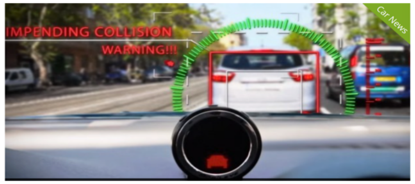
Sequential Attacks on Kalman Filter-based Forward Collision Warning Systems

Yuzhe Ma, Jon Sharp, Ruizhe Wang, Earlence Fernandes, Xiaojin Zhu

University of Wisconsin--Madison

The Forward Collision Warning System (FCW)



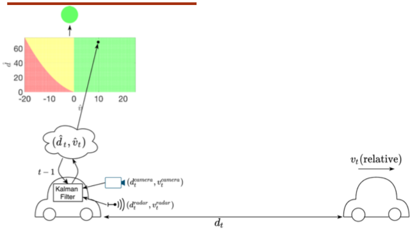
Widely-used in cars today

Represents a step towards autonomous driving

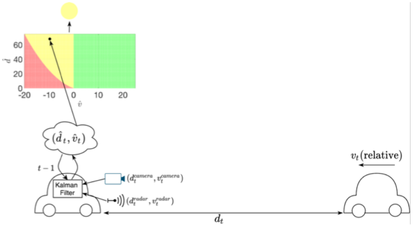
Integrate traditional control and recent ML techniques

Potential security issues not fully understood

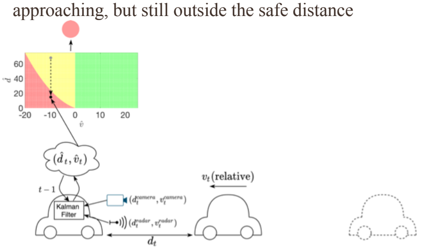
Normal FCW Process



No Danger (green light) Car in front of us is moving away



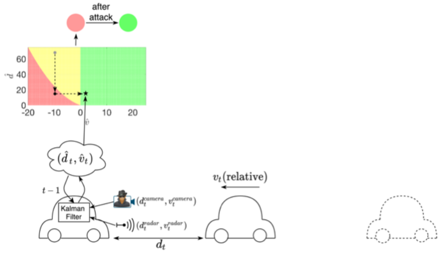
Potential Danger (yellow light): Car in front of us is approaching, but still outside the safe distance



Imminent Collision (red light): Car in front of us is approaching, and is already within the safe distance

Attack Setting

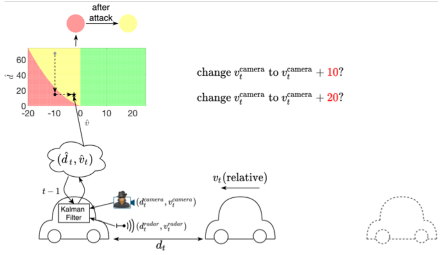
Attack Goal: the attacker aims at changing the warning light produced by the FCW system



Attacker Ability: the attacker can directly manipulate the measurements produced by the camera sensor

Attacker Knowledge: the attacker has full knowledge of the FCW system under attack

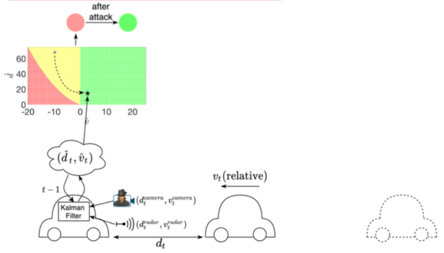
Instantaneous Attack


after attack
60
40
20
0
-20
-10
0
10
20
change v_t^{camera} to $v_t^{camera}+10$?
change v_t^{camera} to $v_t^{camera}+20$?
$(\hat{d}_t, \hat{v}_t)$
$t-1$
Kalman Filter
$(d_t^{camera}, v_t^{camera})$
$(d_t^{radar}, v_t^{radar})$
v_t(relative)
d_t

Attack happens right before the target time step

Successful attack requires large change to measurements due to Kalman Filter smoothing

Sequential/Continuous Attack



Attacker continuously manipulate camera measurements from the beginning until the target time step

Advantage of Sequential Attacks

(More feasible)

Can satisfy physical constraints, e.g., distance in [0m,80m], velocity in [-20m/s, 20m/s]

(More effective)

Exploit the sequential nature of the FCW system

(More stealthy)

