THE UNIVERSITY OF TEXAS AT AUSTIN
CENTER FOR TRANSPORTATION RESEARCH

PRODUCT 0-6845-P1

TXDOT PROJECT NUMBER 0-6845

WORKSHOP MATERIALS

Research Supervisor:
Chandra Bhat

CENTER FOR TRANSPORTATION RESEARCH
THE UNIVERSITY OF TEXAS AT AUSTIN

DECEMBER 2016; PUBLISHED MARCH 2017

http://library.ctr.utexas.edu/ctr-publications/0-6845-P1.pdf

THE UNIVERSITY OF TEXAS AT AUSTIN
CENTER FOR TRANSPORTATION RESEARCH

0-6845-P1

WORKSHOP MATERIALS

Research Supervisor:
Chandra Bhat

TxDOT Project 0-6845: Connected Vehicle Problems, Challenges and Major Technologies

DECEMBER 2016; PUBLISHED MARCH 2017

Performing Organization: Center for Transportation Research The University of Texas at Austin 1616 Guadalupe, Suite 4.202 Austin, Texas 78701	**Sponsoring Organization:** Texas Department of Transportation Research and Technology Implementation Office P.O. Box 5080 Austin, Texas 78763-5080
Performed in cooperation with the Texas Department of Transportation and the Federal Highway Administration.	

THE UNIVERSITY OF TEXAS AT AUSTIN
CENTER FOR TRANSPORTATION RESEARCH

Connected Vehicle Problems, Challenges, and Major Technologies

Project 0-6845

TxDOT Project Manager: Darrin Jensen

Research Supervisor: Chandra Bhat

Researchers: Chang-Sik Choi, Jeffrey Andrews, Lakshay Narula, Todd Humphreys, Robert Heath, Jia Li

COLLABORATE. INNOVATE. EDUCATE.

Connected Vehicle Overview

Safety	Mobility	Infotainment
• Blind spot warning • Forward collision warning • Do-not-pass warning	• Route guidance • Traffic signal speed advisory • Variable speed limit	• Point of Interests (POIs) notification • In-vehicle internet access

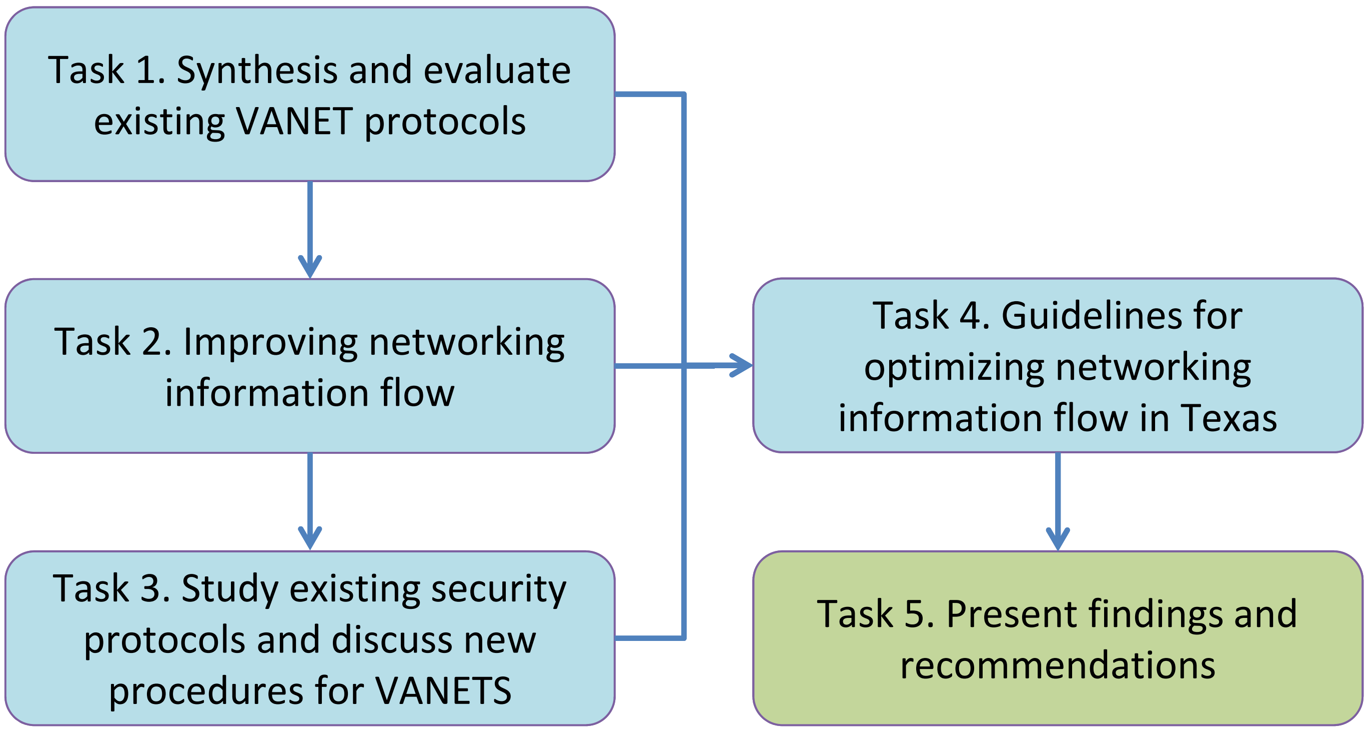
Effectiveness of these applications heavily depends on information flow quality (latency, range, reliability, scalability) and security

Project Scope

Considering and addressing two challenges

- How to optimize information flow quality
  - Comparative performance of DSRC and LTE
  - Cost of DSRC and LTE
- How to improve information flow security
  - Attacks to Connected Vehicles
  - Security Measures Against Attacks

Task Overview



THE UNIVERSITY OF TEXAS AT AUSTIN
CENTER FOR TRANSPORTATION RESEARCH

Work Schedule

	Original Schedule
	Work Completed
RRRRR	Revised Schedule

Created Date: August 25, 2014

Note: Each task must produce one or more deliverables. All deliverables should be submitted to RTIMain@txdot.gov.

	Research Activity	Estimated Cost of Task	FY 2015												FY 2016												FY 2017											
			Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July	Aug
Task 1	Synthesize and evaluate existing VANETs routing protocols and assess the appropriateness of various VANET routing protocols under different	$80,400																																				
Task 2	Improve networking information flow: comparison of IEEE 802.11p (currently used standard) vs 3GPP LTE (potential future standard)	$70,350																																				
Task 3	Detailed study of existing security protocols and demonstration of a new protocol for VANETs	$93,800																																				
Task 4	Develop guidelines for optimizing networking information flow in CV environments in Texas	$60,300																																				
Task 5	Conduct a workshop to present the findings and the recommendations	$30,150																																				
	Monthy Progress Reports			x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x												
	Total (should = 100% of total budget)	**$335,000**																																				

Workshop Organization

- Introduction
- DSRC and LTE Standards, and a Comparative Analysis (30 min)
- Security Challenges (30 min)
- Case Study: Variable Speed Limit (15 min)
- Research team recommendations (to form the basis for group discussions)
- Group Discussion and Pathways Forward
- Conclusion

Task 2: Improve Networking Information Flow: Comparison of IEEE 802.11p vs. 3GPP LTE

Task 1: Synthesize and evaluate existing VANETs routing protocols

Jeffrey G. Andrews & Chang-sik Choi

- Topics:
  - Brief introduction of DSRC and LTE
  - The performance of DSRC and LTE are compared
  - Comparison of deployment costs of DSRC and LTE

Dedicated Short Range Communication (DSRC) Overview

- DSRC is a broad set of vehicular communication standards developed by standard-setting committees within the IEEE and the SAE.
  - In USA, refers to the below protocol stack
  - Uses unlicensed spectrum just below 6 GHz carrier frequency
- DSRC will possibly be required in new cars sold in the USA by about 2020 (ruling pending)

OSI Layer	DSRC Counterparts
Message Layer	SAE J2735
Network and Transport Layer	IEEE 1609.3 (WSMP) or TCP/UDP, IPv6
MAC Sublayer Extension	IEEE 1609.4
PHY and MAC Sublayer	IEEE 802.11p

