InnoSoc

Innovative ICT Solutions
for the Societal Challenges

CHALLENGES AND FUTURE TRENDS OF VANETs SENSOR NETWORKS

FILIP TSVETANOV

F.TSVETANOV@UTP.BG

UNIVERSITY OF TELECOMMUNICATIONS AND POST

FACULTY OF TELECOMMUNICATION

BULGARIA

22.04.16, ZAGREB

InnoSoc

ZAGREB 2016

TOPICS

- SENSOR NETWORKS - VANETs
- STANDARD IEEE 802.11P
- TYPES OF COMMUNICATION VANETs
- SECURITY OF VANETs
- INNOVATION OF SENSORS NETWORKS FOR AUTOMOBILES

VANETs SENSOR NETWORKS

InnoSoc

- A network of tiny autonomous devices embedded in everyday objects or sprinkled on the ground, able to communicate using wireless links.
- Vehicular ad hoc networks has been realized by the technology of dedicated short range communications (DSRC).
- By this DSRC, vehicles can communicate efficiently with other vehicles moving on either the same road segment or adjacent road segments at an intersection for the driving safety.
- This DSRC technology has been implemented by the standard of IEEE 802.11p for vehicular networks.

VANETs SENSOR NETWORKS

InnoSoc

- **IEEE 802.11p** is an approved amendment to the IEEE 802.11 standard to add **wireless access in vehicular environments** (WAVE), a vehicular communication system. It defines enhancements to 802.11 (the basis of products marketed as wi-fi) required to support intelligent transportation systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 ghz uses channels of 10MHz bandwidth (5.85-5.925 ghz). IEEE 1609 is a higher layer standard based on the IEEE 802.11p.

STANDARD IEEE 802.11P

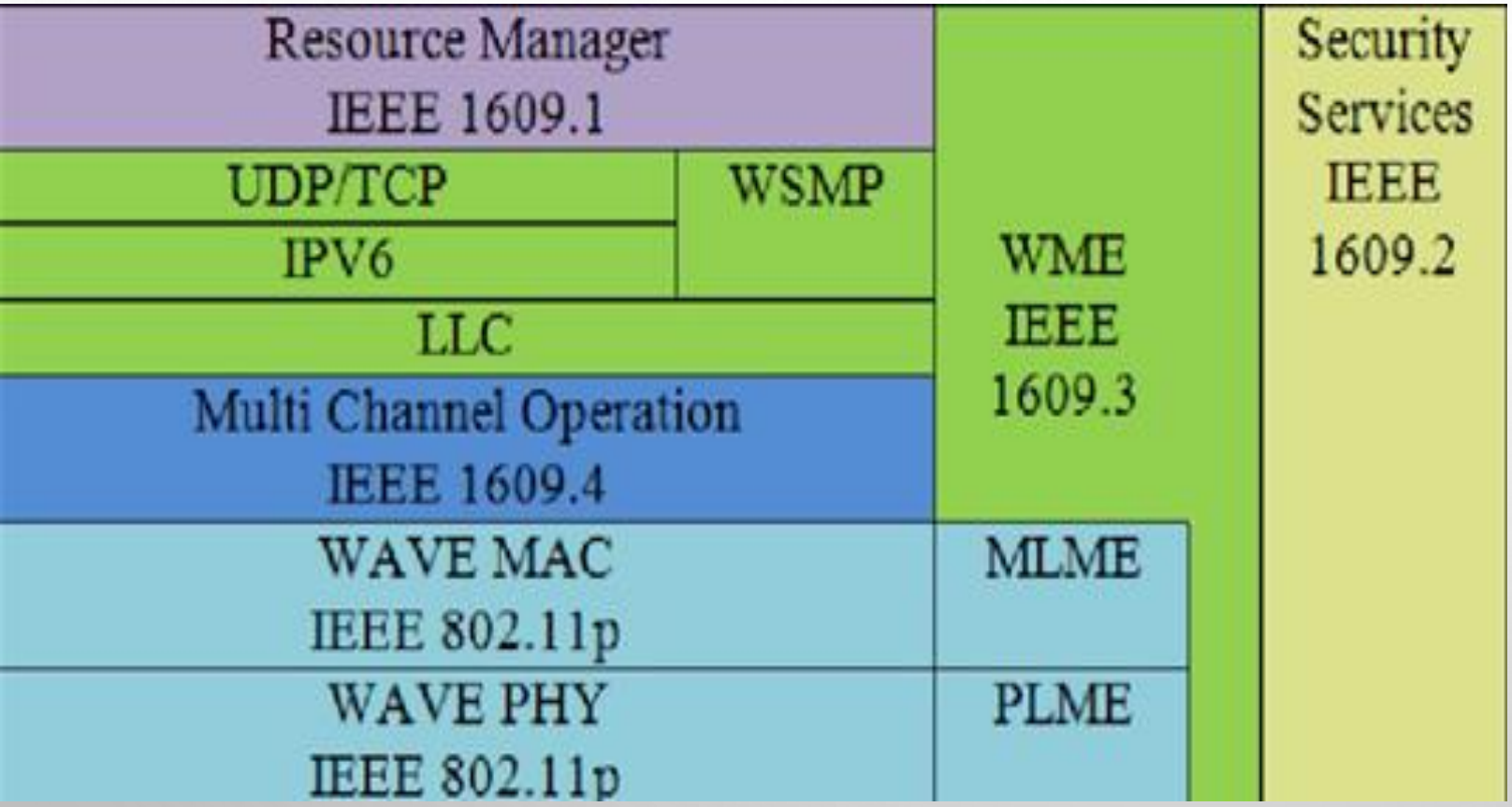
InnoSoc

The 802.11p standard:

- Allowing data exchange between moving vehicles in the 5.9 GHZ band;
- Defines physical and medium access control MAC layers of VANETs;
- The IEEE 1609 working group defined protocol family which developed higher specification based on 802. 11.p who consists of four documents:

- IEEE 1609.1: describes resource manager specification;
- IEEE 1609.2: defines the format and processing of secure messages;
- IEEE 1609.3: cover network and transport layer services;
- IEEE 1609.4: specifies improvement to the IEEE 802.11.p MAC to support multichannel operation.
- IEEE 1609.11: Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS) will define the services and secure message formats necessary to support secure electronic payments.

WAVE STANDART

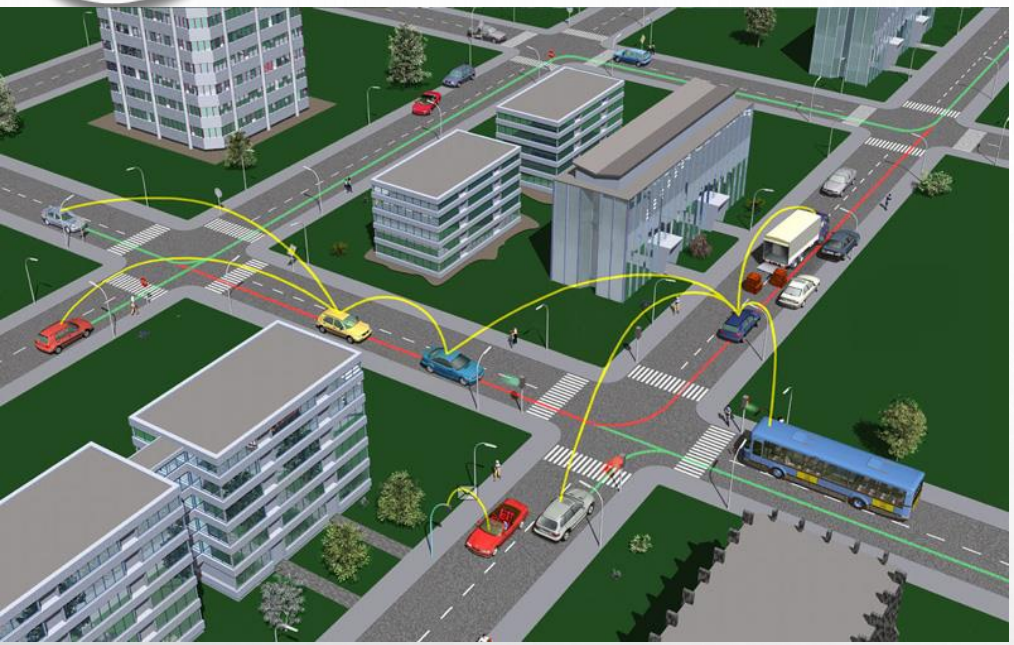


WAVE architecture

- The IEEE 1609 protocol family and IEEE 802.11p together are called WAVE STANDART (Wireless Access in Vehicular Environments).
- This system architecture is used for automobile network communication.

InnoSoc

OVERVIEW OF VANETs

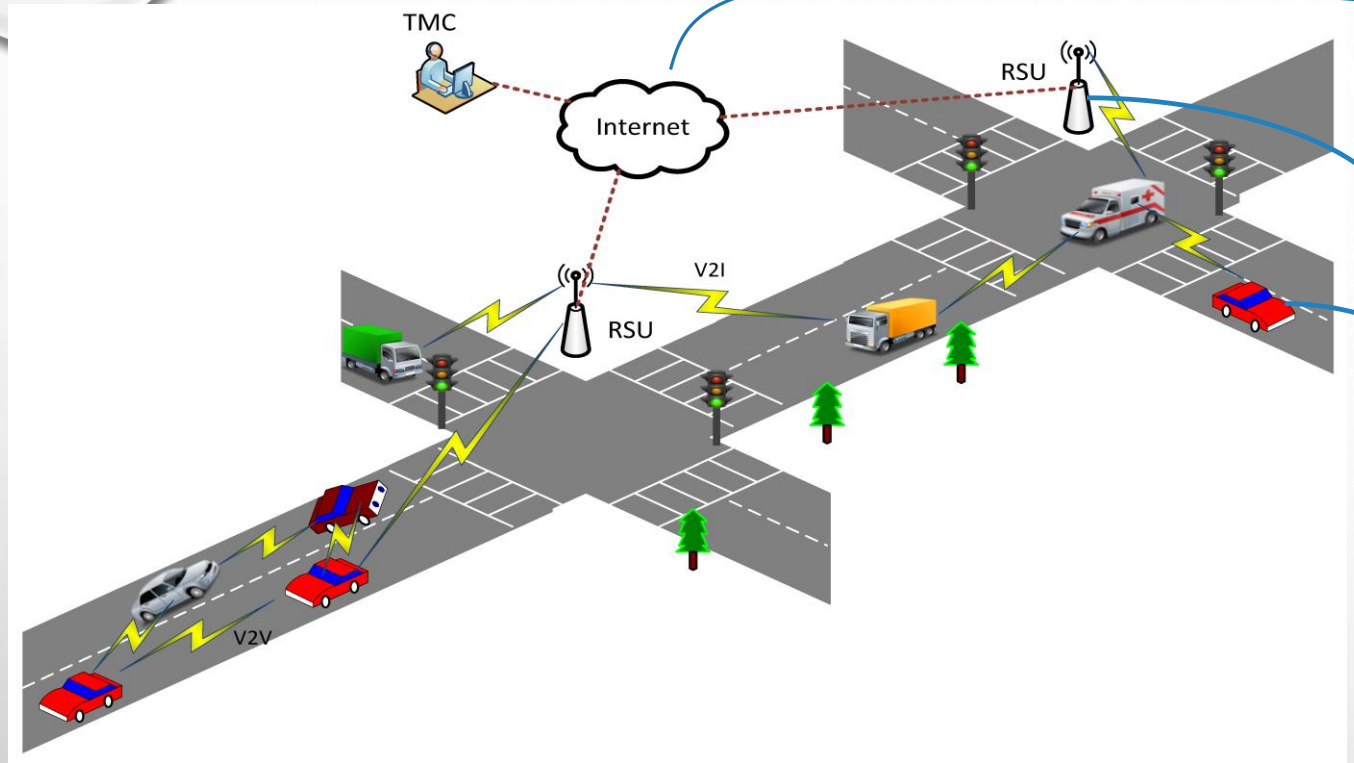


VANET=**V**ehicular **A**d-hoc **NET**work

IMPORTANT ASPECT:

- **high mobility of nodes** in vehicular networks since motor vehicles are moving so fast from each other on the road.
- The high mobility also leads to a **dynamic network topology**, while the links between nodes connect and disconnect very often.
- VANETs have a **potentially large scale** which can include many participants and extend over the entire road network.
- VANETs differ from ***WSN,*** nodes does **not suffer for** any resource like **power and hardware nodes easily mounted in automobiles.**

ARCHITECTURE OF VEHICULAR AD HOC NETWORKS



Generic domain

Infrastructure domain

Mobile domain

[Source: Sai Kiran, Thirumala Rao]

Modern vehicles are designed with powerful communication devices that enable real-time exchange of driving data with each other without a third-party server.

