Wireless Security gets <u>Physical</u>

Srdjan Čapkun

Department of Computer Science

ETH Zürich

SWING, Bertinoro, July 2008

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

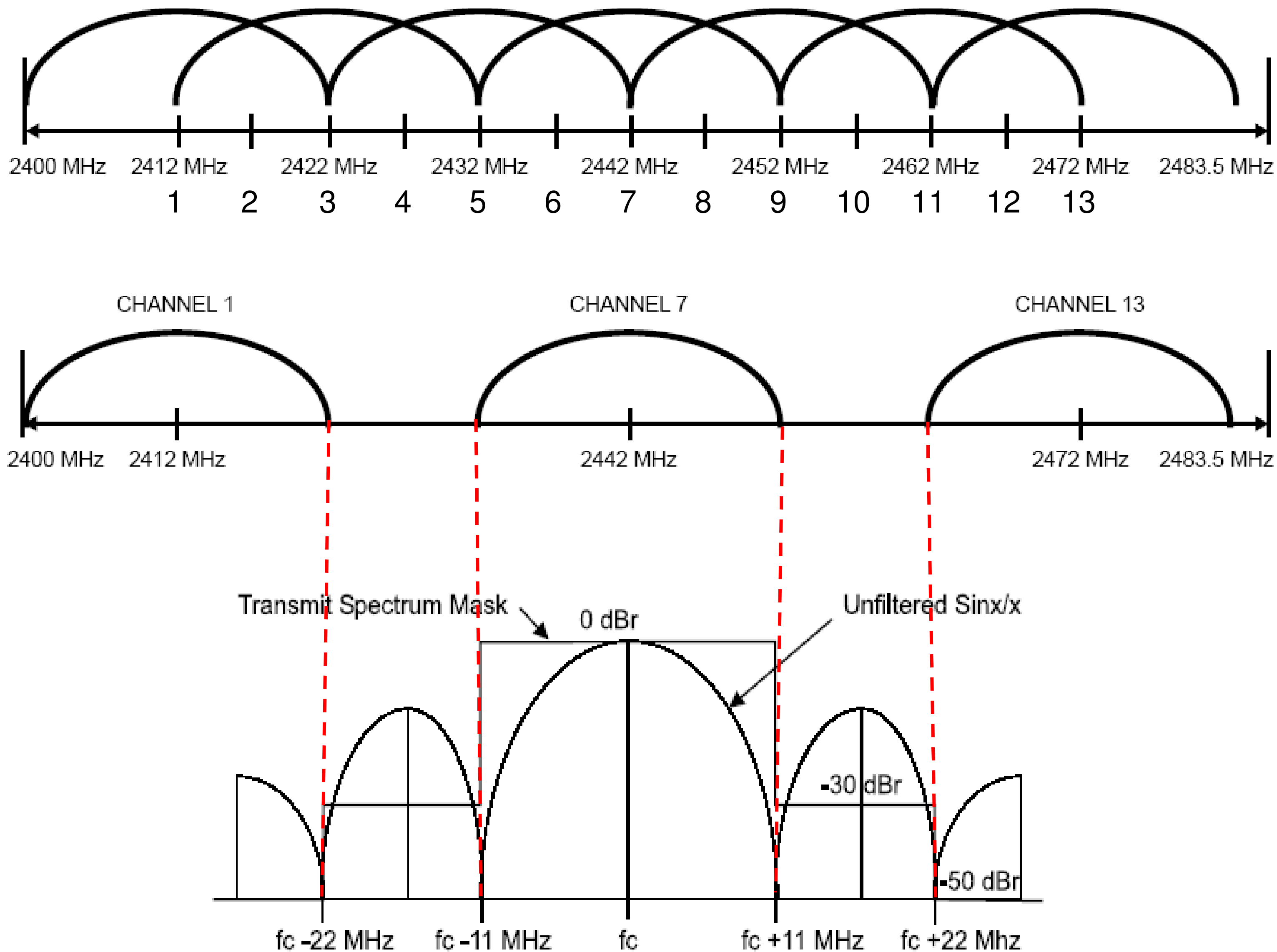
802.11b/g physical layer

- 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)

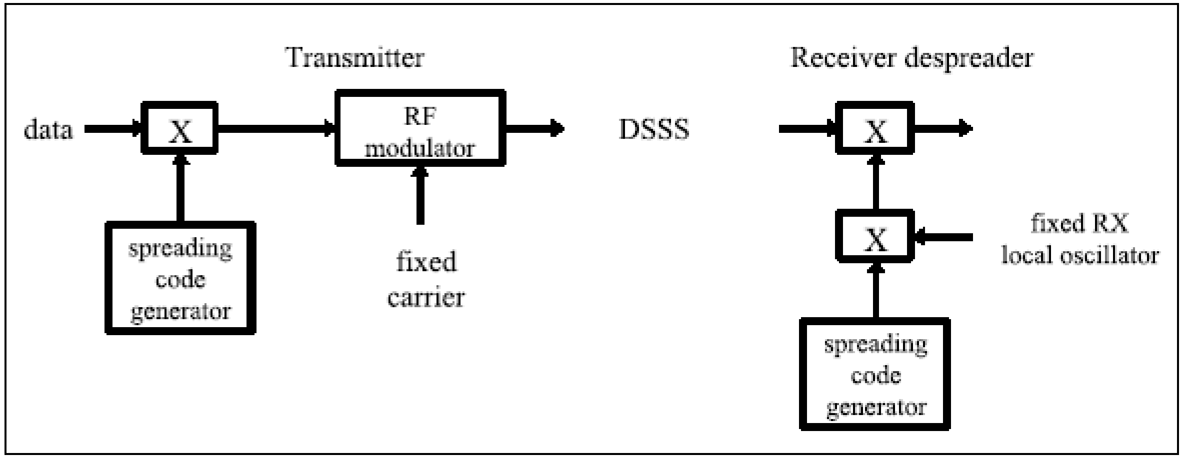
- Coding and modulation schemes determine max. communication speeds (1, 2, 5, 11, 54Mbps, ...)
  - 802.11b at 11Mbps
    - Complementary Code Keying (CCK)
    - Differential Quadrature Phase Shift Keying (DQPSK)
  - 802.11g at 54Mbps
    - Orthogonal Frequency Division Multiplexing (OFDM)

Channel allocation (2-2.4835 GHz)

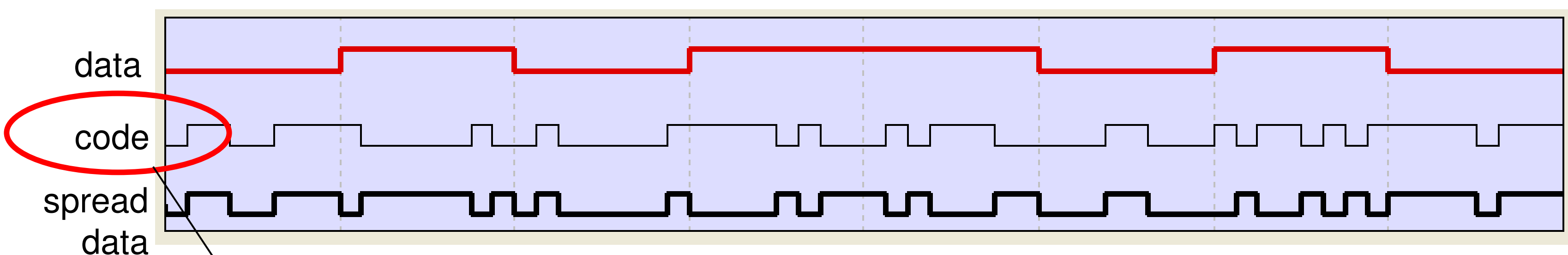


Direct Sequence Spread Spectrum (DSSS)

Basic operation:



Example:



publicly known (e.g. Barker) same for all channels

Jamming 802.11

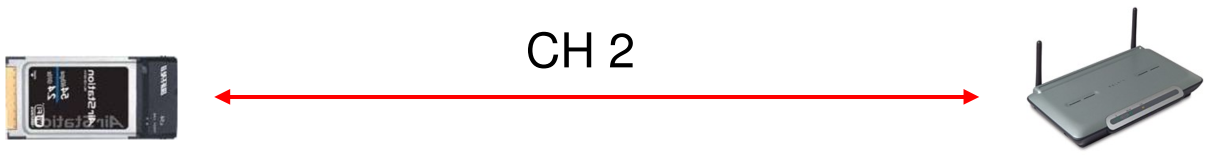
- Spreading techniques in 802.11
  - spreading codes are publicly known
  - e.g. Barker sequence for 802.11b at 1Mbps and 2Mbps = “1 0 1 1 0 1 1 1 0 0 0”
  - spreading codes are the same for *all channels*

