Wireless Security gets Physical

Srdjan Čapkun

Department of Computer Science

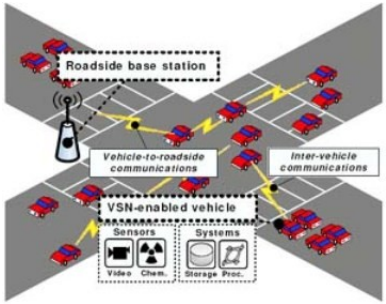
ETH Zurich

SWING Summer School 2008

Age of wireless communication ...

- Mesh Networks (Inter and Inter-home)
- Vehicular Networks
- Sensor/Actuator Networks
- Networks of Robots
- Underwater Networks
- Personal Area (body) Networks
- Satellite Networks (NASA 2007)
- Cellular, WiFi, ..

- Digitalization of the physical world: every physical object will have a digital representation
- “Internet of things” communication with every object/device



Technologies enabling wireless networks

- GSM/UMTS (800, 1900MHz, ...)
- 802.11 (WiFi) (LAN) Wireless Fidelity
  - 2.4 GHz, 54Mbps, 100mW-1W, 30m range
- 802.16 (WiMAX)
  - 10-66 GHz, < 10km coverage
  - 2-11GHz, < 20km coverage
  - 75Mbps (theoretical), 20km, 5Mbps (typically, 5km)
- UWB
  - 3.1 - 10.6 GHz, short-range Gbps communication
  - lower speed, longer range, localization (<2km outdoor)
- 802.15.4 (Zigbee) (WPAN) (Sensor networks)
  - 868 MHz in Europe, 915 MHz in the USA and 2.4 GHz
  - 250kbps, 1mW, ~100m range
  - 4 MHz 8-bit processors
- RFIDs
  - short range identification tags (UHF 868-956 MHz)

Applications of Wireless Networks

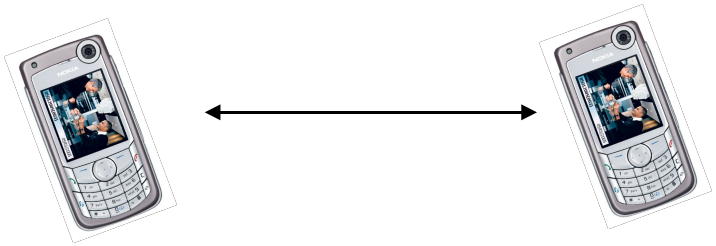
- **Infrastructure-based**
  - Cellular - ANY DATA
  - WiFi access – ANY DATA
  - GPS – LOCATION, TIME
  - Local Area (Indoor) Navigation – LOCATION, TIME

- **Infrastructure-less** (multi-hop)
  - Sensor networks – ENVIRONMENTAL (SENSED) VALUES
  - Ad hoc (e.g. vehicular network) – ANY DATA
  - Mesh networks (e.g., home networks) – ANY DATA

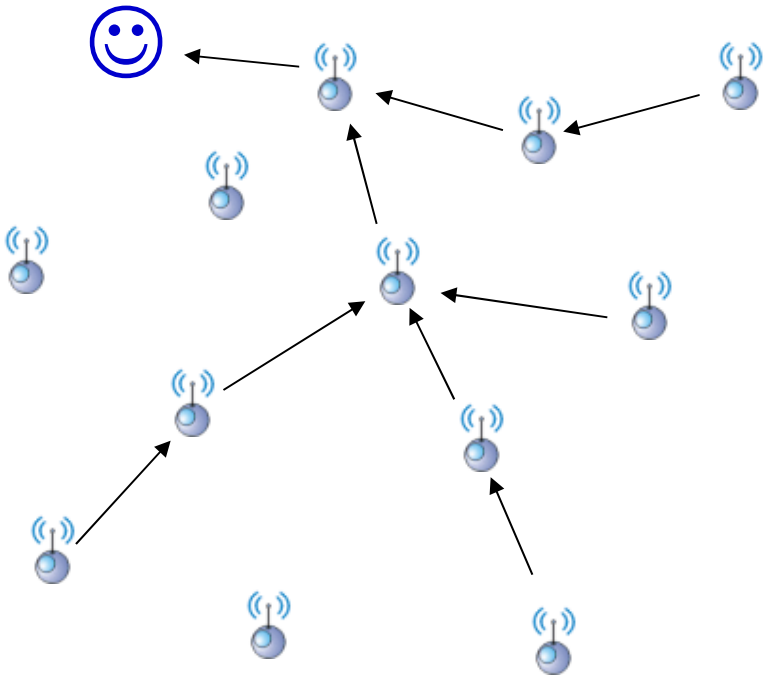
- RFID tags – IDENTITY

Application-specific security goals

Cellular networks
- infrastructure based
- single-hop (to the BS)



Informally: to **communicate privately!!!**
confidentiality is the prime security goal

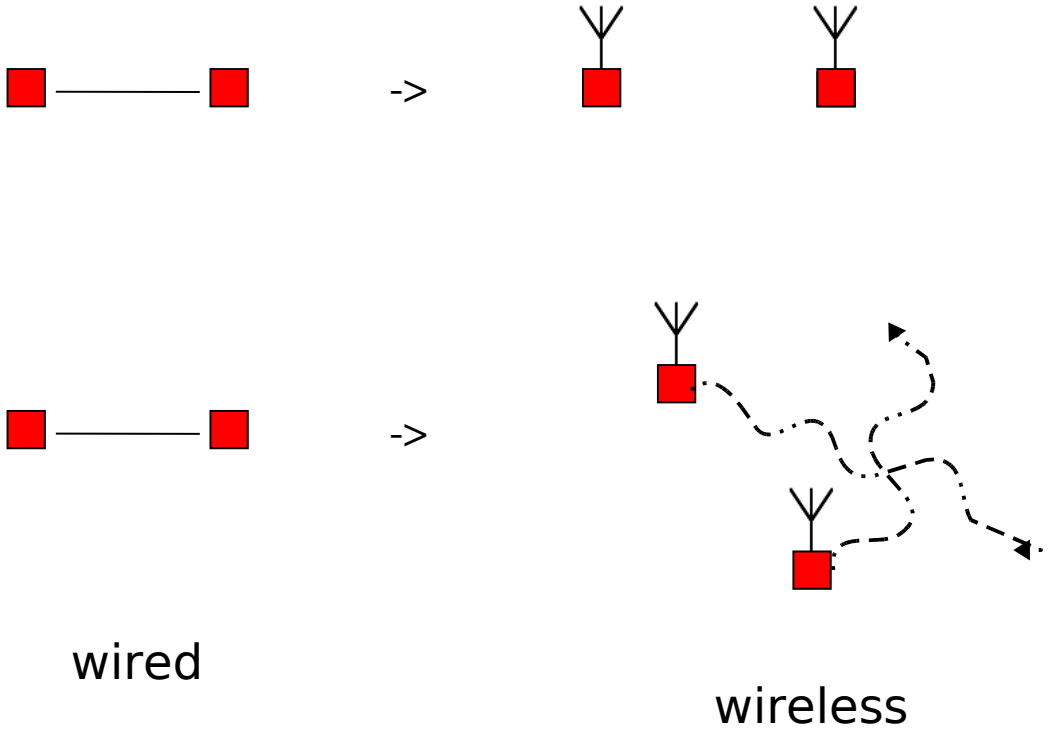


Sensor Networks
- infrastructureless
- multihop
- node compromise
- node sabotage
- displacement
- ...

Informally: to accurately **measure and deliver sensed data**
confidentiality not an issue – data authentication is important

What changed?

- Physical layer
- Physical locations of devices



The change for worse or for better?

- Physical layer
  - “New” risks: insertion, jamming, eavesdropping, ...
  - Opportunities: broadcast, localization, device identification, ...

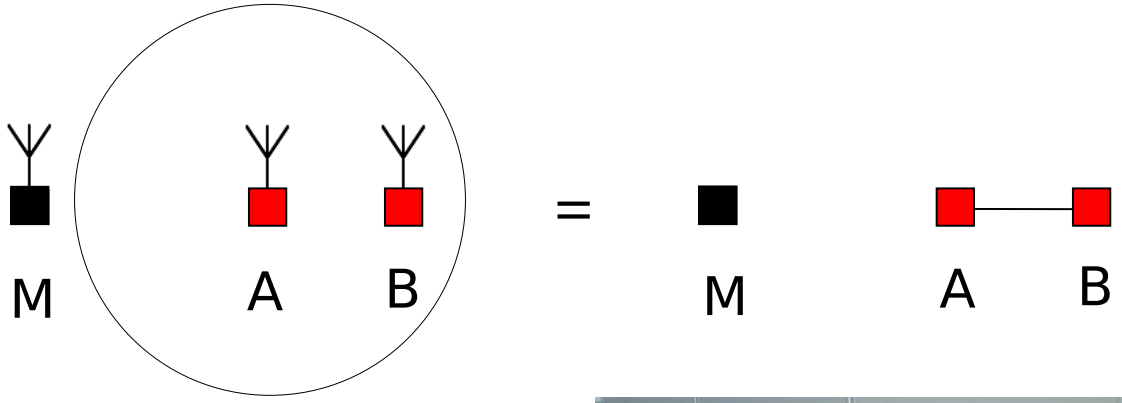
- Physical locations of devices
  - New problems: how do we (securely) localize devices, track them, how do we verify their claimed locations?, location privacy, ..
  - Opportunities: using location information to secure even basic network services (key establishment), access control, data gathering ...

Content

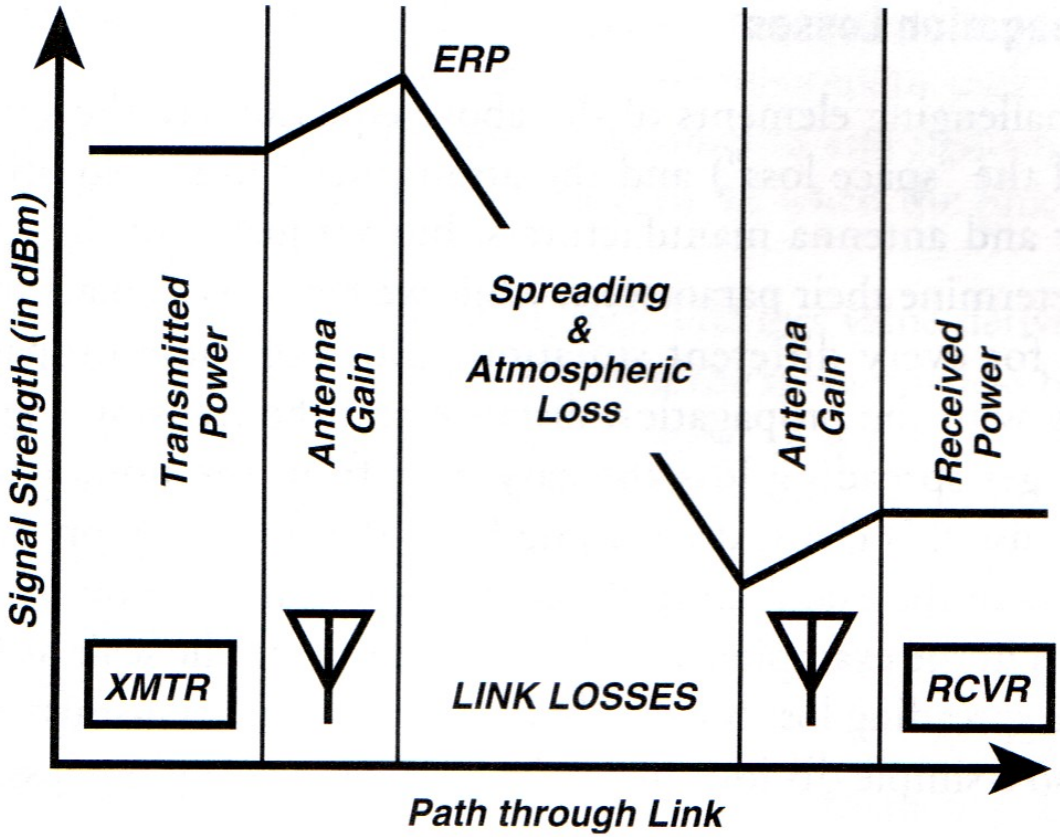
- Wireless channel basics
- Jamming/anti-jamming communication
- Secure Localization
- Location awareness
- Secure Time Synchronization

Wireless Communication Channel

A simple example



Wireless channel



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).

EW

dB, dBm, dBi, ...

Common dB Definitions

dBm	= dB value of Power / 1 milliwatt	Used to describe signal strength
dBW	= dB value of Power / 1 watt	Used to describe signal strength
dBsm	= dB value of Area / 1 meter^2	Used to describe antenna area or radar cross-section
dBi	= dB value of antenna gain relative to the gain of an isotropic antenna	0 dBi is, by definition, the gain of an omnidirectional (isotropic) antenna

A linear number is converted into dB, using the following formula:

$$N(dB) = 10\log_{10}(N)$$

$$N(dBm) = 10\log_{10}(N/1mW)$$

e.g. 1W = +30dBm

Link equation

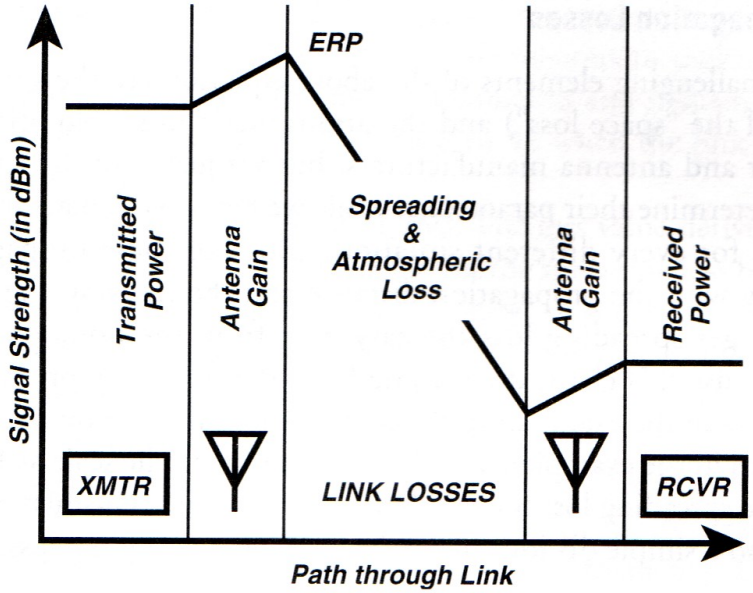
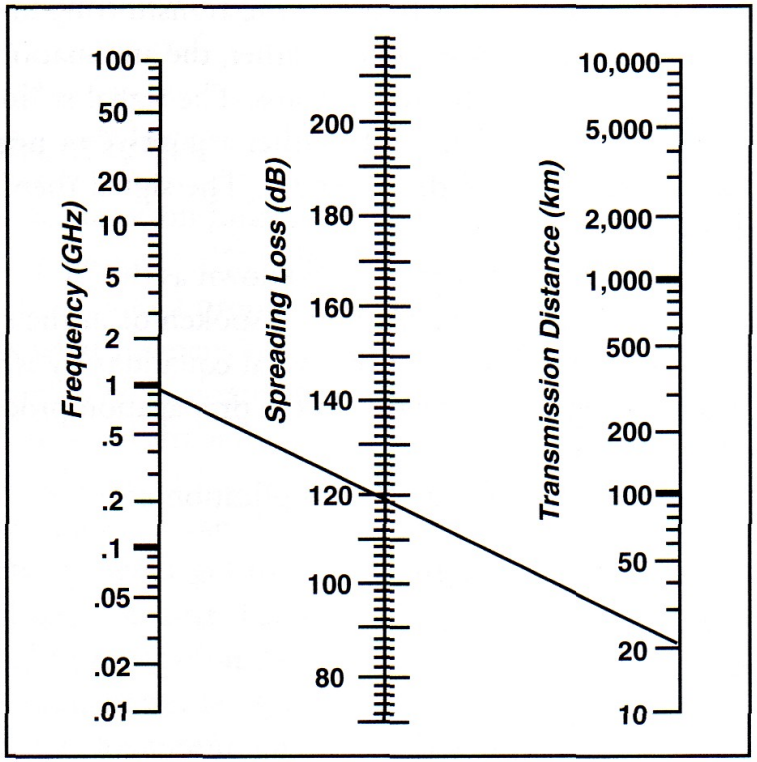


Figure 2.1 To calculate the received signal level (in dBm), add the transmitting antenna gain (in dB), subtract the link losses (in dB), and add the receiving antenna gain (in dB) to the transmitter power (in dBm).

Transmitter Power (1W) = +30 dBm
Transmitting Antenna Gain = +10 dB
Spreading Loss = 100 dB
Atmospheric Loss = 2 dB
Receiving Antenna Gain = +3 dB

$$\text{Received Power} = +30\ \text{dBm} + 10\ \text{dB} - 100\ \text{dB} - 2\ \text{dB} + 3\ \text{dB}$$
$$= -59\ \text{dBm}$$

Spreading loss

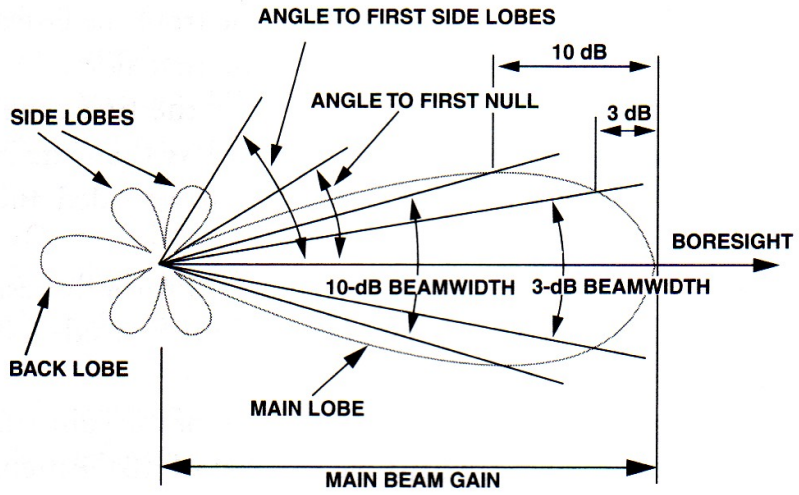


Spreading loss can be determined by drawing a line from the frequency (in GHz) to the transmission distance (in km) and reading the spreading loss (in dB) on the center scale.

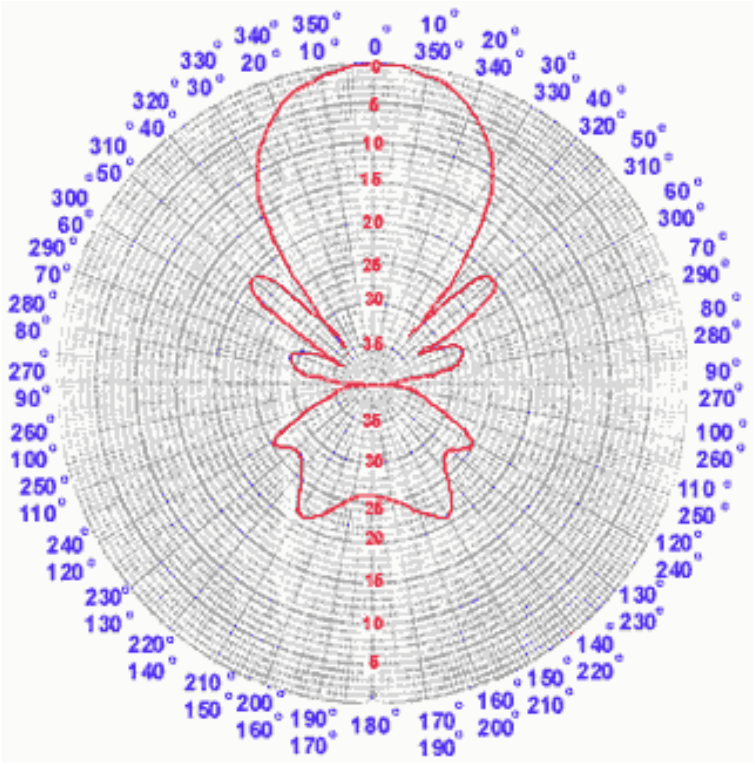
$$L_S\,(in\ dB) = 32.4 + 20\log_{10}(distance\ in\ km) + 20\log_{10}(frequency\ in\ MHz)$$

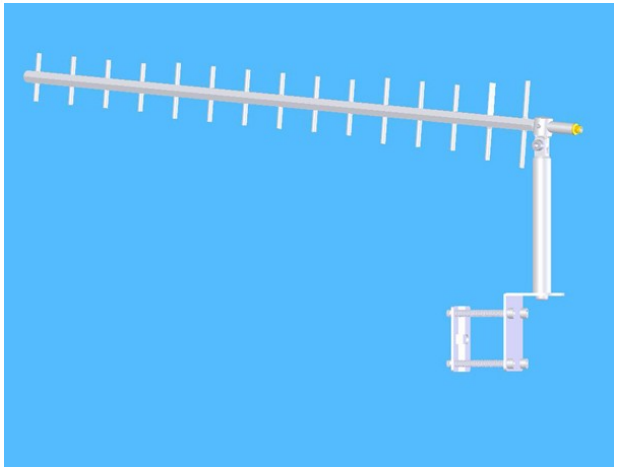
Line of sight – clear weather

Antennas



Antenna parameter definitions are based on the geometry of the antenna gain pattern.

