Internet of Vehicles

Your next connection

The Internet of Vehicles (IoV) is an inevitable convergence of the mobile Internet and the Internet of Things. It’s comprised of all new and current vehicles, either fitted or integrated with two-way RF equipment. It is a converged technology that encompasses information communication, environmental protection, energy conservation, and safety. To succeed in this emerging market, acquisition of core technologies and standards will be crucial to securing strategic advantage.

By Dr. Liu Nanjie (Nanjing University of Posts & Telecommunications)

Concept of IoV

Although the IoV is an emerging concept, some nascent forms exist today. Intelligent Transport Systems (ITS) in Europe and Japan have adopted certain forms of IoV technology. In New Delhi, all 55,000 licensed rickshaws have been fitted with GPS devices so that drivers can be held accountable for their questionable route selection. China’s Ministry of Transport (MOT) has ordered that GPS systems be installed and connected on all long-haul buses and hazmat vehicles by the end of 2011 to ensure good driving habits and reduce the risk for accidents and traffic jams. The Brazilian government has set a goal for all cars in circulation to be fitted with electronic ID chips from its National Automated Vehicle Identification System (Siniav).

The launch of the U.S. National Strategy for Trusted Identities in Cyberspace (NSTIC) is a milestone for IoV. It requires that “security chips” be embedded in all online devices, including those in vehicles. Clearly, the IoV is no longer a matter of IT applications in the automotive industry; instead, it has become a national security concern.

What is the IoV?

IoV technology refers to dynamic mobile communication systems that communicate between vehicles and public networks using V2V (vehicle-to-vehicle), V2R (vehicle-to-road), V2H (vehicle-to-human) and V2S (vehicle-to-sensor) interactions. It enables information sharing and the gathering of information on vehicles, roads and their surrounds. Moreover, it features the processing, computing, sharing and secure release of information onto information platforms. Based on this data, the system can effectively guide and supervise vehicles, and provide abundant multimedia and mobile Internet application services.

Viewed from the network perspective, an IoV system is a three-level “Client-Connection-Cloud” system.

Client system – The client system is a vehicle’s intelligent sensor, which gathers vehicular intelligence and detects driving status and environment. It is a ubiquitous communications terminal that features intra-vehicle, inter-vehicle, and vehicle-network communication. It is also a device that enables IoV addressing and attainment of a trusted vehicular identity in cyberspace.

Connection system – This layer addresses V2V, V2R, V2H and V2I (vehicle-to-Internet) interconnectivity to realize communication and roaming between ad-hoc vehicular networks (VANETs) and other heterogeneous networks. It ensures real-time network ubiquity in terms of functionality and performance. It is also a merging of public and private networking.

Cloud system – The IoV is a cloud-based vehicle
operation information platform. Its ecosystem covers ITS, logistics, cargo/passenger transport, hazmat transport, vehicle repair/fitting, vehicle manufacturing, vehicle dealership, vehicle supervision, insurance, emergency rescue, and mobile Internet, making it a nexus for a variety of copious data sources. Cloud-based functions such as virtualization, authentication, real-time interaction, and mass storage are therefore required. Its application systems also integrate vehicle data gathering, computing, scheduling, monitoring/control, management, and applications.

It is noteworthy that the current GPS+GPRS system is neither true IoV nor IoT; it is only a combined application of existing technologies. Nonetheless, many ITS tests are being implemented based on this technology. It would be unfavorable for any country's strategic priorities and technical innovations if IoV development is based simply on this technology.

**What is GID?**

A vehicular global ID (GID) terminal is at the core of the IoV. It is a communications gateway and integrated or mounted terminal with global ubiquitous network connectivity. It is also an intelligent in-vehicle sensor with global positioning and global online identification (online license plate) functionality. A GID integrates a vehicle’s smart information sensor, networking, and online license plate, as shown in Fig. 1.

**Vehicular status perception** – The GID features various embedded sensors and connects with a vehicular bus, such as onboard diagnostics (OBD) or the controller–area network (CAN), enabling it to perceive and monitor almost all static and dynamic vehicular information, including environmental and status-diagnosis information.

**Ubiquitous communication** – The GID features V2V, V2I, and ad-hoc network communications; intra-vehicle networking; inter-format bridging and relay; and global communication/positioning/roaming capabilities.

**Online license plate** – The GID determines the status of vehicles, networks and users to generate an “online ID” for a vehicle, which is a trusted ID in cyberspace rather than a mere tag.

