Location Spoofing Attacks on Autonomous Fleets

Jinghan Yang

Autonomous Driving

- Bring personal convenience:
  - Personal freedom.
  - Saving money.
  - Safety

Autonomous Driving

- In a community level:
  - Saving parking space.
  - Need less cars in total.
  - Reducing traffic jam.

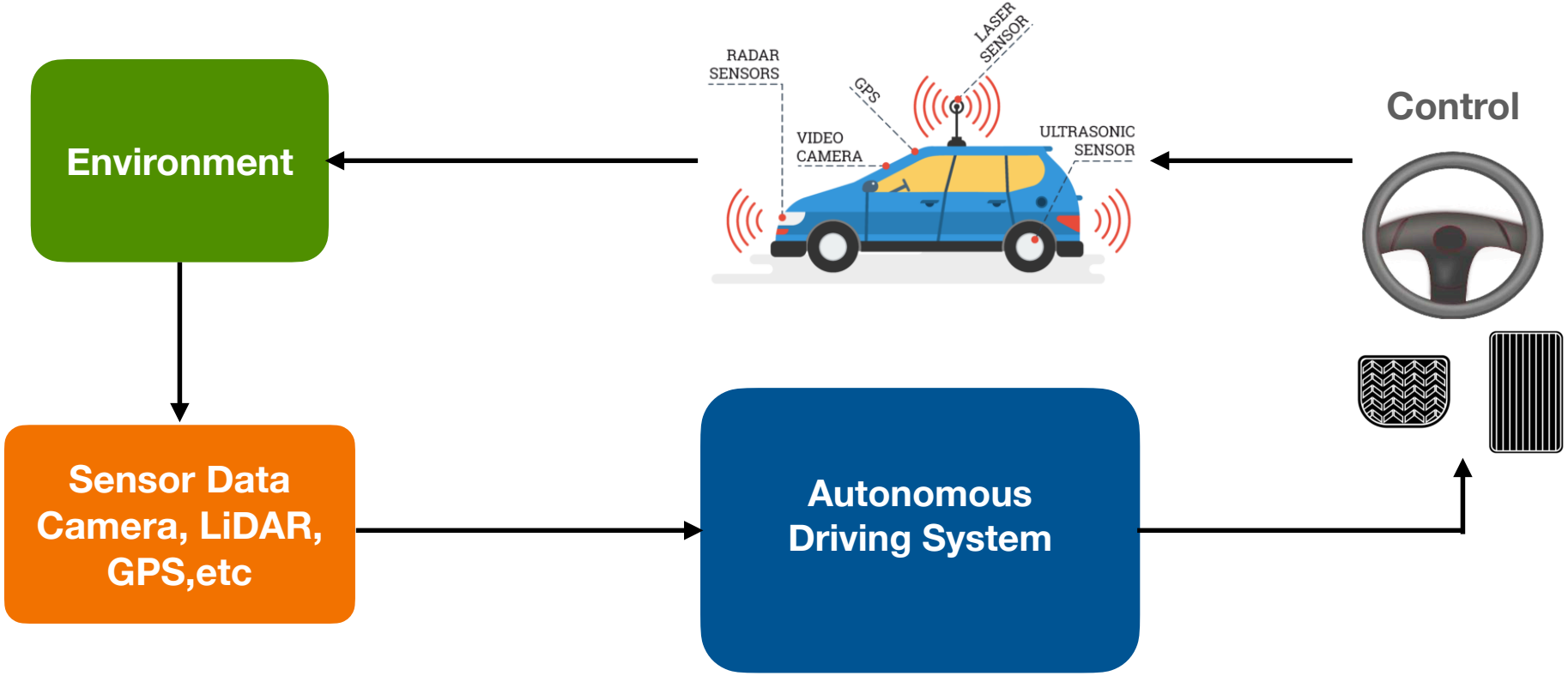
Ridesharing

Is Autonomous Driving Safe?