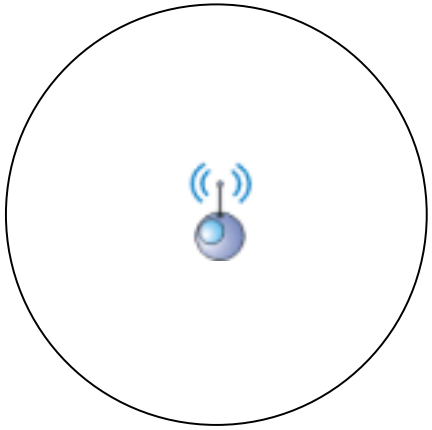




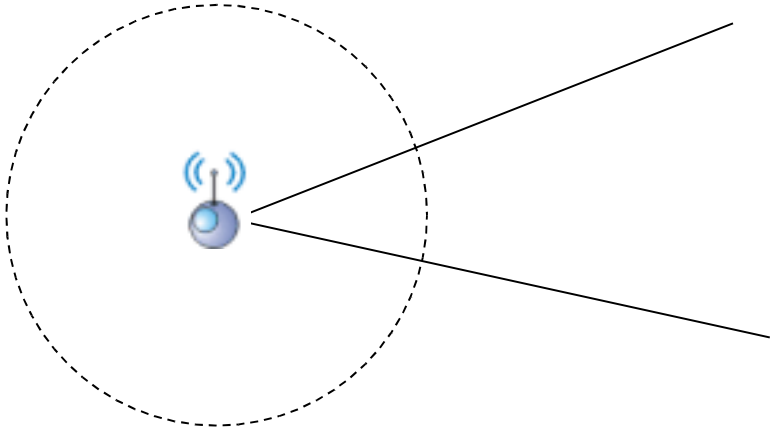
yagi

Directionality vs Gain

omnidirectional



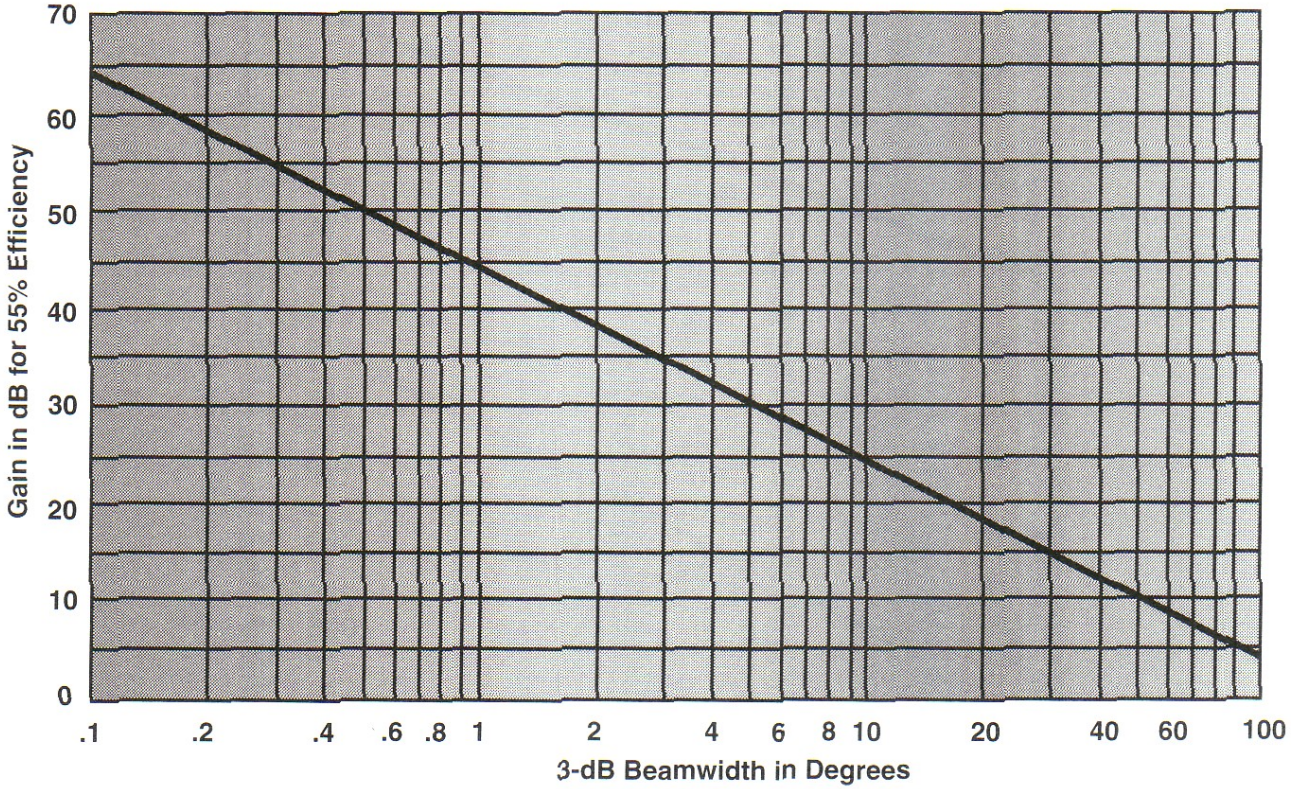
directional antennas



Gain: 2dB

Gain: 10-55dB

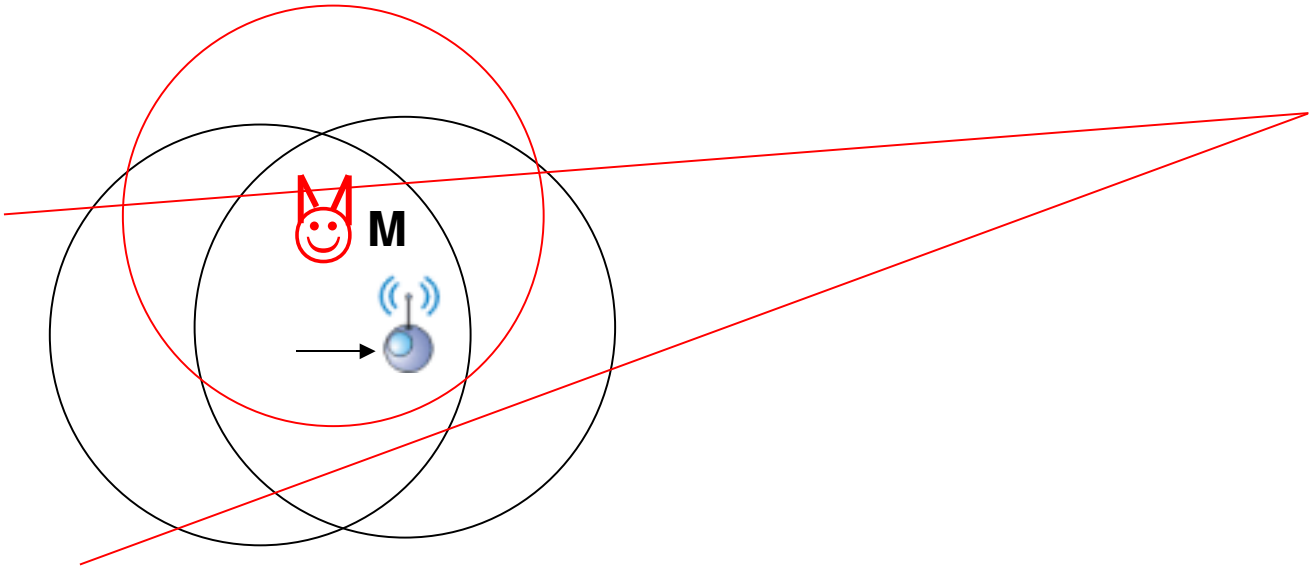
Gain versus Beamwidth



There is a well-defined tradeoff of gain versus beamwidth for any type of antenna. This chart shows the gain versus beamwidth for a parabolic antenna with 55% efficiency.

Implications of antenna gain on security

- Attackers can eavesdrop communication from much longer distances than anticipated
  - Attacks on Bluetooth (designed for 10m range) Reported eavesdropping from 3 km (LOS) !!!



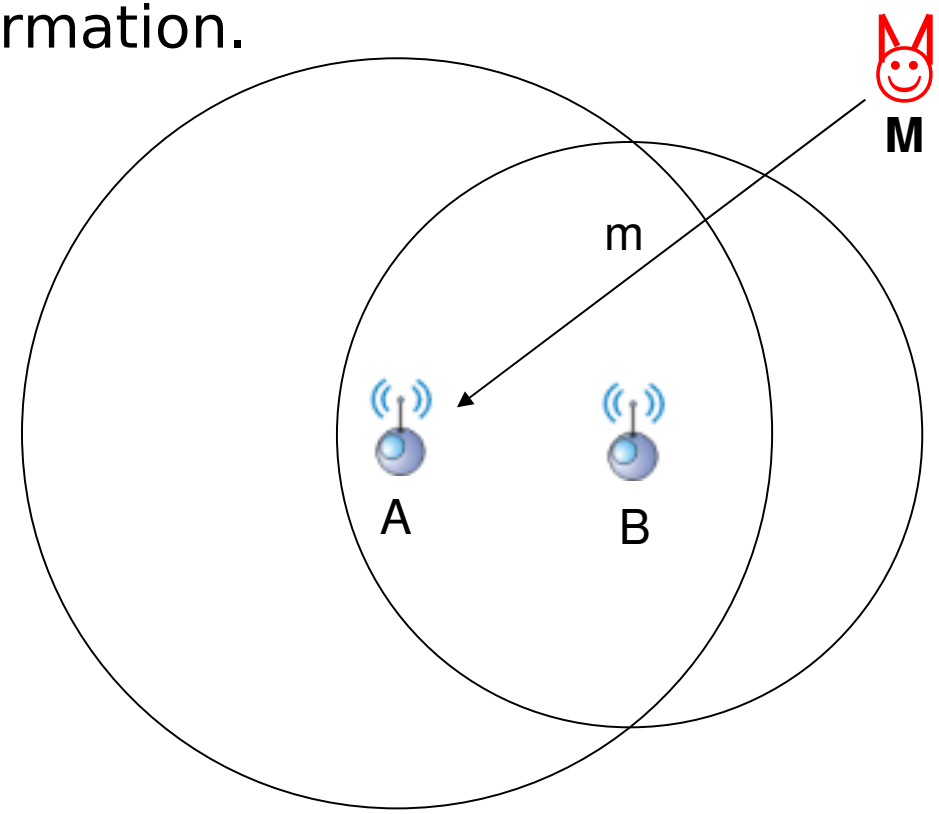
Exercise

- Directional antenna for 802.11b
- Design, build and test

- Some references:
  - http://www.oreillynet.com/cs/weblog/view/wlg/448
  - http://www.netscum.com/~clapp/wireless.html

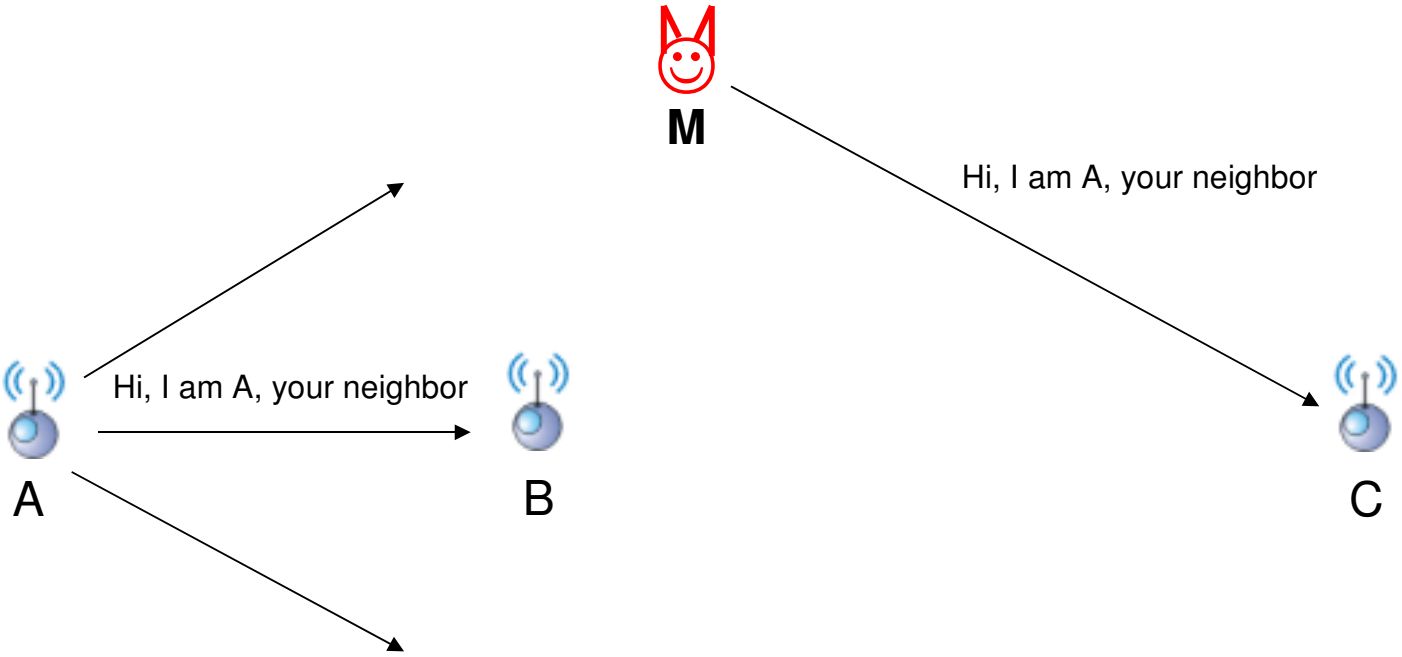
Eavesdropping and message insertion

- Straightforward
- Precondition:
  - The attacker knows the frequency/modulation/coding on/by which the communicating parties exchange their information.



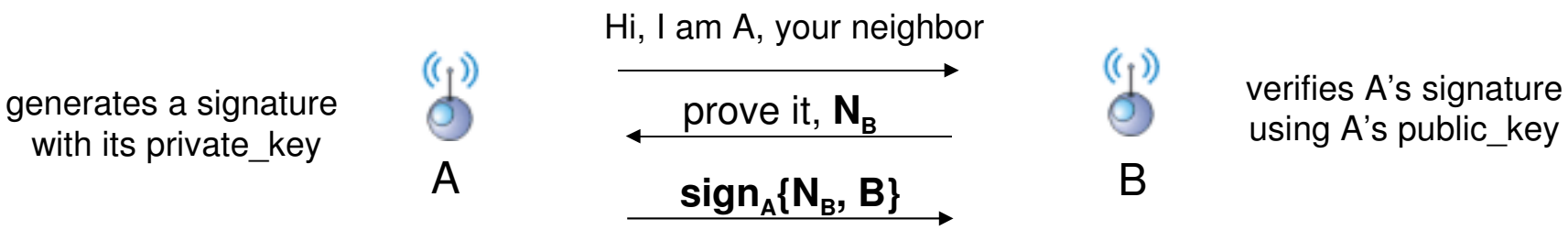
Message replay (1)

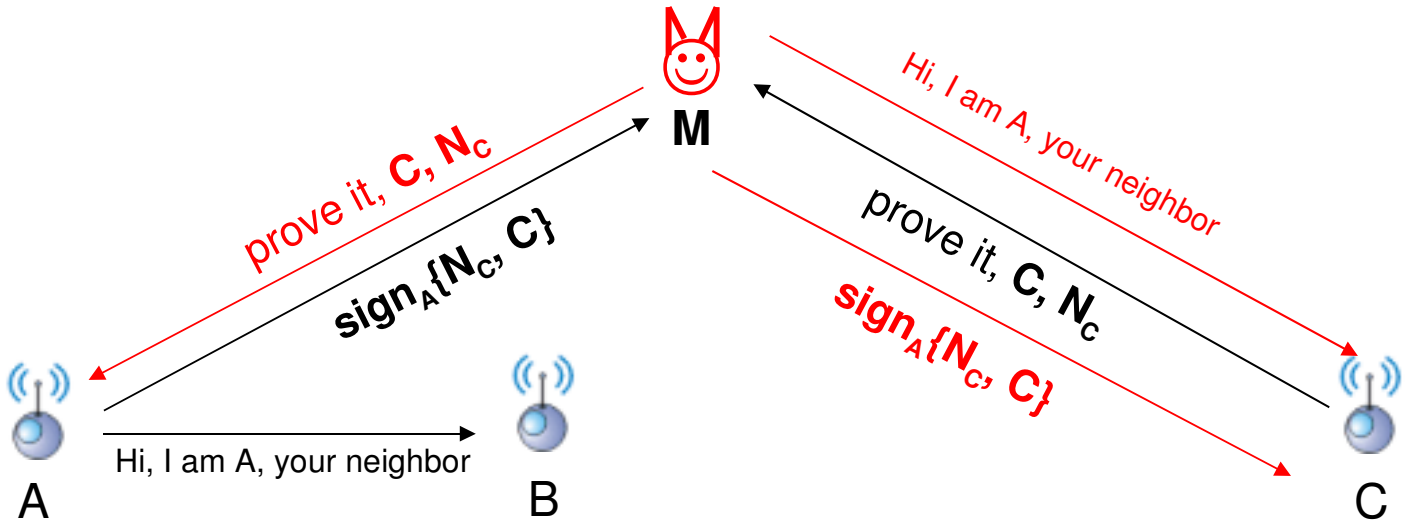
- Replay = message eavesdropping + insertion
- Example: straightforward attack on neighborhood discovery protocols (wormhole)



Message replay (2)

- Does authentication help?





Authentication does not help!

Receiver sensitivity

- The smallest signal (the lowest signal strength) that a receiver can receive and still provide the proper specified output.

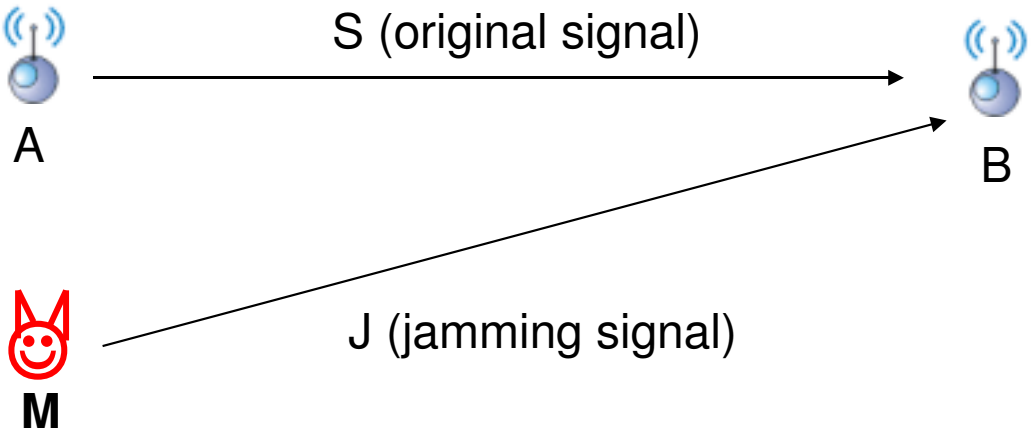
Transmitter Power (1W) = +30 dBm
Transmitting Antenna Gain = +10 dB
Spreading Loss = 100 dB
Atmospheric Loss = 2 dB
Receiving Antenna Gain = +3 dB

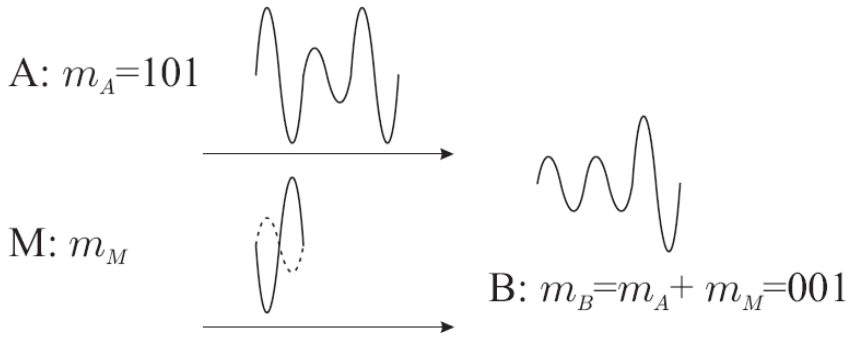
$$\text{Received Power} = +30\ \text{dBm} + 10\ \text{dB} - 100\ \text{dB} - 2\ \text{dB} + 3\ \text{dB}$$
$$= -59\ \text{dBm}$$

e.g., if the receiver sensitivity is -65dBm, the receiver will receive the signal as there is still 6dBm of margin on the link

Adversarial interference: jamming (1)

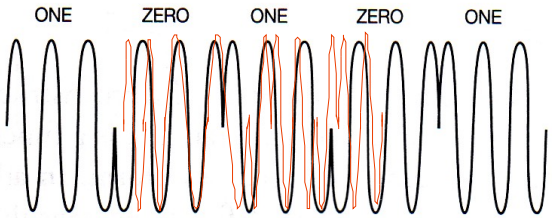
- Transmitting a signals on the same frequency on which the honest parties communicate
- Blocks the reception of the message at the receiver B



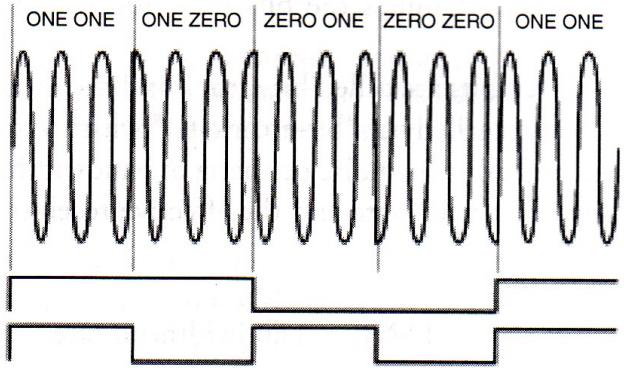


Simple amplitude modulation example

Jamming (2)



In a binary phase shift keyed (BPSK) signal, the FR waveform has one phase to carry 1 and a 180° different phase to carry 0.



In a quadrature phase shift keyed (QPSK) signal, the FR waveform can have four phases. Each phase represents 2 bits of digital data.

