Wireless Security gets Physical

Srdjan Čapkun

Department of Computer Science
ETH Zurich

SWING, Bertinoro, July 2008

Secure Localization
in Wireless 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, ...

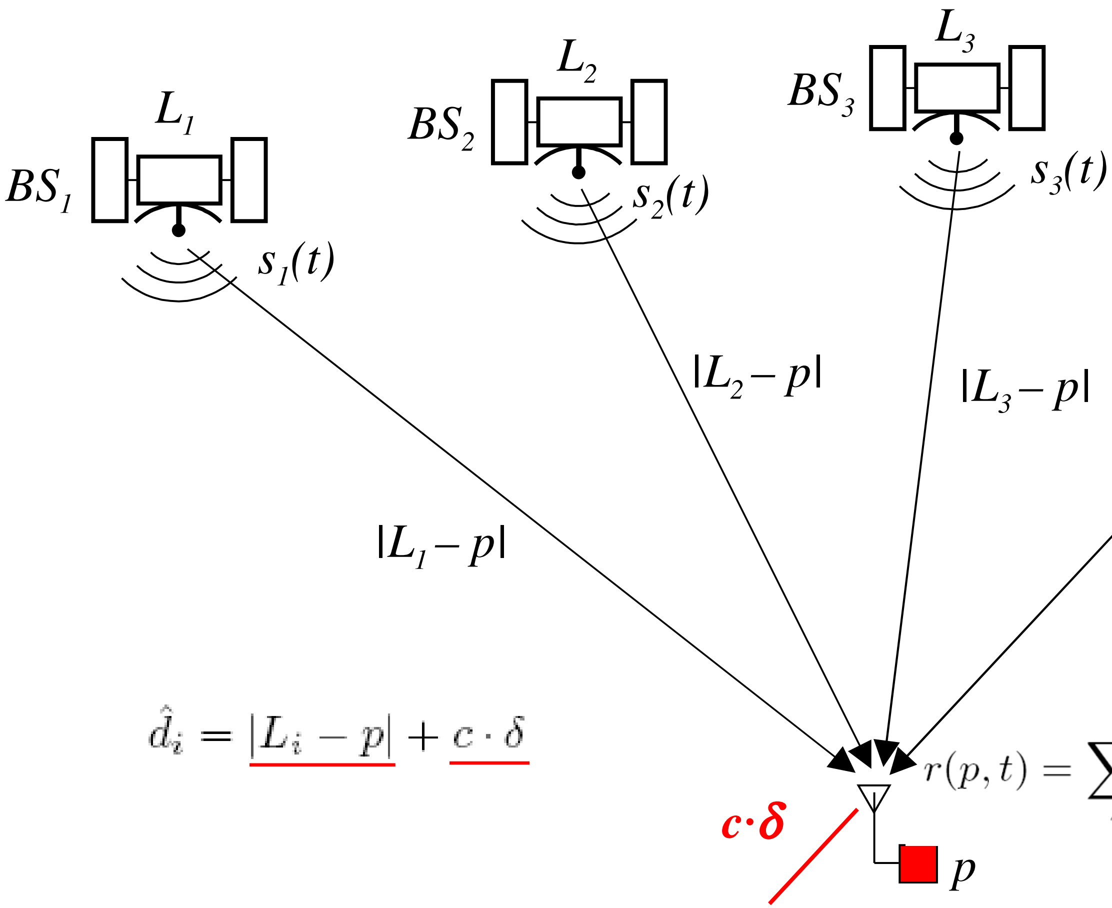
Terrestrial localization systems

- 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), ...

GPS/Galileo (Broadcast ToA Localization)



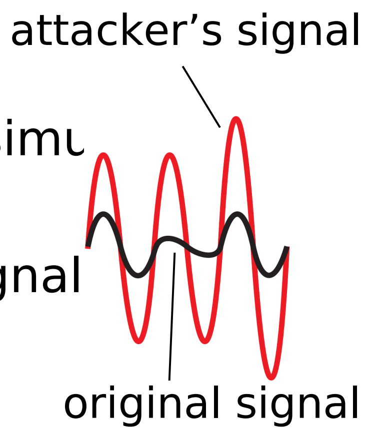
$$\hat{d}_i = \underline{|L_i - p|} + \underline{c \cdot \delta}$$

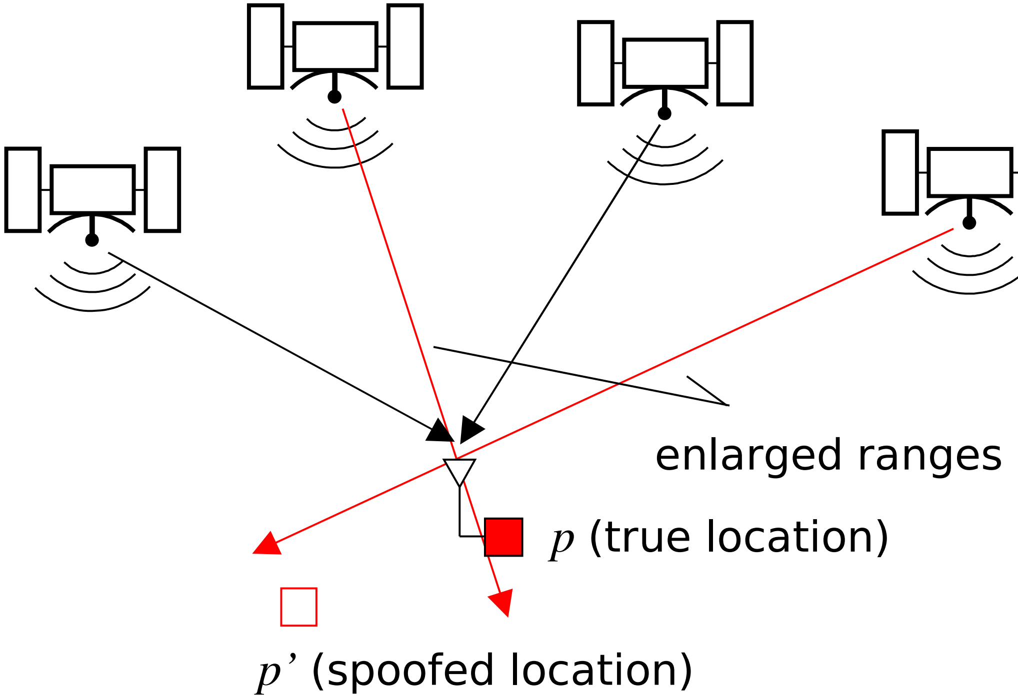
$$r(p,t) = \sum_i A_i(p,t) \cdot s_i(t_s - \frac{|L_i - p|}{c} + \delta) + n(\mathbf{p}, t)$$

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

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 simu
  - 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





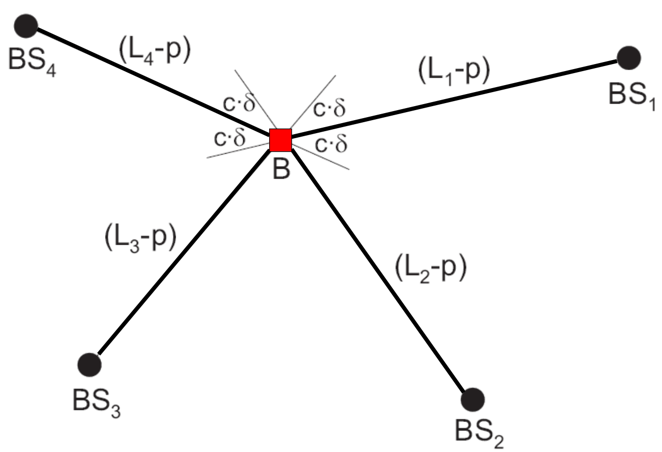
Examples of Documented Attacks on GPS

- 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
- …

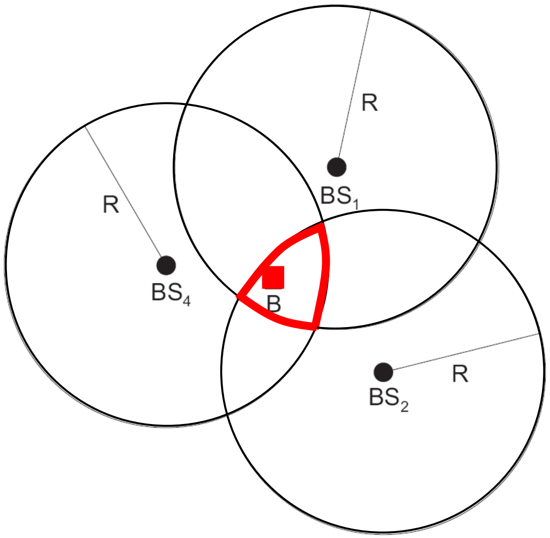
- DoS
  - 2007, CNN: “Chinese test missile obliterates satellite”, “Experts: China now may have the ability to knock-out US GPS and spy satellites”
- …

(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

Vulnerabilities of positioning systems

Measurements
- RF Time of Arrival (TOA)
- Ultrasonic TOA
- Received signal strength (RSS)
- Doppler
- Angle of Arrival (AOA)
- Infrared (proximity)
- Image processing
- ...

Algorithms/techniques
- Multilateration
- Time Difference of Arrival (TDOA)
- FDOA (differential Doppler)
- (Rotating) directional antennas
- Interferometric localization
- Location fingerprinting
- ...

Vulnerabilities
- Signal strength manipulations
- TOA manipulation (pulse-delay)
- TDOA manipulation (e.g., directional antennas)
- FOA manipulation
- Signal overshadowing
- Signal annihilation
- Signal amplification
- Jamming
- Direction manipulation
- ...
- Device compromise
- Collusion/cloning
- ...

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

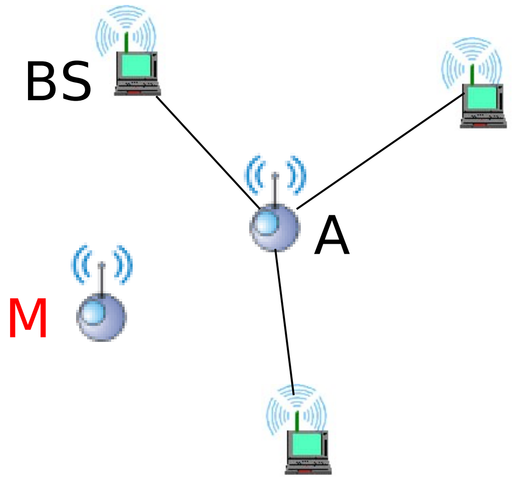
- Compute the correct location of a trusted device in the presence of adversaries

- Compute the correct location of an untrusted device
  (that wants to be localized, e.g., for access)

Two scenarios

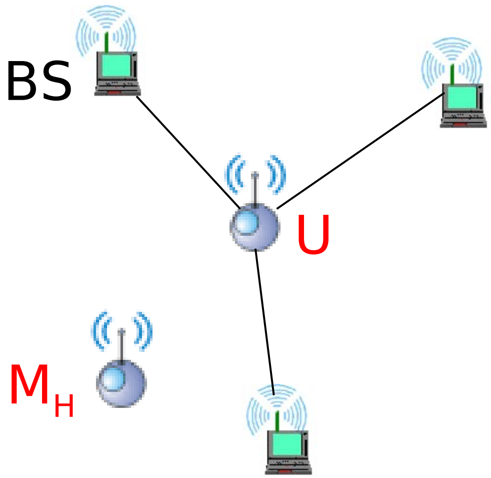
trusted device (A)

- trusted user and/or hardware
- *attacks: external (M)*



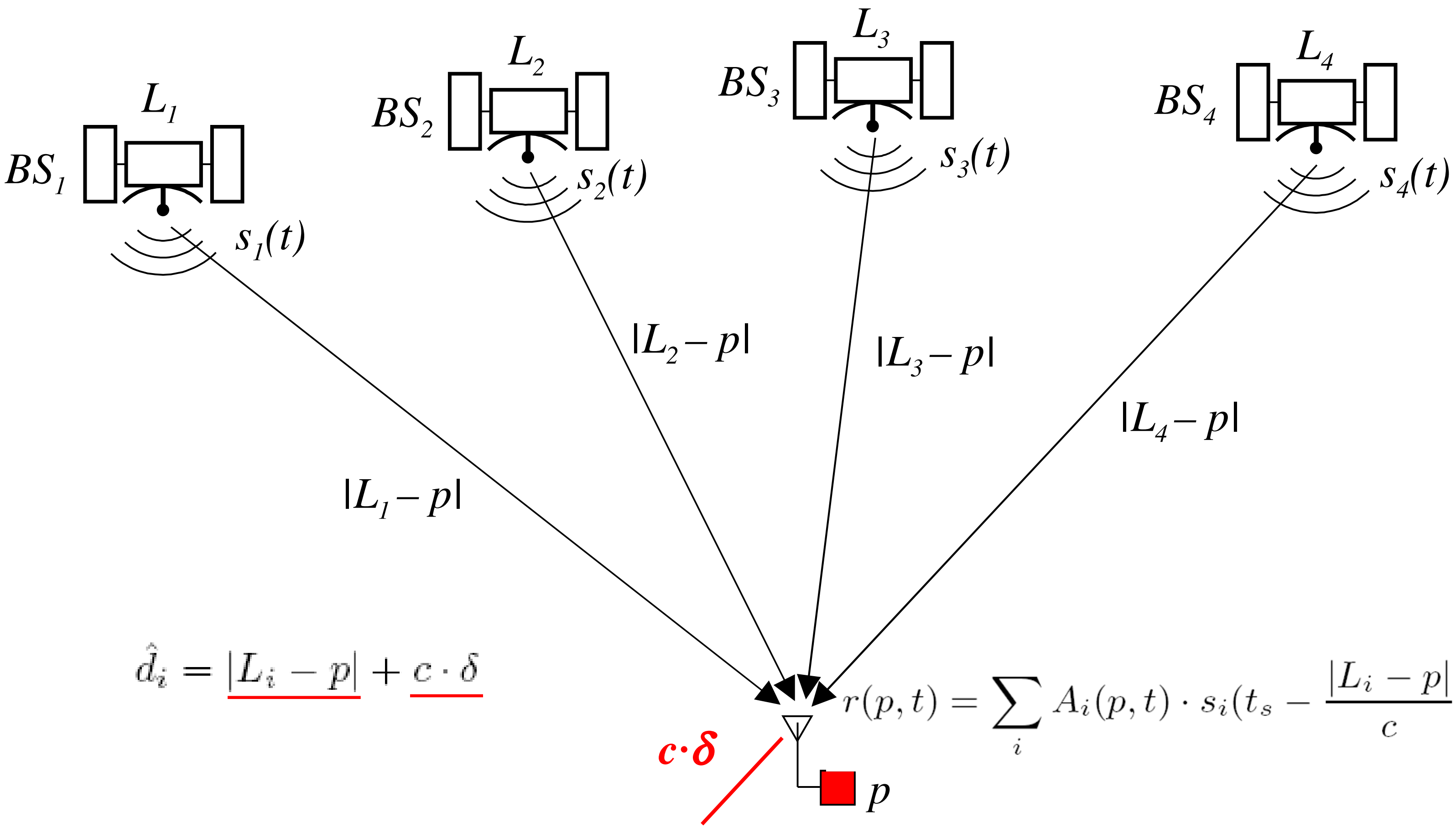
untrusted device (U)

- no trust in user or in hardware
- *attacks: external and internal*



Securing Asymmetric Localization Systems [Kuhn, 2004]

GPS/Galileo (Broadcast ToA Localization)



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

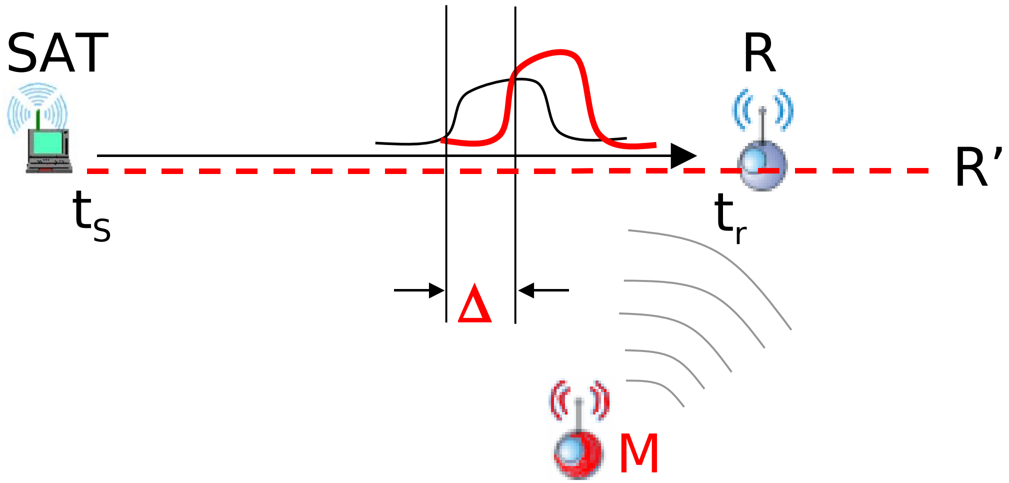
$$r(p,t) = \sum_i A_i(p,t) \cdot s_i\left(t_s - \frac{|L_i - p|}{c} + \delta\right) + n(\mathbf{p}, t)$$

