Vehicle Safety Communications in DSRC

Jinhua Guo, Ph.D.

Director of Vehicular Networking Systems Research Lab
Department of Computer and Information Science
University of Michigan-Dearborn
jinhua@umich.edu

2006 US Army VI Winter Workshop
Outline

• Intelligent Transportation Systems (ITS)
• Dedicated Short Range Communication (DSRC)
• Intelligent Vehicle Applications Enabled by DSRC
• Media Access Control (MAC) Protocols and Quality of Services
• Security and Privacy
What are Intelligent Transportation Systems?

• Information technologies (computing, sensing, and communications) applied to transportation systems
  - To manage it in a safe and efficient manner
  - To monitor traffic conditions (accident, incidents, construction work, major events)
  - Control traffic flow
  - To provide information to the motoring public about traffic conditions
ITS Benefits

- Improved safety to drivers
- Improved traffic efficiency
- Reduced traffic congestion
- Improved environmental quality and energy efficiency
- Improved economic productivity
Achievements to date

- Traffic Management Centers have been created in two-thirds of the 75 largest metropolitan areas.
- Traffic signals and ramp meters have been tuned to improve traffic flow and safety.
- Travel information is more readily available to the public to assist in their travel planning and decision-making.
- Electronic toll collection has been installed on 70% of existing toll road mileage and over ten million toll tags have been issued in North America.
- Non-toll electronic payment applications have begun to appear.
Next Wave: Cooperative Vehicle Highway Systems (CVHS)

• Cooperative Vehicle-Highway Systems (CVHS)
  – Vehicles cooperate with each other and the highway.
  – Information concerning traffic ahead, obstacles, and road and weather conditions were flowing as freely between electronic subsystems on the vehicle and road-side computers.

• Cooperative Systems Rely on
  – Wireless communication
  – Digital map and Satellite Position
DOT ITS Initiative: Vehicle Infrastructure Integration (VII)

• Vision:
  – To achieve nationwide deployment of an integrated communications infrastructure on the roadways and in all production vehicles to enable a broad range of safety and mobility services that today are unattainable.

• Crash prevention and congestion relief through vehicle-to-vehicle and vehicle-to-roadside communication
National ITS Architecture
(http://itsarch.iteris.com/itsarch/html/entity/paents.htm)
Future Intelligent Transportation Systems
5.9 GHz DSRC/WAVE

- 5.9 GHz DSRC (Dedicated Short Range Communications) is a short to medium range communications service that supports both Public Safety and Private operations in roadside to vehicle and vehicle to vehicle communication environments. DSRC is meant to be a complement to cellular communications by providing very high data transfer rates in circumstances where minimizing latency in the communication link and isolating relatively small communication zones are important.

- It is also called WAVE (Wireless Access in Vehicular Environments), IEEE 802.11p
Unique Capabilities of DSRC

- 75 MHz of spectrum in the 5.9 GHz range
- Radio Range: 100 ~ 1000 meters
- Very low latency: 200 microseconds
- Data rate: 6 to 27 Mbps
- Support point-to-point and broadcast communication.
- Vehicle to roadside & vehicle to vehicle
- Highly available
How is DSRC different from other radio communications?

<table>
<thead>
<tr>
<th></th>
<th>DSRC</th>
<th>Cellular Phone</th>
<th>Satellite</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Range</strong></td>
<td>100 ~ 1000 meters</td>
<td>kilometers</td>
<td>thousands of kilometers</td>
</tr>
<tr>
<td><strong>Data Rates</strong></td>
<td>6 to 27 mbps</td>
<td>present &gt;10kbps</td>
<td>future 2-3 mbps</td>
</tr>
<tr>
<td><strong>Latency</strong></td>
<td>200 micro seconds</td>
<td>1.5 ~ 3.5 seconds</td>
<td>10 ~ 60 seconds</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>none</td>
<td>$</td>
<td>$$$</td>
</tr>
</tbody>
</table>
## Comparison With Existing DSRC

