Alma Mater Studiorum – University of Bologna
CdS Laurea Magistrale (MSc) in
Computer Science Engineering

Mobile Systems M course (8 ECTS)
II Term – Academic Year 2022/2023

03 – Mobile IP and Positioning

Paolo Bellavista
paolo.bellavista@unibo.it

Mobility and Handoff Management

- Wireless networking allows ***mobile users*** to benefit from Internet connectivity
- Of course, user movements have to be managed when passing from a coverage area to another one
  - In addition, a user could decide to ***command her handoff between different connectivity opportunities*** (e.g., from WiFi to 4G)
- ***The ongoing active connections should be maintained notwithstanding the user movements***
  - In GSM/3G/4G networks, this calls for proactive resource acquisition for channel allocation (***pre-allocation for the sake of service continuity***)
  - In IP-based networks, *"it could be sufficient"* and *"could be relatively simple"* to keep the ***same IP address for a mobile user notwith. mobility. But is this possible?***

Tradeoff in Location Management

Two possible approaches for enabling the knowledge of the approximated location of mobile nodes:

- Via ***location update*** (*location registration*)
  - The network infrastructure is ***informed (from the external)*** of mobile user location, e.g., due to her explicit registration needed after any handoff
- Via ***location search*** (*terminal paging*)
  - The network infrastructure is ***responsible for retrieving*** the location info about mobile users

Which optimal tradeoff between update and search?

- Dependency on ***frequency of communications wrt location change***, ***dynamic search*** of new location and associated cost, e.g., in terms of ***latency***

Location Update

- Location update solutions
  - ***Static*** (triggering of updates when exiting from a given local area – not necessarily a single cell, …)
  - ***Dynamic*** (triggering that depends on user communications and on mobility patterns)
- Dynamic location update
  - ***Time-based*** (e.g., with fixed and given periodicity)
  - ***Movement-based*** (***forwarding pointers*** and dynamic evaluation of forwarding chains that become too long)
  - ***Distance-based*** (when the distance covered since the last update is considered too large)

- Also ***replication of location data*** (caching or actual proactive replication), both via flat organization and hierarchical one (as always, with consequences on scalability)

Location Search or Terminal Paging

Only a few notes about terminal paging (you remember our discussion when presenting the different wireless connectivity technologies in the first weeks…)

- ***Blanket polling***
  - For example, all cells in a locality under the control of one MSC are polled when a call arrives
  - High paging cost
- ***Expanding ring search***
  - Starting from the last location known for a mobile device
- ***Sequential paging***
  - Based on ***estimated probability of location*** (probability distribution)
  - ***Sequential exploration***, more or less rigid

The Mobility Issue in IP Networks

Problem of joint functionality in IP as a solution for ***identification and locator***

An IP address associated with a mobile node ***depends on the network*** that provides connectivity

- When a user connects to another network, the IP address tends to change
- Packets belonging to ***currently active connections*** ***have to be delivered towards the new IP address***

Intuitive solution (location registration approach):

- What do you do when you change your rented flat?
- Leaving a ***forwarding address*** to the old concierge ("old post-office")
- The old concierge has the duty of forwarding your messages/mails to your new concierge, and then to you

A rapid overview of Host Identity Protocol

A proposal to separate ***identifier*** from ***locator*** at the ***network layer*** of the TCP/IP stack

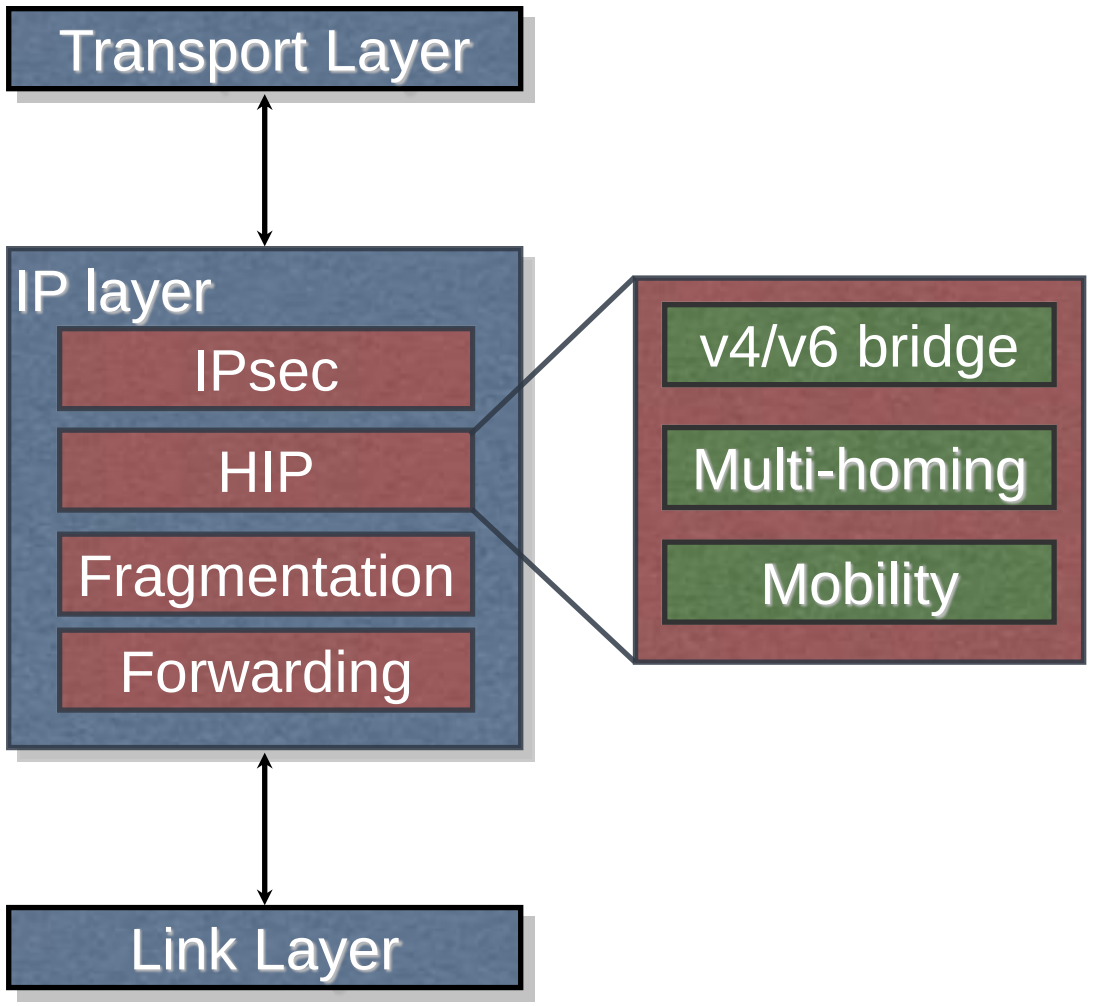
- A ***new name space*** of public keys
- A ***protocol*** for ***discovering and authenticating bindings*** between public keys and IP addresses
  - Secured using signatures and keyed hashes

- ***Architectural change to TCP/IP structure***
- ***A new layer between IP and transport***
  - Introduces cryptographic ***Host Identifiers***
- Integrates ***security, mobility, and multi-homing***
  - End-host ***mobility***, across IPv4 and IPv6
  - End-host multi-address ***multi-homing***, IPv4/v6
  - ***IPv4 / v6 interoperability*** for apps

A rapid overview of Host Identity Protocol

End-to-end, Host ID Tags (HITs)

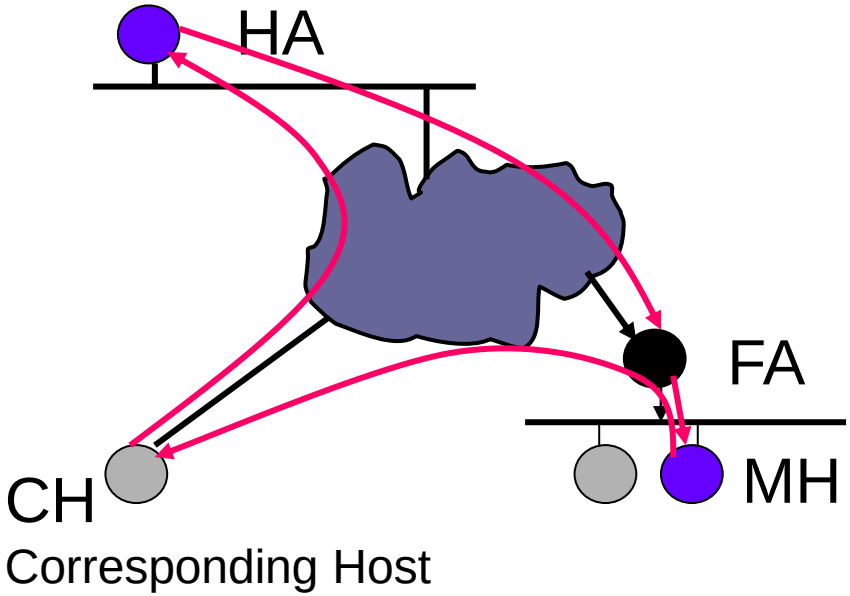
Hop-by-hop, IP addresses



Basic Elements of Mobile IP

- Entities and basic elements for Mobile IP
  - ***Mobile Host (MH)***
  - ***Home Agent (HA)*** – similar to the concept of "old post-office"
  - ***Foreign Agent (FA)*** – similar to the concept of "new post-office"
- ***MH registers the new address at HA***
- HA receives and "captures" the packets addressed to MH and then ***forwards them to FA***, which in its turn ***sends them to MH*** (currently positioned in its locality)

Issue of triangular routing



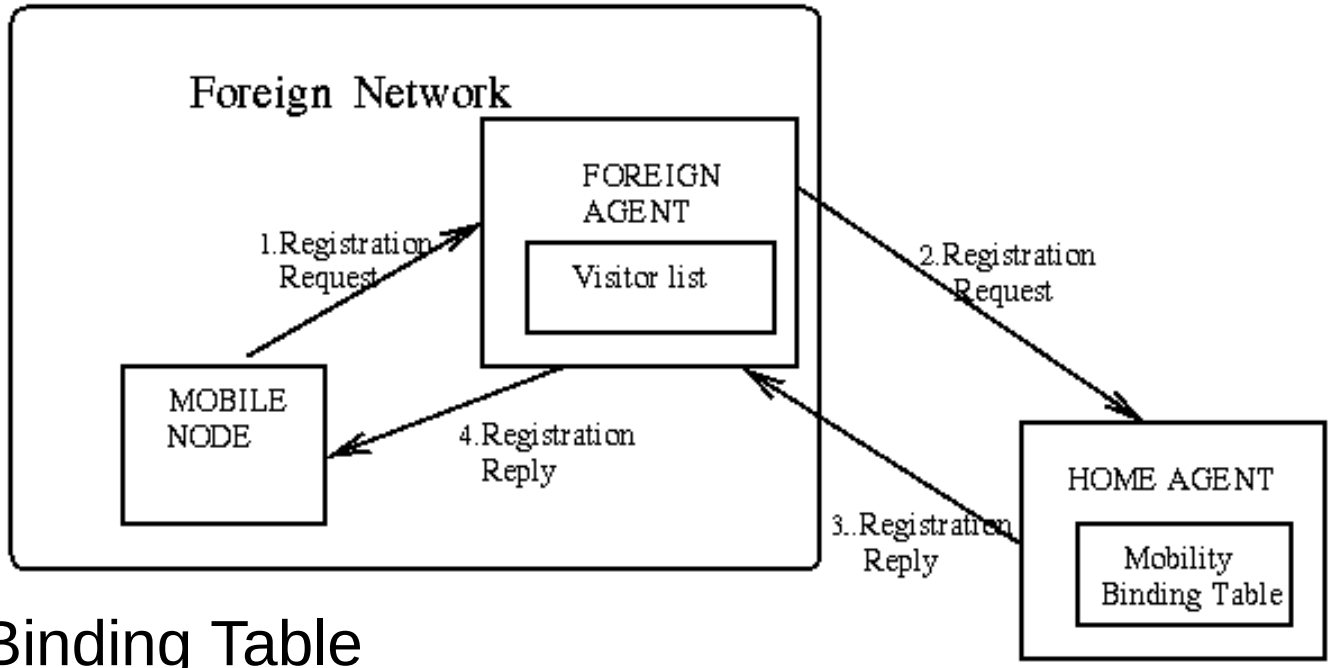
Home Agent (HA)

- It plays the ***role of router***, with some additional functionality
- Positioned in the ***home network of MH***
- It works to maintain the ***mobility binding of MH's IP address with its Care-of Address (CoA)***
  - Address that identifies the ***current location of MH***
- Of course, it works to forward packets to the appropriate network when MH is not in its locality
  - ***Via encapsulation*** (usually ***IP-within-IP tunneling***)

Foreign Agent (FA)

- Actually ***another router with enhanced functionality***
- When MH is not in the same locality as HA, FA is used to send/receive data to/from HA
- FA executes ***periodic advertising*** of itself
  - Advertisement messages carry data about the different available CoAs, in the case a set of them is available
  - MH nodes can choose not to wait for advertisement messages and to stimulate related data exchange ***via a solicitation message***. In your opinion, how?
- Once the MH receives its CoA from FA, ***MH registers this CoA at its HA***
  - The registration request is sent ***through FA***

Address Management



- Mobility Binding Table
  - Kept at MH's HA
  - It maps the association MH's home address & its current CoA
- Visitor List
  - Kept at the FA that is serving the MH
  - It maps the association between MH's home address and its MAC address + HA address

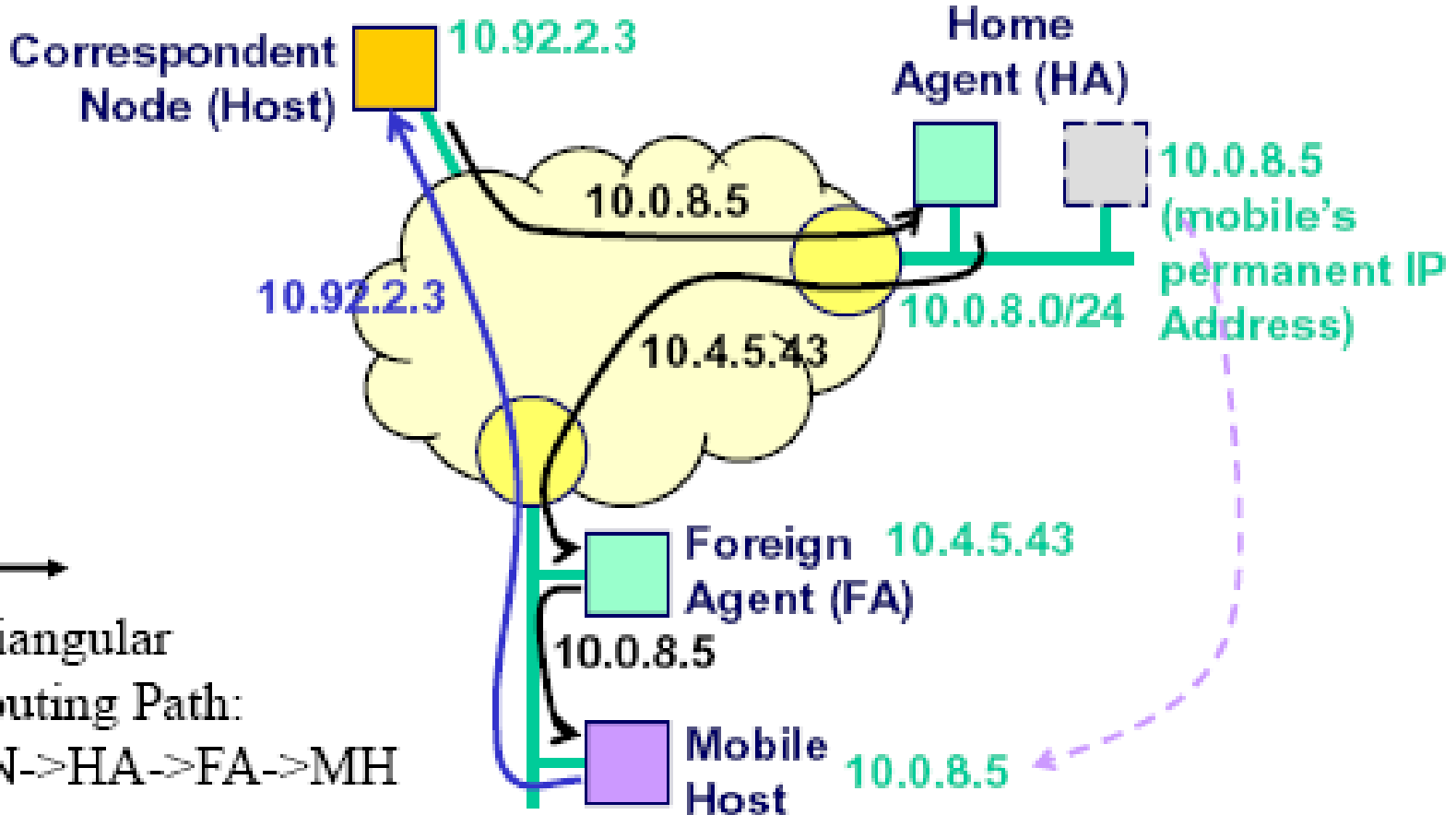
COA Tunneling

Do you remember what a tunnel is (differences if compared with proxies and gateways)?

