

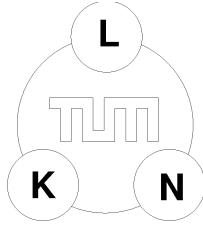
Ad-Hoc Security Support Using DVB - T

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

Munich University of Technology
Institute of Communication Networks

Christian Schwingenschlögl

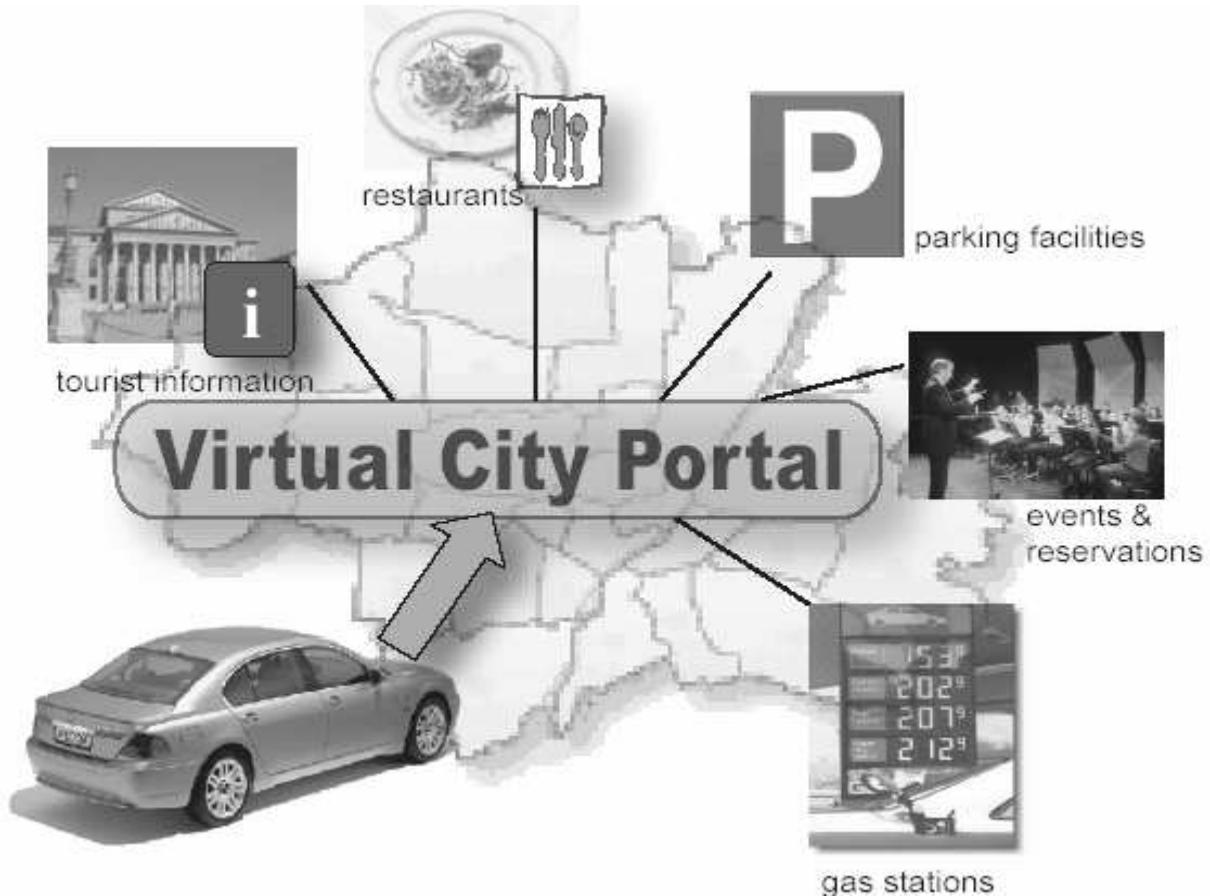


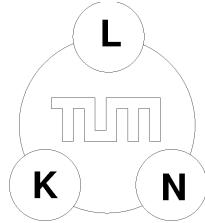


Outline

- 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

