CONFIDENTIAL

DSRC Research Topics for 07-09

Ken Laberteaux

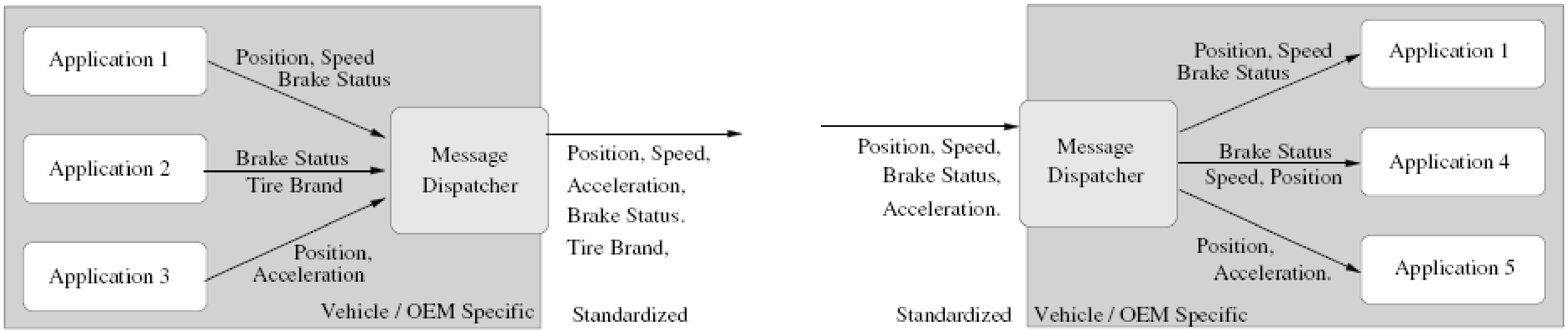
These slides reflect the opinions of the author,
and are not necessarily the views of any organizations
with which the author associates.

CONFIDENTIAL

Standard Message Composition

Goal: Explore, Test, Adopt standard method for safety message composition

<u>Proposed Solution</u> Message Dispatcher

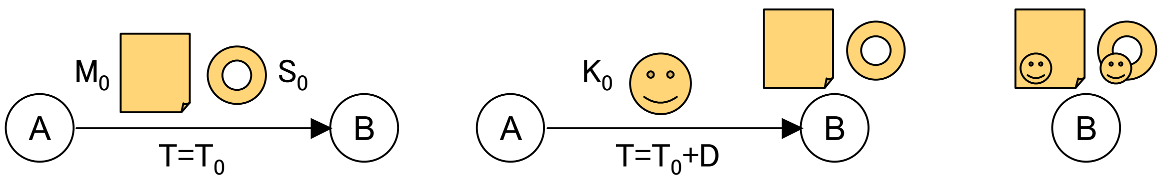


Included in SAE Standard J2735. Also VANET06 Paper *Efficient Coordination and Transmission of Data for Cooperative Vehicular Safety Applications*, Robinson et al.

Security-Message Authentication

Goal: Reduce overhead, "Improve" privacy, Propose certificate dissemination/revocation

<u>Proposed Solution</u> Consider reducing security overhead. One candidate: TESLA authentication with periodic PKI certificate broadcasts. Infrastructure-based revocation



TESLA (Time Efficient Stream Loss-Tolerant Authentication) A "Key" will be transmitted immediately after "message" and "signature" transmission: high-reliability with low communication budget.

CONFIDENTIAL

US-European Cooperation on Security

Harmonization of VANET Security method is desirable

Proposal:

CAMP

CAR 2 CAR
COMMUNICATION CONSORTIUM

VSC-A
Security

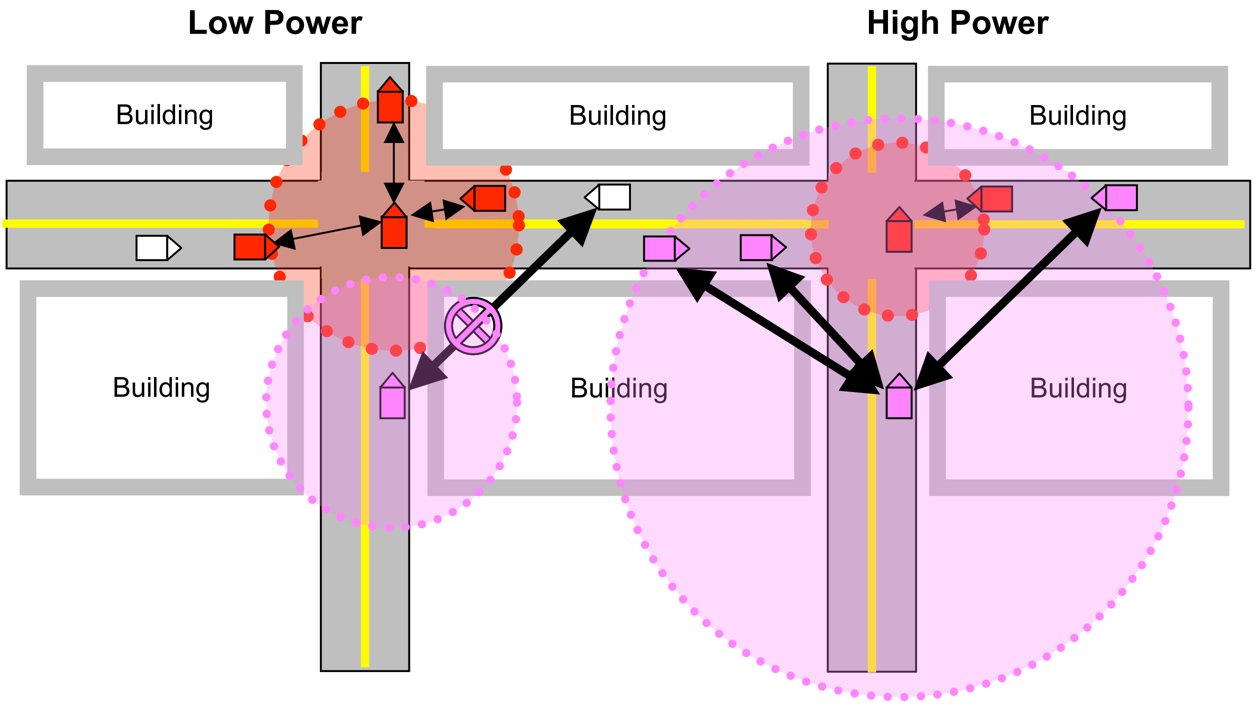
SEVECOM

First Meeting: November 16, 2006, Berlin

CONFIDENTIAL

High Power Testing

Goal: Reduce need for infrastructure by using higher power DSRC



High Power Testing (cont)

DSRC mostly tested at medium power (0.1 watt=20 dBm). High power (4 watt=36 dBm) not tested

Power	*Example*	*Comment*
10 watts	Cell Phone Tower (10 km)	Max DSRC focused antenna output (approx)**
4 watts	CB Radio (5-8 km)	Max DSRC antenna output (approx)*
3 watts	Cell Phone (10 km)	Lower power due to battery
0.8 watts		Max DSRC antenna input (approx)
0.1 watts	WiFi (0.1 km)	Level for past DSRC testing

* DSRC omni-directional antennas often have 3-9 dB of gain. **Max directional antenna output in US is 44 dBm=25 watts (EIRP)

However, DSRC (5.9 GHz) band will not penetrate as well as lower band cell phone and CB

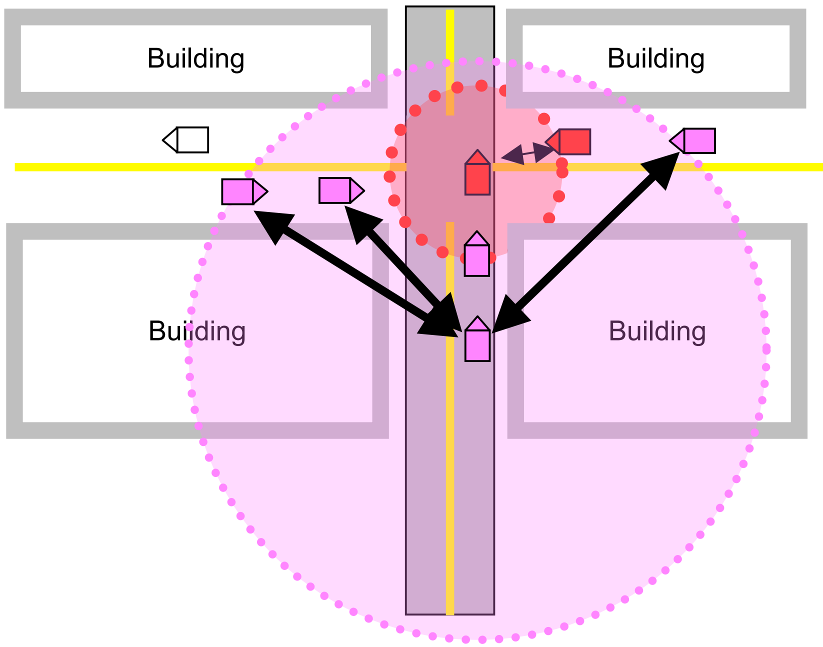
Expected outcome: Full testing of high-power DSRC.
Answer to question: What will it go through?