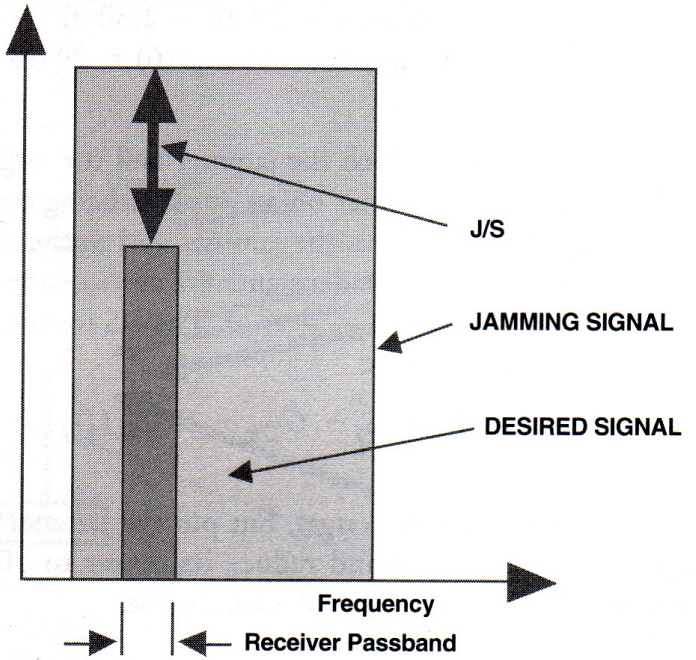
Jamming (3)

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

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

- Jaming to signal ratio: J/S = J – S
- For effective jamming: J/S = 0 to 40 dB (typically 10dB)

P – transmitted power
$G_{T/R}$ – t/r antenna gain
F – tx frequency
D - distance

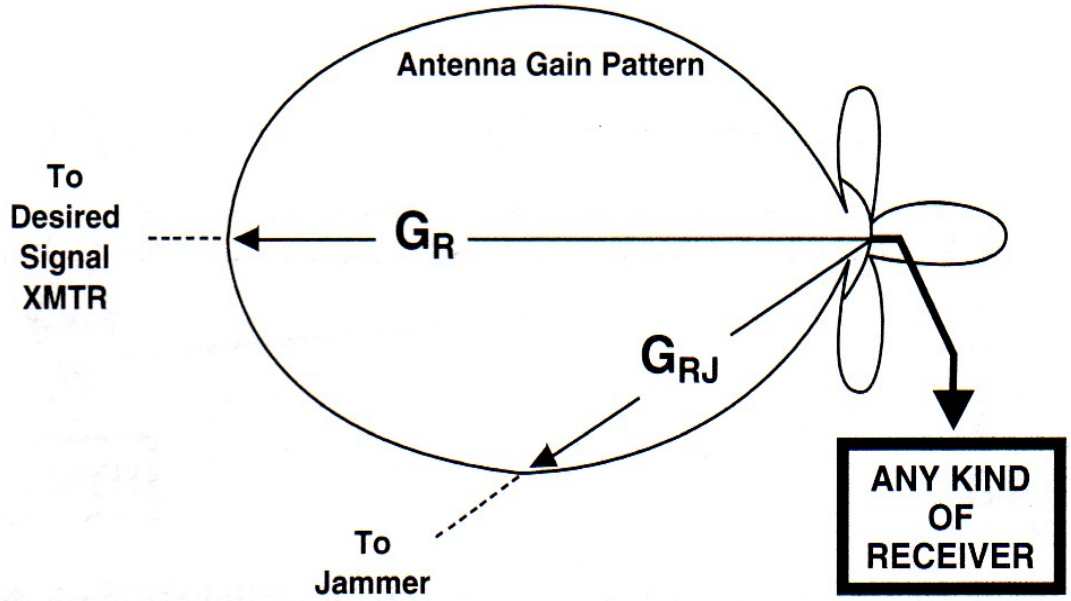


The jamming-to-signal ratio is simply the ratio of the power of the two received signals within the frequency passband of the receiver.

Example:
- jammer uses 100W (50dBm), a. gain 10dB, distance 30km
- transmitter uses 1W (30dBm), a. gain 3dB, distance 10km

J/S = 17dB => probably successful jamming

The importance of jammer's location



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.

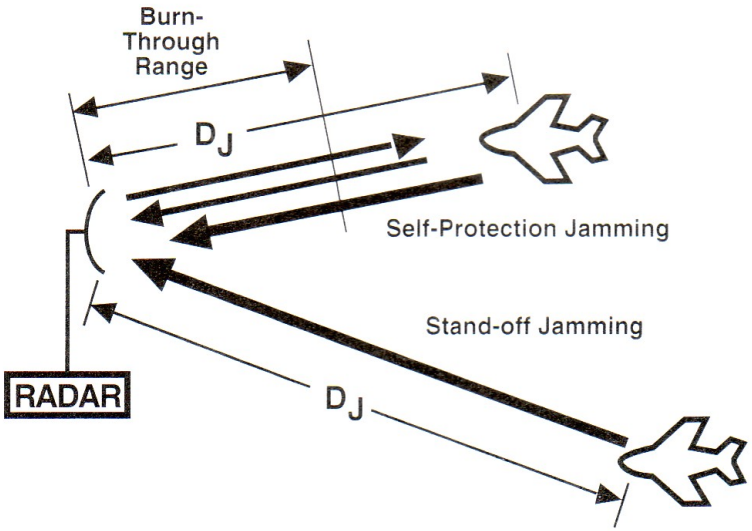
Parameters influencing J/S

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

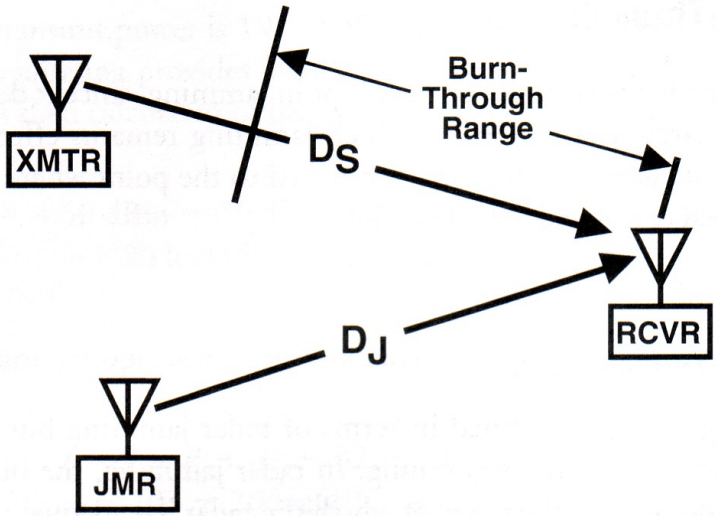
Parameter (Increasing)	Effect on J/S	Type of Jamming
Jammer transmit power	Directly increases on J/S dB for dB	All
Jammer antenna gain	Directly increases J/S dB for dB	All
Signal frequency	None	All
Jammer-to-receiver distance	Decreases J/S as the distance^2	All
Signal transmit power	Directly decreases 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

Burn through range

- The range from which the sender succeeds in communicating with the receiver, despite jamming



The burn-through range is the range from the radar to its target at which the jammer can no longer prevent the radar from doing its job.



The equivalent of radar burn-through against communications jamming occurs when the range from the desired transmitter to the receiver is reduced to the point at which the signal is received with adequate quality.

Classification of jamming

Types of Jamming

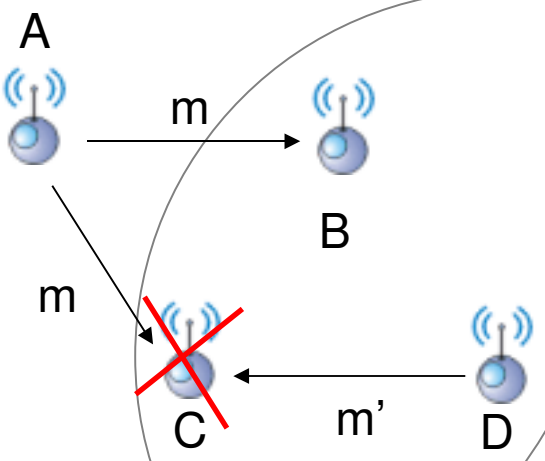
Type of Jamming	Purpose
Communications jamming	Interferes with enemy ability to pass information over a communications link
Radar jamming	Causes radar to fail to acquire target, to stop tracking target, or to output false information
Cover jamming	Reduces the quality of the desired signal so it cannot 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

Jamming on other layers

- Application
- Networking
- **MAC-layer**

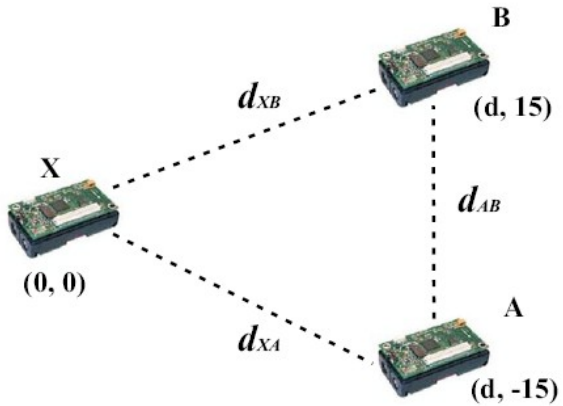
Medium Access Control

- Defines how nodes share the available TIME on the channel.
- Nodes use the same frequency/spreading codes to communicate (e.g., 802.11, 802.15.4, ...)
- MAC defines “fair” ways of accessing the available channel

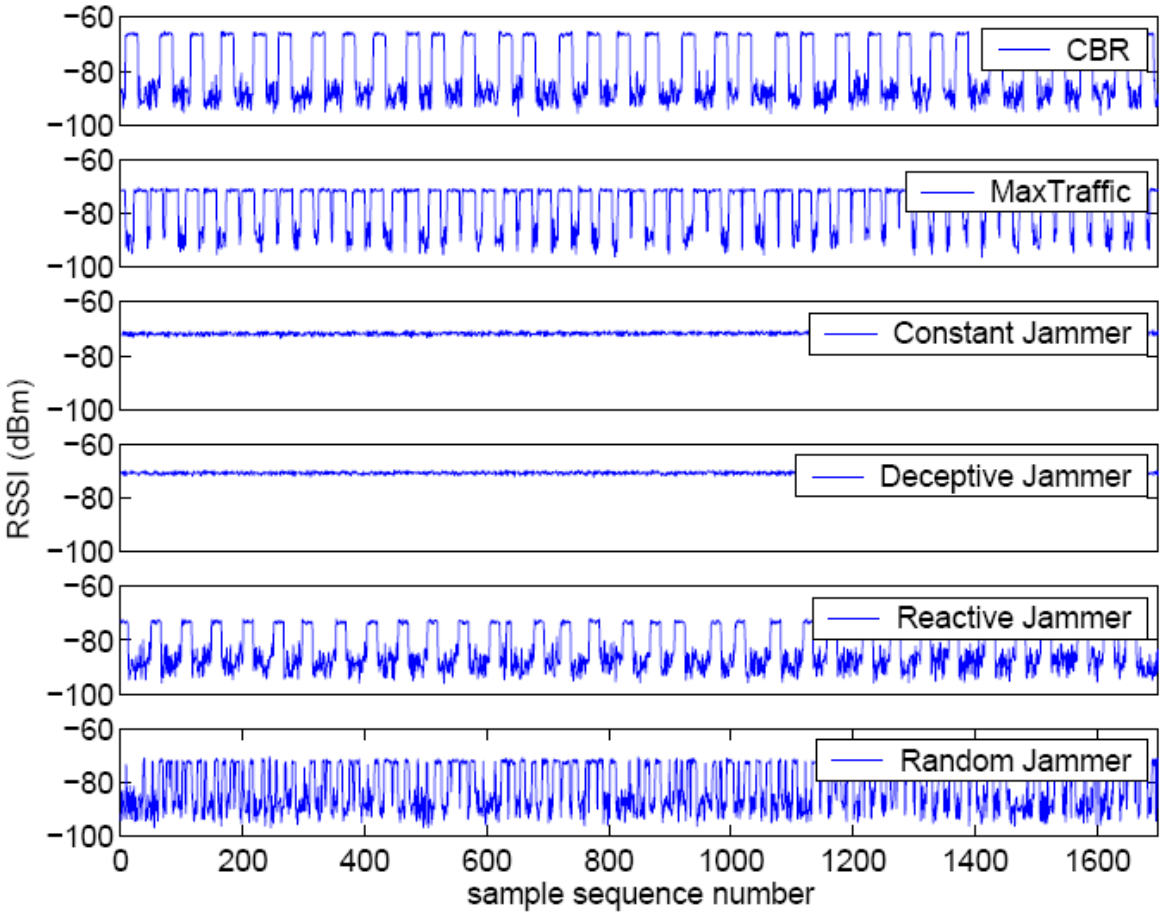


Basic idea: if D senses that the channel is busy, it will not transmit - it will wait until the channel is free !!!

Example: sensor network jamming



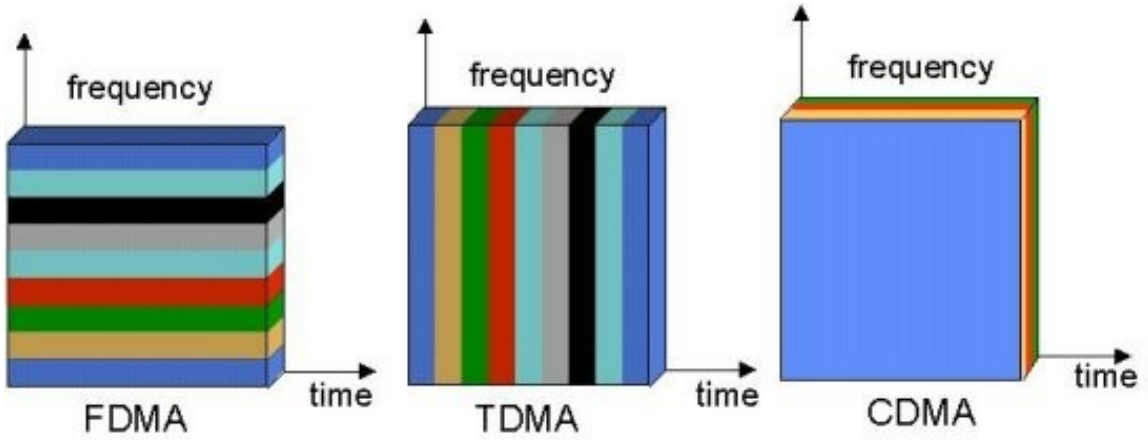
MAC-layer jamming

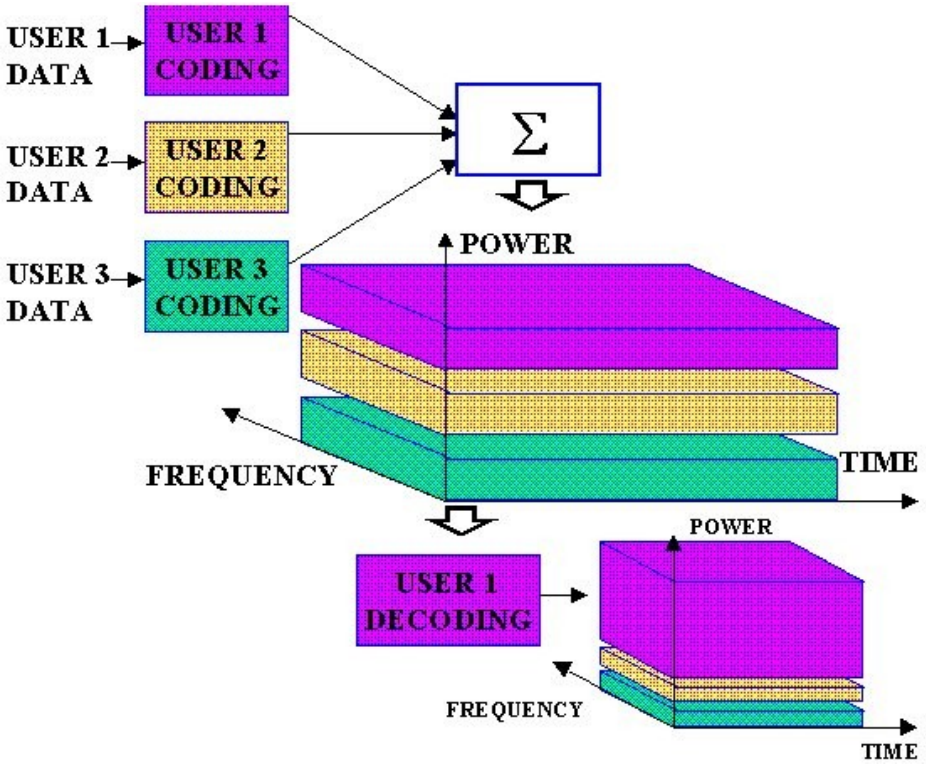


W. Xu, W. Trappe, Y. Zhang, and T. Wood,
"The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," Proceedings of Mobihoc 2005

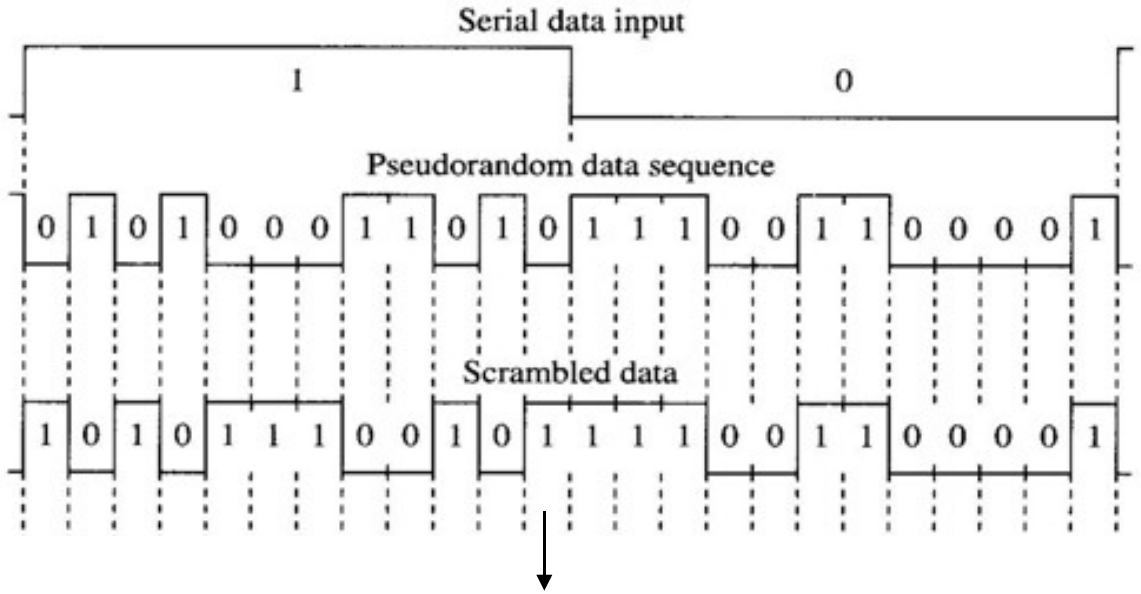
Anti-jamming communication

Background – access schemes





Direct Sequence Spread Spectrum

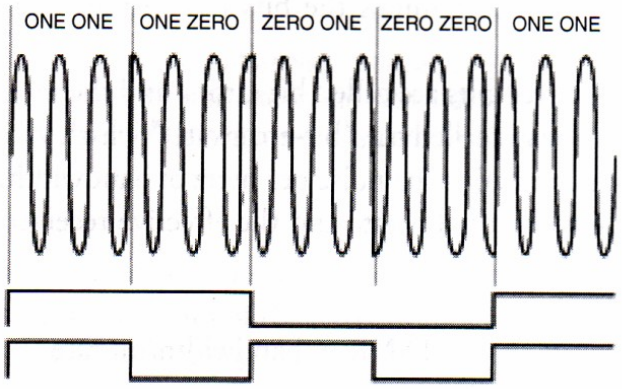


message

spreading code

spread message

modulation (QPSK)



message

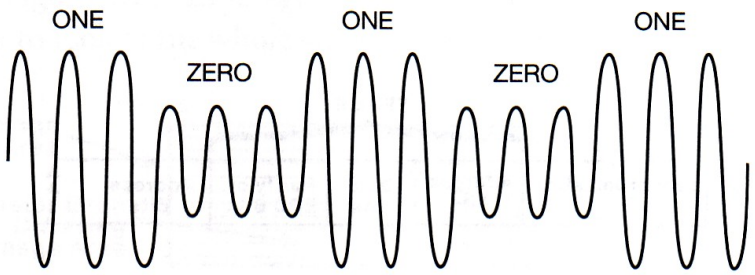
spreading code

used in 802.11, GPS ...

Messages / signals / modulation / spreading

- So far, we talked about signals in terms of signal power
- What about signal shape?
  - frequency (band)
  - amplitude
- Transformation from **message** -> **signal**
  - spreading
  - modulation

Message: **10101**, Modulation: **amplitude**, Frequency: **single frequency (carier)**

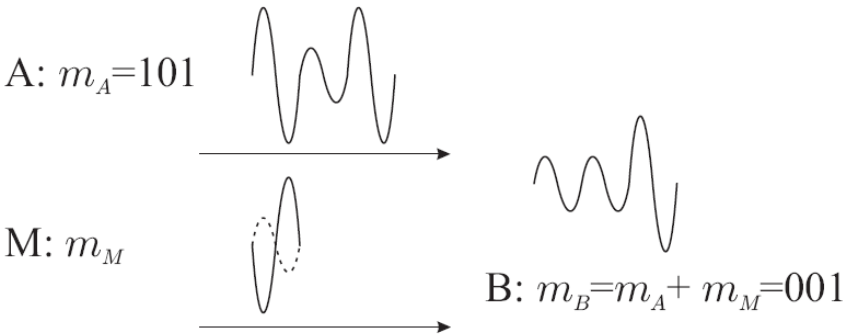


In an amplitude shift keyed (ASK) signal, the FR waveform is amplitude modulated to carry the digital modulation.

