Security of Wireless Networks

Lecture 4

Jamming and Jamming Resistant Communication

Recommended Readings

- Electronic Warfare 101: David Adamy (Chapters 7 and 9)

Communication Jamming

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

The term has been broadly used in a number of contexts and can also refer to unintentional prevention of communication.

Communication Jamming

Carrier: An RF signal that “carries” information

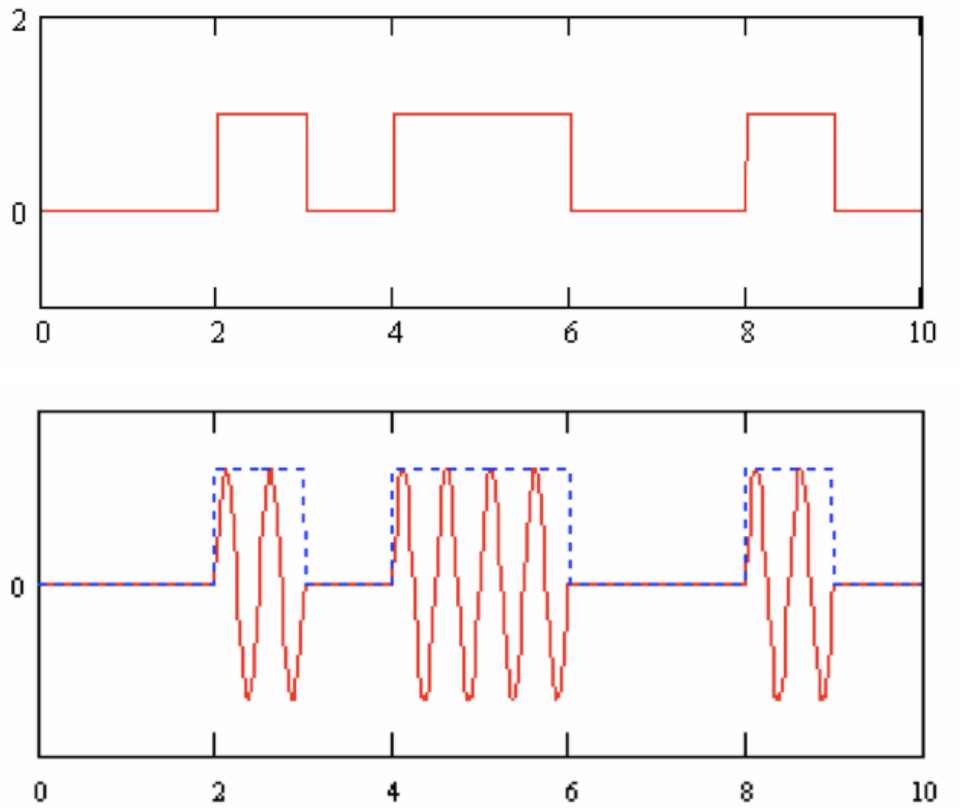
Carrier typically has a much higher frequency than the information (baseband) signal

Also referred to as center frequency

Baseband (information) signal: m(t)

Carrier: sin(2πft) (or cos(2πft))

Modulated signal: ASK(t) = s(t)sin(2πft) Amplitude Shift Keying



Communication Jamming

Carrier: An RF signal that “carries” information

Carrier typically has a much higher frequency than the information (baseband) signal

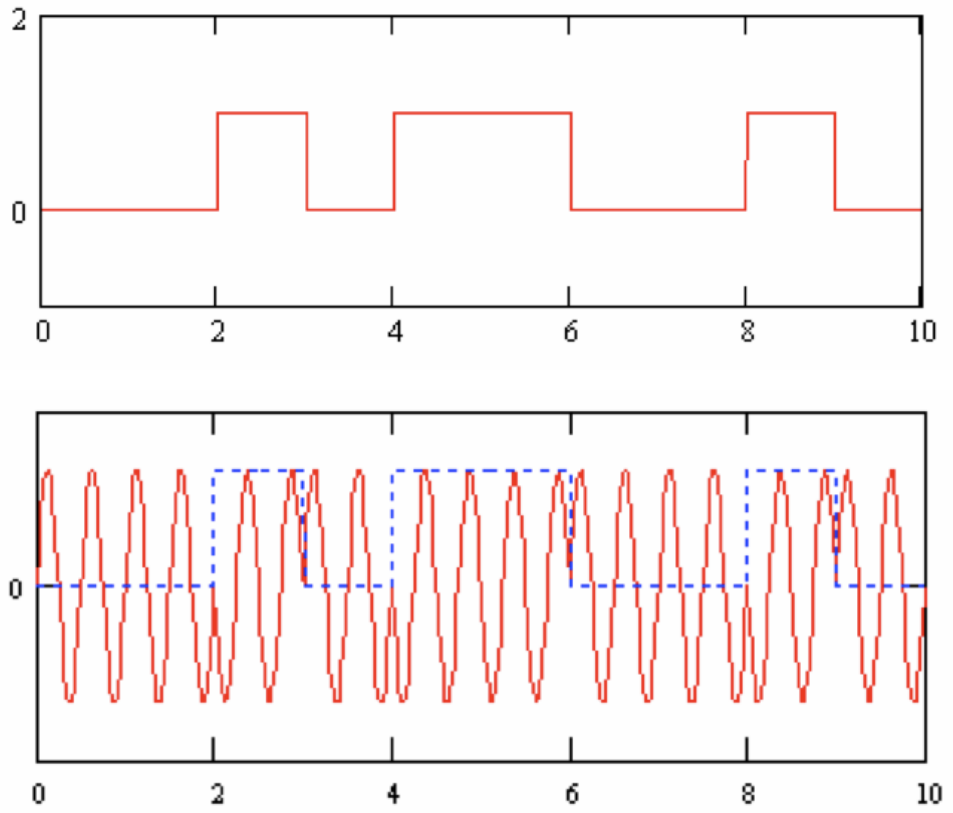
Also referred to as center frequency

Baseband (information) signal: m(t)

Carrier: sin(2πft) (or cos(2πft))

Modulated signal:
BPSK(t) = sin(2πft), b=1
= sin(2πft+π), b=0
Binary Phase Shift Keying (BPSK)

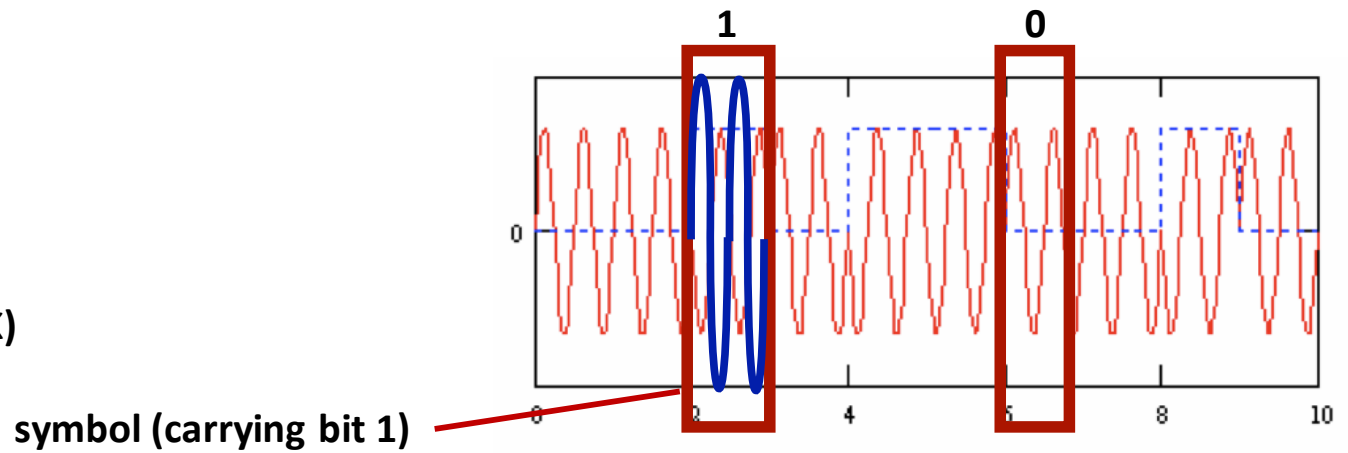
Note: sin(2πft) = cos(2πft+π/2)



Communication Jamming

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

Modulated signal:
BPSK(t) = sin(2πft), b=1
= sin(2πft+π), b=0
Binary Phase Shift Keying (BPSK)



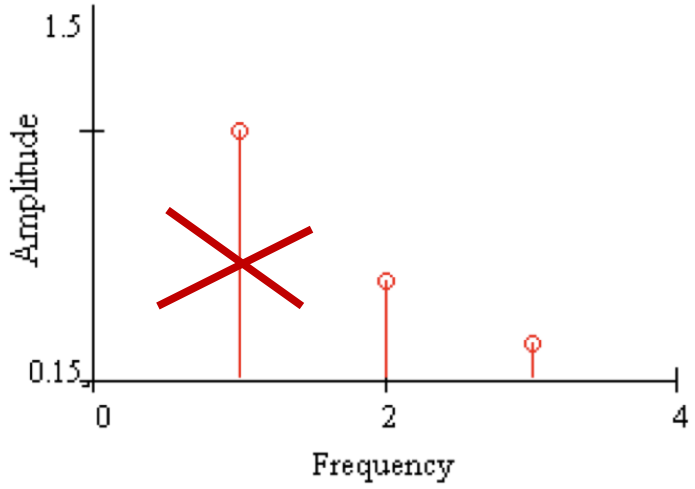
- *Symbol Jamming*: corrupts symbols such that the receiver
  - cannot interpret them or
  - Interprets them incorrectly
- *Communication Jamming*: Corrupt enough bits such that the information cannot be reconstructed (despite Error Correction)

Communication Jamming

- Jamming individual symbols
  - Individual symbols or bits are jammed
  - Most communication systems will do error detection and correction
  - Beyond a certain threshold of corrupted bits (given for each ECC scheme) the message cannot be recovered
  - Targeted low-power jamming of individual bits is not easy and might require synchronization

Communication Jamming

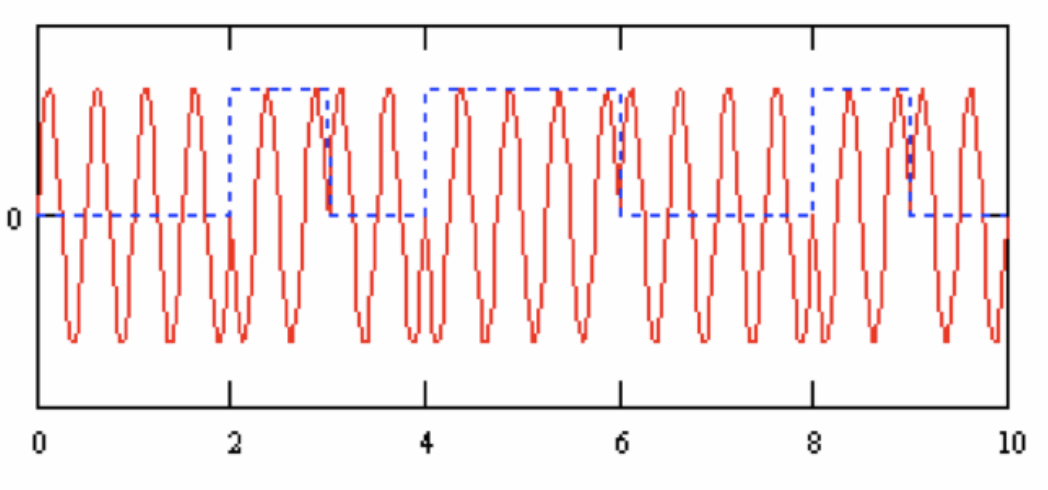
- *Frequency:*
  - To jam, the attacker needs to transmit on the right frequencies during the right time (e.g., all)
  - Partial jamming might not prevent communication (the receiver might still reconstruct the signal)

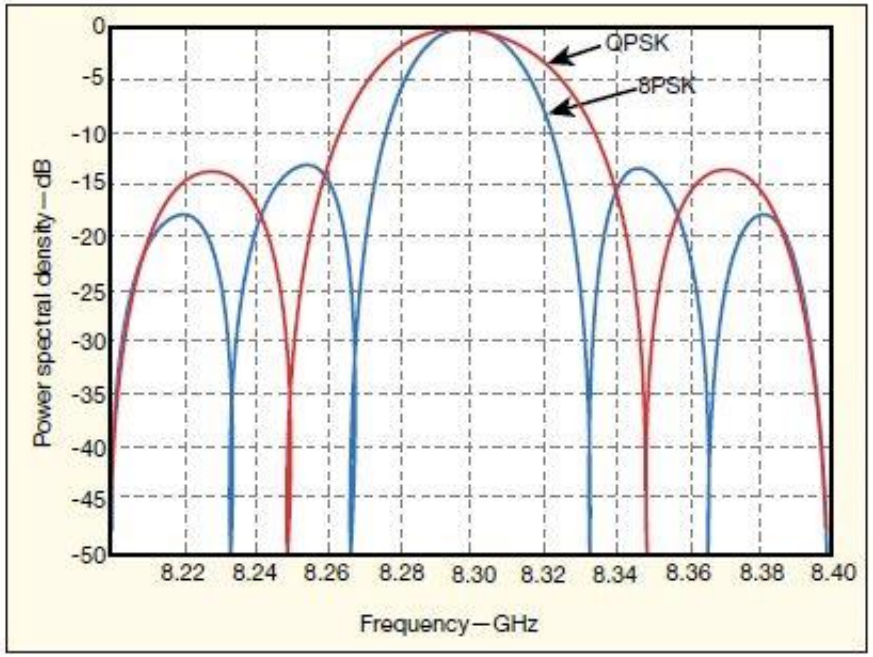


example spectrum

Communication Jamming

- *Example spectrum* (BPSK)





Communication Jamming

- *Assuming the attacker uses the full signal spectrum*
  - It is all about power!

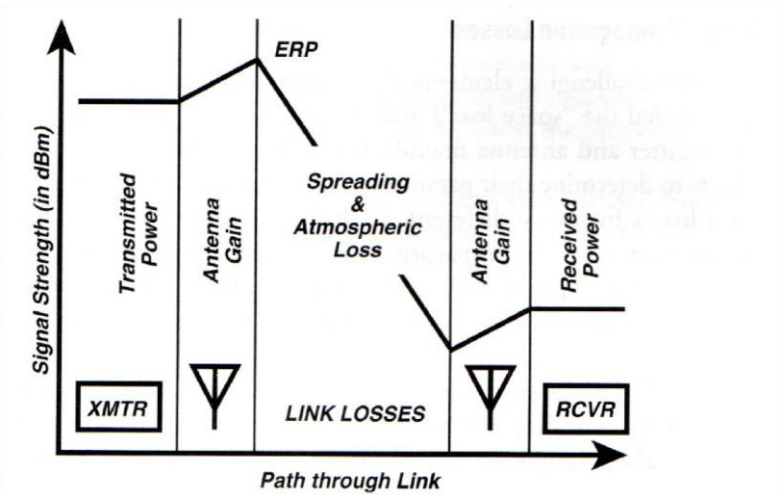
$$S = P_T + G_T - 32 - 20\log(F) - 20\log(D_S) + G_R$$

$$J = P_J + G_J - 32 - 20\log(F) - 20\log(D_J) + G_{RJ}$$

P – transmitted power
G - antenna gain
F – communication frequency
D - distance

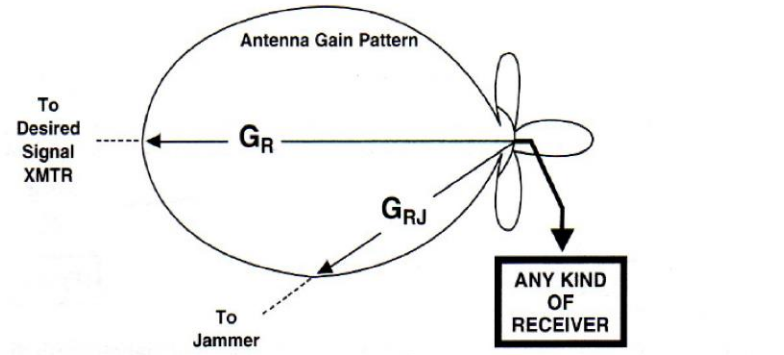
(free space) Path loss directional gain

(Friis transmission equation https://en.wikipedia.org/wiki/Link_budget)



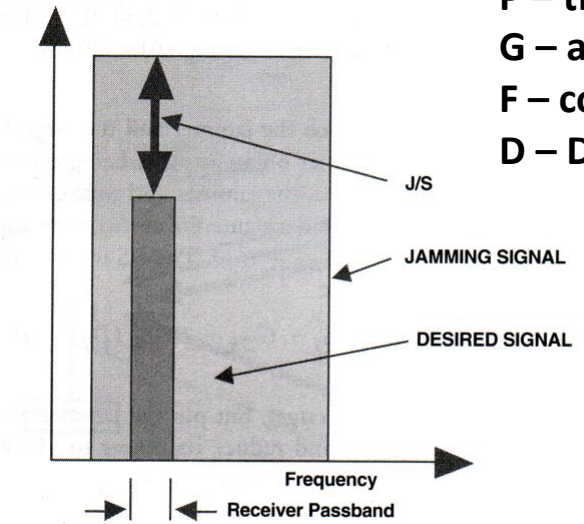
To calculate the received signal level (in dBm), add the transmitting antenna gain (in dB), subtract the link losses (in dB), and add the receiving antenna gain (in dB) to the transmitter power (in dBm).