CONFIDENTIAL

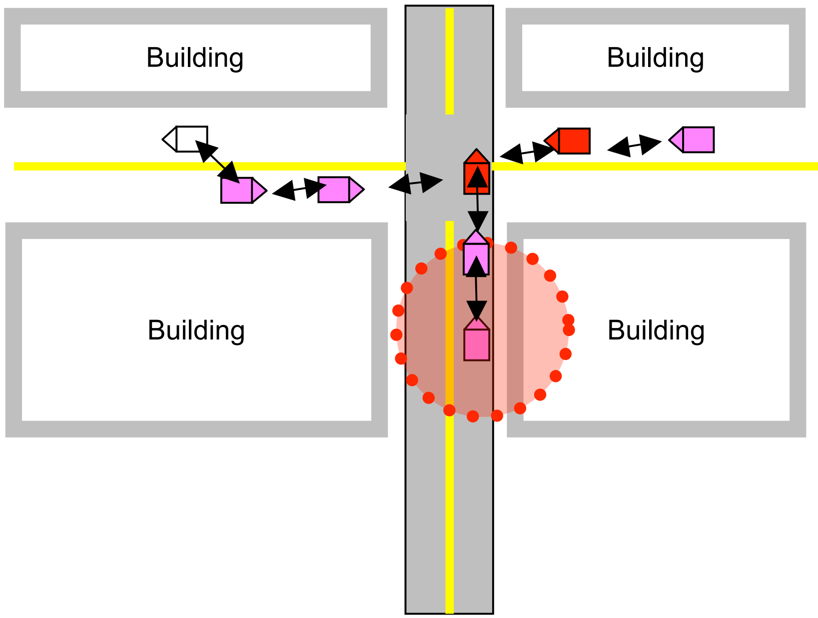
Message Dissemination

Goal: Find Optimal Balance between multi-hop and power control

High Power with Power control



Multi-Hop



CONFIDENTIAL

DSRC Standards Validation

Goal: Validate and Optimize 802.11p(a) for Vehicular Environment

802.11p (PHY for DSRC) is very similar to 802.11a (See UC-Berkeley analysis on right*)

However 802.11a was designed for fixed, indoor usage

**Comparison of Physical Layer between DSRC and IEEE 802.11a,* Wanbin Tang, UC-Berkeley Report, Oct 2006.

PLAN: Verify current 802.11p performance. If needed, investigate small modifications to current 802.11 chipsets to allow best performance for DSRC.

Parameter	**DSRC**	**IEEE 802.11a**
Information Date Rate	3, 4.5, 6, 9, 12, 18, 24 and 27Mbits/s (3,6, and 12Mbits/s are mandatory)	6, 9, 12, 18, 24, 36, 48, and 54Mbit/s.
Modulation	BPSK OFDM QPSK OFDM 16-QAM OFDM 64-QAM OFDM	BPSK OFDM QPSK OFDM 16-QAM OFDM 64-QAM OFDM
Error Correction Coding	K=7 (64 states) Convolutional Code	K=7 (64 states) Convolutional Code
Coding Rate	1/2, 2/3, 3/4	1/2, 2/3, 3/4
Number of Subcarriers	52	52
OFDM Symbol Duration	8.0us	4.0us
Guard Interval	1.6us	0.8us
Occupied bandwidth	8.3MHz	16.6MHz
Frequency	5.850~5.925 GHz	5.15~5.25GHz, 5.25~5.35GHz, 5.725~5.850GHz