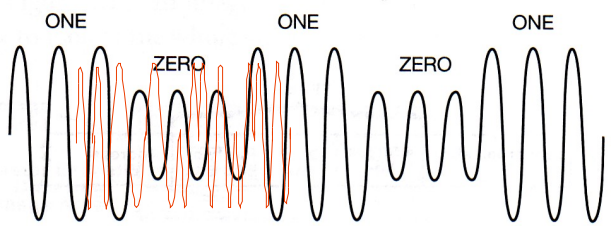
Example: ***AM*** - easy to DETECT, MODIFY and JAMM

- Detection: easy (single frequency)
- Interception/Modification: easy (predictable signals, frequency)
- Jamming: easy (predictability, no robustness)

Modification

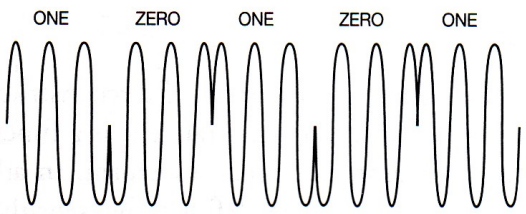


Jamming:

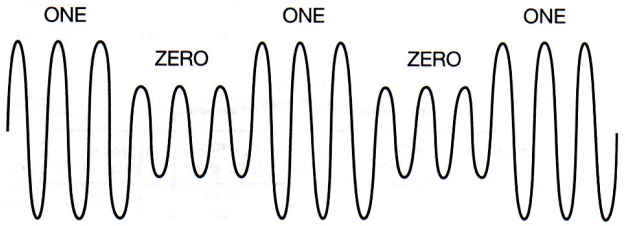


Signal Modulation

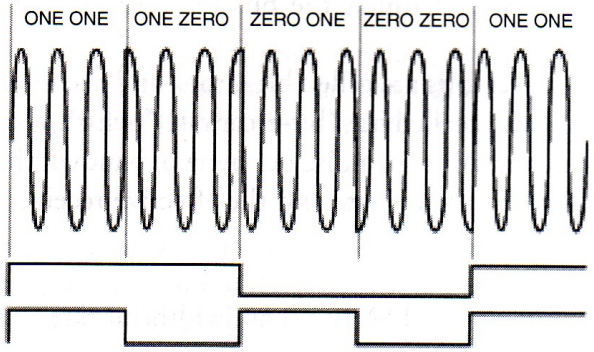
- AM
- FM
- (Q)PSK, ...



In a binary phase shift keyed (BPSK) signal, the FR waveform has one phase to carry 1 and a 180° different phase to carry 0.



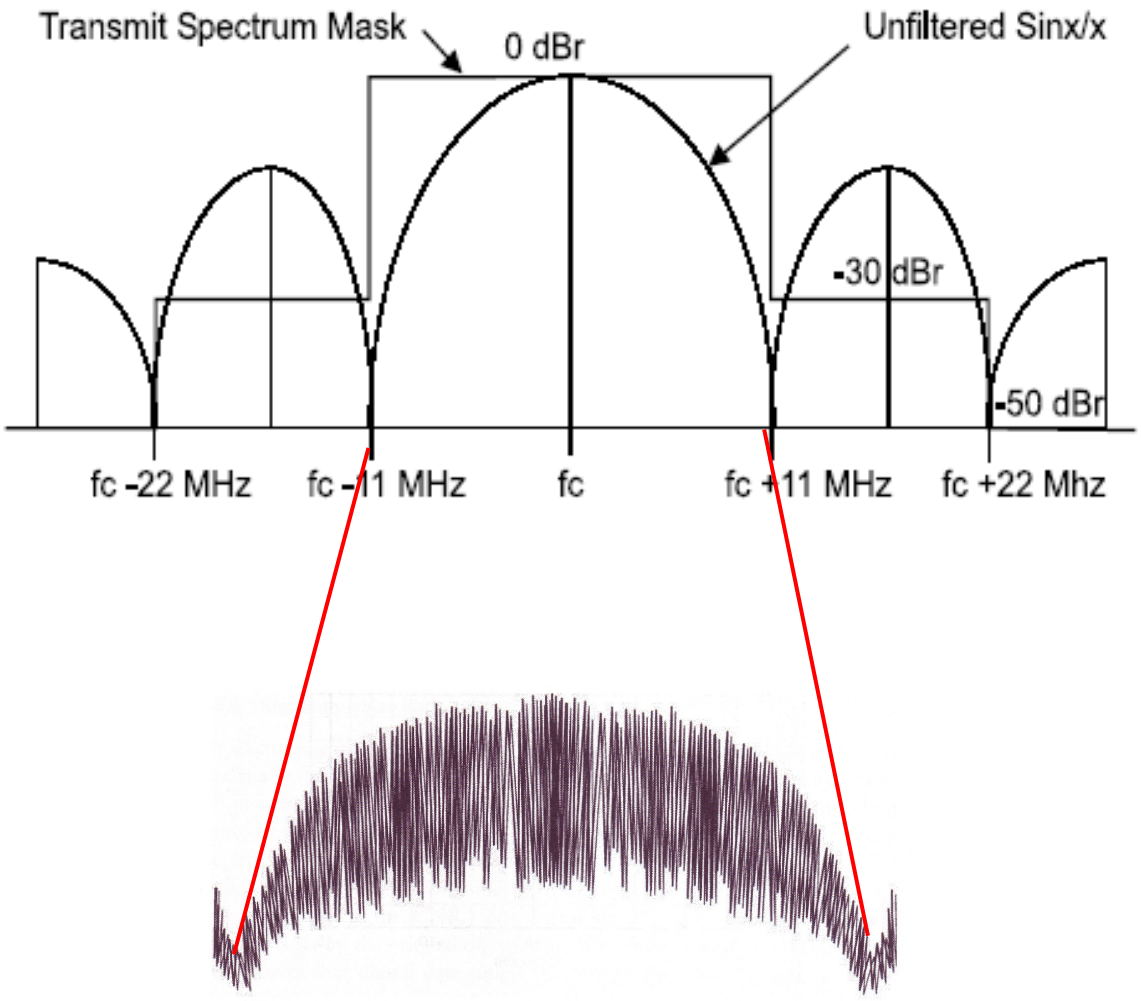
In an amplitude shift keyed (ASK) signal, the FR waveform is amplitude modulated to carry the digital modulation.



In a quadrature phase shift keyed (QPSK) signal, the FR waveform can have four phases. Each phase represents 2 bits of digital data.

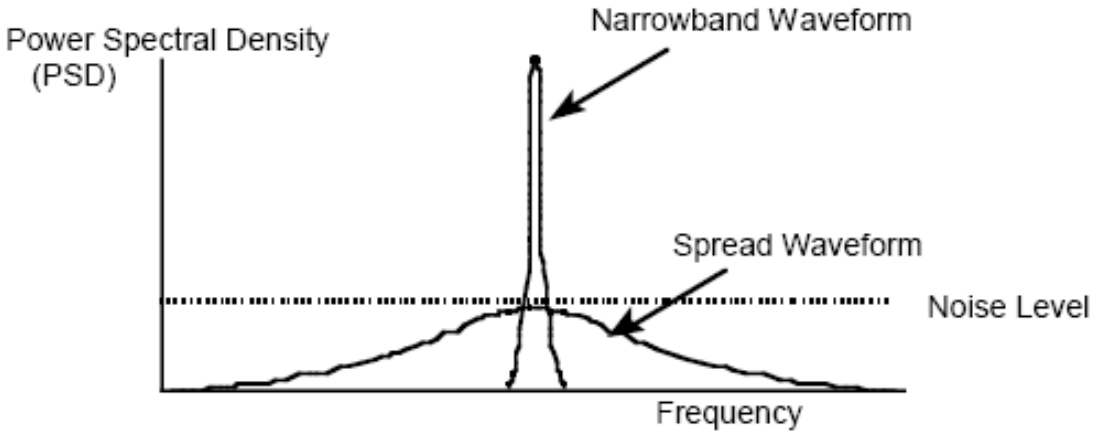
These two modulations result in a wider spectrum being used
(not only signals on the carrier frequency are being transmitted => see the transitions between bits!)

Spectrum of a DSSS signal (QPSK)

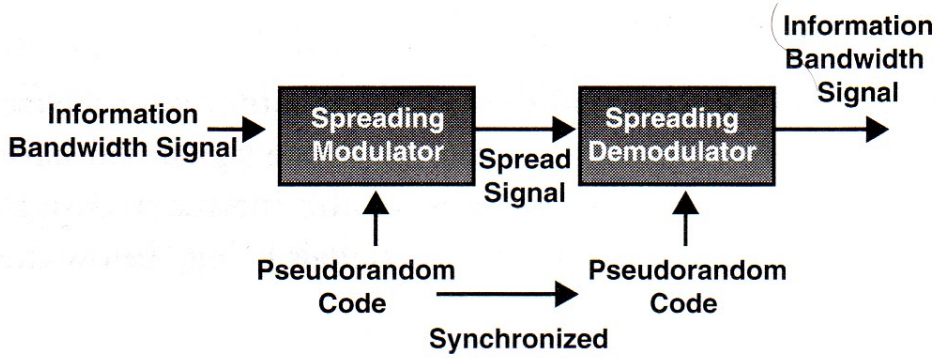


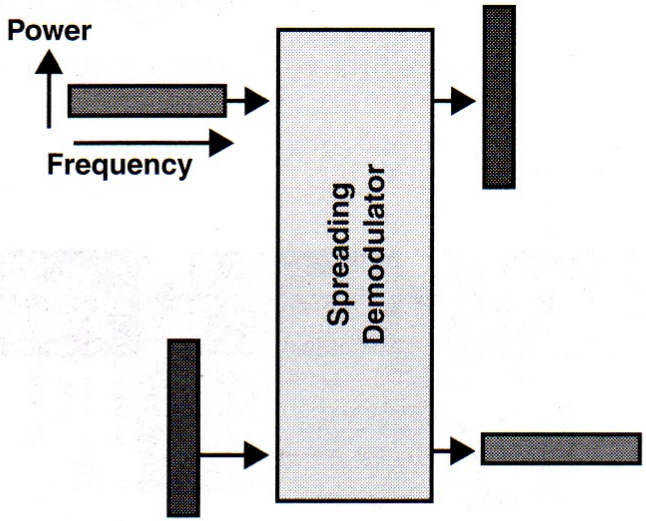
DSSS – (more) difficult to DETECT, MODIFY and JAMM

- Secret spreading code – DSSS **HIDES** THE SIGNAL
- Signal detection is now more difficult
  - signal “hidden” in the noise
  - can be done through energy detection (requires strong signal) or signal characteristic (constant chip rate) (Dillard&Dillard, Detectability of Spread Spectrum Signals, 1989)
- Signal interception/modification difficult - LPI
- Jamming
  - narrowband jamming now requires much higher power
  - broadband jamming still effective



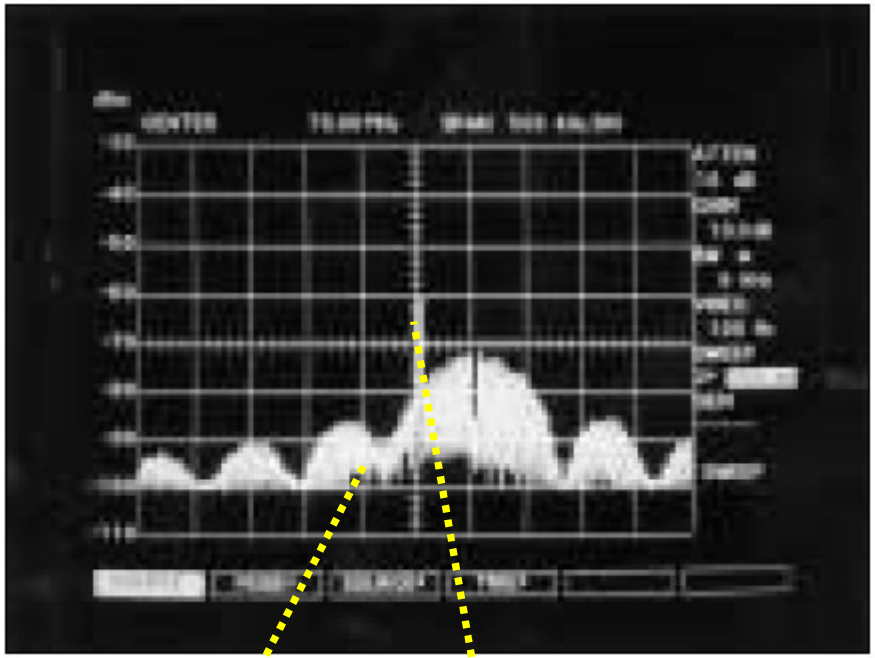
DSSS – antijamming advantage (1)



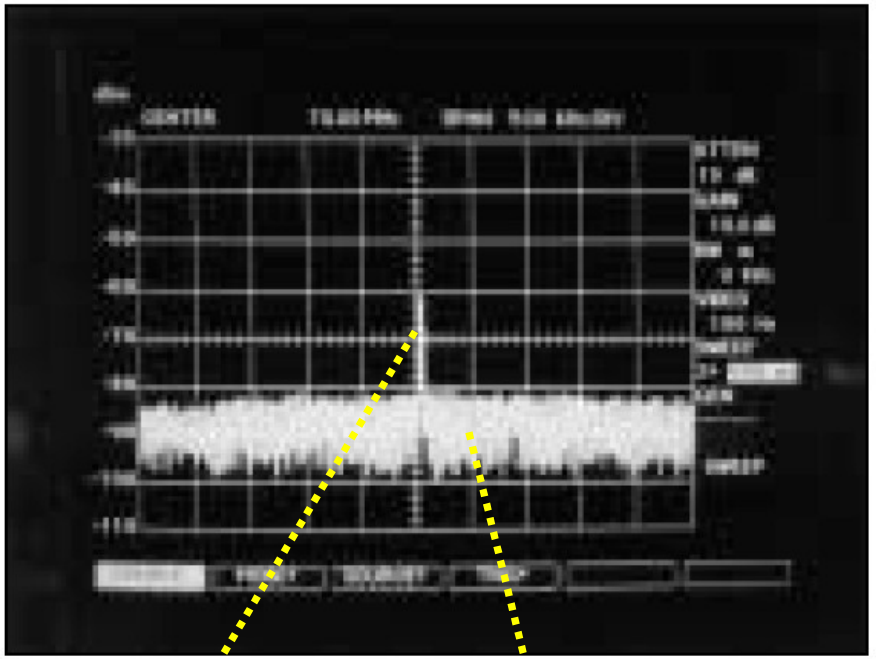


The same process that collapses the frequency spectrum of the spread-spectrum signal back to its information bandwidth spreads any nonsynchronized signal by the same factor.

DSSS – antijamming advantage (2)



Spread signal (BPSK) and (narrowband) interference on the channel



Despread signal and spread interference (at the receiver)

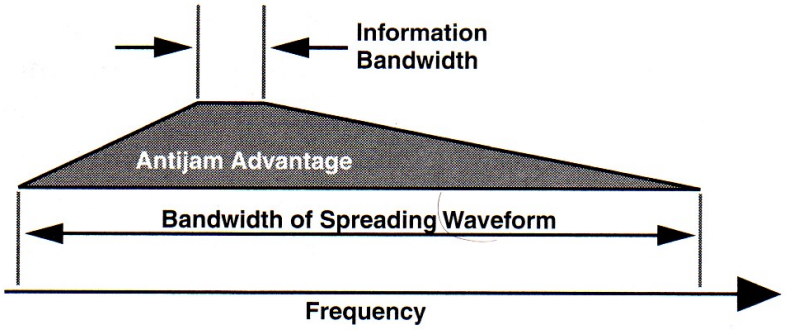
Jamming spread spectrum signals

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

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

- Jaming to signal ratio: J/S = J – S
- For effective jamming: J/S = 0 to 40 dB (typically 10dB)

P – transmitted power
$G_{T/R}$ – t/r antenna gain
F – tx frequency
D - distance



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

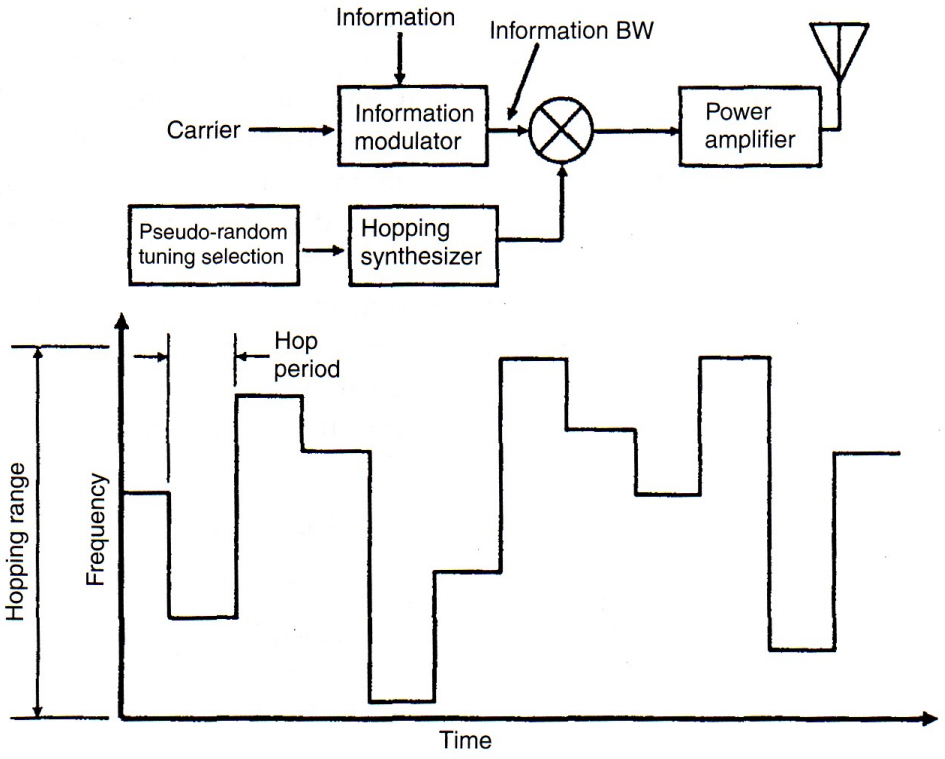
M_J = the jamming margin (in decibels);
G_P = the processing gain (in decibels);
L_{SYS} = the system losses (in decibels);
SNR_{OUT} = the required output SNR.

Example:
- jammer uses 100W (50dBm), a. gain 10dB, distance 30km
- transmitter uses 1W (30dBm), a. gain 3dB, distance 10km

J/S = 17dB => probably successful jamming

FHSS – Frequency Hopping Spread Spectrum

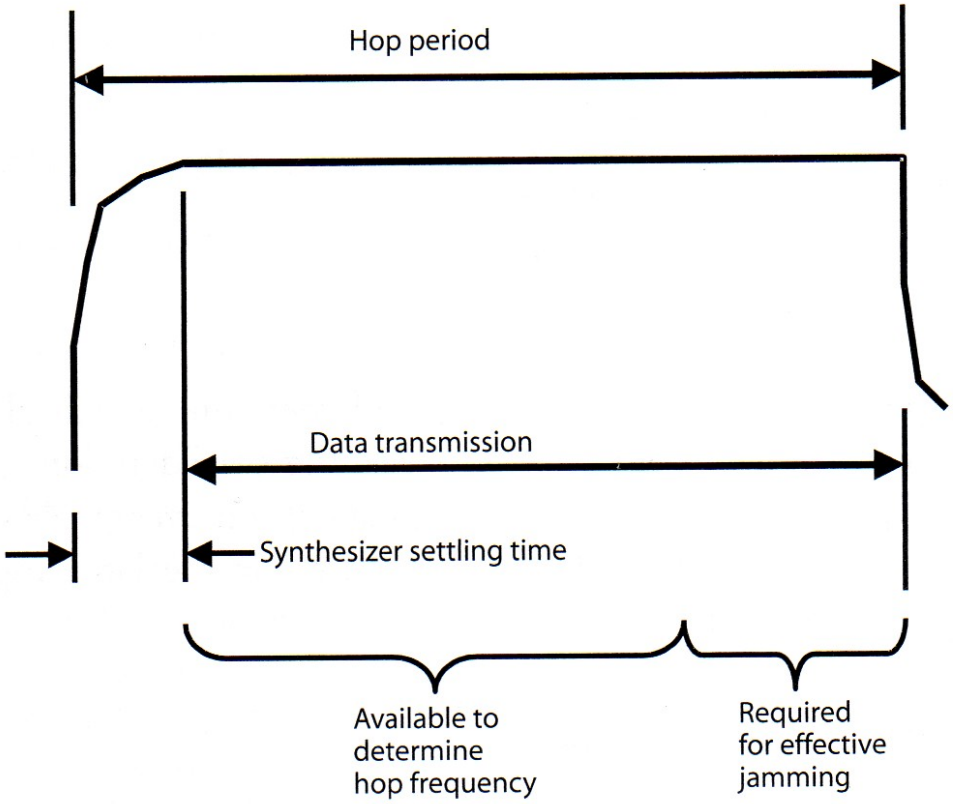
- Synchronized sender and receiver
- Share a key – from the key a sequence of frequencies is derived



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

used in Bluetooth, ...