<table>
<thead>
<tr>
<th>PARAMETERS</th>
<th>902 - 928 MHz Band</th>
<th>5850 - 5925 MHz Band</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPECTRUM USED</td>
<td>12 MHz (909.75 to 921.75 MHz)</td>
<td>75 MHz</td>
</tr>
<tr>
<td>DATA RATE</td>
<td>0.5 Mbps</td>
<td>6 Mbps - 27 Mbps</td>
</tr>
<tr>
<td>COVERAGE</td>
<td>One communication zone at a time</td>
<td>Overlapping communication zones</td>
</tr>
<tr>
<td>ALLOCATION STATUS</td>
<td>No protection</td>
<td>Primary Status (high protection)</td>
</tr>
<tr>
<td>INTERFERENCE POTENTIAL</td>
<td>Many 900 MHz Phones,</td>
<td>Sparsely located Military Radars,</td>
</tr>
<tr>
<td></td>
<td>Many Rail Car AEI Readers,</td>
<td>Very Sparsely located Satellite Uplinks</td>
</tr>
<tr>
<td></td>
<td>Many Spread Spectrum Devices,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wind Profile Radars</td>
<td></td>
</tr>
<tr>
<td>MAXIMUM RANGE</td>
<td>300 ft (at required 30 dBm sensitivity)</td>
<td>1000 m (~ 3000 ft)</td>
</tr>
<tr>
<td>MINIMUM SEPARATION</td>
<td>1500 ft (except where carefully planned)</td>
<td>50 ft (on small zone channels)</td>
</tr>
<tr>
<td>CHANNEL CAPACITY</td>
<td>1 to 2 channels</td>
<td>7 channels</td>
</tr>
<tr>
<td>POWER (Downlink)</td>
<td>Nominally less than 40 dBm (10 W)</td>
<td>Nominally less than 33 dBm (2 W)*</td>
</tr>
<tr>
<td>POWER (Uplink)</td>
<td>Nominally less than 6 dBm (&lt; 4mW)</td>
<td>Nominally less than 33 dBm (2 W)*</td>
</tr>
</tbody>
</table>
OBUs and RSUs

• Equipment in the DSRC Service will be comprised of On-Board Units (OBUs) and Roadside Units (RSUs).
• An OBU is a transceiver that is normally mounted in or on a vehicle, or in some instances may be a portable unit.
• An RSU is a transceiver that is mounted along a road or pedestrian passageway.
• An RSU may also be mounted on a vehicle or hand carried, but it may only operate when the vehicle or hand-carried unit is stationary.
• An RSU broadcasts data to OBUs or exchanges data with OBUs in its communications zone.
DSRC Performance Envelopes

Data Rate (Mbps)

Range (ft)

5850 - 5925 MHz Band Performance Envelope
(Approximate)

Safety Message Services

Emergency Vehicle Services

Toll and Payment Services

Data Transfer and Internet Access Services

902 - 928 MHz Band Performance Envelope

0.5 Mbps
5.9 GHz DSRC
BASIC OPERATING FACTORS

- PUBLIC SAFETY and PRIVATE APPLICATIONS share the band
- INTEROPERABILITY
- LICENSED OPERATION
- PUBLIC SAFETY INSTALLATION PRIORITY
- NON-MUTUAL EXCLUSIVITY FOR PRIVATE INSTALLATIONS
- LIMITED RANGE FOR PRIVATE OPERATIONS
- FREQUENCY COORDINATOR USED TO ASSIGN LICENSES
5.9 GHz DSRC BAND PLAN
with 10 MHz CHANNELS & POWER LIMITS

- **Shared Public Safety/Private**: Control, Med Rng Service, Short Rng Service
- **Dedicated Public Safety**: Veh-Veh, Intersections

**Power Limit**
- Public Safety: 44.8 dBm
- Veh-Veh: 40 dBm

**Frequency (GHz)**
- Public Safety: 5.8 GHz band
- Veh-Veh: 5.9 GHz band

**Channels**
- Public Safety: Ch 172, Ch 174, Ch 176, Ch 178, Ch 180
- Veh-Veh: Ch 172, Ch 174, Ch 176, Ch 178, Ch 180
- Intersections: Ch 182, Ch 184

**Power Limits**
- Public Safety: 44.8 dBm
- Veh-Veh: 40 dBm
- Intersections: 23 dBm

**Technical Details**
- Public Safety/Private: Med Rng Service, Short Rng Service
- Veh-Veh: Intersections

**Frequency Bands**
- Public Safety: 5.8 GHz to 5.9 GHz
- Veh-Veh: 5.9 GHz to 5.925 GHz

**Applications**
- Public Safety
- Veh-Veh
- Intersections
5.9 GHz DSRC BAND PLAN
with 20 MHz CHANNELS & POWER LIMITS
Control Channel Access