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

GPS vulnerabilities

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

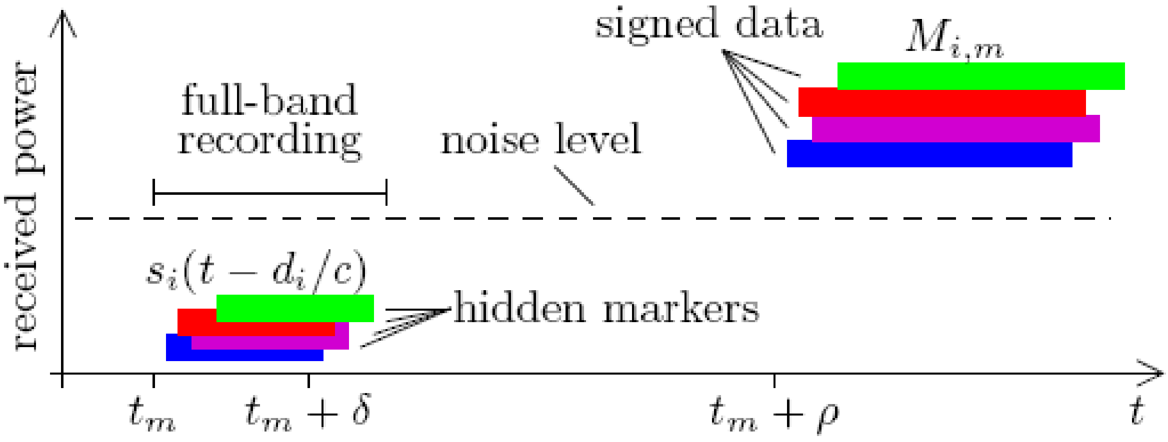
$\hat{d}_i = |L_i - p| + c\cdot\delta$ => $\hat{d}_i = |L_i - p| - c\cdot\delta + c\cdot\Delta_i$



Main Idea

- Devices hold satellite public keys
- At time t, a satellite uses a secret code to spread the navigation signal
- The receiver uses a broadband receiver to receive the whole signal band (receiver does not know the de-spreading code yet)
- At time $t+\Delta t$, the satellite discloses its secret code, signed with its private key

Securing GPS (Kuhn, 2004)



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

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

Short Analysis

- Prevents a replay of individual satellite signals
- Does not prevent replay of aggregated navigation signals

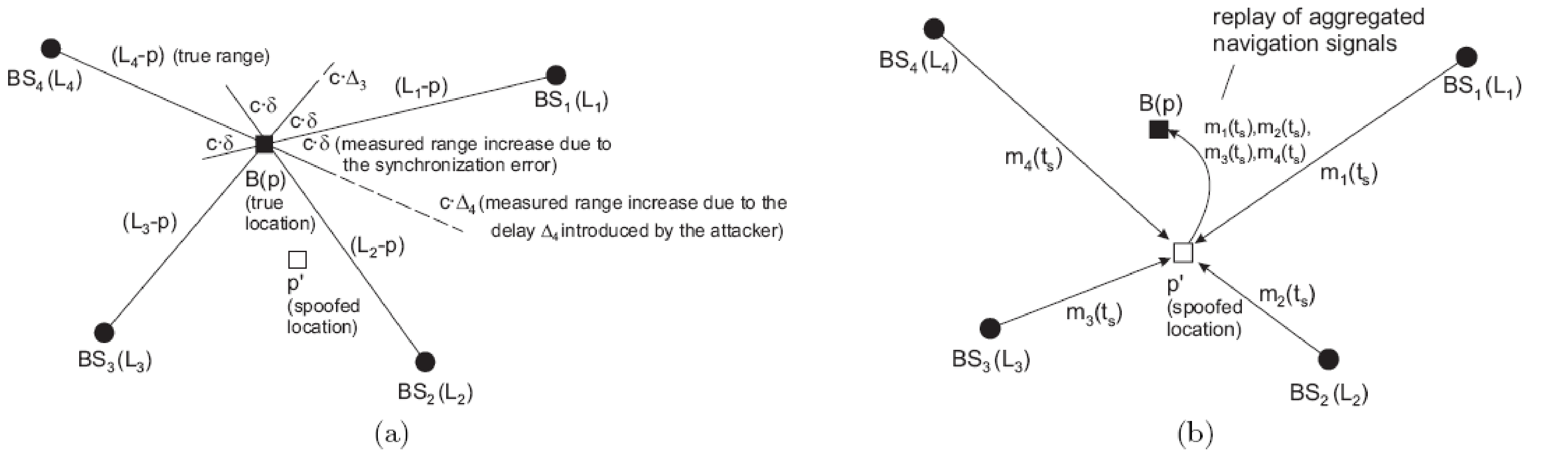


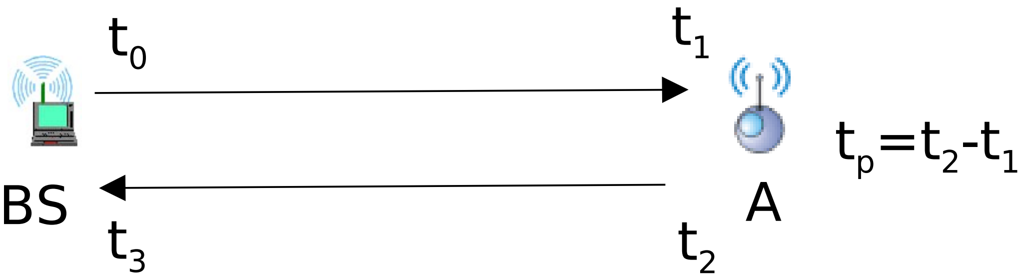
Figure 3. Examples of attacks on localization: (a) Pulse-delay attack. Navigation messages are delayed (i.e., by Δ_3 and Δ_4) by the attacker, causing an increase of measured ranges and the computation of a spoofed location p' by the device B; (b) Replay of aggregated navigation signals. Navigation messages from location p' are relayed to the device B (at location p), which then believes that it is located at p'.

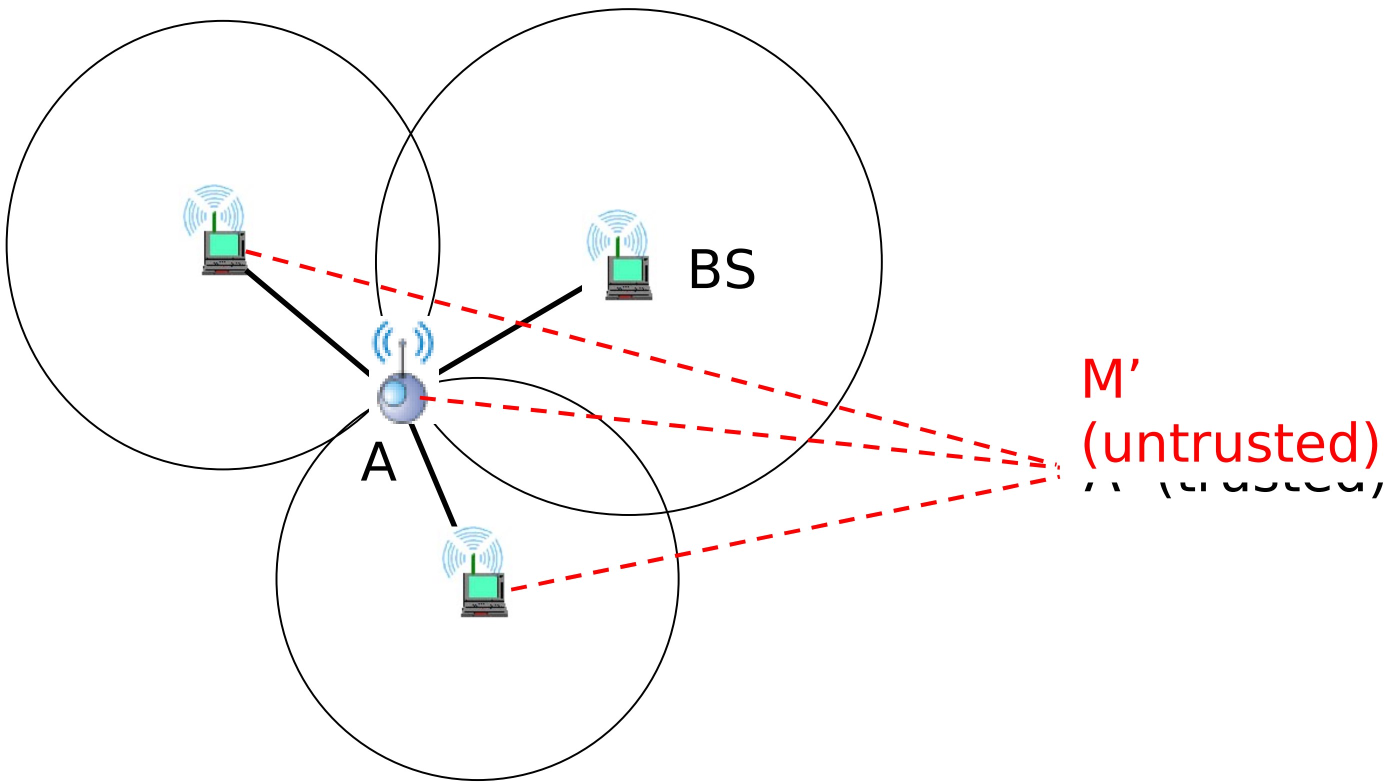
Verifiable Multilateration [Capkun, Hubaux, 2004]

Multilateration

Ranging: time of arrival (TOA) with radio signals

$$d = c\,\frac{(t_3 - t_0) - t_p}{2}$$





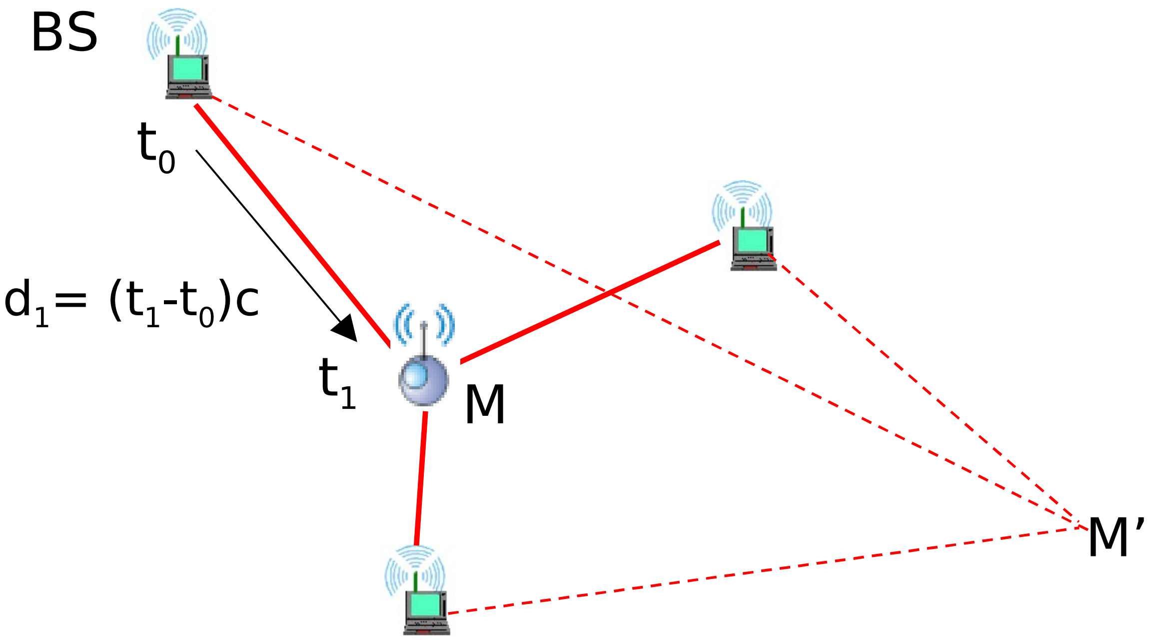
Attacks on TOA Multilateration

Untrusted device (M)

- distance enlargement/reduction
  (reporting false pulse reception time (t_1))

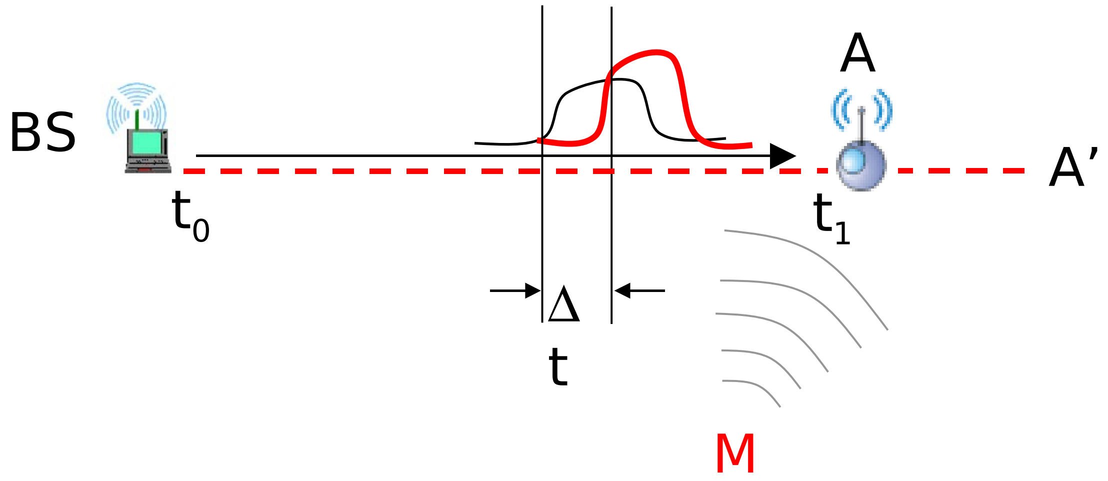
External attacks

- distance reduction/enlargement
  (pulse-delay, signal overshadowing, signal amplification, signal annihilation, replays)



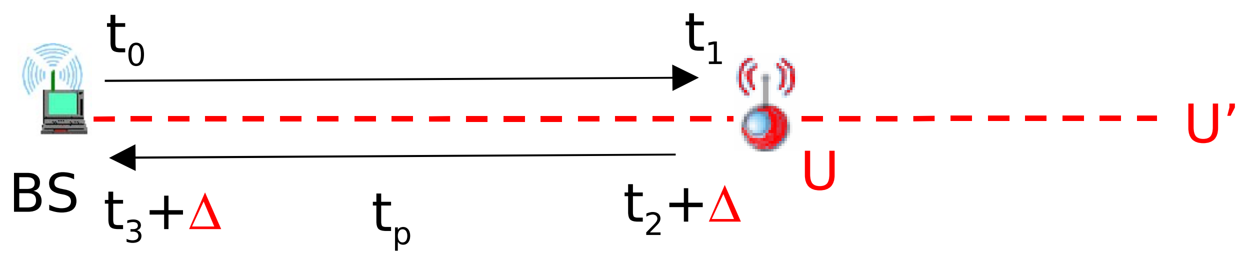
External attacks

- distance enlargement
  - pulse-delay, overshadowing, signal amplification, annihilation
  - example: range pull-out (radar anti-detection technique)
- distance reduction
  - early replays (predictable loc. signals, no freshness)
  - example: GPS signal overshadowing, radar range pull-in



Untrusted device (internal attacks)

Internal pulse-delay attack (untrusted node):



$t_p=t_2-t_1$

$$d = c\,\frac{(t_3+\Delta-t_0)-t_p}{2}$$

U enlarges the measured distance by delaying the response by Δ .

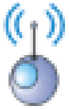
U cannot reduce the measured distance

- *iff* t_p is upper bounded by a small constant ε (distance-bounding*)

Preventing distance reduction: external attacks

- enforcing device (user) authentication and freshness
- making localization signals unpredictable for the attacker

(BS)



(A)

Pick $N_B \in_U \{0,1\}^k$

Pick $N_A \in_U \{0,1\}^k$

$(c, d) \leftarrow \text{commit}(N_A)$

$(BS) \xleftarrow{c} (A)$

$(t_0) \xrightarrow{N_B} (t_1)$

$(t_3) \xleftarrow{N_A \oplus N_B} (t_2)$

N_B and $N_A \oplus N_B$ are unpredictable for the adversary

$m = \{d, N_A, N_B, A, B, t_1, t_2\}$

$M \leftarrow MAC_K\{m\}$

$(BS) \xleftarrow{m, M} (A)$

$$d = v\,(t_3 - t_0 - t_p)\,/2$$

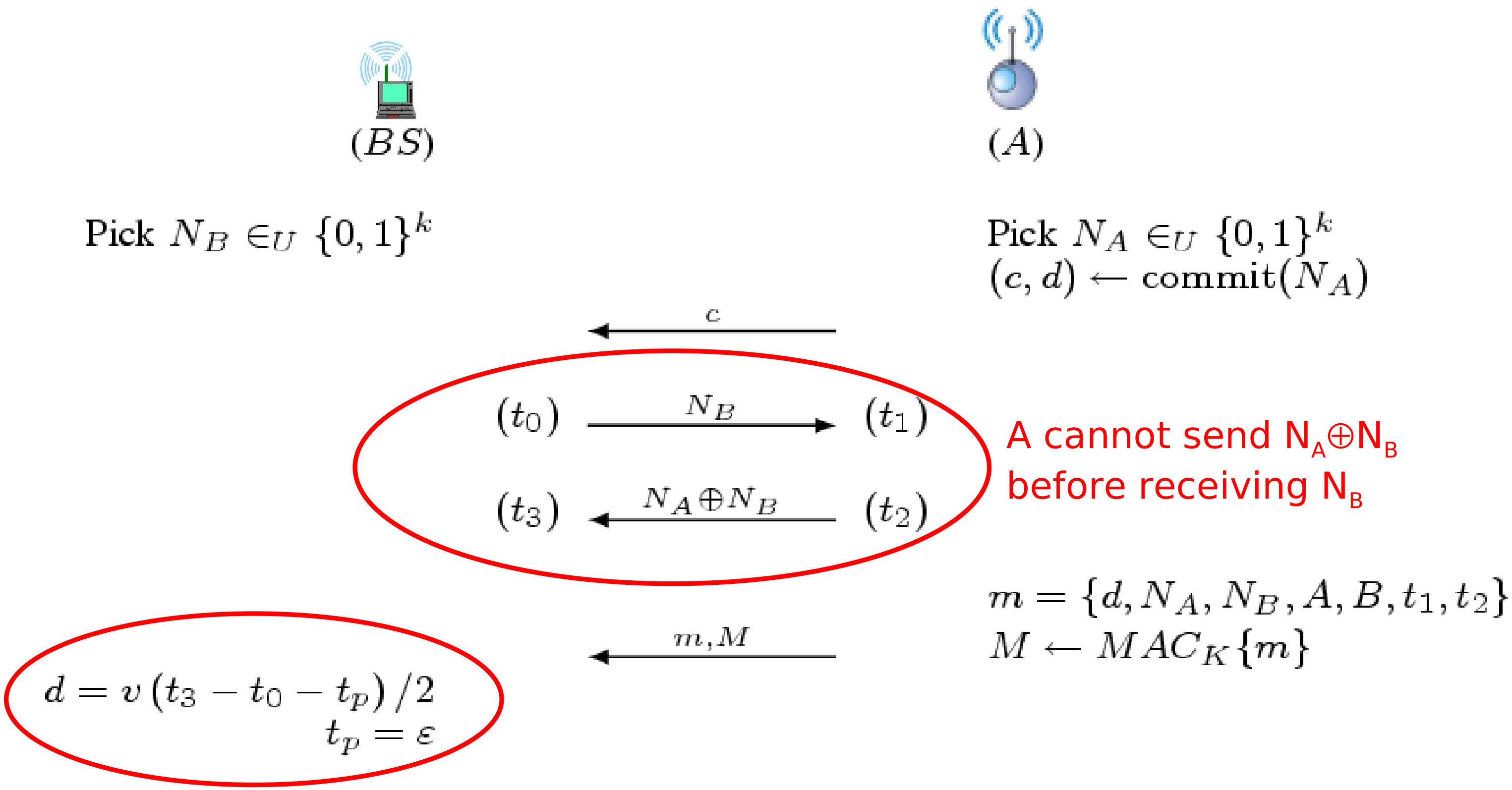
$$t_p = t_2 - t_1$$

authenticated ranging protocol

we still need to trust A to report correct processing time t_p

Preventing distance reduction: internal (and external) attacks

- enforcing device (user) authentication and freshness
- making localization signals unpredictable
- enforcing bounds on processing time