VCP prototype 1

Welcome to munich's VirtualCityPortal

Bookmarks

Parking

Tourist Info

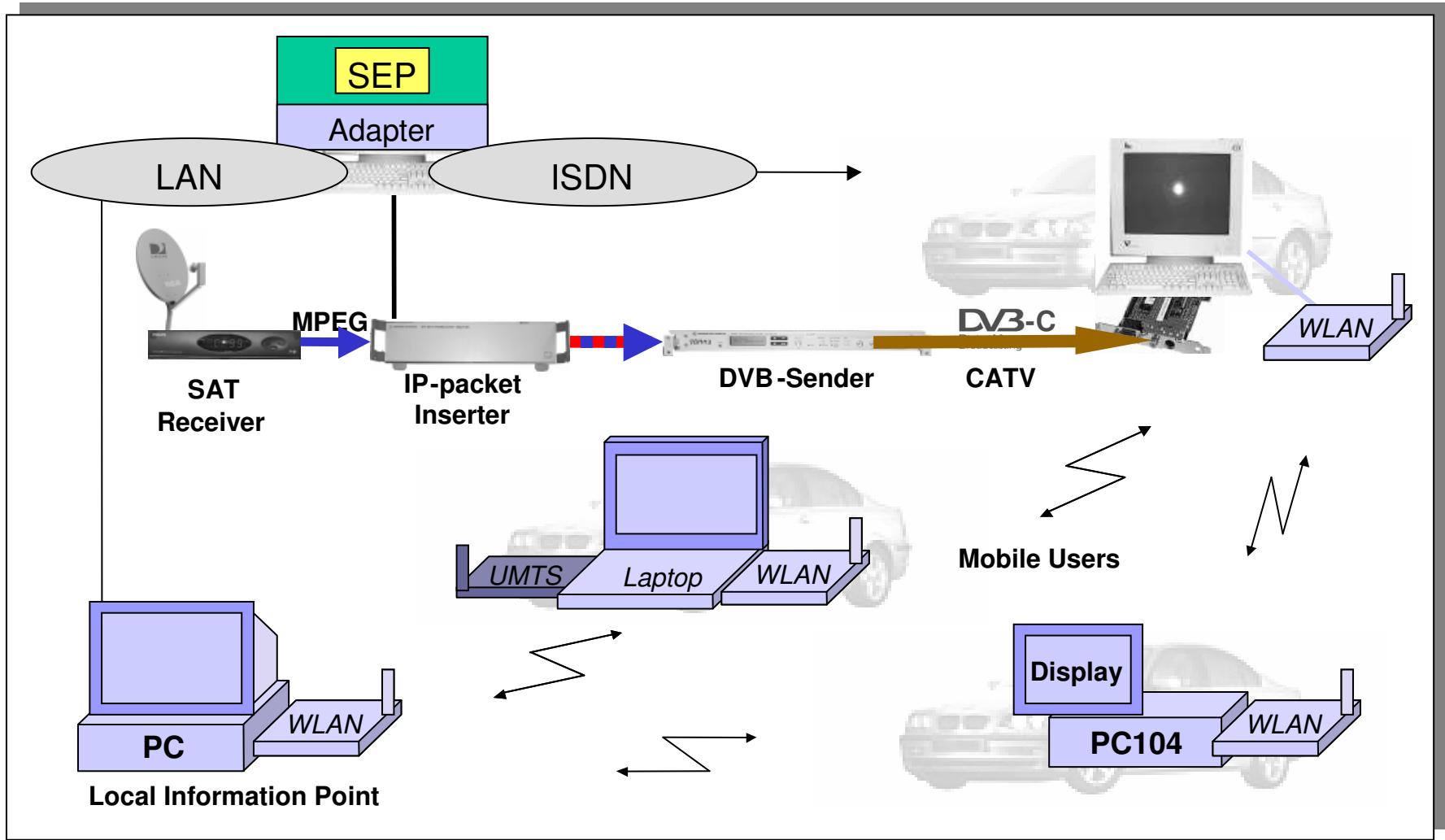
Reservation

VCP Logs

Back

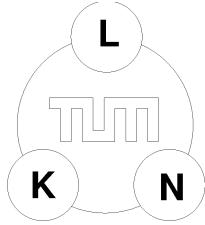
MainMenue

Lab Testbed



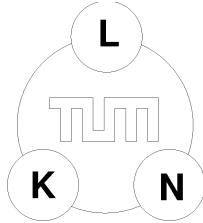
Mobile Testbed





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)



