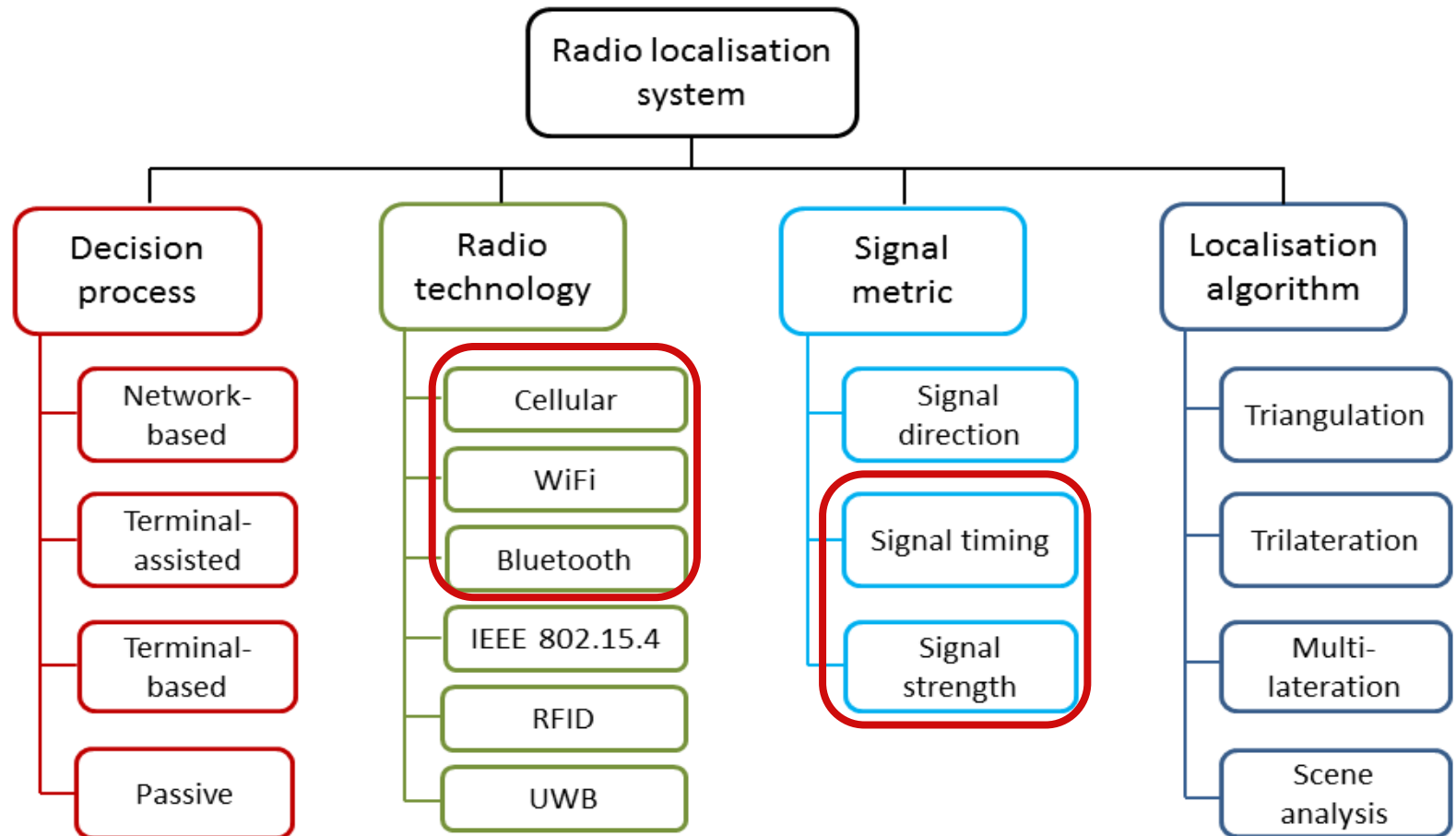# *Active vs Passive localisation strategies*