• Designated to provide “command-and-control regulation used in limited circumstances.”
• Used by both RSUs and OBUs to transmit public safety information and also to advertise the availability of other licensed services.
• All messages must be shorter, e.g. < 200 microseconds
• OBUs are required to listen to the Control Channel every few hundred milliseconds
Single Radio vs Multiple Radio

• When configured to perform well for safety applications, Single RF Unit configurations would have limited efficiency in mobile high volume data transfers

• Multiple RF Units or a Software Defined Radio would allow high transfer rate efficiency during high speed mobile data transactions
DSRC Standards Program

North American 5.9 GHz DSRC Program

Standards Development
- ASTM
- AASHTO
- ITS-A
- IEEE
- SAE
- ISO

DSRC Forum

Implementation/Deployment Plans
- IBTTA
- VSCC
Vehicle Safety Communications Consortium (VSCC)

Government Agencies
- FCC
  - Allocated DSRC Spectrum
- DOT
- NHTSA
- FHWA
- ... (other agencies)

Standards Bodies
- ASTM
- SAE
- IEEE
- ... (other bodies)

CAMP
- Coordinator provides
  interface between
  VSCC and standards bodies
- DOT funds ASTM to lead
  the DSRC standardization
- Cooperative Agreement between
  DOT and OEMs for VSC project
- CAMP provides admin & legal
  support for VSCC and
  interfaces with DOT
DSRC Standardization

- **IEEE**
  - 802.11p – MAC and PHY
  - P1556 – security services
  - P1609 – networking stack
- **ASTM E2213-03**
  - MAC and PHY
- **Related:**
  - NTCIP – message sets and protocols for intelligent transport systems
  - SAE – message sets for ITS
  - IEEE 1512 – message sets for incident management (coordinates with SAE)
Outline

• Intelligent Transportation Systems (ITS)
• Dedicated Short Range Communication (DSRC)
• Intelligent Vehicle Applications Enabled by DSRC
• Media Access Control (MAC) Protocols and Quality of Services
• Security and Privacy
DSRC APPLICATIONS
PUBLIC SAFETY and PRIVATE

PUBLIC SAFETY

• APPROACHING EMERGENCY VEHICLE (WARNING) ASSISTANT (3)
• EMERGENCY VEHICLE SIGNAL PREEMPTION
• ROAD CONDITION WARNING
• LOW BRIDGE WARNING
• WORK ZONE WARNING
• IMMINENT COLLISION WARNING (D)
• CURVE SPEED ASSISTANCE [ROLLOVER WARNING] (1)
• INFRASTRUCTURE BASED – STOP LIGHT ASSISTANT (2)
• INTERSECTION COLLISION WARNING/AVOIDANCE (4)
• HIGHWAY/RAIL [RAILROAD] COLLISION AVOIDANCE (10)
• COOPERATIVE COLLISION WARNING [V V](5)
• GREEN LIGHT- OPTIMAL SPEED ADVISORY (8)
• COOPERATIVE VEHICLE SYSTEM – PLATOONING (9)
• COOPERATIVE ADAPTIVE CRUISE CONTROL [ACC] (11)
• VEHICLE BASED PROBE DATA COLLECTION (B)
• INFRASTRUCTURE BASED PROBE DATA COLLECTION
• INFRASTRUCTURE BASED TRAFFIC MANAGEMENT – [DATA COLLECTED from] PROBES (7)
• TOLL COLLECTION
• TRAFFIC INFORMATION (C)
• TRANSIT VEHICLE DATA TRANSFER (gate)
• TRANSIT VEHICLE SIGNAL PRIORITY
• EMERGENCY VEHICLE VIDEO RELAY
• MAINLINE SCREENING
• BORDER CLEARANCE
• ON BOARD SAFETY DATA TRANSFER
• VEHICLE SAFETY INSPECTION
• DRIVER’S DAILY LOG

