Vehicular Ad hoc Networks (VANET)

Chien-Chung Shen
Degas Networking Group
Computer and Information Sciences
University of Delaware
cshen@cis.udel.edu

“Emergence” of Vehicular Networks

- In 1999, US’ FCC allocated 5.850-5.925 GHz band to promote safe and efficient highways
  - Intended for vehicle-to-vehicle and vehicle-to-infrastructure communication
- EU’s Car2Car Consortium has prototypes in March 2006
- Radio standard for **D**edicated **S**hort-**R**ange **C**ommunications (**DSRC**)
  - Based on an extension of 802.11

Why Vehicular Networks?

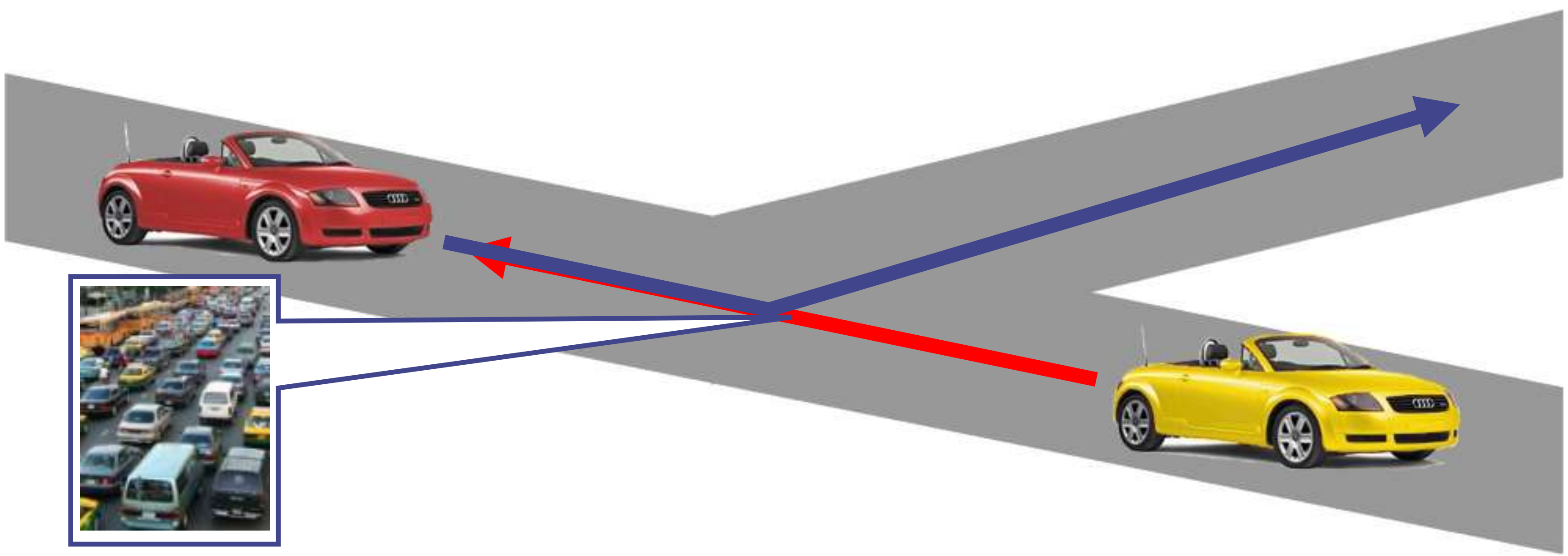
- Safety
  - On US highways (2004):
    - 42,800 Fatalities, 2.8 Million Injuries
    - ~$230.6 Billion cost to society
- Efficiency
  - Traffic jams waste time and fuel
  - In 2003, US drivers lost a total of 3.5 billion hours and 5.7 billion gallons of fuel to traffic congestion
- Profit
  - Safety features and high-tech devices have become product differentiators

Applications

- Congestion detection
- Vehicle platooning
- Road conditions warning
- Collision alert
- Stoplight assistant
- Emergency vehicle warning
- Deceleration warning
- Toll collection
- Border clearance
- Adaptive cruise control
- Drive-through payment
- Merge assistance

Congestion Detection

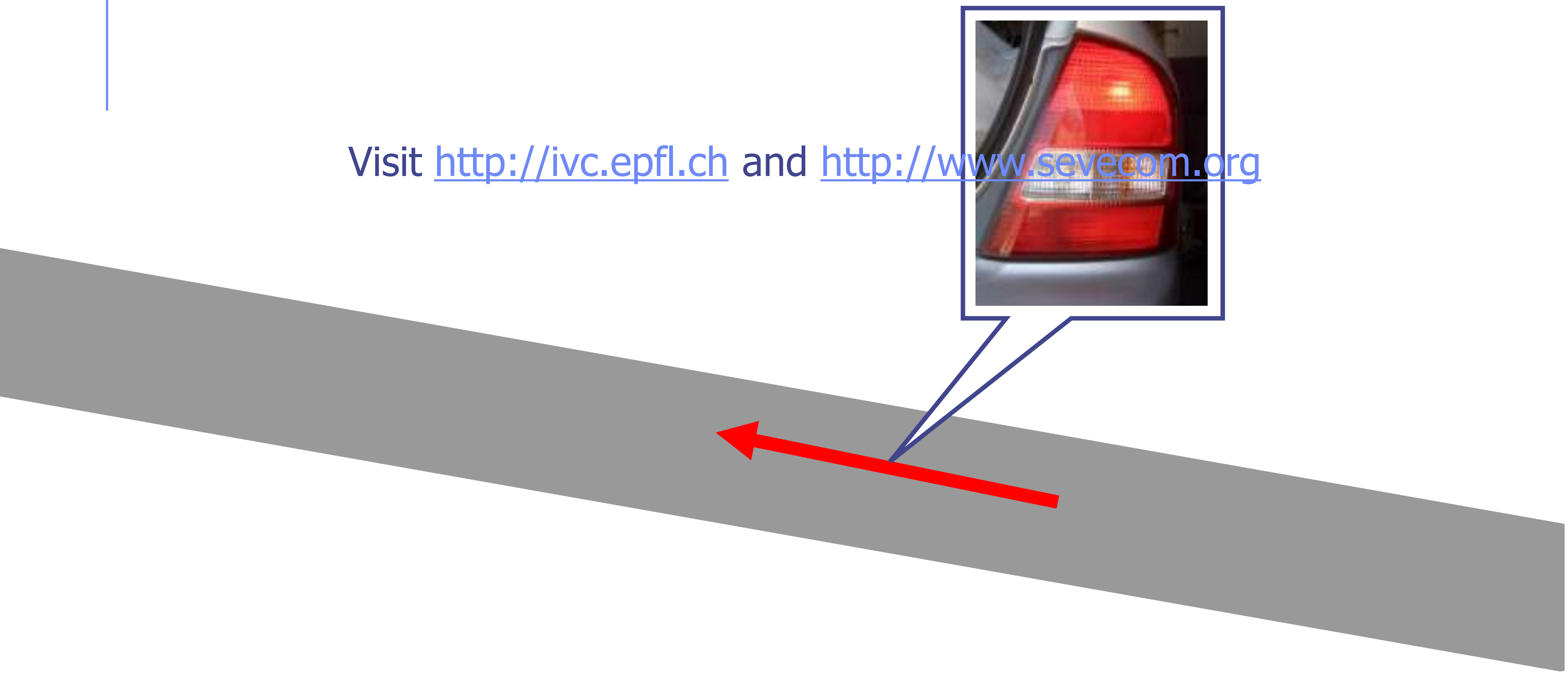
- Vehicles detect congestion when:
  - # Vehicles > Threshold 1
  - Speed < Threshold 2
- Relay congestion information
  - Hop-by-hop message forwarding
  - Other vehicles can choose alternate routes



Deceleration Warning

- Prevent pile-ups when a vehicle decelerates rapidly

Visit http://ivc.epfl.ch and http://www.sevecom.org



References

- ACM VANET Workshops (2004-2008) at http://www.sigmobile.org/events/workshops.html
- IEEE AutoNet Workshops (2006-2008) at http://autonet200*.research.telcordia.com
- **EU work on security**
  - **http://ivc.epfl.ch**
  - **SeVeCom (Secure Vehicular Communication) http://www.sevecom.org**
- (Many) other (major) conferences (workshops) and journals

Outline

- **DSRC and collision warning**
- Data access
- Broadcast and routing
- Information dissemination
- Address configuration
- Security

Cooperative Collision Warning Using Dedicated Short Range Wireless Communications

Tamer ElBatt, Siddhartha Goel, Gavin Holland, Hariharan Krishnan, and Jayendra Parikh, ACM VANET, 2006

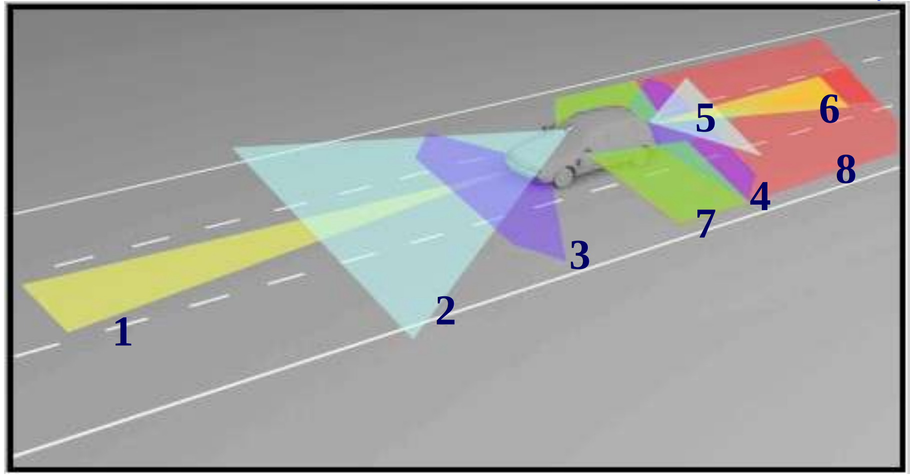
Dedicated Short Range Communications

- What is **DSRC**?
  - High data rate (≤ 27 Mbps), short range (≤ 1 km), multi-channel wireless standard based on 802.11a PHY and 802.11 MAC
  - 1st standard draft developed by ASTM in 2003 and currently being evaluated by:
    - IEEE 802.11 TGp/WAVE: PHY/MAC
    - IEEE 1609.4: Multi-channel coordination
    - IEEE 1609.3: Network-layer protocols
- Why DSRC?
  - Operate in the 75 MHz *licensed spectrum* at 5.9 GHz allocated by FCC for ITS applications
  - Avoid intolerable and uncontrollable interference in the ISM unlicensed bands, especially for safety applications
- Major Differences from IEEE 802.11a:
  - Licensed band operation
  - Outdoor high-speed vehicle applications (up to 120 mph)
  - 7 channels (10 MHz each) for supporting safety and non-safety applications

Motivation

- Vehicle safety research is shifting its focus towards crash avoidance and collision mitigation
  (passive vs. **active** safety)
- Traditional sensors, like radars, have the following limitations:
  - **Limited range (sense immediate vehicles)**
  - **Limited Field of View (FOV)**
  - **Expensive**
- **Cooperative** collision warning systems explore the feasibility of using wireless comm. (e.g. DSRC) for vehicle safety

TRADITIONAL SENSORS

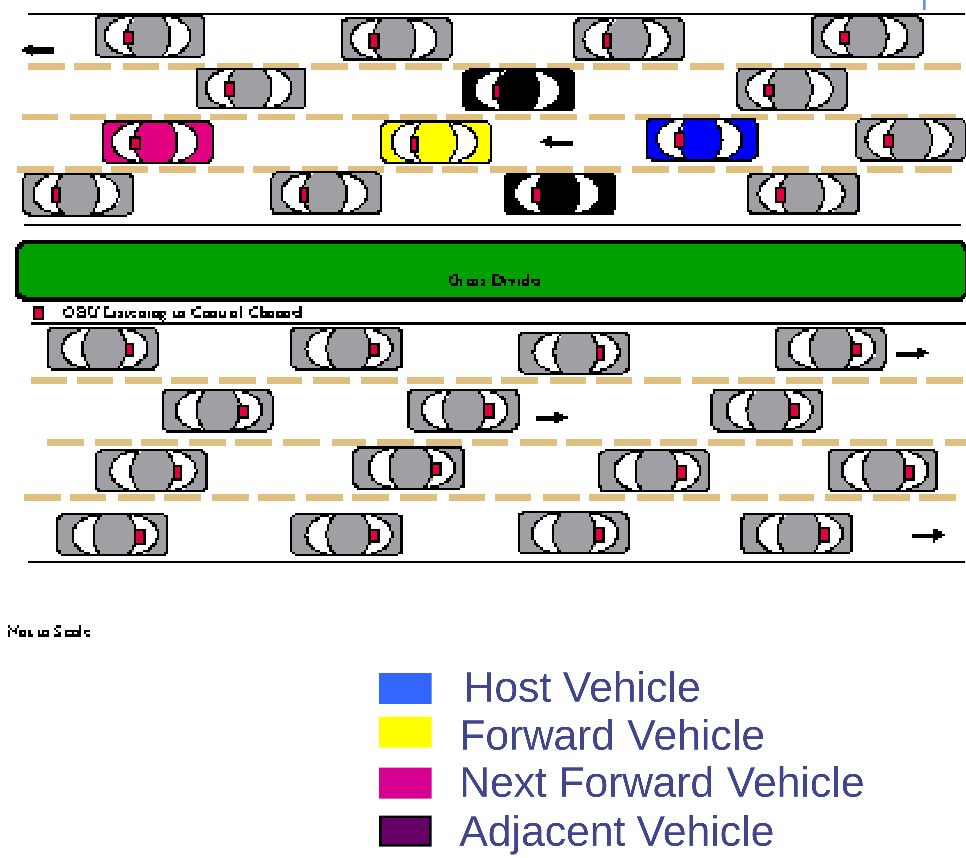


COOPERATIVE COLLISION WARNING (CCW)

"360 Degrees Driver Situation Awareness" using wireless comm.

Examples of CCW Applications

- Forward Collision Warning (FCW)
  - **Host Vehicle (HV) utilizes messages from the immediate Forward Vehicle in the same lane to avoid forward collisions**
- Lane Change Assistance (LCA)
  - **Host Vehicle utilizes messages from the Adjacent Vehicle in a neighboring lane to assess unsafe lane changes**
- Electronic Emergency Brake Light (EEBL)
  - **Host Vehicle utilizes messages to determine if one, or more, leading vehicles in the same lane are braking**
- Requirements:
  - **Wireless Platform**
  - **GPS device with ~ 1-1.5m resolution to properly associate vehicles with lanes**



focus on single-hop broadcast CCW applications

Related Work

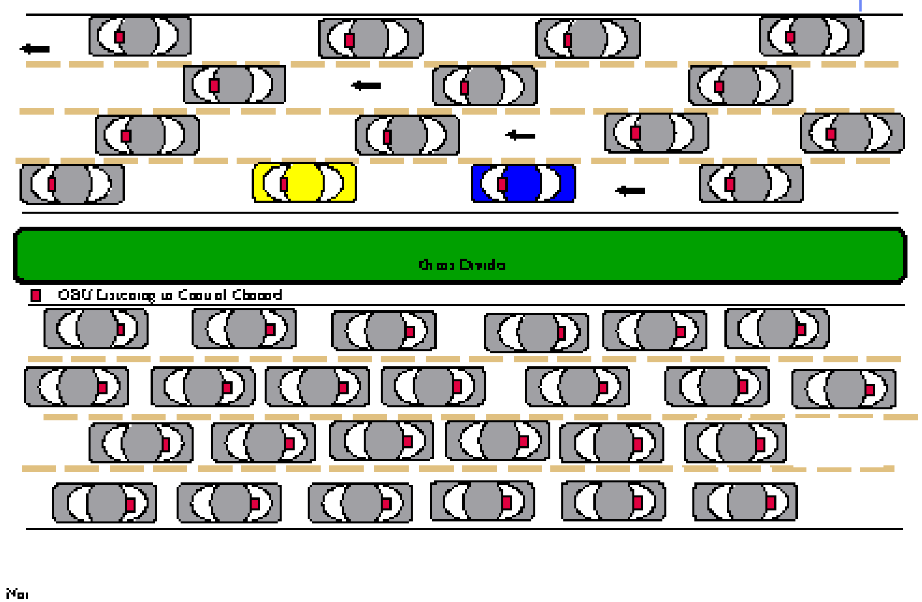
- *Xu et al., 2004:* **impact of rapid repetition of broadcast messages on the packet reception failure of random access protocols**
- *Torrent-Moreno et al., 2004:* **quantify channel access time and reception probability under deterministic and statistical channel models**
- *Yin et al., 2004:* **detailed DSRC PHY layer model incorporated into a VANET simulator supporting generic safety application models**
- *Joint initiative by Government, Industry and Standards Bodies:*
  - Government: **FCC, US DoT (Vehicle Infrastructure Integration (VII)), …**
  - Industry: **Automotive (CAMP [US], C2CC [Europe]), chip makers, system integrators, …**
  - Standards Bodies: **ASTM, IEEE, SAE, ISO, …**

Contributions: i) CCW application modeling

ii) Application-perceived latency metrics

Forward Collision Warning (FCW)

- Application Model
  - **Single-hop broadcasts over UDP**
  - **Broadcast rate: 10 packets/sec**
  - **Packet size = 100 Bytes payload**
- All vehicles broadcast, according to the above model, a small message bearing status information (e.g. location, velocity, ...)
- Measure the quality of reception at a randomly chosen HV for messages transmitted only by the FV
  - **HV ignores messages from other vehicles, based on their relative location**



Host Vehicle (HV)
Forward Vehicle (FV)

Latency of Periodic Broadcast Applications

- Packet-level Metric:
  - Per-packet Latency (PPL): **defined as the time elapsed between generating a packet at the application of the sender and successfully receiving the same packet at the application of the receiver**
    - **Important metric for network and protocol designers**
    - **However, it does not reveal much about the latency of *periodic* applications**

Problem: **Application requirements are not given in terms of packet-level metrics**

- Application-level Metric:
  - Packet Inter-Reception Time (IRT): **defined as the time elapsed between two successive successful reception events for packets transmitted by a specific transmitter**
    - **Directly related to the pattern of consecutive packet losses**

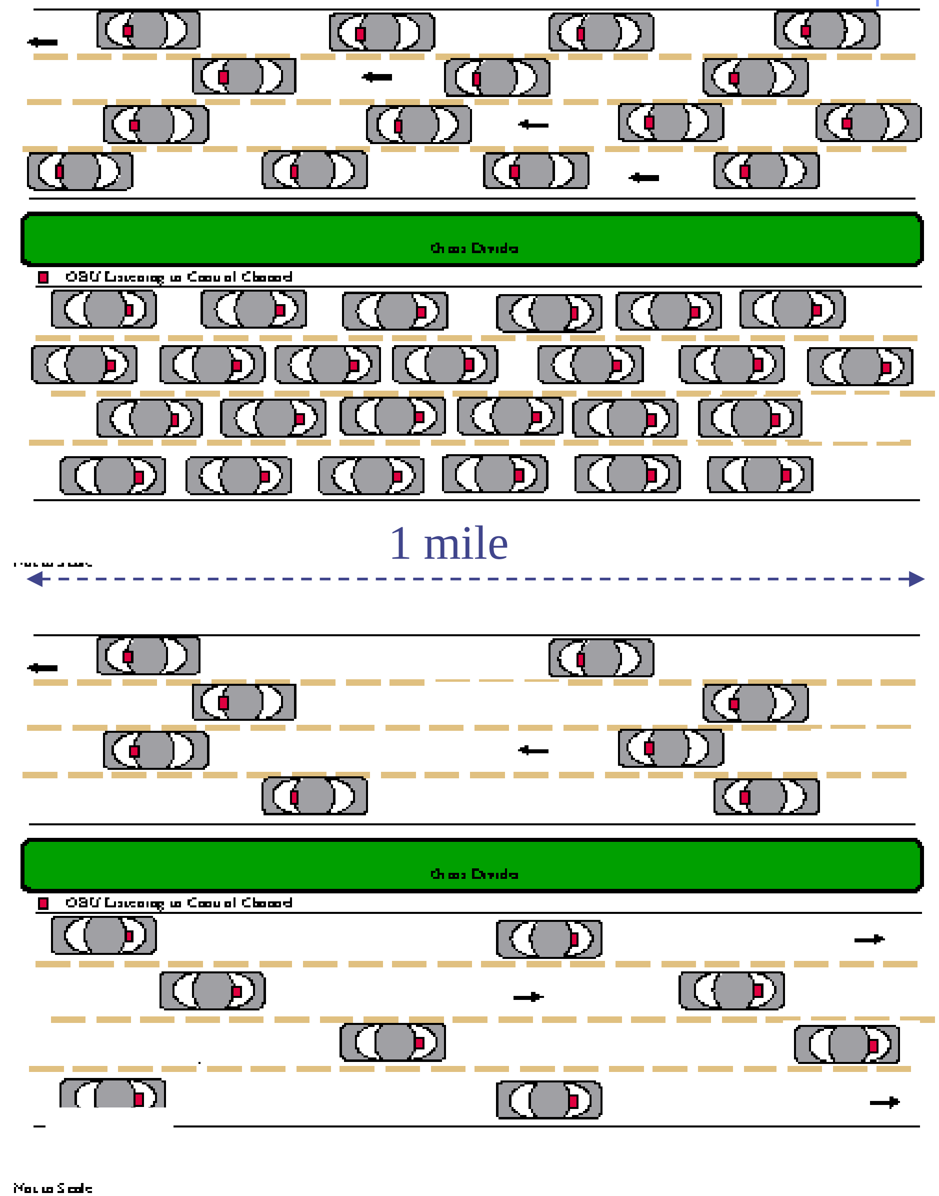
Strong need for performance metrics that bridge the gap between the networking and automotive communities

Simulation Setup

- Simulation Tool: **QualNet™**
- Protocol Stack:
  - **PHY/MAC: DSRC @ 6 Mbps data rate,** single-channel operation
  - **Transport: UDP**
  - **Application: single-hop broadcast @ 10 packets/sec broadcast rate**
- Wireless Channel Model:
  - **Exponential decay with distance**
  - **Path loss = 2.15 out to a distance of ~150m (experimental measurements)**
  - **BER vs. SNR performance of DSRC measured using DSRC test kits from DENSO™**
- Transmission Power: **16.18 dBm (range ~150 meters)**
- Simulation time: **30 sec**
  - **Each vehicle broadcasts 290 messages throughout a simulation run**
- Mobility: **straight freeway**
- # simulation runs: **20**

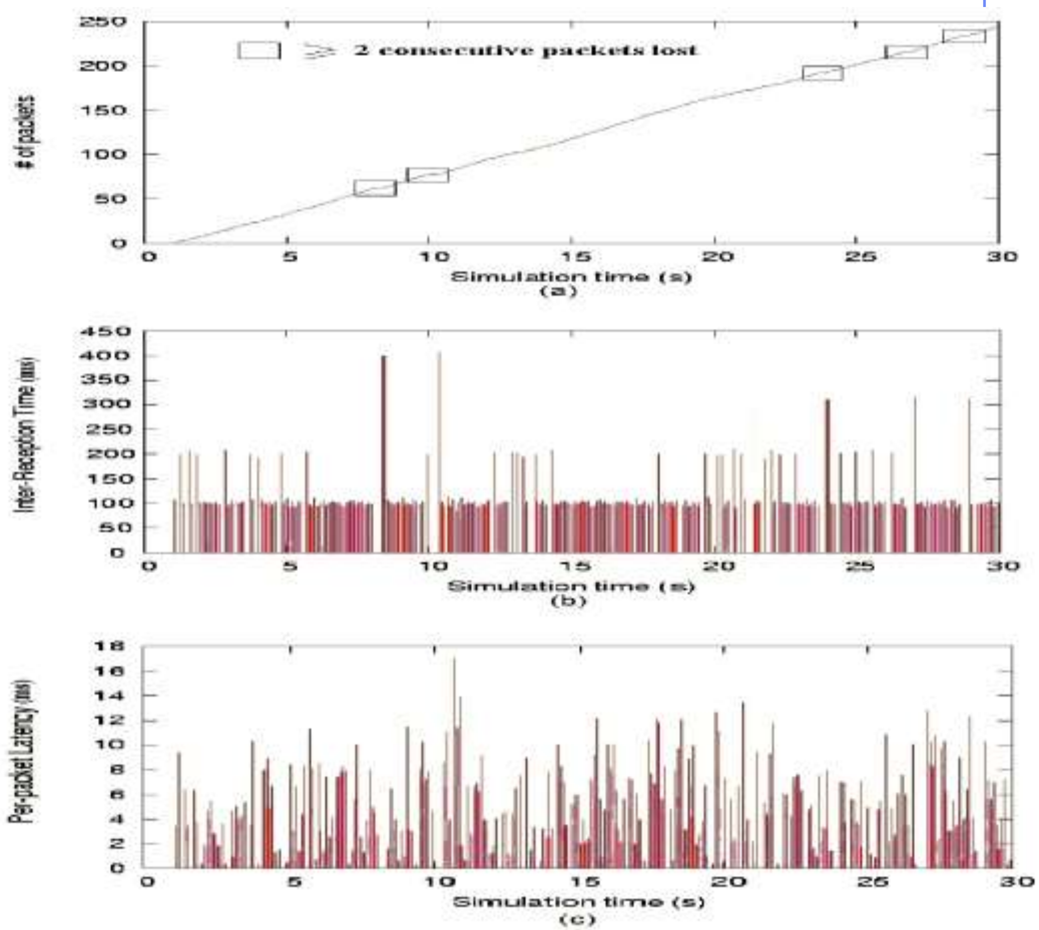
Freeway Mobility Scenarios

- High Density Scenario: (1920 vehicles)
  - **One Side of the freeway**
    - **Stationary vehicles**
    - **Vehicle separation = 5m**
  - **On the other side:**
    - **Avg vehicle speed = 25 mph**
    - **Avg vehicle separation ~10m**
- Low Density Scenario: (208 vehicles)
  - Avg vehicle speed = 65 mph
  - Avg vehicle separation ~61m



FCW performance for a chosen pair of vehicle **(High Density)**

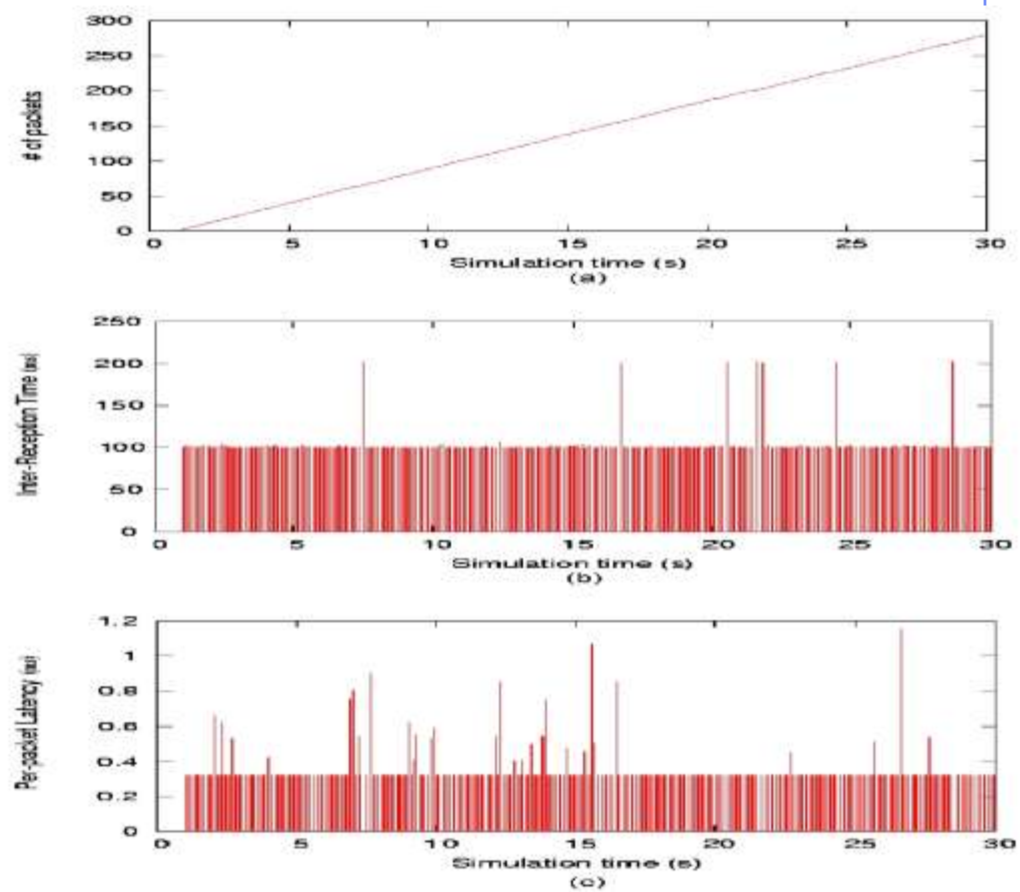
- **Cumulative Packet Reception:**
  - ~ 46 packets lost out of 290 sent
  - But, Max. # consecutive packet losses is only 3
- **Inter-Reception Time (IRT):**
  - Max. ~400 msec, Min. ~100 msec
- **Per-packet Latency (PPL):**
  - Max. ~17 msec, Min. ~0.321 msec



- **Max. IRT stats over 20 runs: Mean = 372.1 ms, SD = 66.3 ms, 95% CI = 58.1 ms**
- **IRT and PPL vary over vastly different ranges (due to consecutive pkt losses)**

FCW performance for a chosen pair of vehicle **(Low Density)**

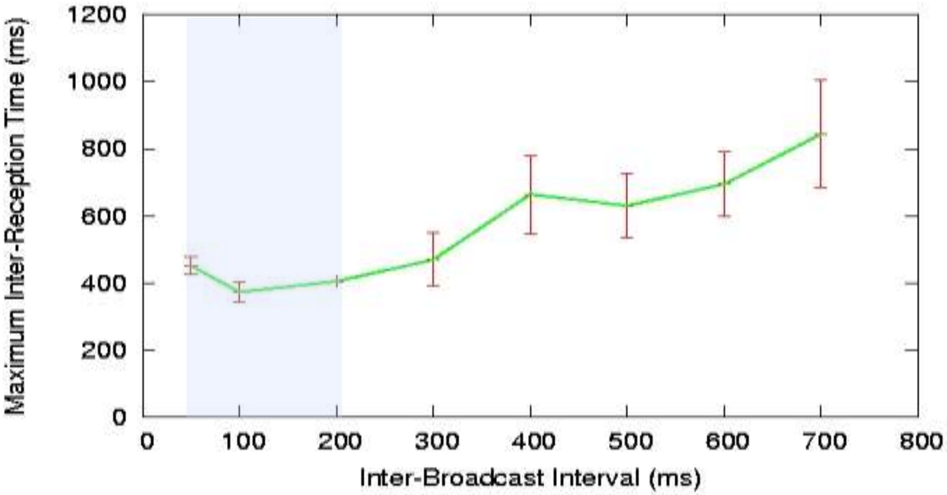
- **Cumulative Packet Reception:**
  - Only 7 packets lost in total
  - No consecutive packets losses
- **Max. Inter-Reception Time (IRT):**
  - Max. = 200 msec, Min. = 100 msec
- **Per Packet Latency (PPL):**
  - Max. ~1 msec, Min. ~0.321 msec