- 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

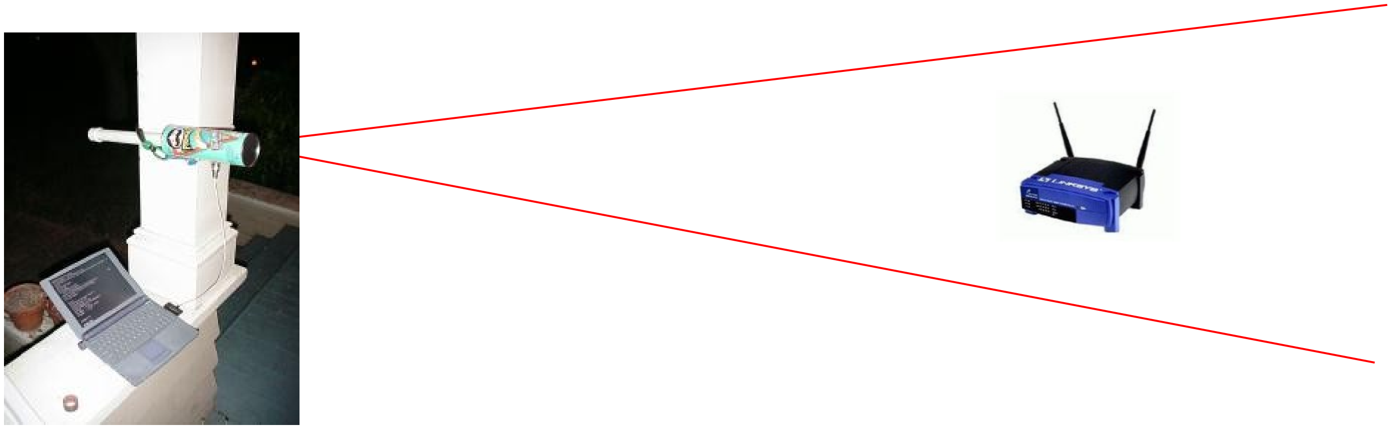
Communication between a client and AP

- 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

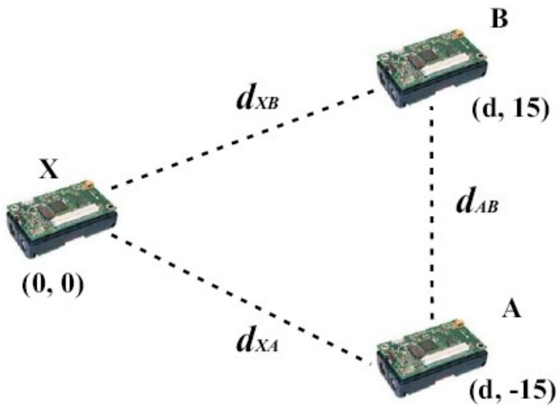


802.11 physical layer security issues

- 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

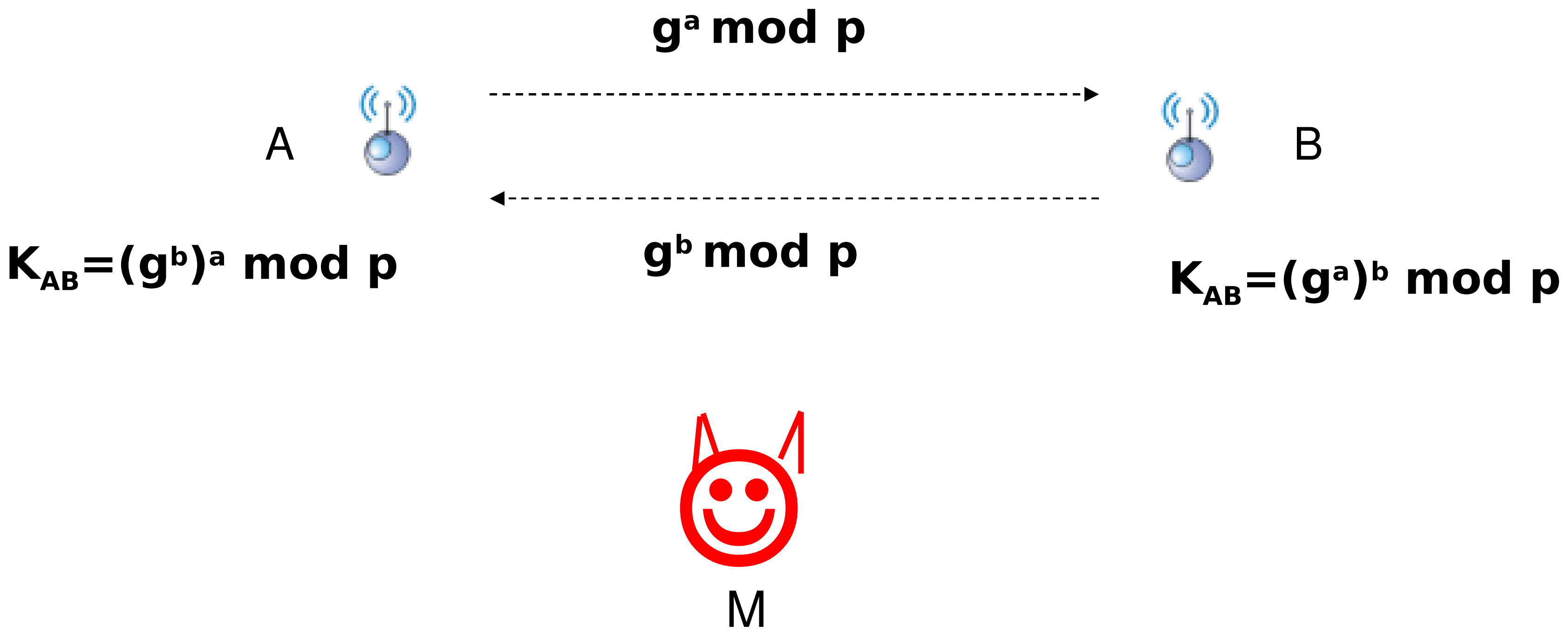
GPS jamming/spoofing

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

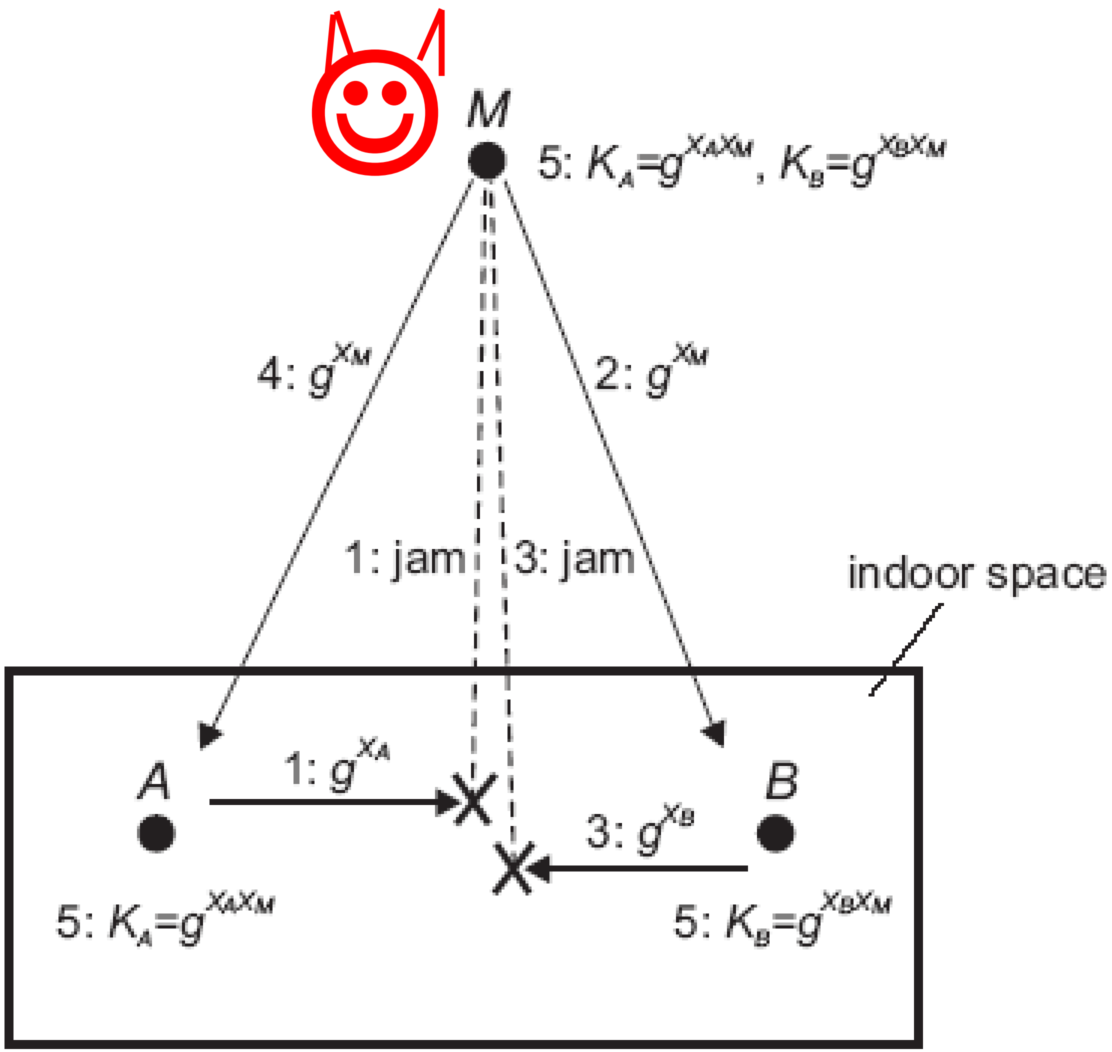
- A stronger signal can *cover* GPS satellite signal and cause the device to register a position different from its true position.

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



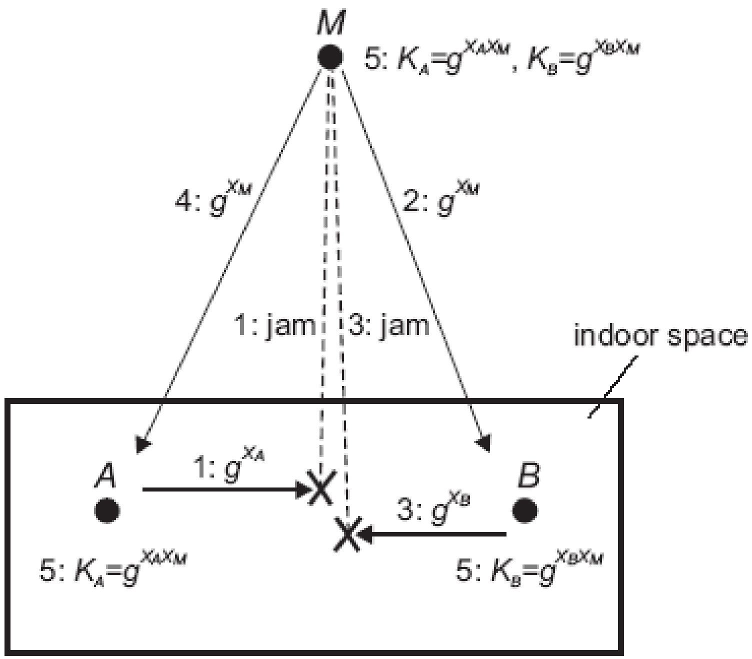
Man in the middle attack



MITM

- If A and B are in each others' power range, and if they can detect jamming MITM is prevented

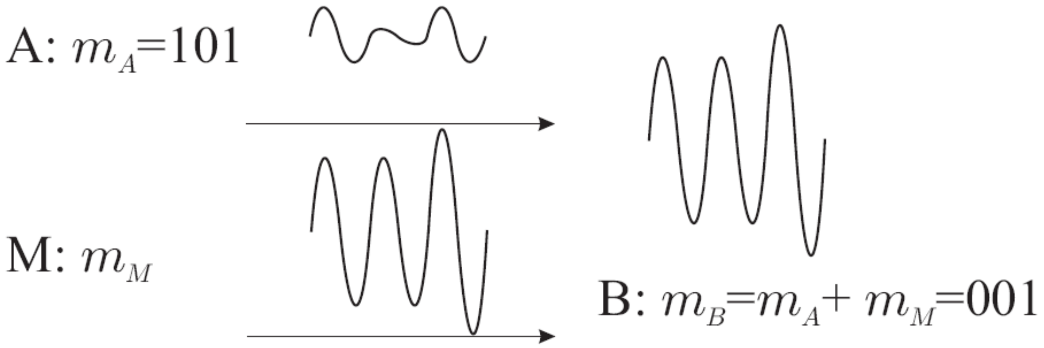
- If A and B are NOT is each others' power range, MITM is possible even without jamming, using only eavesdropping and replay!



Implications of jamming on MITM

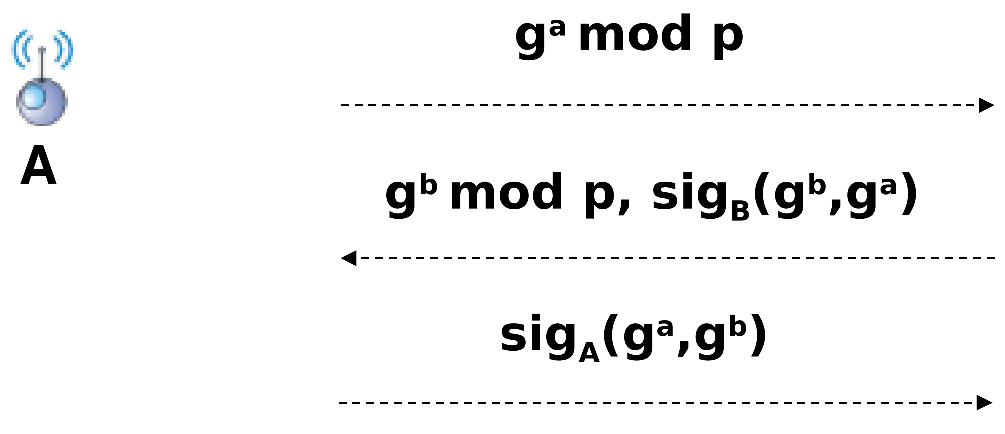
If jamming can be detected, MITM is prevented (if nodes are in each-others power range).

