Ad-Hoc Security Support Using DVB - T

ADHOC-NOW, Sept. 20-21 2002, Fields Institute, Toronto

Munich University of Technology

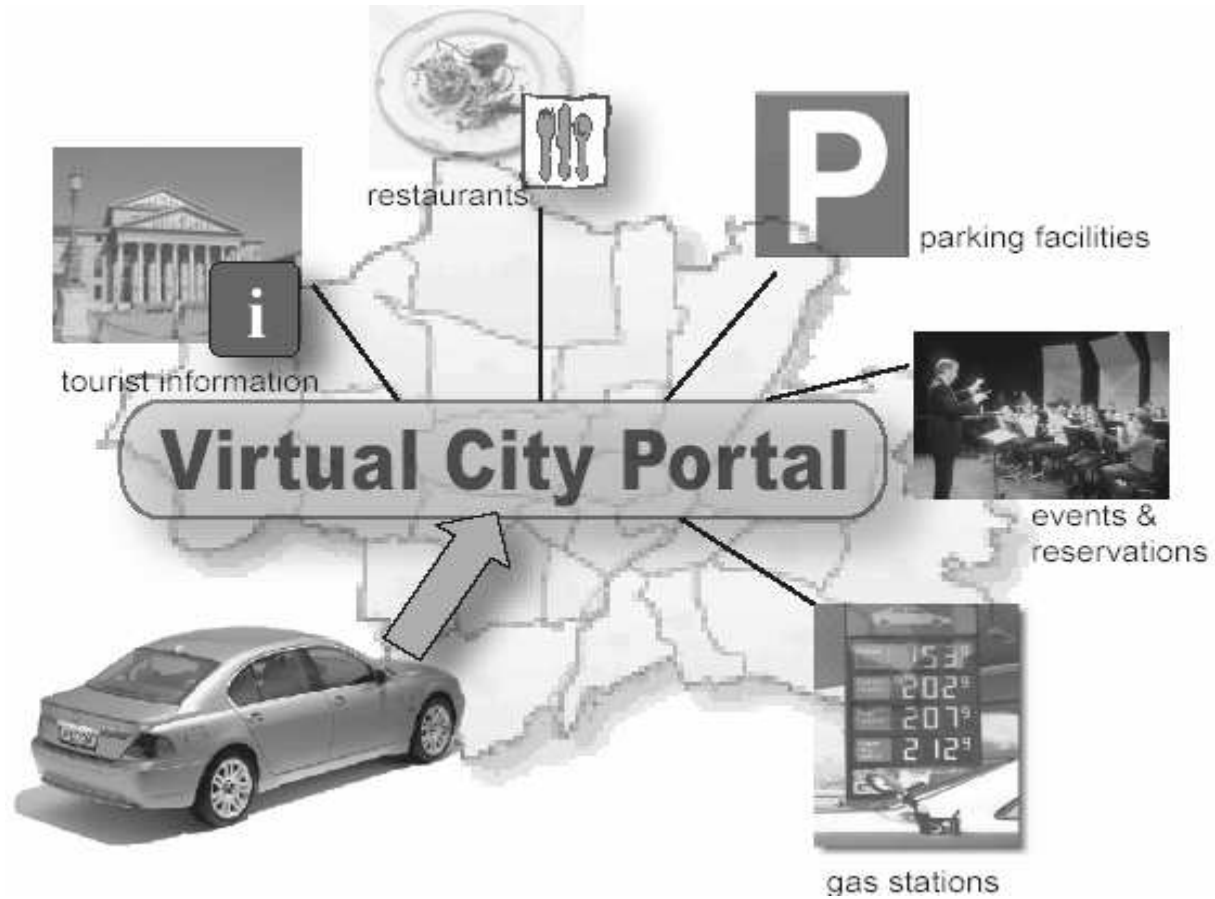
Institute of Communication Networks

Christian Schwingenschlögl

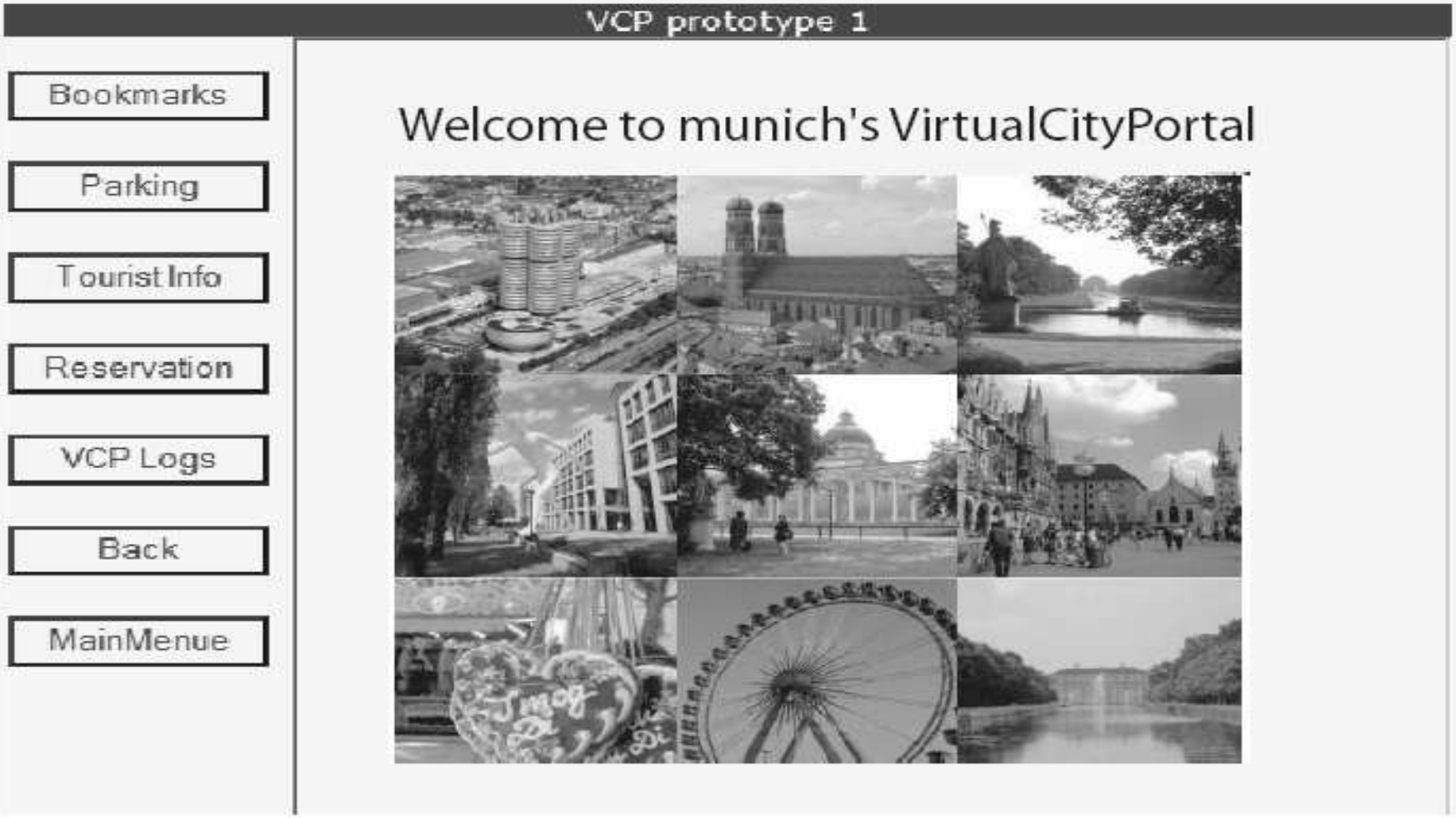
Outline

- Introduction & Motivation:
  The Virtual City Portal
  - Lab Testbed
  - Mobile Testbed
