Wireless Security gets <u>Physical</u>

Srdjan Čapkun

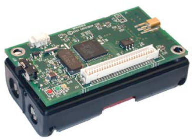
Department of Computer Science
ETH Zürich

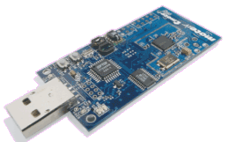
22.03.2009

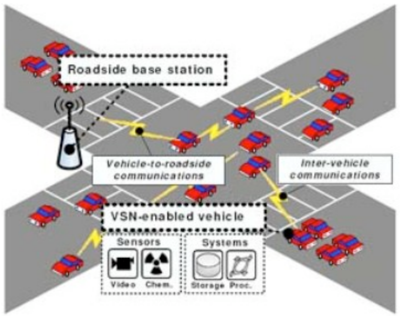
Age of wireless communication ...

- 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







What changed

- 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

Relevant problems

- Secure Localization
- Jamming-resistant Communication
- Device Identification
- Secure Time Synchronization
- Authentication / Pairing

Secure Localization

Secure localization

User's perspective: to obtain a correct information about its own location

Infrastructure perspective: to obtain a correct information about the location of a device

Secure localization goals

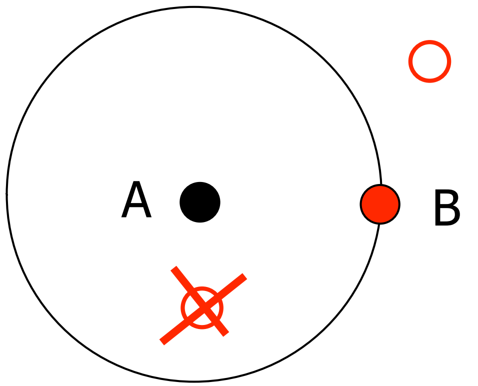
- Compute the correct location of a trusted device in the presence of adversaries
- Compute the correct location of an untrusted device *(that wants to be localized, e.g., for access)*

Why traditional security primitives do not help?

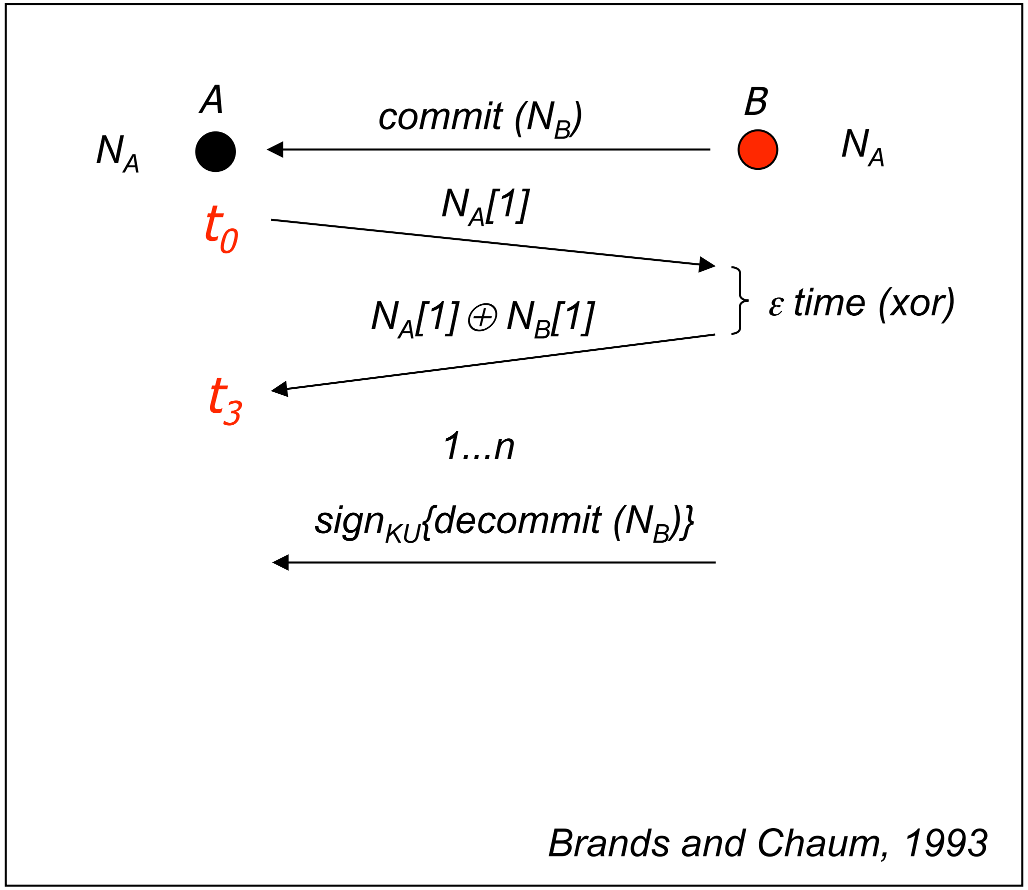
- Confidentiality (using e.g., Encryption)
  - signals are being replayed, delayed, jammed
  - message content is not of relevance for the attacker
- Authentication (using e.g., digital signatures, MACs ...)
  - signals are being replayed, delayed, jammed
  - message origin remains the same (BS)

- We need new security primitives, since attacker
  - Modifies the time of signal arrival and/or
  - Modifies signal characteristics (e.g., RSSI) and/or
  - Introduces/removes signals at/from locations

Example: Distance bounding (Verification)



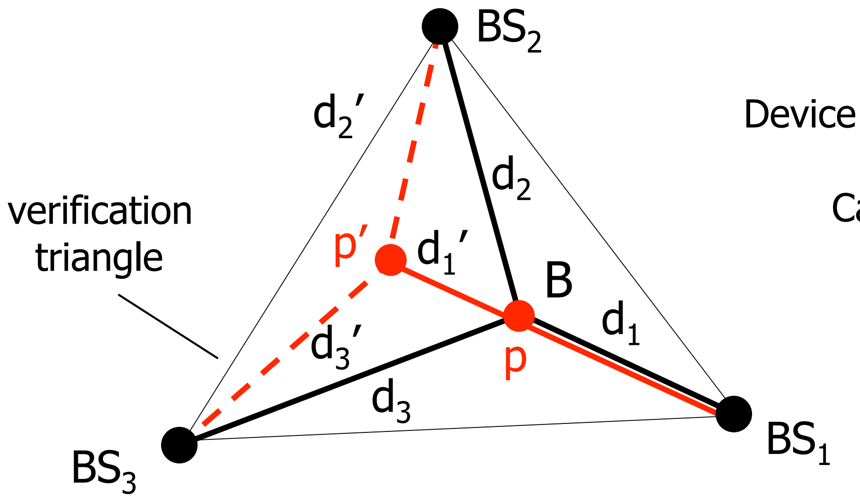
B node cannot pretend to be closer than it really is, only further !!!



Many variants and implementations followed.

From Distance to Location Verification

- Verifiable Multilateration
  - prevent distance reduction attacks (distance bounding)
  - multilateration using distance bounding within a verification triangle



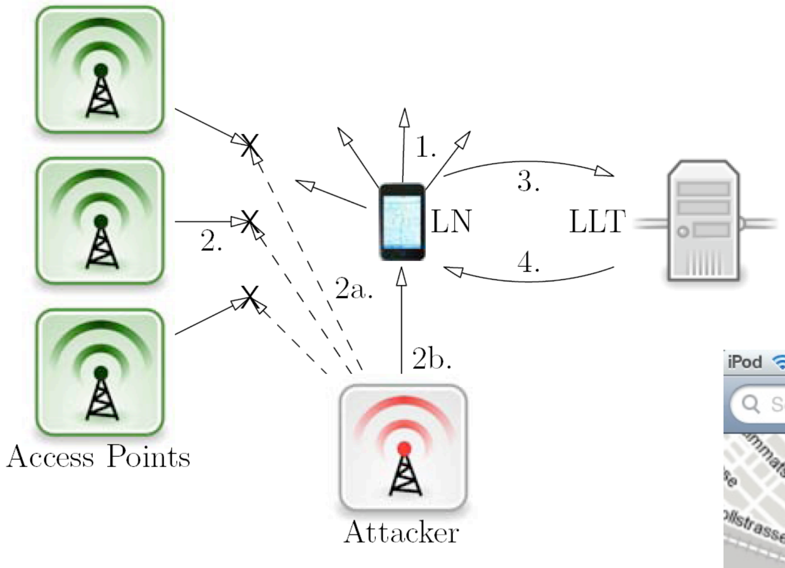
d = distance bound from BS to B

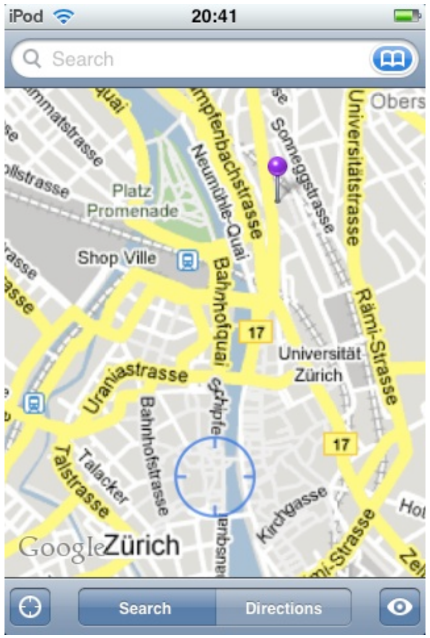
Device cannot cheat on its location within the triangle !!!

