MFORMATION

An Mformation Whitepaper

CONNECTED LIVING: CELLULAR vs. NON-CELLULAR DEVICES

Can Non-Cellular Devices Within Connected Cars, Homes and Cities Generate the Same Revenue as Cellular Devices for Operators?

CONNECTED LIVING:
Cellular vs. Non-Cellular Devices

Can Non-Cellular Devices Within Connected Cars, Homes and Cities Generate the Same Revenue as Cellular Devices for Operators?

Dr. Rakesh Kushwaha
CTO, MFormation Software Technologies
581 Main Street, Suite 600
Woodbridge NJ -07095 -USA

Chuck Link
CTO, Verizon Telematics
2002 Summit Blvd, Suite 1800,
Atlanta, GA 30319 – USA

Abstract

This paper illustrates via case studies, how the use of device control and management functions such as authentication, provisioning and security, can enable operators to monetize M2M with non-cellular devices and create new revenue streams. Case studies within connected home (AT&T Digital Life) and connected car (Daimler and Verizon) are discussed.

As the convenience of seamless connectivity continues to infiltrate our lives, companies are rapidly exploring innovative ways to add value and create new revenue streams. Consumer driven solutions such as wearables, smart meters, smart parking and home automation are growing exponentially. Simultaneously, enterprises within industries such as healthcare and manufacturing are using M2M technology to move away from old business models and improve productivity. As M2M and IoT markets grow, the total amount of connected devices is reaching significant scale: according to Goldman Sachs research, IoT has the potential to connect 28 billion items to the internet by 2020, that is, 10 times as many as there are currently.

Alongside this growth, 3G and 4G networks are advancing at a rapid pace. However, it may be non-cellular networks such as WiFi that become predominant enablers of IoT. Goldman Sachs Research analyst Simona Jankowski mentions in a recent research report, they expect Wi-Fi to be the enabler of the Internet of Things comparing it to what copper was to the landline and 3G and 4G to the mobile Internet.

The proliferation of other, non-cellular wireless communication is due to the fact that within IoT, not every device has to be cellular-connected over a licensed spectrum. For a vast number of devices, the last mile will traverse over unlicensed spectrum such as Wifi, Bluetooth, or Zigbee. These devices will connect in a local area PAN/LAN configuration, aggregating over a common gateway that provides an egress point to a mobile operator’s network.

It has been suggested by Machina Research that within IoT solutions, the majority is likely to be devices connected via short-range technologies to gateways that connect to wide area

networks. Through offering value-added services, operators can take advantage of opportunities which non-cellular connections present.

The ratio of gateway devices to non-cellular devices can range from 1:10 to 1:100. This means that there can be many non-cellular devices involved in one solution, and, as with cellular devices, activities such as service activation, device security, provisioning, authentication and management are just as important within non-cellular devices but present a unique set of challenges. Operators can add value to both IoT partners and end users by offering these features through a stable in-network platform.