Is Autonomous Driving Vulnerable to Malicious Attacks ?

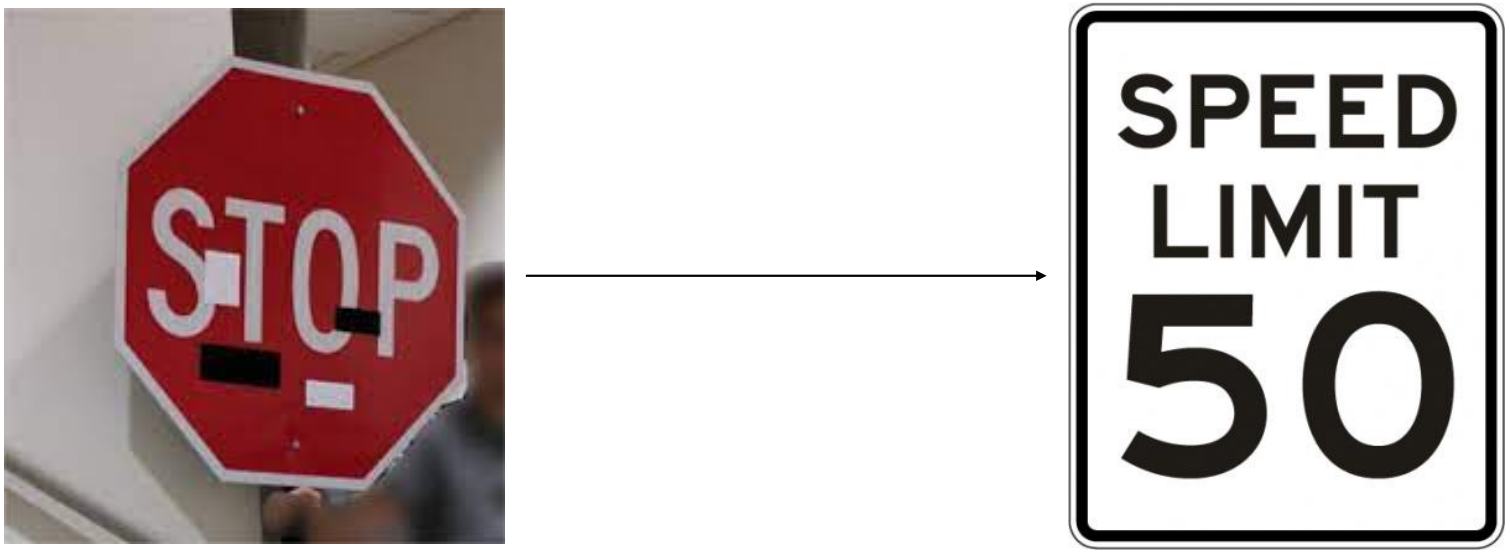
Can we make the autonomous driving car make mistakes ?

How does autonomous car work ?



Attack Autonomous Driving's Perception.

