Shiningintl navigation deception anti drone system operation guide

What is the navigation deception anti-drone system

The essence of navigation deception system is not to rudely interfere with signals, but to play the role of a "scammer" or "copycat GPS satellite". It sends navigation signals to drones that are stronger than real satellite signals, but with completely false content, deceiving the drone's GPS receiver into "believing" that it is flying in another location or along another path. As the real navigation signals from the satellites are weak, normally the signal from the deception system will be adopted by the drones.

Here are the steps how the navigation deception anti-done system works:

Step 1: Monitoring and Analysis the real navigation signals

The deception system will first passively monitor the signals of all GPS satellites (including the United States' GPS, China's Beidou, Russia's Glonass, Europe Galileo ,Japan QZSS and India NavIC) in the current airspace. It will accurately analyze:

signal frequency

Pattern

Navigation message content (including key information such as satellite orbit and timestamp)

This process allows the deception system to fully grasp the GPS signal structure of the 'real world'.

Step 2: Generate false signals

Navigation deception system bases on the analysis of real signals, then the signal generator within the deception system will begin to create "fake signals". These false signals have the following key characteristics:

Consistent structure: The code and data format are exactly the same as the real GPS signal, ensuring that the GPS receiver of the drone can decode normally.

Stronger power: The strength of false signals will be slightly higher than that of real satellite signals. This is the key to successful deception, as receivers typically lock onto and track stronger signal sources (known as the 'near far effect').

False content: This is the essence of deception. The navigation message in false signals contains incorrect positioning and time information.

Step 3: Implement deception (several main modes)

According to tactical objectives, navigation deception mainly has the following operational modes:

Virtual displacement deception

Principle: The system calculates the desired location for the drone to "believe" in (for example, a virtual point at the end of an airport runway), and then generates a complete set of GPS signals. These signals combined will allow the drone to calculate its own coordinates as this virtual point.

Drone response: The drone compared its own sensor data (such as IMU) with GPS data and found a huge contradiction. In the vast majority of cases, drone flight control systems prioritize trusting more "reliable" GPS data. In order to correct this "deviation", the drone will automatically start flying towards the target point it "considers" to be correct (i.e. the actual takeoff point or preset home point), but the coordinates of this target point itself are incorrect. The result is that the drone is induced to fly towards a safe area (such as an open space).

Effect: Inducing landing or driving away. This is the most commonly used mode that can safely guide the drone to a designated location for capture.

Track deception

Principle: More advanced than virtual displacement. The system does not give the drone a fixed false position, but generates a continuous, dynamically changing false flight path.

Drone response: If the drone is in autonomous flight mode (following predetermined waypoints), the deception system can gradually "distort" the coordinates of these waypoints, causing the drone to unknowingly deviate from its original route and fly along a safe path set by the system.

Effect: Control the flight path. It can fly the drone obediently along the set route like a shepherd.

Shiningintl is a professional supplier to provide the whole navigation deception anti-drone solution for the 6 navigation system

Problems in navigation deception anti-drone system

We have discussed the navigation deception system theory in the first paragraph, normally the drones will take the "fake" navigation signal, it can't identify the signal is been modified by the deception system, but there should also 2 problems the "smarter" drones can recognize problems:

1. The navigation signals may stronger than normal standard, as the real navigation signal come the space and go through a long distance, normally

the signal is very weak, but the "fake" signal is emitted from near distance, the signal normally is stronger than the real signal, if the drone smarter, it will find there should has problem in the signal strength. What kind of smart function? The drone has the capability to compare normal signal strength and the signal it received.

2. If the drone has installed the anti-interference antenna, the drone should know that the navigation signal direction, the real navigation signal is from the sky space, if the drone find the navigation signal from other direction, then it can realize some problem with the navigation signal.

Shiningintl navigation deception anti-drone solution

Shiningintl is a professional supplier of anti-drone system, and the technical solution is based on the navigation decoying. As the leading anti-drone solution supplier, Shiningintl navigation deception anti-drone solution can solve the above problems perfectly. Except the two problems above, Shiningintl navigation deception anti-drone system also have lots of features:

1. **Separated controller and processing unit**
   To protect the operator in war field, our system separates design of the controller and processing unit, then the operator can control the system in a long distance, it can protect the operator from harm.
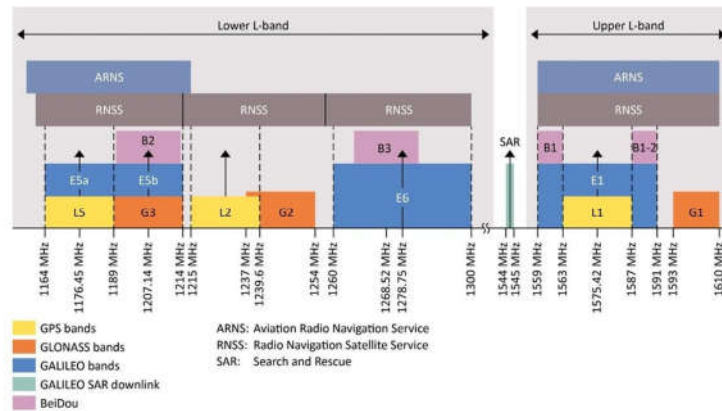
war field ——————long distance——————→ safe area
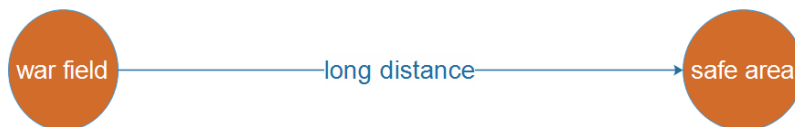
2. **All navigation systems support**
   Includes the all 6 navigation system: USA GPS, China's Beidou, Russia's Glonass, Europe Galileo ,Japan QZSS and India NavIC

3. **Cover all bands of each navigation system**
   Cover the bands from 1.2Ghz to 1.6Ghz, the lower band and upper band, the detail shown as below

4. **Creatively combine navigation jammer and deception(spoofer)**
   Shiningintl navigation deception solution can combine the real navigation signal and fake navigation signal interference, then the drone can't identify which one is the real signal, the anti-interference system on the drones can't work correctly.
5. **combine portable mobility and large area professional field protection**
6. based on Shiningintl anti-drone solution, you can create the portable back-pack similar device, it provides high mobility, you also can create large area protection equipment system, depend on your **purpose** and budget.

7. **Provide control interface for secondary development of network;**
   Shiningintl provides the SDK interface for integration of our navigation deception anti-drone system, the developer can communicate with our system with the RJ45 port.

# Shiningintl navigation deception anti-drone system deployment

Shiningintl navigation deception anti-drone solution provides different level deployment architecture, it can provide flexible deployment choices , the users can choose based on its situation.

1. **Portable equipment(no controller needed)**
   After the system is installed preset configuration, it will automatically work after power on,   in this situation, shiningintl navigation decoy system can be carried by the operator, and no complicated training needed, only power on the system, and the equipment will work perfectly as its preset configuration.
   Advantage：easy to operate, no configuration on field needed.
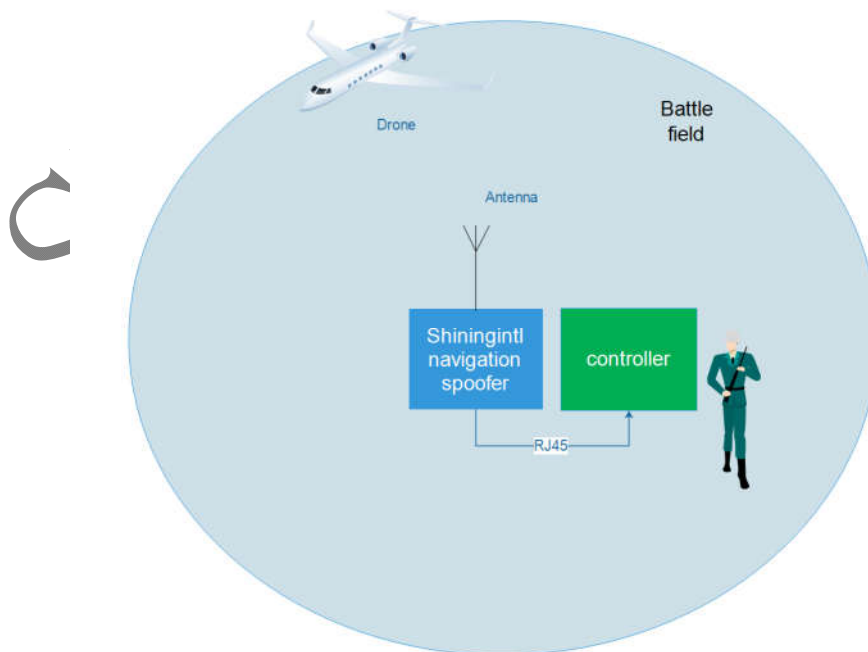   Disadvantage：system has worked as pre-installed parameters
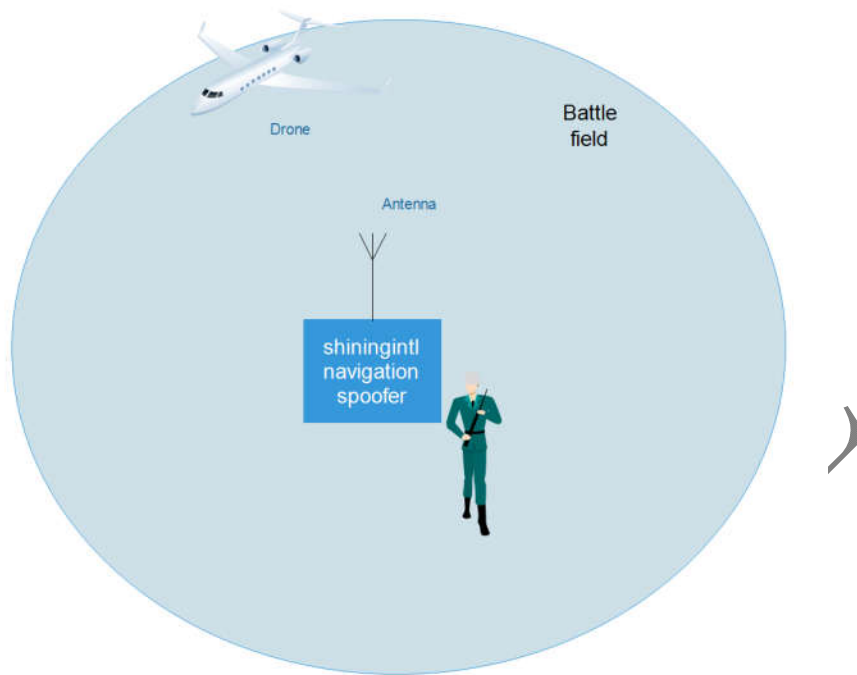
2. On-location full controlled