- *Jamming-to-Signal ratio (J/S):*
  - J/S = J-S (dB)
  - In most communication systems, J/S=0 results in successful jamming



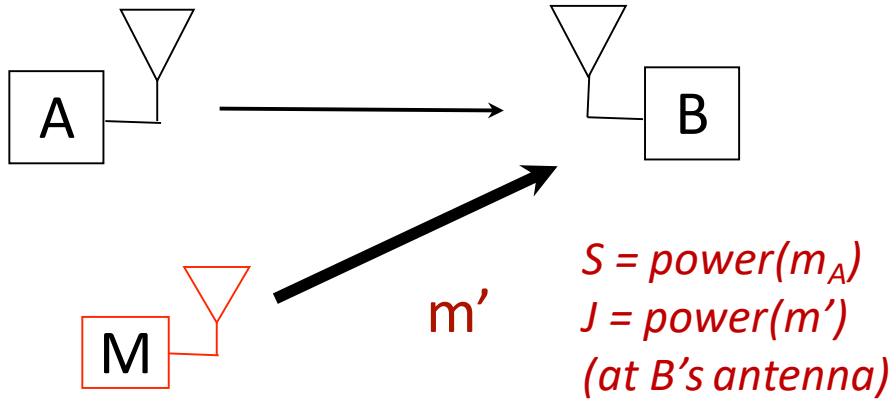
If the receiving antenna is not omnidirectional, its gain to the jamming signal will be different (usually less) than its gain to the desired signal.

Communication Jamming



The jamming-to-signal ratio is simply the ratio of the power of the two received signals within the frequency passband of the receiver.

P – transmitter power
G – antenna gain
F – communication frequency
D – Distance



$$S = P_T + G_T - 32 - 20\log(F) - 20\log(D_S) + G_R$$

$$J = P_J + G_J - 32 - 20\log(F) - 20\log(D_J) + G_{RJ}$$

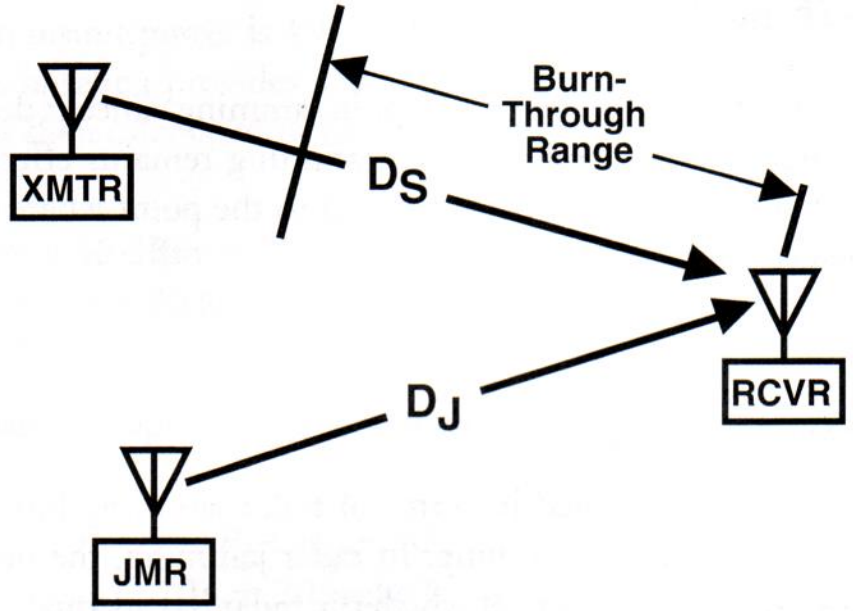
(free space) path losses

directional gain

- Example:
  - Jammer uses 100W (50dBm), antenna gain 10dB, distance 30km
  - Transmiter uses 1W (30dBm), antenna gain 3dB, distance 10km
  - J/S = 17dB => probably successful jamming

Communication Jamming

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



Other Types of Jamming

Types of Jamming

Type of Jamming	Purpose
Communications jamming	Interferes with enemy ability to pass information over a communications link
Radar jamming	Causes radar to fail to acquire target, to stop tracking target, or to output false information
Cover jamming	Reduces the quality of the desired signal so it cannot be properly processed or so that the information it carries cannot be recovered
Deceptive jamming	Causes a radar to improperly process its return signal to indicate an incorrect range or angle to the target
Decoy	Looks more like a target than the target does; causes a guided weapon to attack the decoy rather than its intended target

Communication 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

(Directional)

Communication Jamming - Examples

Transmit power:

Conference-room jammers (Cellular, WiFi)

https://unival-group.com

https://phantom-technologies.com

Up to 8W output power per band

Directionality:

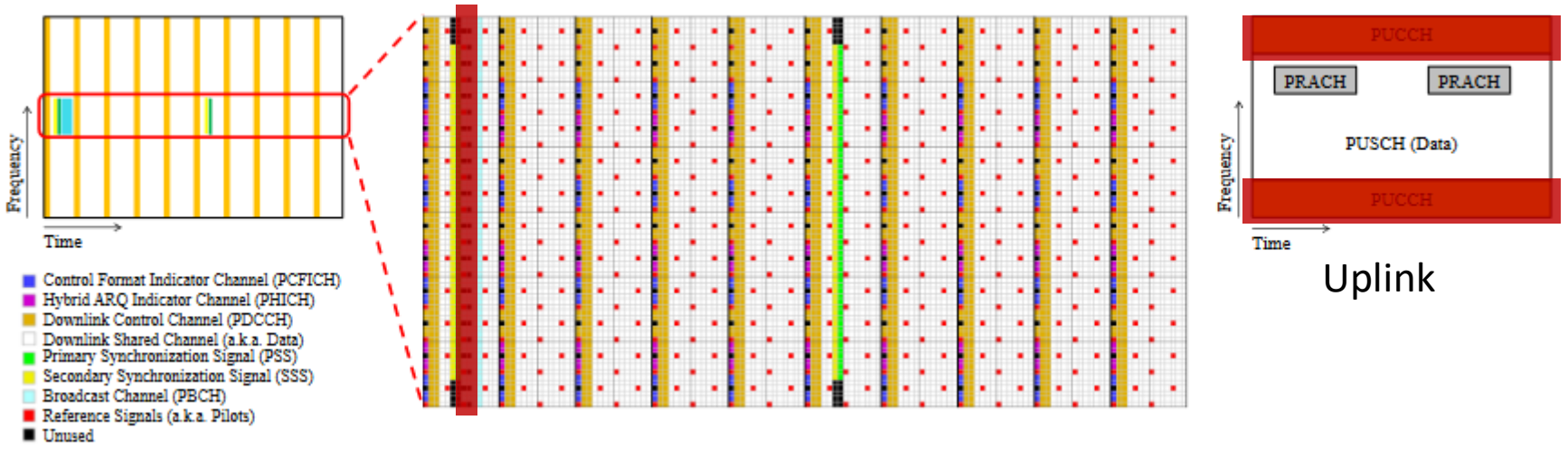
Anti-drone jammer

https://hp-jammer.de/

https://www.technologyreview.com/2017/01/18/154532/in-davos-the-police-will-disarm-your-drone-in-a-heartbeat/

Communication Jamming - LTE

- Knowledge about the protocol can allow for more efficient jamming
- In LTE: Connection establishment relies on information that is transmitted on control channels
  - These control channels can be targeted (might require synchronization)
  - “Protocol-aware” jamming



Downlink

Uplink

Lichtman et al., Vulnerability of LTE to Hostile Interference

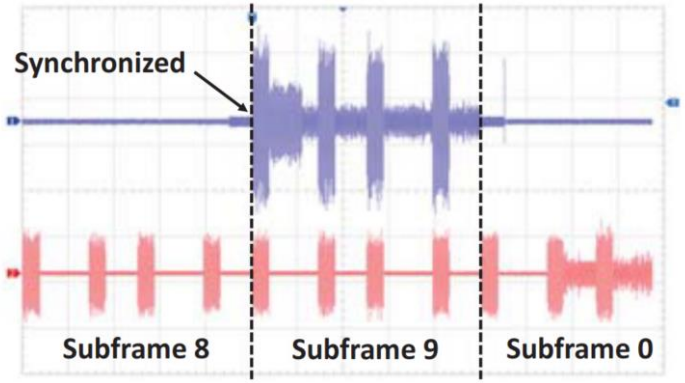
Communication Jamming - LTE

- A synchronized attacker can overshadow broadcast (control) information
  - Can be done with software-defined radios

Can be used for misconfiguration that leads to DoS

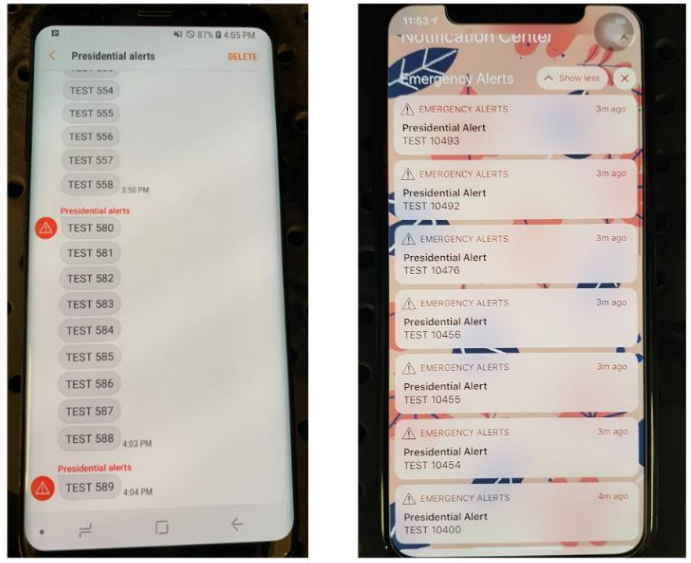
Crafted spoofing signal

Legitimate signal



Yang, Bae, et al. : Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE

Can be used for triggering false “presidential alerts”



Lee, et al: This is Your President Speaking: Spoofing Alerts in 4G LTE Networks MobiSys ’19

Over-the-Air MITM Attacks
on Cellular Network Availability

MITM in Cellular Networks

State-of-the-art attacks rely on fake base stations:

- IMSI catchers
- DoS attacks
- Tracking (Localization)

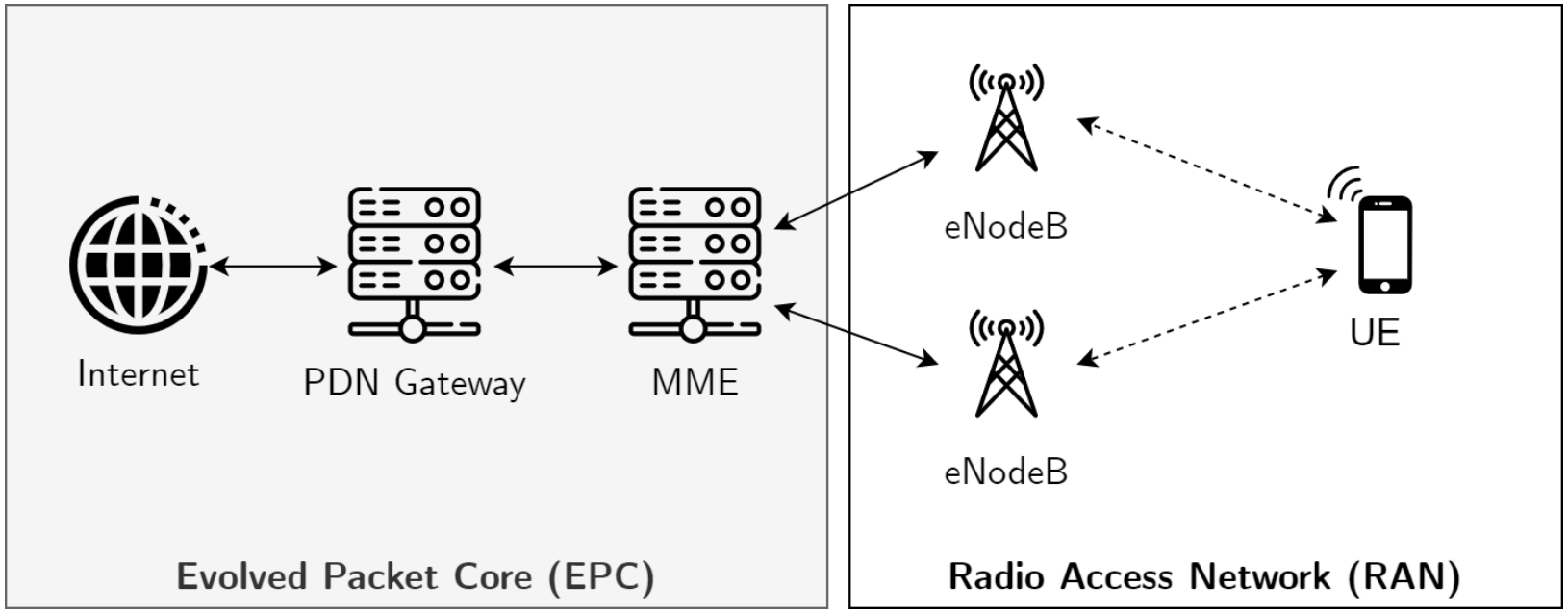
Can we do these attack over-the-air? *(stealthier, …)*

Over-the-Air MITM attacks on Cellular Networks are feasible:

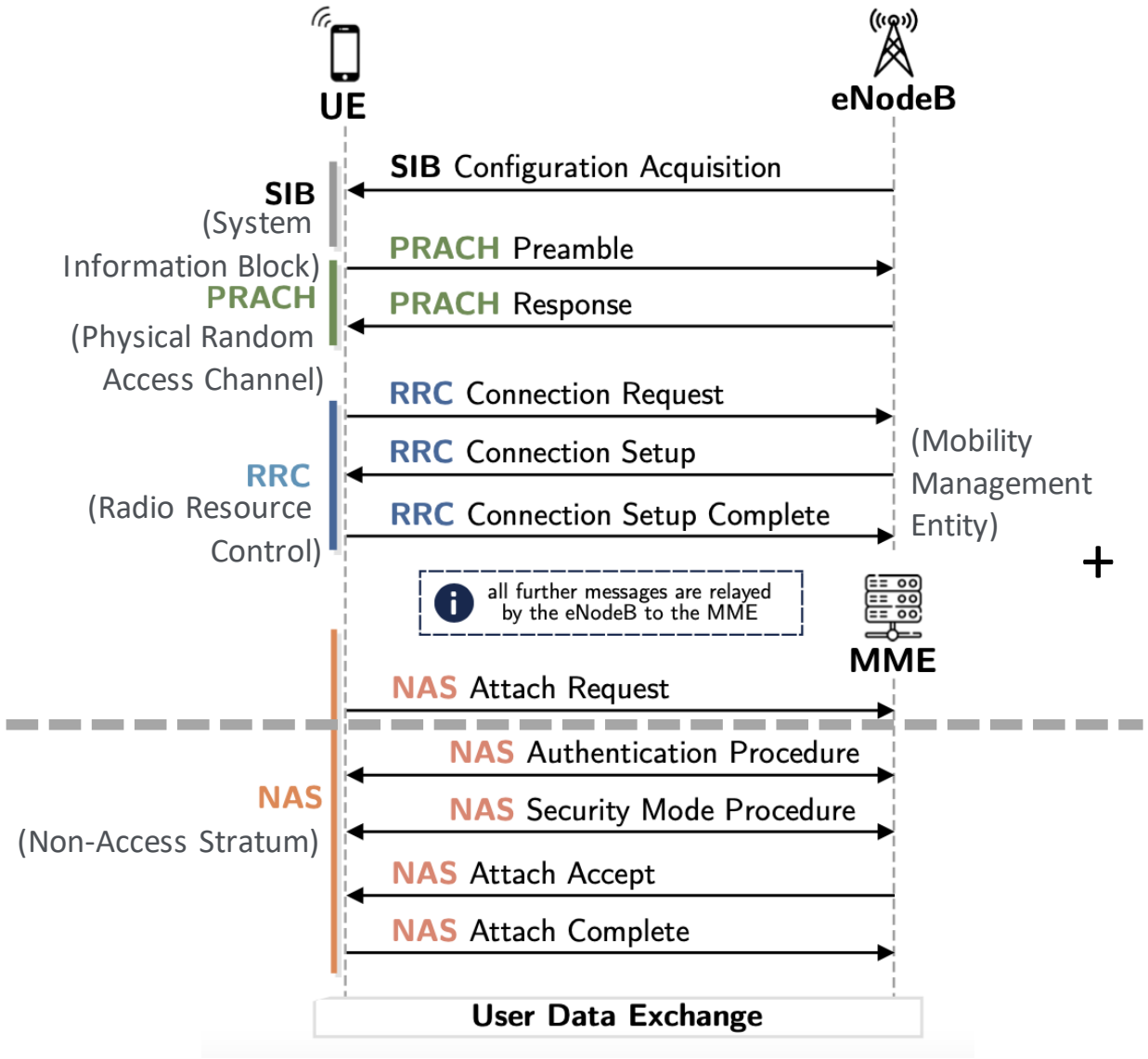
- **Denial-of-Service (DoS) lasting >12h**
- **Tracking:** Localization + Identification

Background: LTE Architecture

1. Core Network (EPC)
2. Radio Access Network (RAN)



Background: UE Attachment / Service Procedure



If the UE is already attached:

UE -> MME: **Service Request**
UE <- MME: **Service Accept**

After the UE is idle (approx. every 6 min of user/phone inactivity), it sends Service Request.

