ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Secure Positioning in VANETs

Maxim Raya

Based on the work of Srdjan Capkun[1] and Jean-Pierre Hubaux

Laboratory for computer Communications and Applications (LCA)

[1]*Now with Safe and Secure IT-Systems Group,*
Informatics and Mathematical Modeling (IMM),
Technical University of Denmark

Outline

- Motivation
- State of the art
- Why GPS is not enough
- Distance measurement techniques
- Distance bounding
- Verifiable multilateration
- Conclusion

Motivation

- Correct location information is essential in VANETs
  - Warnings
  - Geographic routing
  - Location-based services
  - …
- GPS is not enough
- Example attacks: black hole, wormhole, routing loop, path interposition, neighbor puzzle, sybil wall blocking, etc.
- Two approaches:
  - **Secure location verification**
  - **Secure positioning**: stronger but also more difficult to achieve

Positioning systems and prototypes

Satellites:

-**GPS, Galileo, Glonass** *(Outdoor,* ***Radio Frequency (RF) – Time of Flight (ToF)****)*

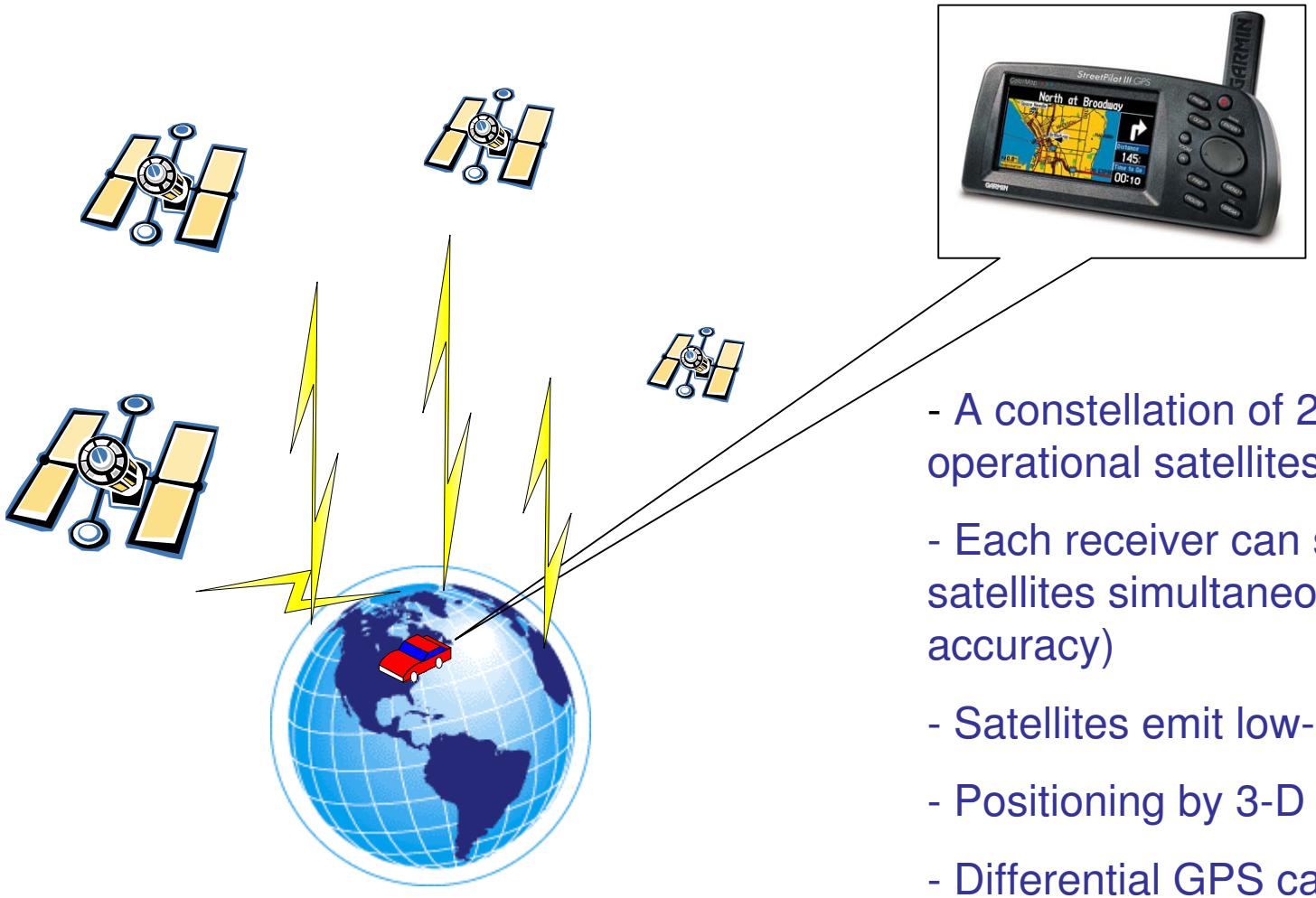
General systems:

- **Active Badge** *(Indoor,* ***Infrared(IR)****),* Olivetti
- **Active Bat, Cricket** *(Indoor,* ***Ultrasound(US)****-based), AT&T Lab Cambridge, MIT*
- **RADAR, SpotON, Nibble** *(Indoor/Outdoor,* ***RF- Received Signal Strength****),* Microsoft, Univ of Washington, UCLA+Xerox Palo Alto Lab
- **Ultra Wideband Precision Asset Location System,** *(Indoor/Outdoor,* ***RF-(UWB)-ToF****),* Multispectral solutions, Inc.

Ad Hoc/Sensor Network positioning systems (without GPS):

- **Convex position estimation** *(****Centralized****),* UC Berkeley
- **Angle of Arrival based positioning** *(****Distributed****, Angle of Arrival)*, Rutgers
- **Dynamic fine-grained localization** *(****Distributed****),* UCLA
- **GPS-less low cost outdoor localization** *(****Distributed****, Landmark-based),* UCLA
- **GPS-free positioning** *(****Distributed****),* EPFL

GPS



- A constellation of 24 Earth-orbiting operational satellites

- Each receiver can see at least 4 satellites simultaneously (to improve accuracy)

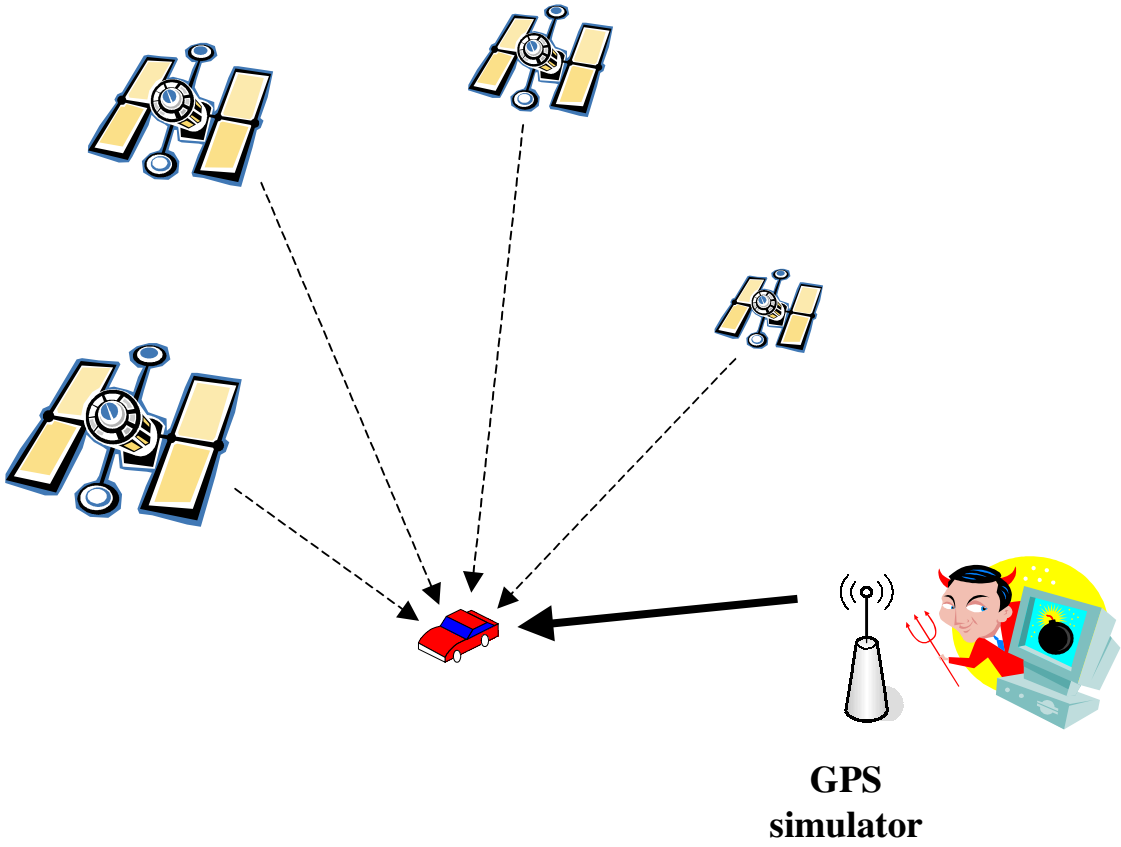
