Security of Wireless Networks AS20

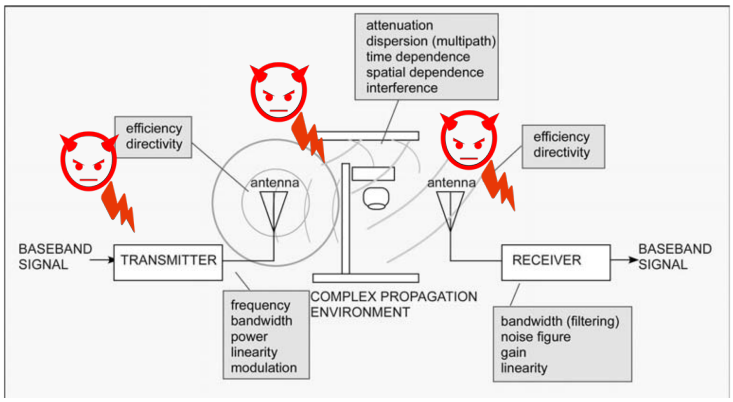
jasonf

Sept 20

Contents

1 Basics of Wireless Communication

1.1 Basics



Radio Frequency Signal (RF):
- Communication using EM radiation waves at frq 3kHz-300GHz.
- Waves created by alternating current at desired communicatino frequency.
- $s(t) = Acos(2\pi f t + \phi)$
- f=frequency (Hz), A=Amplitude, t=time, ϕ=phase, λ=wavelength=c/f, T=period=$1/f$.
- Inverse-square law wrt the distance from the source p proportional to $17d^{\text{`}2}$

Modulation: Signal modulation changes a sine wave to encode information. Different modulation techniques will require different bandwidths for the same data rate.
- Binary Phase Shift Keying (BPSK)
- Amplitude Shift Keying (ASK)

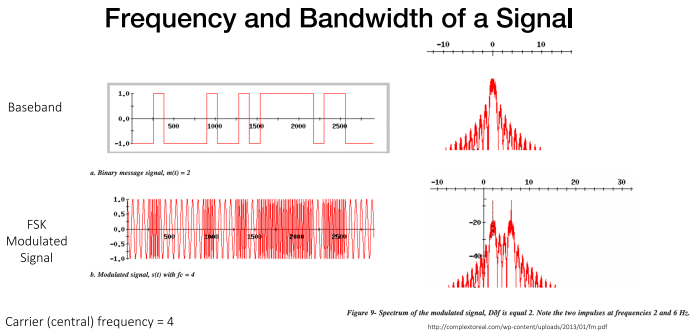
Bandwidth: Bandwidth can be imagined as a frequency width, sort of the fatness of the signal. What is the bandwidth of the modulated signal? It is still the same. The modulated signal takes on the bandwidth of the information signal it is carrying.

Baseband Signal: Actual Information message you want to transmit.s

I/Q Signal representation: Precisely varying the phase of a high frequency carrier sine wave in a hardware circuit according to an input message signal is difficult. Modulated information signal, that is not upmixed to carrier frequency yet (I/Q Data). A simple way of representing amplitude an phase of a signal.

RF Upconverter: generates the carrier signal with amplitude and phase from I/Q data and returns the RF signal.

Frequency and Bandwidth of a Signal: Bandwidth = measure of frequency content of the signal



Note: Different modulation techniques will require different bandwidths for the same data rate.

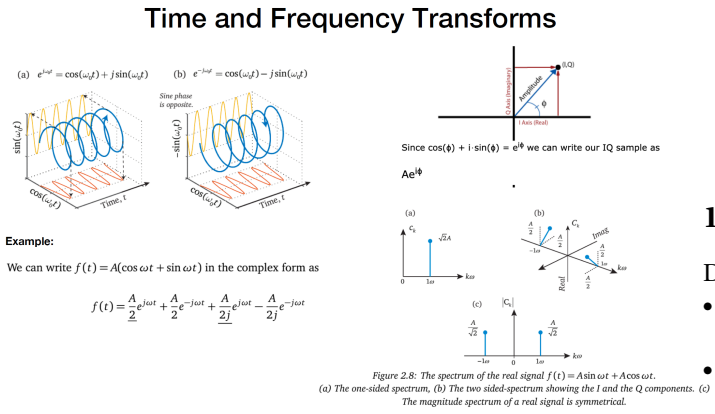


Figure 2.8: The spectrum of the real signal $f(t) = A\sin\omega t + A\cos\omega t$. (a) The one-sided spectrum, (b) The two sided-spectrum showing the I and the Q components. (c) The magnitude spectrum of a real signal is symmetrical.

Antennas and Propagation:

- Tradeoff: Antenna Gain vs Beamwidth
- Beam steering antennas: Phase of the signal to each antenna is adjusted such that all the signals will be in phase, when viewed from a certain direction. Can steer the antenna array to transmit signals or receive signals from specific direction. (example applications Mimo, selective target jamming)

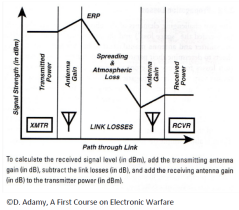
Transmitter Architecture: Key Properties are Transmitted power, carrier frequency, information bandwidth, modulation type.

Receiver Architecture:

- Key Properties: Receiver sensitivity (depends on the antenna, low noise amplifier, mixer)
- Software Defined Receivers SDR: low-cost, traditional components (such as mixers, amplifiers, modulators implemented in software), signal processed in PC.

Wireless Communication: Basics

- *Channel equation:*
- Example
  - Transmitted Power (1W) = +30 dBm
  - Transmitting Antenna Gain = +10 dB
  - *Spreading Loss = 100 dB*
  - Atmospheric Loss = 2 dB
  - *Receiving Antenna Gain = +3 dB*
  - `Received Power`
    `= +30dBm + 10 dB – 100 dB – 2 dB + 3 dB`
    `= -59 dBm`
- *Receiver sensitivity:* The weakest signal from which the receiver can still provide the proper specified output.



To calculate the received signal level (in dBm), add the transmitting antenna gain (in dBi), subtract the link losses (in dB), and add the receiving antenna gain (in dBi) to the transmitter power (in dBm).

©D. Adamy, A First Course on Electronic Warfare

Wireless Communication: Basics

- Decibel: dB, dBi, dBm, ...
  - dBm = dB value of signal strength / 1 miliwatt (mW) used to describe signal strength.
  - dBW = dB value of signal strength / 1 watt (W) used to describe signal strength.
  - dBi = dB value of antenna gain relative to the gain of an isotropic antenna (0dBi is the gain of an isotropic antenna)

- A linear number is converted into dB, by the following formula:
  - $N(dB)=10\log_{10}(N)$
  - $N(dBm)=10\log_{10}(N/1mW)$
  - e.g. 1W = +30dBm
  - Note: log(x)+log(y)=log(xy); log(x)-log(y)=log(x/y)

1.2 Security

Do we need Security in Wireless Networks?

- We can't hide communication by disclosing carrier frequencies, as they can be discovered anyway by broadband receivers.
- We can't reach confidentiality through low power communication. Attacker with a good antenna might still pick up signal even though he is further away.
- Encryption, MAC/Signatures and new measures will help to increase security of wireless networks.

2 Basics of Signal Jamming

2.1 Introduction

Jamming: Entirely preventing or reducing the ability of communicating parties to pass information by the deliberate use of EM signals.

Symbols: Can carry one or more bits of information, depending on the modulation scheme.

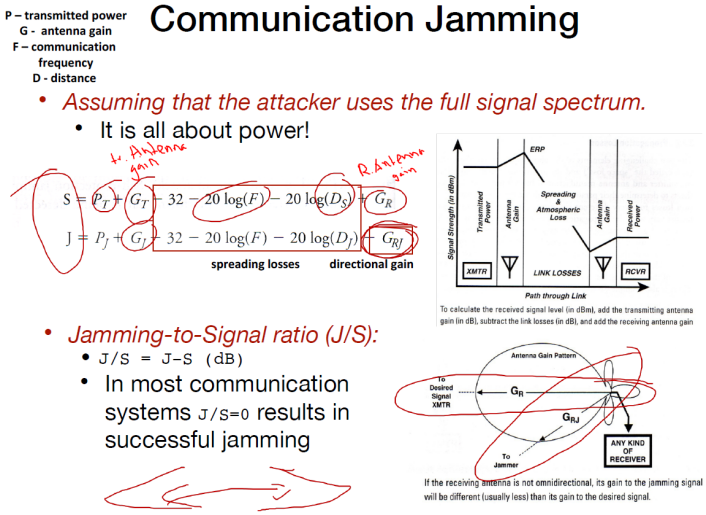
Symbol Jamming: Corrupt symbols such that the receiver either cannot interpret them or interprets them incorrectly

- Most communication systems will do error detection and correction
- Beyond a certain threshold of corrupted bits (given for each ECC scheme) the messages cannot be recovered.

→ Targeted low-power jamming of individual bits is not easy and might require synchronization.

Communication Jamming: Corrupt enough bits such that the information cannot be reconstructed (despite Error Correction).