Jamming FHSS signals: follower jammer



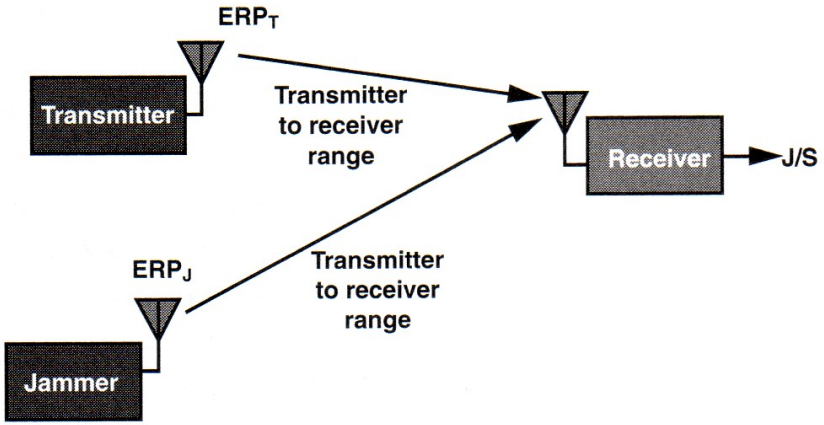
Bluetooth:
79 channels, 1MHz each
1000 hops/second

Jaguar V system:
2320 channels

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

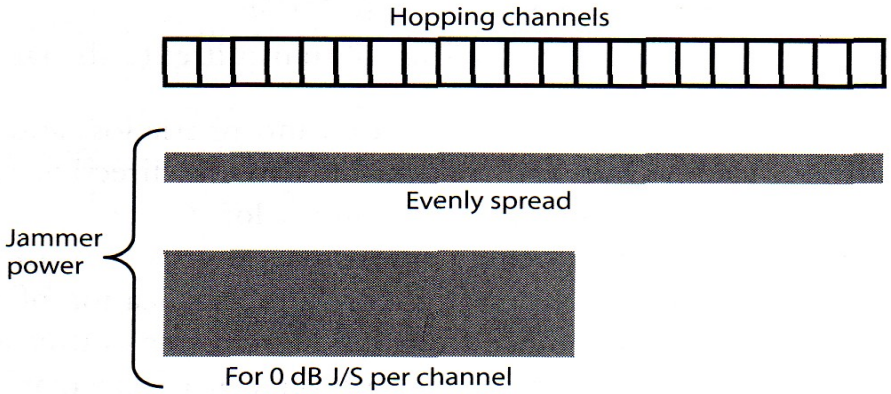
(1) detect the frequency (2) jamm

Jamming FHSS signals: partial band jammer



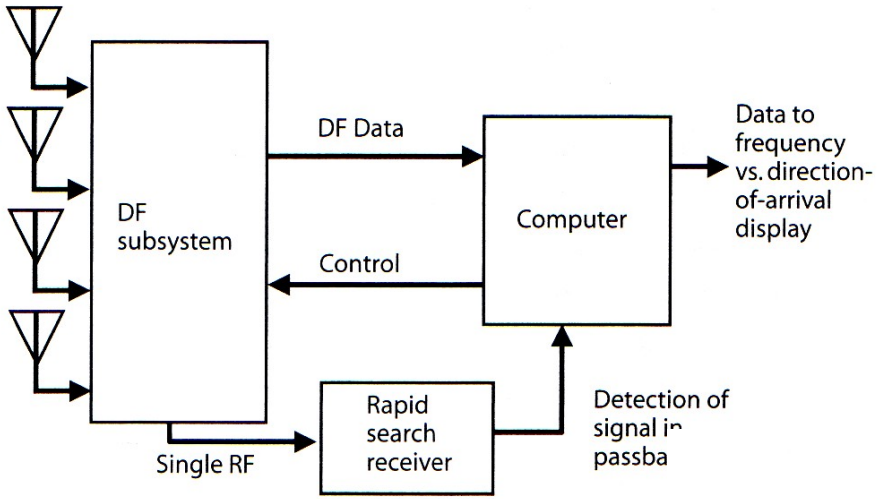
Partial-band jamming optimizes the available jamming power by causing the jamming power per channel to equal the received-signal strength from the transmitter over as many channels as possible.

e.g. J/S=0dB provides sufficient bit error rate



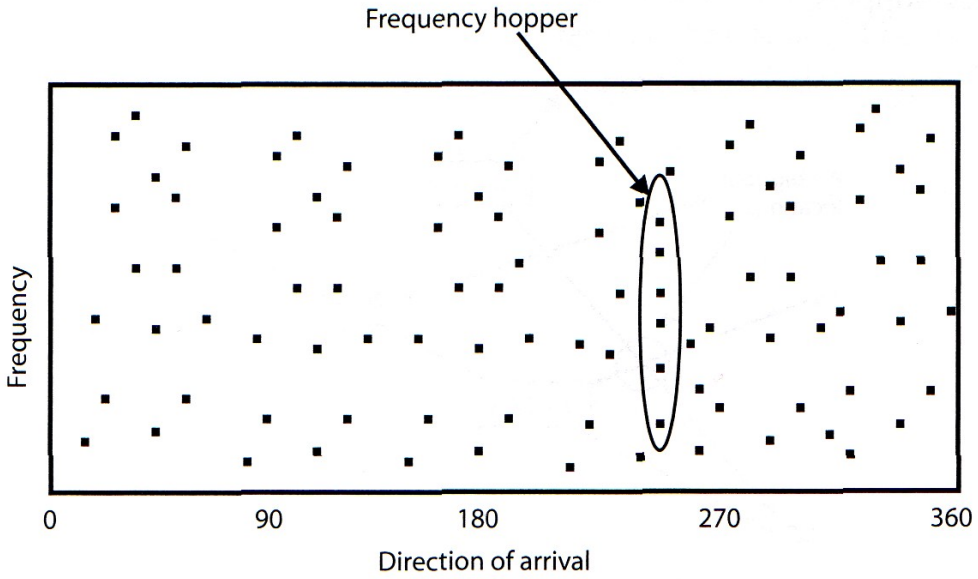
A partial-band jammer distributes its available power to achieve 0 dB J/S in each jammed channel at the jammed receiver.

Finding FHSS transmitters



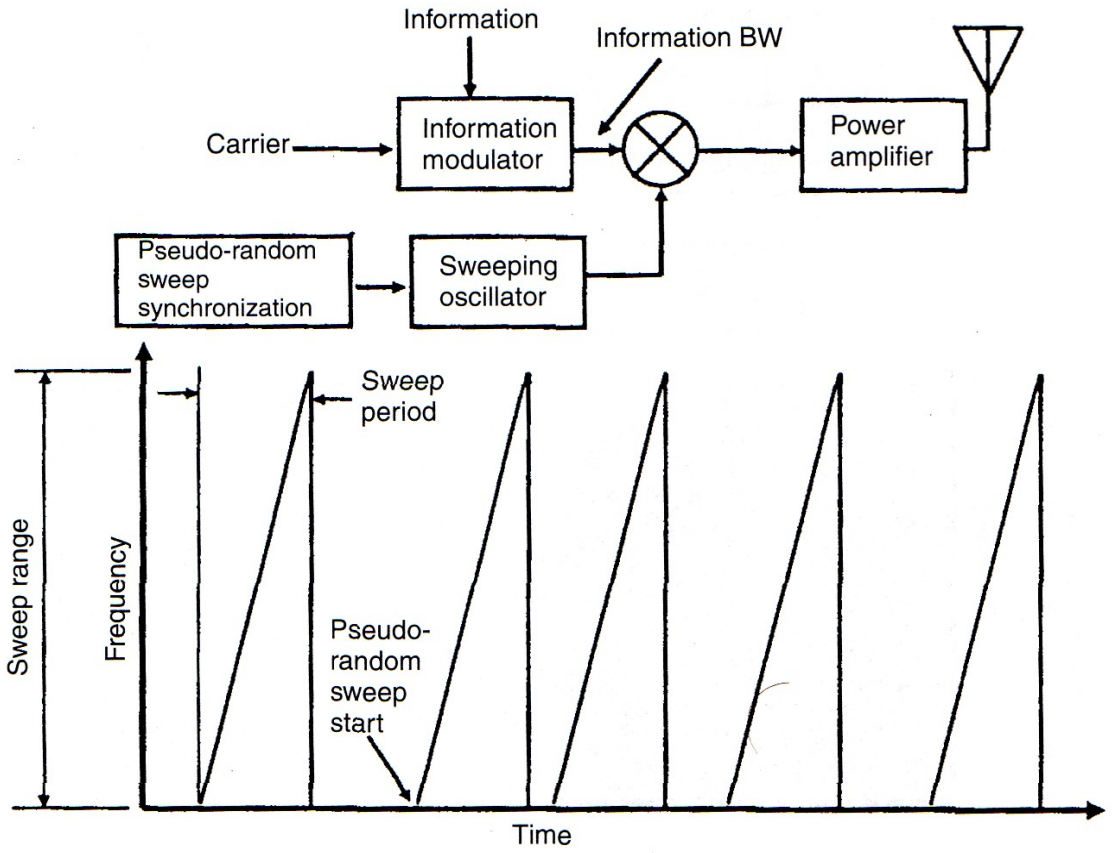
A sweeping DF system for frequency hoppers incl
to detect occupied channels. Then the search is st

Detection of signal direction ...



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

Chirp Signals



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

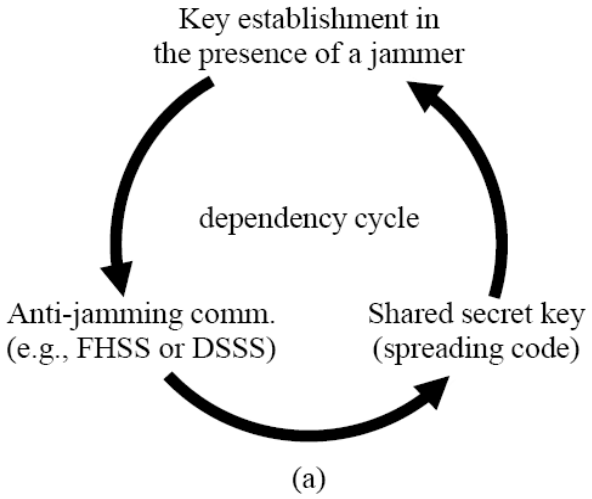
Jamming Chirp Signals

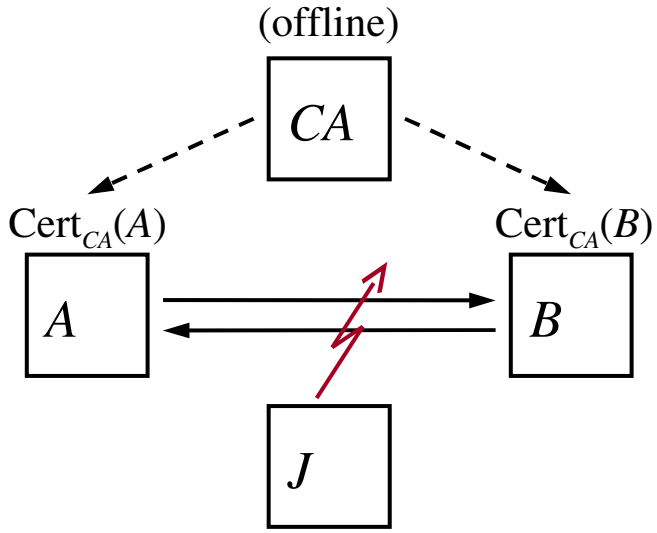
- Narrow-band is not good
- Follower jammer is the best technique
- Partial jamming can be used ...

Anti-jamming communication without shared keys

Problem

- Jamming in Wireless networks pushes us back to pre-PK era.





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

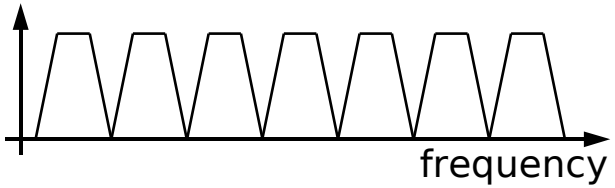
Motivation

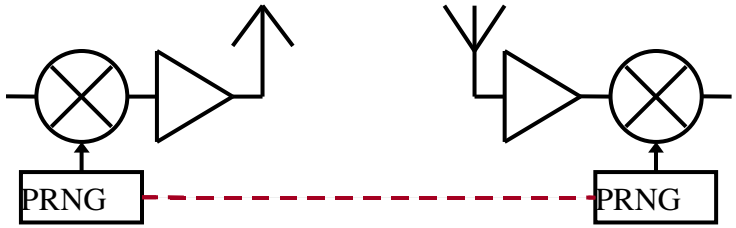
Central question: How can two devices that do not share any secrets establish a shared secret key over a wireless radio channel in the presence of a communication jammer?

- Pre-loading the keys suffers from well-known distribution and revocation problems
- Key establishment protocols using public key cryptography solve most of these problems, but assume a jamming-resilient communication
- **Devices need to communicate to establish shared keys**

Anti-jamming Techniques

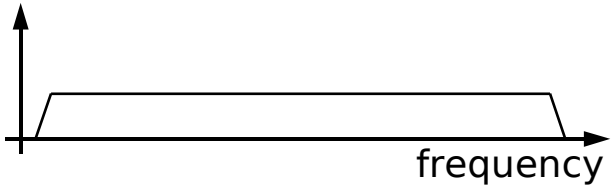
- FHSS: Frequency Hopping Spread Spectrum

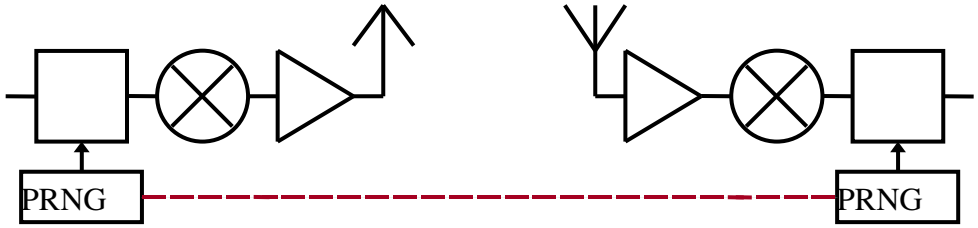




Hopping sequence (PRNG seed) must be known to the sender and receiver but not the jammer

- DSSS: Direct Sequence Spread Spectrum



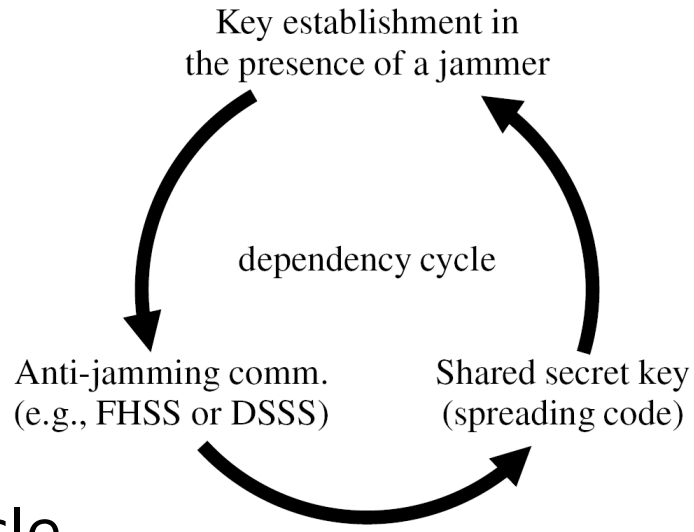


Spreading code (PRNG seed) must be known to the sender and receiver but not the jammer

- **Common anti-jamming techniques rely on pre-shared secret codes (keys)**

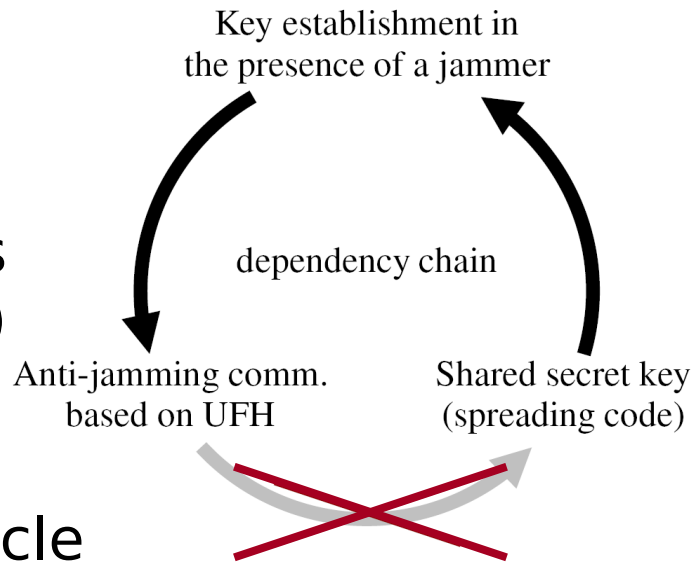
Anti-jamming / Key-establishment dependency

- 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

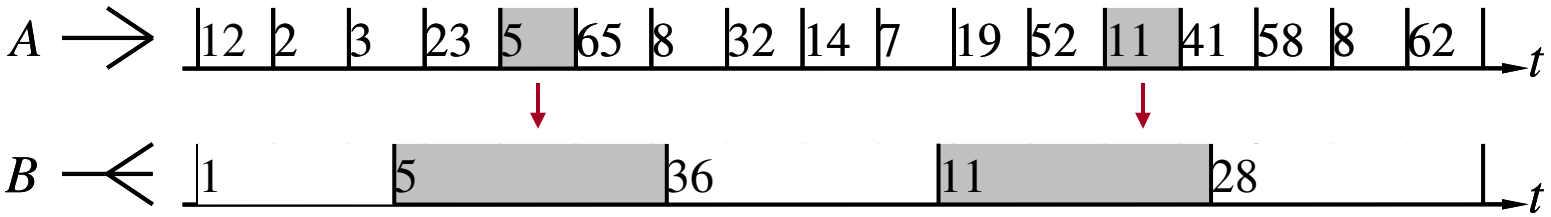


Anti-jamming / Key-establishment dependency

- 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

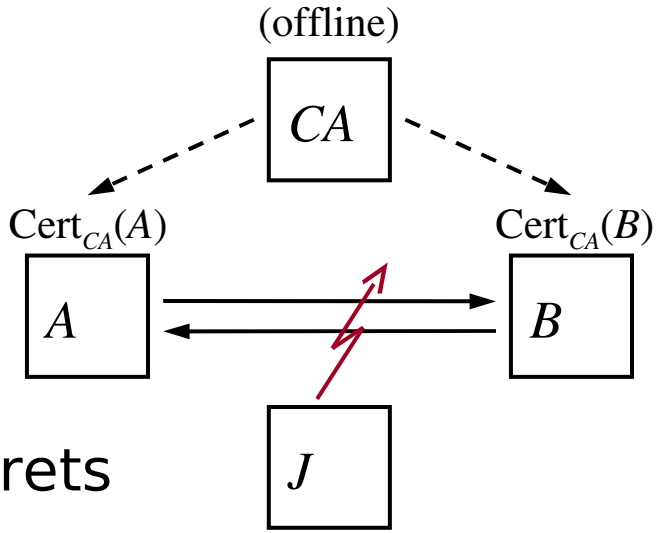


- Key idea: break the dependency cycle by using **Uncoordinated Frequency Hopping** (UFH)



System Model

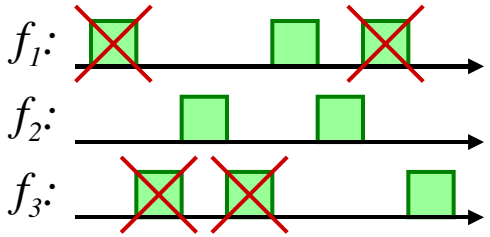
- **Problem:**
  A and B want to establish a shared secret key in the presence of a jammer J



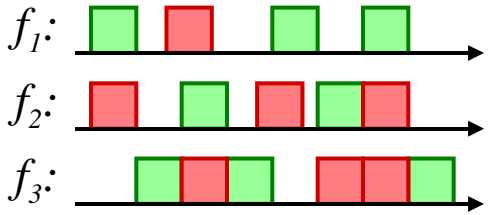
- **Assumptions:**
  - A and B do not share any secrets
  - The clocks of A and B are loosely synchronized O(s)
  - Each node has a public/private key pair and a certificate binding its identity to the public key
  - CA is trusted by all nodes and may be off-line or unreachable by the nodes at the time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

Attacker Model

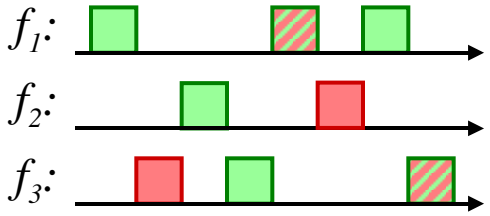
- The attacker J can choose among the following actions:
  - **Jam** existing **messages** by transmitting signals that cause the original signal to become unreadable by the receiver.



  - **Insert** own **messages** that she generated by using known (cryptographic) functions and keys as well as by reusing (parts of) previously overheard messages.

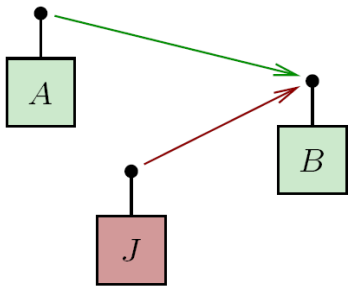


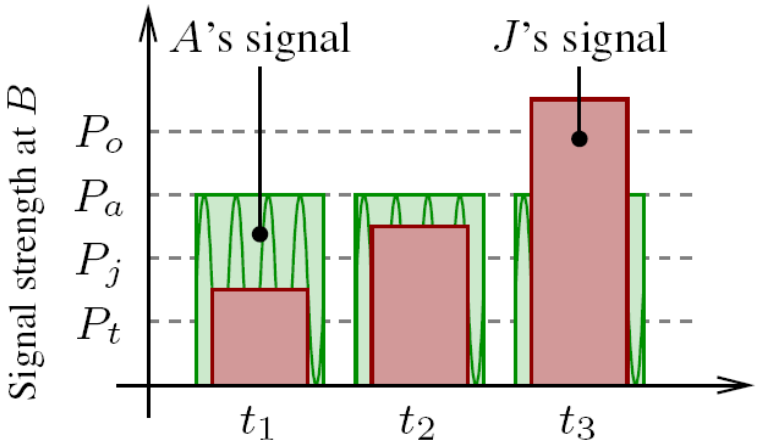
  - **Modify** existing **messages** by e.g., flipping single message bits or by entirely overshadowing (i.e., replacing) original messages.