UE <- MME: **Identity Request**
UE -> MME: **Identity Response (IMSI)**

MME can send this request at any time, e.g., as a response to Attach or Service Request. UE will reply.

Message *Overshadowing*

Capture Effect

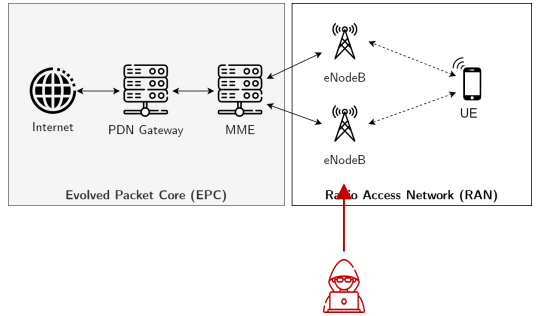
1. Collision of 2 Signals Aligned in Time & Frequency
2. Stronger one will still be decoded by the receiver (UE or eNodeB)

Original Signal
(Data X)

Attacker Signal
(+ 1-3 dB, 1.8dB in our experiments)
(Data Y)

=> the attacker can modify messages UE <-> eNodeB and UE <-> MME.

What can you do with this?
LTE (SigOver) / 5G (SigUnder)



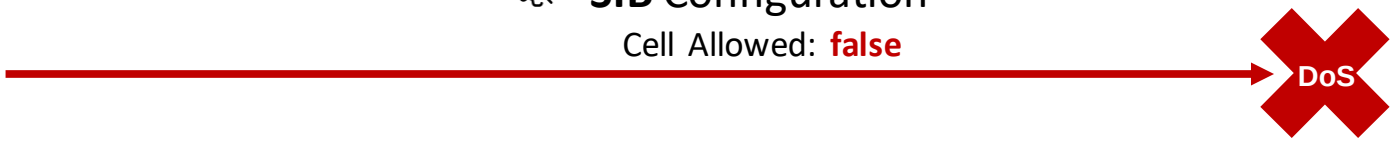
Attacker

eNodeB

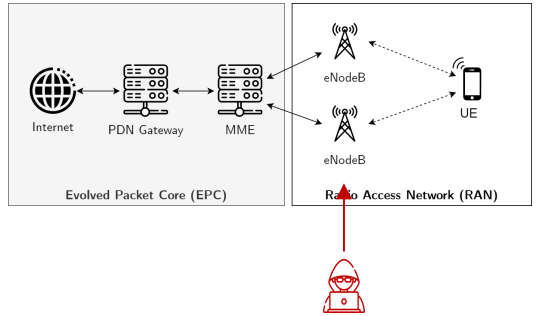
UE

SIB Configuration

Cell Allowed: **false**



What can you do with this?
LTE (SigOver) / 5G (SigUnder)



Attacker

eNodeB

UE

SIB Configuration

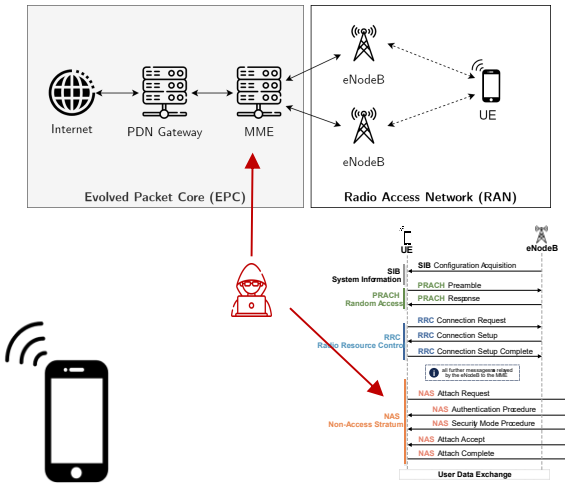
Cell Allowed: **false**

Drawbacks

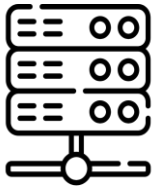
*Low DoS persistence of 10min, **single** cell only*

*Overshadowing of **repeated** messages (every n ms) only*

AdaptOver (2021/22)



Attacker



MME

UE

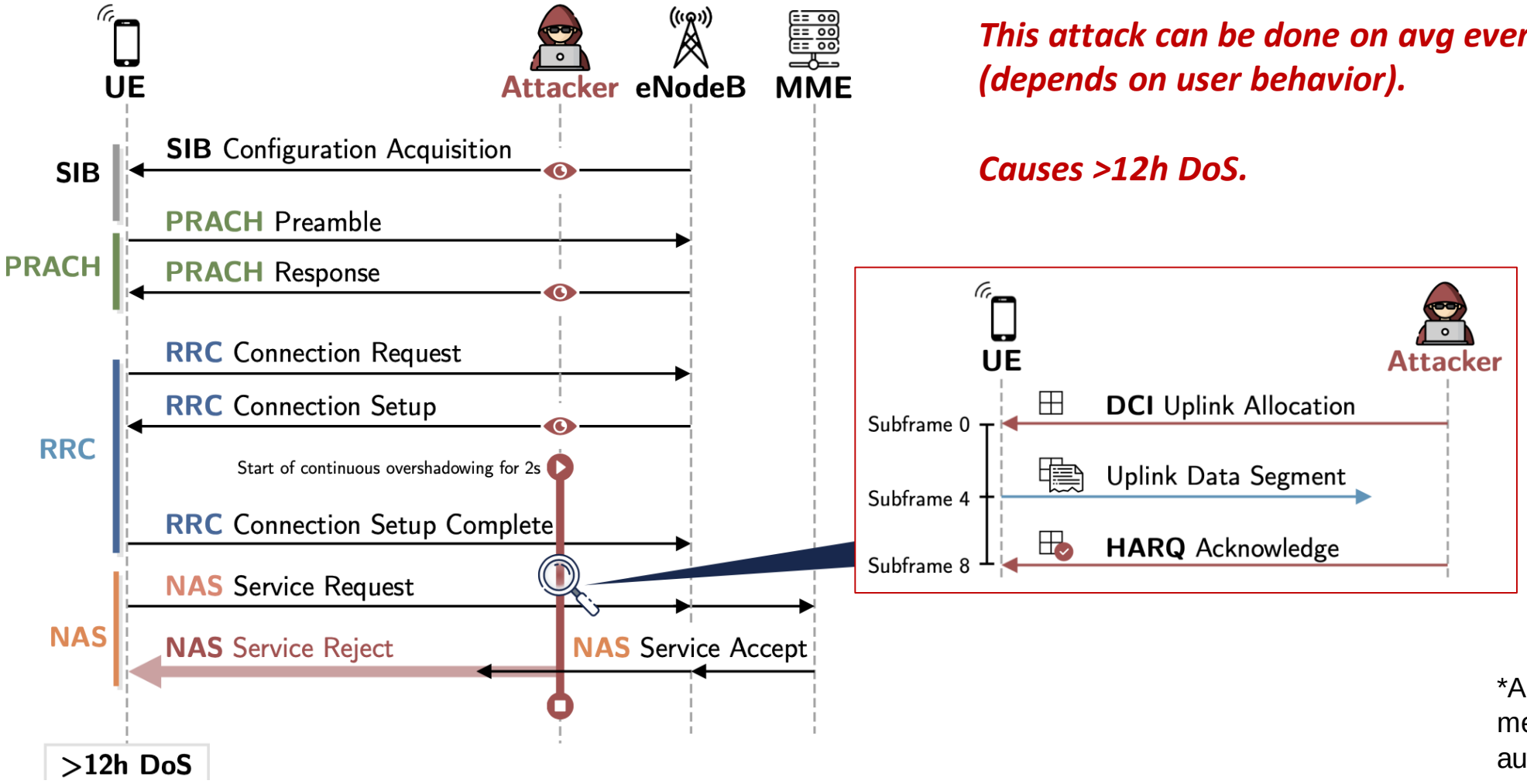
RRC Connection Setup 

NAS Attach Request

NAS Attach Reject

AdaptOver Downlink Sniffer + Downlink Overshadowing

Service Reject Attack

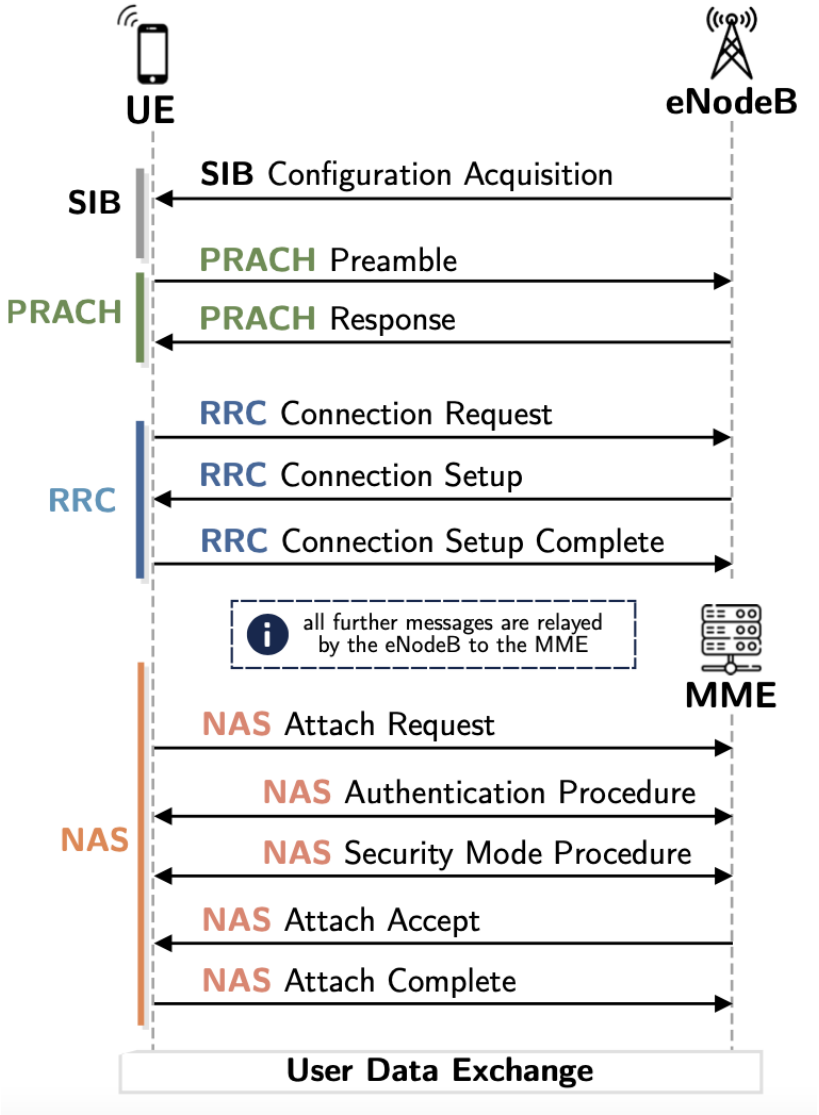


This attack can be done on avg every 6mins (depends on user behavior).

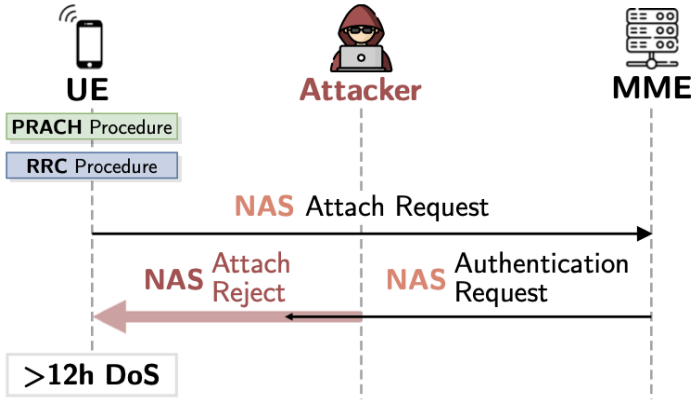
Causes >12h DoS.

*Although service reject messages should be authenticated the attack still works on all tested phones

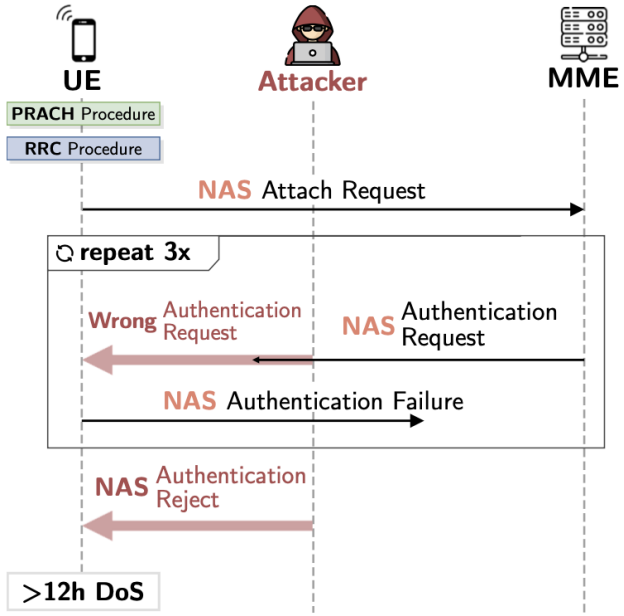
AdaptOver Downlink Sniffer + Downlink Overshadowing



Attach Reject Attack



Authentication Reject Attack

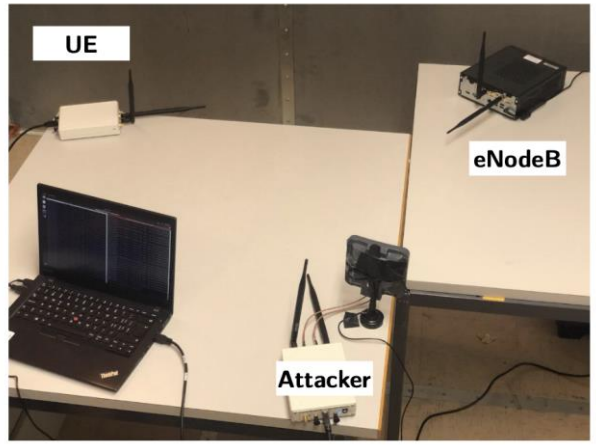


AdaptOver Downlink Sniffer + Downlink Overshadowing: Implementation Results

TABLE I: Attack Results for DoS Attack carried out by AdaptOver

		Service Reject			Attach Reject			Authentication Reject		
Phone	**LTE Modem**	Duration[1]	Action[2]	GUI[3]	Duration[1]	Action[2]	GUI[3]	Duration[1]	Action[2]	GUI[3]
Pixel 2	Qcom. X16 LTE	> 12h	R	☐	> 12h	R	☐	> 12h	R	☐
Pixel 3a	Qcom. X12 LTE	> 12h	T	☐	> 12h	T	☐	> 12h	T	☐
Huawei P20 Pro	Kirin 970	> 12h	T	☐	> 12h	T	☐	> 12h	T	☐
Huawei P30	Kirin 980	> 12h	T	■	> 12h	T	■	>12h	T	■
Huawei P30 Lite	Kirin 710	> 12h	T	☐	> 12h	T	☐	> 12h	T	☐
Samsung Galaxy A8	Exynos 7885	> 12h	T	■	> 12h	T	■	> 12h	T	☐
Samsung Galaxy S10	Exynos 9820	> 12h	T	■	> 12h	T	■	> 12h	T	☐
LG Nexus 5X	Qcom. X10 LTE	> 12h	S	■	> 12h	R	☐	> 12h	R	☐
iPhone 6S	Qcom. Gobi 4G	> 12h	R	■	> 12h	R	■	> 12h	R	■
iPhone 7	Intel XMM 7360	> 12h	T	☐	> 12h	T	☐	> 12h	T	☐
iPhone 8	Intel XMM 7480	> 12h	T	☐	> 12h	T	☐	> 12h	T	☐
iPhone 11	Intel XMM 7660	> 12h	T	☐	> 12h	T	☐	> 12h	T	☐
iPhone 11 Pro	Intel XMM 7660	> 12h	T	☐	> 12h	T	☐	> 12h	T	☐
iPhone X	Intel XMM7480	9.78h	T	☐	> 12h	T	☐	> 12h	T	☐
HTC U12+	Qcom. X20 LTE	> 12h	T	☐	> 12h	T	☐	> 12h	T	☐
OnePlus 7T Pro	Qcom. X24 LTE	> 12h	T	☐	> 12h	T	■	> 12h	T	☐
Xiaomi Mi 9	Qcom. X24 LTE	> 12h	T	☐	> 12h	T	☐	> 12h	T	☐
Xiaomi Mi Mix 3 5G	Qcom. X24 LTE	> 12h	T	☐	> 12h	T	☐	> 12h	T	☐