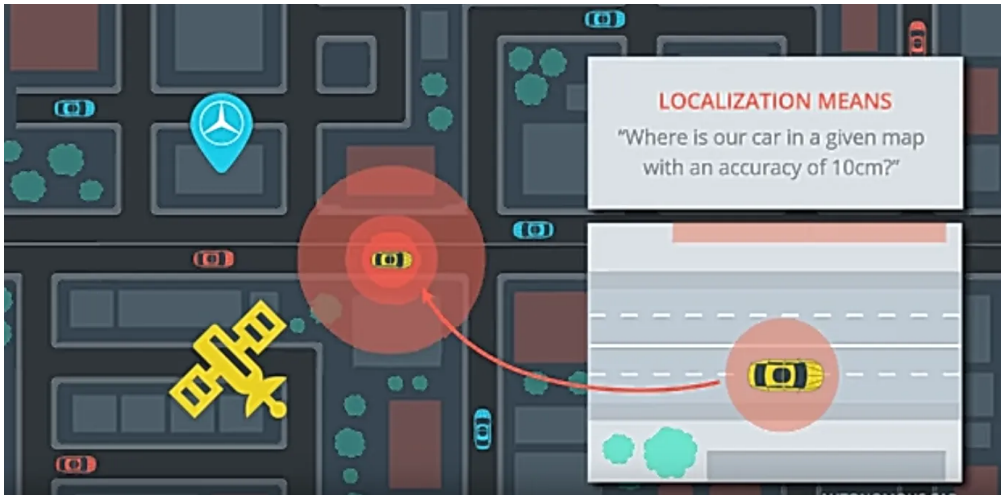
- Attack to the perception module



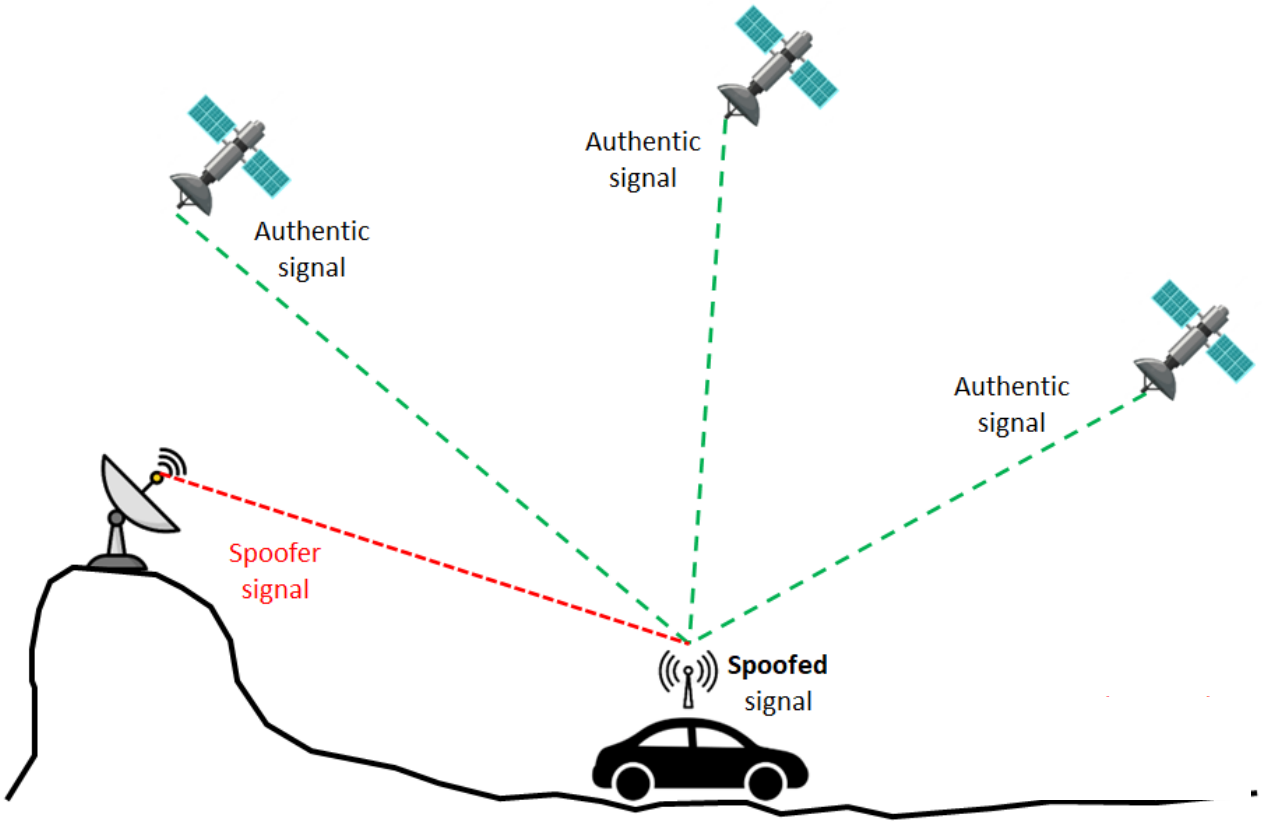
Is Autonomous Driving Vulnerable to Malicious Attacks ?