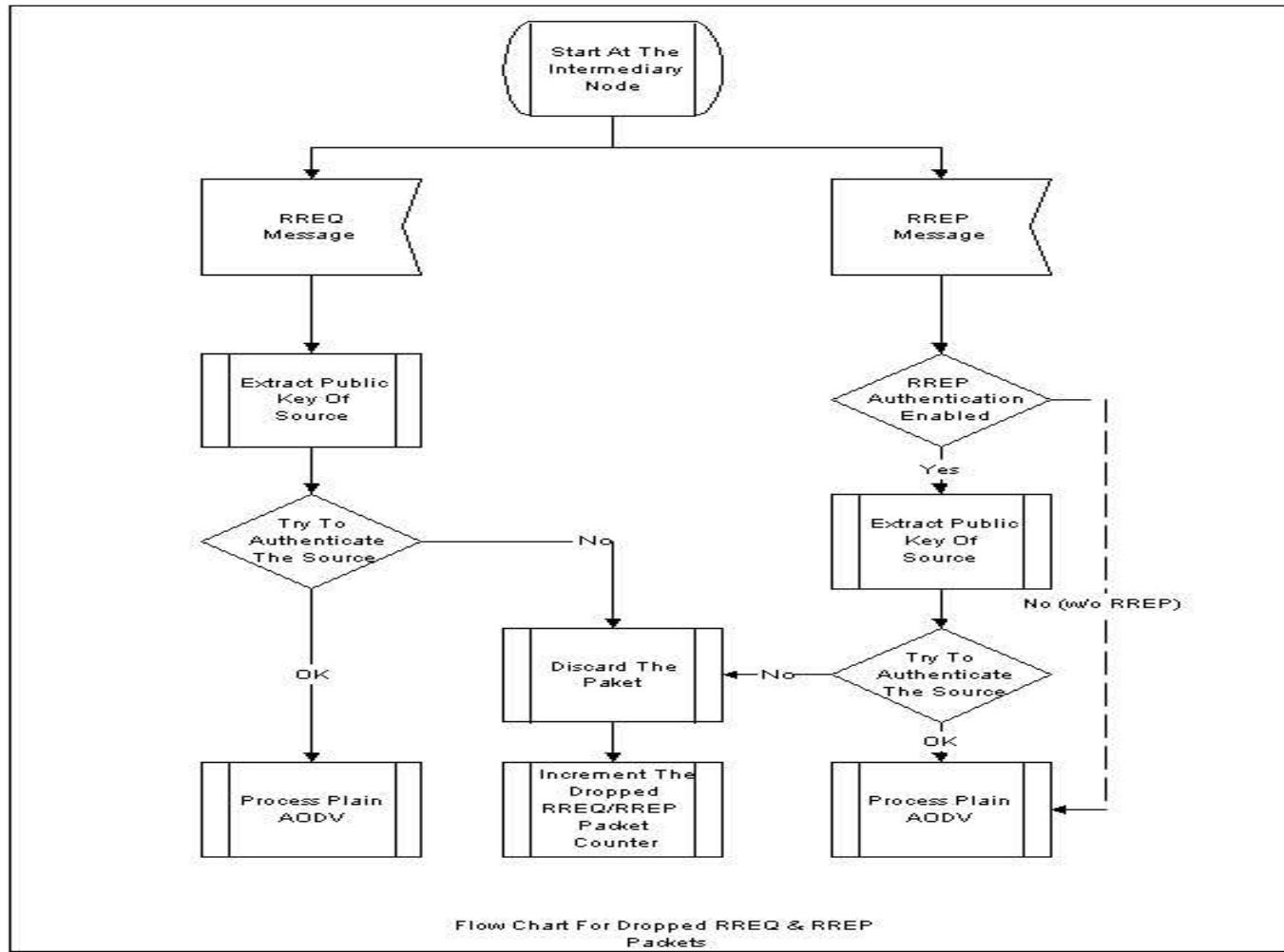
Broadcast AdHoc Security

- 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:

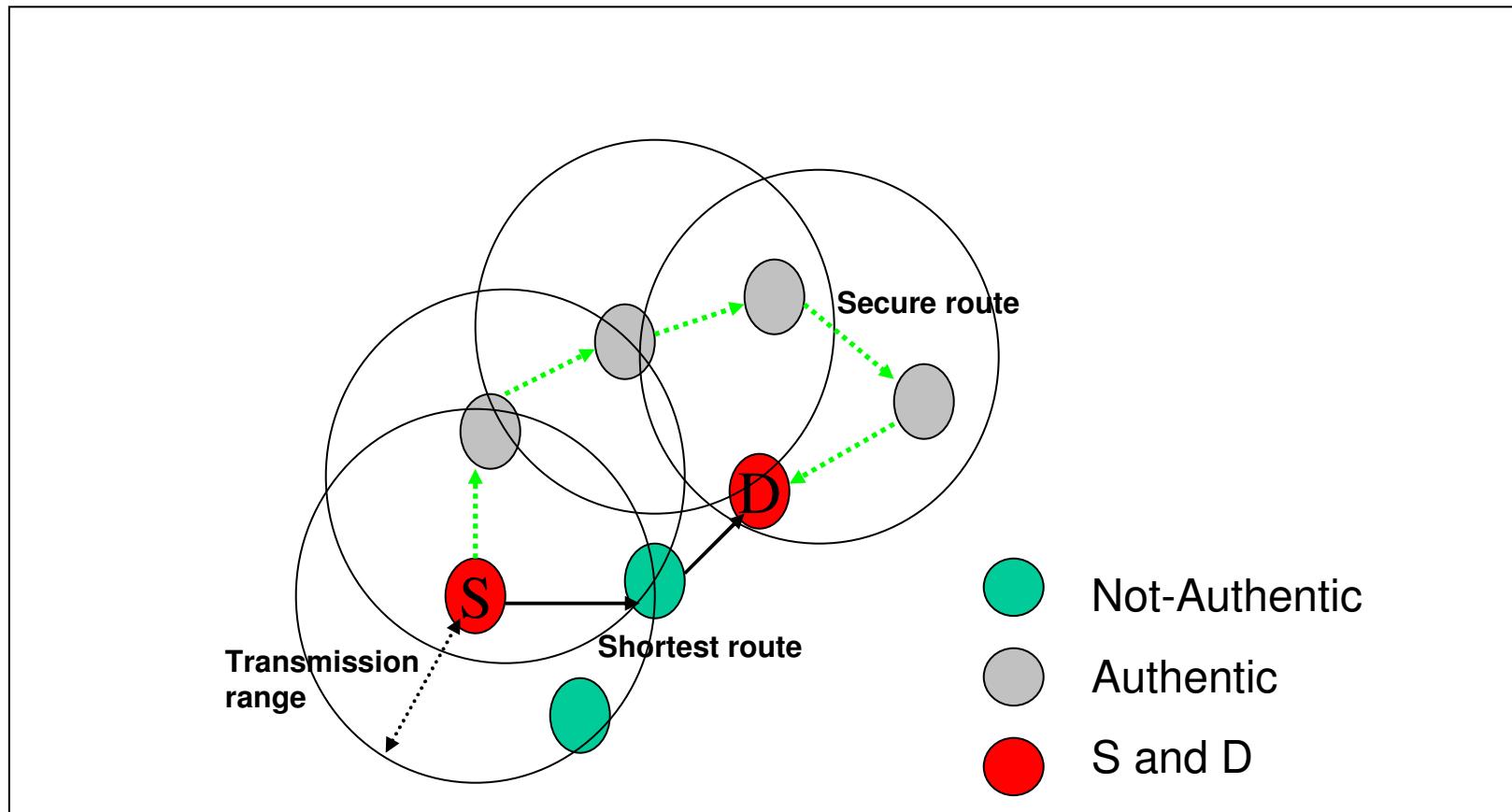
- Only authenticated nodes used for routing