Architecture standard can be divided into three domains: the mobile domain, the infrastructure domain, and the generic domain

InnoSoc

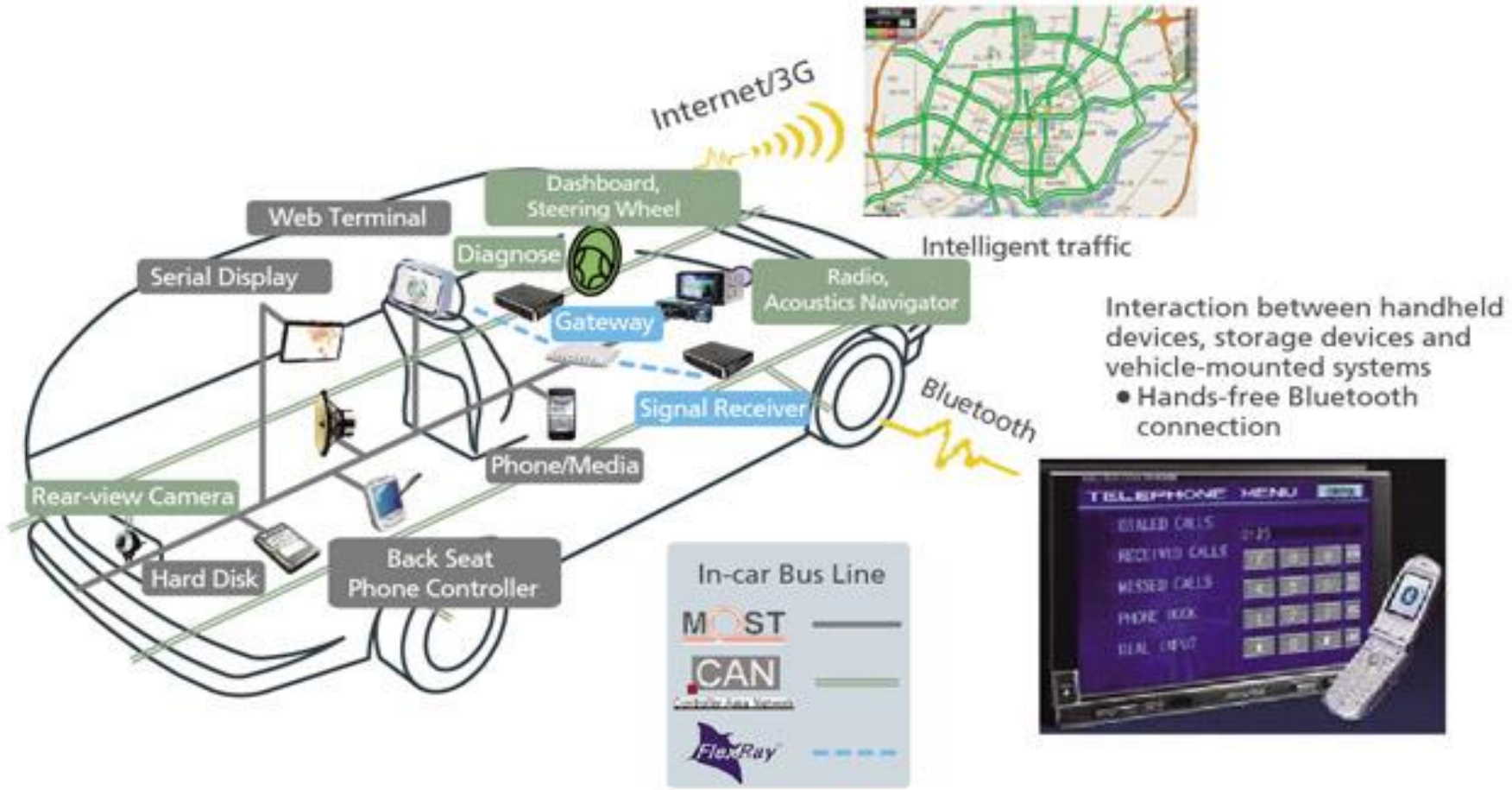
Innovative ICT Solutions for the Societal Challenges

COMMUNICATION ARCHITECTURE FOR VANETs

VANETs can be categorized into four types:

- *In-vehicle communication;*
- *Vehicle-to-Vehicle (V2V);*
- *Vehicle-to-road Infrastructure (V2I);*
- *Vehicle-to-Broadband cloud (V2B).*

IN-VEHICLE COMMUNICATION



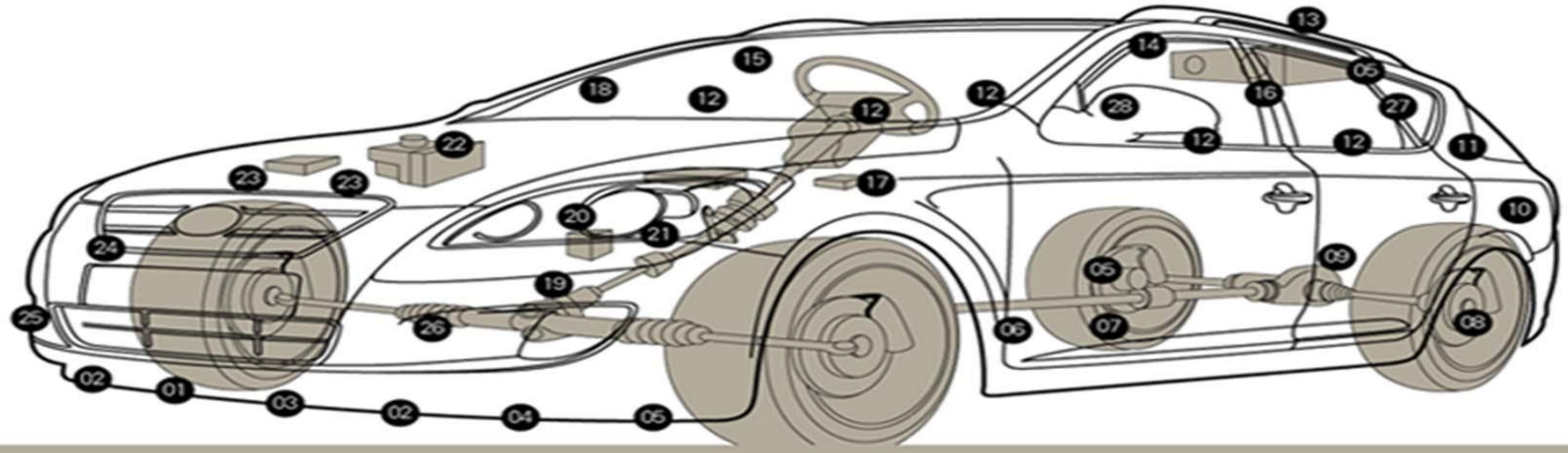
In-vehicle communication system can detect a vehicle's performance and especially driver's fatigue and drowsiness, which is critical for driver and public safety.

[source: http://www.neusoft.com]

IN-VEHICLE COMMUNICATION

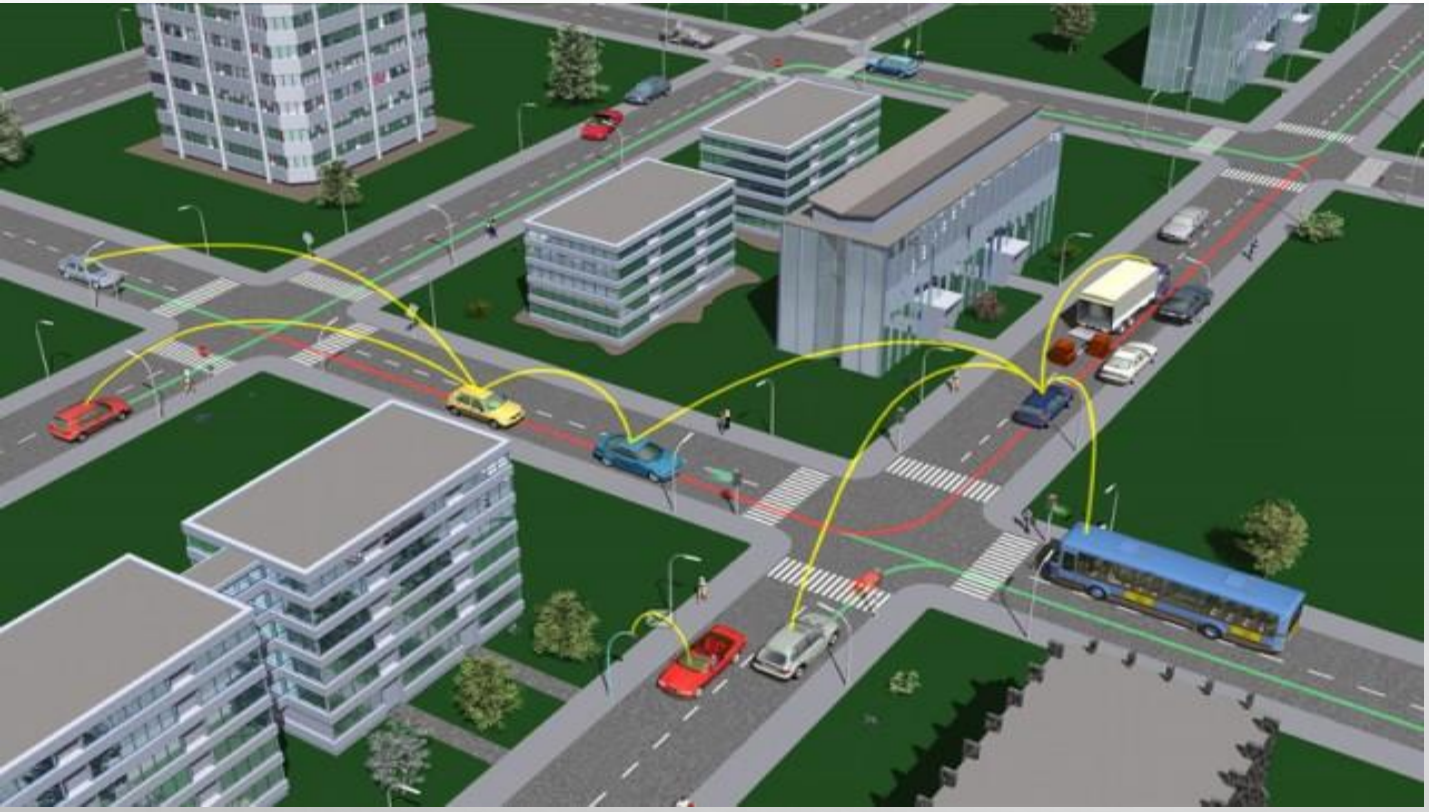
InnoSoc
Innovative ICT Solutions for the Societal Challenges

Advanced Safety Vehicle



1. Road condition sensor
2. Magnetic sensor
3. Vehicle distance sensor
4. Forward obstacle sensor
5. Blind spot monitoring camera
6. Drive recorder
7. Side obstacle sensor
8. Air pressure sensor
9. Inside door lock/unlock
10. Rear obstacle sensor
11. GPS sensor
12. Airbag
13. Road-to-Vehicle / Vehicle-to-Vehicle communication system
14. Rear view camera
15. Water repelling wind shield
16. Seatbelt pretensioner
17. Driver monitoring sensor
18. Headup display
19. Steering angle sensor
20. Electronic control throttle
21. Electronic control brake
22. Fire detection sensor
23. Vehicle speed, acceleration sensor
24. Collision detection sensor
25. Pedestrian collision injury reduction structure
26. Electronic control steering
27. Message display system
28. Hands-free system

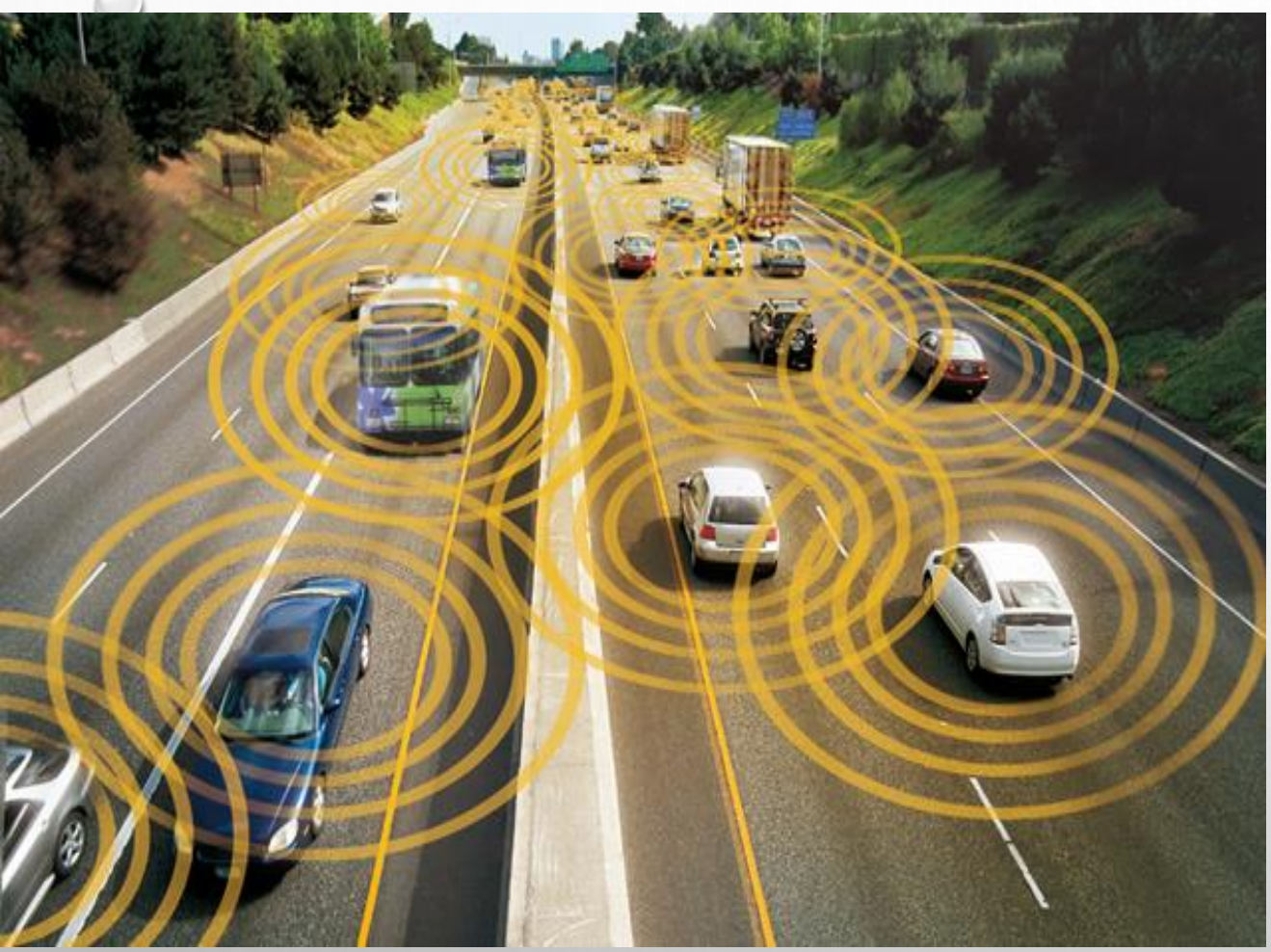
INNOVATION CONCEPTS
VEHICLE-TO-VEHICLE (V2V) COMMUNICATIONS



Source: http://noida.quikr.com

- Comprises a wireless network where automobiles send messages to each other with information about what they're doing.
- This data would include speed, location, direction of travel, braking, and loss of stability vehicle speed, brakes on, anti-lock braking, lane changes, stability control, traction control engaged, windshield wipers on, defroster on, headlamps on in daytime (raining, snowing), gear position (a car in reverse) might be backing out of a parking stall.