- Frequency: To jam, the attacker needs to transmit on the right frequencies during the right time. (e.g., all or strongest frequency). Partial jamming might not prevent communication.
- However, attacker can jam most dominant frequencies and these are likely most important ones for signal transmission.
- Note: Receiver filters signals to the frequencies that he wishes to here, so only jamming w.r.t these frequencies will have effect.



Burn-through range: The range from which the sender succeeds in communicating with the receiver, despite jamming.

- Parameters that influence jamming

The Effect of Each Parameter in the Jamming Situation on J/S

Parameter (Increasing)	Effect on J/S	Type of Jamming
Jammer transmit power	Directly increases on J/S dB for dB	All
Jammer antenna gain	Directly increases J/S dB for dB	All
Signal frequency	None	All
Jammer-to-receiver distance	Decreases J/S as the distance^2	All
Signal transmit power	Directly decreases J/S dB for dB	All
Radar antenna gain	Decreases J/S dB for dB	Radar (self-protect)
Radar antenna gain	Decreases J/S 2 dB per dB	Radar (stand-off)
Radar-to-target distance	Increases J/S as the distance^4	Radar
Radar cross-section of target	Directly increases J/S dB for dB	Radar
Transmitter-to-receiver distance	Increases J/S as the distance^2	Comm
Transmit antenna gain	Directly decreases J/S dB for dB	Comm
(Directional) receiver antenna gain	Directly decreases J/S dB for dB	Comm

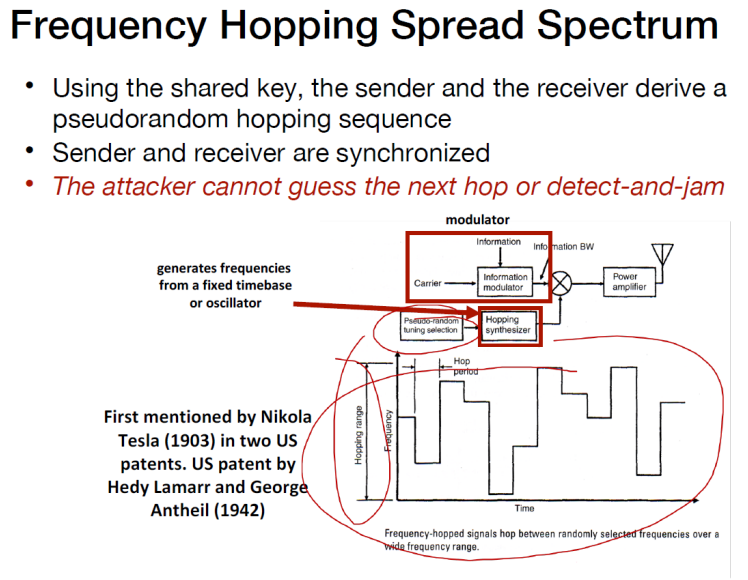
Jamming Implications:

- Denial of Service attacks
- Trick Public WiFi Localization Systems by jamming legitimate Access Points and inserting MACs of APs from other location.
-

2.2 Physical Layer Security

Basic Principle of Jamming Resistant Communication: If you cannot fight, RUN, HIDE (and WAIT). But we need an advantage over the attacker: a shared secret key between the sender and the receiver

2.2.1 Frequency Hopping Spread Spectrum FHSS



→ FHSS makes Partial Band Jammers useless.

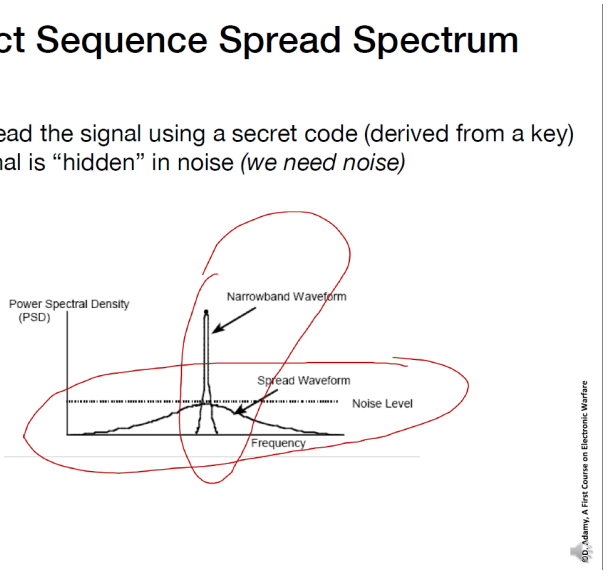
Follower Jammer

- First detects on which frequency communication is taking place and then jams.
- Protection: message encodings that enable message recovery despite of x% of it being corrupted

Detectability/Localization of FHSS transmitters

- FHSS transmitters do not really hide.
- Using AoA (Angle of Arrival) techniques can be localized.

2.2.2 Direct Sequence Spread Spectrum (DSSS)



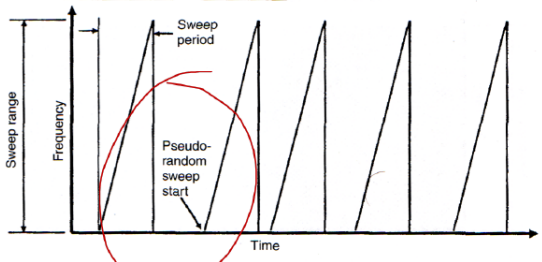
Spreading the frequency bandwidth to achieve DSSS:

- To spread, we need to transmit with a higher symbol rate.
- The original message is multiplied (xored) with a higher frequency spreading code (chips) that is either flipped for 0 or not for 1.
- This results in a signal with higher frequency bandwidth but lower signal power (per frequency band.
- Spreading code generator accepts a secret key.
- DSSS protects against Narrow-band jamming (now needs much higher power), because The same process that collapses the frequency spectrum of the spread-spectrum signal back to its information bandwidth spreads any nonsynchronized narrowband signal by the same factor
- Broad-band jamming is still effective (if you have enough power). Broadband jamming signal stays spreaded after passing through

the spreading demodulator, unless its spreading is synchronized with the secret spreading code of the demodulator.
- Hides the Signal in noise! Signal Detection is more difficult. (Can be done)
- Processing gain = $10log_{10}(f_{spread}/f_{unspread})$

2.2.3 Chirp Signals

Random start and then sweep (can be used with FH)
- Prevents narrow-band and partial-band jamming
- Follower jammers might be an issue



Chirp signals are rapidly swept over a frequency much wider than the information bandwidth of the transmitted signals.

2.3 Further Info

- Difficult to defend against can be only made more difficult.
- Typically combined with jammer detection and "neutralization".
- 802.11b uses DSSS but for interference resilience

3 Broadcast Jamming Resistant Communication

3.1 Introduction

Broadcast Communication
- One sender, many receivers.
- Open system: new receivers may join/witdraw, Any receiver can listen (in contrast to multicast)
- E.g.: radio broadcast, navigation signals.

Attacks on Broadcast Communication
- For pairwise (unicast) communication only consider external attackers
- For Broadcast communication consider external attackers and internal attackers

External Attackers on SS Techniques
- Does not know spreading code / hopping sequence
- Partial-band attacker can still jam. Example: FHSS

Internal Attacker on SS Techniques
- Legitimate receiver knows the spreading code and its synchronization!Can misuse this for jamming
- Group keys do not prevent this attack!

Anti-Jamming Broadcast
- Problem: Base station (BS) needs to broadcast an (authenticated/confidential) message to a large nr. of receivers in an anti-jamming manner.
- Desirable Properties:
  - Detect/ prevent jamming
  - Support a flexible nr of receivers
  - Tolerate a certain fraction of malicious receivers

3.2 Solutions based on Shared Keys

The following solutions rely on a shared secret, and thus follow the multicast strategy rather than broadcast.

3.2.1 Broadcast anti-jamming based on frequency hopping (FHSS)

Coding method provides protection against malicious receivers [Desmedt et al.]
- Base station transmits the same signal simultaneously on multiple frequencies
- Each receiver listens to a subset of these frequencies at a given time
- Threshold scheme: provides protection against up to j-1 colluding receivers
- Public Channel allocation Table: Defines the subset of channels where each receiver R_i is listening. j-i receivers do not cover all channels of any other receiver. Set coverage problem.
- Secret Frequency Allocation Table: The actual frequencies are secret. Created and updated via a pseudo-noise generator.
- The assigned frequencies can be distributed over a broad, non-continuous frequency band.
- Multicast solution
- Successful if: The group of colluders consists of j-1 or fewer members.

System Description:
- Channels $C = \{c_1, c_2, ..., c_m\}$
- Receivers $R = \{R_1, R_2, ..., R_l\}$
- Subsets of channels $CR = \{C_1, C_2, ..., C_l\}$

Theorem: If $|C_i| \geq l + (j-1)d$ for all $1 \leq i \leq l$ and $|C_i \cap C_k| \leq d$ for all $i \neq k$, then (C, CR) is a Broadcast Anti-Jamming System.