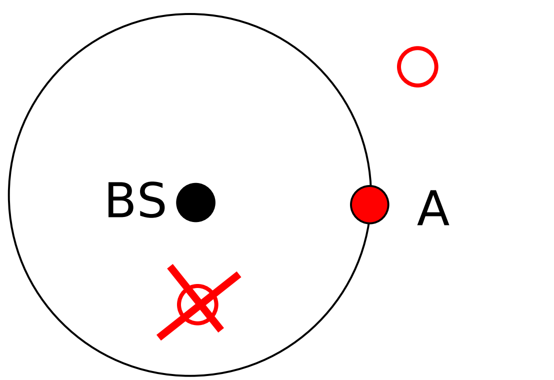
A cannot send $N_A \oplus N_B$ before receiving N_B

A's processing time is upper-bounded by an ε delay

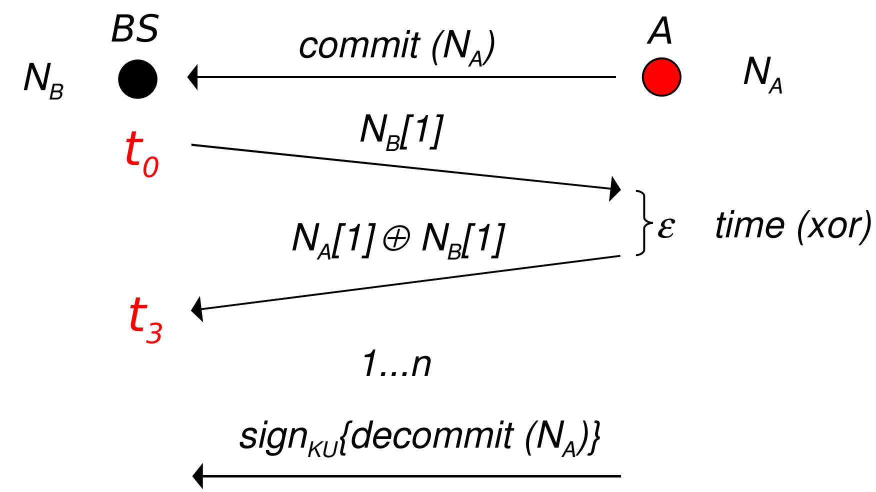
distance-bounding protocol*

*Brands and Chaum, 1993

Example: Distance bounding (Verification)



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



$$d = c\frac{(t٣ - t٠)}{٢}$$

$$t_p = \varepsilon$$

Brands and Chaum, 1993

Many variants and implementations followed.

Summary: prevention of attacks on RF ranging

External attacks

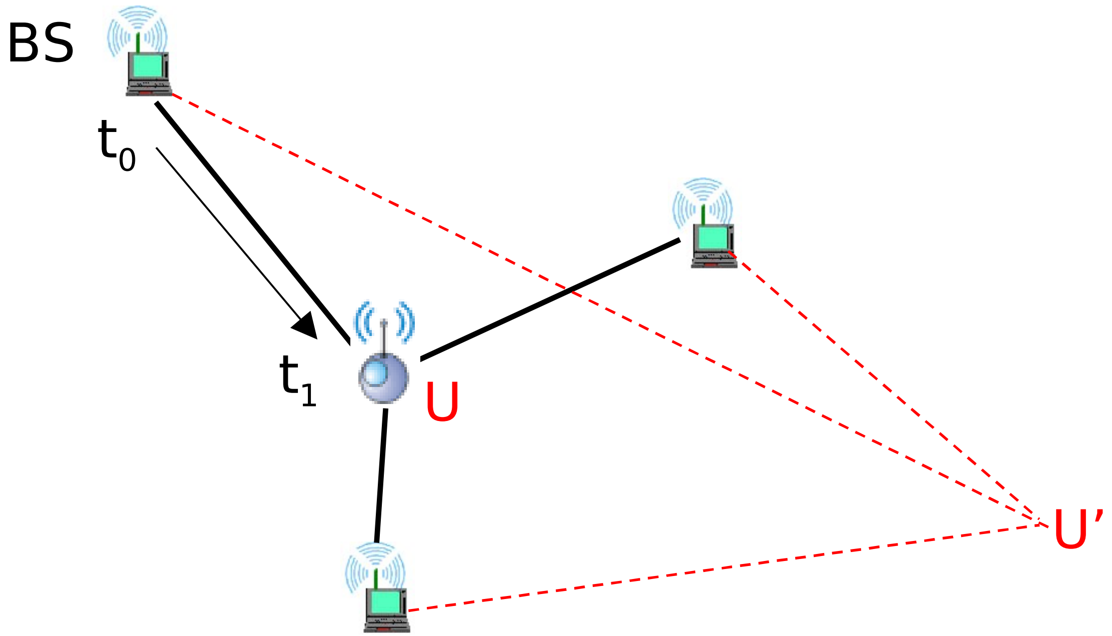
- Distance enlargement is *hard* to detect
  - a sophisticated attacker can *always* jam-and-replay, perform overshadowing, ...
- Distance reduction is *easy* to prevent
  - the signal travels at a speed of light and cannot be made to propagate faster
  - replays can be prevented with authentication and freshness

Untrusted device

- Distance enlargement is *hard* to detect
  - an untrusted device can always delay responses, report false reception times
- Distance reduction *can be* prevented
  - distance bounding protocols

Summary of attacks

- distance enlargement is possible
  - external attacker
  - untrusted node
- reduction is prevented (distance bounding)

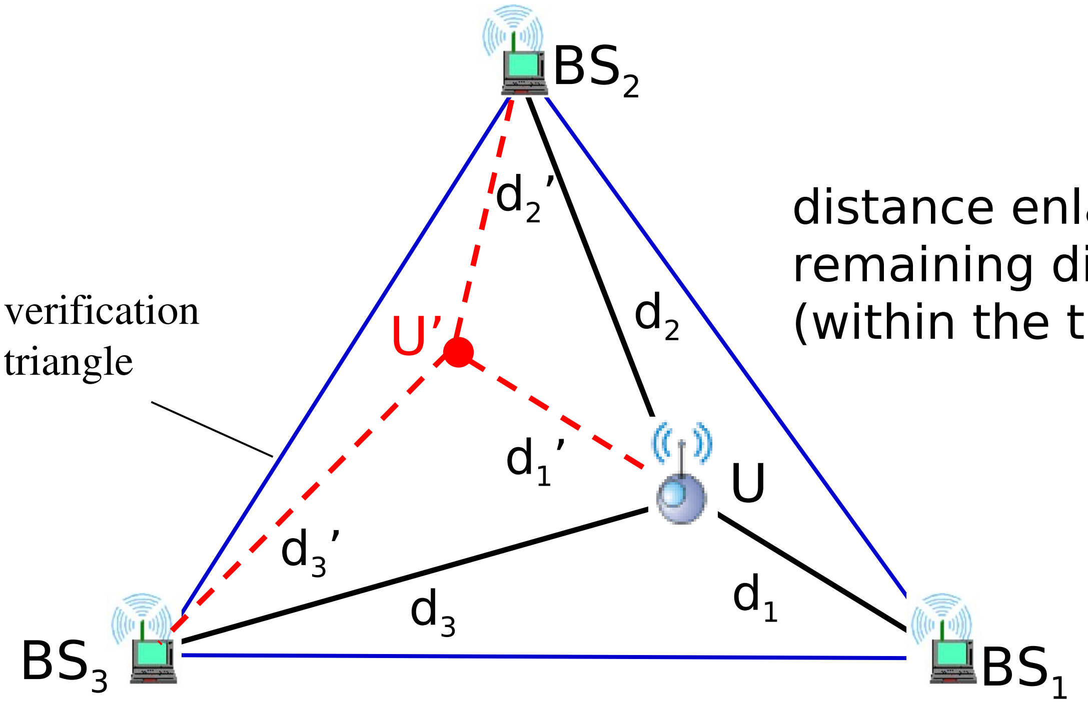


the attacker can still fake its location by only enlarging distances

[VM] Verifiable Multilateration

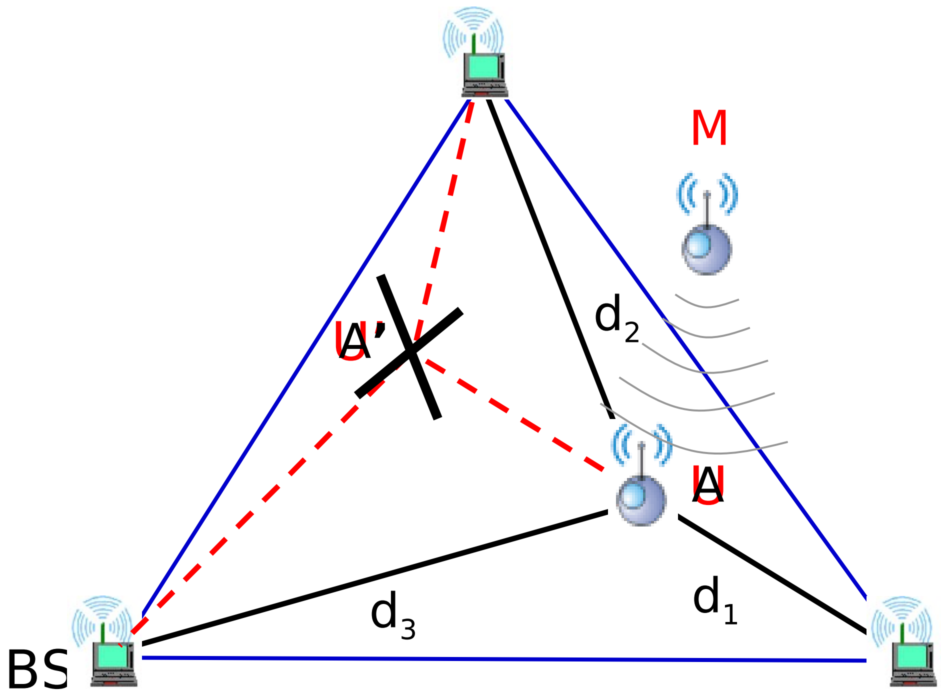
Three simple steps:

1. “Form a triangle” of BSs with known locations
2. Compute the location of a device (multilateration)
3. If the computed location is in the triangle => it is valid (not faked or spoofed)



distance enlargement implies one of the remaining distances being reduced (within the triangle)

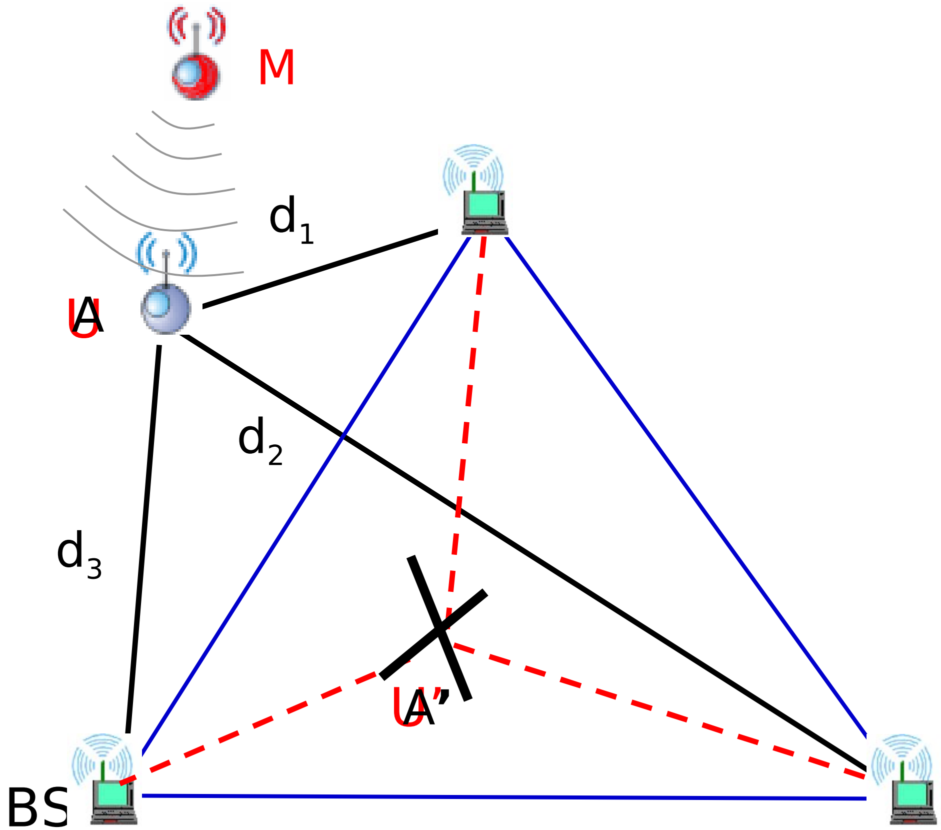
[VM] properties (1&2)



1. an untrusted device U within a triangle
   cannot pretend to be at any other location
   U’ within the triangle

2. a trusted device A within a triangle cannot
   be spoofed to be at any other location A’
   within the triangle

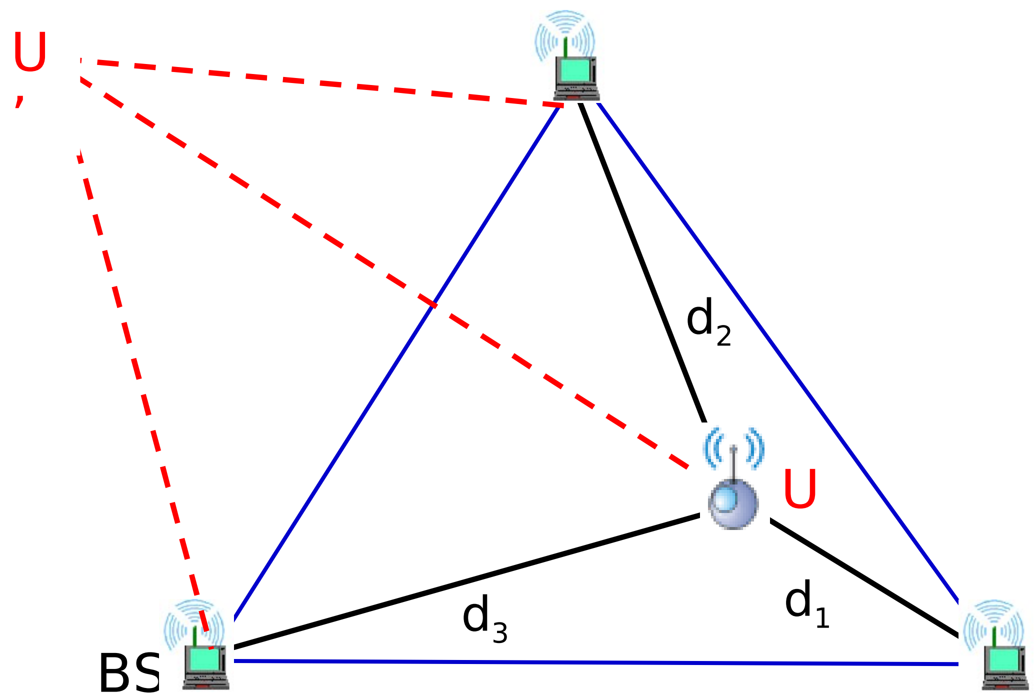
[VM] properties (3&4)



3. an untrusted device U outside a triangle
cannot pretend to be at any location U'
within the triangle

4. a trusted device A outside a triangle cannot
be spoofed to be at any location A'
within the triangle

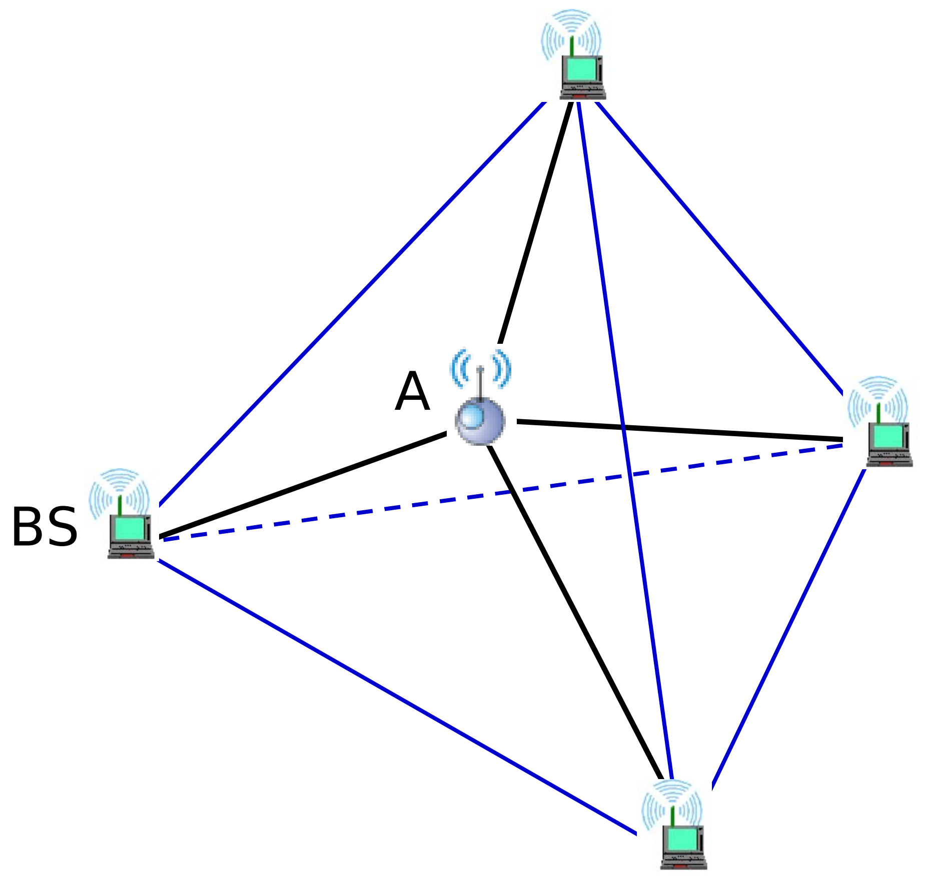
[VM] ‘Moving’ out of the triangle



No incentives.