Channel 172-Multi Channel Behavior

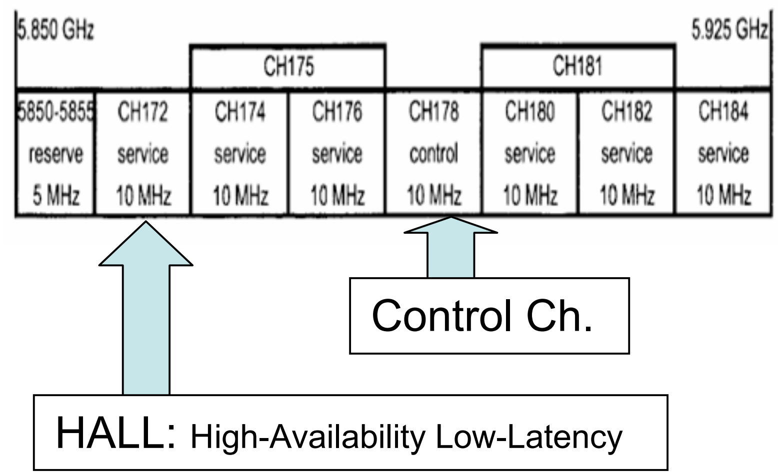
Goal: Find Optimal use of new HALL channel for V2V Safety

New FCC ruling for DSRC Ch 172:

Dedicated V-V Safety for Accident Avoidance and mitigation

However, DSRC requires monitoring Control Channel.

Previously, V-V safety performed in Control Channel.



New FCC rule for 172 channel for safety application

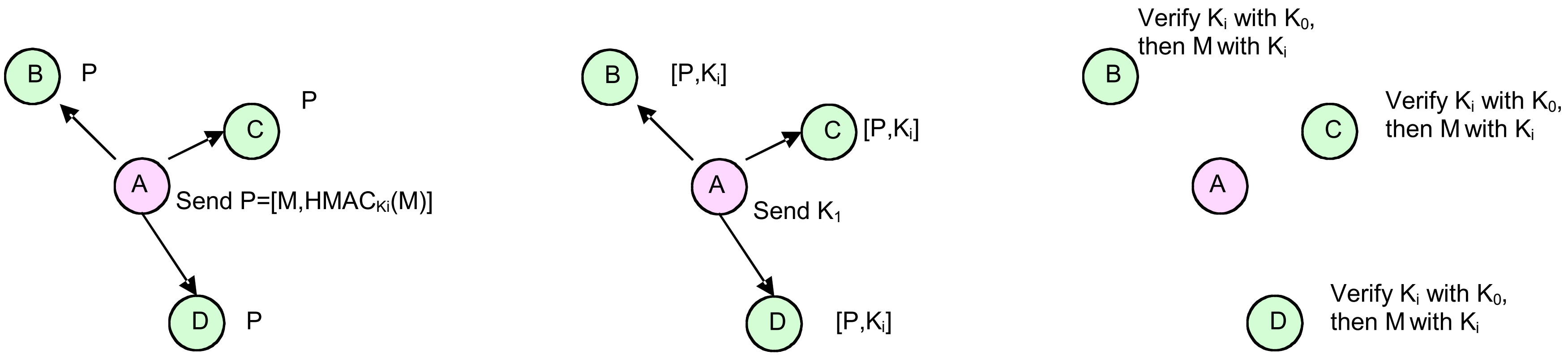
Expected outcome: Recommendation on multi-channel behavior. Multi-channel radio evaluated.

Additional Technical Details on a TESLA-based security scheme for VANET

CONFIDENTIAL

Secure Authentication using TESLA

TESLA (Timed Efficient Stream Loss-tolerant Authentication)



Time $\in [T_{i-1}, T_i)$
A broadcasts message *M* and its signature. *B-D* store unverified message

Time $= T_i = T_{i-1} +$ Ä
A broadcasts its last key, K_i. Further, *B-D* ignore later messages using K_{i-1}

Time $< T_i + \varepsilon + \delta$
B-D receive K_i, verify K_i using K_0, verify message

Small Key's sent after message is sent. Adds Δ delay, but reduces overhead substantially.

CONFIDENTIAL

TESLA Certificates

Certificates bind keys to identities. A *Certificate Authority (CA)* authenticates certificates through signatures.

TESLA Certificate

Node ID (<88)	Node Pub key (256)	CA Signature (512)

TESLA Params (64)	K_0 (80)	Node Signature (512)

TESLA Certificate of PKI strawman. The CA Signature binds the Node ID to the Node's Public Key. If using the Vehicle Identification Number (VIN), the Node ID will be less than 88 bits. The size and contents of Node's public key and CA Signature depends on the PKI signature scheme used. P1609.2 dictates 256 bit ECDSA public keys and 512 bit (or larger) CA Signatures. Certificate

PKI Certificate

Node ID (<88)	Node Pub key (256)	CA Signature (512)

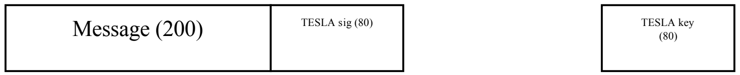
Certificate of TESLA strawman. CA Signature binds the Node ID to the Node's Public Key. In turn, the Node's public key is used to authenticate the Node's anchor, i.e. the TESLA Parameters and the hash chain root K0. If using the Vehicle Identification Number (VIN), the Node ID will be less than 88 bits. The size and contents of Node's public key and CA and Node Signatures depends on the PKI signature scheme used. P1609.2 dictates 256 bit ECDSA public keys and 512 bit (or larger) CA and Node Signatures.