PRIVATE

• ACCESS CONTROL
• DRIVE THRU PAYMENT
• PARKING LOT PAYMENT
• DATA TRANSFER / INFO FUELING (A)
  – ATIS DATA
  – DIAGNOSTIC DATA
  – REPAIR SERVICE RECORD
  – VEHICLE COMPUTER PROGRAM UPDATES
  – MAP and MUSIC DATA UPDATES
  – VIDEO UPLOADS
• DATA TRANSFER / CVO / TRUCK STOP
• ENHANCED ROUTE PLANNING and GUIDANCE (6)
• RENTAL CAR PROCESSING
• UNIQUE CVO FLEET MANAGEMENT
• DATA TRANSFER / TRANSIT VEHICLE (yard)
• TRANSIT VEHICLE REFUELING MANAGEMENT
• LOCOMOTIVE FUEL MONITORING
• DATA TRANSFER / LOCOMOTIVE

ATIS - Advanced Traveler Information Systems
CVO - Commercial Vehicle Operations
EV - Emergency Vehicles
IDB - ITS Data Bus
THRU – Through
V-V – Vehicle to Vehicle
(#) – Applications Submitted by GM/Ford/Chrysler
(A-Z) – Applications Submitted by Daimler-Chrysler
DSRC APPLICATIONS
by COMMUNICATION CATEGORIES

ALL VEHICLES - Short Range (0 – 15 m)
- ACCESS CONTROL
- TOLL COLLECTION
- DATA TRANSFER / INFO FUELING (A)
- TRAFFIC INFORMATION (C)
- DRIVE THRU PAYMENT
- PARKING LOT PAYMENT
- INFRASTRUCTURE BASED PROBE DATA COLLECTION
- RENTAL CAR PROCESSING

ALL VEHICLES - Extended Range (90 – 335 m)
- CURVE SPEED ASSISTANCE [ROLLOVER WARNING] (1)
- INFRASTRUCTURE BASED - STOP LIGHT ASSISTANT (2)
- INTERSECTION COLLISION WARNING/AVOIDANCE (4)
- COOPERATIVE COLLISION WARNING [V \( V \)](5)
- VEHICLE BASED PROBE DATA COLLECTION (B)
- COOPERATIVE ADAPTIVE CRUISE CONTROL (ACC)
- COOPERATIVE VEHICLE SYSTEM – PLATOONING (9)
- HIGHWAY/RAIL [RAILROAD] COLLISION AVOIDANCE (10)
- IMMINENT COLLISION WARNING (D)
- EMERGENCY VEHICLE VIDEO RELAY
- ROAD CONDITION WARNING
- WORK ZONE WARNING

APPLICABILITY UNDER INVESTIGATION
- ENHANCED ROUTE PLANNING and GUIDANCE (6)
- INFRASTRUCTURE BASED TRAFFIC MANAGEMENT – [DATA COLLECTED from] PROBES (7)

ALL VEHICLES – Short - Medium Range (0 – 90 m)
- TOLL COLLECTION
- DATA TRANSFER / INFO FUELING (A)
- DATA TRANSFER / CVO / TRUCK STOP
- DATA TRANSFER / TRANSIT VEHICLE (yard)
- DATA TRANSFER / LOCOMOTIVE

CVO – Short - Medium Range (0 – 90 m)
- MAINLINE SCREENING
- BORDER CLEARANCE
- ON BOARD SAFETY DATA TRANSFER
- UNIQUE CVO FLEET MANAGEMENT
- DRIVER’S DAILY LOG
- VEHICLE SAFETY INSPECTION
- TRANSIT VEHICLE DATA TRANSFER (gate)
- TRANSIT VEHICLE REFUELING MANAGEMENT
- LOCOMOTIVE FUEL MONITORING
- ROLLOVER WARNING
- LOW BRIDGE WARNING

PUBLIC SAFETY - Long Range (300 – 1000 m)
- APPROACHING EMERGENCY VEHICLE ASSISTANT (3)
- EMERGENCY VEHICLE SIGNAL PREEMPTION
- TRANSIT VEHICLE SIGNAL PRIORITY
- GREEN LIGHT- OPTIMAL SPEED ADVISORY (8)
DSRC Interoperability

- The “E-ZPass”, “Title 21”, ASTM V6, and “Sandwich Specification” equipment will continue to be used where cost and regional/national mandates or both require continued operation for those applications that fall within the performance envelope.

- The 5.9 GHz Standards and Equipment will be used for applications that cannot be done with the 915 MHz technology and where service providers want to take advantage of OBUs being built into the vehicles.

- INTEROPERABILITY will be achieved by implementing 5.9 GHz equipment in all DSRC installations. This means adding 5.9 GHz equipment to operate in conjunction with 915 MHz equipment in current and future 915 MHz operations.