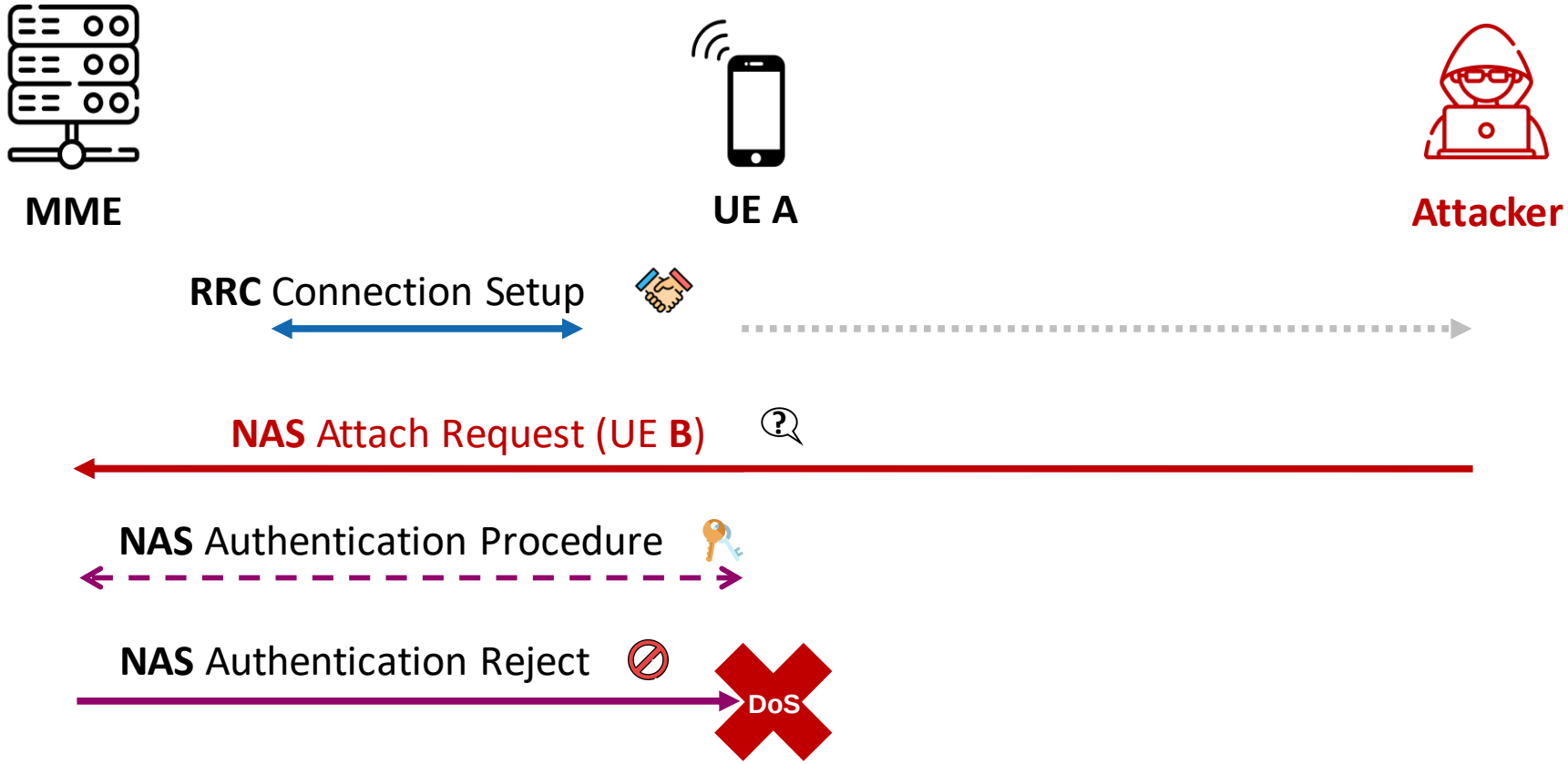
[1] Duration until the UE re-established a connection by itself
[2] Action that will re-connect the phone immediately, **T**: Toggle flight mode, **R**: Restart phone, **S**: Reinsert SIM Card
[3] Whether an indicator on the GUI is present



Network:
Ettus USRP B210 + srsLTE as private LTE eNodeB and core network

Attacker:
Lenovo T490 + Ettus B210

Adaptover (2021/22): NAS Attach Request Forgery – DoS



Physical Layer Security

Jamming resistant communication

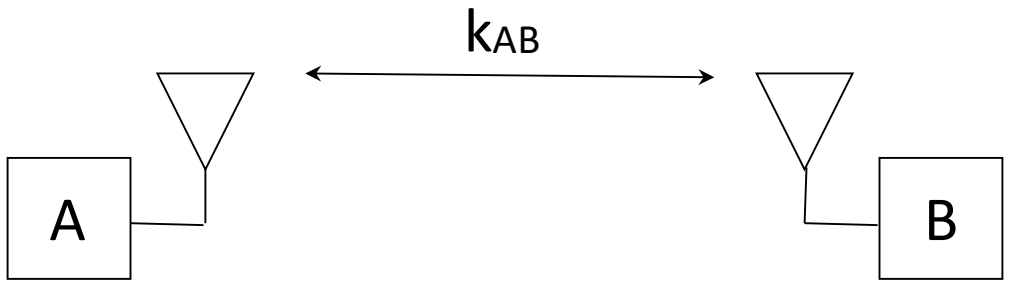
Jamming resistant communication

- Basic principle of jamming resistant communication
  - If you cannot fight, RUN, HIDE, (and WAIT)

- Techniques for Jamming Resistant Communication
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
  - Chirp

Jamming Resistant Communication

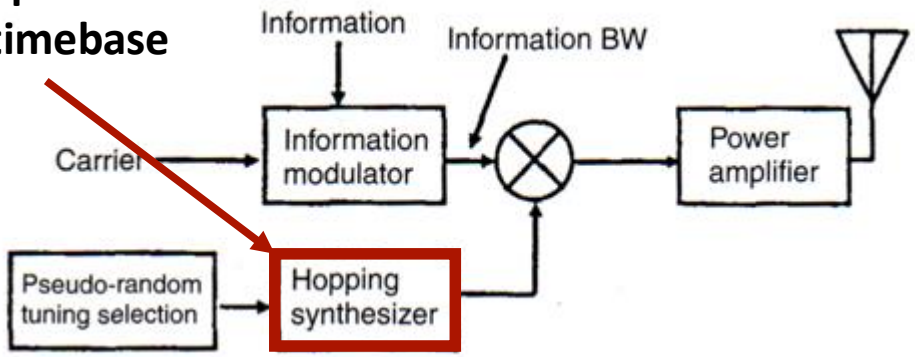
- Basic principle of Jamming Resistant Communication:
  - If you cannot fight, *RUN and WAIT*
  - But we need an advantage over the attacker:
    a shared secret key between the sender and the receiver

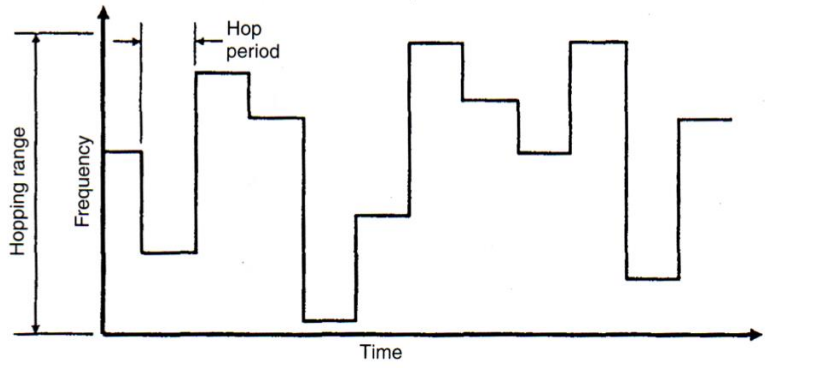


Frequency Hopping Spread Spectrum

- Using a shared key, the sender and the receiver derive a pseudorandom hopping sequence
- Sender and receiver are synchronized
- *The attacker cannot guess the next hop or detect-and-jam*

generates frequencies from a fixed timebase or oscillator



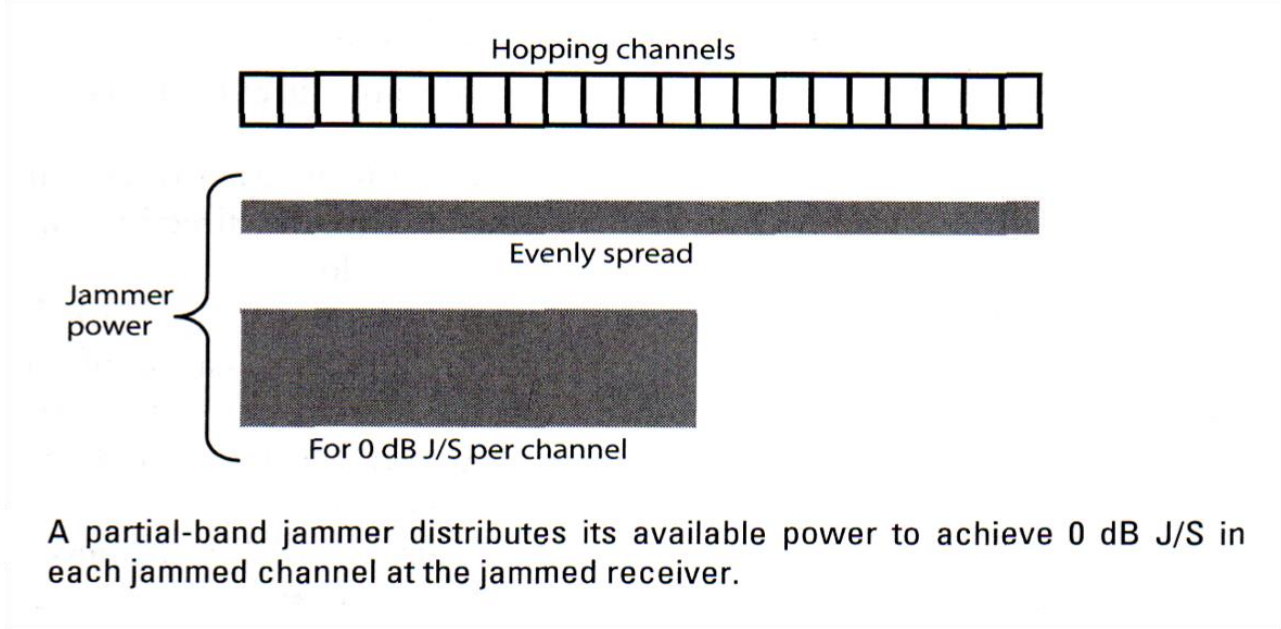


Frequency-hopped signals hop between randomly selected frequencies over a wide frequency range.

First mentioned by Nikola Tesla (1903) in two US patents.
US patent by Hedy Lamarr and George Antheil (1942)

Frequency Hopping Spread Spectrum

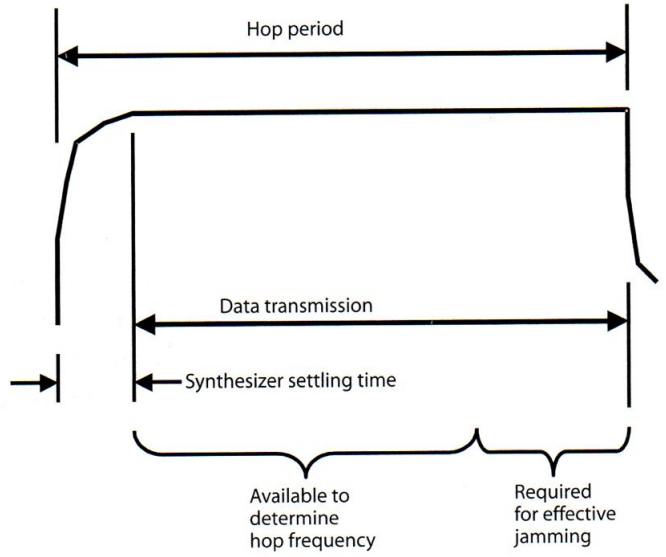
- FHSS Partial Band Jammer
  - Distributes its power such that the jamming power per channel is equal to the received signal strength
  - J/S=0dB provides sufficient Bit Error Rate



A partial-band jammer distributes its available power to achieve 0 dB J/S in each jammed channel at the jammed receiver.

Frequency Hopping Spread Spectrum

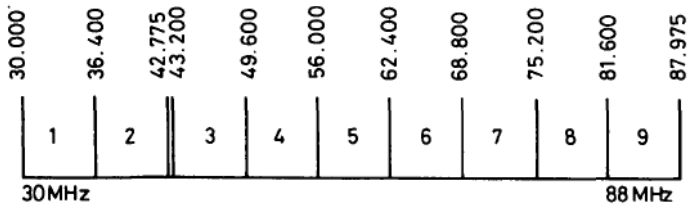
- *FHSS Follower Jammer*
  - First detects on which frequency communication is taking place and then jams.
  - Protection: Message encodings that enable message recovery despite x% of it being corrupted



A follower jammer must determine the frequency of the hop and set its jamming frequency during 67% of the data transmission time.

Bluetooth:
79 channels, 1MHz each
1000 hops/second
Jaguar V system:
50W
2320 channels
50-500 hops/second

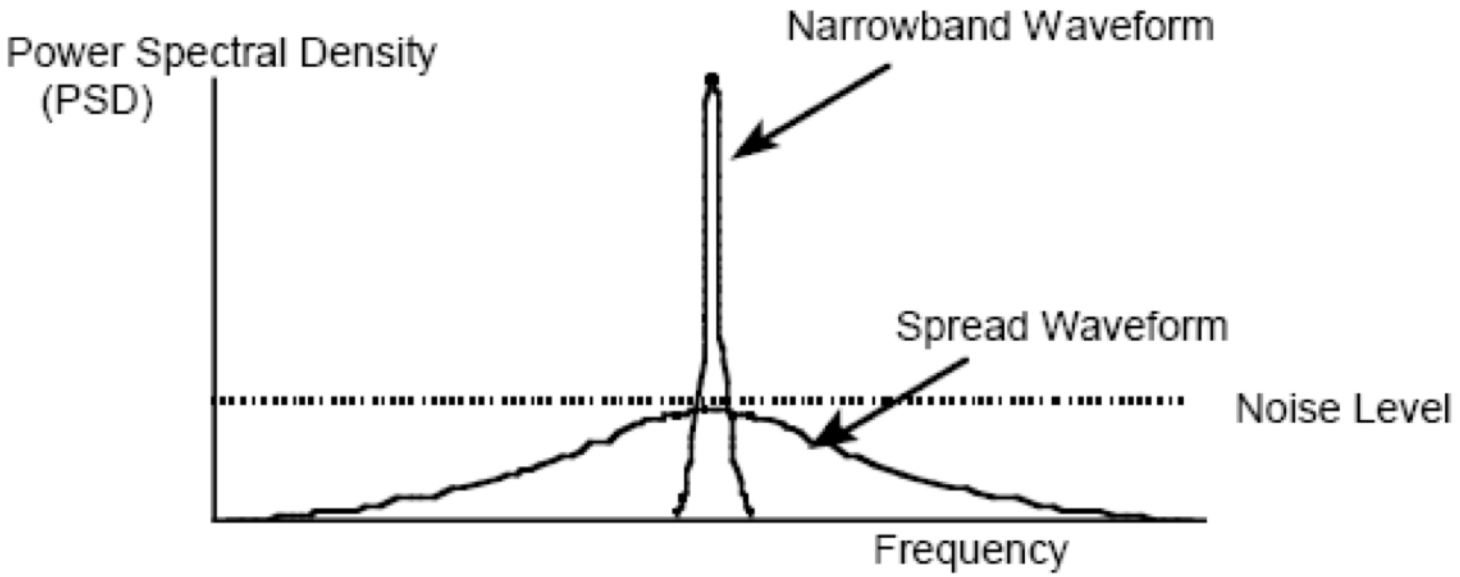
Jaguar-V frequency-hopping radio system
IEEPKOC, Vol. 129, Pt. F, No. 3, JUNE 1982



1 hop band =256 channels spaced by 25kHz
=6.4 MHz

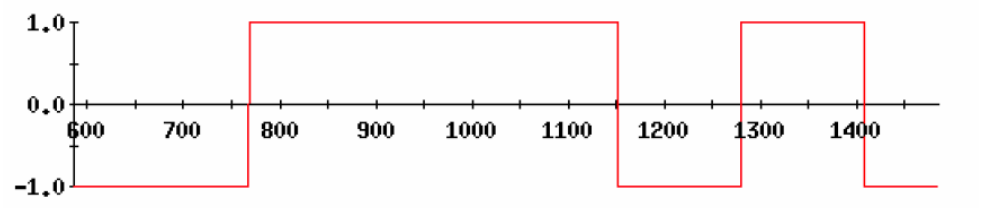
Direct Sequence Spread Spectrum

- DSSS
  - Spread the signal using a secret code (derived from a key)
  - Signal is “hidden” in noise (*we need noise*)

