**Paper: Security of GPS/INS based On-road Location Tracking Systems**

**Summary**:

The paper discusses how GPS being vulnerable to signal spoofing attacks can use Inertial Navigation Systems (INS) as a complementary system, especially in road transportation. It evaluates the security guarantees of INS-aided GPS tracking and navigation and develops algorithms to achieve the goal of traveling to alternate locations without being detected. The algorithms render gyroscope and accelerometer sensors useless and demonstrate the active spoofing of the magnetometer using controlled coils. The article shows that it is possible for an attacker to reach destinations as far as 30 km away without being detected and proposes countermeasures to limit an attacker's ability. The system can be used to counter such attacks by detecting and recommending paths that are difficult to spoof. This is done by introducing algorithms that generate spoofed paths and based on these results, generate the space paths as well using the intuition that paths passed by the former algorithm would avoid detection by INS tracking systems.

**Strengths**:

1. The paper tests usage of algorithm in real time, over different factors like routes and cities to support the claims stated, this bolsters the claims of the proposed solution.
2. Since analog circuitry is more difficult to spoof, this gives protection against DoS attacks entirely and a fair protection against spoofing / relay attacks.
3. The countermeasures suggested to prevent spoofing rely on basic idea of reducing the detours possible for attacker, thus being effective in lowering chances that spoofing succeeds.

**Weakness**:

1. The algorithm 1 for giving list of potential spoofed paths in scoring method assumes road curvature and turn angles for maximizing score but doesn’t take into consideration real time events like weather fluctuations and traffic which might potentially affect the optimum path returned.
2. The memory requirements for having to store space paths to be used for generating spoofed paths is also something to consider when deciding between performance vs memory tradeoff.
3. In real world cases, the driver might not travel on the predetermined route as given by the gps, they do follow their intuition and knowledge which may lead to GPS re-routing. In these cases the spoofing technique wont work.