- Roadside 5.9 GHz equipment will cost much less than current 915 MHz equipment and per lane installations are few, making dual mode installations very cost effective.
Traffic Signal - Green
Traffic Signal - Red

TYPICAL INTERSECTION

COLLISION ANIMATION FOLLOWS
NO COLLISION AVOIDANCE SYSTEM IN OPERATION

ANIMATION

Traffic Signal - Red
Traffic Signal - Green
Note 1: The Emergency OBU transmits a warning to other vehicles that it is coming.
5.9 GHz DSRC VEHICLE TO VEHICLE APPLICATION

EMERGENCY VEHICLE APPROACH WARNING

Note 1: The Emergency OBU transmits a warning to ALERT other vehicles that it is coming.
5.9 GHz DSRC ROADSIDE TO VEHICLE APPLICATION

EMERGENCY VEHICLE SIGNAL PREEMPTION

Note 1: OBU Transmitting the Emergency Vehicle Signal Preemption Request on the Intersection Ch

up to 1000 m (3281 ft)

Not to Scale
5.9 GHz DSRC VEHICLE TO VEHICLE APPLICATION

EMERGENCY VEHICLE SIGNAL PREEMPTION with APPROACH WARNING

Note 1: OBU Transmitting the Emergency Vehicle Signal Preemption Request on the Intersection Ch

Note 2: The Emergency OBU transmits a warning to ALERT other vehicles that it is coming on the Control Channel.

RSU located in the center of the intersection

Emergency Vehicle Approach Warning Communication Zone

RSU on Intersection Ch

OBU on Intersection Ch and Control Ch

up to 1000 m (3281 ft)

Traffic Signal

Traffic Signal

OBUs on Control Ch

ANIMATION

Not to Scale
5.9 GHz DSRC ROADSIDE TO VEHICLE APPLICATION

EMERGENCY VEHICLE APPROACH WARNING - INTERSECTION RELAY

Note 1: The Intersection RSU retransmits the Emergency OBU warning to ALERT vehicles approaching on the side streets.
5.9 GHz DSRC VEHICLE TO VEHICLE APPLICATION

IMMINENT COLLISION WARNING

Note 1: The OBU in the vehicle recognizing the threat transmits a WARNING and COLLISION PREPARATION MESSAGE with the location address of the threat vehicle.

Note 2: Only the OBU in the threatening vehicle processes the message because only it matches the threat address.

Note 3: COLLISION PREPARATION includes seat belt tightening, side air bag deployment, side bumper expansion, etc.

Radar Threat Identification

Traffic Signal

Traffic Signal

OBUs on Control Ch

Not to Scale
5.9 GHz DSRC VEHICLE TO VEHICLE APPLICATION

IMMINENT COLLISION WARNING

ANIMATION

COLLISION IMMINENT FRONT

COLLISION IMMINENT LEFT

Traffic Signal
Traffic Signal
OBUs on Control Ch

Car NOT Stopping

Not to Scale
5.9 GHz DSRC VEHICLE TO VEHICLE APPLICATION

STOPPED EMERGENCY VEHICLE WARNING

Note 1: The Stopped Vehicle Warning message is sent every 50 ms
5.9 GHz DSRC VEHICLE TO VEHICLE APPLICATIONS

COOPERATIVE COLLISION WARNING/AVOIDANCE

1) Vehicles with vehicle to vehicle (v-v) communications capability transmit the vehicle’s position, speed, direction of travel, and acceleration at 12 Mbps. One transmission will be sent every 300 ms. This transmission is intended for all vehicles within 10 sec travel time, thus the transmit power (range) will vary with vehicle speed up to a maximum range of 300 meters (~1000 ft). The minimum range will be 110 m (~367 ft). For example, vehicles traveling at 60 mph would transmit at a power level appropriate to reach approximately 270 m (~880 ft) and vehicles traveling at 25 mph or lower would transmit at a power level appropriate to reach approximately 110 m (~367 ft). All vehicles capable of doing so (having OBU and with vehicle speed and position data available) will transmit these messages and all OBU will receive these messages.

2) Vehicles that receive these transmissions and have collision avoidance processing capability compute the position and probability of collision for all transmitting vehicles every 100 ms.

3) A Caution is given to drivers when a possibility of collision is computed with an avoidance maneuver requirement that exceeds .35 g or the equivalent acceleration for the conditions.

