Generation of Realistic 802.11 Interferences in the Omnet++ INET Framework Based on Real Traffic Measurements

Juan-Carlos Maureira[1] and Diego Dujovne[2] and Olivier Dalle[1]

[1] INRIA, I3S, CNRS, Univ. Nice Sophia, France.
{jcmaurei|odalle}@sophia.inria.fr

[2] INRIA Sophia Antipolis Méditerrannée
dujovne@sophia.inria.fr

March, 6th 2009 / OMNeT++ 2009 Workshop (SIMUTools 2009)

Agenda

Motivation and Goals

- **Motivation**: Provide an OMNeT++ interference model based on real measurements.
- **Goal**: A method to include interference scenarios into OMNeT++ simulations in a non-intrusive way.

Motivation and Goals

- **Motivation**: Provide an OMNeT++ interference model based on real measurements.
- **Goal**: A method to include interference scenarios into OMNeT++ simulations in a non-intrusive way.

Sampling

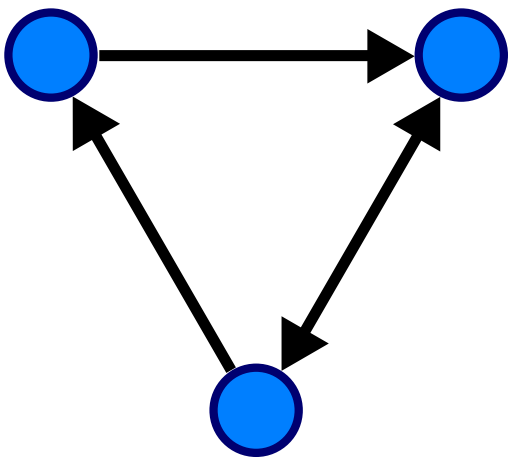
Figure: The Probe

- Based on a set of *Probes* to capture traffic.
- Captured traffic trace content:
  - Source Address (MAC)
  - Reception Timestamp
  - Received Signal Power
  - Transmission Datarate
  - Packet Size

Distance Estimation

Probe - Source distance estimation based on Reception Signal Power sampling and calculation by using Free-Space Pathloss Propagation Model.