D. C. Dimitrova
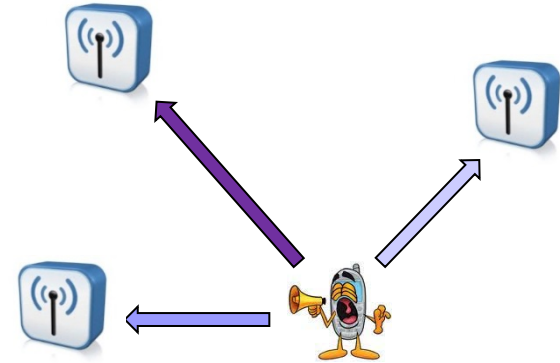
University of Bern

outline

- Localisation systems taxonomy
- Passive system perspective
  - Passive system with RSS
  - Passive system with TOA
  - The eavesdropping challenge
- Active system perspective
  - Network-based
  - Terminal-based
- Discussion

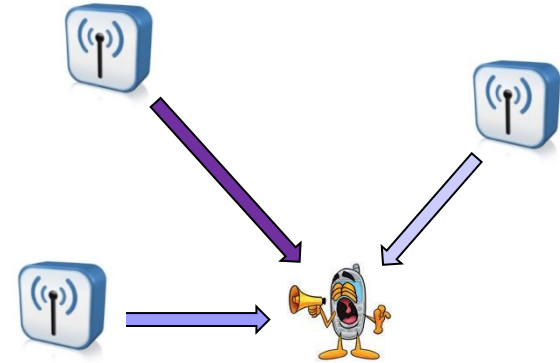# Localisation systems taxonomy

Localisation systems taxonomy

- **Network-based & Network assisted**
  - Full information & computational power
- Terminal-based
  - Limited computation
- Passive
  - Third-party devices
  - Traffic overhearing
  - No feedback

Localisation systems taxonomy

- Network-based & Network assisted
  - Full information & computational power
- **Terminal-based**
  - **Limited computation**
- Passive
  - Third-party devices
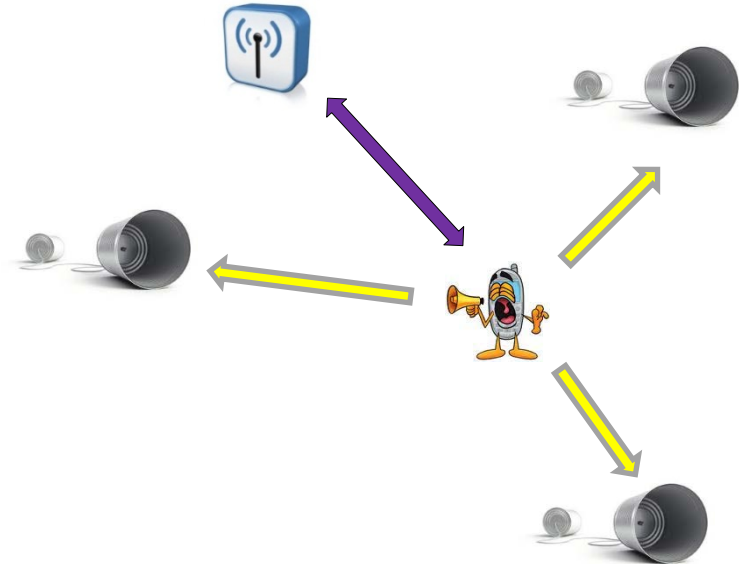 - Traffic overhearing
  - No feedback

Localisation systems taxonomy

- Network-based & Network assisted
  - Full information & computational power

- Terminal-based
  - Limited computation

- Passive
  - Third-party devices
  - Traffic overhearing
  - No feedback
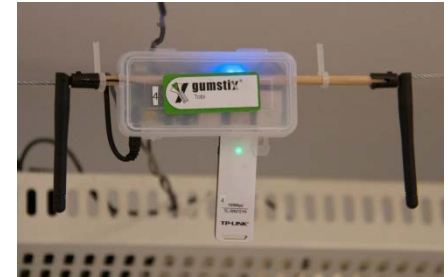
Passive system perspective

- Overview
  - Similar to network-based but more limited
- Advantages
  - Independent third party realisation
  - Computational power
  - Ease of deployment
- Disadvantages
  - Highly dependable on external information, incl. user traffic
  - Sensitive to user's location
  - More technically challenging

Passive system perspective

- RSS-based systems
  - Received Signal Strength (RSS) measurements
  - Vulnerable to power control & terminal location
  - High accuracy often depends on anchor density
- Time-based systems
  - TOA (Time Of Arrival)
    - Requires synchronisation with the terminal & anchors
  - TDOA (Time Difference Of Arrival)
    - Requires synchronisation only among anchors
  - Two-way TOA (RTT)
    - Delay sensitive to local signal processing
    - Does not need synchronisation but terminal participation