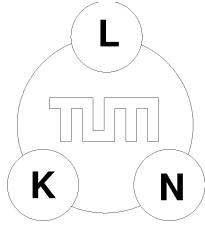
AODV Augmentation



AODV Augmentation

Only “trusted” nodes are used for routing

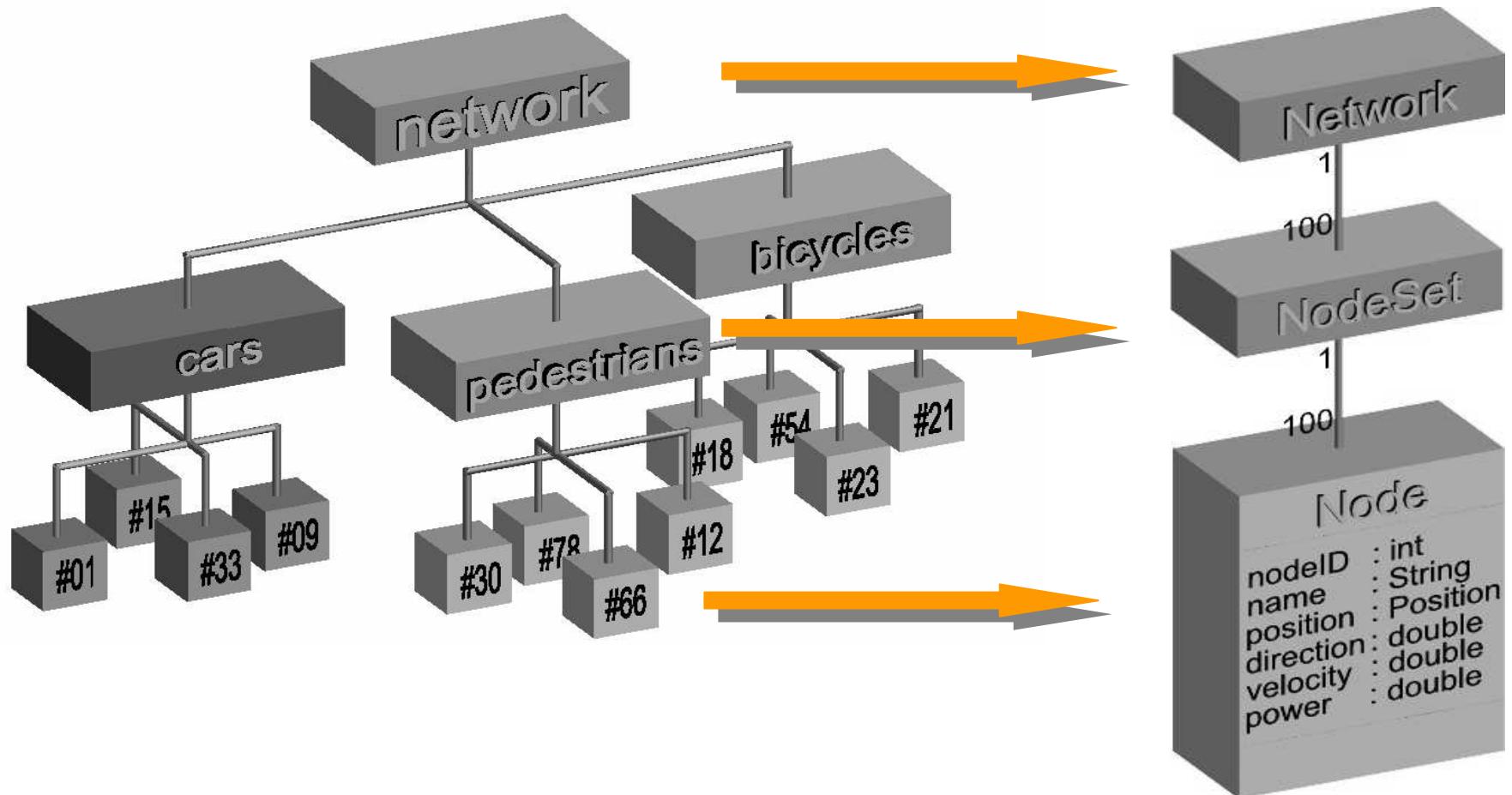


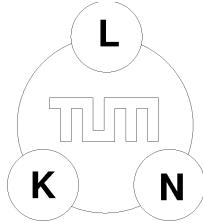


Problems, Optimizations

- 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

The screenshot displays two windows of the AdHoc Simulation Tool.