DSRC Physical and MAC Layer: IEEE 802.11p

- 802.11p is most closely related to 802.11a and 802.11g (Wi-Fi standards)
- Ratified in 2010, it is however very similar to 802.11 from 1999

Property	802.11p	802.11a
Spectral Bands	5.9 GHz (5.850-5.925 GHz)	Several 5 GHz bands just below 5.9 GHz
Channel bandwidth	10 MHz	20 MHz
Total number of OFDM subcarriers	64	64
Modulation	BPSK, QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM
Coding rate	1/2, 3/4	1/2, 2/3, 3/4
Data rates (Mbps)	3, 4.5, 6, 9, 12, 18, 24, and 27	6, 9, 12, 18, 24, 36, 48, and 54
Typical maximum range	500 ft (~ 150m)	200 ft (~ 50m)
MAC Protocol	CSMA/CA	CSMA/CA
Connection Types	BSS and Outside the Context of BSS (OCB): No Setup, just use “Wildcard” messaging	Basic Service Set (BSS): Infrastructure or independent: Slow Setup

LTE for Vehicular Networking

- LTE ("Long Term Evolution") is a blanket name for several 4G Cellular Standards
  - First standardized at end of 2008 but with several subsequent "releases"
  - Current "state of the art" smart phone technology
- Key traits:
  - IP data-based (rather than voice)
  - Larger bandwidth (5, 10, or 20 MHz for each of Downlink, Uplink)
  - Generally uses bands below 3.5 GHz
  - Low complexity and power consumption
  - Excellent range and reliability

Standards Comparison

Protocol	802.11g and 11a	802.11p	3G Cellular	LTE	5G (mmWave)
Bandwidth (MHz)	20	10	5	5, 10, 20	100-1000
Frequency (GHz)	2.4, 5.2–5.8	5.85–5.925	< 3.5 GHz	< 3.5 GHz	> 15 GHz
Data Rate (Mbps)	6-54	3-27	~2 /cell	~72 /cell	> 1 Gbps
Max Transmission range	60 m	150 m	~ 5km	~ 3km	150-200 m
Coverage	Short- Range, Intermittent	Medium-Range, Intermittent	Wide area, ubiquitous	Wide area, ubiquitous	Short range, no deployments
Mobility Support	Low	Medium	High	High	Probably Low
V2I	Yes	Yes	Yes	Yes	TBD
V2V	Yes	Yes	No	Yes (D2D)	TBD
Market Penetration	High	Low	High (decreasing)	High	None (~ 2022)

Key Advantages of LTE for Vehicular Applications

- LTE has several advantages over DSRC stemming from its centralized command-and-control architecture:
  - Dedicated control and overhead channels
  - Centralized scheduling and power control (reduces interference, allows scalability)
  - Rapid retransmissions via HARQ
  - Rapid link adaptation via fast channel state feedback
  - Native support of high mobility and fast handoffs, perfected by cellular industry over three decades
- Uses licensed spectrum with larger allowed transmit power and antenna gain
  - Uses lower frequencies, has better propagation
- D2D extension is under active development, could be used for V2V in the future

Task 1 Wrap up

- DSRC is a stable and mature technology, will eventually be low cost and use unlicensed spectrum
  - However its range and performance are still an open question
  - Many different vendors make inconsistent claims
- LTE has numerous technical advantages over DSRC but one major disadvantage: the requirement for licensed spectrum (and hence an operator agreement/subscription)
- VANETs (V2V) based on DSRC can be used for short-range communication, otherwise require multi-hopping
- Main challenges for LTE vehicular networking are largely non-technical, such as the cost, business model, and backwards compatibility
- 5G Cellular (the next generation after LTE) is targeting vehicular applications as a key use case

TASK 2: COMPARISON

Simulation Parameters (1)

- **Routing protocol:**
  - VANETs have two kinds of packet traffic: BSM broadcast packets and multi-hop packets
  - Routing protocols parameter (AODV or OLSR) controls the behavior of multi-hop packets.
  - AODV (Ad hoc On Demand Vector) routing finds routes when needed, while OLSR (Optimized Link State Routing) monitors all possible routes at all times
- **Number of transmitting vehicles:**
  - Indicates the number of transmitting vehicles in the networks
  - According to DSRC standards, the vehicles transmit a BSM (Basic Service Message) regularly, about every 100 milliseconds
  - Represents the amount of resources consumed
- **Speeds and trajectories:**
  - Indicates the speeds of vehicles and paths that they follow
  - High mobility is a major challenge for DSRC

Simulation Parameters (2)

- **Number of "sinks":**
  - Represents the number of multi-hop streams that contain independent messages (for unique end-points)
  - A random source-destination pair is selected to support a multi-hop stream
- **Transmit power:**
  - Should comply with the DSRC standards, usually max of 28 dBm
  - Lowering transmit power can mitigate interference
- **Basic safety message (BSM) size**
  - BSM compactly contains local information about the transmitting vehicle, such as its speed, GPS location, heading, and acceleration
  - The BSM size should be restricted to less than 200 bytes to control packet congestion

Simulation Parameters (Summary)

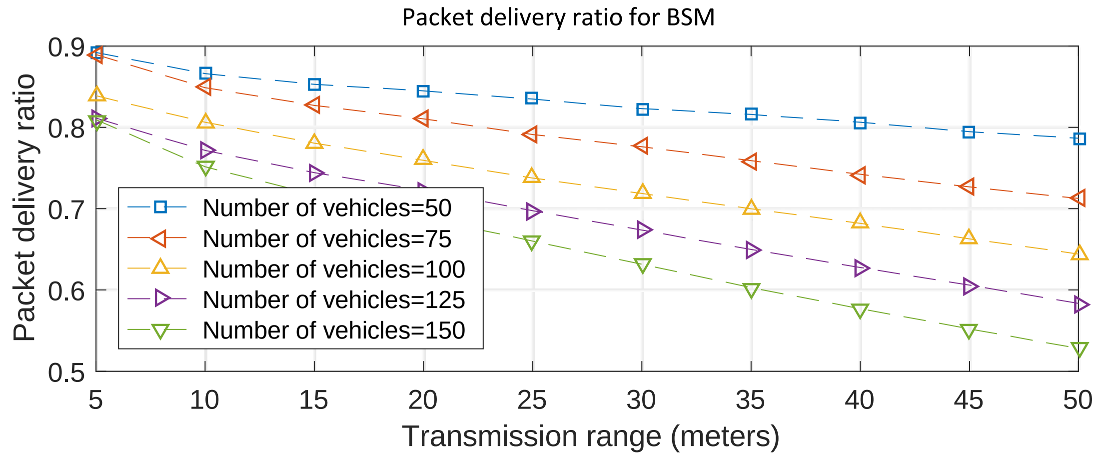
Parameters	Characteristic	Values (default underlined)
Routing	The routing protocol for multihop messages	AODV or OLSR
Protocols Number of Nodes	Number of nodes in the network	50, 100, 150, or 200 nodes
Number of Sinks	Number of data sinks for multihop messages	10, 20, or 30 nodes
Transmit Power	Transmit power of BSM	10, 20, dBm (10, 100 mWatts)
Path Loss Model	The power loss between two arbitrary chosen points	Two ray
Fading	Random fluctuation of signal by small scale diffraction and reflection	Nakagami (m=1)
Node Speed	The speeds of vehicles on the network	22, 33, 44, or 55 mph
BSM Size	The size of safety messages	100, 125, 150, 175, or 200
BSM Interval	The frequency of BMS broadcasting	0.1, 0.2, 0.3, or 0.4 sec
Area	The simulated vehicular area	300 m by 1500 m (0.45 km^2)

