From Securing Navigation Systems to Securing Wireless Communication Through Location-Awareness

Srdjan Čapkun

Department of Computer Science
ETH Zürich

Purdue, 17.10.2007

Age of wireless communication ...

Future networks

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

- Digitalization of the physical world (every physical object will have a digital representation)
- "Internet of things" (communication with every object/device)

ROBOT NETWORKS

RFID

SENSOR NETWORKS

Importance of Correct Location Information

- Safety applications (traffic monitoring/crash prevention)
- Secure Data Harvesting
- Location-based Access Control (to facilities)
- Tracking of valuables (cargo, inventory, ...)
- Protection of critical infrastructures
- Emergency and rescue operations
- ...
- Secure Networking
- ...

Localization Systems

Satellite (Galileo, GPS, Glonass, Beidou)

- global (outdoor) localization, accuracy <3m
- applications: navigation, cargo tracking, ...

Terrestrial localization systems

- indoor localization, accuracy 1cm-1m
- applications: inventory control, access control, protection of critical infrastructures ...
- commercial: Aeroscout (RSS/TDOA), Ekahau, Verichip (TDOA), Wherify (RSS), Multispectral (TOA/TDOA, UWB), academic: Active Bat, Cricket (TOA/TDOA, US), Active Badge (IR), RADAR, SpotON, Nibble (RSS, Location Fingerprinting), ...

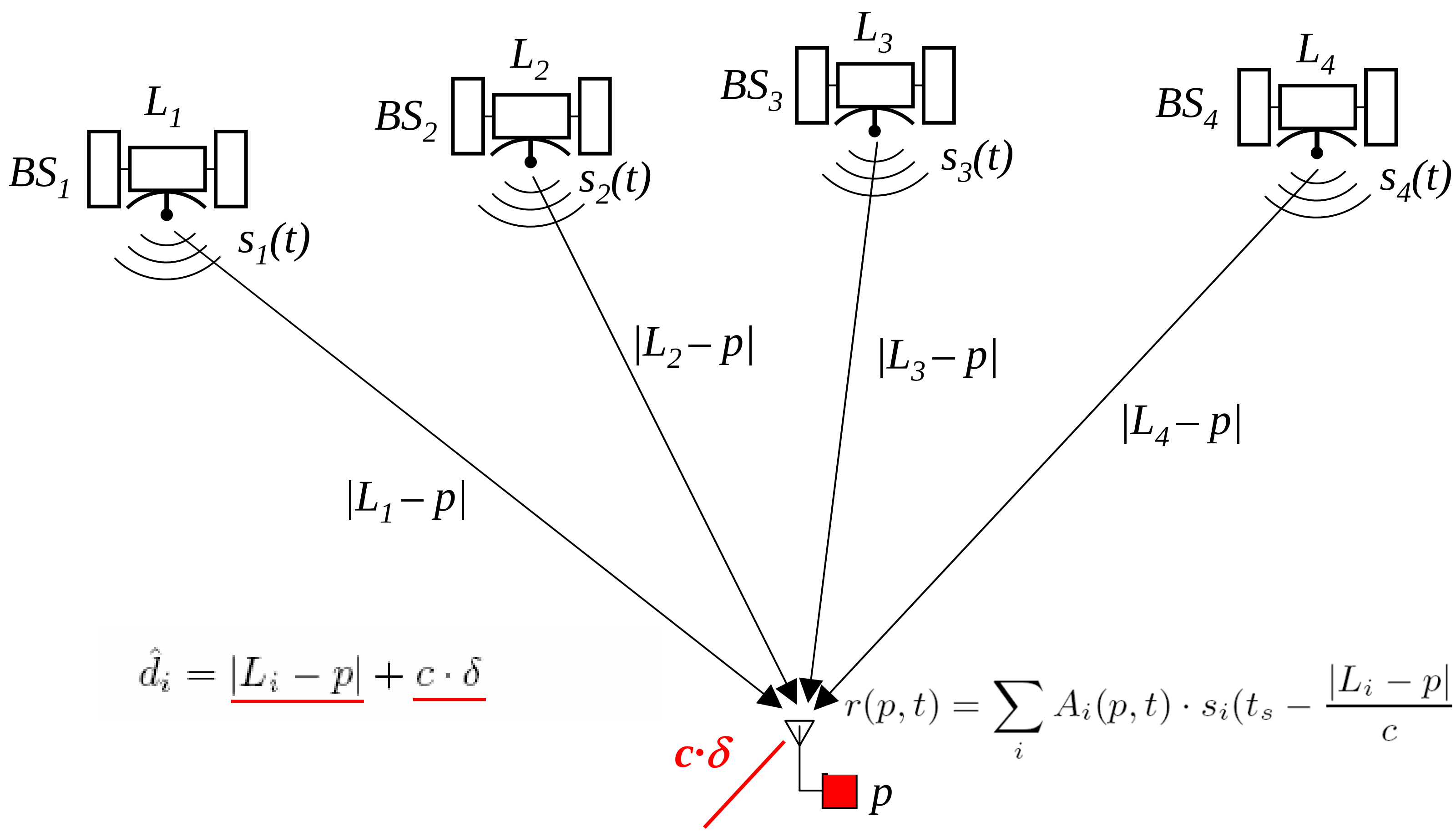
Localization for multi-hop (ad-hoc and sensor) networks

- applications: data harvesting/aggregation, coordinated sensing/actuation, ...
- academic: Convex (Doherty), Angle of Arrival (Niculescu), Beacons (Savvides), Landmarks (Bulusu), Crickets, Interferometric (Maroti), GPS-free (Capkun), ...

Outline

- **Vulnerabilities of Localization Systems**
- Secure Localization (SecNav)
- …

GPS/Galileo (Broadcast ToA Localization)



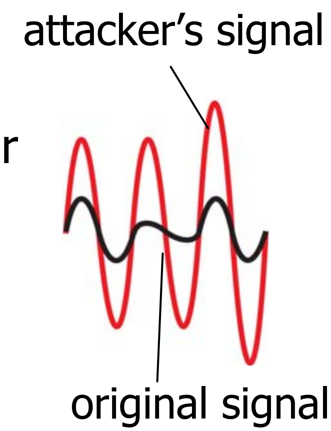
$$\hat{d}_i = \underline{|L_i - p|} + \underline{c \cdot \delta}$$

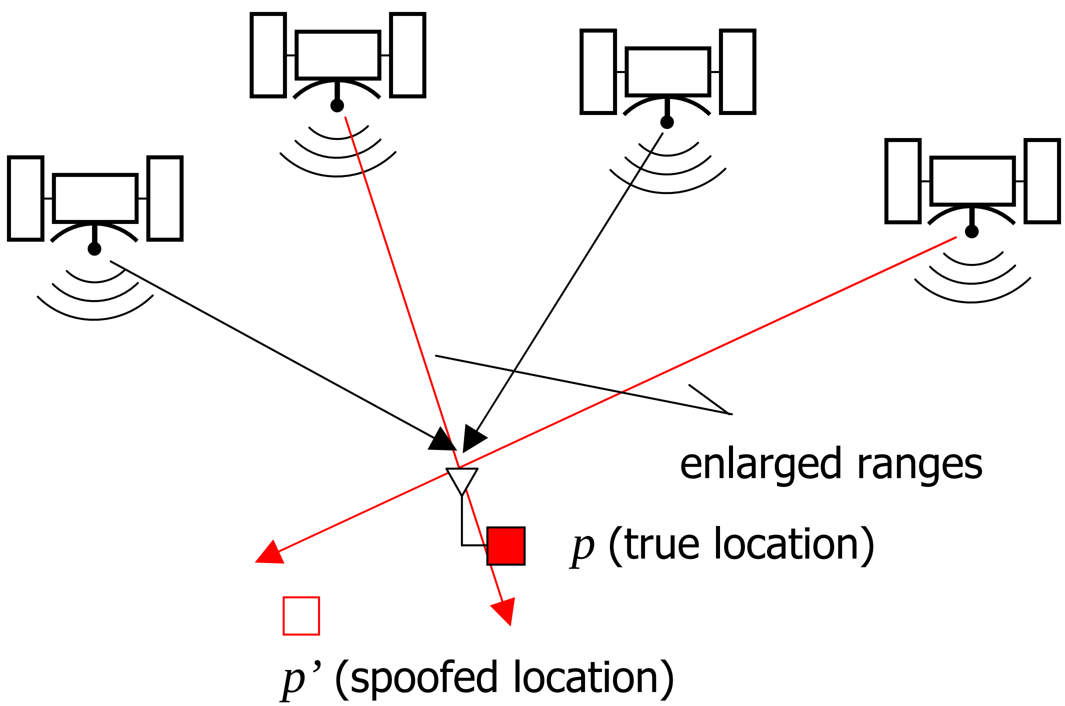
$$r(p,t) = \sum_i A_i(p,t) \cdot s_i(t_s - \frac{|L_i - p|}{c} + \delta) + n(\mathbf{p}, t)$$

$$\begin{aligned}
(t_r^1 - t_s) \cdot c &= |L_1 - \underline{p}| + c \cdot \underline{\delta} \\
(t_r^2 - t_s) \cdot c &= |L_2 - p| + c \cdot \delta \\
(t_r^3 - t_s) \cdot c &= |L_3 - p| + c \cdot \delta \\
(t_r^4 - t_s) \cdot c &= |L_4 - p| + c \cdot \delta
\end{aligned}$$

Attacks on GPS: Location Spoofing

- Range manipulation: signal delay, re(p)lay, jamming (listen/insert)
  - modifies the computed location of the device
- Signal overshadowing
  - With signals from a different location (*p'*) or with GPS simulator
  - GPS signal weak at surface (10^{-15}W)
  - The fake (stronger) signal overshadows the original signal
  - The original signal appears as noise in the fake signal