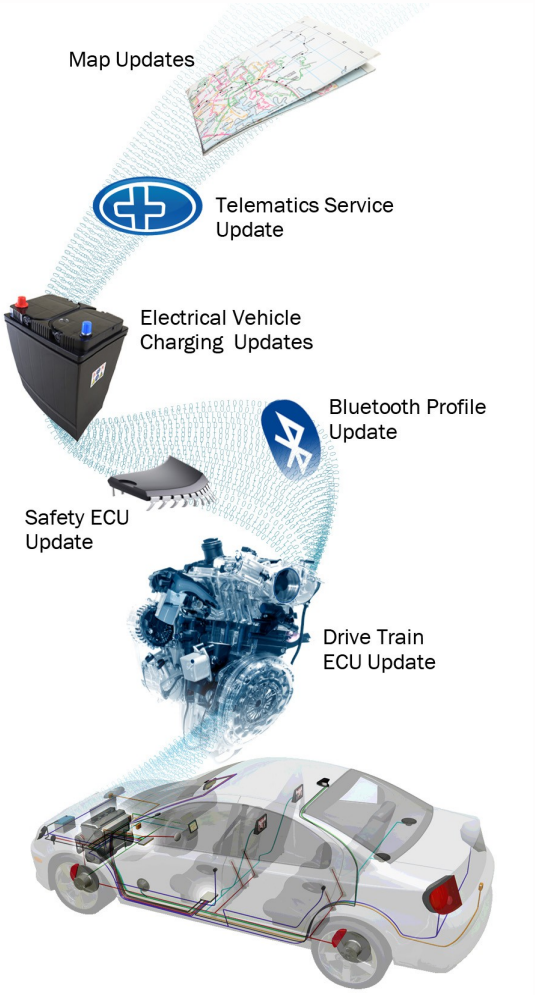

Figure 1. Anatomy of a Connected Car

Within connected cars, it is not only the telematics head unit (which is cellular) that needs to be managed, updated and secured, but numerous software car parts for a multitude of devices and electronic control units in a car that may utilize non cellular networks. The average vehicle has 70 to 100 Electronic Control Units, which control braking, idle speeds, air mixture and dozens of other routine vehicle functions. Such units require software fixes, map updates, ECU updates, service enhancements, personalization, driver profiles and new owner profiles. Take Daimler and Verizon for example. Verizon, through a third party management platform embedded in their network, was able to partner with Daimler and produce MBrace in-car technology. This allowed the carrier to gain extra revenue on many value-adding features such as safety, diagnostics, navigation, infotainment and convenience beyond cellular connectivity of the telematics head unit.

Changing Business Models

Business models for M2M and IoT solutions will rely more on ARPG (Average Revenue Per Group of Devices) or ARPB (Average Revenue Per Bundle) rather than ARPU (Average Revenue per User) so innovative service platforms need to be designed and implemented to efficiently control and manage devices.

Deployments where a smart bundle of cellular and non-cellular devices are creating new revenue streams have already started to emerge. For example, AT&T ’s Digital Life solution, the basic security package includes 3 contact sensors, a keypad, an indoor siren and a wireless control unit with only one device (wireless control unit) being cellular, if that. All of these devices are non-cellular, with the option to add Motion Sensor, Smoke Sensor, 5 Surface-Mount Contact Sensors for an additional cost. Additional non-cellular devices such as Video Camera, Garage door controller, light switch control, thermostat and water controller also can be added.

The complex connected car, which includes 3G/LTE connectivity via telematics head unit, other non-cellular devices connected via CAN (Car area network) bus and other ECUs which are also non-cellular, calls for innovative new business models, including the bundling of services so that maximum value can be created with low marginal costs in the form of ‘add on’ services. These need to be supported by alliances between mobile operators, solution providers and automakers.

How Non-Cellular Control and Management Works

Control and management functions are made possible for non-cellular devices with the availability of a service enablement layer for M2M communication, acting as a layer above network connectivity (such as mobile airtime) and below end user services (such as fleet/freight management, security alarm services). This central management layer is also referenced as Common Services Entity (CSE), as defined by OneM2M and ESTI working group. Useful functions of a central management platform include the ability to remotely enable and disable devices, manage and automate updates of application software, ‘data

warehouse' or store device data prior to processing by end user application and to integrate easily with enterprise systems via APIs.

Key Benefits of an Agile IoT Management Platform

- **Authorisation/Access Control** – security of access to devices and information
- **Connectivity Management** – network connectivity services, SLA management
- **Device Management** – remote software updates, remote diagnostics and maintenance
- **Device Data Security** – security of data received from remote devices
- **Location-based services** – when location of remote device is required
- **Data Warehousing** – storage/processing of downloaded device data
- **Disaster Recovery** – device restoration after disaster event,
- **Enterprise System Integration** – connection to enterprise IT systems
- **Portal Services** – range of support services and reports available via online portal
- **Application Development Tools** – building blocks for end user applications
- **Subscriber billing and charging Services** – vary payment for connectivity
- **Content Delivery** – delivery of appropriately formatted content to connected devices

Non-Cellular Device Hierarchy

Non-Cellular devices can connect directly to the management layer or can connect via a Gateway, for management functions. The gateway approach allows group management functions to such non-cellular devices connected to the gateway. The Gateway as defined in Gateway Management Object in OMA DM specifications provides capabilities to provide management functions to any device with any protocols.

