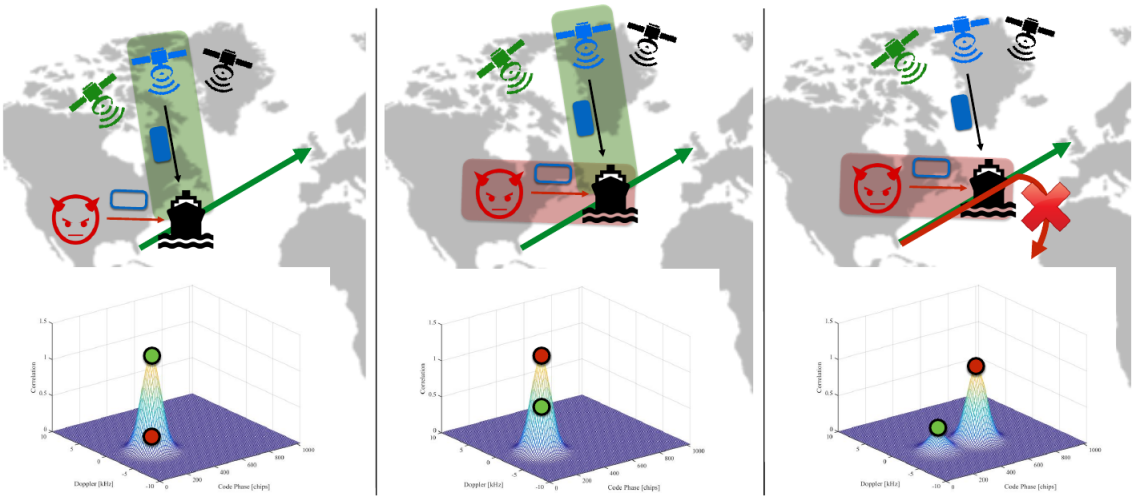

Figure 12: Seamless takeover attack

Angle of Arrival AoA Use multiple antennas (e.g. on both ends of a ship) to calculate the angle of arrival through the phase difference and the known distance between the antennas (see beam steering, Figure 4). In a spoofed scenario, the angles would all be very similar. Restricts the locations from which the attacker can successfully spoof.

Problems: Attacker can use drones to spoof signal from more realistic angle. Reflection of legitimate signal of buildings (thus reaching the receiver at a shallower angle) could be wrongly classified as spoofing. Computationally expensive phase measurement. Hardware modification.

Monitor Signal Characteristic Changes Over time, monitor signal properties such as AGC (Automatic Gain Control), noise level, number of satellites, spatial diversity (AoA) or the autocorrelation peak. Abrupt changes in any of these indicate presence of spoofing.

Seamless takeover attack The attacker starts transmitting a copy of a legitimate GPS signal in sync with the original one, but at low power, having no influence on the receiver. Then the attacker slowly starts increasing the power, until the receiver prefers the attacker signal. Now the attacker can change the GPS signal, and the receiver will keep following.

SPoofing REsistance GPS rEceiver SPREE Leverage peak tracking (of all signal peaks) to detect seamless takeover attacks. Navigation message inspection detects content spoofing.

Cryptographic approach (Kuhn)

1. At time t: satellite uses secret spreading code. Receiver uses a broadband receiver to capture the entire band.
2. At time $t+dt$: Satellite disclosed code, signing the disclosure with its secret key. Receiver verifies signature, de-spreads the signal.

Advantages: Prevents fake signal generation and individual signal delay.

Disadvantages: Requires pre-shared public satellite keys. Does NOT prevent full-band delay. Slightly inefficient (longer latency until signal lock). Replay attacks (?).

5. Secure Distance Measurement

Introduction

Applications: Wireless car keys, contact tracing in a pandemic, autonomous cars.
Attacks: **Replay attacks** are an issue, allowing an attacker to make devices appear physically closer (e.g. if the device naively use the observed signal strength to derive the distance).
Goals: (Provably) secure ranging, protecting against all logical and physical attacks and all attacker abilities. Focus on preventing distance reduction.

Current techniques (overview)

Non-Time-of-Flight:

- Received Signal Strength Indication RSSI (WiFi, Bluetooth, 802.15.4, NFC, RFID) – *insecure*
- (Multi-carrier) phase measurement[5] – *insecure*
- Frequency-Modulated Continuous-Wave FMCW – *insecure*

Time-of-Flight:[6]

- Chirp Spread Spectrum (802.15.4 CSS) – *insecure*
- Ultra Wide Band UWB (802.15.4z) – *proposed*
- WiFi 802.11az – *efforts to secure OFDM-based*
- 5G – *first academic proposals*

Model On a logical level, we have a **verifier V** and a **prover P**, between which we want to measure the distance. A **malicious party M** attacks this.