When ***HA receives packets that are addressed to MH***, HA forwards them to CoA via ***encapsulation***

- The default mechanism for encapsulation, which has to be supported by any Mobile IP agent, is ***IP-within-IP (RFC 2003)***
- HA inserts a ***new IP header*** over the original header for each datagram. Which potential problems do you see for "traditional" IP networks?

Example of Mobile IP Usage



Triangular Routing Path: CN->HA->FA->MH (Mobile IPv4)

* Route Optimization (CN->MH) available in Mobile IPv6

COA: Further Details

Care-of Address (CoA): very often implemented as ***regular IP address***, but ***used ONLY by Mobile IP*** for forwarding purposes and for management functions. ***NOT visible at higher layers (application)***, similarly to a non-public address in NAT networks

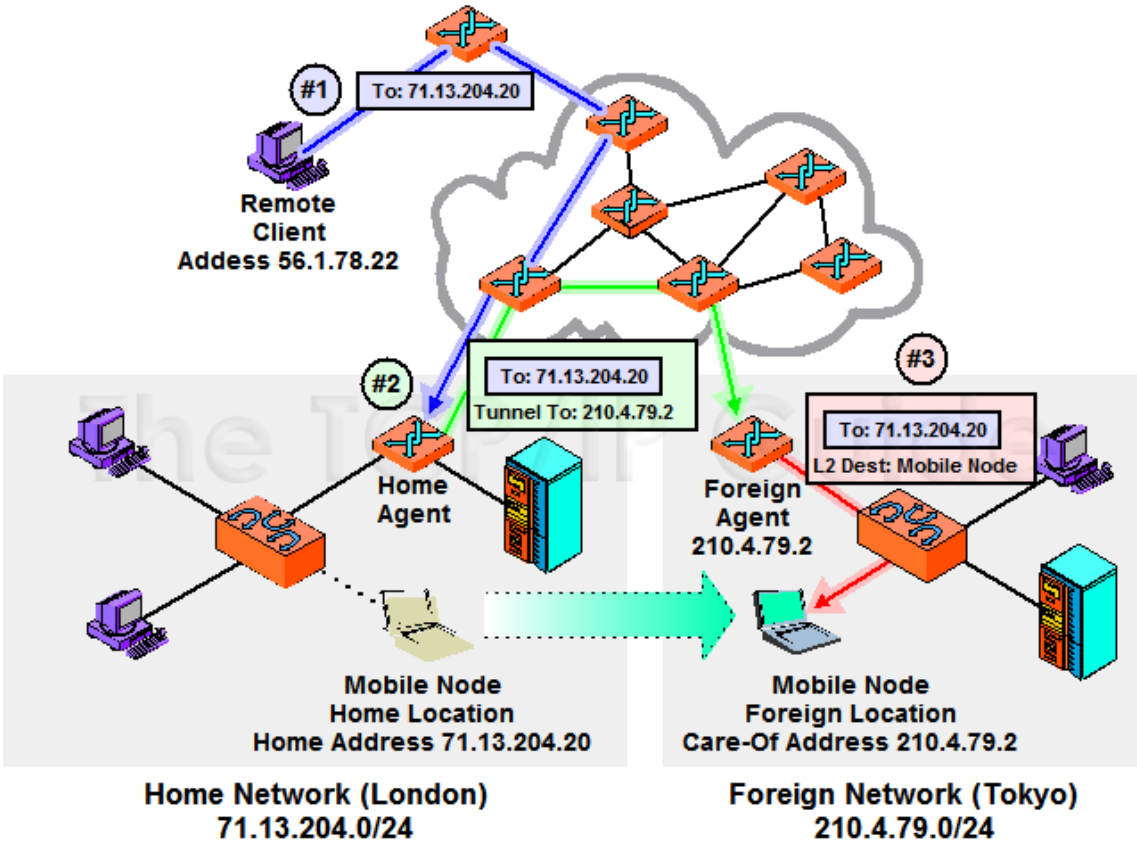
Two different types (corresponding to two different methods of forwarding to HA):

1) Foreign Agent CoA

Provided by FA in its messages of Agent Advertisement

Same IP address of the FA

Mobile node has not a different IP address in the foreign network, ***exploitation of layer 2 differentiation***



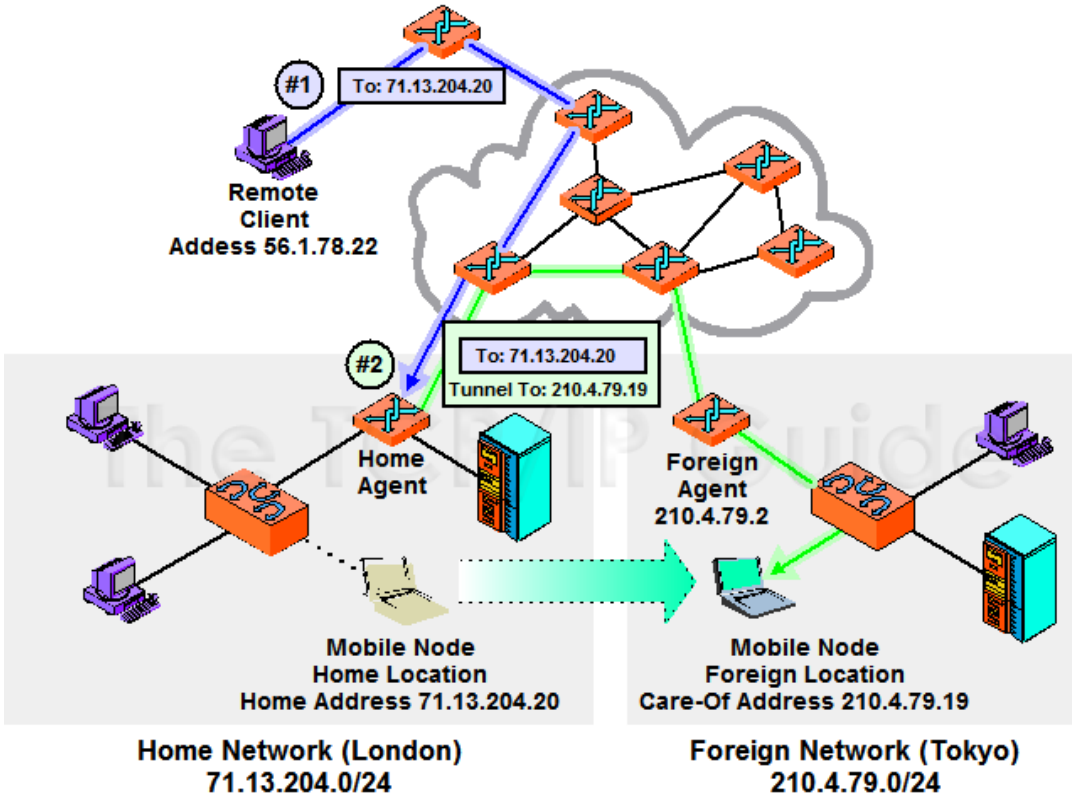
COA: Further Details

2) Co-Located Care-of Address

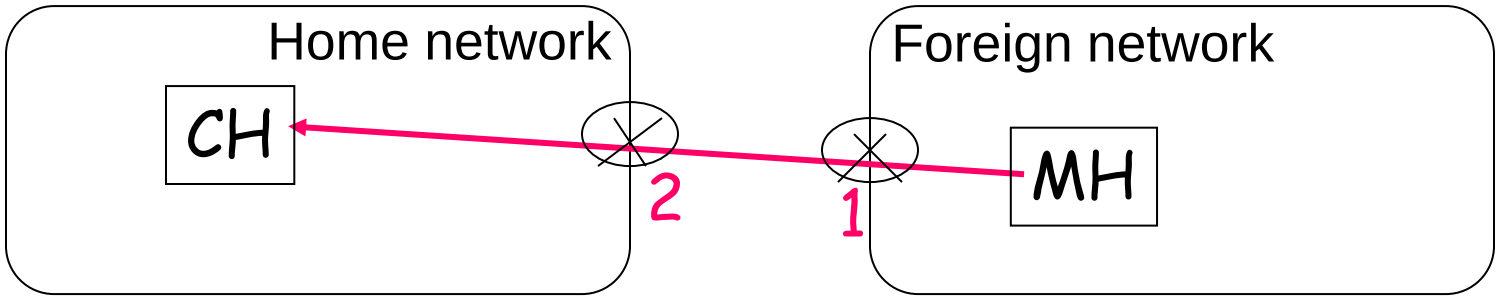
CoA is assigned directly to the mobile node by using some external mechanism/instrument, external to Mobile IP

For instance, manually by the foreign network or automatically via DHCP

In this last case, CoA can be used for traffic forwarding from HA directly to the mobile node



Possible Issues related to Ingress/Egress Filtering

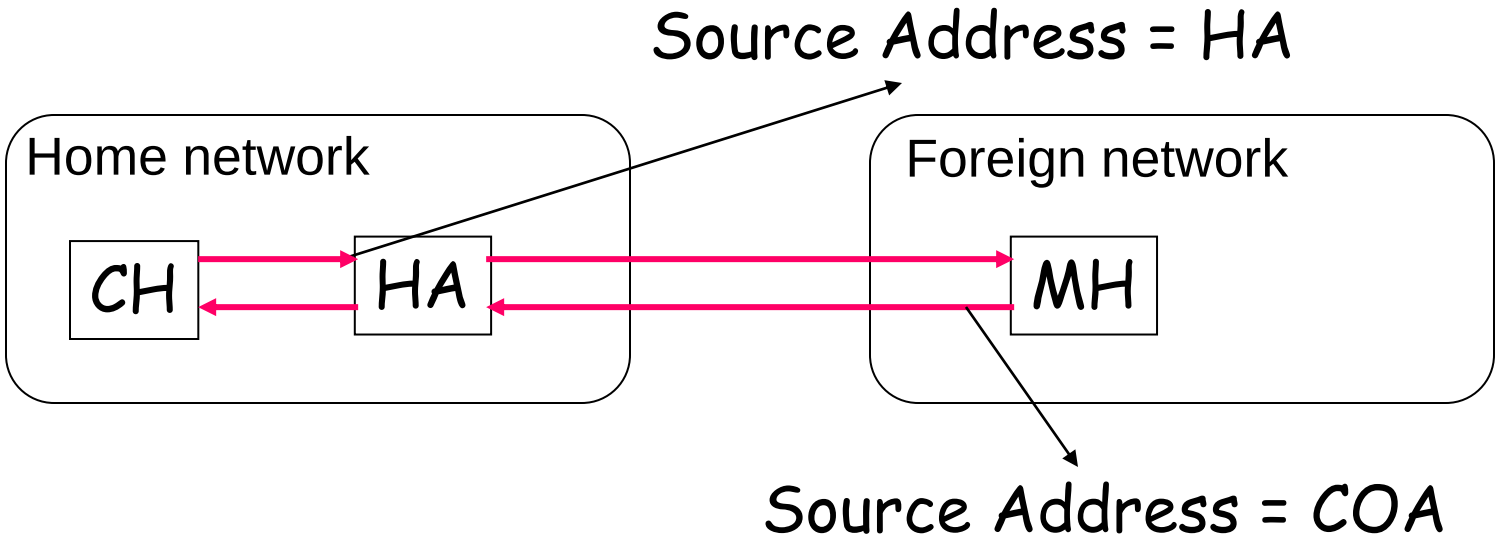


- MH uses its ***home IP address as the source address***
- Routers positioned at domain borders and "security-conscious" may perform ***dropping of MH's packets***
  1. A packet from the internal network has ***source address not belonging to the internal network***
  2. A packet from the external network and addressed to the home network has ***source address NOT belonging to the external network but to the same home network***

Possible Solution: Bi-Directional Tunneling

Selection of ***"safe" path through HA*** for both the possible directions

- ***Slower mechanism*** (higher overhead, higher latency) but more ***conservative in any deployment case***
- Known in the literature as ***quadrilateral routing***



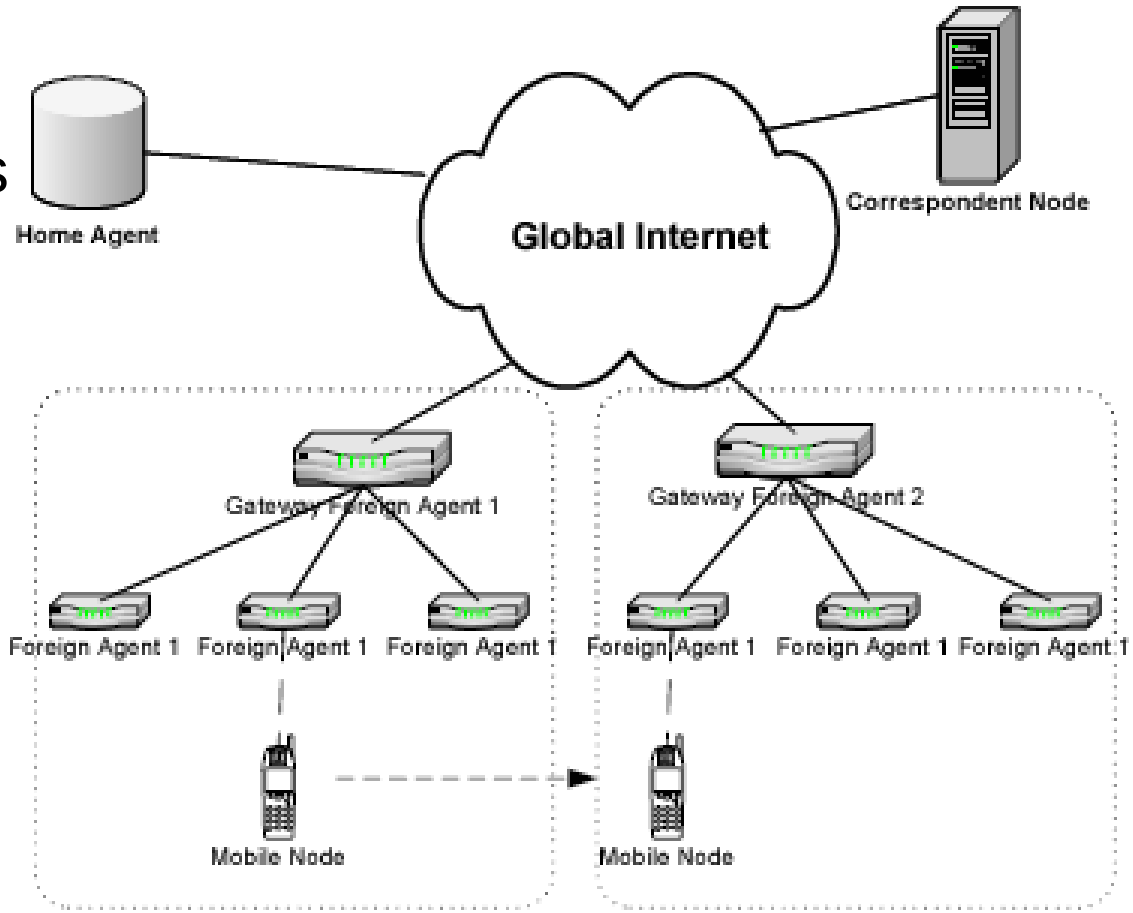
Sub-Optimal Triangular Routing

Which possibilities to optimize the Mobile IP routing mechanism? In which ***runtime conditions*** are these optimizations particularly critical?

