Linux-based Measuring Platform for Time-Based Location Observables in IEEE 802.11 Networks

I. Martin-Escalona, F. Barcelo-Arroyo, E. Zola

(SPEAKER: Enrica Zola)

Joint ERCIM eMobility and MobiSense Workshop, June 2013
1. Indoor positioning
   • Introduction
   • Location platform approaches
2. Goals and requirements
3. The SoftMAC approach in Linux
4. The measuring system
5. Performance assessment
   • Scenario used for collecting data
   • Results
• Several technologies are currently available for indoor positioning in IEEE 802.11
  ✓ Proximity-based
  ✓ Direction of arrival
  ✓ Fingerprinting
  ✓ Range-based

• Time-of-flight (ToF) techniques
  ✓ Time and time-differences can be used as observables
  ✓ Good trade-off between accuracy and complexity
1. Location platform approaches

- Analytical and simulation assessment needs to be verified with real test beds
- Implementation of location techniques
  - Custom hardware
    - Best results in terms of QoS (e.g. 1m of accuracy)
    - Tight design: difficult to upgrade/enhance
  - Custom software
    - More flexible design at the cost of higher error
    - Is the QoS enough for most of the LBS?
Providing a location platform aimed at:

- Providing the best performance
- Supporting legacy hardware
- Portability of the platform to several architectures
- Supporting time-based location techniques
  - 2-way TOA (RTT)
  - Passive TDOA (TDOA)
- Flexibility for adding new features and techniques
3. The SoftMAC approach in Linux

- Measurements taken in the MAC layer of the Linux IEEE 802.11 stack
  - Observing in the WNIC driver
    - Changes in the WNIC driver for observing the ToF
    - Specific changes for each driver
    - Best results
  - The SoftMAC approach (Linux / FreeBSD)
    - Common to all drivers
    - More software layers are crossed
3. The SoftMAC approach in Linux

**SoftMac in Linux: mac802.11 framework**

- **mac80211**: Common MAC operations
- **SoftMAC drivers**: Specific MAC operations
- **cfg80211**: WNIC configuration (succeeds *wireless extensions*)
4. The measuring system

- pos80211
- TCP/IP stack
- Patches
- SoftMAC
- SoftMAC Drivers
- Firmwares
- Device hardware

- System calls
- sockets
- pos80211_ops
- softmac_ops

- Round trip time
- Passive TDOA

Files: main.c, tx.c, rx.c
4. The measuring system

The round trip time plugin

- **Begin**
  - Management frame?
    - `ieee80211_is_mgmt(...)`
  - Yes
    - Timestamping the frame
      - `struct timespec ts; getnstimeofday(&ts); last_tx_time = TIMESPEC_TO_NS(ts); last_tx_clock = get_cycles();`
  - No
    - Transmission event
    - IEEE 802.11 device
    - Access point
    - Data
    - RTT
    - Acknowledgement

- **Begin**
  - Reception event
  - ACK frame addressed to the node?
    - `ieee80211_is_ack(...)`
  - Yes
    - Associated transmission?
      - `last_tx_time < last_rx_time`
      - Yes
        - Computing observable (RTT)
          - `newRTT = (TYPE_OF_POSITIONING_DATA) (last_rx_time - last_tx_time);`
          - `newRTT = (TYPE_OF_POSITIONING_DATA) (last_rx_clock - last_tx_clock);`
        - Storing observable
          - `RTT_CONTAINER_ADD_DATA(rtt_queue, (voidp) newRTT);`
        - Removing the previous associated transmission
          - `last_tx_time = last_tx_clock = MAXIMUM_INTEGER`
  - No

4.1. Linux-based Measuring Platform for Time-Based Location Observables in IEEE 802.11 Networks

Second Joint ERCIM eMobility and MobiSense Workshop, April 2013
4. The measuring system

The passive TDOA plugin

- **Begin**
- **Reception event**
  - **To distribution system?**
    - Yes
    - **Is the frame sent by the active node?**
      - Yes
      - **Timestamping the frame**
        - `struct timespec ts;
        - getnstimeofday(&ts);
        - last_tx_time = TIMESPEC_TO_NS(ts);
        - last_tx_clock = get_cycles();`
      - **Change the plugin status**
        - `tx_status = AWAITING_ACK`
    - No
    - No
      - **Change the plugin status**
        - `tx_status = AWAITING_ACK`
  - No
    - **Change the plugin status**
      - `tx_status = AWAITING_DATA`
- **End**

**Network data flow**

- **Active node**
- **AP**
- **Passive node**
- **RTT**
- **Tx**
- **Rx**
- **t**
- **TDOA**
First results: focused on probing the concept

Assessed scenario:
- Concrete walls
- LOS between nodes
- Dedicated network
- Passive and active STAs separated 0.5 m
- Limited interference
- Static conditions

Experiment:
- 10 x 10.000 pings from the active STA to the AP
- No ping overlapping
The round trip time plugin

a) Raw

b) With Gaussian FILTER
The passive TDOA plugin

a) Raw

b) With Gaussian FILTER
Further questions?