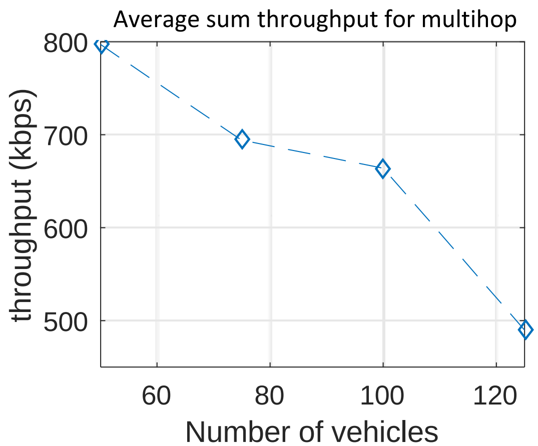
- We develop our own system-level DSRC-based simulation with multihop
- Task 2 focuses not only on testing various parameters but also on stressing the network in order to understand the key variables and bottlenecks

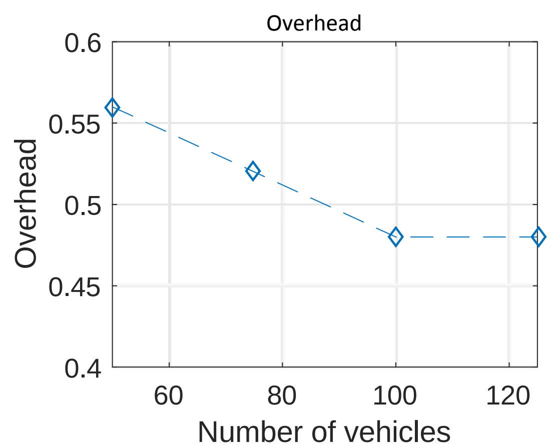
Performance Metrics

- **Packet delivery ratio (PDR)**
  - PDR = Packets successfully received/Total packets transmitted
  - For safety applications, we expect PDR should be greater than 0.9.
- **Overhead**
  - Overhead = 1 – Total application packets/Total transmitted packets
  - Application packets include WAVE and multi-hop packets
  - Transmitted packets include Application packets plus non-application packets such as control packets for the MAC layer
- **Average throughput**
  - Total received multi-hop packets at all sinks in bits averaged over total simulation time (**average sum end-to-end throughput**)

The Effect of Traffic Congestion

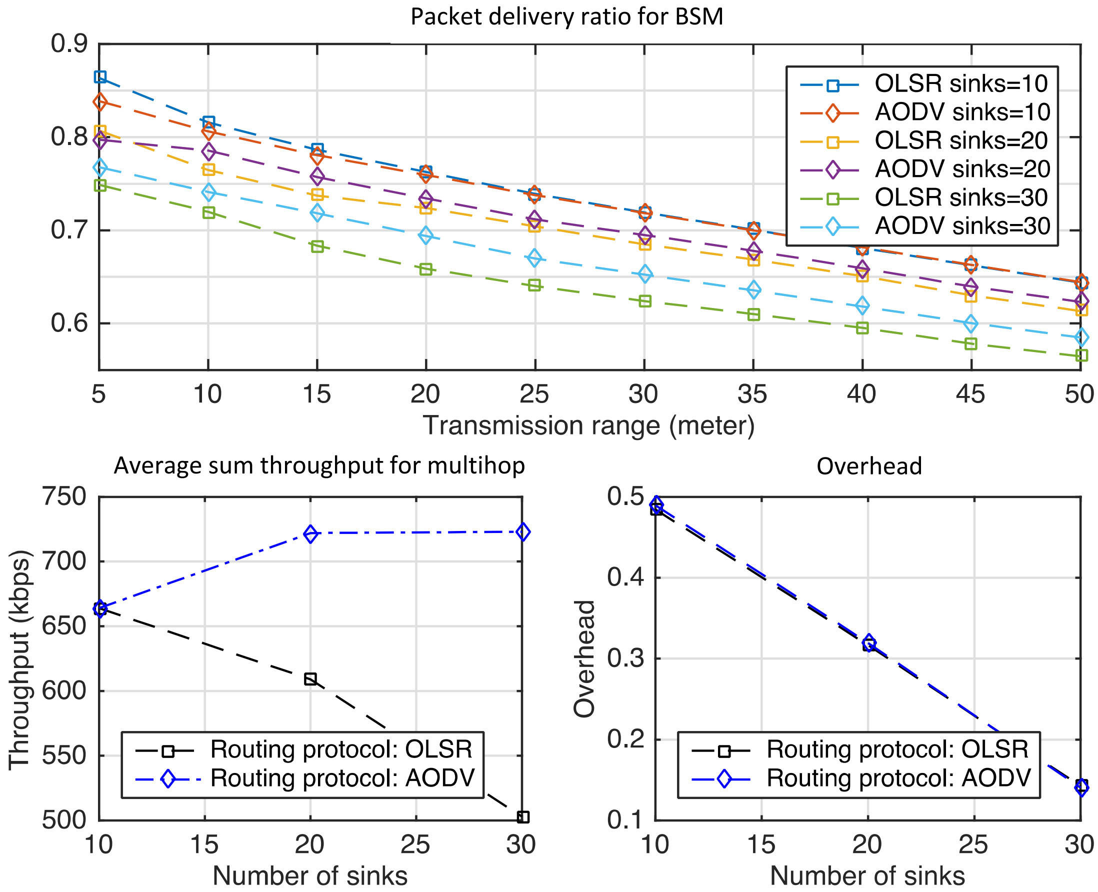






- The number of vehicles in the network varies from 50 to 150
- PDR of BSM decreases with:
  - Number of vehicles (more interference)
  - Transmission range (reduced SNR)
- Throughput and overhead both decrease with number of vehicles

The Effect of the Routing Protocol



- Sinks = number of source-destination pairs
- AODV finds routes only when they are requested
- OLSR discovers all the routes in advance, which constantly burns resources
- As the number of sinks increases, AODV outperforms OLSR.

Technical Comparison Summary

Parameters	DSRC	LTE
Packet delivery ratio	0.82 (100 vehicles/km^2 at 50 meter distance)	>0.95 [MIR]
Throughput	760 kbps (per vehicle)	7.2 Mbps (per vehicle) @ average range = 120m
End-to-end delay	230 msec	50 msec [GHO]
Max distance	130 m	3500 m

- DSRC PDR and Throughput were from our simulations
- LTE Throughput is based on separation of 300m and typical average sum throughput results for an LTE cell
- Maximum ranges are computed by detailed link budget analysis
    - Path loss exponent α = 3 for both DSRC and LTE
    - DSRC being omni-directional, LTE has 27 dBi gain

LTE outperforms DSRC in terms of PDR, T'put, delay, and range

[MIR]: Z. H. Mir and F. Filali, "LTE and IEEE 802.11p for vehicular networking: a performance evaluation," *EURASIP J. on Wireless Commun. and Networking*, vol. 2014, no. 1, pp. 1–15, 2014.
[GHO] A. Ghosh, J. Zhang, J. G. Andrews, and R. Muhamed, "*Fundamentals of LTE*," Pearson Education, 2010.

Deployment Cost Model

- **RSU equipment cost**
  - Includes the cost of RSU, power connection, communication connection, and additional traffic sensors.
  - Derived from recent DSRC deployed data [WRI].
- **RSU installation cost**
  - Includes the cost of installation labor, and inspecting construction.
  - Specifically, we assume labor costs $2,475 and inspection costs $1,075. [WRI]
- **Network planning cost**
  - Includes the cost of identifying radio interference, optimizing RSU sites, developing local maps, and controlling local traffic during construction.
  - Radio surveying costs $1,000, obtaining local map and site planning cost $1,550. Design, traffic control, and system integration costs $4,100[WRI]

[WRI]: J. Wright, et. al., "National connected vehicle field infrastructure footprint analysis," Tech. Rep. FHWA-JPO-14-125, available at http://ntl.bts.gov/lib/52000/52600/52602/FHWA-JPO-14-125_v2.pdf

Deployment Cost Model

- **Backhaul connection cost**
  - This varies greatly depending on the capacity and location.
  - If backhaul for traffic lights is already installed then backhaul cost could be $3,000 or less
  - For connected vehicle applications, this might increase up to $40,000
- **Operating cost**
  - Includes electricity fees and maintenance, plus future replacement costs.
  - Electric fee is calculated based on the U.S. average
  - Annual maintenance cost is assumed to be 5% of RSU equipment cost and RSU installation cost.
  - The replacement cost is calculated based on the assumption that a RSU will be replaced every 10 years
- **Rental fee:**
  - The site rental fee is set at $200, but this can vary a lot, from $0 if using a TXDOT site to several times this for prime private mounting locations