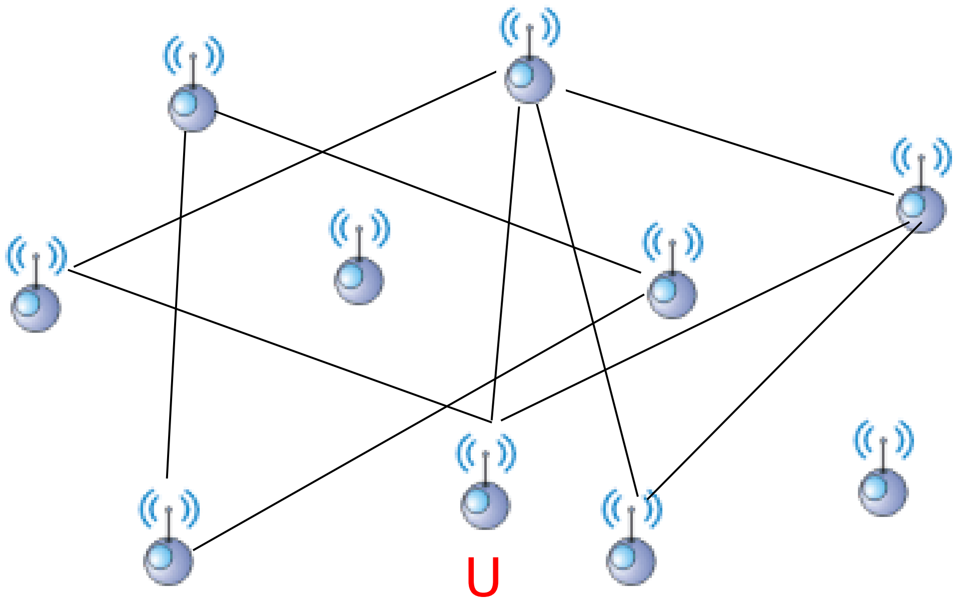
[VM] properties (3D)

- naturally extends to 3-D (ceiling and floor installations indoors)



[VM] More on verifiable multilateration

- Taking into account ranging errors
  - security implications of error estimation
  - GDOP
- Application to sensor networks
  - infrastructure-based
  - distributed
- Extending the same principle to TDOA
  - single distance bounding + synchronized base stations
- Privacy implications (rogue base stations)
- Attacker Collusion



Distance-Bounding

Proposals

- Brands-Chaum [93]
- Capkun-Buttyan-Hubaux [2003], mutual DB
- Sastry-Shankar-Wagner [2003], ultrasonic DB
- Hancke-Kuhn [2005], RFID DB, robustness to message losses
- Capkun-Hubaux [2006]. authenticated ranging
- Singlee-Preneel [2007], mutual, robust to losses
- Rasmussen-Capkun [2008], location-private

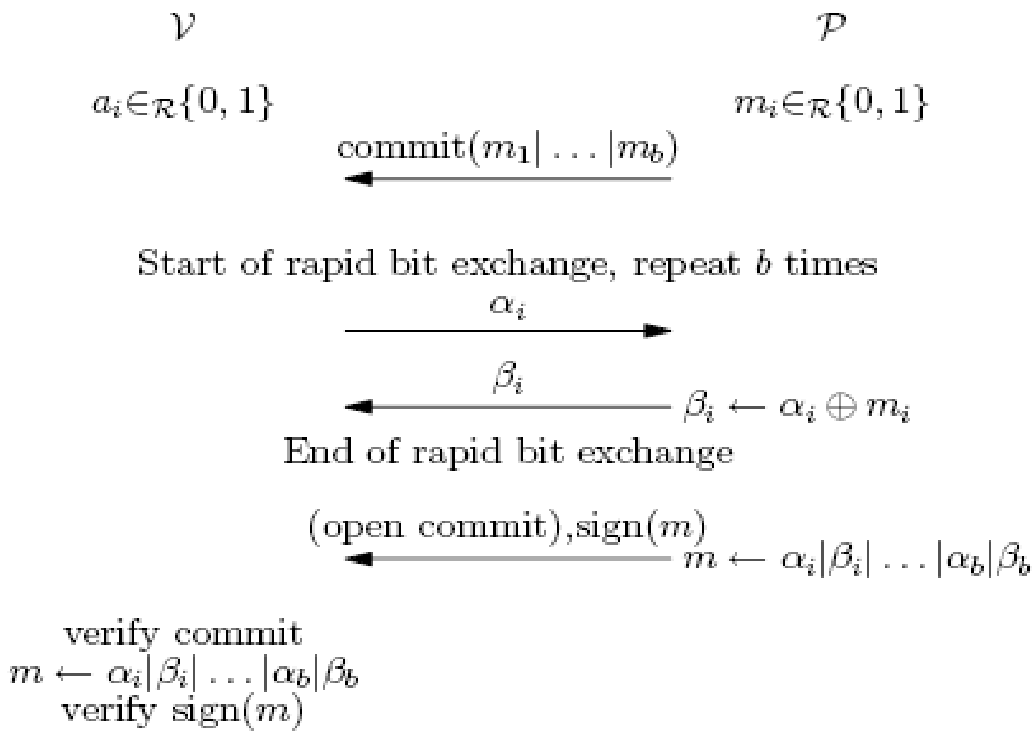
Analysis/Attacks:

- Clulow, Hancke, Kuhn [2006/2008], attacks
- Sedighpour et al [2005], demo of attacks on ultrasonic DB/AR

Implementations:

- Drimer, Murdoch [2007], wired implementation
- Munilla et al. [2006], wireless, 150m acc.
- Reid et al. [2007], wireless, 40m acc.
- Tippenhauer-Capkun [2008], wireless, auth. ranging, 15cm acc.

DB [Brands-Chaum 2003]

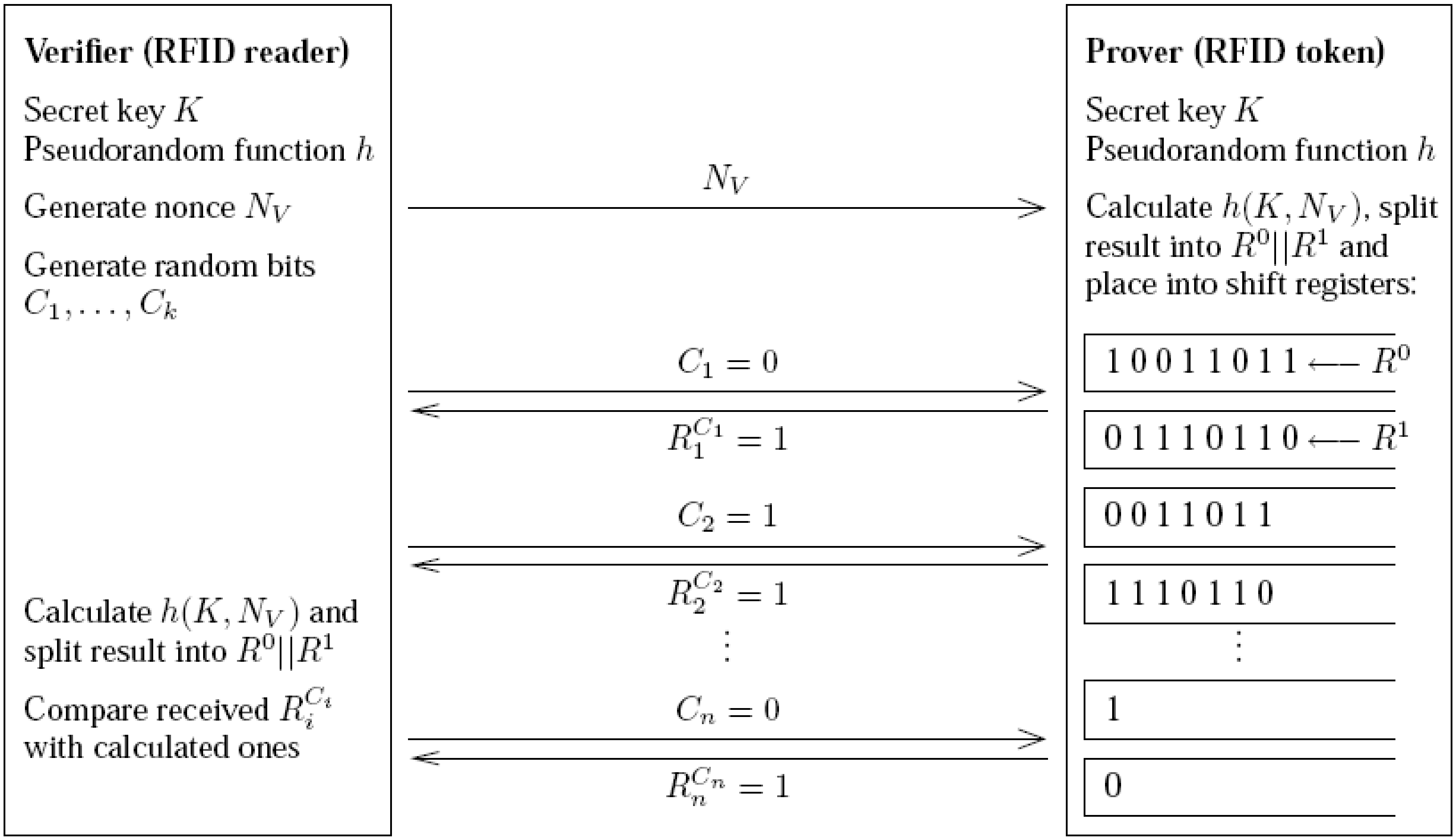


(a) Distance bounding

Mutually Authenticated DB [Capkun-Buttyan-Hubaux 03]

u		v
	— initialization phase —	
generate random numbers $r \in \{0,1\}^{\ell}$, $r' \in \{0,1\}^{\ell'}$		generate random numbers $s \in \{0,1\}^{\ell}$, $s' \in \{0,1\}^{\ell'}$
compute commitment $c_u = H(r\|r')$		compute commitment $c_v = H(s\|s')$
	$\xrightarrow{c_u}$	
	$\xleftarrow{c_v}$	
	— distance-bounding phase —	
the bits of r are $r_1, r_2, \ldots, r_\ell$		the bits of s are $s_1, s_2, \ldots, s_\ell$
$\alpha_1 = r_1$	$\xrightarrow{\alpha_1}$	
	$\xleftarrow{\beta_1}$	$\beta_1 = s_1 \oplus \alpha_1$
	$\ldots$	
$\alpha_i = r_i \oplus \beta_{i-1}$	$\xrightarrow{\alpha_i}$	measure delay between β_{i-1} and α_i
measure delay between α_i and β_i	$\xleftarrow{\beta_i}$	$\beta_i = s_i \oplus \alpha_i$
	$\ldots$	
$\alpha_\ell = r_\ell \oplus \beta_{\ell-1}$	$\xrightarrow{\alpha_\ell}$	measure delay between $\beta_{\ell-1}$ and α_ℓ
measure delay between α_ℓ and β_ℓ	$\xleftarrow{\beta_\ell}$	$\beta_\ell = s_\ell \oplus \alpha_\ell$
	— authentication phase —	
$s_i = \alpha_i \oplus \beta_i \ (i = 1, \ldots, \ell)$		$r_1 = \alpha_1$ and $r_i = \alpha_i \oplus \beta_{i-1} \ (i = 2, \ldots, \ell)$
$\mu_u = mac_{k_{uv}}(u\|v\|r_1\|s_1\|\ldots\|r_\ell\|s_\ell)$		$\mu_v = mac_{k_{uv}}(v\|u\|s_1\|r_1\|\ldots\|s_\ell\|r_\ell)$
	$\xrightarrow{r'\|\mu_u}$	
	$\xleftarrow{s'\|\mu_v}$	
verify c_v and μ_v		verify c_u and μ_u

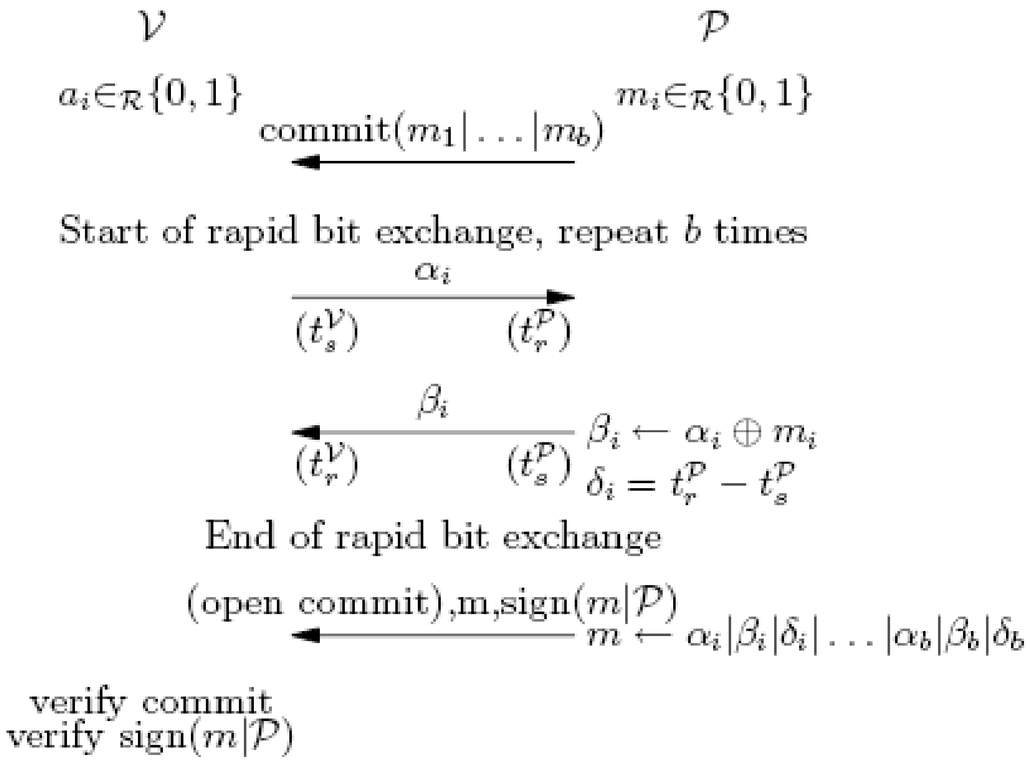
RFID DB [Hanke-Kuhn 05]



$\langle C_i \rangle = 01001100$ will return $\langle R_i^{C_i} \rangle = 11010111$