Spread the manipulation more evenly over time

Sequential Attack Formulation

$$\min_{\delta_t} \quad J = \sum_{t\in\mathcal{T}^a} \delta_t^\top R\delta_t, \qquad (1)$$

$$\text{s.t.} \quad \tilde{y}_t = y_t + \delta_t, \forall t \in \mathcal{T}^a, \qquad (2)$$

$$\tilde{x}_t = A(I - H_{t-1}C)\tilde{x}_{t-1} + AH_{t-1}\tilde{y}_t, \qquad (3)$$

$$\delta_t^i = 0, \forall i \in \mathcal{I}_{\text{radar}}, \forall t \in \mathcal{T}^a, \qquad (4)$$

$$\|\delta_t\| \le \Delta, \forall t \in \mathcal{T}^a, \qquad (5)$$

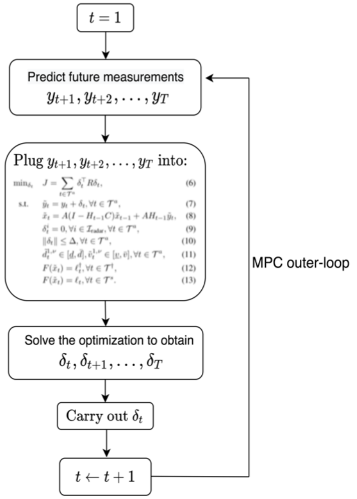
$$\tilde{d}_t^{1,\nu} \in [\underline{d}, \bar{d}], \tilde{v}_t^{1,\nu} \in [\underline{v}, \bar{v}], \forall t \in \mathcal{T}^a, \qquad (6)$$

$$F(\tilde{x}_t) = \ell_t^\dagger, \forall t \in \mathcal{T}^\dagger, \qquad (7)$$

$$F(\tilde{x}_t) = \ell_t, \forall t \in \mathcal{T}^s. \qquad (8)$$

Problem: the future measurements y_t cannot be observed at the moment of attack

Plan Attack with Model Predictive Control (MPC)

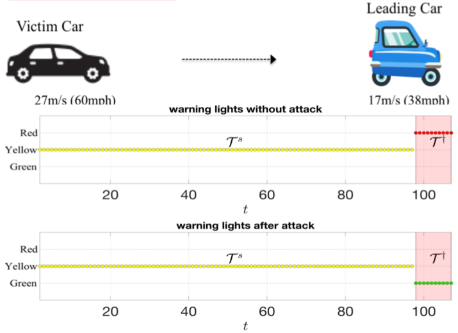

$t = 1$
Predict future measurements $y_{t+1}, y_{t+2}, \dots, y_T$
Plug $y_{t+1}, y_{t+2}, \dots, y_T$ into:
$\min_{\delta_t} \quad J = \sum_{t\in\mathcal{T}^a} \delta_t^\top R\delta_t,$ (6)
s.t. $\tilde{y}_t = y_t + \delta_t, \forall t \in \mathcal{T}^a,$ (7)
$\tilde{x}_t = A(I - H_{t-1}C)\tilde{x}_{t-1} + AH_{t-1}\tilde{y}_t,$ (8)
$\delta_t^i = 0, \forall i \in \mathcal{I}_{\text{radar}}, \forall t \in \mathcal{T}^a,$ (9)
$\|\delta_t\| \le \Delta, \forall t \in \mathcal{T}^a,$ (10)
$\tilde{d}_t^{1,\nu} \in [\underline{d}, \bar{d}], \tilde{v}_t^{1,\nu} \in [\underline{v}, \bar{v}], \forall t \in \mathcal{T}^a,$ (11)
$F(\tilde{x}_t) = \ell_t^\dagger, \forall t \in \mathcal{T}^\dagger,$ (12)
$F(\tilde{x}_t) = \ell_t, \forall t \in \mathcal{T}^s.$ (13)
Solve the optimization to obtain $\delta_t, \delta_{t+1}, \dots, \delta_T$
Carry out δ_t
$t \leftarrow t+1$
MPC outer-loop

Predict future measurements, plan attack, carry out the current manipulation, and enter the next MPC iteration

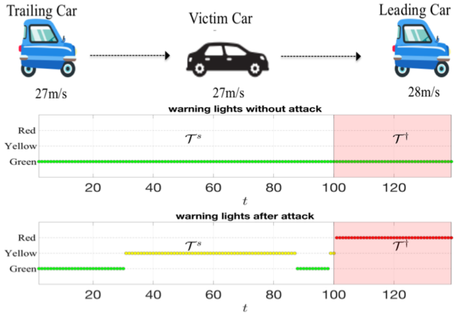
Experimental Setup

We use Carla to simulate real-world driving scenarios

Scenario I: MIO-10



Scenario II: MIO+1



Our Attack Causes Car Collisions

MIO-10

MIO+1

Website: https://sites.google.com/view/attack-kalman-filter

Contact: ma234@wisc.edu