- DVB-T Broadcasts for Security Support
  - Basic Idea
  - Optimizations
- Simulation Tool & First Results
- Outlook

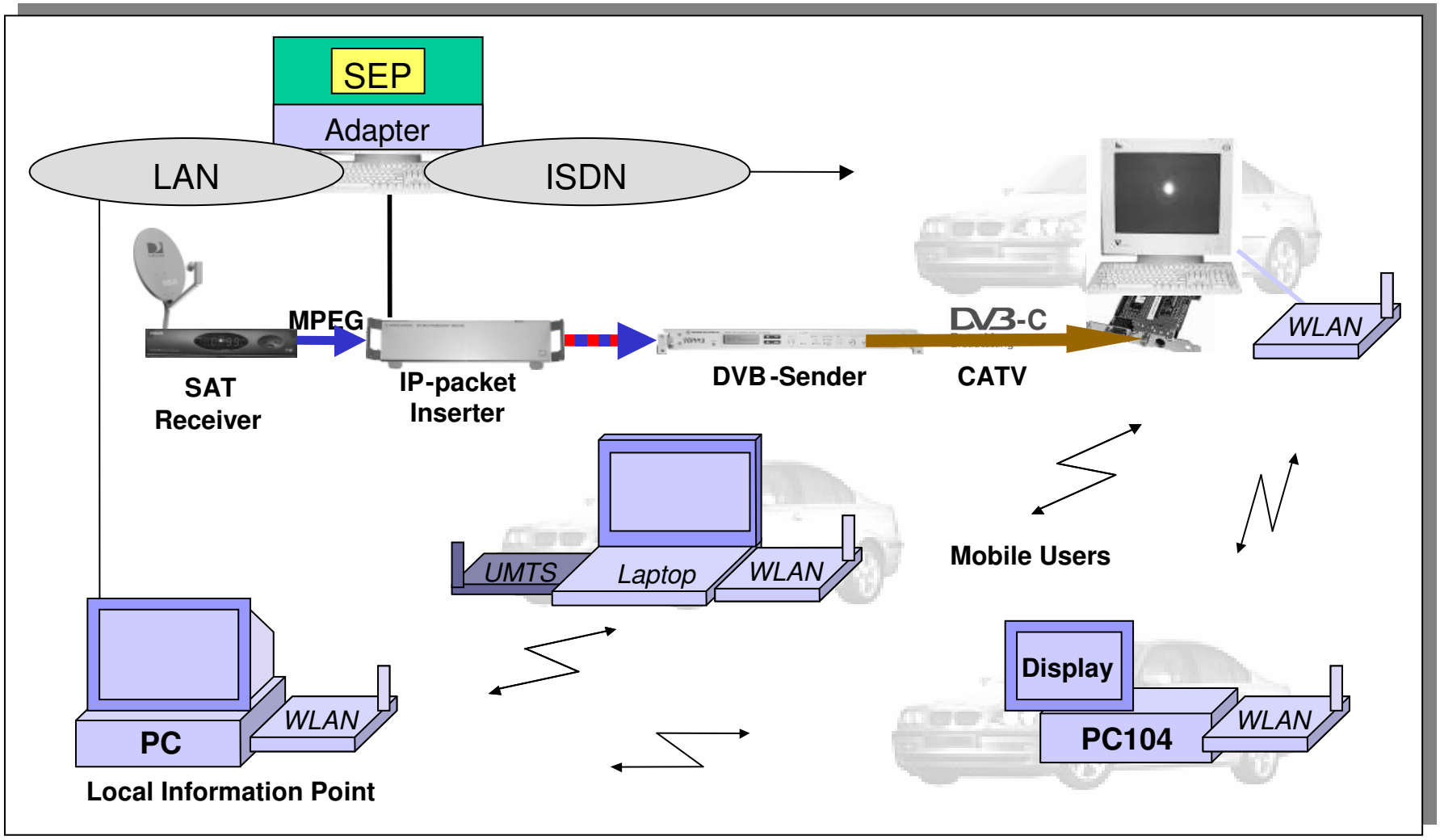
The Virtual City Portal



VCP Screenshot



Lab Testbed


SEP
Adapter
LAN
ISDN
MPEG
SAT
Receiver
IP-packet
Inserter
DVB-Sender
DVB-C
CATV
WLAN
UMTS
Laptop
WLAN
Mobile Users
PC
WLAN
Local Information Point
Display
PC104
WLAN