Network configuration window:

- Area definition:** width: 500, height: 500
- Routing protocol:** AODV
- Number of sets:** 7
- Sets table:**

	Name	ID	Nodes	Mobility Model
1	set_1	#1	1	RM – Node
2	set_2	#2	2	RM – Node
3	set_3	#3	3	RM – Set
4	set_4	#4	4	RM – Node
5	set_5	#5	5	RM – Set
6	set_6	#6	6	RM – Node
7	set_7	#7	7	RM – Node

- More details:** Set selected: set_1 (#1), more...
- Buttons:** Load, Save, Uniform Distribution, etc.

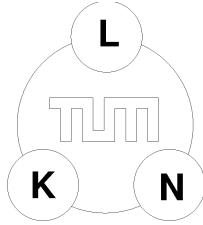
Set configuration window:

- SET:** name: set_3, ID: #3
- Mobility Model:** RM – Set
- Number of nodes:** 3
- Nodes table:**

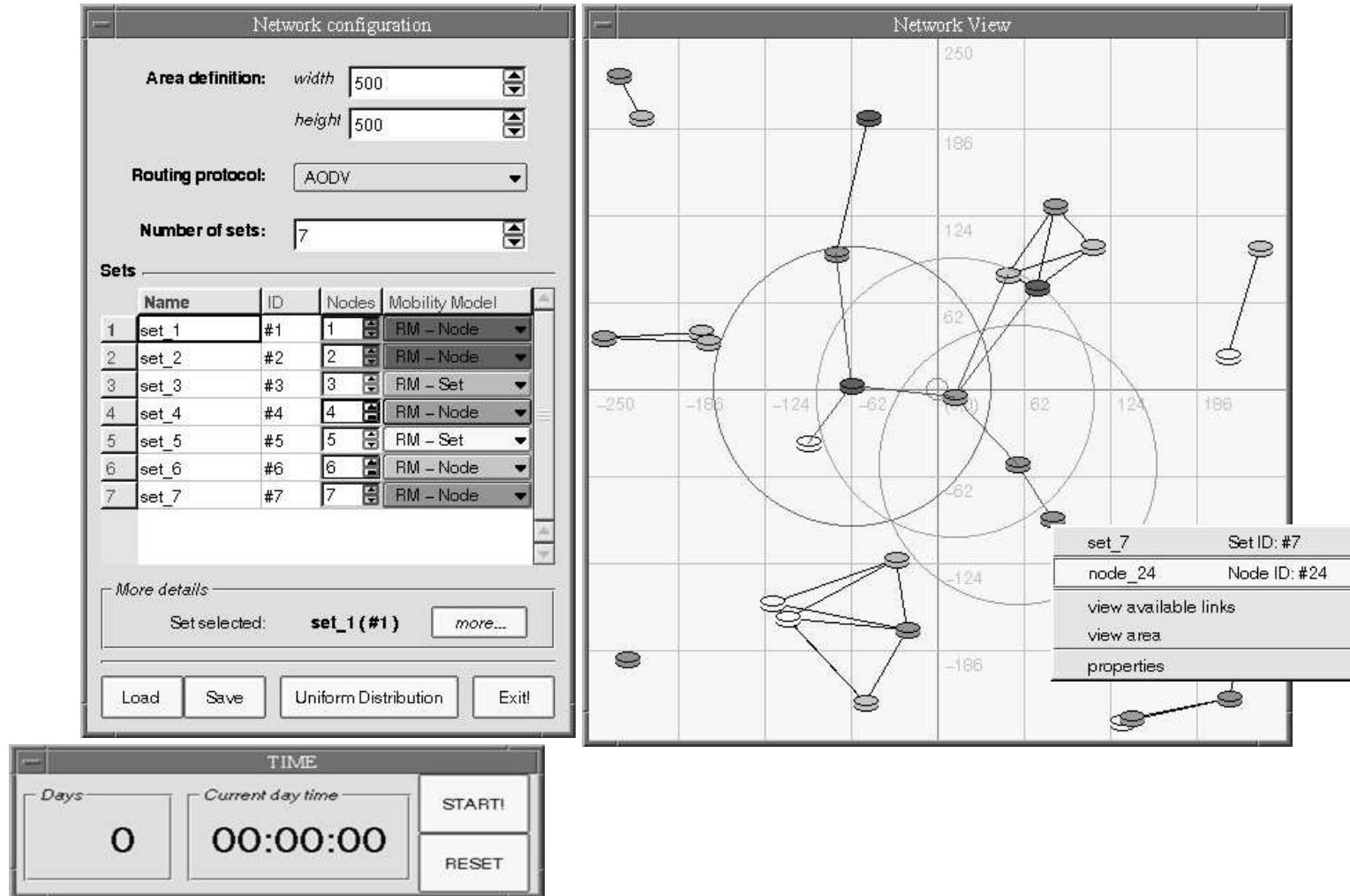
	Name	ID	Pos: (X, Y)	Velocity	Direction	Power
1	node_3	#3	-80.8, -121.8	6.0	-70.0	0.0
2	node_4	#4	-213.4, 194.7	6.0	-120.0	0.4
3	node_5	#5	-165.4, 34.8	2.0	62.0	0.8

- Buttons:** generate random values, remove nodes, Done!