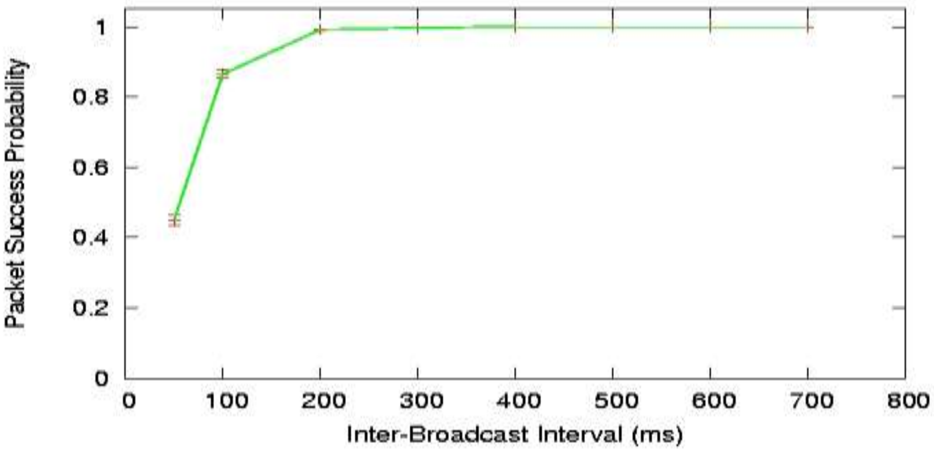


- **Max. IRT stats over 20 runs: Mean = 238 ms, SD = 74.4 ms, 95% CI = 65.2 ms**
- **Performance gap between extreme densities is small**

FCW Broadcast Rate Adaptation

- Motivation: **balance the factors contributing to the packet <u>Inter-reception time (IRT)</u>**
  - **# consecutive packet losses: favors low broadcast rates**
  - **Inter-broadcast interval: favors high broadcast rates**
- High density scenario, 150 m range, 100 Bytes payload
- Examine different Broadcast intervals:
  - **50, 100, 200, ..., 700 msec**

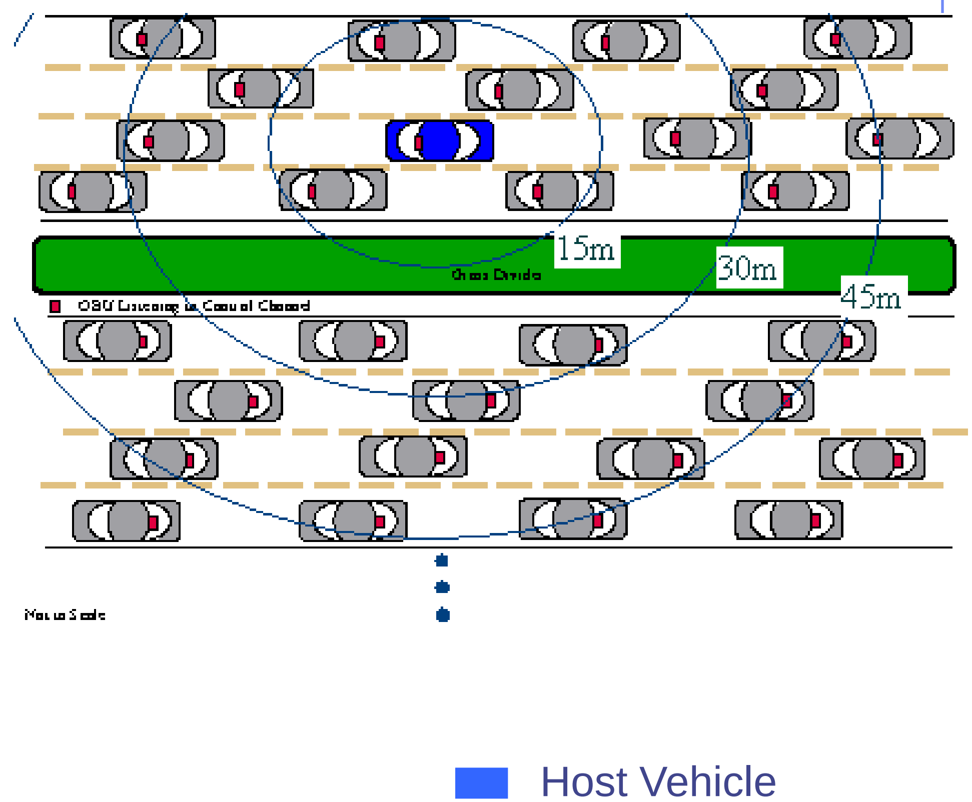




Conjecture: There is an optimal broadcast interval that minimizes IRT

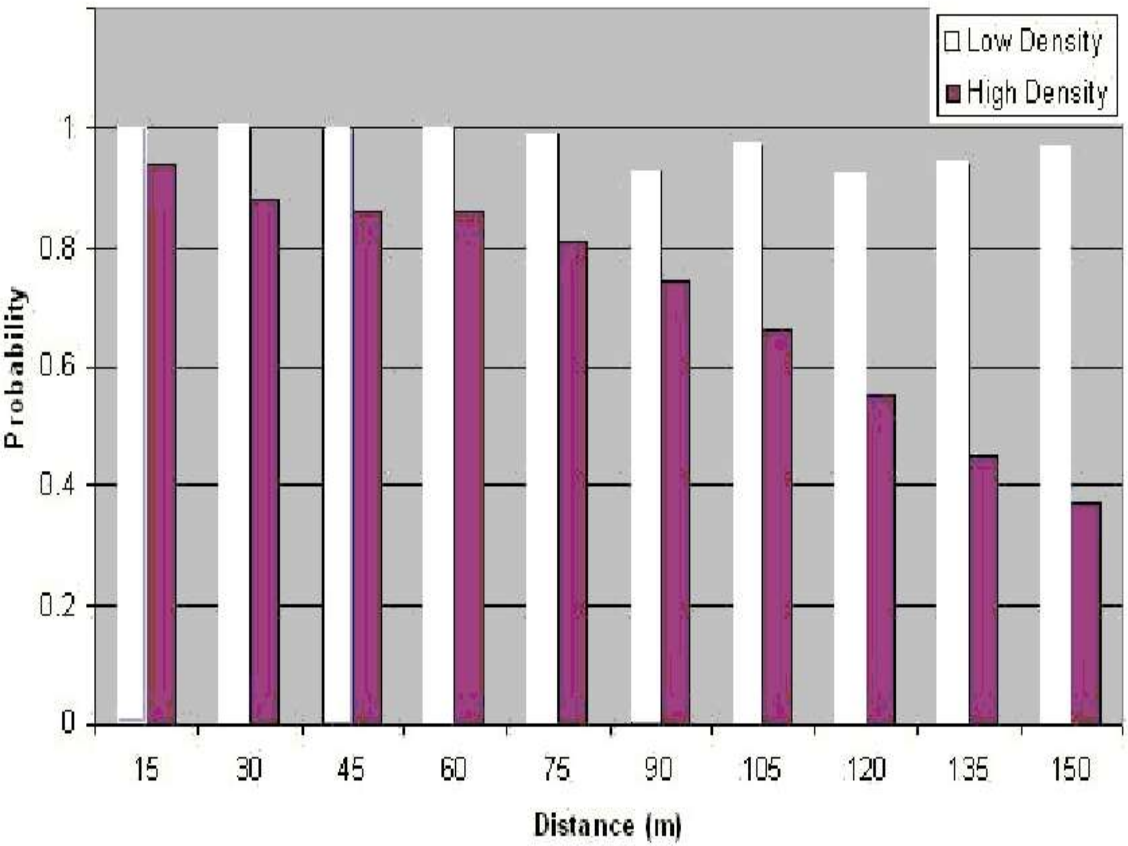
DSRC Performance Trends with Distance

- Objective: **Characterize the behavior of packet success probability with increasing distance from the Host Vehicle**
  - **Transmission Range is fixed**
- All vehicles are stationary
- Measured at a randomly chosen Host Vehicle
  - **150m comm. range is divided into 10 concentric bins at 15m, 30m, 45m, ….**



Packet Success Probability at the HV

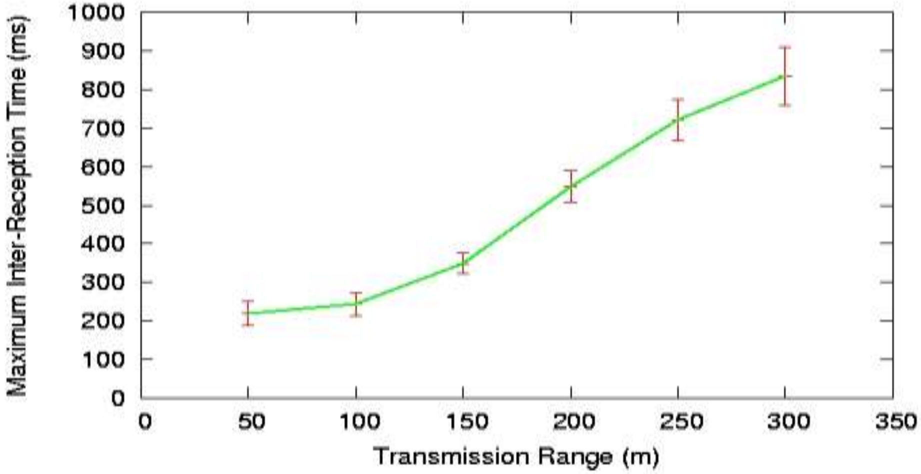
- Success probability varies considerably with distance
  - Good reception from nearby vehicles
  - Even at the edge of the reception range (150m), success probability ~ 38%

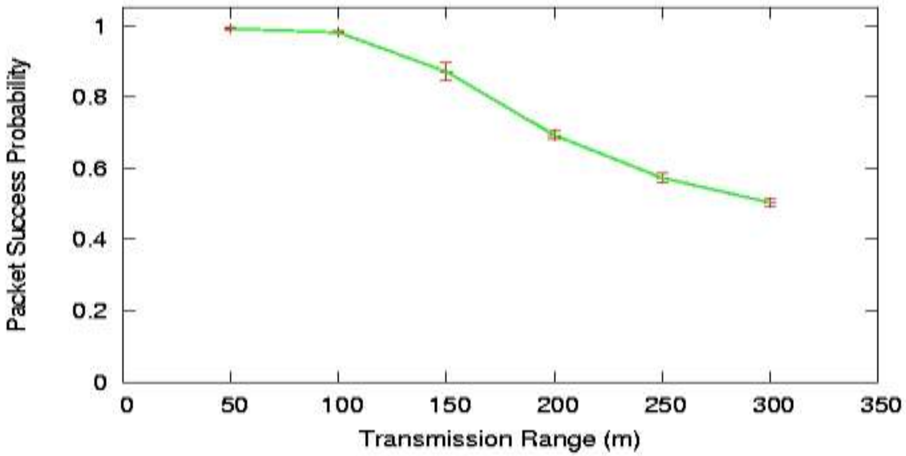


Quality of reception at HV strongly depends on the distance to the relevant sender, as specified by the application

Broadcast Enhancements (Transmission Range)

- Motivation: **gauge the performance improvement attributed to reduced interference using short Tx range**
- Examine different Tx Ranges:
  - **50 m, 100 m, …, 300 m**
- Conduct 20 experiments for each Tx range value
- Observations:
  - **FCW IRT increases with the Tx range due to higher number of successive packet collisions**
  - **50 m range improves IRT by 4-fold over 300 m range**





Dynamic Power Control considerably improves FCW performance

Outline

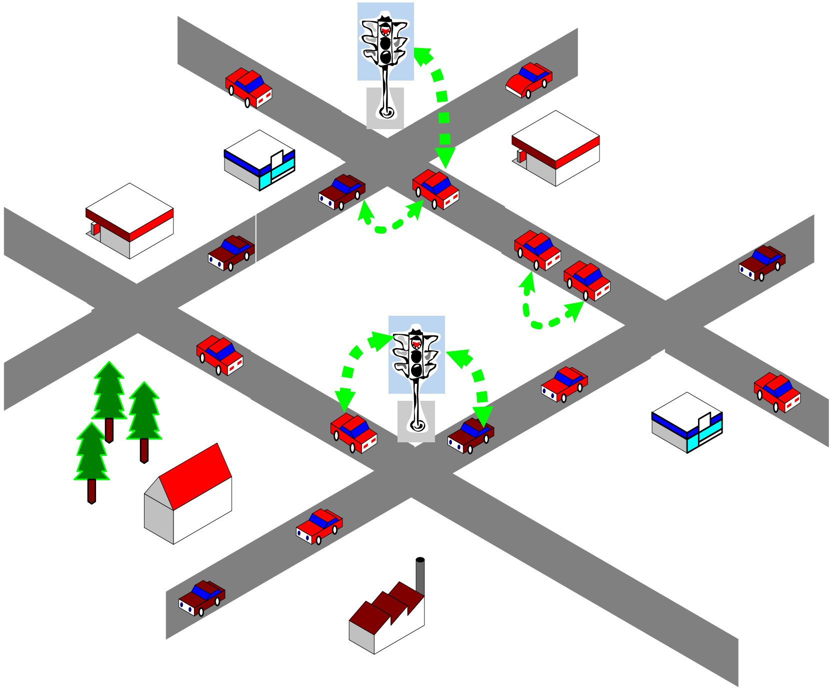
- DSCR and collision warning
- **Data access**
- Broadcast and routing
- Information dissemination
- Address configuration
- Security

On Scheduling Vehicle-Roadside Data Access

Yang Zhang, Jing Zhao and
Guohong Cao, ACM VANET, 2007

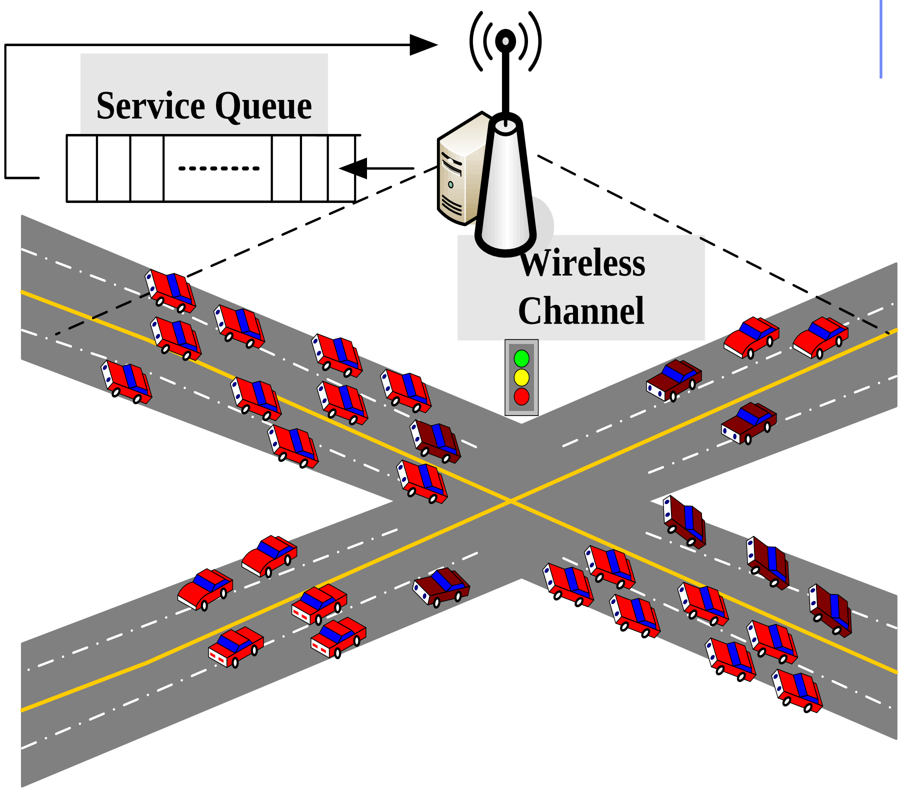
The Big Picture

- Vehicular Ad-hoc Networks - VANET
  - Moving Vehicles
  - RoadSide Units (RSU)
    - Local broadcasting infostations
    - 802.11 access point
- Applications
  - Commercial Advertisement
  - Real-Time Traffic
  - Digital Map Downloading
- Task
  - Service Scheduling of Vehicle-Roadside Data Access



Challenges

- Bandwidth Competition
  - All requests compete for the same limited bandwidth
- **Time Constraint**
  - Vehicles are moving and they only stay in the RSU area for a short period of time
- Data Upload/Download
  - The miss of upload leads to data staleness



Assumptions and Performance Metrics

Assumptions

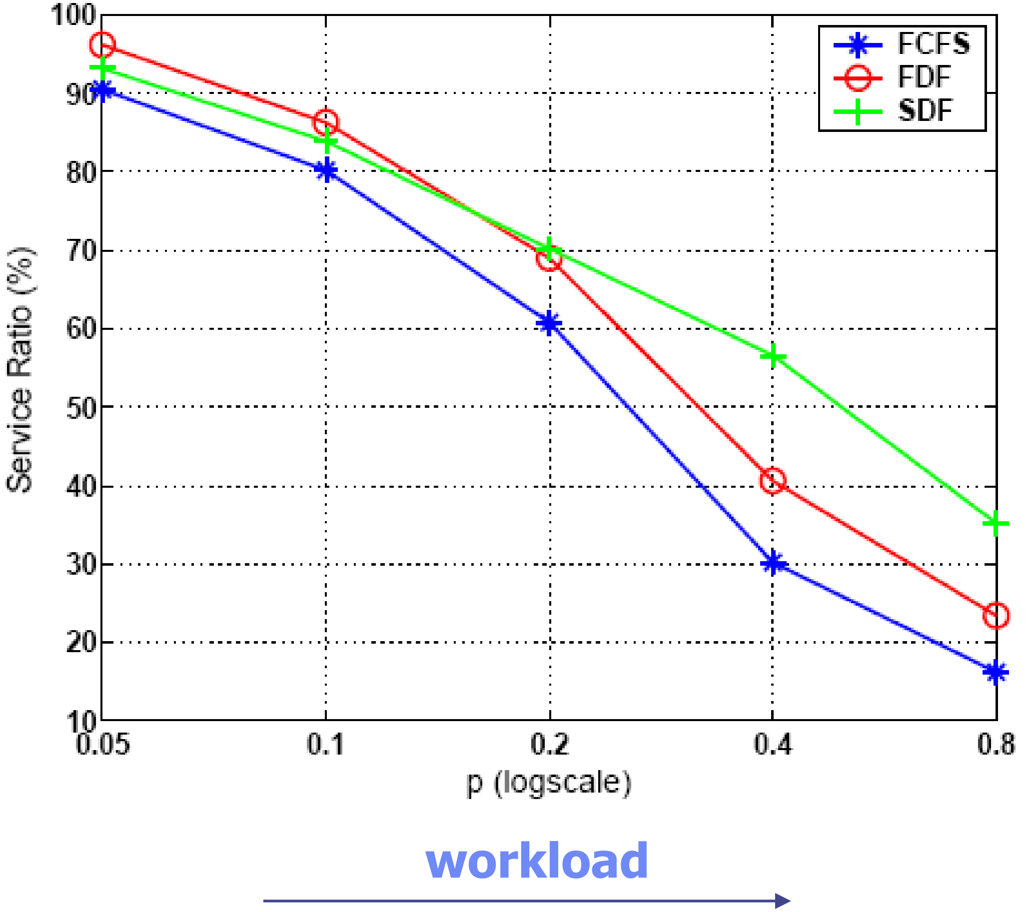
- Location-aware and **deadline-aware**
- The RSU maintains a service cycle
- Service **non-preemptive**

Performance Metrics

- Service Ratio
  - Ratio of the number of requests served **before** the service deadline to the total number of arriving requests.
- Data Quality
  - Percentage of fresh data access
- Tradeoff !!!

Naive Scheduling Policies

- **First Come First Serve** (FCFS): the request with the earliest arrival time will be served first.
- **First Deadline First** (FDF): the request with the most urgency will be served first.
- **Smallest Datasize First** (SDF): the data with a smallest size will be served first.



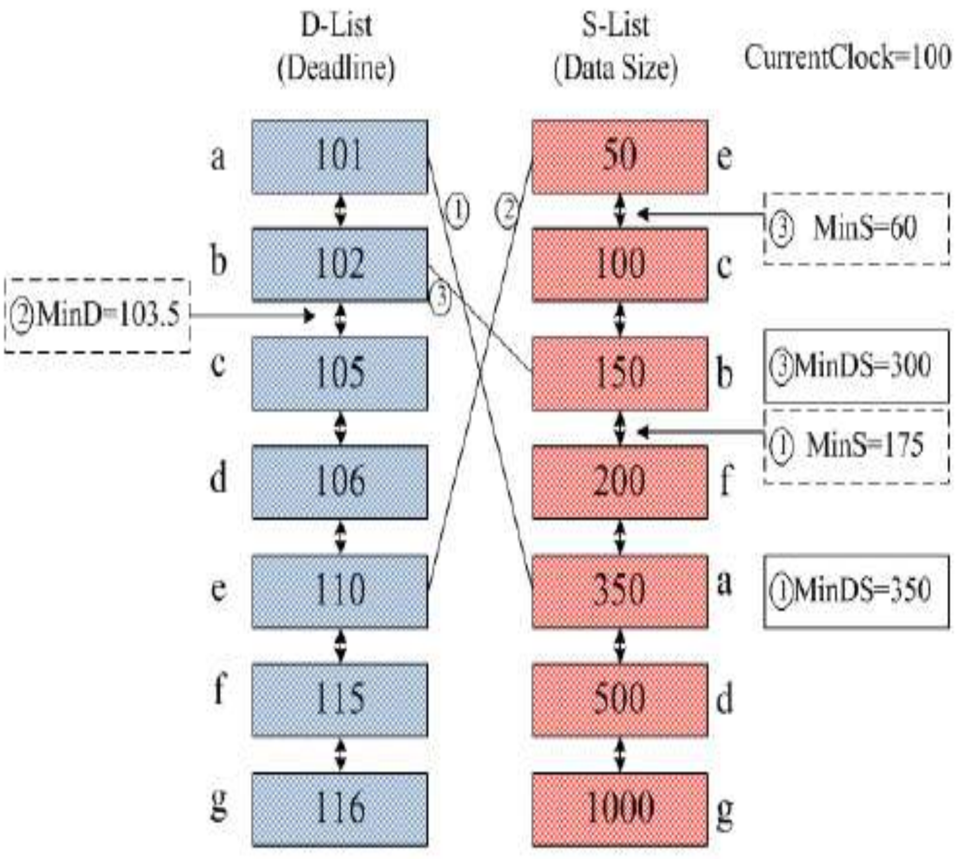
*D*S* Scheduling

- Intuition
  - Given two requests with the same deadline, the one asking for a small size data should be served first
  - Given two requests asking for the data items with same size, the one with an earlier deadline should be served first
- Basic Idea
  - Assign each arrival request a service value based on its deadline and data size, called ***DS_value*** as its service **priority** weight

$$DS\_value = (Deadline - CurrentClock) * DataSize$$

Implementation of *D*S*

- Dual-List
  - Search from the top of D_list
  - Set MinS and MinD
  - Search D_List and S_list alternatively
  - Stops when the checked entry goes across MinD or MinS, or when the search reaches the halfway of both lists.



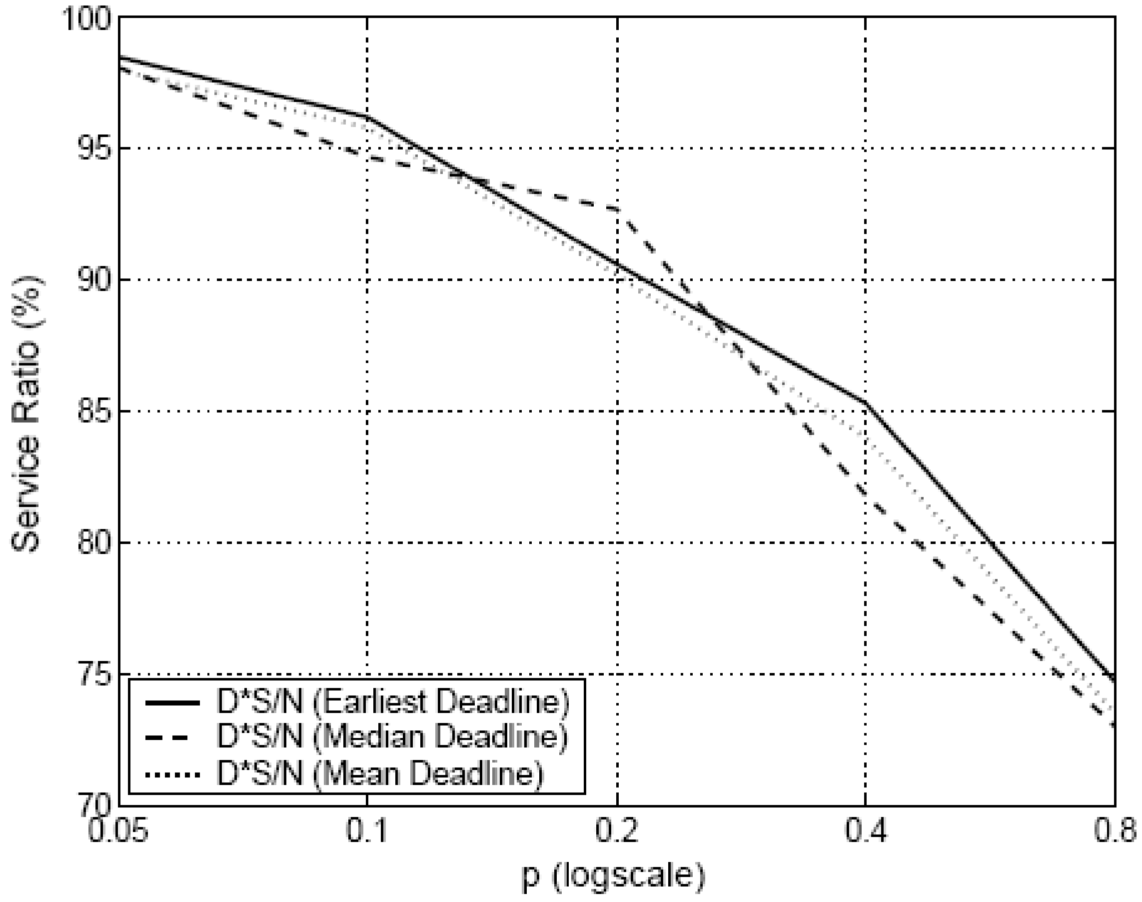
Download Optimization: Broadcasting

- Observation
  - several requests may ask for downloading the same data item
  - wireless communication is broadcast in nature
- Basic Idea
  - delay some requested data and broadcast it before the deadline**s**, then several requests may be served via a single broadcast
  - the data with **more** pending requests should be served first

$$DSN\_value = (Deadline - CurrentClock) * DataSize / Number$$

*D*S/N*: Selection of **Representative** Deadline

- When calculating their *DSN value*, we need to assign each pending request group a single deadline to estimate the urgency of the whole group.



Not too much impact

The Problem of *D*S/N*

- Data Quality !!!