INNOVATION CONCEPTS VEHICLE-TO-VEHICLE (V2V) COMMUNICATIONS



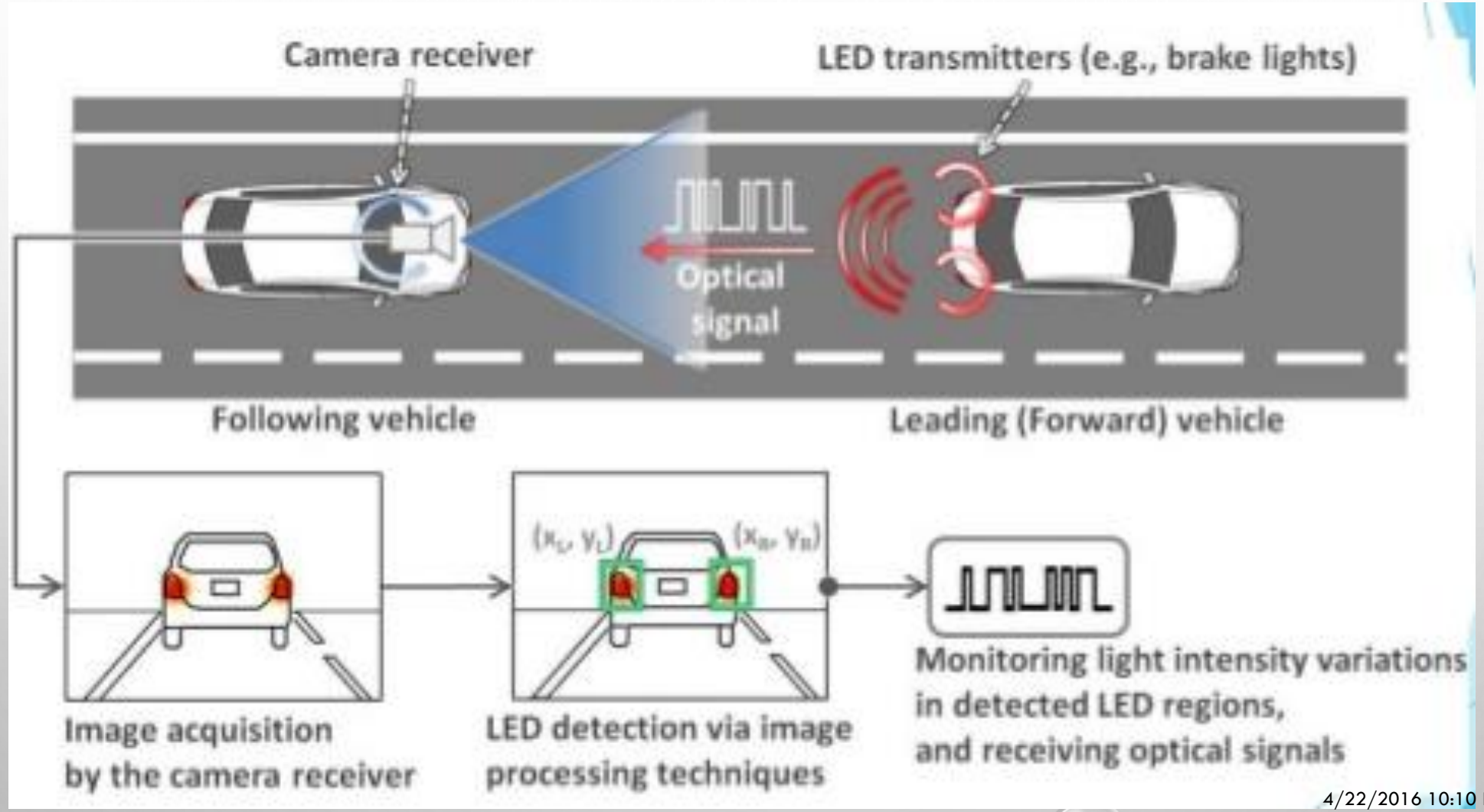
[Source: http://www.thecarconnection.com]

Vehicle-to-vehicle:

- The range is **up to 300 meters** or about 10 seconds at highway speeds.
- Would be a mesh network, meaning every node (car, smart traffic signal, etc.) could send, capture and retransmit signals.
- **Five to 10 hops** on the network would gather traffic conditions a mile ahead.

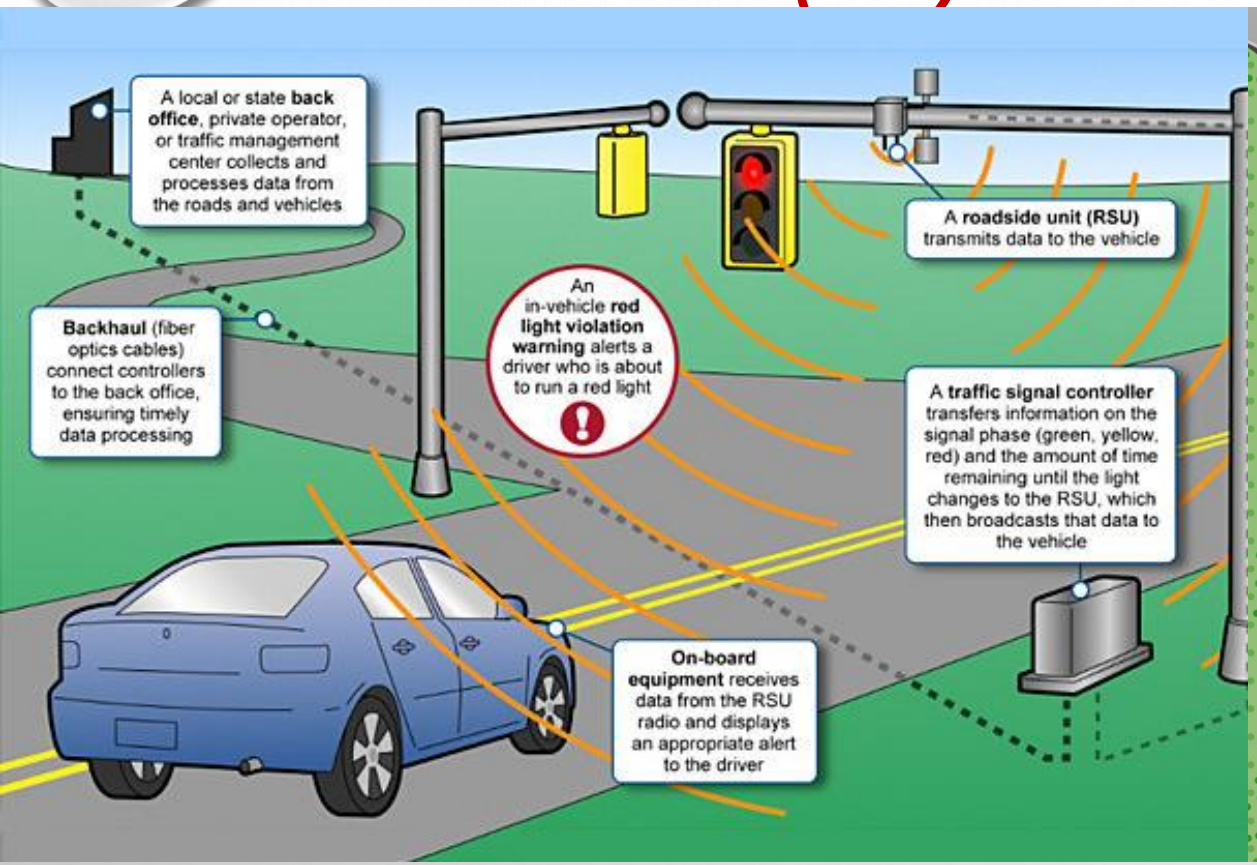
OPTICAL V2V COMMUNICATION

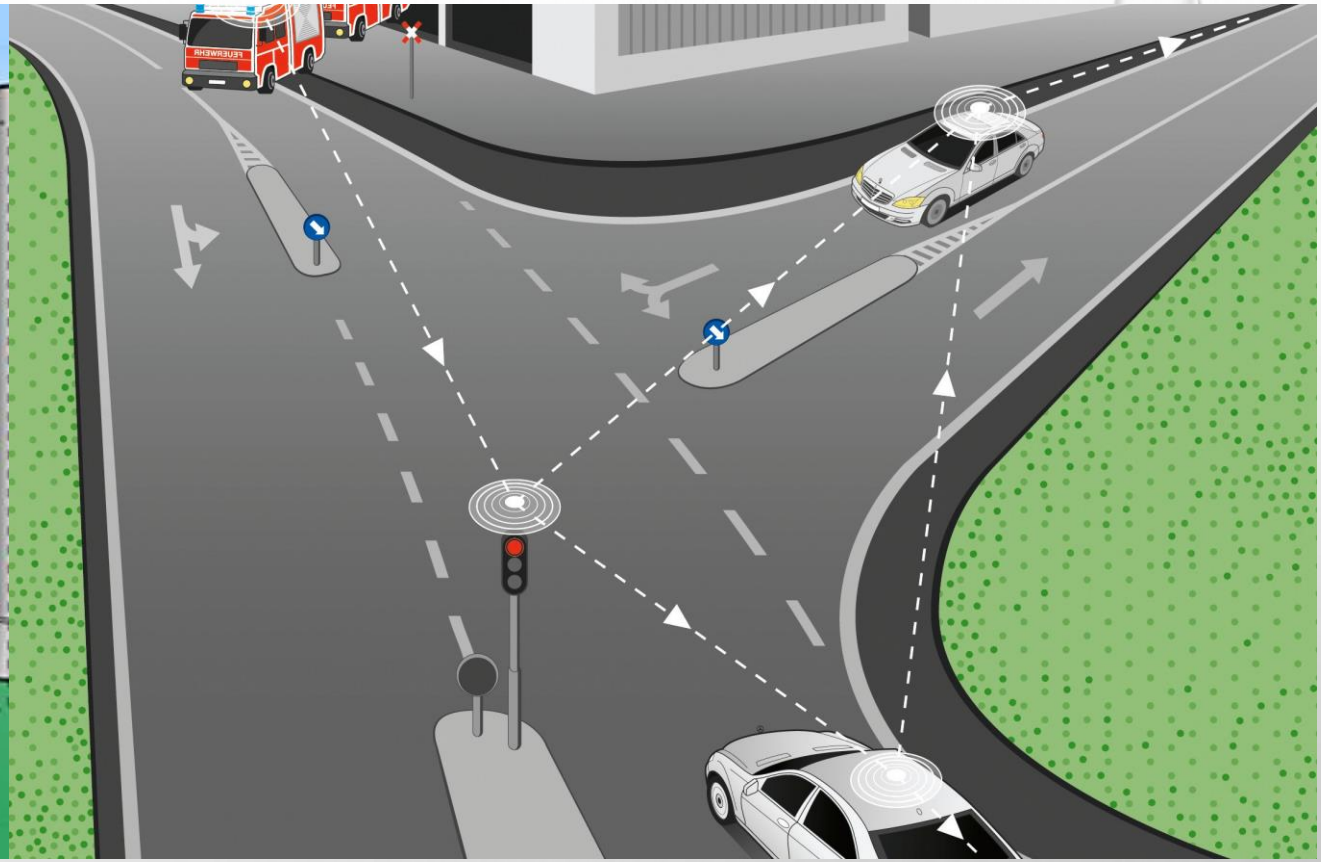
InnoSoc



VEHICLE-TO-ROAD INFRASTRUCTURE (V2I)

InnoSoc

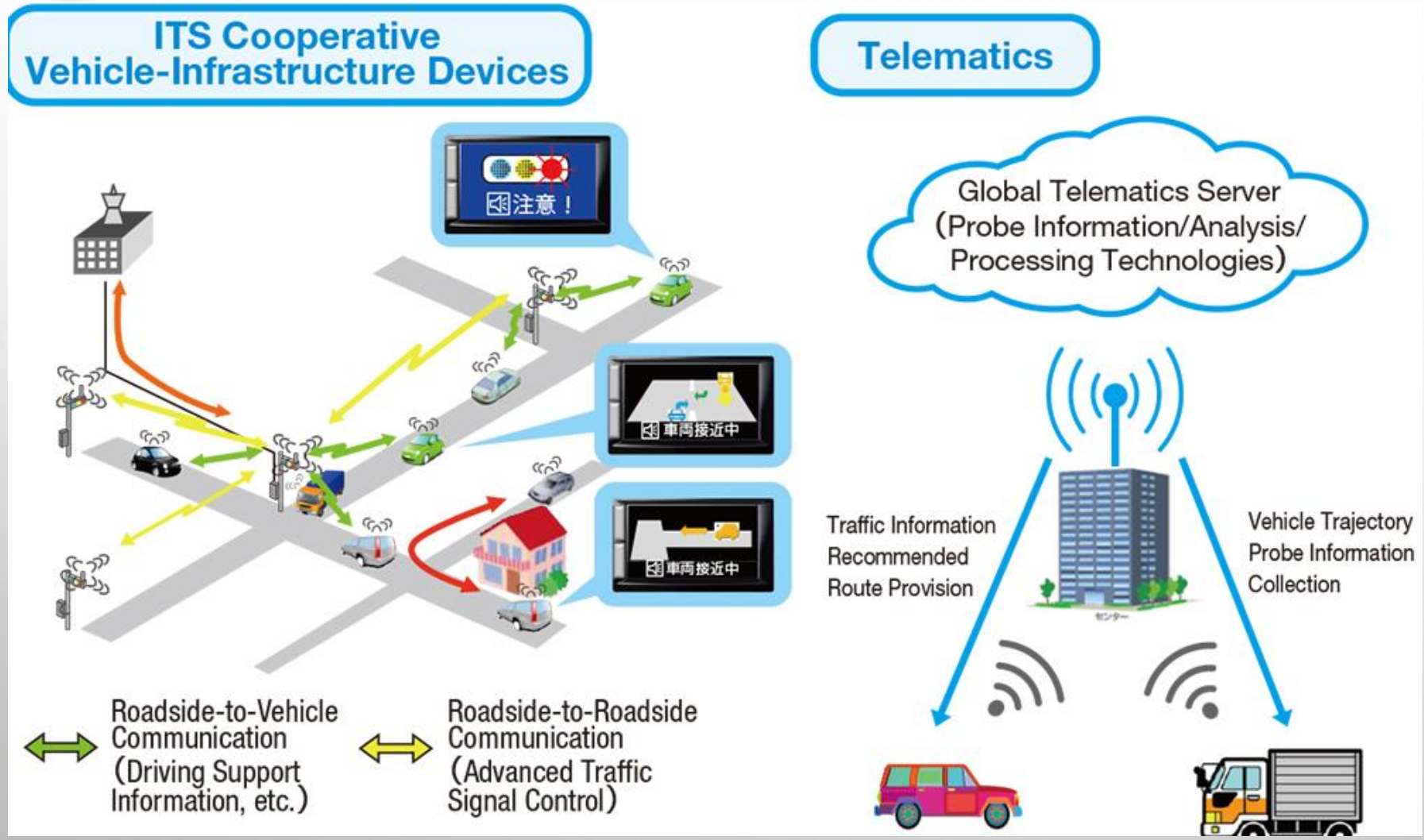




http://www.networkworld.com

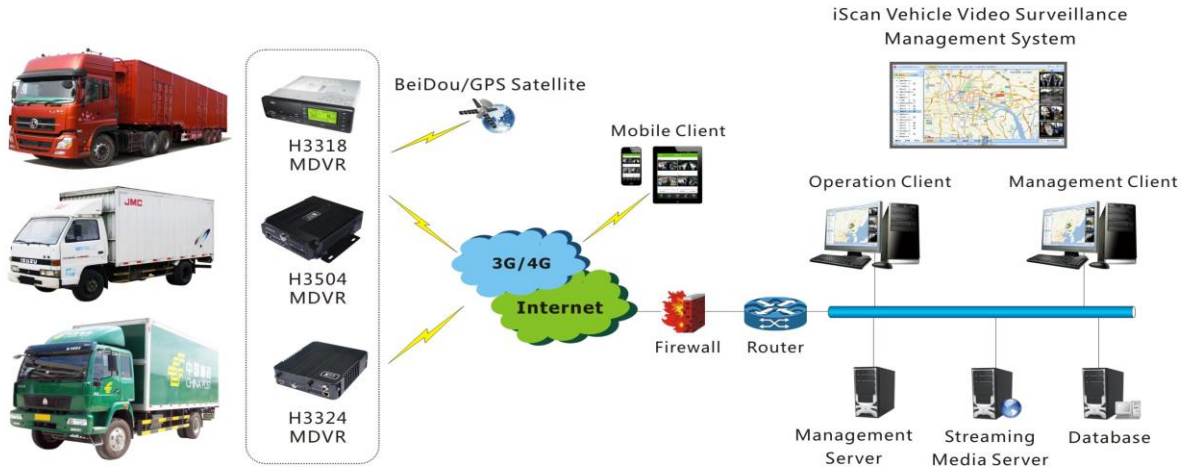
V2I communication enables real-time traffic/weather updates for drivers and provides environmental sensing and monitoring.

