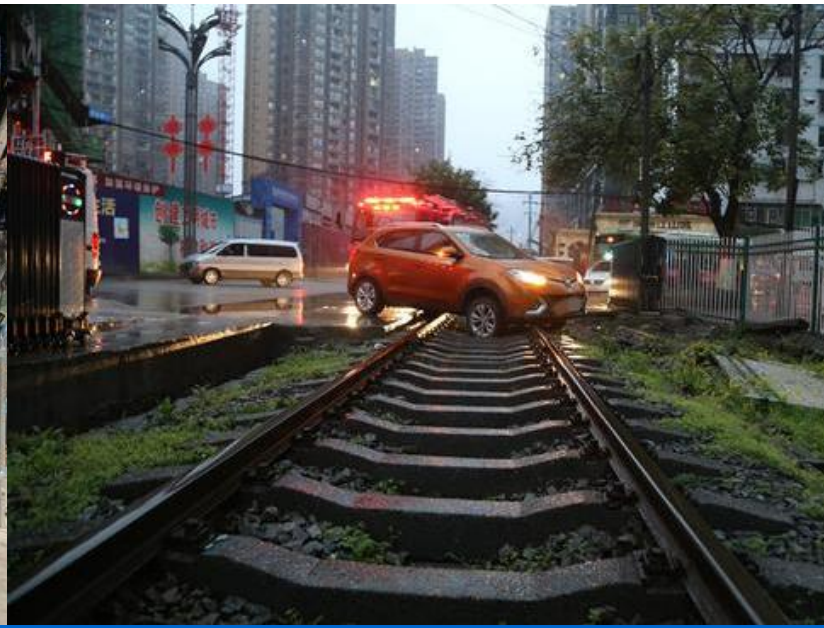
All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems

Curtis Zeng[1], **Shinan Liu**[2], Yuanchao Shu[3], Dong Wang[1]
Haoyu li[1], Yanzhi Dou[1], Gang Wang[1], Yaling Yang[1]

[1]Virginia Tech; [2]UESTC; [3]Microsoft Research

Microsoft Research

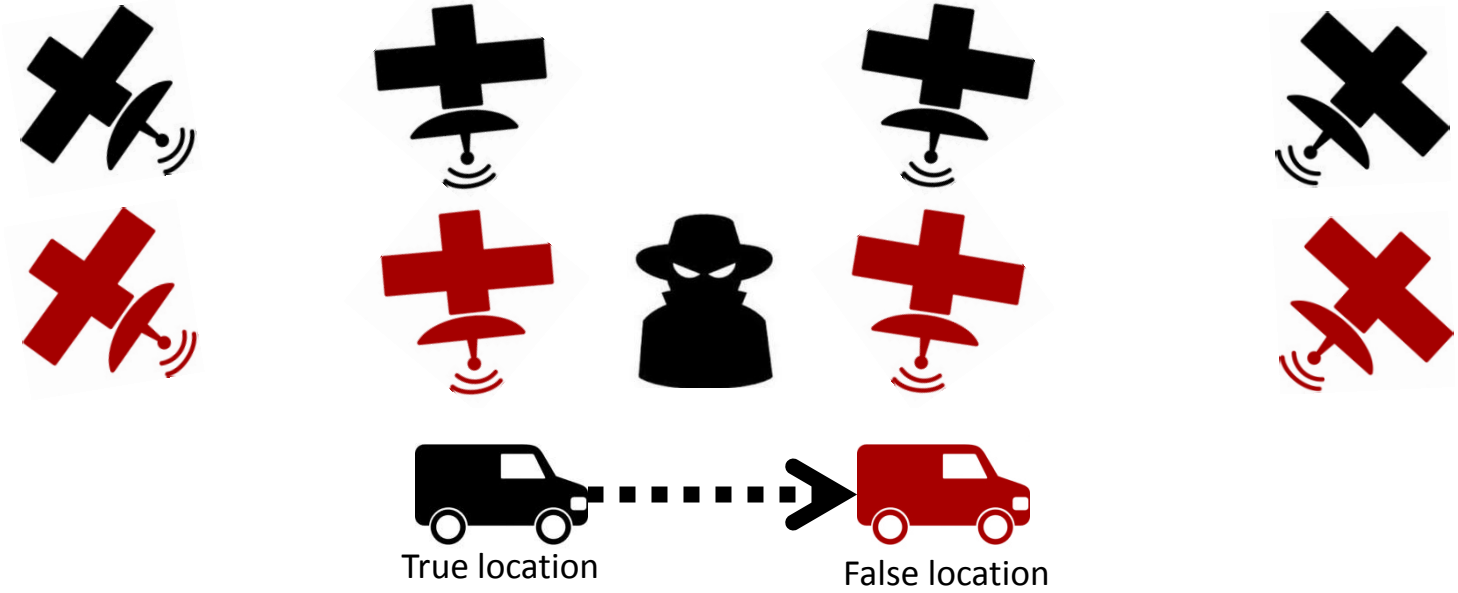
GPS Navigation: Billion Users



GPS malfunction can really lead to real-world consequences

Known Threat: GPS Spoofing

- Civilian GPS is vulnerable to spoofing attacks due to the lack of authentication mechanisms



