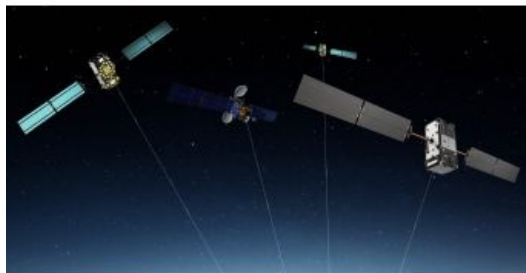


Falsification of Galileo Satellite Signals More Difficult



The European Union (EU) activated its Galileo satellite navigation system in December 2016. The EU is dedicated to setting this system apart from other navigation systems such as GPS, Galileo's US counterpart. Researchers from the Department of Electrical Engineering at KU Leuven (University of Leuven, Belgium) have now risen to this challenge as well: they have designed authentication features that will make it even more difficult to send out false Galileo signals.

Navigation systems are based on satellites that send out signals, including their location. The distance to four or more satellites makes it possible to determine someone's geographical position and time. But this process may go wrong when hackers send out signals of their own that drown out the real ones. As the authentic signals are blocked, the

position information for the navigation system is no longer correct.

Professor Vincent Rijmen and doctoral student Tomer Ashur from the Department of Electrical Engineering (ESAT) at KU Leuven have now advised the European Commission on ways to make Galileo signals more difficult to falsify. Their authentication method involves electronic signatures, similar to methods used for online banking.

To avoid delaying the launch of Galileo the researchers could only use the remaining 'bits' in the signals for authentication purposes. This is why the TESLA method for electronic signatures are supported. They fit into 100 bits. They quickly expire, which is not a disadvantage in the case of satellite navigation because the location is authenticated every 30 seconds or less.

The method still needs to be tested and validated before it can be made available to the general public. The authentication service is scheduled to become publicly available on a number of Galileo satellites in 2018. By 2020 the method will be fully operational. To use it, however, a special receiver for Galileo signals that can also verify the electronic signatures will be needed. These receivers are currently in development.