DSRC Infrastructure Cost Summary

Category	Description	Price
CAPEX	RSU equipment cost/site	$7,480
	RSU installation cost/site	$3,597
	Network planning cost/site	$6,650
	Backhaul cost/site	$5,000
	Total CAPEX	$22,727
OPEX/year	Power consumption/year	$100
	Rental fee/year	$200
	Maintenance cost/year	$332
	Replacement cost/year[9]	$738
	Total OPEX	$1,371

Cost Comparison: DSRC vs. LTE

Coverage areas	No. RSUs	Yearly Cost	Monthly cost
Entire Texas road	1.5M	$5,7B	$95.10
Local roads	1.0M	$3,8B	$64.18
Major collectors	0.32M	$1.2B	$19.78
Principal highways	0.16M	$0.61B	$10.10
Interstates Only	0.016M	$0.062B	$1.04

Connection Type	Service provider	Monthly fee	Modem price
Tablet	Verizon 6GB	$50	$49(2year contract)
	AT&T unlimited	$100	Free
	AT&T 5GB	$50	Free
Internet of Things (IOT)	ATT IOT	$8 (BSM packets only)	$99 (Starter kit)
	ATT IOT (Audi/Porsche)	$10	included

- We consider 10 road side units per every 1 mile (conservative: T=160meter)
- Yearly cost combines the CAPEX and OPEX with return of interest 10 percent
- Detailed cost estimate for DSRC is included in memorandum 2
- A computable excel file is also included as a Deliverable

[Building a True DSRC Network is Very Expensive]

Task 1 and 2 Conclusions

- DSRC's short range and low PDR limits the applications that can benefit from this technology
  - The throughput per vehicle is also about 10x below LTE, and will be another order of magnitude (or more) below 5G
  - Increasing the range by multi-hopping does not appear very feasible
- Building a DSRC-based infrastructure will be quite expensive and time-consuming
  - The cost advantage of DSRC and its free spectrum will decrease or vanish
  - Chicken and egg problem
- We believe most exciting CV applications will probably require LTE or its descendants
  - Even assisted overtaking/passing seems out of DSRC's capabilities

THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

Secure Perception in Connected Vehicles

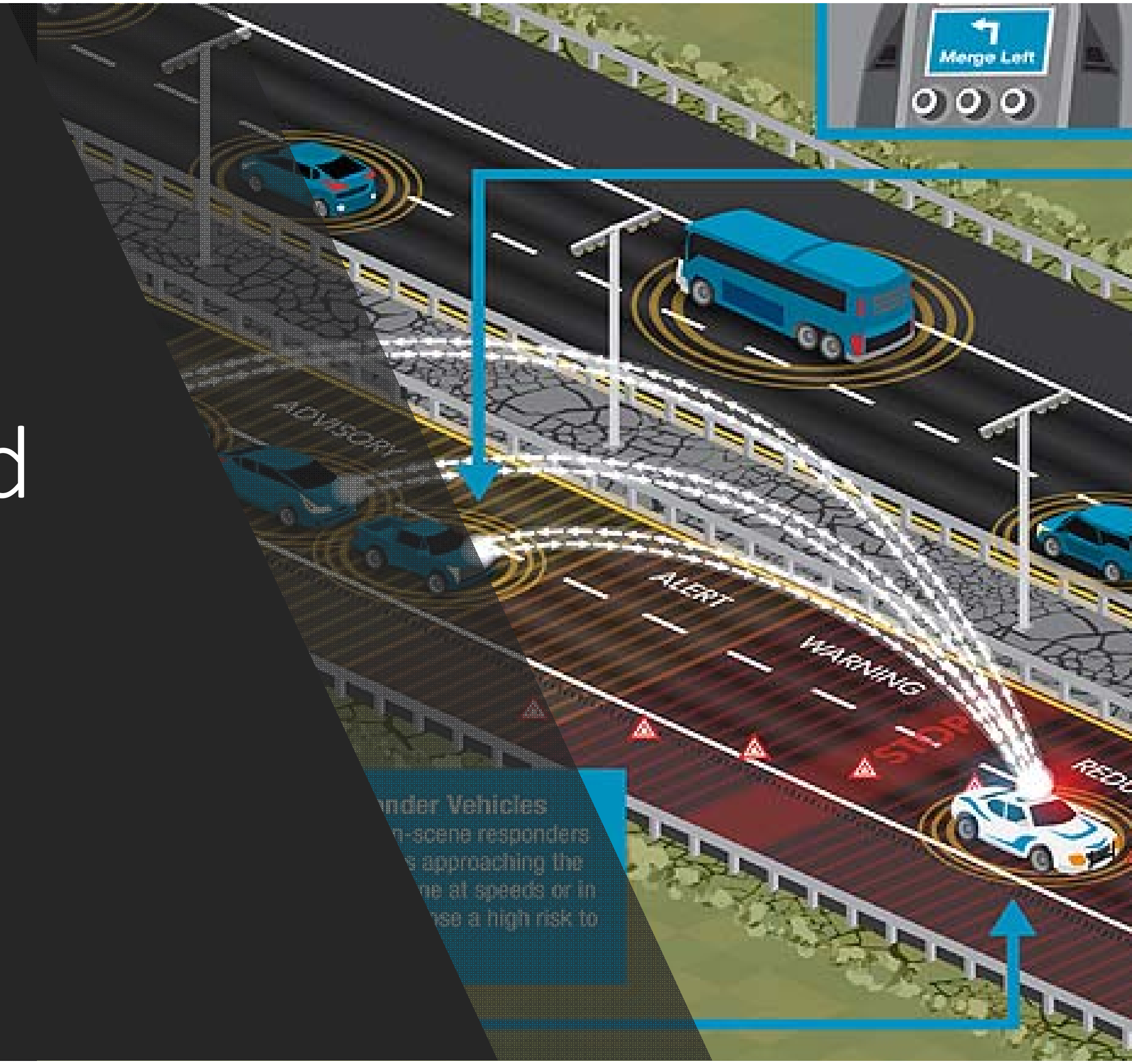
Lakshay Narula[1], Todd E. Humphreys[2]

