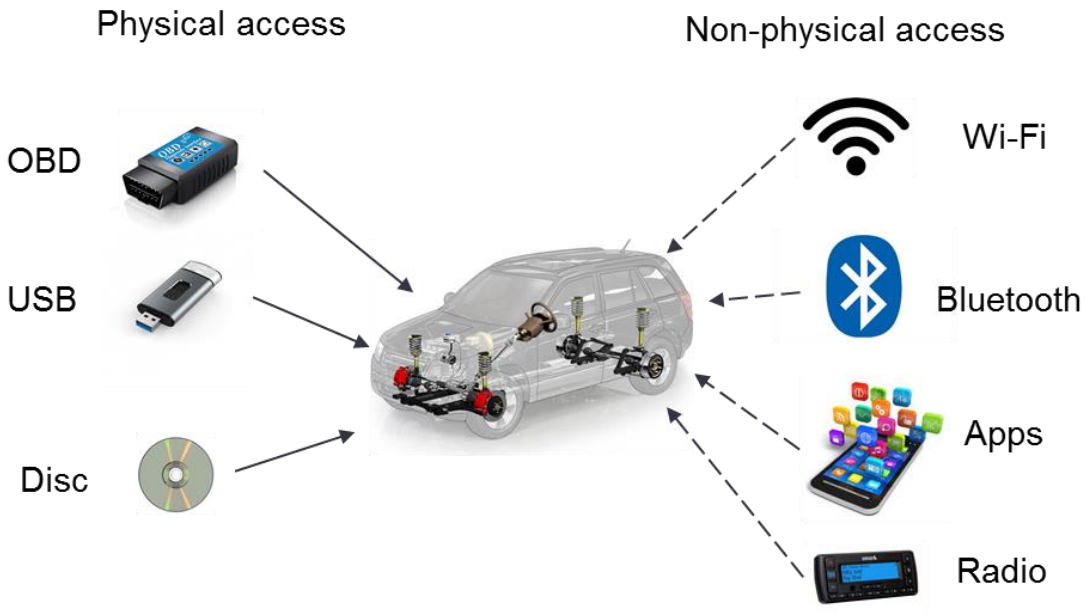
ICCCN 2020

Attack Detection and Mitigation for Sensor and CAN Bus Attacks in Vehicle Anti-lock Braking Systems

Liuwang Kang and Haiying Shen
Department of Computer Science, University of Virginia

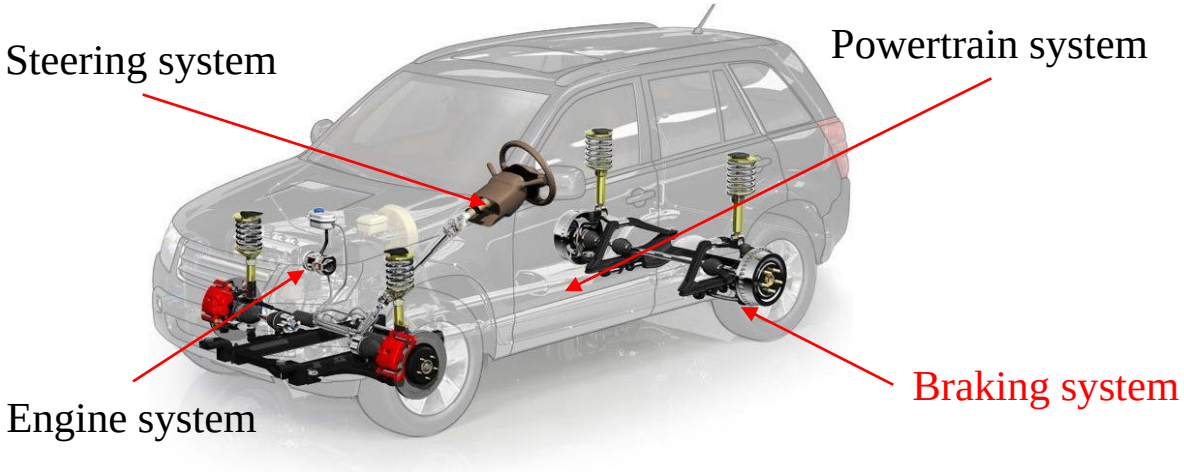
Background

Modern vehicles communicate with outside-vehicle environments through physical and non-physical accesses



Motivation

- Modern vehicles become vulnerable to attacks when communicating with outside-vehicle environments
- Vehicle systems under the attack may fail to work and affect vehicle driving safety

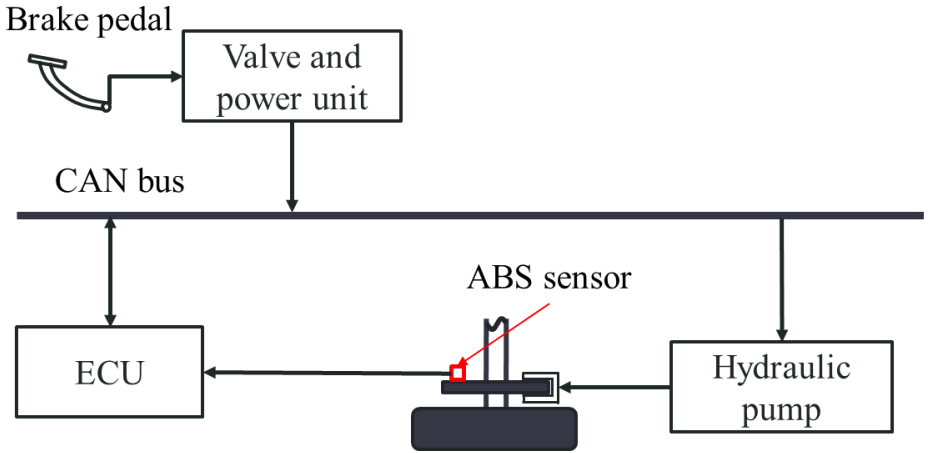


Anti-lock Braking System (ABS)