TESLA Certificates are approximately 2x larger than PKI Certificates (sent 1 Hz/car), BUT…

TESLA Authentication (Keys)

Authentication occurs when a message is *signed* by a trusted key.

TESLA Authentication



Certificate TESLA signature case: A 200 bit Heartbeat message along with its 80 bit signature. In addition, a key is subsequently released to verify the TESLA sig. In some cases, a single TESLA key can be used for multiple TESLA signatures. In this case we assume that signatures and keys are 10 bytes.

PKI Certificate

PKI signature case: A 200 bit Heartbeat message along with its 512 bit signature, assuming that signatures are 64 byte ECDSA as proscribed by P1609.2.

TESLA Keys are much smaller than PKI Keys (sent 10 Hz/car)

With 100 cars, TESLA scheme has 286 Kbps (approx) less overhead than pure PKI

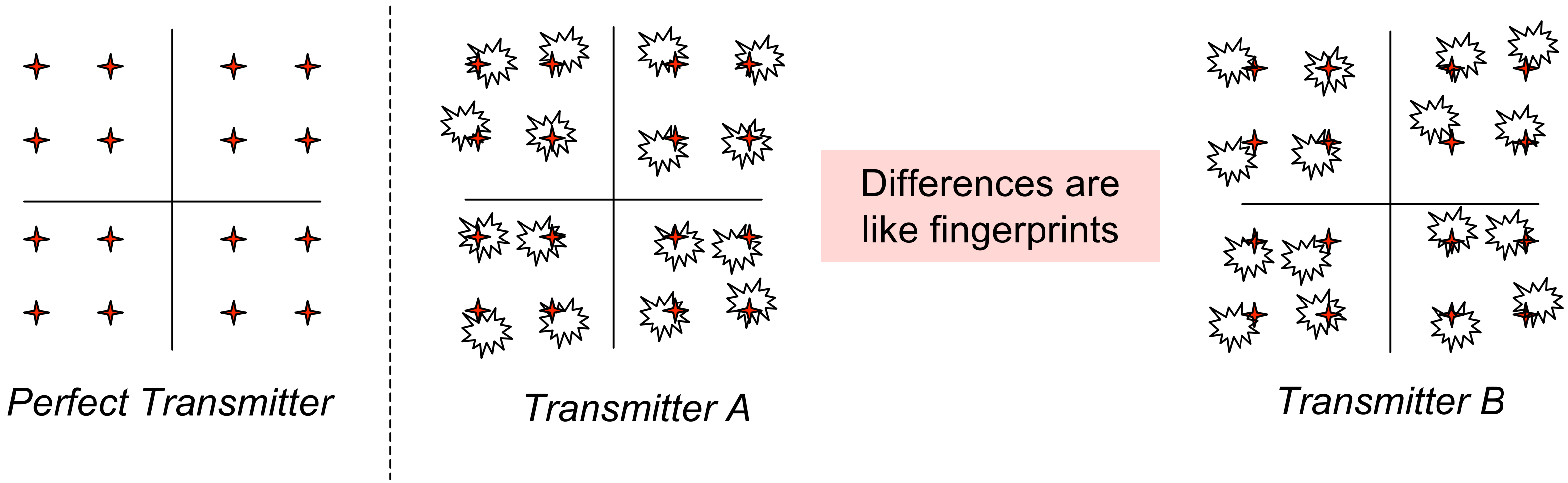
Privacy

Complete privacy **conflicts** with complete accountability.

Acceptable trade-off must be found.

If there is to be accountability, someone (e.g. government) can link a pseudonym to actual identity.

Also, Wireless Fingerprinting will be possible (except with very high cost parts)



Privacy solutions should be proportional to realistic threat model.

Q&A

Ken Laberteaux

Senior Principal Research Scientist

Toyota Technical Center-TEMA

1555 Woodridge Ave.

Ann Arbor, MI 48105 USA

+1 734 995 4307

ken.laberteaux@tema.toyota.com