CAREER: Practical Control Engineering Principles to Improve the Security and Privacy of Cyber-Physical Systems

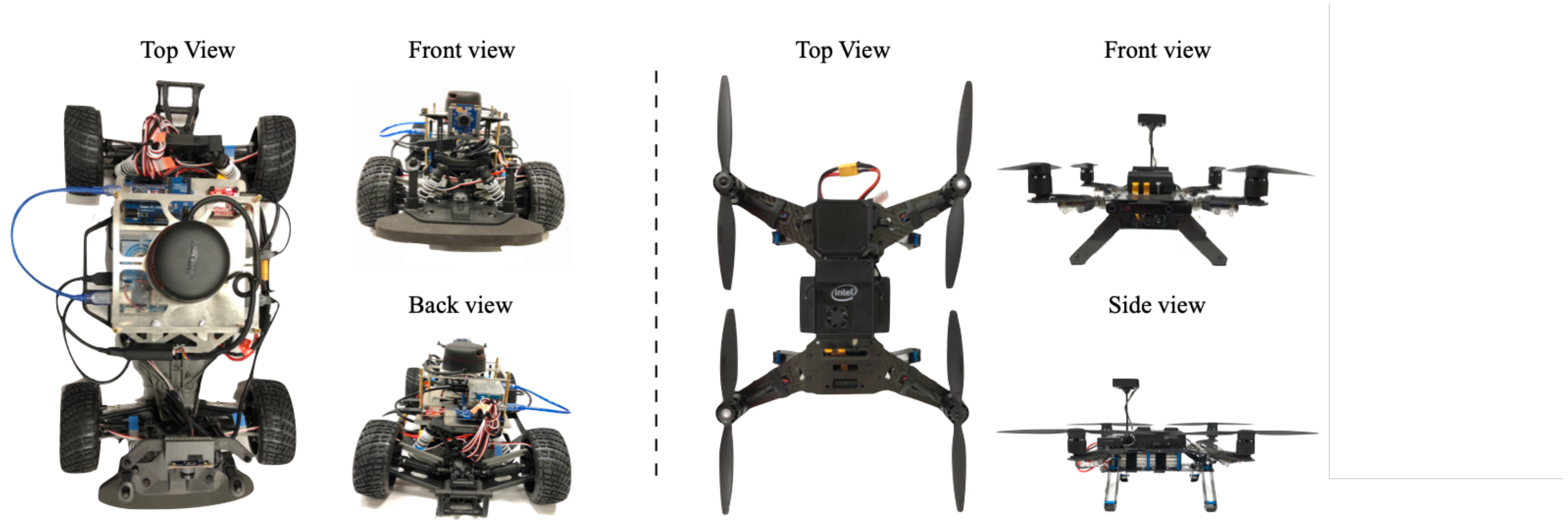
PI: Álvaro Cárdenas, UC Santa Cruz

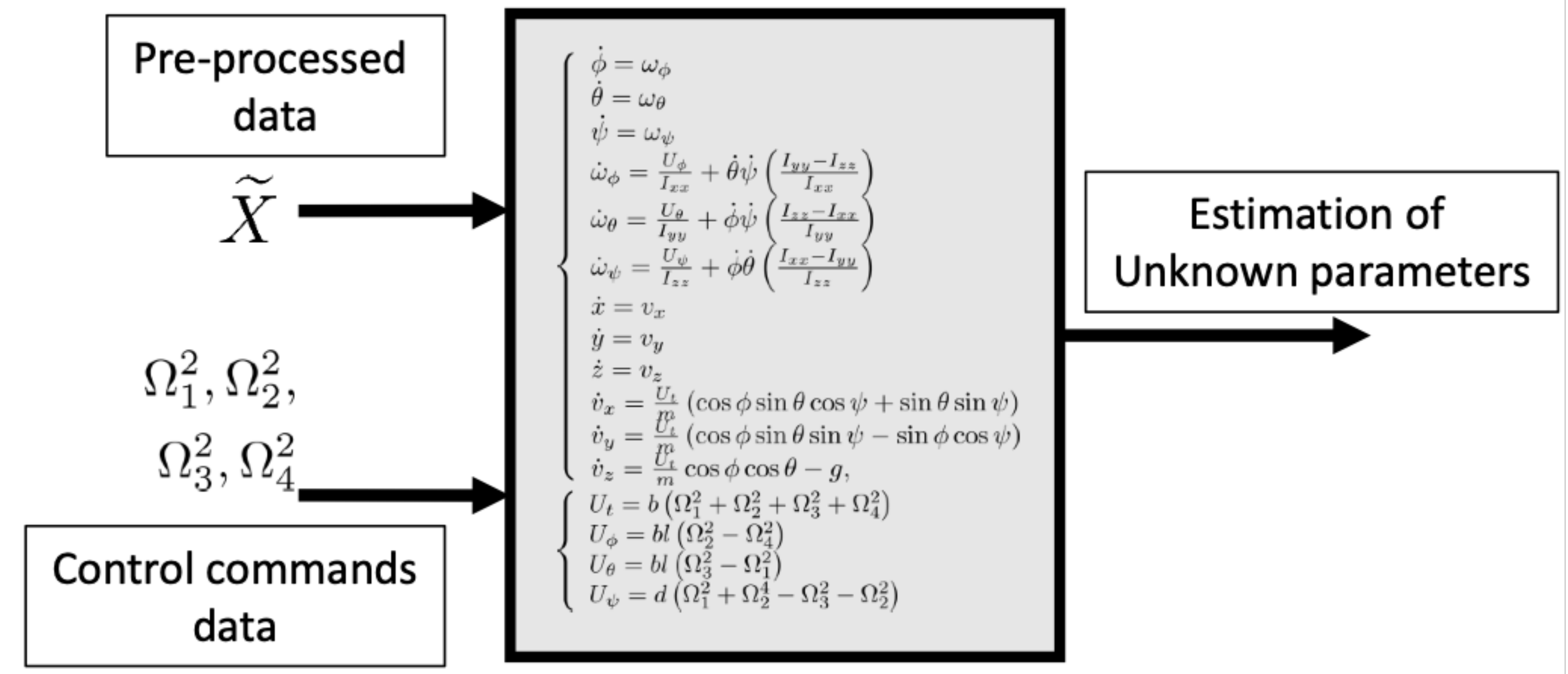
Award # CNS-1931573 (formerly CNS-1553683)

Recent Publications:

- Not everything is dark and gloomy: Power grid protections against IoT demand attacks. USENIX Security 2019
- Adversarial Classification Under Differential Privacy. NDSS 2020
- SAVIOR: Securing Autonomous Vehicles with Robust Physical Invariants. USENIX Security 2020
- Uncharted Networks: A First Measurement Study of the Bulk Power System. IMC 2020
- DARIA: Designing Actuators to Resist Arbitrary Attacks in CPS. IEEE Euro S&P 2020
- Real-Time Attack-Recovery for Cyber-Physical Systems Using Linear Approximations. RTSS 2020
- MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets. CCS 2021