Attacker Model

- P_t, P_j, and P_o: required signal strength *at the receiver* B to insert, jam, or overshadow a message





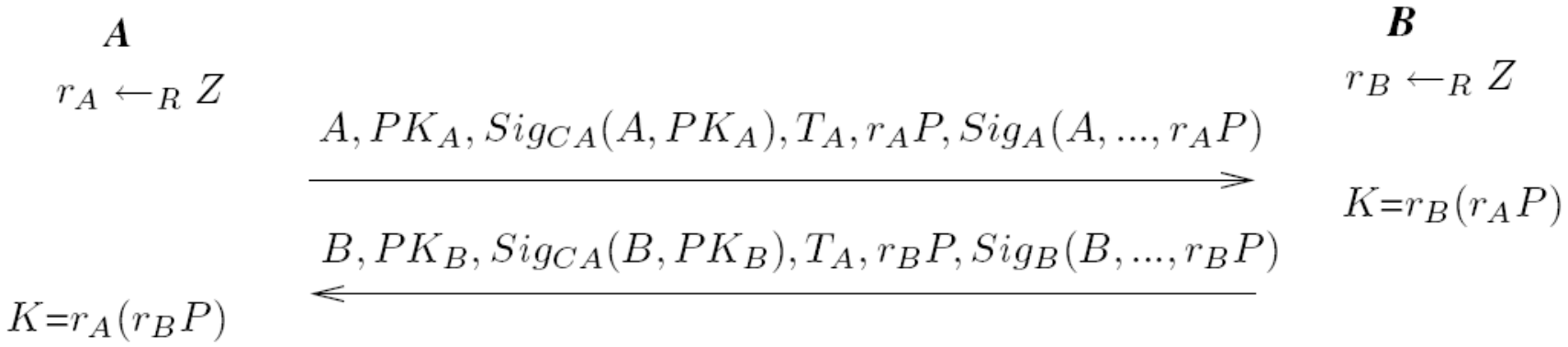
- P_T: total signal strength that attacker J can achieve *at the receiver* B

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

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

Key Establishment Protocol: Sender/Receiver

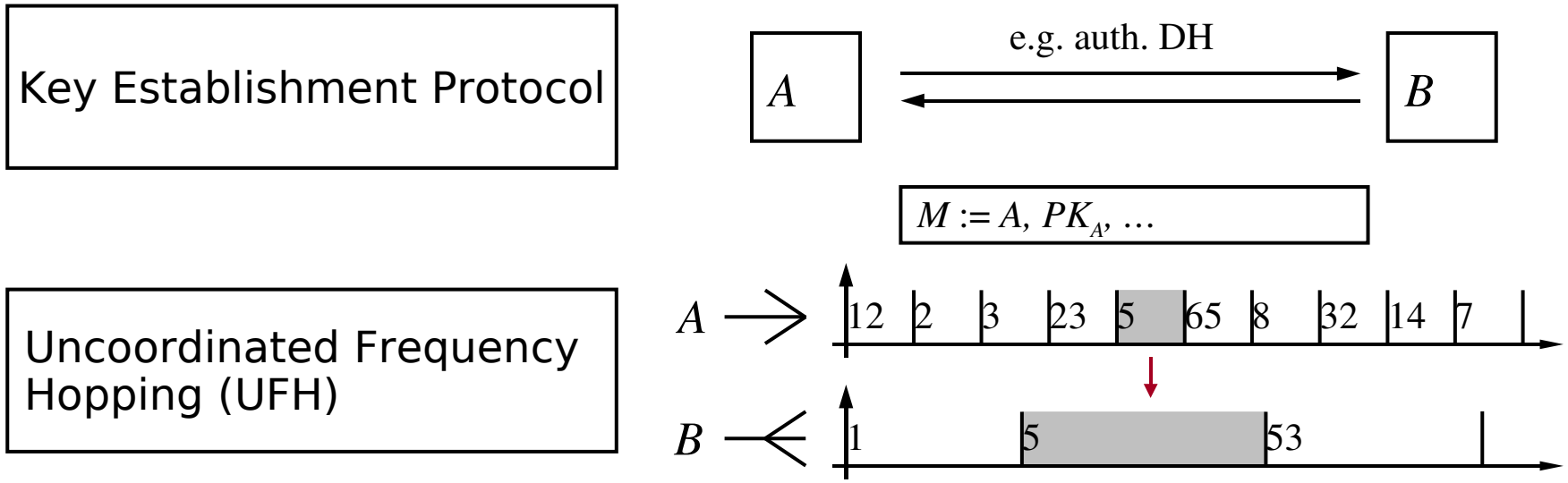
- ECC-based Station-to-Station Diffie-Hellman



- Sender A repeats sending his message until receiving a valid response from receiver B
- Timestamp T and a message history buffer are used to identify already received messages

Jamming-resistant Key Establishment: Solution Overview

- Key idea: break the dependency cycle by using Uncoordinated Frequency Hopping

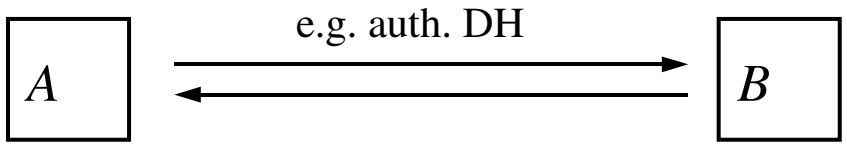


- **Problem:** messages of the key establishment protocol do not fit into a single frequency hop duration (~1000 bits vs. ~100 bits)
- ⇒need for message fragmentation and reassembly

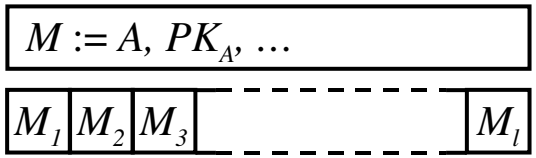
Jamming-resistant Key Establishment: Solution Overview

- Key idea: break the dependency cycle by using Uncoordinated Frequency Hopping

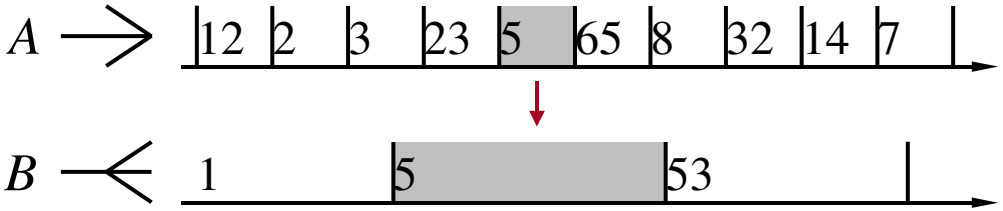
Key Establishment Protocol



Integrity-preserving Message Transfer Protocol

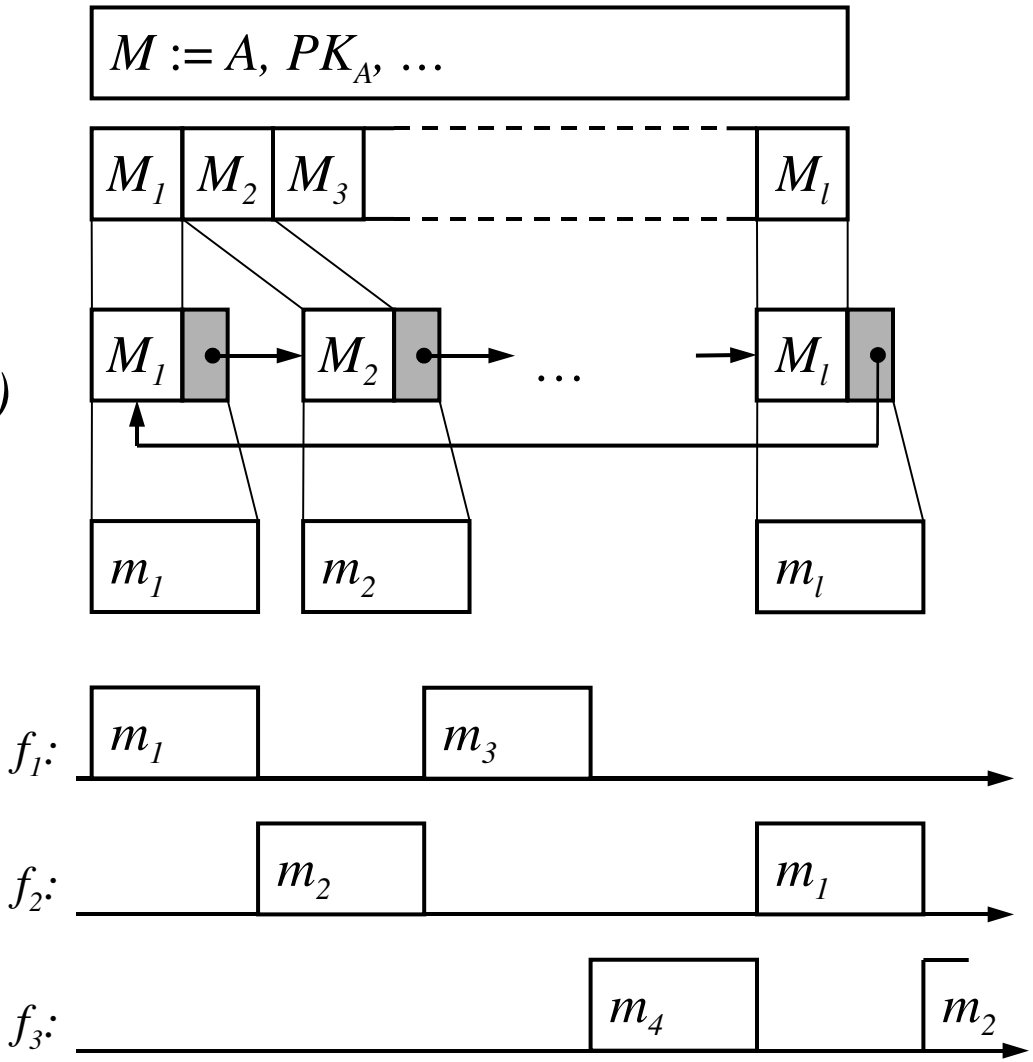


Uncoordinated Frequency Hopping (UFH)



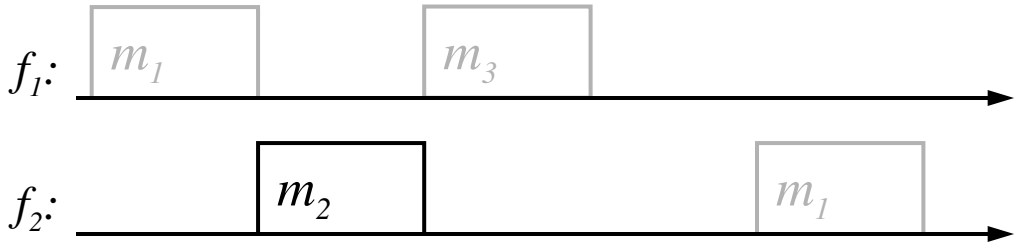
Message Transfer Protocol: Sender

- Fragmentation
- Hash linking
  $h_l := h(m_1),\ h_i := h(m_{i+1} || h_{i+1})$
- Bit coding/interleaving
- Repeated transmission using UFH



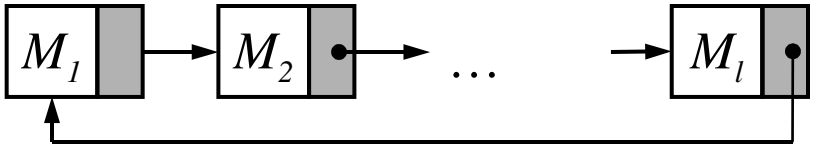
Message Transfer Protocol: Receiver

- Receiving packets

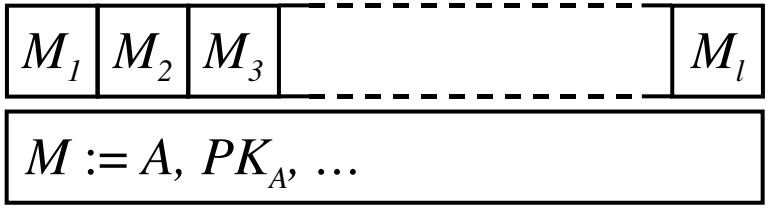


- Bit deinterleaving/ decoding

- Ordering and linking packets

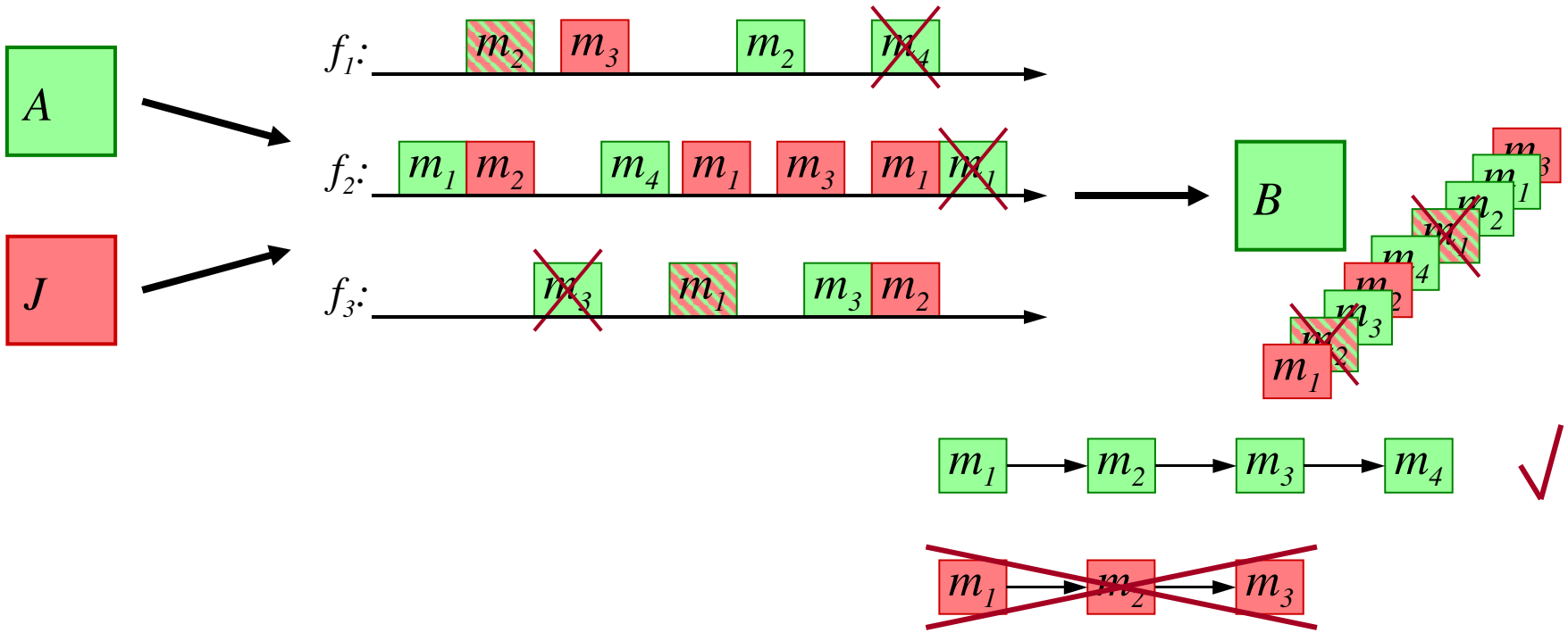


- Message reassambly



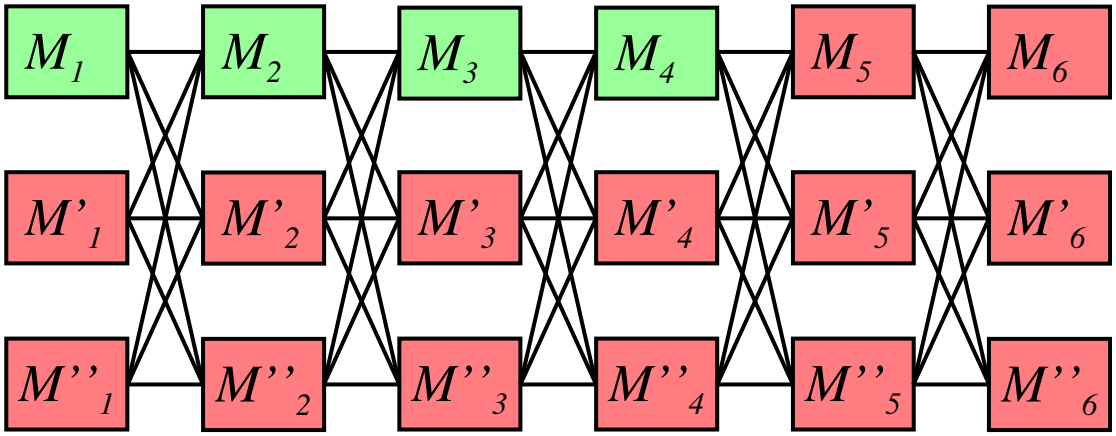
Security Evaluation: Packet Insertion, Mod., Jamming

- UFH is resistant to packet jamming due to the frequency hopping and the packet repetitions in the sending process
- Modified packets are identified using hash links
- Reassembled messages that fail the signature verification or have an expired timestamp are discarded



Security Evaluation: Packet Insertion

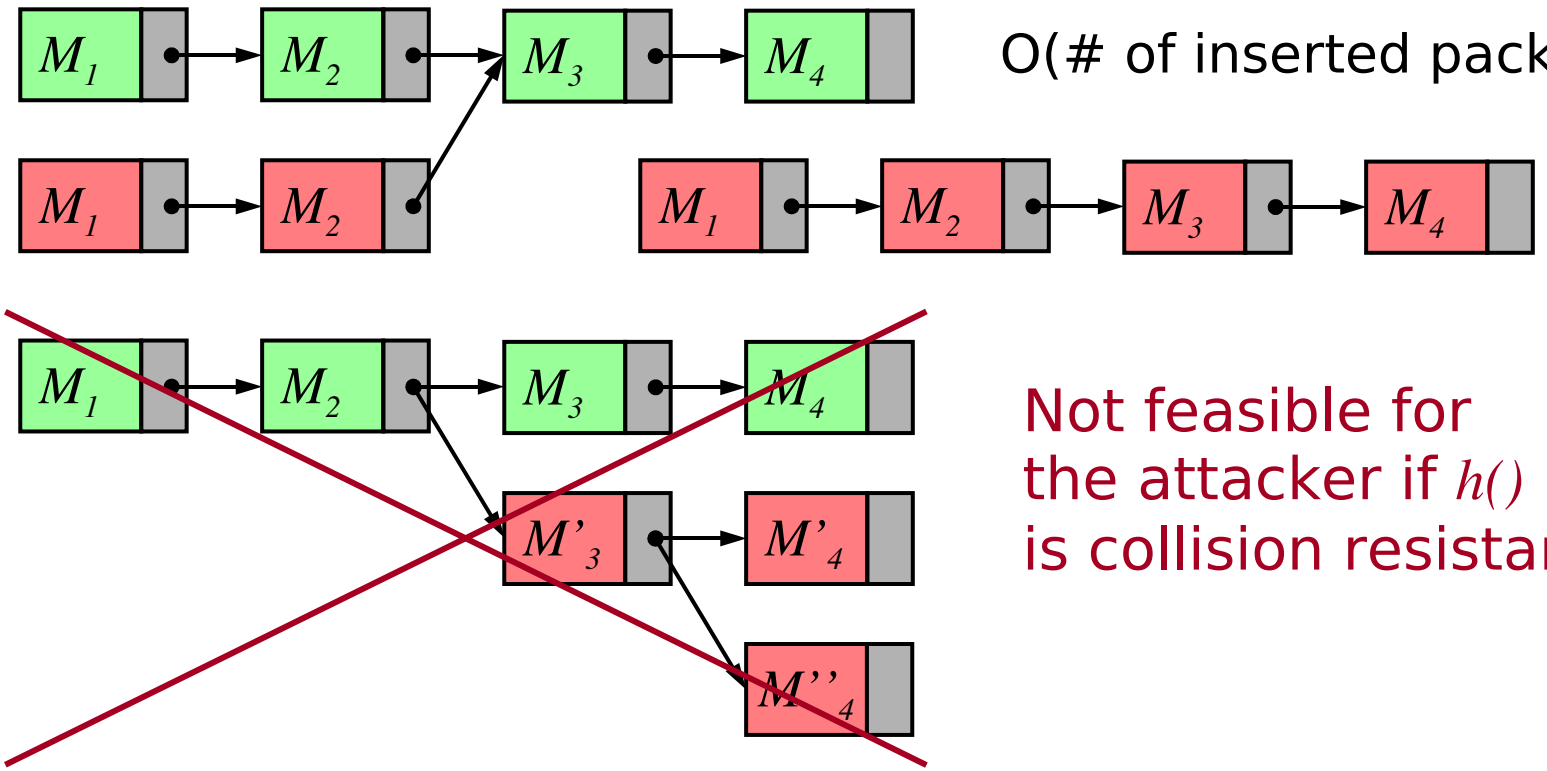
- Packets inserted by the attacker cannot be distinguished from packets inserted by the receiver
- Without the hash links, all possible packet combinations must be reassembled and the resulting messages be verified
- Receiver's workload grows exponentially in the number of maliciously inserted packets, leading to a DoS attack
- Example:



$O(3^{\text{\# of inserted packets}})$

Security Evaluation: Packet Insertion

- Due to the hash links, the attacker can insert new packet chains or create fusions into the legitimate packet chain, but cannot create branches
- This prevents DoS attacks by packet insertions that would make message reassembly infeasible



Performance Evaluation

- Attacker strategies: insert, modify, jam, mixed
- Model different jammer types and express their strength as the probability p_j with which a packet can be jammed
- Proof that jamming is the optimal strategy for the attacker

- Evaluated metrics:
  - Expected number of message retransmissions

$$N(p_m^{\mathcal{A}_C^J}) := \sum_{i=0}^{\infty} \left(1 - \left(1 - \left(1 - p_m^{\mathcal{A}_C^J}\right)^i\right)^l\right)$$