- Ensure slip ratio in the low region [0,0.2] during the braking process

$$\text{Slip ratio} = 1 - \frac{wheel\ radius * wheel\ speed}{vehicle\ speed}$$

- Avoid the wheel-lock phenomenon (driving direction is out of control and the slip ratio is outside of the low region during the braking process)

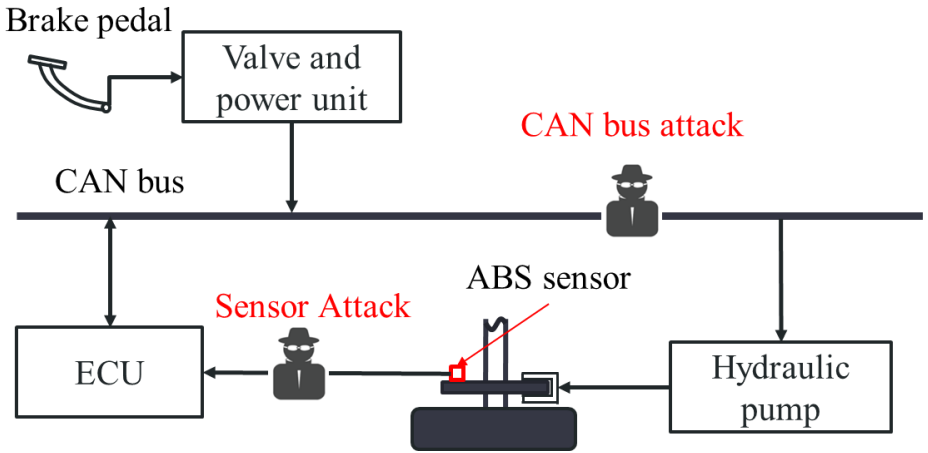


Attacks on ABS

- Ensure slip ratio in the low region [0,0.2] during the braking process

$$\text{Slip ratio} = 1 - \frac{wheel\ radius * wheel\ speed}{vehicle\ speed}$$

- Avoid the wheel-lock phenomenon (driving direction is out of control and the slip ratio is outside of the low region during the braking process)

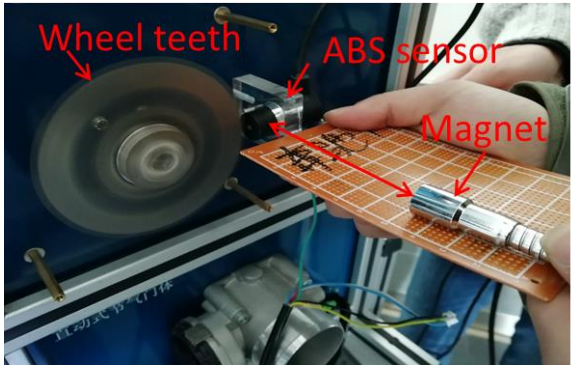


Sensor Attack in Vehicle ABS

Conducted by placing a magnet near the ABS sensor to modify sensor readings

The sensor reading under the ABS sensor attack contains:

- Real wheel speed
- Sensor measurement noise
- Wheel speed attack change



CAN Bus Attack in Vehicle ABS

Injects malicious brake force messages into CAN bus through on board diagnostics (OBD) port

	Arbitration field					Data field			
SOF	ID	RTR	IDE	r0	DLC	Data	CRC	ACK	EOF
1 bit	11 bit	1 bit	1 bit	1 bit	4 bit	0 to 64 bit	16 bit	2 bit	7 bit

A CAN bus attack can be divided into:

- **Malicious message injection attack (MIA):**

  - Sends random brake force message into CAN bus

- **Message suspension attack (MSA):**

  - Sends the maximum brake force message into CAN bus

Related Work

Detect sensor attacks with an interval-based method (IBM) [CSUR'16]

Basic idea:

Builds the sensor model to simulate the sensor operation and generate the interval of all possible values for a given physical variable

Condition:

Sensor readings are outside of the interval

Shortage:

Fail to work when sensor attacker modifies sensor readings at small levels

Related Work

Detect CAN bus attacks with a signal-arrival-time based method (SBM) [PCISR'17]:

Basic idea:

Exploit the regularity of a CAN bus message and model its average signal-arrival-time

Condition:

Arrival time of a CAN bus message is not the same as its average signal-arrival-time