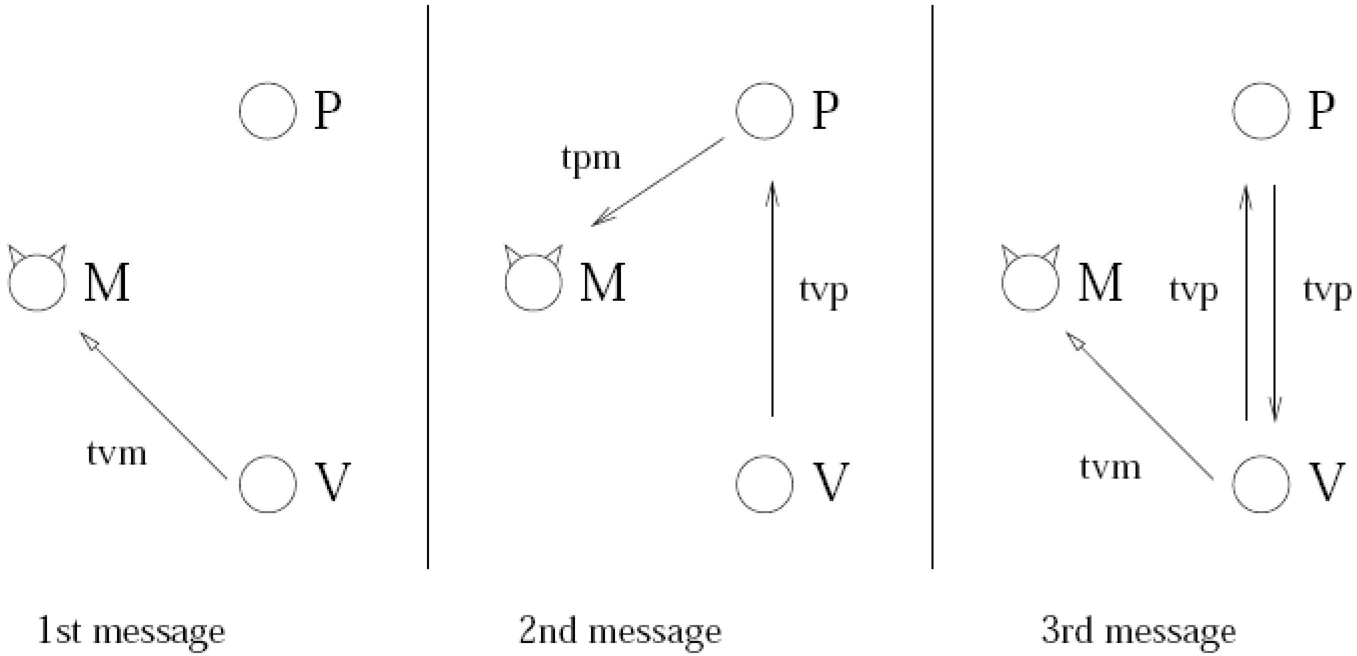
Robust to loses – another protocol by Singlee and Preneel

Authenticated Ranging [Capkun-Hubaux 06]



(b) Authenticated ranging

Location-Private DB [Rasmussen-Capkun 08]



$$T_0 = t_0 + t_{vm}$$
$$T_1 = t_0 + t_{vp} + \delta_p + t_{pm}$$
$$T_2 = t_0 + 2t_{vp} + \delta_p + \delta_v + t_{vm}$$

$$\Rightarrow \quad t_{vp} = \frac{(T_2 - T_0) - \delta_p - \delta_v}{2}$$

Distances leak from DB protocols

Location-Private DB [Rasmussen-Capkun 08]

Location Private Distance Bounding Protocol

$$P \qquad\qquad\qquad V$$

$$N_p \in \{0,1\}^k$$

$$\xrightarrow{E_{K_{pv}}(P,V,N_p)||MAC}$$

$$N_v \in \{0,1\}^k$$
$$HM \in \{0,1\}^j$$

$$\xleftarrow{E_{K_{pv}}(V,P,HM,N_p)||MAC}$$

$$\overset{Rand||HM||N_v||Rand}{\leftsquigarrow}$$

$$\overset{Rand||N_v \oplus N_p||Rand}{\rightsquigarrow}$$

VM implementation [Tippenhauer-Capkun 2008]

Features

- UWB based ToA distance measurement
- "detects leading edge of direct propagation path"
- Serial interface

VM implementation [Tippenhauer-Capkun 2008]

Technical details

- range $\approx$ 50m LoS, 20m NLoS
- Resolution 15cm=1ns
- "mean precision less than 4 cm"
- 75μs antenna switching time at the prover
- pulse repetition rate 2Mp/s
- 56μs packet length, 14 Bytes incl. ECC
- total power: 800mW
- Main frequency range 6.1-6.6 GHz
- Based on Altera Cyclone II FPGA

VM implementation [Tippenhauer-Capkun 2008]

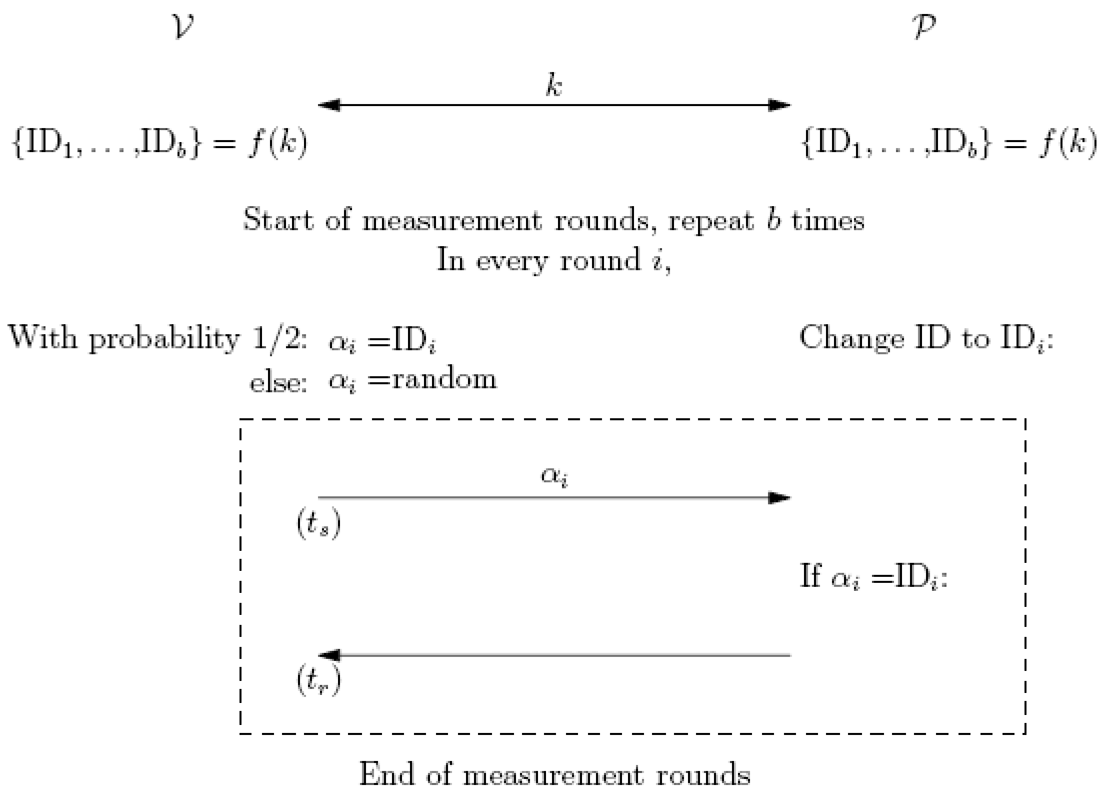
Restrictions

- No data is transmitted in the measurements
- No access control or authentication
- Some features are problematic in the security context
- No access to FPGA code
- No real documentation

Useful features

- 16 bit ID
- IDs can be changed quickly

VM implementation [Tippenhauer-Capkun 2008]



$\mathcal{V}$ processes measurements, $\forall i \leq b$:
If $\alpha_i = \mathrm{ID}_i$ and answer is received, use d_i provided by the device
If $\alpha_i \neq \mathrm{ID}_i$ and answer is received, report attack
If $\alpha_i = \mathrm{ID}_i$ and no answer is received, report loss
If $\alpha_i \neq \mathrm{ID}_i$ and no answer is received, continue
Final distance bound: $\max(d_i)$

Some results

- Measurement results LoS/NLoS

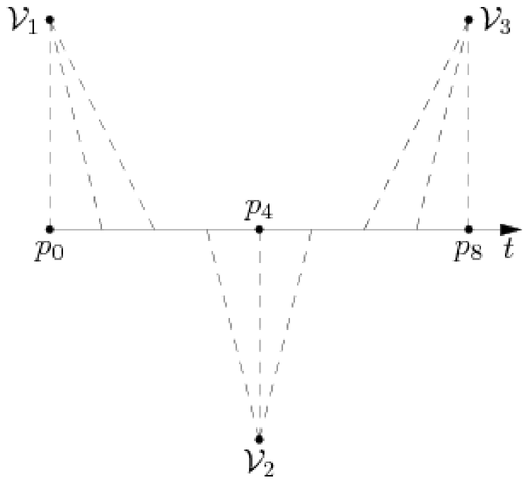
(a) LoS measurements

d in m	σ in cm	losses	$\bar{d} - d$ in cm	$d_m - d$ in cm
5	10.23	0	-5.00	9.25
10	9.60	0	8.25	30.65
15	9.05	0	17.32	36.75
20	9.66	0	24.41	38.95
25	9.54	0	31.94	48.20
30	9.97	0	39.30	58.50
35	9.31	0	44.22	65.65
40	10.23	0	289.99	304.40

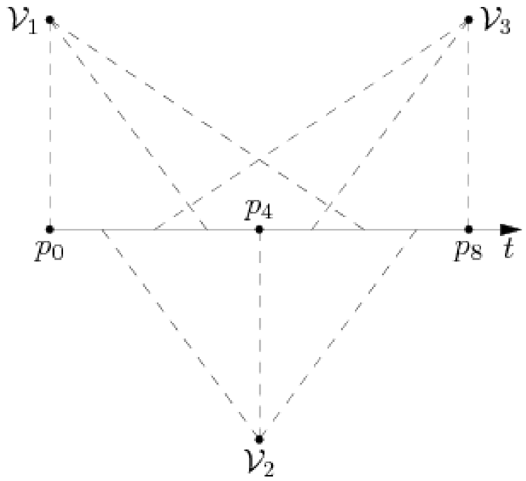
(b) NLoS measurements

d in m	σ in cm	losses	$\bar{d} - d$ in cm	$d_m - d$ in cm
5	8.64	0	40.81	57.10
10	11.54	0	63.61	82.10
15	19.46	0	105.57	132.60
20	16.37	0	123.23	158.35
25	14.92	0	148.54	177.65
30	14.41	0	120.06	147.15
35	253.33	483	240.68	722.35
40	52.78	30	448.13	527.37

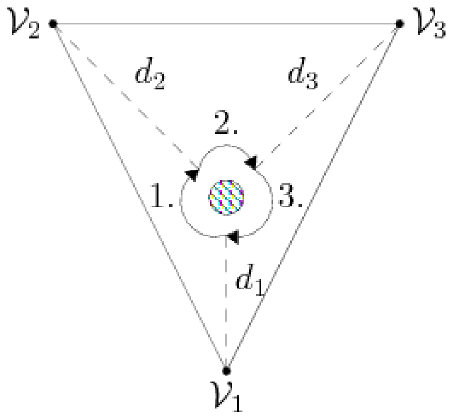
Application to Verifiable Multilateration



(a) Sequential ranging



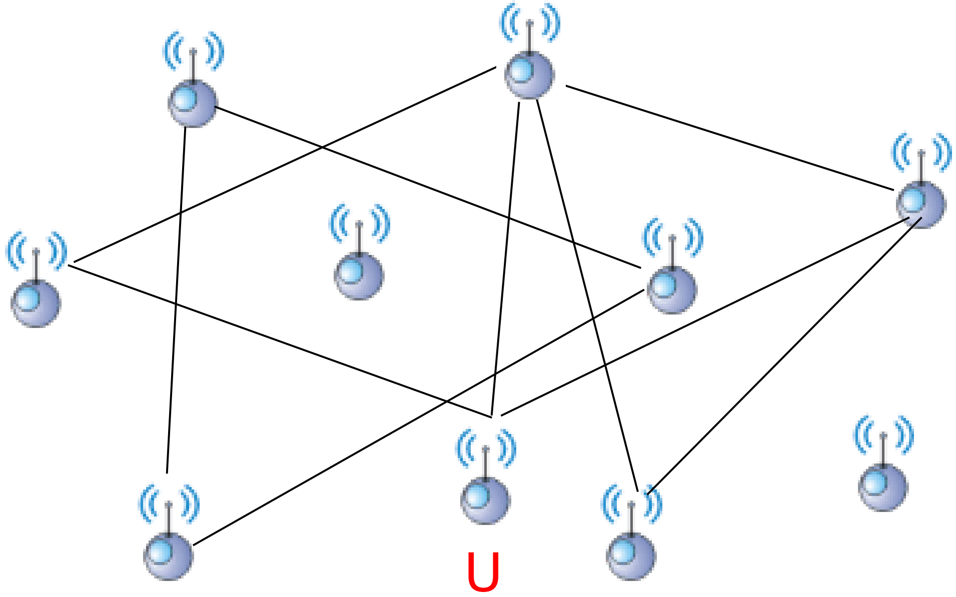
(b) Interleaved ranging



(c) Movement attack

[VM] More on verifiable multilateration

- Taking into account ranging errors
  - security implications of error estimation
  - GDOP
- Application to sensor networks
  - infrastructure-based
  - distributed
- Extending the same principle to TDOA
  - single distance bounding + synchronized base stations
- Privacy implications (rogue base stations)



Capkun, Hubaux, *Secure positioning of wireless devices with application to sensor networks*, INFOCOM 2005, JSAC 2006

US-based Verifiable Multilateration

- RF TOA techniques might me expensive
- Ultrasonic ranging is readily available today
  (only ms processing, 1ms ~ 34cm)
- We again construct verifiable multilateration, now using ultrasonic distance bounding

(BS)		(A)
Pick $N_B \in_U \{0,1\}^k$		Pick $N_A \in_U \{0,1\}^k$ $(c, d) \leftarrow \mathrm{commit}(N_A)$
	$\xleftarrow{\quad c \quad}$	
(t_0)	$\xrightarrow{\quad N_B \quad}$	(t_1)
(t_3)	$\xleftarrow{\; N_A \oplus N_B \;}$	(t_2)
		$m = \{d, N_A, N_B, A, B, t_1, t_2\}$ $M \leftarrow MAC_K\{m\}$
	$\xleftarrow{\quad m, M \quad}$	
$d = v_{sound}\,(t_3 - t_0 - t_p)$ $t_p = \varepsilon$		

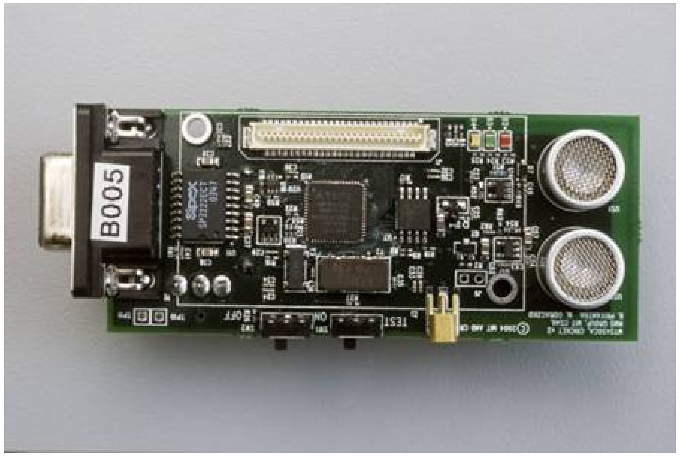
challenge sent through RF
response through US

ultrasonic distance bounding*

*Walters and Felten, 1998

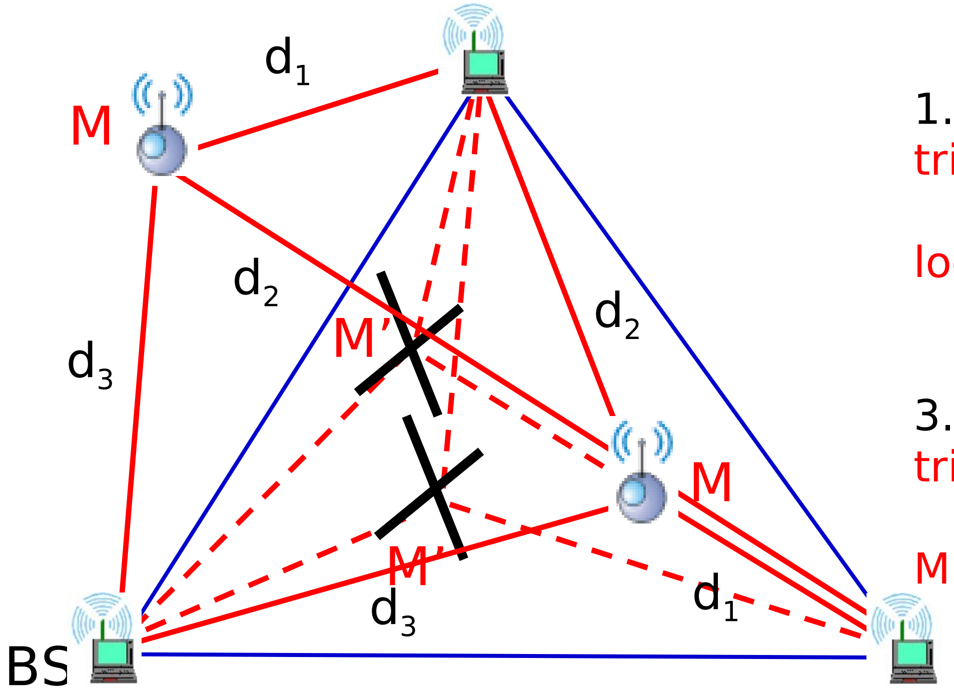
US distance bounding implementation

- Using MIT Cricket platform (Mica sensor platform + ultrasonic channel)
- TinyOS operating system with TinySec (key setup and MAC computations)
- approx. 5 cm accuracy of distance-bounds



US-based Verifiable Multilateration: properties

- with a single untrusted node we retain the same properties as with the RF-based verifiable multilateration