Is the autonomous driving's localization system also vulnerable to malicious attacks?

Autonomous Driving's (GPS) Localization



Attacking Devices: GPS Spoofers



A Practical GPS Location Spoofing Attack in Road Navigation Scenario. (Zeng et. al.)

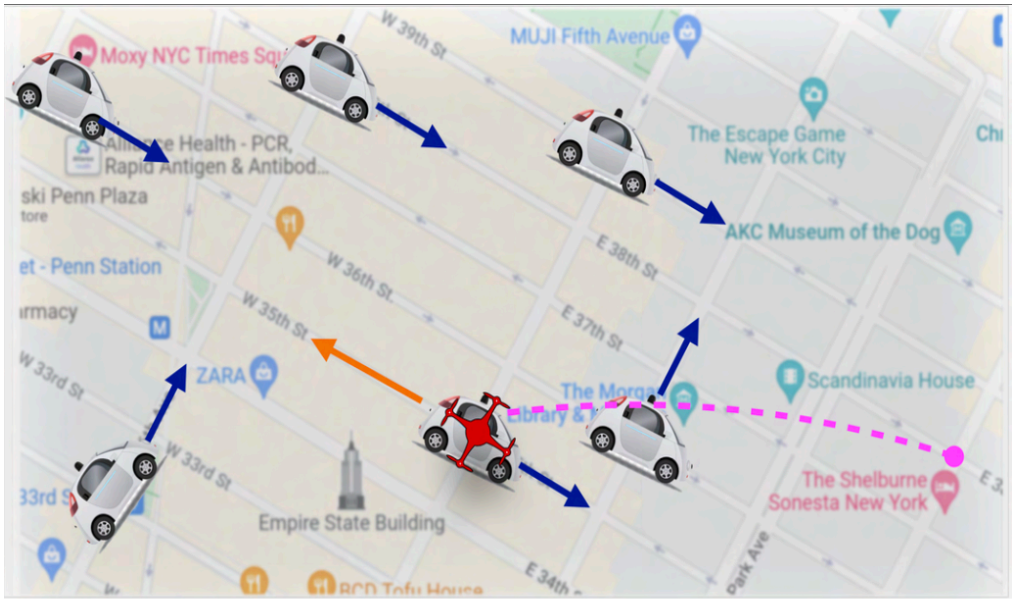
- Low-cost portable GPS spoofers.
- Lunch box size.
- Physically realized in New York.

A Practical GPS Location Spoofing Attack in Road Navigation Scenario. (Zeng et. al.)

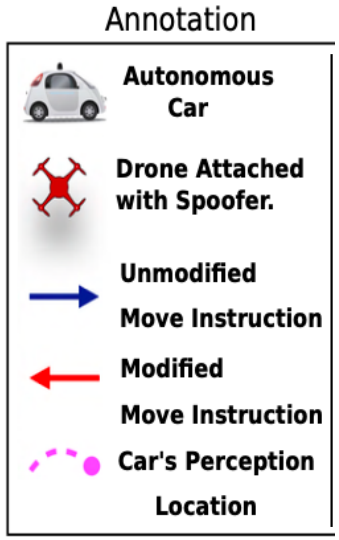
Original navigation route

On-route spoofed location

Attack An Autonomous Driving Fleet



Manhattan in New York



Attacks

- Two attack types:
  - Delay Attack
  - Service Failure Attack

Proposed Methods

Manhattan in New York

Attacking Pipeline

Proposed Methods

Static spoofers

$$\max_{x,y,M'} \sum_{k\in K}\sum_{i\in V}\sum_{j\in\mathcal{N}(i)} y^k_{i,j}\cdot c_{i,j} \tag{1a}$$