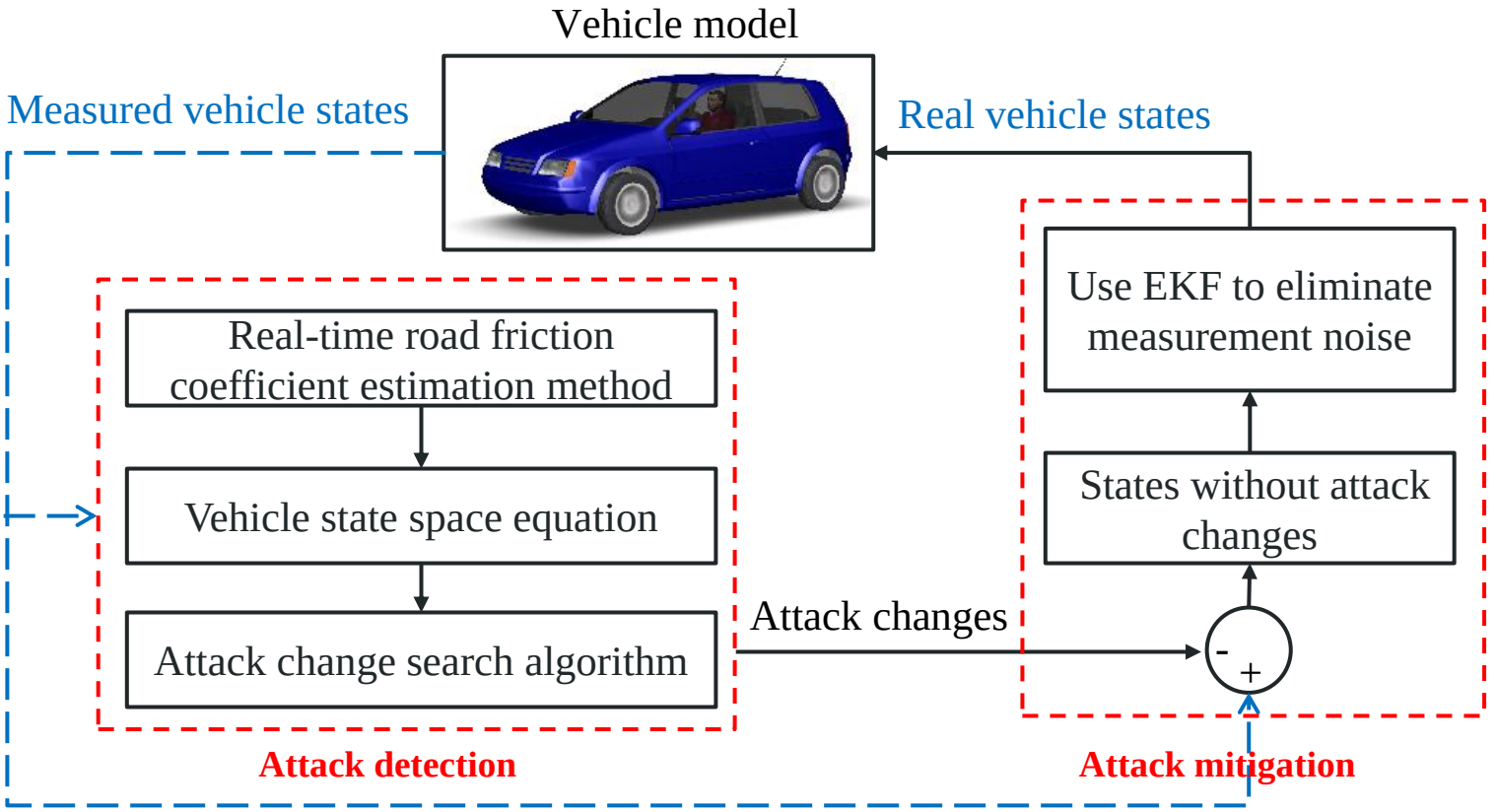
Shortage:

Attack detection accuracy highly depends on CAN bus message samples

Challenges

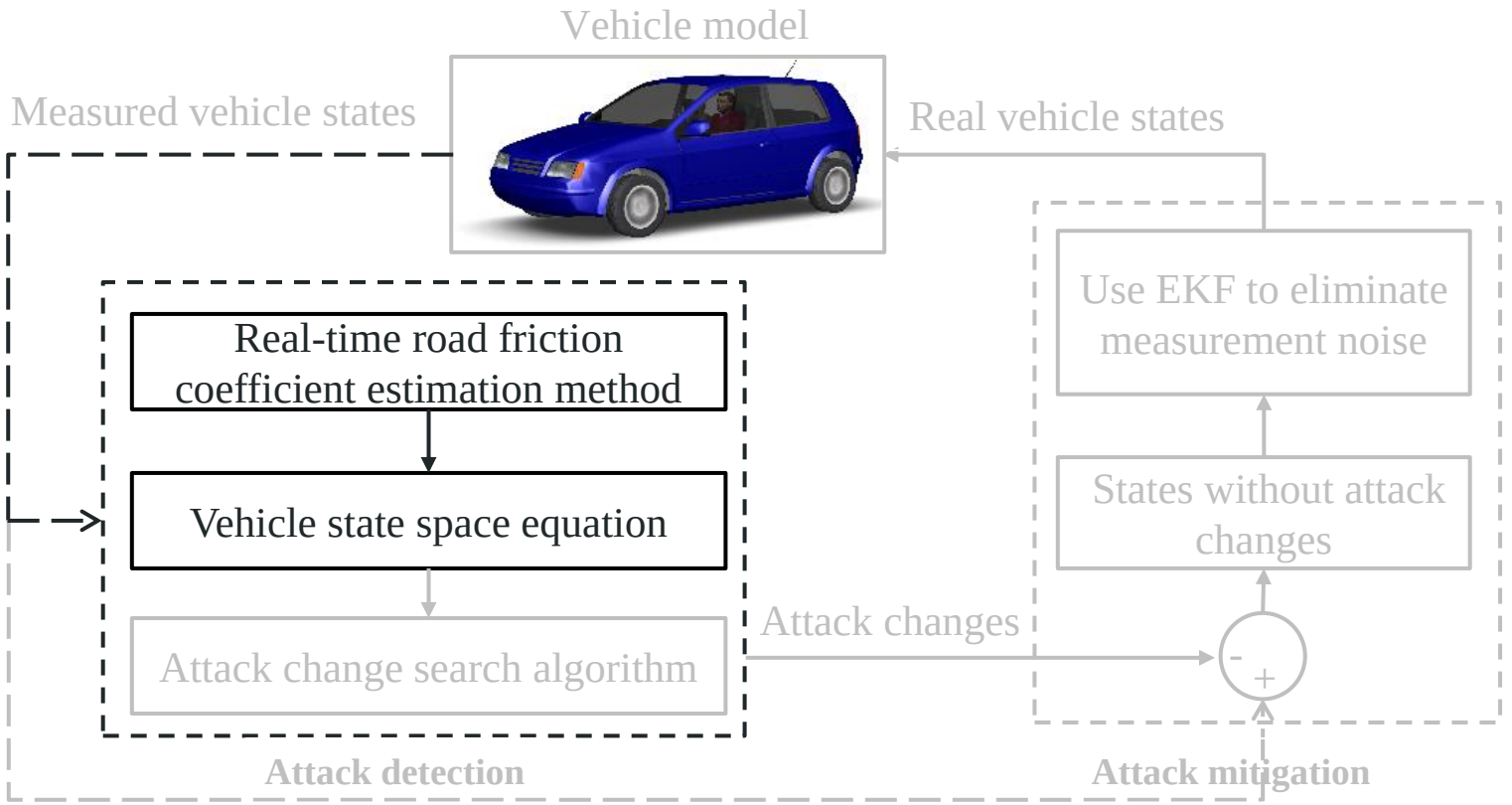
- How to accurately detect both sensor attacks and CAN bus attacks in the vehicle ABS?
- How to mitigate the effects of the detected attack on the vehicle ABS?