  $DSN\_value = (Deadline - CurrentClock) * DataSize / Number$

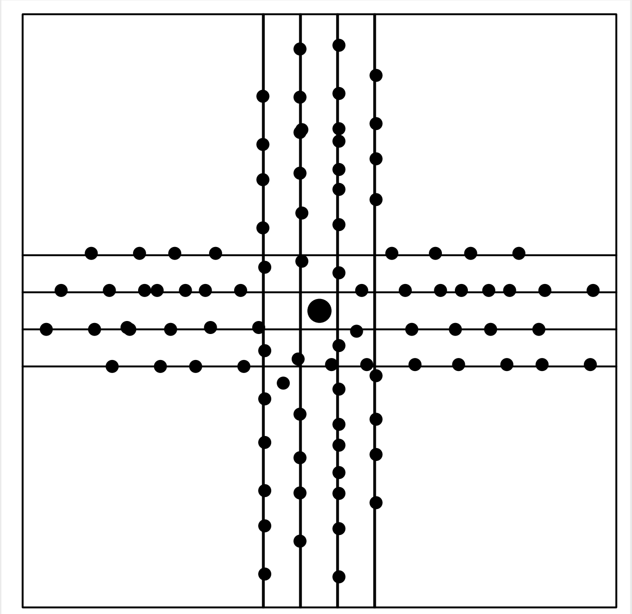
  - For upload request, it is not necessary to maintain several update requests for one data item since only the last update is useful
  - Number value of update requests is always 1, which makes it not fair for update requests to compete for the bandwidth
  - D*S/N can improve the system service ratio but sacrifice the service opportunity of update requests, which degrades the data quality for downloading

Upload Optimization: 2-Step Scheduling

- Basic Idea
  - two priority queues: one for the update requests and the other for the download requests.
  - the data server provides two queues with different bandwidth (i.e., service probability)
- Benefits of Using Two Separate Priority Queues
  - only need to compare the download queue and update queue instead of individual updates and downloads
  - update and download queues can have their own priority scheduling schemes

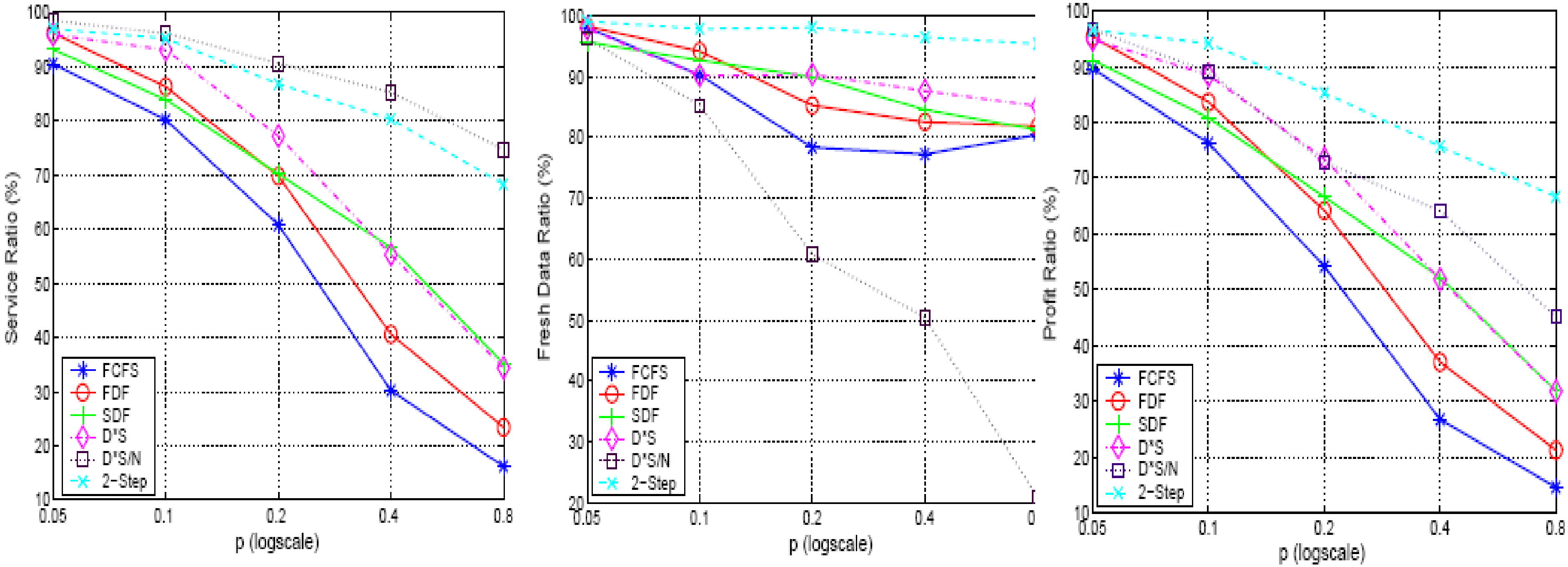
Simulation Setup

- NS-2 based
- 400m*400m square street scenario
- One RSU server is located at the center of two 2-way roads
- 40 vehicles randomly deployed on each lane
- Each vehicle issues request with a probability *p*
- Access pattern of each data item follows *Zipf* distribution



Parameter	Value
Simulation Time	900s
Transmission Rate	$5Mbit/s = 625Kbyte/s$[11]
Vehicle Velocity	15m/s
Wireless Coverage	200 m
Data size	50K $\sim$ 5M, average 2.5M
Vehicle-Vehicle Space	20m
Data set size	25
Zipf Parameter θ	0.8
Update Percentage	10%
Adaptation Window	40s

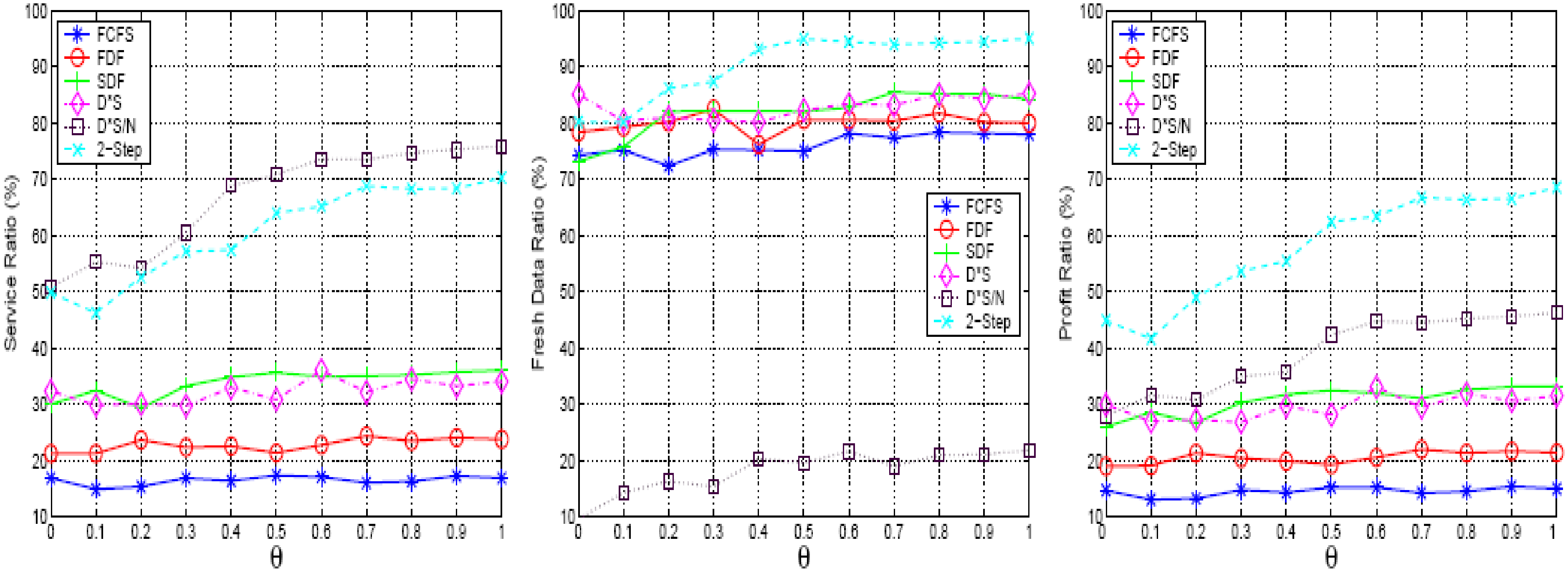
Effect of Workload



(a) Service Ratio (b) Fresh Data Ratio (c) System Profit ($\alpha = 0.5$)

As workload increases, *D*S/N* can achieve the highest service ratio while its data quality degrades dramatically

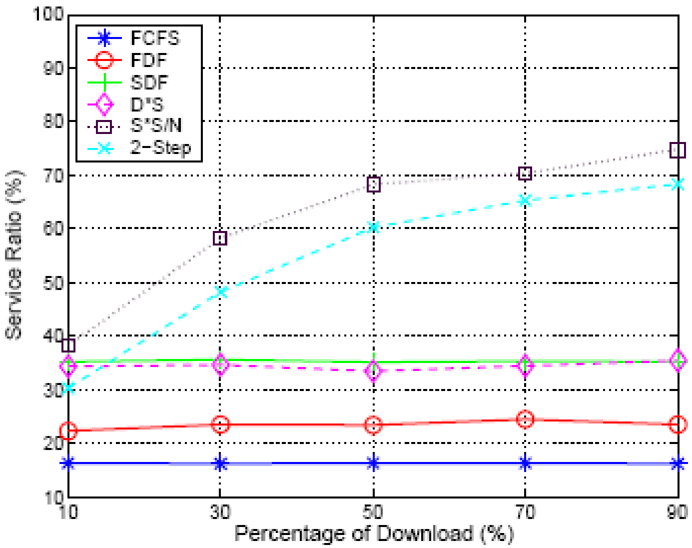
Effect of Access Pattern (θ)



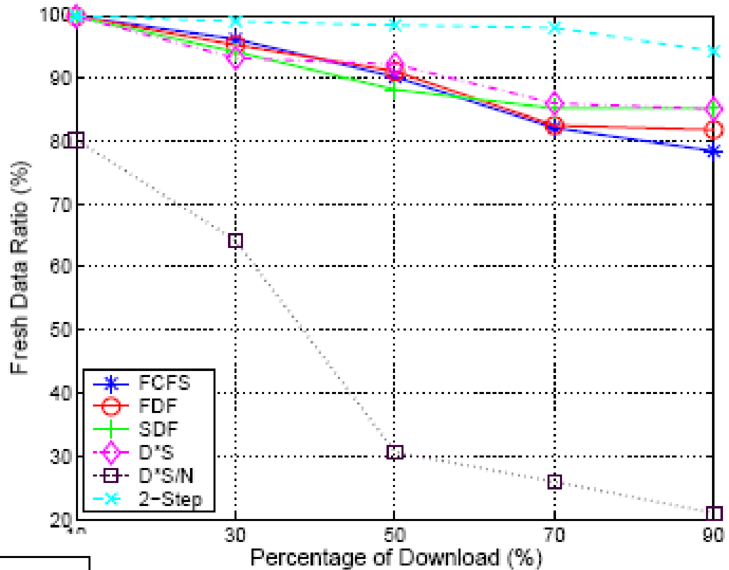
(a) Service Ratio (b) Fresh Data Ratio (c) System Profit ($\alpha = 0.5$)

- Change of θ does not have too much impact on the performance of FCFS, FDF, SDF and D*S
- D*S/N and 2-Step can benefit from the skewness of the data access pattern with the increase of θ

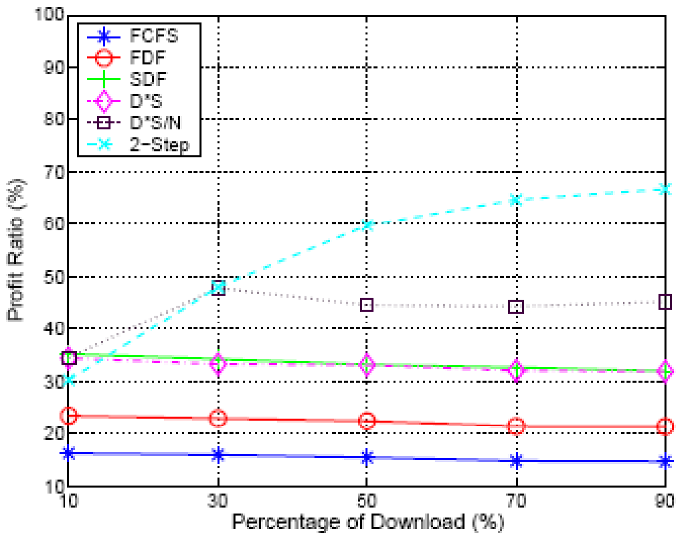
Effect of Access Pattern
(*Download/Update Ratio*)



(a) Service Ratio

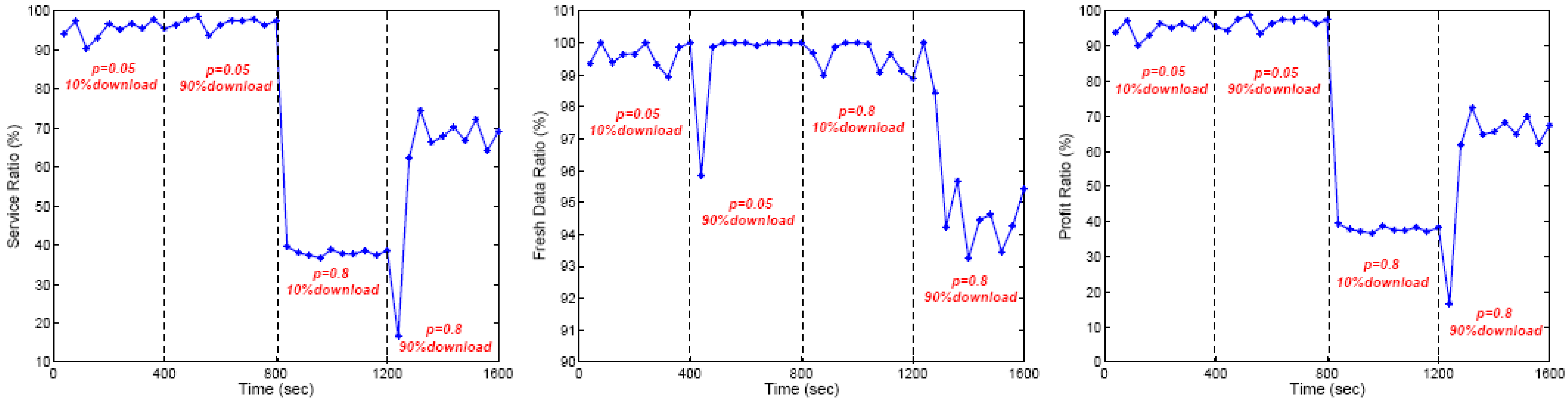


(b) Fresh Data Ratio



(c) System Profit ($\alpha = 0.5$)

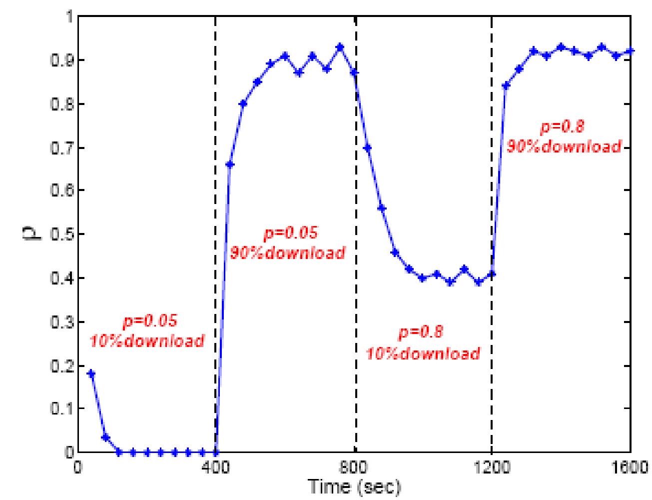
Adaptivity to Workload Condition Change



(a) Service Ratio (b) Fresh Data Ratio (c) System Profit($\alpha = 0.5$)

•2-Step scheme can achieve good performances in almost all scenarios.

• ρ adapts quickly when workload condition changes



(d) ρ

Outline

- DSCR and collision warning
- Data access
- **Broadcast and routing**
- Information dissemination
- Address configuration
- Security

V2V Applications: End-to-End or Broadcast-Based?

Mario Gerla, ACM VANET 2007 Panel

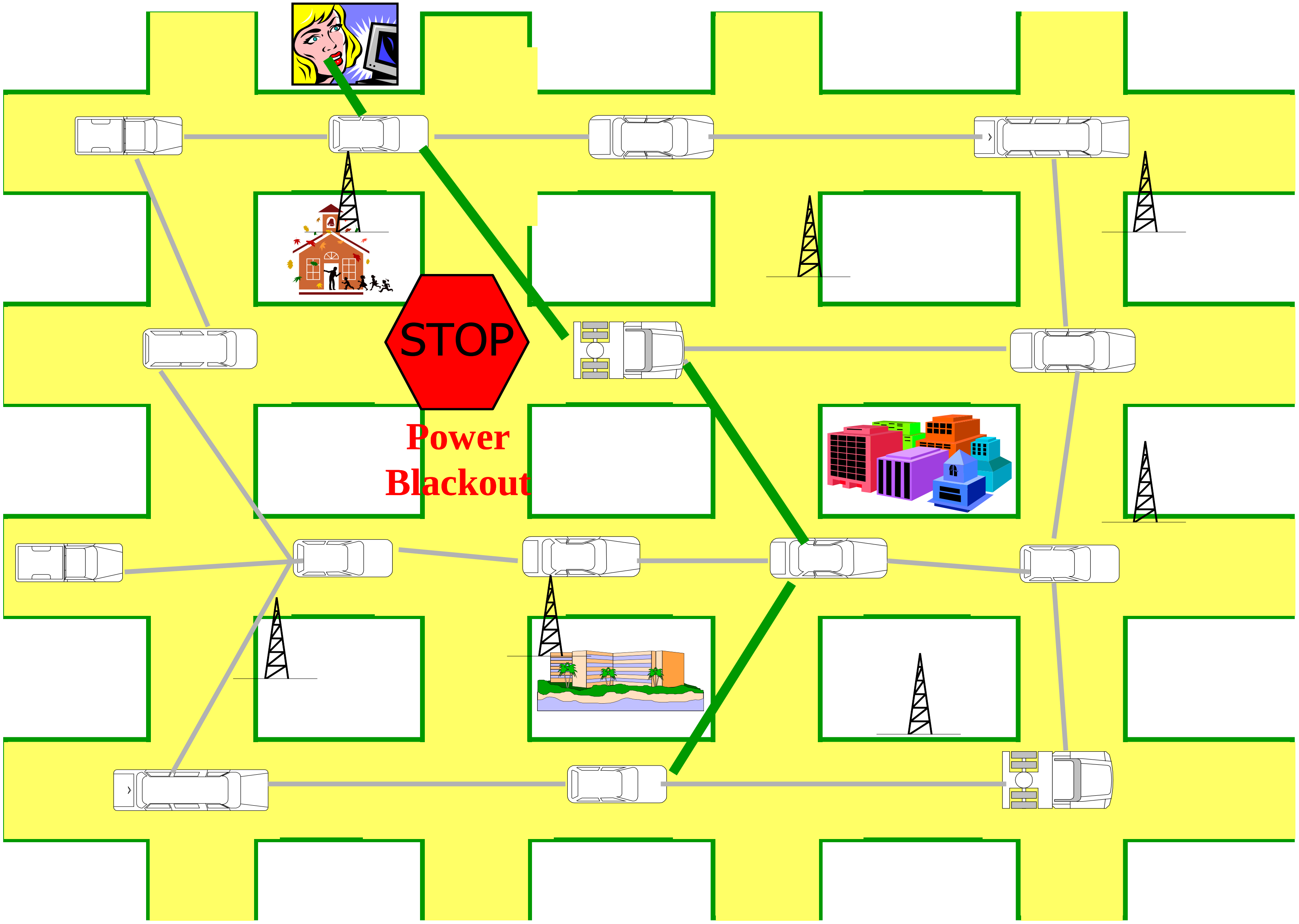
End-to-End vs. Broadcast

- VANET E2E networking (without infrastructure) extremely challenging:
  - An urban VANET may have over 100,000 nodes
  - Nodes move in unpredictable ways
  - End-to-end routing is hard
    - AODV and OLSR do not scale
    - Geo-routing can get trapped in "dead ends"
    - Geo Location Service not very scalable
  - TCP over several hops "in motion" is a nightmare!
  - Intermittent connectivity in most cases
- So, end-to-end applications are hard to deploy
- However....

Where Are the E2E Applications?

- Very few urban scenarios/applications require "true" E2E networking:
  - Emergency, disaster recovery (*e.g.*, earthquake, terrorist attack, etc.)
  - Urban warfare
- Generally, these are situations where the infrastructure has failed
- In these cases, …

Vehicular Grid as Emergency Net



Broadcast Based Applications

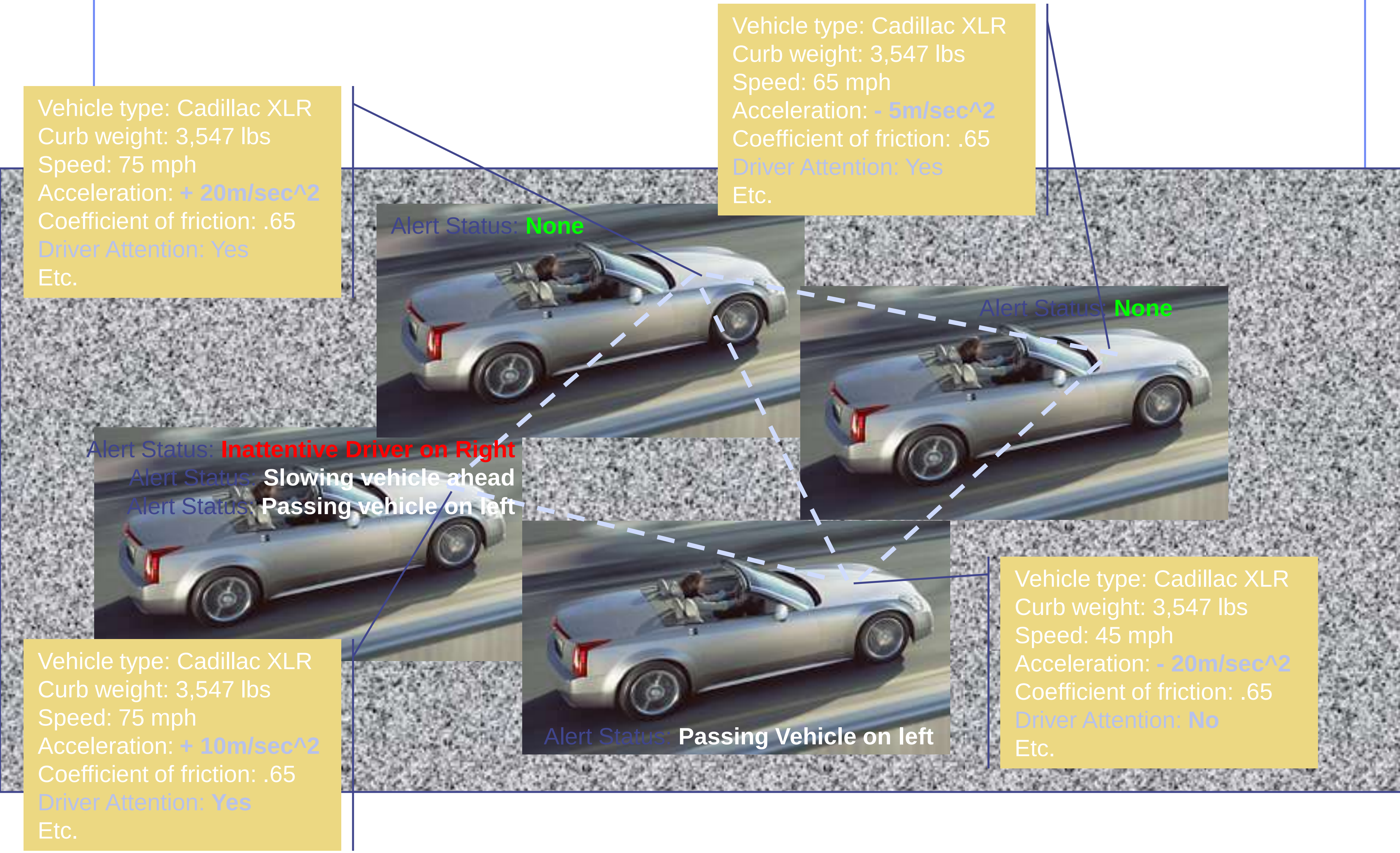
- The most popular VANET applications are "broadcast" based
  - Safe navigation - neighborhood broadcast
  - Content sharing - P2P proximity routing
  - Distributed urban sensing - epidemic dissemination

Leading V2V Application

safe, efficient driving to reduce casualties

- Vehicle-2-Vehicle communications
- Vehicle-2-Roadway communications
- Intelligent Highway (*e.g.*, platooning)
- Intersection Collision Warning
- Etc.

Car-to-Car Broadcast for Safe Driving



Location Aware Content

infotainment

- Location relevant multimedia files
  - Local ads
  - Local news
  - Tourist information
  - Video clips of upcoming attractions
  - etc.

Incentive for V2V Communications

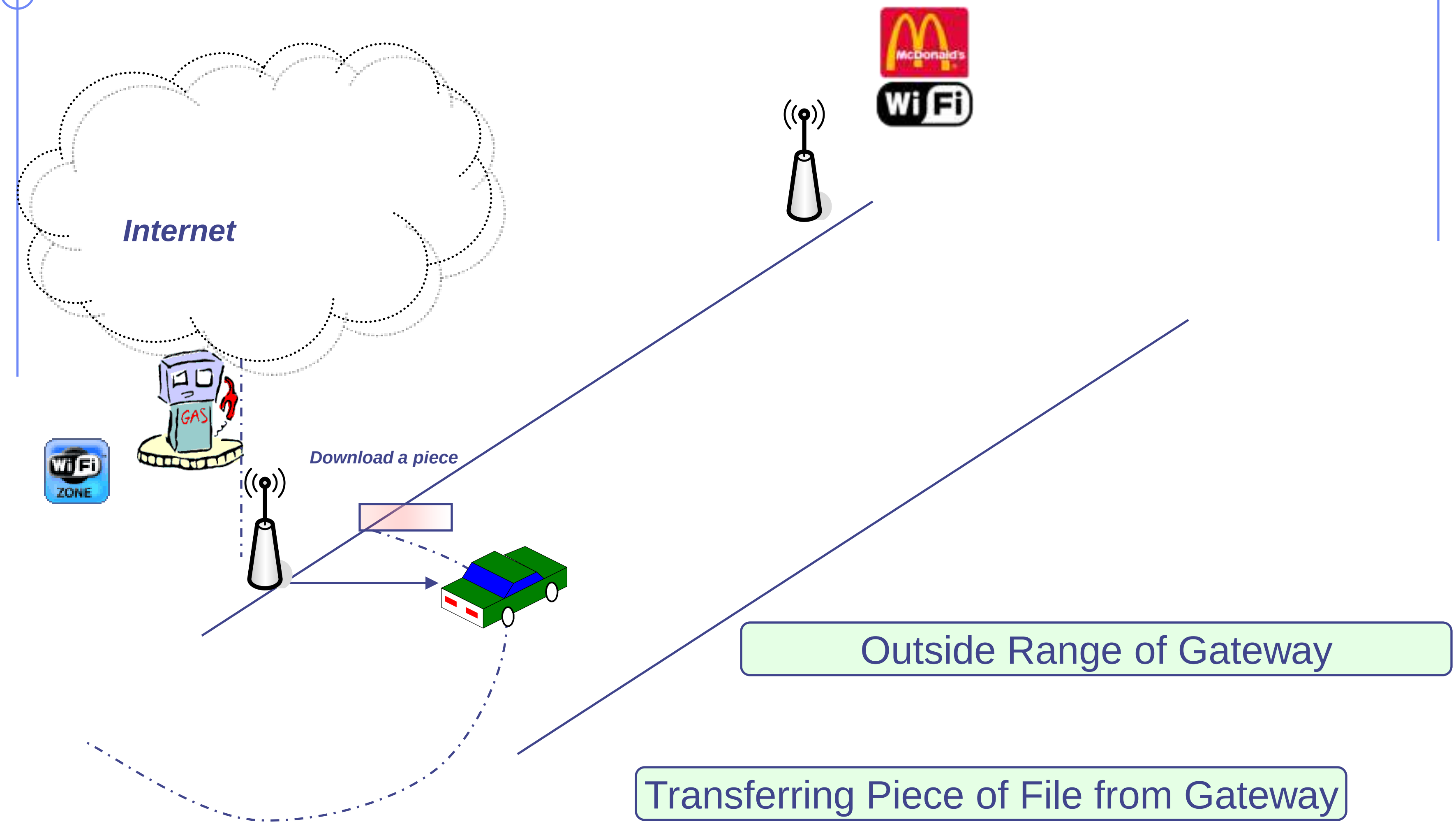
Problems:

- Every car stopping at gas station for full download is a nuisance
- Downloading from GPRS/3G too slow and quite expensive

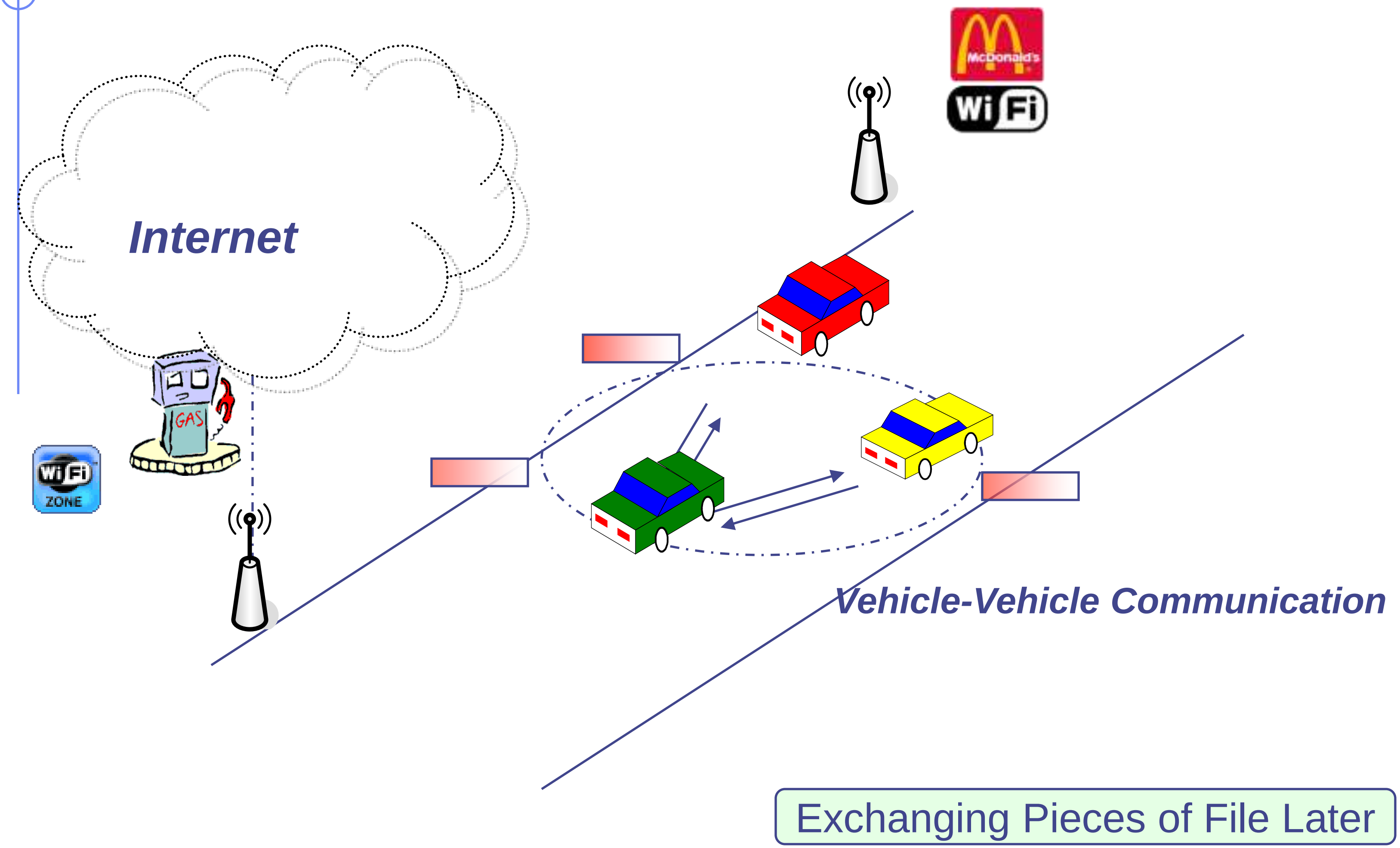
Observation: many other drivers are interested in download sharing (like in the Internet)