Passive system perspective

- WiFi/BT (indoor) test-bed
  - Sensor nodes with WiFi & BT interface
  - RSS-based

- Pros:
  - User data easily identifiable
  - Non-complex traffic processing
  - Cheap hardware

- Cons:
  - Dependent on user activity
  - Large RSS fluctuations -> many anchors
 - May require knowledge on Ptx

Data base & processing

Gateway

Sensor group

Passive system perspective

- GSM test-bed
  - Networked-USRP nodes with GPS rx
  - SDR-based signal processing
  - TDOA-based
- Pros:
  - No knowledge on Ptx (TDOA)
  - Less vulnerable than RSS (time)
  - Less anchors needed
- Cons:
  - Dependent on user activity
  - User data not easily identifiable
  - Requires synchronisation (TDOA)
  - Complex traffic processing (specialized sw)
  - Costly hardware

RF front end → ADC → GNU Radio + SW

GNU Radio + SW → DAC → RF front end
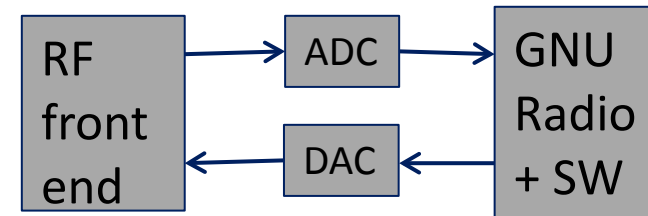
Data base & processing

Sensor group

Passive system perspective

- **User identification**
  - Three IDs: IMEI, IMSI, TMSI
  - Only few messages carry an ID
    - -> single messages, if missed no ID recovery
  - IMSI non-trivial relation to TMSI
    - -> TMSI may be challenging to use
  - User encryption
    - -> decreases the number of useful messages
- **User activity**
  - Localisation depends on location updates or user activity (service requests), e.g., paging, connection

Passive system perspective

- ## Synchronisation between devices

  - Needed for TDOA

  - Sets effective lower bound on the localisation error

  - Best is GPS-based

    - Long-term offset compensation

  - Remaining short term clock offset

    - In the order of 200ns -> 60m
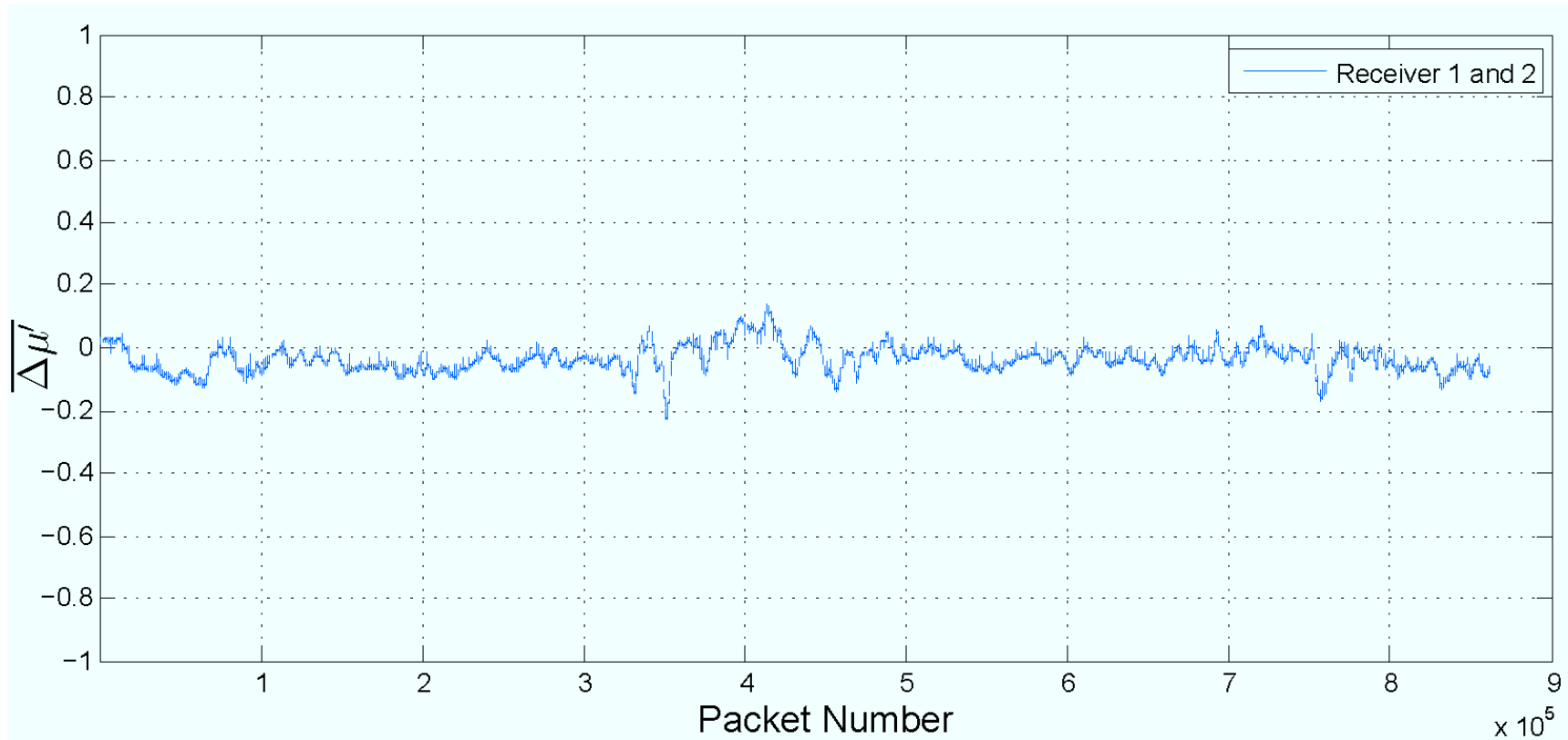
    - Can be compensated but increases complexity