- Problem:
  - covert jamming
  - signal overshadowing

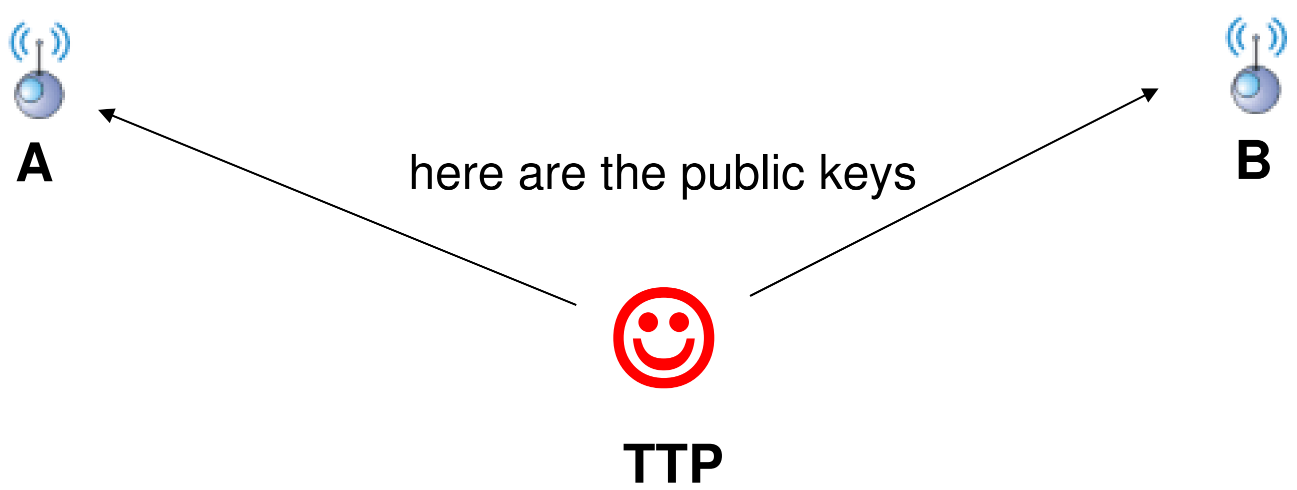


Deceptive jamming

Solution to the MITM: authentication of DH contributions



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



Example attack: Skyhook (iPhone) localization

- Skyhook localization system – uses public WiFi access points and GSM stations

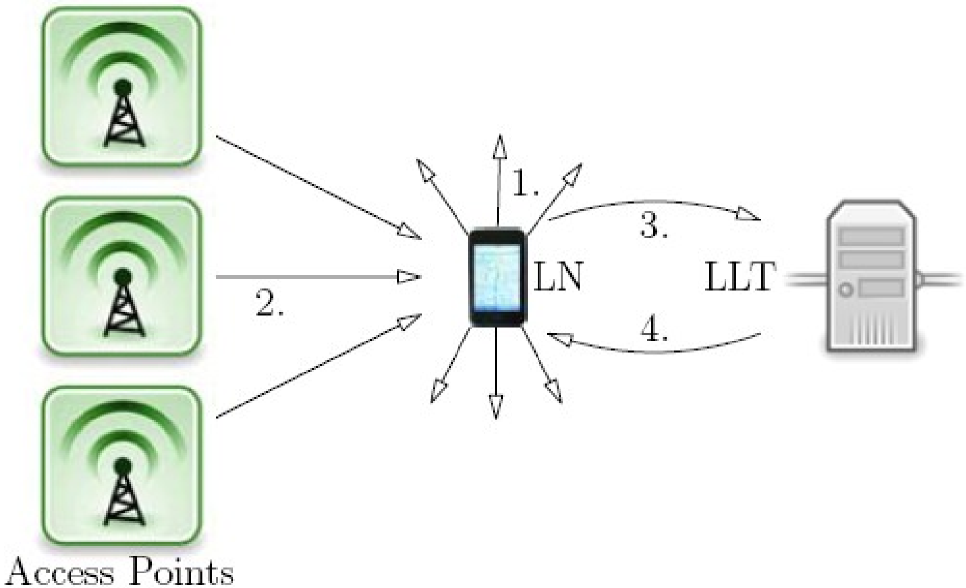
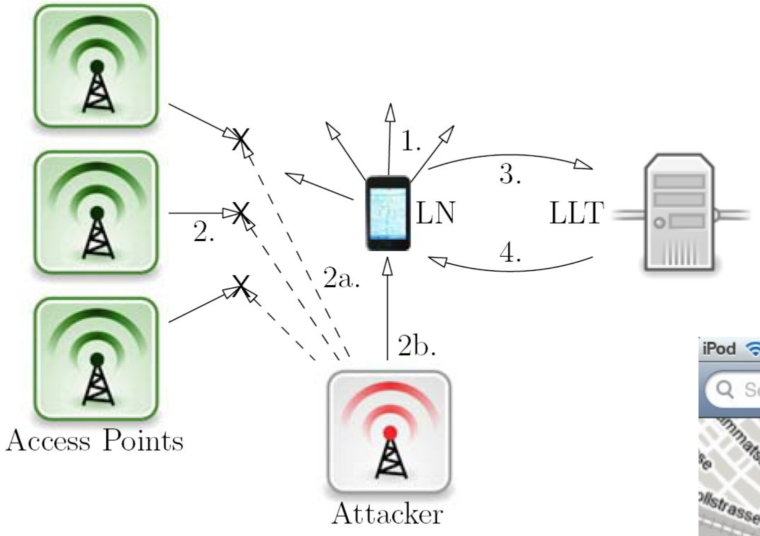


Figure 1: The Skyhook localization process. 1. The LN broadcasts a probe request frame. 2. APs reply with a response beacon frame. 3. The LN queries the LLT server. 4. The server returns data about observed APs. 5. The LN computes its location.

Example attacks: iPhone localization system

- Attack goal: device displays an incorrect location
- Attack: Jam signals from legitimate APs
  insert messages with MACs corresponding to other APs



- More attacks:
  database poisoning, ...

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
  - Localization

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 ...

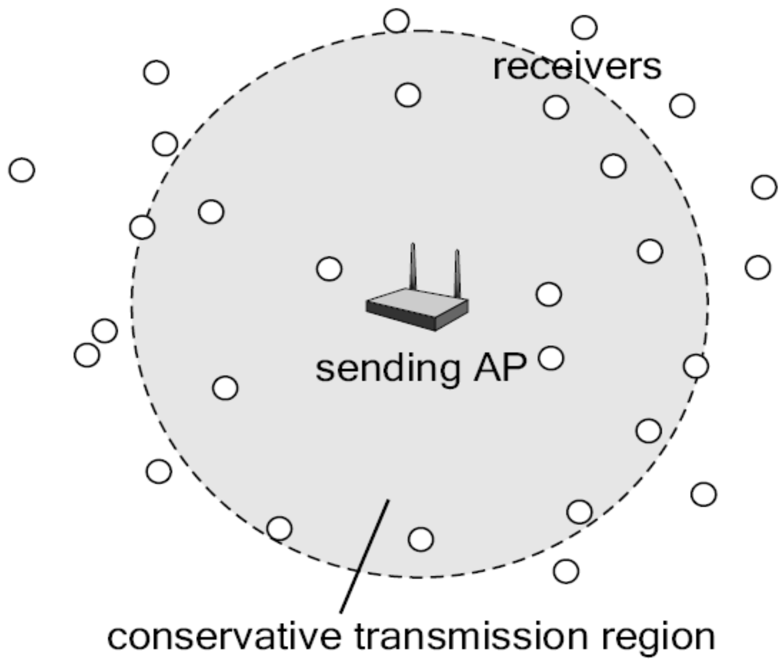
Using Location for Authentication

- Authentication through presence awareness
- Authentication through absence awareness

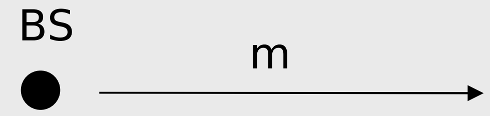
Integrity-codes: authentication through presence awareness

Authentication through presence awareness

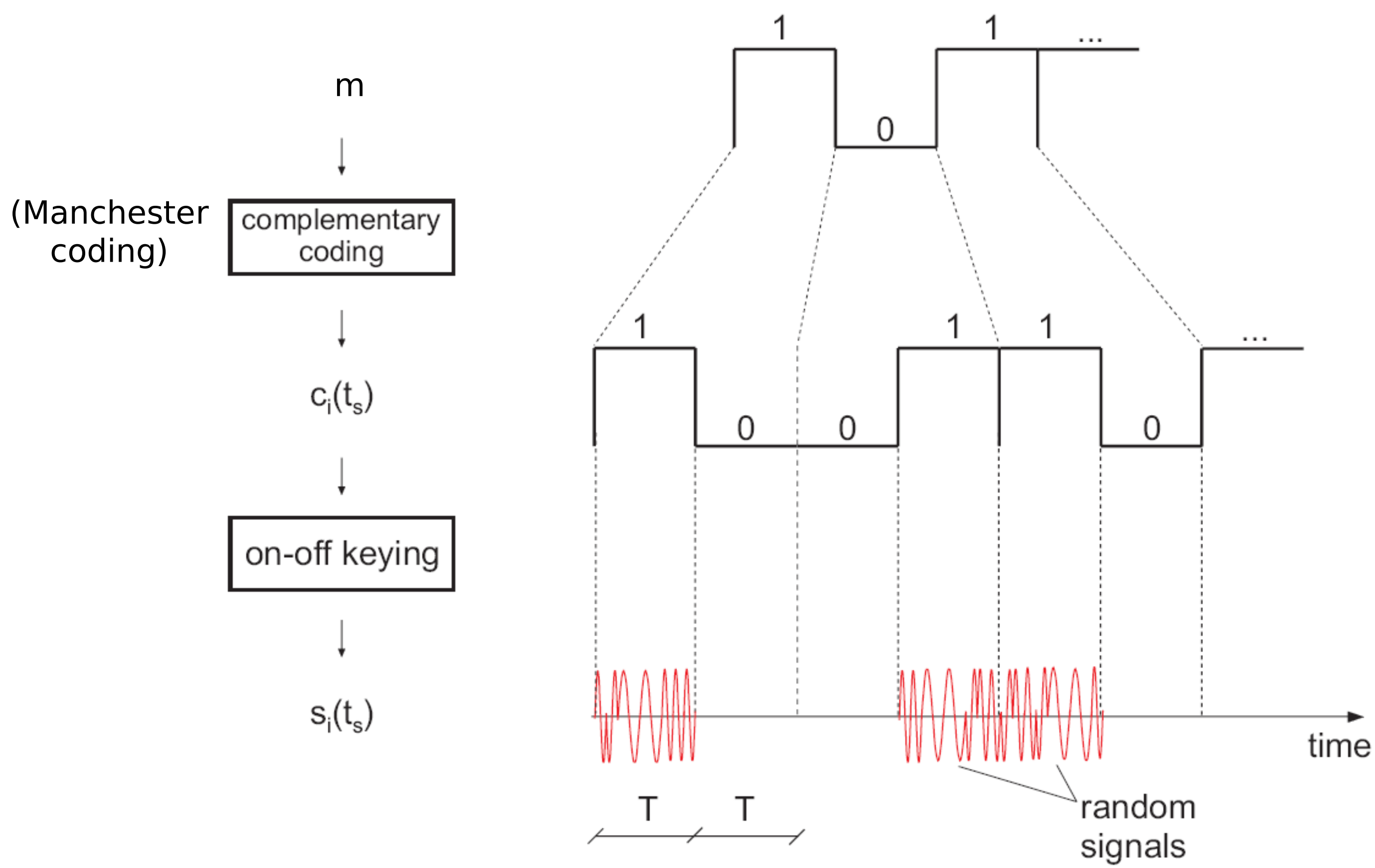
- Main idea:
  - Use special message encoding (Integrity coding)
  - Receiver(s) know that they are in range of the sender (presence awareness)