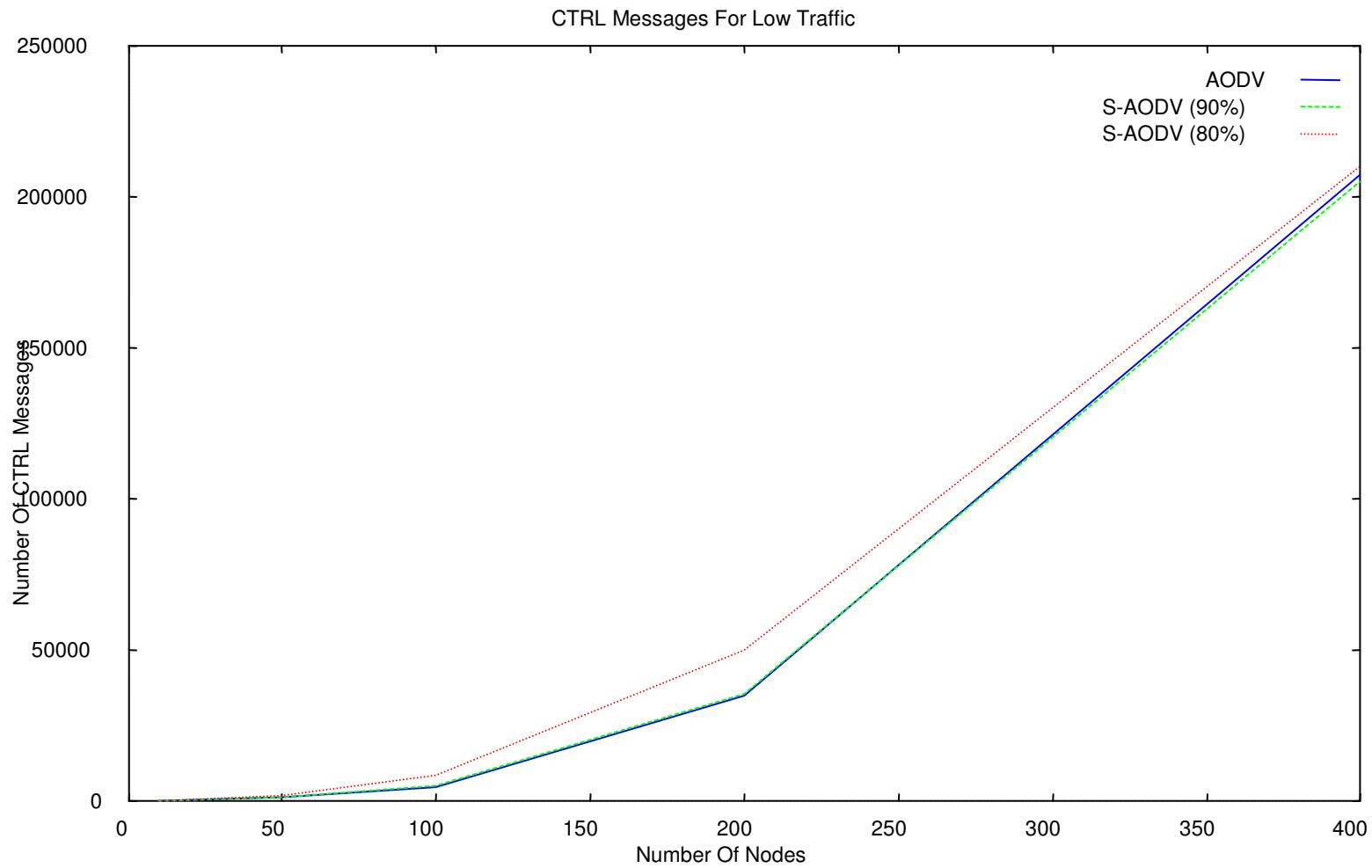
A blue arrow points from the 'More details' section of the Network configuration window towards the 'Set selected' field in the Set configuration window.