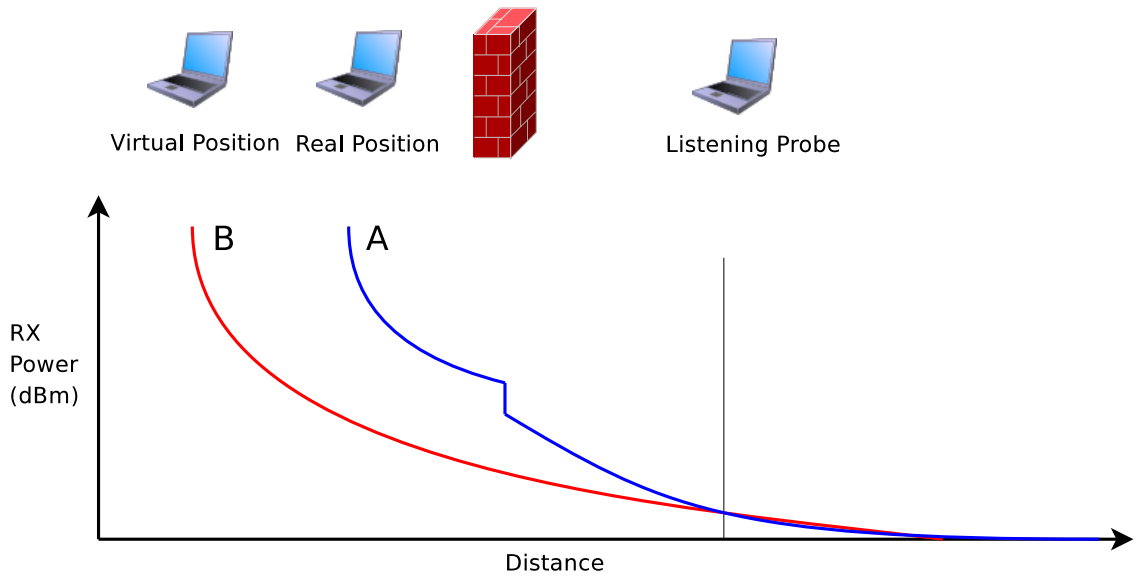
Localization of the Sources



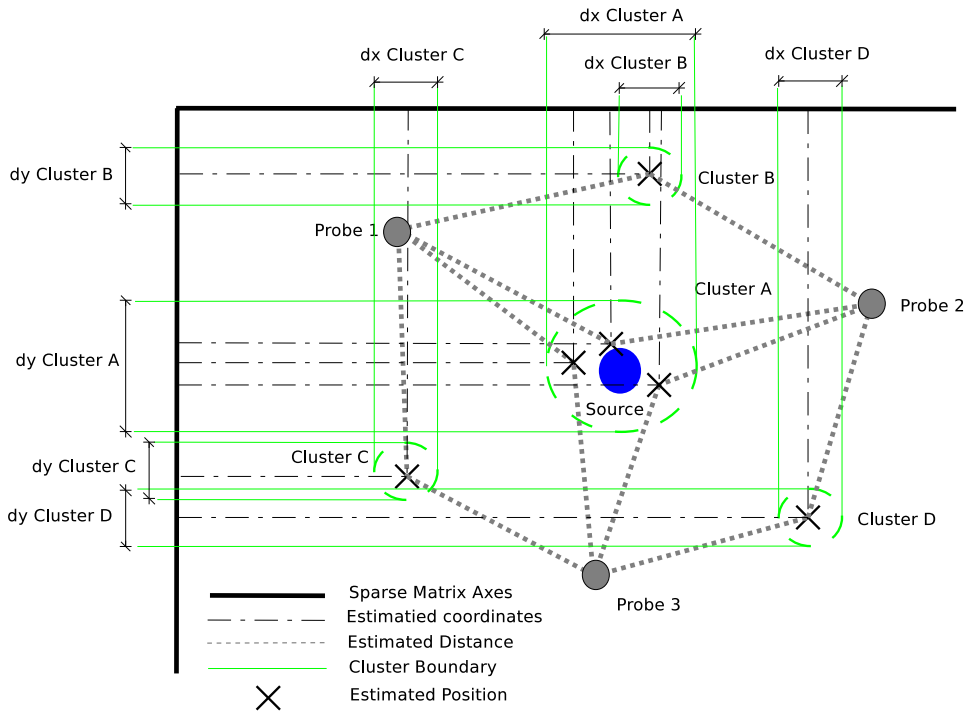
- Based on:
  - Triangulation by using *Probes* positions and the Distance between the *Detected Sources* from each *Probe*.
  - Sparse-Matrix Clusterization Analysis.

Virtual Position

Position required to measure the same signal strength without obstacles in the line-of-sight.

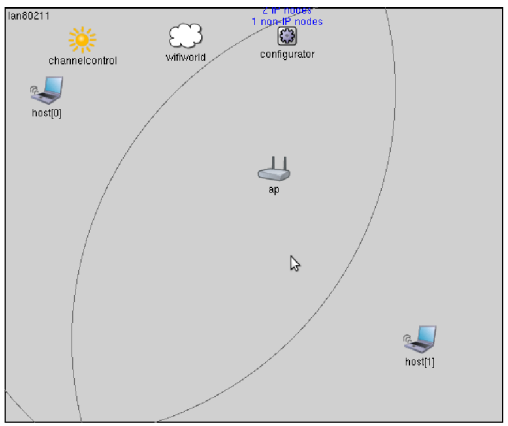


Sparse-Matrix Cluster Analysis



The estimations of the Detected Sources Position's are clusterized according how close they are (euclidean distance).

Integration into the Simulation



- Traffic Generation:
  - From recorded traces.
  - Injected from the estimated source's positions.
- INET Framework:
  - Traffic Generation.
  - Shadow Sources (light or complete)
  - Channel Controller Module.
  - Wifi World Compound Module.