Can only pretend to be outside of the triangle.

Example: Attacks on 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, ...

Other approaches

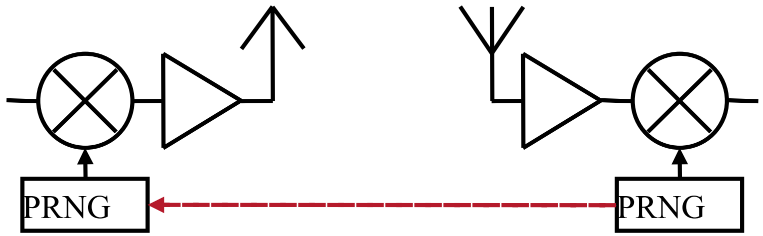
- Location Verification using Hidden / Mobile Stations
- Broadcast Secure Localization
- RSS-based Secure Localization
- UWB-based Systems
- …

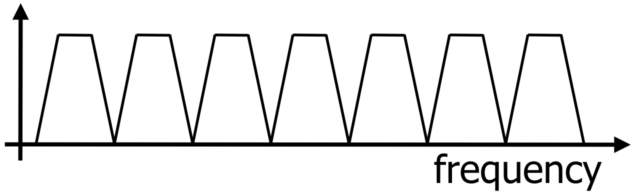
http://www.syssec.ethz.ch

Anti-Jamming Broadcast and Key Establishment

Anti-jamming Techniques

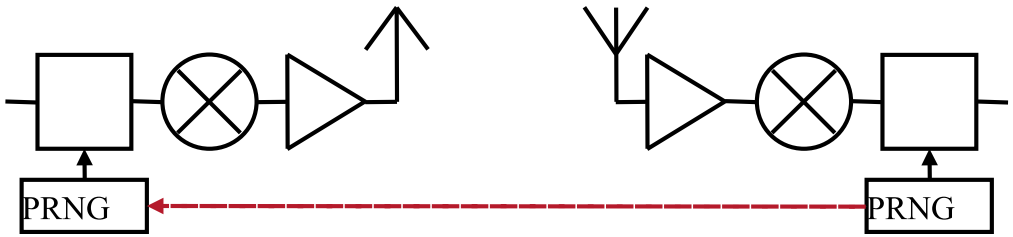
- FHSS: Frequency Hopping Spread Spectrum

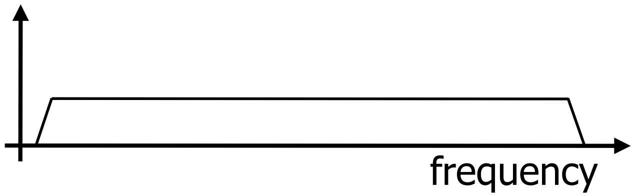




Hopping sequence (PRNG seed) must be known to the sender and receiver but not the jammer

- DSSS: Direct Sequence Spread Spectrum



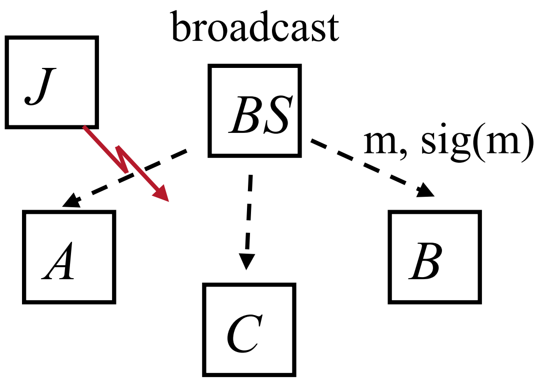


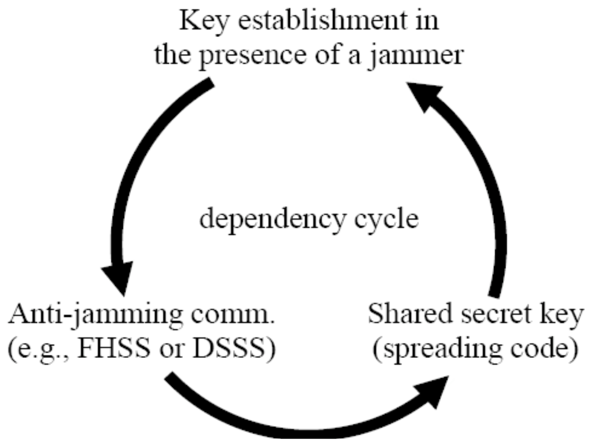
Spreading code (PRNG seed) must be known to the sender and receiver but not the jammer

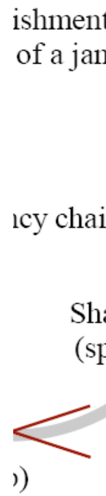
- **Common anti-jamming techniques rely on pre-shared secret codes (keys)**

Anti-jamming broadcast and key establishment

Problem: BS needs to broadcast a message to a large number of unknown receivers in an anti-jamming manner

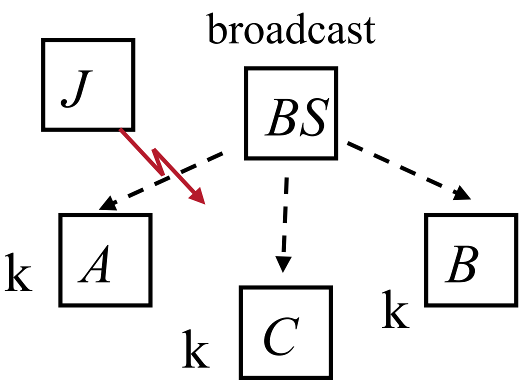






Anti-Jamming techniques rely on shared keys, but broadcasting node cannot share the same key with all recipients => dependency

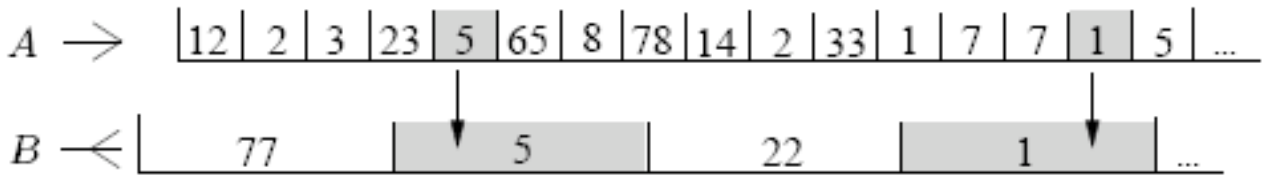
---



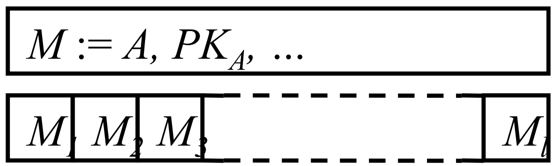
The receivers might be untrusted and/or unknown!

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

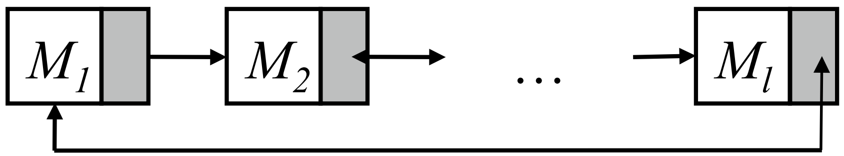
One solution: Uncoordinated Frequency Hopping



Problem: A message might be too long (contains a signature as well)
Solution: Fragment message and transmit each fragment in one slot

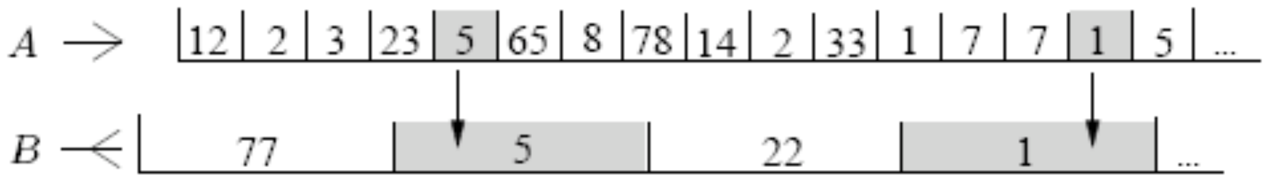


Problem: Fragments are not individually authenticated (poisoning attack)
Attacker might insert its own fragments => computationally infeasible message reconstruction.
Solution: Link fragments (e.g., using hash-links)