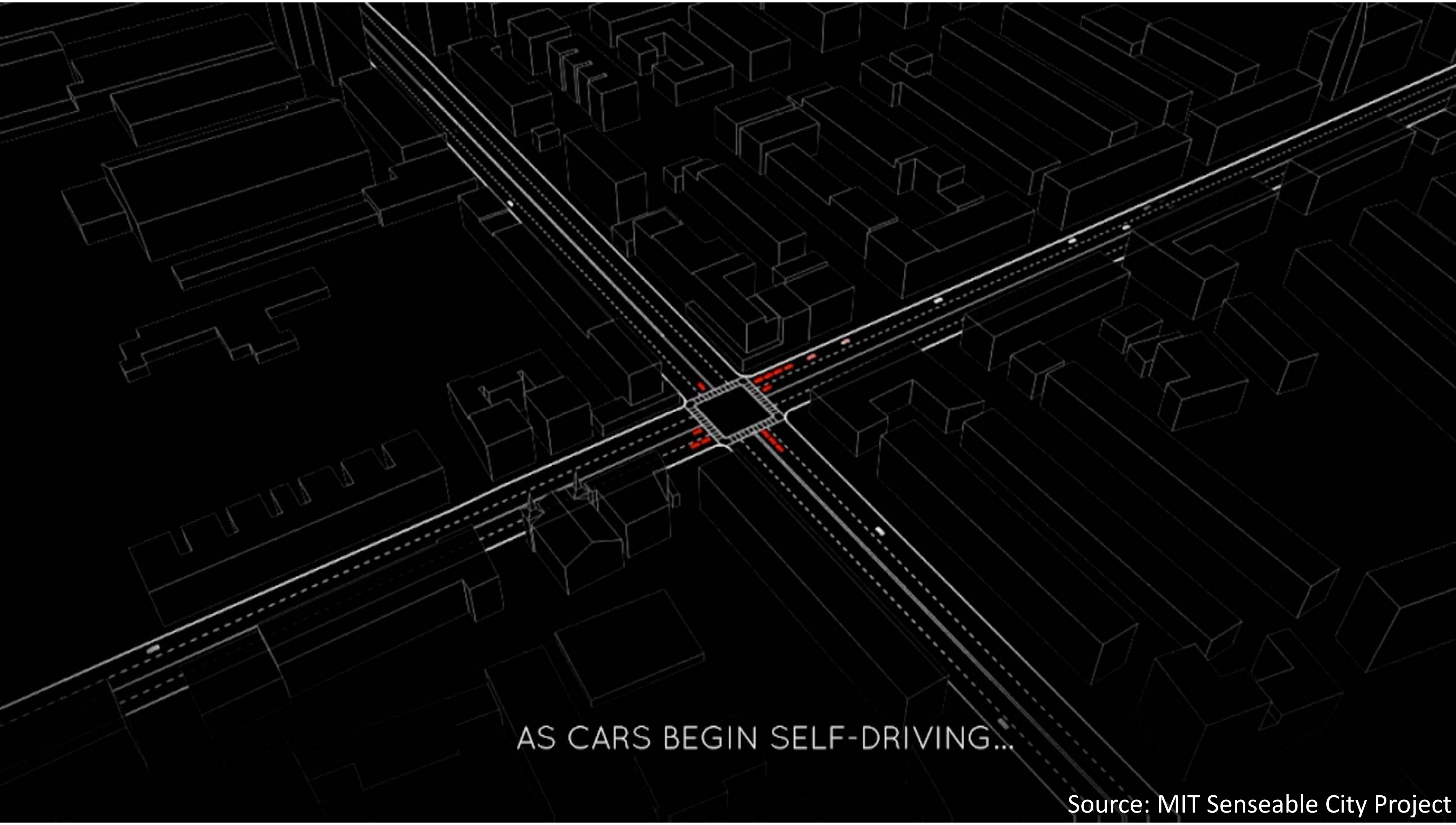
[1]Department of Electrical and Computer Engineering, The University of Texas at Austin

[2]Department of Aerospace Engineering and Engineering Mechanics, The University of Texas at Austin

TxDOT 0-6845 Workshop| November 29, 2016

The Connected Vehicle Dream





Source: MIT Senseable City Project

The Inconvenient Reality of Security

Security Measures in DSRC Standard

IEEE 1609.2 standard for **message security, encryption, and authentication**: A big improvement over some previous standards such as ADSB.

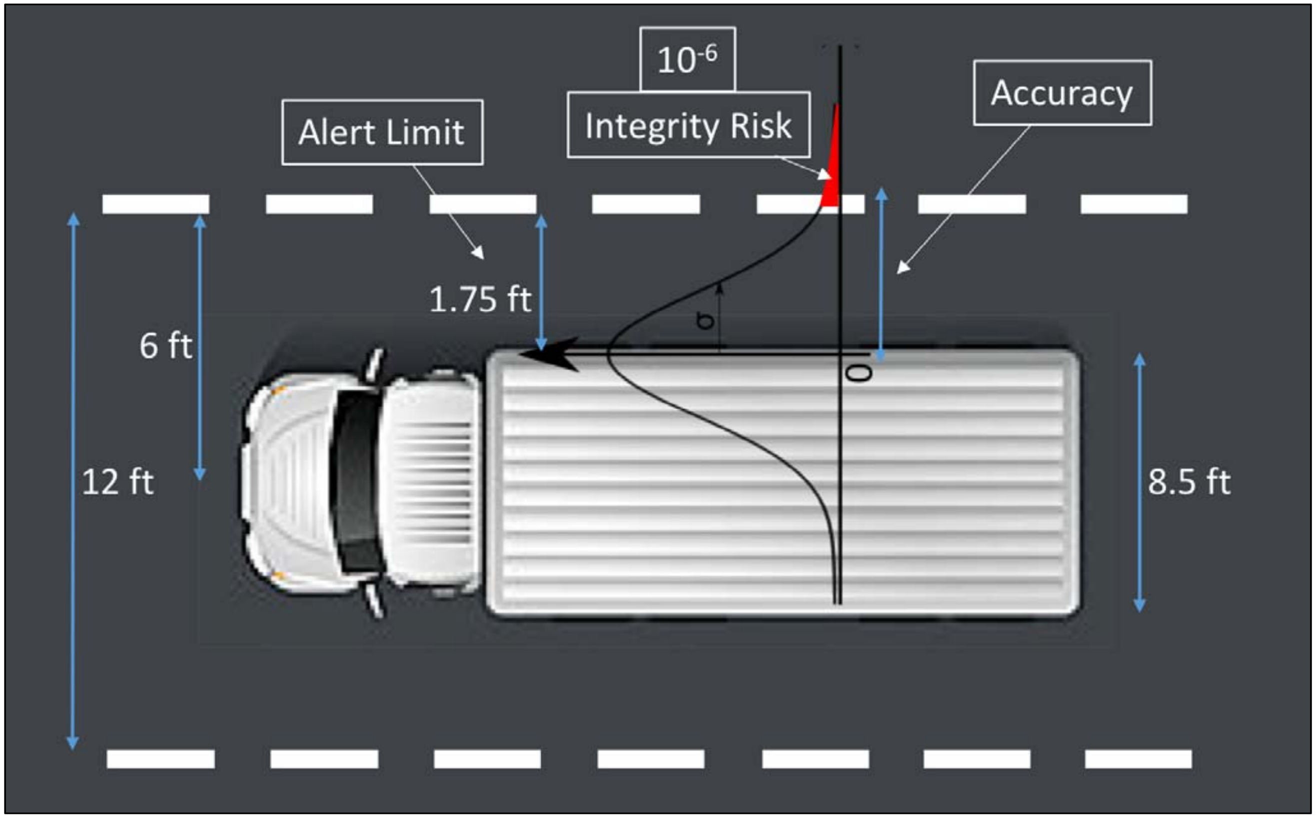
Even so, DSRC does not address the question of a **certified vehicle reporting false position** and velocity.

Are such assumptions vindicated in view of the safety-of-life applications that DSRC supports?

Hacking COTS DSRC equipment to execute **such attacks would not be straightforward**. Would anyone be interested?

Safety of life and **strengthening of human trust in machines** (not just for connected vehicles, but also for other future technologies)

Alert Limits



Why is it important to analyze system accuracy requirements when discussing security?

Motivation:
If a system is able to verify, with complete certainty, that the advertised position is accurate to within 100 meters, is it helpful?

Major Connected Vehicle Security Challenges

1. Secure Self-Localization
2. Internal Attacks
3. DSRC Certificate Revocation Policy

Problem 1: Secure Self-Localization

Connected vehicles require a decimeter-accurate secure position solution for safe operation.

GPS is the most economical and widely used positioning solution.

The UT Radionavigation Lab has led global research in GPS spoofing and anti-spoofing in the last 7-8 years.

Picture shows a recent demonstration of Two-Antenna RTK solution that provides (1) instantaneous centimeter accurate position, and (2) robust anti-spoofing capability.