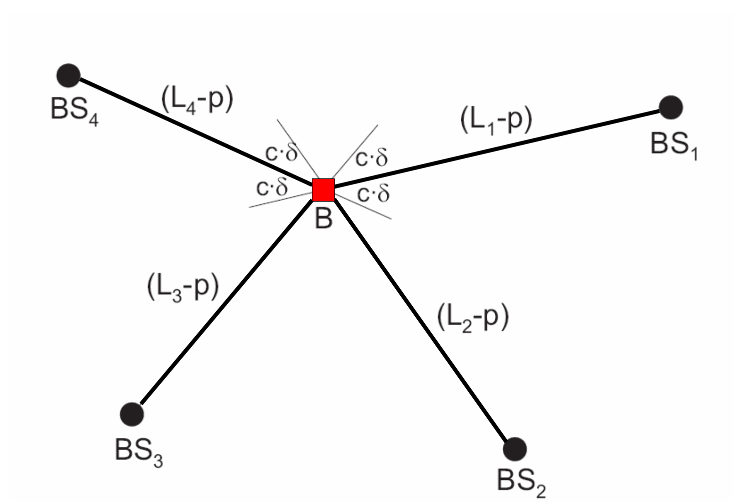


Examples of Documented Attacks on GPS

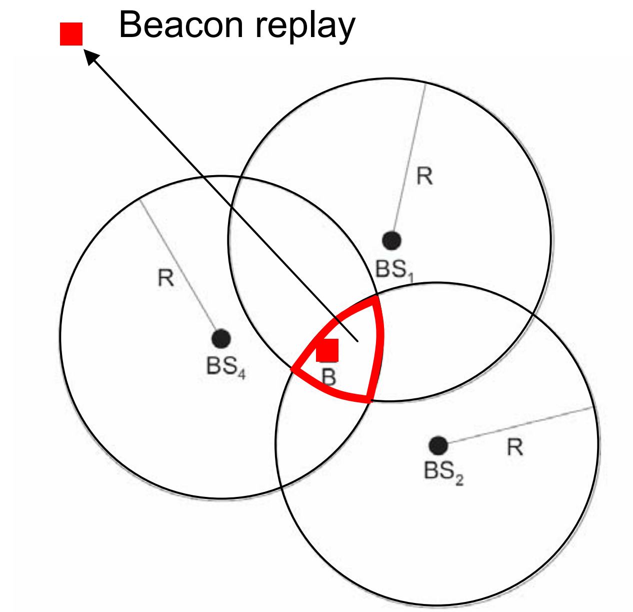
- Location spoofing through signal overshadowing
  - 1999, Los Alamos NL report: Cargo trucks stolen in Russia using GPS device spoofing
- Jamming
  - 2000, The Sunday Times "French secret service jams US and UK tank GPS devices in Greece"
  - War in Iraq, US army GPS jammed by Iraqi forces
- DoS
  - 2007, CNN: "Chinese test missile obliterates satellite",
    "Experts: China now may have the ability to knock-out US GPS and spy satellites"
- ...

(All) Localization Systems Affected

- Time-of-Arrival (TOA) broadcast systems (GPS,...)
- (Round trip) Time-of-Arrival Systems (US and RF-based)
- Time-Difference-of-Arrival (TDOA) Systems
- Beacon-based systems (e.g., for sensor and WiFi networks)
- RSSI-based systems
- US-based systems



TOA LOCALIZATION



BEACON-BASED LOCALIZATION

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)

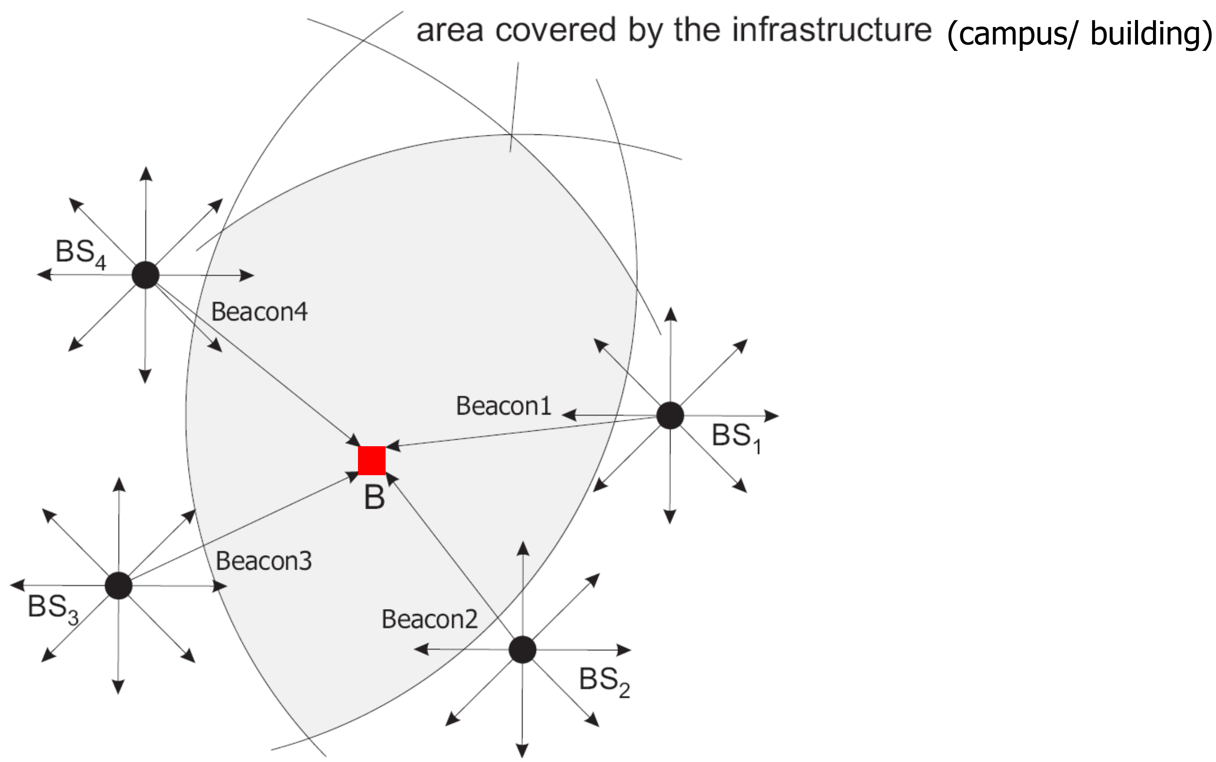
- We need new security primitives, since attacker
  - Modifies the time of signal arrival and/or
  - Modifies signal characteristics (e.g., RSSI) and/or
  - Introduces/removes signals at/from locations

Outline

- Vulnerabilities of Localization Systems
- **Secure Localization (SecNav)**
- …

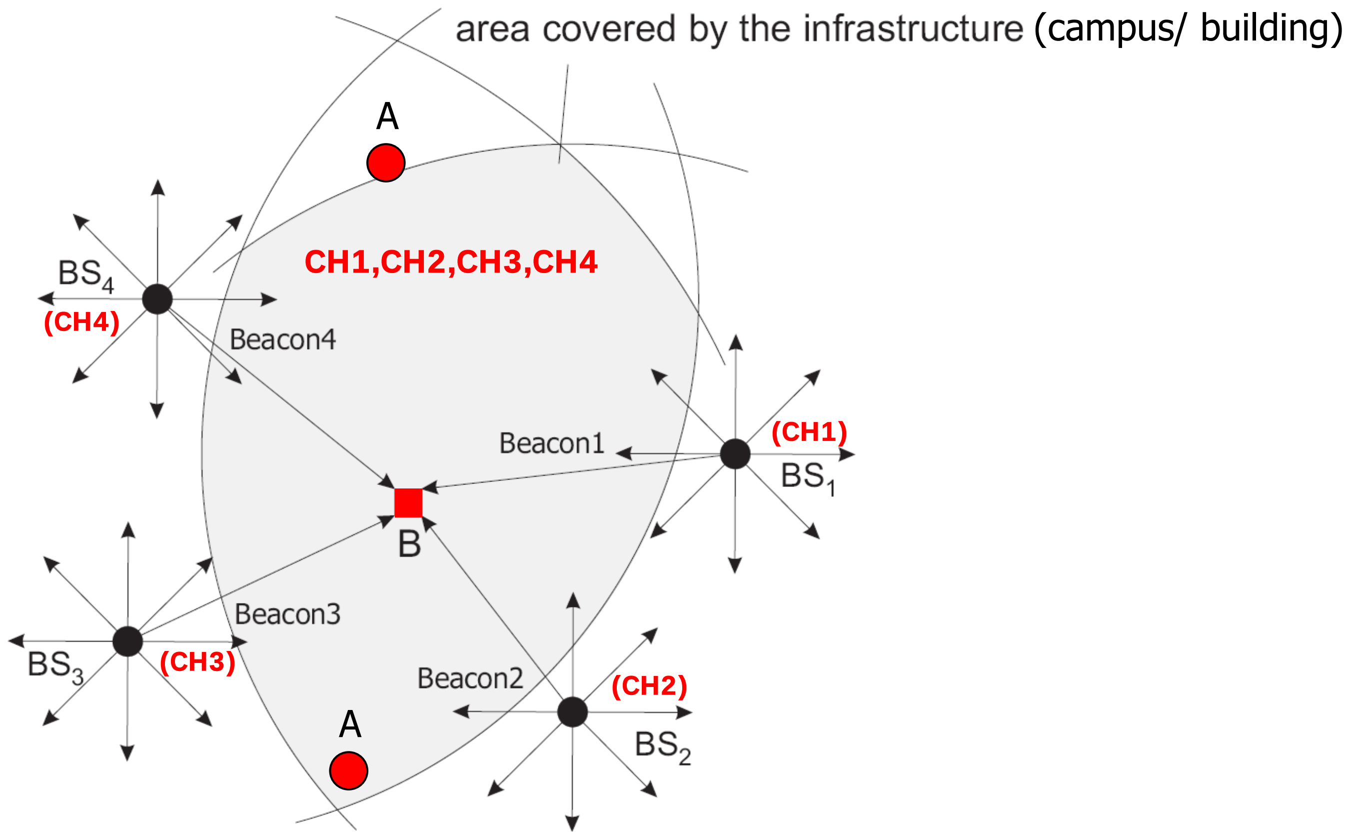
Secure Localization

- **Goal:** compute correct location of a (trusted) device in the presence of an attacker
- **SecNav:** Secure Broadcast Localization and Time-synchronization
  - Prevents range/beacon manipulation attacks
  - Prevents overshadowing attacks
  - Does not prevent jamming (detection only)
- Can be equally deployed with beacon-based and with ToA schemes