Integrity Coding

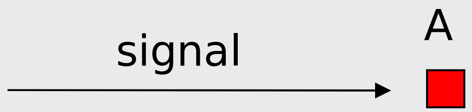


- k-bit Beacon1 spread to 2k bits (1->10, 0->01) (H(m) = k/2)
- transmitted using on-off keying (each “1” is a fresh random signal)

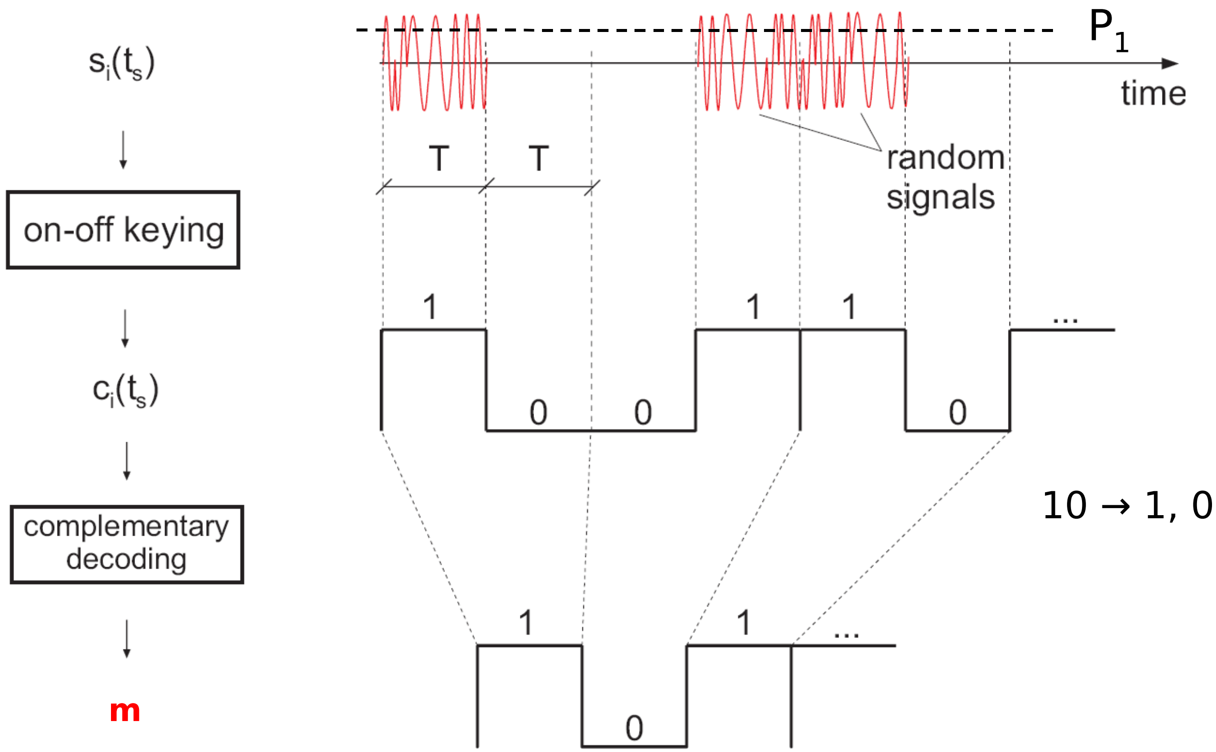


H(m) = the number of bits “1” in m (Hamming weight)

Integrity Decoding



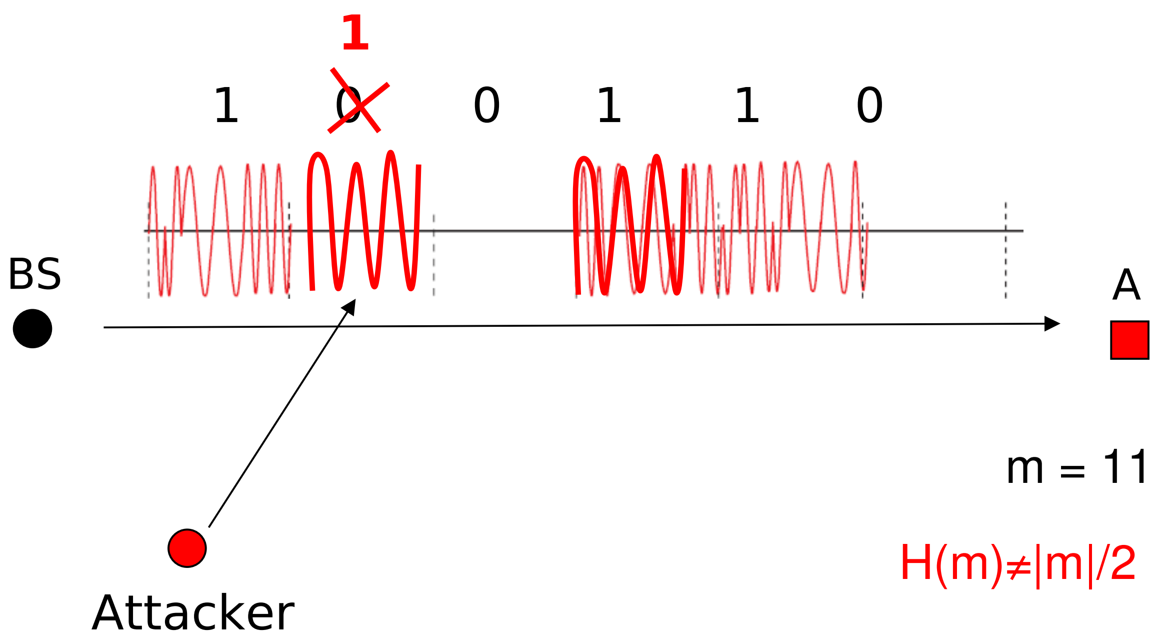
- Beacon detection:
  - presence of signal (>P_1) during T on CH1 interpreted as “1”
  - absence of signal (<P_0) during T on CH1 interpreted as “0”
- Beacon integrity and authenticity verification
  - IF H(m)=|m|/2 THEN “m” was not modified in transmission



10 → 1, 01 → 0 (Manchester)

Integrity Coding Analysis

- Message Hamming weight is a public parameter H(m)=|m|/2=2
- Attacker can change 0 → 1 and NOT 1 → 0 (except with **ε**)
- A can detect all modifications of the message on channel CH1
- A knows that BS is transmitting on CH1



m = 110110

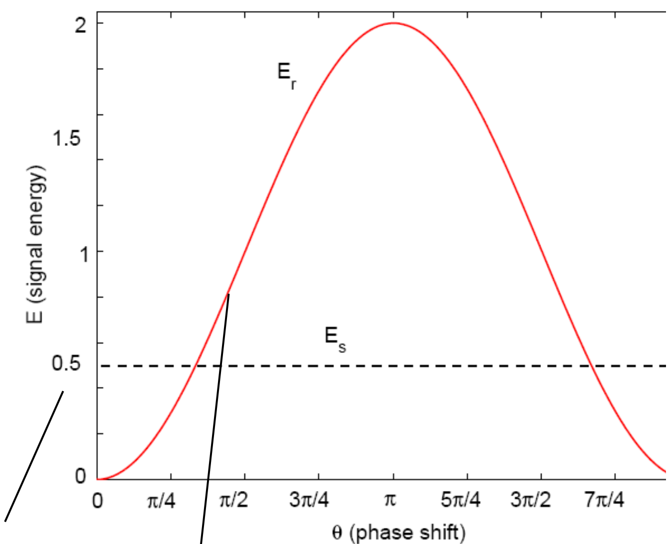
H(m)≠|m|/2 => m is invalid

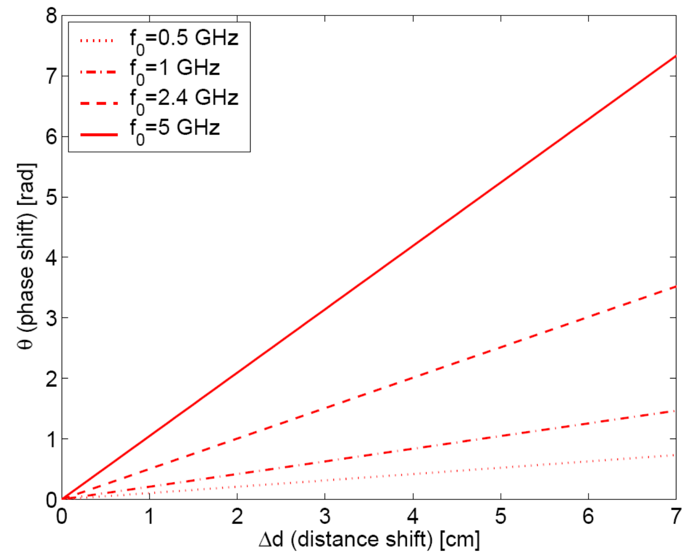
IC: Anti-blocking property of the wireless channel

- ($1 \not\to 0$)
- phase shift

$$\underbrace{r(t)}_{\text{receiver}} = \underbrace{\cos(\omega_0 t)}_{\text{sender}} - \underbrace{\cos(\omega_0 t - \theta)}_{\text{adversary}}, \text{ where } \theta \in [0, 2\pi)$$

$$E_r = \int_0^{T_s} r^2(t)dt$$
$$\approx 2T_s \sin^2\left(\frac{\theta}{2}\right)$$





original signal energy

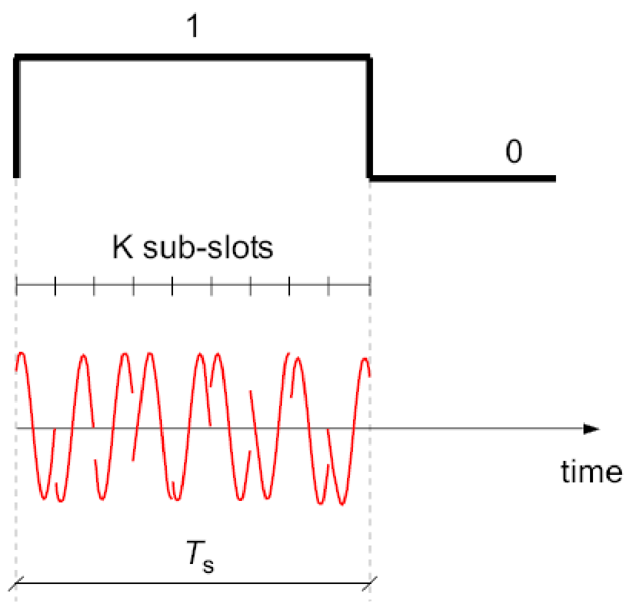
signal energy of the cumulative sender + attacker signal

error in distance estimation (by the attacker)

IC: Randomization At the Sender

- K-slotted signal (spreading)
- Φ random (e.g., choosen uniformly from $[0,2\pi)$)