- What happens if MH is in the same sub-network of CH and HA is currently located at the other side of the planet?
  - Of course, performance advantages if we could perform ***direct routing*** of packets without passing through agents
- Optimization: let's allow ***CH to know the MH's CoA*** (MH registers its CoA at CH, ***standard in MobileIPv6 – MIPv6***)
  - The process is started by HA, which notifies CH via "binding update"
  - MH encapsulates its packets to avoid issues associated with source-address filtering, but ***sends them directly to CH***
  - CH creates ***its own tunneling towards MH***

Hierarchical Mobile IPv6 (HMIPv6)

- ***Mobile Anchor Points*** (MAPs) play the role of Gateway Foreign Agents ***structured in a hierarchy***
- They are configured statically in HMIPv6 and shared by all mobile nodes



Hierarchical Mobile IPv6 (HMIPv6)

- ***Local Subnet Handoff***
  - COA registration at the local MAP when the handoff is local between subnets that are included in the same MAP domain
- ***MAP Domain Handoff***
  - Registration of a regional CoA (RCoA) at both HA and CN, in response to handoff towards a new MAP domain

Which is the “right” size for a service area (domain) of a MAP? How many hierarchical levels?

Research Directions: Dynamic MAP (I.R. Chen et al, J. Wireless Pers. Comm, 2007)

- Mobile nodes self-organize into MAPs dynamically, based on ***ratio between Service rate and Mobility Rate (SMR)***
- The ***optimal size*** of a DMAP service area is ***dynamic*** and determined according to the suitable dynamic tradeoff between service management costs (per packet delivery) and location management costs (per location update)

It collapses towards MIPv6 when SMR is sufficiently large (because the size of DMAP domains decreases when growing SMR); it ***degenerates into HMIPv6*** when DMAP size is fixed

Research Directions: WMM (D.W. Huang et al, IEEE T.Mobile Comp, 2008)

Wireless Mesh Network Management Mechanism (WMM)

- Based on ***caching of location info*** at mesh nodes with routing and location management functionality
- Pointer forwarding for handoff management
- Replication and “weak” consistency
  - Two cached tables: routing table and proxy table (with location info about the mobile nodes)
- Opportunistic update of location caches in the case of routing
  - Updates are included in packet headers
- Routing by using the two tables: if insufficient info then ***1) towards mesh infrastructure***, then ***2) flooding***

Proxy MIPv6 (PMIPv6)

Why PMIPv6 when we have MIP?

Main problems with MIP:

- Clients must implement MIP in the kernel (MIP mobility is *host-based*)
  - difficult to implement kernel changes
  - difficult to deploy (clients need software upgrade to get MIP support)
- *Handoff* procedure is not efficient
  - large delay

- PMIPv6 (RFC5213) is ***completely transparent*** to mobile nodes (use of a „proxy“ to do the handoff work)
- PMIPv6 is meant to be used in ***localized networks*** with limited topology where handoff signaling delays are minimal

PMIPv6 Terminology

- ***Local Mobility Domain (LMD):***

  Network that is PMIP-enabled, contains 1 LMA and multiple MAGs

- ***Local Mobility Anchor (LMA):***

  All traffic from and to MN is routed through LMA, maintains a set of routes for each MN connected to the LMD

- ***Mobile Access Gateway (MAG):***

  performs mobility-related signalling on behalf of its MNs, the access router (first hop router) for the MN

- ***NetLMM:***

  Network based Localized Mobility Management (IETF working group for network-based mobility support)

- ***Binding Cache:***

  Cache maintained by LMA; it contains Binding Cache Entries (BCE), with fields MN-ID, MAG proxy-CoA and MN-prefix

PMIPv6 Terminology

- ***Binding Update List:***

  Cache maintained by MAG with info about attached MNs

- ***Proxy Binding Update (PBU):***

  PMIP signaling packet sent by MAG to LMA to indicate a new MN, with the fields MN-ID (e.g., MN MAC), MAG address (proxy-CoA) and handoff indicator (whether MN-attachment is new or a handoff from another MAG)

- ***Proxy Binding Acknowledge (PBA):***

  Response to a PBU sent by LMA to MAG, contains MN-ID, MAG address and prefix assigned to MN

- ***Proxy care of address (proxy-CoA):***

  IP address of public interface of MAG

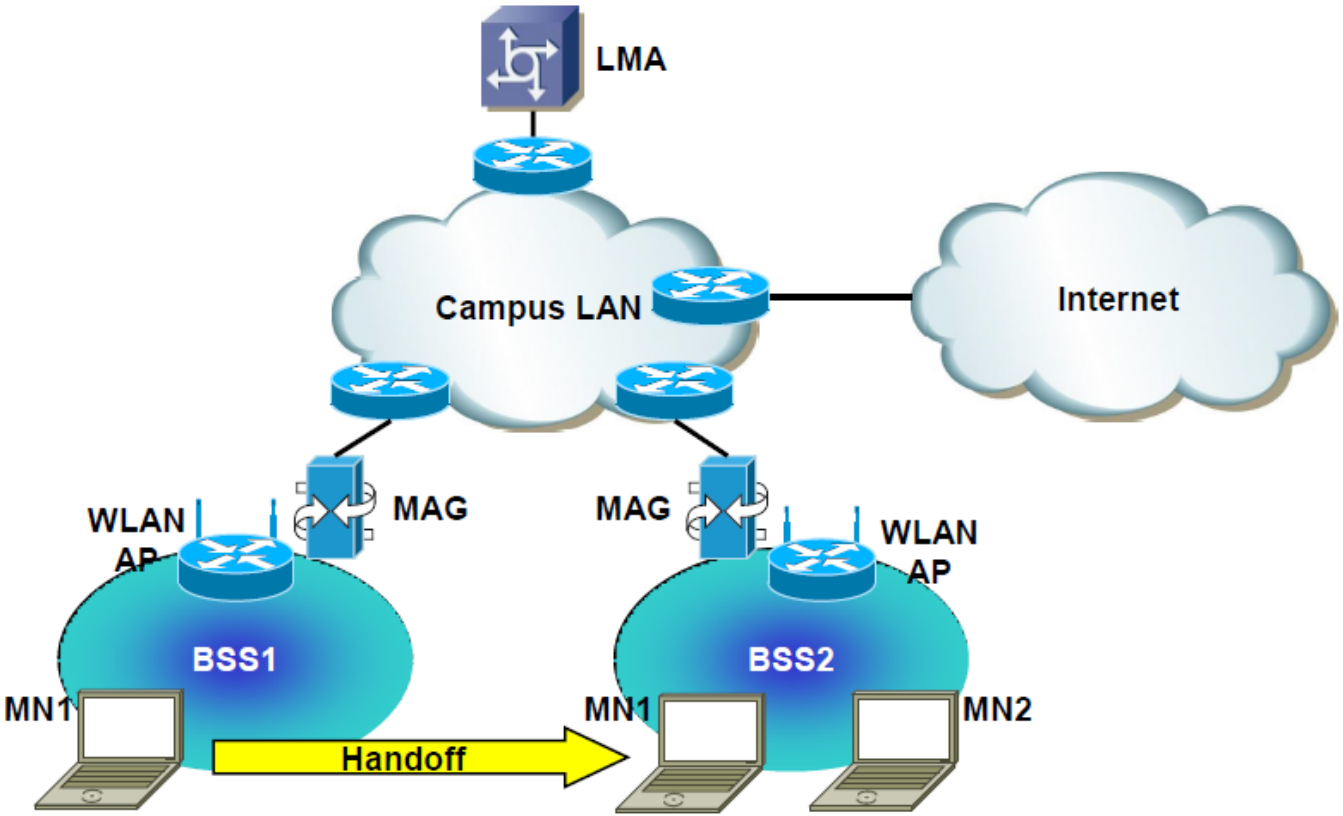
PMIPv6 Architecture and Deployment

- ***Mobile Node Identifier (MN-ID):***

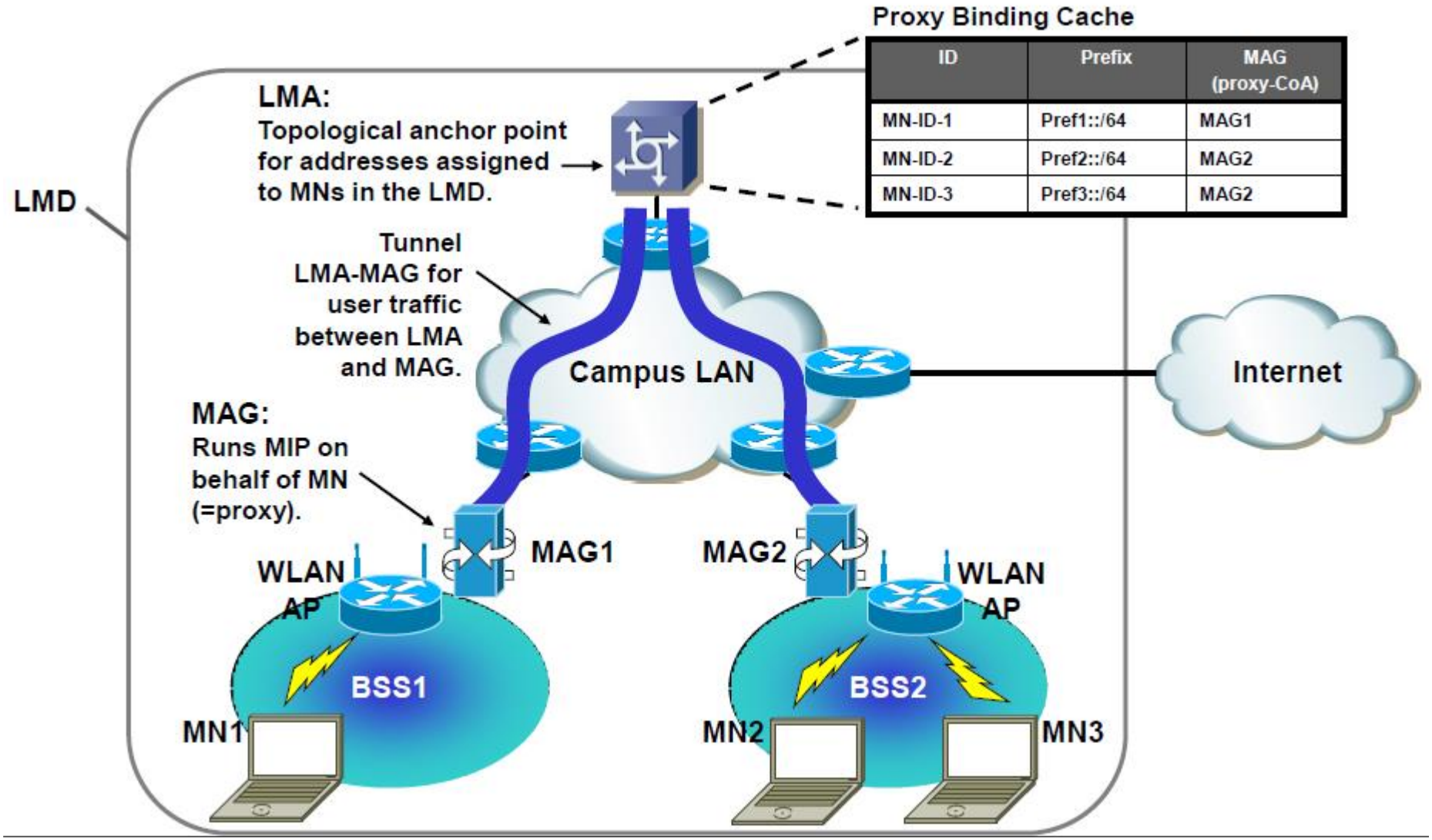
  Unique MN identifier, e.g., one of its MAC addresses but also HIP.

- ***Home Network Prefix:***

  Prefix assigned to MN by LMA

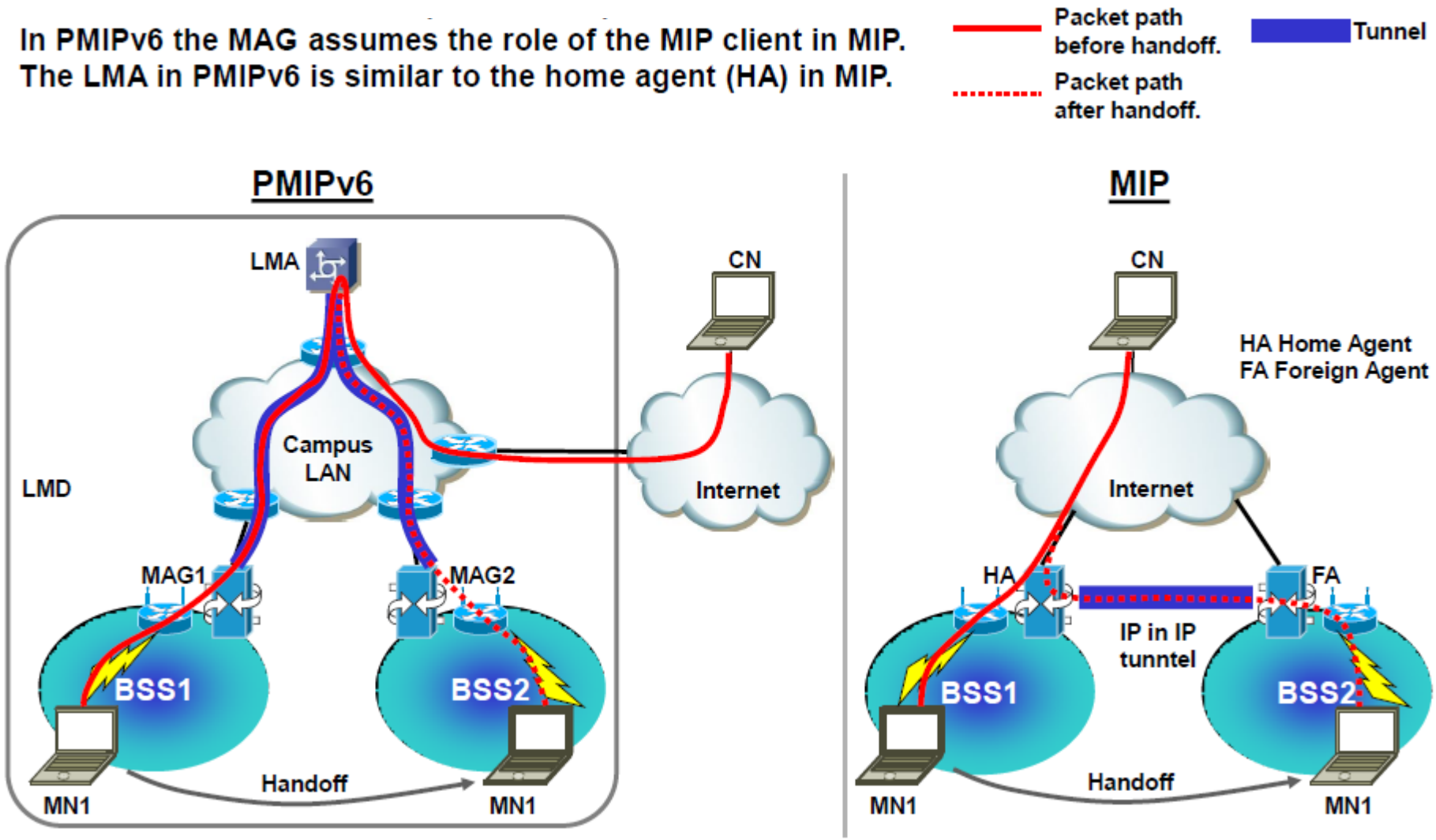


General PMIPv6 Setup



PMIPv6 vs. Mobile IP

In PMIPv6 the MAG assumes the role of the MIP client in MIP.
The LMA in PMIPv6 is similar to the home agent (HA) in MIP.



