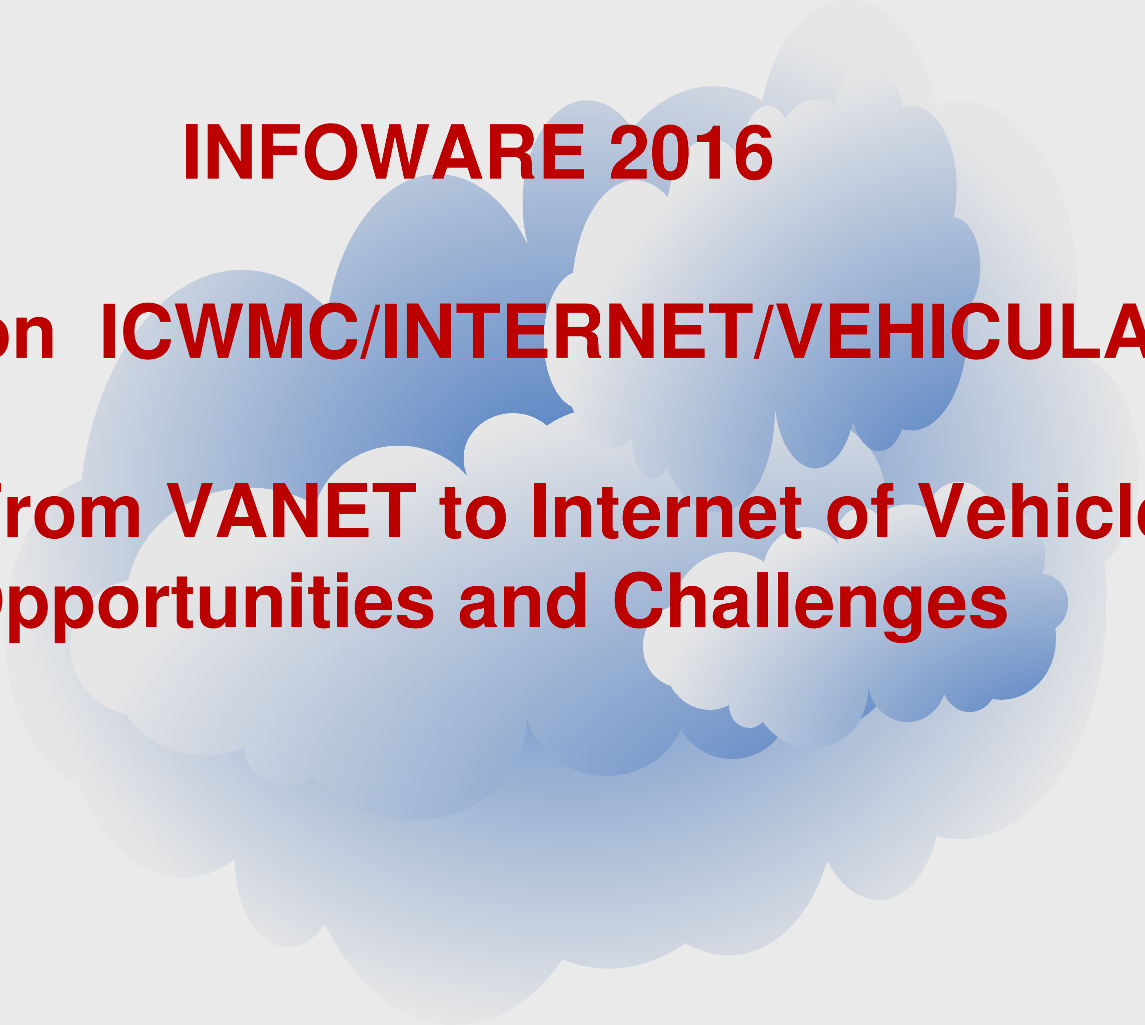
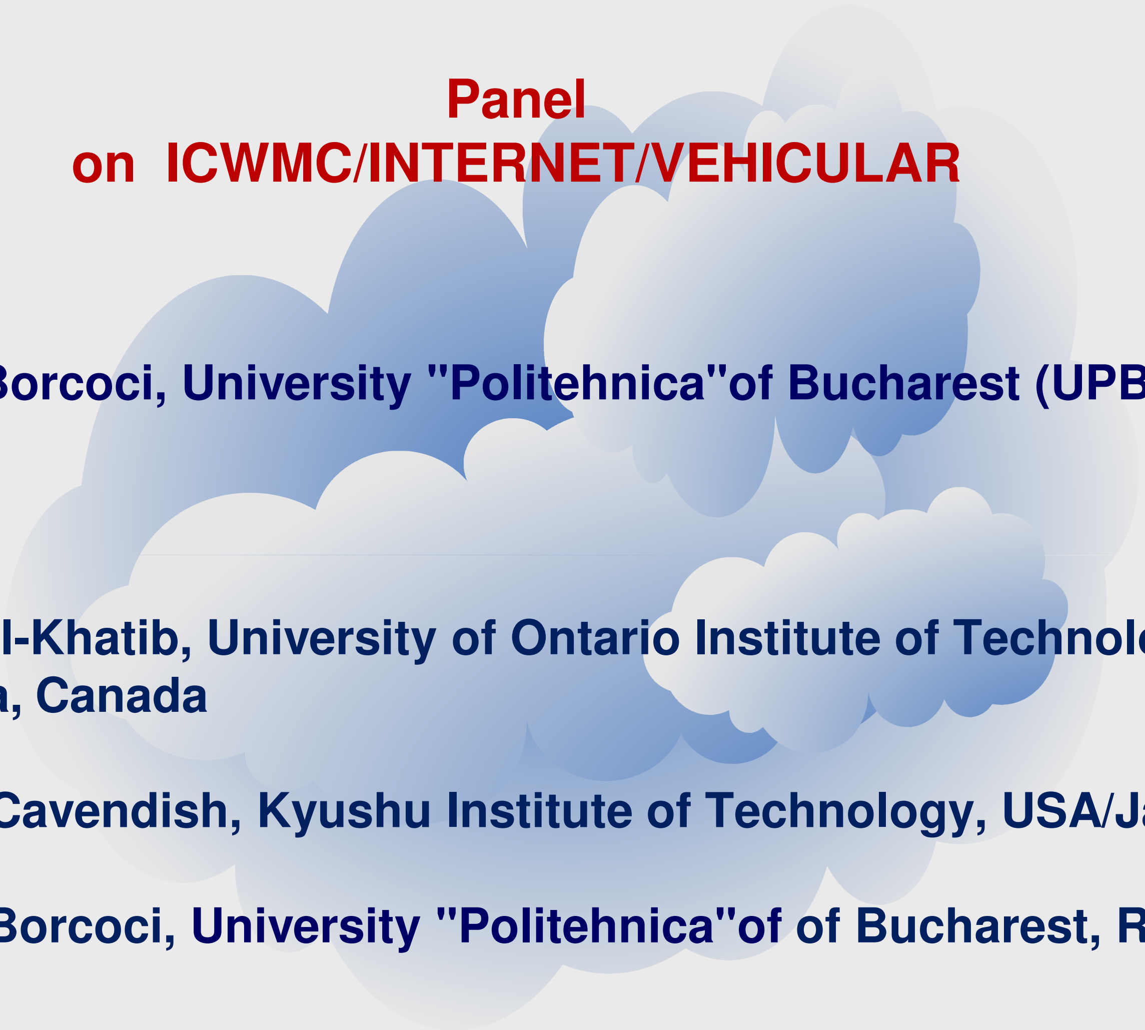
INFOWARE 2016

