GNSS Spoofer

REPLEX

Recently, the drone market grows rapidly, malicious use of drones such as precision bombing and illegal filming has become a social issue. Since drones are small, fast and move through the air, they can attack by ignoring existing ground defense systems.
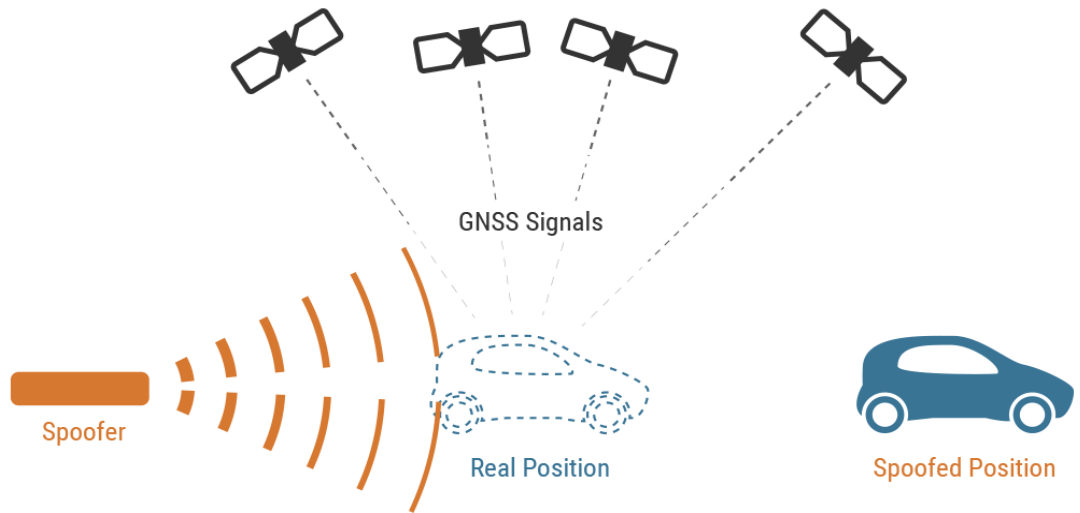
Replex has developed GNSS Spoofer which can make deceptive position signals that can prevent drones from flying normally. Replex's Hellosat can protect infrasture such as nuclear power plants, gas facility, water facility and Data center from drone threats.

※ Features
- Compact, light-weight, powered by battery
- Effective for all devices using GPS
- Custom-made according to the needs of user
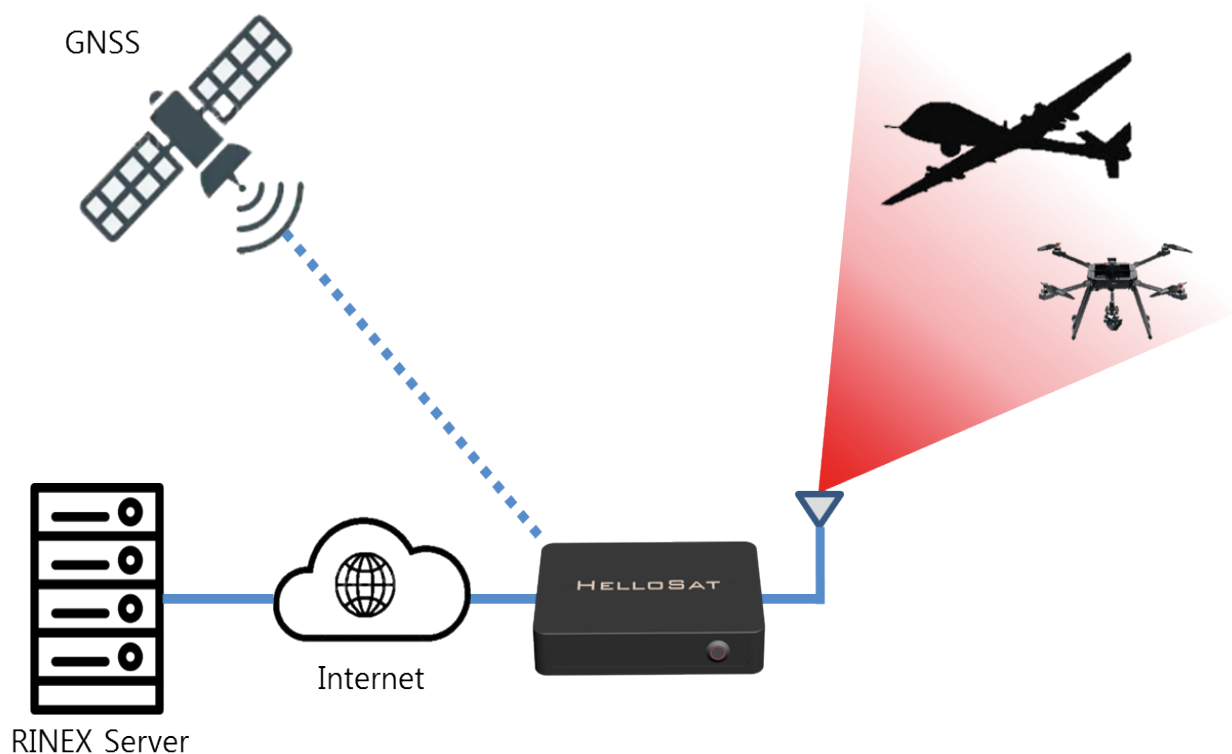
REPLEX
www.replex.co.kr