Solution: cooperative P2P downloading

CarTorrent: Basic Idea



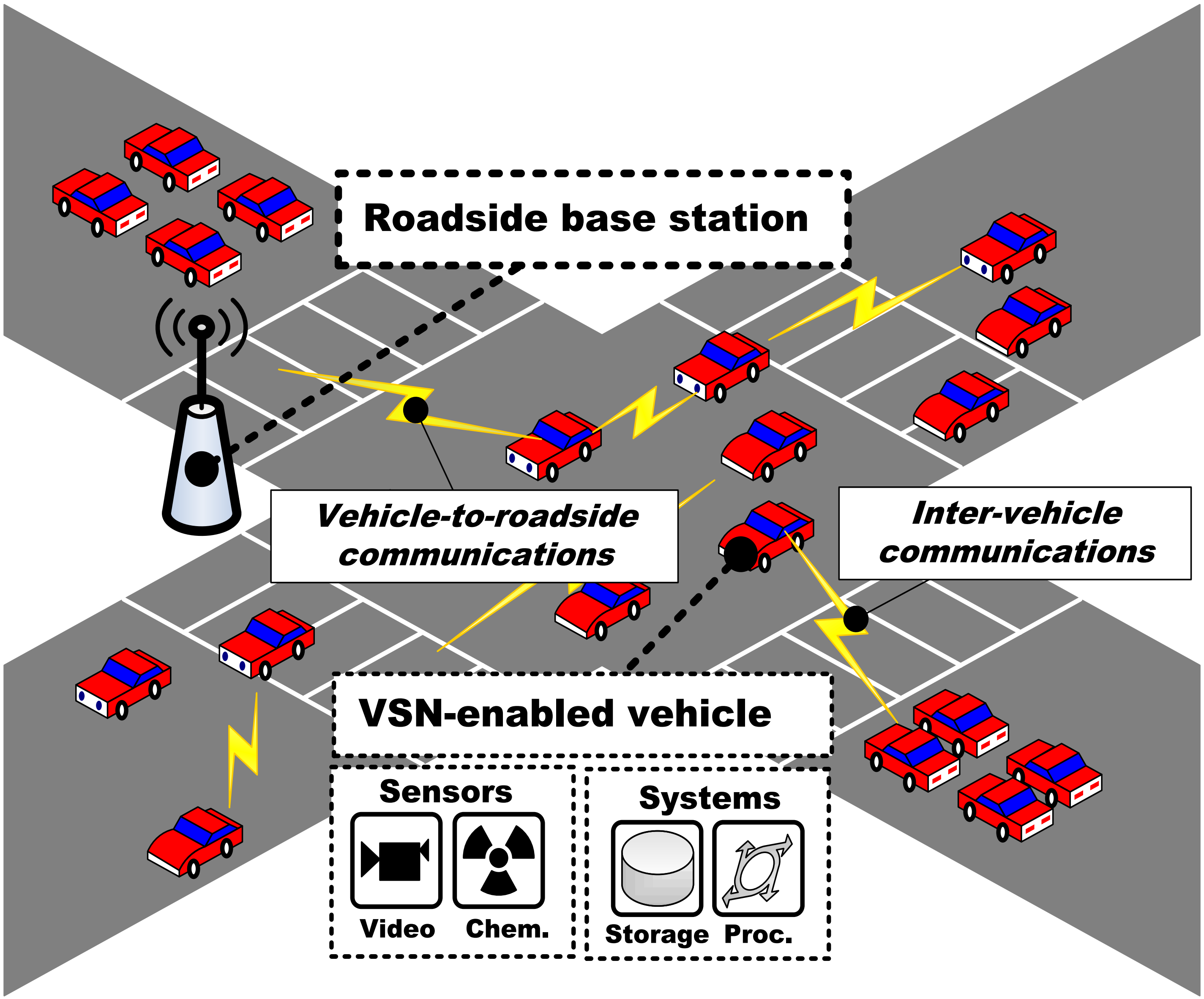
Cooperative Download: CarTorrent



Environment Sensing/Monitoring

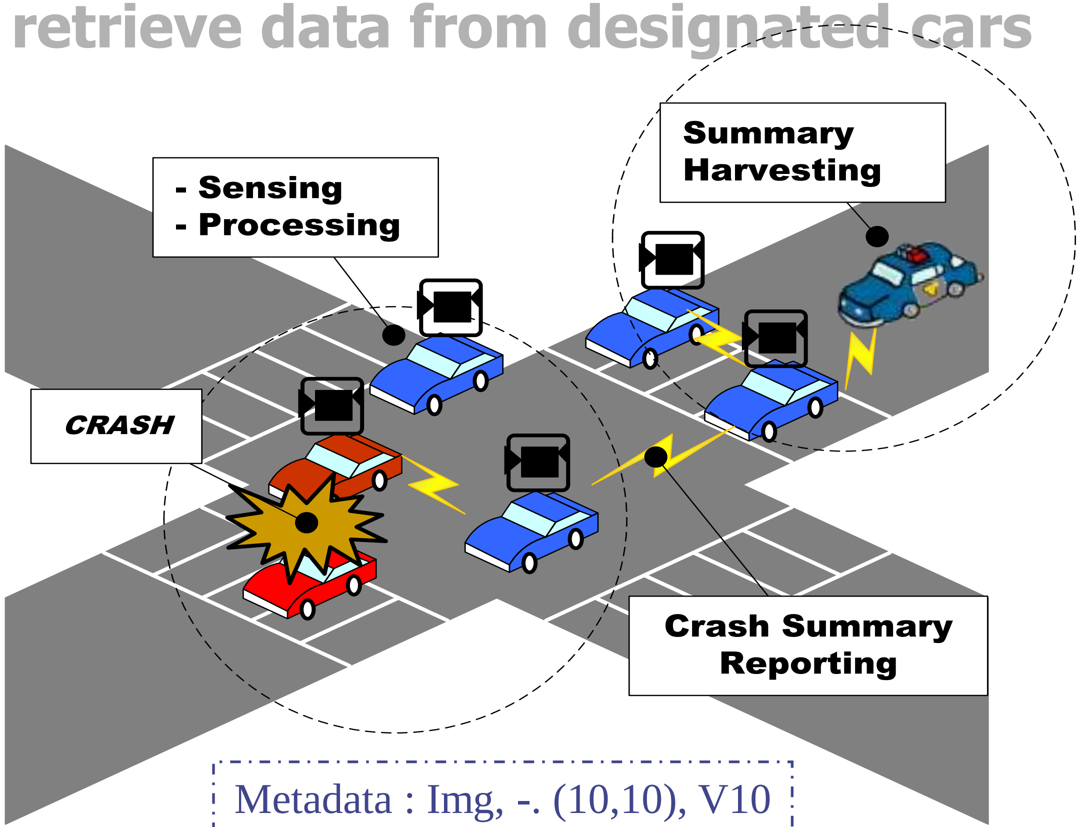
- Pavement conditions (eg, potholes)
- Traffic monitoring
- Pollution probing
- Pervasive urban surveillance
- "Unconscious" witnessing of accidents/crimes

Vehicular Sensor Network



Accident Scenario: Storage/Retrieval

- **Designated Cars (eg, busses, taxicabs, UPS, police agents, etc):**
  - Continuously **collect** images on the street (store data locally)
  - Process the data and **detect** an event
  - **Classify the event as Meta-data** (Type, Option, Location, Vehicle ID)
  - **Epidemically disseminate ->** distributed index
- **Police retrieve data from designated cars**



How to Retrieve Data?

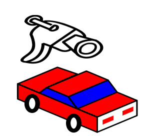
Two main options:

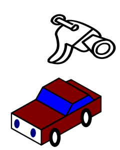
- Upload to first AP within reach (Cartel project, MIT)
- "Epidemic diffusion":
  - *Mobile nodes* periodically broadcast *metadata* of events to their neighbors
  - A *mobile agent* (the police) queries nodes and harvests events
  - Data dropped when stale and/or geographically irrelevant

Both options are broadcast based!

Epidemic Diffusion

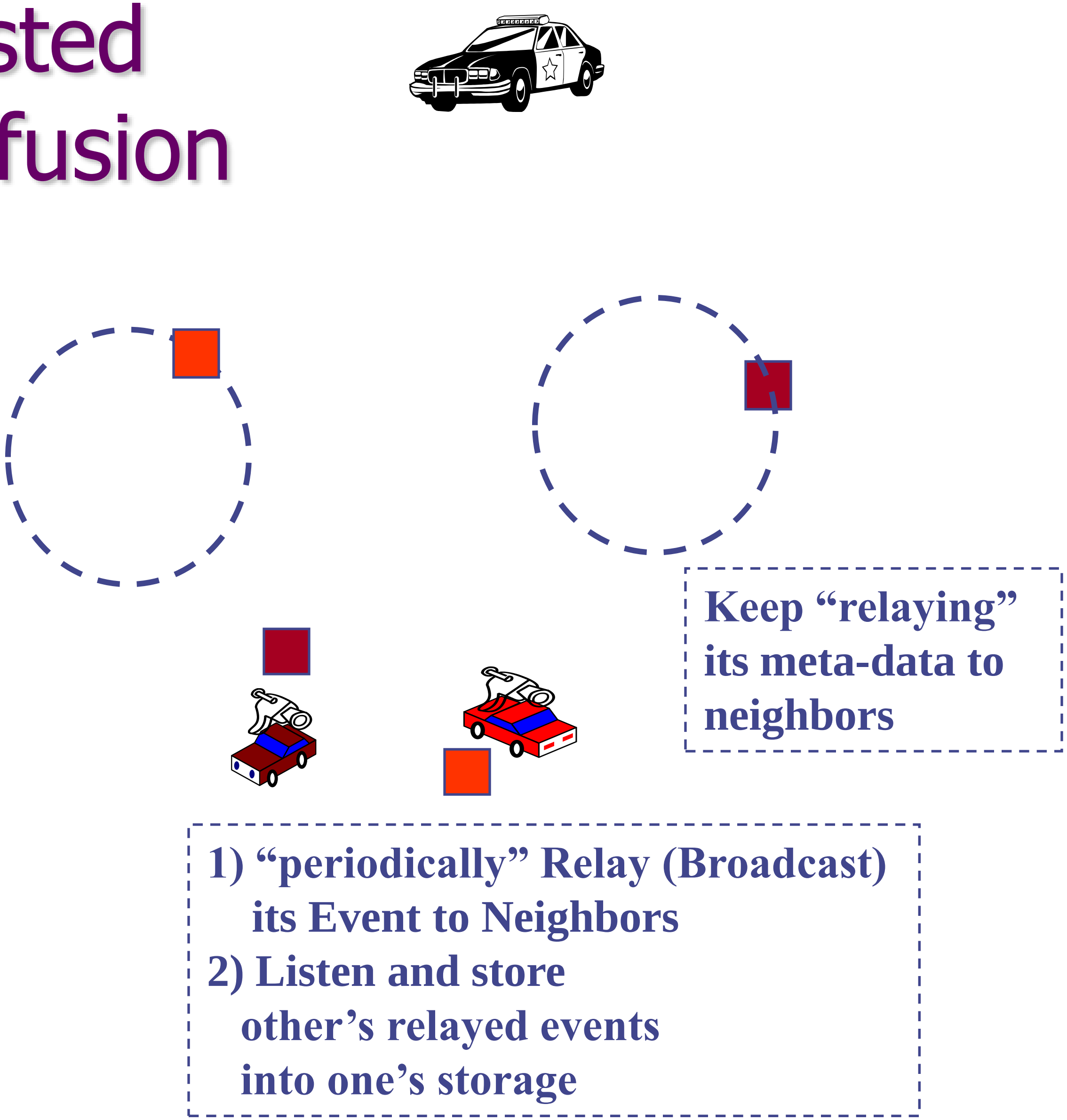
Mobility-Assisted Metadata Diffusion



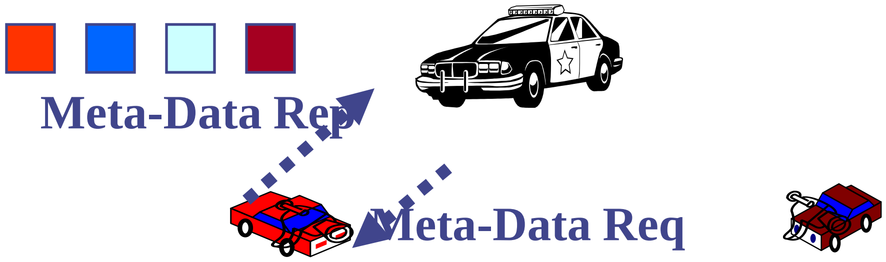


Epidemic Diffusion

Mobility-Assisted Metadata Diffusion



Epidemic Diffusion
Mobility-Assisted Metadata Harvesting



1. Agent (Police) harvests Meta-Data from its neighbors
2. Nodes return all the meta-data they have collected so far

Open Issues

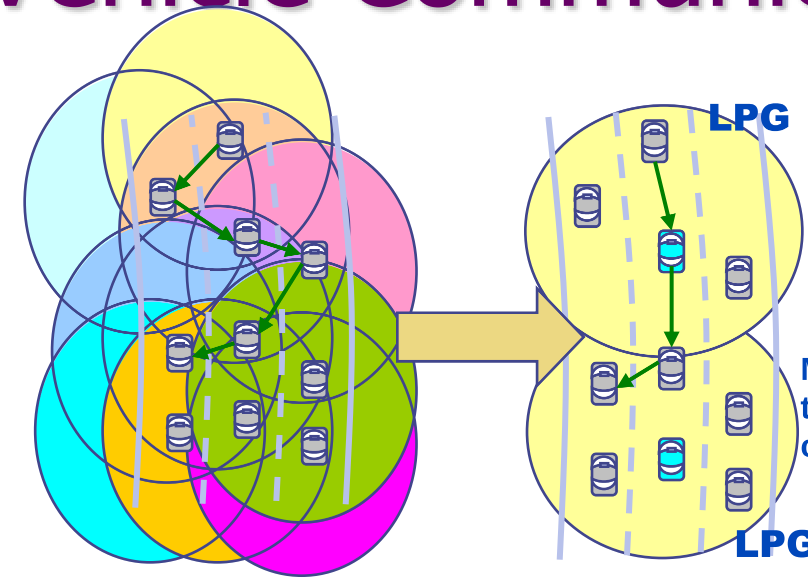
- Future VANET applications will be broadcast, proximity routing based
- However, proximity and broadcast only remove the E2E complexity
- Enormous challenges still ahead:
- Navigation safety
  - "liability" stigma
  - strict delay constraints
- Location aware content, Infotainment
  - Driver distraction -> more accidents???
  - Virus scare!!!
- Urban Sensing
  - Business model not clear (who makes money?)
  - Privacy issues

Integrated Local Peer Group (LPG) Organization and Routing

Wai Chen, Jasmine Chennikara-Varghese, Taek-Jin Kwon, Toshiro Hikita, and Ryokichi Onishi, IEEE AutoNet, 2006

LPG-Based Vehicle Communications

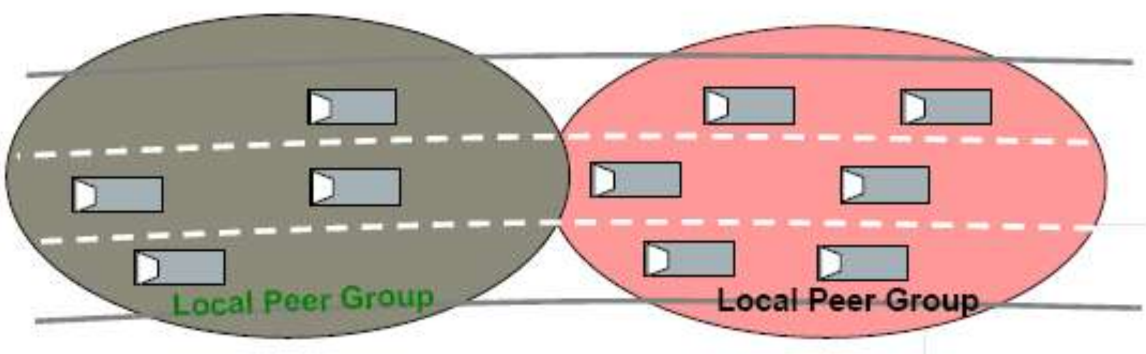
Message flooding; Transmission interference



- Objective: Investigate vehicle group based technology for multi-hop vehicle communications
  - For safety communications (e.g. smooth lane change, emergency warning of braking, intersection crossing)
- Deliver messages quickly and efficiently in vehicle groups and stop messages at group boundary *(Intra-group communication)*
- When necessary, pass messages to other groups *(Inter-group communication)*

LPG Approach

- Use LPGs to organize neighboring vehicles
- Embed some coordination among vehicles to support media access control, routing, multicast operations:
  - Tight coordination (within LPG)
  - Looser coordination (among LPGs)
- LPG can adapt to remain reasonable size (e.g., number of hops)
  - Support merging and splitting of groups
- Within each LPG, one-hop and multi-hop communication supported
- Group association does not change while within the same LPG

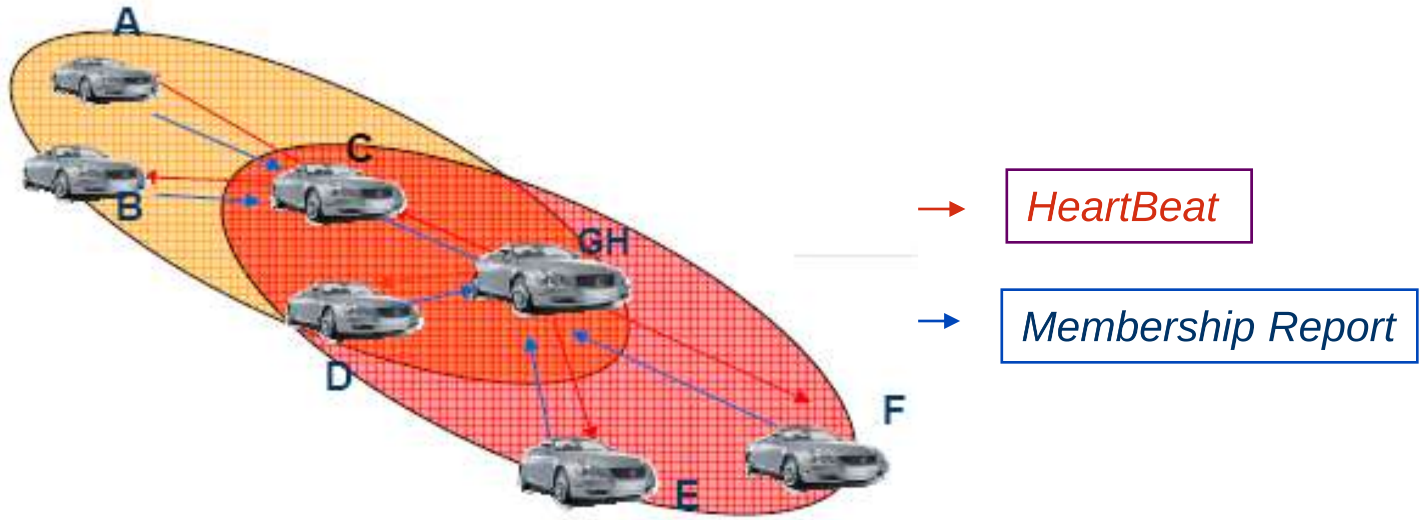


Group-Header Based LPG Organization

- LPG Identity:
  - Created by the group header (GH) within LPG
  - LPG is identified by an LPG ID plus the GH ID
  - When a group splits, LPG ID may be duplicated but GH ID is different
- Group Header (GH)
  - This node creates and maintains identity for LPG
  - GH handles changes in LPG membership
- Group Node (GN)
  - Node in LPG which is not a group header
  - Periodically sends status to GH to continue being part of the LPG
  - Can become a GH if current GH disappears

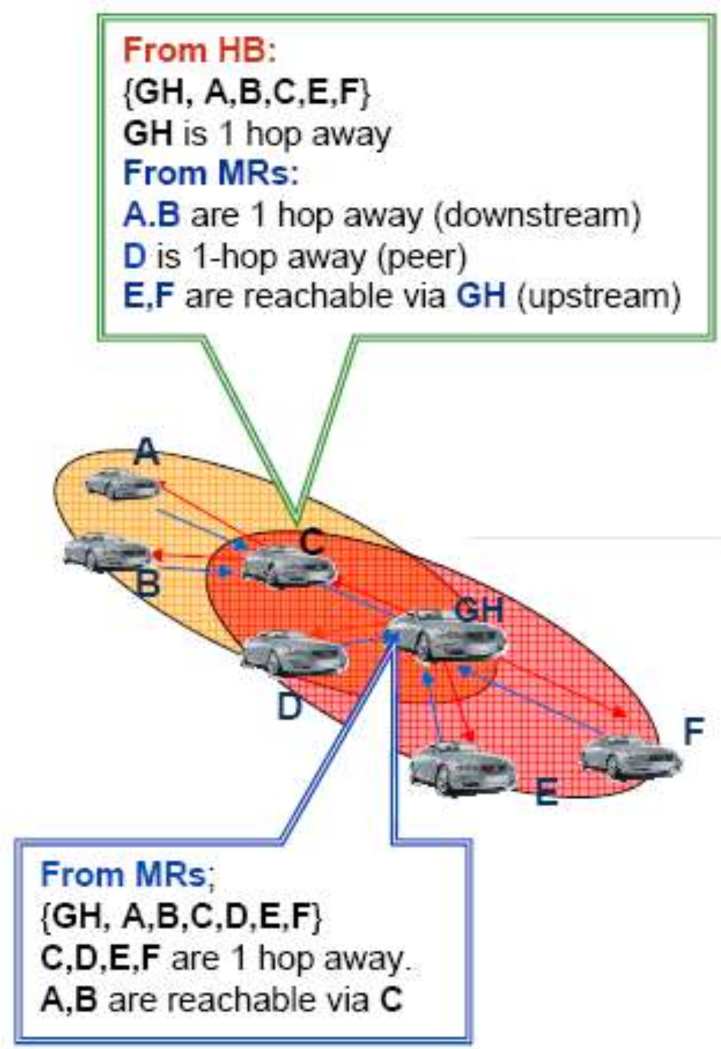
LPG Control Messages

- GH periodically broadcasts HeartBeat (HB) with LPG ID, GH info and member list of LPG
  - HB forwarded by all nodes until max Hop Count (HC) reached
- GNs respond to the HB with a Membership Report (MR) to maintain membership in the LPG
  - MR relayed back by nodes to GH following reverse path of HB

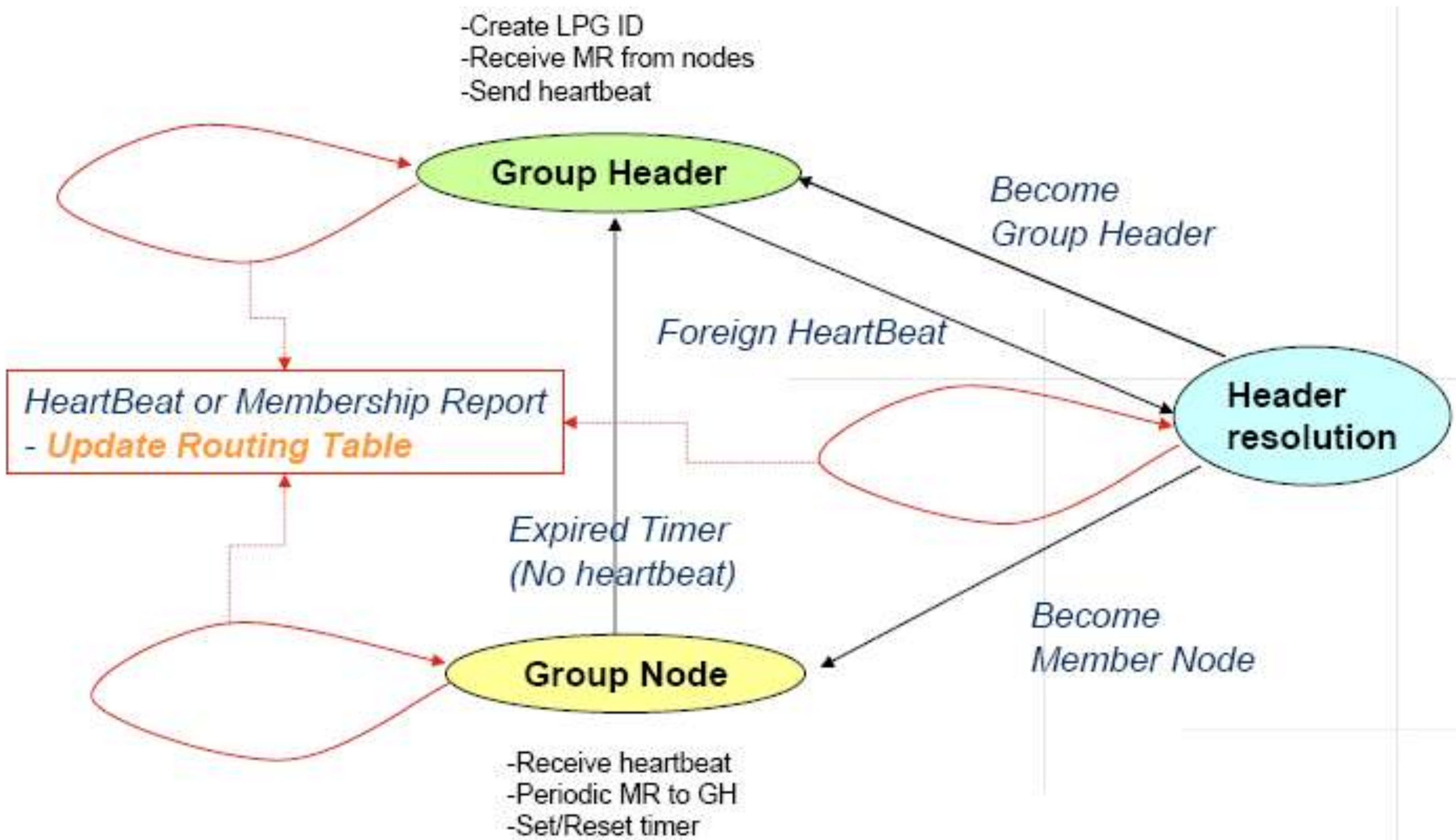


LPG-based Routing Protocol (LBR)

- Use existing LPG control messages
- From fresh HB get member list
  - Include members in routing table
  - Extract next-hop info toward GH from HB
  - Default next-hop to every other node is set as GH
- From overheard duplicate HB
  - Determine peer nodes
  - Determine upstream nodes based on the HC
- From overheard MR
  - Intermediate nodes to GH can collect downstream node info
  - Originating node of MR and next-hop to reach originating node of MR
- Routing entries updated every HB cycle

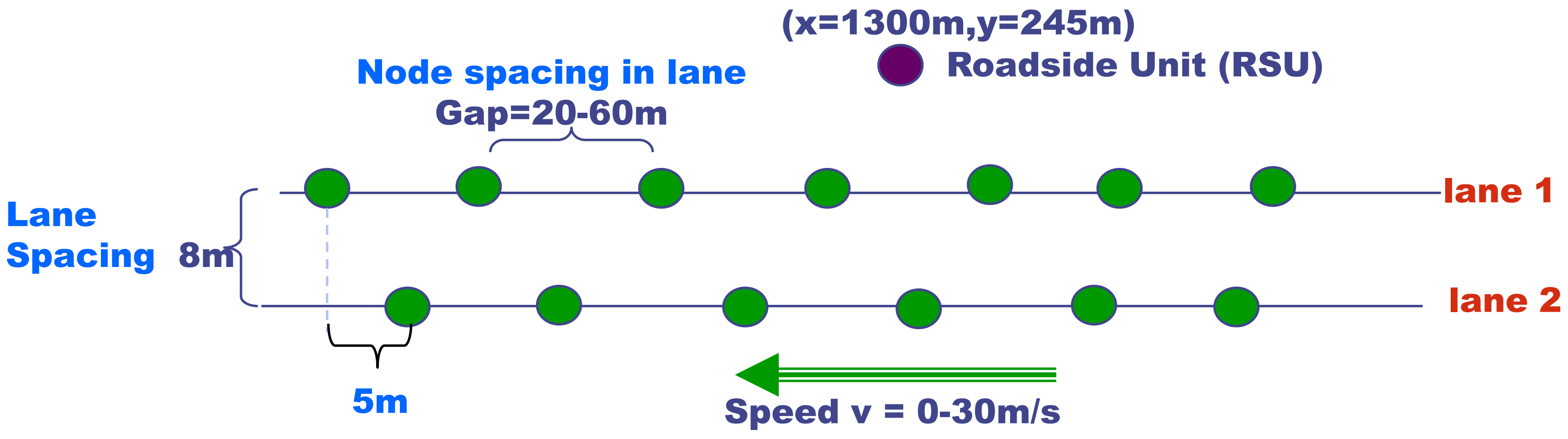


LPG/LBR State Machine



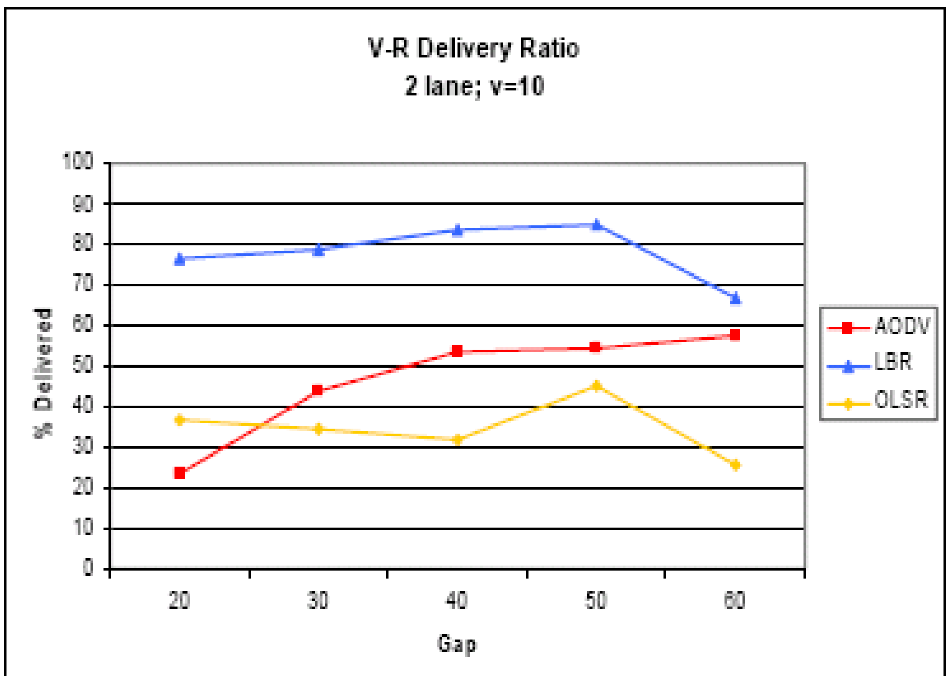
Scenario: Vehicle to Roadside Unit

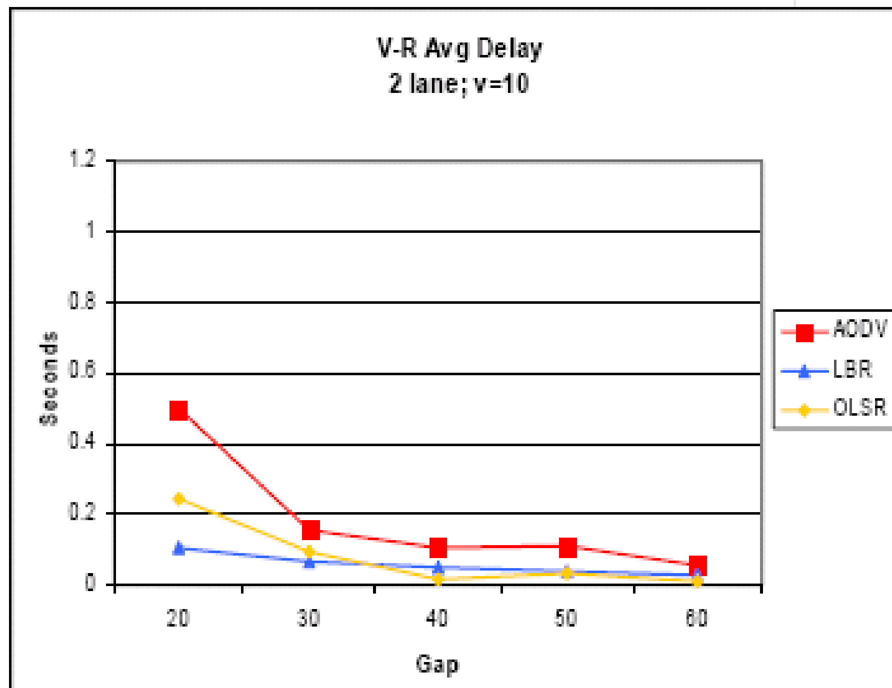
- Nodes per lane vary from 16 (gap=60m) to 46 (gap=20m)
- 802.11a radio
- Nodes send CBR to fixed RSU
  - CBR rate 5pkts/sec; packet size 512bytes