Panel on ICWMC/INTERNET/VEHICULAR

Topic: From VANET to Internet of Vehicles: Opportunities and Challenges



Panel
on ICWMC/INTERNET/VEHICULAR



Moderator

Eugen Borcoci, University "Politehnica"of Bucharest (UPB), Romania

Panelists

Khalil El-Khatib, University of Ontario Institute of Technology - Oshawa, Canada

Dirceu Cavendish, Kyushu Institute of Technology, USA/Japan

Eugen Borcoci, University "Politehnica"of of Bucharest, Romania

Panel on ICWMC/INTERNET/VEHICULAR

From VANET to Internet of Vehicles (IoV)

- Internet of Vehicles (IoV) evolves as a new theme of research and development from ITS and vehicular ad hoc networks (VANETs)
- **Why IoV ?**
  - Strong motivation for the real world to develop such technology
  - Not yet sufficient deployment comparative to the needs
  - IoV special class of Internet of Things- having specific requirements
  - Complex business models and large set of actors (users, providers, authorities, etc.)
  - IoV relationships with other topics and technologies
    - ITS, VANET
    - Future Internet, IoT, Smart cities
    - Mobile technologies, WiFi, 4G, 5G
    - Cloud computing, Fog computing
    - Security and Privacy -related specific technologies
    - Social networks, User-centric services
    - Safety related systems
    - …..

From VANET to Internet of Vehicles (IoV)

- **(IoV) includes different types of communications:**
  - vehicle-to-
    - vehicle (V2V)
    - roadside (V2R)
    - infrastructure of cellular networks and Internet (V2I)
    - personal devices (human) (V2D/V2P)
    - sensors (V2S)
- **Technical still open issues and challenges are related to :**
  - Models/business models
  - security and privacy
  - relevant use cases identifications and requirements
  - relationships with other technologies
  - architecture, protocol stack
  - network model
  - scalability, etc.

Panel on ICWMC/INTERNET/VEHICULAR

- **Possible (main) topics for this panel:**
  - *What are the most important opportunities for IoV in the context of IoT/Smart cities*
  - *Which are the drivers , challenges and obstacles to be solved in order to prepare a large scale deployment?*
  - *What candidates exist as support tehnologies ?*
  - *……*

Panel on ICWMC/INTERNET/VEHICULAR

- **Short presentations:**
- **Khalil El-Khatib**
  - **Connected Vehicles: Unlocking the Power of IoT**
- **Dirceu Cavendish**
  - **Vehicular Security and Autonomous Driving**
- **Eugen Borcoci**
  - **IoV – Challenges and General Architectural Solutions**
- **Thanks !**
- **Floor for the speakers…..**

Panel on ICWMC/INTERNET/VEHICULAR

Topic: From VANET to Internet of Vehicles: Opportunities and Challenges

IoV – Challenges and General Architectural Solutions

Eugen Borcoci
University Politehnica Bucharest
Electronics, Telecommunications and Information Technology Faculty (ETTI)
Eugen.Borcoci@elcom.pub.ro

InfoWare 2016 Conference, November 13-17, Barcelona

IoV challenges and general architectural solutions

- The traditional **Intelligent Transport System (ITS)** has evolved towards vehicular communication
  - Main communications: V2V and V2R → VANET