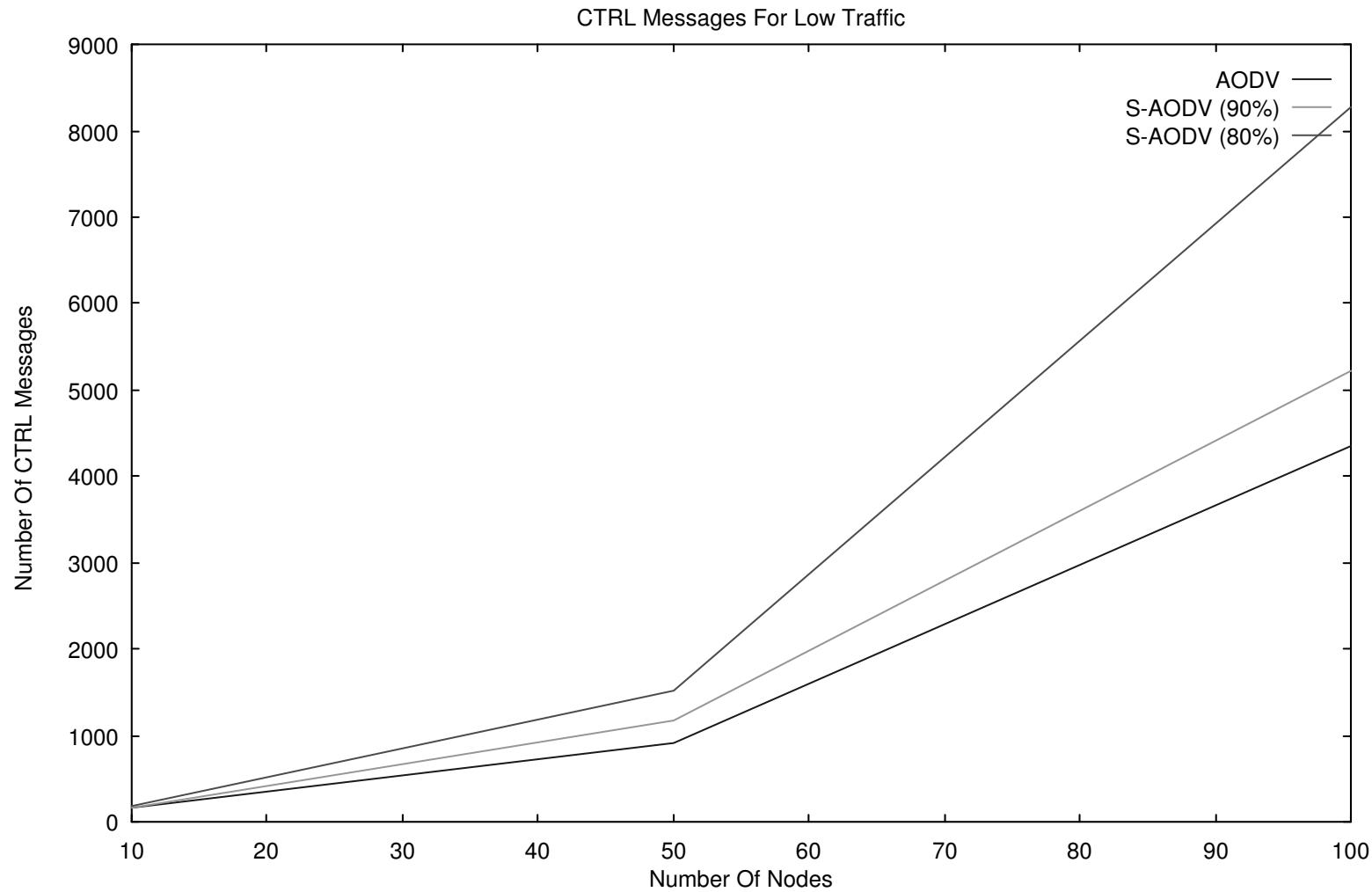
AdHoc Simulation Tool



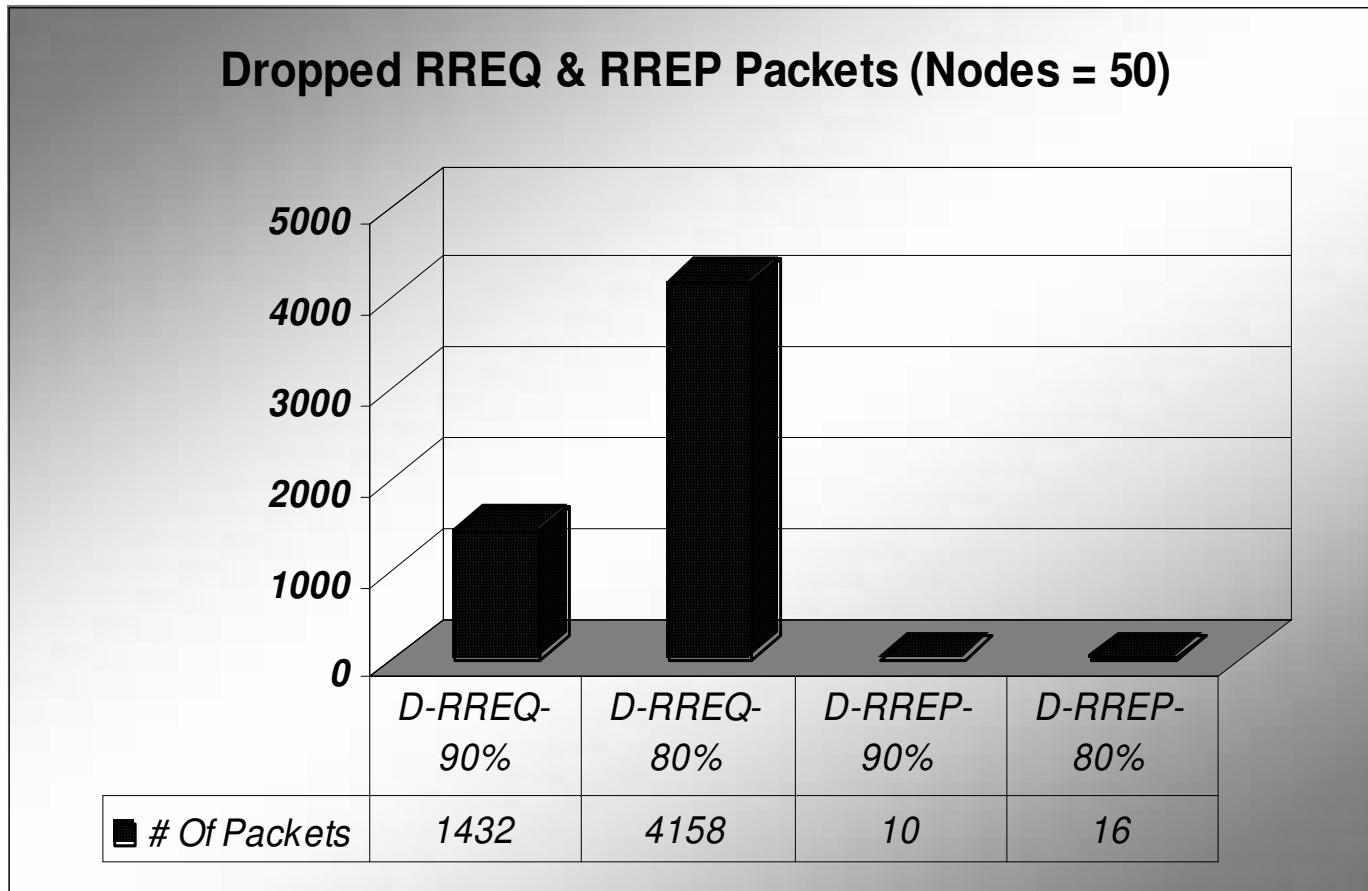
Preliminary Results



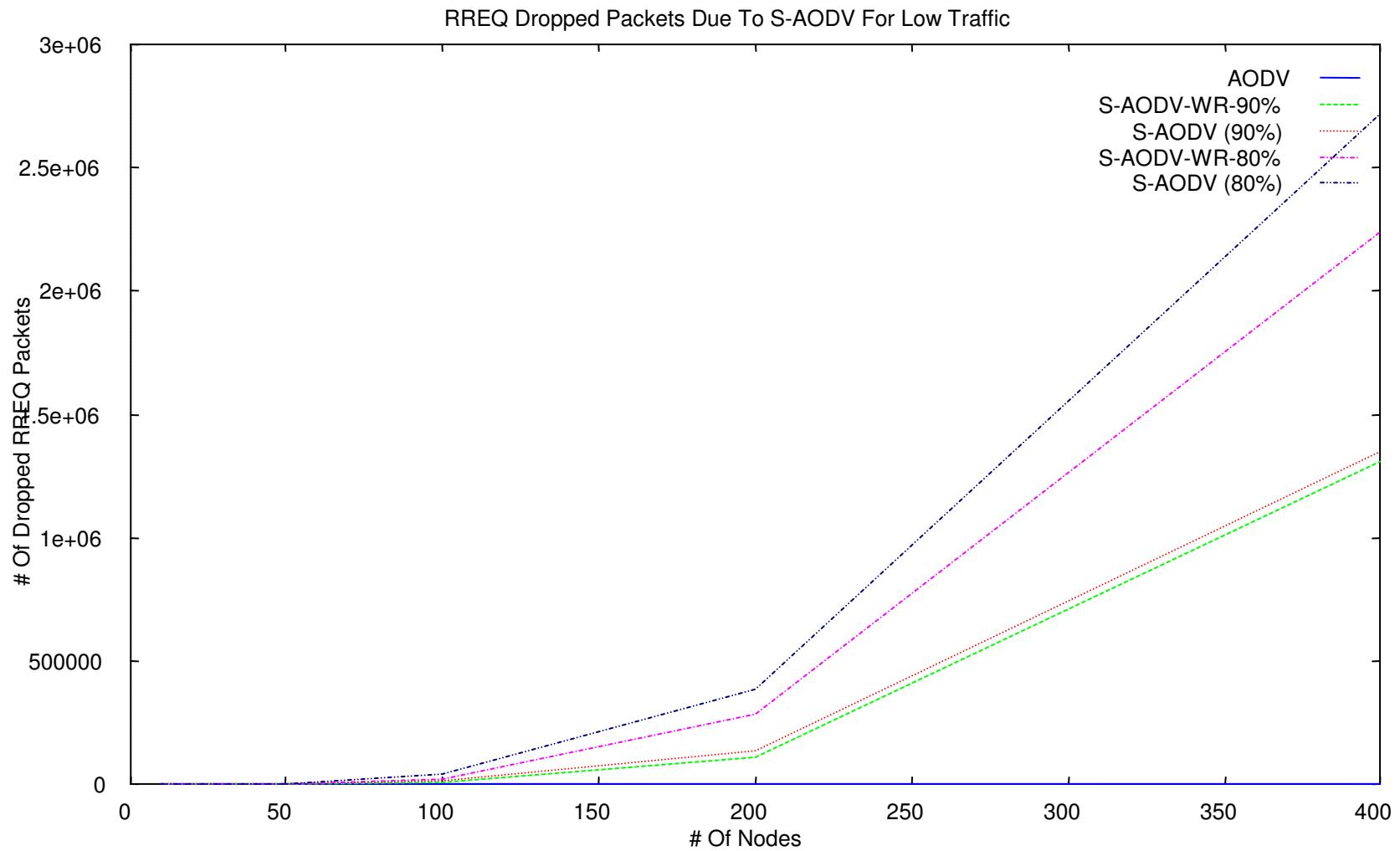
Preliminary Results

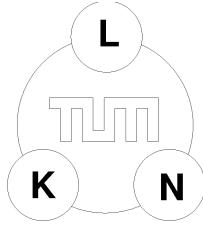


Preliminary Results



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!