- Satellites emit low-power signals

- Positioning by 3-D trilateration

- Differential GPS can improve accuracy from several meters to a few centimeters.

GPS Security – Example of attack

- A GPS simulator can send strong fake signals to mask authentic weak signals



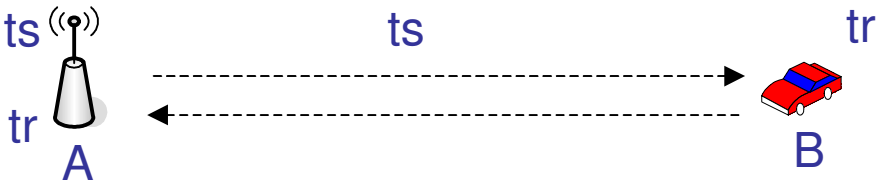
GPS Security

- Other vulnerabilities
  - Relaying attack: connects the receiver to a remote antenna
  - Signal-synthesis attack: feeds the receiver with false signals
  - Selective-delay attack: introduces a position error
- Security solutions
  - Tamper-resistant hardware
  - Symmetric crypto
    - Problem: an authenticated receiver can hack the system
  - Asymmetric crypto
    - Problem: additional delay

Distance measurement techniques

- Based on the speed of light (RF, Ir)

$d_{ABm}=(tr-ts-t_{procB})c/2$

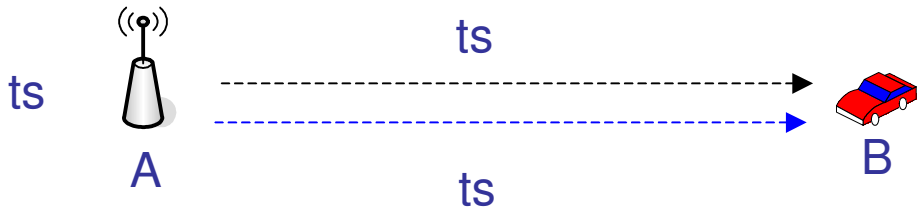


$d_{ABm}=(tr-ts)c$

(A and B are synchronized - ToF)

(A and B are NOT synchronized – Round trip ToF)

- Based on the speed of sound (Ultrasound)