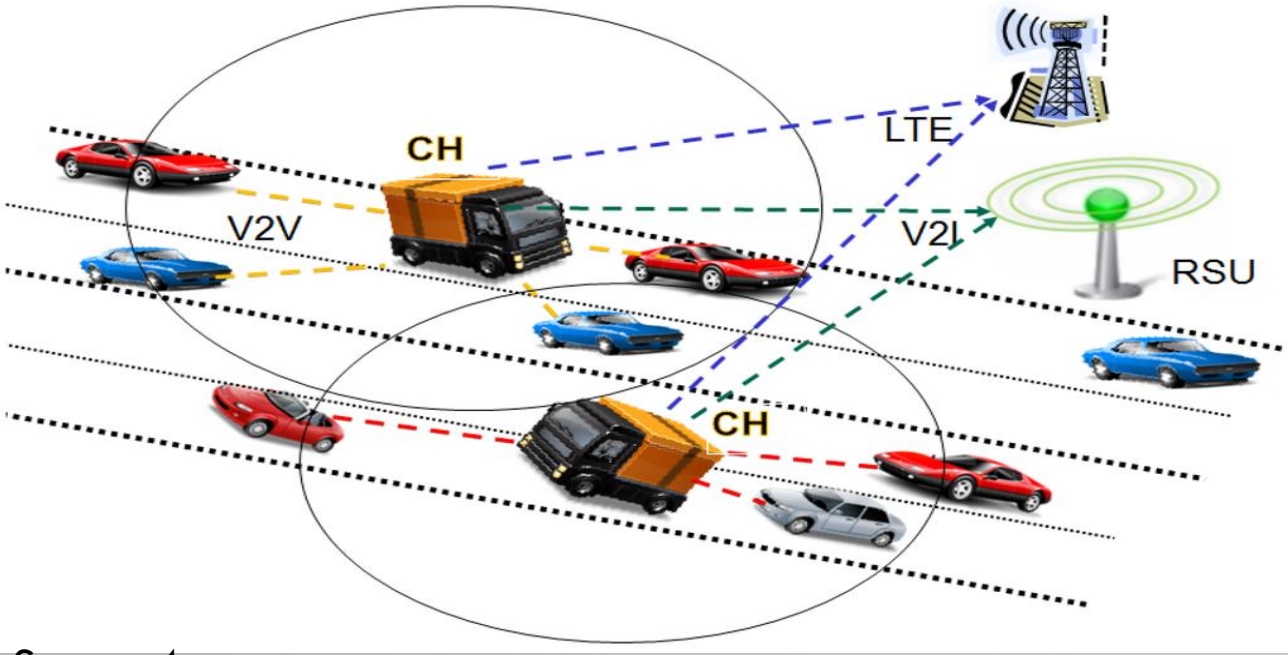
VEHICLE-TO-ROAD INFRASTRUCTURE (V2I)



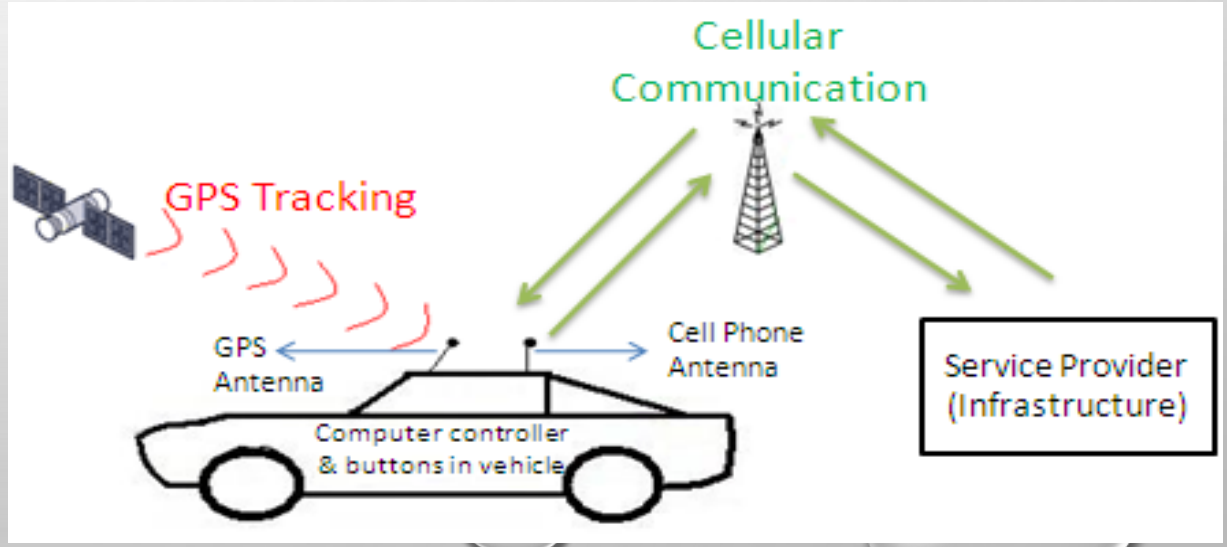
Telematics is a computer and electronic technology involved in our cars -- it's called telematics.

VEHICLE-TO-BROADBAND CLOUD (V2B) COMMUNICATION





- Vehicles may communicate via **wireless broadband mechanisms such as 3G/4G.** As the broadband cloud may include more traffic information and monitoring data as well as infotainment, this type of communication will be useful for **active driver assistance and vehicle tracking**



Source 4

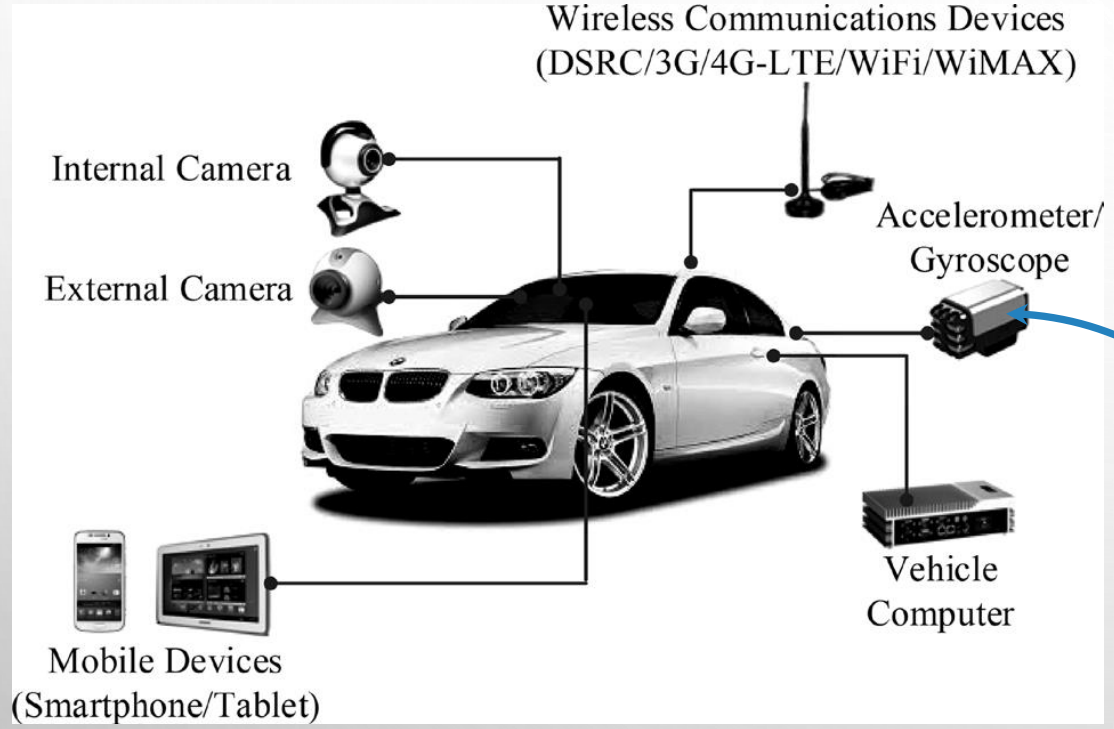
CHALLENGES AND FUTURE TRENDS OF VANETs

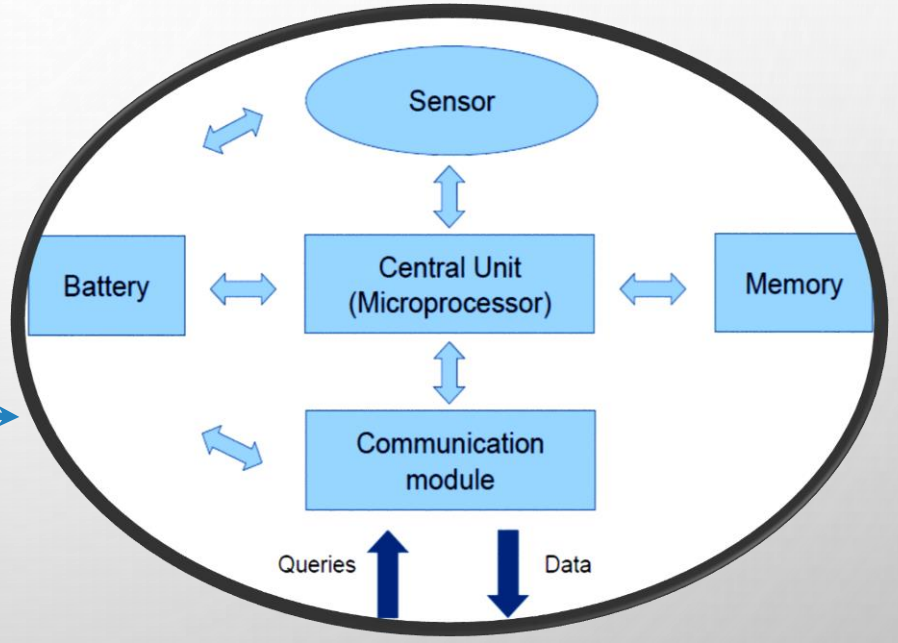
DETERMINED OF:

- SMART SENSORS;
- SMART AND SELF- DRIVE AUTOMATED CARS;
- NEW INFORMATION TECHNOLOGIES:
  - ✓ IoT TECHNOLOGY;
  - ✓ Mobile cloud computing in vehicular networks.

