VAN
(VEHICLE AREA NETWORKS)

SHINYOUNG CHO

CONTENTS

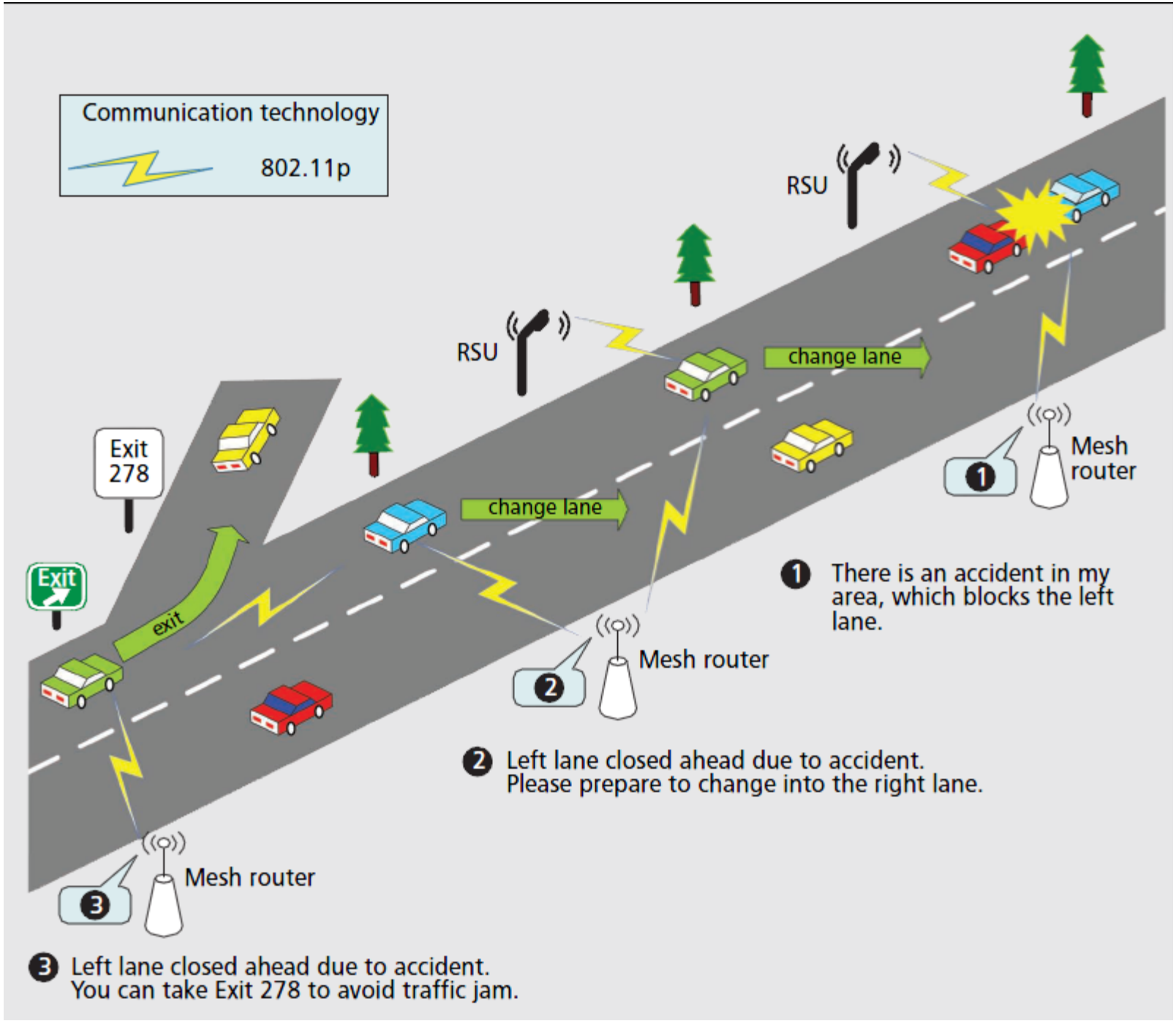
DEFINITION

Vehicle Area Networks(VAN)