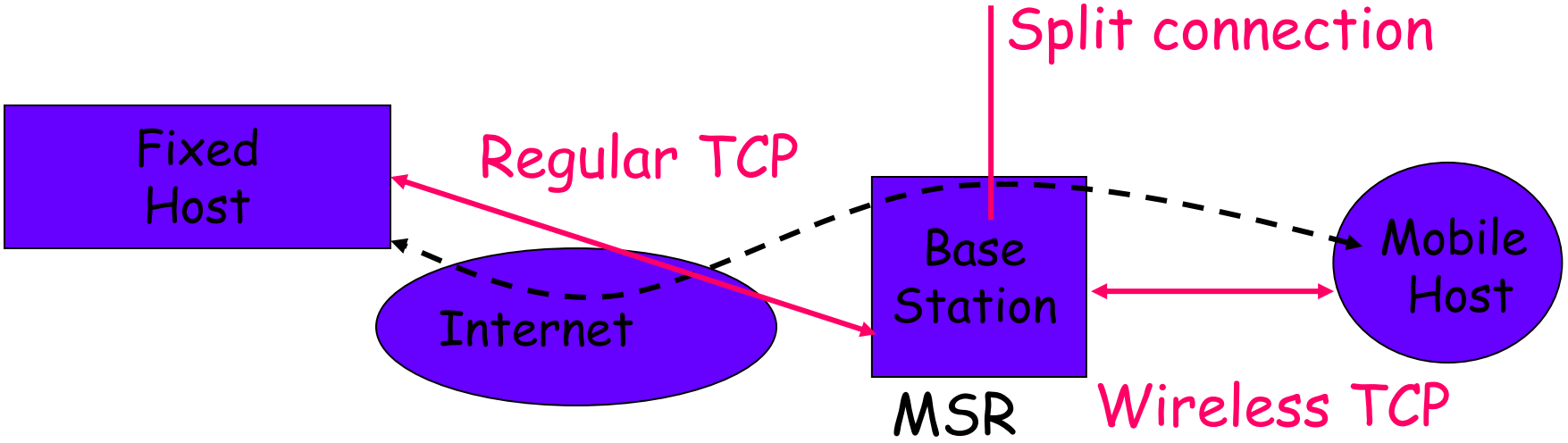
Is Mobile IP (and variants) Sufficient?

- ***Standard non-modified TCP*** leads to a ***significant degradation of performance*** over wireless links
- Why?
  - Wireless links are affected by high Bit Error Rate (BER) and by frequent disconnections/re-connections
  - In the TCP perspective, the above characteristics are observed as ***random & bursty packet losses***
  - In TCP, ***ALL packet losses*** are counteracted as if they were ***symptoms of network congestion;*** therefore, they generate reduction of the transmission frequency (in multiplicative way), with slow growth, step by step…

I-TCP: Basic Idea

Exploitation of a “split-connection” approach

- Traditional standard TCP between Fixed Host (FH) and Mobile Source Router (MSR)
- Wireless TCP between Mobile Host (MH) and MSR

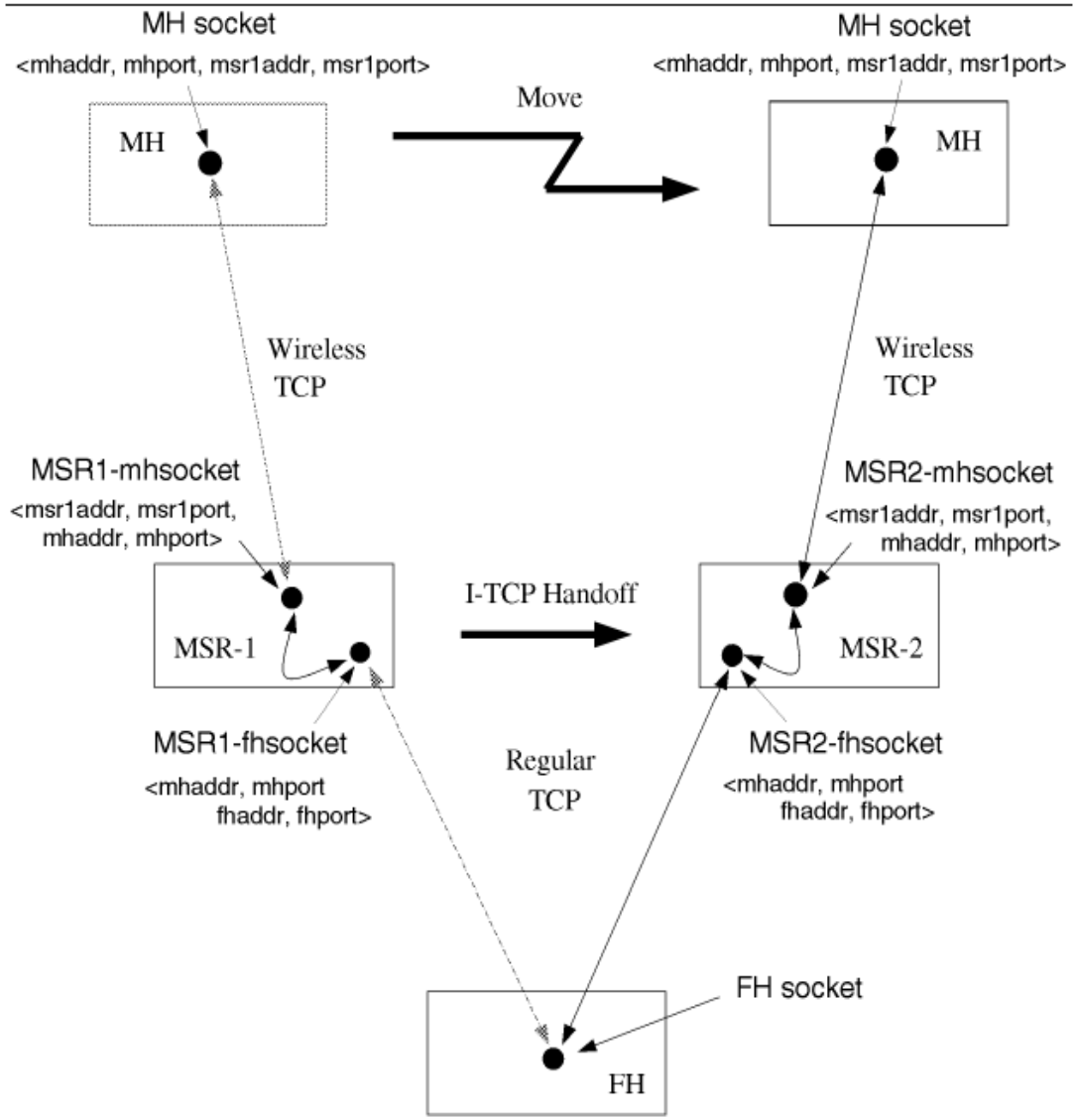


Split Connection: Pros and Cons

- Advantages
  - ***It separates flow and congestion control over the two segments*** (wireless and wired links managed separately)
  - ***Retro-compatibility with TCP*** (FH may NOT be aware of MSR)
- Disadvantages
  - ***Violation of the classical end-to-end semantic*** (we will discuss it later – *end-to-end principle*)
  - ***MSR maintains state***
    - MSR fault/failure may generate connection loss
    - Handoff latency grows for the need of state transfer
  - If NO specific optimizations are put in place, data replicas at MSR

I-TCP

- ***Built on top of Mobile IP***
- MSR acts as proxy for MH
  - It plays the role of MH twin image and forwards its state to the new MSR in the case of handoff
- I-TCP does not reduce the ***end-to-end reliability***
  - Provided that there is no MSR fault /failure and no MH disconnection for an indefinite time interval
- Suitable for ***throughput intensive applications***



Handoff in I-TCP

- ***Strongly integrated with the registration procedure in Mobile IP***
  - Handoff starts when MH triggers the registration of the new CoA at HA
- ***Transfer of the socket state operated by an I-TCP daemon*** towards the new MSR
- ***Buffering of transmitted data segments*** during the execution of the handoff procedure – to prevent from congestion control
- It should be rapid in order to avoid the creation and transfer of non-necessary replicas

By summarizing…

Some ***solution patterns/directions*** that we have already met and that have general validity:

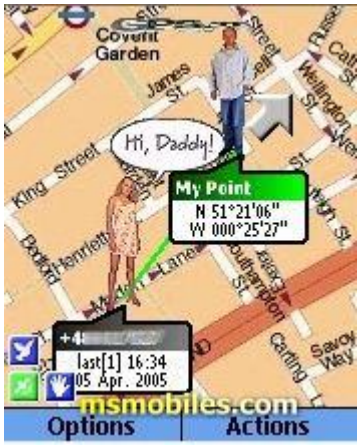
- ***Fixed anchor point*** (home)
- ***Proxy*** (more or less transparent, at different layers)
- ***Hierarchical organization*** for ***scalability***, more or less dynamic
  - Grouping/clustering
  - Differentiated functionality/features within a group
- Decisions (and protocols) that exploit the ***locality concept***, by trying to converge towards a desired global behavior without the need of global heavyweight coordination
- Approach towards ***approximated*** (but lightweight) and ***optimistic solutions***

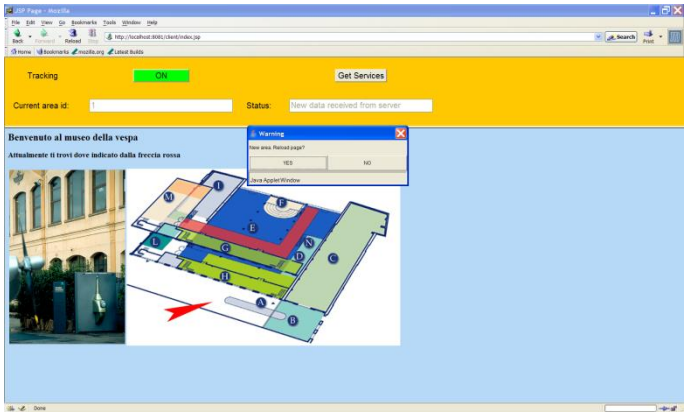
Localization (or Positioning): Why?

Recent class of services, of growing popularity:

Location-Based Services (LBS)

- E-911 Emergency assistance
- Advertising
- Tracking: e.g., based on regular mobility traces and habits
- Virtual Tour: which point of interest is near to you?
- Service discovery
- ***Optimization of ad hoc communications***





How to Obtain Positioning Info?

- Many LBS applications ➔ very differentiated requirements
  - E-911: ***on request*** (xy coordinates)
  - advertising + virtual tour: ***location changes*** (room, street, …)
  - Network support: ***every X minutes*** (network area)
  - Navigation support: ***every X seconds*** (xy coordinates)
- Additional non-functional requirements :
  - Low power consumption, usability, simplicity, privacy, ...

The natural consequence is =>

Many positioning systems with differentiated characteristics

Taxonomy: Physical vs. Symbolic

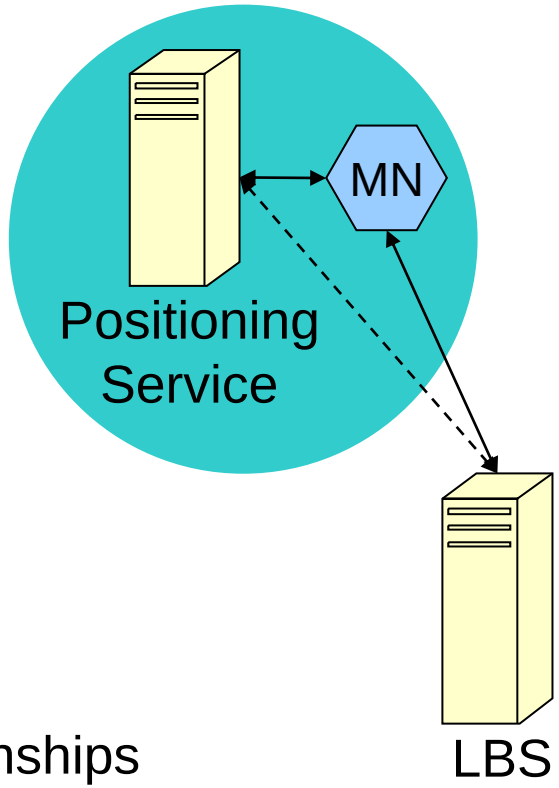
- ***Physical***
  - Associated with info more suitable for machine processing
  - WGM84 Location (GPS) - latitude, longitude, ellipsoid height (altitude)
- ***Symbolic***
  - Associated with info more suitable for human speaking/thinking
  - ***Layered location info*** - {Italy, Bologna, EngSchool, DISI, Lab2}

Also ***Absolute vs. Relative***

- ***Absolute***
  - Single reference system for any positioned item
  - Physical or symbolic
- ***Relative***
  - Relative to the location of another item
  - Typically physical and suitable for ad-hoc env.