Mobile Testbed

Broadcast AdHoc Security

- AdHoc Security:
  - Complicated, usually large communication overhead (distributed, no central entities)
  - Still very active research issue
- Basic Idea:
  - Use DVB-Broadcasts from Trusted Third Party
  - Cyclic rebroadcast of Public Keys
  - Optional: availability of a global clock (coordinated action like e.g. key refresh)

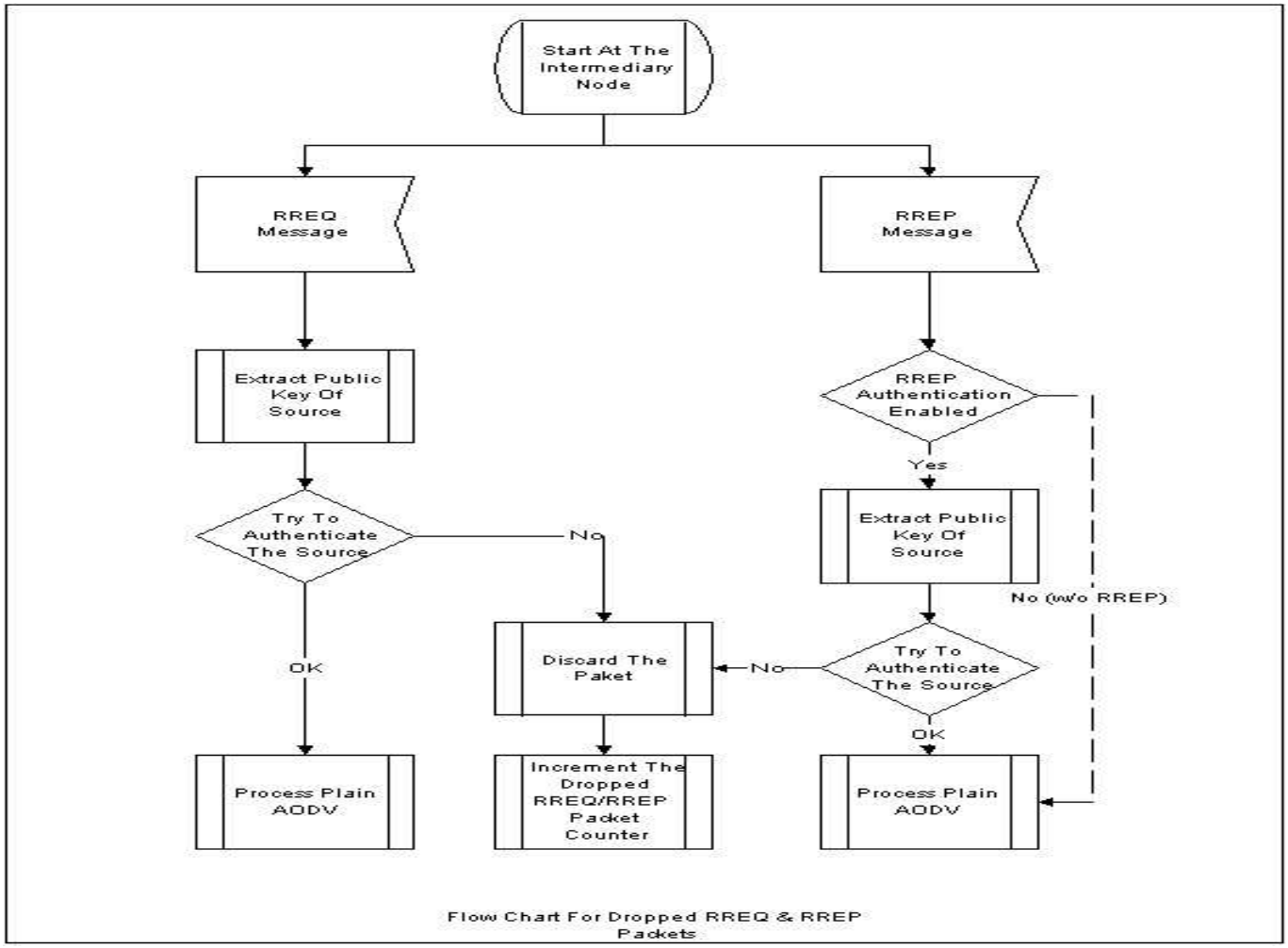
Broadcast AdHoc Security

- A Certification Authority (CA) is formed using a DVB Sender
- All mobile nodes keys are registered at the CA (DVB sender)
- The key of the CA is known to all the nodes
- Each node has a DVB receiver
- The DVB sender (CA) will broadcast the nodes' signed public keys periodically

AODV Augmentation:

- Only authenticated nodes used for routing

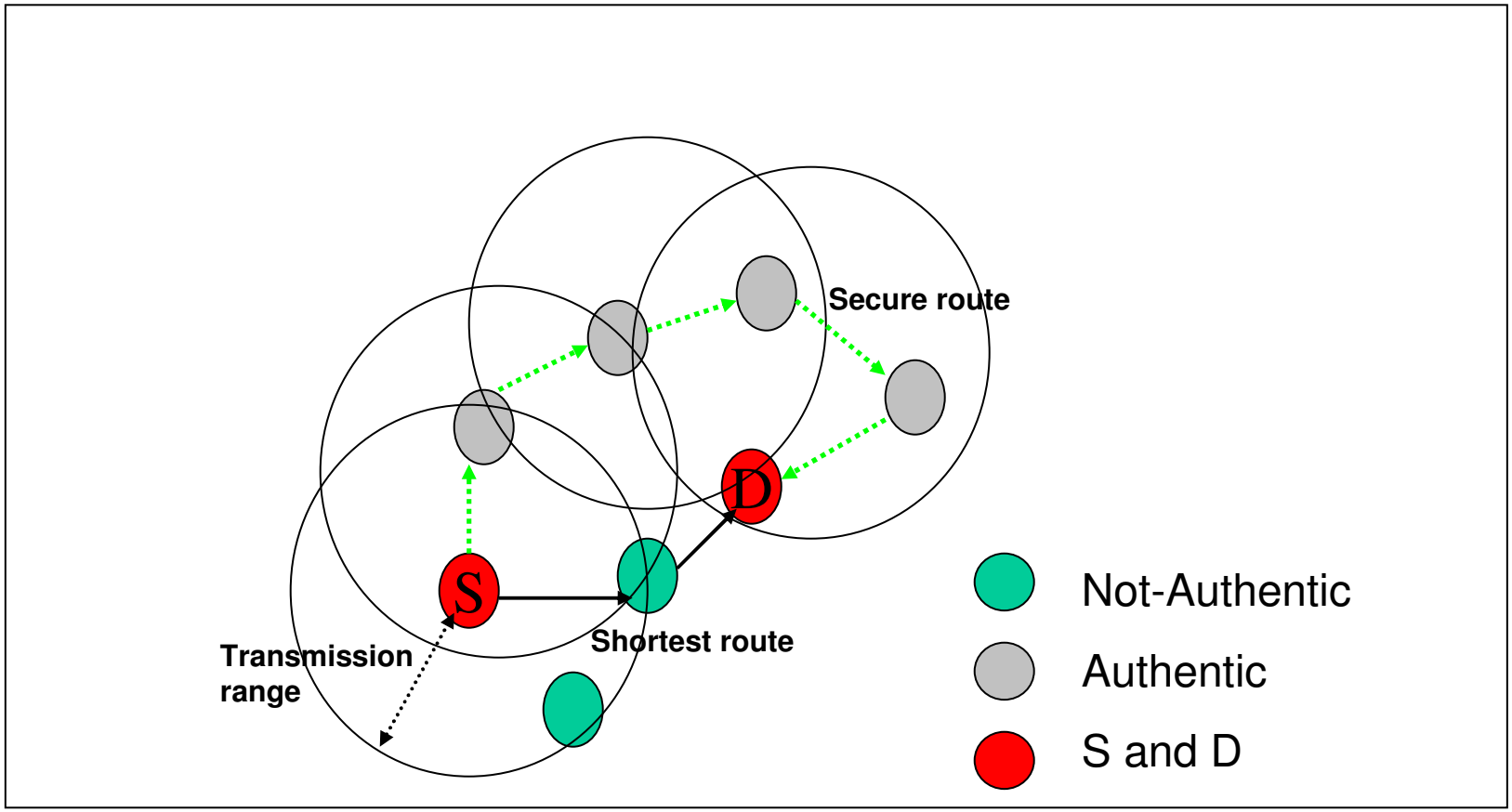
AODV Augmentation



Flow Chart For Dropped RREQ & RREP Packets

AODV Augmentation

Only “trusted” nodes are used for routing

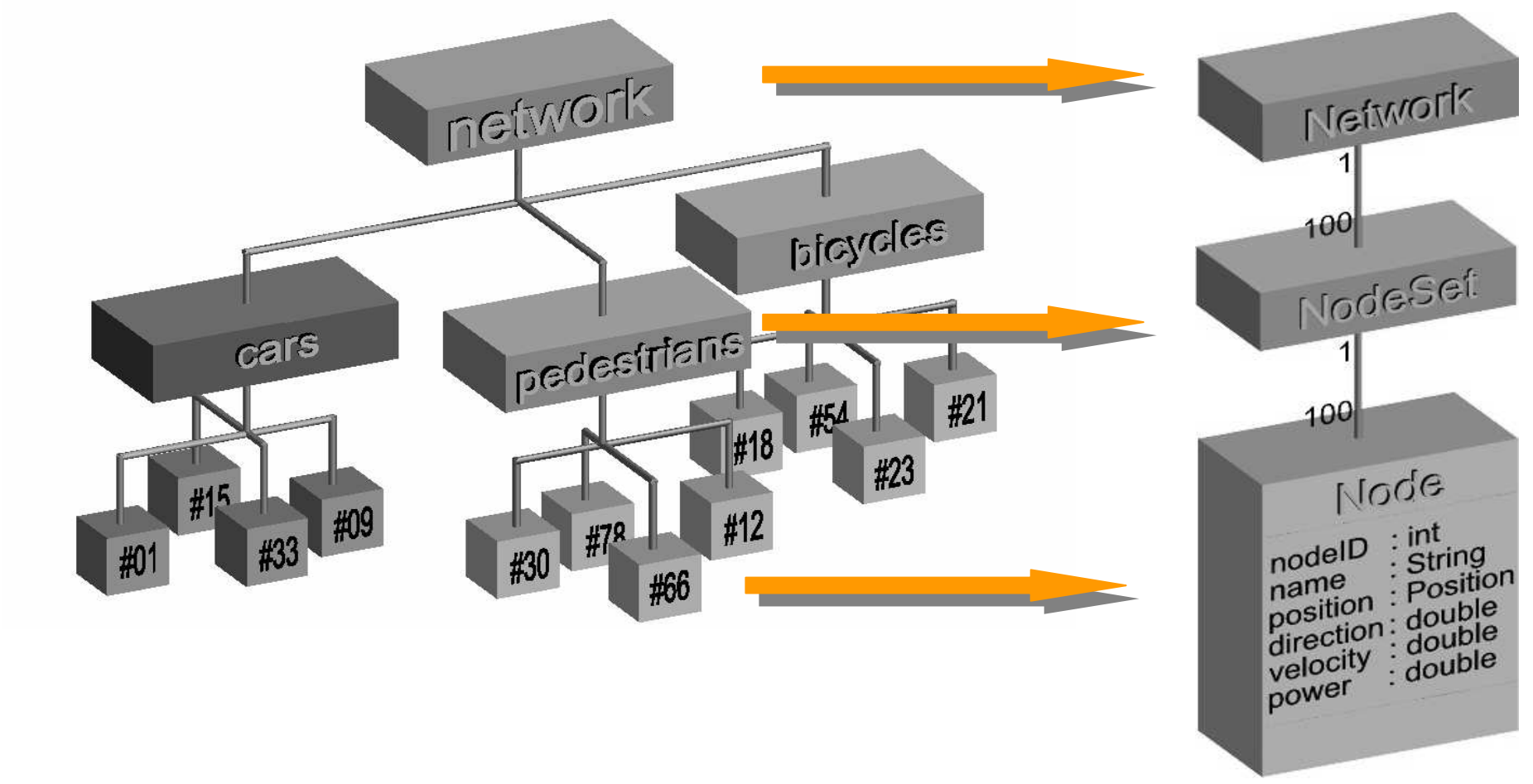


Problems, Optimizations