Method Validation

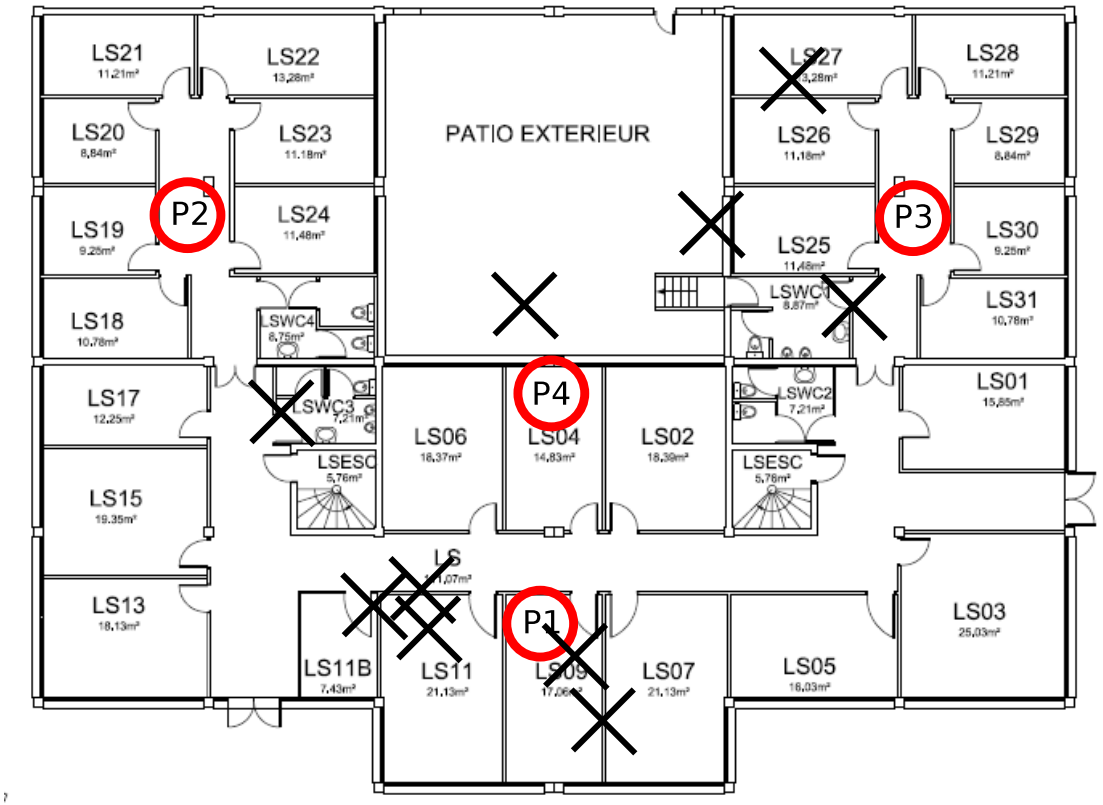


Figure: Experimental Scenario

Method Validation

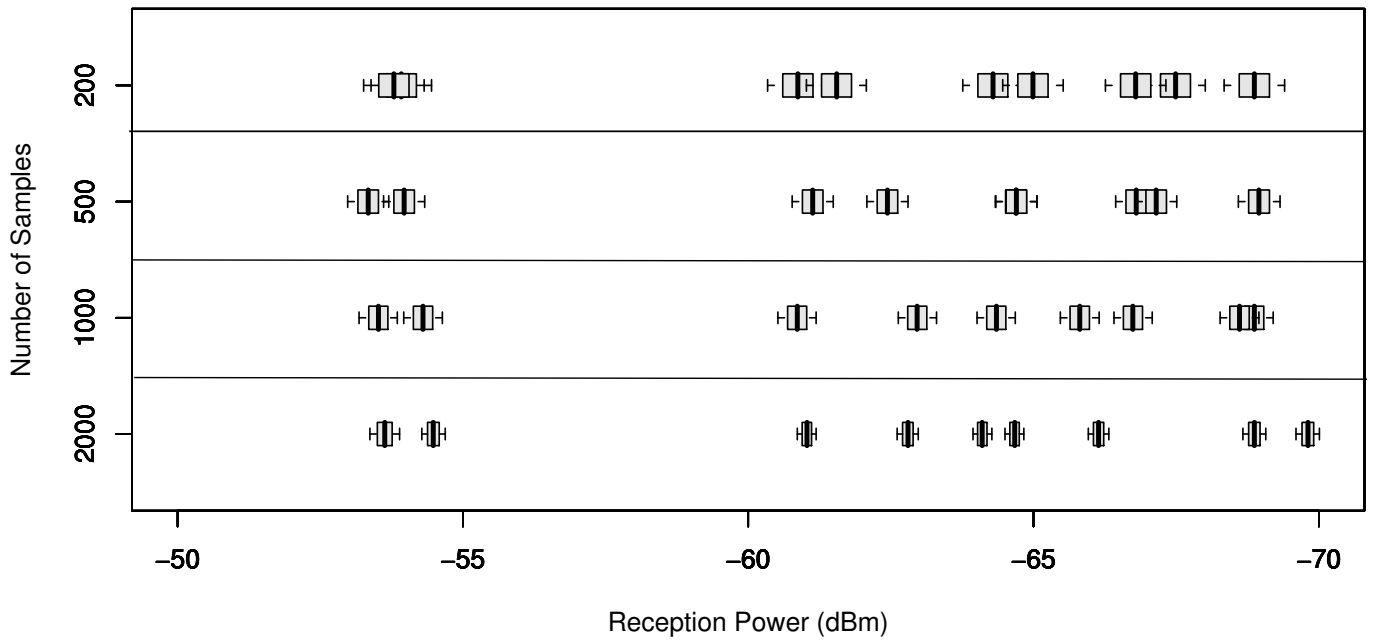


Figure: Multiple Range Test for Reception Power Estimation