See also the Brands-Chaum protocol (not discussed in HS20).

Additionally, we assume the worst case for the users but the best case for the attacker (bad channel/noise/multipath versus perfect channel → attacker guesses will seem like noise).

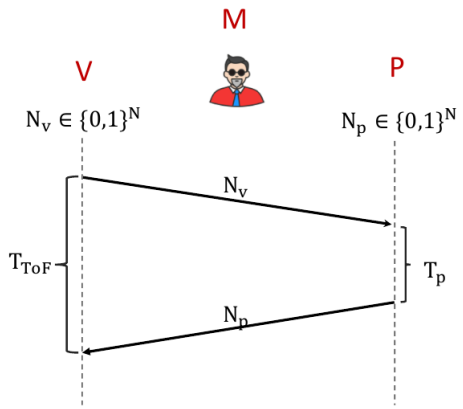

Figure 13: Model of the distance bounding scenario

[5] The distance is proportional to the phase.
[6] Calculate via $d = c \cdot (t_{tof} - t_{proc})/2$ where t_{tof} is the time between sending and receiving the signal and t_{proc} is the known processing time on the responding device.
In general, manipulating time is harder than manipulating signal properties (strength, phase).

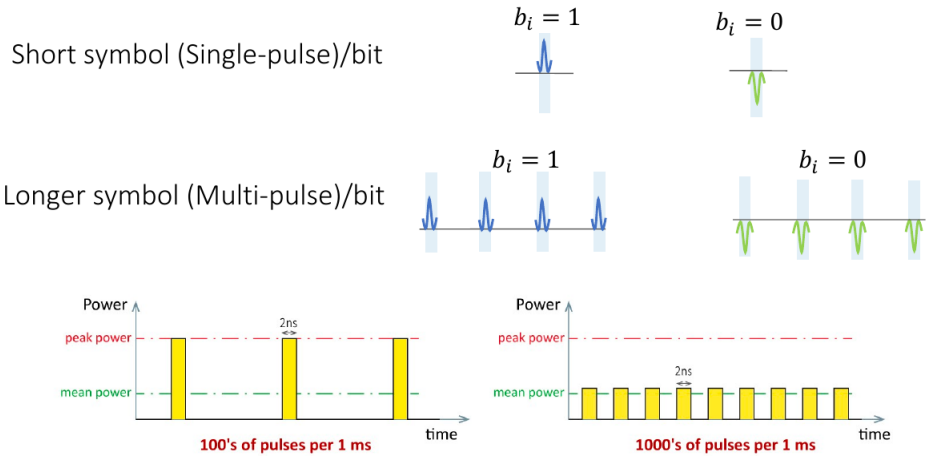

Figure 14: Bit representation: single- versus multi-pulse

Types of attacks (frauds)

- **Distance fraud:** A dishonest P tries to change its distance to V.
- **Mafia fraud:** Honest V, P being attacked by an external M.
- **Terrorist fraud:** Dishonest P and M collude to change P's distance.
- **Distance hijacking:** Dishonest P leverages an honest P to change its distance.

Physical layer: Representing bits as pulses (UWB) There are two design options to represent a bit: either with a single strong pulse or a sequence of weaker pulses. Single pulses may not be detected reliably (distance, interference), so the aggregate over several pulses is the preferred representation.

Early-Detect/Late-Commit attack (ED/LC) This attacks shortens the distance, since the receiver receives the first symbols earlier than it should have.

1. Attacker sends noise (at time T_A)
2. Attacker learns correct symbol (at time T_{ed})
3. Attacker commits to correct symbol (at time T_{lc}), by sending the remaining pulses such that the sum over all pulses matches.

Note that this attack is not possible with single pulses. A single pulse is usually 1-2 ns long, so the attacker can cheat by at most 15-30 cm (performance/security tradeoff).

ED/LC Solution 1: Pulse Reordering UWB-PR Interleave pulses of subsequent symbols according to some cryptographic reordering. Thus the start and end time of a symbol is unpredictable, and the attacker can only guess.
The probability of an attack decreases [increases] with the number of interleaved bits [number of pulses per bit].

ED/LC Solution 2: Variance Based Detection Statistically analyse the received versus the expected pulses. This forces the attacker to "guess better" to reduce the variance and make their error indistinguishable from the noise.