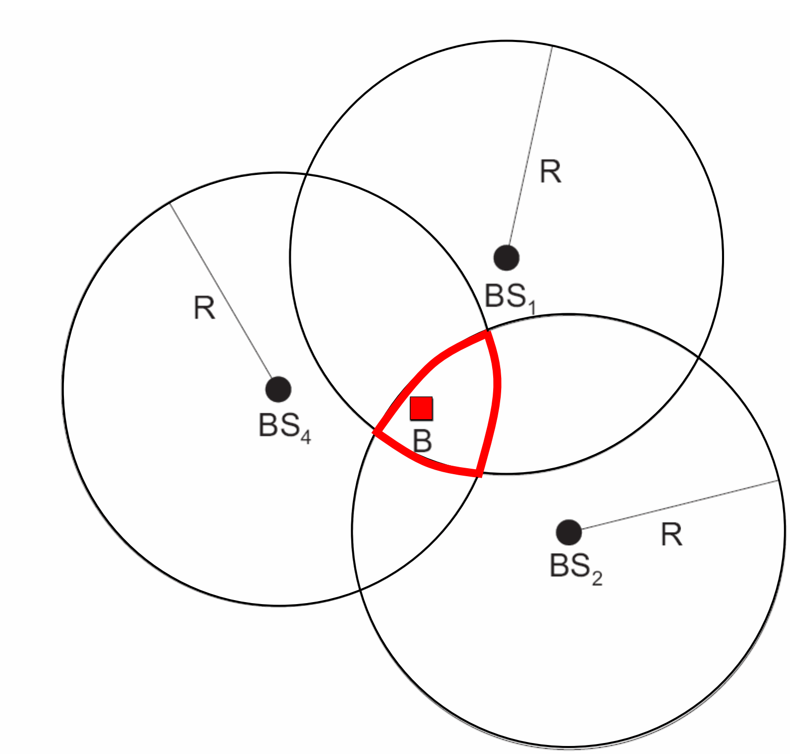
SecNav: Basic Assumptions

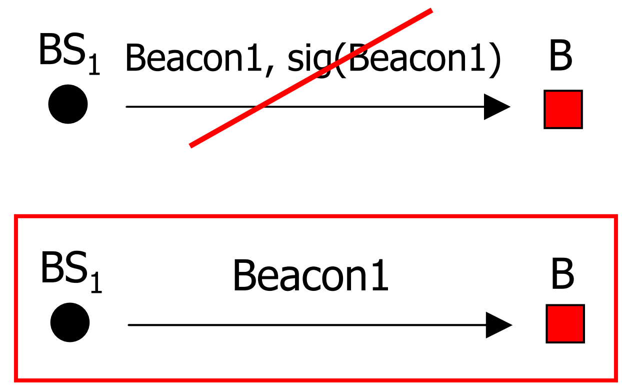
- Deployed in a pre-defined coverage area (e.g., university campus, building)
- The user (B) is aware of its presence in the coverage area
- The area is covered with signals from legitimate stations (BS) (non-overlapping channels)
- Attacker (A) can deploy any number of rogue stations



SecNav: Beacon-based Localization

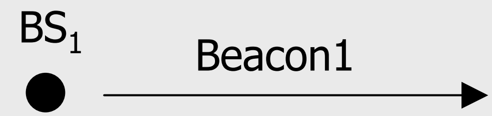
- BSs permanently broadcast INTEGRITY CODED beacons
- B determines it's location at the intersection of (known) BS ranges
- B does not share a key with the BS, does not hold the PK of BS
- Beacons are not signed, encrypted, ...



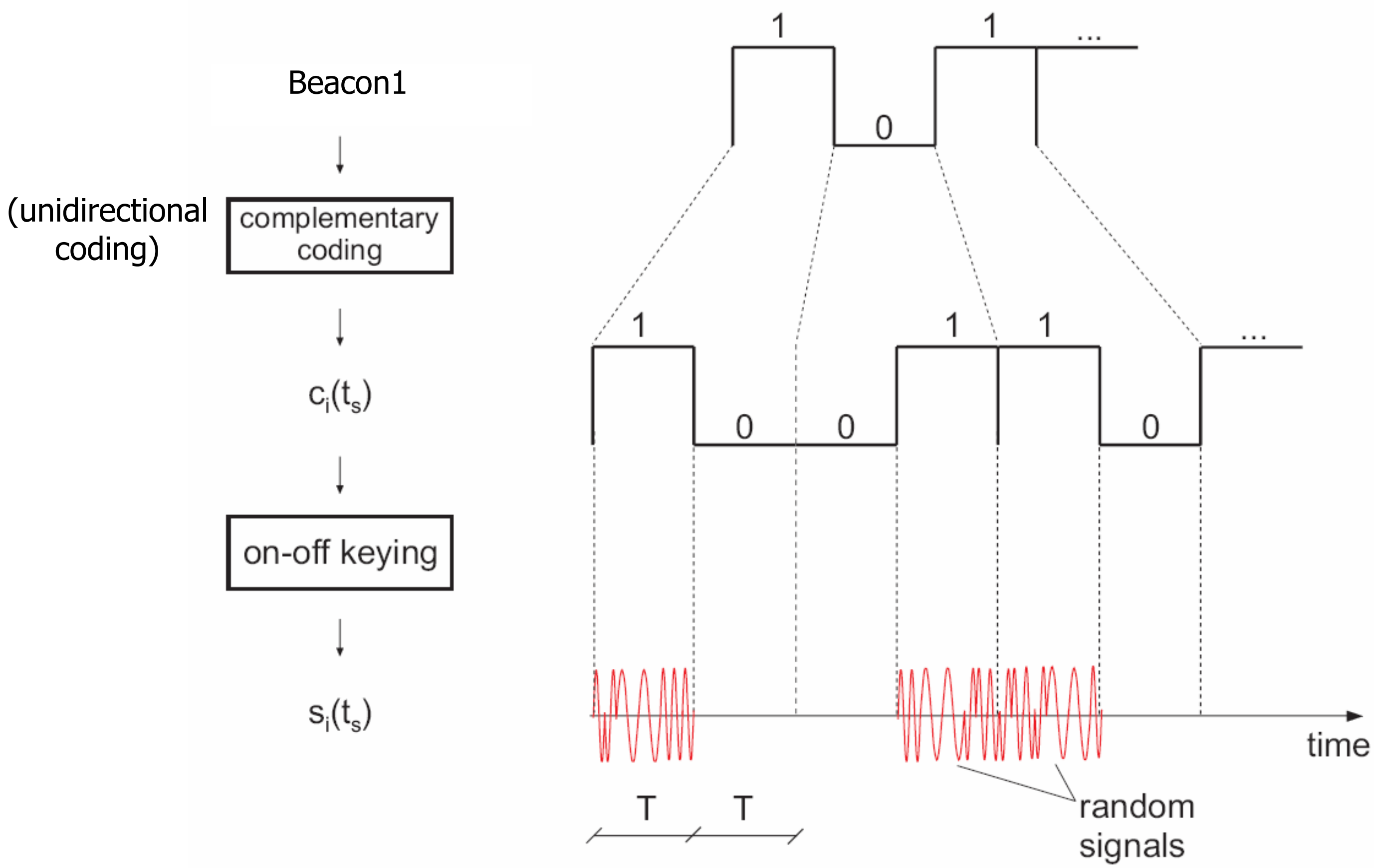


CH1: Beacon1 = "BS1, timestamp"
CH2: Beacon2 = "BS2, timestamp"
...

Integrity Coding

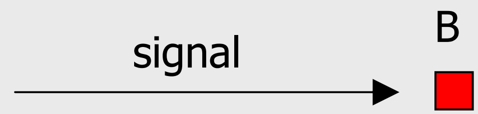


- k-bit Beacon1 spread to 2k bits (1->10, 0->01) (H(Beacon1) = k/2)
- transmitted using on-off keying (each "1" is a fresh random signal)