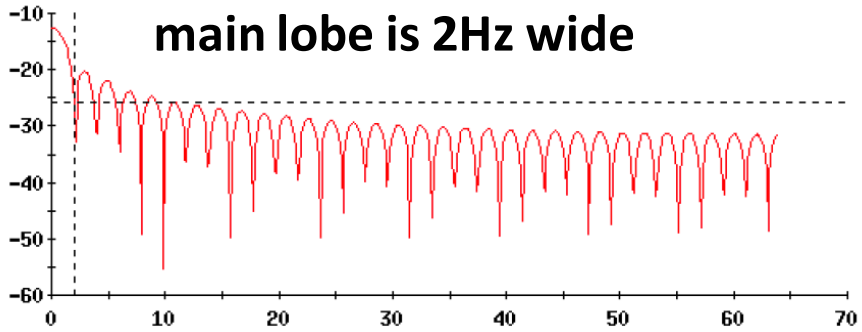


Direct Sequence Spread Spectrum

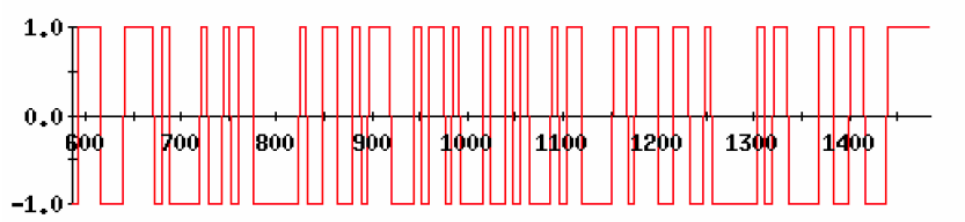
- DSSS
  - Spreading (baseband)
  - To spread, we need to transmit with a higher symbol (bit) rate. *Makes sense?*



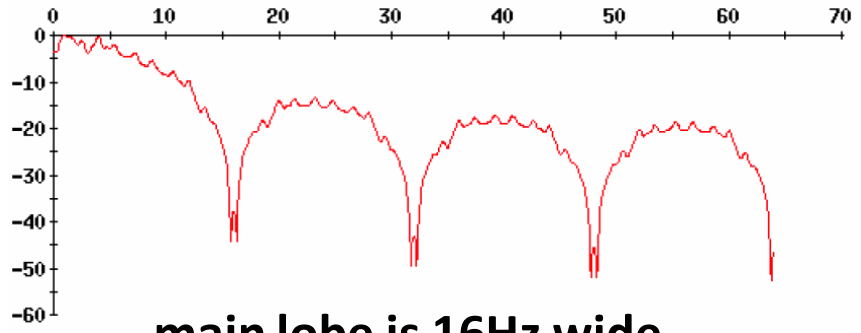
symbol rate is 2



main lobe is 2Hz wide



symbol rate is 16



main lobe is 16Hz wide

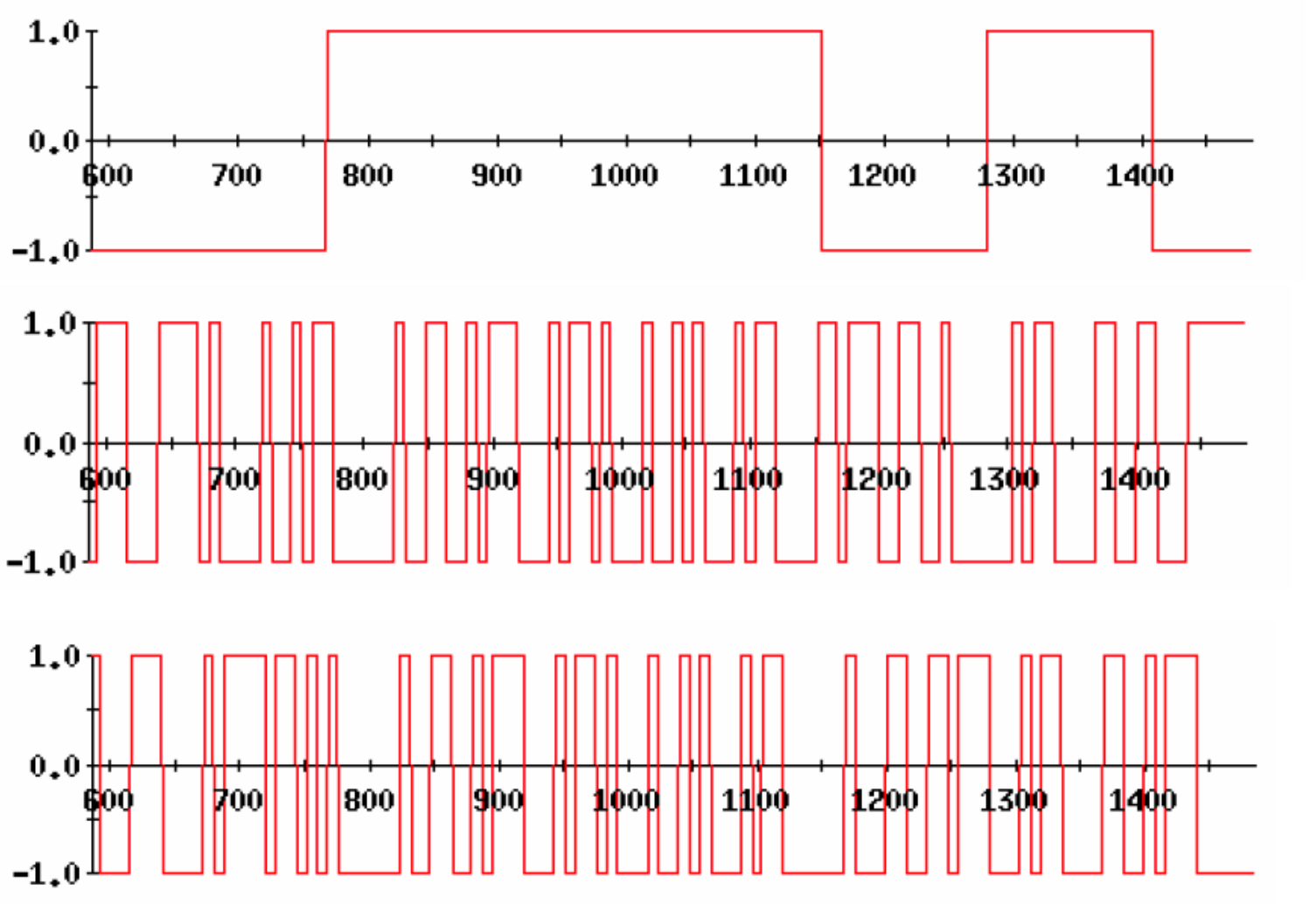
Direct Sequence Spread Spectrum

The ratio of the chip rate to the information bit rate is the *processing gain (PG)*

information (bits)

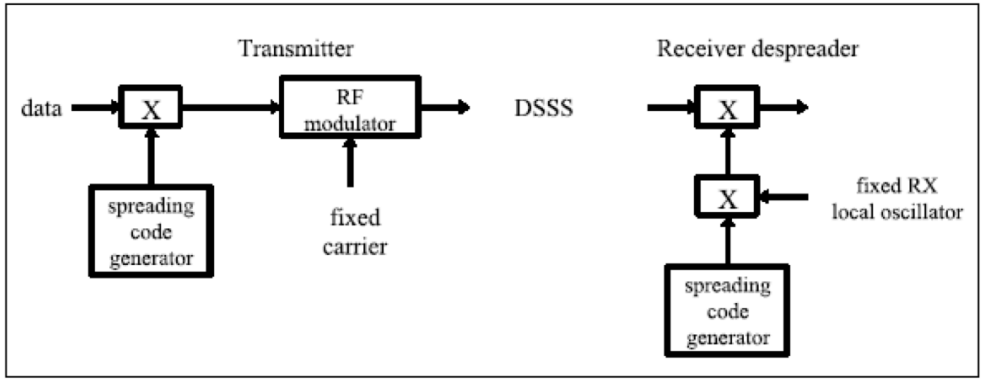
spreading code (chips)

spread signal



Direct Sequence Spread Spectrum

- Spreading and Modulation

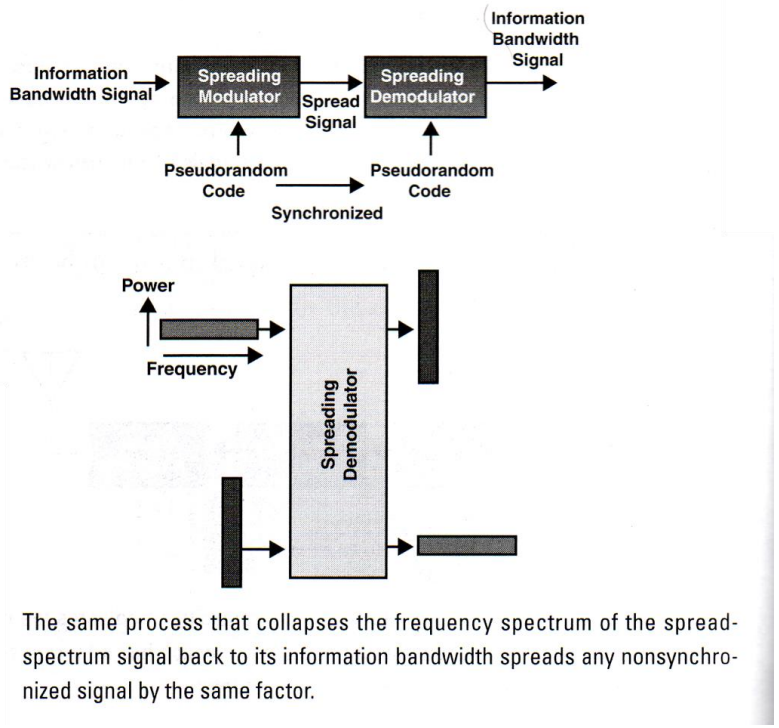


Spreading code is produced by a spreading code generator

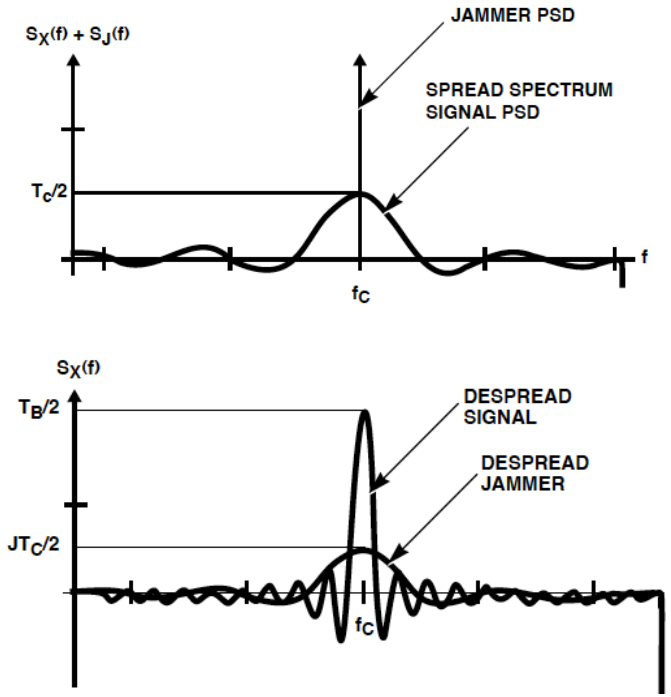
- Some systems operate with public spreading codes (to mitigate interference)
- For anti-jamming purposes, pseudo random sequences need to be long and infrequently repeat (wide spread)
- They need to have *good auto and cross correlation properties*

Direct Sequence Spread Spectrum

- DSSS under Narrow-band Jamming
  - Using a code on a narrow-band jamming signal spreads the signal (cross/auto correlation properties of the codes).

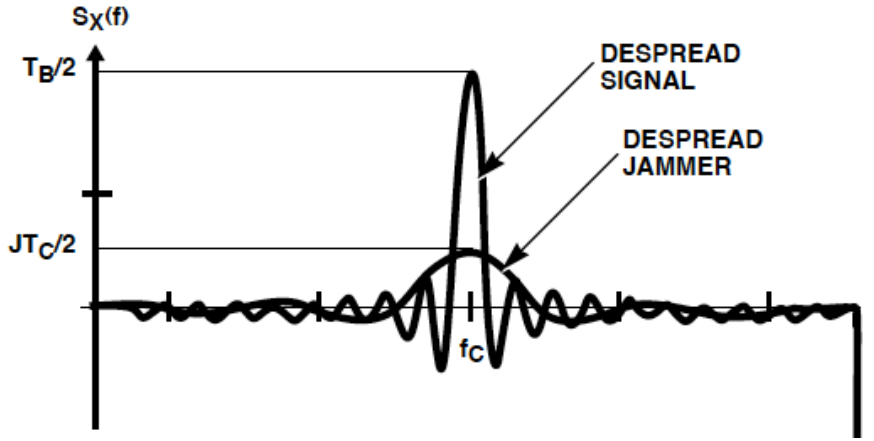


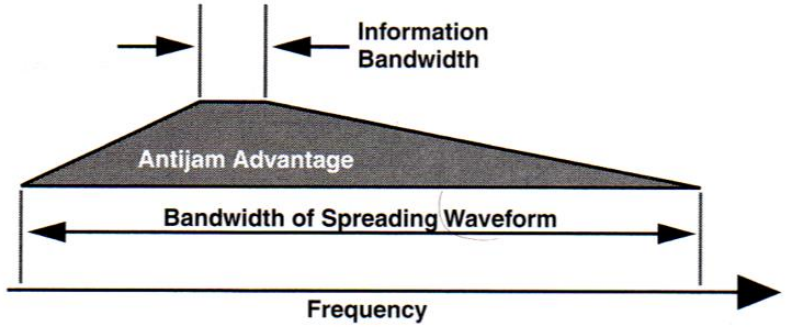
The same process that collapses the frequency spectrum of the spread-spectrum signal back to its information bandwidth spreads any nonsynchronized signal by the same factor.



Direct Sequence Spread Spectrum

- *DSSS under Narrow-band Jamming*
  - Jamming margin
    (The level of interference (jamming) that a system is able to accept and still maintain a specified level of performance, such as maintain a specified bit-error ratio even though the signal-to-noise ratio is decreasing)





In order to jam a spread-spectrum signal, it is necessary to get sufficient jamming energy through the despreading process, which discriminates against nonsynchronized signals by the ratio of the spreading bandwidth to the information bandwidth.

Jamming margin: $M_J = G_P - L_{SYS} - SNR_{OUT}$

where

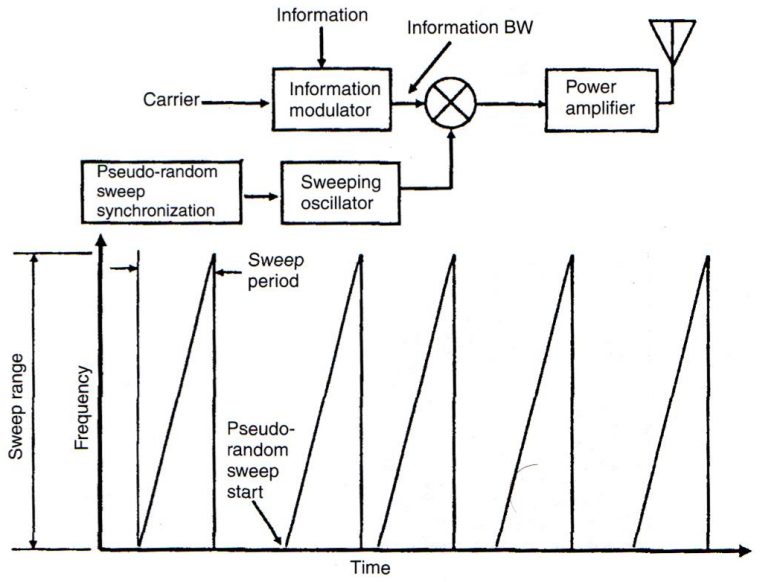
M_J = the jamming margin (in decibels);
G_P = the processing gain (in decibels);
L_{SYS} = the system losses (in decibels);
SNR_{OUT} = the required output SNR.

Direct Sequence Spread Spectrum

- Summary
  - DSSS hides the signal in the noise
  - Signal detection is now more difficult (w/o code)
    - Can be done through energy detection (requires strong signal) or signal characteristics (constant chip rate)
      (Dillard&Dillard, Detectability of Spread Spectrum Signals, 1989)
  - Signal interception/modification difficult – LPI
  - Narrowband jamming now requires much higher power
  - Broadband jamming still effective (if you have enough power)

Chirp Signals

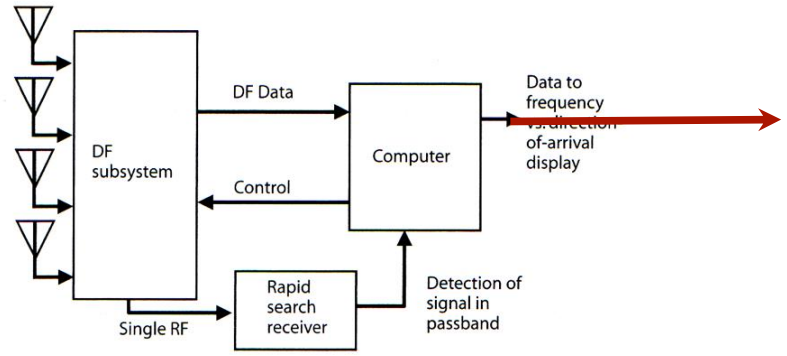
- Random start and then sweep… (can be used with FH)
  - Prevents narrow-band and partial-band jamming
  - Follower jammers might be an issue



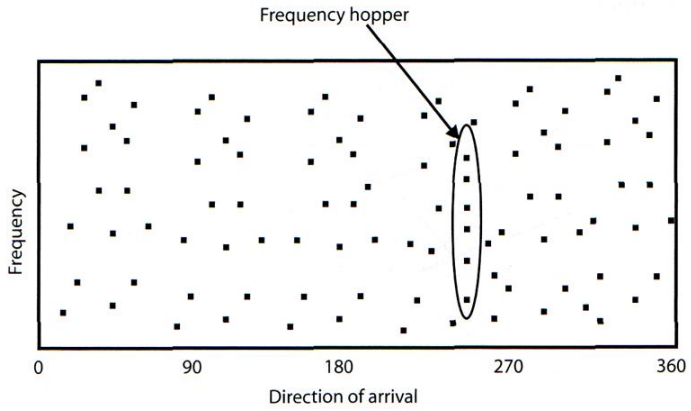
Chirp signals are rapidly swept over a frequency much wider than the information bandwidth of the transmitted signals.