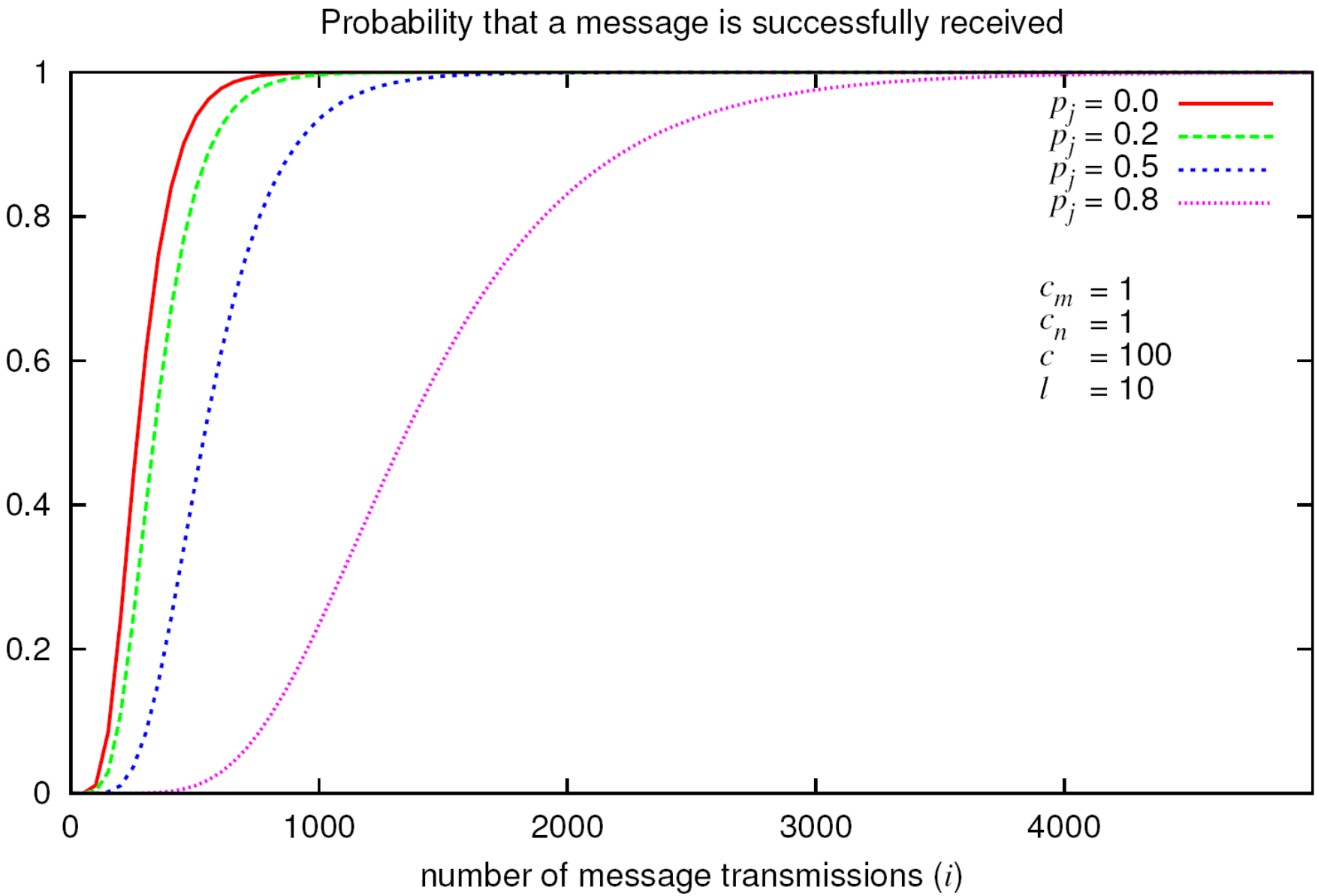
$$p_m^{\mathcal{A}_J} = 1 - \prod_{i=0}^{c_m - 1} \left(1 - \min\left\{\frac{c_n}{c - i}, 1\right\}(1 - p_j)\right)$$

l: fragments per message

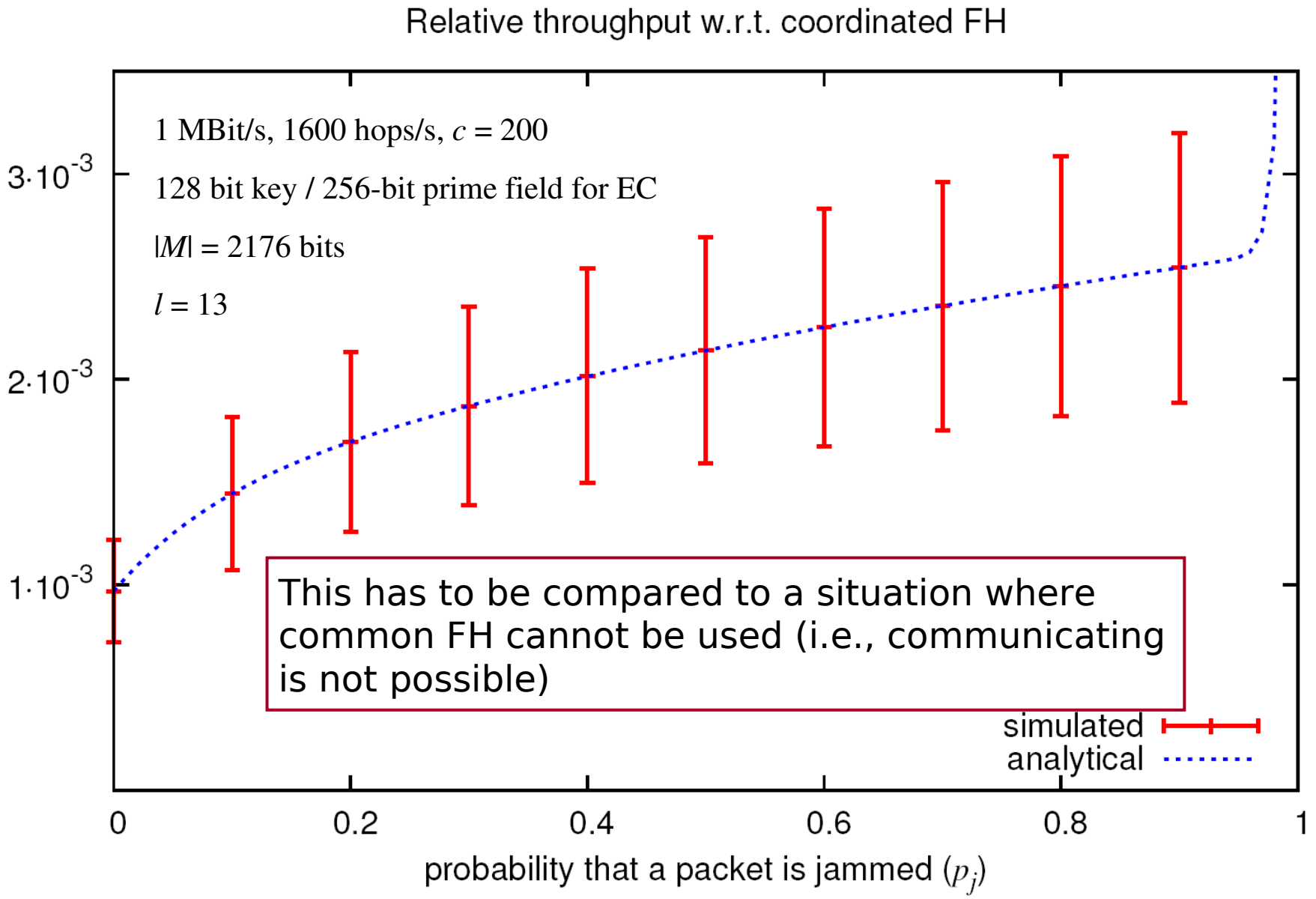
c: num. freq. channels
c_n: num. reception channels
c_m: num. sending channels

  - Expected relative throughput Φ
  - Expected duration to establish a shared key T

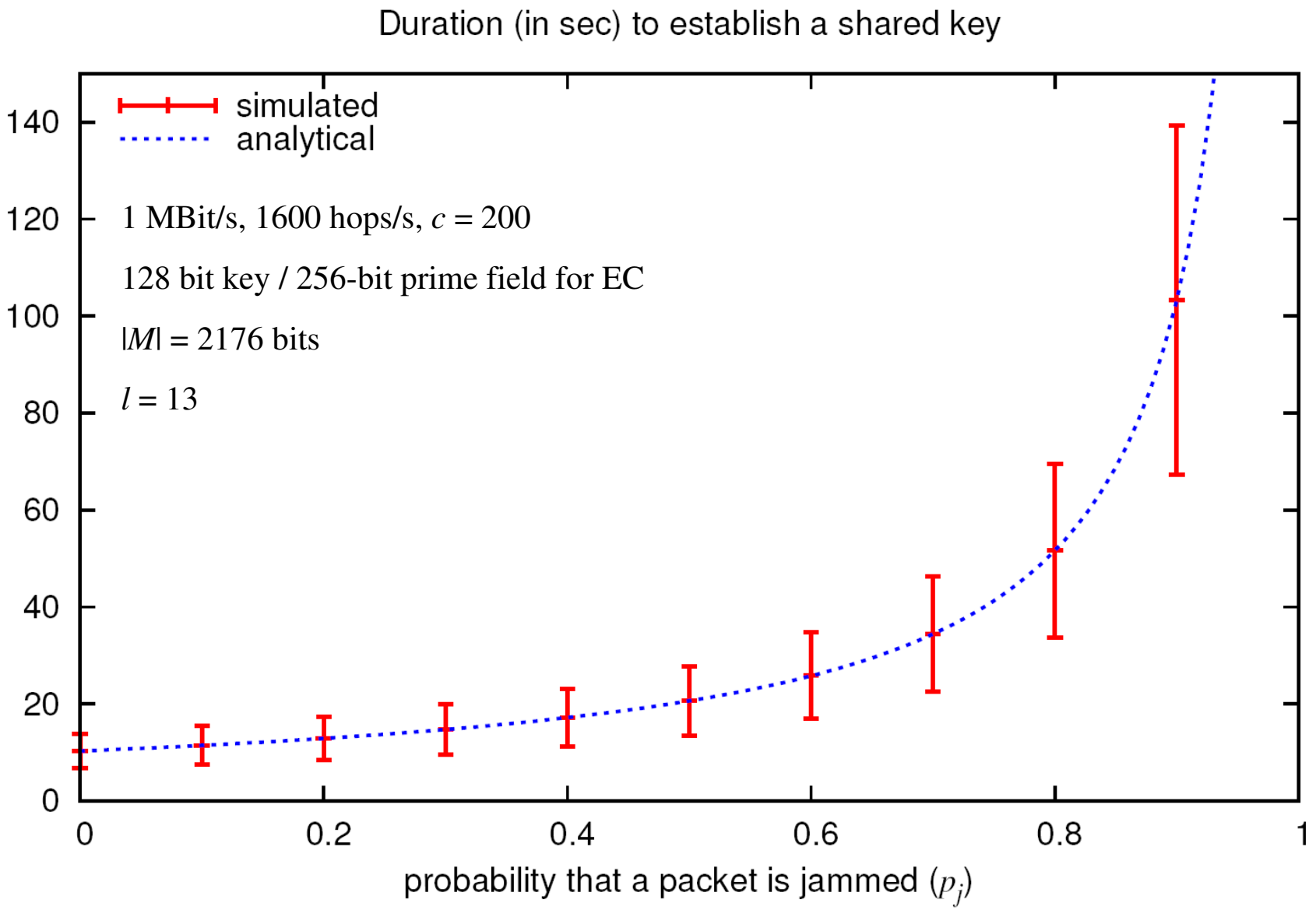
Performance Evaluation: # of retransmissions



Performance Evaluation: Illustrative Example

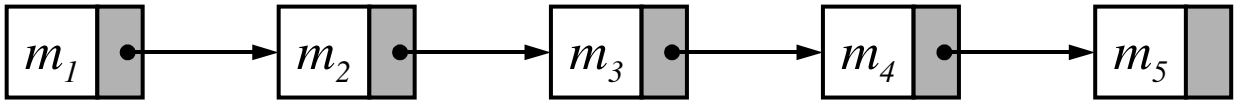


Performance Evaluation: Illustrative Example



Discussion: Enhancing the Message Fragmentation

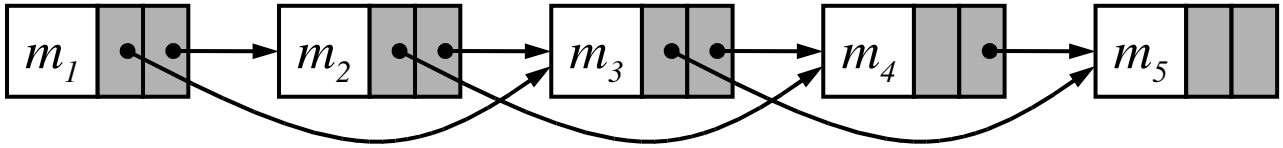
- Property of the proposed hash link chains: All fragments must be received before a message can be reassembled



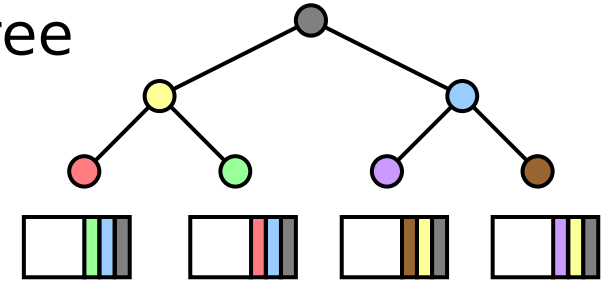
- Possible enhancement: “Verifiable” erasure/fountain codes
  - Use erasure coding to split a message into n fragments such that any subset of l fragments can be used to reconstruct the message (i.e., packets contain redundant information)
  - Augment each packet such that the message it belongs to can be efficiently identified

Discussion: Alternative Fragmentation Schemes

- Approach 1: Add additional hash links such that a missing fragment can be bypassed



- Approach 2: Build a Merkle Hash Tree and append values to verify root (distillation codes, C. Karlof et al.)



- Disadvantage: overhead per fragment increases (redundant data, ≥ 2 hashes) ⇒ either we need more fragments or the packet size (and thus also the jamming probability) increases

Summary and Conclusions

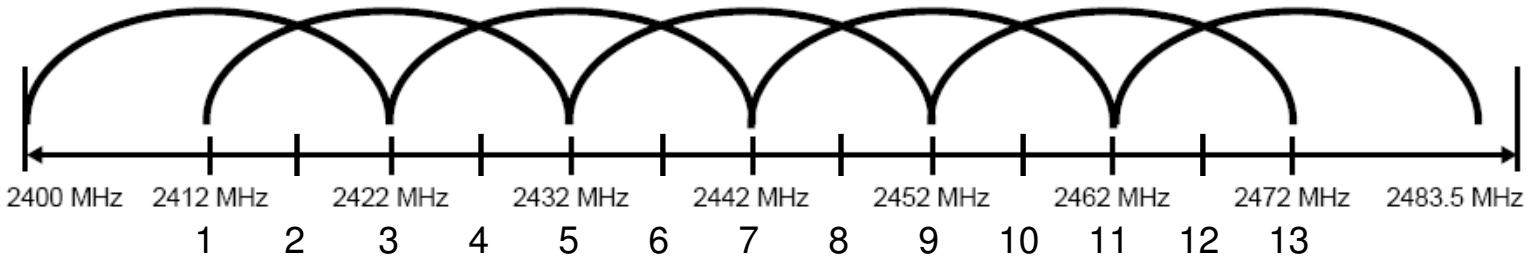
- Problem: anti-jamming/key-establishment dependency cycle
- Can be broken using UFH
- UFH achieves the same level of anti-jamming protection as coordinated FH at the cost of a lower throughput

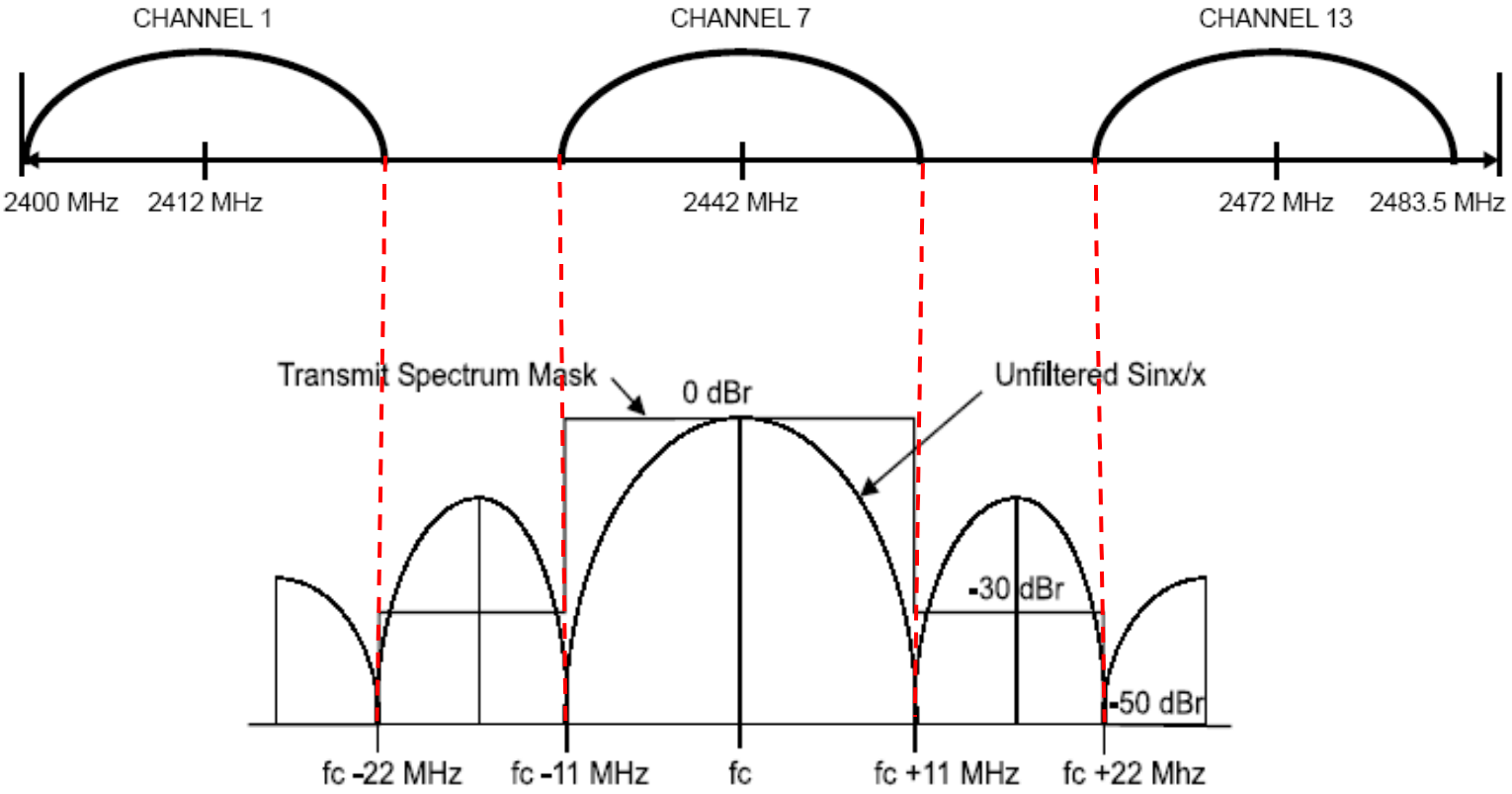
Impact of jamming on (e.g. WiFi) networks

802.11b/g physical layer

- 2.4 GHz (2.4–2.4835 GHz) 14 channels
  - Central channel frequencies are 5 MHz apart
  - 13 used in EU, 11 US
- Supports two spread spectrum techniques
  - Direct Sequence Spread Spectrum (DSSS)
  - Frequency Hopping Spread Spectrum (FHSS)
- Coding and modulation schemes determine max. communication speeds (1, 2, 5, 11, 54Mbps, ...)
  - 802.11b at 11Mbps
    - Complementary Code Keying (CCK)
    - Differential Quadrature Phase Shift Keying (DQPSK)
  - 802.11g at 54Mbps
    - Orthogonal Frequency Division Multiplexing (OFDM)

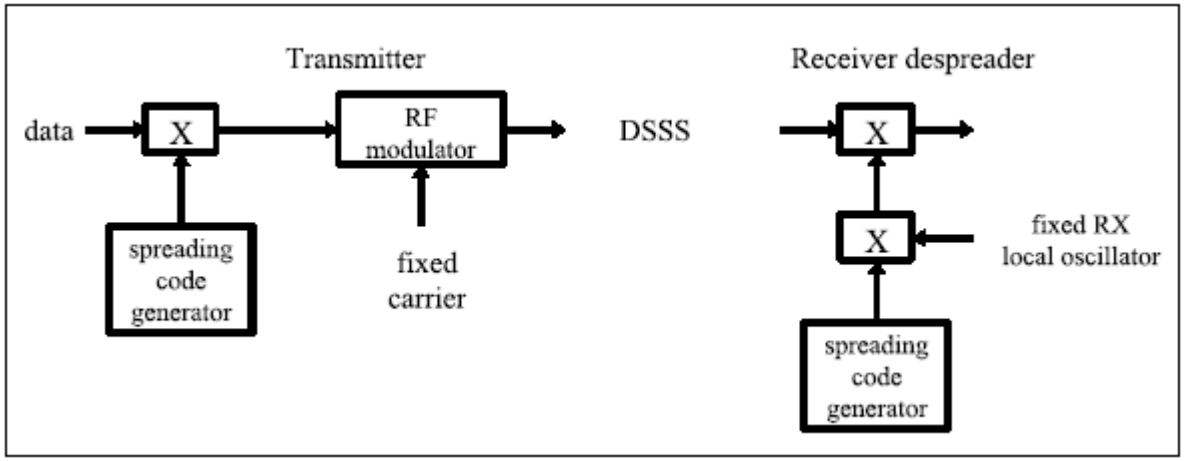
Channel allocation (2-2.4835 GHz)