GPS Spoofing in Free Space

In 2012, a drone was diverted in White Sands, New Mexico

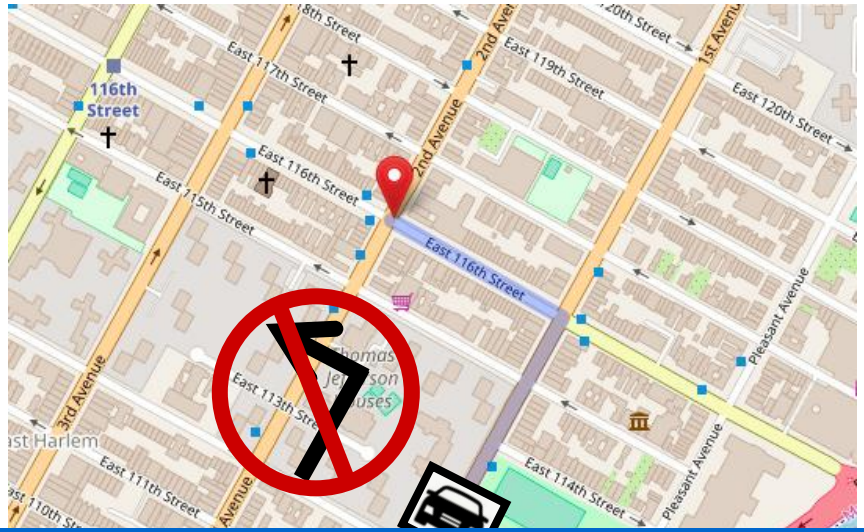
In 2013, a yacht was diverted on the way from Monaco to Greece

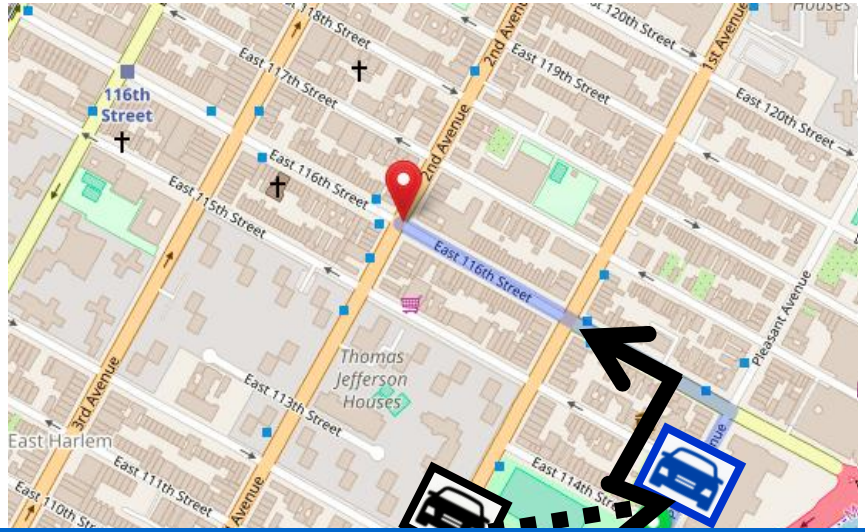
Successfully diverted in open air/on open water

Spoofing Road Navi: Challenging

Real world 

Navigation map 





"Turn left" - physically impossible instruction!