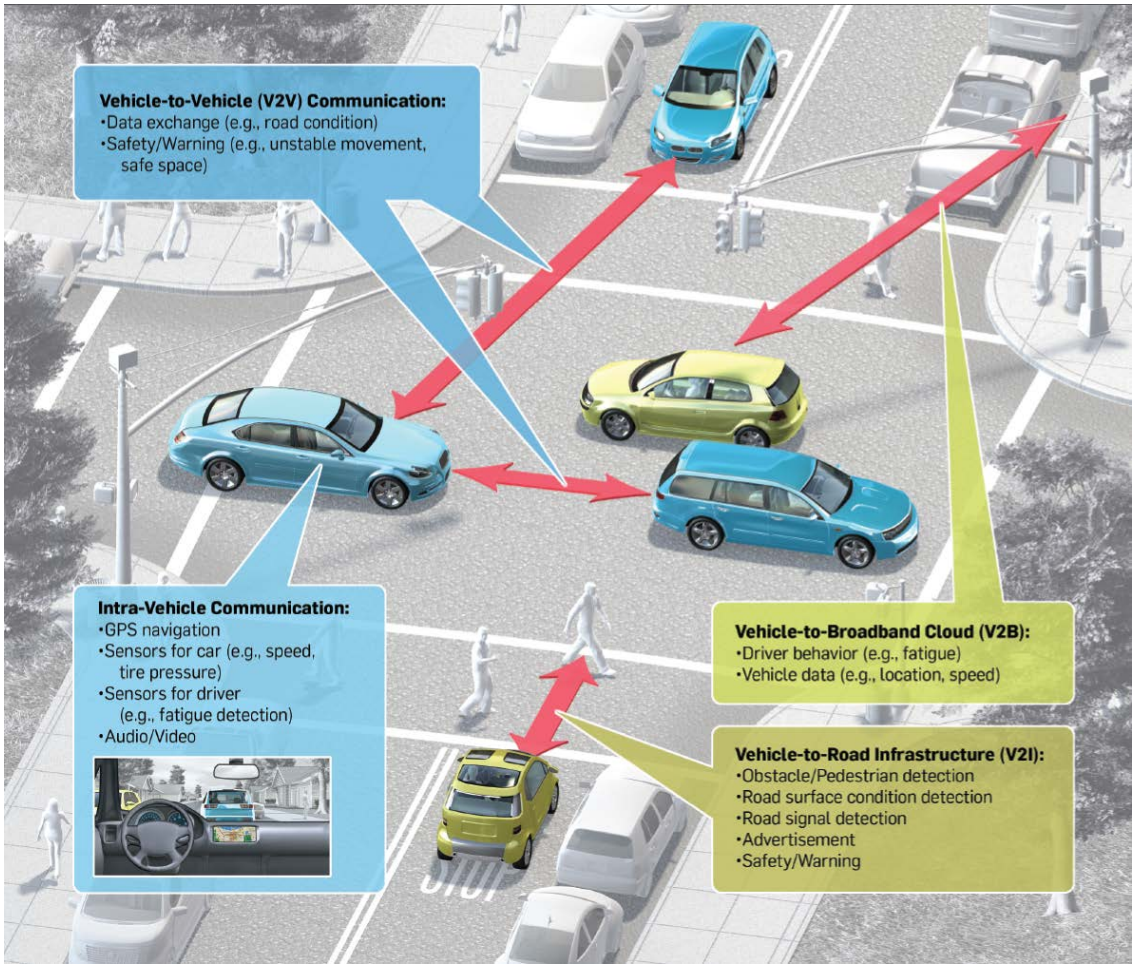
- A local area network in and around a moving vehicle
- Enables devices in and around the vehicle to communicate, either directly connected or through wireless protocols over the Internet