Method Validation

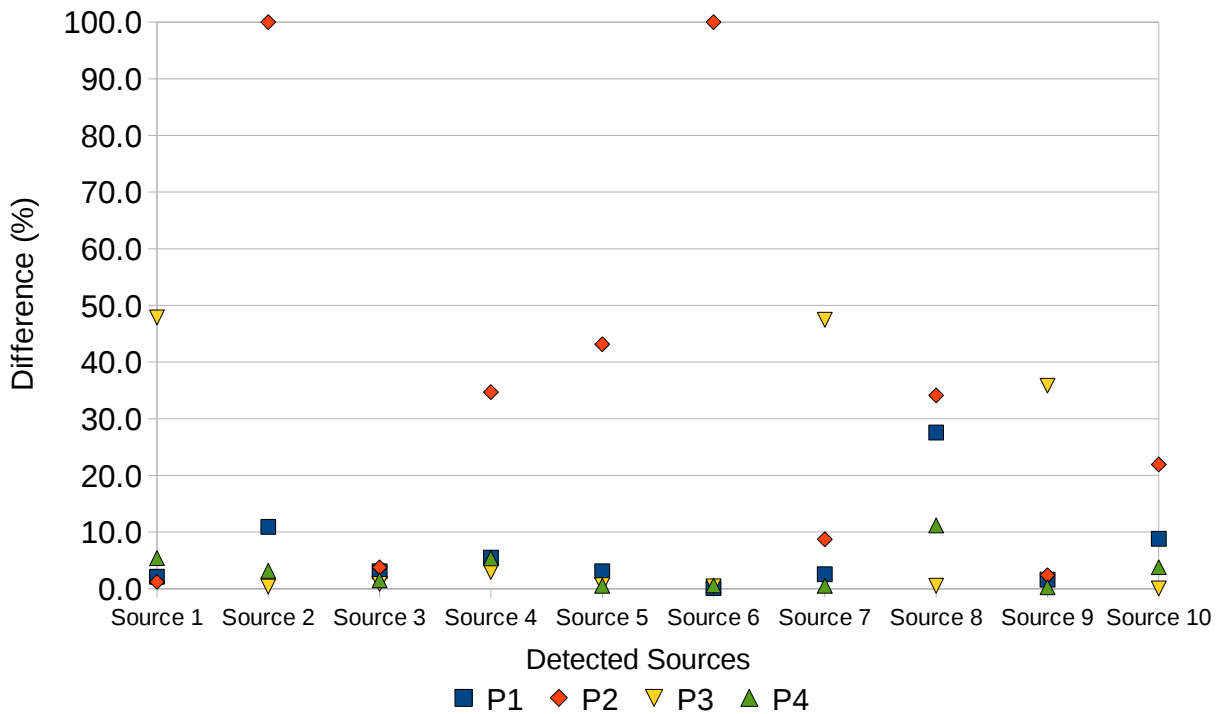


Figure: Differences Between Measured and Simulated Values

- 62.5% under 10% error.
- 13.5% between 10% and 20% error.
- 5% was 100% wrong.