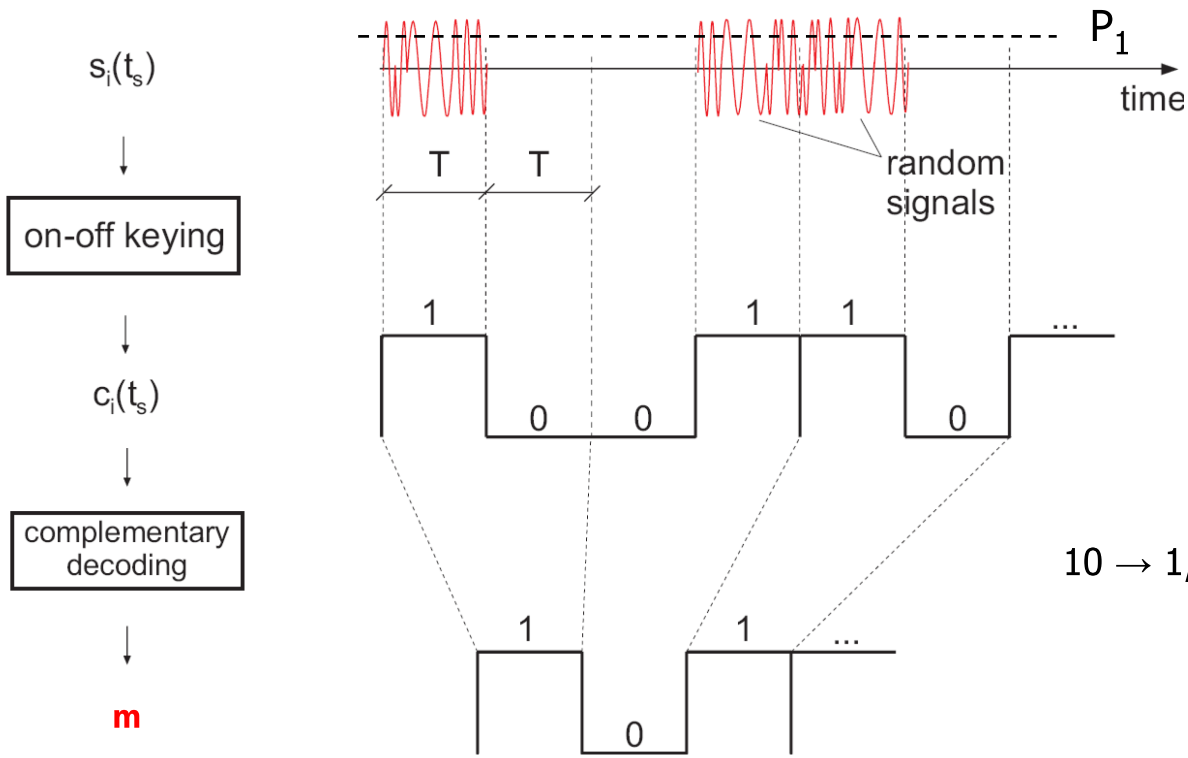


H(Beacon1) = the number of bits "1" in Beacon1 (Hamming weight)

Integrity Decoding



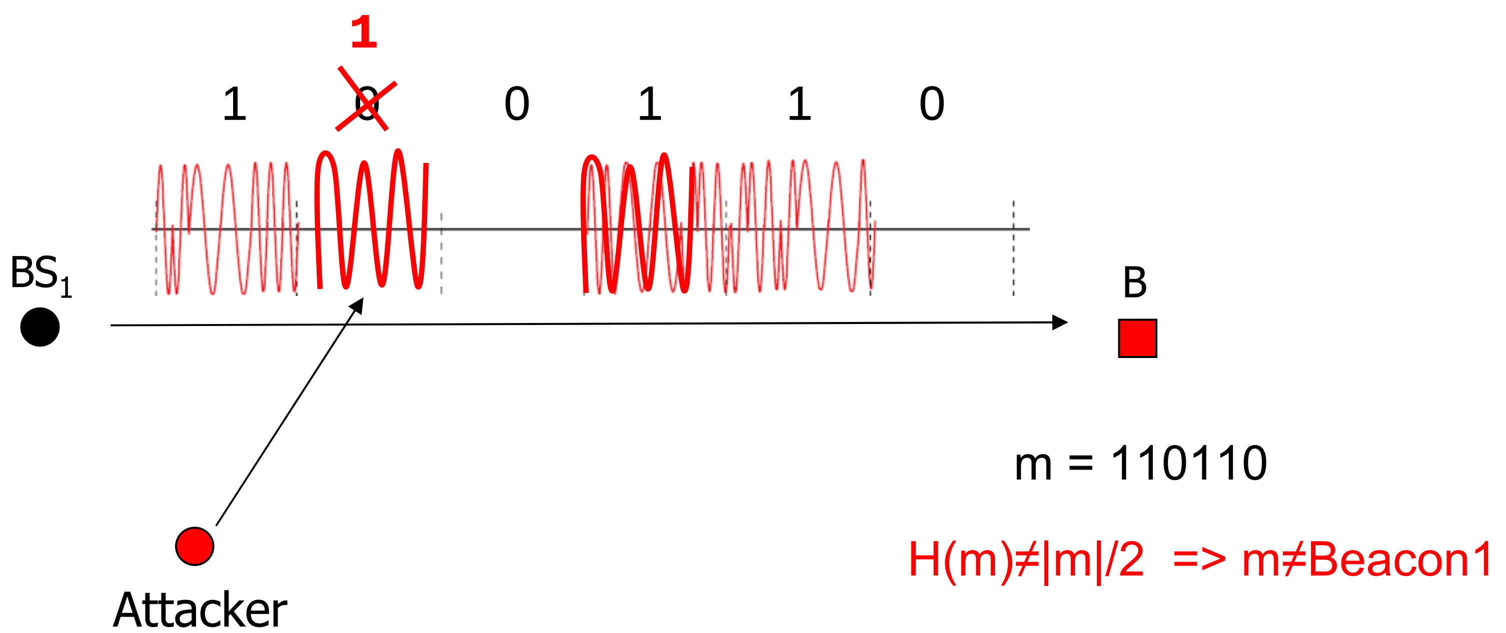
- Beacon detection:
  - presence of signal ($>P_1$) during T on CH1 interpreted as "1"
  - absence of signal ($<P_0$) during T on CH1 interpreted as "0"
- Beacon integrity and authenticity verification
  - IF H(m)=|m|/2 THEN "m" was not modified in transmission
  - since it was sent on CH1 => BS1, and "m" = Beacon1



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)
- B can detect all modifications of the message on channel CH1
- B knows that BS1 is transmitting on CH1



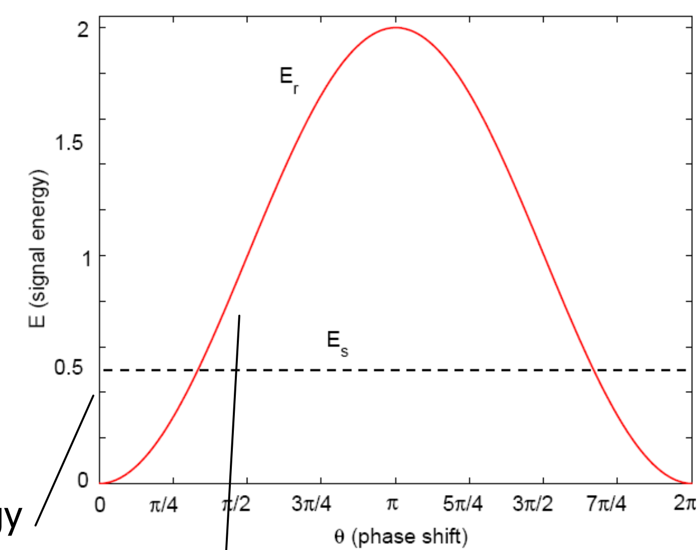
IC: Anti-blocking property of the wireless channel

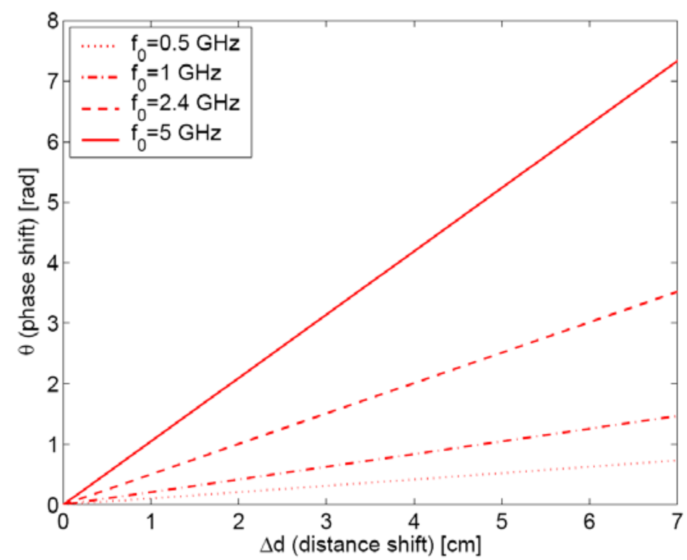
- $(1 \not\to 0)$
- phase shift

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

$$E_r = \int_0^{T_s} r^2(t)dt$$

$$\approx 2T_s \sin^2\left(\frac{\theta}{2}\right)$$





original signal energy

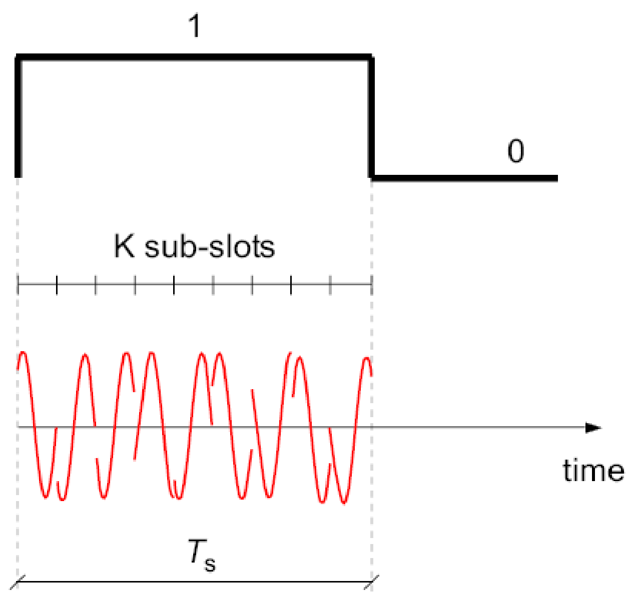
signal energy of the cumulative sender + attacker signal

error in distance estimation (by the attacker)

IC: Randomization At the Sender

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

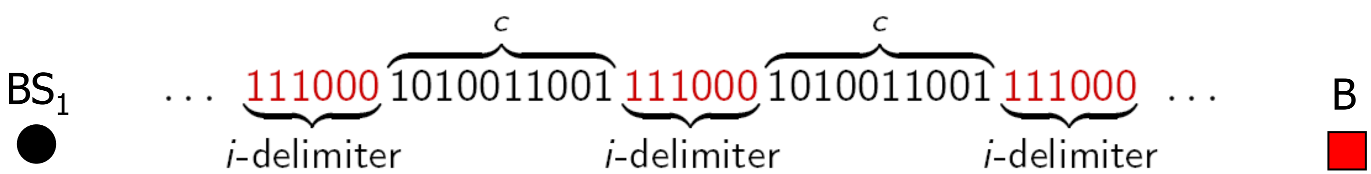
$$\underbrace{R(t)}_{\text{receiver}} = \underbrace{\cos(\omega_0 t + \Phi)}_{\text{sender}} - \underbrace{\cos(\omega_0 t - \Theta)}_{\text{adversary}}, \quad \Phi \in_U [0, 2\pi)$$



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

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.