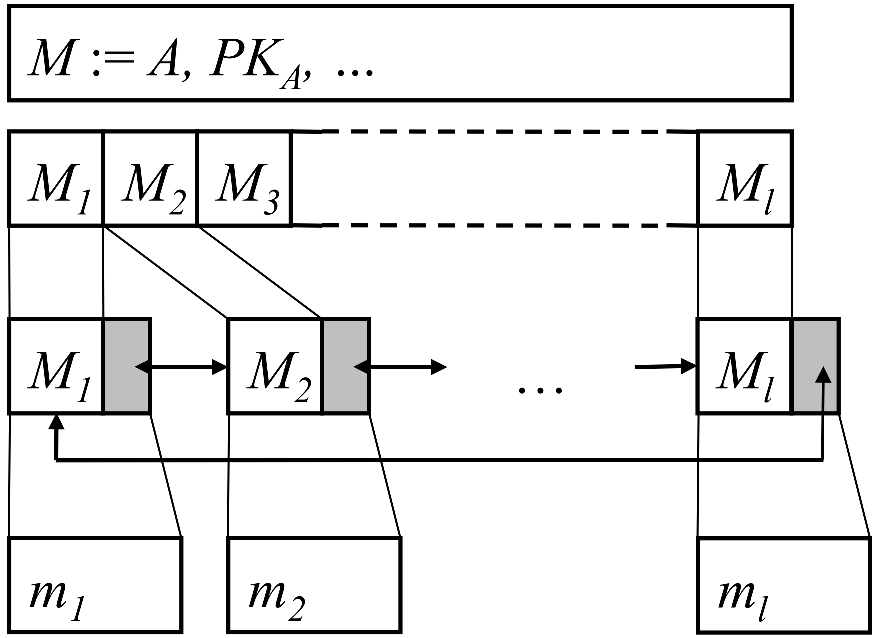


$$h_l := h(m_1),\ h_i := h(m_{i+1} || h_{i+1})$$

Solution: Uncoordinated Frequency Hopping



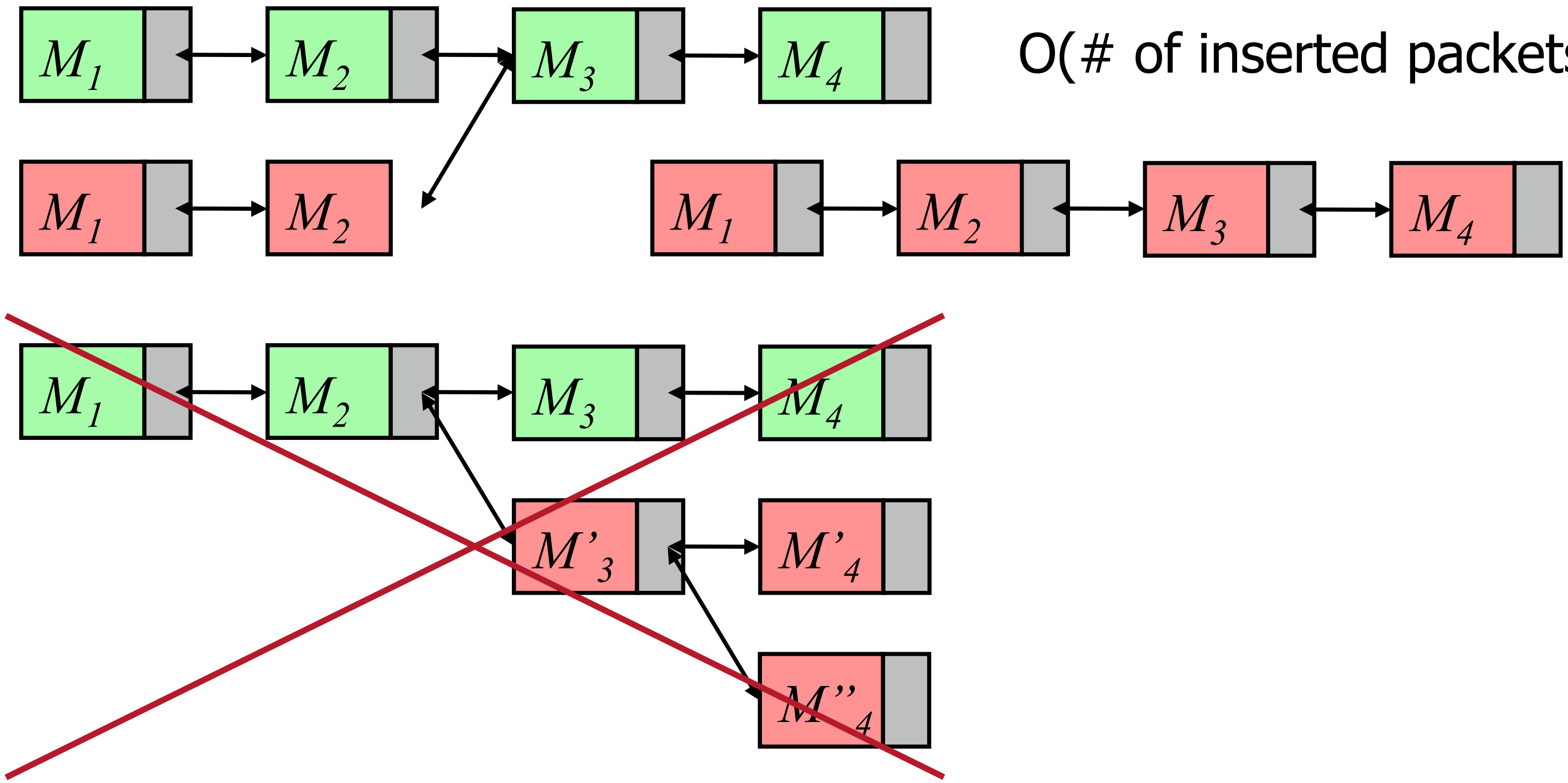
- Fragmentation
- Hash linking
  $h_l := h(m_l),\ h_i := h(m_{i+1}||h_{i+1})$
- Bit coding/interleaving



Other approaches: accumulators, turbo-codes, short signatures, Merkle trees …

UFH: analysis

Uncoordinated Frequency Hopping: brief analysis
insertion/poisoning



O(# of inserted packets)

Cross-layer (DoS on communication and on computation)

Broadcast Anti-jamming Communication: Summary

- Key establishment-anti-jamming dependency cycle
- New solutions break this dependency

- Other ideas:
    - Yvo Desmedt (pre-shared sets of hopping sequences)
    - UDSSS (Uncoordinated Direct Sequence Spread Spectrum)
- Implementations using SDR (0.2-300s latency)

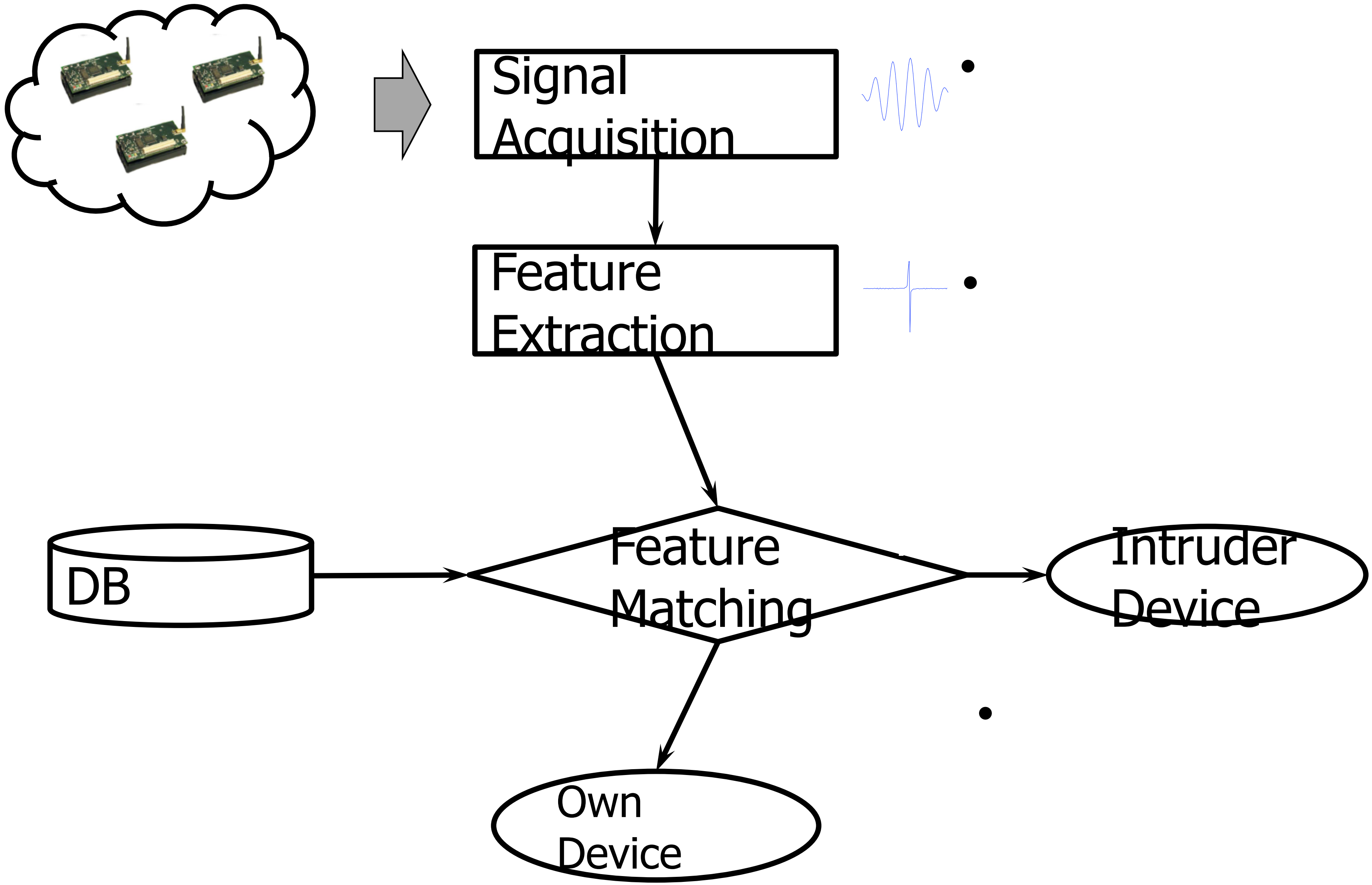
UFH and UDSSS achieve broadcast anti-jamming communication at the expense of the reduced communication throughput.