$$\sum_{j\in\mathcal{N}(i)} y^k_{j,i} = \sum_{u\in\mathcal{N}(j)} y^k_{j,u} \qquad \forall k\in\{1,\dots,K\}, i\in V : i\neq s_k, d_k \tag{1b}$$

$$\sum_{i\in\mathcal{N}(s_k)} y^k_{s_k,i} = \sum_{i\in\mathcal{N}(d_k)} y^k_{i,d_k} = 1 \qquad \forall k\in\{1,\dots,K\} \tag{1c}$$

$$y_{i,j} + y_{j,i} \leq 1 \qquad \forall\ i,j\in V \tag{1d}$$

$$M'_{i,u,\alpha} = \sum_{j\in V} M_{j,u,\alpha} x_{i,j} F_{i,j} + M_{i,u,\alpha}\cdot\left(1-\sum_j x_{i,j}\right) \forall i\in V,\alpha\in A \tag{1e}$$

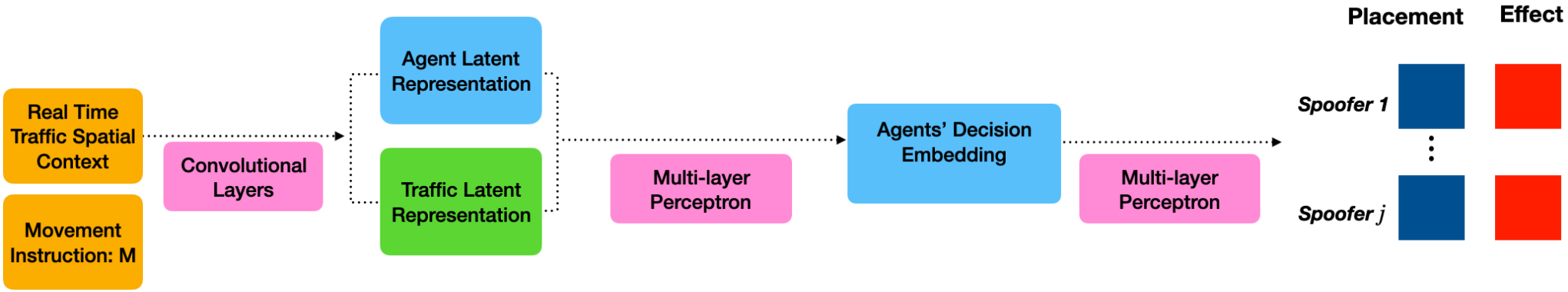
$$y^k_{i,i+\alpha} = \sum_{j\in\mathcal{N}(i)} y^k_{j,i} M'_{i,d_k,\alpha} \qquad \forall k\in\{1,\dots,K\}, i\in V\setminus s_k, \alpha\in A \tag{1f}$$

$$y^k_{s_k,s_k+\alpha} = M'_{s_k,d_k,\alpha} \qquad \forall k\in\{1,\dots,K\},\alpha\in A \tag{1g}$$

$$\sum_{i,j} x_{i,j}\leq B; \quad \sum_j x_{i,j}\leq 1 \quad \forall i\in V. \tag{1h}$$

Proposed Methods

Dynamic spoofers



Open streetMap and Uber Movement

- Geolocation information: Open streetMap
- Traffic: Uber Movement.
- Manhattan

Experiment Results

Spoofing Budget	#Target Cars	Travel Time	**Proposed** Delay Ratio	**Greedy** Delay Ratio	**Random** Delay Ratio
1	1	200	**0.90**	0.89	0.03
5	5	262	**2.0**	1.2	0.09
5	10	242.7	**1.11**	0.67	0.05
10	20	252	**1.0**	0.78	0.09

TABLE IV: The delay ratio in the *dynamic-dynamic* case in a $dist - 1000$ traffic network induced by spoof devices with spoofing radius 1.

Experiment Results