Problem 2: Internal Attacks

Phantom and Invisible Cars

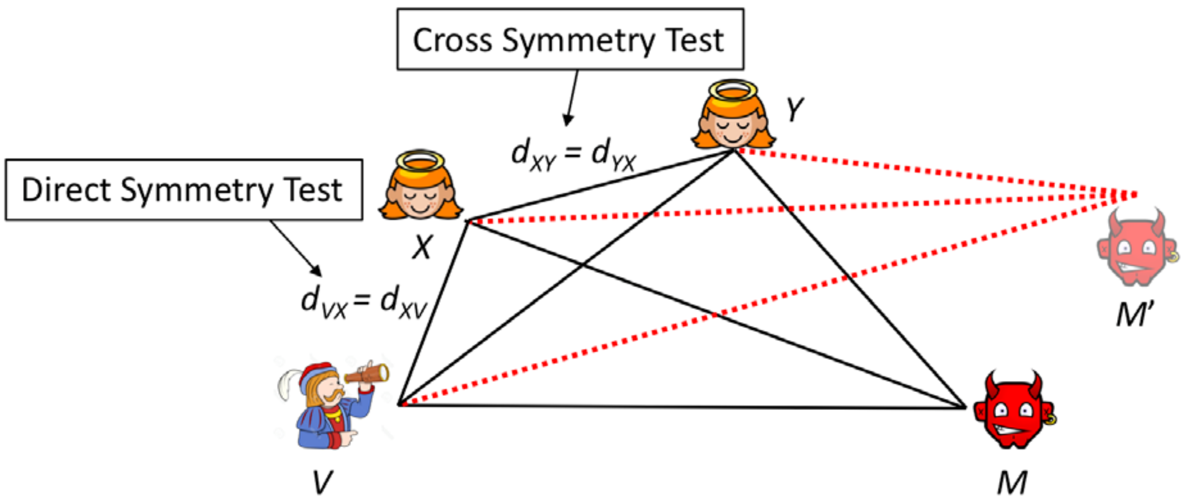
A **phantom car** is fictitious: perhaps a radio device claiming a position right in front of the honest vehicle.

An **invisible car** claims a position that is far away, but is really a close neighbor of the honest vehicle.

These attacks would go unnoticed as DSRC has no provision for verifying the claims made by certified vehicles.

Problem 2: Internal Attacks

State-of-the-art Neighbor Position Verification Scheme



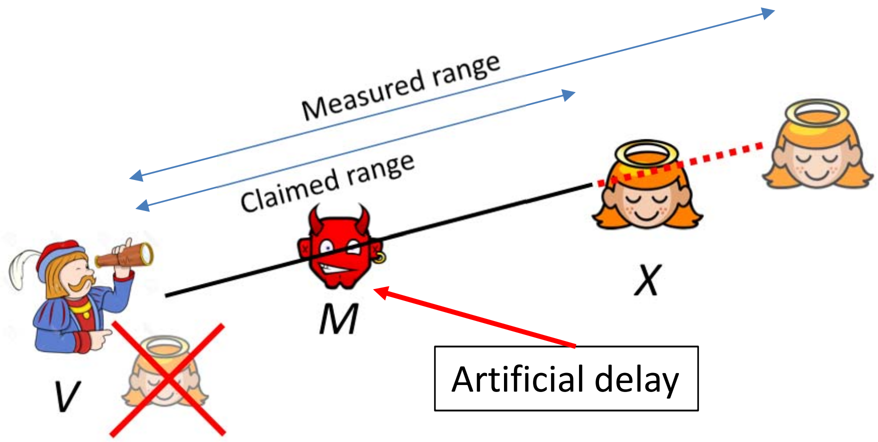
Based on time difference between transmit timestamp and receipt timestamp.

Claim: An internal attack can be detected as long as the number of honest verifiers is greater than the number of colluding internal attackers.

Fiore, Marco, Claudio Ettore Casetti, Carla-Fabiana Chiasserini, and Panagiotis Papadimitratos. "Discovery and verification of neighbor positions in mobile ad hoc networks." *IEEE Transactions on Mobile Computing* 12, no. 2 (2013): 289-303.

Problem 2: Internal Attacks

But we just opened a new can of worms …



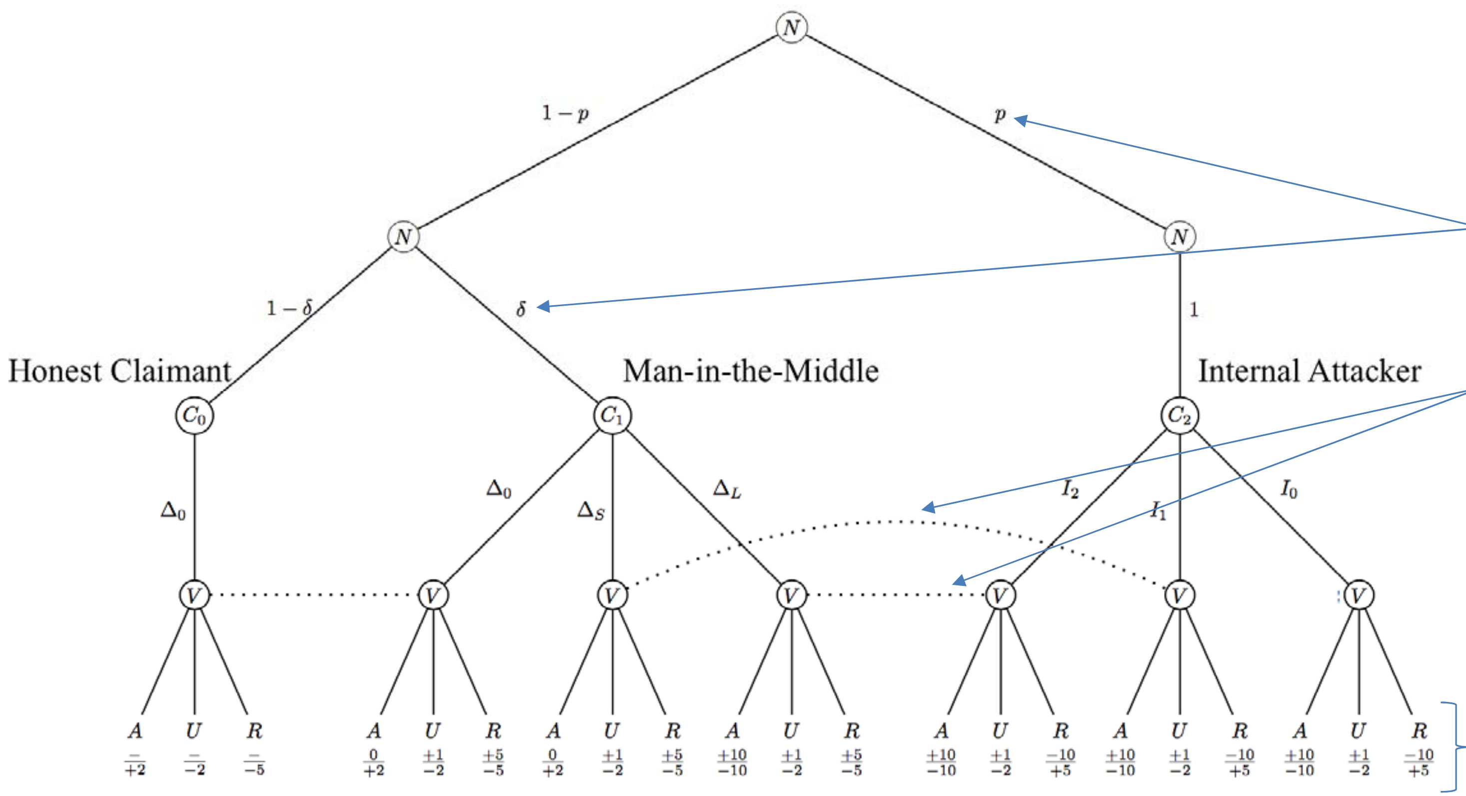
If the time-of-flight is artificially increased, then **advertised range won't match time-of-flight**.

It is easy for a man-in-the-middle attacker to **tarnish the reputation of an honest vehicle**.

From *Verifier*'s perspective, this attack looks no different than an Internal attack. In this case, it must not flag the claimant as malicious. In the case of an Internal attack, it should.

Take-away:
It is perhaps **not optimal to have fixed strategies for fixed observations**. The *Verifier* must take a **Bayesian approach** to formulate a **mixed strategy** and **keep the attacker guessing**.

Solution 2: Game Theoretical Analysis



Verifier has prior beliefs about the claimant.

After receiving the claim, the *Verifier* builds posterior beliefs about the claimant.

Verifier acts optimally under its posterior beliefs.

Problem 3: Certificate Revocation

The *linkage values*-based Secure Credential Management System (SCMS) is an improvement over the credential management system deployed in Europe.

However, the standard is not conclusive about what classifies as misbehavior and under what circumstances the credentials are revoked.