InnoSoc
ZAGREB 2016

SMART SENSORS

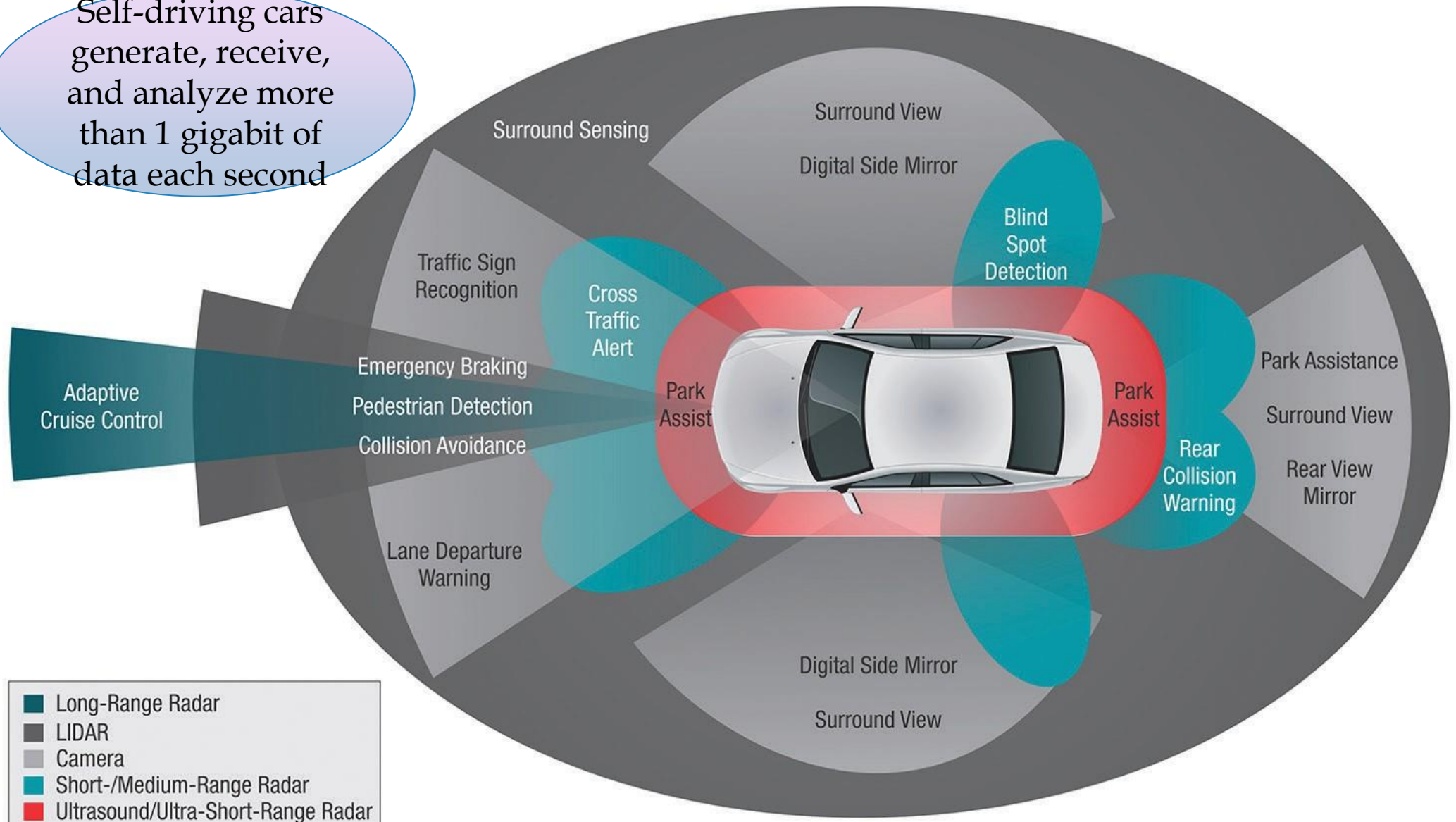




InnoSoc
Innovative ICT Solutions for the Societal Challenges

INNOVATION SMART OR SELF-DRIVING CARS

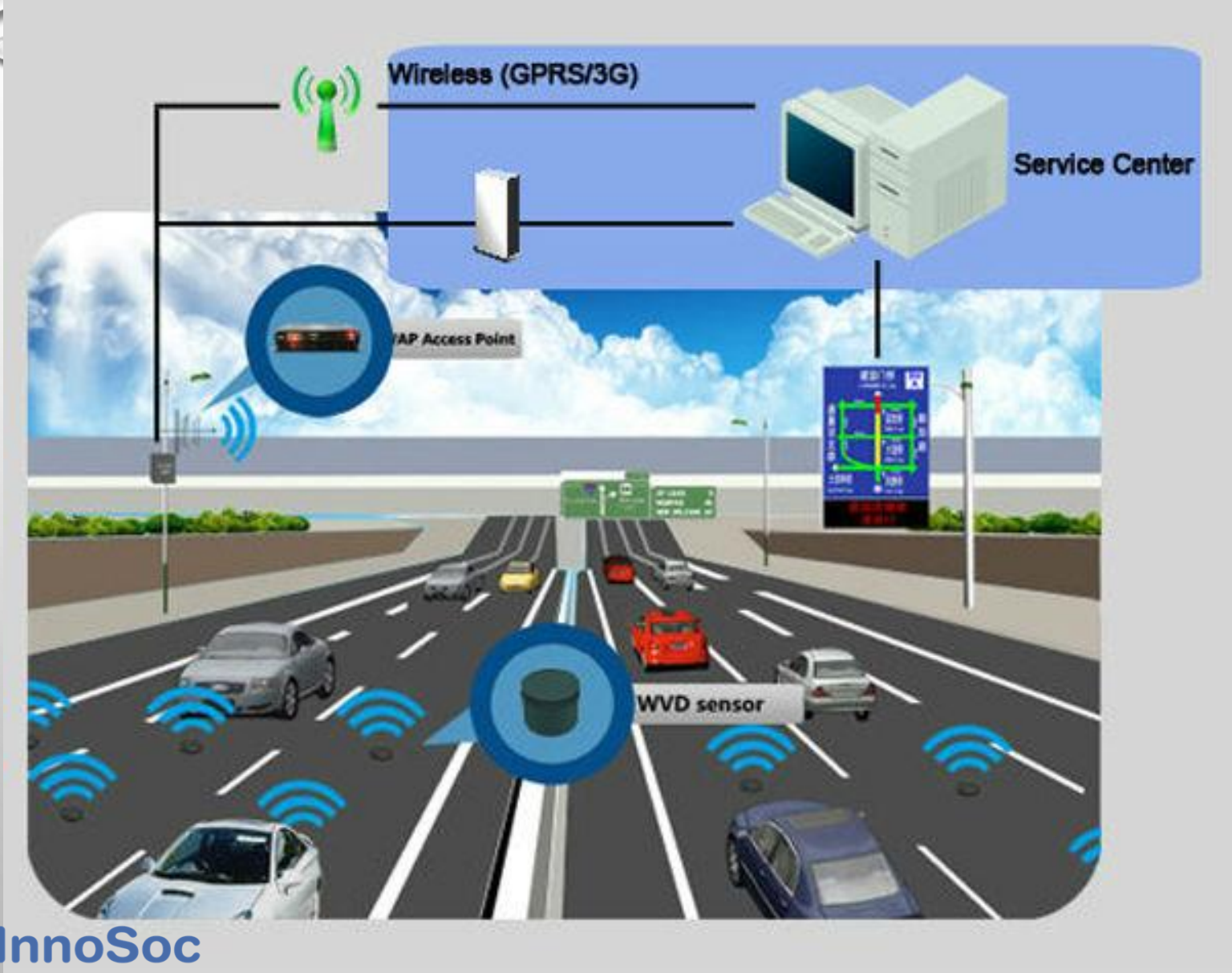
Self-driving cars generate, receive, and analyze more than 1 gigabit of data each second



Assisted and automated driving relies on multi-modal systems with input from a variety of sensors, including ultrasound, radar, LIDAR (LIght Detection and Ranging) and cameras **Satellite communications**, as well as radio communications with V2V and V2I, are necessary for positioning, localization, highway conditions and other information.

Working in real time

WIRELESS VEHICLE DETECTION



WVD (wireless vehicle detection) sensor is designed for pursuit of high efficiency and low cost ITS (intelligent transport system) traffic application systems.

Based on technology of magnetic detection and uPower® wireless sensor network, sensors can be **easily embedded under the road** in few minutes without any wiring, to acquire dynamic traffic flow information with no maintenance for many years.

Applications:

Traffic flow measurement
Speed measurement
Driving direction detection
Red light enforcement
Vehicle counting
Traffic signal optimization
Entrance controlling
Vehicle classification
Traffic information guidance

IoT AND VAHICLE

- The Internet of Things (IoT) is the **network of physical objects** - devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data.
- The IoT allows **objects to be sensed and controlled remotely across existing network infrastructure**, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit.
- When IoT is built up with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities [7].

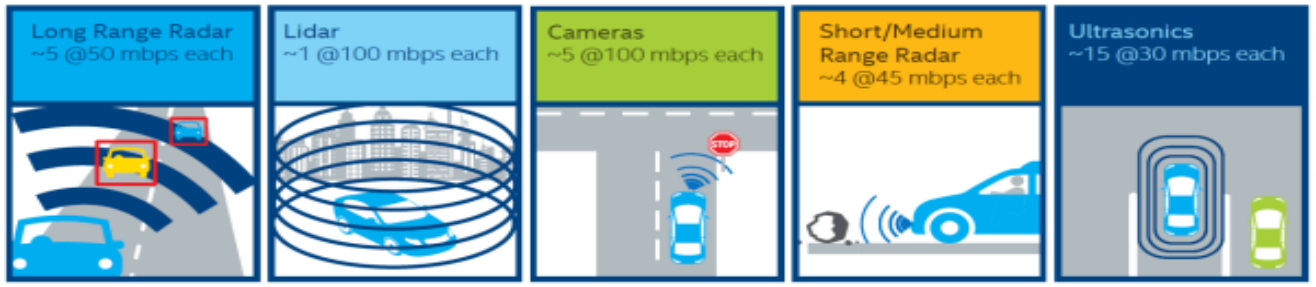
IoT AND VAHICLE

- Internet of things (IoT) connectivity is **transforming the relationship** between automakers and drivers.
- **Connected cars are "moving IoT sensors",** providing fast amounts data about performance, maintenance, driver behavior and more.
- The Internet of Things is already **transforming automobiles.**
- Though automakers have focused much of their attention on connecting cars to existing voice and data networks, **the real payoffs will come as vehicles become capable of sensing data to each other,** and their surroundings and of communicating with their drivers, each other and the infrastructure around them.

IoT AND VAHICLE

- **Increase loyalty** through deeper insights and closer relationships with customers;
- Continually refine and **improve** their vehicles, and build better cars in the future;
- Gain a competitive edge by safely **extending the compelling Internet services** that customers use in other areas of their lives to the hours they spend on the road;
- Deliver **new high-value services such as stolen vehicle tracking, emergency assistance, remote entry, usage-based insurance (UBI) and many others.**

Sourse: http://www.psfk.com



IoT TECHNOLOGY

- The latest fleet management solutions take advantage of the **IoT to help fleet operators**:
- Comply with environmental and safety regulations;
- Optimize maintenance and logistics for more efficient operations;
- Monitor and optimize routes, maintenance, driver behavior, and vehicle health (including tire pressure) to reduce fuel consumption;
- Monitor driver performance and vehicle status for better safety;
- Perform preventative maintenance to improve vehicle valuation

HOW WILL IoT WORK FOR A CONNECTED VEHICLE?

InnoSoc
ZAGREB 2016

There are five ways to develop apps for vehicles.

1. Run apps in the in-vehicle entertainment systems (blackberry QNX CAR, windows embedded automotive, automotive grade Linux and android).

2. Use a link to a smartphone (airbiquity, opencar, cloudcar, smartdevicelink / applink, mirrorlink, apple carplay, google open automotive alliance and windows in the car).

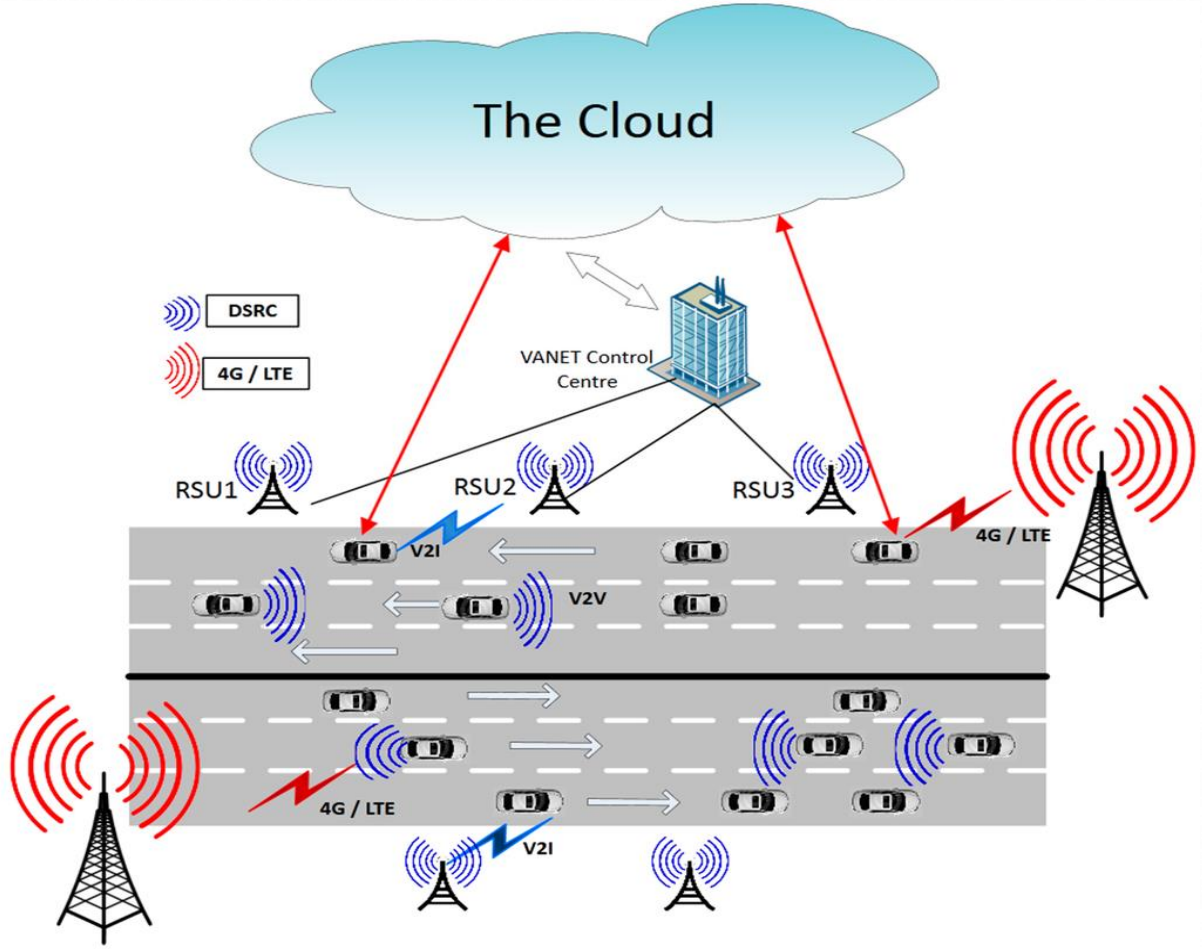
3. Remote access to the vehicle through an API (Automaker Nissan activated a remote access feature that let owners of its Leaf electric car remotely adjust climate controls and check battery status via a smartphone app., ford remote API, airbiquity, reverse engineering of vehicle protocols).

4. Access to data through the on board diagnostics port called OBD-II (dash labs, mojio, carvoyant, metromile and smartdrive.Io).

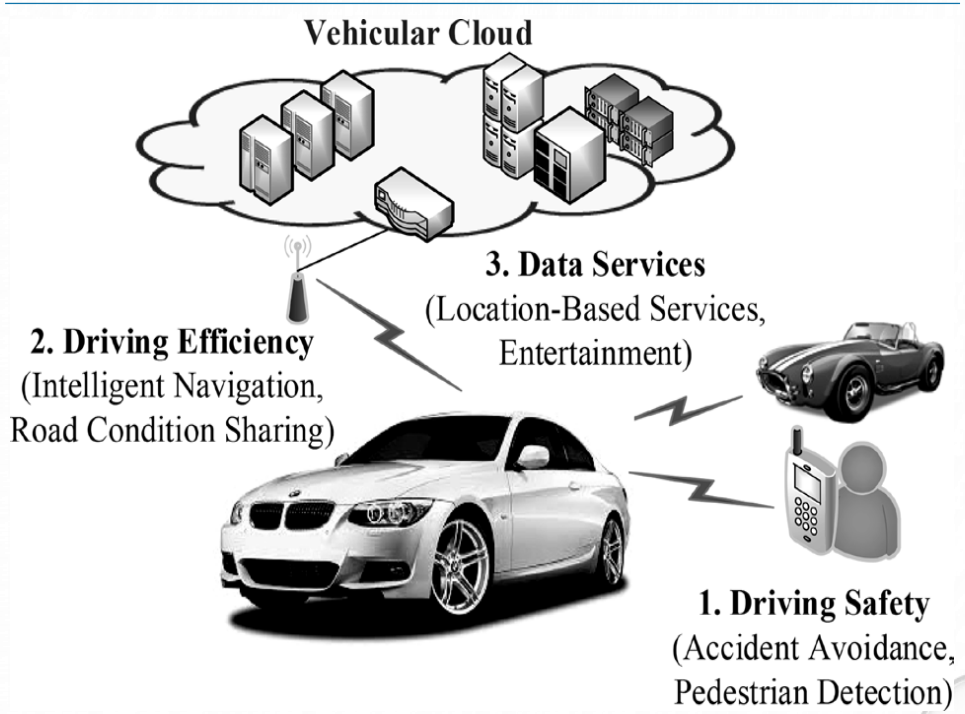
5. New and emerging initiatives (W3C automotive and web platform business group and openXC).