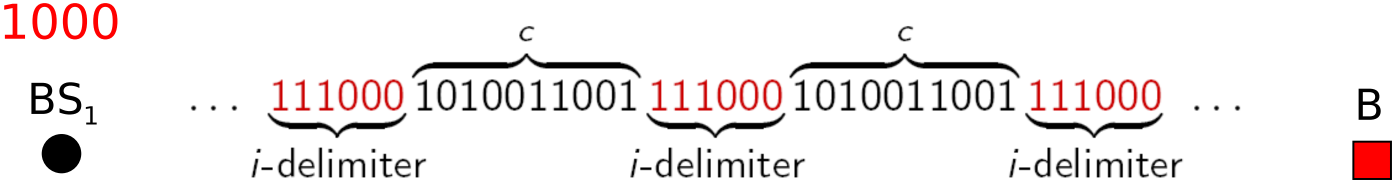
$$\underbrace{R(t)}_{\text{receiver}} = \underbrace{\cos(\omega_0 t + \Phi)}_{\text{sender}} - \underbrace{\cos(\omega_0 t - \Theta)}_{\text{adversary}}, \quad \Phi \in_U [0, 2\pi)$$



$$\mathbb{P}\left[K_{\text{attenuated}} \leq K_\varepsilon\right] \geq 1 - \varepsilon$$

IC: Synchronization via Incongruous (i) Delimiters

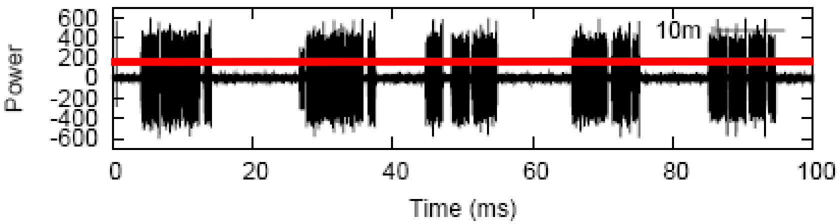
- Receiver does not have to know the length of the message in advance.
- "Correct" code, received between two subsequent i-delimiters is authentic.
- For Manchester coding, an optimal integrity-delimiter is simply 111000



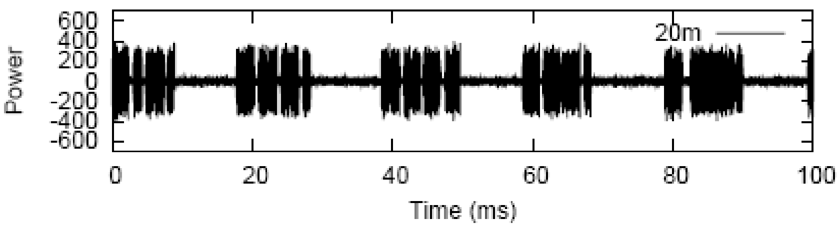
- "111000" cannot be a part of any codeword.

Implementation

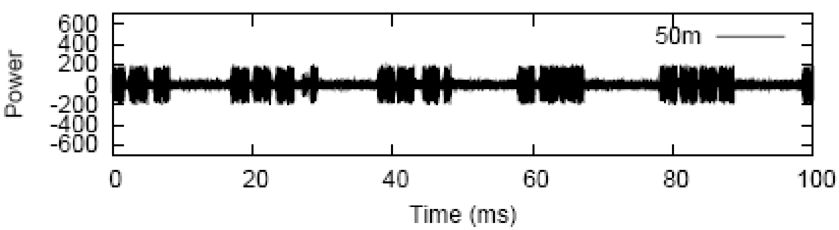
10m



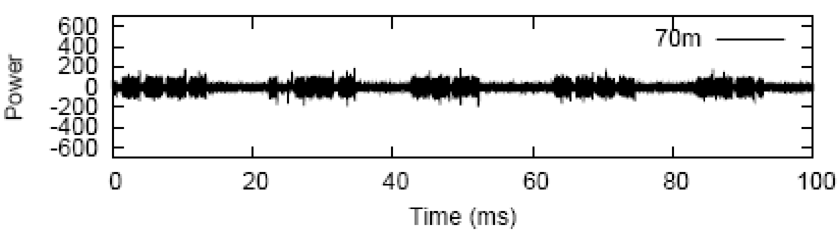
20m



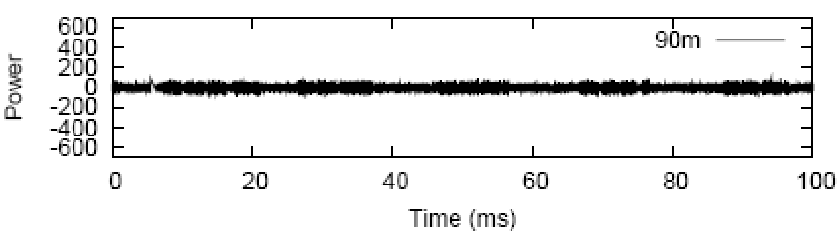
50m

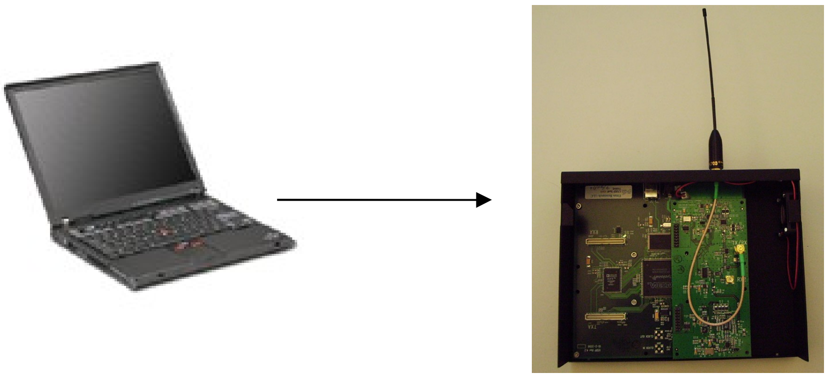


70m



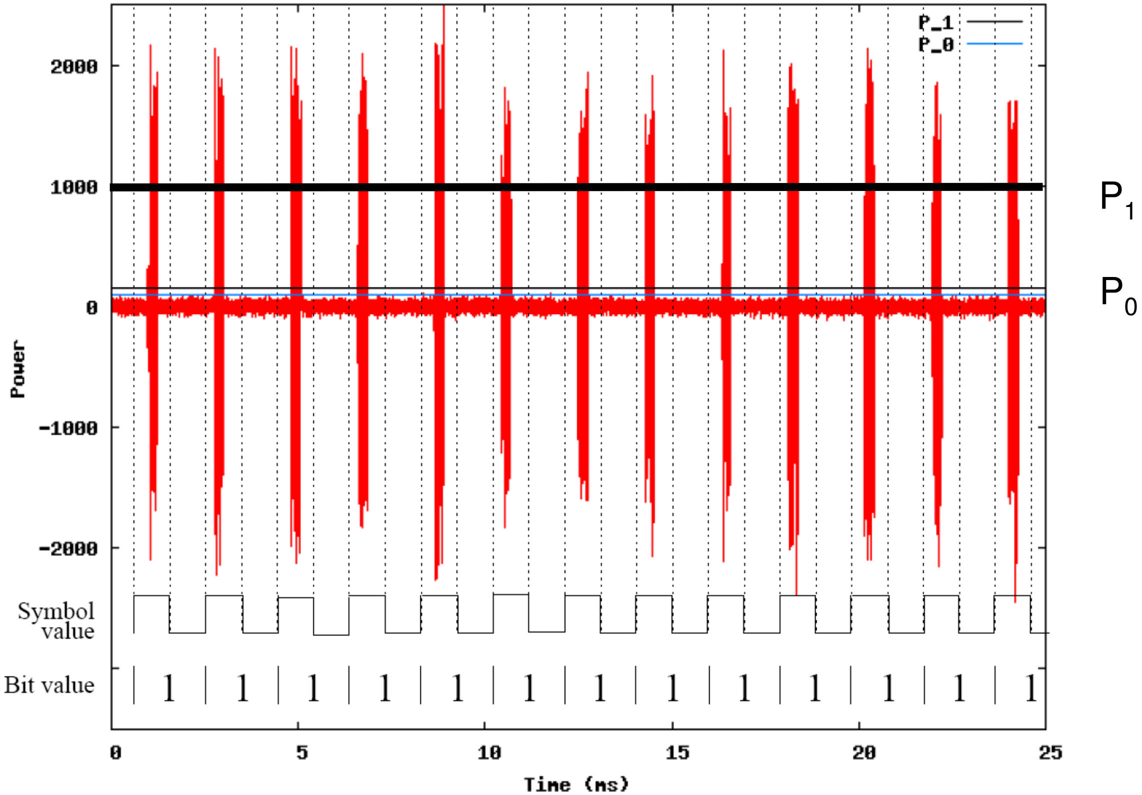
90m





SecNav: Navigation Message Rate

- With 802.11-based implementation: 500b/s
- With custom-built devices (433 MHz, Atmel): 20kb/s
- Clock Synchronization
  - theoretically O(ns) (signal cannot be shifted by the attacker)
  - with low-cost and off-the-self implementations O(μ s)



Integrity Coding: Summary

BS

- sends Integrity-coded messages (e.g., localization beacons or time-synchronization timestamps) on a designated channel

Node/User

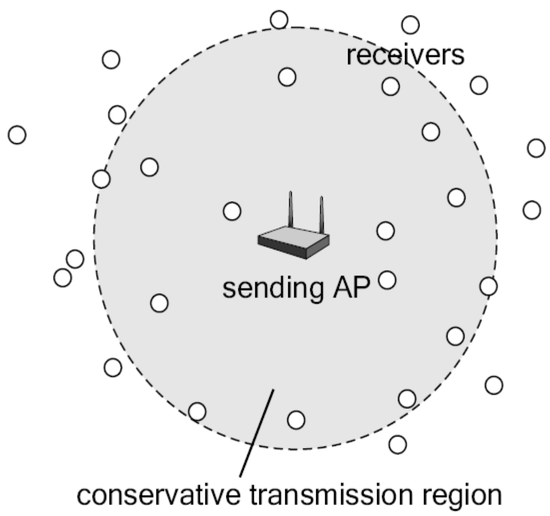
- knows the coverage area
- is aware of its presence in the covered area (e.g., ETHZ campus)

Attacks

- Overshadowing results in all 1s being received => incorrect H(m)
- Jamming results in all 1s being received => incorrect H(m)
- Replay results in an incorrect H(m)

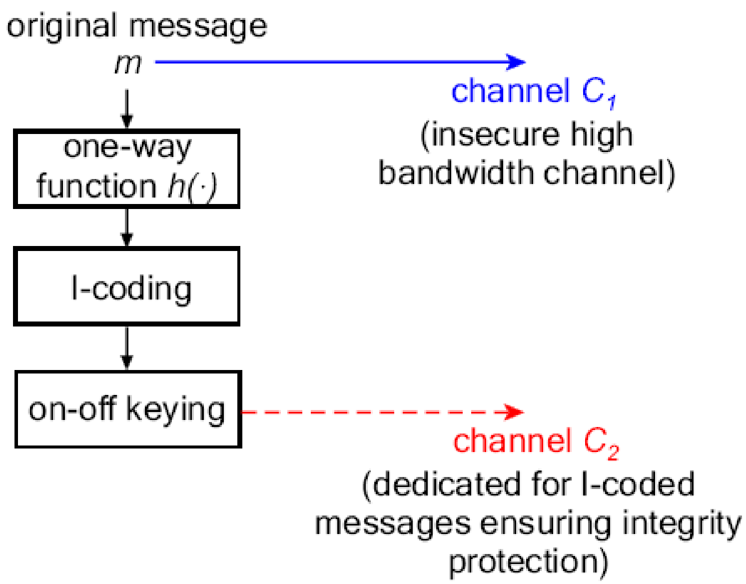
Benefit

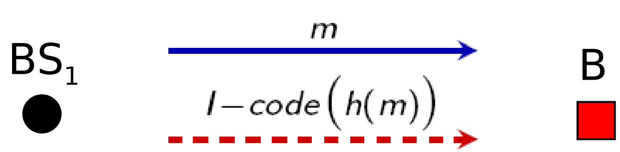
- Broadcast authentication and message integrity protection through presence awareness