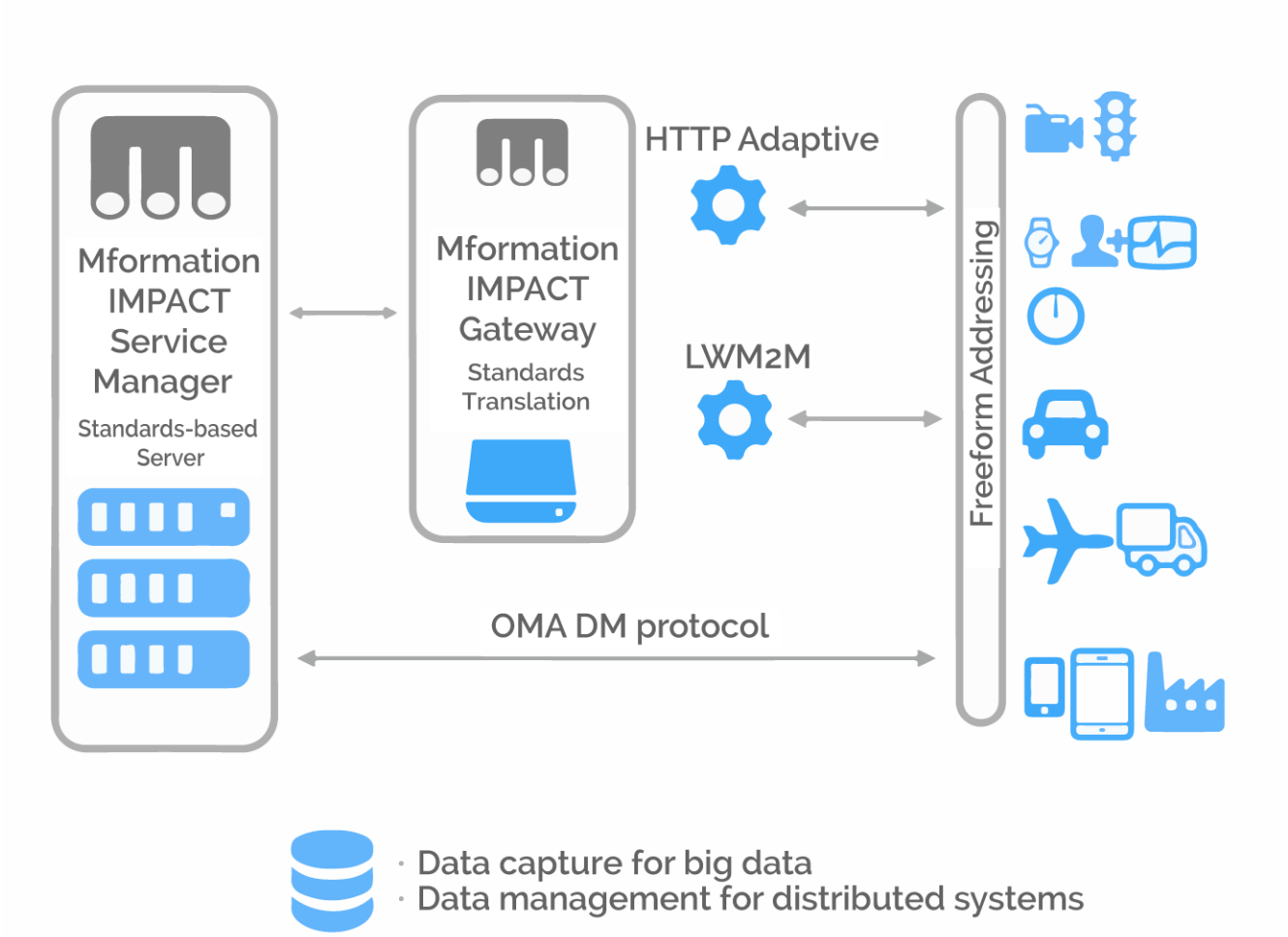

Figure 2. Mformation Cellular and Non-Cellular Device Management Architecture

IoT devices will commonly be connected to a gateway that is in turn connected to a DM server. This establishes a network level hierarchy for non-cellular devices. The device management (DM) server functionality in turn can be specialized to cater to each vertical, as the data gathering requirements and analytics vary significantly from vertical to vertical.

The types of DM commands used depend not only on the vertical but also if they apply to an individual device or to a group of devices controlled via the gateway. Just as DM commands can be considered hierarchical (group or individual), data return from the devices can also be

structured as individual or aggregate. Getting aggregate information from a group of devices will be needed to scale data reporting in M2M networks.

Other important factors to consider when enabling revenue from non-cellular are authentication, provisioning, and security of devices.

Authentication

Authentication of non-cellular devices requires novel schemes to ensure that the device either sitting behind the gateway or connection directly is a legitimate device. While the gateway or cellular device can be authenticated using standard cryptography and non-cryptography used in schemes networks, non-cellular devices require alternate authentication schemes that require mutual authentication between the gateway and the non-cellular devices. Unique identifiers such as IMEI are not available for non-cellular devices; hence secure schemes using certificates and that require periodic challenge response between the gateway and non-cellular devices are required.

Provisioning

Provisioning billions of non-cellular devices such that services provided on these devices can be billed and customer care operations can be provided. Example, if non-cellular devices operate behind a gateway, the gateway should be remotely provisioned to allow a fixed number of devices.

Security