$d_{ABm}=(tr(RF)-tr(US))s$

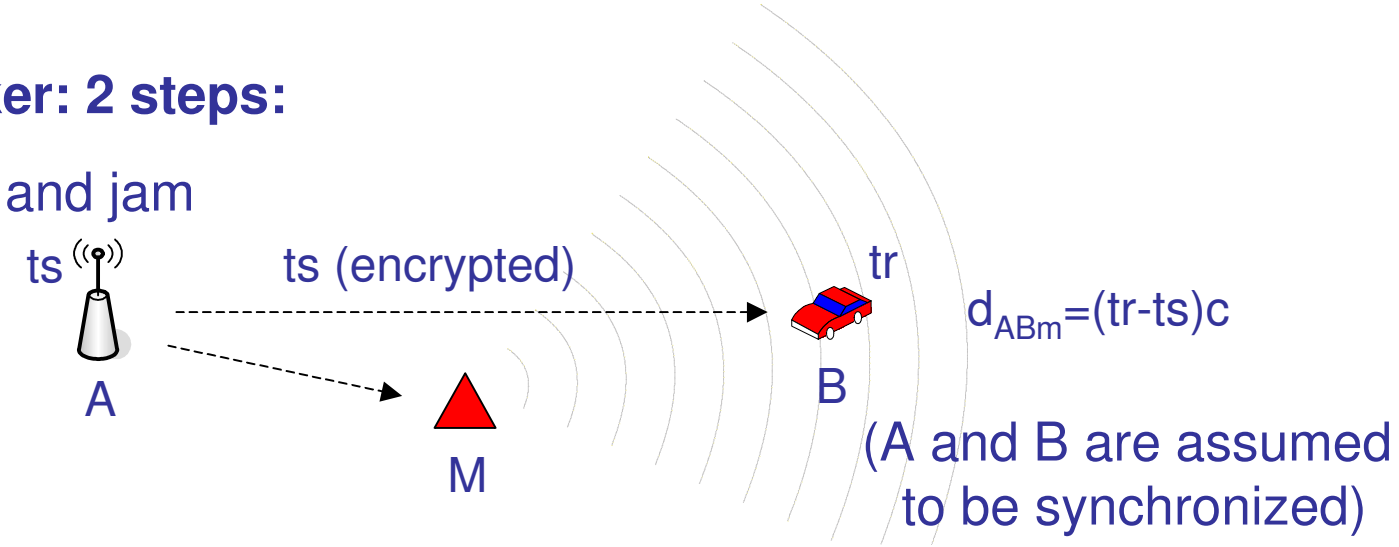
- Based on Received Signal Strength (RSS)

Attacks on RF and US
ToF-based techniques

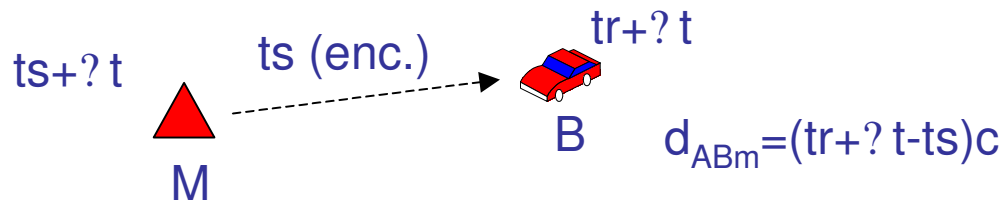
- Insider attacker: cheat on the time of sending (**ts)** or time of reception (**tr)**

- Outsider attacker: 2 steps:

1. Overhear and jam



2. Replay with a delay ?t



=> $d_{ABm} > d_{AB}$

Summary of possible attacks on distance measurement

	Insider attackers	Outsider attackers
RSS (Received Signal Strength)	Distance enlargement and reduction	Distance enlargement and reduction
Ultrasound Time of Flight	Distance enlargement and reduction	Distance enlargement and reduction
Radio Time of Flight	Distance enlargement and reduction	Distance enlargement only

The challenge of secure positioning

- **Goals:**
  - preventing an **insider attacker** from **cheating about its own position**
  - preventing an **outsider attacker** from **spoofing the position of an honest node**

- **Our proposal: Verifiable Multilateration**

Distance Bounding (RF)

- Introduced in 1993 by Brands and Chaum (to prevent the Mafia fraud attack)