Optimization

- Coping with the low-throughput of the Integrity(I-coded) channel
  - similar to the use of digital signatures *sig(h(m))*





Optimal Message Authenticator

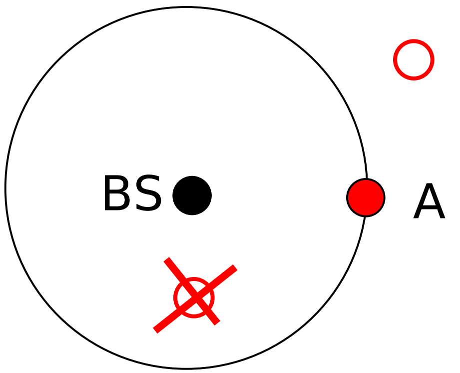
- Hash functions are time-variant (e.g., 160b)
- Need for a flexible, time-invariant solution

BS_1		Bob
Given m		
Pick $N_A \in_U \{0,1\}^k$		Pick $N_B \in_U \{0,1\}^k$
$(c, d) \leftarrow \mathrm{commit}(m \Vert N_A)$		
	$\xrightarrow{c}$	
	$\xleftarrow{N_B}$	
$s_A \leftarrow N_A \oplus \widehat{N}_B$	$\xrightarrow{d}$	$\widehat{m} \Vert \widehat{N}_A \leftarrow \mathrm{open}(\widehat{c}, \widehat{d})$
	$\xrightarrow{s_A}$	$s_B \leftarrow N_B \oplus \widehat{N}_A$
		If $s_A = s_B$, "Accept" $\widehat{m}$

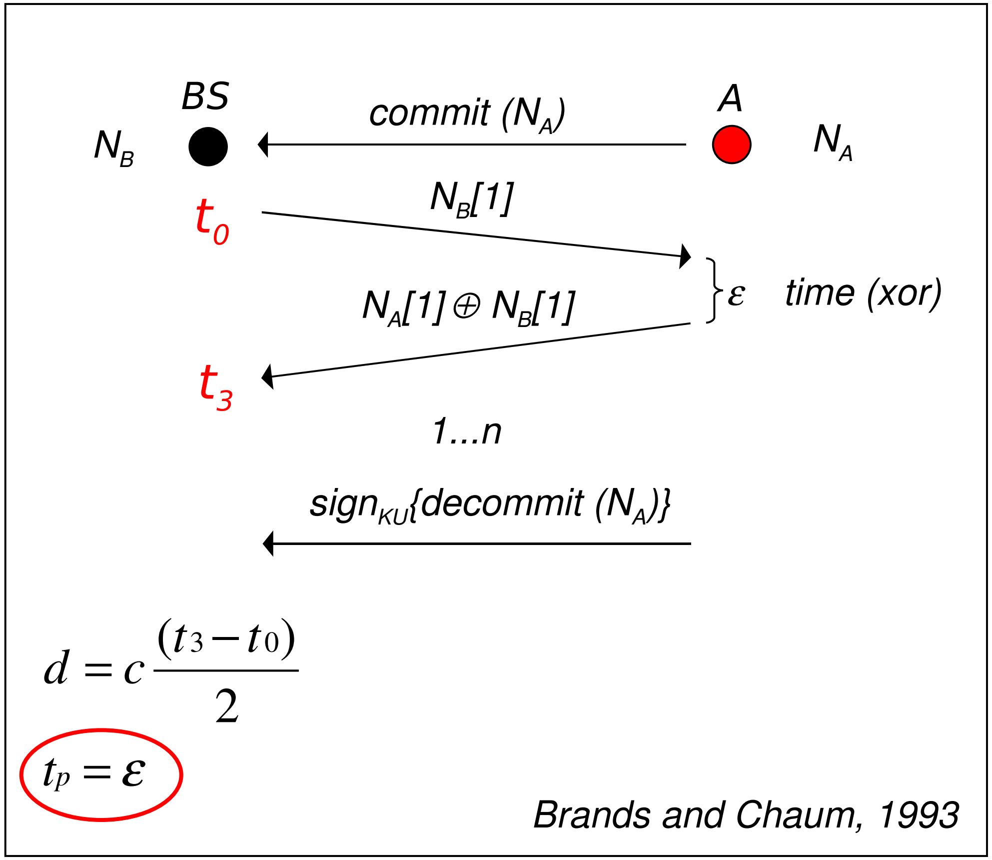
- s_A transmitted using I-codes
- free choince of size of s_A (security depends on $|s_A|$)
- time-invariant

Integrity-regions: authentication through attackers absence awareness

Example: Distance bounding (Verification)

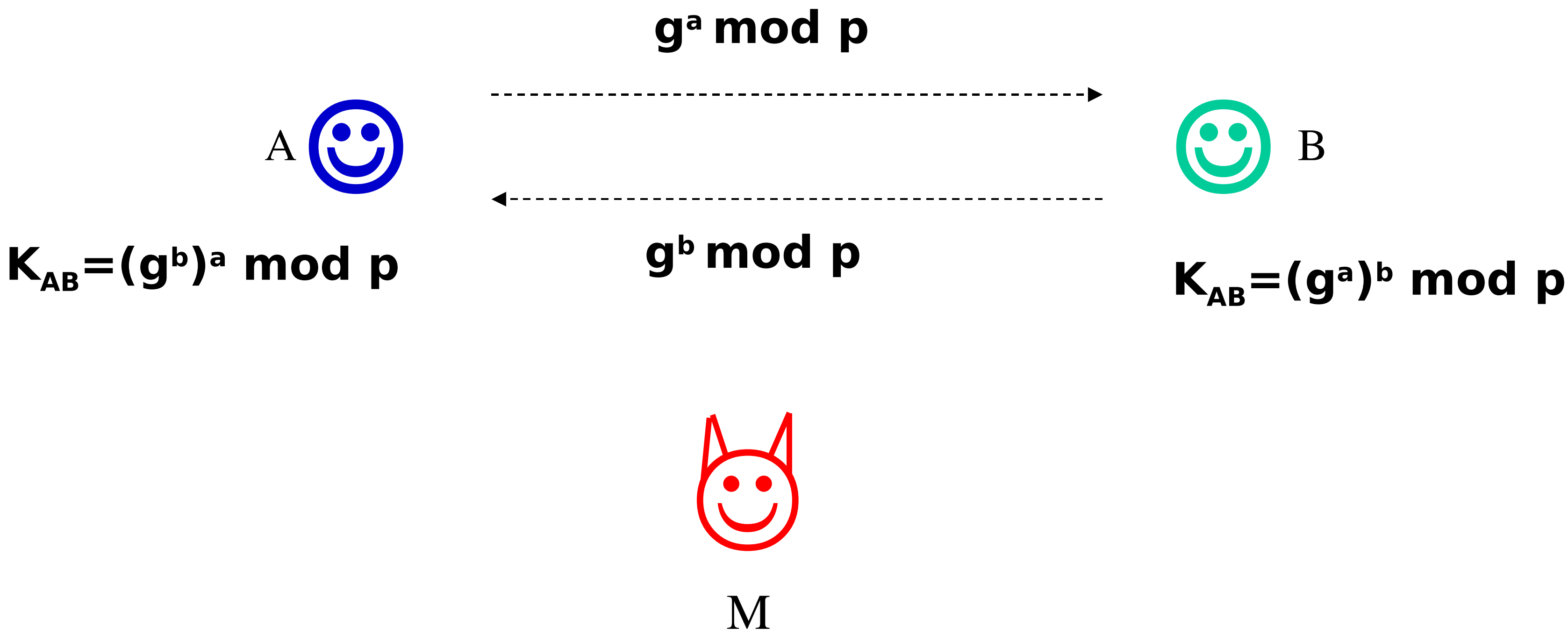


A node cannot pretend to be closer than it really is, only further !!!

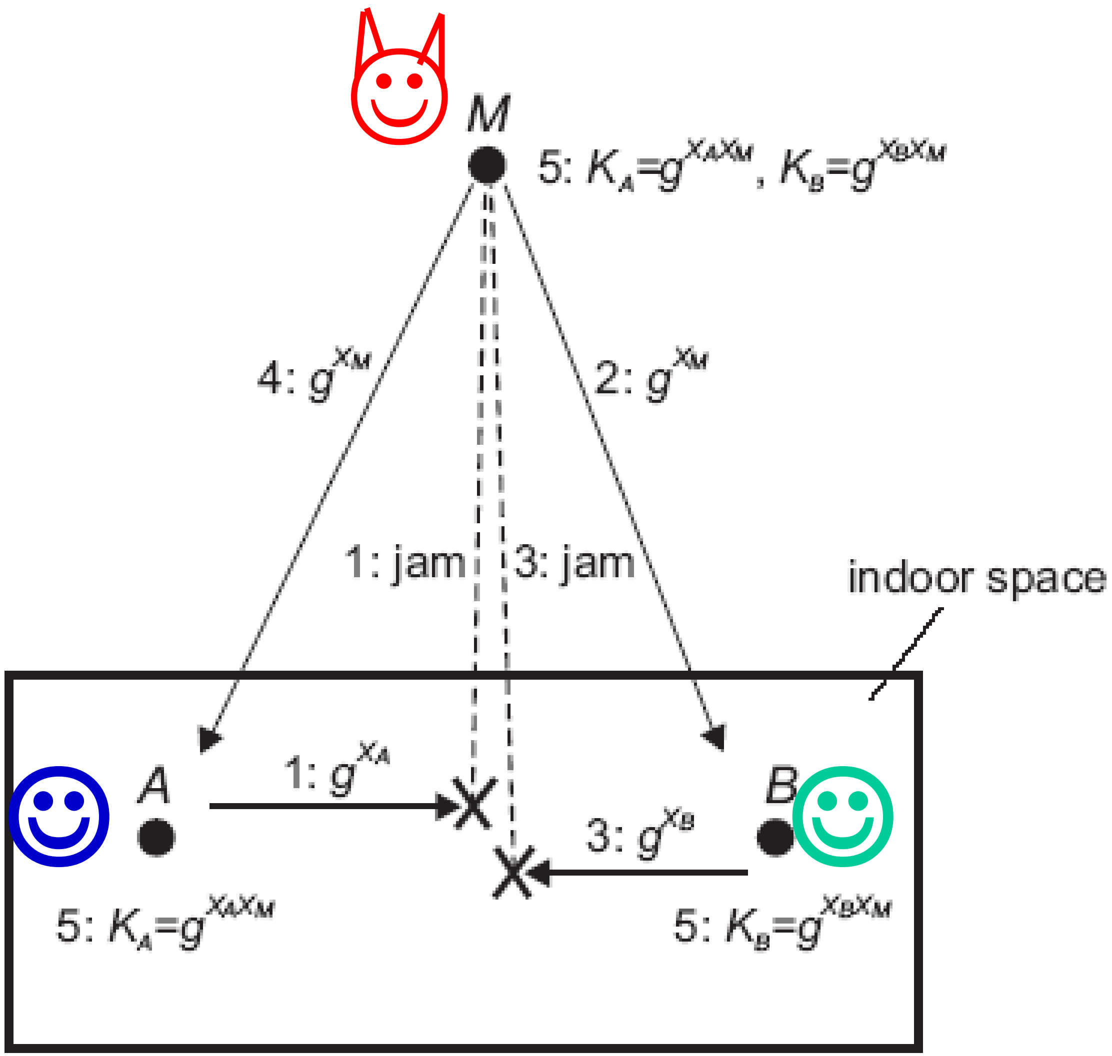


Many variants and implementations followed.