Integrity Coding: Summary

BS

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

Node/User

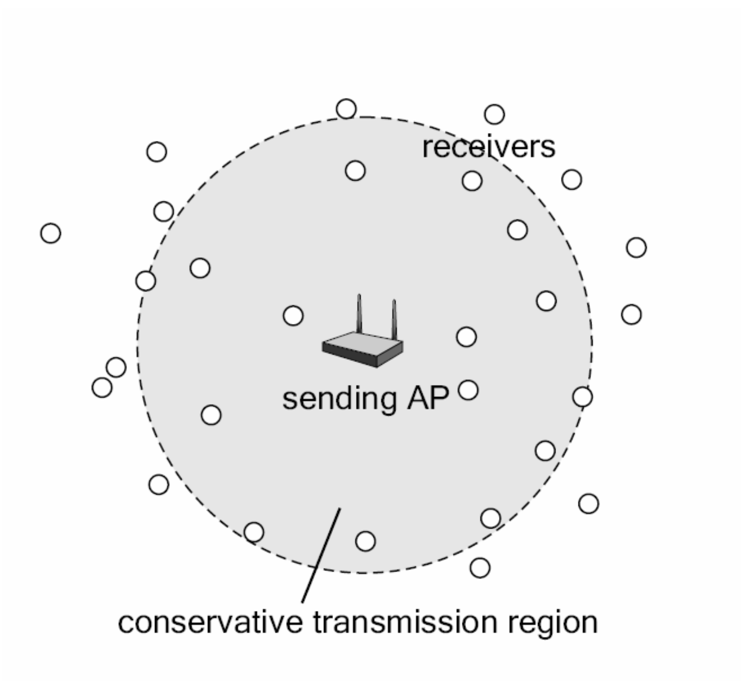
- knows the coverage area
- is aware of its presence in the covered area (e.g., ETHZ campus)

Attacks

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

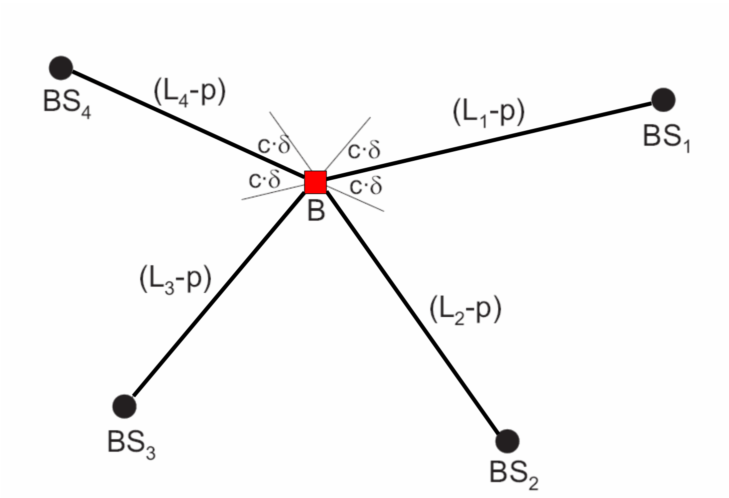
Benefit

- Authentication and message integrity protection through presence awareness

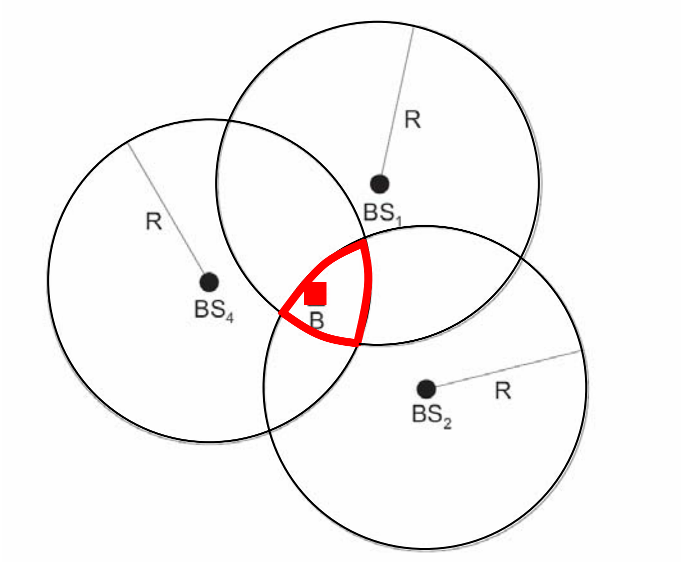


SecNav: Using I-coded beacons / ranging

- Beacon-based schemes
  - replay / insertion / overshadowing / jamming is detected by the receivers
- ToA-based schemes:
  - range enlargement prevented (replays/insertion/overshadowing detected)
  - aggregated signal replay (overshadowing) prevented



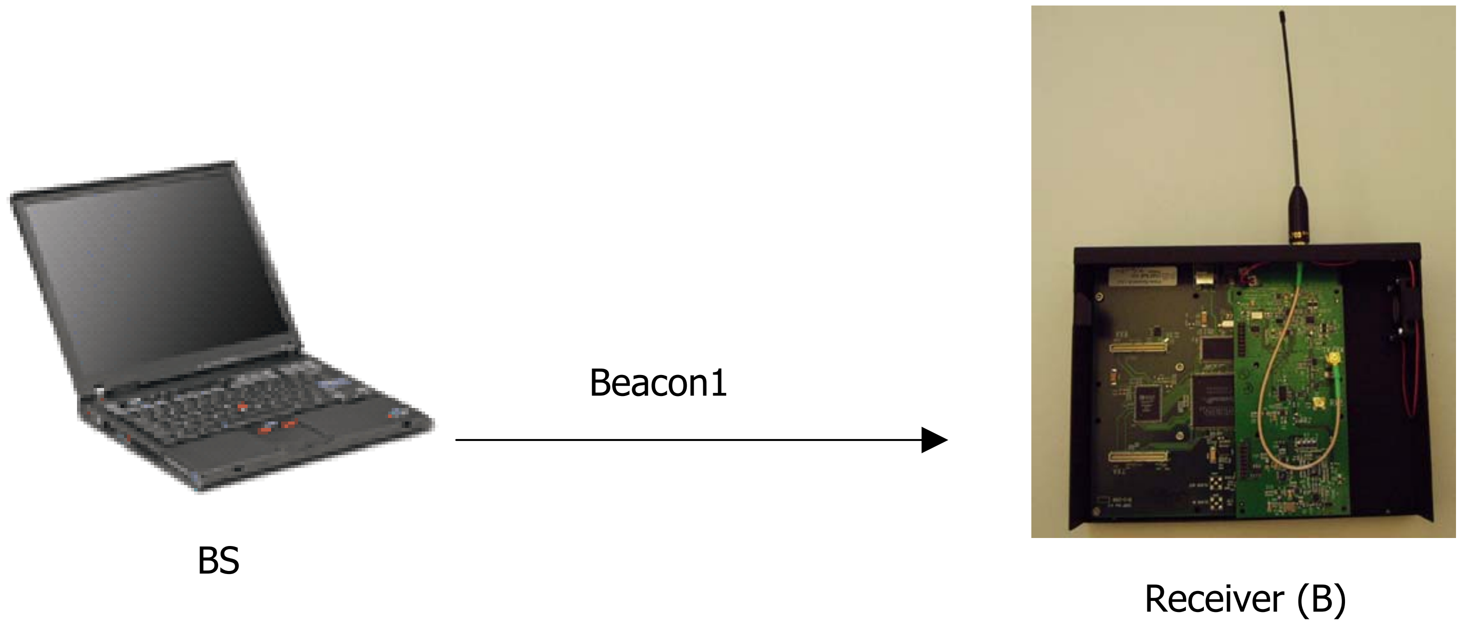
TOA LOCALIZATION



BEACON-BASED LOCALIZATION

SecNav: Implementation (using 802.11b)

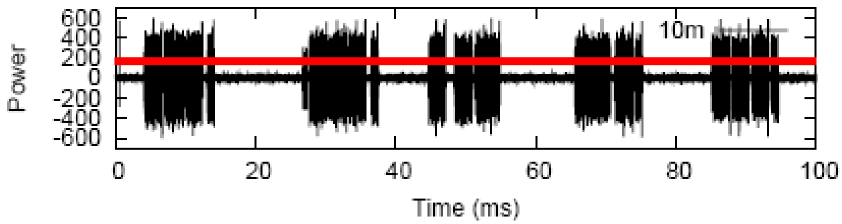
- **BS:** PC with a built-in Atheros 5212, 802.11a/b/g wireless network card (802.11b with 100mW transmission power)
- **Receiver:** Ettus software radio (2.4GHz daughterboard, 64Ms/s sampling rate, 12b resolution, can process 16MHz wide signals)