In this case, the operator can adjust the parameters on location anytime anywhere,

Advantage: adjust the parameter on time.

Disadvantage: the operator is in the war field, it may lead to harm if been attacked.


3. On-location full controlled with Shiningintl jammer

In this case, the shiningintl navigation jammer is included, the shiningintl navigation jammer and spoofer cooperate together.

Advantage: improve the system reliability, the shiningintl navigation jammer has interfered the real navigation signal locally, the "fake" signal is much reliable to the drones.

Disadvantage: the operator still in dangerous environment.
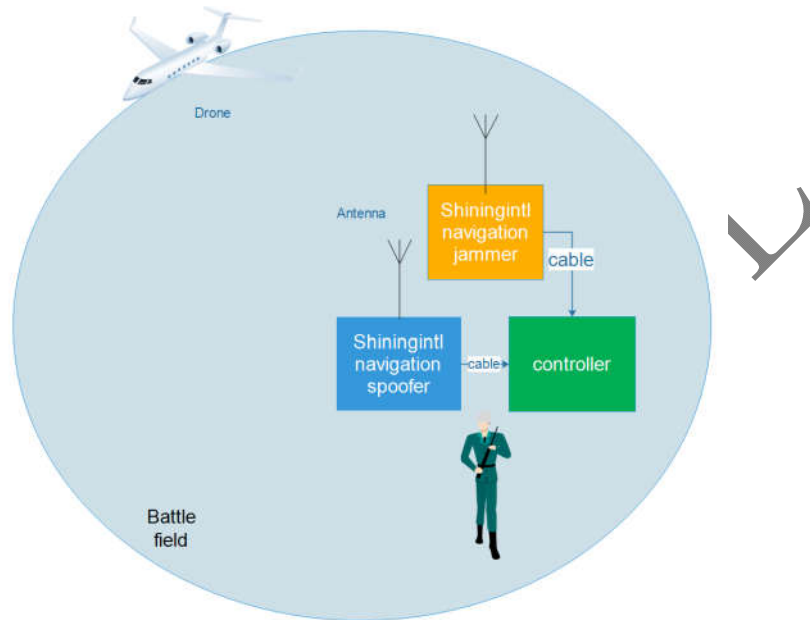

4. Remote safe control

In order to protect the operator from harm of drone or missile, this deployment design separates the shiningintl navigation deception equipment and the controller location, the equipment and the controller is connected with optical fiber, then the operator can be miles and several tens of miles away from the battle field.

