GPS SPOOFING AND MITIGATION STRATEGY

BY

D R DEEPAK VENGATESH
ARVIND P JAYAN
PAVARAKSHANA DHEVI S

WHAT IS GPS SPOOFING?

GPS spoofing is an active attack in which transmitters mask themselves as GPS satellites and intentionally send misleading signals such that the position computed by a GPS receiver on receiving such counterfeit signals is wrong , and the integrity and accuracy monitoring code on that receiver does not detect the fault.

HOW TO DO IT?

The spoofing of GPS signal is done by placing a phony receiver in the proximity of the actual navigation device . The fake receiver masks itself as the actual receiver and receives the GPS signal and then this co-ordinates are modified and then sent to the actual device . The actual device receives these fake signals taking it for the real ones .

TYPES OF SPOOFING
(FROM LITERATURE)

- **Software code spoofing** - a receiver is uploaded with malware and the receiver appears to function normally ; the receiver's location is then altered via the modified software.

- **Differential Corrections Spoofing -** where a Digital Corrections System (DCS) signal is spoofed. The problem with this is that DCS is used to enhance the location of the receiver's location to 1-3 meters, so a DCS spoofing attack would be limited to those 1-3 meters .

- **GPS Signal Constellation Spoofing -** this uses a GPS signal generator to produce a navigationally consistent signal set which is similar to the actual satellite generated signals.

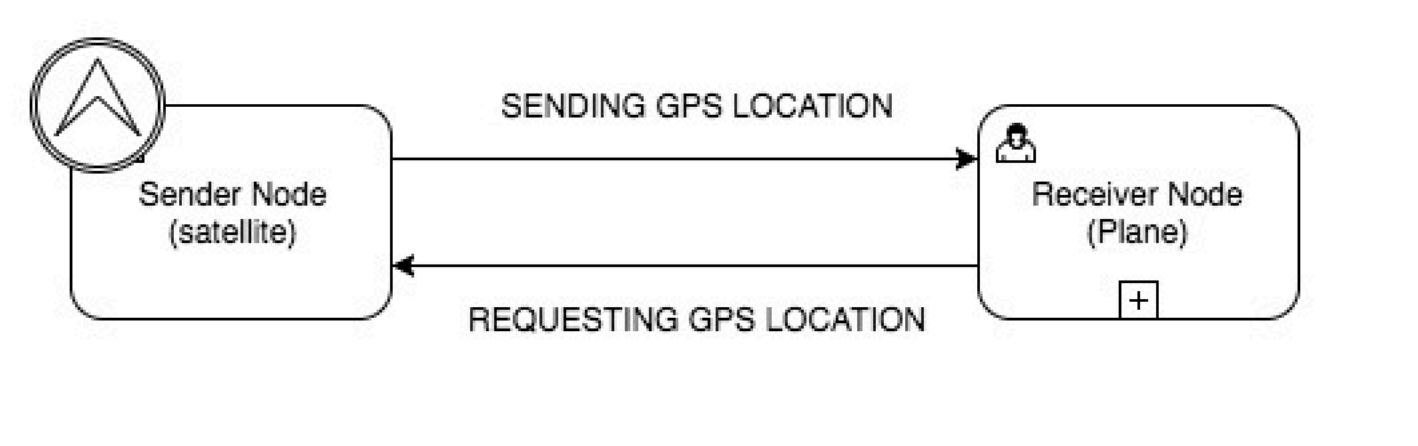
EXISTING MITIGATION STRATEGIES

- Monitoring the absolute and relative signal strength of the received signal from different satellites.
- Monitoring the satellite signal codes and the number of satellite signals received.
- Checking the time interval between each of the received satellite signal because the signals from different satellites usually take different times to reach the receiver . If all the signals come at a single instant then there is a chance that the signals are fake which is being sent by a satellite simulator.
- Using inertial sensors to plot the receiver’s trajectory and comparing this data with the received signals to verify it’s correctness.

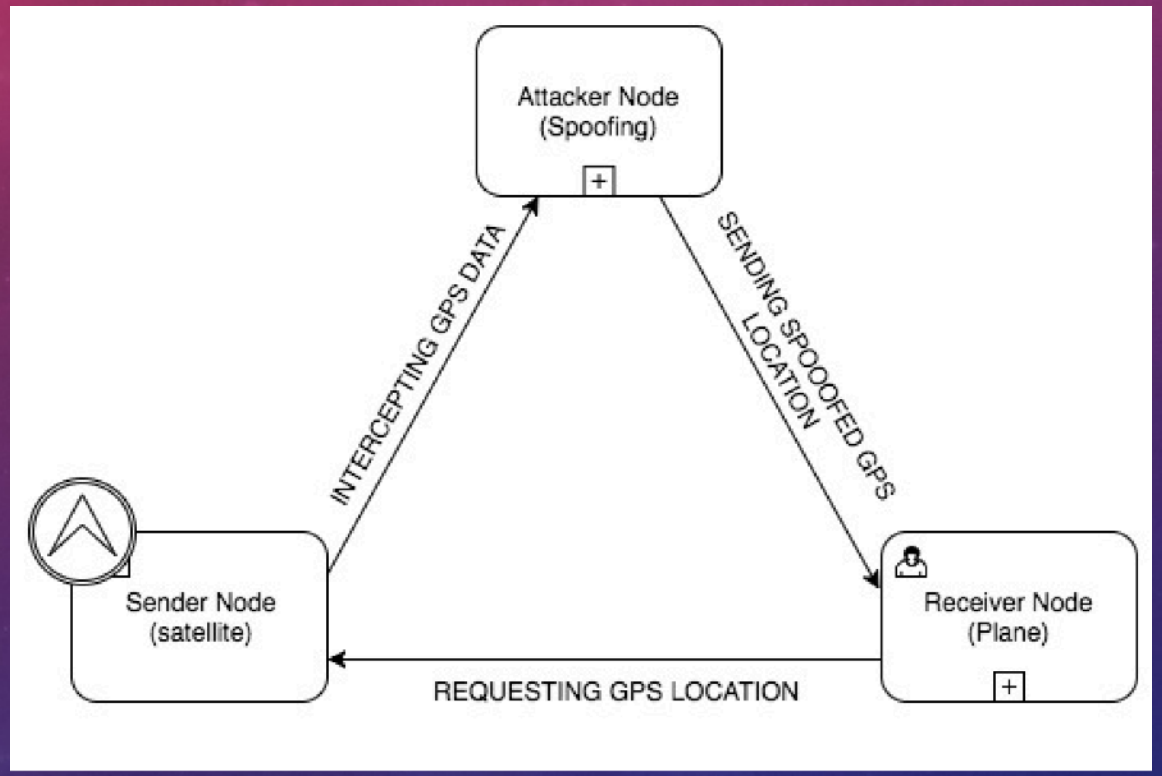
OUR IDEA

Our model for spoofing would be using 3 nodes – a sender , a receiver and an attacker . The attacker will target the authentication details of the sender and mask the spoofed data and re-transmit it to the receiver .

ACTUAL ARCHITECTURE



SPOOFING ARCHITECTURE



OUR MITIGATION STRATEGY

We will be using an open source public key cryptosystem like NTRU which is a light weight protocol . This system has proven to be having significantly better performance . This will help in quick and efficient authentication .

COST BENEFIT ANALYSIS

- We won’t be changing the physical aspects of the navigation system by using non – cryptographic techniques like increasing the number of antennas or changing the wavelength of the signal which would result in changes to the cost, size of receivers .
- Using cryptographic techniques helps us reduce the cost of setting up this system .