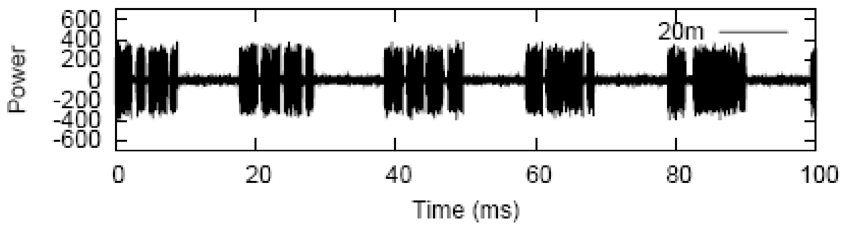
Future: 802.11-2-802.11

SecNav: Base Station Range (LoS)

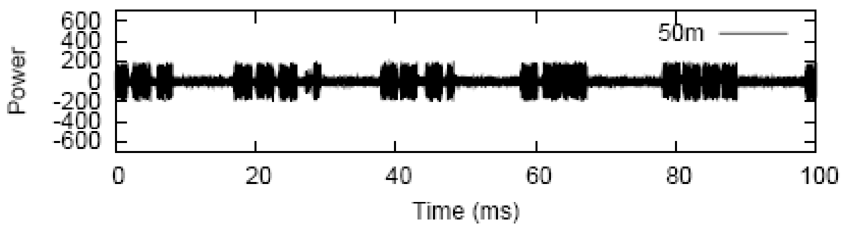
10m



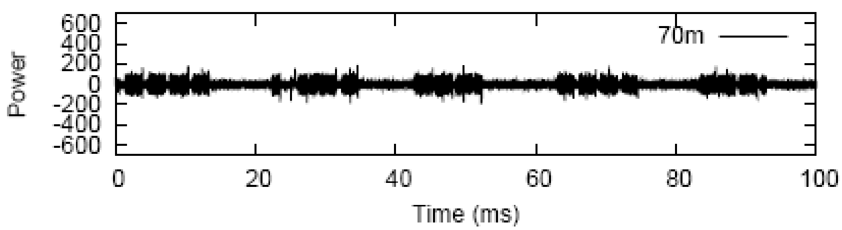
20m



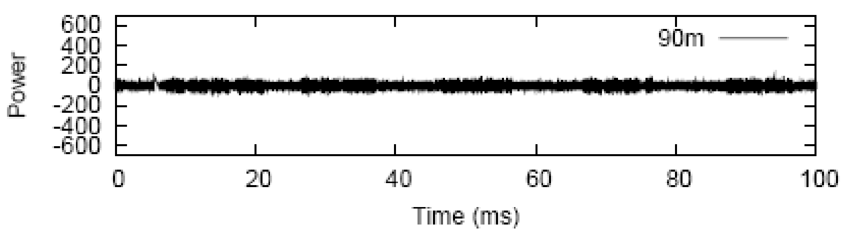
50m



70m



90m

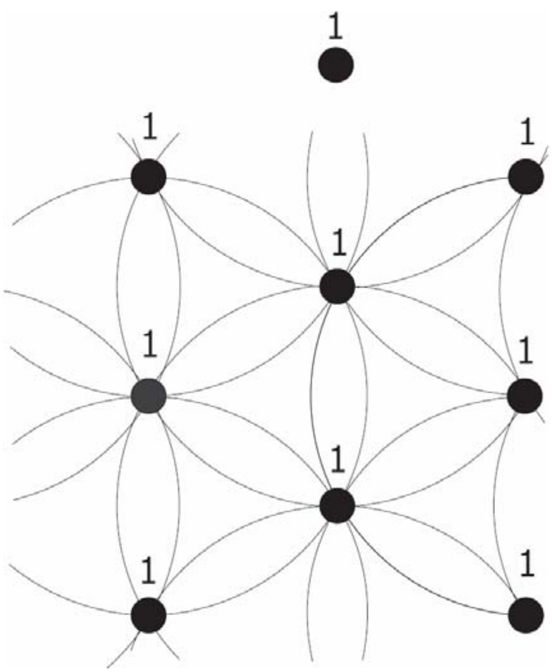


- successful message decoding up to 100m
- dedicated (navigation) channels used
- no resilience to dedicated jamming
- resilience to occasional interference

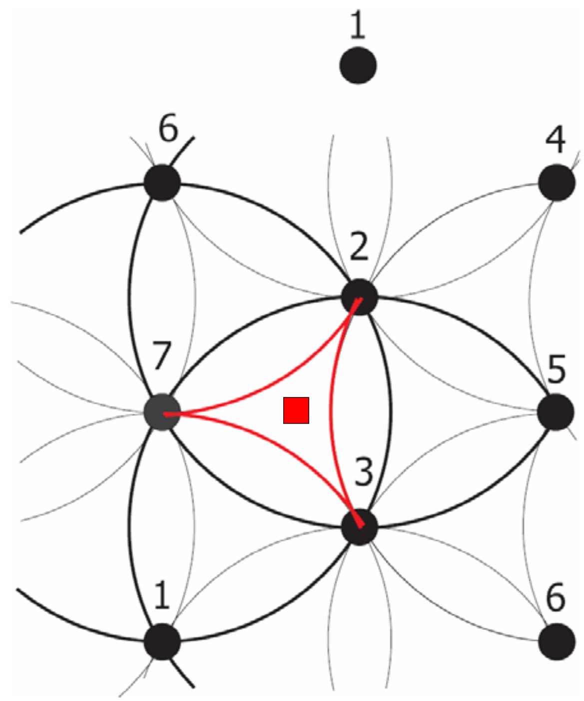
- we used 802.11b (shared spectrum)
- future work: use of DSSS and FHSS

SecNav: Coverage / Localization Accuracy

- Beacon-based
  - Depends on the density of BSs: $A_{3b} = R^2\left(\sqrt{3} - \frac{\pi}{2}\right)$ $A_{4b} = R^2\left(\frac{9\sqrt{3} - 4\pi}{6}\right)$
- ToA: depends on the ranging accuracy (<1m)



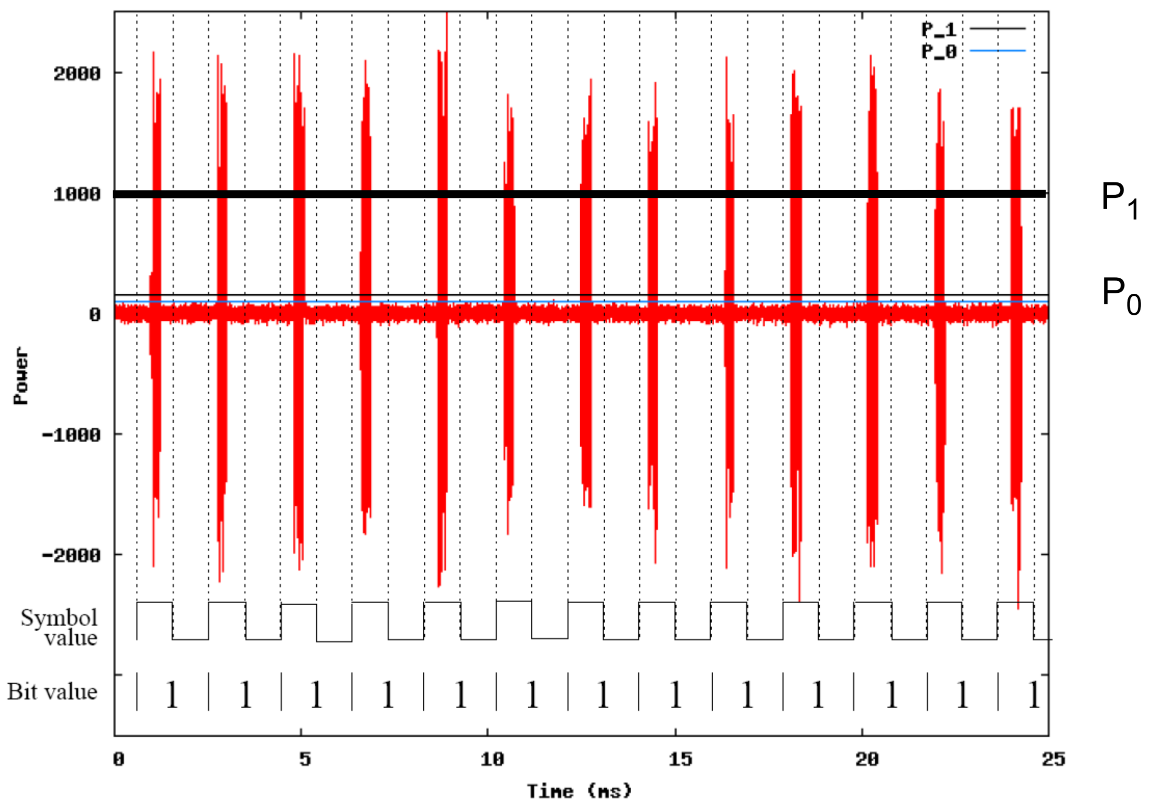
FULL COVERAGE WITH A SINGLE CHANNEL



FULL COVERAGE WITH 7 CHANNELS – NO MUTUAL INTERFERENCE

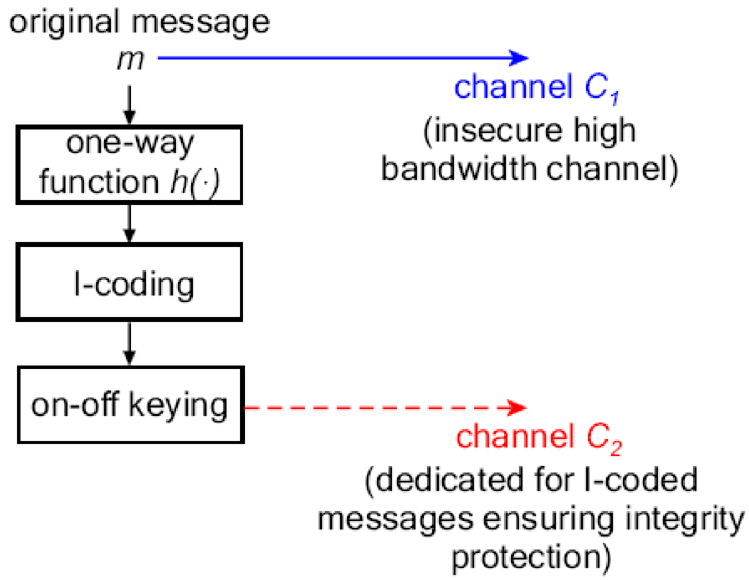
SecNav: Navigation Message Rate

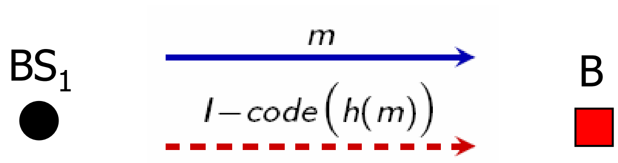
- With 802.11-based implementation: 500b/s
- With custom-built devices (433 MHz, Atmel): 20kb/s
- Clock Synchronization
  - theoretically O(ns) (signal cannot be shifted by the attacker)
  - with low-cost and off-the-self implementations O(μs)