GPS

Data base & processing

Sensor group

Passive system perspective

Passive system perspective

- Synchronisation with data traffic
  - User identification needs message recovery
  - Message recovery needs synchronisation with user
- Challenges
  - Uplink is not meant for synchronisation
    - Only for fine tuning
    - Shorter training sequence
  - Synchronisation depends on user position
- Method
  - Use training sequence in uplink to recover synchronisation
  - Reaches 80-90% recovery rate
    - if synchronisation is lost needs to recover -> lost messages

Passive system perspective

- ## Complex traffic processing
  - – For data synchronisation
  - – For message parsing
  - – For message timing

- ## Message timing
  - – Timestamp accuracy depends on signal bandwidth
    - Advanced signal processing is needed for timing
    - Expected accuracy 40ns -> 12m (ideal propagation)
  - – Oversampling may help
    - ADC rate not supported by the software processing
    - Proper sample selection is needed

RF front end → ADC → GNU Radio + SW → DAC → RF front end
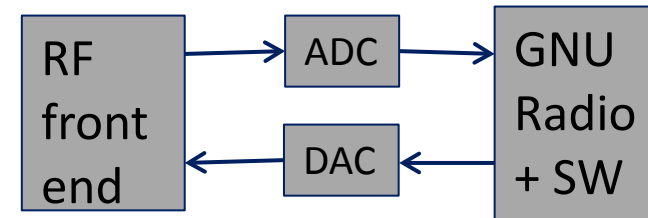
Passive system perspective

- Costly hardware
  - USRP about $1500
  - Processing power
    - Embedded devices not enough power
    - Networked devices need machine
  - Wide-band processing
    - Standard USRP up to 20MHz
    - Advanced options much more expensive
  - Pros: less anchors needed

Data base & processing

Sensor group

Active system perspective

- Network-based & terminal-assisted
  - Inherent issues based on parameter (RSS or time)
  - TDOA challenges depend on signal bandwidth
- Pros:
  - User identification inherently available
  - No user synchronisation issues
  - Anchors synchronisation potentially easier
  - Traffic processing already included
- Cons:
  - Dependent on user activity
  - Difficult to step-in (provider owned for cellular)

Active system perspective

- Terminal-based
  - Inherent issues based on parameter (RSS or time)
  - TDOA challenges depend on signal bandwidth
- Pros:
  - User identification inherently available
  - Non-dependent on user activity
  - No user synchronisation issues
  - Traffic processing already included
- Cons:
  - Requires deployment on the terminal
  - Anchors synchronisation is necessary
  - Terminal may lack computational power

Discussion

Discussion

- Do you have experience with localisation?
- Which system type (active, passive) was deployed?
- Which parameter (RSS, time) was used?
- What is your impression/lessons learnt?
- Which system you would like to use?
- Where do the bigger challenges lay?