Device Identification

Motivation

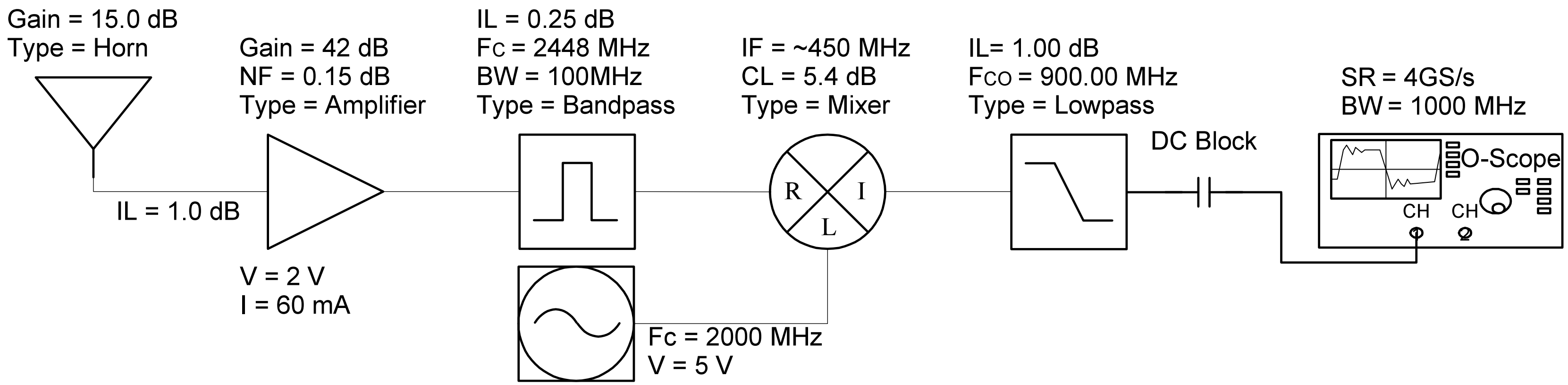
- Reliable identity verification of wireless devices is important.
- Such a task becomes challenging under threats:
  - device identity spoofing
  - device cloning
  - key compromise
- To address the challenge, we explore the physical characteristics of the radio signal for identification.
- These characteristics cannot be easily modified.
- Therefore they present a clear advantage over traditional methods for identity verification.

