July 2022

DATA SOVEREIGNTY AND DATA RESIDENCY COMMUNICATIONS INVOLVING LOW EARTH ORBIT SATELLITES

Robert Barton

Jerome Henry

Dave Zacks

Francesco Basile

DATA SOVEREIGNTY AND DATA RESIDENCY COMMUNICATIONS INVOLVING LOW EARTH ORBIT SATELLITES

AUTHORS:
Robert Barton
Jerome Henry
Dave Zacks
Francesco Basile

ABSTRACT

In a Low Earth Orbit (LEO) satellite system, LEO satellites can collect data and relay the data to ground stations. Today, many countries and regions within the world (e.g., the European Union (EU), provinces or states within a country, or a country itself) have strict data sovereignty policies that do not allow sensitive data to be transmitted outside of national, regional, state, or provincial borders. Thus, if a LEO satellite is to collect ground terminal data from a sensor device (such as operational data of non-urban emergency vehicles), it must do so within bounds of the data residency and sovereignty polices based on the location of the customer. In other words, for the LEO satellite to be compliant, it cannot relay data to just any ground station - it must do to one that meets the requirements of the sovereignty policy. Presented herein is a technique to enforce data sovereignty policies when data is collected by LEO satellites in order to ensure that, when the data is passed back to ground stations, data sovereignty policies are enforced.

DETAILED DESCRIPTION

As LEO satellites pass overhead for an LEO satellite system, the satellites collect data from sensors. Once data is collected by an LEO satellite, the data needs to be relayed down to a ground station. Such data transmission may happen in one of several ways:

1. A large constellation of LEO satellites may relay the data through other LEO satellites in the constellation until the data reaches an LEO satellite that is currently passing over a ground station (typically through lasers) - this method is generally low latency;

2. A small constellation of LEO satellites may include only a handful of satellites. In a small constellation system, the LEO satellites will cache data until the satellites pass over a ground station during their orbit. Such satellites will typically pass over a ground station several times a day. This model is popular with many Internet of Things (IoT) satellite startups; or
3. An LEO satellite relays data to a higher-orbit satellite, such as a Medium Earth Orbit (MEO) or a Geostationary Earth Orbit (GEO) satellite. The higher-orbit station will then relay the traffic to a ground station. This model is generally more expensive than other LEO satellite systems.

In all cases, ground stations may be positioned in various parts of the globe, and the ground stations may or may not be located in the same country as the ground terminals.

Today, many countries and regions within the world (e.g., the EU, provinces or states within a country, or a country itself) have strict data sovereignty policies that do not allow sensitive data to be transmitted outside of national, regional, state, or provincial borders. Thus, if an LEO satellite is to collect ground terminal data from a sensor device (such as operational data of non-urban emergency vehicles), it must do so within bounds of the data residency and sovereignty polices of the customer. In other words, for an LEO satellite to be compliant with data sovereignty policies, it cannot relay data to just any ground station, but rather must relay data to a ground station that meets the requirements of a given sovereignty policy of a customer.

Thus, there is a need to align data sovereignty policies of a customer with data transmissions from LEO satellite systems back to ground stations to ensure compliance of such systems.

This proposal provides a technique to enforce data sovereignty policies when data is collected by LEO satellites in order to ensure that, when the data is passed back to ground stations, data sovereignty policies are enforced.

Consider, for example, that a constellation of LEO satellites is deployed, along with a series of ground stations placed around the globe. The LEO satellites can collect data from ground terminal devices as they fly over (e.g., sensors such as vehicles, agriculture sensors, forest fire detection sensors, Department of Homeland Security sensors, etc.). The

LEO satellites must then relay the data to ground stations when they come into range of the ground stations.

In accordance with this proposal, the LEO constellation operator can implement a data sovereignty/data residency (DR/DS) policy mechanism through a front-end tool that allows each customer to define their data sovereignty policy. The policy for each device can be stored in a DR/DS database that can reference every authorized device that can transmit data to the LEO constellation, along with a list of compliant ground stations that may receive the relayed data. The DR/DS database may be locally cached on the satellite, or it may be provided via a ground server.

For example, a customer may define a policy for any scenario, such as:

- Data transmitted from any the Department of Homeland Security ground terminals may only be relayed to ground stations physically within the United States;
- Data transmitted by a European defense sensor device may only be downloaded to a ground station within a North Atlantic Treaty Organization (NATO) country; or
- Data transmitted from a healthcare wearable sensor may only relay patient data to a Health Insurance Portability and Accountability Act (HIPPA) compliant ground station.

For small constellations of LEO satellites that are not able to relay data to other satellites and must cache the data, each time the LEO satellite comes within range of a ground station it will synchronize its local DR/DS database with a master DR/DS database on the ground, allowing it to update new devices, along with their policy.

In essence, DR/DS policy definitions can be used to enforce a system through which LEO satellite can identify DR/DS policies for corresponding devices in order to relay data/traffic to a ground station that meets the corresponding DR/DS policies. Thus, the novelty of this proposal can be realized by defining which ground stations are acceptable for downlink transmission of data, in accordance with one or more DR/DS policies.