What is GNSS spoofer?

GNSS signal spoofing consists of broadcasting fake signals –over the real GNSS signals– in order to take control of a GNSS receiver that will continue to track those signals in error. GNSS is very sensitive to this type of attack due to the weakness of satellite signals at the earth's surface and the fact that these signals are public and not protected as such. A successful spoofing attack consists of taking control of a receiver without it noticing the attack. The goal of the attack is to introduce an erroneous result for position or timing or both.

GNSS Signals

Spoofer

Real Position

Spoofed Position

Fields of Application

• GNSS Vulnerability test
• Counter-drone against drone intrusion
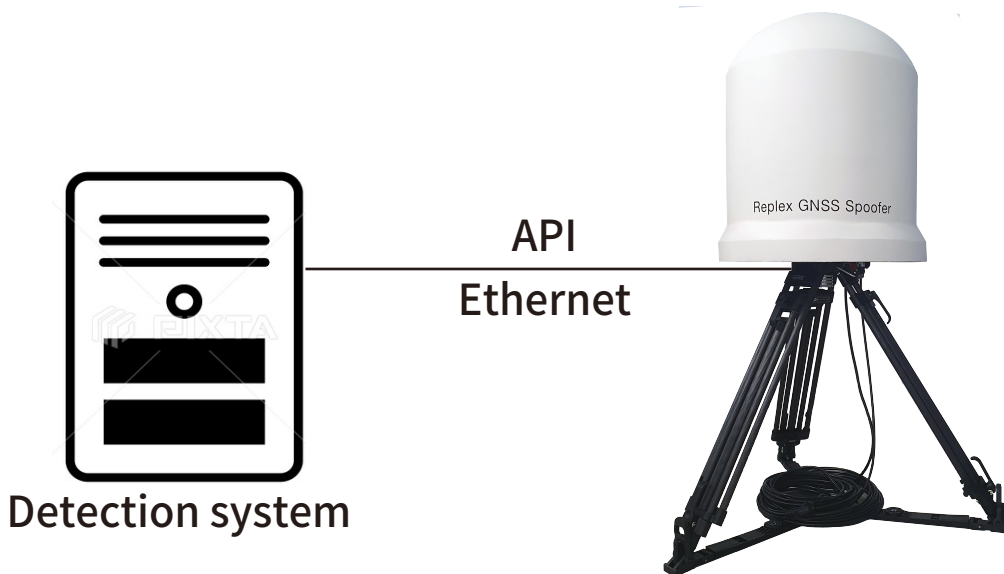• Improved GPS shaded areas such as tunnels

GNSS

HelloSat

Internet

RINEX Server

Product List

Hellosat-S3000

Main System	i5 PC
Operating System	Window/LINUX
Consellation	GPS L1/GLONASS L1
Output Signal Level	10W
RF Channel Frequency	1,575.42MHz/1,602MHz
Number of Satellites	All in view
Sampling Frequency	2.5MHz
Main Function	RINEX generation
	Time synchronization
	GNSS signal generation
	Jamming signal generation
Size	50X50X60cm
Weight	19kg

System configuration

API
Ethernet

Detection system

EMP & HPEM
SOLUTIONS PROVIDER