Simulation Testbed

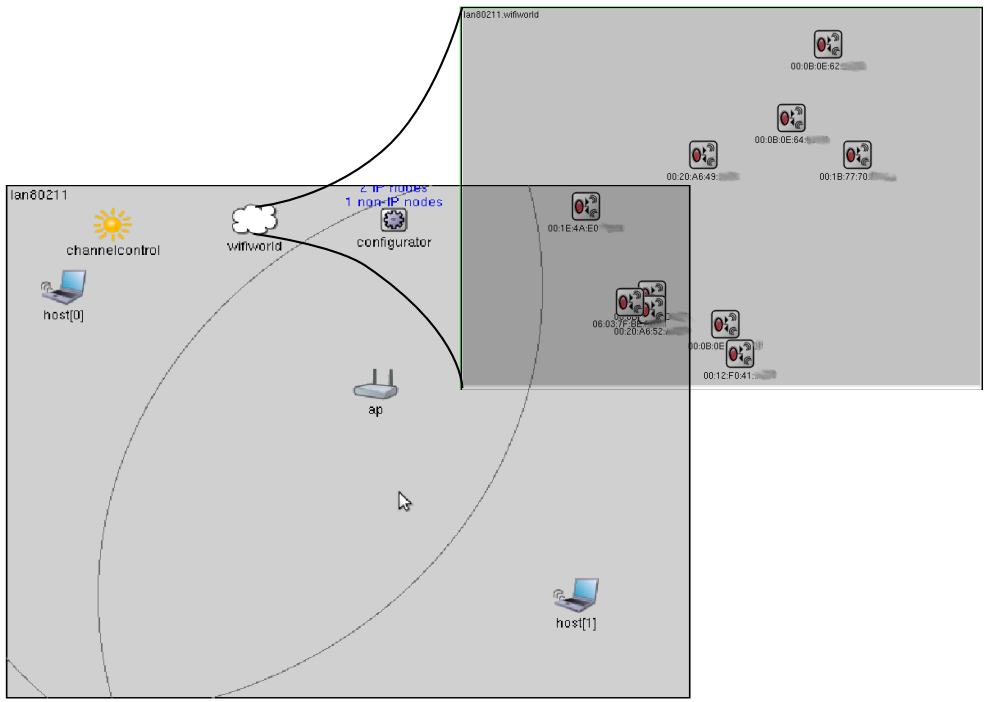


Figure: Simulation Scenario: The Hidden Station Problem

Simulation Results

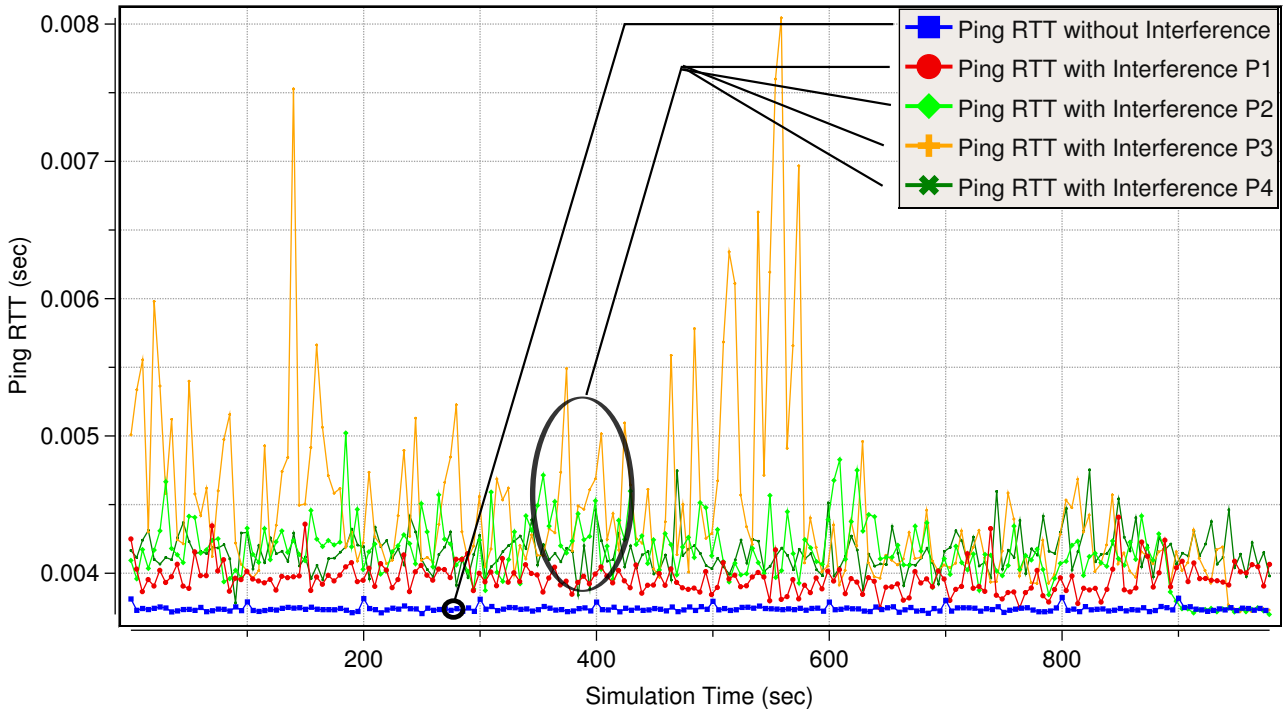