When an LEO satellite comes within range of a sensor (or group of sensors), data is transmitted from the sensor(s) to the satellite. This data is stored queued on the satellite until it can be transmitted to a ground station. For each customer, the data is stored in a compartmentalized format, preventing data sharing or leakage from one customer to another.

When the LEO satellite passes overhead and makes a connection with the ground station, it first verifies the identity of the device. The satellite then accesses the DR/DS policy database, and a satellite router can then append a series of bits to the header of an to IP packet (e.g., metadata, IPv6 extension headers, etc.), with a set of known identifiers of ground stations that may be used for this data (which are compliant to the policy).

Thereafter, the LEO satellite can either relay the data along a sky path until it reaches a satellite that is overhead a compliant ground station, or it can continue to cache the data until it passes over a compliant ground station later at a later time. When the satellite is over a compliant station, the data can be relayed to the ground. As the ground station receives the transmission, the same validation can be performed. Data that is not compliant is rejected and the station can signal to the satellite the rejection along with a reason for the rejection.

Figure 1, below, provides an example illustration of various operations that may be performed in accordance with the technique of this proposal.

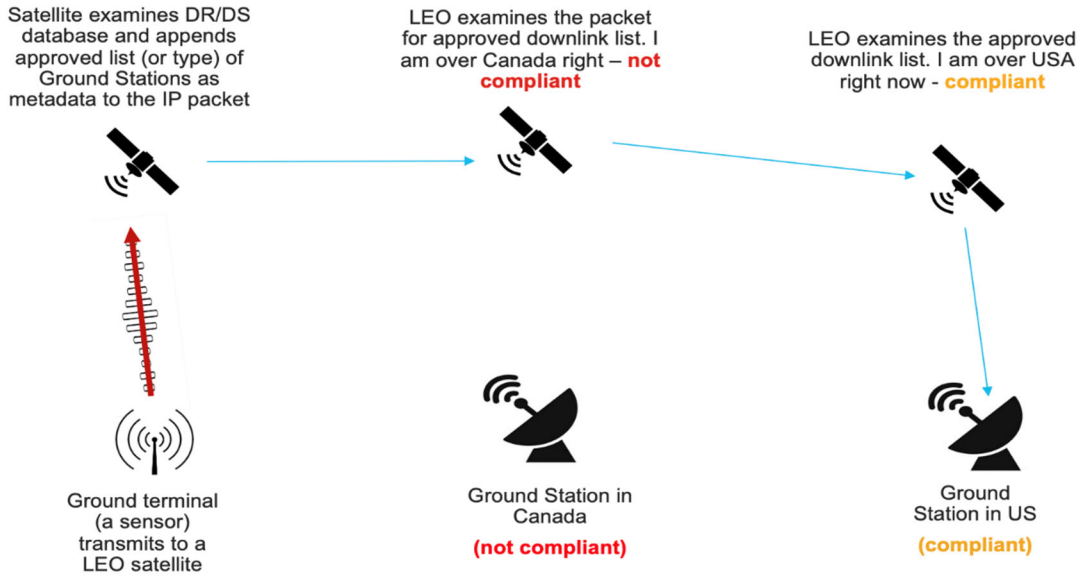

Figure 1: Example Operational Illustration

In some instances, a DR/DS policy may also include details that can be expanded to include not just the type of customer, but also the type and/or sensitivity of data. For example, if any data includes Personally Identifiable Information (PII) and is sensitive (e.g., health data transmitted from wearables, etc.), the data may be marked with a data sensitivity identifier. When the data collector on the LEO satellite sees this PII marker, the data collector can retain the PII marker in the packet beyond the ground station. For example, some sensors in a health system may not include PII data, but other data from this same health care provider will include such PII data (e.g., from wearables, etc.). In this case, only the sensitive data would be augmented with the PII indicator, providing further details to the data relay on the LEO satellite that this data may only be downlinked to specific ground stations that meet data privacy and control standards (such as HIPPA compliance).

Further, the technique proposed herein can also be extended to techniques that may involve identifying the origin device, including identification of the device during an onboarding phase, and linking to a mapping function in the satellite that links the device identity with a policy generated by an end customer. Additionally, the technique may further be extended to identify an application being used by a device that has a data sovereignty policy that has been generated by a customer. Further, the technique may be extended to marking data or a packet generated by a policy-sensitive application or device that can be recognized by other satellites in a constellation, as well as by a ground station. Moreover, the technique can be enhanced to enable enforcement by a ground station that may refuse a download of non-compliant data from an LEO satellite and/or, conversely, by an LEO satellite may refuse to downlink data to a non-compliant ground station in which, in some instances, the LEO satellite can search for a compliant ground station.

In summary, this proposal provides various techniques through which data sovereignty policies can be enforced for LEO satellite communications such that, when data is transmitted from an LEO satellite to a given ground station, data sovereignty policies can be enforced.