MOBILE CLOUD COMPUTING IN VEHICULAR NETWORKS

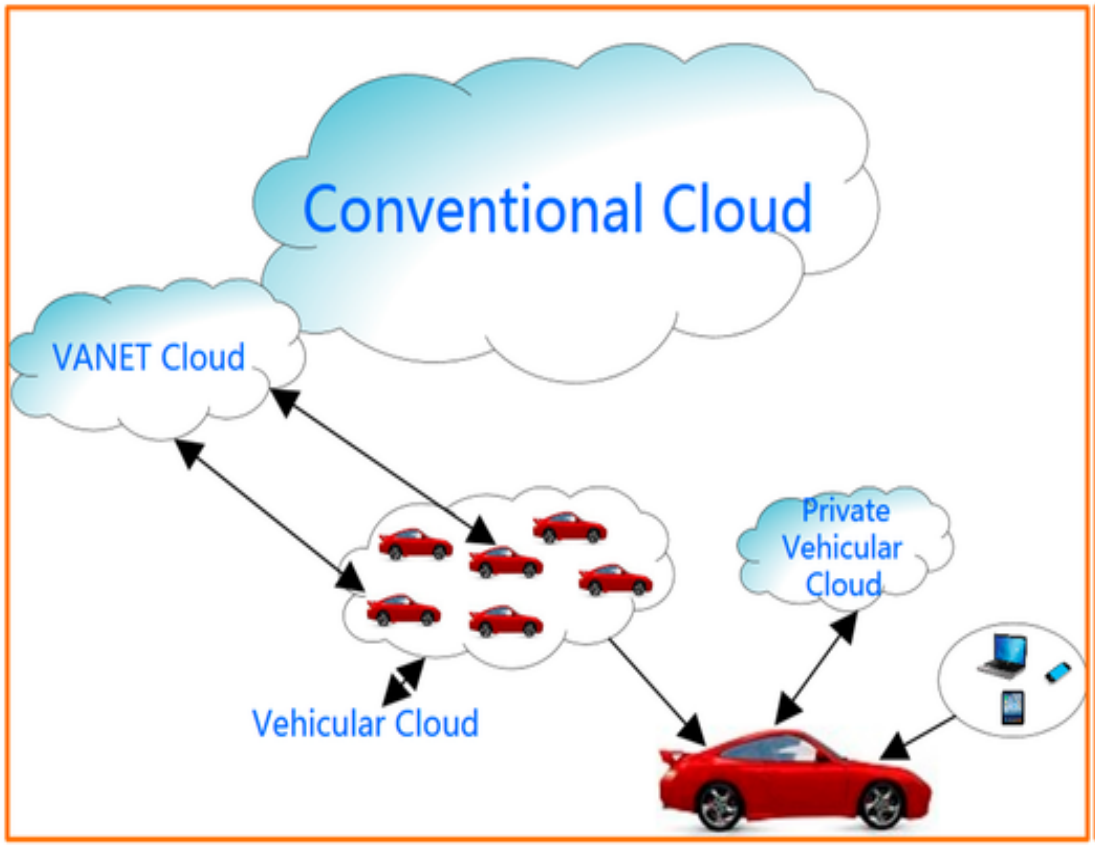
Mobile cloud computing can support various cloud services for smart road networks, such as pedestrian protection for the driving safety.



Source: Kamran Zaidi and Muttukrishnan Rajarajan



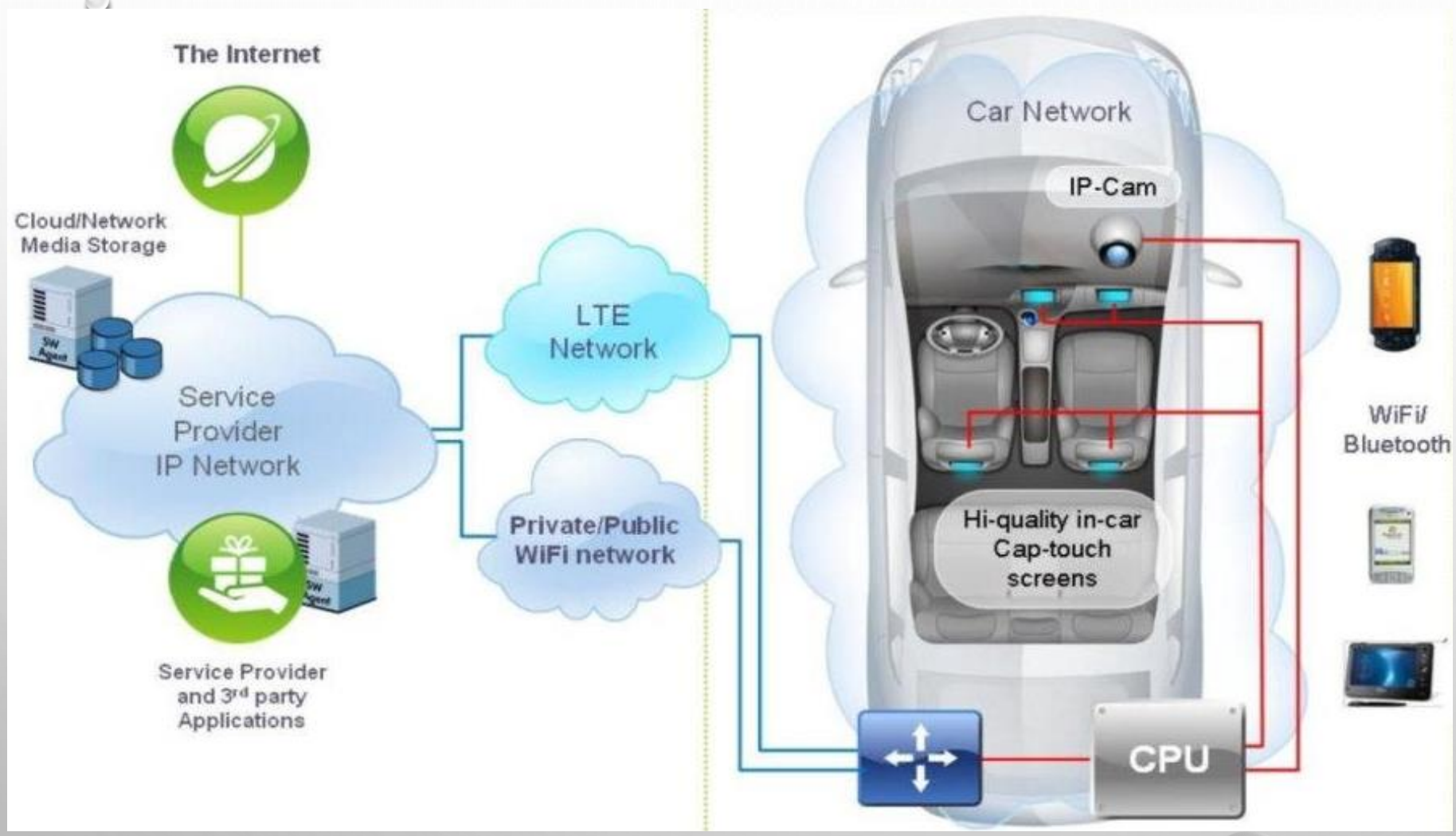
MOBILE CLOUD COMPUTING IN VEHICULAR NETWORKS



VANETs in the Cloud	Vehicular Cloud	Private Vehicular Cloud
Traffic Information	Data Storage	Data Storage
Weather Information	Computing Resources	Computing Resources
Toll Collection	Weather Data Collection	Hotspot
Infotainment Services	Multimedia Pooling	

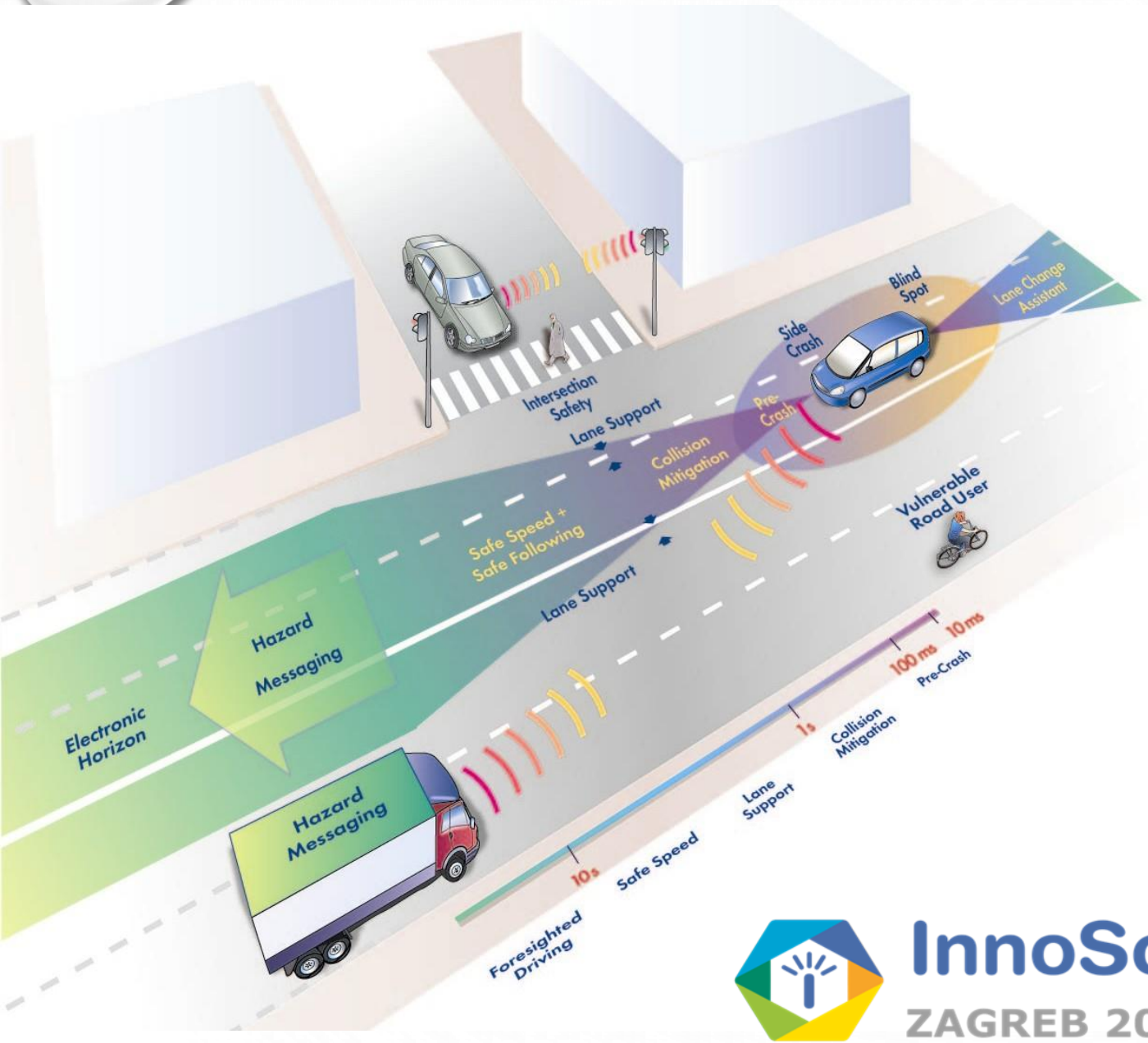
Source: Kamran Zaidi and Muttukrishnan Rajarajan

MOBILE CLOUD COMPUTING IN VEHICULAR NETWORKS



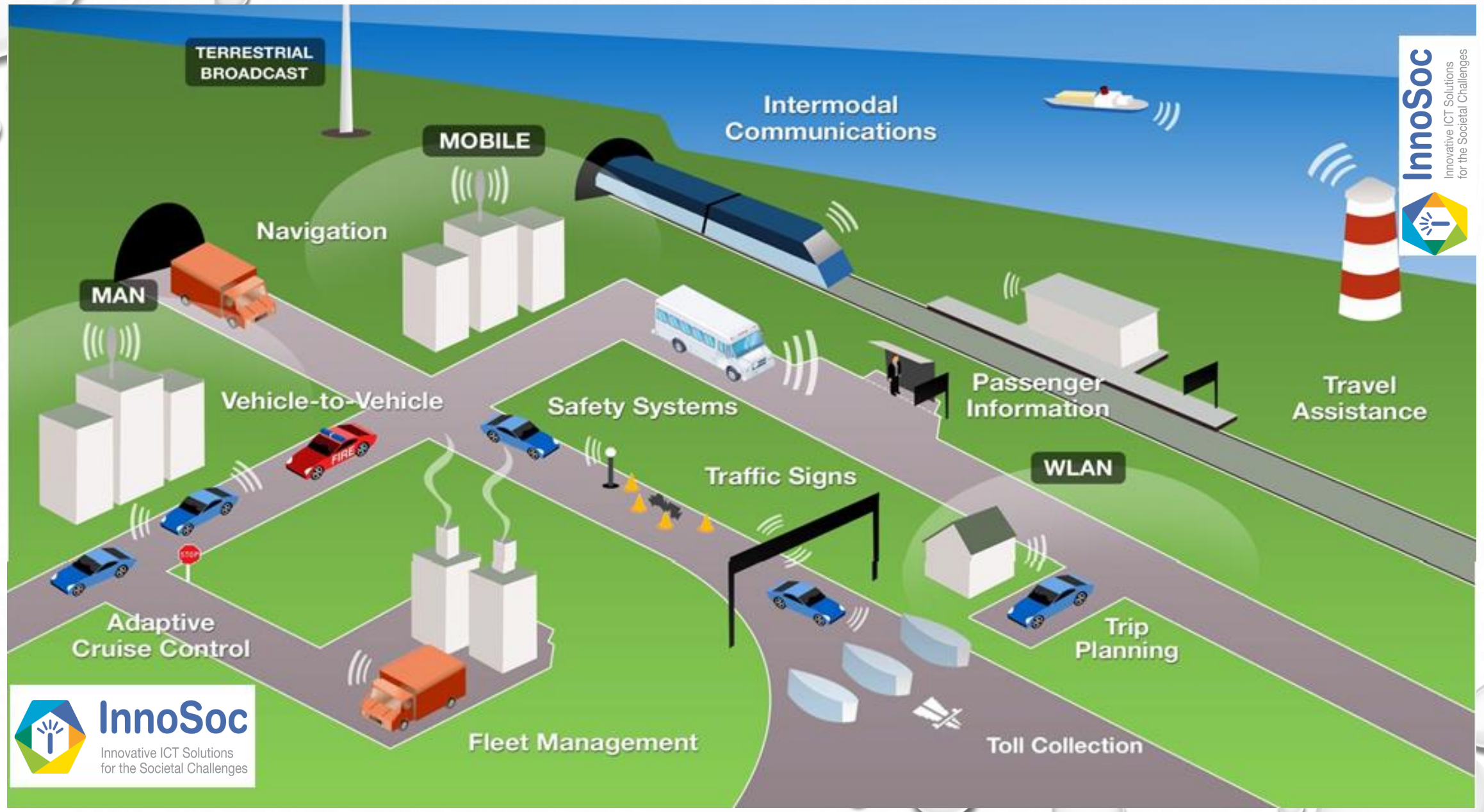
Intelligent network + in car hardware and software = LTE connected car

INTELIGENT TRANSPORT SYSTEMS



- The concept of ITS include a network of sensor nodes that share information among themselves and with servers off the road.
- The sensors can transmit a signal to a nearby road sign that warns of deceleration, change the direction of movement, etc., Which increases driving safety.
- So realize concept "smart roads".