Challenges

- Random/naïve manipulations do not work
  - Cannot cope with road constraints, e.g., road shape, speed limit
  - Create physically impossible routes

- Human driver in the loop
  - Need to avoid alerting human drivers (stealthy)

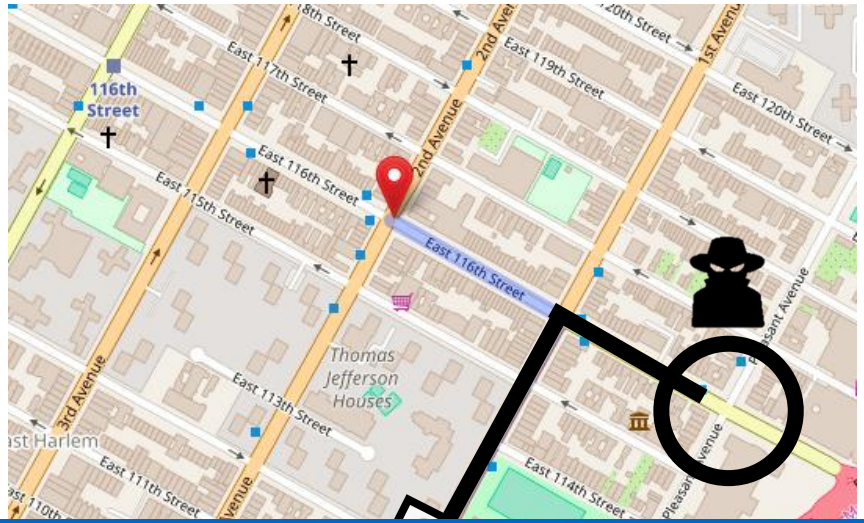
First to explore the feasibility of such attack

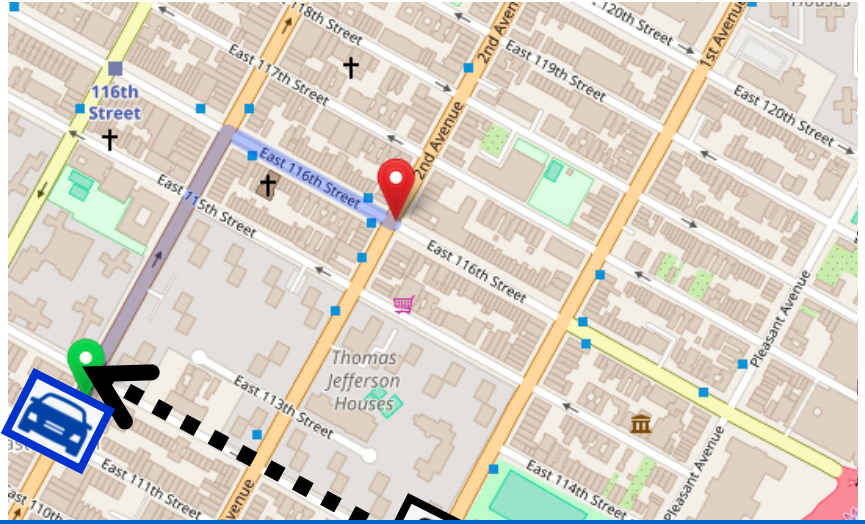
What is the stealthy attack ?

Stealthy Attack

Real world

Navigation map





Navigation instructions lead to attacker's pre-defined location

Concepts & Core Idea

Real world 

Navigation map 

Assumption: know rough destination area or checkpoint

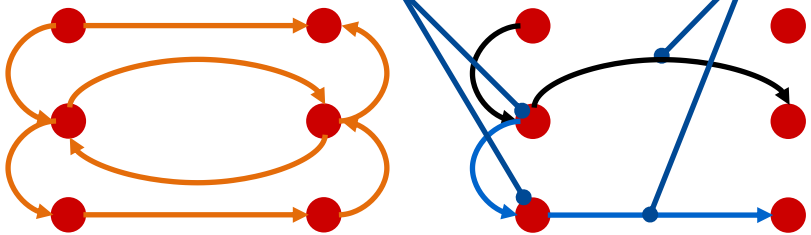
Goal: find ghost route to mimic the shape of victim route