3.2.2 Dynamic Jamming Mitigation

Broadcast anti-jamming based on DSSS [Chiang and Hu]
- Counteract jamming by using a balanced binary key tree. Each node corresponds to a spreading code. Each user N_i is assigned to a leaf and knows all codes on the path from the root.
- The BS transmits on...
  - a disjoint cover of codes, i.e. all users can decode using exactly one code (of their many codes they got). Not necessarily the leaf node b.c. nodes on the path reach multiple users, so base station does not have to send with seperate code for all users.
  - a set of test codes
- If a user receives a message on a test code but not on the corresponding detectable code, it reports jamming.
- Splitting and reforming the tree allows the transmitter to send each transmission on $\leq 2j+1$ codes, where j is the (expected upper) nr of jammers.
- Requires highly flexible base station (sending and receiving on a potentially large nr of codes) and feedback channels. Not applicable to unidirectional broadcast.
- Nr of secrets grows with nr of receivers.
- multicast solution

3.3 Broadcast Anti-Jamming Techniques Without Shared Secrets

Goal: BS broadcasts authenticated message to a large nr of unknown/untrusted receivers in an anti-jamming manner.
Applications: alarm broadcast, navigation signals, ...
Problems:
- The prior schemes (Desmedt, Chiang) do not work for unknown receivers (they need a shared secret) and also Public-key crypto does not help.
- Anti-Jamming Key Establishment depends on jamming-resistant communication.

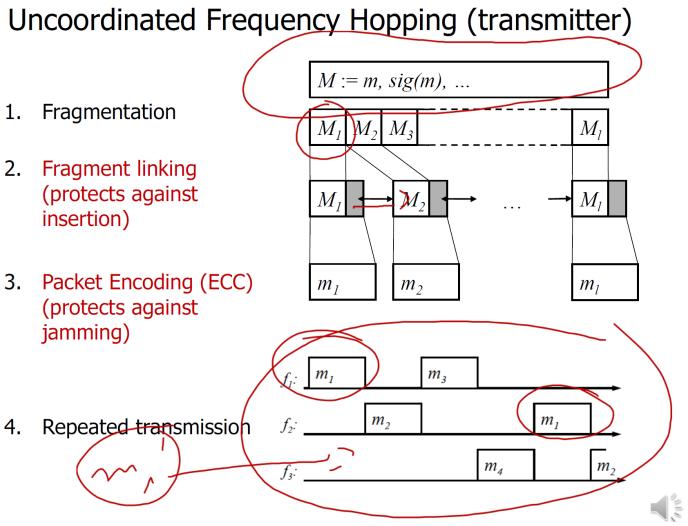
Solution Sender uses random hopping sequences / spreading codes unknown to the receiver. The attacker cannot predict which channels will be used (neither can the receiver). Latency and Throughput will probably decrease through this procedure (UDSSS definitely

has reduced latency compared to DSSS).

Attacker Model:

- goal: prevent communication
- actions: Jam, Insert, Modify

3.3.1 Uncoordinated Frequency Hopping (UFH)

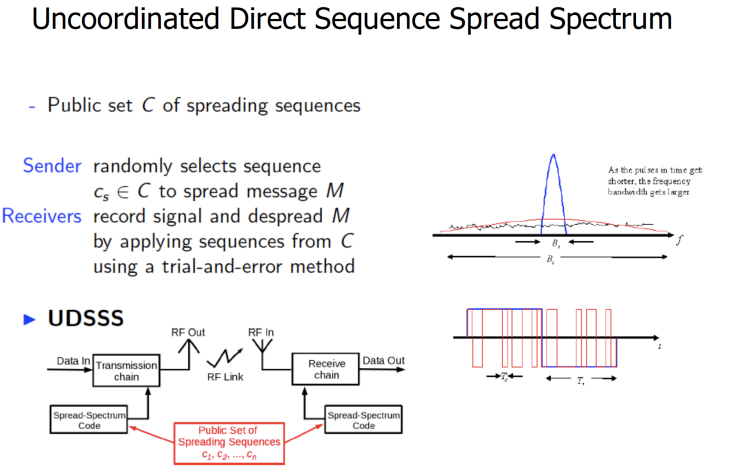


Throughput: Can be improved by using broadband receivers.

Problem: Fragments are not individually authenticated, thus we need cryptographic fragment linking (Hash linking, One-way Accumulators, Short signatures) and signature verification to achieve message integrity. If not Attacker can perform a DoS attack by increasing the space over which receiver has to try to link fragments, by inserting fake fragments. Signatures and accumulators are better than hash linking b.c. they reduce this search space!

3.3.2 Uncoordinated Direct Sequence Spread Spectrum (UDSSS)

Basic Idea: Public code set C composed of n code sequences, each of which is composed of l spreading codes containing N chips. Successful despreading requires to hit the correct spreading sequence and the correct synchronization.



Message Repetitions: due to both the lacking synchronizatino between sender and receivers and the possibility of successful jamming attacks.

Throughput: Can be improved by using parallelization.

Further Optimization: Use UDSSS to transmit the spreading key only. First transmit message M using a random spreading code K, then transmit the spreading code K using UDSSS. Smaller spreading code set, Quicker decoding, Longer messages and more flexible security level.

Applications: For positioning and/or time-synchroization

3.4 Application of Anti-Jamming Techniques to Key Establishement

Problems with Key Establishement:

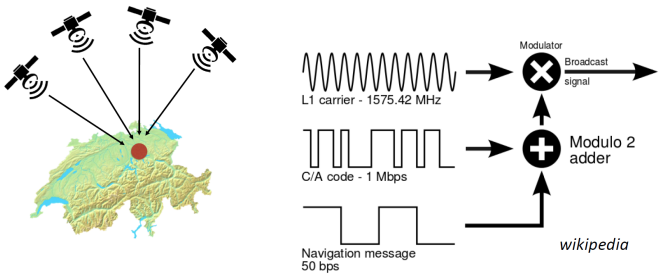
- Pre-sharing symmetric keys: Efficient but a trusted third party is needed, suffers from network dynamics problems (new nodes joining, key revocation, key compromise)
- Key establishment: Based on public-key crypto (RSA, DH), requires reliable communication.

Key Idea: break the anti-jamming/key-establishment dependency cycle by using UFH.

4 Security of GNSS

Global Positioning System (GPS):

- 24 satellites at about 20'200 km above earth. Each satellite transmits navigation messages containing its location and precise time of transmission.
- Unique pseudorandom codes are used
- GPS receiver measures each navigation message's arrival time and estimates its distance to the satellite.
- Receivers position and time is calculated using trilateration.
- **C/A (Coarse Acquisition) codes:** (Coarse Acquisition) codes: Gold Codes, 1023 chips, transmitted at 1.023 Mbits (i.e., repeats every 1ms), uses L1 only
- **P (precision) codes:** 6.1871×10^{12} chips long, transmitted at 10.23 Mbit/s, (i.e. repeats once a week), uses L1 and L2 only
- **Y (P(Y)) code:** encrypted P code (modulated with secret W)
- L1 = 1575.42 MHz, L2 = 1227.60 MHz
- DSSS is used to make the signal more robust (b.c. of distance we end up below noice level at receiver)

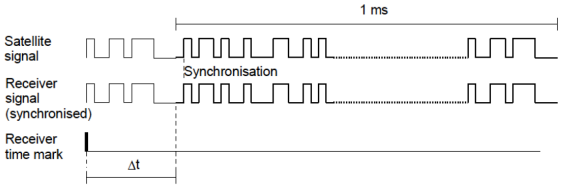


	Gain (+) /loss (-)	Absolute value
Power at the satellite transmitter		13.4dBW (43.4dBm=21.9W)
Satellite antenna gain (due to concentration of the signal at 14.3°)	+13.4dB	
Radiate power EIRP (Effective Integrated Radiate Power)		26.8dBW (56.8dBm)
Loss due to polarization mismatch	-3.4dB	
Signal attenuation in space	-184.4dB	
Signal attenuation in the atmosphere	-2.0dB	
Gain from the reception antenna	+3.0dB	
Power at receiver input		-160dBW (-130dBm=100.0*10^{-18}W)

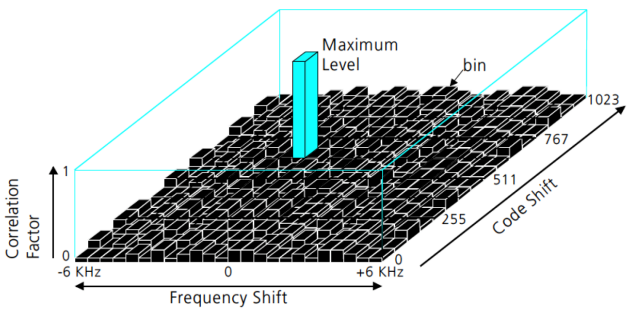
Satellite signal: The time to transmit all this information is **12.5 minutes**. By using the navigation message, the receiver is able to determine the transmission time of each satellite signal and the exact position of the satellite at the time of transmission.