- **VANET – has many limitations; still not a large scale deployment**

- **Recent approach: IoV**
  - **global network of vehicles – enabled with Wireless Access Technologies (WAT) ,involving Internet and other heterogeneous networks**
  - **IoV – special case of IoT**

  - **IoV Target domains:**
    - vehicles driving (classic – in VANET) +
    - urban traffic management, automobile production,
    - repair and vehicle insurance, road infrastructure construction and repair, logistics and transportation, …

IoV challenges and general architectural solutions

- **Comparison VANET/IoV**
  The IoV advanced features can be considered as well as challenges
- ***Commercial , objectives, architecture***
  - **VANET**: architecture supports only specific apps (safety, traffic efficiency) and Internet is not available (due to specific architecture)
  - **IoV:** high opportunities for various apps (safety, traffic optimization and efficiency, infotainment apps, ..) due to IoV-business oriented architecture
- ***Collaboration capabilities:***
  - **VANET**: specific architecture, non-collaborative, no Internet collaboration
  - **IoV:** collaboration between heterogeneous nets, reliable Internet service
- ***Communication types:***
  - **VANET**: V2V, V2R
  - **IoV:** V2V, V2R, V2I, V2P, V2S
- ***Processing power and decision capabilities:***
  - **VANET**: limited (local simple decisions), low volume data
  - **IoV:** high – (cloud based), big data, data mining, ..

IoV challenges and general architectural solutions

- **Comparison VANET/IoV (cont'd)**

- ***Compatibility with personal devices***: VANET: limited; IoV : any PD
- ***Scalability:***
  - **VANET**: non-scalable (consequence of its architecture)
  - **IoV:** scalable (integration of VANET, WiFi, 4G/LTE, ..)

- ***Connectivity:***
  - **VANET:** vehicles can be connected/disconnected- depending on network availability
  - **IoV:** always , one can use the best network type

- ***Network/environment awareness:***
  - **VANET:** limited (neighborhood of the vehicle)
  - **IoV:** global network awareness is possible (cloud-assisted)

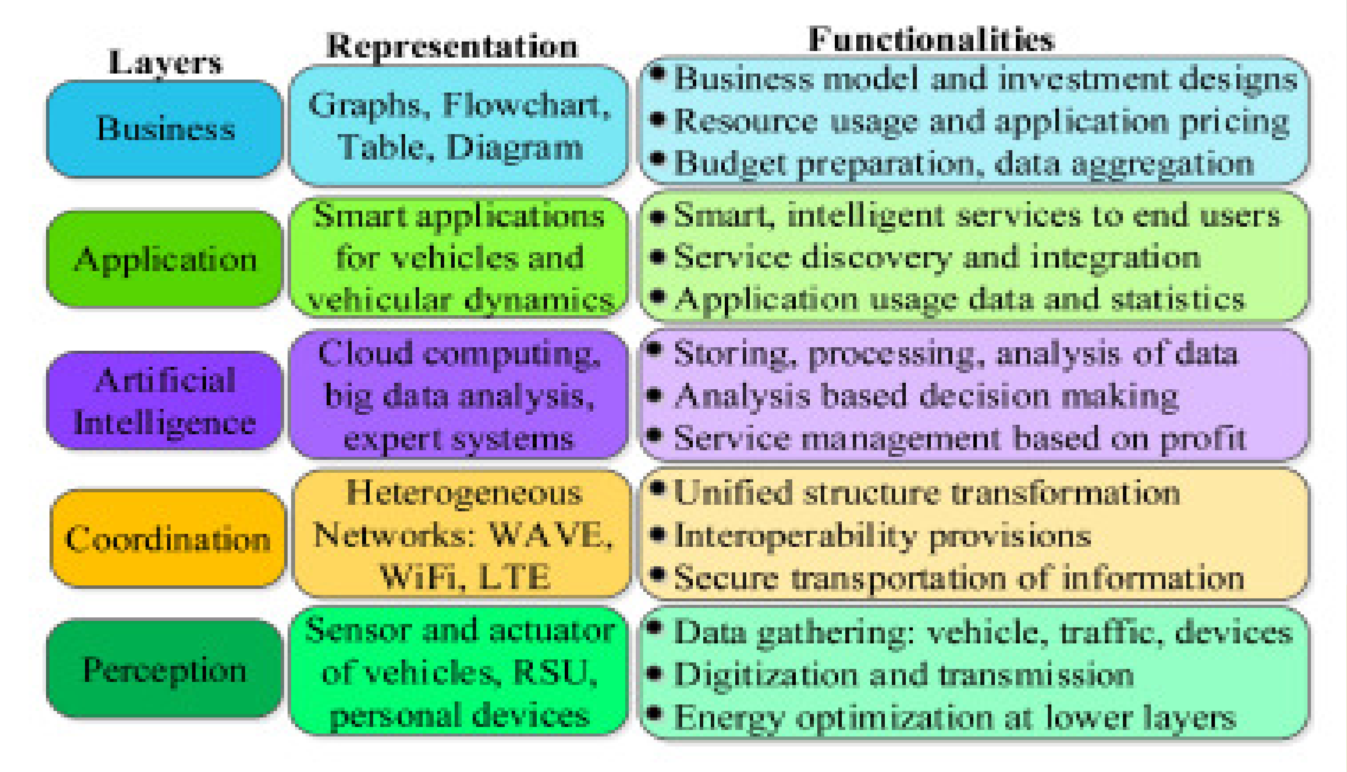
- ***Cloud Computing (CC) compatibility***:
  - **VANET**: limited (possible, but currently not supported)
  - **IoV**: main operations can be based on CC