Simply put, the GID addresses problems with traditional radio frequency identification (RFID) that include its one-way nature, limited range & coverage, lack of speed, passive and unintelligent operation, lack of perception and communication, high cost, lack of standardization, and its ease of loss or damage. The GID also features the V2V, V2I, and global roaming/coverage required for the IoV, making it more than a mere telematics instrument. More importantly, GID provides vehicles with “cyber license plates” or “cyber IDs,” thereby solving the most difficult problem with IoT – the fact that an address cannot be separated from its network ID. GID brings greater online visibility by uniquely distinguishing all vehicles worldwide. In addition, by working with the back-end cloud system, GID submits vehicle and driving status, and even in-vehicle black-box information, at any time.

Dynamic, multi-source data obtained from the GID can be utilized for IoV, machine movement, ITS, and cloud computing.
With GID capabilities, the IoV need no longer rely solely on static, external information sources. Sources can now be more diverse and far-reaching, but this will require major changes to ITS technologies.

**Fig. 1 GID vs. RFID**

Vehicle and traffic status information can be gathered from the CAN bus and other sources; such information covers driving (location, direction, speed, and acceleration), status (inside and outside temperature, air flow, and tire pressure), power (fuel pressure, rotational speed, and oil level), vehicle safety (seatbelt, airbag, and door/window lock status), and environment (weather, road conditions, and congestion levels).

**GID-based IoV system**

**Mutual IoV & ITS development**

IoV development has everything to do with ITS, automotive electronics, and mobile Internet access. Next-gen ITS development requires the overcoming of challenges such as comprehensive traffic status information access, timely detection of road conditions and vehicle operating status, and intelligent release of information based on relevant factors such as vehicle/road conditions, thereby providing travelers with more effective traffic information; this makes transportation more eco-friendly and efficient.

ITS depends on the road and the vehicle equally. Traditional ITS solutions involve static and fixed road-related elements such as roadside units (RSUs), video shooting, roadside displays, RFID readers, traffic condition displays, and pressure-sensitive coils, but overlook the fact that vehicles themselves are the most relevant factors that affect traffic conditions, accidents and the roadside environment.

The advent of GID-based IoV represents the evolution and advancement of traditional M2M and telematics. With GID capabilities, the IoV need no longer rely solely on static, external information sources. Sources can now be more diverse and far-reaching, but this will require major changes to ITS technologies.

**Relationships between IoV and cloud computing**

The IoV will eventually generate much more information than the telecom industry. Take the ITS for example; the
entire smart process of gathering, processing, and releasing dynamic traffic information from various sources across a city will require a petabyte-scale \((10^{15})\) information processing system. Cloud computing would seem suitable for handling data of this magnitude. In a cloud framework, systems for comprehensive information gathering and processing, road traffic status monitoring, vehicle regulation and guidance, signal control, system interlocking, prediction or information release must be integrated with the entire smart system. Information is shared among these systems so that unified decisions are made. Cloud services related to the IoV and ITS fall into the following three categories as shown in Fig. 2.

**Platform as a Service (PaaS)** — Includes bulk GPS data and GID data processing, ITS holographic data processing, cloud storage, information mining and analysis, information security, and data buses.

**Software as a Service (SaaS)** — Through basic cloud services and third-party service resources, any developer may create certain applications that support IoV and ITS from various terminals (PC browsers and mobile phones).

**Opportunities and challenges**

The IoV combines Internet, IoT, communication, automotive production, automotive after-sales service, ITS, automotive insurance, traffic control, LBS and mobile Internet elements. It will bring about fundamental changes to ITS, urban congestion management, transport & logistics, urban traffic, public facility construction, telecom operations, terminal manufacturing, and our collective lifestyle. However, it remains difficult to unify...
the concept and scope of IoV from different perspectives. As a result, top-level design for the IoV must be done from a nationwide perspective.

Issues yet to be resolved

**Converged V2V and V2I communication** – V2V and V2I represent two systems within a single vehicle. Few vehicles have V2V capabilities, while V2I is used to a limited extent on ordinary public networks and does not guarantee real-time data; 802.11p is also not entirely capable of bridging and converging V2V and V2I.

**Open CAN buses** – CAN protocols vary with vehicle make and model, which constitutes a huge obstacle to IoV establishment.