Taxonomy: Centralized vs. Distributed

- ***Centralized***
  - A central system processes collected info and ***determines the location of any considered item***
- ***Distributed***
  - Each participant determines its ***own location***



Privacy issues:

- Network communication ➔ intrinsic limitation, no privacy in strict severe sense, or need for the establishment of trust relationships
- Any location-dependent info that is made visible reduces the user privacy

Taxonomy: Accuracy & Precision

- ***Accuracy***: error range (e.g., in meters)
- ***Precision***: trust degree associated with the error range (confidence, in percentage)
  - GPS: accuracy = 10m, precision = 95%

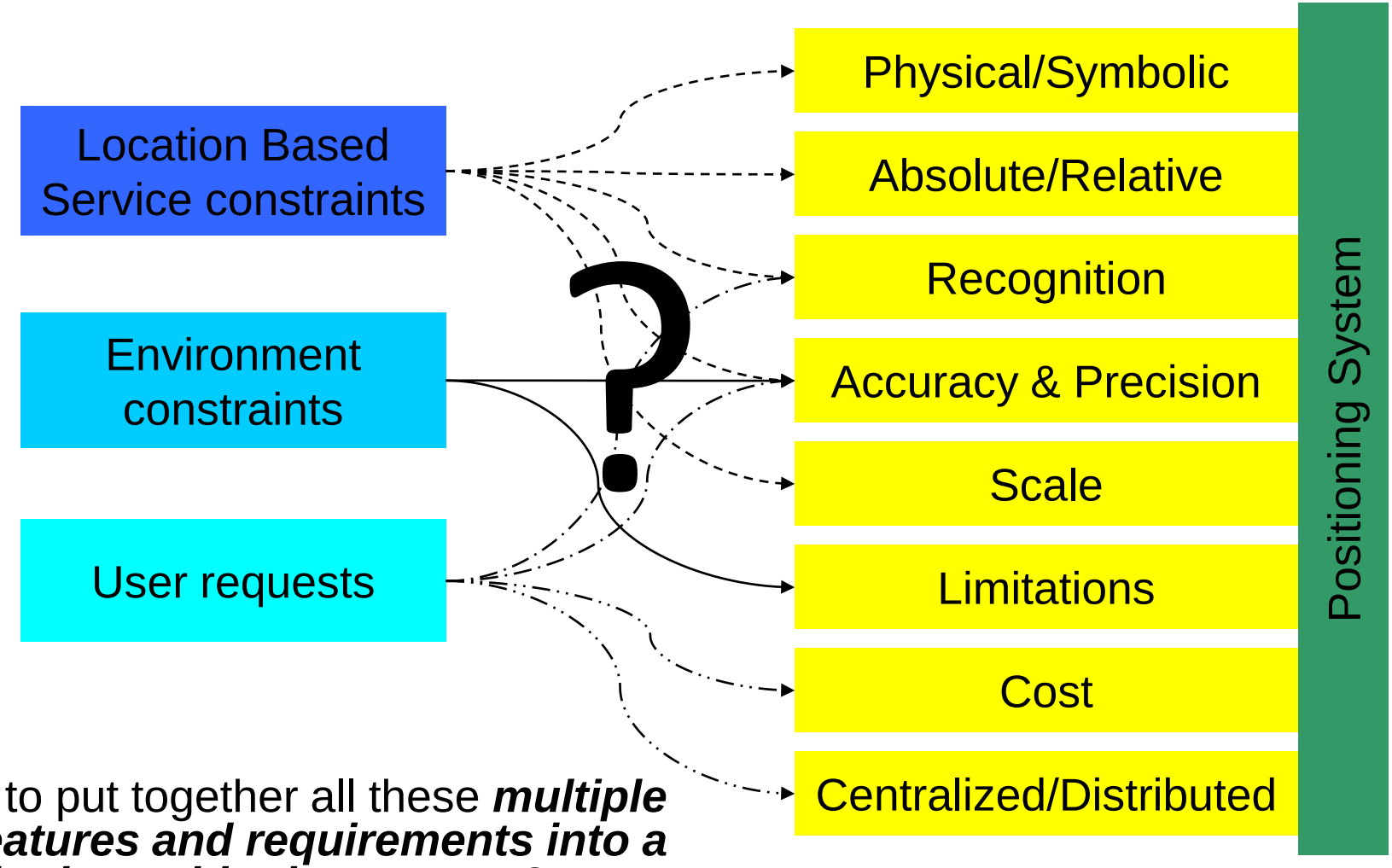
Accuracy and precision usually depend strongly on the employed positioning system and on the conditions of the deployment environment

- ***Scalability***
  - Which area and of which size? For instance, coverageArea / #infrastructUnit
  - How many users? For instance, #user/(infrastructure unit * time unit)
  - How many positioning resources used? With which complexity of the infrastructure and middleware support?

Taxonomy: Costs and Limitations

- ***Costs***. In terms of:
  - time, infrastructure, infrastructure deployment, client side, additional dedicated hardware, battery consumption, memory consumption, computing power consumption, …
- ***Limitations***
  - Where/when is it possible to exploit it?
    - For instance, indoor vs. outdoor

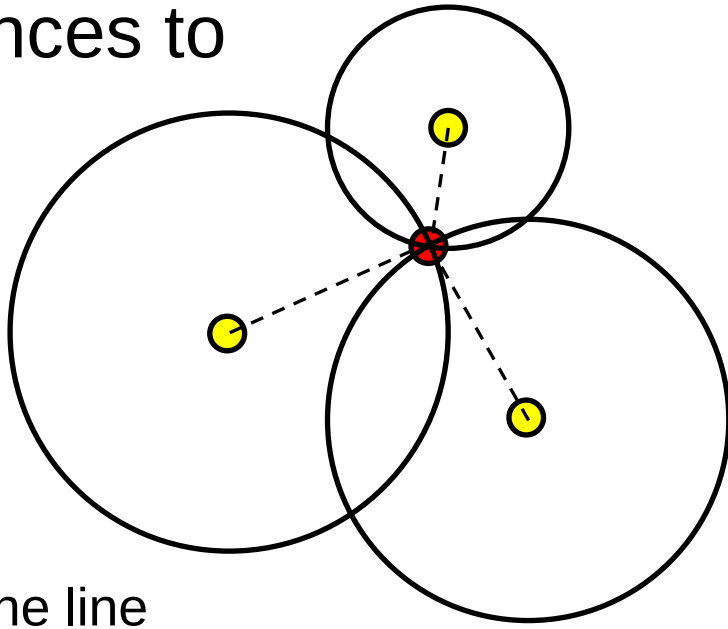
Design Choices or Technical Constraints?



How to put together all these ***multiple features and requirements into a single positioning system***?

2D ➔ 3 circumference

- Higher number of circumferences to ***mitigate errors*** in distance measurement

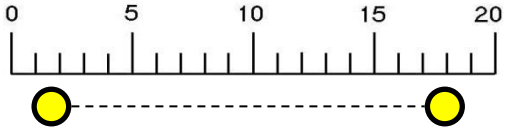


Note that:

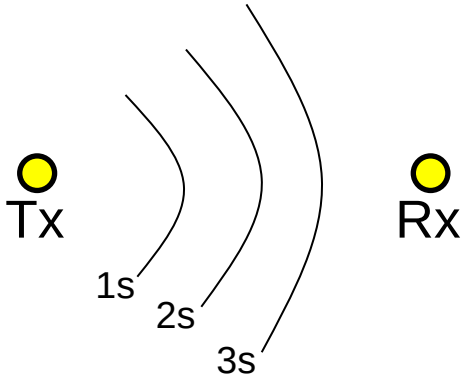
- 2 variables, 3 measurements
- 2 measurements are sufficient only if in the line between two reference points (tangent circumferences)

Distance Determination: How?

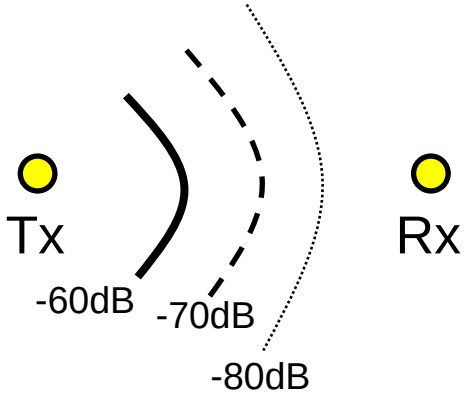
- Direct measurement



- Time of Arrival (ToA)
  - distance = signal speed * ToA



- Received Signal Strength Indication (RSSI)
  - Power and signal attenuation/fading



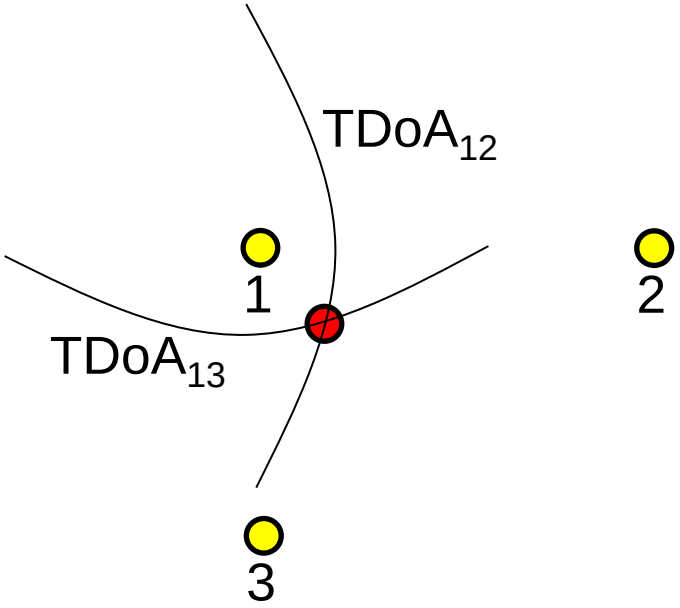
Commonly employed technologies

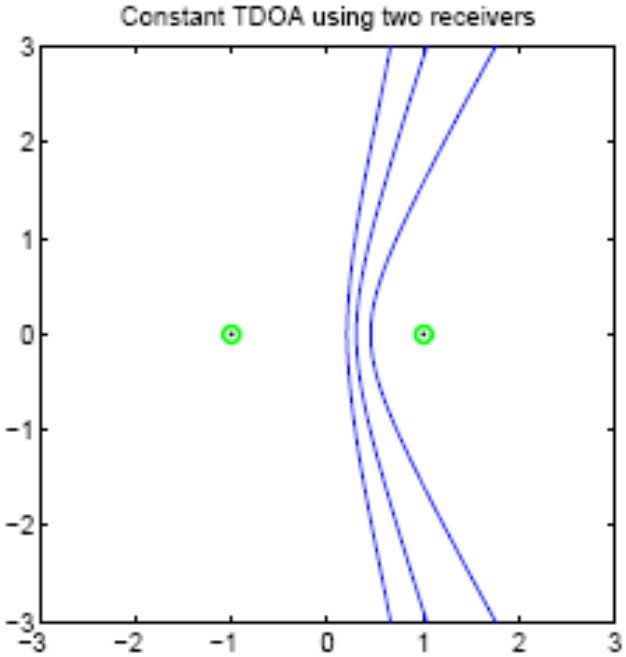
InfraRed (IR), RadioFrequency (RF), UltraSound (US)

Time Difference of Arrival

2D ➔ 2(3) hyperboles

- hyperbole: point place where points are at the same Time Difference of Arrival (TDoA) from two reference points





three different TDoA:
0.4, 0.6, and 0.9 scale units

Angulation

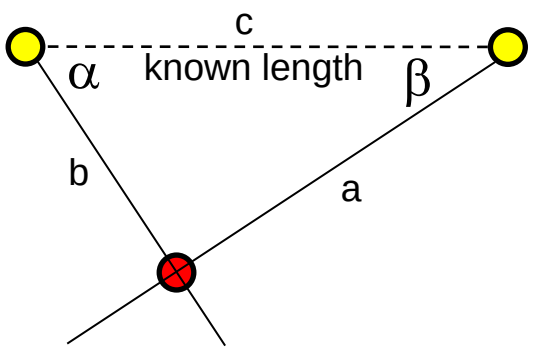
- Pre-requisite:
  - To be aware of the distance between the two reference points
- 2D ➔ 2 angles ➔ 2 measurements

Carnot's theorem

$a^2=b^2+c^2-2bc \cdot cos\alpha$

$b^2=a^2+c^2-2ac \cdot cos\beta$

2 equations with
2 variables (a, b)

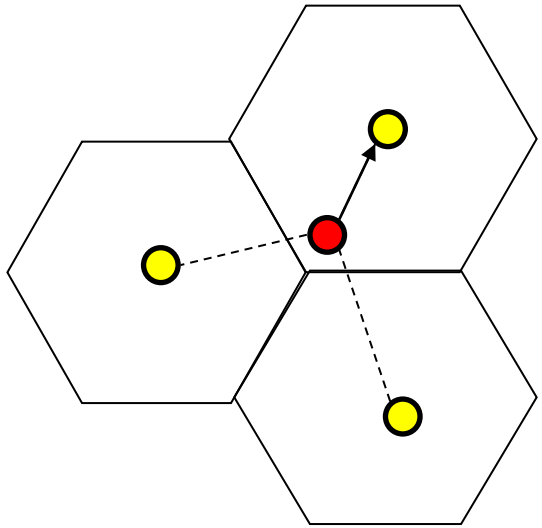


Euler's theorem

$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta}$$

Proximity

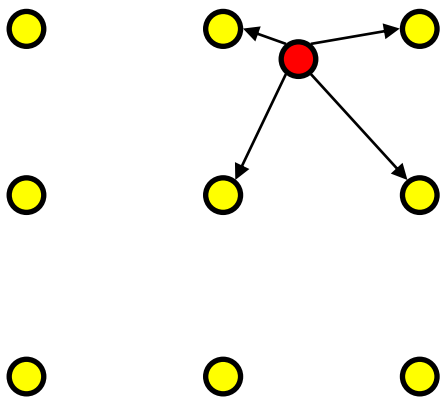
- ***Current location ≡ closest reference point***
  - ToA, RSSI, ...
- Physical contact
  - mouse, keyboards, seats, …
- ***Cell working as "Care of"***
  - Accuracy depending on cell range



- Automated systems for identification
  - Credit card, highway fee payment systems (Telepass, e-toll systems, …), fidelity cards (fuel, shopping malls, ...),RFIDs (building access, e.g., at the School of Engineering and Architecture)

Analysis of Deployment Env: Scene Analysis

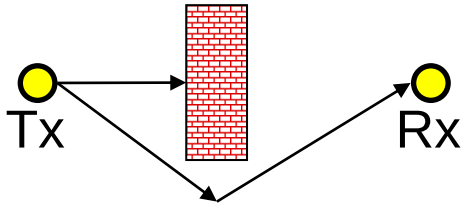
- ***Inference of location info*** by using ***passive observation of "physical phenomena"*** (images, RSSI, ...), but without exploiting physical values such as distances, angles, hyperboles, …
- Requisite: ***knowing the deployment environment***
  - Whether and how the environment changes as time passes by?



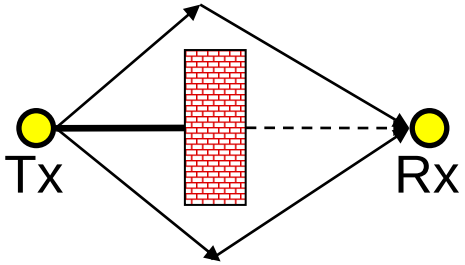
- ***Preliminary phase***
  - Environment monitoring/observation and collection of sensed data
- ***Operational phase***
  - Environment monitoring/observation and comparison between currently observed data and "historical data"

Error Sources

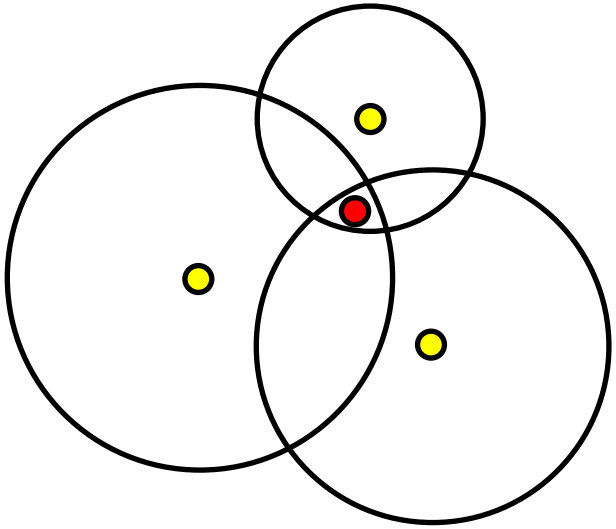
- Non Line Of Sight (NLOS)

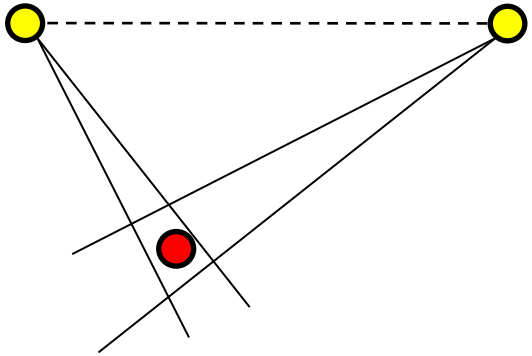


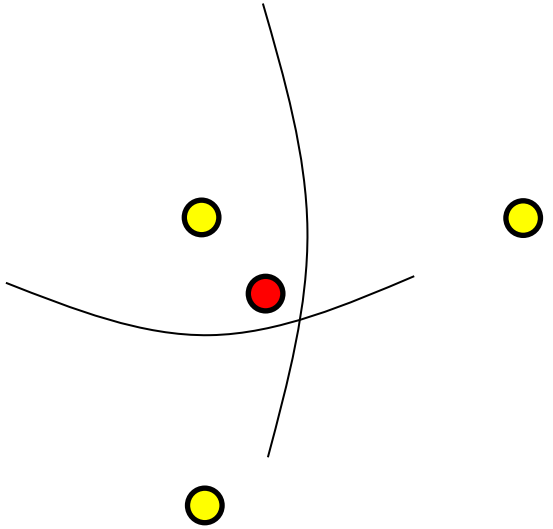
- Fading:
  - Multipath
  - Shadowing



- Clock synchronization







Positioning Systems for Ad-hoc Networks

- Relevant goal: ***to achieve topological and positioning info*** for
  - Maintaining connectivity
  - Optimizing traffic
- ***Cooperative methodologies***, with uniform role for any node:
  1. Each node receives range and positioning data from neighbor nodes
  2. It solves a ***local problem*** of positioning
  3. It transmits the result to neighbors
- Distributed algorithms ***with NO need of global communications***
  - Particularly suitable when node mobility is limited