- Satellite time and synchronization signals
- Precise satellite orbital data (ephemeris)
- Time correction information to determine the exact satellite time
- Approximate orbital data for all satellites (almanac)
- Correction signals to calculate signal transit time
- Data on the ionosphere
- Information on the operating status (health) of the satellite

Time of Arrival: Measuring signal travel times in GPS



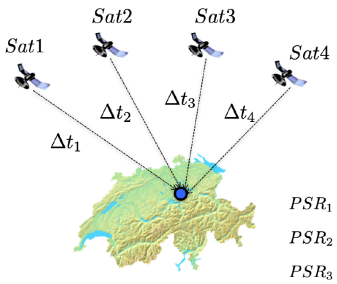
GPS: Time of Arrival + Doppler



We need to find best correlation between spreading code and received signal w.r.t. 2 dimensional signal. Along frequency shift (due to doppler effect that either squeezes or broadens signal, meaning increase or decrease frequency) and along code shift duet to synchronization of spreading code with received signal.

Received signal will be below thermal noise but despreaded signal will appear above noise level.

GPS: Estimating Position



τ	Receiver clock error
$(x_{sati}, y_{sati}, z_{sati})$	Known satellite coordinates
(x, y, z)	User co-ordinates
Δt_i	Signal transit times

$$PSR_1 = \sqrt{(x_{sat1} - x)^2 + (y_{sat1} - y) + (z_{sat1} - z)^2} + c \cdot \tau$$
$$PSR_2 = \sqrt{(x_{sat2} - x)^2 + (y_{sat2} - y) + (z_{sat2} - z)^2} + c \cdot \tau$$
$$PSR_3 = \sqrt{(x_{sat3} - x)^2 + (y_{sat3} - y) + (z_{sat3} - z)^2} + c \cdot \tau$$
$$PSR_4 = \sqrt{(x_{sat4} - x)^2 + (y_{sat4} - y) + (z_{sat4} - z)^2} + c \cdot \tau$$

(x, y, z) is determined by solving the above equations using Taylor series linearization and simplification

4.1 GPS Signal Spoofing Attack

- Attacker transmits specially crafted signals identical to sattellite signals but at higher power to overshadow legitimate satellite signals. But either modify navigation message contents or manipulate the time of arrival.
- Receiver computes a false location base on the attackers spoofing signals
- There is an increasing availability of commercial GPS signal generators and low-cost radio hardware, which makes such an attack easy.
- Civilian GPS are not authenticated and can be generated OR delayed. Military GPS signals can only be delayed

4.2 Detection and Mitigation of GPS Spoofing

Countermeasures:

- Infrastructure modifications: Adding cryptographic authentication to the navigation messages.
- Receiver end modifications:
  - Spatial characteristics of the received signal (e.g. Angle of arrival, carrier phase measurements)
  - Other physical-layer characteristics of the received GPS signals (received signal strength, AGC)
  - Additional sensors or receivers to validate the estimated position, velocity and time.

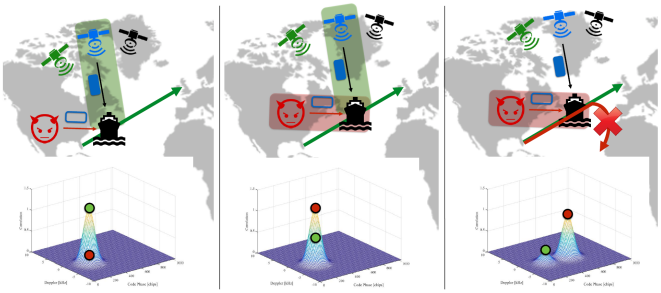
Angle of arrival: is a function of the measured signal phase difference σ at two close antennas and their separation D.
To mitigate spoofing attack, check if the signal truely comes from the direction where the satellite should be. Problem: Legitimate GPS signal may bounce of objects (multipathing) and thus not have expected angle and an attacker could use a drone to transmit the signal from there. And to reliably detect angle of arrival we need two antennas.

Monitoring Signal Characteristics: Detect spoofing without changes to GPS, but monitoring of signal characteristics:

- AGC, Noise level, nr. of satellites
- Autocorrelation Peak Distortion
- Spatial Diversity (AoA)

4.2.1 SPREE - Spoofing Resistant GPS Receiver

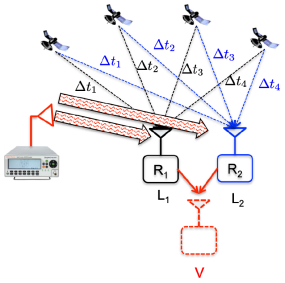
- The first GPS receiver capable of detecting (up to an accuracy) all known spoofing attacks.
- A novel auxiliary peak tracking technique enables detection of a seamless takeover attacks (tracks all peaks).
- Perform some sanity checks on the peaks to detect if a peak is even possible or reasonable.



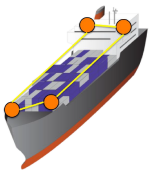
NON-Time-of-Flight:
- RSSI measurement (e.g., WiFi, Bluetooth, 802.15.4, NFC / RFID) – Insecure
- Phase (multi-carrier) measurement (e.g., Atmel AT86RF233) – Insecure
- FMCW (Frequency-Modulated Continuous-Wave) – Insecure

Time-of-Flight:
- Chirp Spread Spectrum (802.15.4 CSS, ISO/IEC 24730-5) – Insecure
- **Ultra Wide Band (UWB)** IEEE 802.15.4z (Aug 2020) – proposed for secure ranging
  https://standards.ieee.org/standard/802_15_4z-2020.html
- **WiFi** IEEE 802.11az, Next Generation Positioning, effort to secure OFDM-based ranging https://www.ieee802.org/11/Reports/tgaz_update.htm
- 5G, first academic proposals towards secure ranging

4.2.2 Leveraging Spatial Diversity



Attacker transmits omnidirectionally
=> Both R1 and R2 compute their positioning at V



If d(R1,R2) is known
=> spoofing detection

Test if positions of different antennas match up relatively to each other. An attack now is still possible but it reduces the locations, where he can place spoofers (The GPS Group Spoofing Problem). The attacker needs to find GPS signals, transmission times and spoofer locations such that the location or time of each victim is spoofed to the desired location/time.

Broadcast systems like GPS cannot be fully secured, this would require bidirectional communication or communication from the device to the infrastructure.

4.2.3 Cryptographic Countermeasures

Proposal for a Secure GPS (Kuhn): Devices hold satellite public keys. At time t, a satellite uses a secret code to spread the navigation signal

- The receiver uses a broadband receiver to receive the whole signal band (receiver does not know the despreading coe yet)
- At time t + dt, the satellite discloses its secret code, signed with its private key
- The receiver gets the code, verifies the signatures and despreads the signals.

-> Prevents the generation of fake signals and their individual shifts.
-> Prevents pulse-delay of individual signals, but not of aggregated signals (full band)

- there are some issues with its efficiency.

5 Secure Distance Measurement

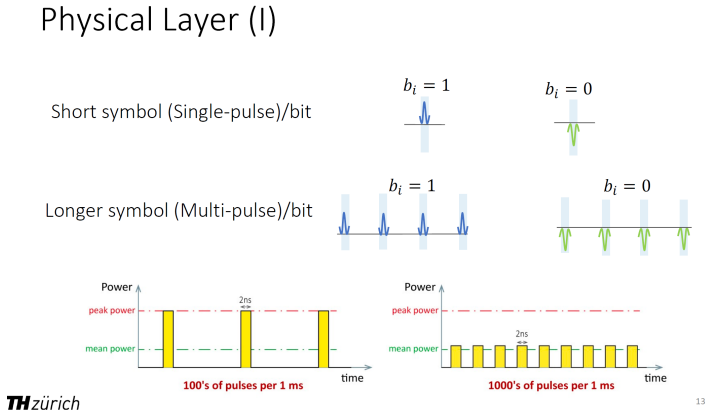
Applications:

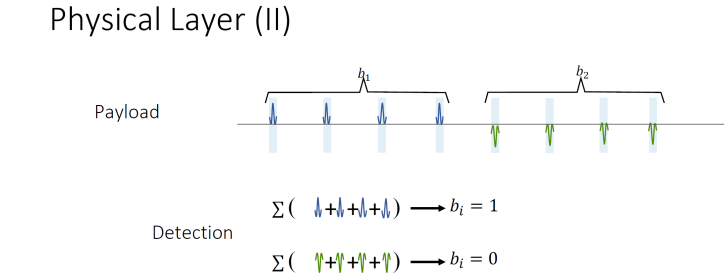
- Mitigate car key relay attack.
- Mitigate Contact Tracing Wormhole attacks.
- Mitigate Car distance spoofing attack.

-> We need ranging that is (provably) secure from all logical and physical layer attacks.

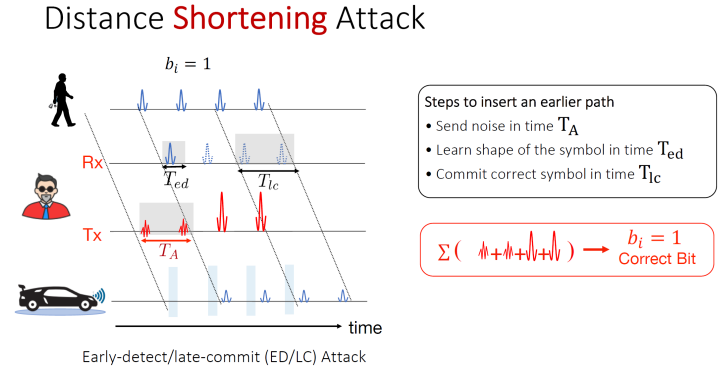
Ranging Techniques

Distance Bounding: There are different scenarios and attacks. But the most common scenario is:
V and P want to measure distance and trust each other, M tries to manipulate this process.