Attack Detection and Mitigation System



Attack change: value change of wheel speed or brake force because of sensor attacks or CAN bus attacks

Attack Detection and Mitigation System



Vehicle Brake Model

Vehicle state space equation

- Predict wheel speed

$$w(t+\Delta) = w(t) - \frac{F_L(t)r}{J_w}$$

- Predict brake force

$$F_L(t+\Delta) = \sigma\big(\lambda(t), \mu(t)\big)F$$

where $\sigma(\lambda,\mu) = \frac{C\lambda}{(\lambda+1)F} - \frac{C|\lambda|\lambda}{3\mu F^2(\lambda+1)^2} + \frac{C\lambda}{(\lambda+1)F}$.

r: Wheel radius

J_w: Wheel rotational inertia

F_L: Brake force

μ: Road friction coefficient

F: Vehicle weight

C: Tire stiffness

$\lambda = \frac{v-rw}{v}$: slip ratio calculation

v: Vehicle speed

μ changes greatly for different road conditions in practice

Vehicle Brake Model

Real-time road friction coefficient estimation method

$$\sigma(\lambda,\mu)=\frac{C\lambda}{(\lambda+1)F}-\frac{C|\lambda|\lambda}{3\mu F^2(\lambda+1)^2}+\frac{C\lambda}{(\lambda+1)F}$$

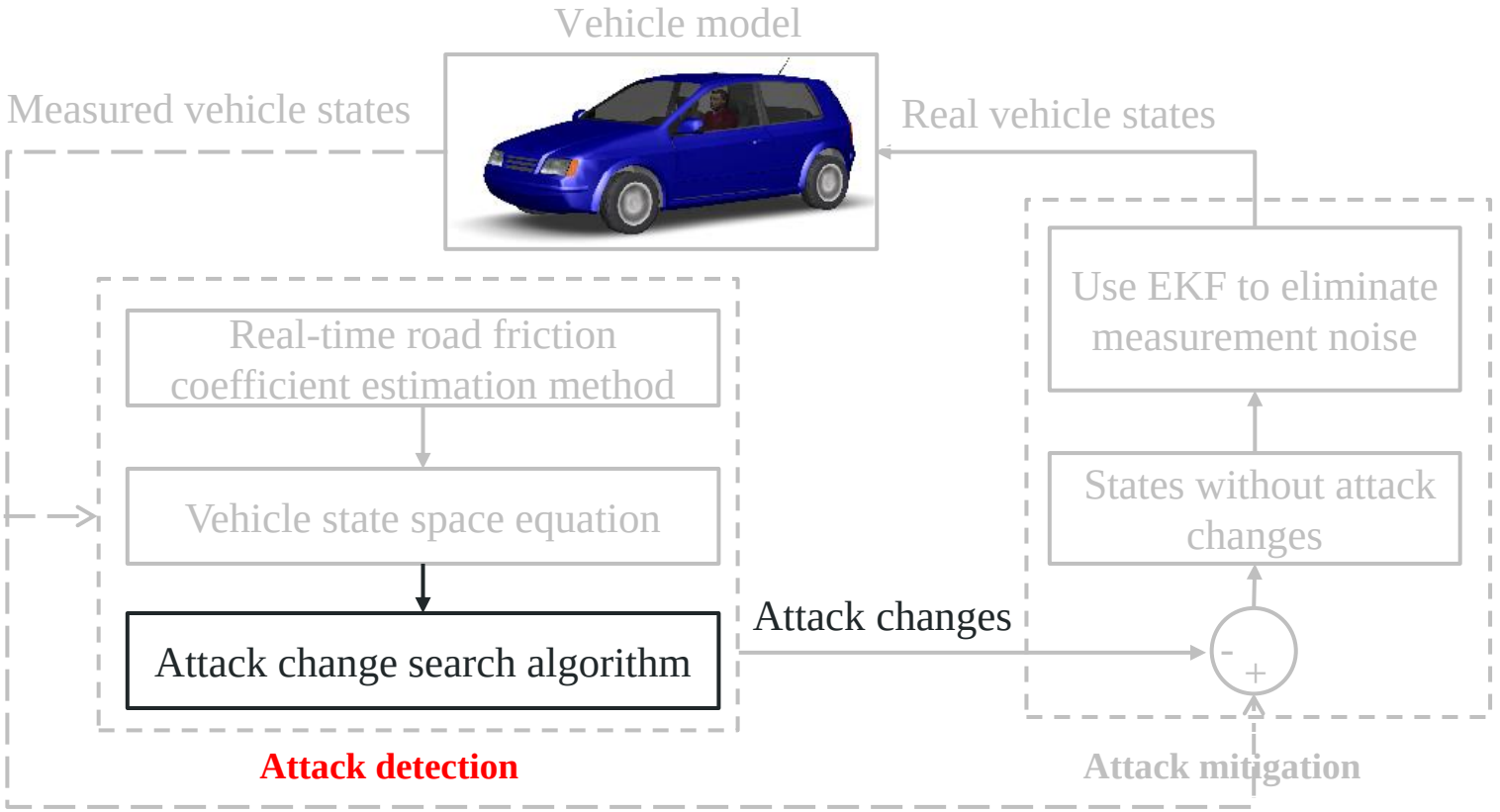
Firstly multiplied by vehicle weight F and then derived into

$$F_1=\begin{bmatrix}C & \frac{-C^2}{3\mu} & \frac{C^3}{27\mu^3}\end{bmatrix}\begin{bmatrix}\lambda & \frac{\lambda^2}{F} & \frac{\lambda^3}{F^2}\end{bmatrix}^T$$