Detectability of FHSS/DSSS (LPI)

- *Detectability / Localization of FHSS transmitters*
  - FHSS transmitters do not really "hide"
  - Using AoA techniques can be detected
  - Other possible techniques include differential RSS localization, TDoA, etc ...



9 A sweeping DF system for frequency hoppers includes a rapid search receiver to detect occupied channels. Then the search is stopped while a DF is taken.

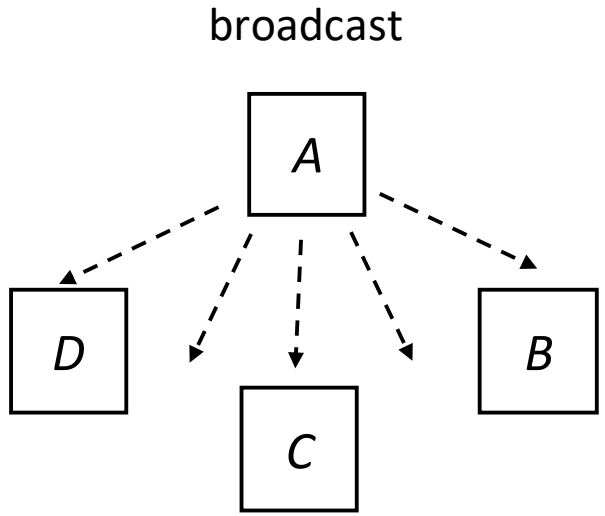


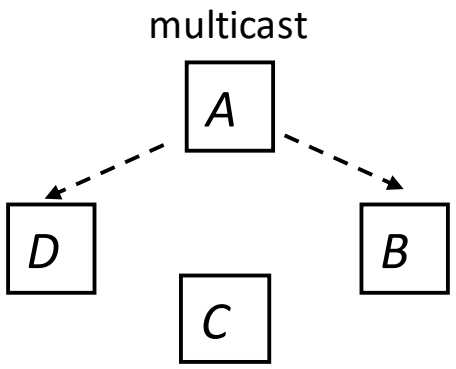
i.40 When collected DOA data shows multiple frequencies at one angle of arrival, a frequency hopper is identified.

Broadcast Jamming-Resistant Communication

Broadcast Communication

- *Broadcast communication*
  - One sender, many receivers
  - Open system
    - New receivers may join, receivers may withdraw
    - Any receiver can listen (in contrast to multicast)



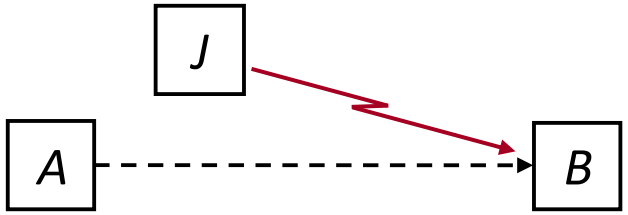


Examples:

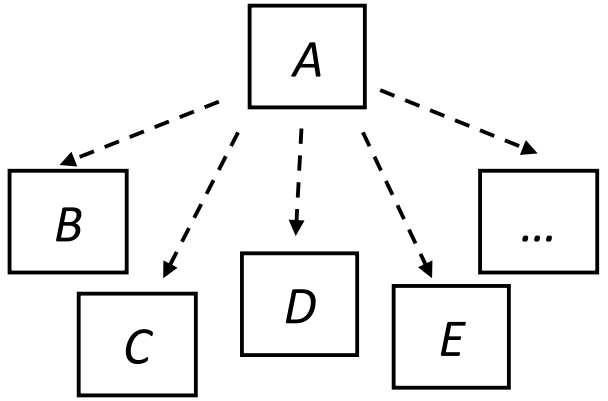
- Radio (audio) broadcast (AM, FM, …)
- Navigation signals: satellite-based (GPS), terrestrial (LORAN)

Attacks on Broadcast Communication

- For pairwise (unicast) communication we only consider *external* (*outsider*) *attackers*
  - A and B are mutually trusted
  - Attacker uses only public information



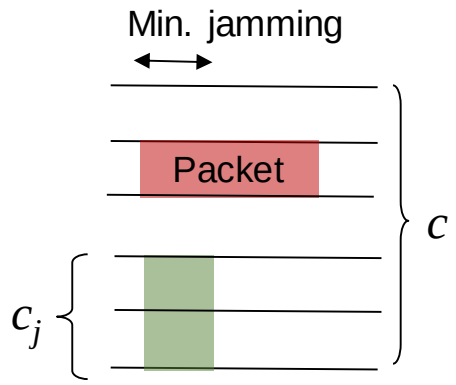
- Broadcast communication
  - High and unknown number of receivers
  - Receivers are potentially untrusted
  - We need to consider *external attackers* and *internal* (*insider*) attackers
  - Group keys?



External Attackers on SS Techniques

- *External attacker*
  - Does not know the spreading code / hopping sequence
  - Partial-band attacker can still jam. Example: FHSS

c = # frequency channels
c_j = # channels the jammer jams
n_j = # jamming cycles per packet (given by min. jamming period, packet length, and jammer capabilities)



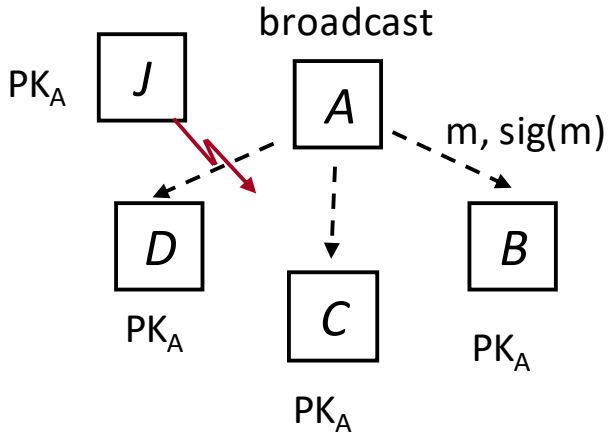
p_j = Probability that the packet is jammed

$$= 1 - (1 - c_j/c)^{nj}$$

Typical computation of jamming probability via the inverse

Anti-jamming Broadcast *Without Shared Keys*

- Problem: BS needs to broadcast an (authenticated) message to a large number of *unknown/untrusted receivers* in an *anti-jamming manner*.



- Applications: alarm broadcast, navigation signals, etc…

But …

Anti-jamming communication relies on shared secret keys

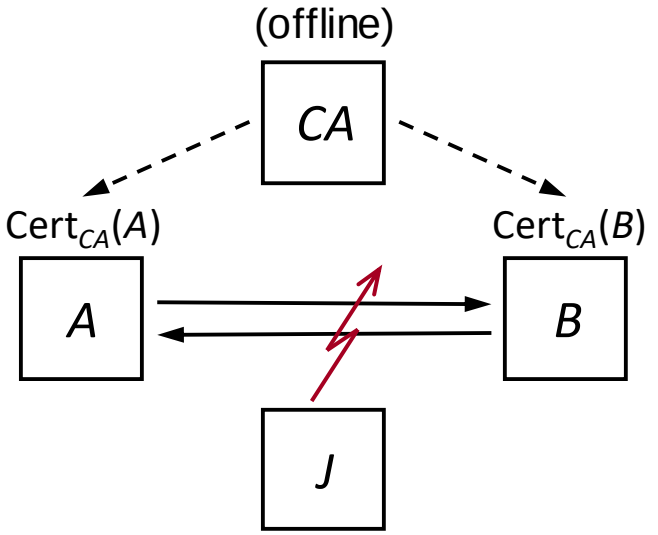
In anti-jamming broadcast we cannot rely on shared keys (unknown/untrusted receivers)

Public-key crypto does not help

Anti-Jamming Key Establishment

Problem:

A and *B* want to establish a shared secret key in the presence of jammer J



Assumptions:

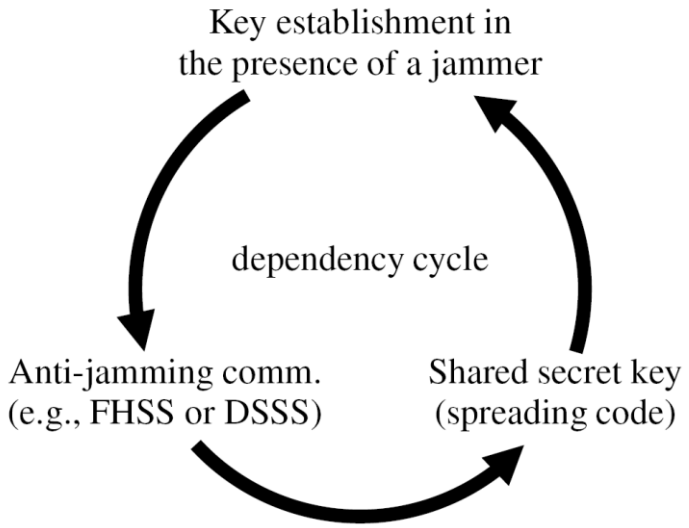
- *A* and *B* do not share any secrets
- The clocks of A and B are loosely synchronized O(s)
- Each node has a public/private key pair and a certificate binding its identity to the public key
- *CA* (Certification Authority) is trusted by all nodes; it may be off-line or unreachable by the nodes at the time of communication

Anti-Jamming / Key-establishment Dependency

Key establishment depends on jamming-resistant communication

Common anti-jamming techniques require a shared secret key (code)

Leads to an anti-jamming/key-establishment dependency cycle



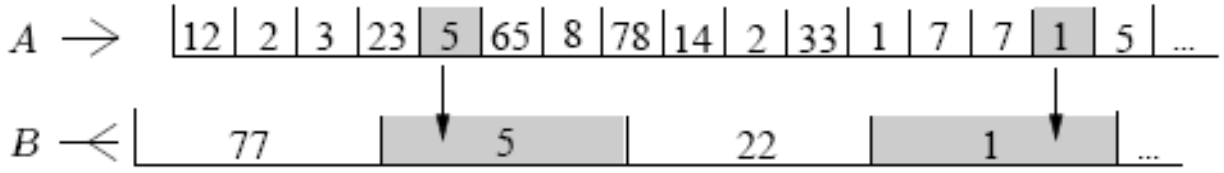
Two Solutions: UFH and DSSS

Basic idea:

- If you cannot coordinate the sender and the receiver – Don't!
- Sender uses random hopping sequences / spreading codes unknown to the receiver (public set)

Two solutions:

- Uncoordinated Frequency Hopping Spread Spectrum (UFH)
- Uncoordinated Direct Sequence Spread Spectrum (UDSSS)

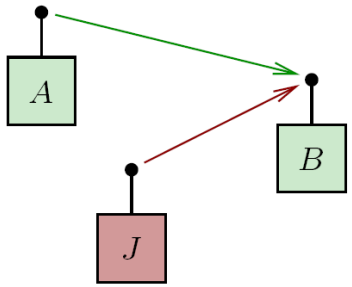


Rationale:

- The attacker cannot predict which channels will be used (neither can the receiver)
- Equivalent to FH in jamming protection (but not in throughput)
- Throughput can be improved by using broadband receivers (c_t, c_r)

Attacker Model

- Attacker goal: to prevent communication!
- Attacker actions: *Jam*, *Insert*, *Modify*
- Attacker types: Responsive, Sweep, Random, …
- Attacker strength (channels/time to jam/sense): c_s / t_s, c_j / t_j
- Power to insert, jam, and overshadow: P_t, P_j, and P_o
- P_T : total signal strength that attacker J can achieve at the receiver B



- Given the number of frequency channels on which the attacker inserts (c_t), jams (c_j), and overshadows (c_o),

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

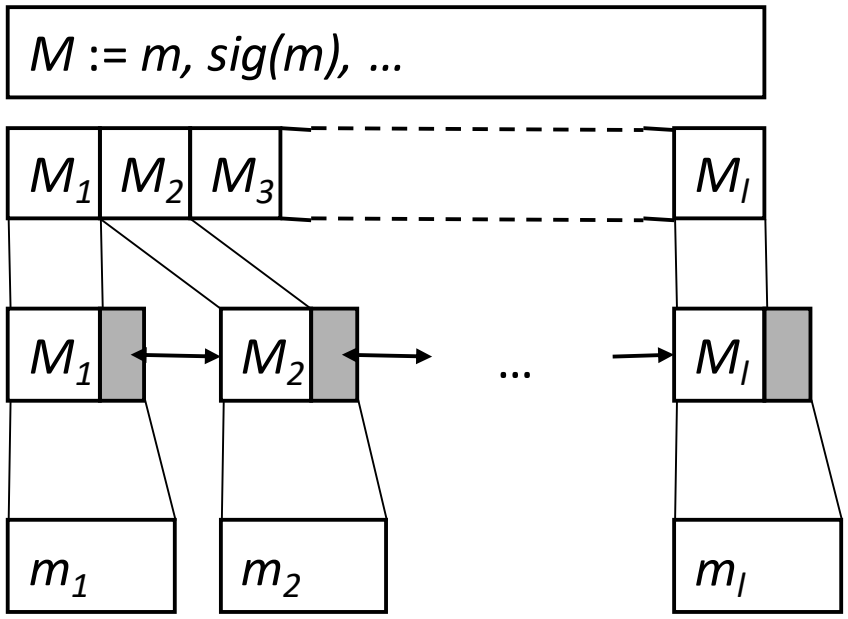
Uncoordinated Frequency Hopping (transmitter)

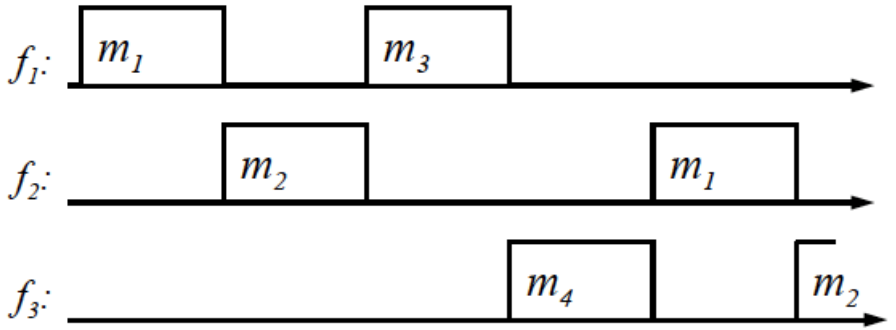
1. Fragmentation

2. Fragment linking
   (protects against insertion)

3. Packet Encoding (ECC)
   (protects against jamming)

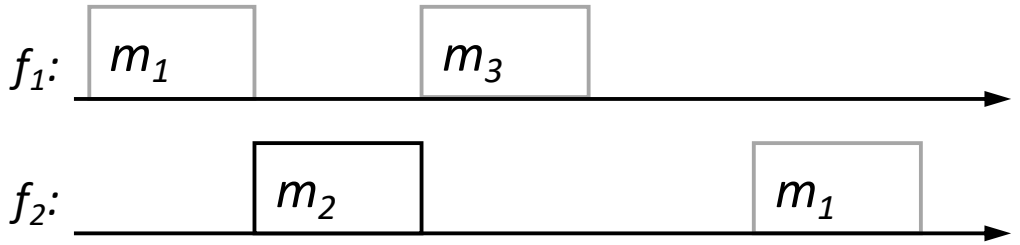
4. Repeated transmission



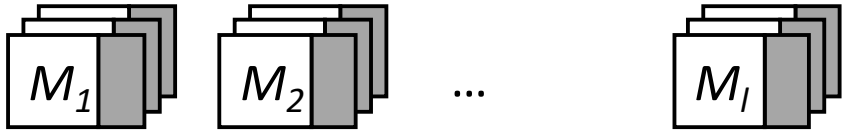


Uncoordinated Frequency Hopping (receiver)