Optimization

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





SecNav: Summary

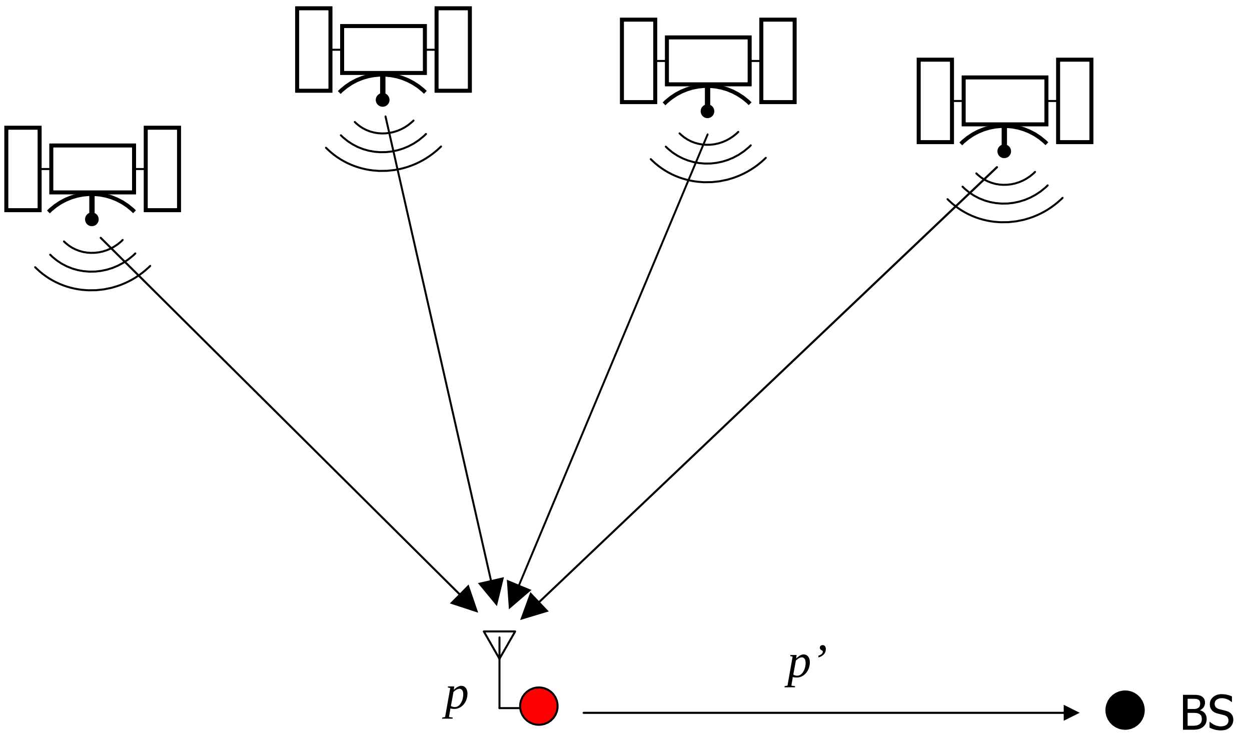
- SecNav
  - Secure (Broadcast) Localization
  - Secure (Broadcast) Time-Synchronization
  - Prevents all known attacks on localization/time sync. (excluding DoS)
- Can be implemented using legacy (e.g., 802.11b) and low-power platforms (e.g., Sensor Networks).
- Can equally work with Time-of-Arrival and Beacon-based broadcast Localization Systems
- Applications: generally suitable for secure navigation in campuses, buildings, compounds ...

Outline

- Vulnerabilities of Localization Systems
- Secure Localization (SecNav)
- …

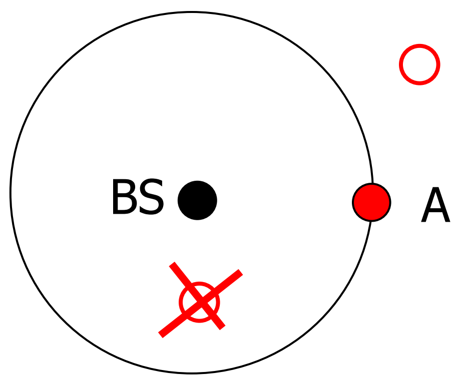
Location Verification

- **Goal:** verify (or compute) the location of an untrusted device.

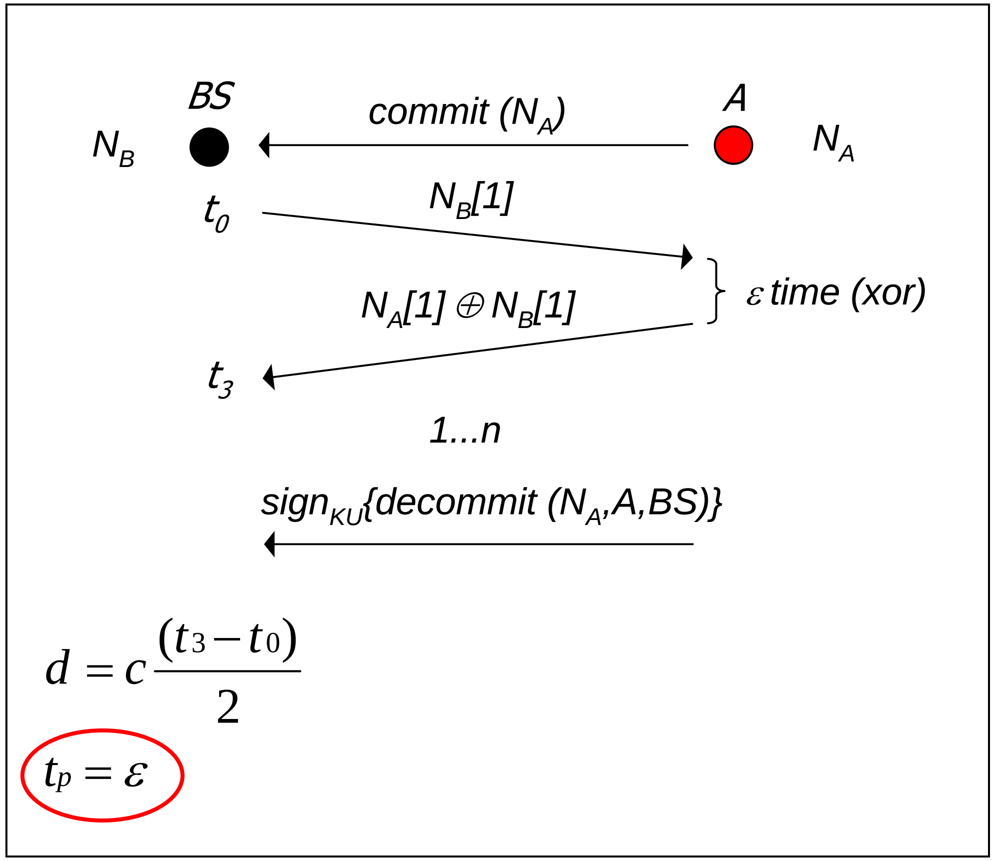


- If a device knows its correct location, will it report the true location to the BS?
- How to verify/measure a location of an untrusted device?

Distance bounding (Distance Verification)



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

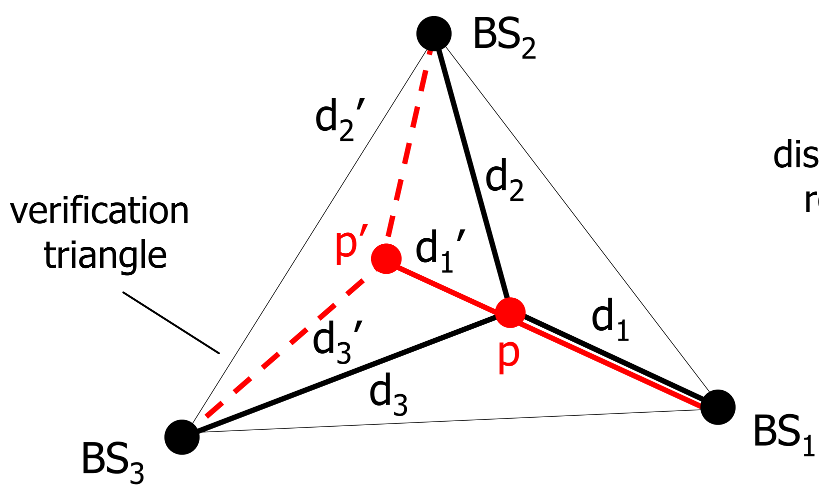


DB/Authenticated ranging protocols:

- Brands, Chaum 93 (wired, smartcard-ATM)
- Capkun, Buttyan, Hubaux, 2003 (wireless)
- Sastry et al., 2003 (US)
- Kuhn, 2005 (wireless)