Advantage: the operator can be far away from the battle field to keep safety

Disadvantage: need to install the optical cable before
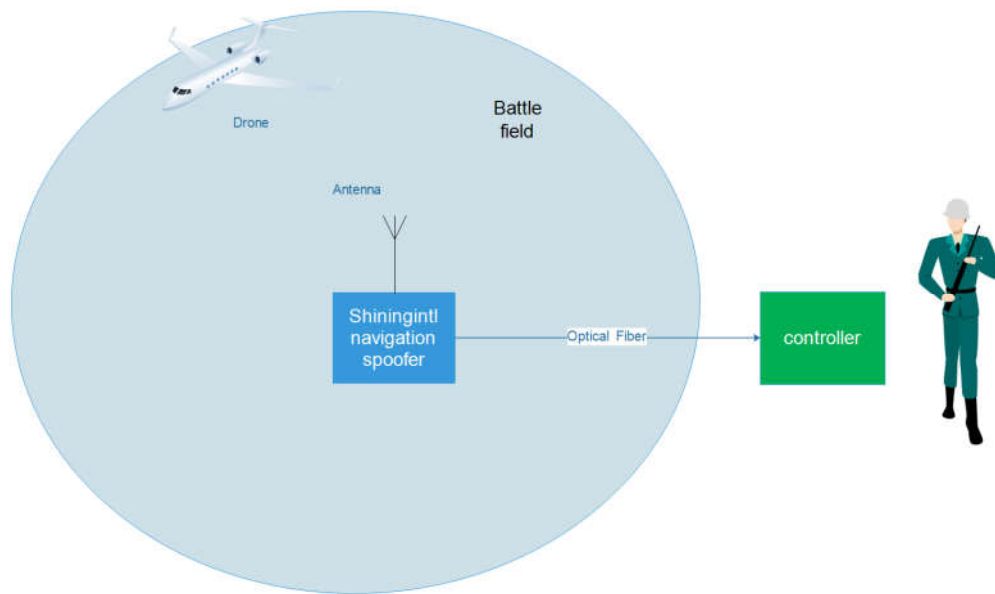
5. Remote safe control with Shiningintl jammer
   Combine the navigation spoofer and the navigation signal interference
   Advantage: higher reliability and safety
   Disadvantage: need to install the optical cable before
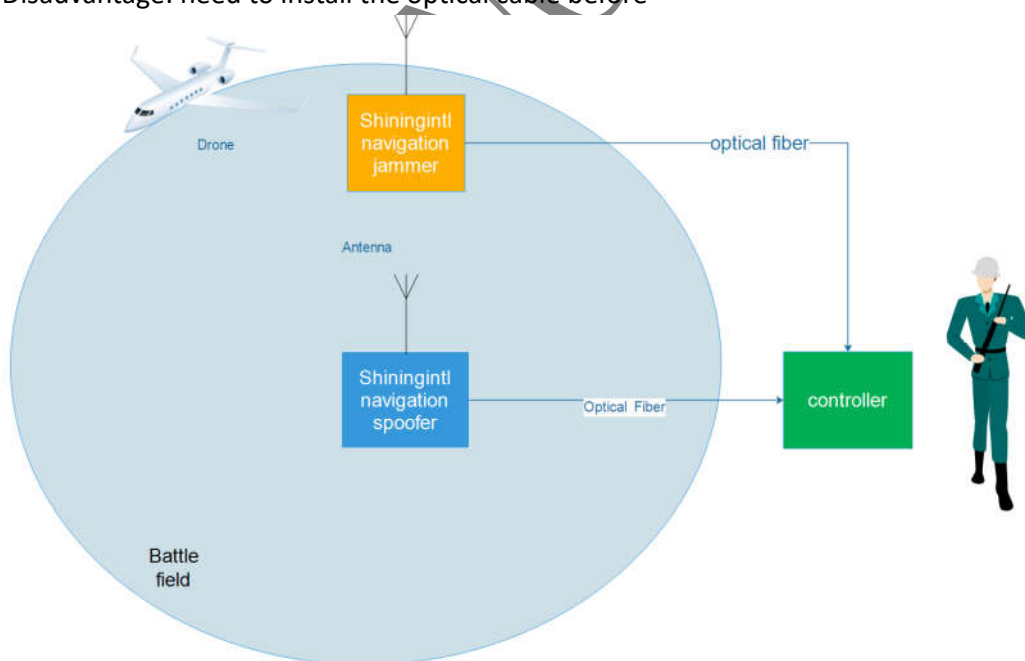
6. Remote multi spoofer with Shiningintl jammer
   If the drones install latest anti-inteference antenna, they may identify the navigation signal has problem comparing to the real signals, in order to overcome this problem, you can combine multiple spoofers and jammer, in this case, you can choose this deployment design as below.
   Advantage: can provide the higher reliability and safety, the drone

anti-interference function can't work, and the protected area will be safe.
Disadvantage: the cost will be higher