**Precise vehicle positioning** – Assisted GPS (AGPS) cannot fully satisfy vehicle positioning requirements for IoV; it is also insecure and does not carry the weight of law. A more precise and regulated navigation system is needed.

**IoV standards** – Various institutions, bureaus, branches of the military, and enterprises have their own respective understandings of the IoV; but which, if any, will become dominant? Rules and standards will involve compromise, but someone will have to go first. National security will have to be balanced with innovation and standardization.

In addition, the GID encompasses in-vehicle device functions required for the IoV, but standards need to be unified for GID-cloud and cloud-terminal communication protocols as soon as possible. Communication ubiquity must also be established for all relevant network elements, if the IoV is to work at all.

**IoV operation** – The IoV entails an extremely large amount of data, beyond the limits of ordinary platforms. To ensure security and credibility, the IoV must be on a ‘real-name’ basis. Each vehicle will carry a number of mobile terminals, persons, and devices. It will have multiple attributes and be multihoming. As a result, IoV operators will be neither traditional telecom operators nor mobile Internet SPs, automakers, or auto dealerships. There are obvious needs for virtual operation.

There are also a large number of technical difficulties and obstacles to cloud platform opening and interface, as well as network visualization, positioning and computation, timely retrieval, and data mining & analysis. A plethora of new problems will also emerge as the industry deepens.

Bright future for IoV

As a special form of communication that combines industrial and IT applications, the IoV will be the next focus for telecom and Internet transformation. It is an emerging field for the automotive industry, where IoV development is second only to “going green” in priority; this presents many opportunities.

First, online vehicle status check, annual inspection, and monitoring will come to pass, if they do not already. It will be possible to remotely determine a vehicle’s operational legality, regulatory compliance, and license status of the driver, which will reduce vehicle management costs, change industries, and save lives.

Secondly, vehicles will have IDs in cyberspace. This will amount to an online presence on a quasi-real-name basis, which will no doubt make the operation of falsely registered, smuggled, and illegally modified vehicles much more difficult. It will also enable easy bundling with mobile payment and driver & passenger information records, thereby increasing overall security and creditability in cyberspace and the physical world as well. Cyber license plates and black boxes alone will spawn entire industries.

Thirdly, the IoV will supplement the RFID+GPS system to create a fully-encompassing ecosystem. As mentioned above, the GID is a new type of in-vehicle terminal that features processors, sensors, communicators, security IDs, memory, and wireless bridges. It has greatly expanded the capacity of the RFID/GPS industries and changed the

---

Perspectives

IoV will be the next focus for telecom and Internet transformation. It is also an emerging field for the automotive industry, where IoV development is second only to “going green” in priority; this presents many opportunities.
A large number of smart terminals will emerge tailored to the IoV, both in-vehicle and handset. With these terminals in hand, the IoV will be integral to the mobile world.

foothold of current ITS and IoV terminals. It enables real-time information release and intelligent route navigation by mobile terminals when used together with the existing ITS; it will doubtlessly influence the entire ITS landscape.

The IoV also enables new mobile Internet and LBS (location-based service) applications. It introduces numerous physical items into cyberspace, while avoiding identity infringement issues, thereby assuring unique mapping between the virtual and physical worlds. It will cause a sharp increase in the number of mobile Internet customers and create new gold mines in online privacy protection and trusted ID services.

The IoV will generate robust data services. It enables multi-level [such as R2I (road-to-Internet), R2V (road-to-vehicle), V2H and V2I] data storage and query, as well as six-degree association with industry chains relevant to vehicles, thereby interconnecting all aspects of human life. Mass data storage, processing, distribution, applications, e-commerce and digital transactions will all require a physical platform for completion. Said platform will be much larger than existing communication platforms, as it will convert a lot of effort in the physical world into the same in cyberspace. As a result, the IoV will doubtlessly help drive the cloud computing boom, becoming one of the first practical large-scale cloud IoT applications.

Finally, a large number of smart terminals will emerge tailored to the IoV, both in-vehicle and handset. In the future, IoV terminals should come with special man-to-machine interfaces, be able to connect to in-vehicle screens, and serve as mobile payment terminals. They should also feature IoV LBS and SNS functionality, as well as all special IoV cloud services such as ITS, automotive insurance, rescue, positioning & search, vehicle checking, remote diagnostics, and networking with the GID. With these terminals in hand, the IoV will be integral to the mobile world.