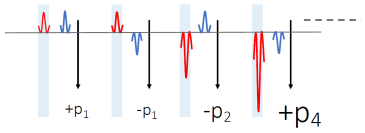
Single pulse might not be detected at the receiver (distance, interference).
We need to aggregate over several pulses => increase robustness and range.



Early-detect/late-commit (ED/LC) Attack

Performance/Security Tradeoff: We need longer symbols (multi-pulse) for performance (range and robustness). However, longer symbols are vulnerable to above attack

Why not Simply Randomize Pulses (insecure)



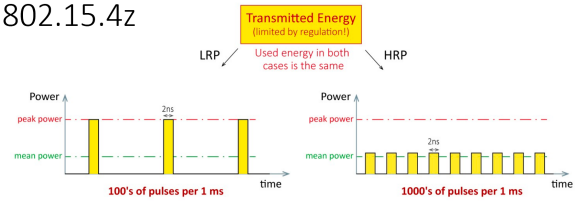
Attack:
- Predict the polarity of pulses correctly
- Compensate for wrong guesses with a higher transmission power

With more pulses the attacker has more chances to ***guess and correct*** *=> autocorrelation is not secure*

ETH zürich

17

IEEE 802.15.4z



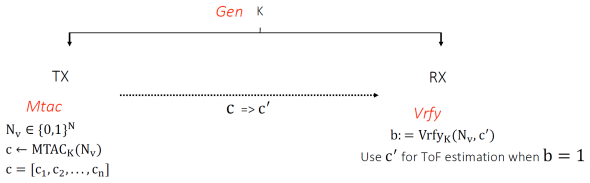
Low Rate Pulse (LRP)
- Single ranging requires few (e.g. 100) pulses
- Can use single pulse mode
- Efficient multi-pulse mode with UWB-PR
- Open security specification
- Low-cost and low-energy

High Rate Pulse (HRP)
- Single ranging requires 1000s to 10000s pulses
- Cannot use single pulse mode (energy too low)
- UWB-PR and variance seem inefficient in HRP
- Some HRP implementations use STS with autocorrelation over a limited time range (not secure).
- Still no open security specification (proprietary)

https://www.3db-access.com/article/17

Message Time of Arrival Codes (MTACs)

- A new class of cryptographic primitives that verify integrity of message arrival time
- Single-pulse/bit, UWB-PR and Variance Based Detection are all different MTACs



ETH zürich

Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Measurement in IEEE Symposium on Security and Privacy (S&P), 2020

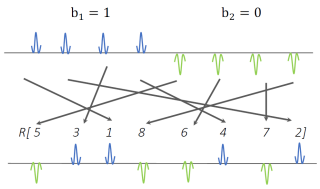
23

Best case for Attacker and worst case for Users:

- Victims: Have to assume bad channel, noise, ...low SNR –> have to tolerat errors.
- Attacker: has perfect channel to the victim and no noise –> can guess and compensate (guesses will seem like noise and mpath)

5.1 UWB Solutions

Solution 1: UWB with Pulse Reordering (UWB-PR)



Cryptographic operations on pulses
- Symbol interleaving through pulse reordering

Verification: Aggregate the energy

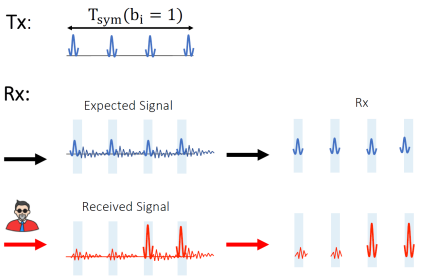
Information needed for the ED/LC attack is lost
- Shape of the symbols is hidden
- Start and end time of symbols is unpredictable

Attacker can only guess!

- Probability of attack reduces with the number of interleaved bits
- Probability of attack increases with the number of pulses per bit

ETH zürich

Solution 2: Variance Based Detection



Attackers goals:

1. Create the correct bits (i.e., increase the mean)

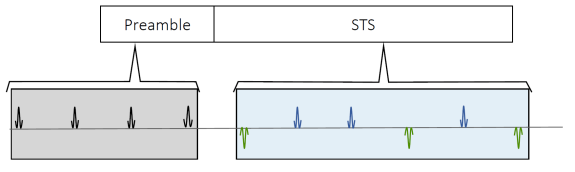
2) Minimize the error energy (i.e., reduce the variance)

3) Make the error indistinguishable from noise

ETH zürich

- Perform statistical analysis (eg., Variance of the expected and received signal)

Solution 3: Scrambled Timestamp Sequence



- Can be public and have good correlation properties
- Generated Cryptographically (not good correlation properties)
- Time-of-flight estimation (autocorrelation)
- Time-of-flight verification (autocorrelation)

Secure? Two autocorrelations need to match ...

ETH zürich

21

UWB Summary:
- UWB can be used to provide precise, performant, and secure ranging
  - Can use challenge-response protocol at logical layer.
  - Distance commitment at the physical layer
  - Design MTACs (Gen,Mtac,Vrfy) to preserve the integrity of arrival time.
- 80.15.4z:
  - LRP open and secure in both single-pulse/bit and multi-pulse/bit modes
  - HRP security is proprietary and needs further analysis.
  - Attacks exist on different HRP implementations
  - Not clear if we can build a fully secure and efficient HRP based system.

5.2 Secure Ranging in 5G

TODO

6 Wireless Security in Critical Transport Infrastructures

Air Traffic Control:
- Primary Surveillance Radar (PSR): Ground based radar. Measures time difference between the signal transmission and reflection. (independent surveillance)
- Secondary Surveillance Radar (SSR): Inspired by Identify Friend or Foe (IFF) during WWII. Transponder-based interrogation. (Dependent surveillance)

A new Wireless Threat Model:
- Domains moving towards increased use of Digital Communication Networks and Automation
- Widespread availability of cheap COTS software-defined radio technology and Domain knowledge
- Legacy systems, which were practically secure for decades, can now be attacked by (almost) anybody.

6.1 Real-World Privacy Issues in Aviation

- Anybody owning a software-defined radio can eavesdrop on aviation communication.
- ACARS (comm. between planes and ground) uses proprietary crypto
- Location of planes can be triangulated, everyone can track planes in real-time
- Aircraft Identification: ICAO 24-bit address unique for every aircraft transponder. Not trivially and legally changed. Metadata also includes aircraft type and registered operator for most airframes.

Countermeasures:
- Web Tracker Blocking: Request flightradar24 etc. to filter out your plane.
- Obscured Ownership: Many private aircrafts ar not in any database (military) or registered to shell or trus companies.
- Switch off position broadcast

6.2 Active Attacks on Wireless Security

- Jamming Attacks
- Modification Attacks
- Injection Attacks (e.g. Ghost Aircraft Flooding Attack)

6.3 Examining Interactions of Safety and Security

Deaths on planes are increasingly being caused by malicious acts rather than technical failures.

Safety: Dealing with failure
- Experience: Increasing mean time to failure of a system via root cause analysis.
- Redundancy: Decreasing likelihood of failure of system as a whole.

Security is not the same thing as safety!
- Redundancy alone does not protct against determined threat actors, who can circumvent different insecure systems at the same time.
- Breaches will happen in the current environment, recovery is key. Considerations of impact of breach on humans in the loop (pilots, controllers) must be taken.

Lessons learned from study with attacks on important plan controls: Attacks impact safety, in the short and in the longer term. Concrete impact is still complex to predict but we need to look at the system as a whole!

6.4 Agile Security Countermeasures

There is no crypto in ATC communication now and for a long time coming. Instead, we can exploit physical layer data (timing, signal strength, Doppler shift et.) to improve the security of several key functions of ATC communication. It's really hard though not impossible to cheat physics.

Crowdsourcing and Physics may bridge us over until A secure Aviation system can be deployed. We can build transparent detection and mitigation measures that raise the attack difficulty back towards nation state levels until we get built-in security.

6.5 Satellite & Maritime Infrastructure

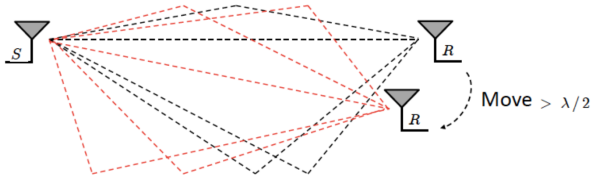
Lessons learned: Its bad wherever you look. Use end-to-end encryption wherever you are. You never know where the next hop actually is

7 Confidentiality and Authentication based on Physical-layer

Can we leverage the physical layer for confidentiality, authentication and access control? In a complex, multipath-rich environment, channels exhibit time-varying, stochastic and reciprocal fading.the attacker does not know and cannot remotely measure multipath fading components

7.1 Channel-based Key Establishment

Wireless Channel



- In a complex, multipath-rich environment, channels exhibit ***time-varying, stochastic and reciprocal*** fading.
- For receivers that are > λ/2 away, channels are not correlated.