IoV challenges and general architectural solutions

- **Examples of IoV specific technical challenges**
  - **Localization accuracy**
    - Should be better than for GPS, solve the GPS temporary unavailability
    - ~5m (GPS) → ~50 cm (IoV)
  - **Localization privacy**
    - Some methods like: Pseudonym switching, silent period, mix zone- not yet fully solved problems
  - **Location verification of neighboring vehicle**
    - Issues: cost of infrastructure – if directional antennas are used; overload of the beaconing approach; un-thrusty neighbour in cooperative approach
  - **Radio propagation problems and related models**
    - LOS, NLOS issues
  - **Operational and management – related problems**
    - Collaborative work issues
    - Computational complexities (tasks splitting among the entities of the network model)
    - Disruption reduction - need
    - …

IoV challenges and general architectural solutions

- **IoV generic, layered architecture**
  - 3 architectural planes: operation, management, security plane
  - The generic layers are mapped to the actual architectural protocol stack:



Layers	Representation	Functionalities
Business	Graphs, Flowchart, Table, Diagram	• Business model and investment designs • Resource usage and application pricing • Budget preparation, data aggregation
Application	Smart applications for vehicles and vehicular dynamics	• Smart, intelligent services to end users • Service discovery and integration • Application usage data and statistics
Artificial Intelligence	Cloud computing, big data analysis, expert systems	• Storing, processing, analysis of data • Analysis based decision making • Service management based on profit
Coordination	Heterogeneous Networks: WAVE, WiFi, LTE	• Unified structure transformation • Interoperability provisions • Secure transportation of information
Perception	Sensor and actuator of vehicles, RSU, personal devices	• Data gathering: vehicle, traffic, devices • Digitization and transmission • Energy optimization at lower layers

Source: O. Kaiwarta, A.H Abdullah, Y.Cao, et. al., "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects" IEEE Access, SPECIAL SECTION ON FUTURE NETWORKS: ARCHITECTURES, PROTOCOLS, AND APPLICATIONS, September 2016

IoV challenges and general architectural solutions

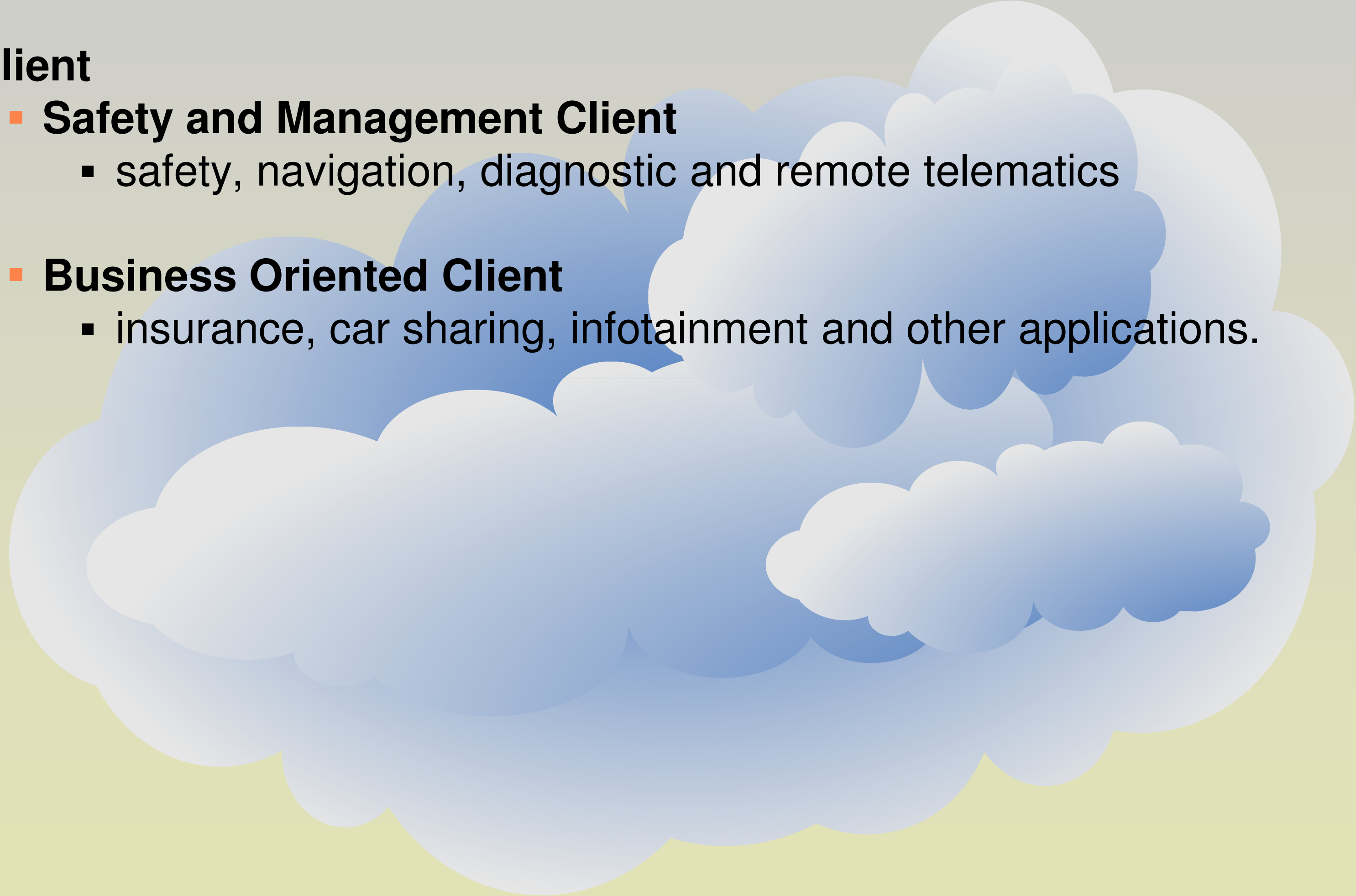
- **IoV proposed [1] network model : Cloud + connection + clients**
- **Cloud:**
  - basic CC services
  - Smart ITS applications
  - Information consumer and producer
- **Connection**
  - Two major components of a connection:
    - **Third Party Network Inter Operator (TPNIO)** -management of the connection
    - **Gateway of Internetworking (GIN).** - represents the connection itself
  - **TPNIO**
    - Components : Global Handoff Manager (GHM), Global Authentication, Authorization and Billing (GAAB), Service Management (SM), Network Database (NDB) and Operator Database (ODB).
  - **GIN**
    - Mobility Management (MM)
    - Local Authentication Authorization and Billing (LAAB)
    - Traffic Management (TM)