Assumption Based Coordinates (ABC)

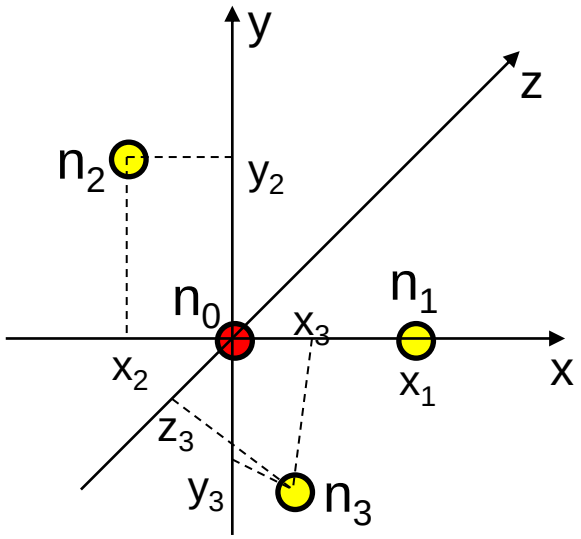
- ***Anchor node***: node with an a-priori known location
- Assumption Based Coordinates
  - Known data: relative distance between nodes
    - Distances may be affected by errors
  - ***Any anchor node creates its own map of relative distances for any node at one-hop distance from it***

$$x_1 = r_{01}$$

$$\begin{cases} x_2 = \dfrac{r^2_{01} + r^2_{02} + r^2_{12}}{2r_{01}} \\ y_2 = \sqrt{r^2_{02} - x_2^2} \end{cases}$$

$$\begin{cases} x_3 = \dfrac{r^2_{01} + r^2_{03} + r^2_{13}}{2r_{01}} \\ y_3 = \dfrac{r^2_{03} - r^2_{23} + x_2^2 + y_2^2 - 2x_2x_3}{2r_{01}} \\ z_3 = \sqrt{r^2_{03} - x_3^2 - y_3^2} \end{cases}$$

r_{jk}: distance between node j and node k



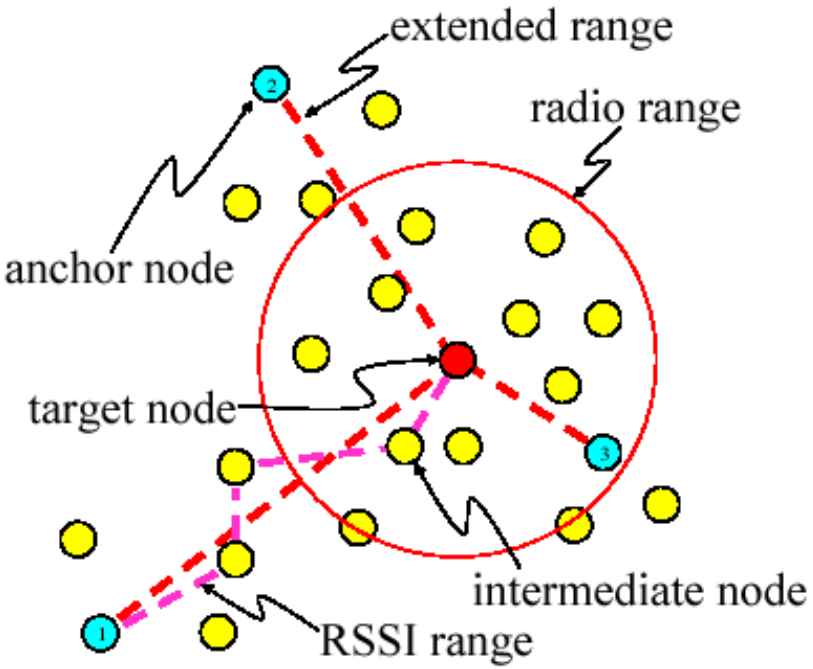
$n_1=(x_1, 0, 0)$

$n_2=(x_2, y_2, 0)$

$n_3=(x_3, y_3, z_3)$

Triangulation via Extended Range and Redundant Association of Intermediate Nodes (TERRAIN)

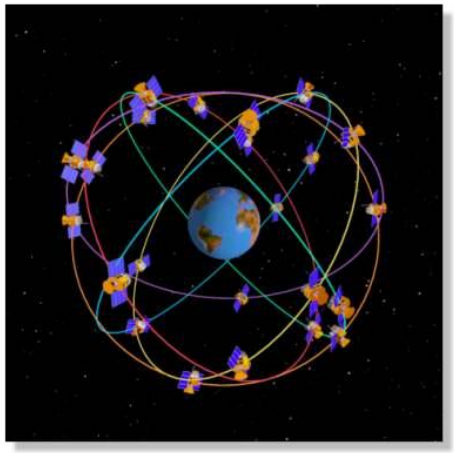
- To create ***a single map of nodes that exploits data about nodes at multi-hop distance***
- extended range = #hop * average node distance



Positioning Systems with Dedicated Hardware

Hardware special-purpose specifically developed and added to obtain location info

- Based on RadioFrequency, InfraRed, (Ultra)Sound
- It improves accuracy and precision ☺
- It tends to increase device size and energy consumption ☹



Notable example of external positioning solution = Global Positioning System

- USA Department of Defense (DOD)
- At least 24 satellites that operate in orbit at 11000 miles (around 18000km) from ground
  - http://tycho.usno.navy.mil/gps.html
    - First satellite: 14 Feb 1989
- Most widespread positioning system (it is not the only one…)

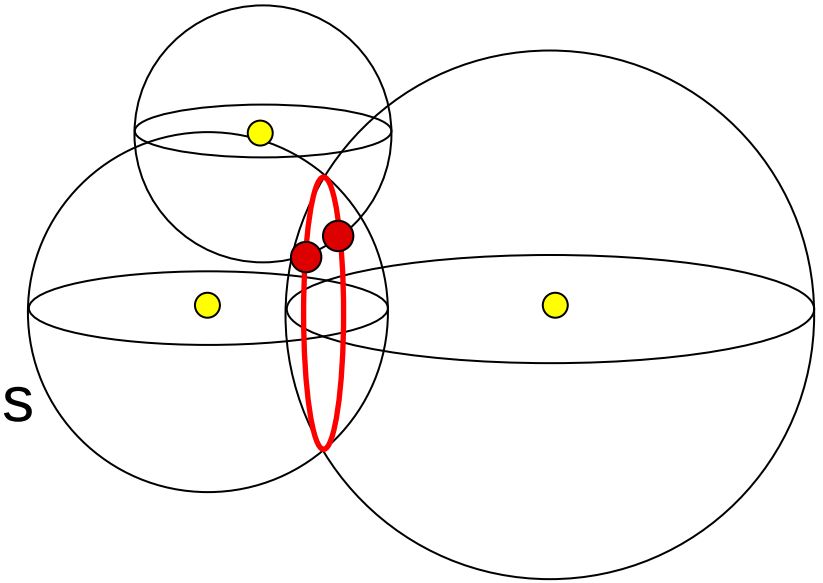
GPS: How does it Work?

- ***Info that are known*** thanks to GPS:
  - Satellite position
  - Signal propagation time from satellite to client (around 60ms)
    - distance = ToA*light speed

- How to use this info?
  - ***Lateration + ToA***

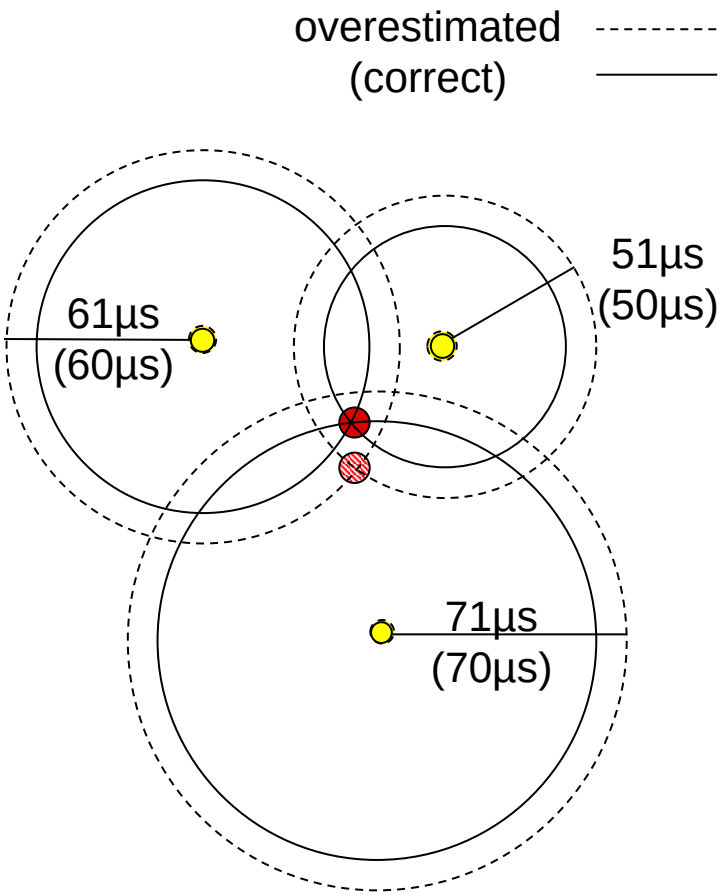
- 3 satellites ➔ 2 possible positions
  - 1 position however is NOT on the terrestrial surface

    (space/ultra-atmospheric elevation)



GPS: Synchronization

- ***ToA → need of having synchronized clocks***
  - satellites with atomic clock
    - High accuracy
  - clients with “regular” clock
    - Accuracy issues
- Error of 1µs → around 300m
- ***Synchronization***, by exploiting protocol with 4 satellites (3 for 2D solutions): ***client clocks are affected by shifting*** until the completion of sync operation



2D example with sync errors

GPS Errors

Additional further ***potential sources of error***:

- Atmospheric conditions: ionosphere (0-30m) and troposphere (0-30m) refract GPS signal ➔ speed change of GPS signal
- Errors due to Ephemerides: exact positioning of the satellite orbit (1-5m)
- Clock drift: also atomic clocks are not perfect (0-1.5m)
- Measurements “noise” (0-10m)
- Selective Availability: since 2000, introduced by purpose by the DoD (0-70m)
- Multipath: very tall buildings, mountains, ... (0-1m)

For higher accuracy ➡ ***differential GPS***

Differential GPS (D-GPS)

as an example of Ground Based Augmentation System

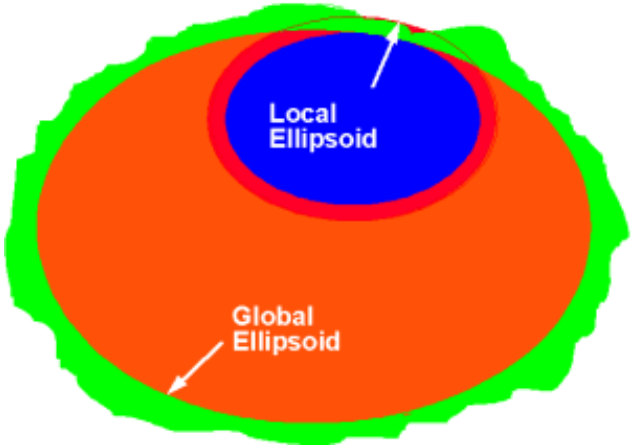
- It exploits a ***base station*** (or other infrastructure element) ***with a perfectly known position*** to calculate ***differences*** from exact positioning and discard errors (systematic errors)
- GPS clients operate the usual processing and behavior
- ***Better accuracy (even 15-50cm vs. 50-100m)*** by obtaining systematic error vector and subtracting it from the non-differential GPS-obtained location

Source	GPS	D-GPS
Ionosphere	0-30m	Mostly Removed
Troposphere	0-30m	All Removed
Signal Noise	0-10m	All Removed
Ephemeris Data	1-5m	All Removed
Clock Drift	0-1.5m	All Removed
Multipath	0-1m	Not Removed
SA	0-70m	All Removed

By Summarizing, GPS…

- Physical + absolute location
  - WGS84 World Geodetic System: latitude, longitude, and ellipsoid height (it compensates continent movements)
- Distributed
- High costs: infrastructure (!!!) + client
- Scalability: completely distributed ➔ optimal scalability
- No identification + distributedness ➔ user privacy
- Accuracy = 100m/<1m, precision = 95%
- Strong limitations: ***only outdoor***

  (need of LOS)



Not only GPS: Active Badge

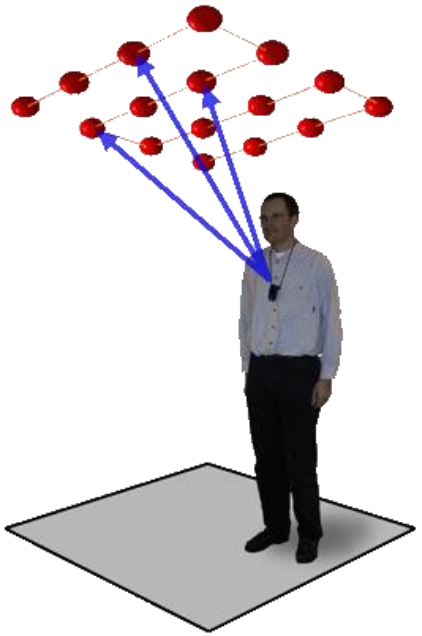
Olivetti Research Laboratory (now AT&T Cambridge):
one of the first approaches to the localization issue

- ***Infrared technology***
  - Badge ***periodically emits a unique identifier***
  - Sensor network receives signals from badges (need of proximity, typically same room)
  - Central server collects data from sensors
- Proprieties:
  - Based on proximity
  - Symbolic, absolute
  - User identification
  - Low cost
  - Accuracy (room grain)
  - IR does not work well in presence of solar light and fluorescence

Active BAT

AT&T Active BAT

- Substantially ***Ultra-Sound (US) technology***
  - Badge emits a unique identifier to a central server
  - Central server
    - It triggers the badge (via RF), asking it for sending the US signal
    - It resets US receivers that are installed on ceiling
    - It collects data
    - It calculates the badge position
- Proprieties:
  - ToA, physical, absolute, identification, low cost, accuracy = 9 cm, precision = 95%

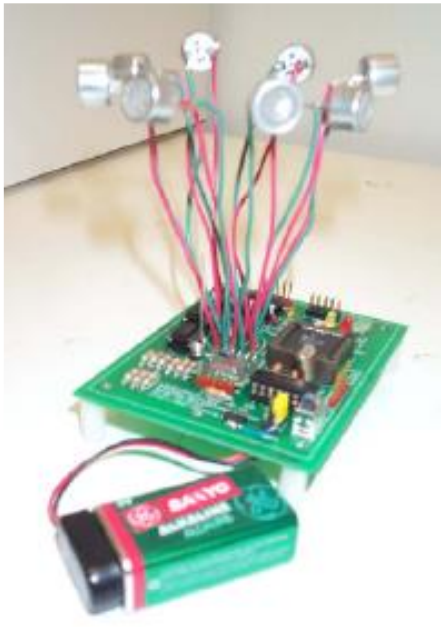


AHLoS: Ad-Hoc Localization System

UCLA AHLoS

- RF and US technologies
- Lateration + ToA
  - RSSI vs. RF, US

WINS (900 MHz RF)