4) A Warning is given to drivers when a possibility of collision is computed with an avoidance maneuver requirement that meets or exceeds .50 g or the equivalent acceleration for the conditions.

5) If it can be determined that two vehicles are on an intercepting course, both will use the transmission range of the faster vehicle.
5.9 GHz DSRC VEHICLE TO VEHICLE APPLICATIONS

COOPERATIVE COLLISION WARNING/AVOIDANCE

(with closely spaced vehicles @ 60 mph)

- OBU Receiving on the Vehicle to Vehicle channel
- OBU Transmitting and Receiving on the Vehicle to Vehicle channel @ 12 Mbps

Note: The vehicle’s position, speed, direction and acceleration message is nominally sent every 300 ms with a range of 300 m (~1000 ft).
5.9 GHz DSRC VEHICLE TO VEHICLE APPLICATIONS

COOPERATIVE COLLISION WARNING/AVOIDANCE

(with closely spaced vehicles @ 25 mph)

- OBU Receiving on the Vehicle to Vehicle channel
- OBU Transmitting and Receiving on the Vehicle to Vehicle channel @ 12 Mbps

Note: The vehicle’s position, speed, direction and acceleration message is nominally sent every 300 ms with a range of 110 m (~367 ft) (with closely spaced vehicles @ 25 mph)
5.9 GHz DSRC VEHICLE TO VEHICLE APPLICATIONS

COOPERATIVE COLLISION WARNING/AVOIDANCE

STOPPING VEH. WARNING

- Routine position, speed, direction messages
- Vehicle Brake Lights
- OBU Listening to Control Channel
- OBU Transmitting on Control Channel

In-Vehicle Display and Annunciation

Road Blocked

Stopping message

Not to Scale
Note 1: The Stopped Vehicle Warning message is sent in the direction of arriving traffic when the stopping vehicle’s brakes are being applied and its speed drops 20 mph below the speed limit of the road or its speed drops below 5 mph.

Note 2: The Stopped Vehicle Warning message is sent every 100 ms with a range of 1000 ft.
5.9 GHz DSRC ROADSIDE TO VEHICLE APPLICATION

TOLL COLLECTION (Open Road) in service channel

The Toll Collection RSU operates on a Service Channel and is located on the gantry above the lanes. 

Note 1: OBU approaching the toll zone are instructed to switch to a service channel in order to conduct the transaction.

Note 2: Users are allowed to proceed at highway normal speeds while the toll is paid.

Note 3: Implementers use Time Division to isolate vehicle communications and angle of signal arrival to locate vehicle.

Not to Scale
Outline

• Intelligent Transportation Systems (ITS)
• Dedicated Short Range Communication (DSRC)
• Intelligent Vehicle Applications Enabled by DSRC
• Media Access Control (MAC) Protocols and Quality of Services
• Security and Privacy
Challenges

- Communications points are moving at high speed
- Must operate as master/slave when talking to roadside, peer-to-peer directly
- Must acquire in milliseconds
- Must change channels in microseconds
- Must control power dynamically to decrease interference
- Must always get the most important message through first
- Must have bulletproof security
- Must preserve anonymity for end users
Protocol Stack

- Geoadressed applications (e.g. active safety)
- IP Applications (Deployment)
- WAVE Short Message Apps

- TCP / UDP
- IPv6

- C2C-CC Network Layer
- LLC/MAC (IEEE 802.11p)
- P1609.4

- PHY (IEEE 802.11p)
Two Different Type Applications

• Broadcast
  – Safety messages
  – Preempt use by other applications

• Transactional
  – Tolling
  – Commercial Vehicle Operations
  – Typically Client-Server Architecture
  – Advertised by RSUs, consumed by OBUs
The 802.11 Protocol Stack

Part of the 802.11 protocol stack.
Major Difference in PHY between WAVE and IEEE 802.11a

- **Operating environment**: Outdoor versus Indoor
- **Mobility requirement**: DSRC requires OBU to OBU communication, each runs at speed up to 120 Mph. IEEE 802.11a only requires stationary or walking speed
- **Maximum data rate**: DSRC up to 27 Mbits/s, IEEE 802.11a up to 54 M bits/s
- **Subcarrier frequency spacing**: IEEE 802.11a doubles that of DSRC, so could tolerate more carrier frequency offset
- **Guard period**: DSRC doubles that of IEEE 802.11a, could tolerate more delay spread
The 802.11 MAC Sublayer Protocol

(a) The hidden node problem.  (b) The exposed node problem.
The 802.11 MAC Sublayer Protocol (2)

The use of virtual channel sensing using CSMA/CA.
The 802.11 MAC Sublayer Protocol (3)

A fragment burst.