INTELIGENT TRANSPORT SYSTEMS



WIRELESS SENSOR NETWORK ARCHITECTURES FOR ITS

- Network architecture for ITS applications using WSN technology, depending on the needs and the cost.
- Information exchange can be performed either through ad-hoc communication, using infrastructure, or hybrid.
- Distinguish two types of sensors: on-road and on-vehicle sensors. The combination of sensor types and communication paradigms gives to various applications.

InnoSoc
ZAGREB 2016

REQUIREMENTS FOR THE SMART ROADS

Reliability: in WSN based ITS many critical decisions must be token regarding the received information. So, the lost in some data packets can lead to unwanted system behavior. The harsh environment conditions and the lossy nature of wireless link raise the probability of lost data which require **reliable communication protocol.**

Real-time: despite receiving reliable information, real time reception may be also more or less critical regarding the application. **Ensuring delay guarantee** in WSN is challenging and must be dealt by the underlying solution.

Heterogeneity: the coexistence of many WSN based its solutions technologies is primordial for **long life of the system**.

Security: wireless communications impose more security issues namely, jamming and criminality attacks, physical compromising of notes, etc. This makes **security handling mandatory** for any proposed WSN based solution.

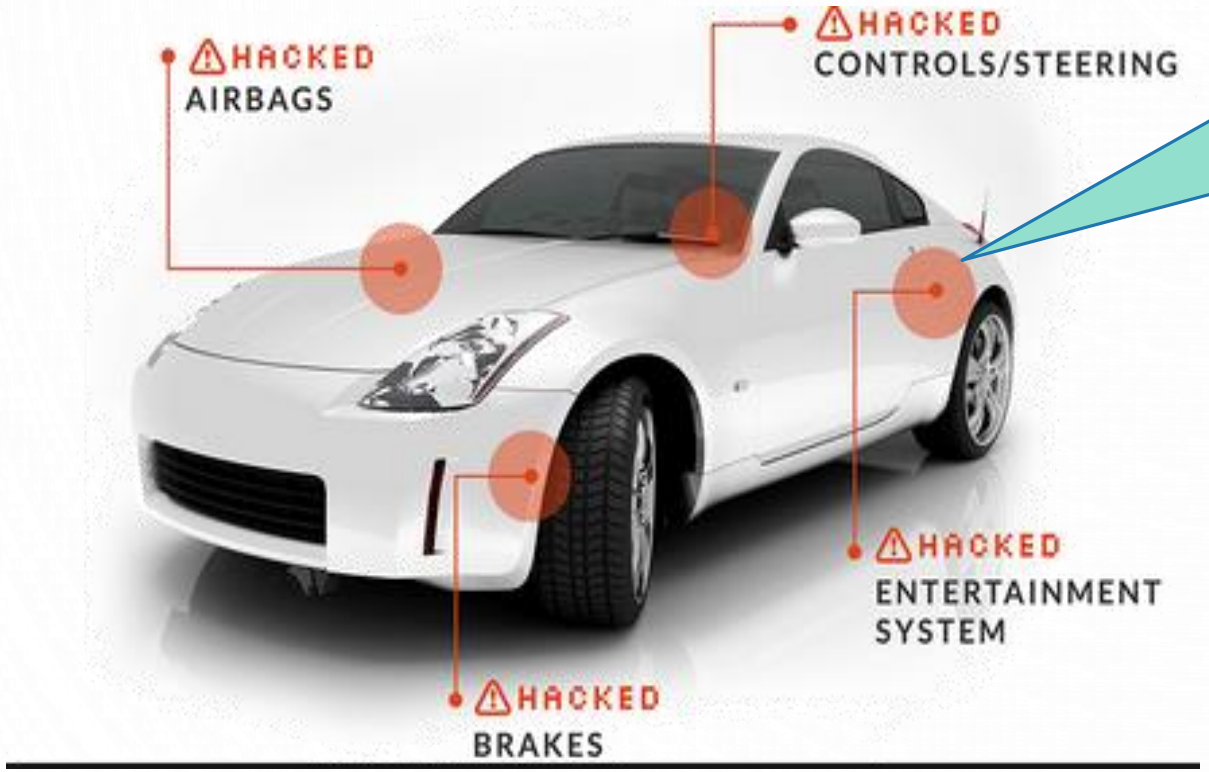
SECURITY IN VANETs

- **When data compromised, the whole system suffers;**
- **The nature of VANETs could lead to malicious attacks.**
  - Predictable movement of nodes;
  - High mobility of victim/attacker;
- **Adversaries (hostile) could break the system.**
  - Data sinkholes (black hole);
  - Feed false information;
  - Sybil attacks;
  - Flood system.
- Security measures must be taken to avoid malicious attacks on the system.

ATTACHERS:

- **Insider or outsider**
  - ✓ Insider- valid user
  - ✓ Outsider-intruder, limited attack options
- **Malicious or rational**
  - ✓ Malicious –no personal benefit, intends to harm other users;
  - ✓ Rational-seeks personal benefits, more predictable attack;
- **Active or passive**
  - ✓ Active: generates packets, participates in the network
  - ✓ Passive: eavesdrop, track users.

SECURITY IN VANETs



Hackers can attack car through **CAN bus,** every computer is connected to system that influences vehicle's parts like horn and seat belts to steering, breaks.

A motivated attacker can realize these threats by identifying and exploiting attacks via a number of 'entry points'.
Examples include wireless interfaces such as cellular, Bluetooth and keyless entry systems, diagnostic port, sensors and attacks on the electronic control units themselves.

SECURITY REQUIREMENTS FOR VANETs

1. **Authentication In Vehicular Communication** every message must be authenticated, to make sure for its origin
2. ***Availability*** -Vehicular network must be available all the time, for many applications vehicular networks will require real time, these applications need faster response from sensor networks or even Ad Hoc Network, a delay in seconds for some applications will make the message meaningless and maybe the result will be devastating.
3. ***Non-repudiation*** -Non-repudiation will facilitate the ability to identify the attackers even after the attack happens.

SECURITY REQUIREMENTS FOR VANETs

4. Privacy- Keeping the information of the drivers away from unauthorized observers, this information like real identity, trip path, speed.

5. Real-time constraints -Vehicles move in high speed, this will require a real-time response in some situation, or the result will be devastating.

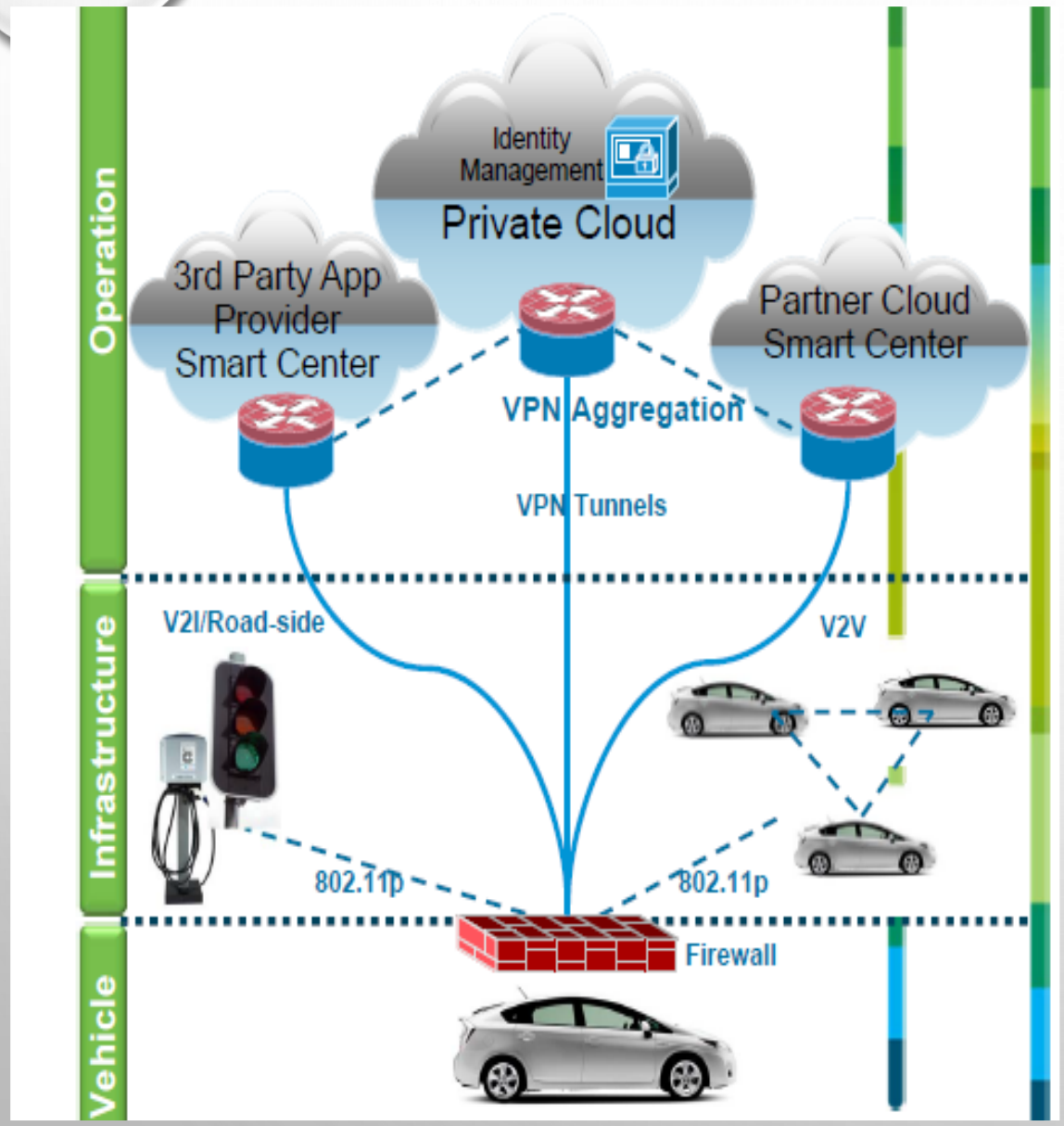
6. *Integrity* -Integrity for all messages should be protected to prevent attackers from change them, and message contents to be trusted.

7. Confidentiality -The privacy of each driver must be protected; the messages should be encrypted to prevent outsiders from gaining the drivers information.

InnoSoc
Innovative ICT Solutions
for the Societal Challenges

SECURITY CONNECTIVITY

InnoSoc
Innovative ICT Solutions for the Societal Challenges



Highly security communication from car to wider network

- Encryption;
- Wide range of VPN technology;
- Security tunnels to OEM, partners, third party applications providers.

Comprehensive security In –vehicle protection

- Strong firewall
- Intrusion Prevention;
- Antivirus/malware protection

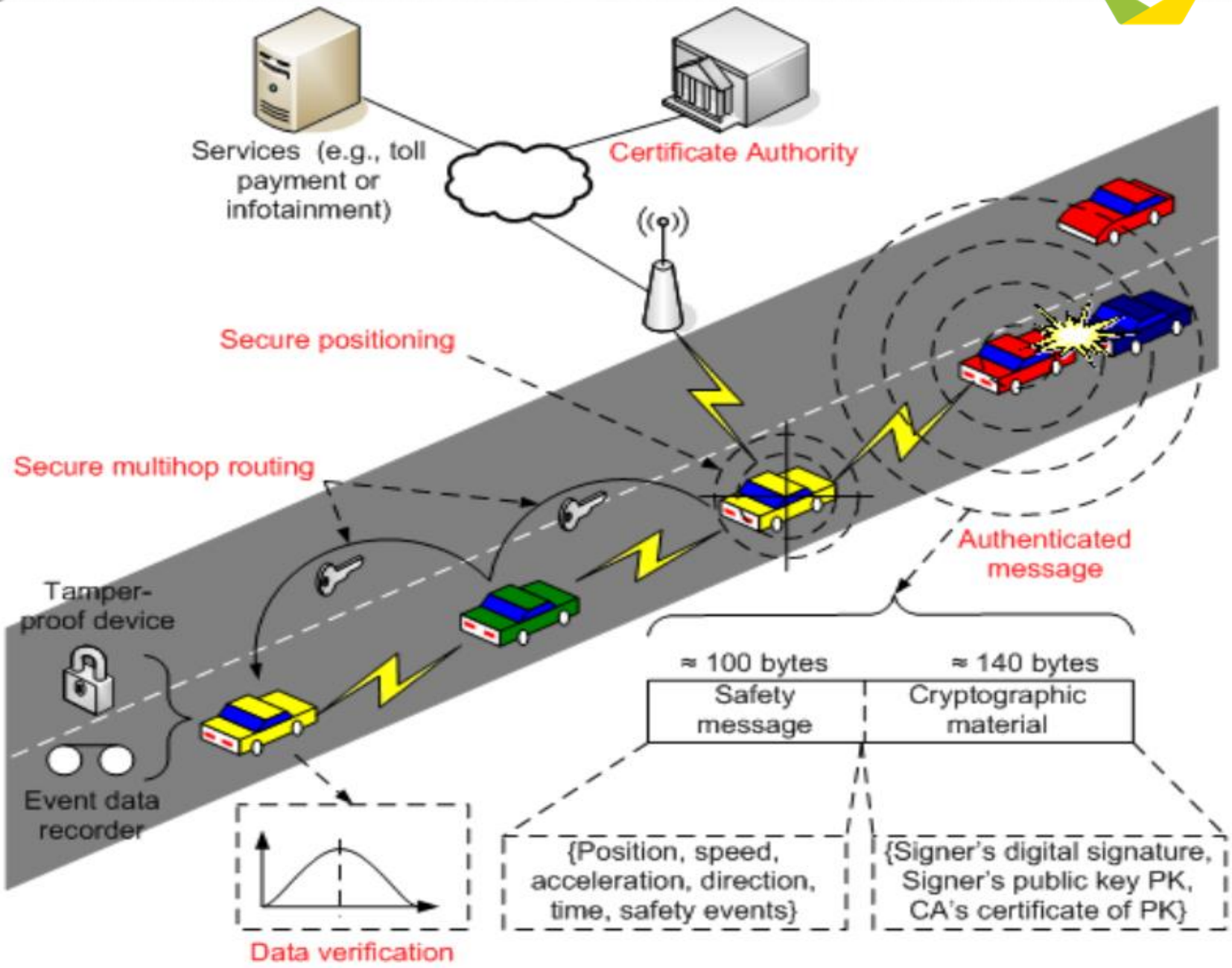
On-demand security connectivity

- V2V, V2I;