Route Searching Algorithm

Goal: find ghost route to mimic the shape of victim route

Turn pattern matching

Concatenate victim routes



Map → Directed Graph → Exhaustive BFS

Iterative searching

Search ends whenever the attack goal is met

Attack Consequences

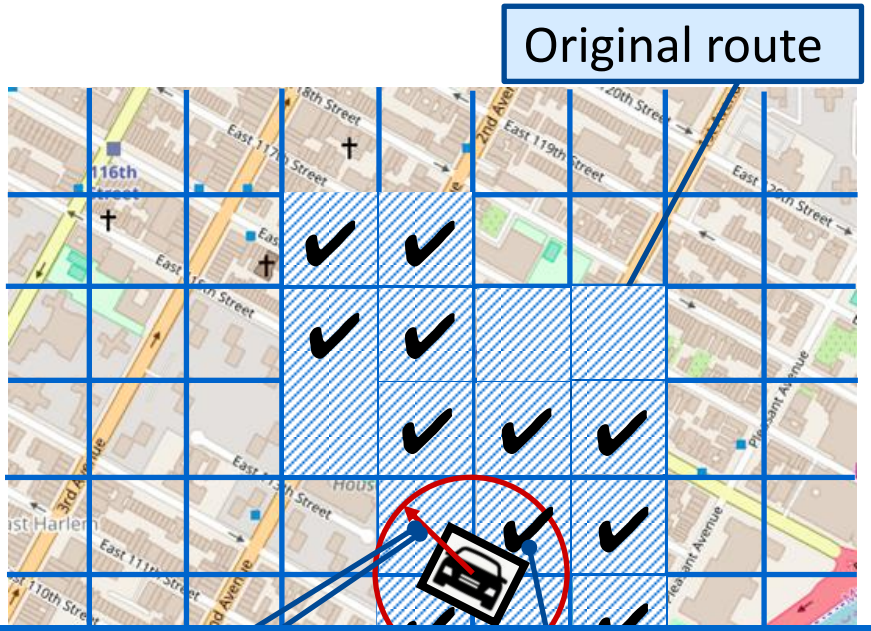
- Deviating: detour the victim with no specific target destination 
- Targeted deviating: divert the victim to bypass a pre-defined location 
- Endangering: divert the victim to dangerous situations like wrong-way driving on a highway 

Trace-driven Simulation Results

- 600 real-world trips randomly selected from New York City and Boston taxi datasets
  - Run basic attack and iterative attack (two iterations)
- Deviating: on average, 335 and 3507 qualified victim routes per trip
- Endangering: 599 out of 600 (99.8%) contains wrong-way road segments

A wide range of attack opportunities & real danger

Targeted Deviating Results

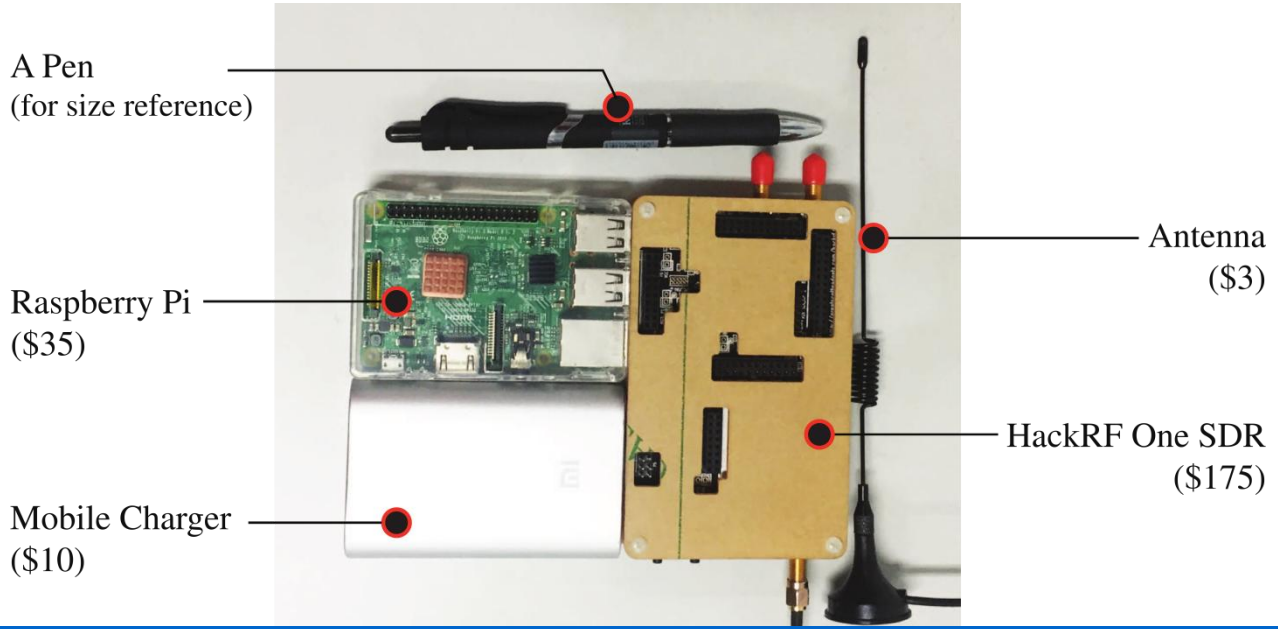


- Evaluation metric: *hit rate*
  - How likely a pre-defined location is feasible
  - # diverted / # candidate
- Results: 70% median hit rate with 500m radius in Manhattan

Even random pre-defined locations are highly reachable

Is the attack feasible in real world?