Location Verification (Verifiable Multilateration)

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

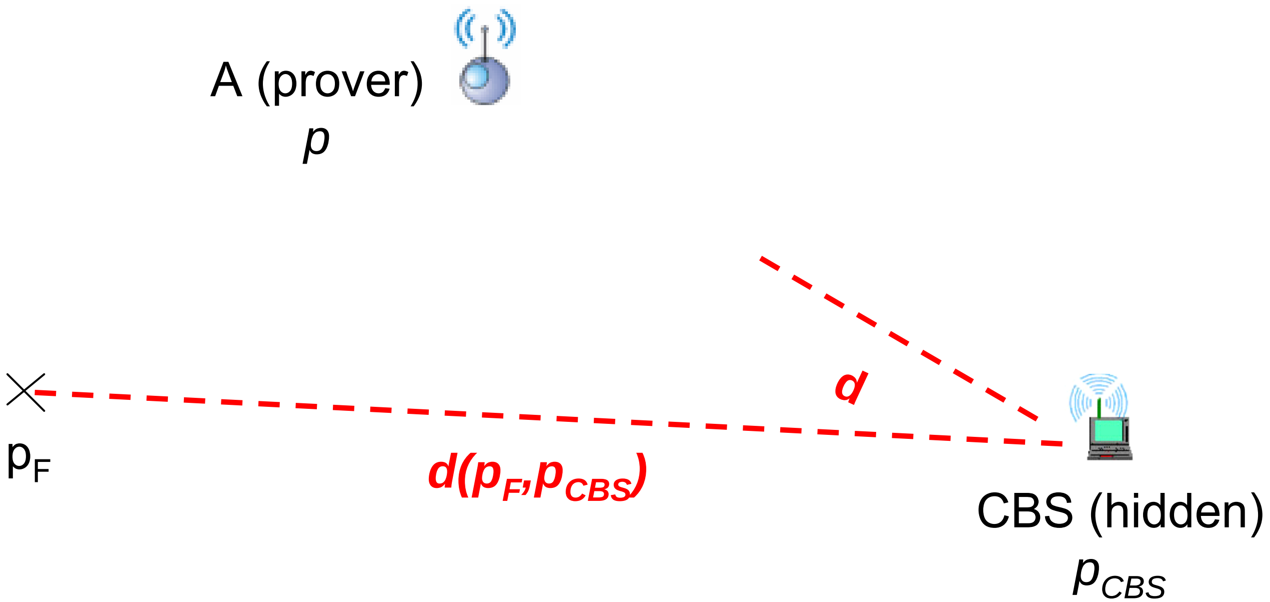


distance enlargement implies that one of the remaining distances needs to be reduced (within the triangle)

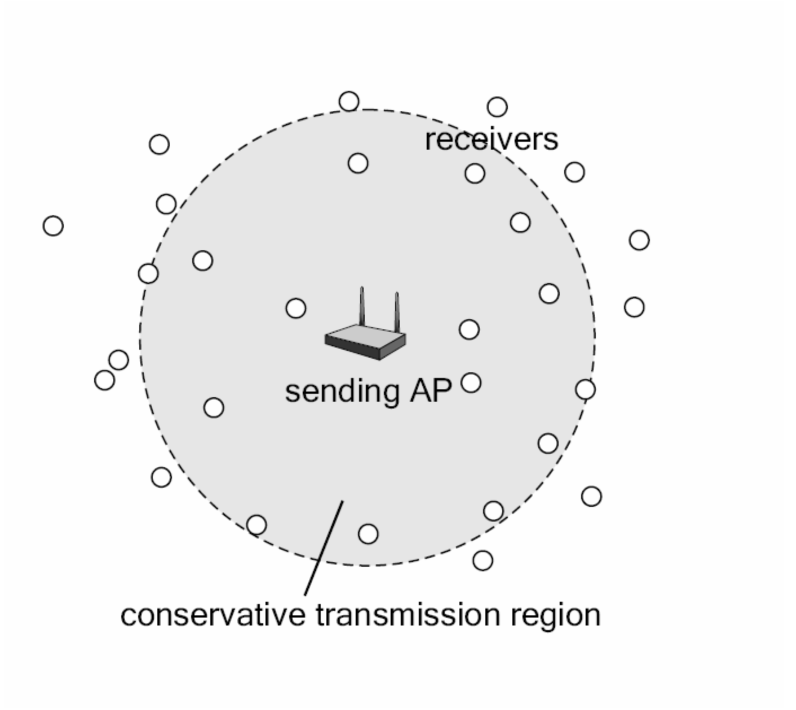
- Can be used to verify locations of devices in the triangle/triangular pyramid ...

Location Verification

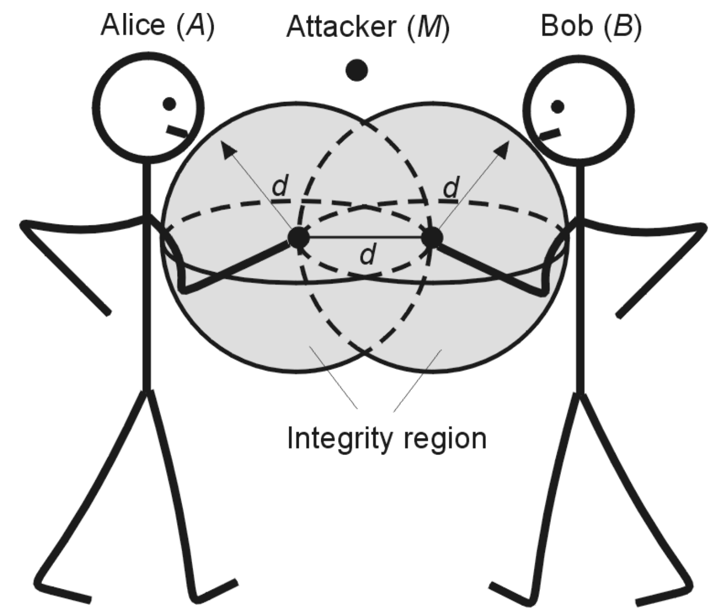
- Location Verification with Hidden/Mobile Stations
  - rely on hidden locations of verification stations
  - compare the claimed location and the measured location



Location awareness



Authentication through presence awareness
(e.g., I-codes)



Authentication through (attacker) absence awareness
(measuring the distance from which
the message originates)

(e.g., I-regions)

Current Approaches for Secure Localization/Time Synchronization

Distance Verification:

- Brands and Chaum, **Distance-Bounding (in wired networks)**, 1993. (DV)
- Shankar, Sastry, Wagner, **Location Verification using US distance-bounding**, ACM WiSe 2003 (DV)
- Capkun, Buttyan, Hubaux, **Mutual Authenticated Distance Bounding,** ACM SASN 2003
- **...** (mainly DB-based approaches)

Secure Localization and Location Verification

- Kuhn 2004, **Securing Broadcast Navigation with Hidden Spreading Codes**, IHW, 2004 (SL)
- Lazos, Poovendran, **Securing Localization with Directional Antennas**, WiSe 2004 (SL)
- Li et al. and Liu et al., **Statistical Methods for Secure Localization in Sensor Networks**, IPSN 2005
- Zhang et al.. **Secure localization in Ultra-wideband Networks**, JSAC 2006 (SL)
- Capkun, Hubaux, **Verifiable Multilateration**, TR 2004, IEEE INFOCOM 2005, JSAC 2006 (SL and LV)
- Lazos, Capkun, Poovendran, **w Directional Antennas/Distance Bounding**, IPSN 2005 (SL)
- Capkun, Cagalj, Srivastava, **Hidden and Mobile Stations**, IEEE INFOCOM 2006 (LV)
- Capkun, Ganeriwal, Anjum, Srivastava, **RSSI-based Secure Localization**, 2006 (SL)
- Rasmussen, Capkun, Cagalj, **SecNav**, MobiCom 2007 (SL)
- Sedighpour, Capkun, Ganeriwal, Srivastava, **Demo: Attacks on US Ranging**, ACM SenSys 2005

Secure Time Synchronization

- Ganeriwal, Capkun, Han, Srivastava, **Secure Time Synchronization**, ACM WiSe 2005 (Pairwise)
- Rasmussen, Capkun, Cagalj, **SecNav**, ACM Mobicom 2007 (Broadcast)
- Manzo, Roosta, Sastry, **Time Synchronization Attacks in Sensor networks,** In SASN 2005 (STS)
- Sun et al.. Tinysersync: **Secure Time Synchronization in Sensor Networks**, CCS 2006 (STS)

Conclusions

- Future (and current) wireless networks and their applications depend on correct location and time information
- Localization and Time Synchronization are highly vulnerable to attacks by signal manipulation
- Traditional security primitives are not adequate
  - deal with message content, not with signals and their characteristics
- We need new primitives

- Location awareness can support basic security protocols
  - Authentication through presence awareness
  - Authentication through (attacker) absence awareness

Links/references

- SecNav:
  - Rasmussen, Capkun, Cagalj, SecNav, MobiCom 2007
  - Cagalj, Capkun, ..., Integrity-codes, S&P 2006 (I-codes)
- Location Verification
  - Capkun, Hubaux, Verifiable Multilateration, Infocom 2005/JSAC 2006
  - Capkun, Rasmussen, ..., Verification based on Hidden and Mobile Base Stations, Infocom 2006, TMC 2007
  - Capkun, Buttyan, Hubaux, ACM SASN 2003
- Device pairing (Key establishment)
  - Capkun, Cagalj, Integrity-regions, ACM WiSe 2006
  - Cagalj, Capkun, Hubaux, Key Establishment in Wireless P2P Networks, Proceedings of IEEE, 2006
- http://www.securelocalization.com
- Srdjan Čapkun, capkuns@inf.ethz.ch