IoV challenges and general architectural solutions

- **IoV proposed [1] network model : Cloud + connection + clients (cont’d)**

- **Client**
  - **Safety and Management Client**
    - safety, navigation, diagnostic and remote telematics

  - **Business Oriented Client**
    - insurance, car sharing, infotainment and other applications.



IoV challenges and general architectural solutions

Conclusions

- IoV- powerful development in the IoT framework, following ITS, VANET
- IoV has many promises but also these constitute, as well, challenges:
  - Commercial, objectives, architecture
  - Collaboration capabilities
  - Communication types
  - Security and privacy
  - Processing power and decision capabilities:
  - Compatibility with personal devices
  - Scalability:
  - Connectivity aspects
  - Network/environment awareness
  - Cloud Computing (CC) compatibility
- Layered architecture: based on current developments in ITS, WAVE, VANET
  - More open architecture than in VANET
  - Full Internet connectivity
  - Collaboration possibility among hetero access technologies

IoV challenges and general architectural solutions

- Thank you !

IoV challenges and general architectural solutions

- **References**

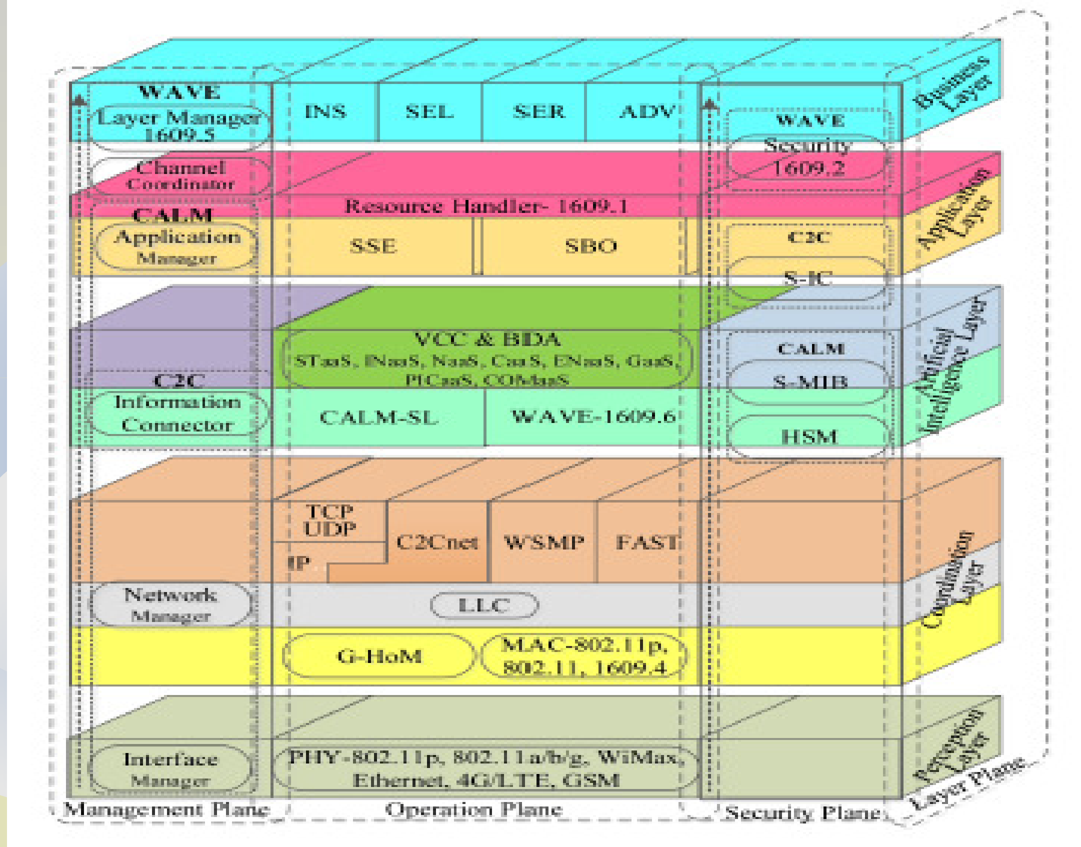
1. O. Kaiwarta, A.H Abdullah, Y.Cao, et. al., “Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects” IEEE Access, SPECIAL SECTION ON FUTURE NETWORKS: ARCHITECTURES, PROTOCOLS, AND APPLICATIONS, September 2016.
2. Y. Fangchun, W. Shangguang, L. Jinglin, L. Zhihan, and S. Qibo, ``An overview of Internet of Vehicles,'' *China Commun., vol. 11, no. 10,* pp. 115, October 2014.
3. M. Saini, A. Alelaiwi, and E. Saddik, ``How close are we to realizing a pragmatic VANET solution? A meta-survey,'' *ACM Comput. Surv.,* vol. 48, no. 2, 2015, Art. no. 29.