Figure: Ping Round Trip Time contrast.

Simulation Results

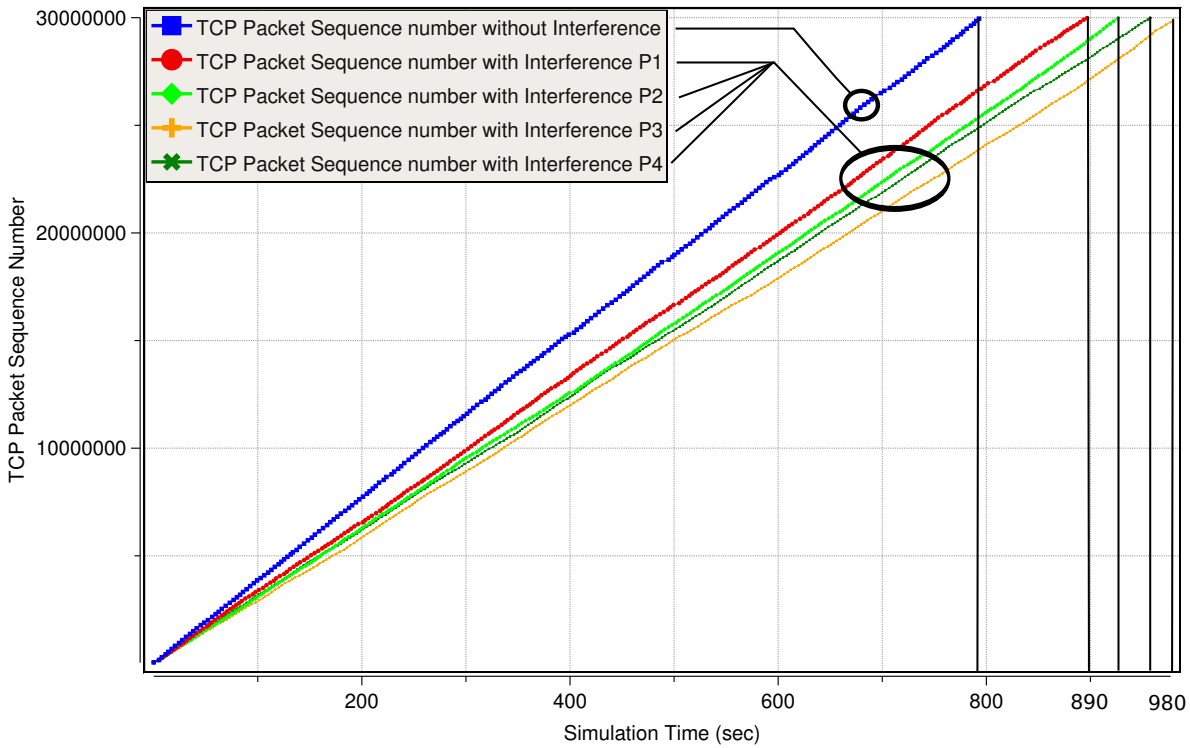


Figure: FTP TCP sequence number (downloading time) contrast.

