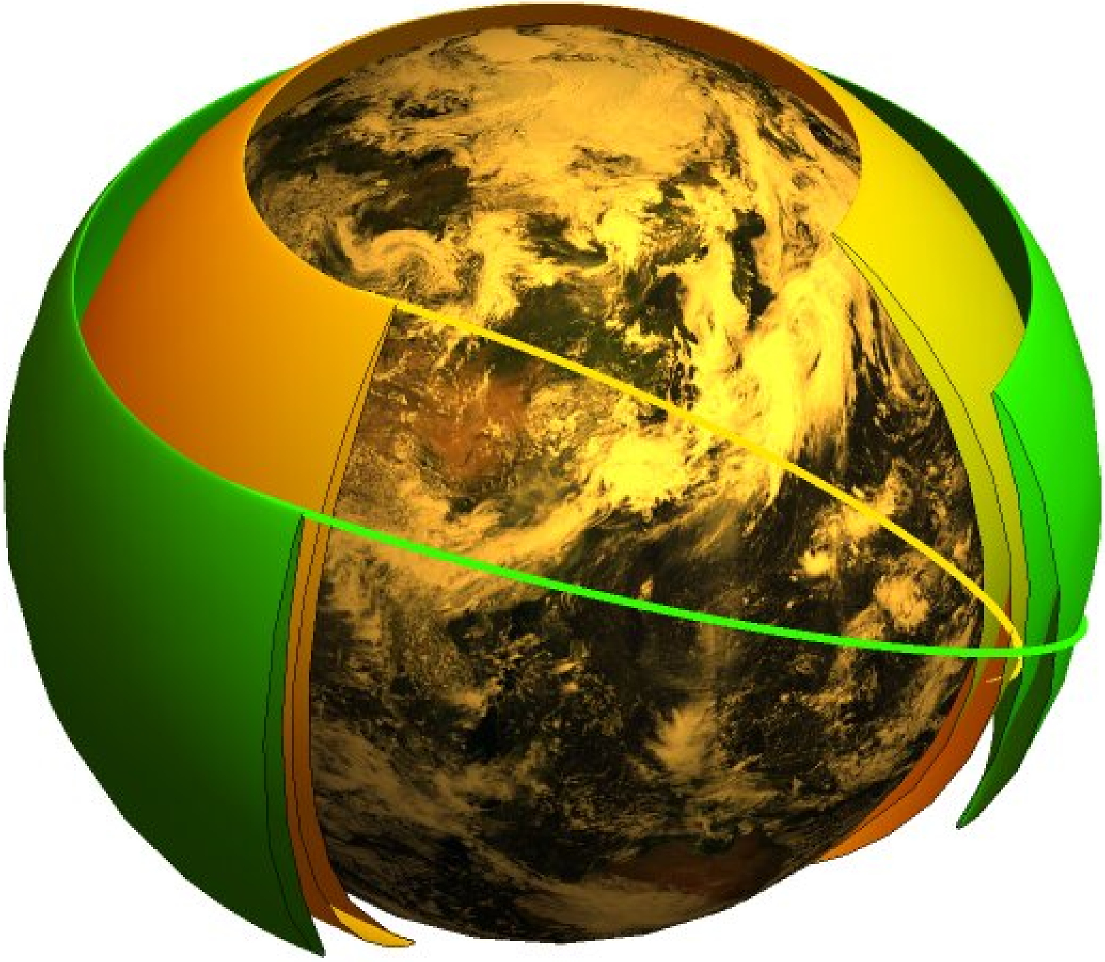
PHYS.ORG

How will Starlink's packet routing work?

November 4 2020, by Andy Tomaswick



Credit: SpaceX

SpaceX's Starlink satellite cluster has been receiving much headline space recently as it continues adding satellites at a breathtaking pace.

Much of this news coverage has focused on how it's impacting amateur skygazers and how it could benefit people in far-flung regions. But technical details do matter, and over on Casey Handmer's blog, there was a recent discussion of one of the most important aspects of how Starlink actually operates—what will it do with its data?

In networking lingo, data is quantized into "packets," which are sets of ones and zeros that computers can understand. In the case of Starlink, these packets will bounce between ground stations and a series of satellites parked in nine separate low-Earth orbits. Each orbit will contain a number of satellites, and each satellite's covered territory will overlap with the satellites to the north and south of it. When the constellation is complete, every spot on Earth will be covered by at least two Starlink satellites.

Future versions of the satellites will use lasers to communicate amongst themselves. But for now, they have to use ground stations to talk to other satellites. Therefore, there will be a great amount of packet passing between satellites, ground stations and end user terminals. The information that describes such a convoluted path for each packet must be stored somewhere. That somewhere is called the "metadata."

Metadata is commonly used to denote the parts of a data packet that don't contain the actual information being passed. It contains information like the length of the packet, the originating point, and the destination. Arguably, this data is more valuable than the content of most packets. It would allow an interested party to see who is connected to who, when they communicated, and how much information was being shared. In some situations, such as when Osama bin Laden's courier took a call from an old friend, this type of metadata can have deadly consequences.

Privacy is therefore central to any system that hopes to become the backbone of the internet. That safety net will have to tackle many potential challenges, including the satellites themselves potentially logging the data or a malefactor intercepting the beams used to communicate between a satellite and ground station. Encryption can solve some of these problems, such as packet interception, but would not solve others, such as the FBI forcing SpaceX to log traffic from one particular Starlink user.

In his blog, Casey tackles the problem from the ground up, describing a system that exposes a bare minimum of information to each step in the packet routing process. This simplified system would have to account for things like satellite movement, satellite loss, and myriad other potential complications, but at its core, it could work. Casey calculates that, at a minimum, a router (or satellite) can be exposed to only two to three bits of information, simply enough to send the packet on its way and maintain its integrity.

The example he uses to show this simplified methodology describes a packet traveling from Los Angeles to New York. The first satellite simply has a bit showing it that it must transmit the packet "northeast." Data identifying its originating location is then removed from the packet, and new information showing the directionality for the next satellite is revealed in the same two- to three-bit space. The receiving satellite simply knows that a packet arrived from the southwest, how long the packet is, and that it also needs to pass the packet to the northeast. This simplified directionality is continued until the last satellite passes the information to the ground station, which can then pass the packet along to the end user in New York.

This simplified directionality approach would combine with another anti-hacking technique known as a "keying" system. In Casey's example, there are two separate keys—one for "time" and one for "space." Each key, which is required even to access the metadata of a packet, would be valid for a very short period of time, and would update continuously depending on the satellites geophysical location and what time the packet was received. Even with the key, if someone managed to intercept the packet, the key would expire within a second and the packet would become useless.

Details on the exact system operation can be seen in Casey's blog. There is no guarantee that SpaceX would implement such a solution, and as Casey himself says, "I haven't spent years working only on this problem." But the solution he presents is elegant and could potentially soothe privacy concerns that would come with the territory for any globe-spanning interconnected space network. If nothing else, the discussion of a solution to the privacy and efficiency problem can give Starlink even more time in the limelight.

Provided by Universe Today

Citation: How will Starlink's packet routing work? (2020, November 4) retrieved 23 April 2024 from https://phys.org/news/2020-11-starlink-packet-routing.html