System Overview

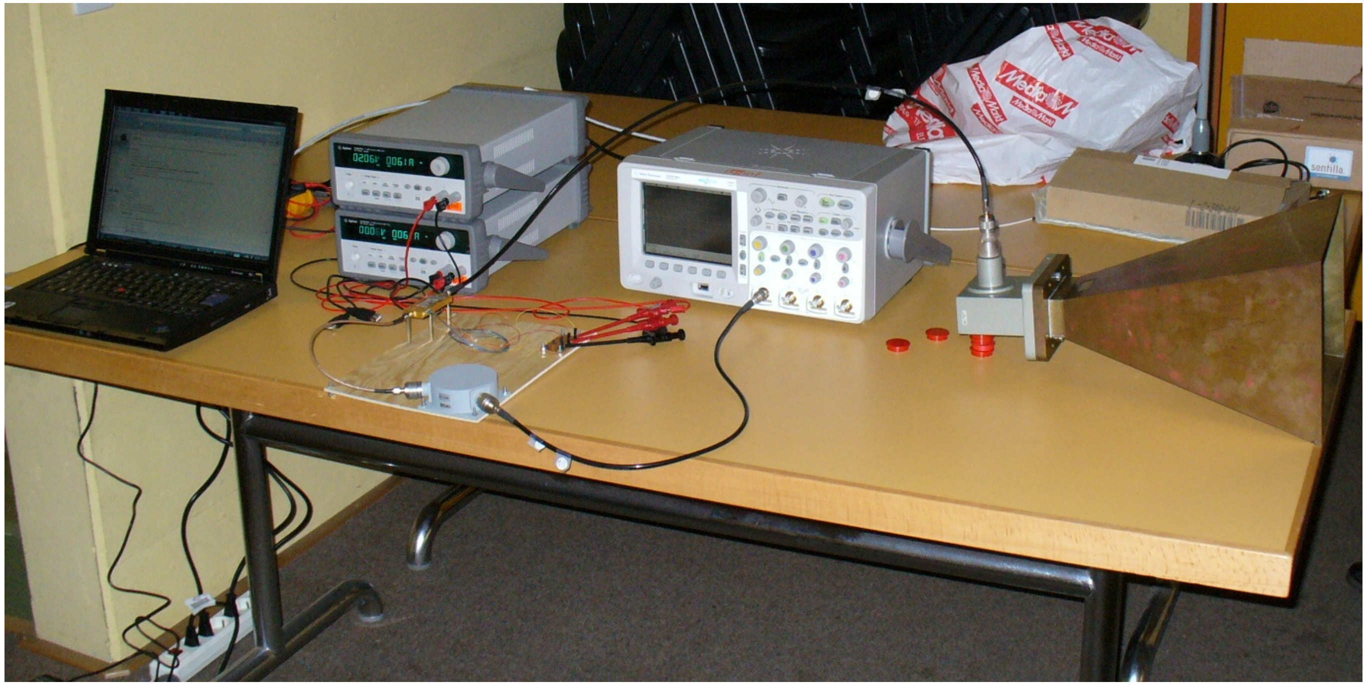


-
-
-
-
-
-
-

Signal Acquisition

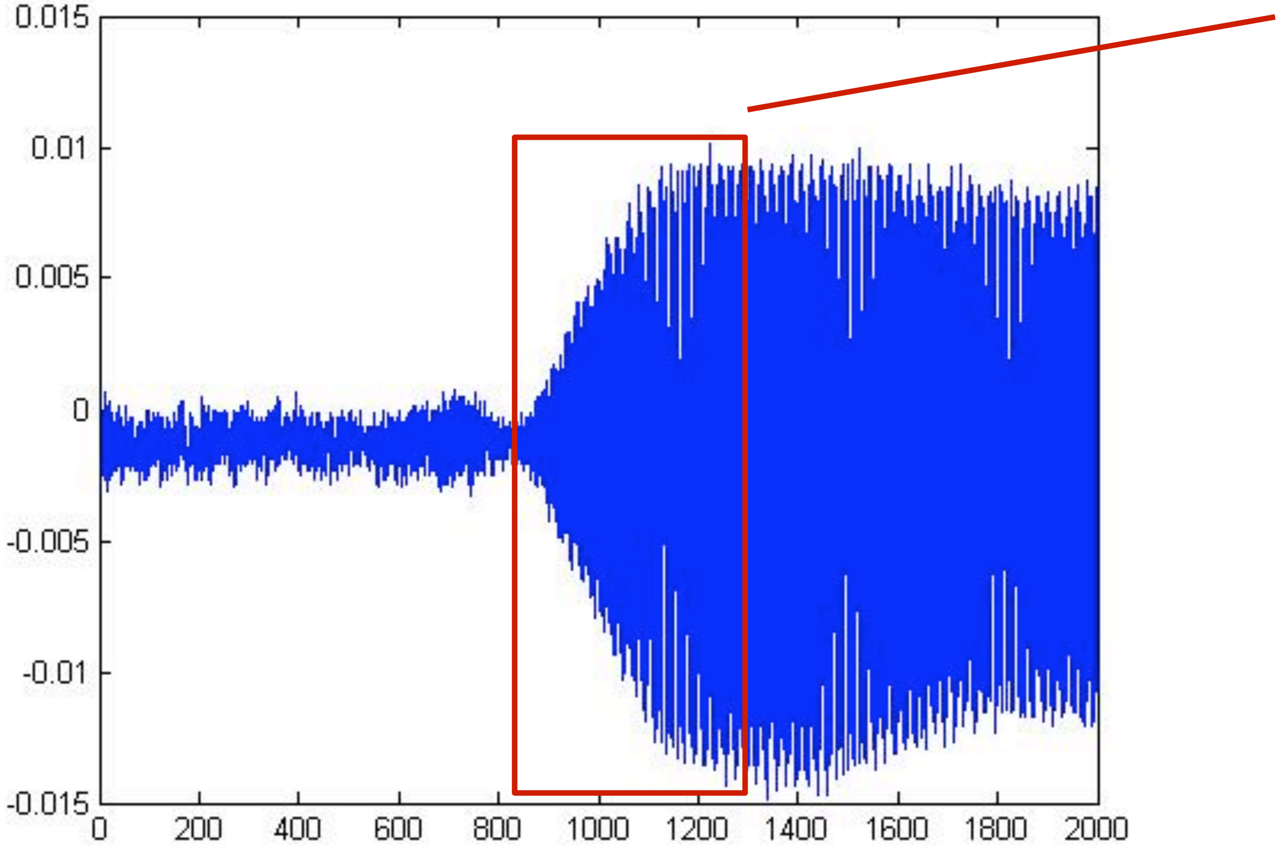


- The Hardware Setup is critical
- Only **high-quality** RF components do the job



Feature Extraction

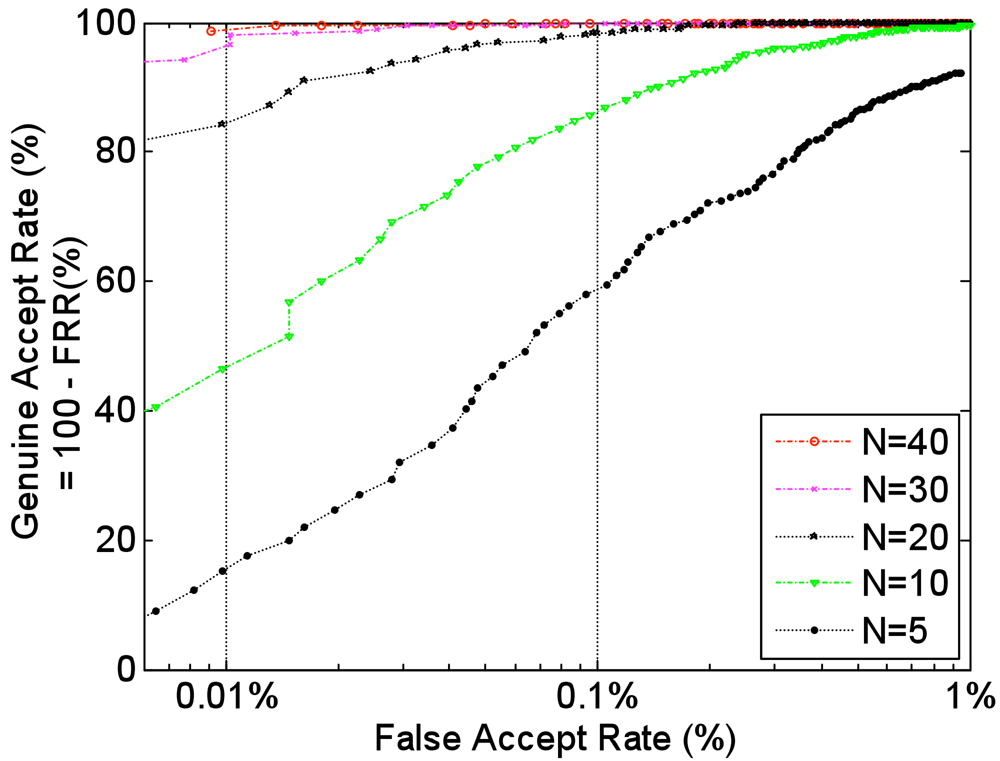
- a ramping up period referred to as transient



Feature Matching Results (1/2)

- 50 identical Tmote Sky sensor nodes, 10 meters
- Equal Error Rate (EER) = 0.0024 (0.24%)
- Accuracy comparable to biometric fingerprint recognition

FAR	FRR	GAR = 1- FRR
0.01%	0.72%	99.28%
0.1%	1%	99%
1%	0%	100%
>1%	0%	100%



Feature Matching Results (2/2)

- Stability over a distance
  - 10 identical Tmote Sky sensor nodes
  - 10 meters vs. 40 meters
  - Accuracy (10 meters) ~ Accuracy (40 meters)

- Stability over voltage supply
  - 2x1.5 AA vs. 2x1.2 NiMH batteries
  - Accuracy is stable

- Stability over antenna polarization
  - 3 different antenna polarizations
  - Only 4 sensors got correctly identified

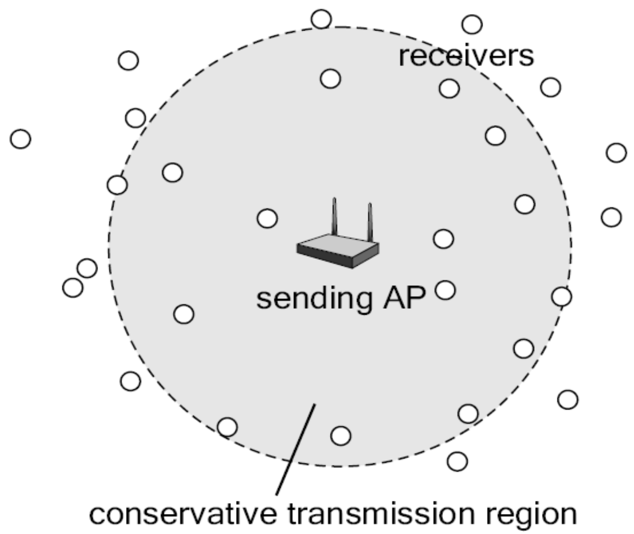
Attacks

- Impersonation attacks
  - Involves recreating the device fingerprint in order to impersonate a targeted device
  - E.g., faked transient signal concatenated with data
- Denial-of-Service attacks
  - Involves preventing a device identification procedure from correctly recognizing the devices
  - E.g., jamming only the transient signal

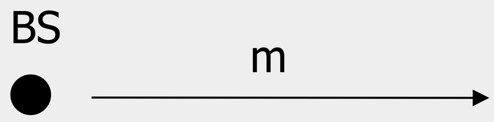
Broadcast Authentication Without Shared Keys