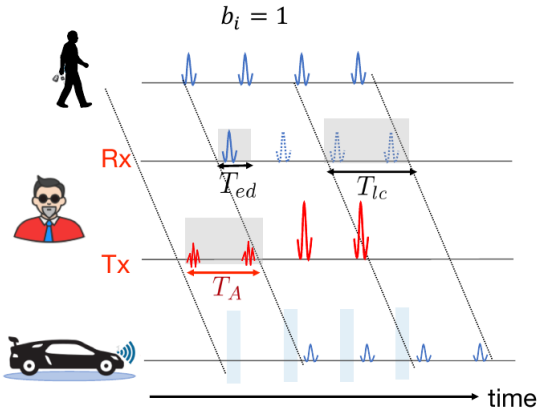

Figure 15: Early-Detect/Late-Commit attack (ED/LC)

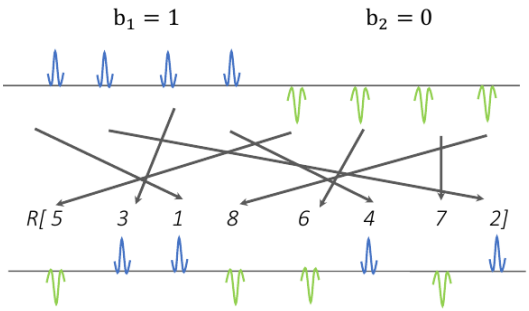

Figure 16: Pulse Reordering

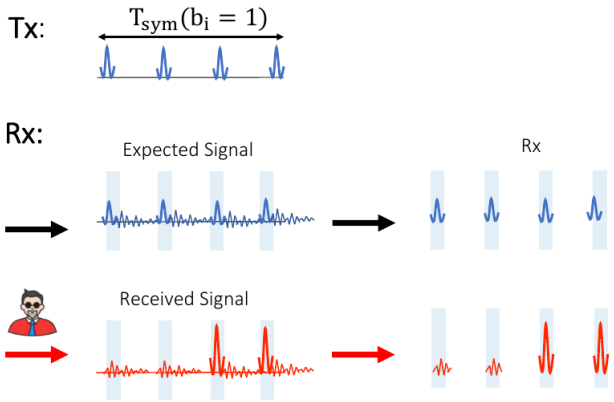

Figure 17: Variance Based Detection

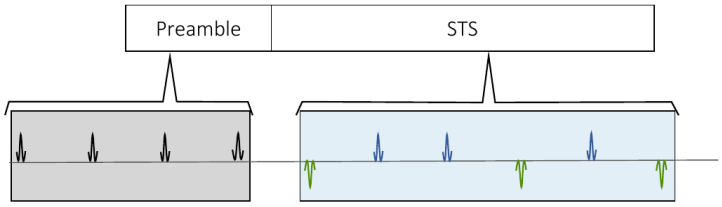

Figure 18: Scrambled Timestamp Sequence

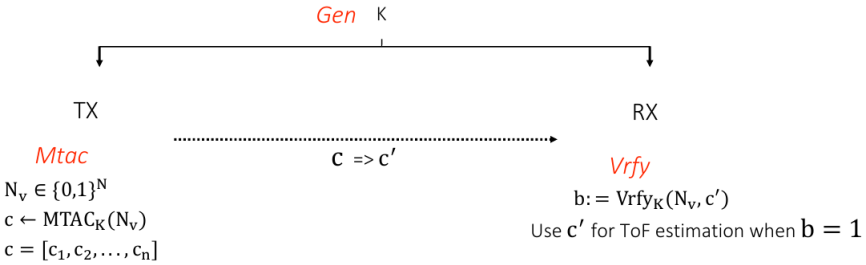

Figure 19: Message Time of Arrival Code MTAC

ED/LC Solution 3: Scrambled Timestamp Sequence After the preamble (high correlation) which is used for ToF *estimation*, send a Scrambled Timestamp Sequence STS (encrypted with a shared secret, low autocorrelation) to use for ToF *verification*.
See IEEE 802.15.4z. Security not formally proven and unclear!

IEEE 802.15.4z LRP versus HRP

Low Rate Pulse LRP	High Rate Pulse HRP
Can use single pulse	No single pulse (energy too low)
Multi-pulse with UWB-PR efficient	UWB-PR + variance-based seem inefficient
Open security specs	No open security analysis
Low-cost, low-energy	

Message Time of Arrival Code MTAC New class of cryptographic primitives that verify the integrity of message arrival time. E.g.: single-pulse, UWB-PR, Variance-based detection.

Verifiable Multilateration Multiple verifiers with known locations want to determine the position of a prover. C.f. GPS trilateration. E.g. to position autonomous cars using cell towers.

Future Work

- Secure Positioning (e.g. verifiable multilateration)
- WiFi 802.11 and 5G ranging (some initial work)
- Efficient implementation + deployment

A. Imprint

This document closely follows the lecture slides of the *Security of Wireless Networks* lecture in the autumn 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.