A : generate random nonces N_A, N'_A

: generate commitment $commit = h(N_A, N'_A)$

$A \rightarrow BS$: $commit$

BS : generate random nonce N_{BS}

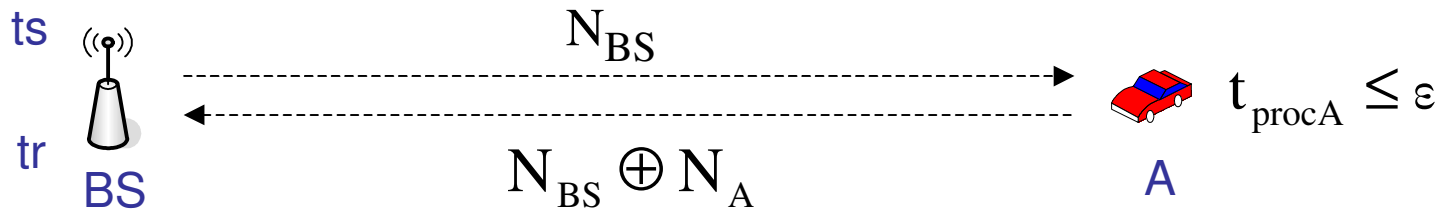
$BS \rightarrow A$: N_{BS}

$A \rightarrow BS$: $N_{BS} \oplus N_A$

BS : measure the time t_{BSA} between sending N_{BS} and receiving $N_{BS} \oplus N_A$

$A \rightarrow BS$: $N'_A,\ sig_{K_A}(A, N'_A)$

BS : verify if the signature is correct and if $commit = h(N_A, N'_A)$



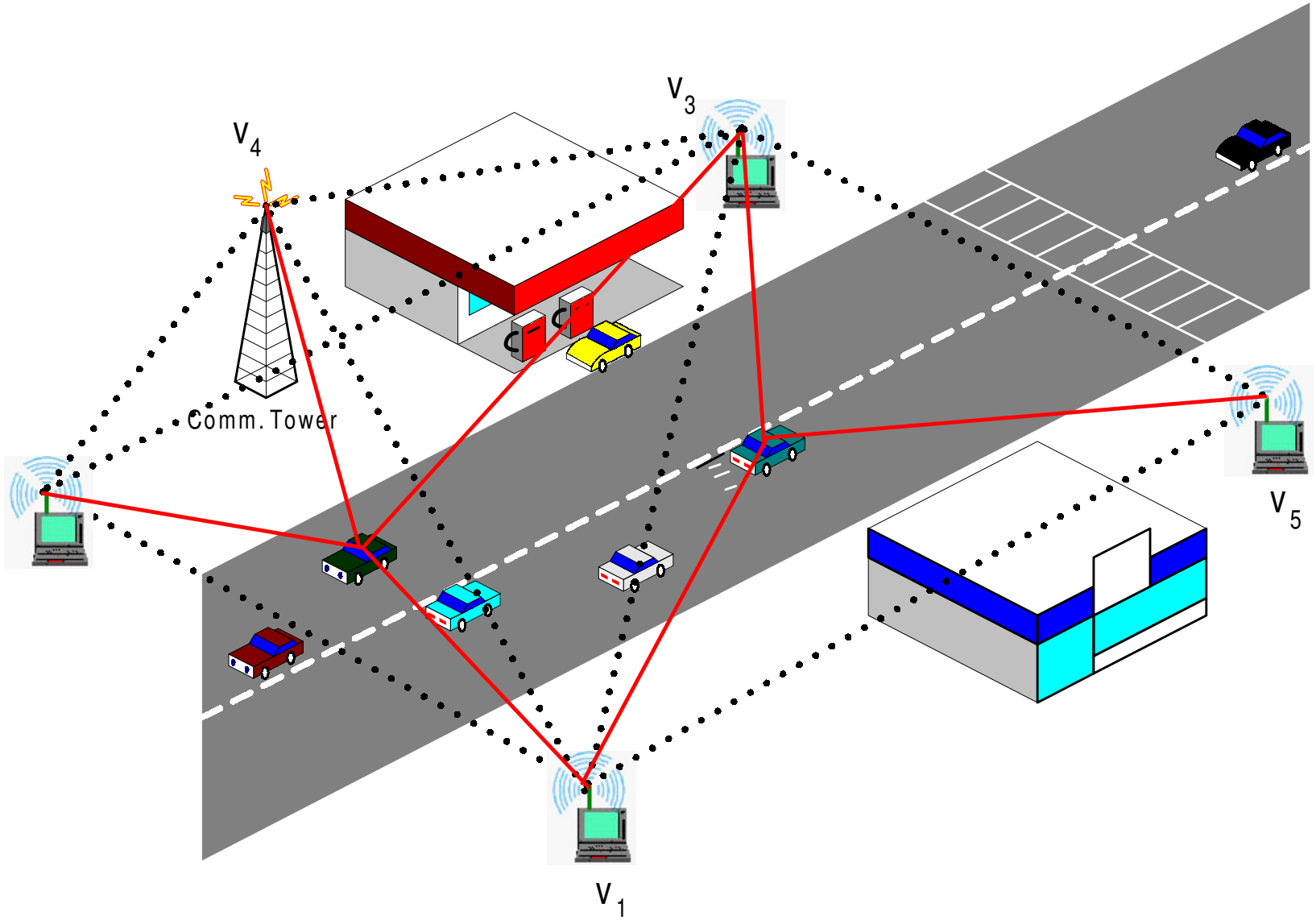
d_{real} = db = (tr-ts)c/2 (db=distance bound)