IoV challenges and general architectural solutions

- **Backup slides**

IoV challenges and general architectural solutions

- IoV : example of a layered protocol stack

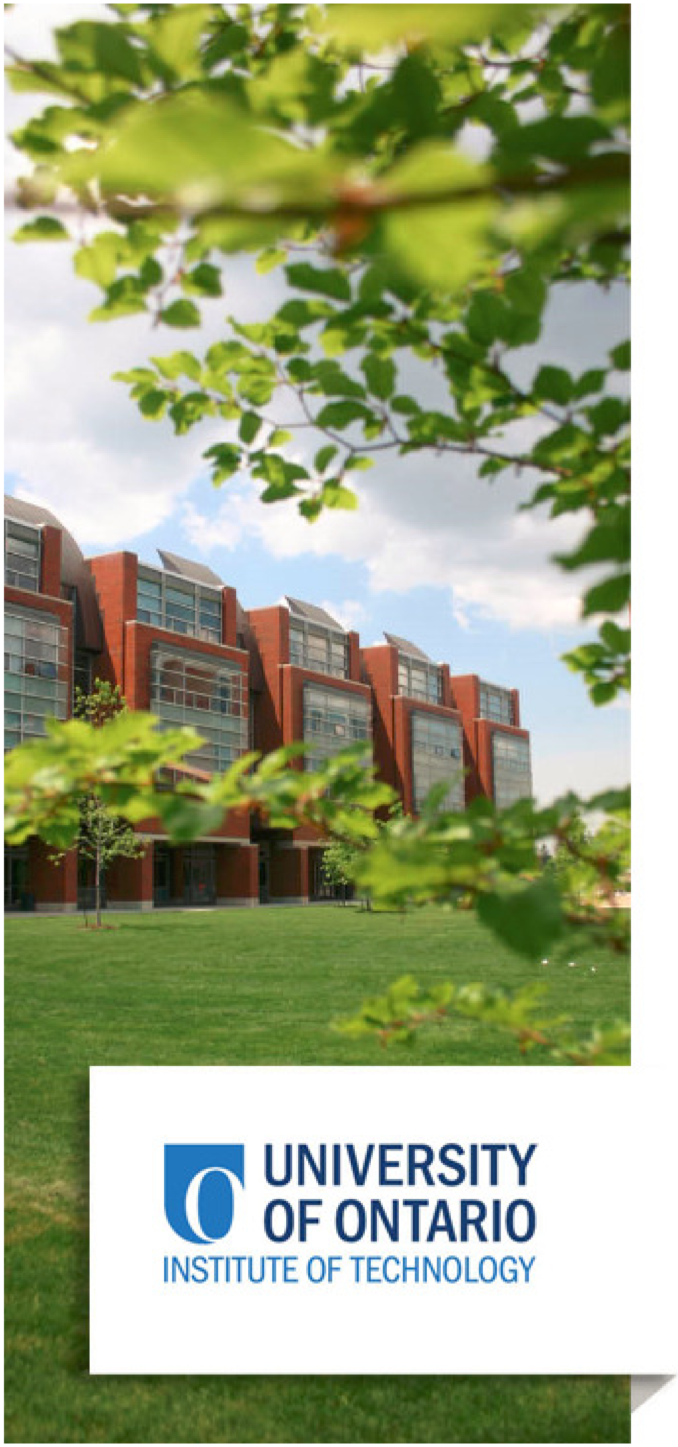


Source: O. Kaiwarta, A.H Abdullah, Y.Cao, et. al., "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects" IEEE Access, SPECIAL SECTION ON FUTURE NETWORKS: ARCHITECTURES, PROTOCOLS, AND APPLICATIONS, September 2016

IoV challenges and general architectural solutions

- List of Acronyms

CALM	-Continuous Air interface for Long and Medium distance
DSRC	-Dedicated Short Range Communication
GPS	-Global Positioning System
GIN	-Gateway of Internetworking
ITS	-Intelligent Transportation System
LLC	-Logical Link Control
OBU	-On Board Unit
RSU	-Road Side Unit
SM	-Service Management
TPNIO	-Third Party Network Inter Operator
VANET	- Vehicle Ad-hoc Networks
V2V	- Vehicle to Vehicle
V2R	- Vehicle to Roadside
V2I	- Vehicle to Infrastructure of cellular networks and Internet
V2D/V2P	- Vehicle to Personal devices (human)
V2S	- Vehicle to Sensors
V2X	- Vehicle-to-everything
WAVE	- Wireless Access for Vehicular Environments



UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

Connected Vehicles: Unlocking the Power of IoT

Khalil El-Khatib

Faculty of Business and IT

Thursday Nov 17, 2016

IoT and Vehicles: Where Did it Start?