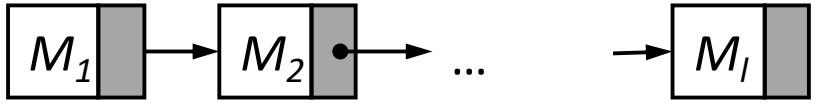
1. Receiving packets



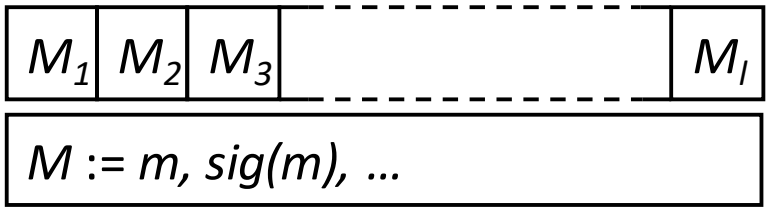
2. Packet decoding



3. Ordering and linking

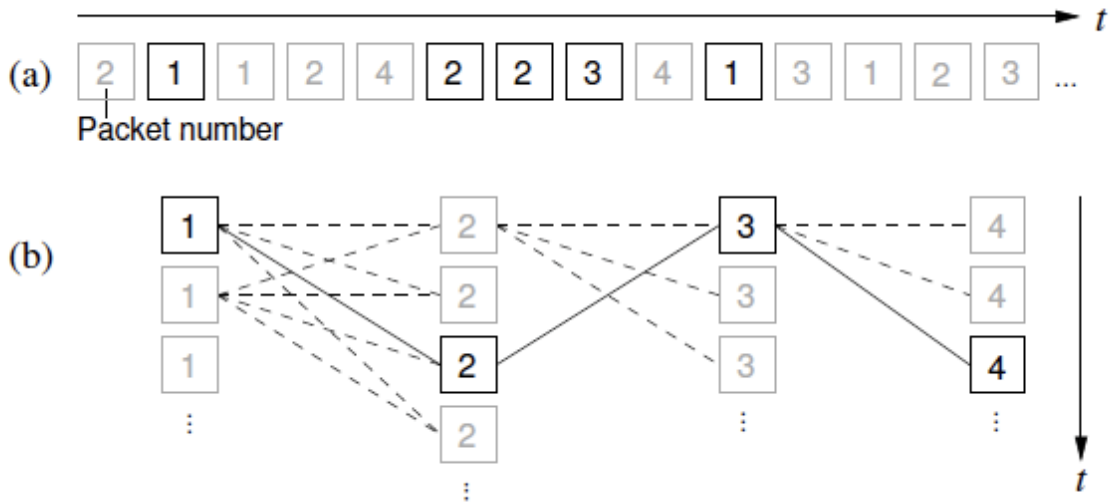


4. Message reassembly and signature verification



Security analysis: Fragment linking

Problem: Fragments are not individually authenticated (pollution attacks)



$(I+1)^{\ell}$

Signature verification at each candidate message (after reassembly)

In the best case, I=1 … (depends on the attacker's # of channels, power, …)

but ℓ is large; $\ell = \frac{message\ size}{slot\ size}$ (>20)

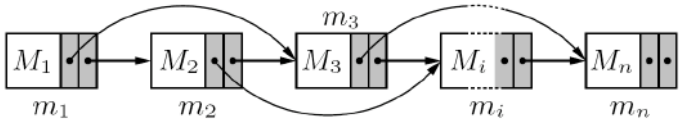
Result: Attacker performs a DoS attack on the logical level instead of the physical

Security analysis: Fragment linking

Problem: Fragments are not individually authenticated (pollution attacks)

Solution: Cryptographically link fragments (no reliance on shared key) to achieve message integrity

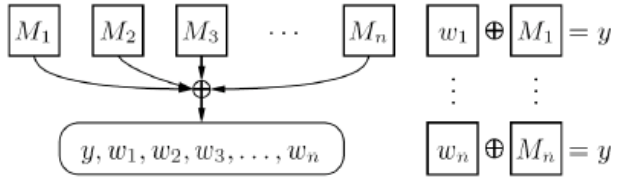
Hash linking



$$m_i := id||i||l||M_i||h_{i+1}||\ldots||h_{i+\alpha}$$

Min 1 hash

One-way Accumulators



$$m_i := id||i||l||M_i||w_i$$

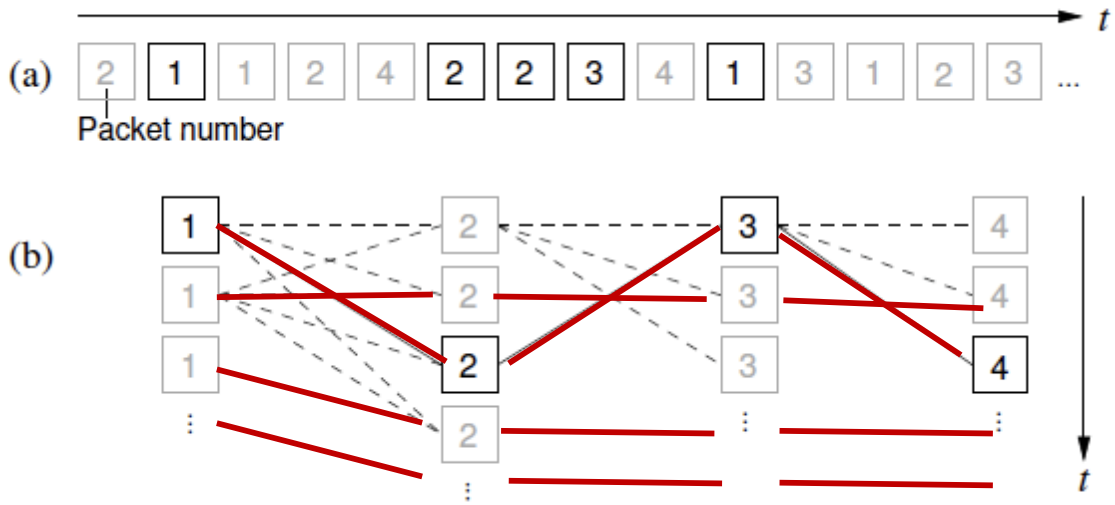
1 witness

Short signatures

$$m_i := K_M||i||l||M_i||Sig_{K_M^{-1}}(K_M||i||l||M_i)$$

1 short signature

Security analysis: Fragment linking



Gain: Instead of $(I+1)^{\ell}$ signature verifications, reduction to $(I+1)\ell$ hash/accum/signature verifications + $(I+1)$ signature verifications

Signatures and accumulators better than hash linking

Possible extensions:

- Use linking with erasure codes, e.g., Fountain codes
- Reconstruct the message from any *k* fragments.

Security analysis: Packet Encoding

Defined by the jamming resistance ρ and coding rate r_c

- Packet transmission time:
- #channels that the attacker can (blindly) jam during the transmission:
- #channels that the attacker can scan during the transmission
- #channels that the attacker can block during the transmission

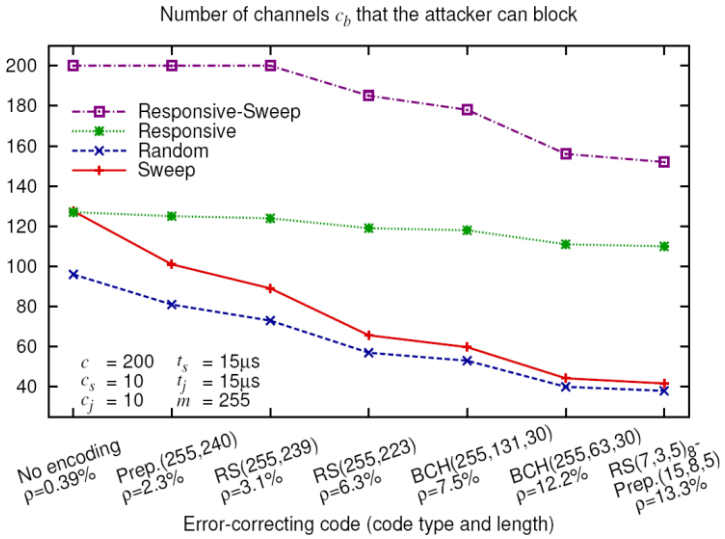
$$t_m = |m|B/r_c$$

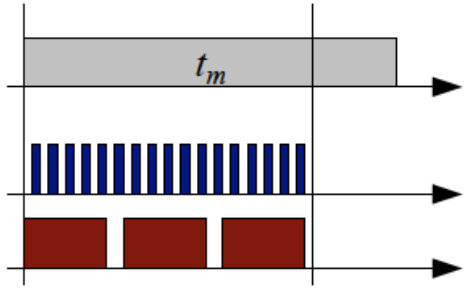
$$n_j := \frac{t_m}{\rho t_m + t_j}$$

$$n_s := \frac{t_m - \rho t_m - t_j}{t_s}$$

$$c_b = n_j c_j + n_s c_s$$

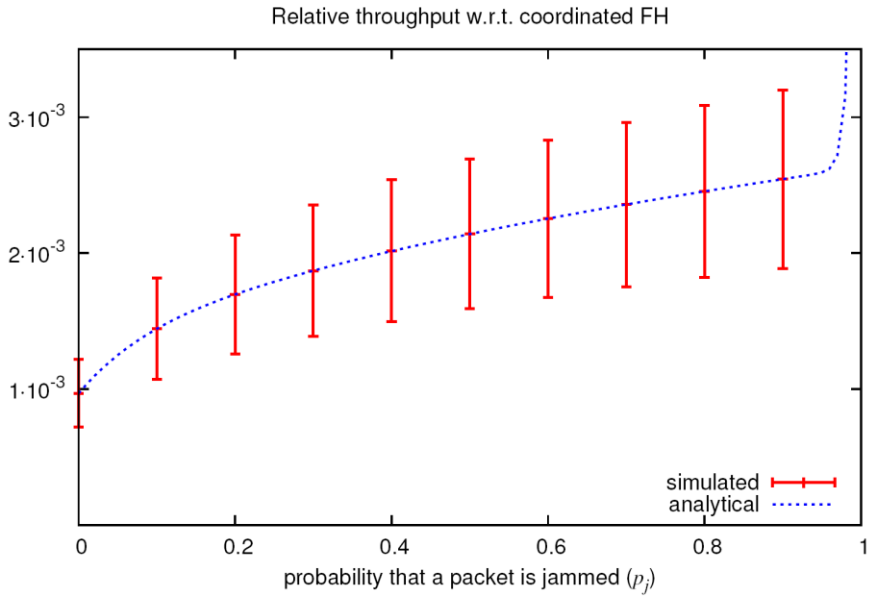
$$p_j = \frac{c_b}{c}$$





Performance Results

- Optimal # of channels ($c^*=2c_b$)



- Some results (c=200, 1MBit/s, 1600 hops/s, ECC signature, |M=2176|, ℓ=13)
  - Throughput: 1000x slower than FH
  - Latency: 2 – 100s (different attacker strengths)

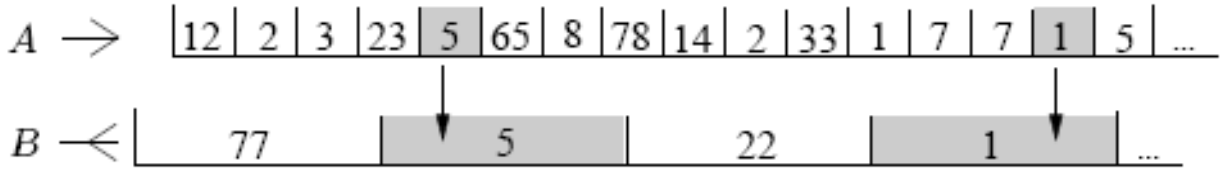
Two Solutions: UFH and DSSS

Basic idea:

- If you cannot coordinate the sender and the receiver – Don't!
- Sender uses random hopping sequences / spreading codes unknown to the receiver (public set)

Two solutions:

- Uncoordinated Frequency Hopping Spread Spectrum (UFH)
- Uncoordinated Direct Sequence Spread Spectrum (UDSSS)

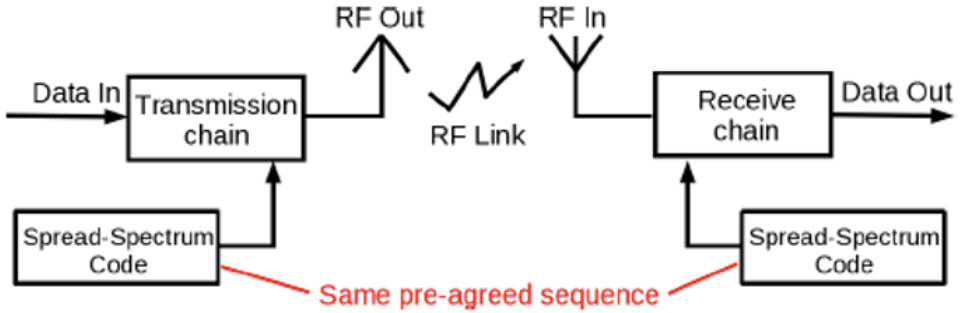


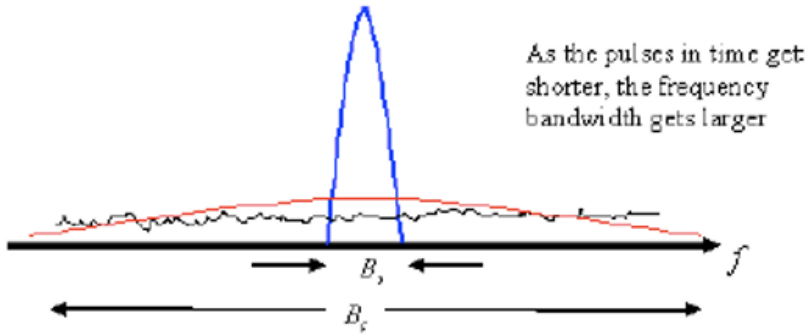
Rationale:

- The attacker cannot predict which channels will be used (neither can the receiver)
- Equivalent to FH in jamming protection (but not in throughput)
- Throughput can be improved by using broadband receivers (c_t, c_r)

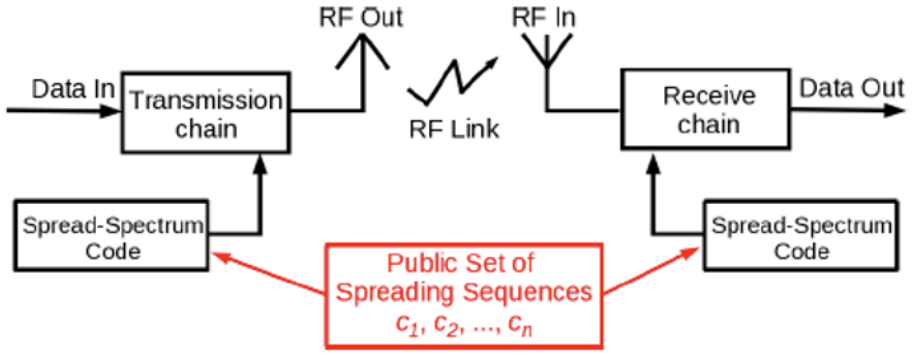
Uncoordinated Direct Sequence Spread Spectrum

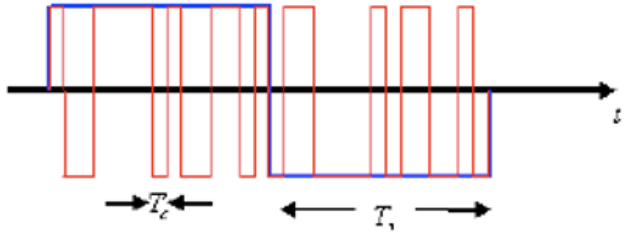
- DSSS





- UDSSS





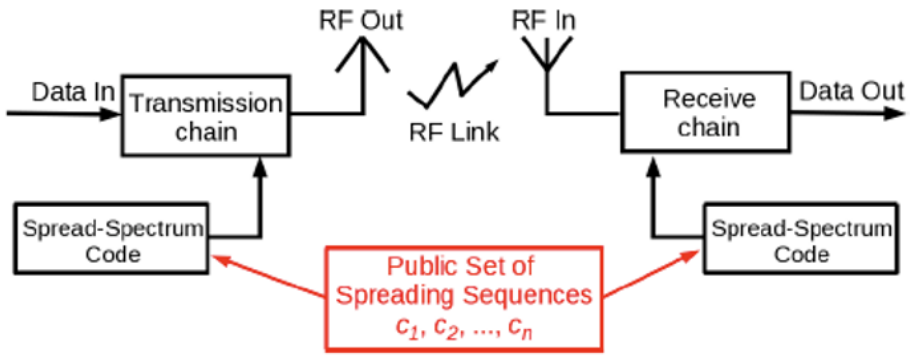
Uncoordinated Direct Sequence Spread Spectrum

Public set *C* of spreading codes

Sender randomly selects sequence
$c_s \in C$ to spread message *M*

Receivers record signal and despread *M*
by applying sequences from *C*
using a trial-and-error method