Easy to deploy and manage

- Centralized identity &policy management;
- Authentication, authorization, accounting

SECURITY ARCHITECTURE



Ataks on the firmware sensors and built-street sensors

- For the firmware sensors is also not digitally signed and access to them is not only authorized, the attacker can **change the firmware or changing the configuration of sensors**.
- An attacker who just wants to cause problems, for example, can to select the **built-street sensors to communicate on different radio channels of access points, effectively cutting the wireless connection between them.**

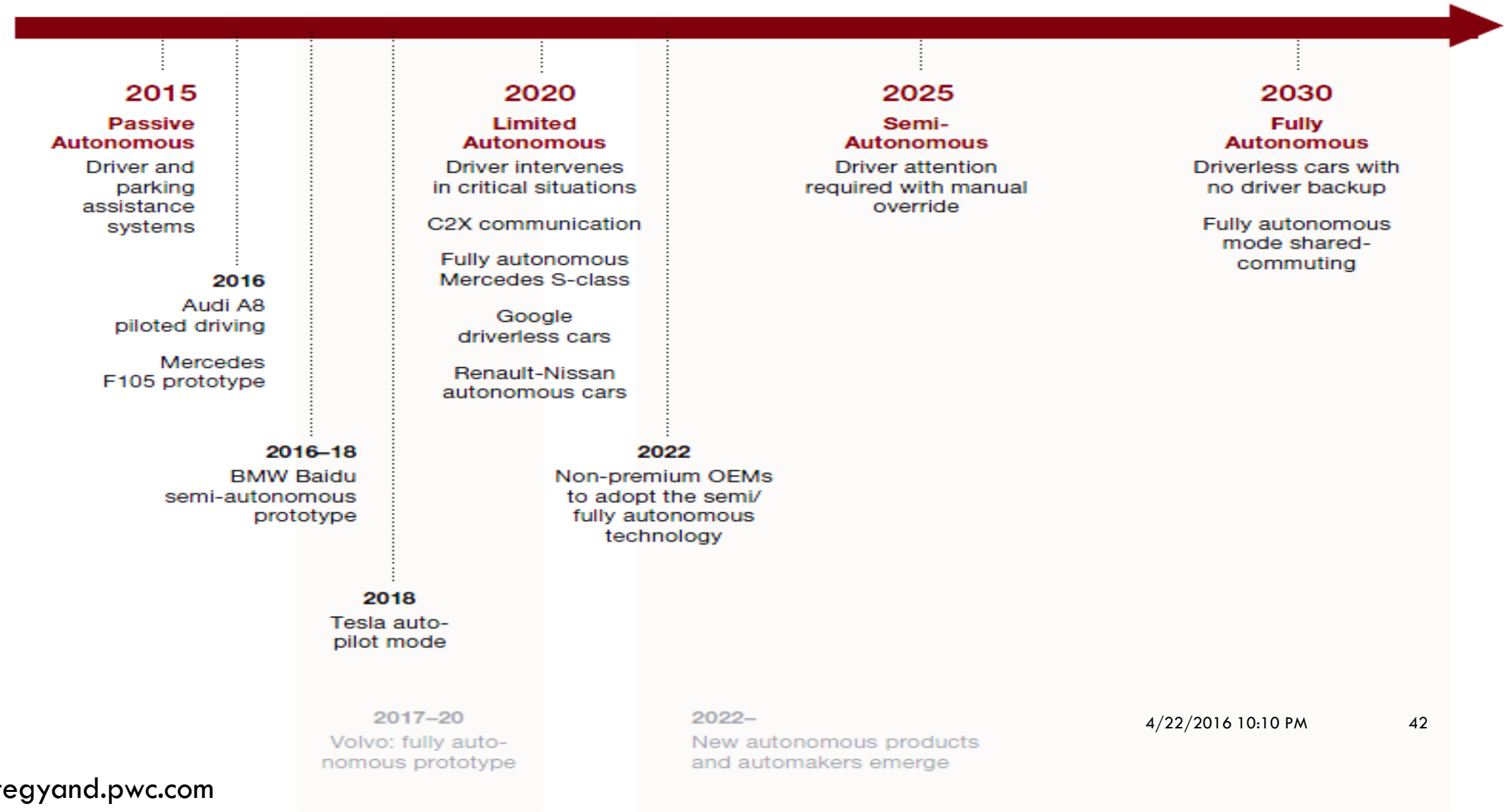
InnoSoc
Innovative ICT Solutions for the Societal Challenges

TYPES OF ATTACKS FOR TRAFFIC LITE

InnoSoc
Innovative ICT Solutions for the Societal Challenges

1. **Denial of service** - stopping normal light functionality for traffic lite, set all lights to red. This would cause traffic congestion and considerable confusion for drivers. This state can be triggered remotely, but cannot be reset without physical access to the controller.
2. **Traffic congestion** - attacks could be made against the entire traffic infrastructure of a city which would manipulate the timings of an intersection relative to its neighbors. The effect would be that of a poorly managed road network, causing significant traffic congestion but remaining far less detectable than overt actions.
3. **Light control an attacker can also control lights for personal gain**. Lights could be changed to be green along the route the attacker is driving away.

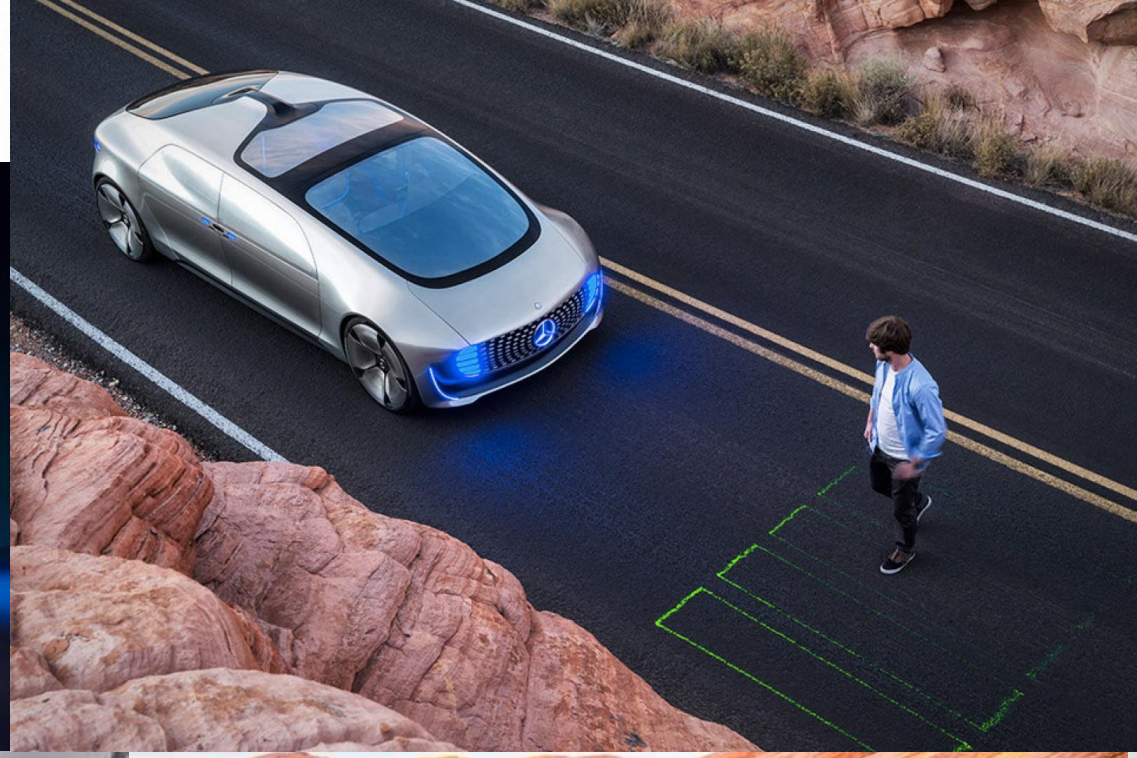
TRENDS FOR INTRODUCTION OF INNOVATION IN THE AUTOMOTIVE INDUSTRY



source:
www.strategyand.pwc.com

InnoSoc

Innovative ICT Solutions for the Societal Challenges

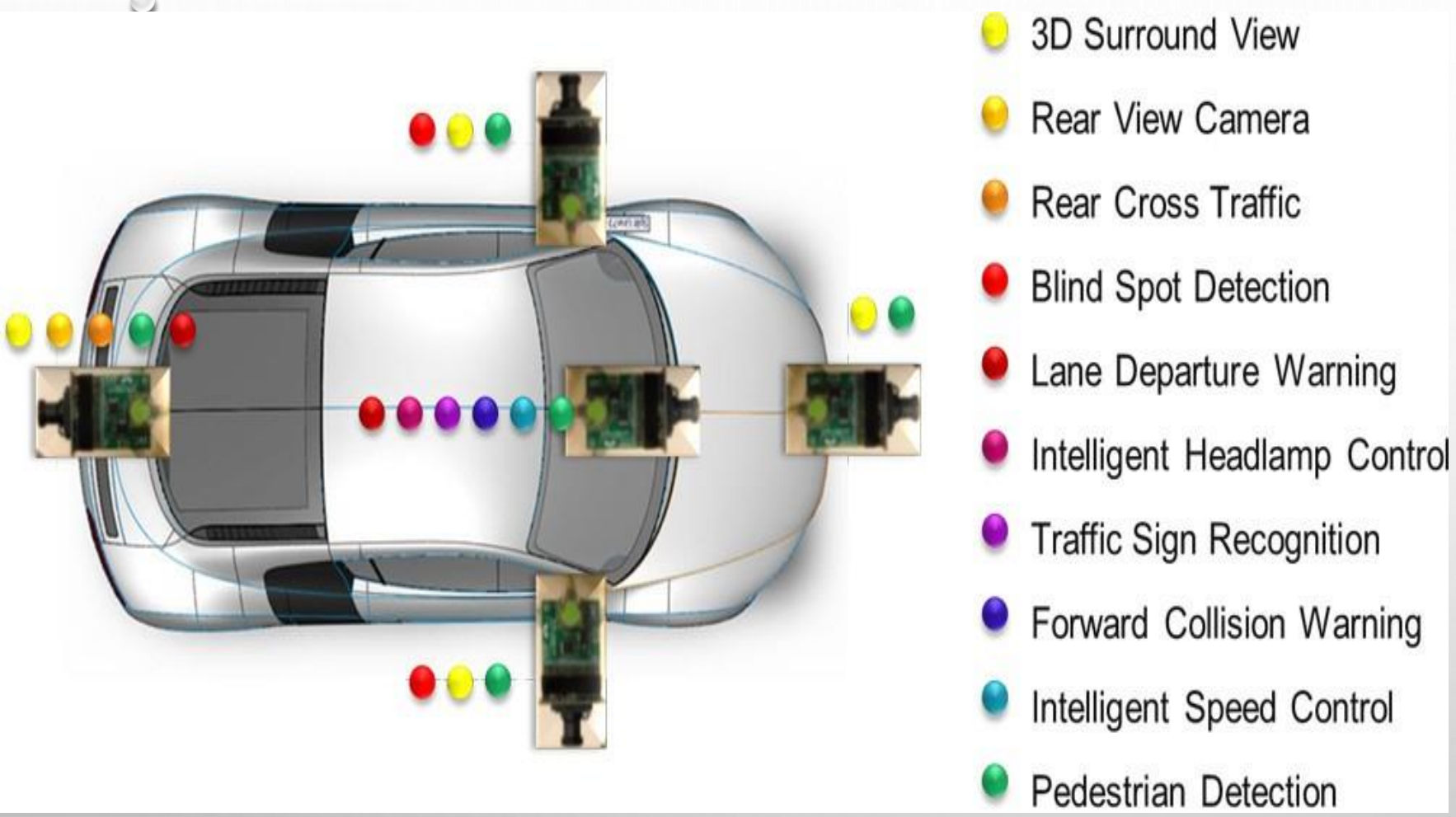


InnoSoc
Innovative ICT Solutions for the Societal Challenges

Audi A8

Tesla

INNOVATION



For **the connected automobile, innovative apps and wireless devices** are being made possible mostly thanks to wireless technology innovations like Wi--Fi, Bluetooth Smart, near field communications (NFC), and GPS. Combine that with breakthroughs in batteries that have allowed equipment to become smaller and less dependent power supply, and IoT technology is hurdling

CONCLUSION

- ✓Primary challenge in designing vehicular communication is to provide good delay performance under the constraints of vehicular speeds, high dynamic topology, and channel bandwidth;
- ✓ The cooperation between vehicular clouds and the Internet clouds in the context of vehicular management applications has become a critical challenge to researchers.
- ✓Avoiding accidents and minimizing resource usage are both important theoretical research challenges;

InnoSoc
Innovative ICT Solutions
for the Societal Challenges

REFERENCES

1. Wenshuang liang, zhuorong li, hongyang zhang, shenling wang, and rongfang bie, 2015, Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends, International Journal of Distributed Sensor Networks, Volume 2015, 11 pages.
2. Sai Kiran, Thirumala Rao, (2010), ReddyArchitectural Crises in Vehicular Ad-Hoc Networks, Global Journal of Computer Science and Technology Vol. 10 Issue 2 (Ver 1.0), 2010 P a g e 31
3. http://www.networkworld.com/article/2993888/security/six-key-challenges-loom-over-car-communication-technology.html
4. Leandros A. Maglaras , Ali H. Al-Bayatti, Ying He, Isabel Wagner and Helge Janicke, Social Internet of Vehicles for Smart Cities, J. Sens. Actuator Netw. 2016, 5(1), 3;
5. Kamran Zaidi and Muttukrishnan Rajarajan, Vehicular Internet: Security & Privacy Challenges and Opportunities, Future Internet 2015, 7(3), 257-275;
6. Ghassan Samara, Wafaa A.H., Al-Salihy, R. Sures, (2010), Security Analysis of Vehicular Ad Hoc Networks (VANET), Second International Conference on Network Applications, Protocols and Services, p.p.56-62
7. https://en.wikipedia.org/wiki/Internet_of_Things
8. Flavio Bonomi and others, The Smart and Connected Vehicle and the Internet of Things, http://tf.nist.gov/seminars/WSTS/PDFs/1-0_Cisco_FBonomi_ConnectedVehicles.pdf

InnoSoc

Innovative ICT Solutions for the Societal Challenges

THANK YOU !

InnoSoc

ZAGREB 2016