Distance bounding characteristics

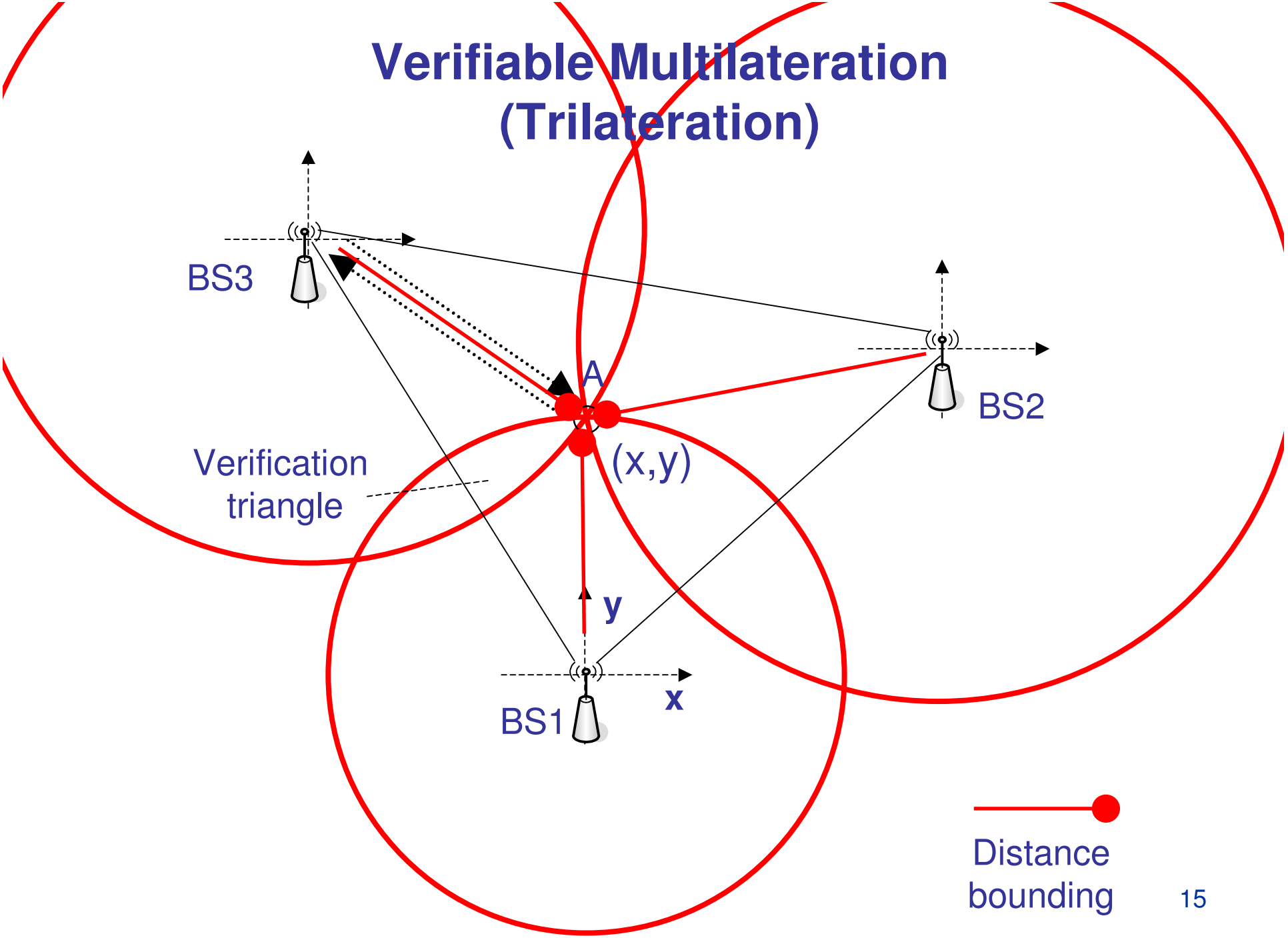
- **RF distance bounding:**
  - nanosecond precision required, 1ns ~ 30cm
  - UWB enables clock precision up to 2ns and 1m positioning indoor and outdoor (up to 2km)
- **US distance bounding:**
  - millisecond precision required,1ms ~ 35cm