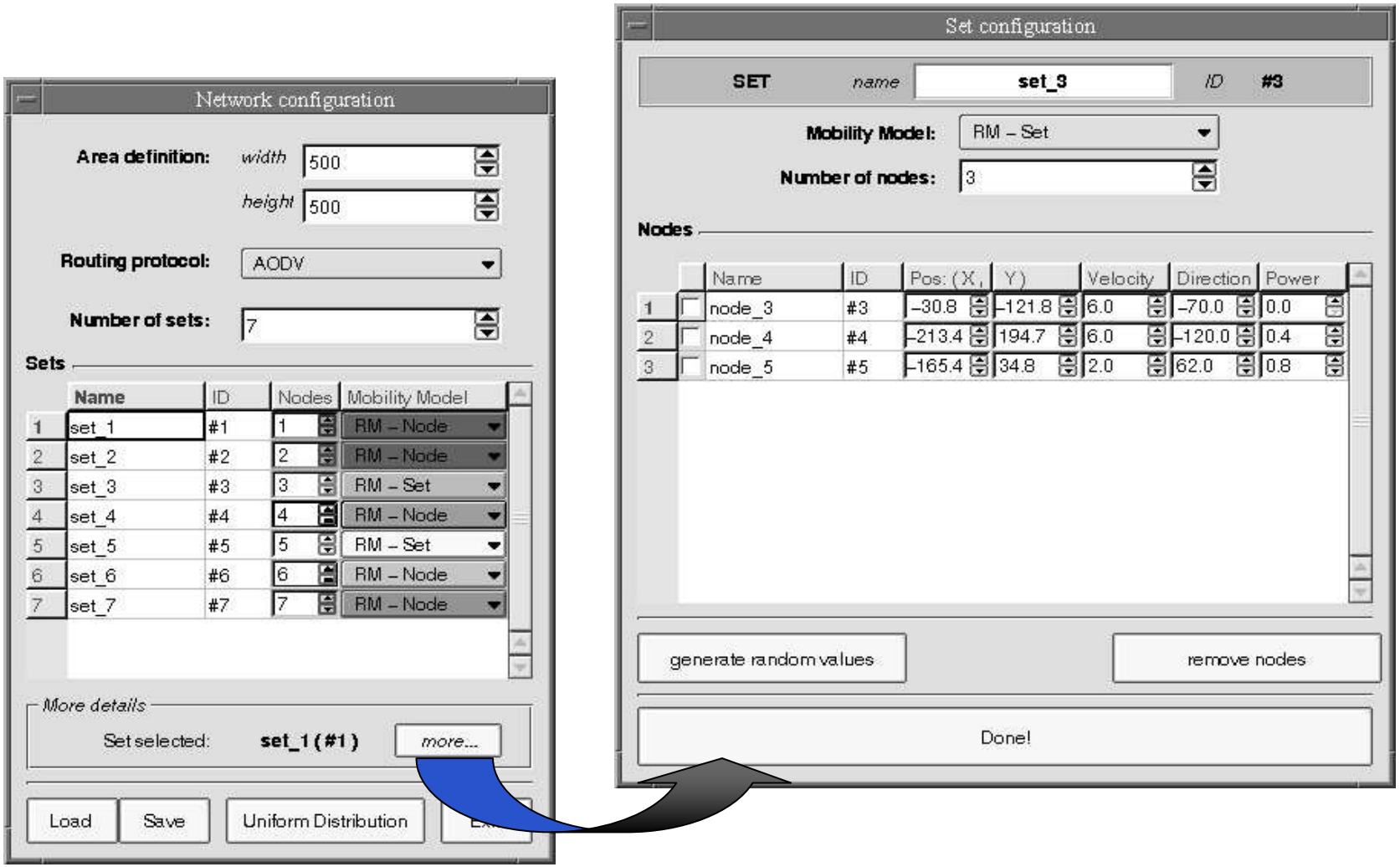
- Problems:
  - Longer delay for route establishment
  - Limited DVB-bandwidth (high number of nodes)

- Optimizations:
  - Registration of Vehicles within DVB range (Virtual City Portal, Local Information Points)
  - Web of Trust
  - GPS-Enhancements (Caching)