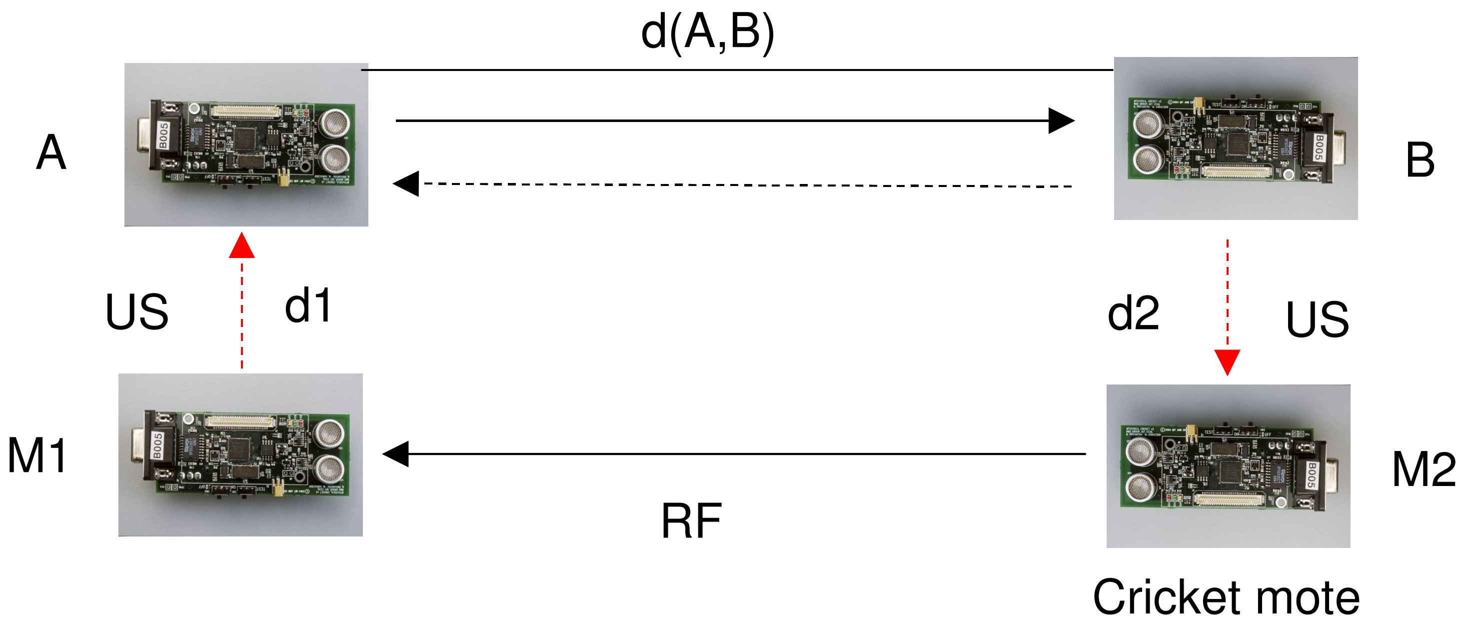
1. an untrusted device M within a triangle
   cannot pretend to be at any other location
   M' within the triangle

3. an untrusted device M outside a triangle
   cannot pretend to be at any location M'
   within the triangle

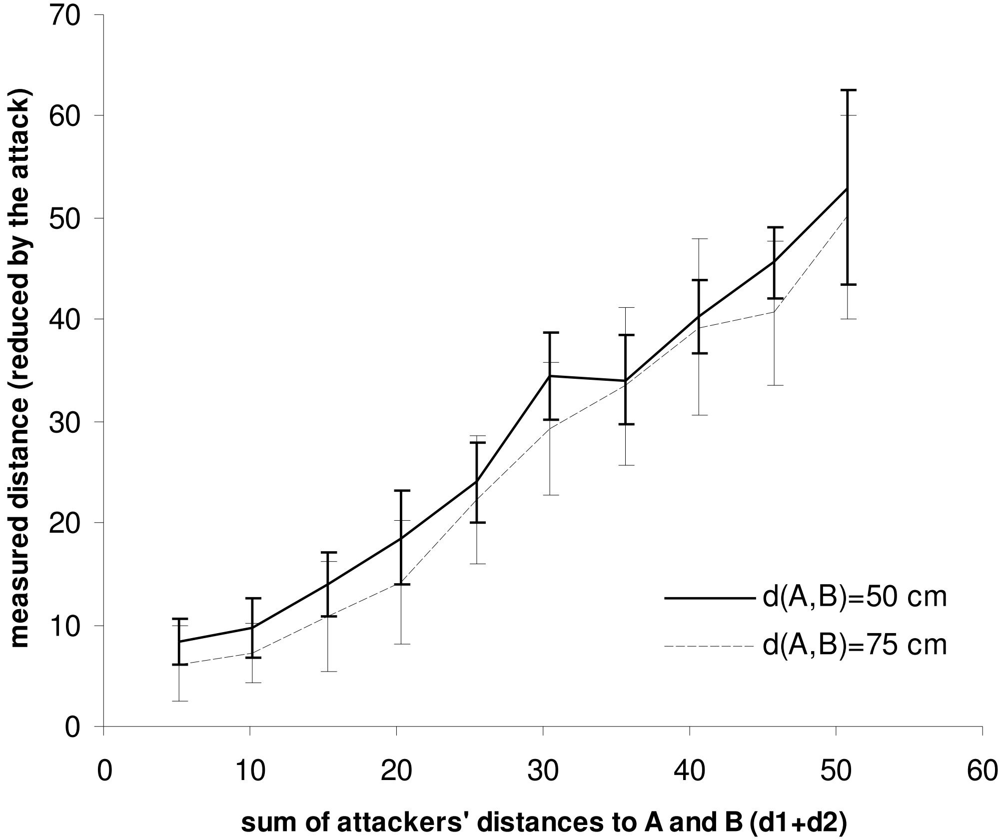
US-based Verifiable Multilateration: properties

- ultrasonic ranging/bounding is not robust to external distance modification attacks
  - distance enlargement (pulse-delay, i.e., jam-and-replay)
  - RF wormhole attacks

- Experimental setup

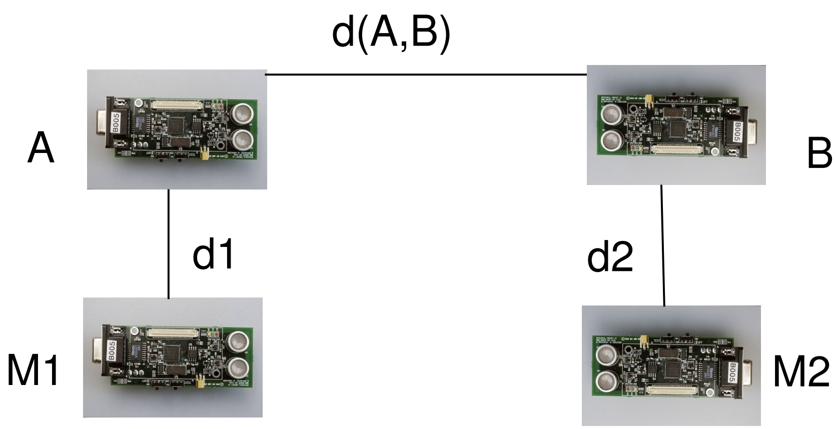


Results



- the maximal distance reduction depends on attackers' distances to victim nodes

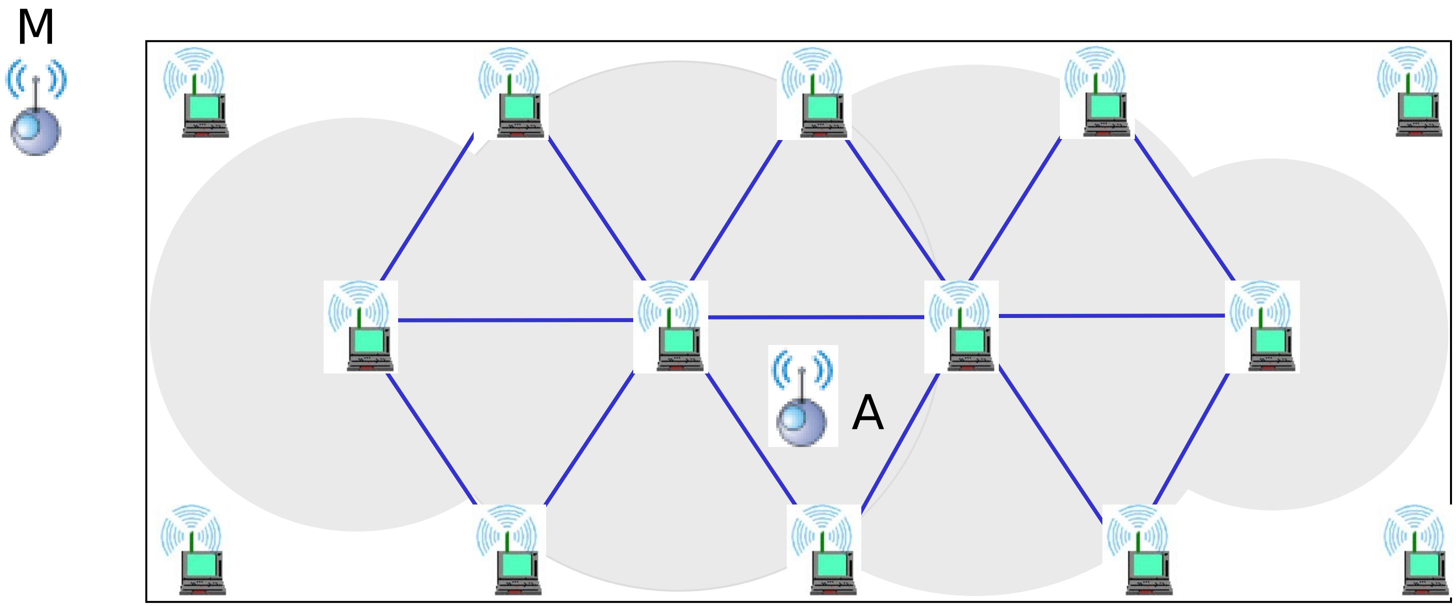
- no limits on distance enlargement



Sedighpour, Capkun, Ganeriwal, Srivastava, Sensys 2005

Implications of distance reduction attacks on US-based VM

- These are both positive and negative results:
  - negative in a sense that external attackers can reduce the measured distances
  - positive in the sense that to reduce distances, attackers need to be close to the base stations
- We can therefore still use US-based VM in some access control scenarios.



Location Verification With Hidden and Mobile Stations
[Capkun et al, 2006]

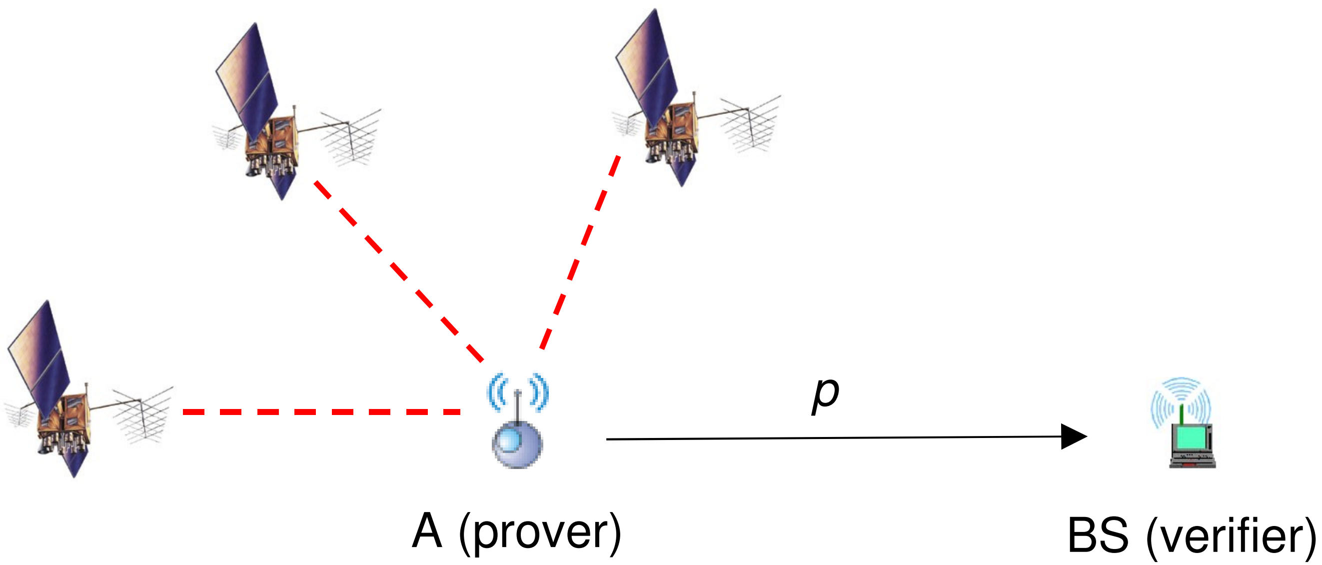
[Hidden]

- Capkun, Cagalj, Srivastava, Infocom 2006

+ Rasmussen, TMC 2008

- reliance on base stations with hidden locations
- mobile stations that enable verification of sensor locations

[Hidden] Problem: Location Verification



Assumptions:

- A obtains its location ***p*** through e.g., GPS
- A is not trusted by B to report the correct location
- BS holds a public key of A *(can authenticate A)*

How can BS ***verify*** the reported location ***p*** of A?

Note: A wants to be localized but wants to cheat on its location!

[Hidden] Motivation

Being able to securely verify a position of a node enables:

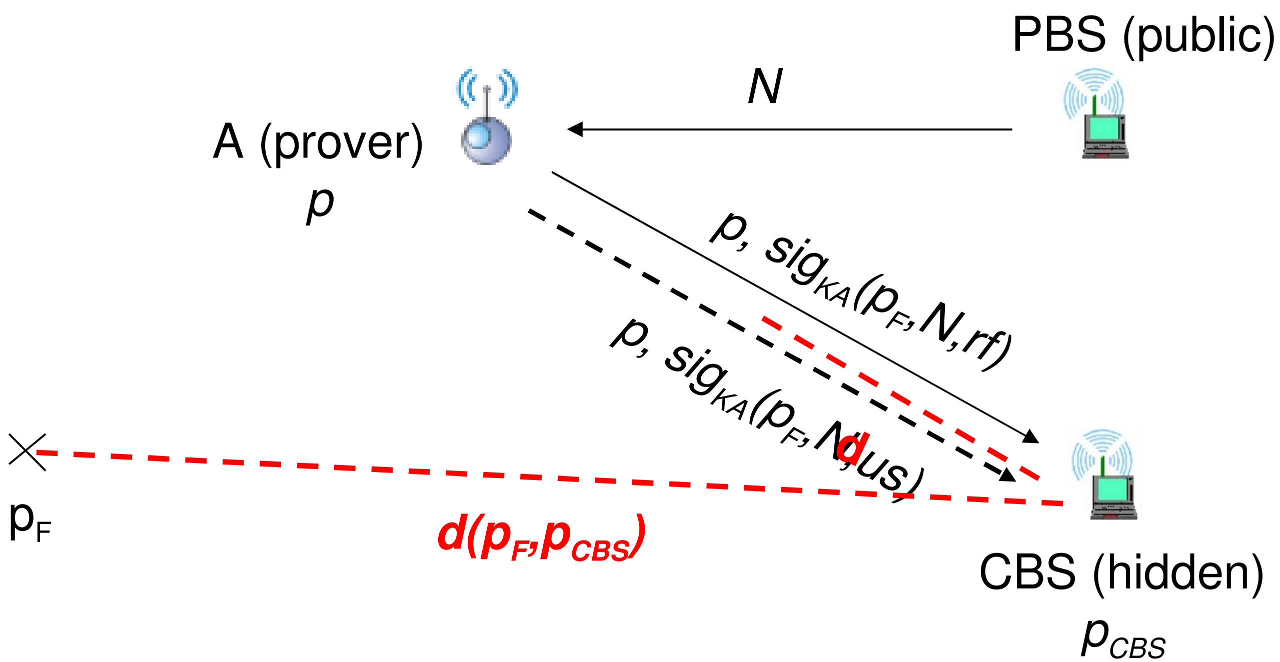
- Location-based access control
- Location-based charging
- Detection of displacement of valuables
- Monitoring and enforcement of policies (e.g., traffic monitoring)
- Secure location-based and encounter-based routing (ad hoc networks)
- Secure data harvesting (sensor networks)
- ...

[Hidden] Main idea

- Idea:
  - hide the location of (a subset of) base stations from the prover

- Note:
  - hidden base stations are passive (do not transmit any messages over their radio channel)
  - size of hidden base stations corresponds to the size of the localization region (i.e. in a room, these can be tiny sensors)

Location verification with Hidden Base Stations



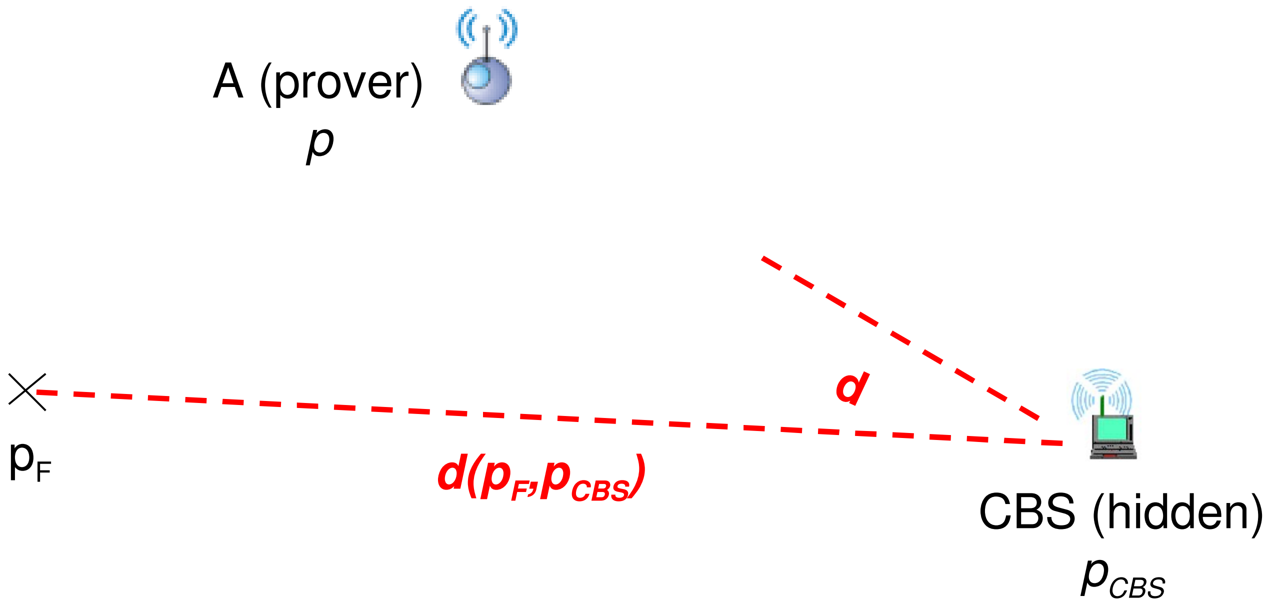
But can the prover make $d(p_F,p_{CBS}) = d$?