Authentication through presence awareness

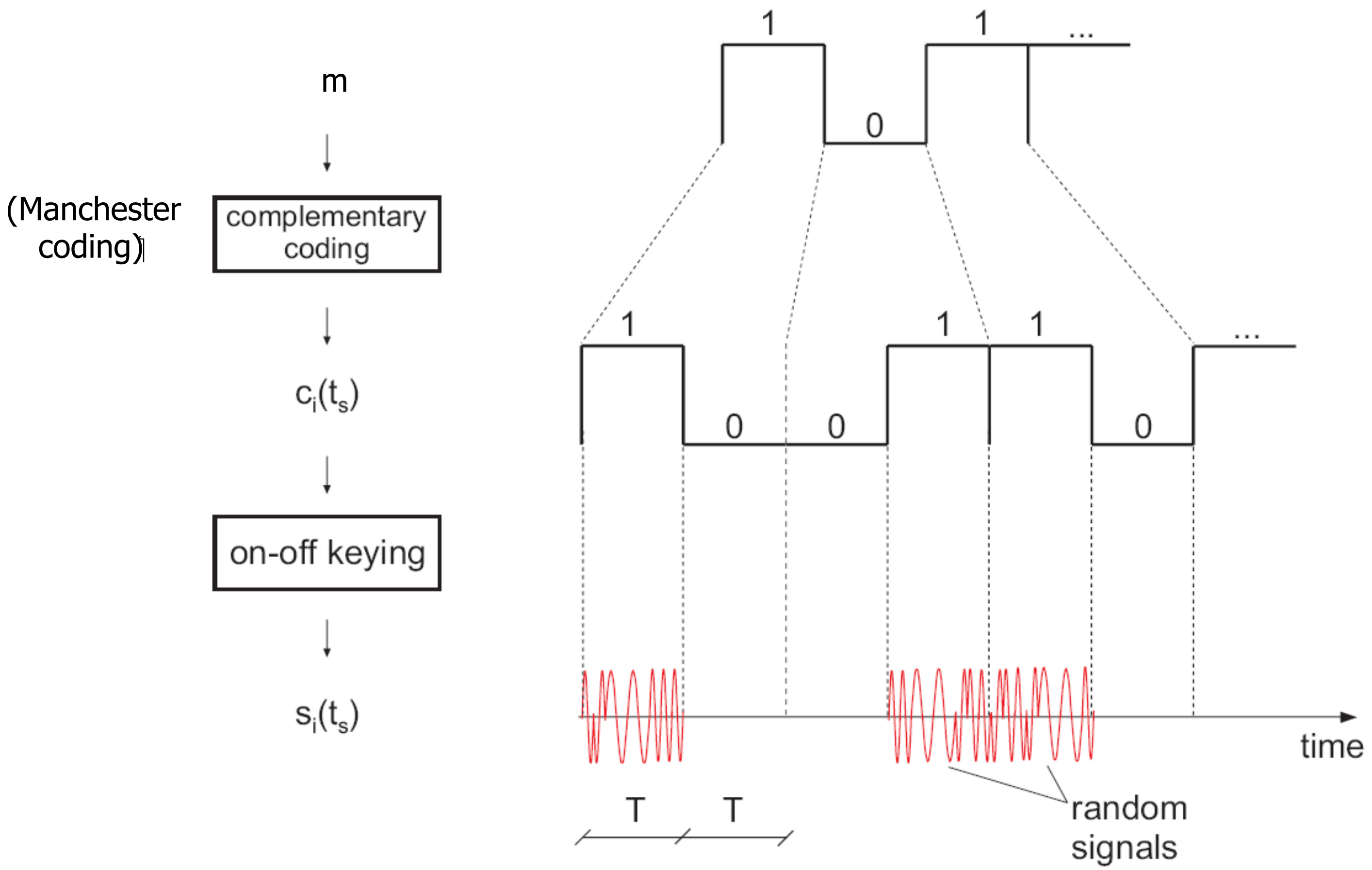
- Problem: How to authenticate messages from a sender with which the receivers do not share keys / hold authentic certificates.
- Main idea:
  - Use special message encoding (Integrity coding)
  - Receiver(s) know that they are in range of the sender (presence awareness)
  - The sender is permanently transmitting (e.g., navigation)



Integrity Coding

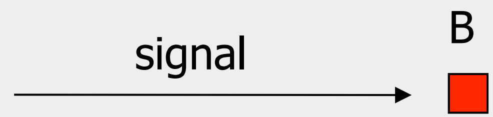


- k-bit Beacon1 spread to 2k bits (1->10, 0->01) (H(m) = k/2)
- transmitted using on-off keying (each "1" is a fresh random signal)

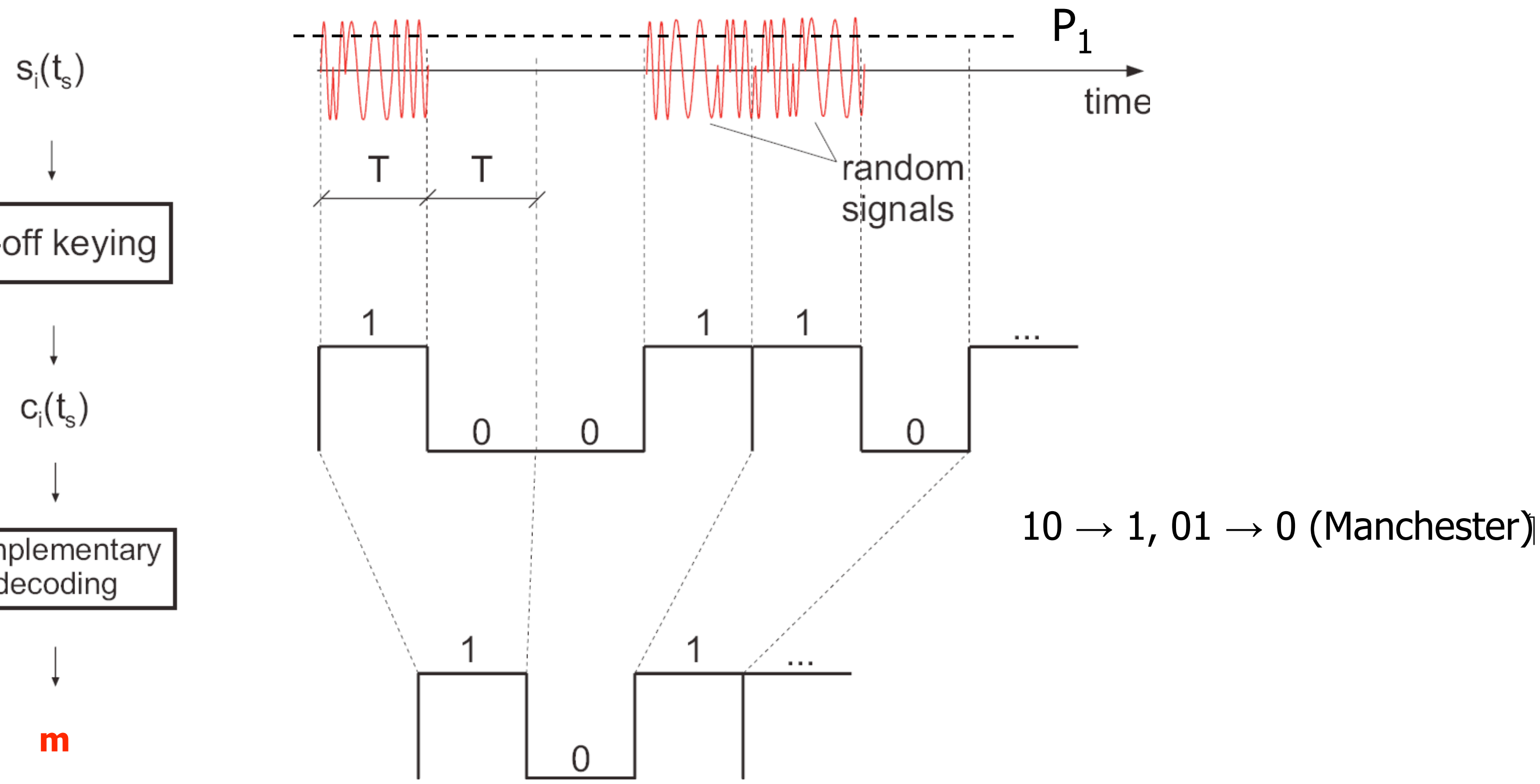


H(m) = the number of bits "1" in m (Hamming weight)

Integrity Decoding

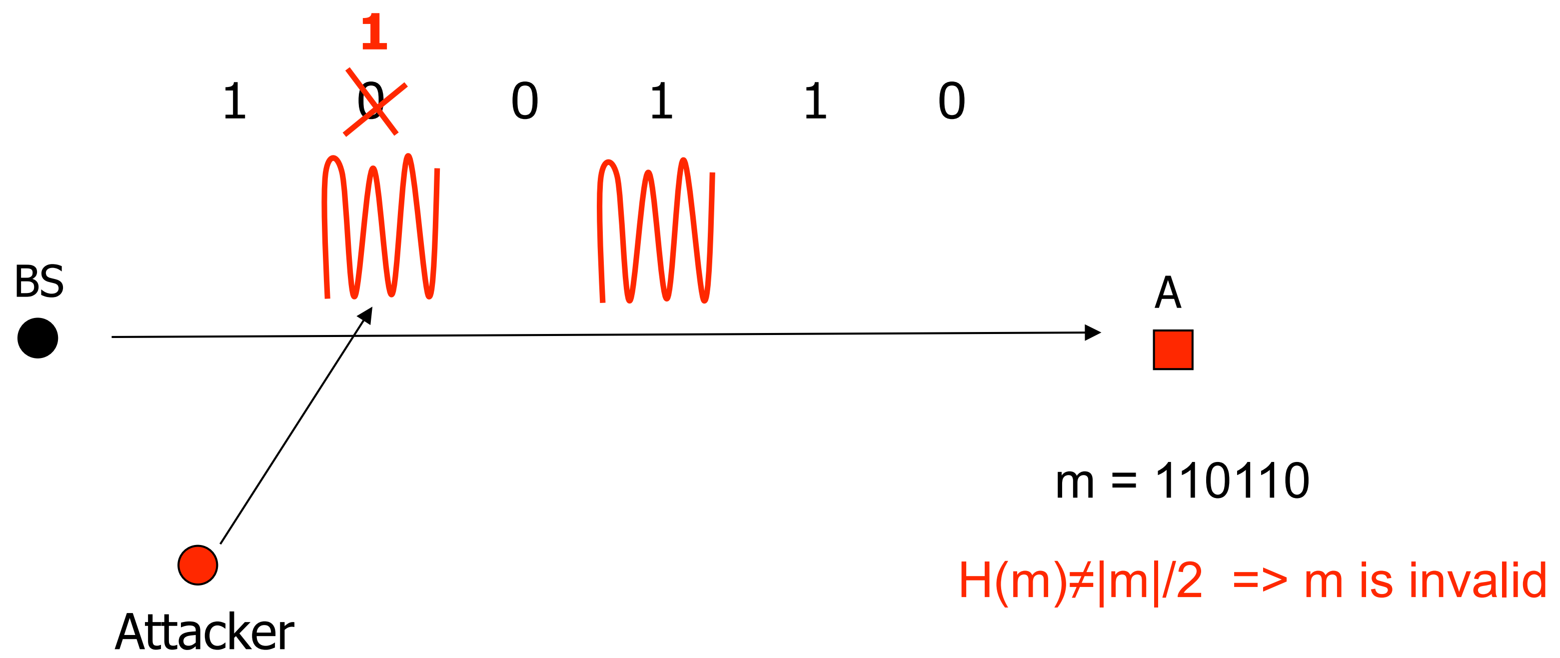


- Beacon detection:
  - presence of signal ($>P_1$) during T on CH1 interpreted as "1"
  - absence of signal ($<P_0$) during T on CH1 interpreted as "0"
- Beacon integrity and authenticity verification
  - IF H(m)=|m|/2 THEN "m" was not modified in transmission