Simulation Results

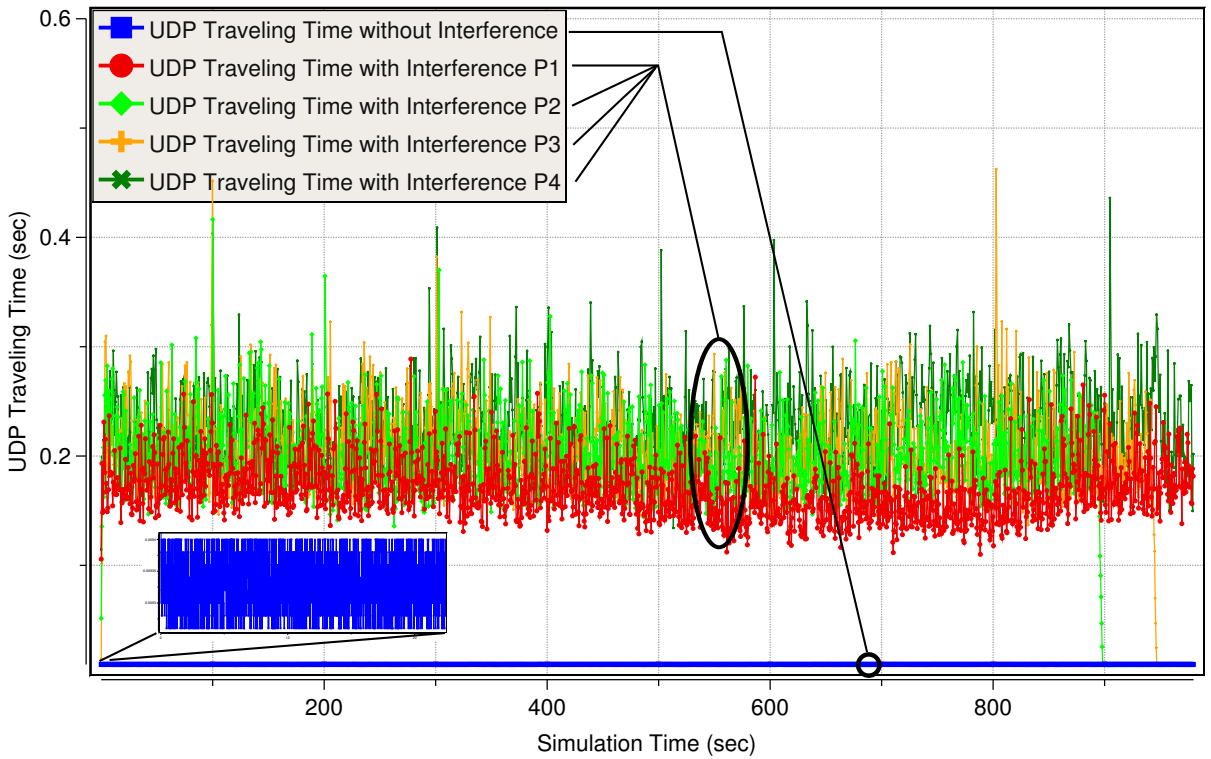


Figure: UDP Streaming delivery time contrast.

Summary

- We presented a method to introduce interference scenarios in studied systems based on observations.
  - Interfering traffic characterizations come from a real scenario (recorded scene).
- The method is easily repeatable with commodity hardware.
- Permits to evaluate two types of interaction between the Studied System and the interfering background traffic
  - How the system reacts in front of the interferiring traffic. (one way interaction).
  - How the interferiring traffic and the system affect each other. (two way interaction)
- Further Work
  - Improve precision of the location estimation.
  - Validate with more scenes and measure differences.