=> the channel between S and R will be 'random' and will not be known to the attacker
=> a natural wiretap channel

The attacker does not know and cannot remotely measure multipath fading components, however both communication participants have the same fading. Use this for key agreement protocol. Fading is measured using Channel impulse response (CIR).

1. S sends a well-known signal to R
2. R detects the difference from received signal to expected signal, which correspond to the fading.
3. R sends the same signal to S, and he computes the fading. Now both have a random symmetric random fading component, which they can use to derive a key.

Analysis

- No authentication!
  - Secret key established but with which device?
  - Cannot use channel information to authenticate
- No guarantees on the environment
  - Is the environment multipath-rich?
  - Can attacker pre-measure environment [TmarPhD2012]?
  - Can attacker be verified to be > λ/2 away?
- Questionable benefits over existing PK/SK schemes
  - Information-theoretic guarantees claimed in some papers but unclear how these hold.

- Most schemes consider only passive adversary
- Active attacks
  - Influence and discover the established key. [EberzESORICS12]
  - Abuse the lack of authentication

7.2 Ensuring Secrecy with Multiple Input Multiple Output Antennas (MIMO)

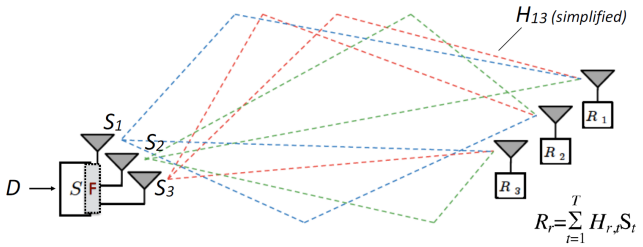
By using multiple antennas the sender can:
- steer the signal towards the receiver and away from the attacker.
- Use jamming to interfere with the attacker, but not with the receiver.

Modeling the Channel

- At the receiver, signal has different phase and amplitude
- Channel is modeled as a single complex number:
  - Captures both change in amplitude (real part) and phase (imaginary part).
  - Represents cumulative effects of all multipath components.

7.2.1 Zero Forcing

Zero Forcing

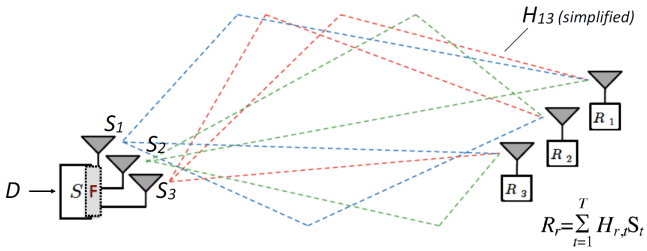


- S knows the channels to R_1 and to attackers R_2,R_3
- *R = H **F** D = H S*
- *H: channel matrix*
  D: data matrix (conf. data)
- ***F*** is a transmission filter, constructed given ***H**, s.t.*:
  - R_1 = confidential data
  - R_2,R_3 = no (useful) data

7.2.2 Orthogonal Blinding

In this scenario the sender knows the channel to the legitimate receiver, but does not know the channels to the attackers around (more realistic scenario). Thus he only knows partial entries of H (H would contain the channels to all possible receivers not only the legitimate one). The sender will randomly generate the missing parts of H in such a way that most surrounding attackers would be jammed and R receives confidential data.

Orthogonal Blinding



- S knows the channels to R_1 ***but not to attackers***
- *R = H **F** D = H S*
- *H: channel matrix (part randomly generated)*
  D: data matrix (conf. data and noise)
- ***F*** is a transmission filter, constructed given ***H**, s.t.*:
  - R_1 = confidential data
  - R_2,R_3 *(attackers)* = ***data + jamming signal (noise)***

Analysis

- Stronger guarantees than SISO schemes:
  - beamforming focuses the energy to the receiver
  - jamming interferes with the attacker

- No authentication!
- No guarantees on the environment
- Questionable benefits over existing PK/SK schemes

- Passive attacks: known plaintext attack **[SchulzNDSS2013]**
  - *Attacker trains a filter until it finds a plaintext and thus discovers the channel between S and R.*
- Active attacks:
  - Abuse the lack of authentication.

SISO = single input single output (single antenna)

7.3 Jamming for Confidentiality

Orthogonal blinding / Zero forcing: Transmit noise into the nullspace of the receiver's channel.
- no pre-established secrets
- used for key establishment

Friendly Jamming: Transmit noise which the receiver subtracts
- Receiver know the seed used tog enerate the noise.
- Eavesdropper cannot seperate signal and noise.
- Jamming signal is much stronger and covers the spectrum of the data signal.
- If distance between jamming antenna and signal antenna (both at sender) > $\lambda/2$, attacker equipped with two antennas can seperate signals from J and D (different channels)
- I distance beween tscheggi nöd sl. 18

Example IMD Shield IMD shield jams the eavesdropper, but also legitimate readers, however shield can be removed.

Friendly Jamming Security Arguments: Security properties in the friendly jamming scenario.

Friendly Jamming Security Arguments

- One of the main security assumptions:
  - If DJ < λ/2, *the attacker cannot separate signals from J and D irrespective of the number of antennas or their directionality.*

- However,
  - Confidentiality holds only for a single-antenna attacker.
  - *A MIMO-like attacker CAN separate the signals and recover the confidential message, from a number of locations.*

Note: A MIMO-like attacker can seperate the jamming and data signal as long as they do not stem from the same antenna, as is the case in the IMD Shield. This is the case because the two signals J and D have different arrival times at the two antennas of the attacker, which makes them distinguishable at ideal attacker placements.

Multipath: So far, we looked at line of sight (LOS) channels, no reflections (at least for friendly jamming)

- Multipath will introduce more variation of amplitudes of components.
- Change the phase offsets of the signals.
- Potentially prevent us from cancelling the jamming signals, so we have stronger guarantees.

Lessons Learned Using Jamming for confidentiality is not without risk.

- MIMO-like attacker can retrieve data despite DJ < $\lambda/2$
- The attack work from many locations (with some post-processing)
- The attack can be effective even when jammer and source are mobile.
- Note: Friendly jamming works well for access control in the sense that it is very hard for the attacker to make its signal receive the device under consideration.

Signal Manipulation Simple setup with two directional antennas, one directed to the sender and one to the receiver, creates artificial multi path that suppresses the transmitted signal at the receiver. The receiver does not know that any message was even sent by the transmitter.

7.4 Broadcast Authentication

Integrity Codes: Broadcast Authentication base on Presence Awareness.

Setup: Broadcaster (known to be present and sending at known channel frequency) and listeners that do not have pre-shared keys or distributed credentials (e.g. certificates/ public keys). Example would be an AP in the airport broadcasting its public key in presence of a potential rogue AP, that tries to send rogue public keys.

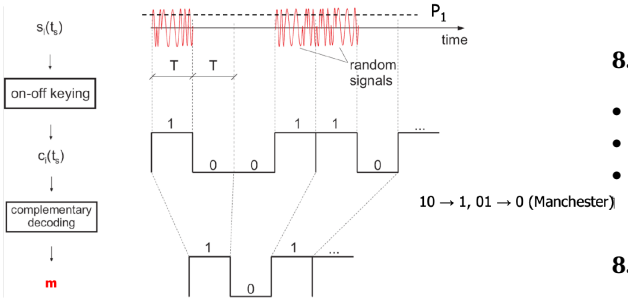
Integrity Codes: *Protocol*

*Reception (**R**eceiver):*

- Presence of *any signal* (>P1) during T interpreted as "1"
  Absence of signal (<P0) during T interpreted as "0"

Integrity Verification

- IF H(m)=|m|/2 THEN "m" was not modified in transmission



Now attacker can only inject 1, assuming he cannot cancel out the amplitude of existing 1s. However injected 1s result in non equal numbers of 1s and 0s, so it can be detected.

8 Broadcast Authentication Device Pairing

8.1 Broadcast Authentication (Tesla)

Broadcast Authentication:

- One sender, a nr. of receivers (possibly malicious and unknown to the sender)
- All receivers need to verify the authenticity of the sender's messages
- We could do this with public-key crypto, but this is too expensive for some low power devices.