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

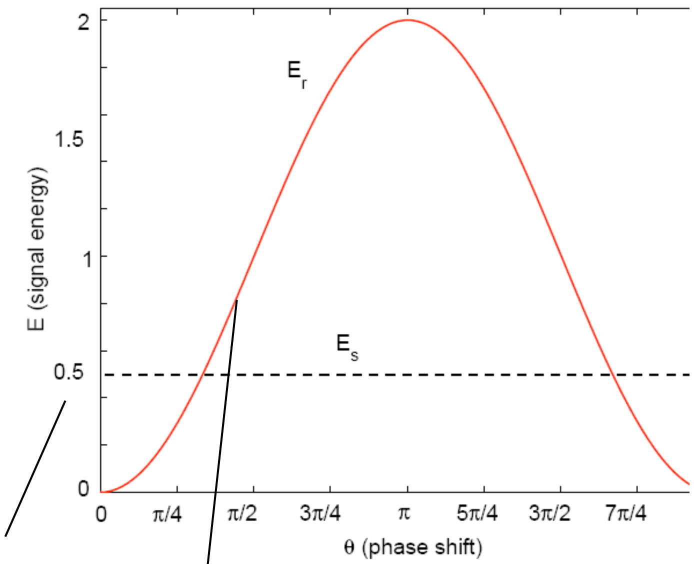


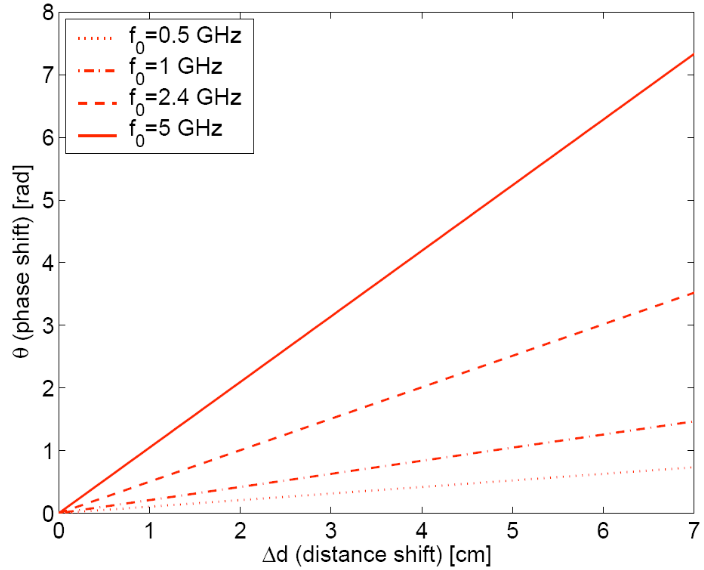
IC: Anti-blocking property of the wireless channel

)0 → 1(•

- phase shift

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





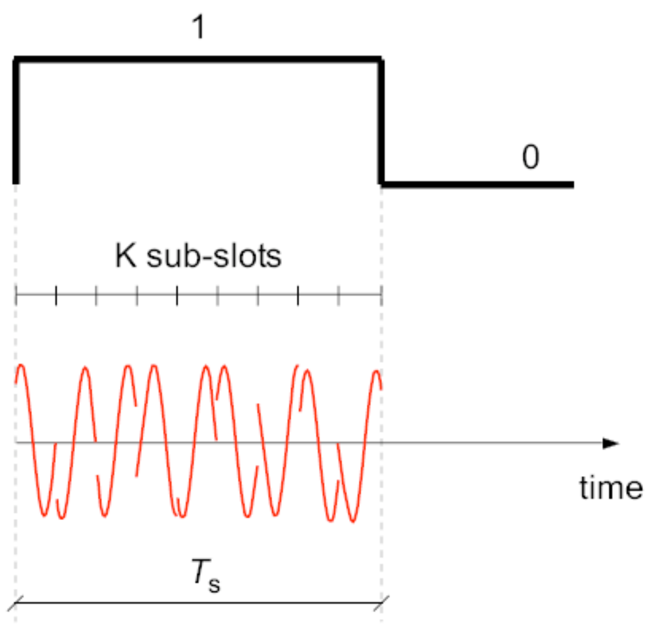
original signal energy

signal energy of the cumulative sender + attacker signal

error in distance estimation (by the attacker)

IC: Randomization At the Sender

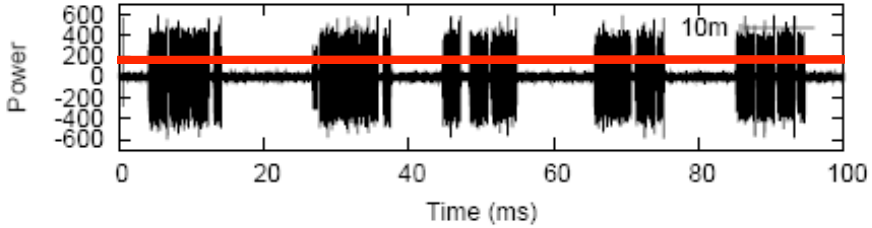
- K-slotted signal (spreading)
- Φ random (e.g., choosen uniformly from $[0,2\pi)$)



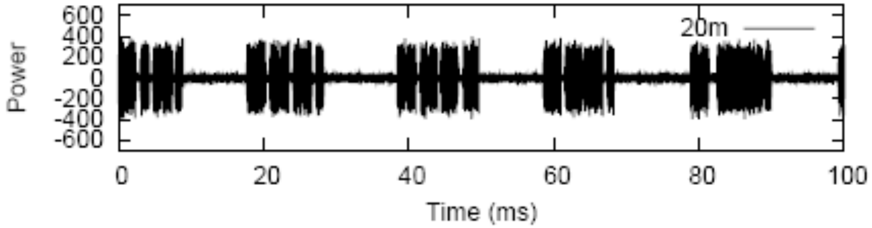
$$\mathbb{P}[K_{\text{attenuated}} \leq K_{\varepsilon}] \geq 1 - \varepsilon$$