V-R: 2 Lane

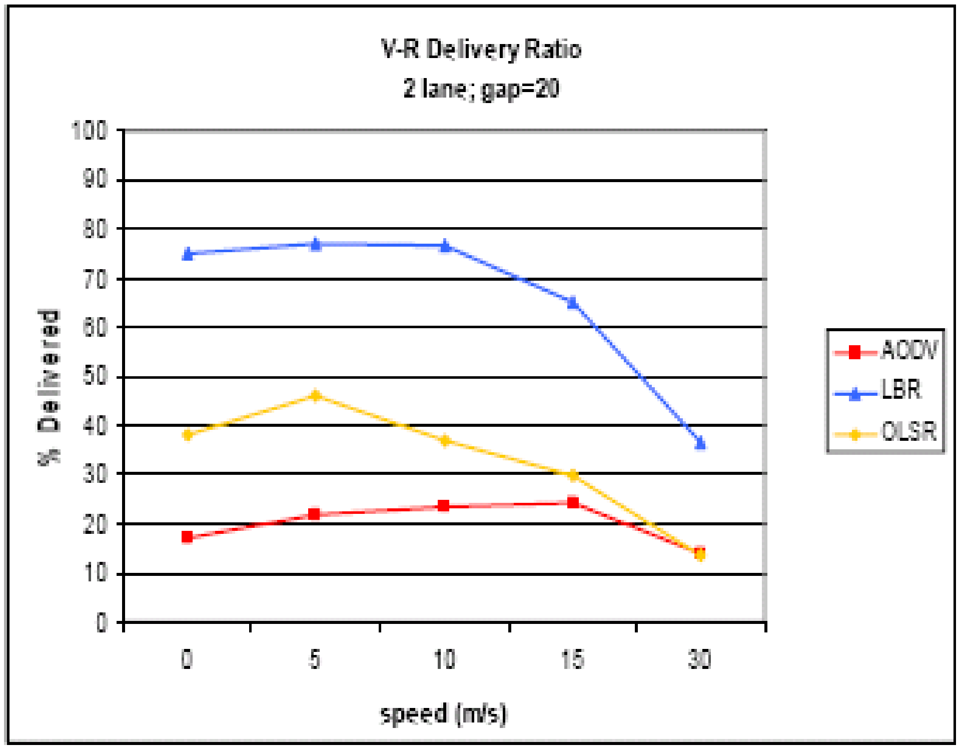
Delivery Ratio and Average Delay *speed=10m/s*; vary gap

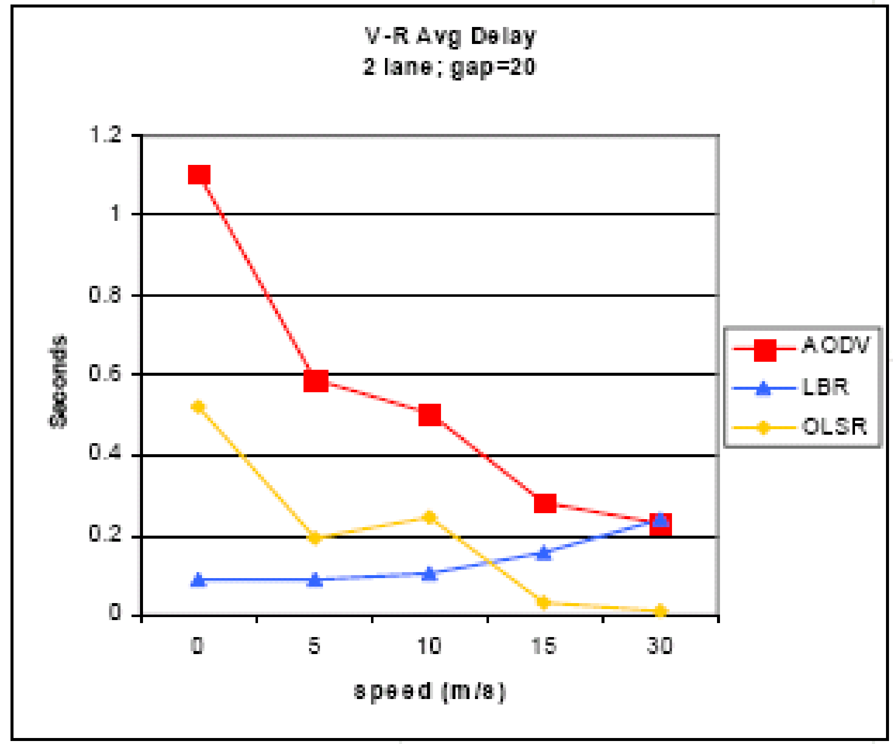




V-R: 2 Lane

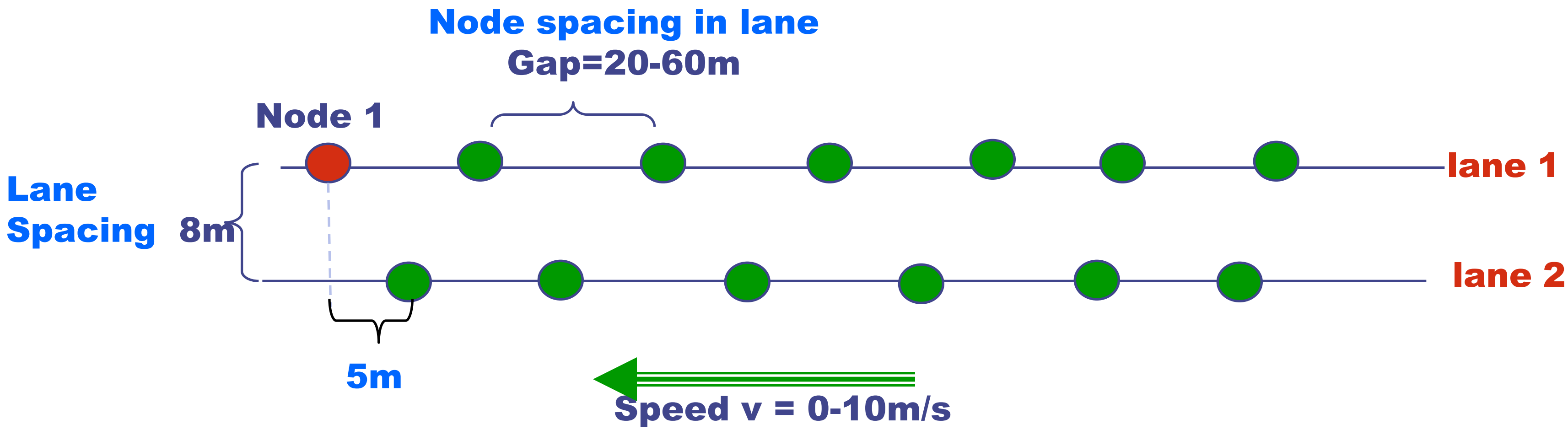
Delivery Ratio and Average Delay vary speed; *gap=20m*





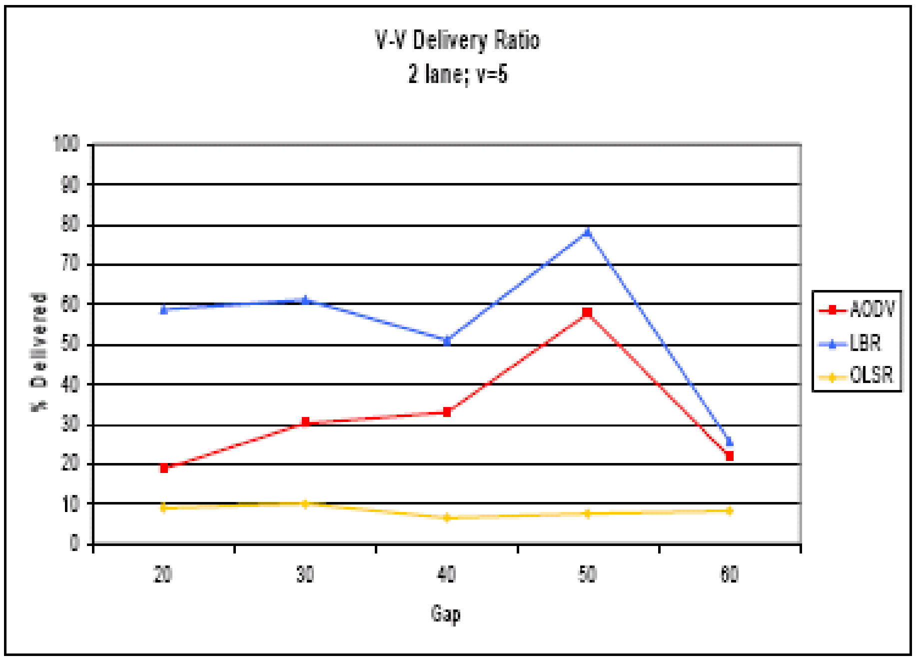
Scenario: Vehicle to Vehicle

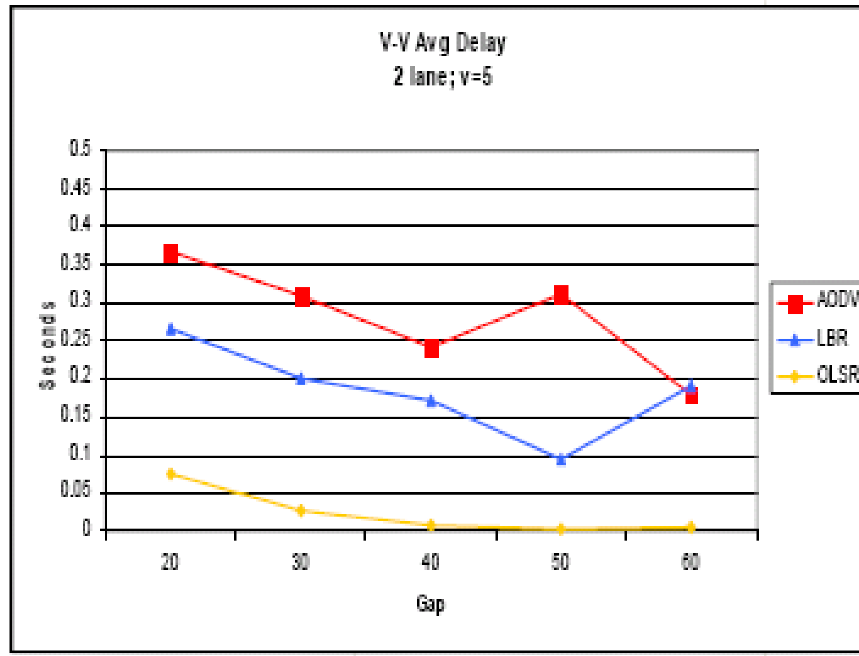
- Node 1 sends a CBR stream to each node
  - CBR rate 2pkts/sec; packet size 512bytes



V-V: 2 Lane

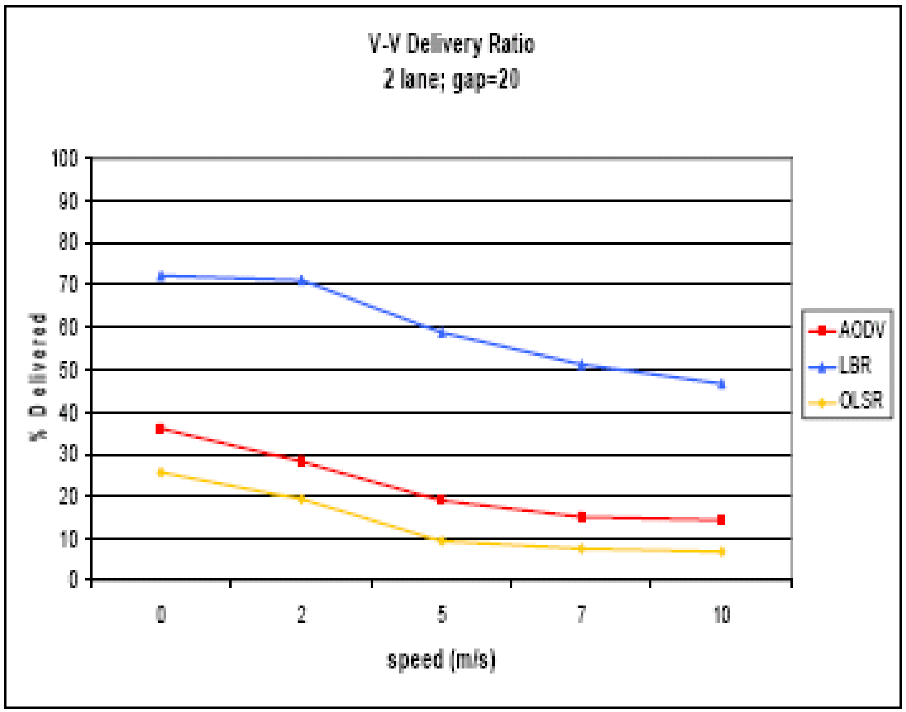
Delivery Ratio and Average Delay *speed=5m/s*; vary gap

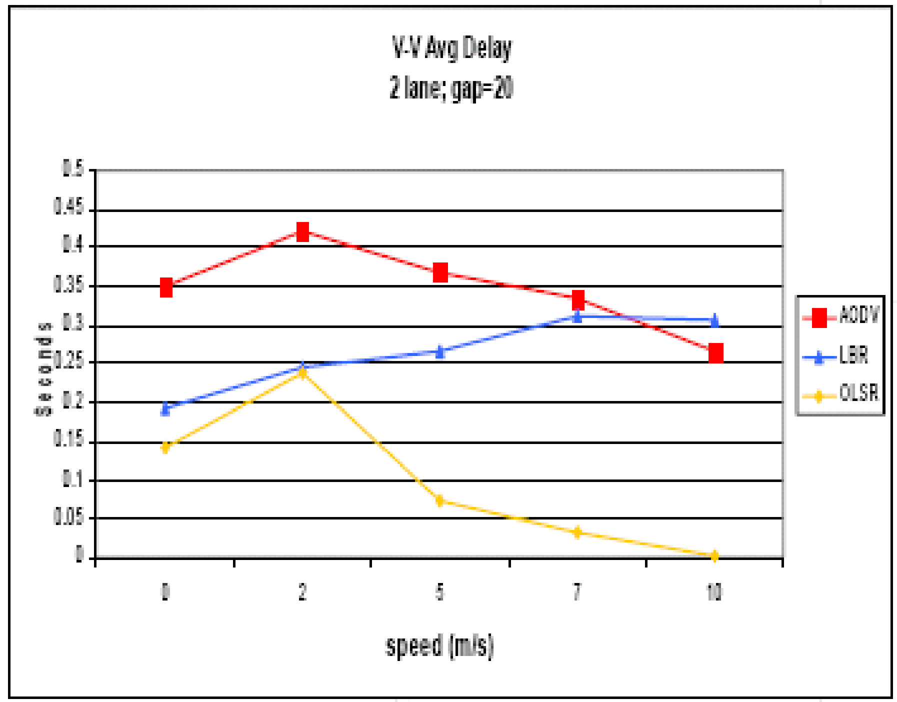




V-V: 2 Lane

Delivery Ratio and Average Delay vary speed; *gap=20m*





A Static-Node Assisted Adaptive Routing Protocol in Vehicular Networks

Yong Ding, Chen Wang, and Li Xiao, ACM VANET, 2007

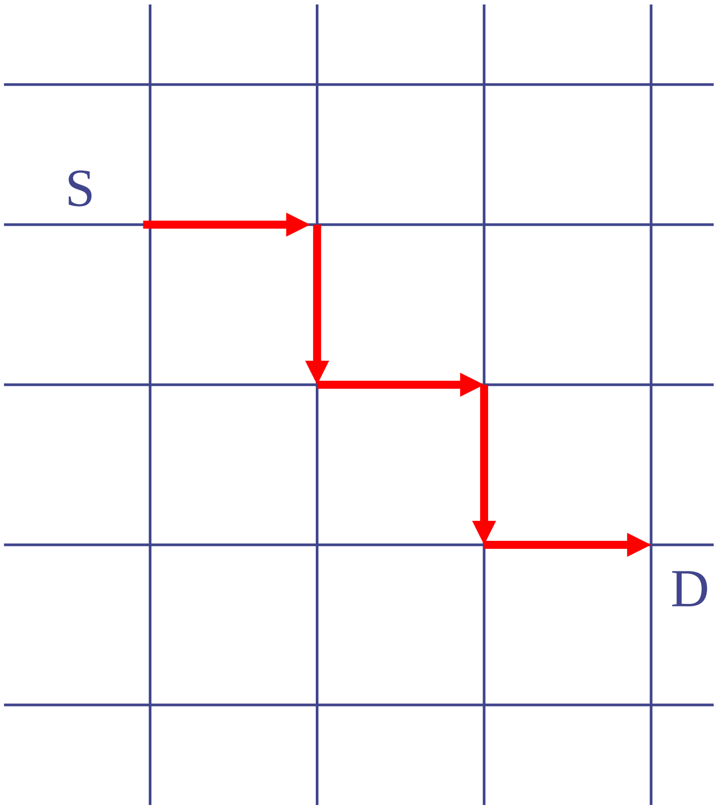
Background

- Many potential useful applications envisioned in vehicular networks
  - Safety applications
  - Real-time traffic estimation for trip planning
  - Media content sharing
  - Improving sensing coverage
  - Delivery networks
    - Transfer data from remote sensor-nets to Internet services
    - Vehicles send queries to remote sites (gas station, restaurant, etc.)

Multi-hop routing protocol is needed.

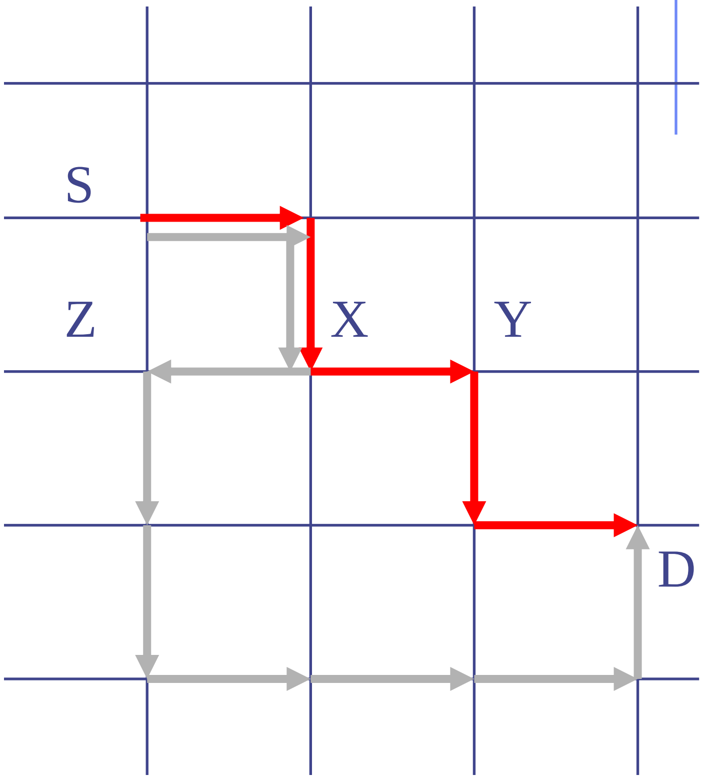
Background

- Multi-hop routing protocols in vehicular networks
  - MDDV [VANET'04], VADD [Infocom'06]
- Basic Idea
  - Use geographic routing
  - **Macro** level: packets are routed intersection to intersection
  - **Micro** level: packets are routed vehicle to vehicle



Motivation

- Under high vehicle densities
  - Both MDDV and VADD work well
- Under **low vehicle densities**
  - When a packet reaches an intersection, there might not be any vehicle available to deliver the packet to the next intersection at the moment.
  - MDDV: not considered
  - VADD: Route the packet through the best currently available path
    - A **detoured path** may be taken



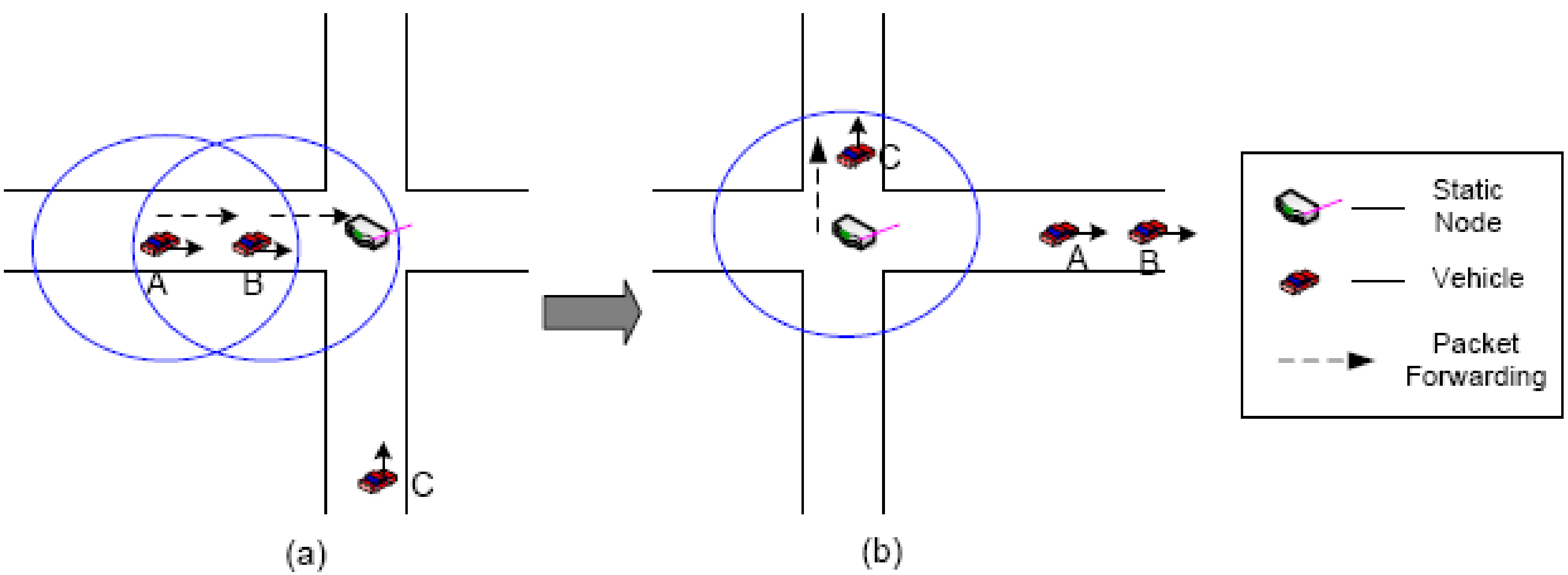
Motivation

- Improve the routing performance under low vehicle densities
  - Vehicle densities vary with time everyday
  - Gradual deployment of vehicular networks

- SADV design
  - Deploy static nodes at intersections to assist packet delivery
    - Can be embedded in traffic lights
  - Prevent packets from being delivered through detoured paths

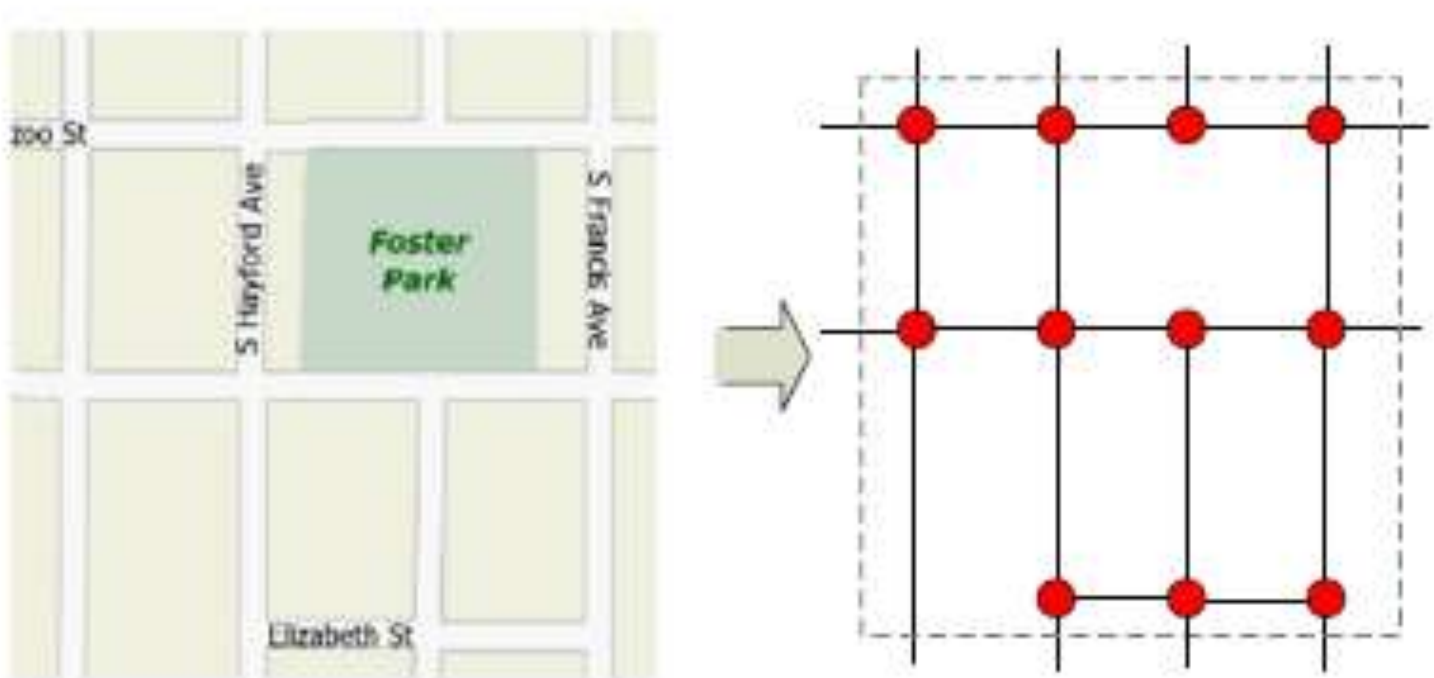
SADV Design

- Basic Idea:
  - A packet in node *A* wants to be delivered to a destination
  - The best path to deliver the packet is through the northward road
  - The packet is stored in the static node for a while
  - The packet is delivered northward when node *C* comes



SADV Design

- System Model
  - Abstract the road map as a directed graph where
    - Vertices represent intersections
    - Edges represent road segments



SADV Design

- Denote the static node deployed at intersection v_i as s_i
- The expected delay of delivering a packet from s_i to s_j through road v_iv_j

$$d(s_is_j) = w(s_is_j) + t(s_is_j)$$

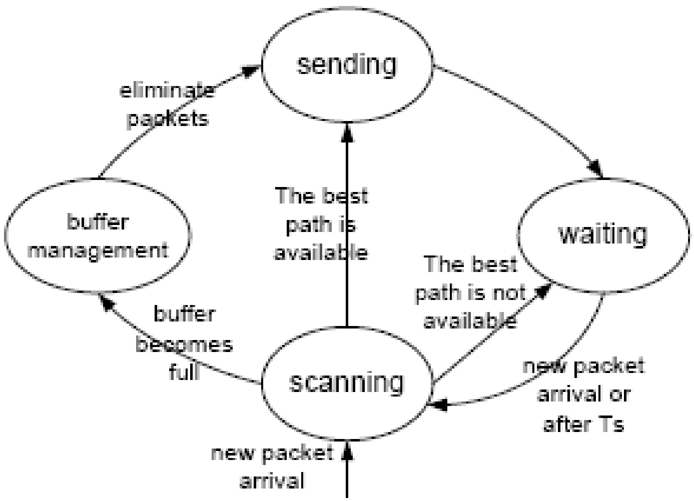
where

$$w(s_is_j) = 1/\lambda = 1/(speed(v_iv_j) \cdot density(v_iv_j))$$
$$t(s_is_j) = f(density(v_iv_j) \cdot speed(v_iv_j) \cdot length(v_iv_j))$$

- SADV tries to deliver the packet through the shortest expected delay path to the destination.

SADV Design

- Transactions of packets at static nodes
  - Forward the packet along the best path
  - If the best path is not available currently, store the packet and wait
  - Buffer management



- Transactions of packets in vehicles along roads
  - Greedy geographic forwarding used to route the packet to the next static node

SADV Design

- Packet Elimination Strategies
  - Choose some packets, and send them through the best currently available paths right now.
  - Commonly used strategies
    - FIFO: the packets that stay the longest in the buffer.
    - FILO: the most recently arrived packets.
  - FIFO and FILO are not efficient

SADV Design

- Least Delay Increase:
  - Basic Idea:
    - Reduce the increase in overall packet delivery delay caused by sending packets along sub-optimal paths.
  - A priority vector $[p_1, p_2, \ldots, p_m]$ defined for each packet
    - m is the number of adjacent roads of the static node
    - p_i denotes the ranking of the optimality of the *ith* adjacent road
    - e.g., [2, 1, 3, 4]
  - Instant rank of a packet:
    - the rank of the best currently available path
    - e.g., if the first and fourth roads are available currently, instant rank = 2
  - Elimination strategy:
    - Eliminate the packets with the highest instant rank
    - Send these packets through the current best paths

SADV Design

- Link Delay Update (LDU)
  - Expected link delay are estimated based on statistical information
    - Vehicle densities on the roads vary with time
    - Vehicle density is quite stable during a period of time
  - Use static nodes to help get more accurate delay estimation
    - Let adjacent static nodes measure the delay of the corresponding link, and propagate the delay measurement
    - Each static node updates its delay matrix according to the received up-to-date delay measurement.