Broadcast Authentication without PK Crypto: Two approaches:

- Delayed Key Disclosure (Cheung, Tesla)
- Presence Awareness

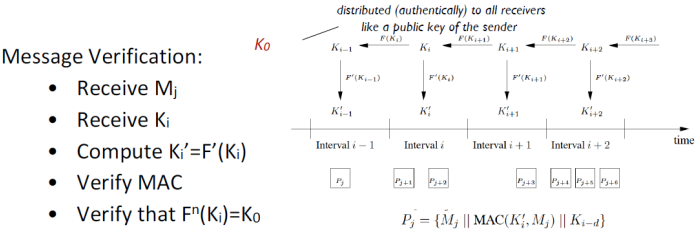
8.1.1 Delayed Key Disclosure

- Uses purely symmetric primitives (MACs)
- Asymmetry from delayed key disclosure
- Self-authenticating keys (one-way hash chains)
- Requires loose time synchronization

Broadcast Authentication based on Delayed Key Disclosure (TESLA)

Message Verification:

- Receive M_j
- Receive K_i
- Compute $K_i' = F'(K_i)$
- Verify MAC
- Verify that $F^n(K_i) = K_0$
- *Verify that the message was received within the key validity interval (before the key was disclosed)*



$P_j = \{\tilde{M}_j \,||\, \mathrm{MAC}(K_i', M_j) \,||\, K_{i-d}\}$

- The keys are authenticated using one-way hash chains
- The messages are authenticated using the keys
- If the key is used after the interval, the message is ignored

8.2 Wireless Device Pairing

Problem: Given a pair of wireless devices without preloaded keys/credentials (mobile phones, printers), how do they establish a secret key in the presence of an adversary (passive or active (MITM attack))?

8.2.1 Diffie-Hellman Protocol

DH protocol enables secret key establishement by public communication. But DH is not secure against active attackers (MITM attaks). Therefore DH messages need to be authenticated, need PK crypto.

8.2.2 Short String Comparison

- Establish key k using DH
- Hash the key h(k) and display on both devices
- Compare the displayed values (160 bits = 20 characters)

8.2.3 Seeing is Believing

Send the public key over an authentic channel (visual barcode / scanner)

8.2.4 Loud and Clear

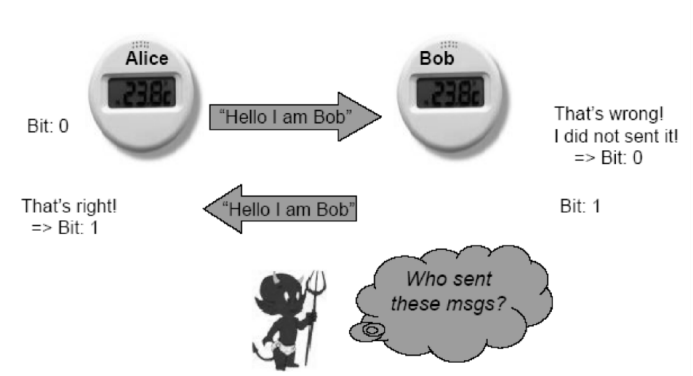
Human-assisted string comparison using voice communication. A's PK transmitted over the wireless channel and h(pk) mapped to a reconizable sentence which i transmitted over wireless channel. B compares the the sentence to the hash of PK.

8.2.5 Integrity Regions

- Establish key k using DH
- Authenticate DH keys by Physical proximity
- if the DH key comes from a close proximity it comes from a friend

8.2.6 Shake Them Up

- Rely on the fact that the attacker does not know which device transmits at which time.
- Assume that A and B communicate over a wireless anonymous broadcast channel
- Eve can read the exchanged packets but cannot identify the src of the packets.
- Problems: Need synchronization (done through shaking), Signal fingerprinting (power, frequency,...)



9 Wifi Security

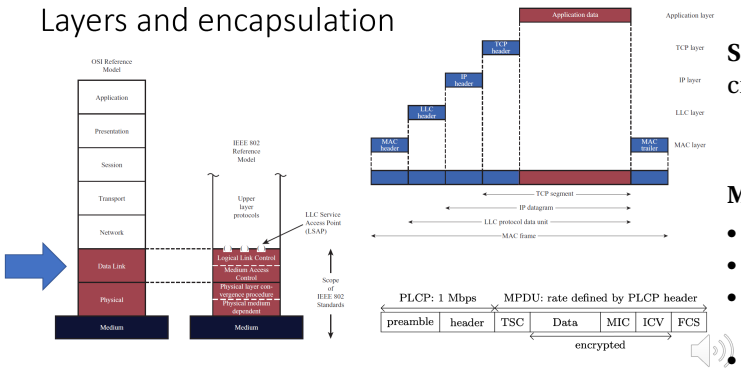
9.1 Basic concepts of WiFi

Terminology

- Station (STA) or client: terminal with access to wireless media.
- Access Point (AP): Station integrated to wireless media and distribution system.
- Basics service set (BSS): Group of stations using same radio frequency.

Channels:

- WiFi standards provide radio frequency ranges, typically 2.4 or 5 GHz
- Each range is divided into several channels with 5MHz spacing



Medium Access Control

- Multiple devices share the same communication medium.
- Goals: Reliable data delivery, Security
- Why handle these services at MAC layer? Can be more efficient than higher layer (e.g. tcp), can be safer than rely on applications or higher layer protocols.

CSMA/CA: Carrier-Sense Multiple Access with collisiona avoidance, this entire mechanism is the Distributed Coordination Function (DCF)

1. Carrier sense: prior to sending, check if medium is idle.
2. Collision avoidance: If another node detected, wait for randomized "backoff period".
3. Transmit entire frame, wait for ACK, if no ACK, wait for backoff period.

Hidden node problem: E.g. B can communicate with A and C and A cannot communicate with C. Potential solution: After backoff transmit Request to send (RTS) to AP, wait for Clear to send (CTS) from AP

Frames: allow 3-4 addresses (usually: sender, AP, destination). Frame types are Data, Control, Management (e.g. power)

Basic security goals:

- Communication security (confidentiality, integrity)
- Access contol (authentication)
- Communication fairness (equal throughput)

9.2 Basic Manipulations

Communication Fairness:

- Previously mentioned DCF is proven to be fair, assuming all stations follow the rules.
- Unfair channel usage: Modify the driver to not backoff.
- if all stations use selfish backoff, then throughput will vary because of collisions, but only station with the strongest signal will be able to send

Simple Jamming: How to turn your WiFi device into continuous jammer?

1. Disable carrier sense
2. Reset interframe space and disable backoff
3. Don't wat for ACK
4. Queue large number of frames for transmission

Different ways to block WiFi frames: Trigger carrier sens of transmitter, or Mangle the frame at receiver (prevent receiving, need more power)

Selective Jamming: Listen, Decode prefix of incoming frame, decide whether to jam. But one needs to be fast!

Man-in-the-middle position:

- Useful building block for many attacks
- Why not selective jamming? Success rate not 100%
- Main idea: Clone AP on a different channel, forward frames from fake AP to real AP.
- How to make victims connect to fake AP?
  - Selectively jam beacons/probes (may not work)
  - Continuously jam real AP -> clients switch (probably works)

9.3 WiFi Security Standards

9.3.1 WEP

- first WiFi security standard (1997)
- Goal: provide some level of communication protection (Confidentiality, Integrity, Access control)
- few years later WEP fully broken
- Checksum: Compute plaintext P = (M, c(M)), used for integrity protection (not a good idea!)
- Encryption: Encrypt using RC4 stream cipher, C = P xor RC4(IV, k)
- Send (IV, C)

Problem 1: Confidentiality

- Keystream reuse problem
  - If $C_1 = P_1 \oplus RC4(IV, k)$ and $C_2 = P_2 \oplus RC4(IV, k)$
  - Then $C_1 \oplus C_2 = P_1 \oplus P_2$
- Keystream reuse implications
  - **One known plaintext** reveals another
  - **No know plaintext:** often redundancy to recover both from $P_1 \oplus P_2$
- Keystream reuse in WEP
  - IV space is 24 bits → repeats after half a day (5 Mbps)
  - Standard does not mandate IV change
  - Some device set $IV = 0$ on reboot

Ways to predict plaintext
- Known structure like IP headers
- Packet injection from Internet

Borisov et al. "Intercepting Mobile Communications: The Insecurity of 802.11." MobiCom'01

Problem 2: Integrity The checksum used (CRC-32) is not a cryptographic MAC. Controlled message modifications are possible.

Problem 3: Access Control

1. AP sends challenge in plaintext
2. Station replies with WEP encryption of challenge (proof of key posession)
3. AP completes network association

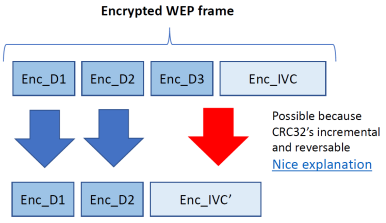
- Simple attack: Monitor legitimate authetication -> learn plaintext/ciphertext pair. Derive Keystream (xor), compute valid response for new challenge.