(without knowing p_{CBS})

Two ways of cheating:

- A lies about its location (sends p_F)
- A cheats on the measured distance d

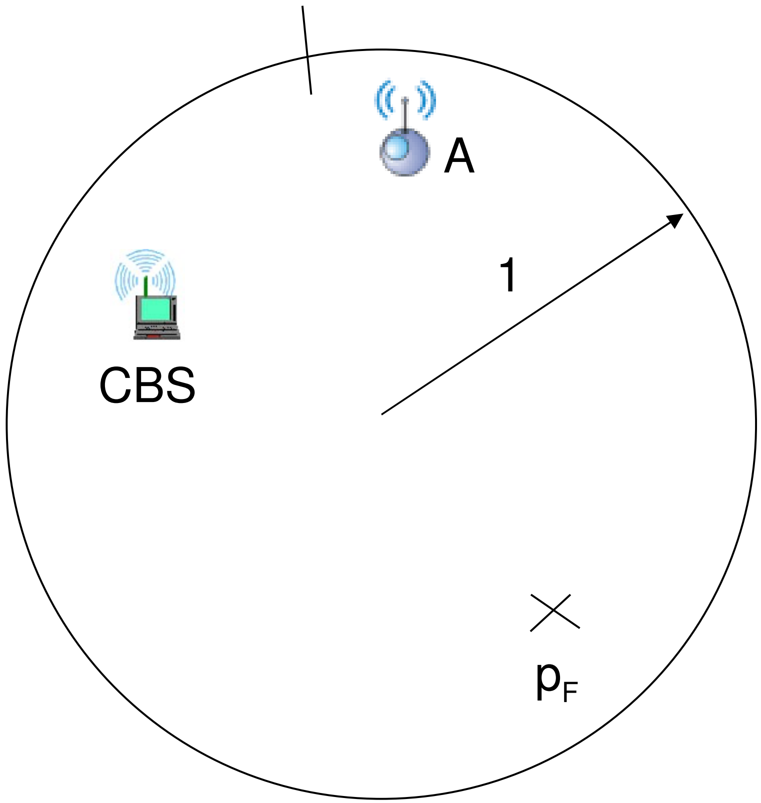
Attacker's success probability



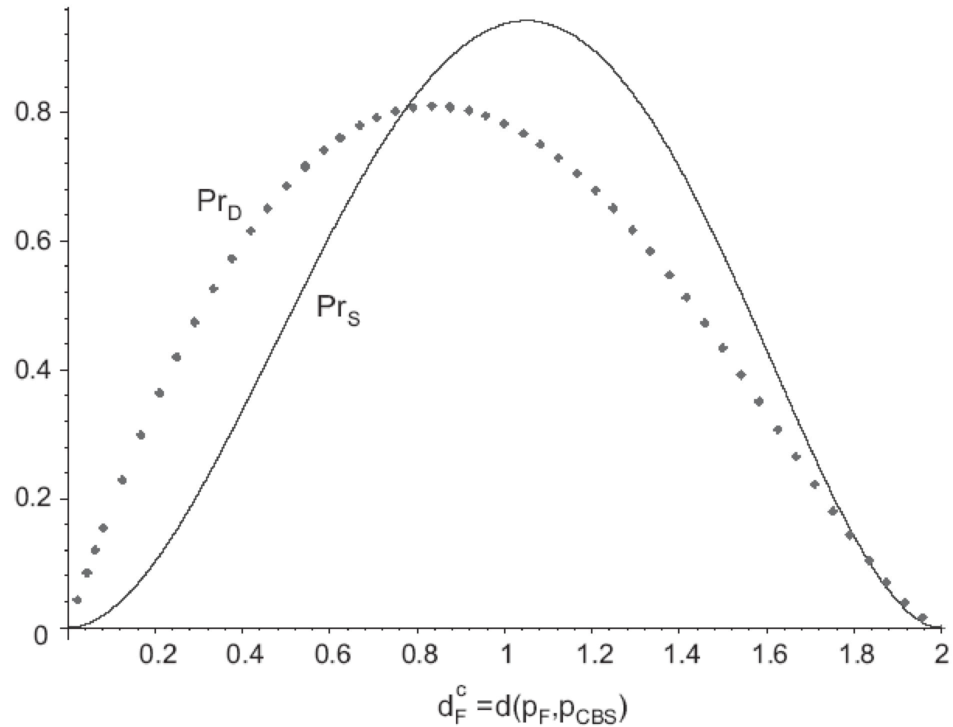
P_of_attacker_success = prob($d(p_F, p_{CBS}) - d \leq \Delta$)

Δ = the expected error depending on the localization and ranging accuracy

Attacker's success probability (guessing distances)



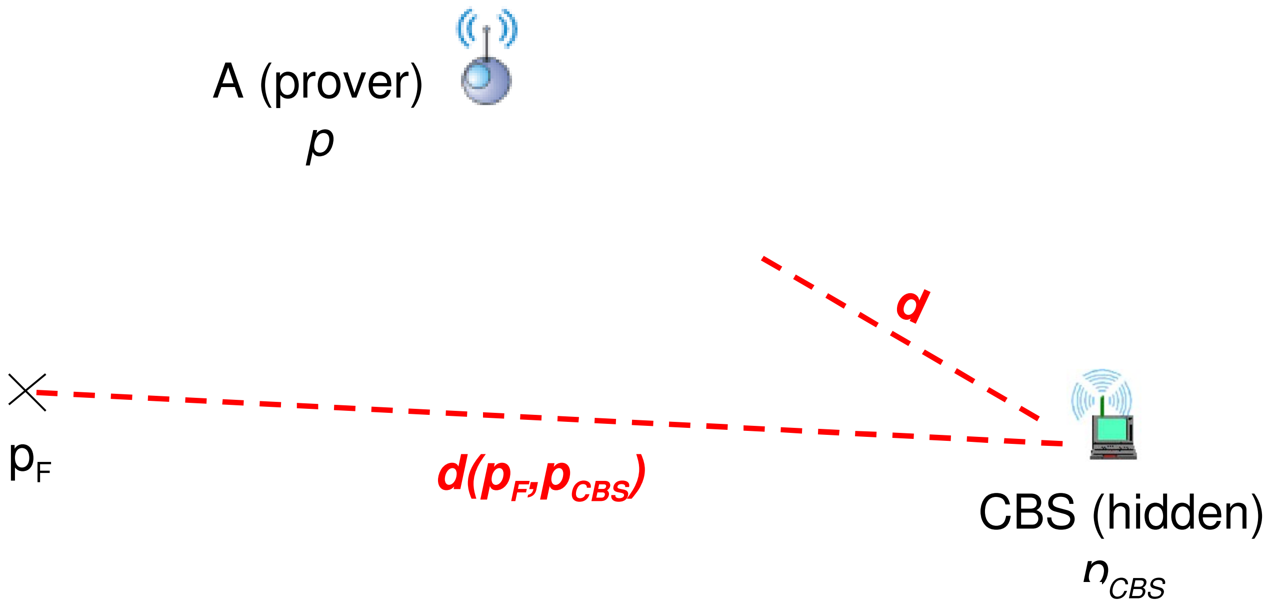
Observation 1:



not all distances are equally likely

Observation 2: not all all locations are equally easy to fake
(the easiest if p_F is in the center of the disk/sphere)

Attacker's success probability



$$Pmax_D^n = \left(\frac{4\Delta(R-\Delta)}{R^2}\right)^n$$

$$Pmax_B^n = \left(\frac{6\Delta(R-\Delta)^2 + 2\Delta^3}{R^3}\right)^n$$

Δ = *the expected error depending on the localization and ranging accuracy*

R = *the radius of the disk/sphere*

n = *number of hidden base stations*

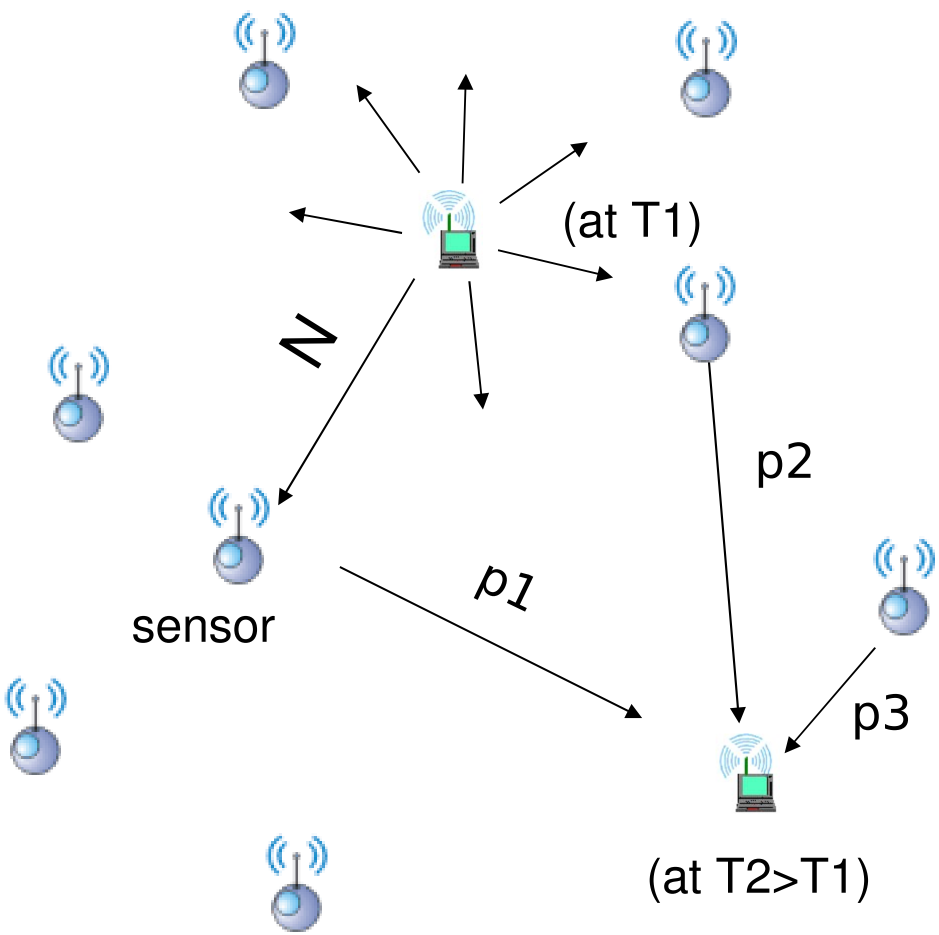
Some examples

- US localization/US ranging
  - R=10m (US range)
  - Δ =10cm
  - 10 BSs
  - p_attacker_success ≈ $(10^{-2})^{10}$

- GPS localization / UWB ranging
  - R= 2km
  - Δ = 4m
  - p_attacker_success ≈ $(0.005)^{10}$

- UWB localization / UWB localization ranging
  - R = 2 km
  - Δ = 20 cm
  - p_attacker_success ≈ $(10^{-4})^{10}$

Making use of mobile Base Stations



with mobile CBS there is no need for PBS, but the latency increases

Practical issues

- The size of the guessing space
  - you can hide somewhere and somewhere you cannot

- Repeated guessing
  - occasional repositioning of BSs
  - large number of BSs (sensors) in the space
  - mobile BSs do not suffer from this problem (the stations move for “*every*” verification)

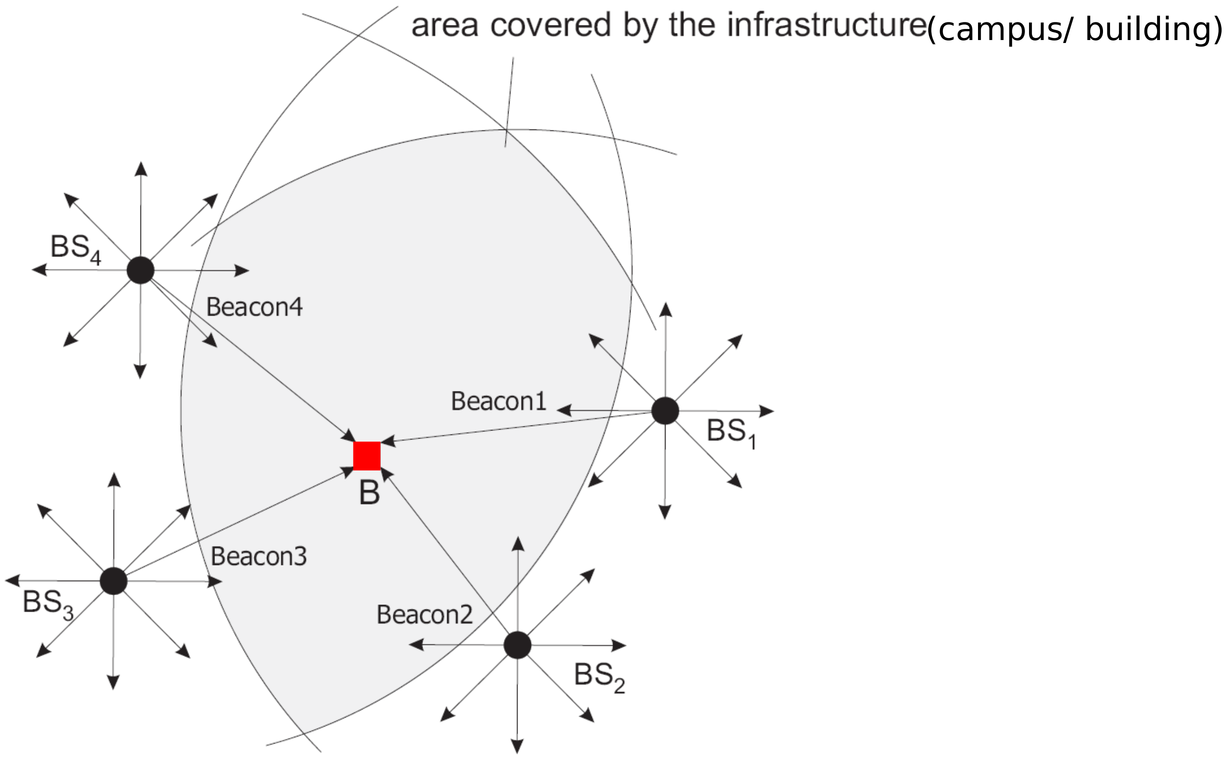
- Communication between hidden base stations
  - cabling
  - LPI signals
  - mobile BSs do not suffer from this problem (latency issues)

- Works equally well with TDOA

SecNav [Rasmussen, Capkun, Cagalj, 2007]