- Long way from the original vehicle
- 20 years ago, data was one way into the car
  - Global navigation satellite systems
  - Traffic information over the radio
  - Bluetooth connectivity mostly to feed data to the car
- Internet of Things (IoT) is about adding computing and communication power to real-life physical objects

IoT and Vehicles: Where is it Now?

- Modern cars
  - More than 50 networked computers:
    - Average new car has 40 to 50 computers that run 20 million lines of software code, more than a Boeing 787,
  - Networks on wheels

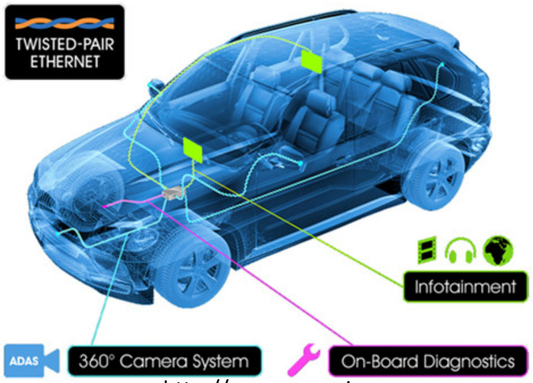
IoT and Vehicles: Where is it Now?

- Basic data is coming out of the car:
  - Vehicles making calls in case of crash
    - eCall system, GM OnStar
  - Vehicles are talking to each other and to the infrastructure
    - Intelligent Transport Systems: V2V, V2R
  - Vehicles revealing information about their components, the driver, and their surrounding
- Gartner predicted that, by 2020, there will be 250 millions connected on the road

Enabling Large Data Collection

- Ethernet in the car: OABR (OPEN Alliance 100Mbps BroadR-Reach®)
  - Multiple Ethernet switches connecting all ECU
  - From multiple ECU to a single Vehicle data center with virtualized ECU
- Vehicles more connected to the internet

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY



http://www.opensig.org

What to Expect?

- Unlock the power of data gathered by the car.
- Help drivers with maintenance, diagnosis, repair, …
- Provide driver with alert
- Provide feedback on driving patterns
- Incorporate social network aspects
- Connect with insurance
- M2M (payment at the meter)
- Real-time traffic alerts
- Assisted driving
- Autonomous cars
- Integration with home networks.

IoT and Vehicles

- Vehicles will be an integrated component in the Internet of Things (IoT).

(Automotive 2025: Industry without borders (IBM Institute for Business Value))

  - Self healing
  - Self socializing
  - Self driving
  - Self integrating
  - Self configuring
  - Self learning

Things to Watch for

- Security: another 9/11 by cars.
- Infringement upon civil liberties.
- Fading barriers between IT and vehicles.

Internet 2016 Panel

Vehicular Security and Autonomous Driving

Dirceu Cavendish, Kyushu Institute of Technology, Japan

Network Design Research Center

Vehicular Communication Today

Our vehicles are about to undergo significant changes

Intra-communication

- CAN bus
- Infotainment system

Inter-communication

- Key fob system
- Mobile to vehicle apps

What lies ahead

- Vehicle to server systems
- Vehicle to vehicle communication

Vehicular Communication & Security

2016 vehicular security events

- ■ Nissan remote AC system
- ■ Tesla control highjack

A remote vulnerability for Tesla's Model S has been demonstrated by researchers from Keen Security Lab, a division of the Chinese internet giant Tencent. The vulnerability was confirmed by Tesla's product security team and has already been patched via an over-the-air software update, as Keen worked with Tesla to fix the flaw before going public.

The vulnerability compromises the CAN bus that controls many vehicle system in the car. It requires the car to be connected to a malicious wifi hotspot to take control and works via the in-car web browser. It's an admittedly narrow set of circumstances required to compromise the car, but would present a clear opportunity for a determined attacker to cause significant harm.

In a video demonstration, a researcher uses the car's mapping search function to find the nearest charging point. At that point, the researchers take over both the infotainment and instrument cluster screens and remotely unlock the doors. They were also able to open the trunk, fold a side mirror, and activate the brakes while the vehicle was in motion. Researchers were also able to remotely open the sunroof, move the power seats, and activate the signal lamps.

http://www.theverge.com/2016/9/19/12985120/tesla-model-s-hack-vulnerability-keen-labs

Drivers of Nissan Leaf cars were warned their electric cars could be remotely accessed by hackers via the internet to control some of its systems.
The flaw was discovered by Australian security researcher Troy Hunt and is focused on the Nissan Leaf's mobile app.
While the flaw won't allow hackers to take control of the car's driving systems or unlock doors, it can command the car to turn up the heating or air conditioning, running down the car's battery and leaving a driver stranded.
Hunt said in a blog post that using a web browser and knowledge of the target vehicle's identification number (VIN), it was possible to take control.

https://internetofbusiness.com/nissan-leaf-electric-cars-vulnerable-to-cyber-attacks/ - Feb 2016

Network Design Research Center

Vehicular OS & Security

Vehicular Operating System

- Integrates Infotainment system with car controls (CAN bus)
- Evolution towards Autonomous Driving Assisted System (ADAS)

Initiatives

■ QNX (Blackberry): http://www.qnx.com/content/qnx/en/solutions/industries/automotive/index.html

■ Automotive linux: https://www.automotivelinux.org/

Your vehicle is your next “mobile computing platform”

Autonomous Driving

Autonomous driving levels

- Level 0: human – human total control

- Level 1: Semi-autonomous – most controls exercised by driver, with few time epoch auto-aids:
  - Break on proximity, blind spot warning signs.