RF Distance Bounding	Distance enlargement only	Distance enlargement only
US Distance Bounding	Distance enlargement only	Distance enlargement and reduction

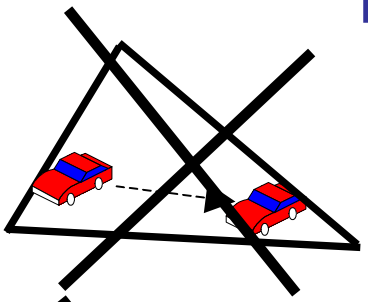
How to *securely* locate a vehicle



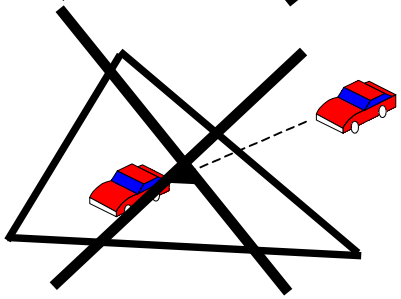
Verifiable Multilateration (Trilateration)



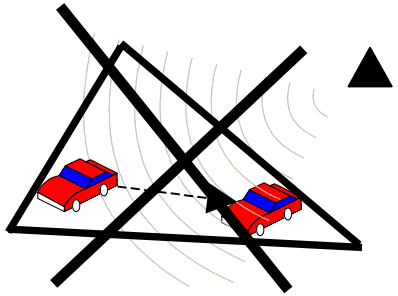
Properties of Verifiable Multilateration



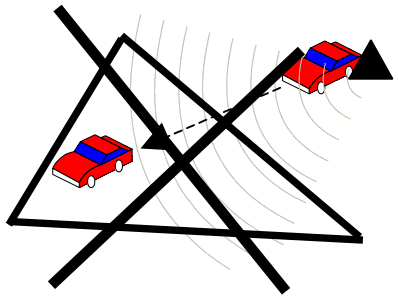
- a vehicle located within the triangle cannot prove to be at another position within the triangle except at its true position.



- a vehicle located outside the triangle formed by the verifiers cannot prove to be at any position within the triangle



- an outsider attacker cannot spoof the position of a vehicle such that it seems that the vehicle is at a position different from its real position within the triangle



- an outsider attacker cannot spoof the position of a vehicle such that it seems that it is located at a position within the triangle, if the vehicle is out of the triangle

The same holds in 3-D, with a triangular pyramid instead of a triangle

Conclusion on secure positioning

- New and challenging research area
- Solutions will probably be hybrid and rely on GPS, RSUs, and mutual distance estimation
- Time of flight seems to be the most appropriate technique

- More information available at: http://spot.epfl.ch

Srdjan Capkun and Jean-Pierre Hubaux, Secure Positioning of Wireless Devices with Application to Sensor Networks, *Infocom 2005*