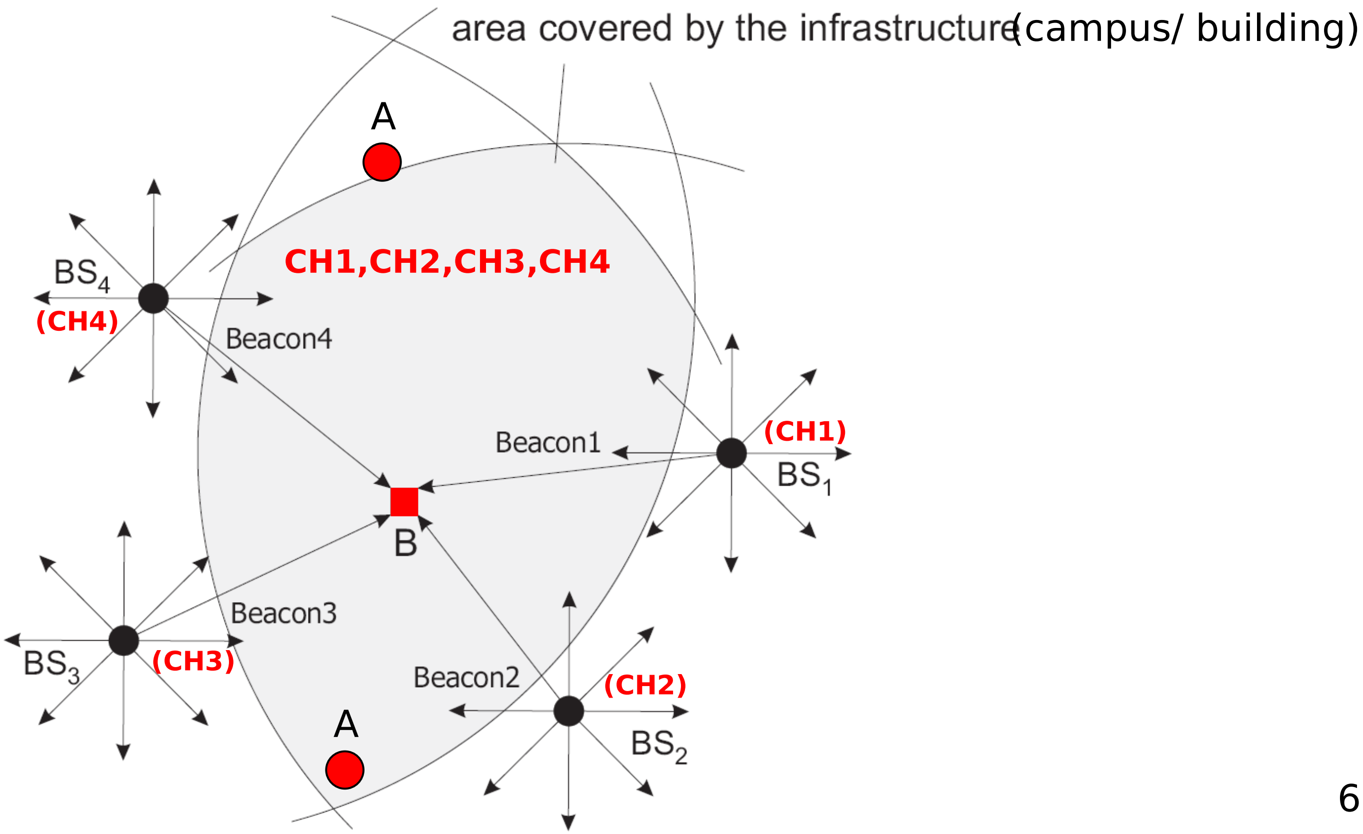
Secure Localization

- **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



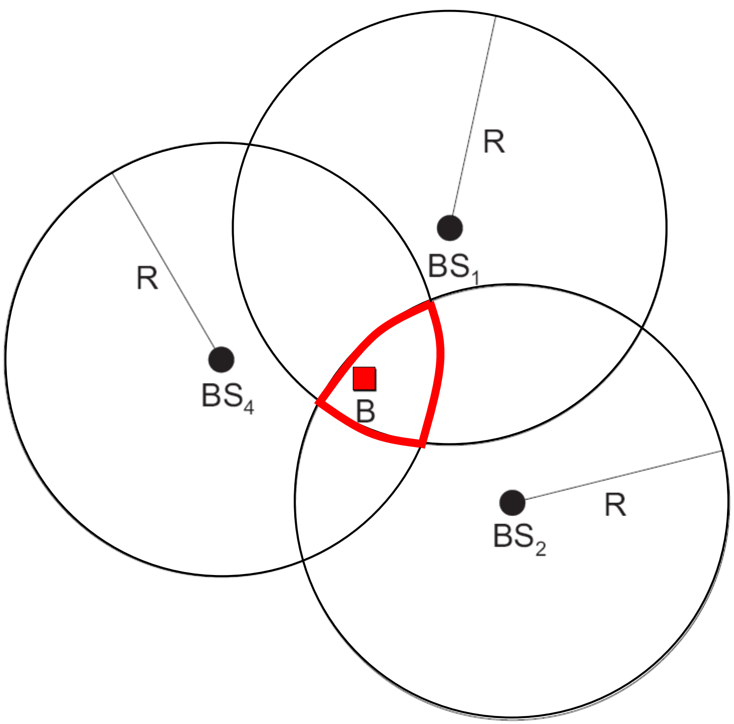
SecNav: Basic Assumptions

- 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

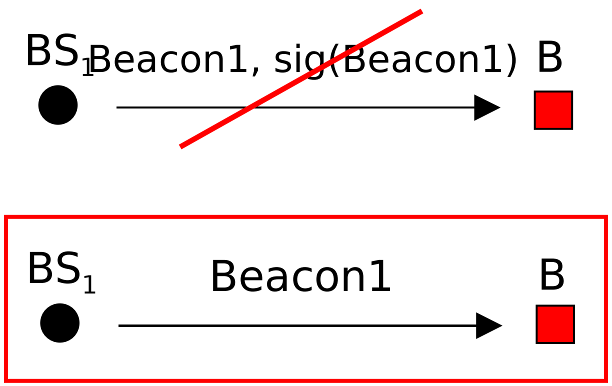


SecNav: Beacon-based Localization

- 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, …



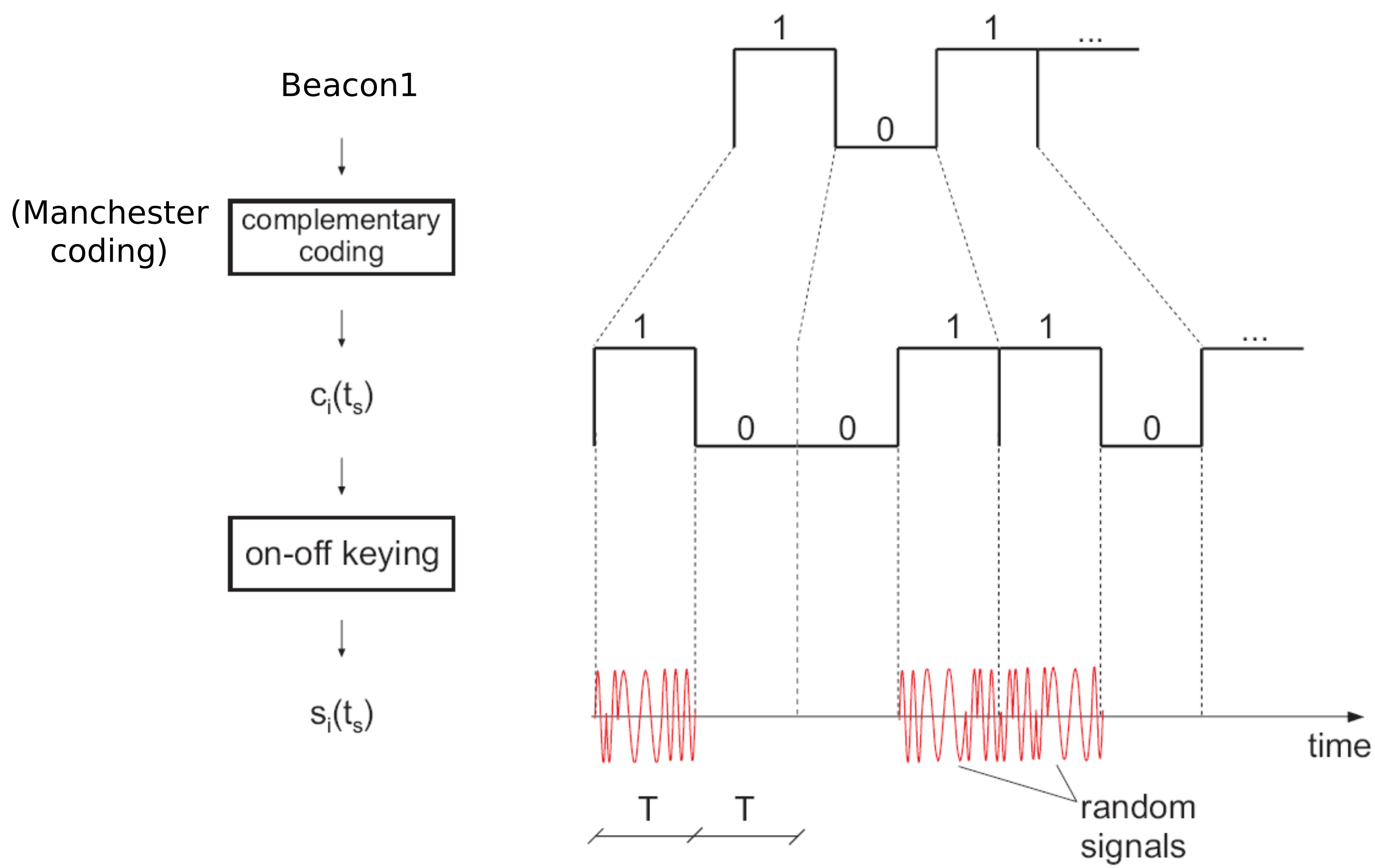
BEACON-BASED LOCALIZATION



CH1: Beacon1 = “BS1, timestamp”
CH2: Beacon2 = “BS2, timestamp”
…

Integrity Coding (Cagalj, Capkun et al., S&P 2006)

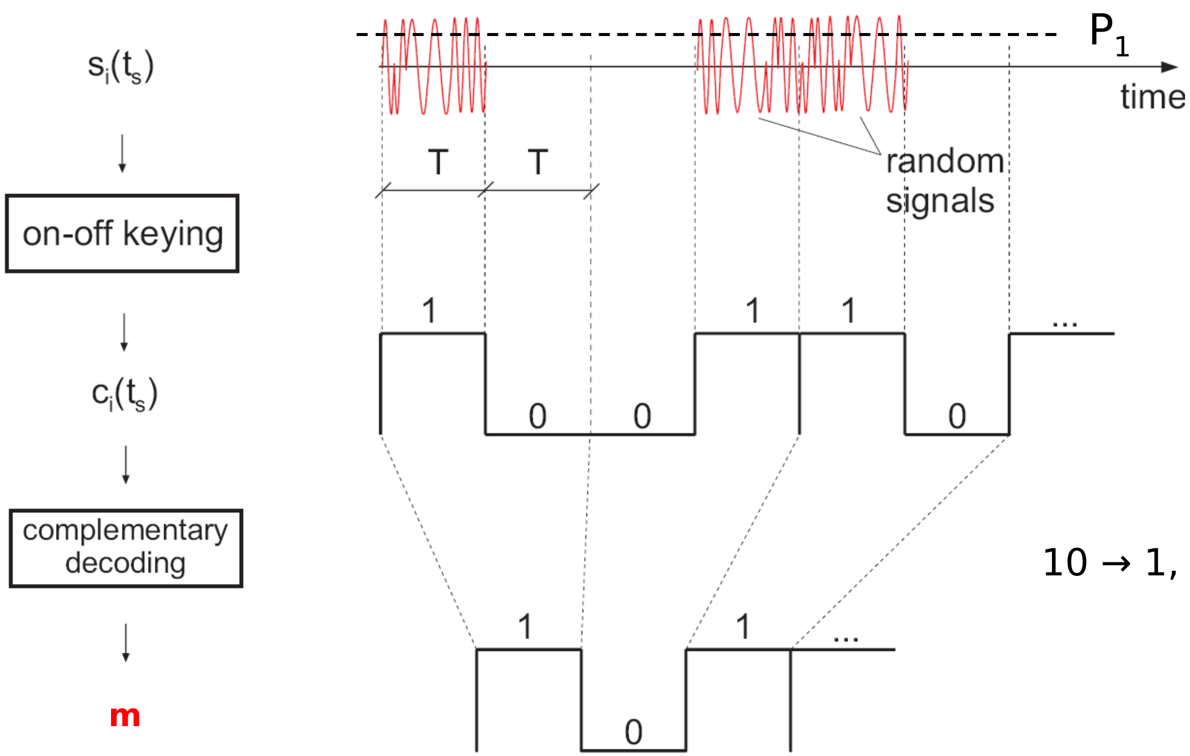
- k-bit Beacon1 spread to 2k bits (1->10, 0->01) (H(Beacon1) = k/2)
- transmitted using on-off keying (each "1" is a fresh random signal)



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

Integrity Decoding

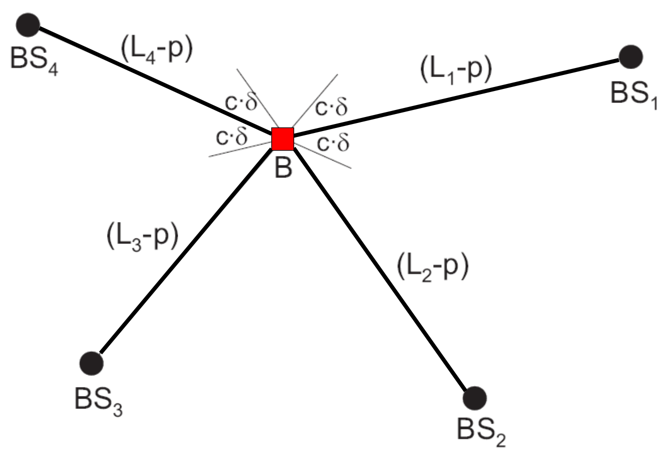
- Beacon detection:
  - presence of signal ($>P_1$) during T on CH1 interpreted as "1"
  - absence of signal ($<P_0$) during T on CH1 interpreted as "0"
- Beacon integrity and authenticity verification
  - IF H(m)=|m|/2 THEN "m" was not modified in transmission
  - since it was sent on CH1 => BS1, and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



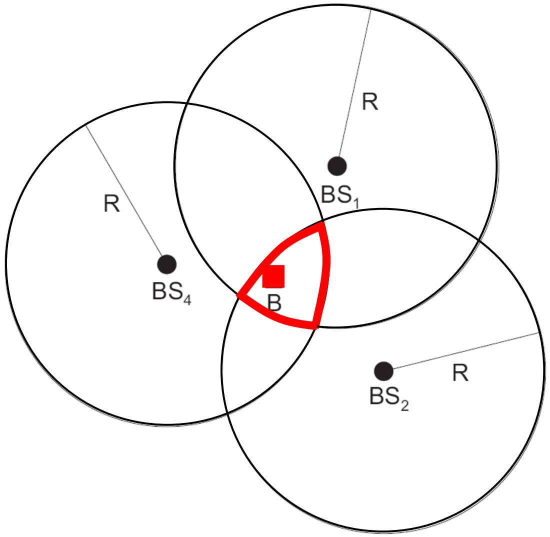
10 → 1, 01 → 0 (Manchester)

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



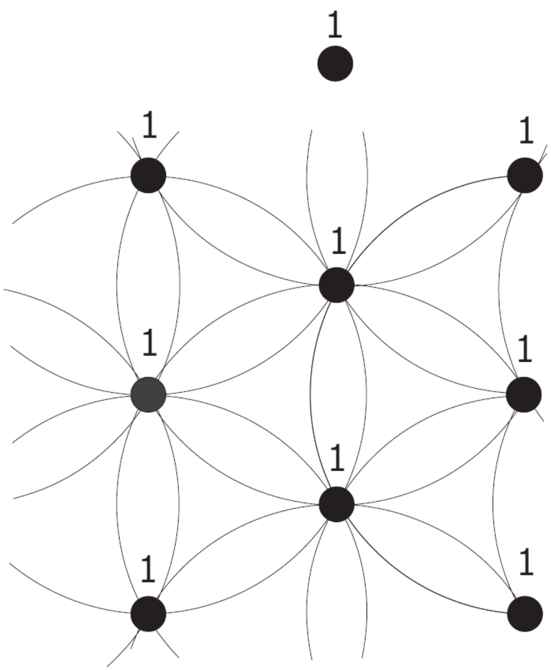
TOA LOCALIZATION



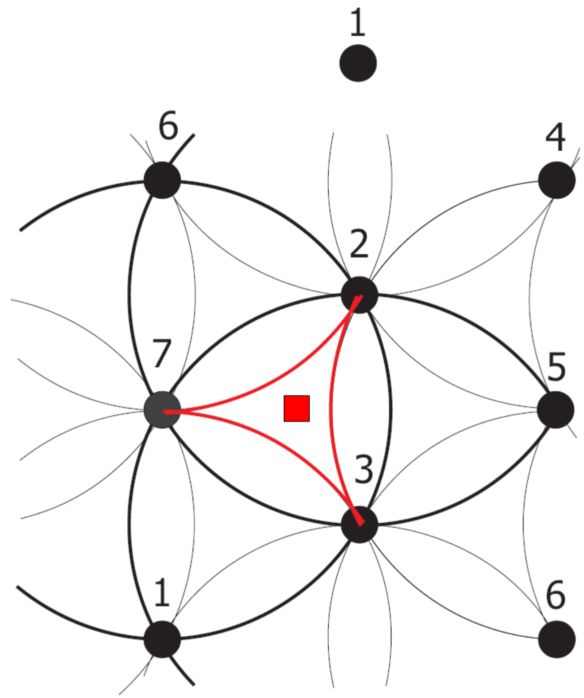
BEACON-BASED LOCALIZATION

SecNav: Coverage / Localization Accuracy

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



FULL COVERAGE WITH A SINGLE CHANNEL



FULL COVERAGE WITH 7 CHANNELS – NO MUTUAL INTERFERENCE

SecNav: 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 ...

- First implementation of a Secure Localization System

Current Approaches for Secure Localization/Time Synchronization

- Brands and Chaum, **Distance-Bounding (in wired networks)**, 1993.
- Shankar, Sastry, Wagner, **Location Verification using US distance-bounding**, WiSe 2003
- Capkun, Buttyan, Hubaux, **SECTOR: Secure Verification of Node Encounters,** ACM SASN 2003
- Kuhn 2004, **Securing Broadcast Navigation with Hidden Spreading Codes**, IHW, 2004
- Lazos, Poovendran, **Securing Localization with Directional Antennas**, WiSe 2004
- Ganeriwal, Capkun, Han, Srivastava, **Secure Time Synchronization**, ACM WiSe 2005
- Capkun, Hubaux, **Verifiable Multilateration**, IEEE INFOCOM 2005, JSAC 2006
- Lazos, Capkun, Poovendran, **w Directional Antennas/Distance Bounding**, IPSN 2005
- Li et al. and Liu et al., **Statistical Methods for Secure Localization in Sensor Networks**, IPSN 2005
- Manzo, Roosta, Sastry, **Time Synchronization Attacks in Sensor networks,** In SASN 2005
- Sedighpour, Capkun, Ganeriwal, Srivastava, **Demo: Attacks on US Ranging**, ACM SenSys 2005
- Capkun, Cagalj, Srivastava, **Hidden and Mobile Stations**, IEEE INFOCOM 2006/TMC 2008
- Zhang et al.. **Secure localization in Ultra-wideband Networks**, JSAC 2006
- Capkun, Ganeriwal, Anjum, Srivastava, **RSSI-based Secure Localization**, Tr 2006
- Sun et al.. Tinysersync: **Secure Time Synchronization in Sensor Networks**, CCS 2006
- Rasmussen, Capkun, Cagalj, **SecNav**, MobiCom 2007
- Tippenhauer, Capkun, **UWB Secure Ranging**, Tr 2008
- Rasmussen, Capkun, **Location Privacy of Distance Bounding Protocols**, CCS 2008