SADV Design

- Multi-path Data Dissemination
  - Multi-path routing has the potential to further decrease packet delivery delay.
    - Link delay estimation may not be very accurate
    - Increase the chance of hitting a better path
  - Packets are delivered through multiple paths only at static nodes.
    - Assume a packet is in s_i at present
    - N(s_i): the set of adjacent static nodes of s_i
    - s_i delivers the packet to a subset of N(s_i)
      - The best and second best paths

SADV Design

- Partial Deployment of Static Nodes
  - Define a node deployment I as

$$I_i = \begin{cases} 1 & \text{if} \quad \text{there is a static node at intersection } v_i; \\ 0 & \text{if} \quad \text{otherwise.} \end{cases}$$

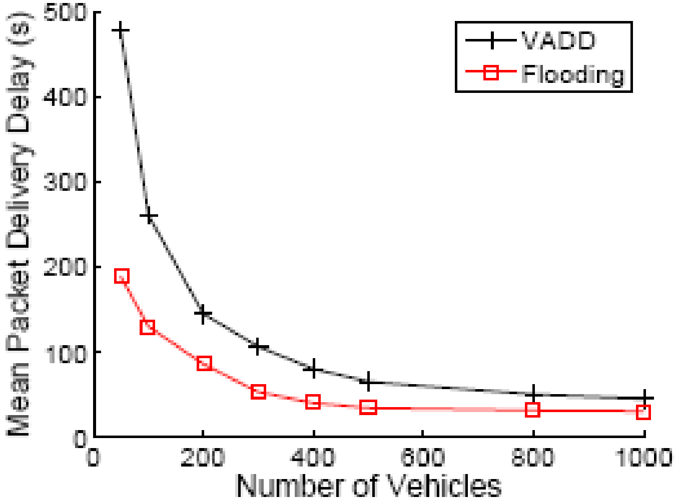
  - Problem:
    - Find the optimal node deployment I^* such that the average packet delivery delay in the network is minimized given a fixed number of static nodes.
  - Several heuristic strategies:
    - Uniform Deployment
    - High-Degree Preferred
    - High-Speed Preferred

Performance Evaluation

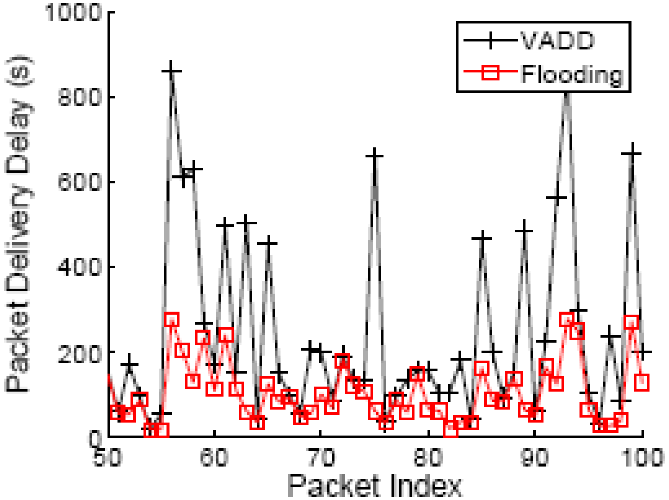
- Simulation Setup
  - Extract road map from TIGER
    - Range: 4000m x 5000m
    - Speed limit of roads: 25 ~ 70 mph
    - Number of intersections: 70
  - Wireless communication range: 200m
  - Vehicle mobility
    - Each vehicle select a random destination
    - Choose a fastest or shortest path with equal probability
  - Communication pattern
    - Random source, random destination

Performance Evaluation

- Performance degradation under low vehicle densities



(a) Mean Packet Delivery Delay

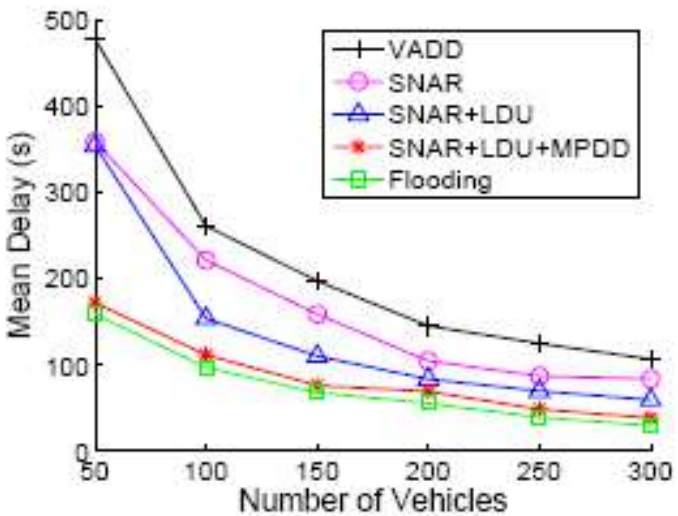


(b) Packet Delivery Delay under 100 Vehicles

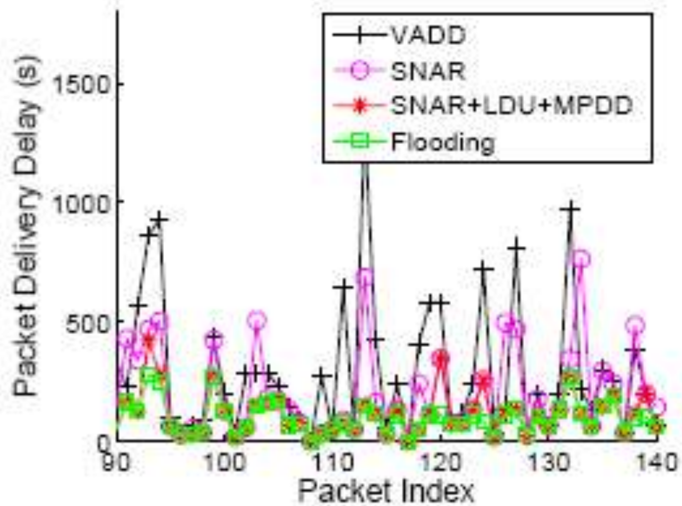
Flooding: vehicles exchange packets whenever they can communicate; the fastest way to deliver a packet.

Performance Evaluation

- SADV reduces delivery delay under low vehicle densities



(a) Mean Packet Delivery Delay

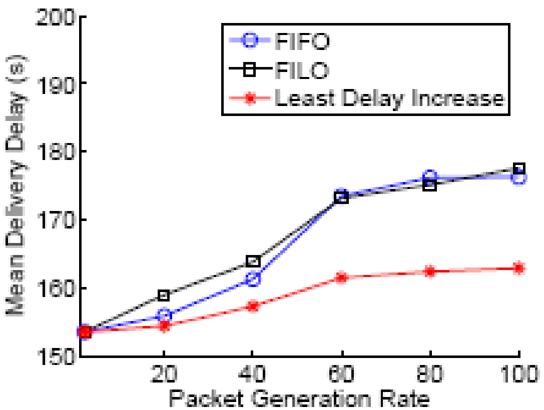


(b) Packet Delivery Delay for Individual Packets

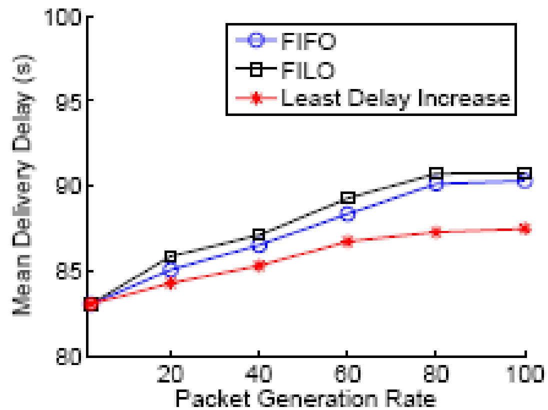
SNAR: use static nodes to assist routing
LDU: link delay update
MPDD: multi-path data dissemination

Performance Evaluation

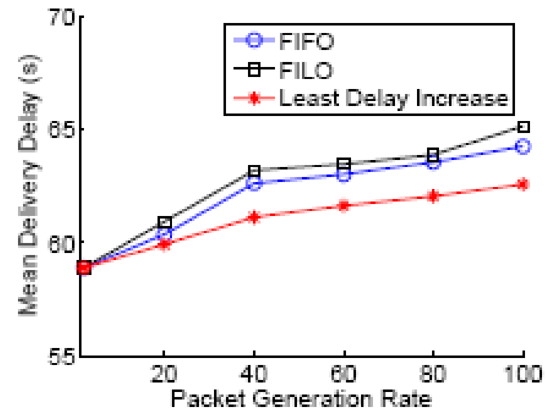
- Comparison of buffer management strategies
  - Use SNAR+LDU
  - *Least Delay Increase* strategy outperforms FIFO and FILO



(a) 100 vehicles



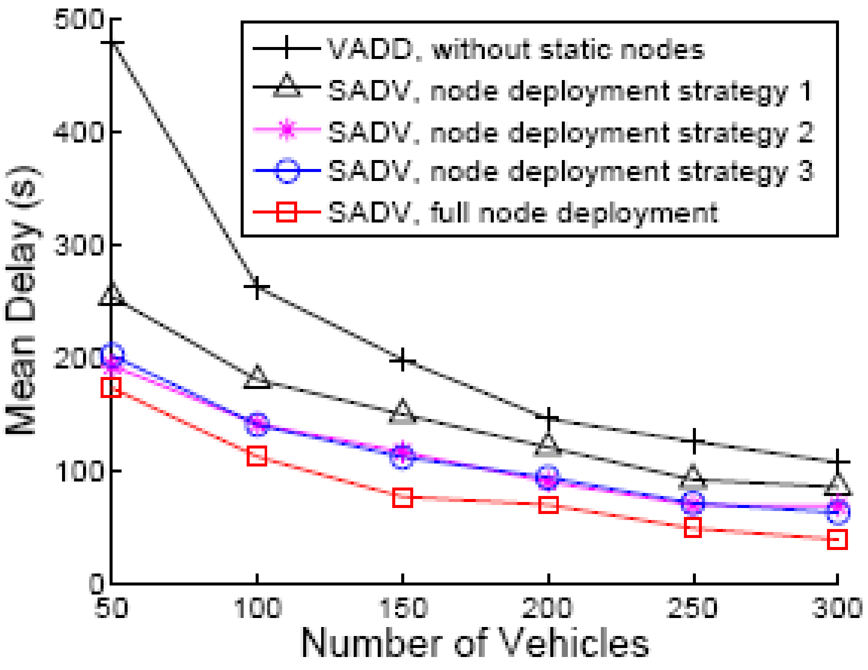
(b) 200 vehicles



(c) 300 vehicles

Performance Evaluation

- Comparison of different partial deployment strategies
  - Total 70 intersections, 35 static nodes deployed
  - *High-Degree Preferred* and *High-Speed Preferred* Strategies achieve similar performance, and outperforms *Uniform Deployment* strategy.



Conclusion

- Multi-hop data delivery performance may degrade under median or low vehicle densities when the network is frequently disconnected.
- SADV is able to improve data delivery performance by
  - Storing packets in static nodes and wait for the best delivery paths to become available.
  - Measuring link delay periodically so that routing decisions can be made adaptive to the changing vehicle densities.
  - Using multi-path routing to increase the chance of hitting a better delivery path.

Outline

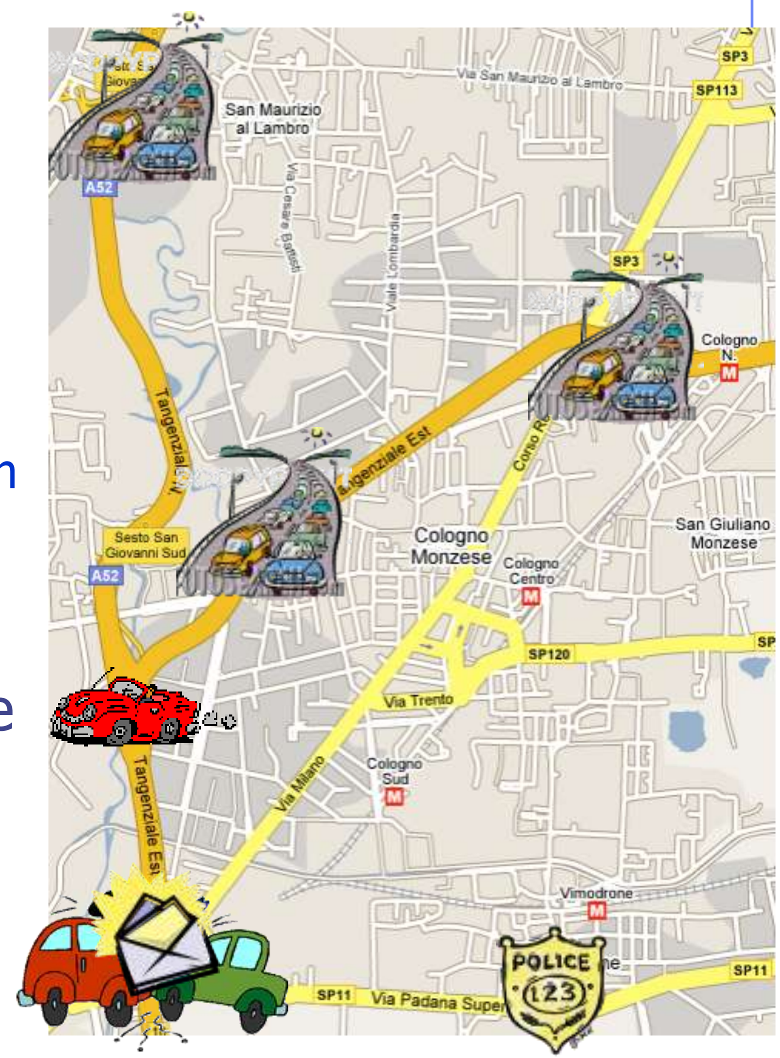
- DSCR and collision warning
- Data access
- Broadcast and routing
- **Information dissemination**
- Address configuration
- Security

Lightweight Information Dissemination in Inter-Vehicular Networks

Davide Sormani, Gabriele Turconi, Paolo Costa, Davide Frey, Matteo Migliavacca, and Luca Mottola, ACM VANET, 2006

Information Dissemination
Motivation & Scenario

- Two cars crash while traveling southbound on a highway, nearby vehicles cooperate to:
  - inform the closest ambulance and police stations
  - alert approaching vehicles telling them to slow down
  - notify the highway entrances north of the accident
- Messages should ideally propagate
  - towards specific target areas
  - along the routes where the vehicle density is higher

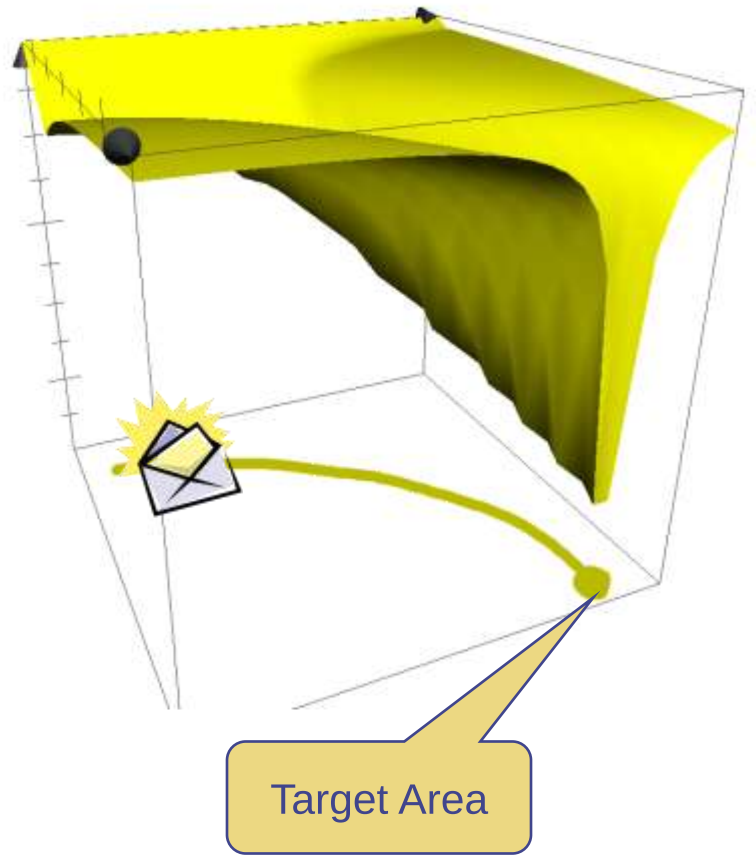


Information Dissemination

- An approach to routing messages towards specific target areas while considering the underlying vehicle density
- A **propagation function** to ***encode*** the target areas and the preferred paths to reach these areas
  - study how to embed the propagation function within various protocols, by making use of
    - probabilistic forwarding
    - store & forward
  - evaluate the impact of the information brought by the propagation function on the protocols' performance
    - in sparse as well as dense networks
- A first step towards the definition of more complex protocols
  - e.g., using predictions of future movements

System Model
The Propagation Function

- Each vehicle knows its geographical *location* and communication range
- The propagation function f_p maps *locations* to a *numerical value*
- Target areas are the sets of locations where f_p returns a value *lower* than a threshold v_{th}
- Protocols should ideally steer messages towards locations where f_p returns the *lowest* values along the directions of ***maximum decrease***

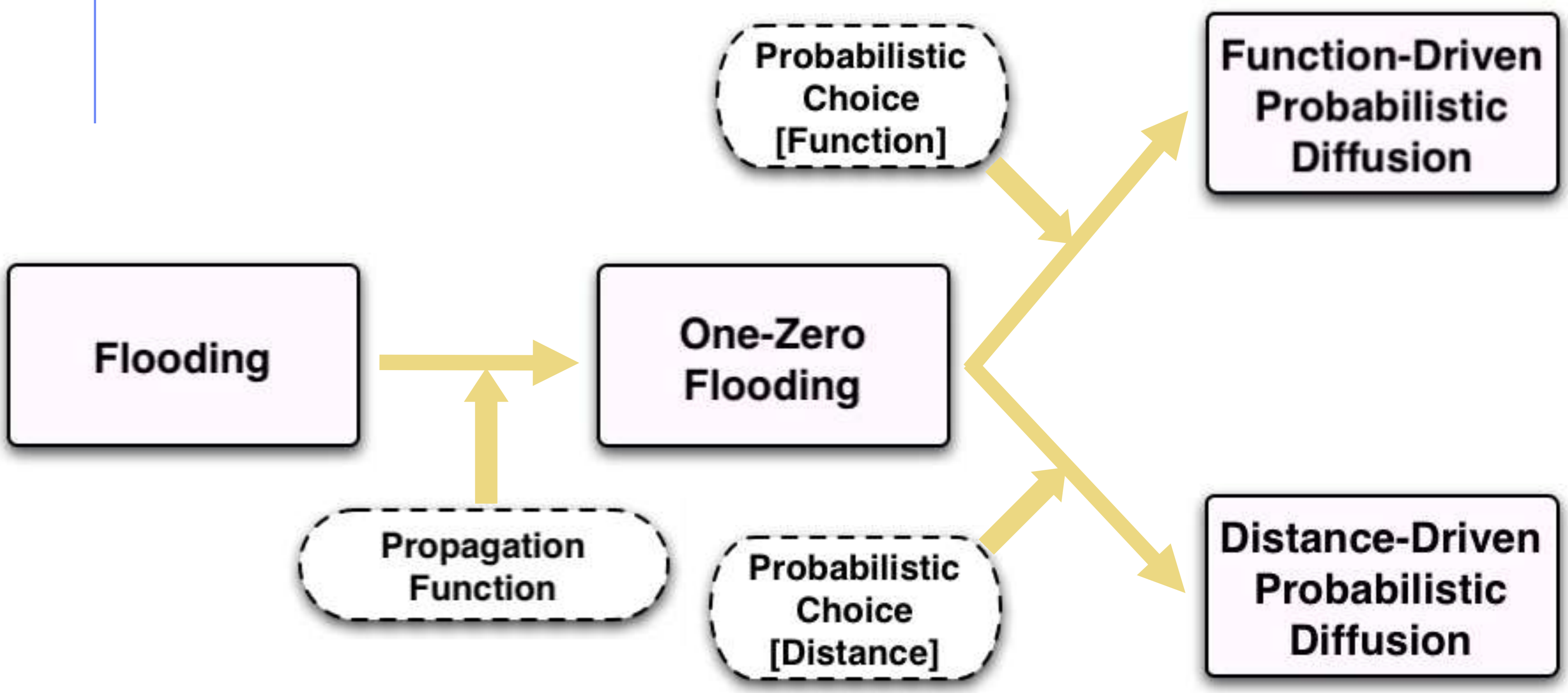


Protocols - Overview

- Messages are **always broadcast**
  - include sender location, sender communication radius, and propagation function
- Forwarding decisions are taken on the receiver side
  - *no need to maintain neighborhood information*
- ***Probabilistic*** *schemes* forward messages only with a given probability
  - achieves good delivery with little overhead
- ***Store & Forward*** *techniques* use vehicles as “mules” to physically carry data
  - suited in sparse networks

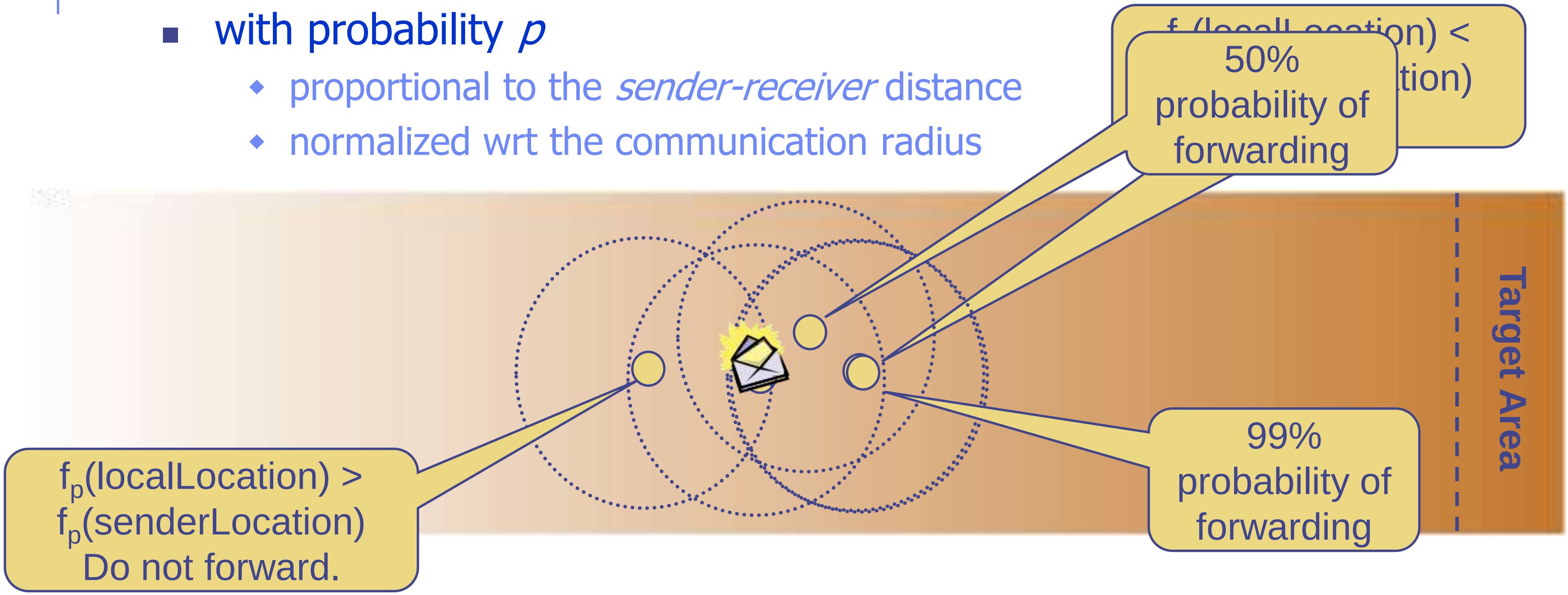
Protocols - Connected Scenarios

- Instantaneous connectivity between source node and destination area



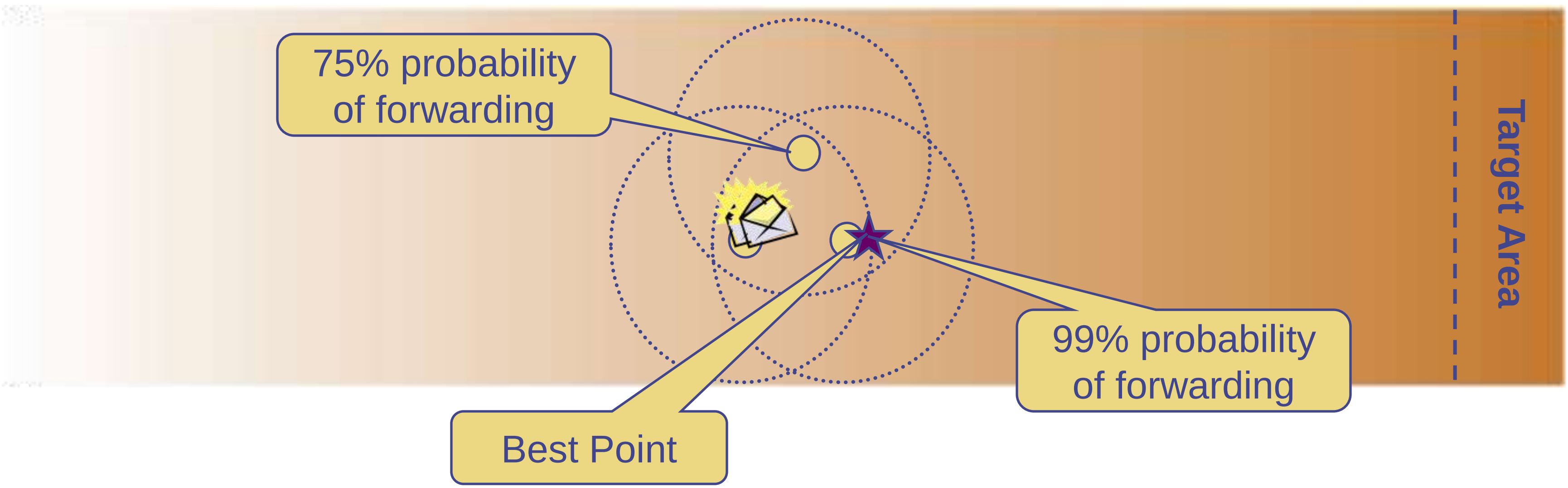
Protocols - Connected Scenarios (1/2)

- **One-Zero Flooding:** *let messages proceed towards the target area*
  - forwards when $f_p(localPosition) < f_p(senderPosition)$
- **Distance-Driven Probabilistic Diffusion:** *let messages proceed by jumping on long-distance hops*
  - forwards when $f_p(localPosition) < f_p(senderPosition)$
  - with probability *p*
    - proportional to the *sender-receiver* distance
    - normalized wrt the communication radius



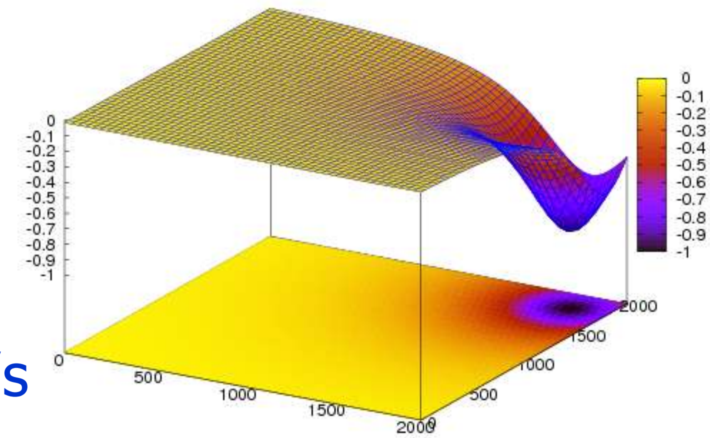
Protocols - Connected Scenarios (2/2)

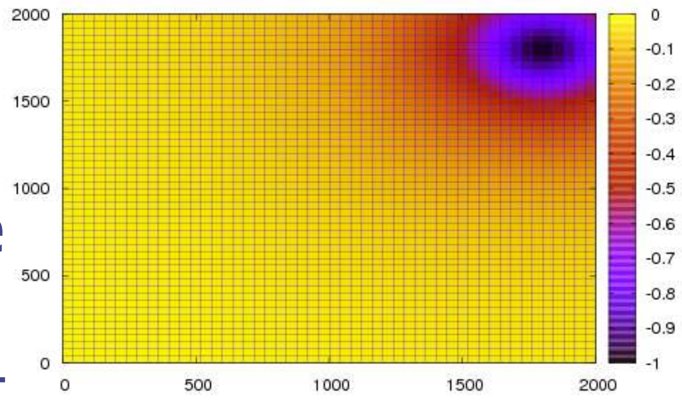
- The best point is the location within the sender physical communication radius where f_p returns the lowest value
- Function-Driven Probabilistic Diffusion: *let the messages proceed along trajectories ending at the target area*
  - forwards when $f_p(localPosition) < f_p(senderPosition)$
  - with probability p
    - proportional to the difference in f_p at the *sender* and *receiver* locations
    - normalized wrt the difference in f_p at the *sender* and *best point* locations



Evaluation - Simulation Settings

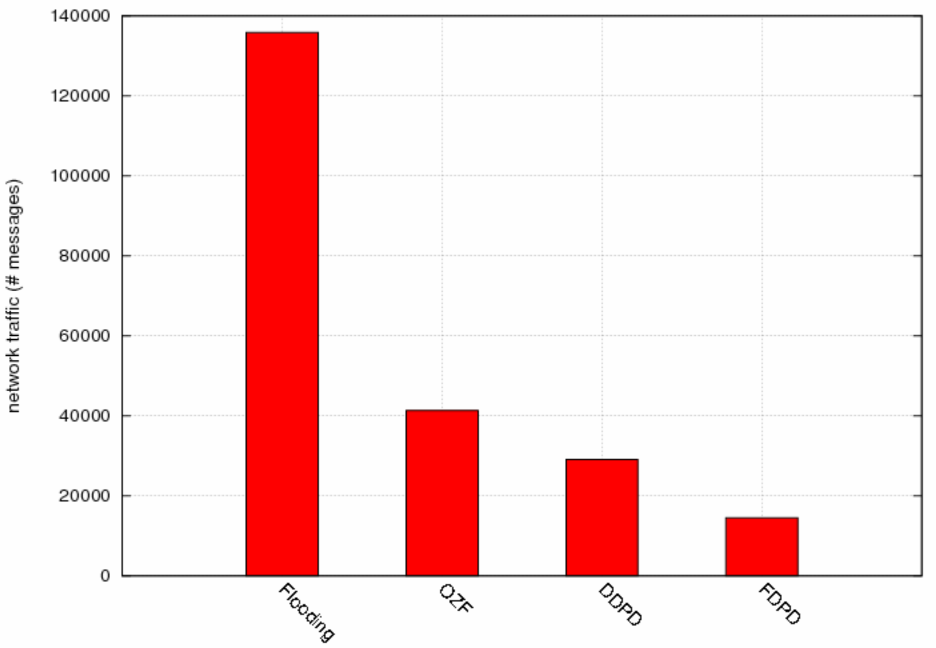
- *J-Sim* simulator with IEEE 802.11 MAC layer
- *Two-Ray Ground* propagation model
- *Manhattan* mobility model
  - vehicles moving at 5 m/s to 20 m/s
  - no dependence on node speed
- Consider a propagation function with a single minimum
- Each vehicle publishes a message per second addressed to a circle with radius 100 m in the top right corner





