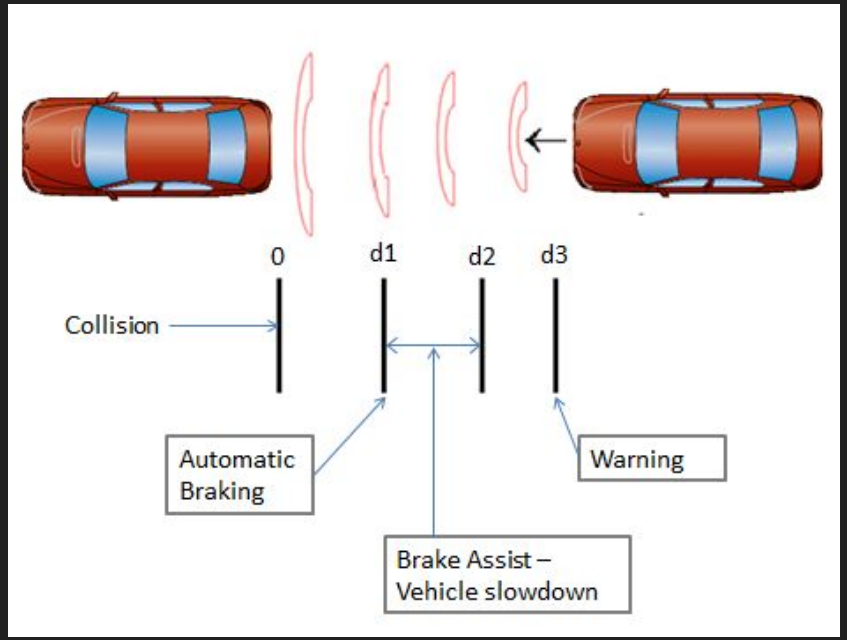
Stealthy Attacker Complexity in Cyber-Physical Systems

Research Proposal by Uday Shankar

CPS: combined software and mechanical components

- Example: automatic emergency braking system
- Model: system and supervisor



Attacks are Dangerous!

- Attacker might send fake data to sensors
- Confuse the car’s sensors => crash??

Stealthy Attacks are VERY Dangerous!

- If errors can be detected (by supervisor), the car can just stop
- It’s important to understand such attacks

(Sufficiently powerful) attackers can always be stealthy.

- [Goes, Kang, Kwong, Lafortune; 2017] “Stealthy Deception Attacks for Cyber-Physical Systems”

The attacker must be quite powerful

- Attacker is modeled as a string-edit function
- Has the ability to insert/delete events (sensor readings)
- As many or few as it wants

Definition III.1. Given a system G and a subset $\Sigma_a \subseteq \Sigma_o$, an attacker is defined as a function $f_A : P(\mathscr{L}(G)) \times (\Sigma_o \cup \{\varepsilon\}) \rightarrow \Sigma_o^*$ s.t. f_A satisfies the following constraints:

- $f_A(\varepsilon, \varepsilon) \in \Sigma_a^*$;
- $\forall s \in P(\mathscr{L}(G)),\ e \in \Sigma_o \backslash \Sigma_a$: $f_A(s,e) \in \{e\}\Sigma_a^*$;
- $\forall s \in P(\mathscr{L}(G)),\ e \in \Sigma_a$: $f_A(s,e) \in \Sigma_a^*$.

What if the attacker is less powerful?

- Limited insertion/deletion ability
- Computational constraints
- Relative to the supervisor/controller of the system?

Comparing attacker and supervisor complexity

- How complex does an attacker/supervisor have to be to guarantee/prevent a stealthy attack?

Challenges

- Need to come up with motivating examples
- Notion of complexity that makes sense in this context is not well-studied

Summary

- Studying stealthy attacks on cyber-physical systems with Eunsuk Kang
- Stealthy attacks are very scary in safety-critical situations
- Comparing the relative complexity of attackers and supervisors