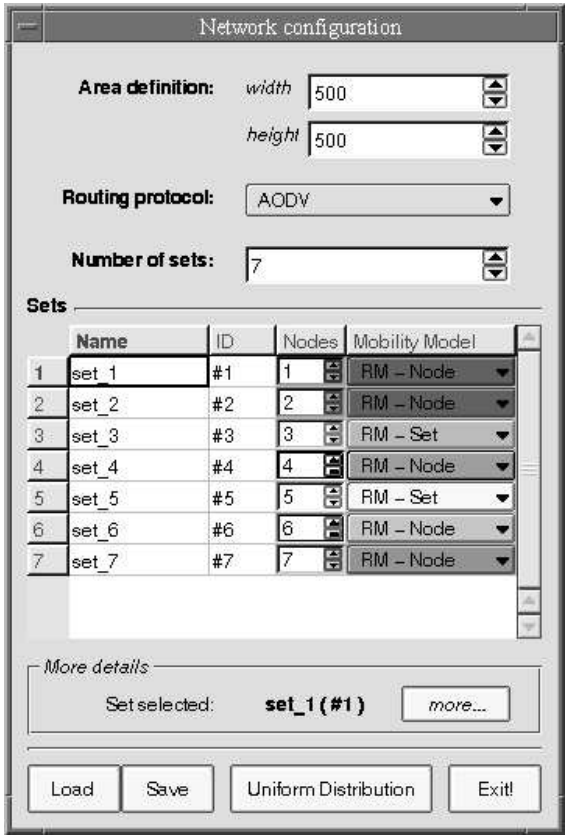
AdHoc Simulation Tool

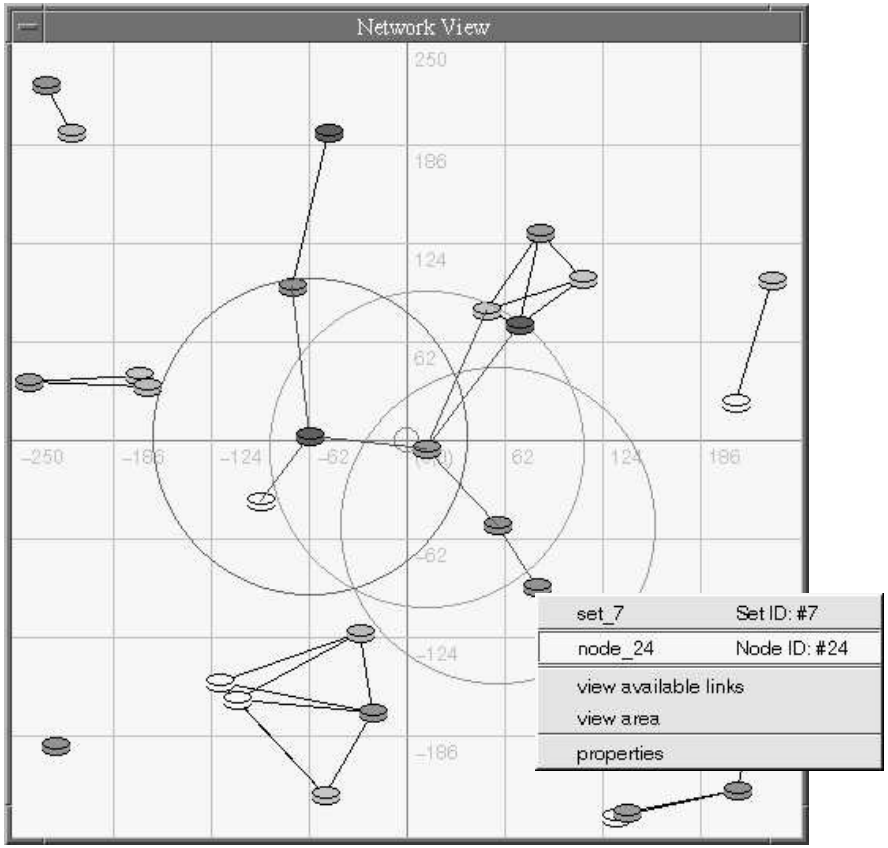


AdHoc Simulation Tool

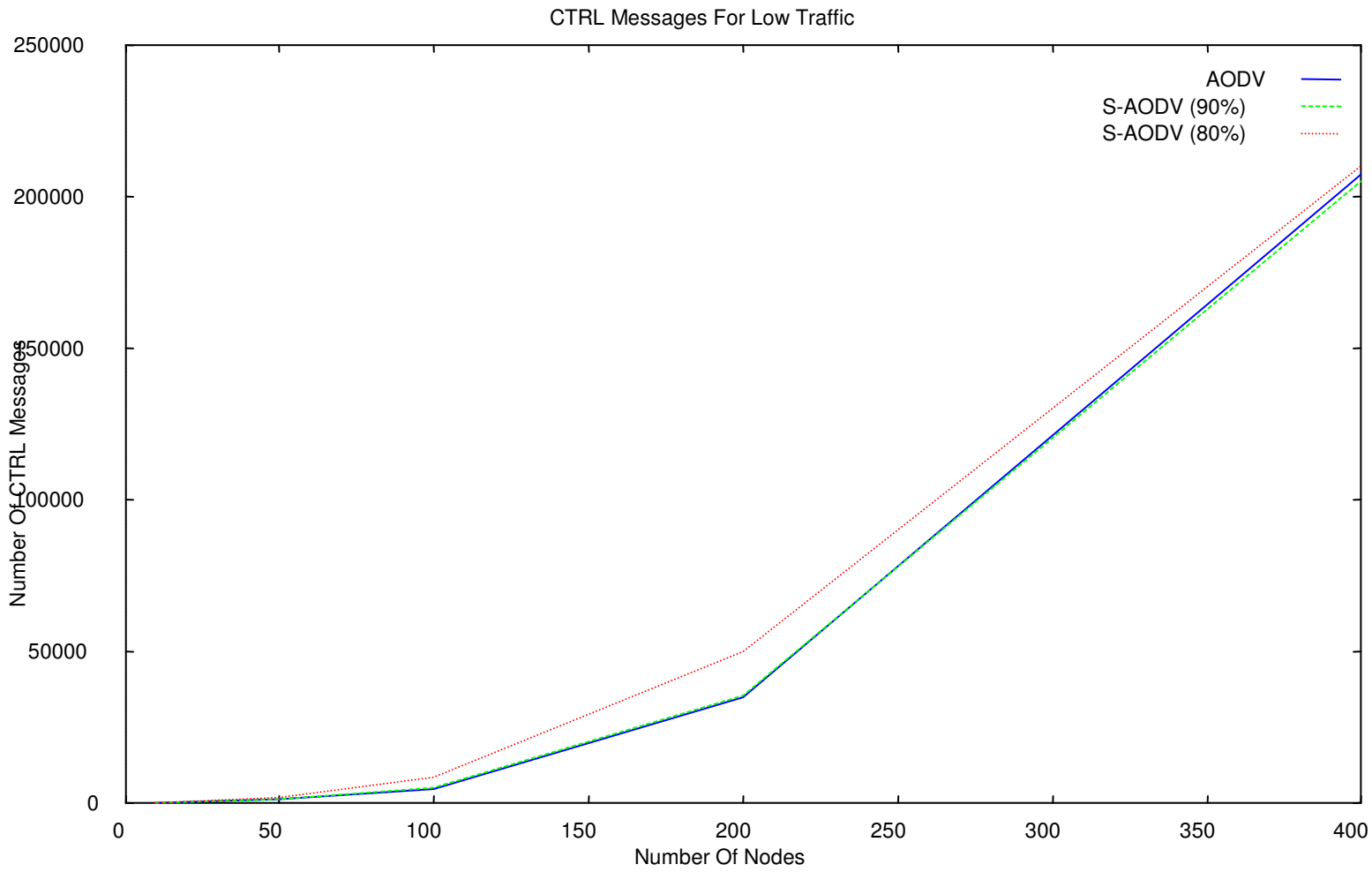


AdHoc Simulation Tool

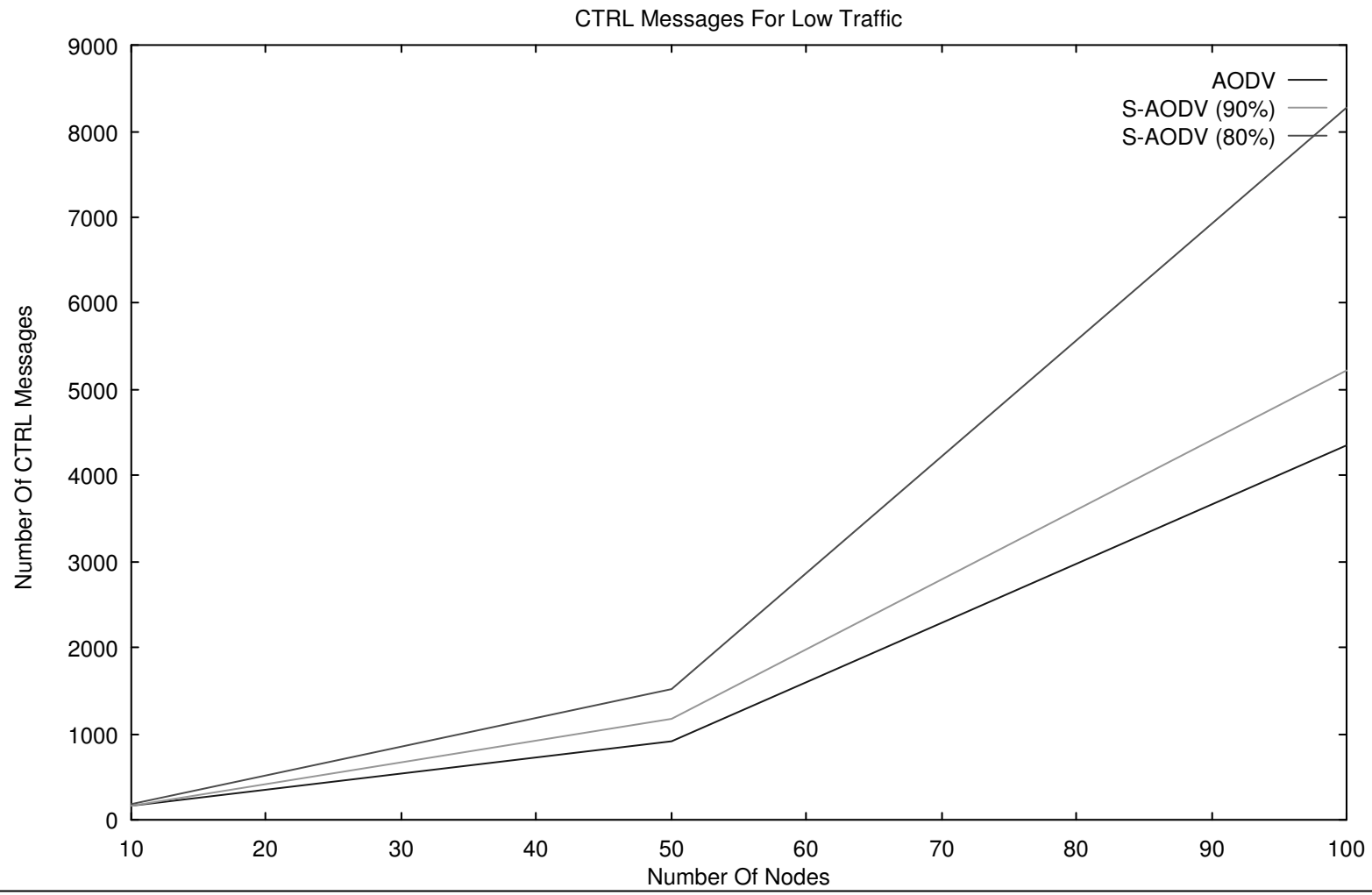




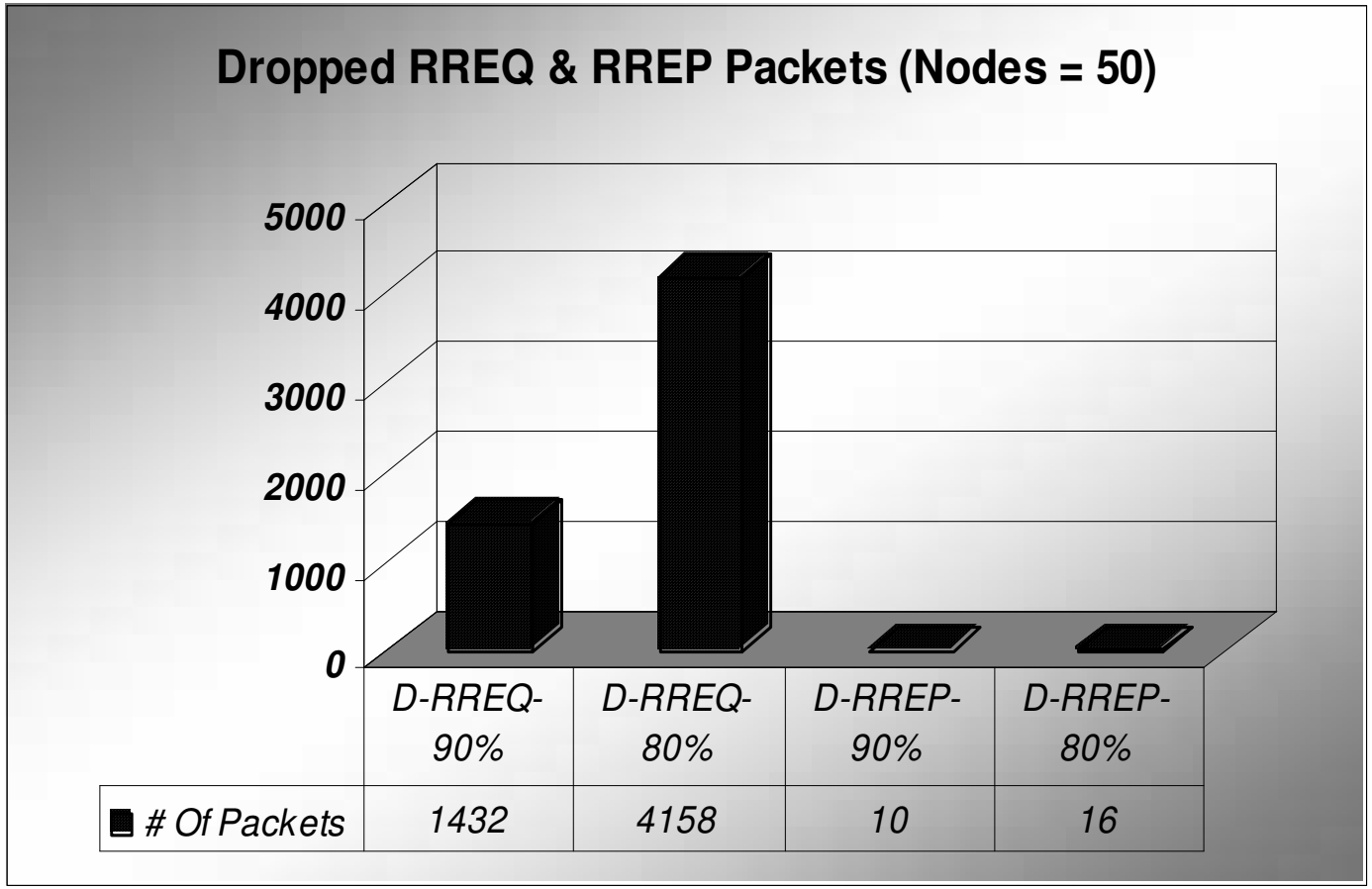