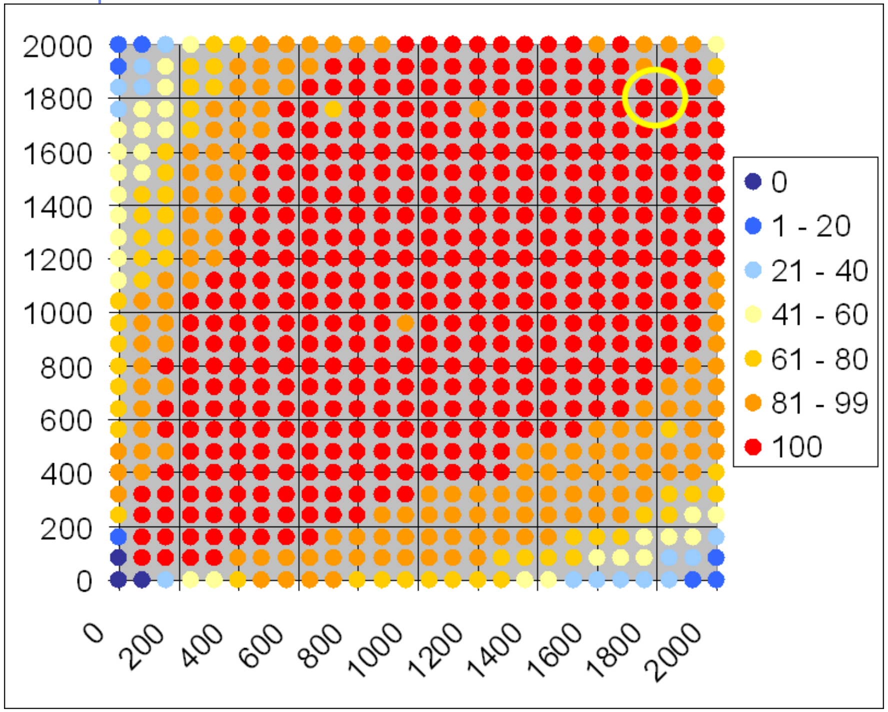
Evaluation - Dense Networks

- 200 nodes/km^2, modeling a urban setting

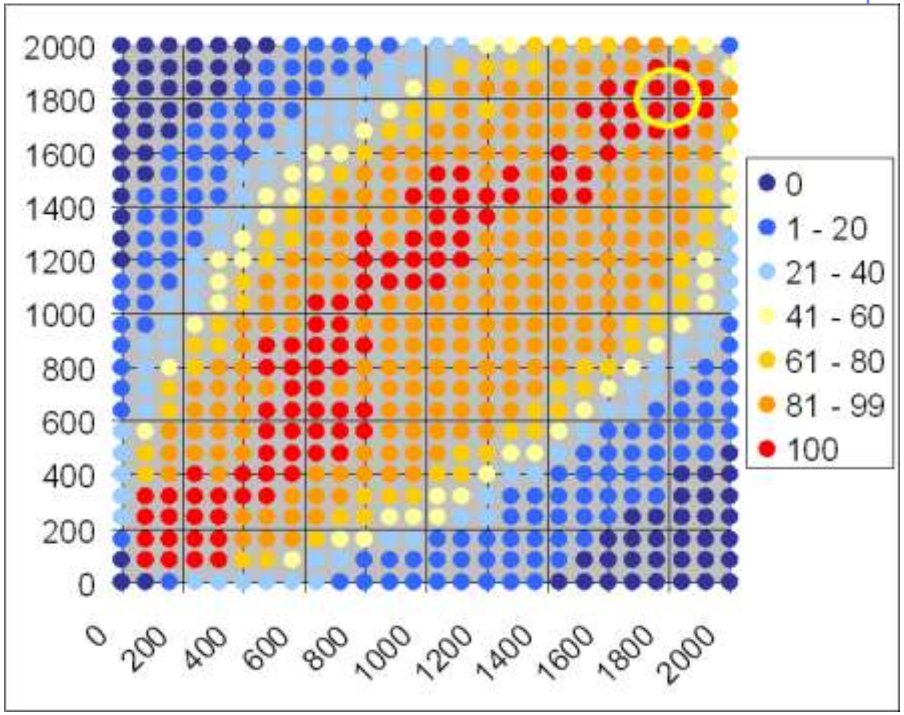


Dense Networks - Diffusion Charts

- 900 probes regularly scattered overhear messages



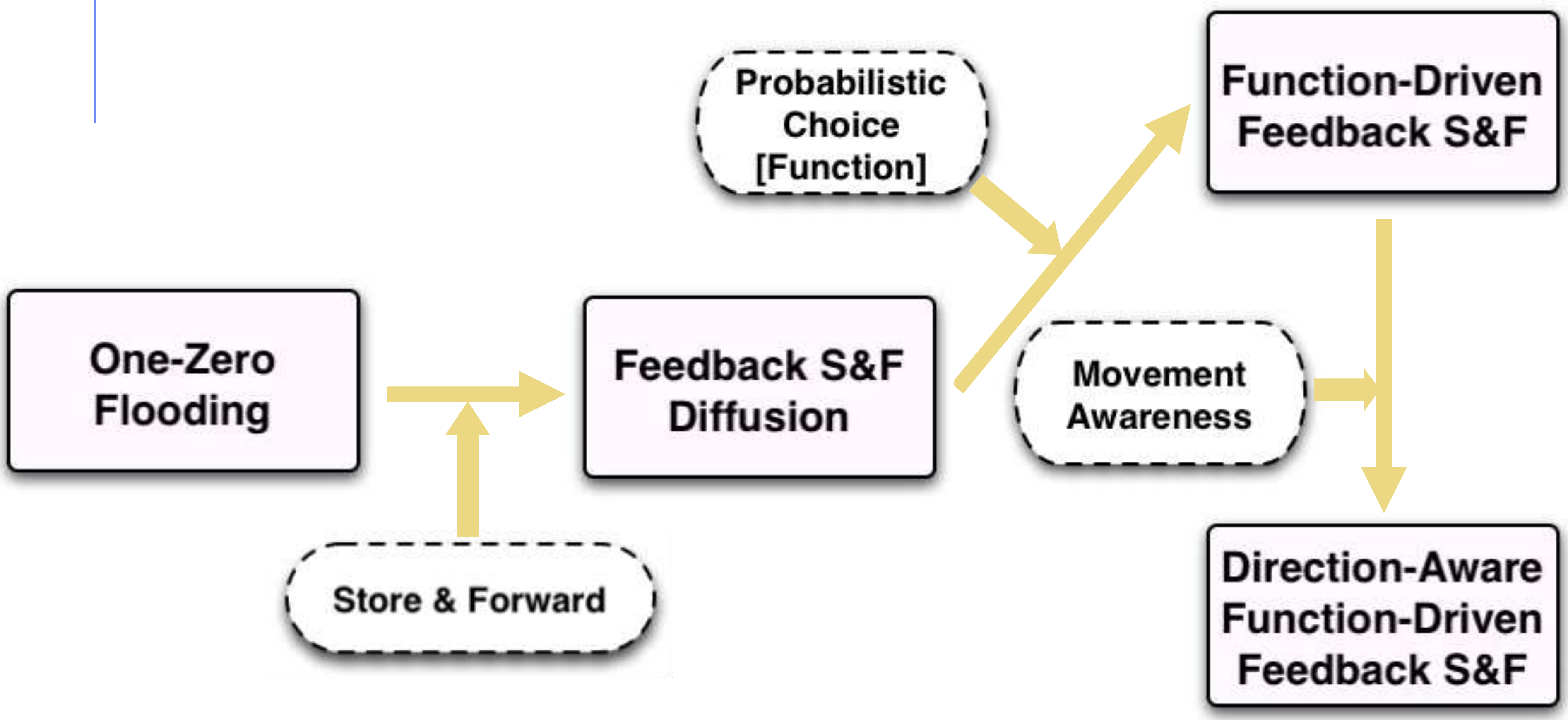
Distance-Driven Probabilistic Diffusion



Function-Driven Probabilistic Diffusion

Protocols - Disconnected Scenarios

- Assumes the ability to store messages at intermediate nodes
- Suited for **sparse** networks



Protocols - Disconnected Scenarios (1/2)

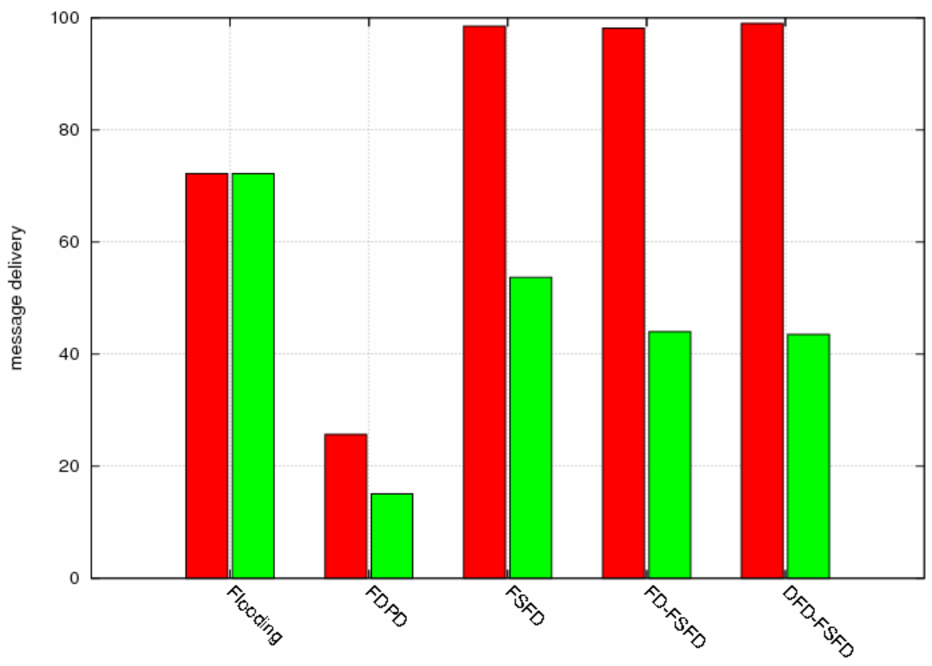
- S&F useful also to circumvent local minima, dealing with non-convex propagation functions, avoid physical obstacles (e.g., buildings)
- Feedback S&F Diffusion: *let the messages be carried until other nodes in "better" positions are found*
  - on message receipt, act as in One-Zero Flooding
  - schedule a per-message timeout
    - re-forward the message on timeout expiration, and re-schedule timeout
    - drop message if overheard from a node located where f_p returns lower values

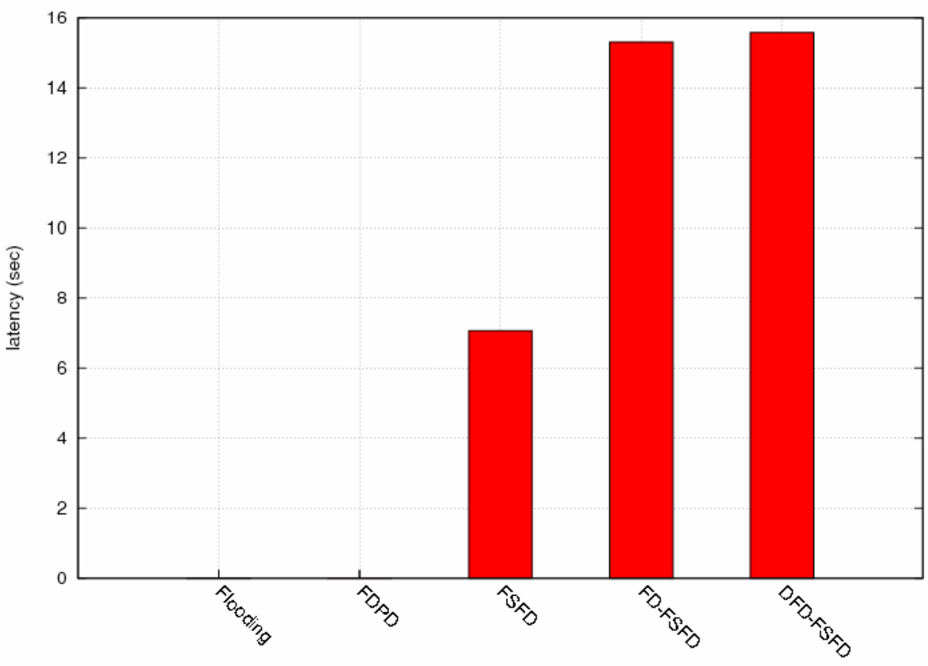
Protocols - Disconnected Scenarios (2/2)

- Probabilistic Feedback S&F Diffusion:
  - same as Function-Driven Probabilistic Diffusion on message reception (using best point)
  - same as previous protocol in S&F
- Distance-Aware Probabilistic Feedback S&F Diffusion:
  - same as Function-Driven Probabilistic Diffusion on message receipt (using best point)
  - schedules timeout only if the node is moving towards the target area
    - evaluate the angle between the direction of movement and the gradient of f_p, if less than 90° schedules timeout

Evaluation - Sparse Networks

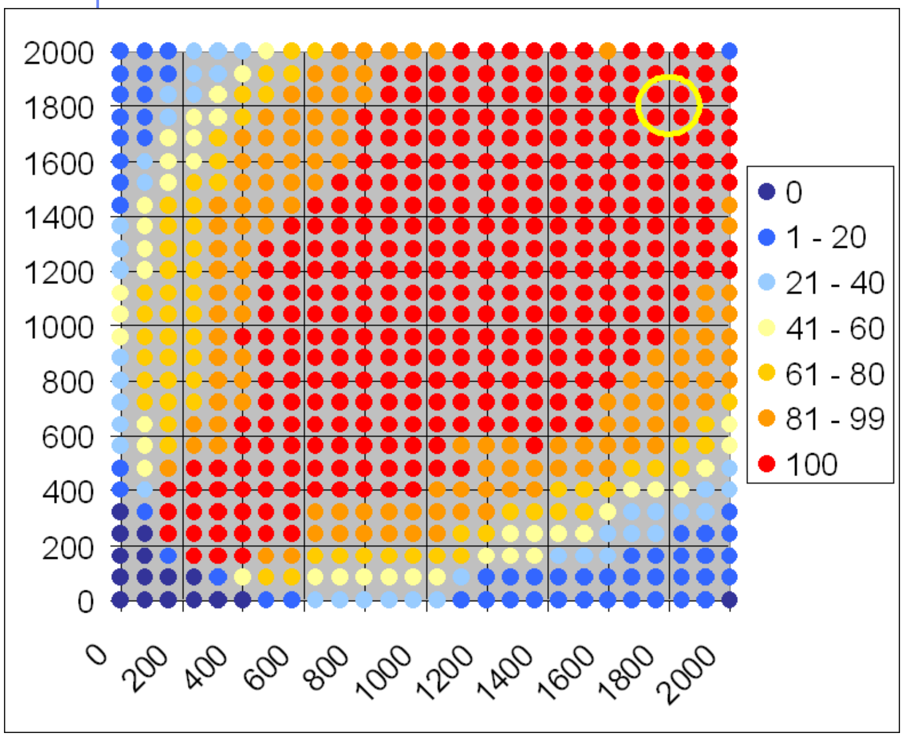
- 50 nodes/km^2, modeling a rural environment



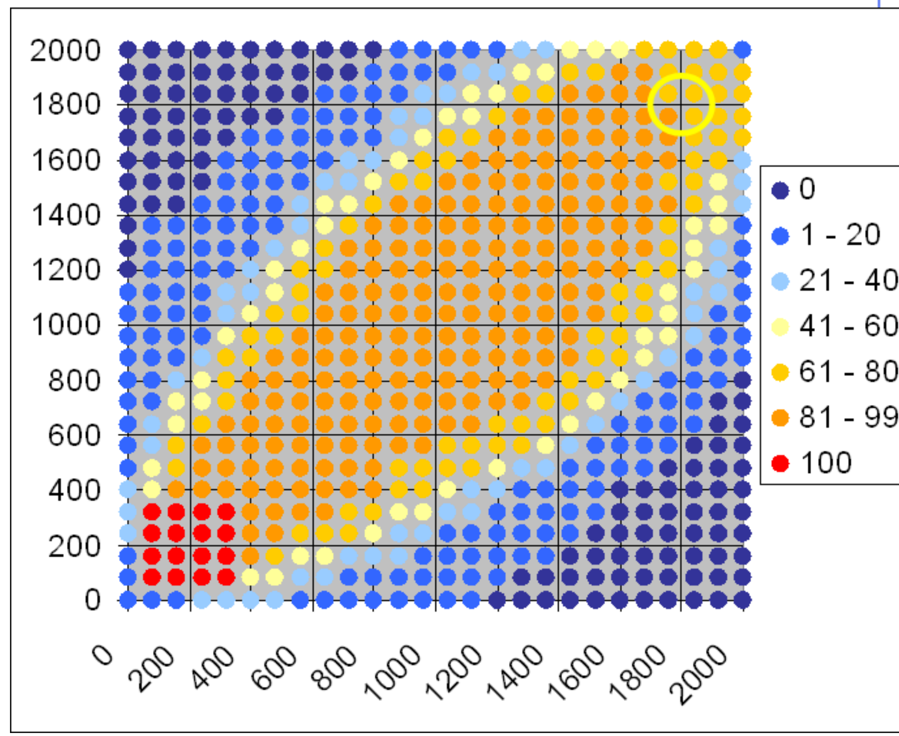


Sparse Networks - Diffusion Charts

- 900 probes regularly scattered overhear messages



Feedback S&F Diffusion



Probabilistic Feedback S&F Diffusion

Outline

- DSCR and collision warning
- Data access
- Broadcast and routing
- Information dissemination
- **Address configuration**
- Security

Vehicular Address Configuration

Maria Fazio, Claudio E. Palazzi, Shirshanka Das, and Mario Gerla,
AutoNet, 2006

Introduction

- Any networking session (e.g., TCP) and application requires unique identifiers for peer communicating nodes
  - **Unique ID** (*e.g*., Vehicle ID No) not the same as **routable address** (*e.g.,* geo address)
  - In the Internet, IP address was originally designed as BOTH unique ID and as routable address
  - Major problems with maintaining sessions when routable address changes – i.e., during handoff (solutions: Mobile IP, IPv6, tunneling etc.)

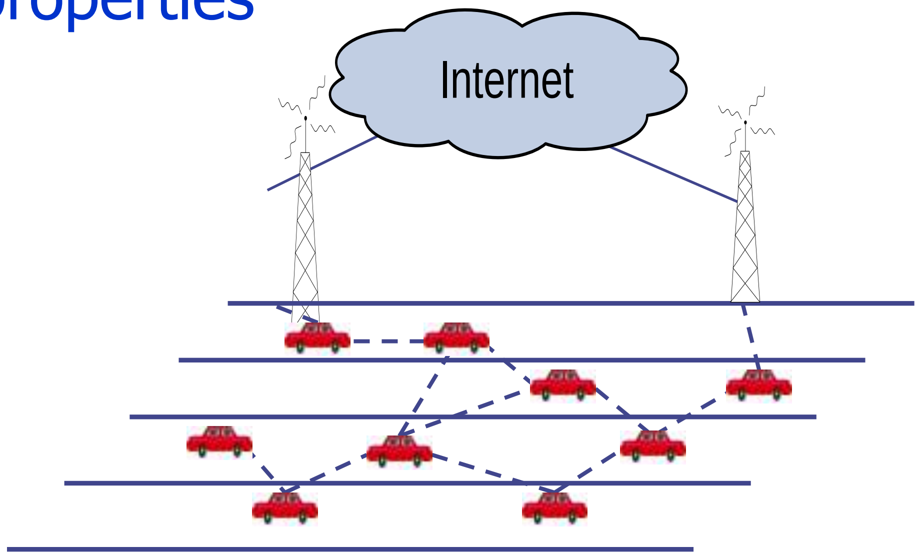
Introduction (cont.)

- In MANET, the IP address is used as "unique" ID (for TCP, UDP and at times, even for routing, e.g., AODV)
- Thus, we need IP address auto-configuration of nodes that leads to "unique" IP addresses
- Utilizing IPv6 in place of IPv4 does not eliminate the need for address auto-configuration procedure [RFC2462]
  - IPv6 is just another tunneling method, that assists in hand off
  - RFC 2462, "IPv6 Stateless Address Autoconfiguration"

Auto-configuration in VANETs

- Auto-configuration of IP addresses (such that assignment is unique) requires specific investigation for the VANET scenarios

- Solution developed for traditional ad-hoc networks cannot be directly applied to VANETs
  - VANETs have peculiar properties



VANET unique properties

- High density of nodes (many cars in few meters on a highway or in town)

- High absolute speed (20-80mph)
  - but low **relative** (to other cars) speeds (3-20 mph)

- Practically "infinite" network diameter
  - Millions of cars in a large metropolis

Problem Statement

- Create an auto-configuration service for VANETs with the following properties:
  - High reliability (i.e., low ID collision rate) of the address configuration
  - Low signal overhead generated by the system
  - Low configuration time
    - Especially important for nodes engaged in real-time applications

Background

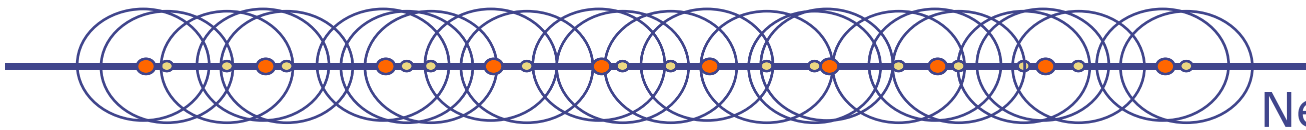
- Decentralized approach
  - ALL nodes contribute to the configuration task
    - control traffic does not scale

- Best Effort approach
  - provide correct routing without ensuring unique node addresses (note: most ad hoc routing schemes use IP as routable address)
  - Generates serious delays when address duplications have to be solved among sessions, say at TCP level

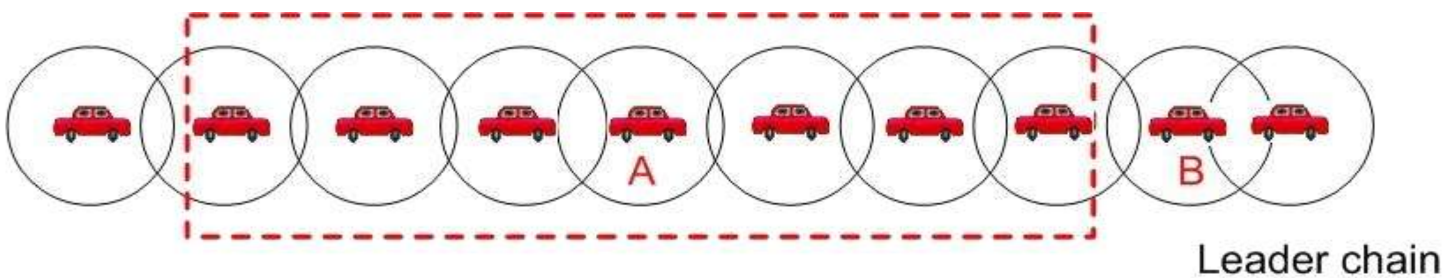
- **Leader**-based approach
  - Hierarchical structure to configure nodes and perform DAD (Duplicate Address Detection) procedure only within a cluster

Proposed VAC Solution

- Leader-based solution

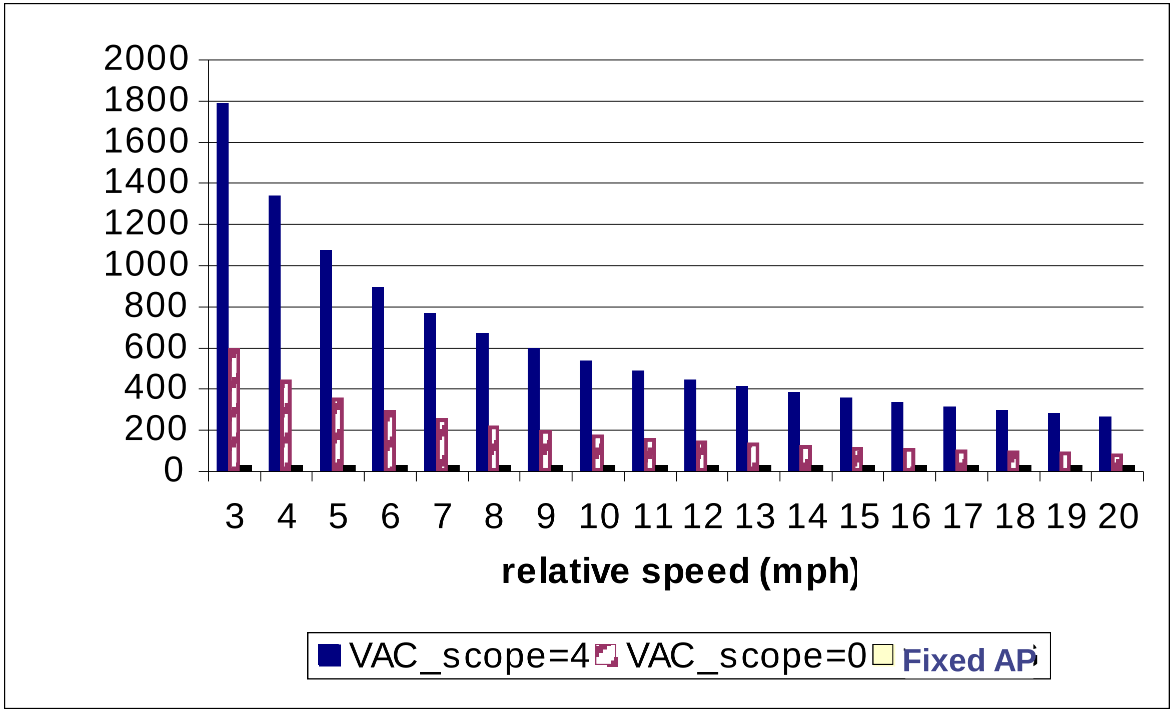


- Leaders proactively organized in a chain and work like DHCP servers
  - Each leader dispenses DHCP addresses
- Guarantee unique address within ***SCOPE***



The *SCOPE of Leader A* is the area covered by the set of Leaders whose distance from A is less or equal to *scope* hops.

VAC vs. DHCP Server on Fixed APs



- With DHCP on Fixed APs (Access Points)
  - Very frequent changes of nodes' IP addresses
  - routing, TCP and thus ad-hoc networking services may fail if an area is not covered by at least one AP

VAC vs. Traditional Leader-based Solutions

- In traditional Leader-based approaches:
  - Leaders are responsible for a sub-network that is limited in size
  - Each Leader has to be aware of ALL OTHER leaders in the network
  - The address configuration task is performed by nodes
    - Leaders only verify duplicate addresses and manage network merging
- VAC overcomes these limitations…

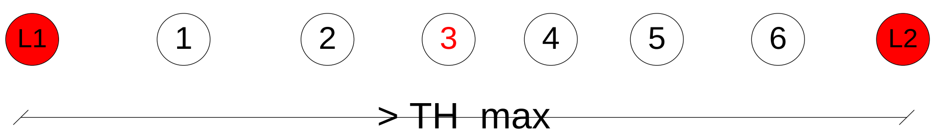
VAC’s Tasks

- Construction and maintenance of the Leader chain:
  - Leaders join and leave the chain
- Configuration of nodes’ addresses:
  - Address management/assignment the network
  - Duplicate Address Detection (DAD)

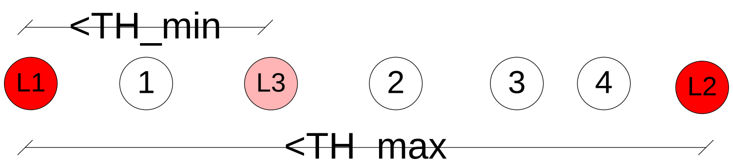
Leader Chain's Configuration and Maintenance

- TH_max and TH_min are thresholds for maximum and minimum distance between two Leaders

Distance(L1, L2) > TH_max → A new Leader (L3) is elected



Distance(L1, L3) < TH_min → A Leader (L3) becomes normal

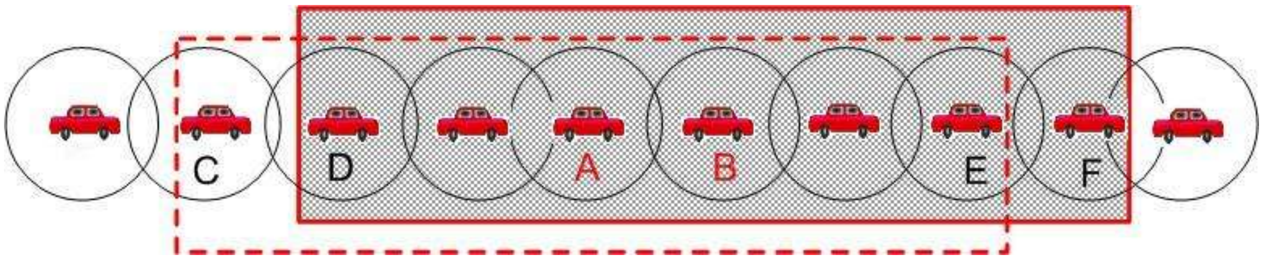


Address Configuration

- Synchronization of address information among Leaders
  - Address space partitioned in sets of addresses
  - Each Leader in a SCOPE has a different set of addresses to assign
    - Synchronization through Hello packets
- Modified DHCP protocol to assign addresses to nodes that make a request

Address Maintenance

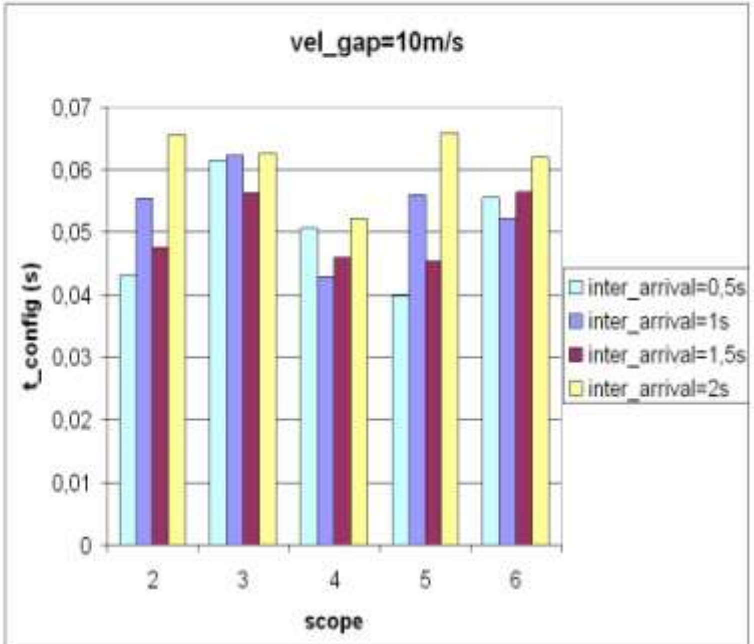
- DAD procedure verifies whether an address in the SCOPE ceases to be unique due to nodes' mobility
  - A node configured from Leader A has a valid address even outside A's range if it remains in A's SCOPE
  - Requires only single-hop communications between nodes and Leader

