March 2021

Routing of Network Traffic on a Per-Application Basis

James Mattis

Ryan Weekes

Tomasz Wasilczyk

Guru Nagarajan

Sanjay Lal

See next page for additional authors

Inventor(s)
James Mattis, Ryan Weekes, Tomasz Wasilczyk, Guru Nagarajan, Sanjay Lal, Kevin Meier, Jean Chalard, and Chris Weir

Routing of Network Traffic on a Per-Application Basis

ABSTRACT

Wireless applications in certain domains, e.g., automotive, Internet-of-Things (IoT), etc., consume substantial amounts of bandwidth. A user accustomed to data consumption on a mobile device may be surprised to find the substantially larger amounts of data consumed via telemetry by wireless devices and sensors on their automobile. Reciprocally, a car manufacturer may not want a customer to pay for telemetry. This disclosure describes techniques to route network traffic to specific network interfaces on a per-application basis. The techniques can be implemented in a device operating system, and provide mechanisms for users and original equipment manufacturers (OEMs) to separate data costs for usage of various applications, thereby enabling a robust, secure, and connected experience.

KEYWORDS

- Application-based routing
- Bring your own device (BYOD)
- Network interface selection
- Smart TV
- Data plan
- Over-the-air (OTA) update
- Connected automobile

BACKGROUND

Wireless applications in certain domains, e.g., automotive, Internet-of-Things (IoT), etc., consume substantial amounts of bandwidth. A user accustomed to data consumption on a mobile device may be surprised to find the substantially larger amounts of data consumed via telemetry by wireless devices and sensors on their automobile. Reciprocally, a car manufacturer may not want a customer to pay for telemetry.

A related circumstance is the bring-your-own-device (BYOD) policy of enterprises, which can unduly burden employees who use their data connections on behalf of their employer. Another related situation where an original equipment manufacturer (OEM) of connected electronic devices, e.g., smart TV, smart speaker, smartwatch, etc., wants to offer to a user a new data-consuming service that the user is hesitant to pay for.

In the above instances, a device, e.g., a car, a smartphone, a TV, etc., is owned by the user but is used for bandwidth-consuming services that the user may be unsure about paying for, or that the device-manufacturer or an employer is interested in paying for.

Although mobile carriers can, in a procedure known as zero-routing, reconcile data used by carrier-side apps to charge the user differentially (e.g., zero for carrier-side apps versus normal charges for other apps), all traffic is routed identically, e.g., not on a per-application basis to specific network interfaces.

DESCRIPTION

This disclosure describes techniques to route network traffic to specific network interfaces on a per-application basis. For example, in automobiles with wireless connections, bandwidth consumed by certain applications, e.g., safety, sensors, navigation, etc., can be paid for by the automobile OEM, while others, e.g., relating to in-car entertainment, can be paid for by the user. Similarly, in a BYOD scenario, data usage attributable to the user's employer, e.g., work-related applications, can be paid for by the employer, while personal data usage can continue to be paid for by the user. The specific splitting of data usage charges can be across two or even more entities, and can differ based on users, types of devices, or other factors.

This disclosure describes techniques that enable users and OEMs (or employers) to manage data costs, thereby enabling a robust, secure, and connected experience. Routing to

different network interfaces on the device on a per-application basis obviates the need for reconciliation with the carrier.