Preliminary Results



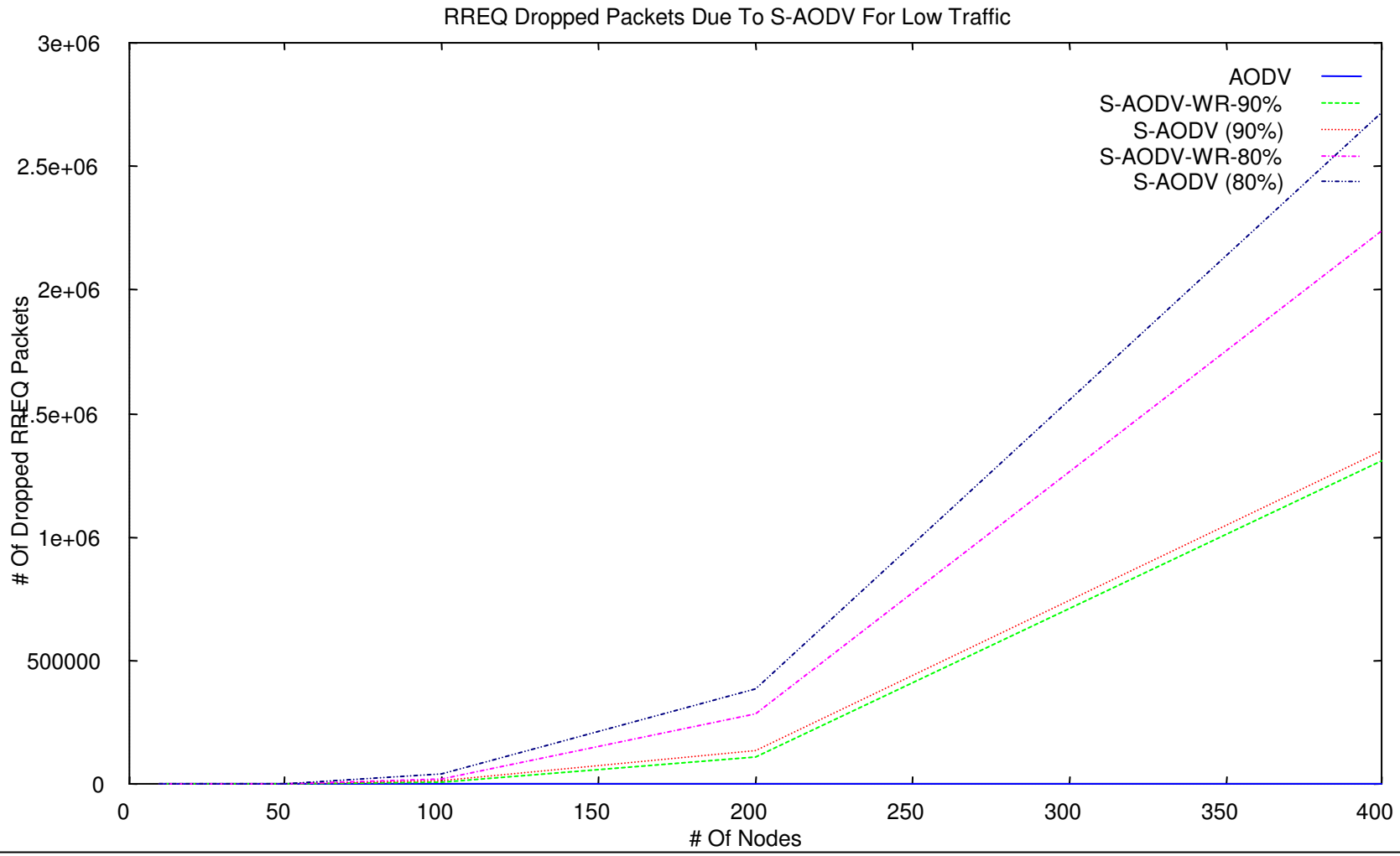
Preliminary Results



Preliminary Results



Preliminary Results



Outlook

Ongoing Work:

- More Studies on DVB-T Security Performance
  - Road-based Mobility Models & LAR enhancements
  - Security Optimizations
    (Key-Caching, Web of Trust, Position-Based)
  - Comparison of Simulation Results with GlomoSim
    (Effects of lower-layer abstraction)

- Conceptual Work on Secure Ad-Hoc Multihop Communication
  - Broadcast supported
  - Local Information Point supported
  - Cellular support

Thank you for your attention!