Secure firmware package running at the lowest level of the software tack on device hardware, ensures security at various levels. However, M2M systems can be subject to attack by any number of means. Individual devices can send malicious data or overwhelm the gateway by sending excessive data resulting in a data implosion problem. In the extreme, a group of M2M

devices can launch a DDOS attack on the gateway or the entire network. Hence, secure schemes on the gateway should continuously monitor data patterns along with DPI to ensure correct behavior. Even The gateway should be able to shut off any or all ports to prevent malicious M2M devices from affecting the entire network. The continuous monitoring of the various ‘things’ should result in proactive actions prior to system failure or malfunction.

Conclusion

A management platform specifically designed as an integral part of the IoT infrastructure, can enable the communication provider to take advantages of opportunities in non-cellular IoT devices, as demonstrated in the Daimler and Verizon’s connected car solution and AT&T digital home solution. The unique challenges for non-cellular devices present in relation to authentication, provisioning and security and device hierarchy, further highlight the importance of a dedicated platform for such key functions. A management platform that can enable growth, which in turn translates into greater revenue with the bundling of services, as shown in the AT&T Digital Life example, is key to creating new revenue streams for operators and growing the IoT market.

Sources

http://news.investors.com/technology/062714-706520-wifi-has-advantages-over-cellular-networks-in-m2m.htm

http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf

http://docbox.etsi.org/workshop/2010/201010_M2MWORKSHOP/01_SettingTheScene/VISWANATHAN_ALCATELLUCENT.pdf

http://www.gartner.com/newsroom/id/2636073

https://machinaresearch.com/static/media/uploads/white_paper_machina_research_m2m_platform_sept_2012.pdf

http://www.beechamresearch.com

CONTACT US

If you would like to receive additional information on our company and our innovative mobility management solutions, please feel free to contact us.

Mformation Software Technologies, LLC

581 Main Street, Suite 600
Woodbridge, NJ 07095