A fragment burst.
The 802.11 MAC Sublayer Protocol

Interframe spacing in 802.11.
Distributed Coordination Function

• All nodes are allowed to contend for the shared medium simultaneously.
• CSMA/CA mechanism and random back-off scheme are used to reduce frame collisions.
• After detecting the channel is idle, a node further waits for a $DIFS$ period and invokes a back-off procedure. The back-off is given by

$$\text{Back-off Time} = \text{rand} (0, CW) \times \text{slottime}$$
EDCF (Enhanced Distributed Coordination Function, 802.11e] – Traffic Category

• The EDCF provides differentiated access to the WM for 8 priorities.
  – Priorities are numbered from 0 (the lowest priority) to 7 (the highest priority).

• The set of MSDUs with the same priority is refer to a Traffic Category (TC).
EDCF – Access Category

• EDCF defines *access category (AC)* mechanism to support the priority mechanism at the non-AP QSTAs.

• An AC is an enhanced variant of the DCF which contends for *transmission opportunity (TXOP)* using the set of parameters such as $\text{CW}_{\text{min}}[\text{AC}]$, $\text{CW}_{\text{max}}[\text{AC}]$, $\text{AIFS}[\text{AC}]$, etc.
EDCF – Access Category (2)
EDCF – Access Category (3)

• A station starts a back-off counter after detecting the channel being idle for an arbitration inter-frame space (AIFS[i])

\[ AIFS[i] = SIFS + AIFSN[i] \times slottime \]

For high-priority classes, low AIFSN values are assigned to give higher priorities for them.
Outline

• Intelligent Transportation Systems (ITS)
• Dedicated Short Range Communication (DSRC)
• Intelligent Vehicle Applications Enabled by DSRC
• Media Access Control (MAC) Protocols and Quality of Services
• Security and Privacy
Security Needs

• **Authenticity**: the system must assure that the packet/data are generated by a trusted source.

• **Integrity**: the system must assure that the packet/data has not been tampered with or altered after it was generated.

• **Privacy/Anonymity**: the full identity of a vehicle sending each packet/data should be kept private.

• Accountability, Revocation capability, Real-time constraints

• **However, it is very difficult to ensure both authenticity and anonymity at the same time.**
Potential Attacks

• Bogus information
• Imposture
• Denial of service
• Eavesdropping
• Replay legitimate messages
Threat mitigation

- Authenticate messages
  - Targets of messages are “all vehicles on the road”, so need public-key Signatures
- Encrypt confidential data
- Current proposal: for broadcast, high-priority messages (public/vehicle safety) a new compact certificate format and a public key algorithm with particularly short keys
Anonymity

• Potential abuses of vehicle tracking systems are rife
  – Stalkers
  – Terrorists
  – Law Enforcement Tracking
  – Automatically issued speeding tickets
  – Rental car agencies issuing fines for going out of state
Anonymity Requirements

• The privacy principles of ITS America include an “Anonymity Principle” that states: “Where practicable, individuals should have the ability to utilize Intelligent Transportation Systems on an anonymous basis.”

• Important in principle
  – Also, people who are concerned about tracking might disable their radio, impacting the safety and other benefits.
  – Need to reassure people that Big Brother isn’t in the passenger seat.
Anonymity in Practice

• Need to protect against:
  – Wireless-only attacker who links transmission to vehicle
  – Attacker who links multiple transmissions to vehicle, and then links vehicle to a single transmission by (eg) physical observation – tracking.

• Need to ensure that:
  – It’s difficult for an attacker with off-the-shelf equipment to build a tracking system
  – It’s difficult for you to be tracked by an unknown party
    • Users can opt in to services in the course of which they may be subject to tracking, but should not be tracked otherwise

• So:
  – Remove identifying marks, as much as possible, from broadcast messages
  – Encrypt transactional messages
Identifying marks

- MAC addresses
- IP addresses
- If messages are signed, signature and certificates
IP Addresses

- Long-lived IP addresses can in theory be used as a tracking token
- In practice, system is not designed for handoff of IP sessions from one RSU to another
  - so long-lived IP sessions happen when you’re stationary
  - Less of a risk from tracking
- All devices on IVN will change IP address when the OBU moves from one RSU communication zone to another
Random MACs

- Generate a random MAC
  - Out of the local address space
  - Collision probability insignificant with small groups
    - 46 random bits
    - How many cars can fit in 300 meters?