Low-cost Portable GPS Spoofer ($223)



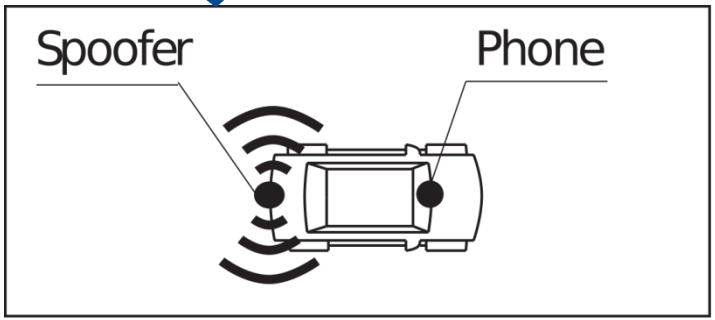
Open-source hardware & software

Legal Permission & Ethics

- Experiments exclusively done in China with temporary legal permission from local authority and local IRB approval (#17-936)
- Controlled measurements at outdoor parking lot
  - After midnight with no one around
  - Spoofing signals do not affect outside
- Real-world driving
  - After midnight with minimum traffic
  - Min tx power (-40 dBm) + attenuators (-30 dBm) + car body shielding (-15 dBm) + two-meter propagation loss (-42.41 dBm) = not affected (-127.41 dBm)

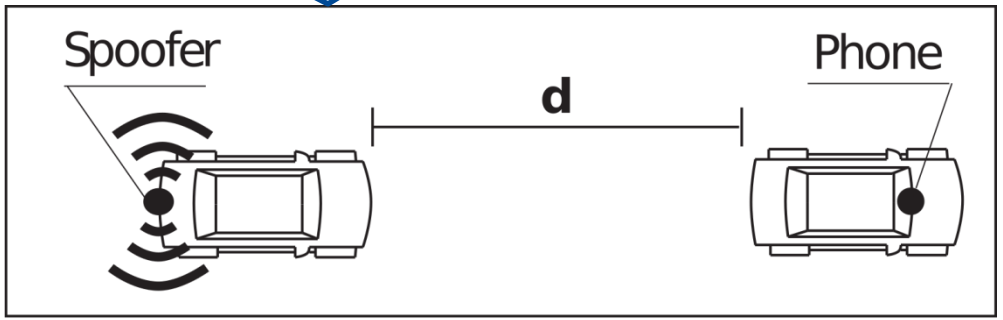
Controlled Measurements

- Average takeover time: around 40 seconds



Hide spoofer on the victim car

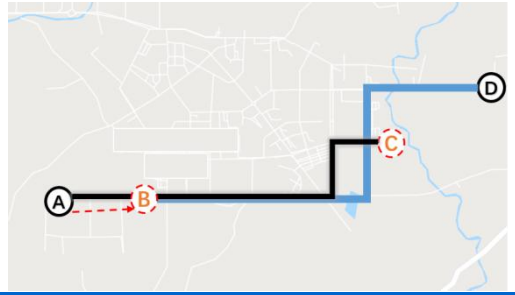
- Takeover distance: 40-50 meters
- Consistent signal lock-on while driving



Carry spoofer and tailgate the victim car

Real-world Driving

- Attack setup: same-car (no real users involved)
  - One author drives a Ford Escape and strictly follows navigation instructions from Google Maps
  - The other author attacks from the backseat



Trigger instructions in time and divert to 2.1 & 2.5 km away

Can human user detect it?

User Study with Driving Simulator

- Let users drive in a simulator
  - They play truck drivers to “deliver packages” from location A to B
  - See if they can be diverted without noticing the attack
  - [illegible] can/cannot detect the attack

Experiment setup

Simulator view

Google Street View

More details and demo video link in the paper

Key Results

- Attack success rate: 95% (38 out of 40)
  - Two users detect it by cross-checking surrounding environment and navigation map to find inconsistency
    - Highway vs. local way
- Users are more likely to use GPS in unfamiliar areas
  - Not enough pre-knowledge/time to check the inconsistency
- Most users experienced GPS malfunction in real life
  - Unstable GPS signal does not alert users

Discussions

- We explore the feasibility of stealthy manipulation of road navigation systems in three steps
  - Route searching algorithm, capability measurements & real-world driving, human-in-the-loop user study
- A potential defense inspired by the user study results
  - Using sensor fusion for cross-checking
  - Encryption, ground infrastructures, modifications for GPS receiver hardware/software have much higher cost and longer deployment cycle

Questions