9.3.2 WPA / TKIP

- The second WiFi security standard (2003) Wifi Protected Access (WPA)
- Main challenge: Design that works with legacy (WEP) devices, Firmware or driver update
- Goals: No keystream reuse, cryptographic MAC
- Constraints: Compatible with RC4/WEP hardware
- Enhancements: Augment encryption with per-packet key mixing. RC4 keystream filtering. New integrity protection mechanism (MICHAEL). Replay protection using counters (TSC)

ChopChop technique

- **Starting point**
  - Unknown key
  - Unknown plaintext
- **Steps**
  1. Record encrypted frame
  2. Remove last data byte
  3. **Guess** chopped **plaintext byte**
  4. Contruct encrypted checksum
  5. Check correctness using **AP as oracle**
  6. Correct guess → learn plaintext byte
  7. **Repeat/chop** next byte



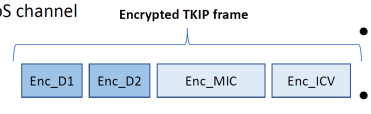
Possible because CRC32's incremental and reversable
Nice explanation

End result:
- Known plaintext packet →
- Known keystream for one packe

WPA/TKIP attack

- **Observations**
  - TKIP frame has MIC (MICHAEL) and ICV (CRC)
  - False MIC → failure report (**oracle!**)
  - MIC algoritm is reversable
  - Counter (STC) is separate for each QoS channel
- **Attack**
  1. ChopChop approach (+ waiting)
  2. Learn plaintext MIC value
  3. Rerverse to learn MIC key

End result:
- Decrypt **one packet** (AP → station)
- Ability to inject 7 packets (per QoS)



Beck and Tews. "Practical attacks against WEP and WPA." WiSec'09

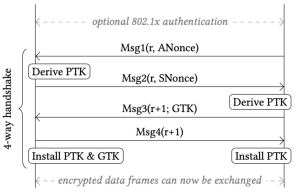
Another Attack: Statistical tests reveal biases in WPA/TKIP key stream.

9.4 WPA2

- Introduced in 2004
- Better communication protection. Confidentiality using AES-128 in counter mode, Integrity usin CBC-MAC, Authenticate then encrypt
- WPA2 Handshake supports mutual authentication, session key agreement (PTK)
- Protocol proven secure in 2005
- Vulnerable to dictionary attacks: The handshake contains a MIC (Message Integrity Code) which makes it vulnerable to dictionary attack. Once the adversary has the MIC, he can try to compute it himself with guessed passwords and compare it with the captured MIC. That way, the adversary can bruteforce all possible passwords from a dictionary offline without having to interact with the AP.

Key Reinstallation Attack (KRACK) – 2017

- **Goal:** keystream reuse
- **Observations**
  - AP retransmits Msg3 if no response
  - Each time client **reinstalls** same PTK
  - Reset counter for CCMP protocol
- **Approach:** replay Msg3
- Interesting point
  - Proven properties still hold
  - Models do not capture **when** key installed



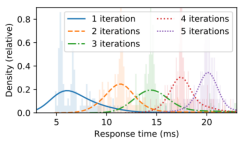
Vanhoef and Piessens. "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 ." In CCS 2017.

9.4.1 WPA3

- The latest WiFi security standard
- Updated crypto: confidentiality using AES-128, Integrity using SHA-384 HMAC
- New Handshake: Password-based authentication and key agreement

WPA3 handshake analysis (2020)

- Downgrade attacks
  - Transition mode: WPA3 and WPA2 handshake
  - Downgrade to WPA2 → detected → record handshake → dictionary attack
- Timing attacks
  - Recall: pwd is converted to group element
  - Execution time (iterations) may depends on pwd
- Also cache leakage, brute forcing pwd...



Vanhoef and Ronen. "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd." In S&P 2020.
More info: https://wpa3.mathyvanhoef.com/

10 Cellular Security

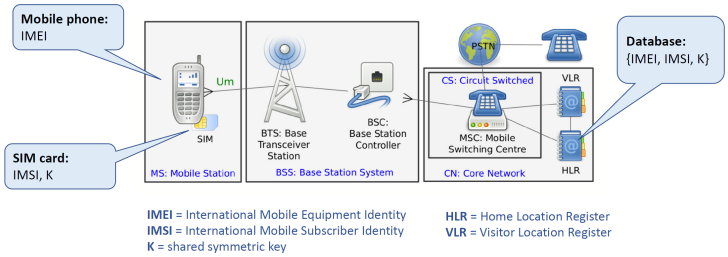
10.1 1G: Analog

- Medium Access Control (MAC): Available bandwidth split using FDMA
- Connects Mobile Stations through Base Stations to the Mobile Telecommunications Switching Office.
- Handover protocol
- Essentially no security.
- Problem: Eavsdropping, Mobile cloning (billing fraud)

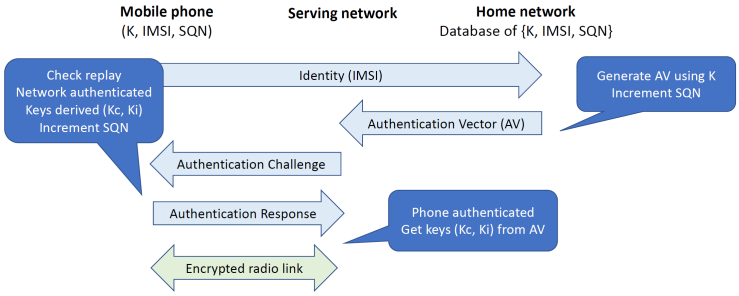
10.2 2G: GSM

- Digital System
- Digital control channels: new features (SMS, Security mechanisms)
- GSM Global System for Mobile Communications

GSM architecture



3G authentication overview



Security model

- All security based on symmetric shared keys
- GSM defines 3 Algorithms: A3 (auth), A8 (key deriv), A5 (encryption)
- Operators can choose A3 and A8 as they are on SIM
- No mutual authentication
- Encryption with fast Linear Shift Feedback Register (LSFR)

Problems

- Nohls attack, attack on A5 encryption with state tables (or rainbow tables): Pre-compute chains, check if key matches. Main enabler of this attack is 64 bit security.
- Attack on A8 (key derivation), recover Ki through side-channels, however operator can replace A8
- No integrity protection: GSM has no integrity protection, probably because of performance reasons. Adding MAC of 64 bits to each frame would lead to an overhead of 56%. And also in voice channel modifications usually are not a problem.
- No mutual authentication: GSM does not authenticate Base station (b.c. Required equipment used to be very expensive for a BS). Calls encrypted limited damage. However, fake BS can identify and track user, and perform man in the middle attacks (we look at this later)

10.3 SS7 Vulnerabilities

SS7: Signalling network 7 used in both GSM and 3G systems.

- Protocol suite used to: route calls, coordinate roaming, deliver SMS
- Original trust model: walled garden, few participating operators and all trust each other, expensive equipment needed.
- GSM grew dramatically and cheap equipment appeared, original trust model no longer valid.

Location tracking:

- Get IMSI and address of current MSC (Mobile Switching Center)
- Request the cell id of the subscriber from the current MSC
- main enabler: Protocol Flaw in the GMLC

Intercepting Calls:

1. Attacker overwrites service control function's address with a fake one
2. Attakcer can then redirect the call to a proxy relay which can then fully record the conversation. Man in the middle.

10.4 3G: UMTS

- UMTS: Universal Mobile Telecommunications System
- W-CDMA wideband code-division multiple access, seperate spreading for each user
- New authentication and key agreement (AKA) protocol, mutual authentication, mutual replay protection.
- Integrity protection and encryption with KASUMI block cipher based on 8 rounds Feistel network, fast on hardware.

Denial of Service attack on 3g: Use a cell phone jammer, cheap but illegal. Also possible DoS attack on paging, as this takes place before authentication

Man in the middle (fake BS):

- 3G authentication (AKA) is mutual
- But we can use simple downgrade attack

Femtocells: Operator provides small BS to customer to improve coverage in places like indoors. Problem is that they are considered trusted but provide much easier physical access for an attacker.

User tracking: In AKA mobile provides its identity (IMSI) before authentication, Operator assigns temporary identity (TMSI), user tracking possible to some extent. Fixes: dont send IMSI in plaintext or use pseudonyms at beginning of AKA.

10.5 4G: LTE (Long Term Evolution)

Overview:

- Orthogonal frequency division multiplex (OFDM)
- Multiple antenna techniques like MIMO
- Encryption usning AES-CTR, AES-CMAC
- Mutual authentication and SQN for replay detection
- The service area of operator divided into Tracking Areas (TAs)
- no integrity protection on user messages
- no confidentiality of paging
- no confidentiality on lower layers

Location tracking

- Enabler: GUTI reallocation depends on operator, availability was seen more important than privacy in this particular case.
- Setup fake BS
- Learn user presence in Tracking Area (TA)
- Learn precise location (fake BS sends unprotected RRC COnnection Reconfig

Man in the Middle

1. Learn user from encrypted traffic
2. Modify encrypted traffic –> redirection. Deliver to false DNS server.

Modify specific message bits attack:

- observe connection establishments in area
- learn many TMSIs
- page victim, isolate his TMSI
- record packet
- xor with whatever you want
- packet will be accepted because aes ctr does not authenticate

4G: Attack Vectors / Attack Strategies

SigOver

- Overshadow single message or small part of subframe
- Only low power required
- Integrity-protected messages can not be spoofed
- Stealthiness
- Low J/S (averaged over time)

Fake base station

- Masquerading a legitimate base station
- Requires high power for UE to lock on
- Could be detected by UE as no security context can be set up
- High J/S (averaged over time)

Man-in-the-middle

- Fake base station with UE capabilities
- Fake UE impersonates UE and fake eNodeB is used to communicate with victim UE
- Same/similar limitations as fake base station approach

The ultimate attack: Synchronized fake base station?