- Level 2: auto functions engaged for a time period (engage/disengage):
  - Cruise control, lane centering, parking.
  - May require driver intervention

- Level 3: Engaged auto does not require instantaneous driver interference
  - Safety features guarantee safe engagement for long periods of time.

- Level 4: Fully autonomous – Full A to B trip autonomously engaged.
  - Roadway monitoring; Pavement condition sensoring;

Autonomous Driving & Threats

Threat types

- Vehicular sensoring
  - GPS: spoofing
  - Radar: Small dangerous objects
  - Camera: object occlusion; object distraction; non-standard road demarcation
  - Proximity: position/range attacks
- Autonomous Driving Aided System
  - Image processing pattern recognition failures (e.g. stop sign miss)
  - Auto driving logic failure: unexpected scenario; software error

Mitigations

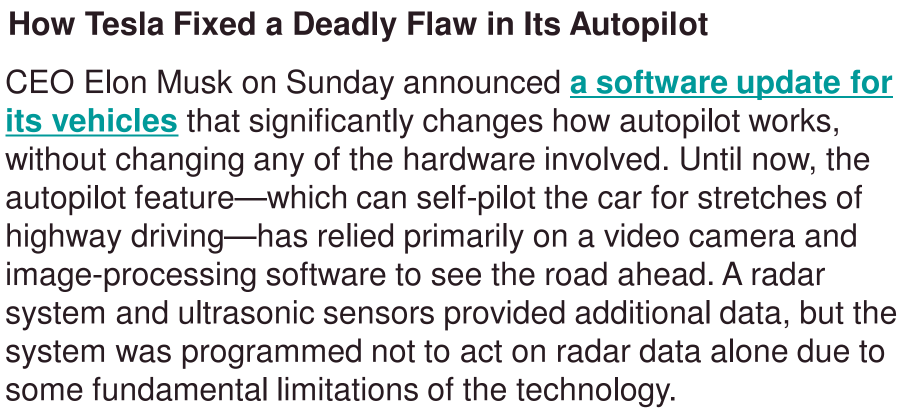
- Multiple sensor sources with consistency checks
- Multiple position camera sources and checks
- Secure communication protocols

- Emergency procedures: collision avoidance procedures
- Self-learning: crowdsourcing driving performance, near misses, and collision events;

Security and Crowdsourcing

Vehicle Crowdsourcing

- Safety: unpredictable situations; failures
  - ADAS algorithm design and tuning
- Performance: Accuracy verification and performance improvements
- Insurance
  - Risk assessment
  - Crash forensics



How Tesla Fixed a Deadly Flaw in Its Autopilot

CEO Elon Musk on Sunday announced **a software update for its vehicles** that significantly changes how autopilot works, without changing any of the hardware involved. Until now, the autopilot feature—which can self-pilot the car for stretches of highway driving—has relied primarily on a video camera and image-processing software to see the road ahead. A radar system and ultrasonic sensors provided additional data, but the system was programmed not to act on radar data alone due to some fundamental limitations of the technology.

http://www.slate.com/articles/technology/future_tense/2016/09/how_tesla_s_software_update_fixed_a_deadly_flaw_in_autopilot.html - Sept 2016

INFOWARE 2016

Panel on ICWMC/INTERNET/VEHICULAR

Topic: From VANET to Internet of Vehicles: Opportunities and Challenges

Conclusions

Panel
on ICWMC/INTERNET/VEHICULAR

Moderator

Eugen Borcoci, University "Politehnica"of Bucharest (UPB), Romania

Panelists

Khalil El-Khatib, University of Ontario Institute of Technology - Oshawa, Canada

Dirceu Cavendish, Kyushu Institute of Technology, USA/Japan

Eugen Borcoci, University "Politehnica"of of Bucharest, Romania

From VANET to Internet of Vehicles: Opportunities and Challenges

Conclusions

- **Internet of Vehicles (IoV)** – novel, rich set services in comparison with ITS, VANET
  - **Expected opportunities/services**
    - Help drivers: alert, feedback on driving patterns, assisted driving, maintenance, diagnosis, repair, …
    - Autonomous cars
    - Integration with Internet, home networks and other IoT systems
    - Incorporate social network aspects
    - M2M services,
    - Real-time traffic alerts
    - ….
- **Integration in IoT needs** : Self - healing, -socializing, -driving, -integrating, - configuring, - learning

From VANET to Internet of Vehicles: Opportunities and Challenges

Conclusions (cont'd)

- **Autonomous driving** – important set of services
  - Autonomous driving levels- require specific approach
  - Critical aspects
    - Autonomous Driving & Threats
    - Security and Crowdsourcing

- **IoV challenges related to:** architecture, collaboration capabilities, communication types, security and privacy, decision capabilities, compatibility with personal devices, scalability, connectivity issues, network/environment awareness, cloud computing compatibility

- **Architecture**:
  - multiple plane: operation, management, security (re-using ITS, WAVE, etc. technologies + novel ones)
  - network model : Cloud + connection + clients

From VANET to Internet of Vehicles: Opportunities and Challenges

- **THANKS!**