Medusa (US)

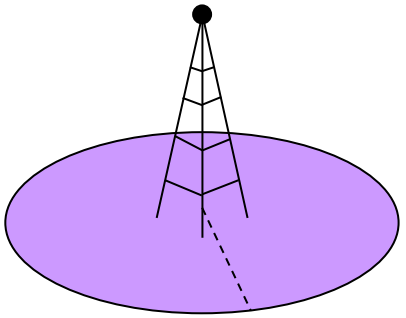
Property	RSSI	UltraSound
Range	same as radio communication range	3m
Accuracy	2-4m for WINS	2cm for Medusa
Measurement Reliability	hard to predict, multipath and shadowing	multipath mostly predictable, time is a more robust metric
Hardware Requirements	RF signal strength must be available	US transducers and amplifier circuitry
Additional Power Requirements	none	tx and rx signal amplification
Challenges	large variances in RSSI readings, multipath, shadowing, fading effects	interference, obstacles, multipath

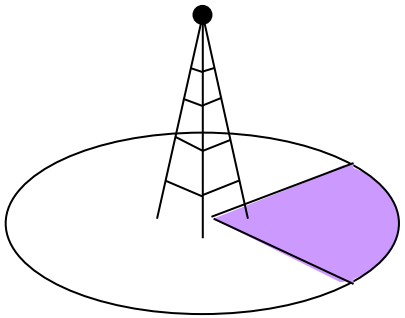
Positioning Systems with NO Dedicated Hardware

Exploiting what is ***already available for communication purposes***, e.g., GSM/GPRS/UMTS, Bluetooth, 802.11

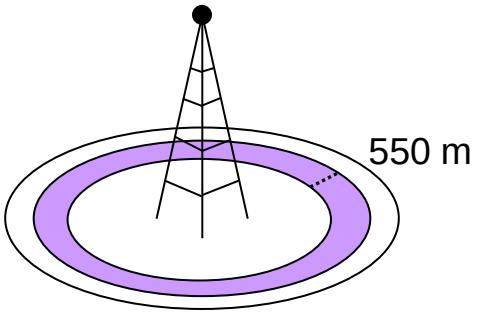
For example, ***GSM cellular and network-based positioning***

- Cell Global Identity (CGI)
- Angle of Arrival (AoA)
- Timing Advance (TA)
- Signal Strength
- Uplink Time of Arrival (UL-ToA)
- Uplink Time Difference of Arrival (UL-TDoA)

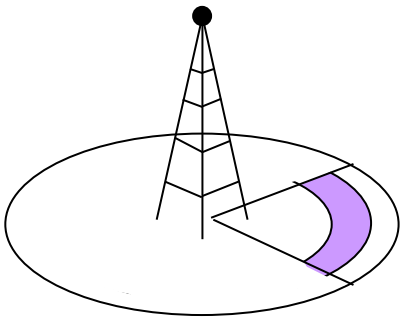




CGI
(with directional antennas)



CGI + TA



CGI + TA
(with directional antennas)

Positioning based on GSM

Or, ***again in GSM, Mobile Station (MS)-based***

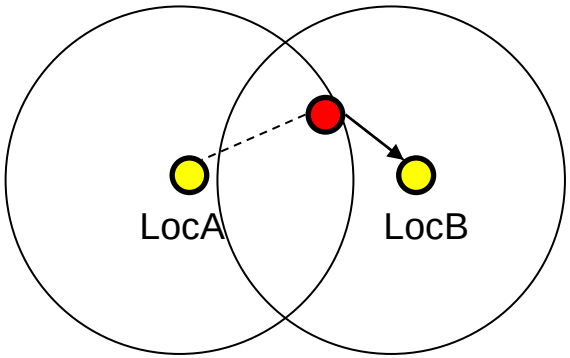
- Enhanced - Observed Time Difference (E-OTD ≡ TDoA)
  - At least three Base Transceiver Stations in visibility
- Timing Advance
  - At least two "forced" handovers

Technology	Computation locality	User Controlled Privacy	Modifications		System Accuracy	
			HW	SW	urban environment	rural environment
CGI	network	no	none	none	> 100m	< 35 Km
CGI+TA	network	no	none	none	> 100 m	circle of arc of 550 m
UL-ToA	network	no	GPS for clock synch		150 m	50 m
UL-TDoA	network	no	GPS for clock synch		50 m	80 m
E-OTD	MS	yes	none	yes	200 m	60 m

Positioning based on Bluetooth

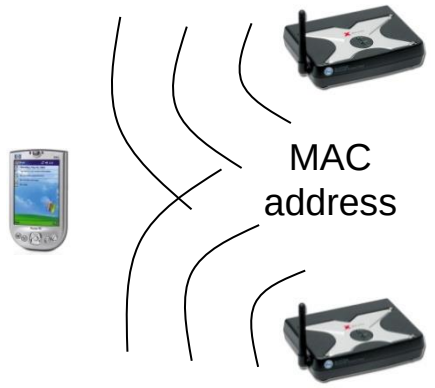
- ***Bluetooth is low cost and with coverage range that is relatively limited*** ➔
  - proximity, accuracy < BT range (around 10m)
  - symbolic, absolute, distributed
- Possible solution:
  - ***BT devices installed at Points Of Interest (POIs)***
  - DB with POI locations:

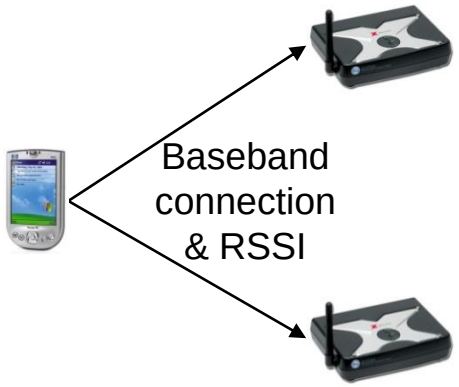
    association between BT POI MAC Address → POI location
  - Visibility of multiple BT devices
    - Selection of the closest one ➔ with highest RSSI

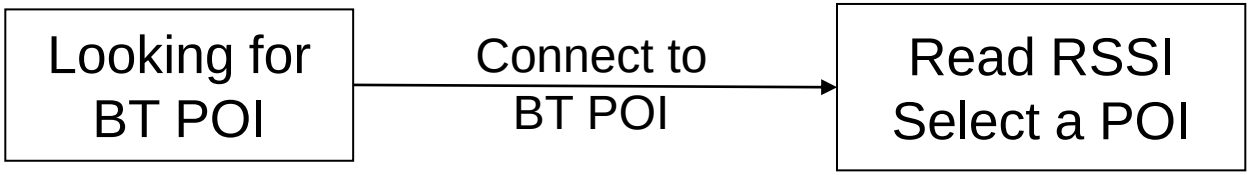


How It May Work

1. POIs perform ***broadcast*** of their MAC address
2. Device overhears POI messages
3. Device ***connects to the visible POIs***
4. For each POI, device ***measures***
   RSSI of the established connection
5. Device calculates its own location
   by comparing the measured RSSI values







Bluetooth allows Differentiated Privacy Levels

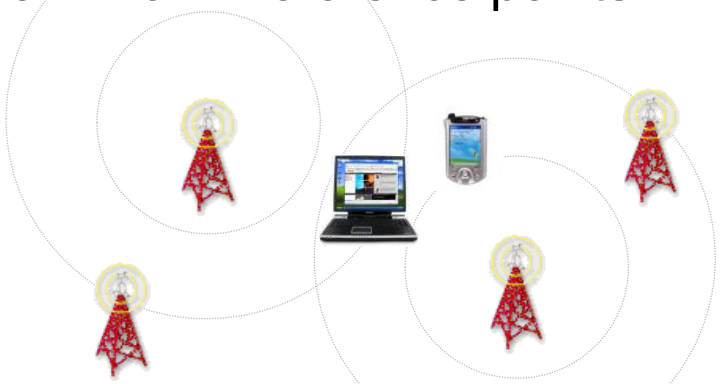
Device may be willing to know which POIs are close to it, but sometimes not to make them aware of its own presence. Let us recall that ***wireless communications may be asymmetric***

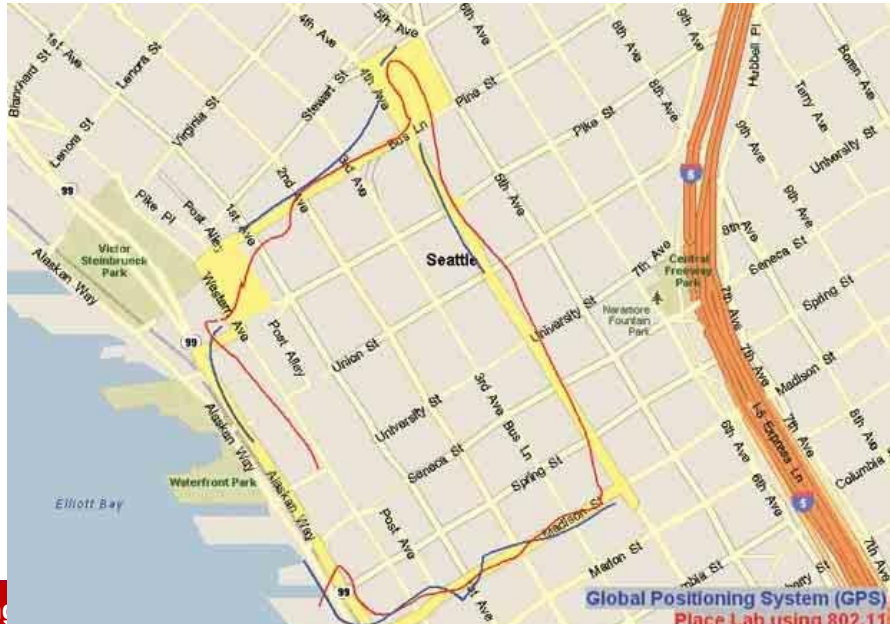
- BT client:
  - inquiry scan on
    - Any neighbor BT POI can see the device
  - page scan on, inquiry scan off
    - POIs CANNOT see the device but can try to connect to it if they know the device identifier
  - Inquiry scan off, page scan off ***(NO visibility of RSSI, but…)***
    - ***stealth mode***: none can see the device (until the device does not connect voluntarily…)

PlaceLab

Basic idea: ***to exploit wide-scale WiFi deployment***

- Urban areas with “dense” coverage by WiFi APs
- WiFi APs ***send beacons with unique IDs*** (MAC addresses of the APs)
- Positioning WiFi devices by using a ***map of correspondences between base-station-IDs and locations***
- Many possible algorithms to calculate approx position based on known reference points





PlaceLab: Which Primary Issues?

- ***To build a world-wide DB with the positions of all WiFi APs***
  - How to estimate AP positions if exact data are not available?
- Good algorithms for accurate positioning
  - Tradeoff between ***accuracy and calibration overhead***
- ***Accettable privacy model*** for a large public of users
  - Who determines location?
  - How does the final user keep under her control her location info?

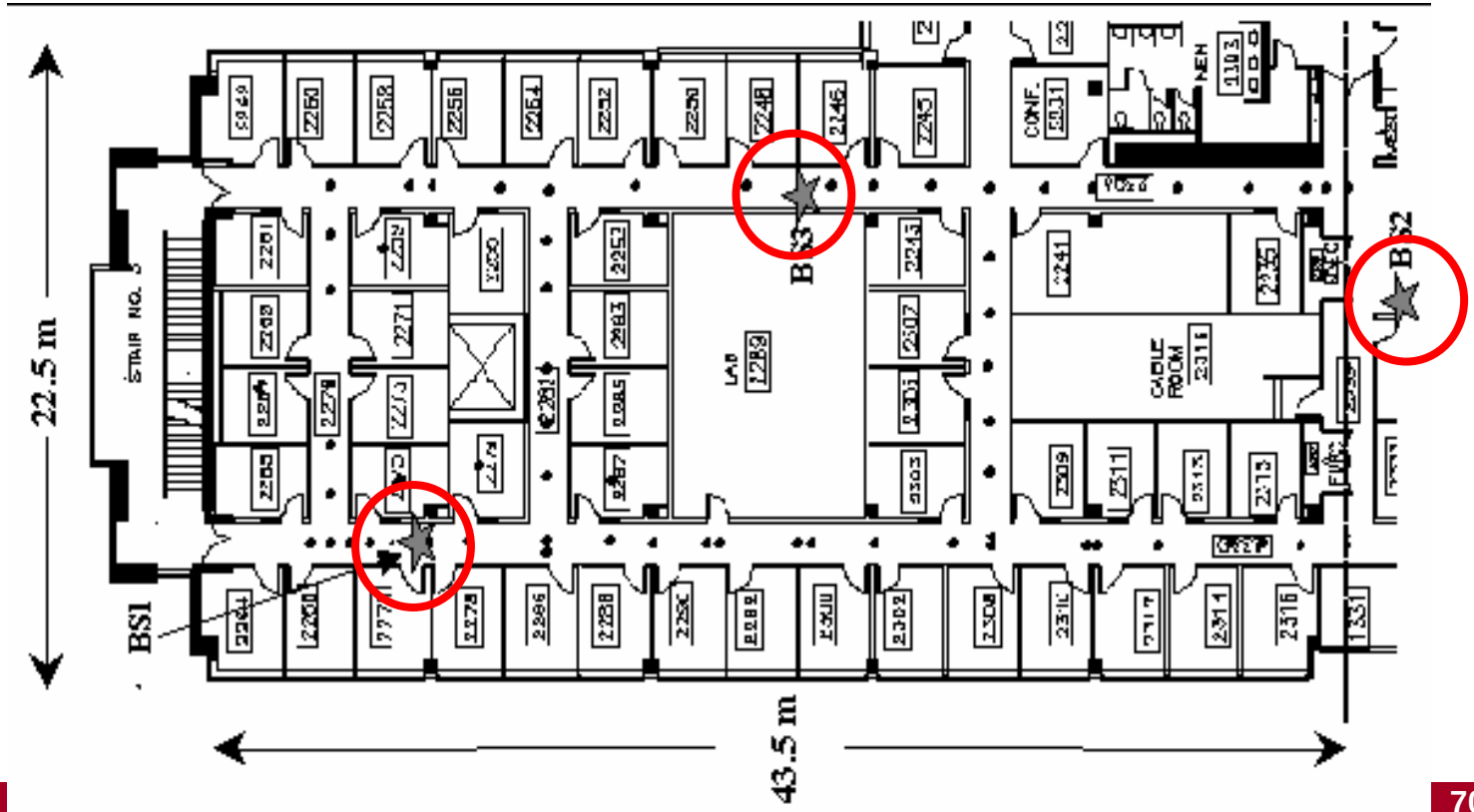
PlaceLab: Methodology

- ***Training phase***
  - To collect beacons from WiFis via “war driving” with devices equipped with ***IEEE802.11+GPS***
  - From this data campaign, to store
    - GPS coordinates
    - AP lists
  - It requires work for around 1hr per km^2
  - To build a ***map of the radio signal starting from the collected traces***

- ***Positioning phase***
  - To exploit the radio map to position final users
  - Possibly to compare the estimated position with the result returned by GPS, in order to enable further refinement

RADAR: Basic Idea

- To some extent, similar to PlaceLab, ***for indoor envs***
- Scenario: IEEE 802.11 APs
- Scene analysis (*fingerprinting*) based on RSSI
  - two phases: first phase is off-line, then real-time phase



RADAR: Off-line and Real-Time Phases

- ***Off-line phase***
  - Collection of ***empirical data from the field, accumulated at the infrastructure side***
    - Mobile clients ***periodically broadcast UDP packets*** that include ***location and spatial orientation***, manually inserted by users
    - APs collect and store ***RSSI values (average) of received UDP packets, with associated timestamp*** (need for node sync)
    - server puts together the data collected from any participant AP
- ***Real-time phase***: device tracking
  - Mobile clients ***periodically broadcast UDP packets***
  - Centralized server calculates positioning info
    - Nearest Neighbor in Signal Space (NNSS), with Euclidean distance between RSSI values, or
    - Algorithms based on history, or…