F_1: equals to brake force when vehicle brakes and driving force when vehicle accelerates

F_1, λ, F and C are known, road friction coefficient μ can be estimated in real time

Attack Detection and Mitigation System



Attack Change Search Algorithm

Attack change optimization problem:

Given sets of historical measured vehicle states $\hat{X}$, attack change optimization problem is formed to determine attack changes $\emptyset$

$$\underset{X(t-\tau\Delta),\emptyset}{\operatorname{argmin}} \sum_{j=t-\tau\Delta}^{t} ||\hat{X}(j) - \tilde{X}(j) - \emptyset(j)\,||^2$$

Measured vehicle states $\hat{X}(j) = \begin{bmatrix} \hat{w}(j) \\ \hat{F}_L(j) \end{bmatrix}$

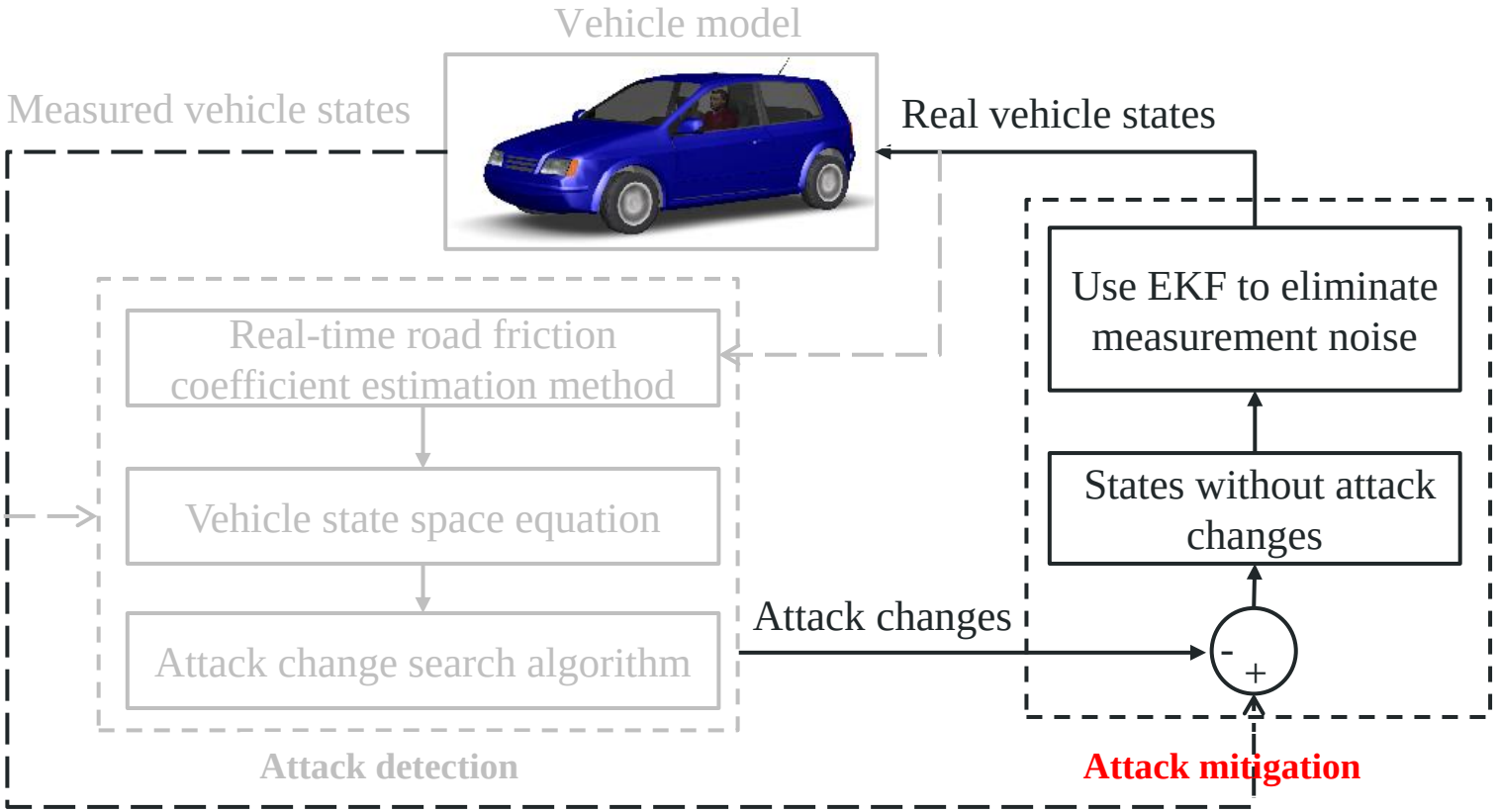
Predicted vehicle states $\tilde{X}(j) = \begin{bmatrix} \tilde{w}(j) \\ \tilde{F}_L(j) \end{bmatrix}$

Attack changes $\emptyset(j) = \begin{bmatrix} \emptyset_w(j) \\ \emptyset_{F_L}(j) \end{bmatrix}$

Solution: attack changes $\emptyset$ from $t - \tau\Delta$ to t

Attack changes $\emptyset$ are non-zero if the vehicle ABS is attacked

Attack Detection and Mitigation System



Attack Mitigation Part

Attack mitigation strategy:

1. Subtract attack changes ϕ from measured vehicle states $\hat{X}$ and use Extended Kalman Filter (EKF) to update final vehicle states $\tilde{X}$:

$$\tilde{X} = \tilde{X} + K(\hat{X} - \emptyset - \tilde{X})$$

where K is Kalman gain matrix in EKF and used to eliminate sensor measurement noise

2. Send final vehicle states $\tilde{X}$ to the hydraulic pump in the vehicle ABS

Performance Evaluation

Experiment settings: conduct vehicle ABS attack simulation using CarSim and MATLAB to evaluate our system

- Explore effects of Magnets on ABS sensor
- Test performance of our proposed system

Comparison methods:

- IBM [CSUR'16] for sensor attack detection
- SBM [PCISR'17] for CAN bus attack detection

Evaluation aspects:

- Attack detection accuracy
- Attack mitigation efficiency

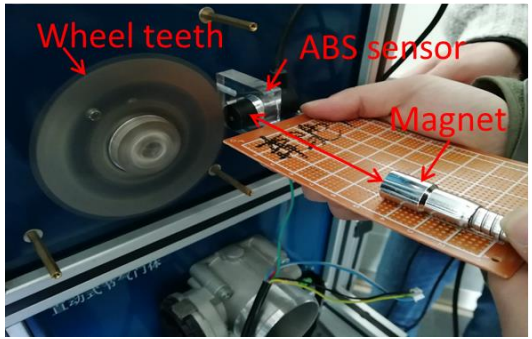
Demos

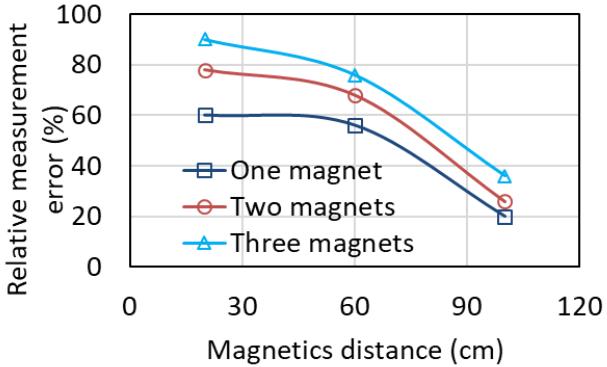
Magnet's Effects on ABS Sensor

We did real sensor attack experiments on one ABS sensor type (Bosch0201210):

- Record sensor readings when the distance changes
- Calculate relative measurement errors of the ABS sensor

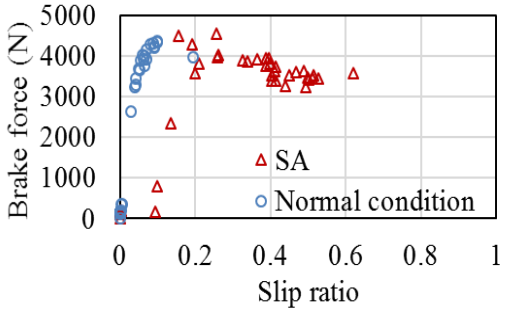
In sensor attack simulation, we use sensor readings when one magnet is 100cm away from the ABS sensor



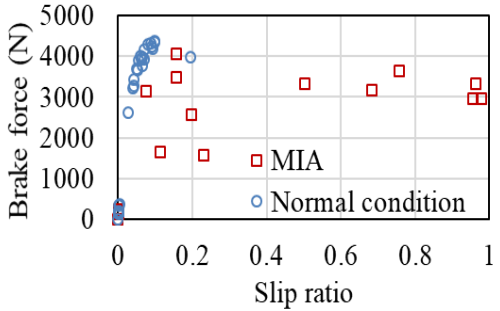


Evaluation of Attack Detection

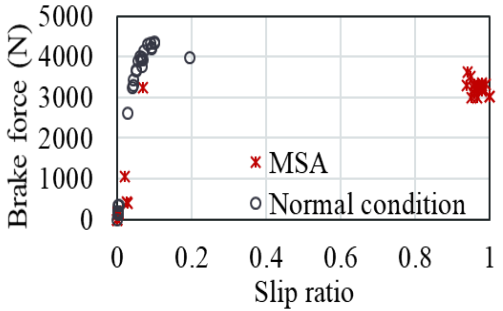
- When vehicle ABS is attacked by SA, MIA or MSA, the slip ratio is outside of the low region (0-0.2)
- The vehicle ABS fails to work and the wheel-lock phenomenon will happen



Slip ratio under SA



Slip ratio under MIA



Slip ratio under MSA

Evaluation of Attack Detection

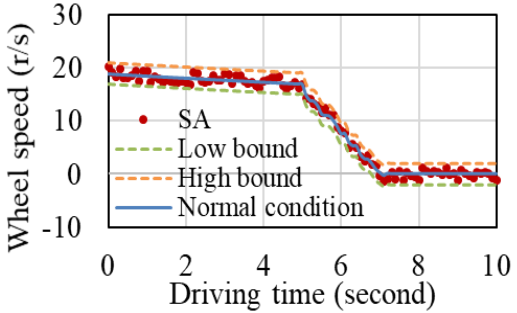
Detection results with existing methods (IBM and SBM):

- IBM fails to detect SA in vehicle ABS

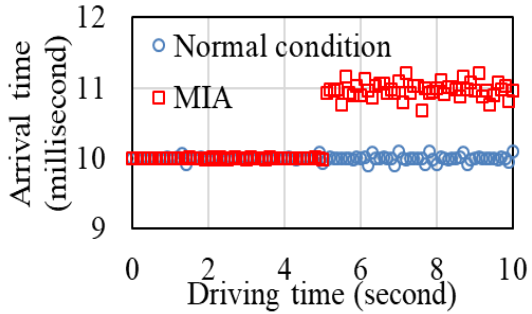
- The sensor reading is still in the interval of wheel speed