Key objective

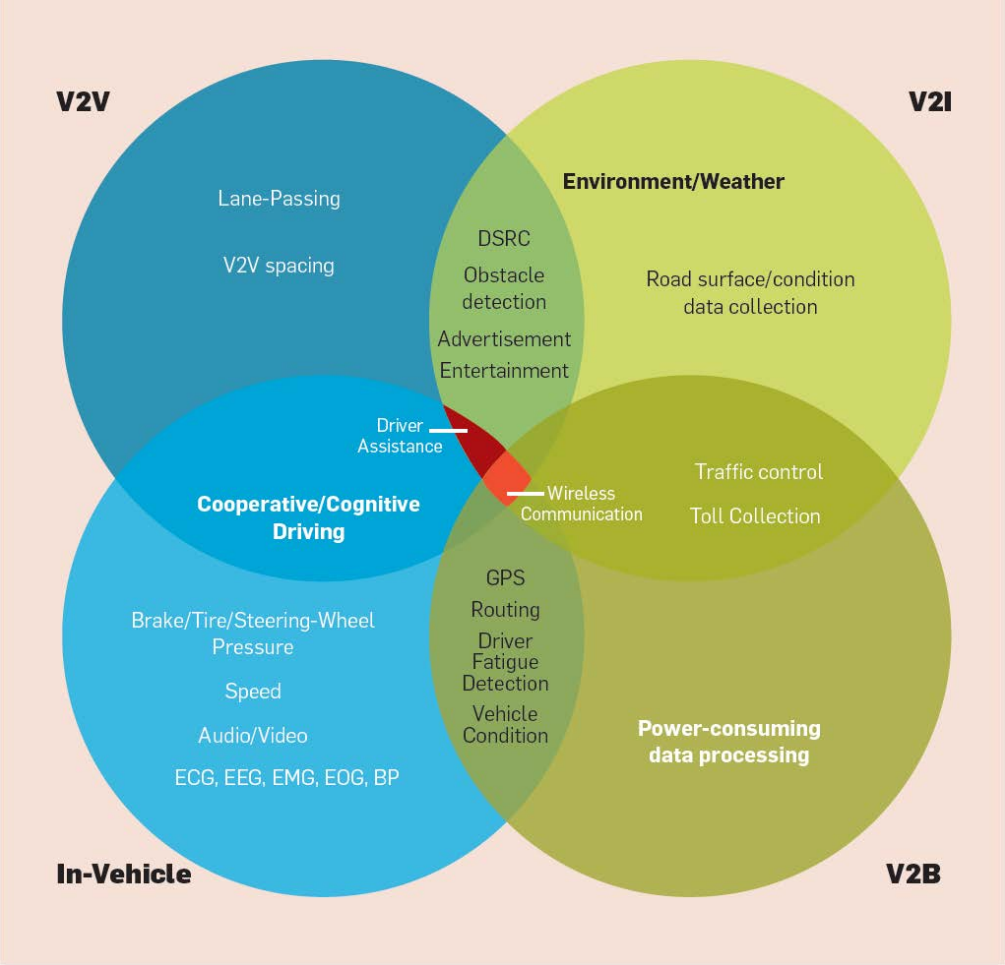
- To improve driver and vehicle safety


Communication technology
802.11p
RSU
RSU
change lane
change lane
Exit
278
Exit
exit
Mesh
router
Mesh router
Mesh router
1 There is an accident in my area, which blocks the left lane.
2 Left lane closed ahead due to accident.
Please prepare to change into the right lane.
3 Left lane closed ahead due to accident.
You can take Exit 278 to avoid traffic jam.

CENTRAL VISION OF VAN(1/2)



CENTRAL VISION OF VAN(2/2)



[VAN key components and functions]

IN-VEHICLE VAN(1/4)

In-Vehicle Data Collection/Analysis Systems.

Intelligent intra-vehicle communication system

- A major stream of research in the area of intelligent vehicle systems

Onboard equipment(OBE)

- Collect information from the driver or vehicle
- Analyze and classify the data collectively to predict or detect driver fatigue

IN-VEHICLE VAN(2/4)

Onboard equipment(OBE) (cont'd)

- Standard vehicle information
  - Speed
  - Pressure on the brake
  - Gas pedal
  - Steering wheel rotation
  - Global positioning system(GPS) routing
  - Driver behavioral information(ex. Facial expression)
  - Physiological signals(ex. BP, EGC)

IN-VEHICLE VAN(3/4)

In-Vehicle Communication Network.

Interconnect all Onboard equipment(OBE)s

	CAN	LIN	FlexRay	MOST	J1850
Application	soft real-time	low cost low speed	hard real-time	multimedia	diagnostics
Bandwidth	500kpbs	19.6kpbs	10Mbps	24.8Mbps	41.6kpbs
Control	multi-master	single-master	multi-master	timing-master	multi-master
Bus Access	CSMA/CA	Polling	TDMA	TDM/CSMA	CSMA/NDA
Redundancy	No	No	Yes	No	No
Physical Layer	Electrical	Electrical	Electrical Optical	Optical	Electrical

[Common in-vehicle protocols]

IN-VEHICLE VAN(4/4)

Top Challenges

- *Car-Suited Physiological Sensors*
- *In-Vehicle Data Analysis*
- *Generic Plug and Play Gateway*

Existing Solutions

- *Intel In-Vehicle Devices*
- *Software for Automotives*

VEHICLE-TO-VEHICLE COMMUNICATION(V2V)(1/2)

V2V communication

- Provide a data exchange platform
- Expand driver assistance
- Facilitate active safety vehicle system development

Wireless connectivity

VEHICLE-TO-VEHICLE COMMUNICATION(V2V)(2/2)

Top Challenges

- *Hardware/Software/Firmware*
- *Cooperative Communication*

Existing Solutions

- *Vehicle Telematic*

VEHICLE-TO-CLOUD COMMUNICATION(1/3)

Vehicles communicating with a broadband cloud

- Communicate via wireless broadband mechanisms
  - 3G/4G, LTE, WiMAX, etc

Useful for..