- When to change MAC
  - At startup?
    - Allows tracking for individual trips
    - Not really acceptable
      - Track me from point A to point B
      - Real-life traffic analysis!
  - When the signing key changes
    - Order every 5-10 minutes
    - Close monitoring can follow transitions
Anonymous Certificates

• Broadcast messages from an OBU
  – *must* be authenticated
    • Otherwise, attacker with radio could simply generate fake brake light messages and foul up traffic
  – *must not* be traceable to a specific OBU

• Some techniques to do this
  – Issue an OBU with a large number of certificates, which it works through at random
    • Currently preferred approach
    • 10,000 certificates allows a new certificate every five minutes for a month!
      – Actual rollover algorithm will be more complicated
    • Each certificate contains a unique identifier, but no distinguishing information
  – Other technique: Group signatures
Group Signature

- It allows members of a group to sign messages on behalf of the group.
- Signatures can be verified with respect to a single group public key, but they do not reveal the identity of the signer.
- It is not possible to decide whether two signatures have been issued by the same group member.
- In case of a later dispute, group manager can open signatures to reveal the identity of the signer.
Group Signature Properties

• Only group members are able to correctly sign messages (unforgeability).

• It is neither possible to find out which group member signed a message (anonymity) nor to decide whether two signatures have been issued by the same group member (unlinkability).

• Group members can neither circumvent the opening of a signature nor sign on behalf of other group members; even the group manager cannot do so (security against framing attacks).
Group Management

- Vehicles
  - Emergency Vehicles
    - Fire Truck
    - Ambulance
    - Police Cars
  - Transit Vehicles
  - Commercial Vehicles
  - Customer Vehicles

- Roadside Units
  - Intersection Units
  - Roadway Units
  - Toll Collection Units
  - Parking Lot Units
Tamper-Resistant Devices for Key Management

• Keys stored inside a vehicle computer can be vulnerable to use, abuse, duplication, and modification by an unauthorized attacker.

• To protect keys, we will store them in a tamper-resistant hardware device. This device offers physical protection to the keys residing inside them, thereby providing assurance that these keys have not been maliciously read or modified.
Secure and Privacy-Preserving Communication Framework

Application Layer

Outgoing Message

- Capability check
- Signature generation
- Signature Verification
- Authorization check
- Anomaly Detection

Communication Layer

- Firewall

Access Control List

Group membership key

Tamper-Resistant Chip
Open Research Issues

• The efficiency of the group signature mechanism
  – Short group signature
• Key certification
• Key revocation
Deployment

- Standards complete within 4-6 months
- Development, initial deployment can use existing 802.11a products
- Spectrum available for test, development now
- Chicken and egg problem
- Public-private partnership potential
  - Safety application typically need <15% of capacity
  - Shared roadside infrastructure
  - Shared costs
  - Safety applications have priority access
VSCC Deployment Timeline

• Near-term solutions, deployable in the U.S. Market between 2007 and 2011
  – Traffic Signal Violation Warning
  – Curve Speed Warning
  – Emergency Electronic Brake Lights

• Mid-term solutions, deployable in the U.S. between 2012 and 2016
  – Pre-Crash Warning
  – Cooperative Forward Collision Warning
  – Left Turn Assistant
  – Lane Change Warning
  – Stop Sign Movement Assistance
DSRC Summary

What is it? Short to medium range, low latency, high data rate communications.

Who developed it? Government and Industry in ASTM and IEEE standards groups.

When would it be advantageous to use it? Any situation requiring short to medium range communications between vehicles and the roadside or between vehicles where the environment is changing or data needs to be transferred at high rates. Think short-range highway advisory radio.

When will products be available? Estimated Mid 2004.

When will it be available as original equipment in new cars? Estimated 2006 to 2008.

What plug replaceable technology can be used for some data transfer applications in the interim? IEEE 802.11a.
References

• “DSRC Tutorials,” http://www.leearmstrong.com/
• W. Whyte, “Safe at Any Speed: Dedicated Short Range Communications (DSRC) and On-road Safety and Security,” RSA Conference 2005