- SBM successfully detects MIA and MSA in vehicle ABS

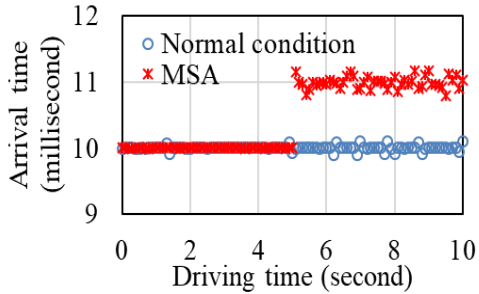
- Arrival-time of brake force messages is not the same as average arrival time



SA detection result with IBM



MIA detection result with SBM



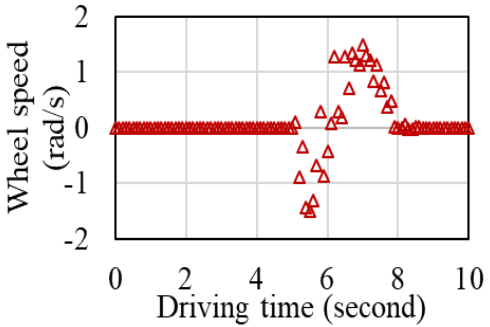
MSA detection result with SBM

Evaluation of Attack Detection

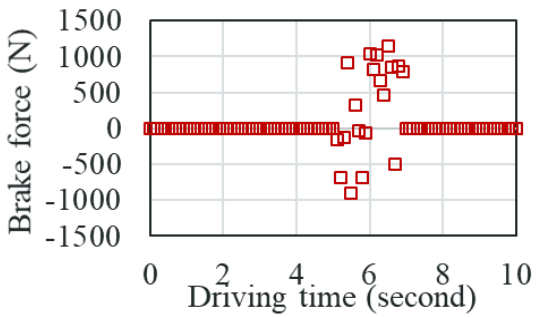
Detection results with our system:

- For SA situation, wheel speed attack change is non-zero
- For MIA and MSA situations, brake force attack change is non-zero

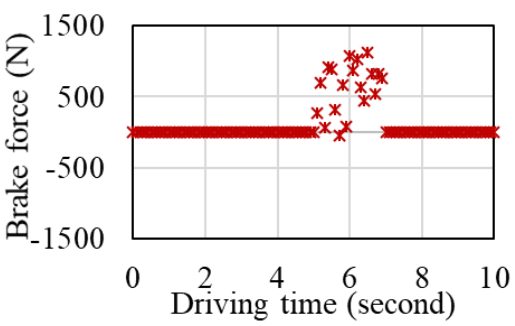
Our system successfully detects SA, MIA and MSA in vehicle ABS



Attack change under SA



Attack change under MIA



Attack change under MSA

Evaluation of Attack Detection

We simulated total 400 braking processes (300/400 attacked) to further test attack detection accuracy of our system:

- One type of attacks (SA, MIA and MSA) or no attack is launched randomly during the braking process
- IBM, SBM and our system are applied to detect these attacks

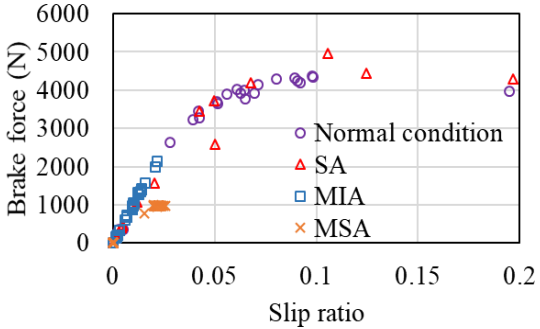
Attack detection accuracy comparisons among IBM, SBM and our method

Detection method	IBM	SBM	Our system
SA	28.3%	0	**92.7%**
MIA	0	63.6%	**91.8%**
MSA	0	51.1%	**90.7%**

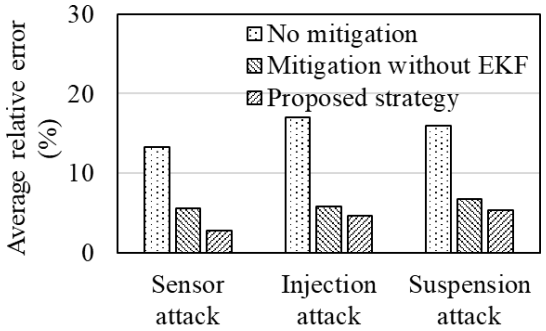
Evaluation of Attack Mitigation

Attack mitigation performance of our system:

- Slip ratio stays in low region and vehicle ABS works normally
- EKF in our system improves attack mitigation performance by eliminating sensor measurement noise



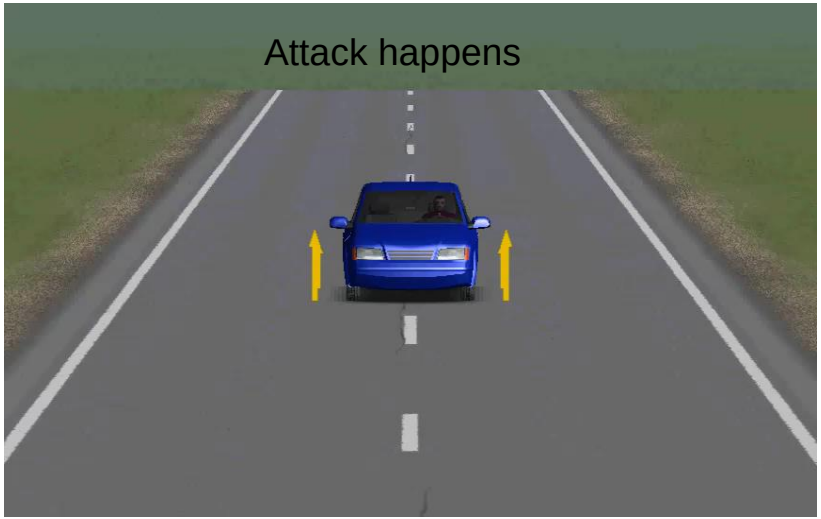
Brake force and slip ratio with our system under different attack situations