- Active driver assistance
- Vehicle tracking in network fleet management

VEHICLE-TO-CLOUD COMMUNICATION(2/3)

V2B networks can provide useful information

- Outgoing data
  - Vehicle-centric information
  - Driver-centric information
  - Audio/video
  - ➢ Forwarded to a central monitoring server for further analysis and storage
- In-coming data
  - Receiving data from a central office
  - Infotainment
  - Entertainment (ex. Multimedia streaming)
  - Internet

VEHICLE-TO-CLOUD COMMUNICATION(3/3)

Top Challenges

- *Communication Latency*
- *Gateway*
- *Data Processing*
- *Fleet Management*
- *Security*

VEHICLE-TO-ROADSIDE INFRASTRUCTURE COMMUNICATION (1/2)

Vehicle-to-road communication

- For environmental sensing and monitoring

Information

- Speed limit
- Weather condition information
- Road conditions
- Sensed data of road surface

VEHICLE-TO-ROADSIDE INFRASTRUCTURE COMMUNICATION (2/2)

Top Challenges

- *Next Generation of Car Radars*
- *Prioritization*

Existing Solutions

- *Radio-Frequency Identification(RFID) technology*

COMMUNICATION STANDARDS FOR VAN

Communication protocols for VAN

- *IEEE 802.11p*
- *IEEE 1609*
  - *IEEE P1609.1 : resource manager*
  - *IEEE P1609.2 : security issues in WAVE*
  - *IEEE P1609.3 : network protocol layer standard in WAVE*
  - *IEEE P1609.4 : multichannel WAVE operations*
- *ASTM E2213-03*

SECURITY AND PRIVACY OF VAN(1/2)

How false or stolen data

- Insert false information
- Eavesdrop private information
- Use private information

The mobility feature of vehicles

- Be carefully designed to avoid overwhelming the radio link bandwidth with sudden node density fluctuations

SECURITY AND PRIVACY OF VAN(2/2)

VAN Communication

V2V

- The client side should be equipped with content inspection or anomaly detection engines to combat intrusions, phishing, spam, and denial-of-service attacks

V2B

- A central monitoring station can assess normalcy of a driver's behavior and diagnose a vehicle's malfunction occurrences

V2I

- The security against undesired or malicious incoming data becomes a challenge

SECURE COMMUNICATION(1/2)

Secure Communication

- Message authentication
- Integrity
- Accountability
- Privacy protection

Current research on security in vehicular communication protocols

- Periodic beaconing
- Flooding
- Geocast
- Positionbased mechanisms

SECURE COMMUNICATION(2/2)

Top Challenges

- *Adapting to Future Platforms*
- *Secure Beaconing*
- *Privacy Issues*
- *Real-world Simulation*
- *Securing Vehicle Access Control and Theft Prevention*

Existing Solution

- Secure Vehicular Communication(SeVeCom) project
  - Customized hardware security modules (HSM)
    - Protects private keys for digital signature generation
    - Handles the key and device management

CONCLUSION

Key elements of VAN

Intelligent in-vehicle systems

V2V, V2B, V2I

Main challenges and solutions

IEEE/ASTM standards

VAN security and privacy

REFERENCE

- **Maid Faezipour, Mehrdad Nourani, Adnan Saeed, Sateesh Addepalli, “Progress and Challenges in Intelligent Vehicle Area Networks”, Communication of the ACM, Feb. 2012**
- **Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, Xuemin Shen, “Security in Vehicular Ad Hoc Networks”, IEEE Communications Magazine, Apr. 2008**
- **Frank Kargl, Levente Buttyan, Ta-Vinh Thong, Giorgio Calandriello, Albert Held, Antonio Kung, Jean-Pierre Hubaux, “Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges”, IEEE Communications Magazine, Nov. 2008**