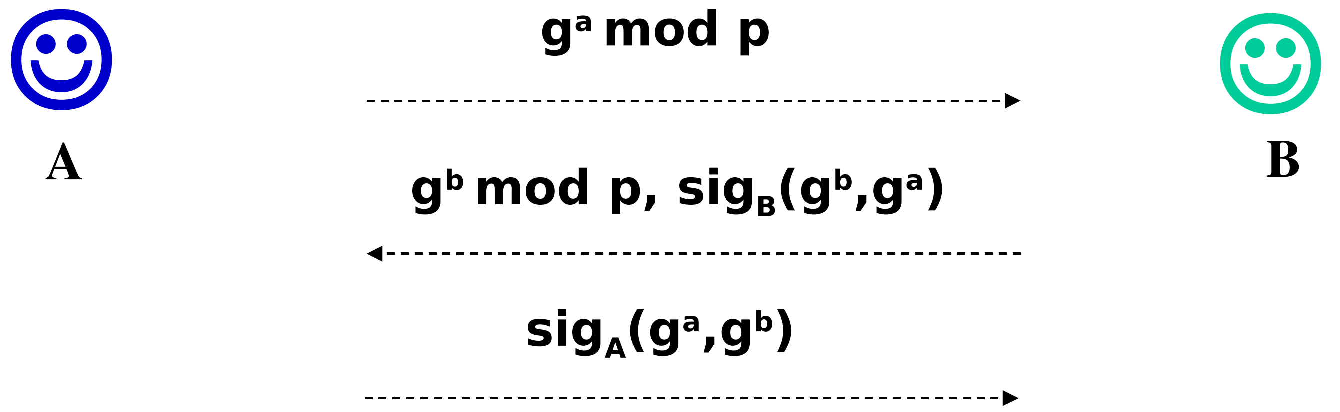
Key establishment – DH



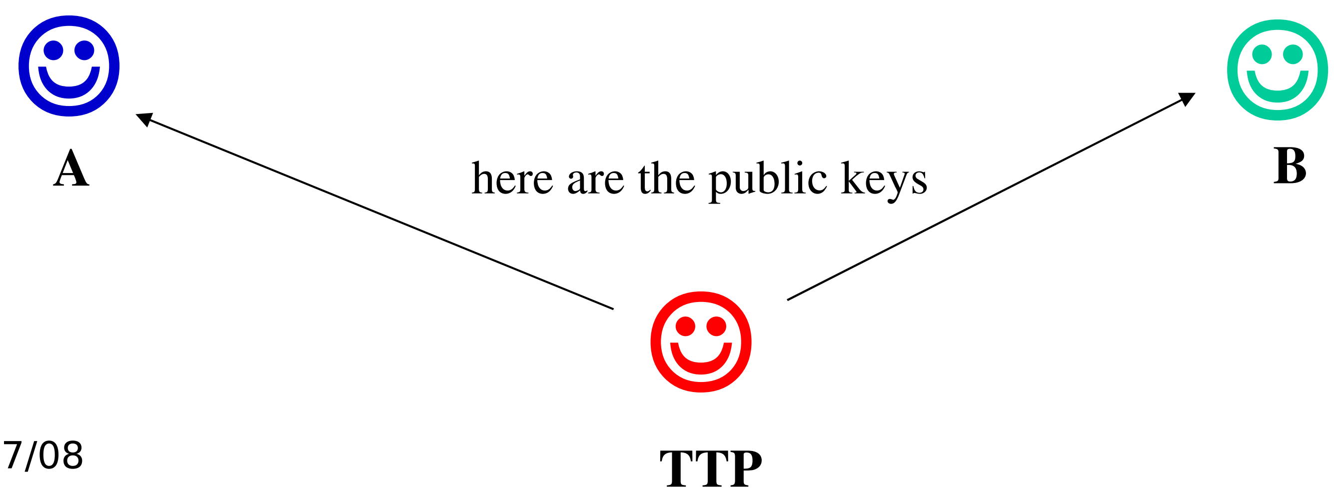
Man in the middle attack



Solution to the MITM: authentication of DH contributions



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



Our goal: avoiding certificates

☺ A

g^a mod p

g^b mod p

☺ B

Visual recognition, conscious establishment of keys

☺ A

☺ B

h(g^a)

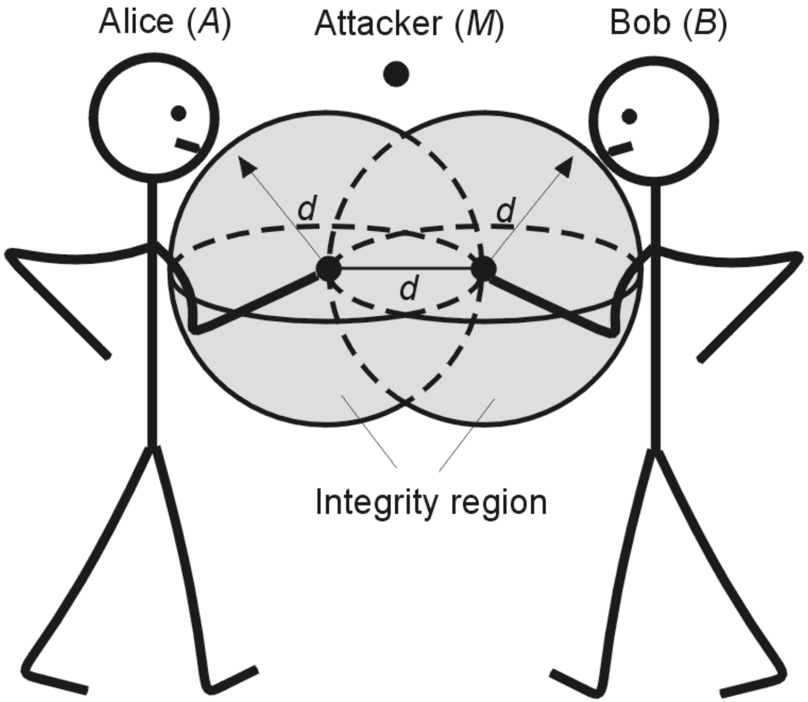
h(g^b)

Existing solutions

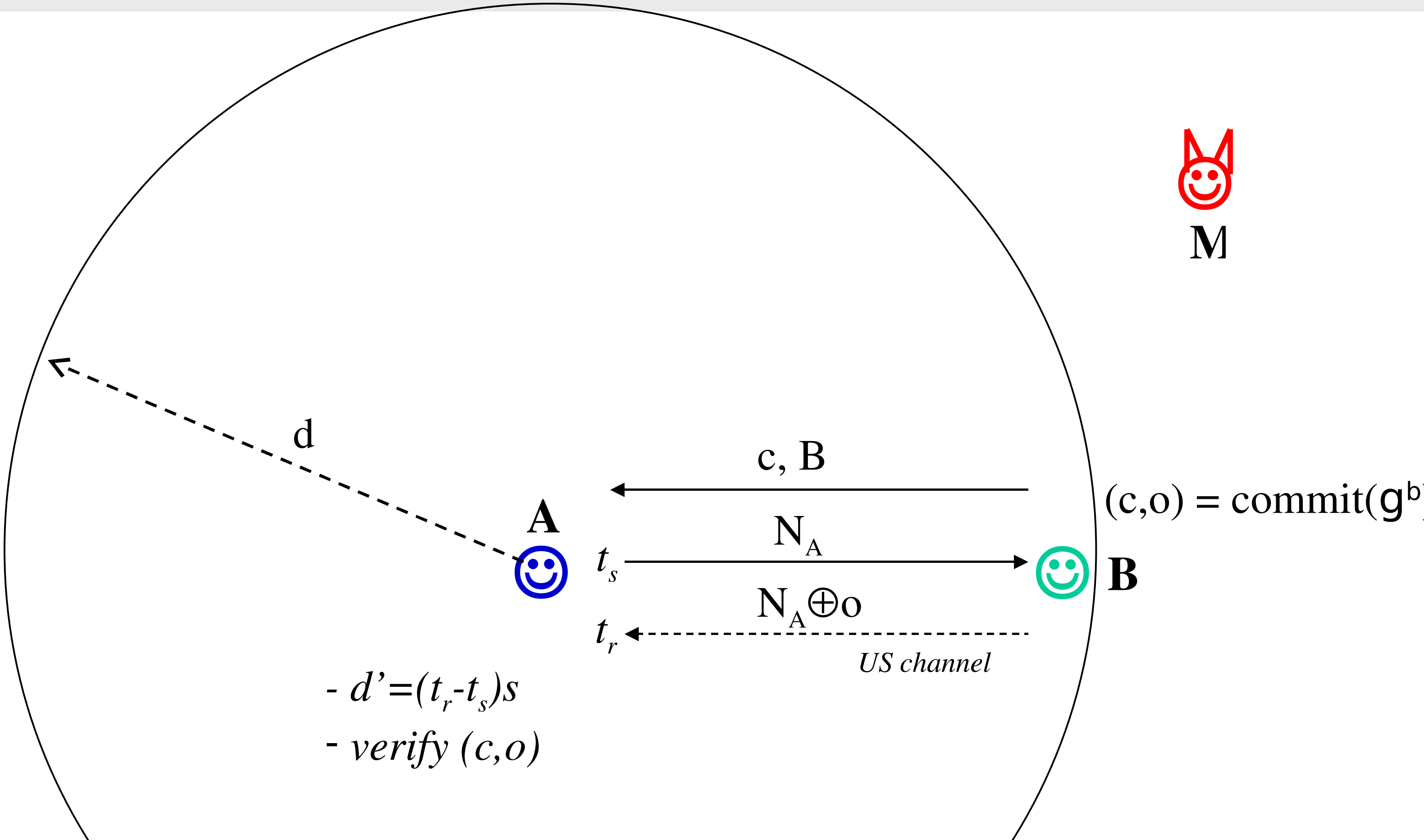
- Stajano and Anderson propose the *resurrecting duckling* security policy model **(physical contact)**
- Balfanz et al. *location-limited channel* (e.g., **an infrared link**)
- Asokan and Ginzboorg propose a solution based on **a shared password**
- Perrig and Song, hash visualization **(image comparison)**
- Maher presents several methods to verify DH public parameters **(short string comparison)**, found flawed by Jakobsson
- Jakobsson and Larsson proposed two solutions to derive a strong key from a **shared weak key**
- Dohrmann and Ellison propose a method for key verification that is similar to DH-SC **(short word comparison)**
- Gehrmann et al., (**short string comparison)**
- Cagalj et al. **(short string comparison (1/2 string size))**
- Capkun, et al. key establishment for self-organized mobile networks (**IR channel, mobility**)
- Castellucia, Mutaf (**device signal indistinguishability**)
- Cagalj, Capkun, Hubaux, **distance-based verification, channel anti-blocking**
- Cagalj, Capkun, **Integrity-codes (awarness of presence)**

From Distance Verification to Message Auth. (I)

- Main idea:
  - bind messages to distances &
  - keep your friends close
- Authentication through (attacker) absence awareness
  - No reliance on propagation assumptions