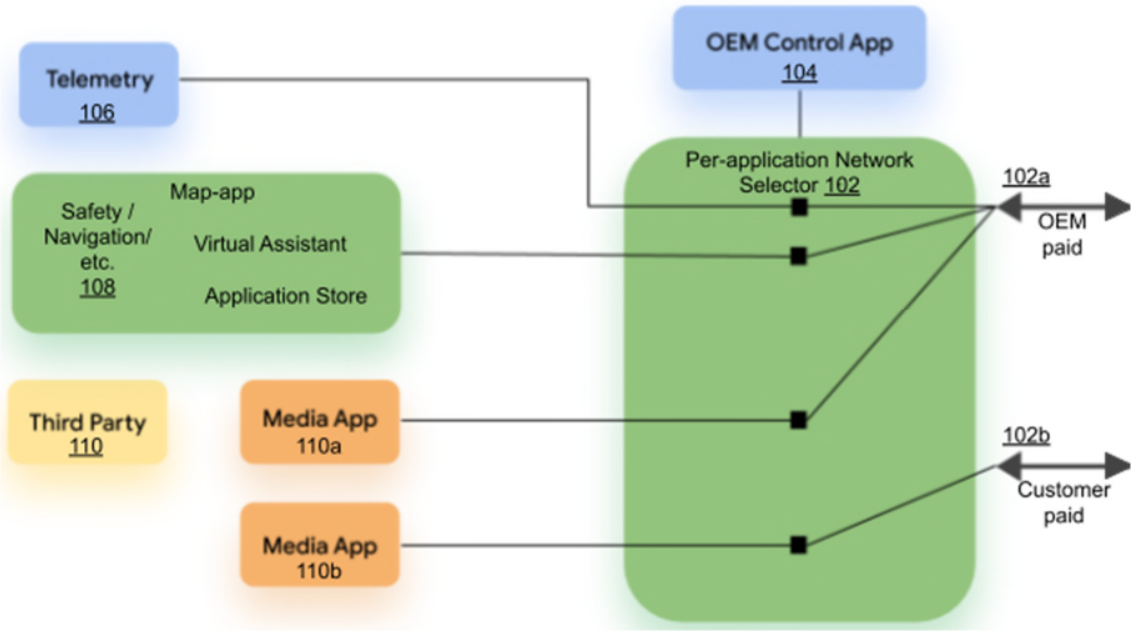

Fig. 1: Routing of network traffic on a per-application basis

Fig. 1 illustrates the routing of network traffic on a per-application basis. Such routing can be controlled by a device operating system. A per-application network selector (102) is a module that routes network traffic originating from various applications to one of multiple network interfaces, e.g., an OEM-paid network interface (102a), a customer-paid network interface (102b), etc. The per-application network selector can be configured by an OEM control app (104), which enables the OEM and/or customer to route data from particular applications to particular network interfaces.

For example, in an automobile, telemetry data (106), safety and navigation data (108), and other data important to automotive function can be routed to an OEM-paid network interface. Data from third party apps (110), e.g., a media app (110b), can be routed to a customer-paid network interface. As a marketing offer, the OEM can pay for a non-critical

application, e.g., a media app (110a), in which case, data from that media app is routed to the OEM-paid network interface.

In another example, an OEM of a smart TV or smartphone can offer to pay for data usage by certain OEM-origin (pre-loaded) apps, in which case such data is routed to the OEM-paid network interface. At the same time, data used by apps downloaded by the user are paid by the user, e.g., such data is routed to the customer-paid network interface.

Similarly, in the BYOD scenario, data consumption that arises from work-related applications is routed to a network interface paid for by the employer, while data consumption that arises from personal applications is routed to a network interface paid for by the device owner.

The described network interfaces have no relationship to the type of physical layer standard being used. For example, the OEM-paid network interface can use cellular (4G, LTE, etc.), WiFi, Bluetooth, ethernet, or any other physical link, and in an order of preference specified by the OEM. Similarly, the customer-paid network interface can use cellular (4G, LTE, etc.), WiFi, Bluetooth, ethernet, or any other physical link, and in an order of preference specified by the customer. The service providers for the OEM-paid and the customer-paid networks are not constrained to be the same.

More example applications of the described techniques follow.

- A TV OEM can work with hotels to route certain applications over hotel-managed networks such that the TV OEM pays for data used by those applications when invoked by hotel guests. For example, a hotel guest can be offered a one-hour subscription to the hotel's WiFi network for a particular streaming service, where the one-hour subscription is paid by the TV OEM.

- An OEM can provide a subscription-based service, where, with an active subscription, certain applications are routed over an OEM-paid network. For example, a certain set of applications in the head unit of a car can be routed over an OEM-paid network based on a subscription fee. Alternatively, the applications, even if they run on the head unit of the car, can communicate over the user's smartphone connection.
- Network traffic can be disabled on a device, e.g., a rented car or a company-owned laptop, except for some apps until the user logs in to a portal on which the device is managed.
- Selected applications on company or rental cars can be provided internet connectivity paid for by the enterprise, while other applications can have connectivity paid for by the user or renter. In general, any Internet-connected asset that is rented out or is in the field can use company-paid or user-paid connectivity based on application.
- Important updates can be automatically provided to equipment, e.g., cars, smart TVs, etc. even if the user doesn't have a personal data plan.
- OEMs can enable devices to opportunistically connect to networks of their partners (e.g., coffee-shop, mall, or airport WiFi networks; particular cellular providers; etc.).

CONCLUSION

This disclosure describes techniques to route network traffic on a device to specific network interfaces on a per-application basis. The techniques can be implemented in a device operating system, and provide mechanisms for users and original equipment manufacturers (OEMs) to separate data costs for usage of various applications, thereby enabling a robust, secure, and connected experience.