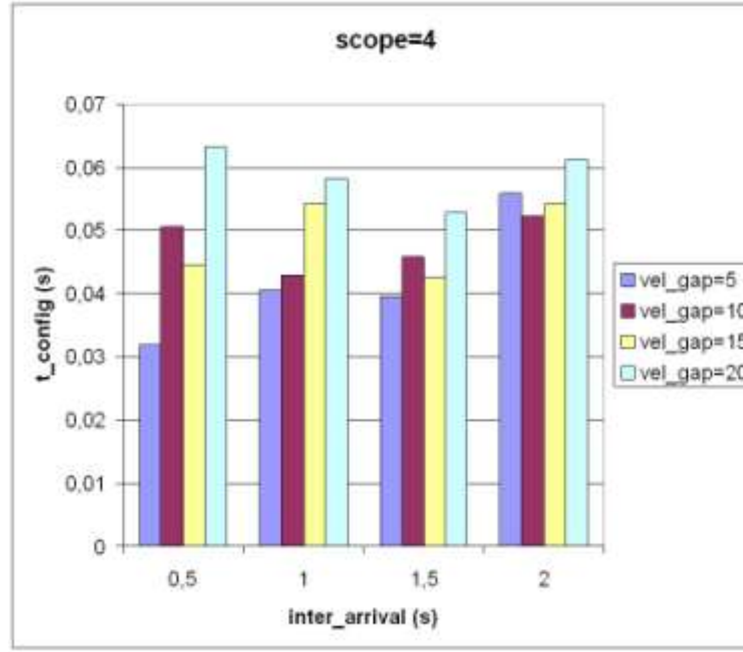


Evaluation Assessment

- QualNet simulator v3.7
  - 50 nodes
  - 15000mx20m terrain (single direction of travel?)
- Parameters
  - *scope*: size of the SCOPE set
    - 2, 3, 4, 5, 6
  - *Vel_gap*: maximum difference between cars' speed
    - 5, 10, 15, 20m/s.
  - *Inter_arrival*: a new car enters the highway every…
    - 0.5, 1, 1.5, 2s

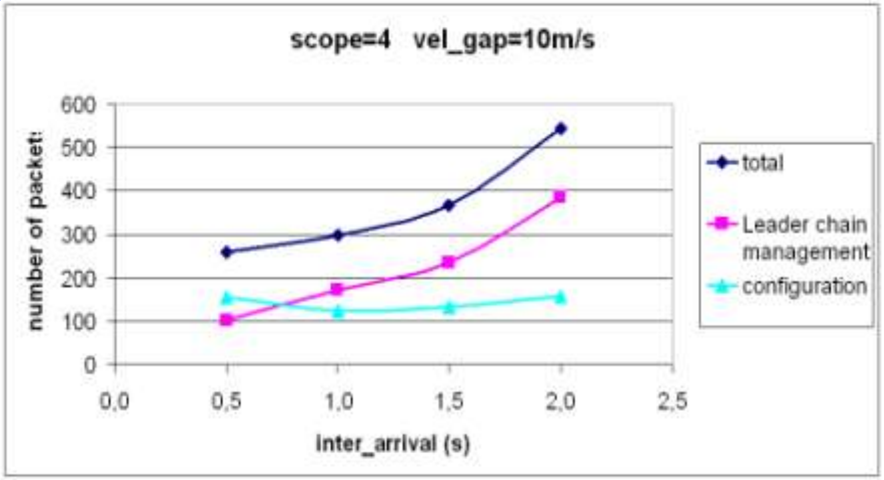
Evaluation: Configuration Time

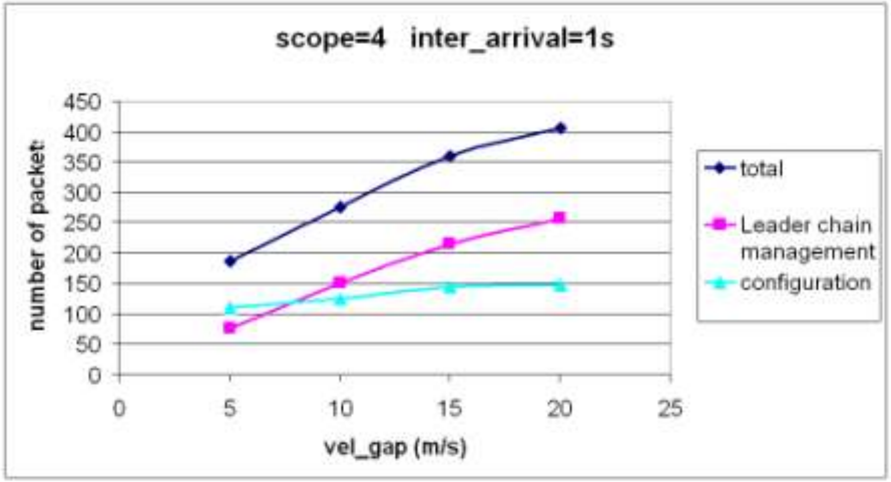




- Low configuration time for all scope size and cars' interarrival times
  - Always less than 70ms
  - Allows also real-time application

Evaluation: Overhead





- Leader chain management is more affected by vehicles' **density** and **speed** than address configuration
  - VAC address assignment is very stable
- Cross-layer techniques could be exploited to piggyback messages for Leader chain management on beacons periodically sent by routing algorithms

Outline

- DSCR and collision warning
- Data access
- Broadcast and routing
- Information dissemination
- Address configuration
- **Security**

Challenges in Securing Vehicular Networks

Bryan Parno and Adrian Perrig,
HotNets-IV, 2005

Why VANET Security?

- Adding security as an afterthought is rarely pretty
- Utility and ubiquity of vehicular networks will make them likely targets for attack
- Attacks may have “deadly” consequences

Sample VANET Security Contexts

- Traffic congestion detection applications that alert drivers to potential traffic jams
  - *e.g.*, vehicles detect when the # of neighboring vehicles exceeds a threshold, and then relay the info to vehicles approaching the congested location
- Deceleration warning systems
  - *e.g.*, broadcast warning messages when speed reduces suddenly and significantly

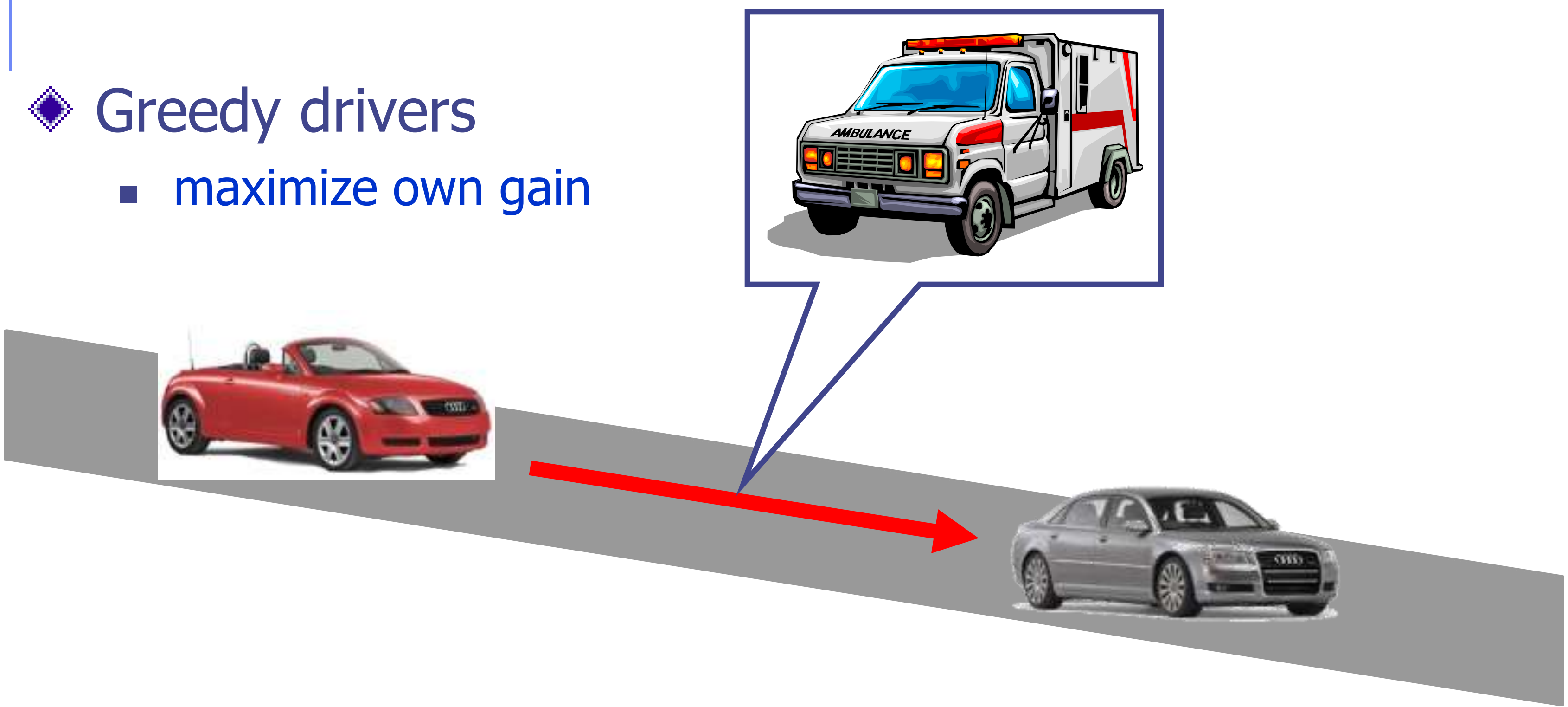
Contributions

- Analyze security **challenges** specific to VANET
- Introduce security **primitives** for security applications
- Discuss vehicular **properties** that can support security systems
- Present two security **techniques** that leverage unique vehicular properties

Classes of Adversaries

The nature and resources of adversary determine the **scope of defenses** needed to secure a VANET

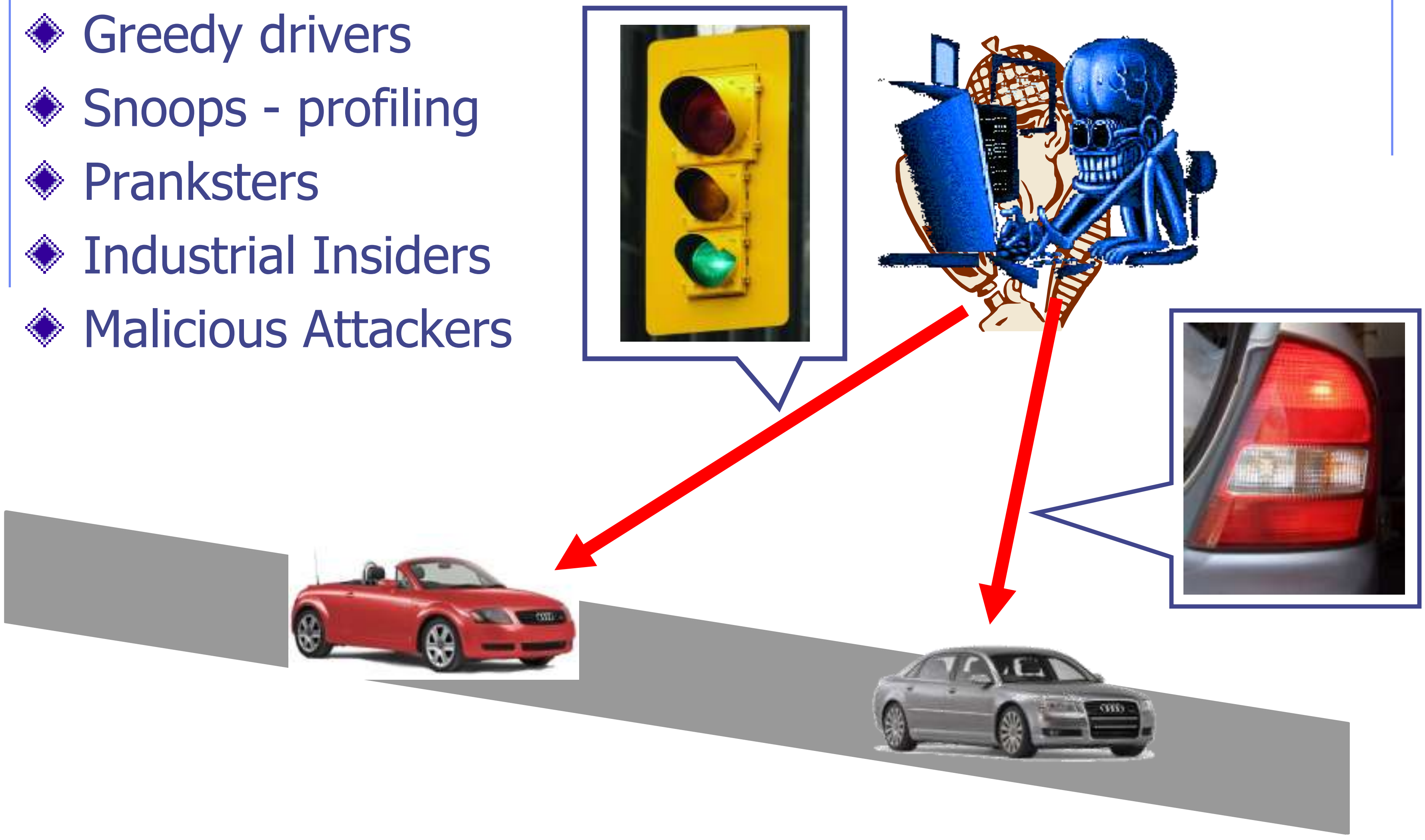
- Greedy drivers
  - maximize own gain



Classes of Adversaries

In increasing order of threat severity

- Greedy drivers
- Snoops - profiling
- Pranksters
- Industrial Insiders
- Malicious Attackers



Attacks

- Denial of Service (DoS) Attgacks
  - Overwhelm computational or network capacity
  - Deadly to applications with real-time response
  - Dangerous if users rely on the service
  - *e.g.*, prevent deceleration warning from reaching other drivers
- Message Suppression Attacks
  - Drop congestion alerts
  - *e.g.*, suppress congestion alert to create gridlock
- Fabrication Attacks
  - Lie about congestion ahead or lie about identity
  - *e.g.*, greedy driver gaining advantages
  - authentication vs. privacy
- Alteration Attacks
  - Replay transmissions to simulate congestion
  - authentication vs. privacy

Challenges: **Authentication** vs. **Privacy**

- Ideally, each vehicle should only have one identity with strong authentication
  - Prevents Sybil or spoofing attacks (e.g., spoofed congestion) – prevent one vehicle from claiming to be hundreds in order to create an illusion of congestion
  - Allows use of external mechanisms (e.g. law enforcement of forensic evidence)
- Drivers value their privacy
  - Legal requirements vary from country to country
  - Vehicles today are only partially anonymous – license plate is publicly displayed
  - Lack of privacy may lead to lack of security

Challenges: **Availability**

- Many applications will require real-time responses
- Increases vulnerability to DoS attacks
- Unreliable communication medium
  - Studies show only 50-60% of a vehicle's neighbors will receive DSRC's broadcast

Challenges: **Mobility**

- Mobility patterns will exhibit strong correlations
- Transient neighborhood
  - Many neighbors will only be encountered once, ever
  - Makes reputation-based systems difficult
- Brief periods of connectivity
  - Vehicles may only be in range for seconds
  - Limits interaction between sender and receiver

Challenges: **Key Distribution**

- Manufacturers
  - Requires cooperation and interoperability
  - Each manufacturer must trust competitors
- Government
  - DMV (Department of Motor Vehicle) distribution
  - Handled at the state level, so also requires cooperation and interoperability
  - Running a Certificate Authority (CA) is <u>non-trivial</u>

Challenges: **Low Tolerance for Errors**

- Many schemes rely on probabilistic guarantees
  - With 200 million cars in the US, if 5% use an application that works 99.99999% of the time, still more likely to fail on some car
  - Need stronger guarantees in life-and-death applications
- Focus on prevention, rather than detection & recovery
  - Safety-related applications may not have margin for driver reaction time

Challenges: **Bootstrap**

- Initially, only a small percentage of vehicles will have DSRC radios
- Limited support deployment of infrastructure
- Ad hoc protocols allow manufacturers to incorporate security without deviating from their business model

Vehicular Properties Support Security

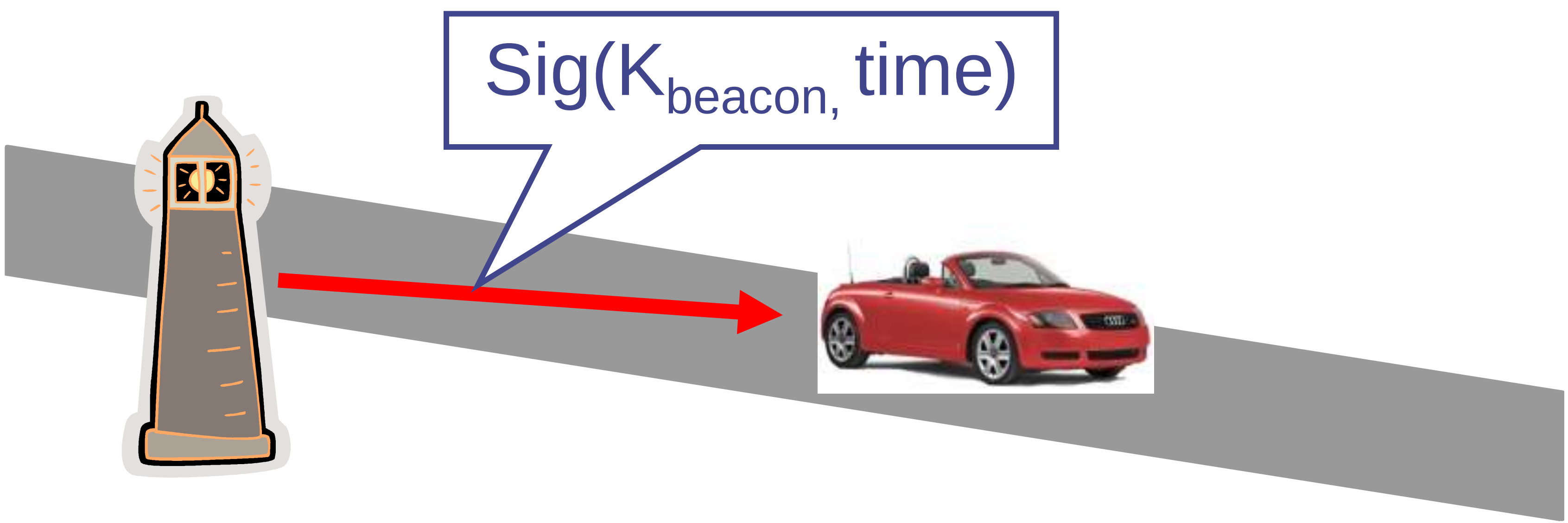
- Regular Inspections
  - Most states require annual inspection
  - Download updates, Certificate Revocation Lists (CRLs), new certificates
  - Use software attestation to verify vehicle
- Honest Majority
  - Most drivers prefer not to tinker with their cars
    - May void warranty or violate the law
  - Must protect against worms
    - Leverage existing work for PCs
    - Trusted Platform Modules may help eventually

Vehicular Properties Support Security

- Additional input from human drivers
  - Presumed intelligent operator at each node
  - Cannot distract driver, but can still gather or infer data
    - E.g., ignored deceleration warning may indicate a false positive
- Existing enforcement mechanisms
  - For many attacks, attacker must be in close physical proximity
  - May be sufficient to identify the attacker

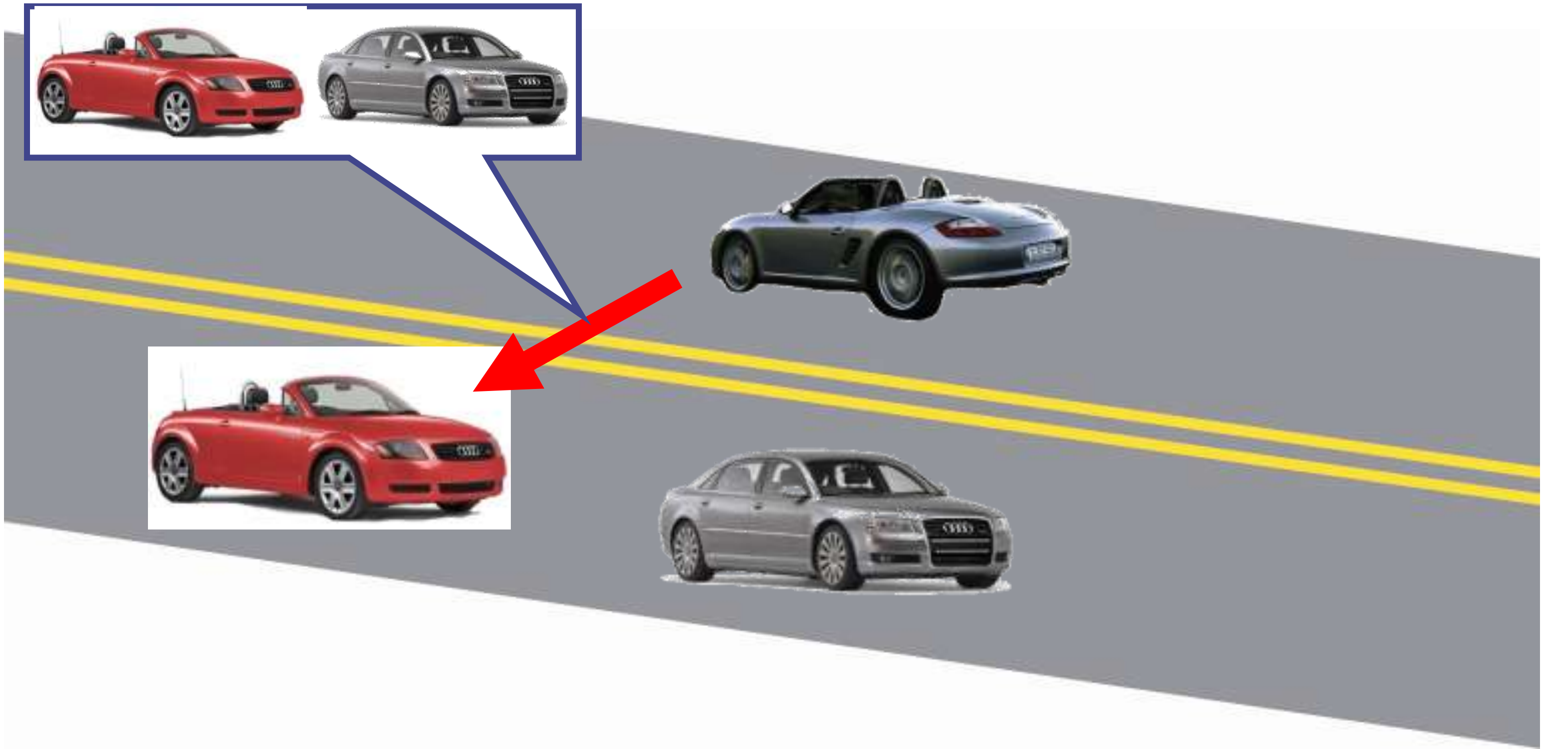
Security Primitives: Secure Message Origin

- Determine a message did indeed originate at a given location
- Prevents attacks
  - Road-side attacker cannot spoof vehicles
  - Attacker cannot modify legitimate messages to simulate congestion
- **Beacon**-based approach – vehicle includes beacon's packet within their message to prove that the vehicle was at beacon's location at that time



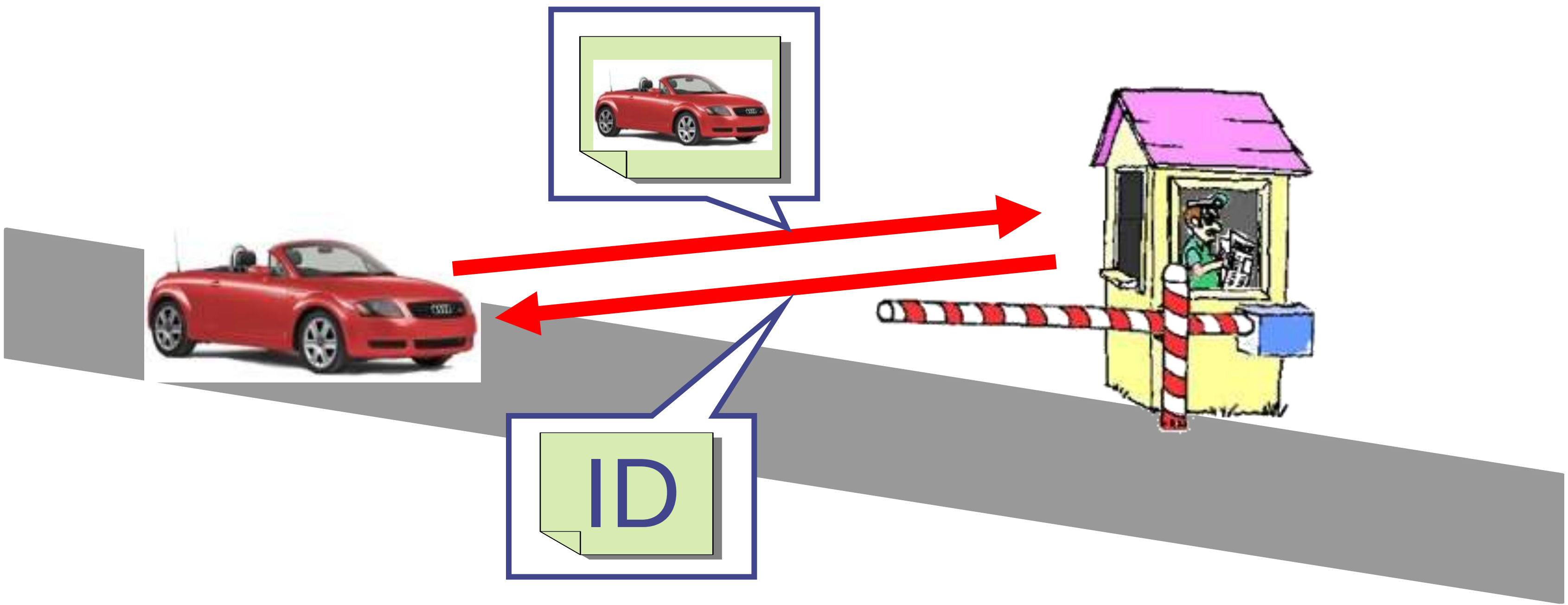
Security Primitives: Secure Message Origin

- Alternately, use ***entanglement***
  - Each vehicle broadcasts:
    - Its ID
    - Ordered list of vehicles it has passed
  - Establishes *relative* ordering
  - Add resiliency by evaluating consistency of reports from multiple vehicles



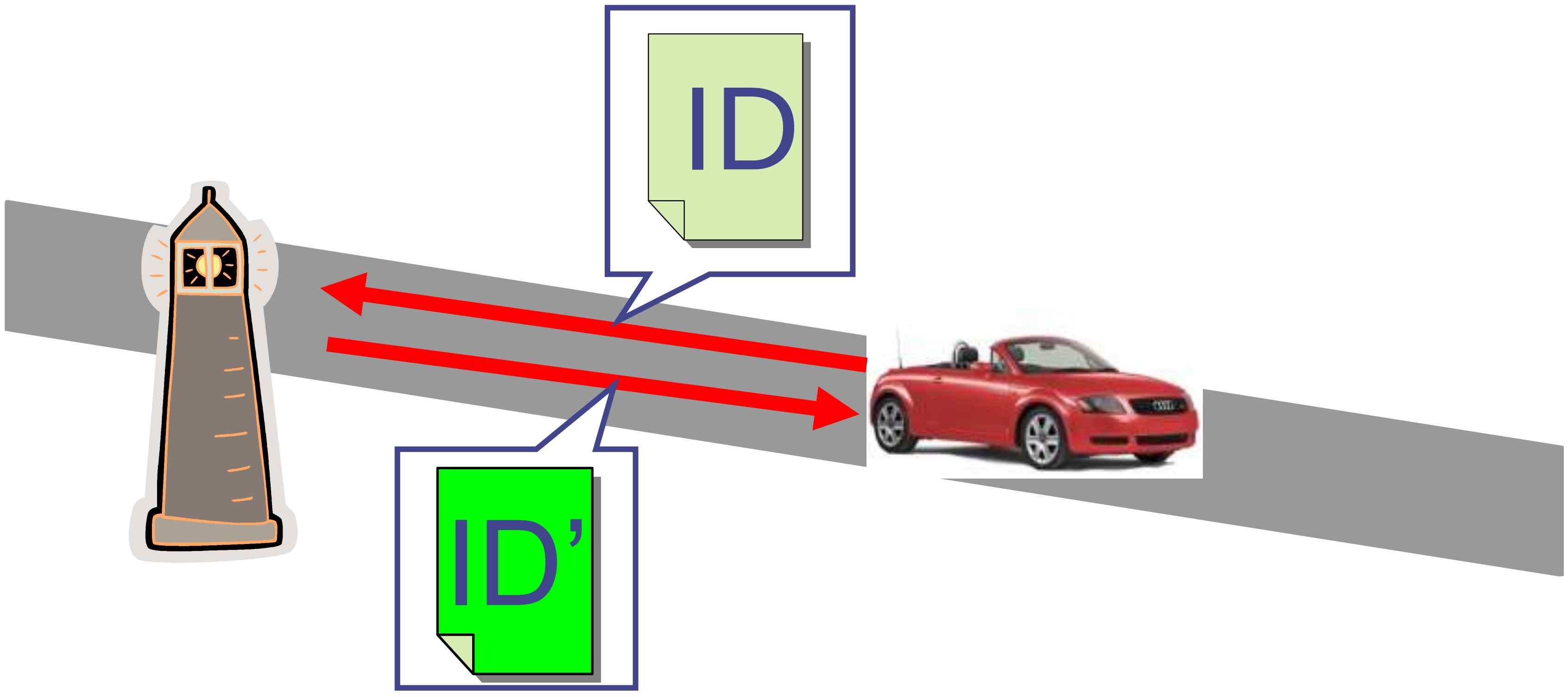
Security Primitives: Anonymization Service

- Many applications only need to connect (associate) information to a vehicle, not to a specific identity
  - Authenticate to **anonymization service** with permanent ID
  - Anonymization service issues temporary ID
  - Optionally include escrow for legal enforcement
- Ideal environment: toll roads
  - Controlled access points
  - All temporary IDs issued by the same authority



Security Primitives: Anonymization Service

- To provide finer granularity, use *reanonymizers*
  - Anonymization service issues short-lived certificates
  - Reanonymizer will provide a fresh ID in response to a valid certificate



Additional Security Primitives

- Secure **Aggregation**
  - Securely count vehicles to report congestion
- Key Establishment
  - Temporary session keys for platooning or automatic cruise control
- Message Authentication and Freshness
  - Prevent alteration and replay attacks