Integrity region protocol

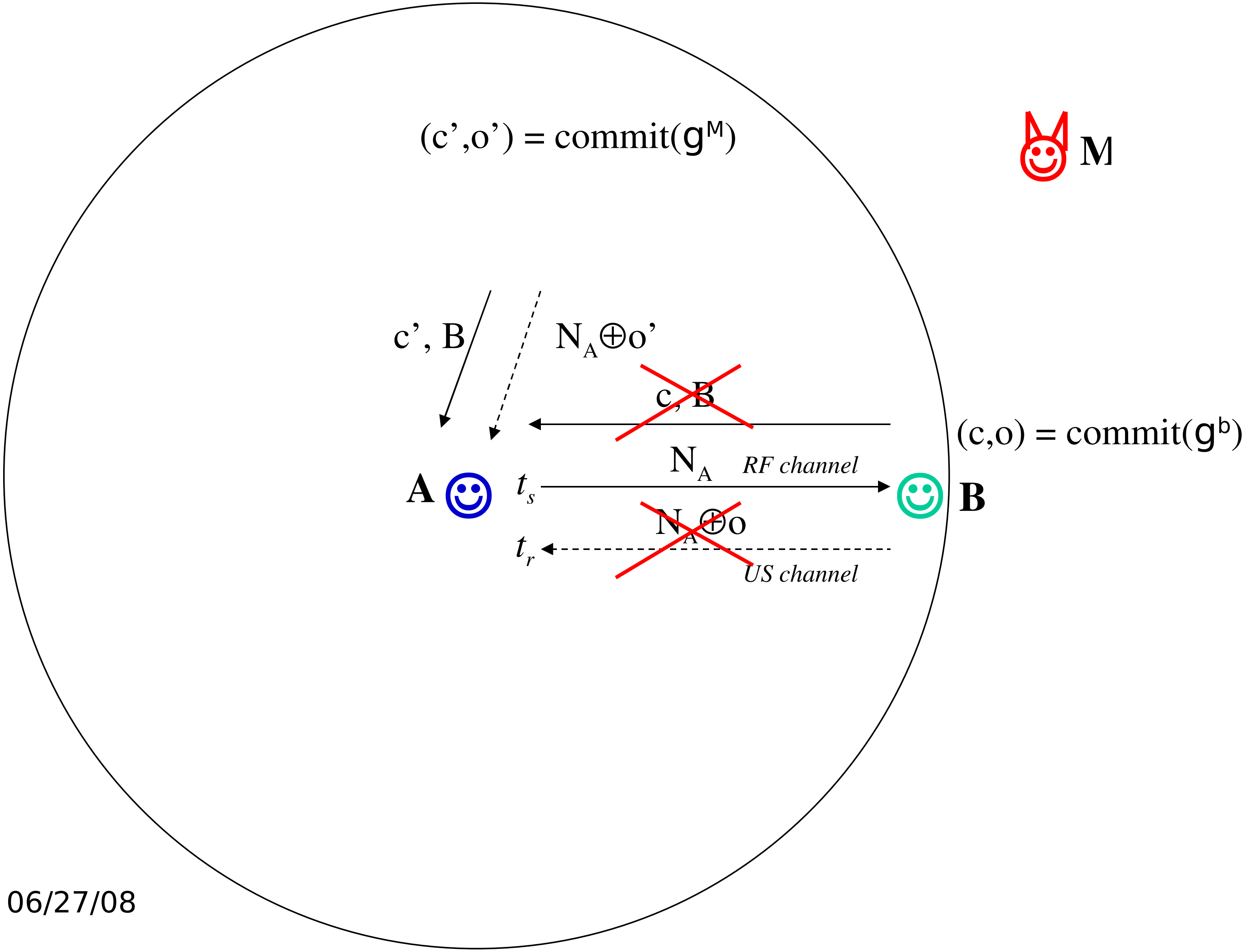


A:

1) **Verify** that the measured distance ***d'*** is within its (A's) integrity region ***d***.
2) **Verify** (e.g., visually) that there are **no devices** at any distance d'‘≤ d'
   (i.e., closer to A than B is).

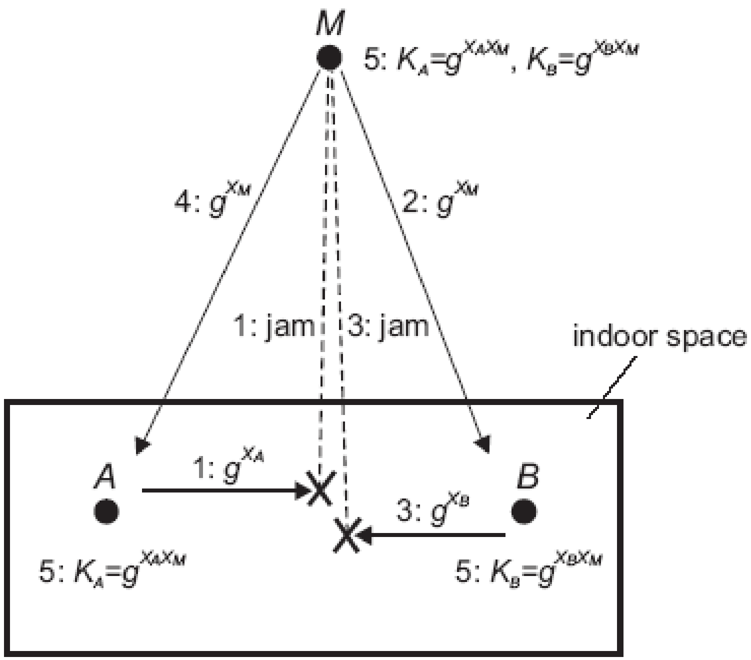
If the two verifications pass, A accepts that message g^b was generated by B and was not altered in transmission.

Short analysis of the implementation with US distance-bounding

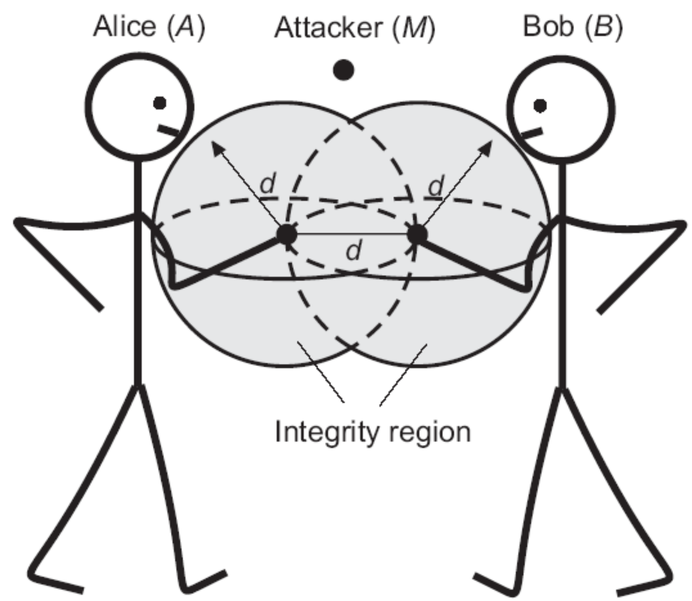


Main consequence of Integrity regions

- Forcing the attacker to be physically close to the devices to perform the MITM attack.

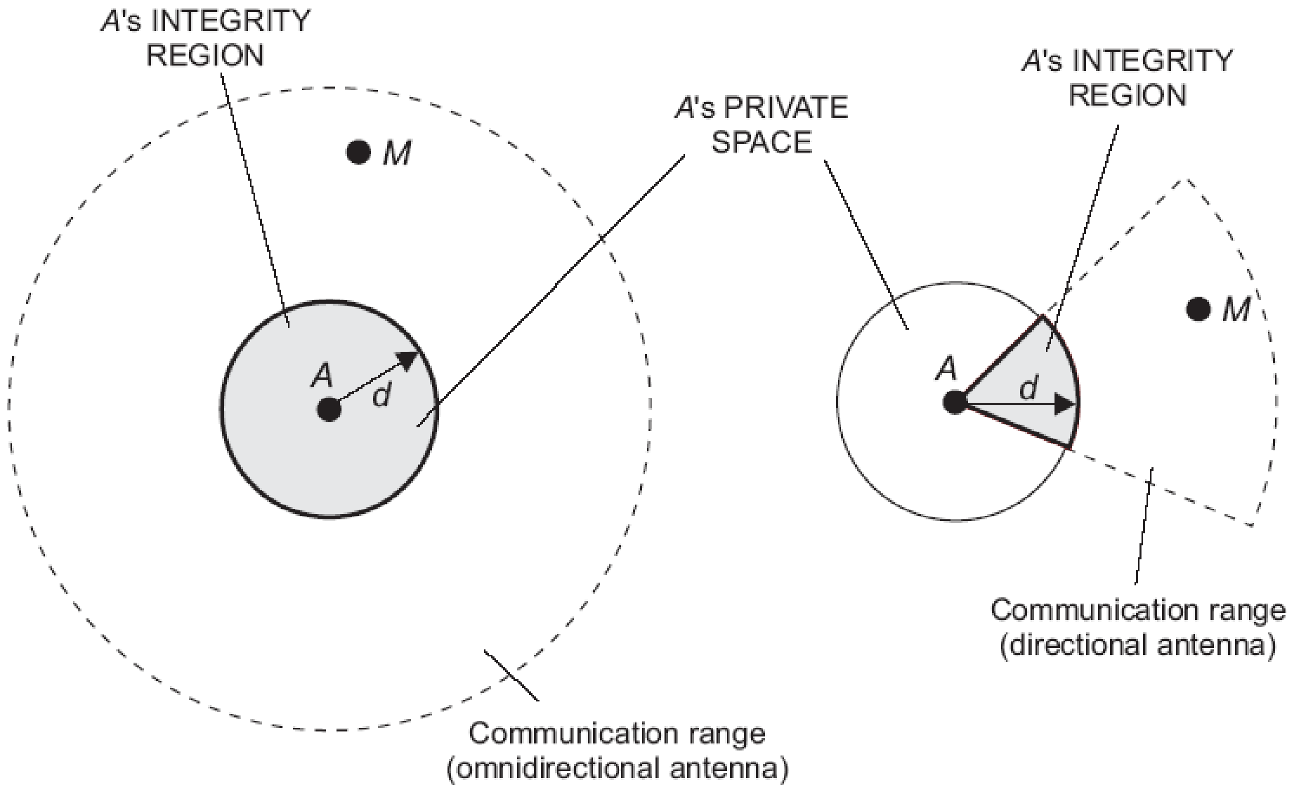


without integrity regions



with integrity regions

Integrity-regions with (omni)directional antennas



Summary/future work

- Physical presence of the attacker (i.e., the attacker cannot be omnipresent (physically))
- Honest devices (users) can have an awareness of presence (distance, space, surrounding devices)

References

- Brands, Chaum, Distance Bounding Protocols, Eurocrypt '93
- Capkun, Cagalj, Integrity Regions: Authentication Through Presence in Wireless Networks, WiSe'06
- Capkun, Cagalj et al., Integrity Codes: Message Integrity Protection and Authentication Over Insecure Channels, S&P(Oakland)'06, TDSC'08
- Key Establishment in P2P Networks, Cagalj, Capkun, Hubaux, Proc. of IEEE, 2006
- Tippenhauer, Rasmussen, Pöpper, Capkun, iPhone and iPod Location Spoofing: Attacks on Public WLAN-based Positioning Systems, Tr ETHZ'08
- http://www.syssec.ch/press/location-spoofing-attacks-on-the-iphone-and-ipod