Implementation

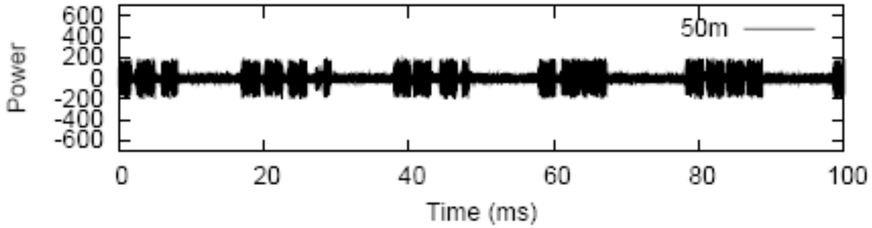
10m



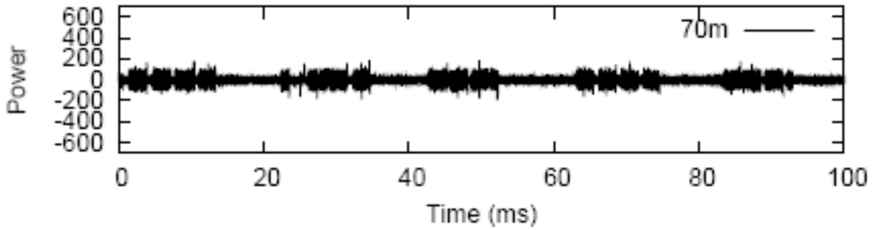
20m



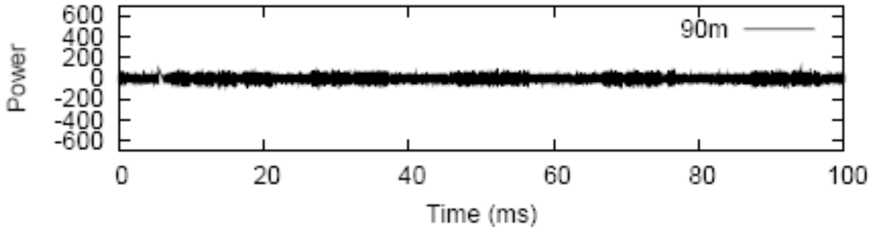
50m

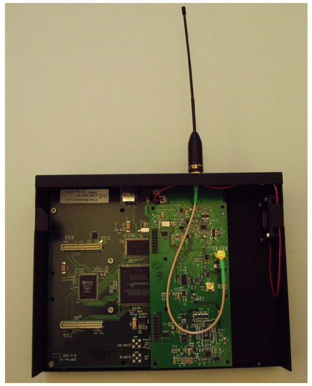


70m



90m





Integrity Coding: Summary

BS

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

Node/User

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

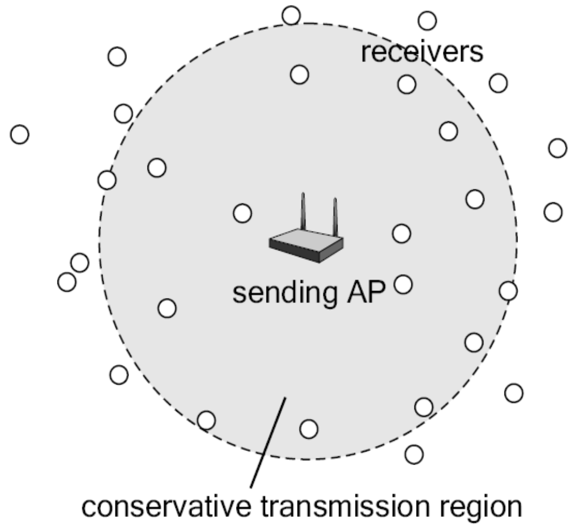
Attacks

- 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)

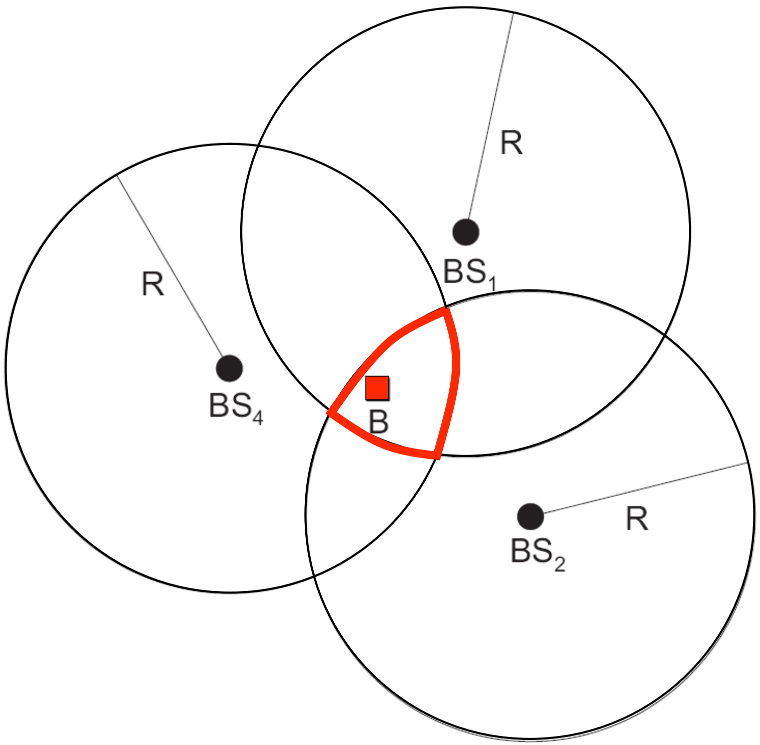
Benefit

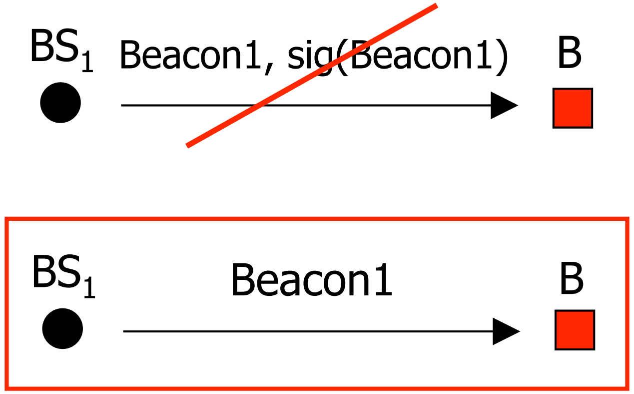
- Broadcast authentication and message integrity protection through presence awareness



SecNav: Beacon-based Localization

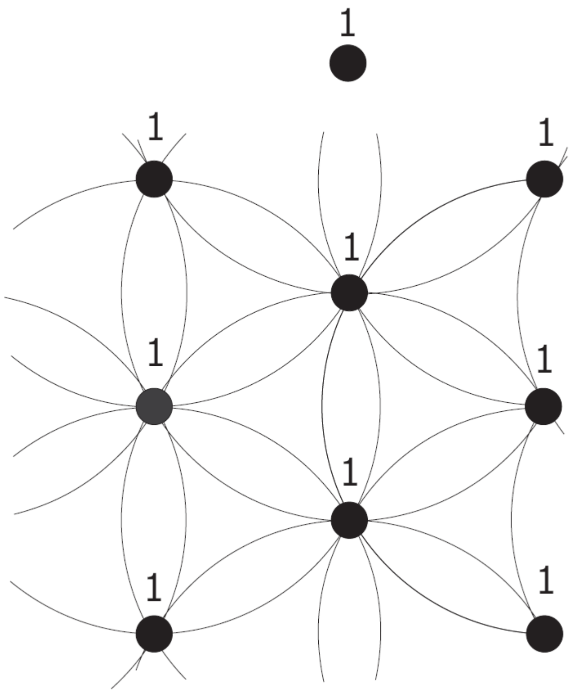
- BSs permanently broadcast INTEGRITY CODED beacons
- B determines it's location at the intersection of (known) BS ranges
- B does not share a key with the BS, does not hold the PK of BS
- Beacons are not signed, encrypted, ...

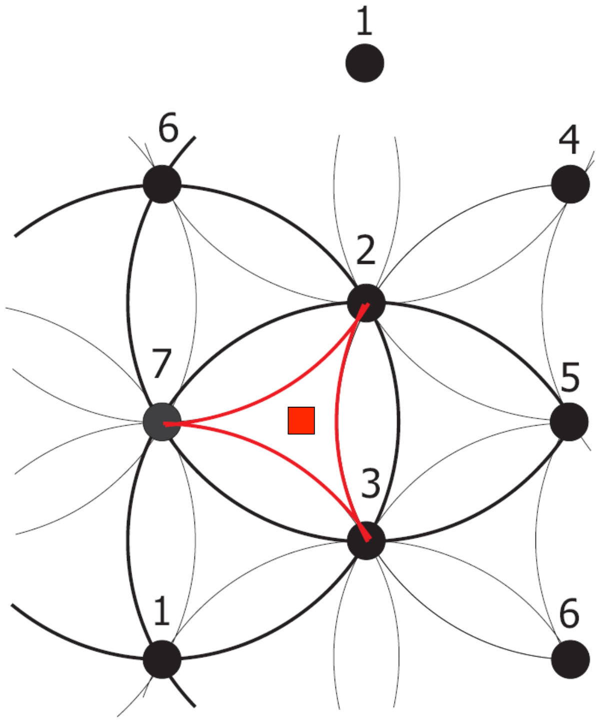




SecNav: Coverage / Localization Accuracy

- Beacon-based
  - Depends on the density of BSs:
- ToA: depends on the ranging accuracy (~15cm)





Summary/Conclusion

- We should not abstract-away the physical layer
  - When reasoning about the security of Wireless Networks we need to consider:
    - Their physical layer
    - Physical node locations and how they are obtained
- ... and make use of the physical layer and the locations

References

- Brands, Chaum, Distance Bounding Protocols, Eurocrypt '93
- Capkun, Hubaux, Secure Positioning in Wireless Networks, Infocom'05, JSAC'06
- Rasmussen, Capkun, Location Privacy of Distance Bounding, CCS'08
- Tippenhauer, Capkun, UWB-based Secure Ranging and Localization, Tr ETHZ'08
- 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
- Strasser, Poepper, Capkun, Cagalj, Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping, S&P(Oakland)'08
- Strasser, Poepper, Capkun, Efficient Uncoordinated FHSS Anti-jamming Communication, ACM MobiHoc 2009
- Tippenhauer, Rasmussen, Pöpper, Capkun, Attacks on Public WLAN-based Positioning Systems, ACM MobiSys 2009
- Boris Danev, Srdjan Capkun, Transient Based Identification of Sensor Nodes, ACM/IEEE IPSN 2009

- Other research: http://www.syssec.ethz.ch/