Do a few instances of reported false claims lead to revocation? How do we take MITM attacks or NLOS signals into account?

If a number of infringements are allowed, wouldn't the malicious vehicles prefer to stay in the *gray zone* where their credentials are not revoked?

<u>Take-away</u>: SCMS Revocation Policy is a work-in-progress.

Recommendations

Secure Self-Localization is essential: Two-antenna RTK is one promising solution.

Adopt Game Theoretically Optimal strategies for Neighbor Position Verification.

DSRC Sensor paradigm: DSRC Fusion with Radar for Enhanced Security.

Standardize misbehavior detection and revocation policy in SCMS.

Case Study

Connected Vehicle-Enabled Variable Speed Advisory

Is this the most ground-breaking application of the connected vehicle technology?

No, but…

- ✓ No reliance on automated vehicle technology
- ✓ Works with low penetration of connected vehicles
- ✓ Allows incremental infrastructure roll-out by TxDOT
- ✓ Impacts traffic management on major freeways in Texas

Variable Speed Advisory

- Reduces stop-and-go congestion by speed harmonization
- Prevents or reduces severity of rear-end crashes
- Reduces travel time

Germany has reported 20-30% reduction in crashes on freeways with variable speed limits.

Severity of traffic shockwaves have significantly been reduced in the Netherlands.

Approaches to Variable Speed Advisory

Variable Speed Display Signs

DSRC Beacons (or LTE Small Cells)

Approaches to Variable Speed Advisory

Other Common Infrastructure

- Inductive loops
- Traffic cameras
- Power connection
- Communication backhaul
- et cetera …

Traditional or Wireless?

Which approach to Variable Speed Advisory should TxDOT take?

Connected Vehicle Penetration

Visibility/Communication Range

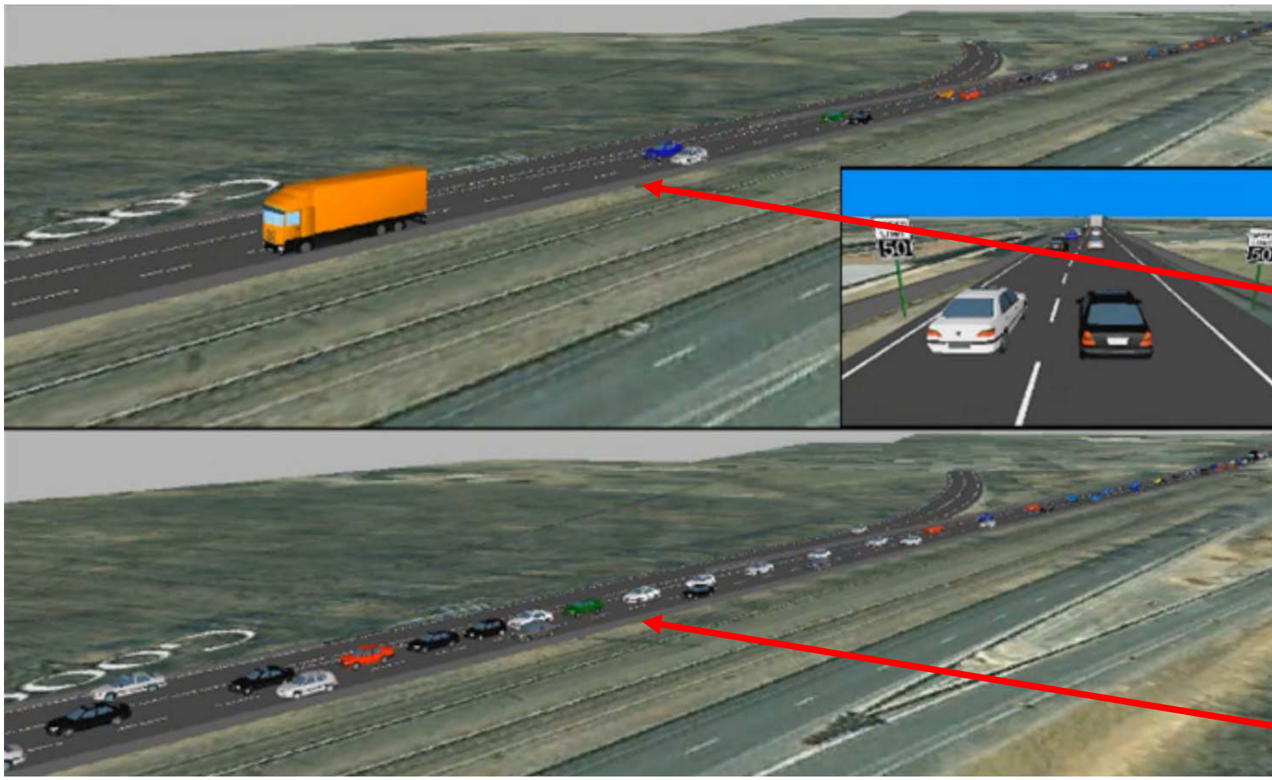
Ease of Installation

Cost to TxDOT

Scalability to Multi-lane Freeways

Distance between Consecutive Signs

Connected Vehicle Penetration



Screenshot of an FHWA simulation (using VISSIM®) of I-66

Traditional variable speed display signs do not rely on connected vehicles.

With variable speed limit
(20% compliance)
Speed range: 28 – 63 mph

DSRC approach can be successful with ≈40 – 50% penetration (achievable by 2030).

Without variable speed limit
Speed range: 0 – 44 mph

Visibility/Communication Range

Visibility of speed limit signs

- Advertised as 1100 feet (less than a quarter-mile)
- Can be much less in inclement weather or dense traffic

Communication range of DSRC

- Typically close to a quarter-mile, but may vary based on local conditions
- Other wireless technologies such as LTE have much larger range

Ease of Installation

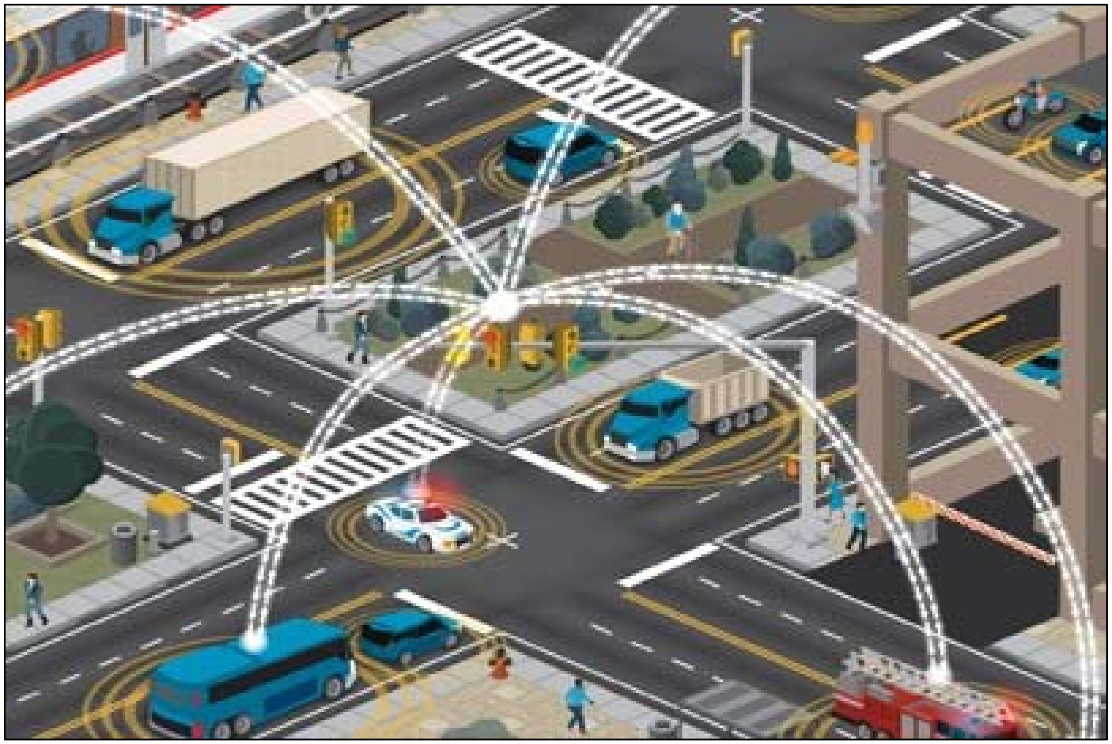
- ❖ Speed limit signs must ideally be overhead
  - Lane closure for installation
  - Heavy equipment involved