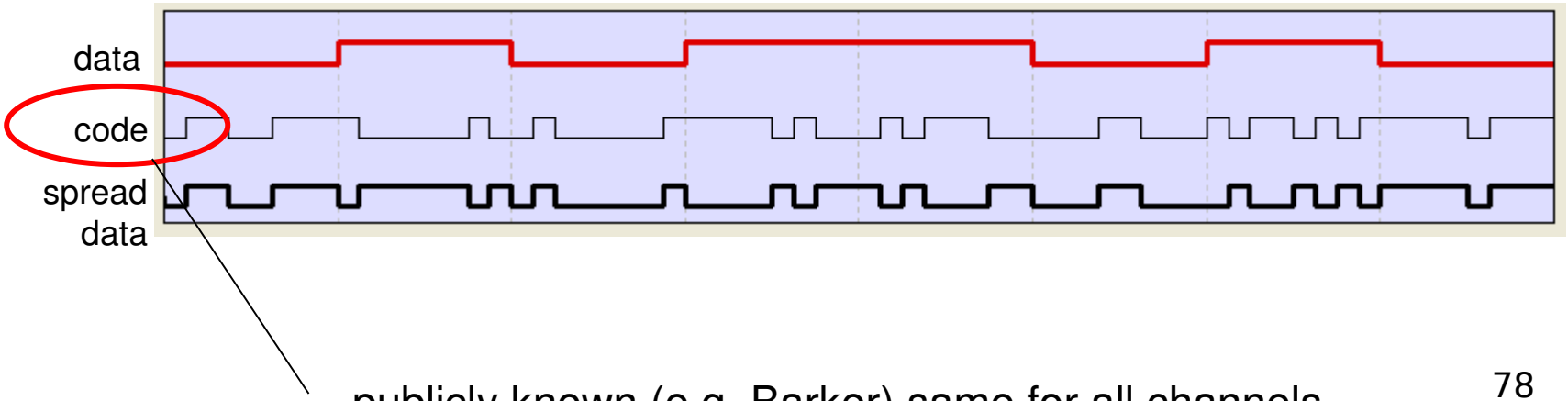


Direct Sequence Spread Spectrum (DSSS)

Basic operation:



Example:



Jamming 802.11

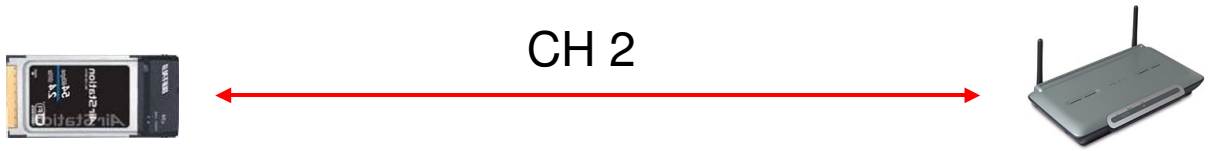
- Spreading techniques in 802.11
  - spreading codes are publicly known
  - e.g. Barker sequence for 802.11b at 1Mbps and 2Mbps = “1 0 1 1 0 1 1 1 0 0 0”
  - spreading codes are the same for *all channels*

- Spreading codes in 802.11 *are not used for confidentiality*

- Jamming:
  - *jammer knows the codes* and therefore can jamm any channel by transmitting symbols using the same codes ...
  - even if the attacker uses adjacent channels the throughput will be affected (there are only 3 non-overlapping channels)
  - there is no solution for this DoS attack on 802.11

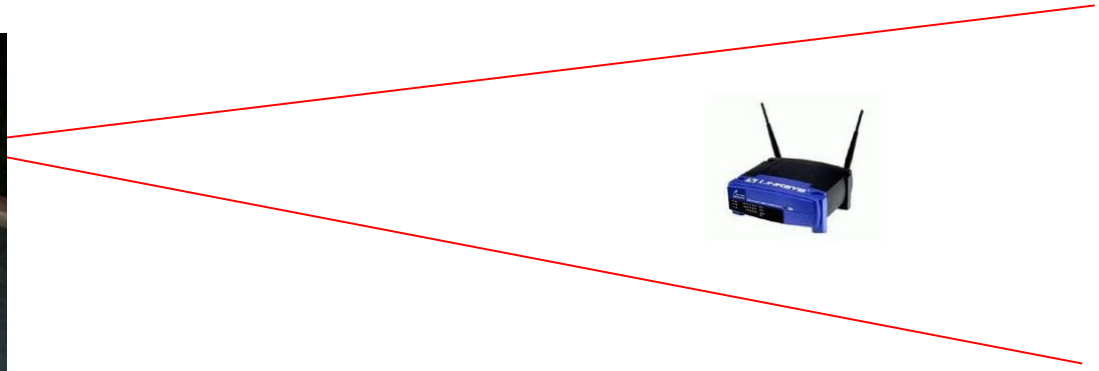
Communication between a client and AP

- AP communicates with the clients using a single channel (e.g. CH 2)
- Only one client communicates with an access point at a time (regulated by the 802.11 MAC protocol)
- The signal is filtered (fc ± 22MHz) to eliminate (part of the interferences from neighboring channels)
- Significant interference remains on the channel
  - from neighboring channels (channels are only 5MHz apart)
  - from the environment
- The use of DSSS provides some resilience to interference

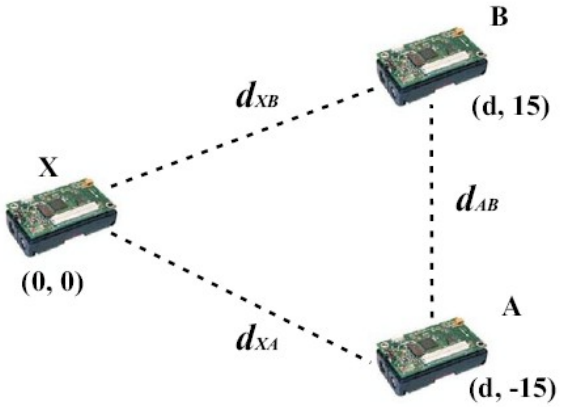


802.11 physical layer security issues

- handles interference
- 802.11 PHY cannot cope with active jamming
  - it was not designed to be resistant to jamming
  - easy intercept
  - easy DoS attacks
  - the attacker still needs a high-power transmitter to cover a large area
  - an attacker with an directional antenna can ‘aim’ at the victim AP and disable it (line of sight (LoS))



Sensor network jamming



Shared spectrum – known codes
MAC-layer jamming

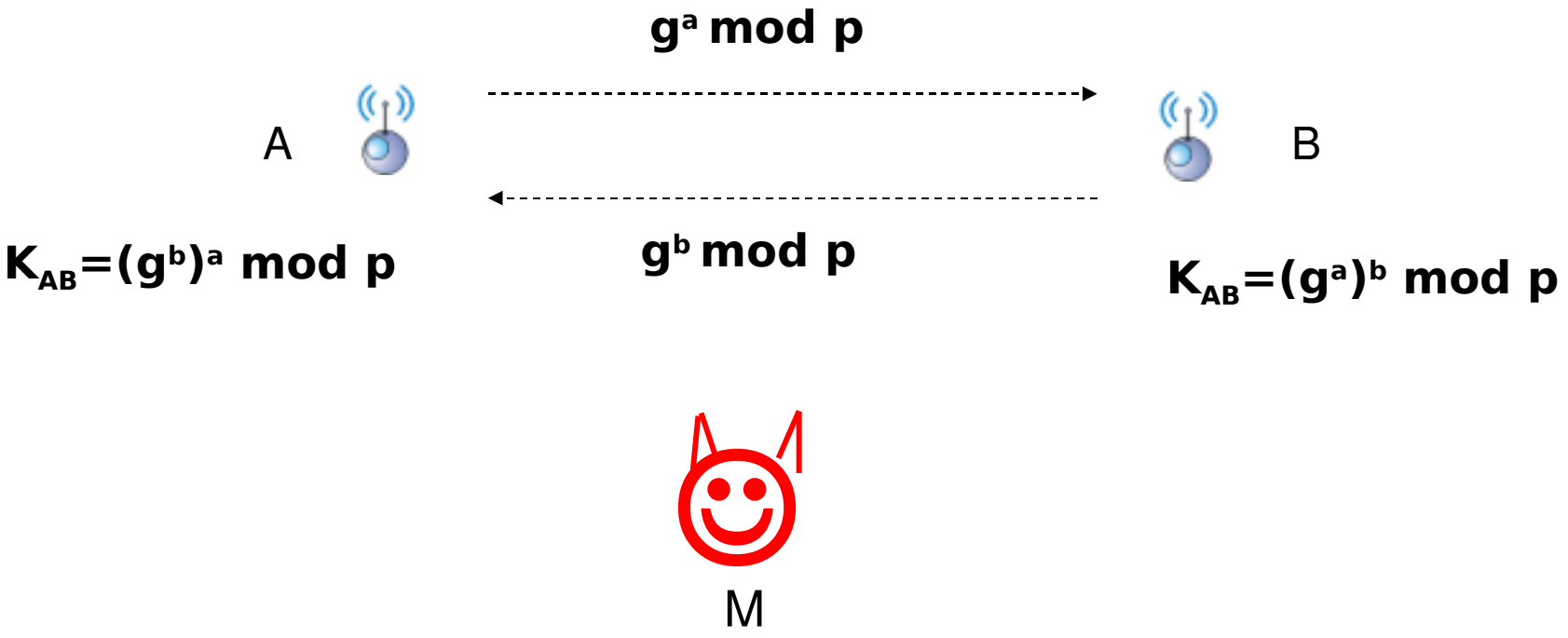
GPS jamming/spoofing

- Received GPS radio signal has a strength is about $1x10^{-16}$ W at the Earth's surface.

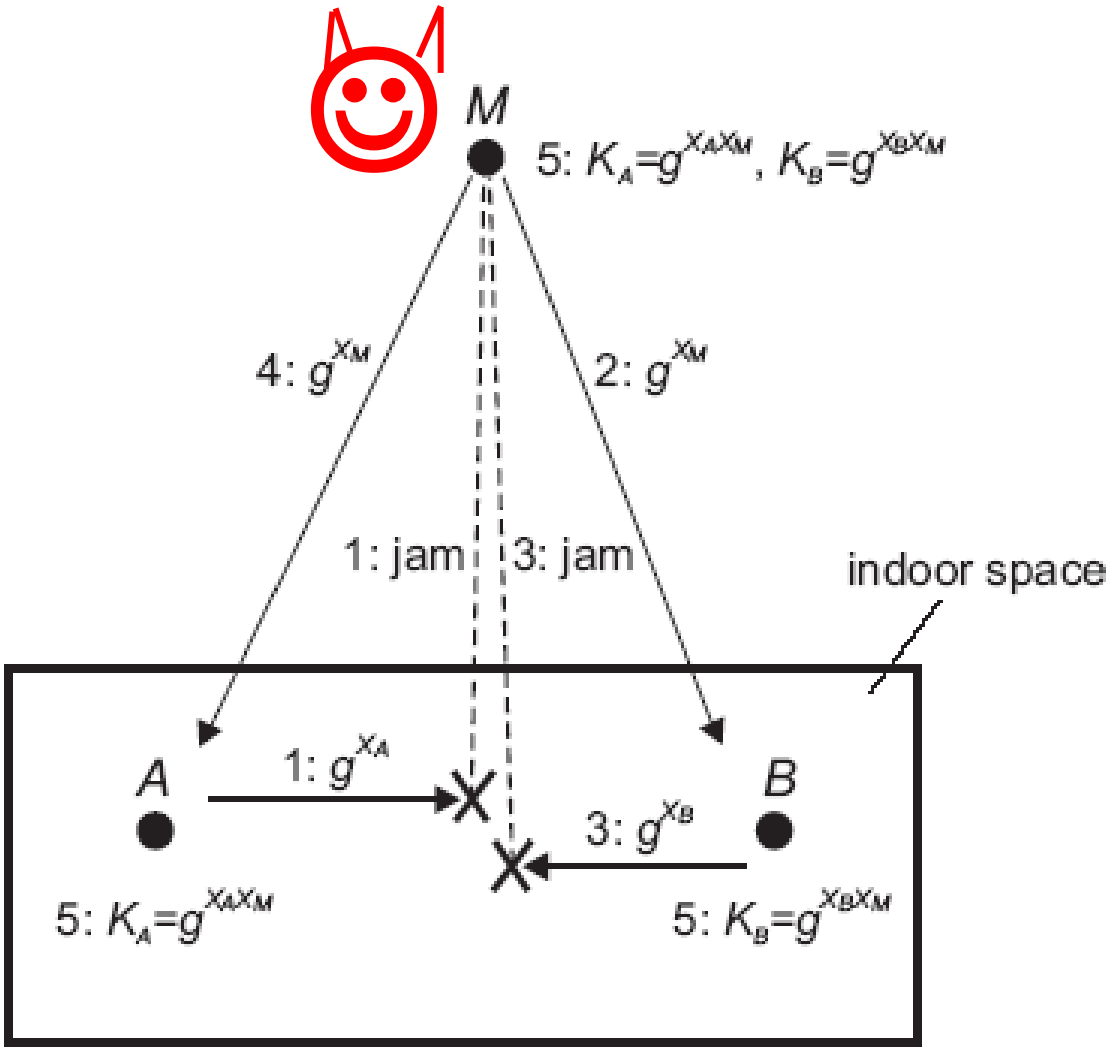
- A stronger signal can *cover* GPS satellite signal and cause the device to register a position different from its true position.

Think GPS Cargo Tracking = High Security? Think Again,
Roger G. Johnston, Jon S. Warner, Los Alamos National Laboratory, 2004

Implications of Jamming – MITM on DH

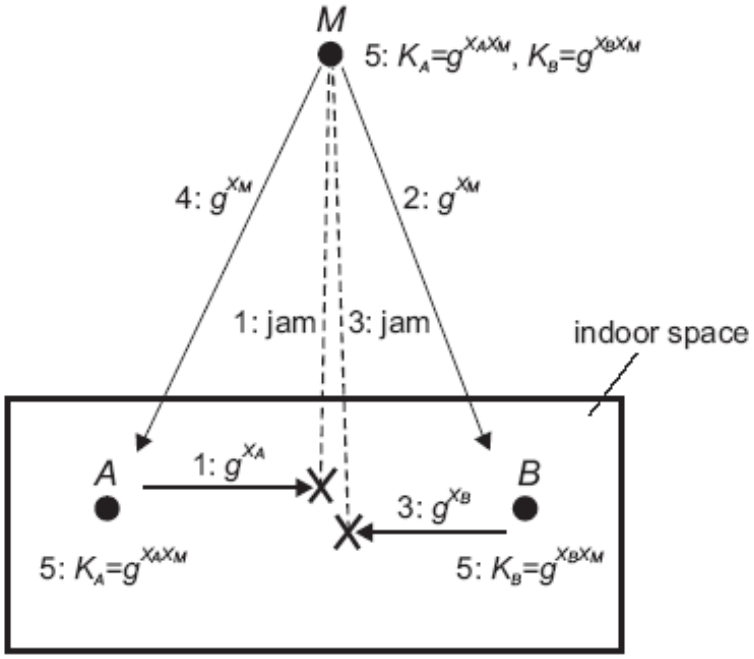


Man in the middle attack



MITM

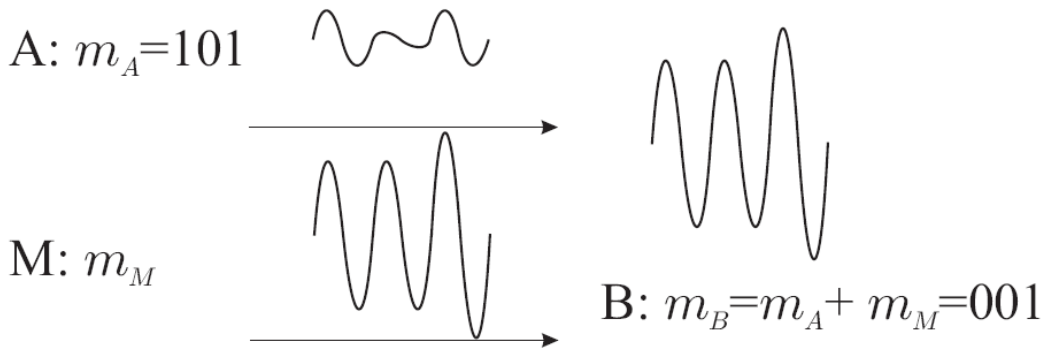
- If A and B are in each others' power range, and if they can detect jamming MITM is prevented
- If A and B are NOT is each others' power range, MITM is possible even without jamming, using only eavesdropping and replay!



Implications of jamming on MITM

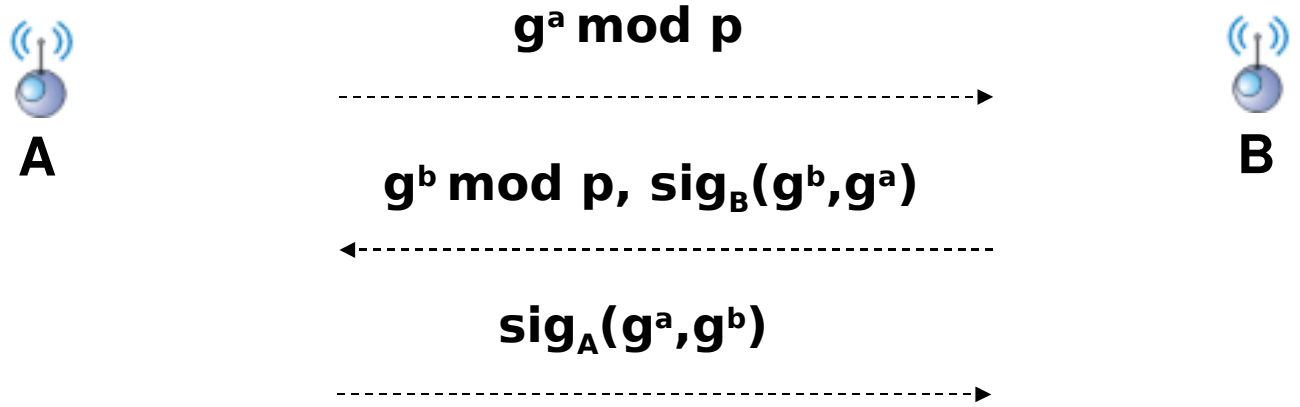
If jamming can be detected, MITM is prevented (if nodes are in each-others power range).

- Problem:
  - covert jamming
  - signal overshadowing

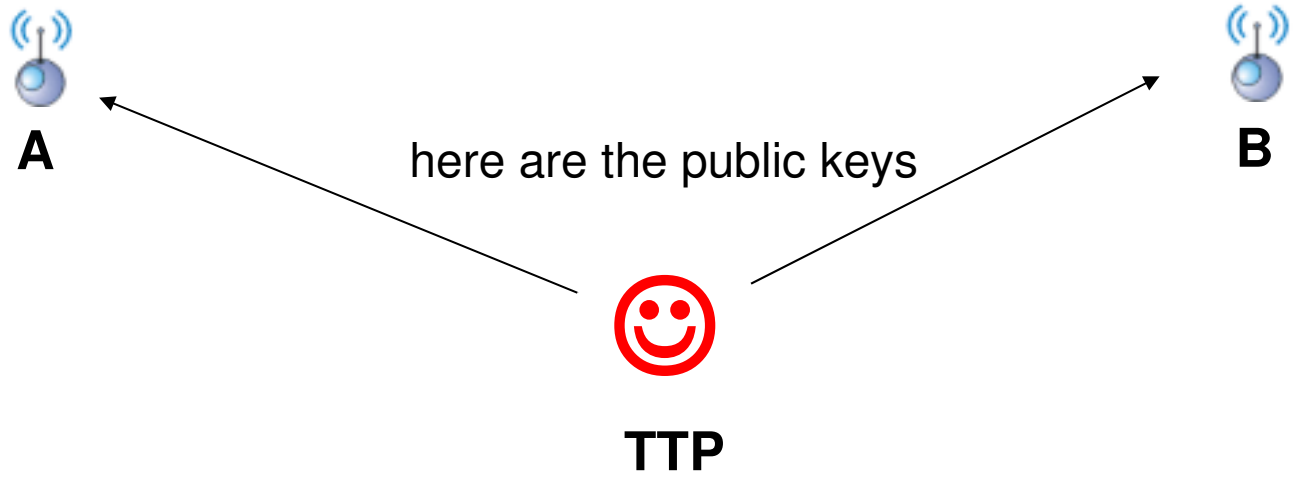


Deceptive jamming

Solution to the MITM: authentication of DH contributions



Uses signatures ... (DH contributions **are authenticated**)



Conclusion on jamming

- Open problem
- Power, power, power
- Gains achieved using spread spectrum techniques ...
- Full protection is not really feasible (shared medium)

- If we cannot prevent, we can at least detect jamming
  - jammer location

- **Affected systems:** almost all
  - GPS, weak signals (10^{-16} W)
  - 802.11 (known sequences)
  - GSM/UMTS/ ...
    feasible for all cellular standards
  - Sensor networks

References

- D. Adamy, A First Course on Electronic Warfare, book
- D. Adamy, A Second Course on Electronic Warfare, book
- W. Xu, W. Trappe, Y. Zhang, and T. Wood, *“The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,”* Proceedings of Mobihoc 2005
- M. Strasser, C. Popper, S. Capkun, M. Cagalj, “Anti-jamming Key Establishment using Uncoordinated Frequency Hopping”, Proceedings of IEEE Symposium on Security and Privacy 2008
-
- ... other work: Radha Poovendran, Wenjun Xu, Wade Trappe, Guevara Noubir ...