- UDSSS



Public set *C* of spreading codes

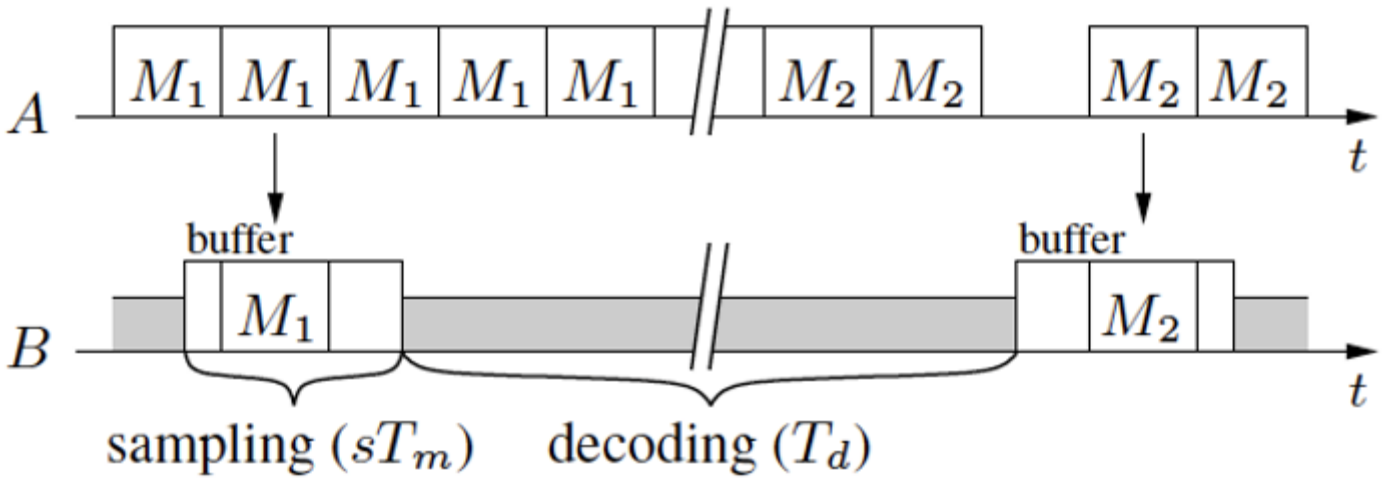
Sender randomly selects sequence
$c_s \in C$ to spread message *M*

Receivers record signal and despread *M*
by applying sequences from *C*
using a trial-and-error method

- UDSSS

Uncoordinated Direct Sequence Spread Spectrum

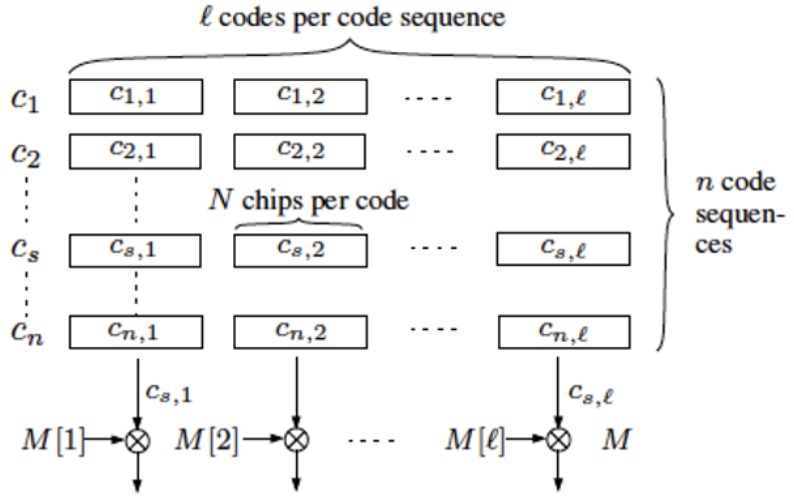
- Message repetitions, due to
  - lacking synchronization between sender and receivers
  - The possibility of successful jamming attacks



Uncoordinated Direct Sequence Spread Spectrum

- Code Set *C* composed of *n* code sequences
- Each code sequence is composed of *ℓ* spreading codes containing *N* chips

  - E.g., N = 100 chips
    → 20 dB processing gain
  - Auto-correlation and cross-correlation properties

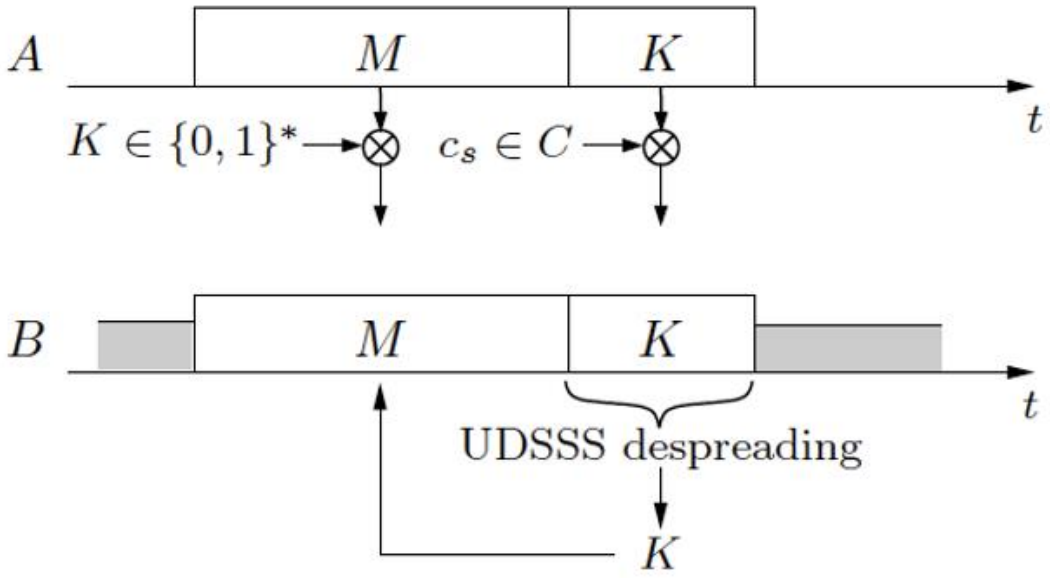


- Successful despreading requires to hit the correct spreading sequence *and* the correct synchronization

UDSSS: Optimization

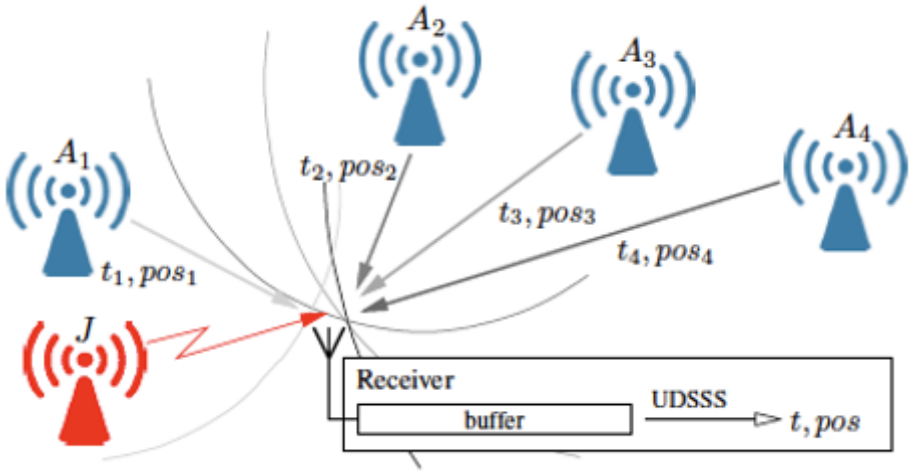
- **Idea**: Use UDSSS to transmit the spreading key only
- **Trick**: First transmit message *M* using a random spreading code *K*, then transmit the spreading code *K* using UDSSS

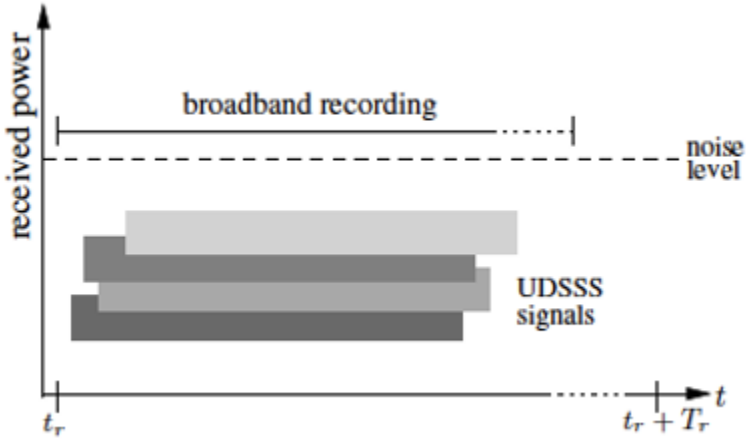
- **Advantages:**
  - Smaller spreading code set
  - Quicker decoding
  - Longer messages
  - More flexible security level



UDSSS: Example Application

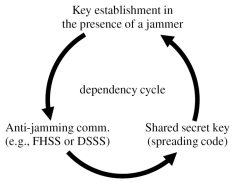
- For positioning and/or time-synchronization
- Requirements:
  - Signals from three to four different base stations
  - Precise time-stamping of signal reception
- UDSSS provides
  - Anti-jamming transmission of multiple signals in parallel
  - Precise time-stamping of signal reception (despite delayed recovery) & updated time-stamps in each transmitted message
  - Anti-spoofing protection of authenticated messages



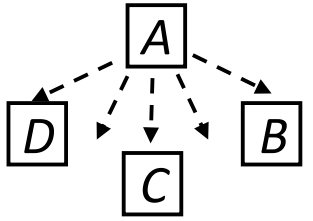


Summary

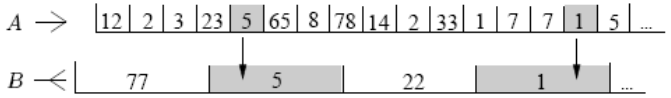
- Anti-jamming – key-establishment circular dependency



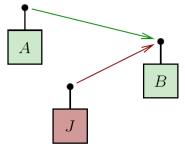
- Broadcast anti-jamming problem



- UDSSS and UFH



- New attacker models



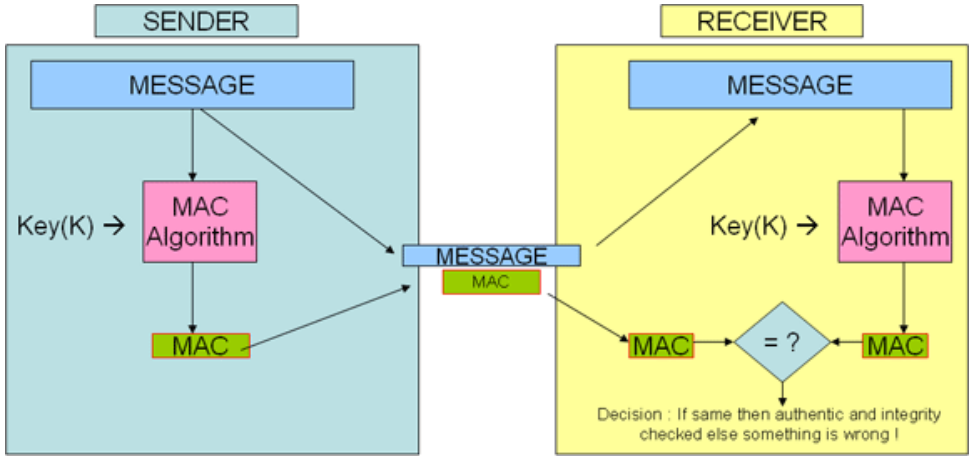
- Applications

Physical Layer Security

Application of (Broadcast) Anti-Jamming Techniques to Key Establishment

Applications for Shared Keys in Wireless Networks

- Shared keys are required / used for:
  - Communication techniques (DSSS, Frequency Hopping)
  - Encryption of messages
  - Integrity protection of messages (MACs = Message Authentication Codes)



[www.answers.com]

  - Authentication / authorized access
  - …

The Problem with Key Establishment

Key establishment is a challenge

Pre-sharing Symmetric Keys

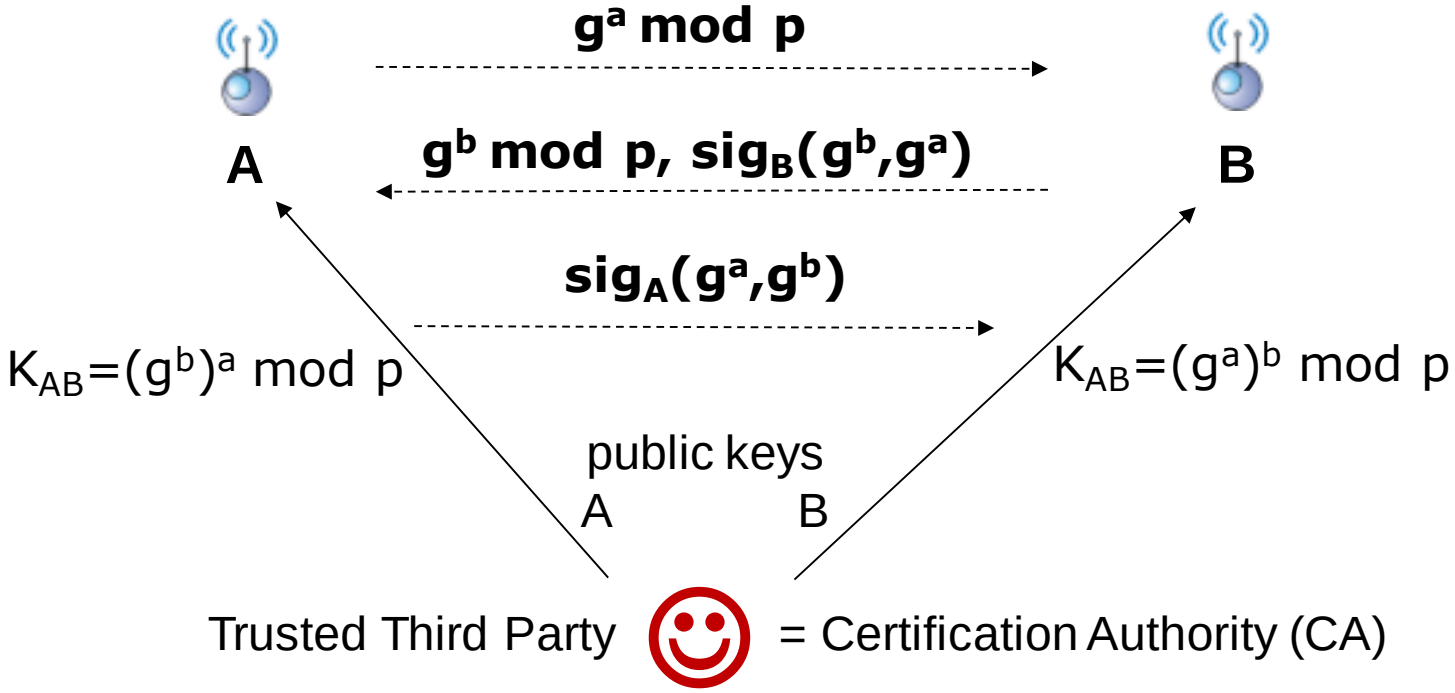
- A Trusted Third Party (TTP) pre-loads the keys
- Efficient (+)
- Suffers from network dynamics problems (-):
  - New nodes joining, key revocation, key compromise

Key Establishment

- Based on public-key (asymmetric) cryptography
- Prominent examples: RSA, Diffie-Hellman (DH)
  - Based on computational hardness of factorization (RSA) or discrete logarithm (DH) problem
- Requires reliable communication

DH Key Establishment

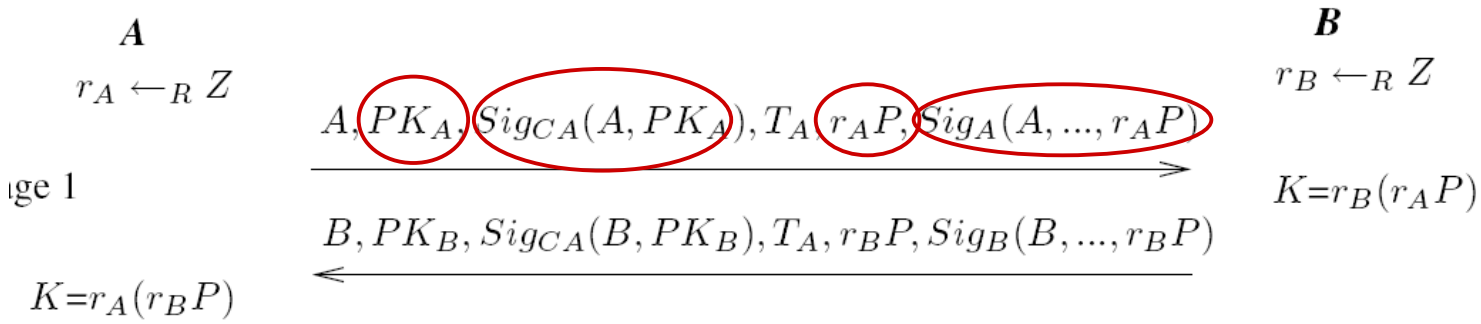
- Nodes A and B do not share any secrets, but possess certificates of their public keys
- Authenticated Diffie-Hellman Protocol (using signatures)



- *Conventional SS-Techniques cannot be used for the communication due to the missing shared secret*

Key Establishment Protocol: Sender/Receiver

- ECC-based Station-to-Station Diffie-Hellman
  - P lies on elliptic curve $E(F_q)$, CA = Certification Authority
  - PK_A= A's public key, Sig_A= A's signature, r_AP= A's key contribution



- Elliptic Curve Cryptography (ECC) enables to reduce the key length while maintain the level of security
  - E.g., 128-bit security level [NIST] → 256 bit prime fields on elliptic curves and 512 bit keys (vs. 3072-bit key for RSA)
- Use UFH to transmit the messages