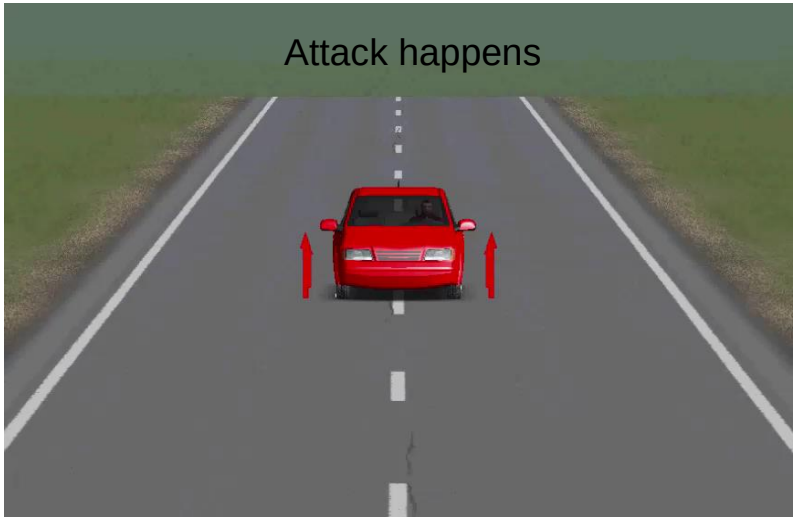
Average relative errors of brake force under different attack situations

Demos

- Initial vehicle velocity - 65 km/h and Road friction coefficient - 0.8
- Vehicle ABS under **SA** (one magnet is 100cm away from ABS sensor)



Attacked ABS without our system

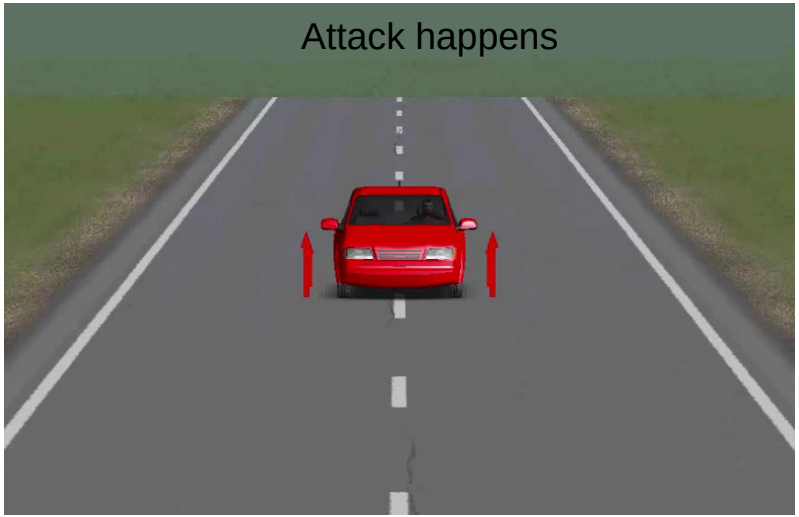


Attacked ABS with our system

Demos

- Initial vehicle velocity - 65 km/h and Road friction coefficient - 0.8
- Vehicle ABS under **MIA** (sends random brake force between 1000 Newton and 4200 Newton)

Attacked ABS without our system

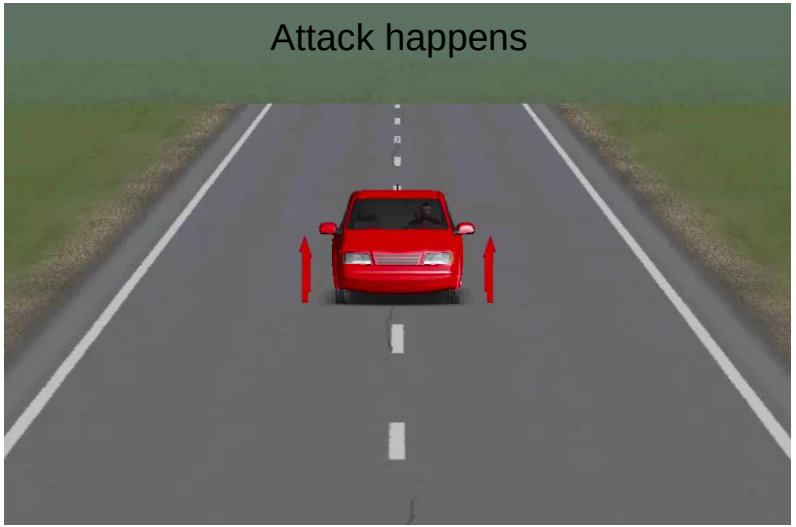


Attacked ABS with our system

Demos

- Initial vehicle velocity - 65 km/h and Road friction coefficient - 0.8
- Vehicle ABS under **MSA** (sends the maximum brake force - 4200 Newton)

Attacked ABS without our system



Attacked ABS with our system

Summary

We proposed an attack detection and mitigation system to detect sensor and CAN bus attacks in the vehicle ABS and mitigate their effects:

- Analyzed which vehicle states can be attacked and how to implement them in practice
- Built a vehicle brake model and an attack change search algorithm for attack detection and mitigation
- Did the simulation to verify our system

Future Work

- Attack detection accuracy of our system reaches around 91% because of limitation of vehicle state prediction accuracy (93.7%)
- Other systems in modern vehicles are vulnerable to attacks and may result in driving safety problem

Thank you!