Ekahau: Basic Idea

- Model of world-environment that is ***stochastic, not deterministic***; it is recognized that ***signal measurements are intrinsically affected by error and noise***
- ***Model calibration*** is solved as a ***machine learning problem***: again, ***scene analysis based on RSSI values***

- ***Rail tracking principle***:
  - ***Current location is probably near the most recent calculated locations for that device***
  - Users can follow only ***allowed paths*** (*legal paths*, e.g., NO wall traversing) ➔ ***Hidden Markov Model***

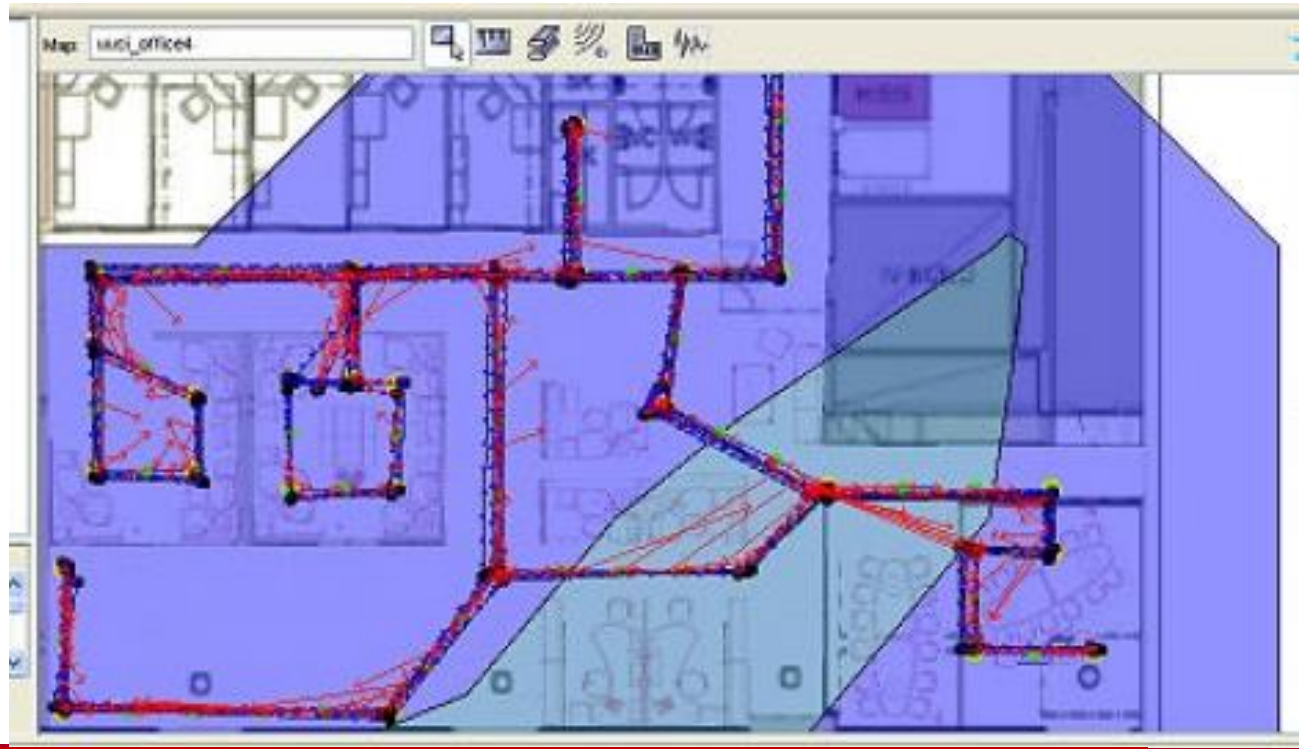
Ekahau: Architecture and Principles

Similar to RADAR (learning phase, RSSI fingerprinting) but...

- ***Mobile devices collect RSSI data*** (not the APs) and send them to a centralized server only when needed to determine their location ➔ therefore, mobile devices CAN choose when/whether to be positioned by the server
- **Rail tracking** with environment map and allowed paths

Ekahau: Main Characteristics

- Physical & symbolic
- Absolute
- Low cost?
  - Data collection is time-consuming
- Privacy:
  do we trust in the Ekahau server?



Sensor Fusion: Positioning Fusion

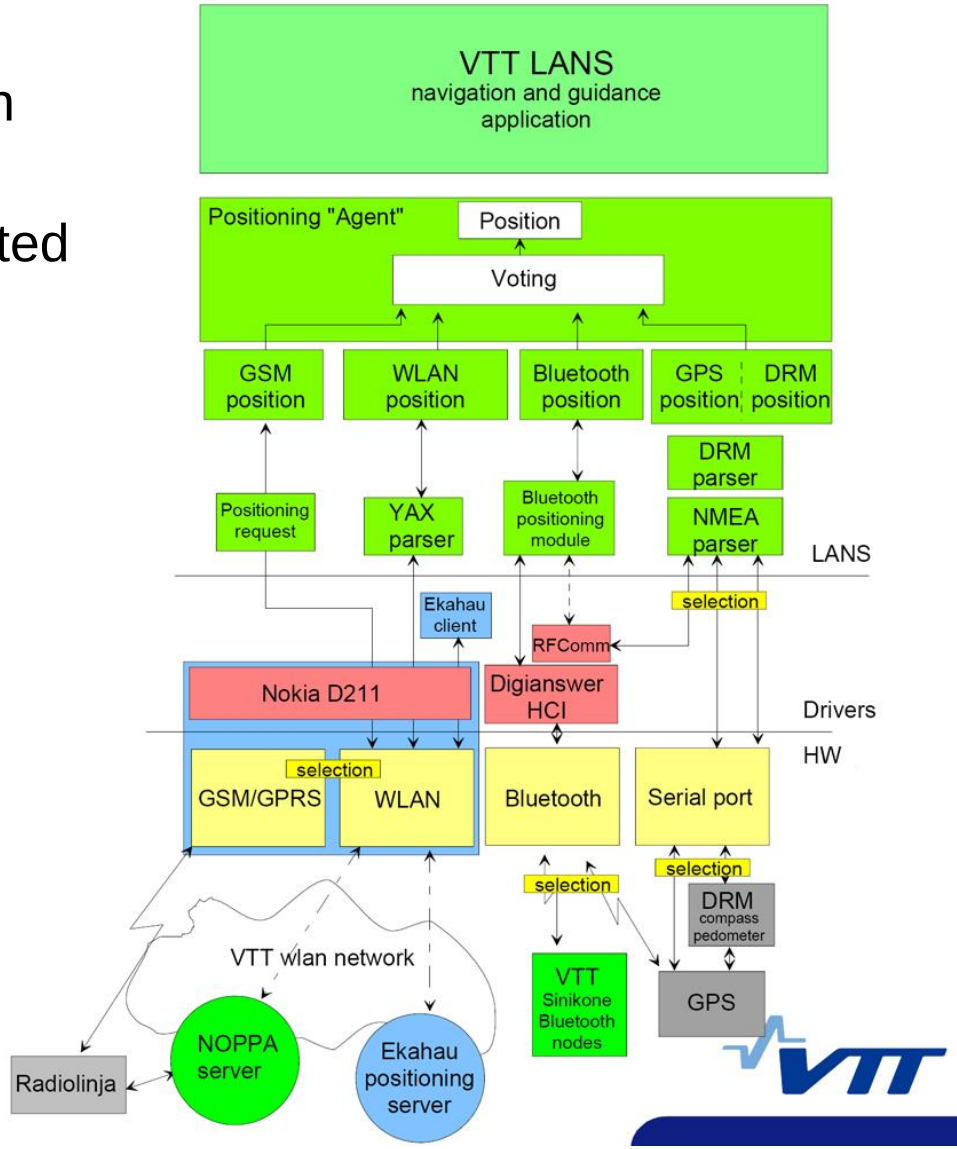
- In general, approach with N data sources that are aggregated to obtain M output results
- From raw data to structured/aggregated data at a higher abstraction level

This approach is possible also for positioning.
For example, VTT solution:

- NO aggregation, ***pure selection***
- Vote mechanism, election
  Maximization of

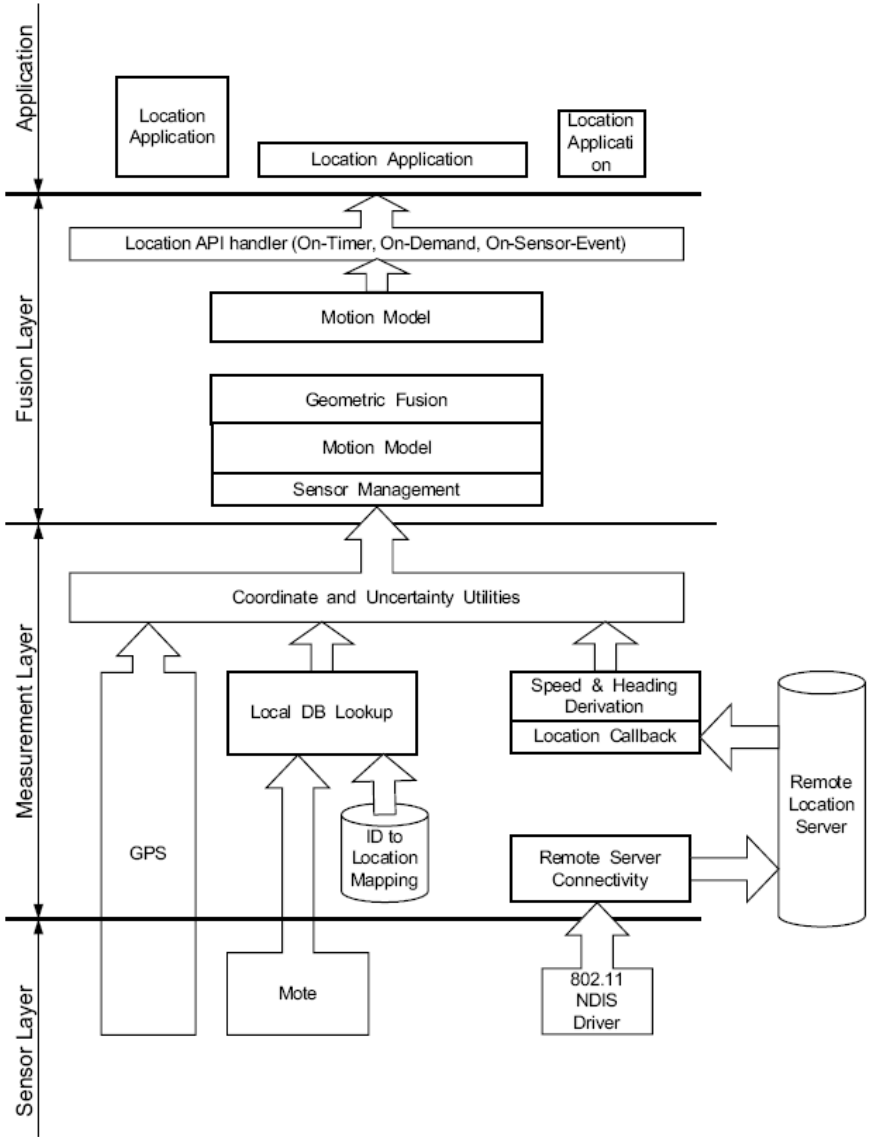
$$k_n = \frac{1}{t_{age} * v + \varepsilon}$$

speed v, positioning age t_{age}, accuracy ε



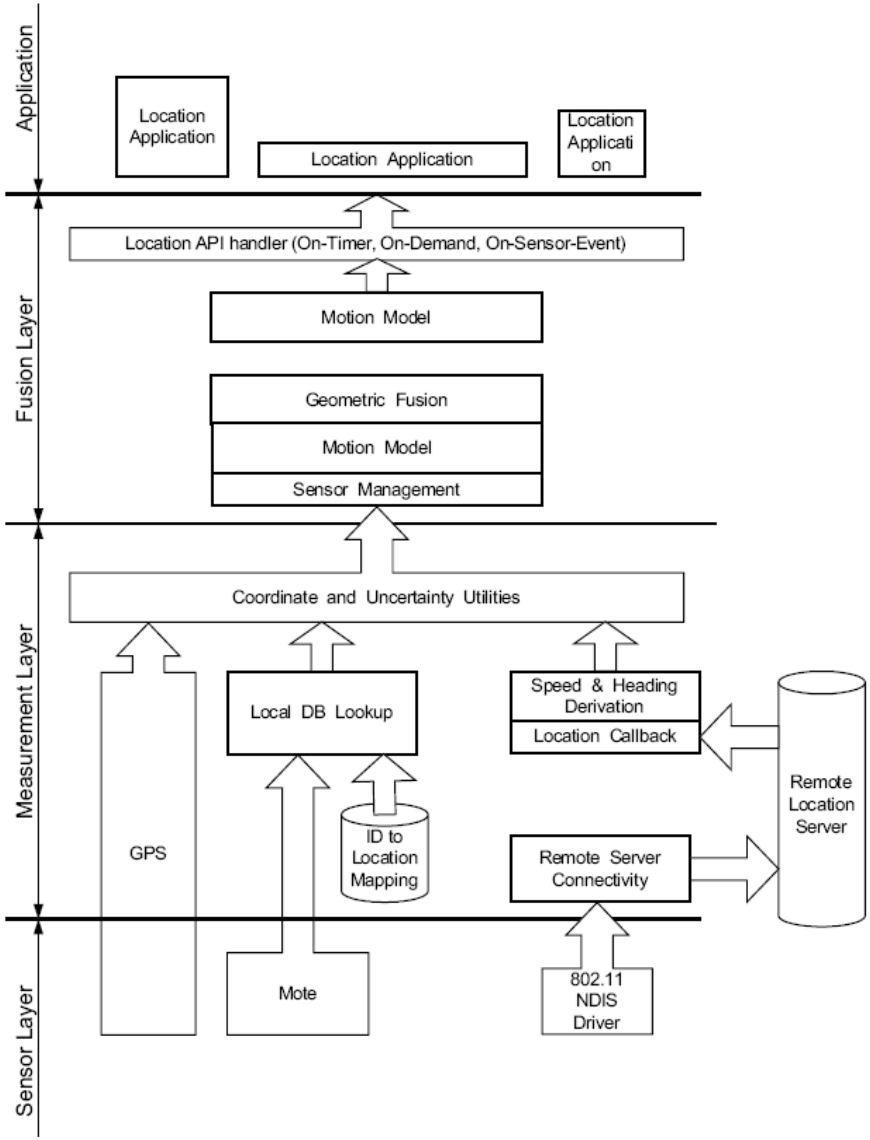
Universal Location Framework

- ***Multiplicity of positioning systems***
  - GPS, IEEE 802.11, Mote (low-cost sensor by UC Berkeley)
- Measurements in WGS-84 format
  - GPS: raw data
    - Accuracy info added
  - 802.11: RADAR-like
    - Altitude info added
    - Battery consumption management
  - Mote: proximity → WGS-84
    - From symbolic to physical data



Universal Location Framework

- ***Fusion***
  - Sensor management
    - ***one or multiple together?***
    - ***accuracy & precision***
  - Mobility model
    - exploitation of data about speed and spatial orientation
  - Determination of the “merged” value
- ***Location API that is uniform and high level***
  - Automated update, manual, periodic
- ***Cross-layer management of sensors and location info quality***



PoSIM and JSR-179

Positioning System Integration and Management (PoSIM)

- Based on “translucent” approach
  - ***Transparency***: Policy & Data Managers
  - ***Visibility***: Positioning System Access Facility
- Compliant with standard Java JSR-179 (if you want to go into deeper technical details…)