- ❖ DSRC beacons can be installed on the roadside
  - ✓ No lane closures
  - ✓ Convenient installation

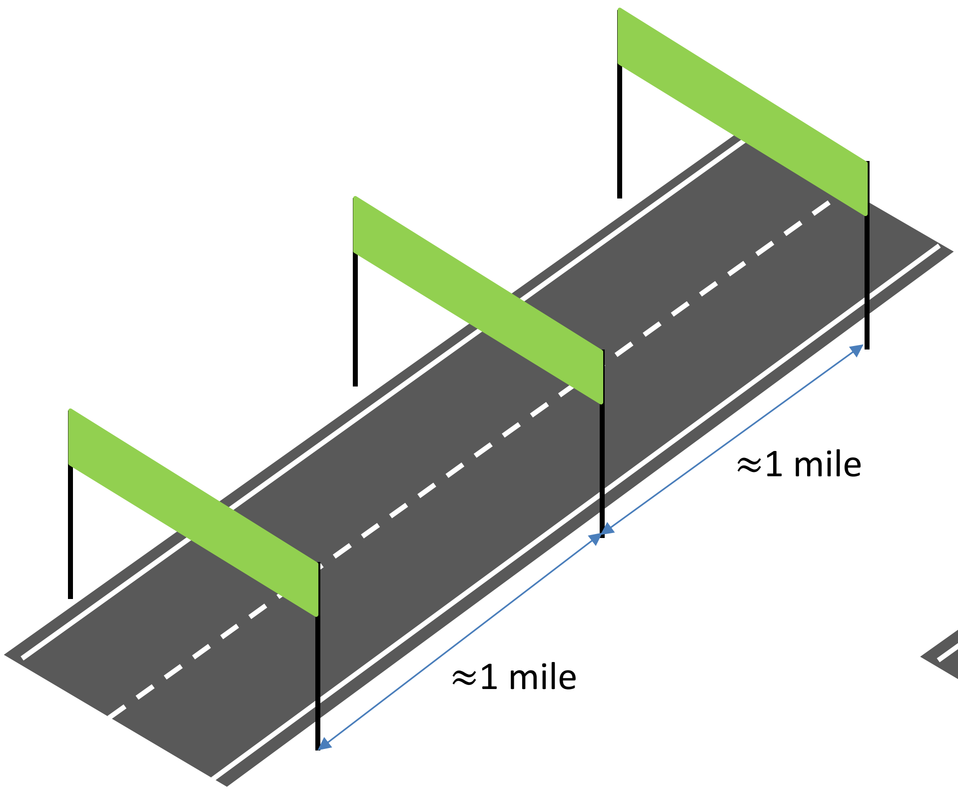
Multiple Lanes

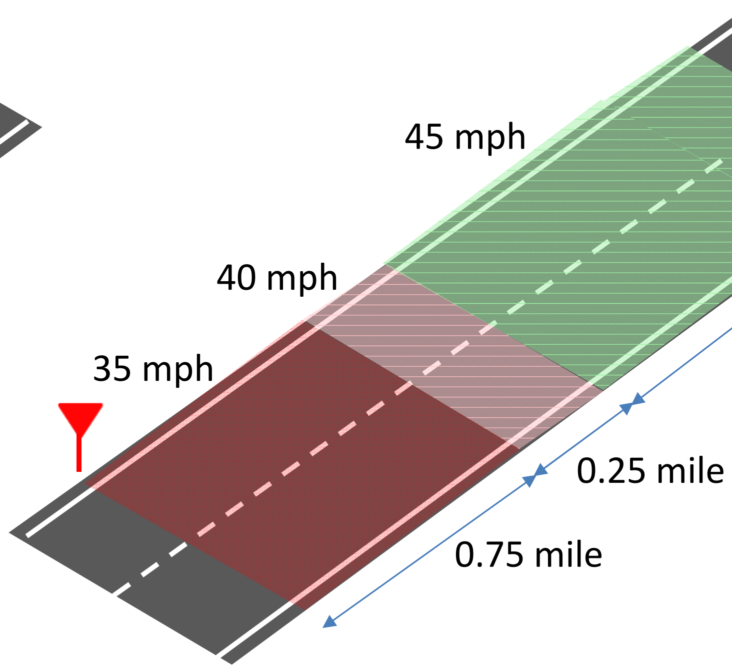
A separate variable speed display sign is needed for each lane.

A single DSRC roadside unit can handle multiple lanes.



Distance Between Consecutive Signs





Cost Comparison (Excluding Common Costs)

30-miles

6-lanes

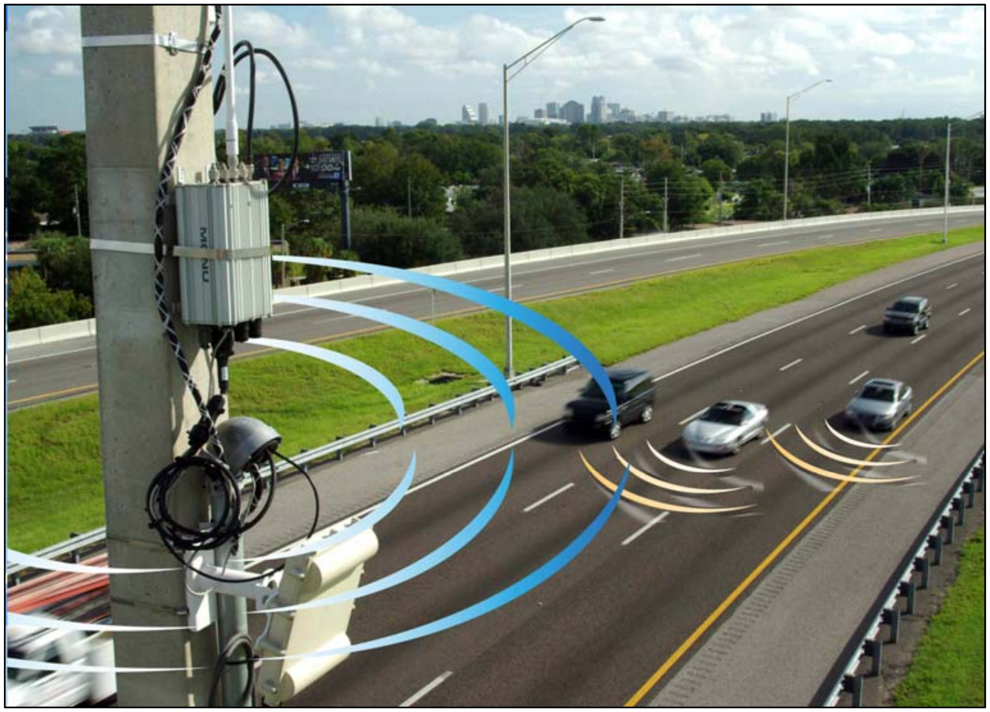
1-mile separation

	Traditional Speed Display	DSRC Beacons
Equipment Cost (per unit)	$3,700	$1,000
Installation Cost (per unit)	$50,000	$2,475
Power Consumption (per unit)	147 W	4 W
Number of Units Required	180	30
Total Equipment Cost (differential)	$3,700*180 = $666,000	$1,000*30 = $30,000
Total Installation Cost (differential)	$50,000*60 = $3,000,000	$2,475*30 = $74,250
Total One-Time Cost (differential)	$3,666,000	$104,250
Total Annual Power Consumption (differential)	$27,450	$126

Deployment Recommendations

Low Connected Vehicle Penetration: Portable DSRC RSU

Non-recurrent Congestion



High Connected Vehicle Penetration: DSRC Infrastructure

Recurrent Congestion