SAVIOR: Securing Autonomous Vehicles with Robust Physical Invariants

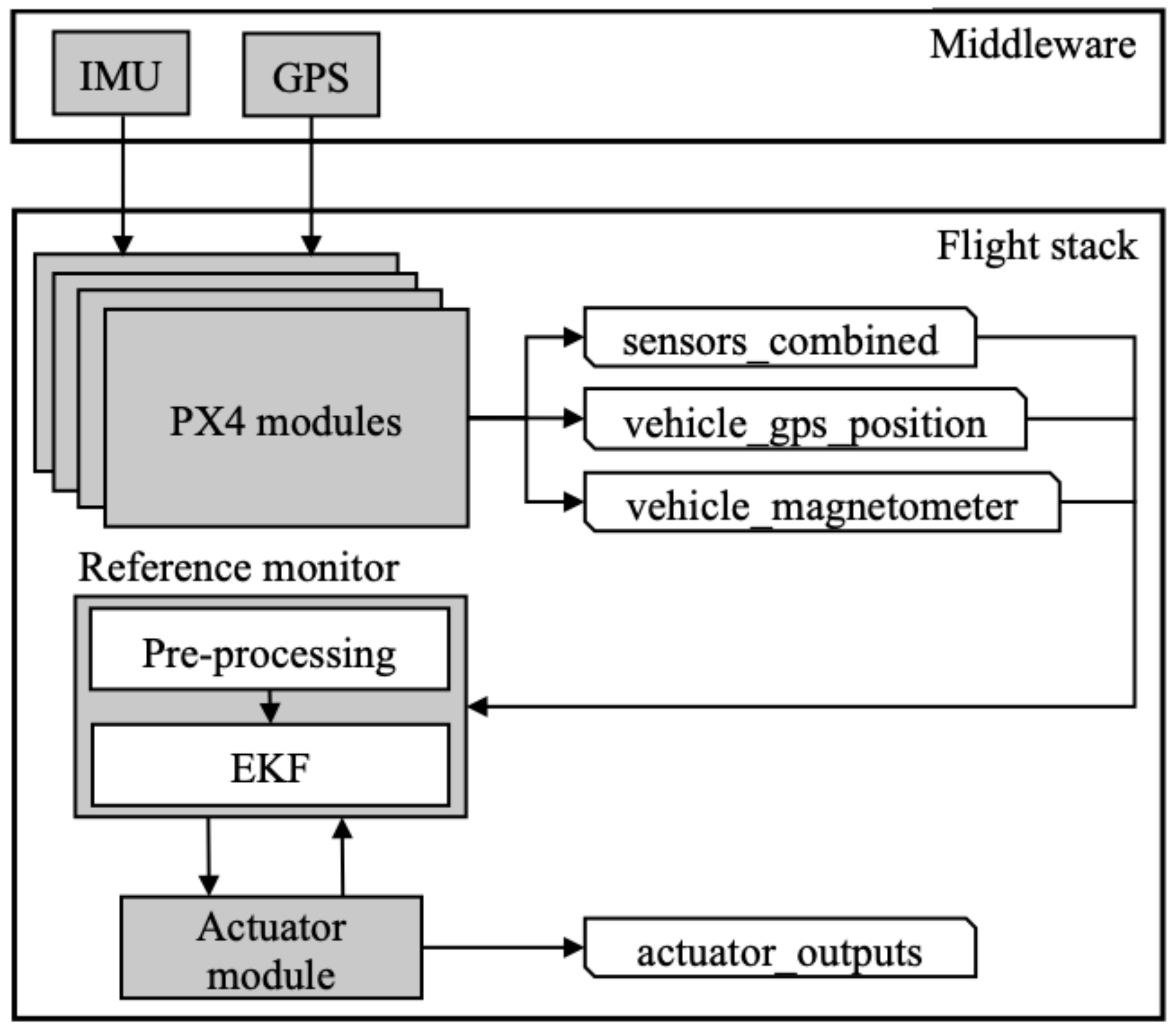




$$\begin{cases} \dot{\phi} = \omega_\phi \\ \dot{\theta} = \omega_\theta \\ \dot{\psi} = \omega_\psi \\ \dot{\omega}_\phi = \frac{U_\phi}{I_{xx}} + \dot{\theta}\dot{\psi}\left(\frac{I_{yy}-I_{zz}}{I_{xx}}\right) \\ \dot{\omega}_\theta = \frac{U_\theta}{I_{yy}} + \dot{\phi}\dot{\psi}\left(\frac{I_{zz}-I_{xx}}{I_{yy}}\right) \\ \dot{\omega}_\psi = \frac{U_\psi}{I_{zz}} + \dot{\phi}\dot{\theta}\left(\frac{I_{xx}-I_{yy}}{I_{zz}}\right) \\ \dot{x} = v_x \\ \dot{y} = v_y \\ \dot{z} = v_z \\ \dot{v}_x = \frac{U_t}{m}(\cos\phi\sin\theta\cos\psi + \sin\theta\sin\psi) \\ \dot{v}_y = \frac{U_t}{m}(\cos\phi\sin\theta\sin\psi - \sin\phi\cos\psi) \\ \dot{v}_z = \frac{U_t}{m}\cos\phi\cos\theta - g, \end{cases}$$

$$\begin{cases} U_t = b\left(\Omega_1^2 + \Omega_2^2 + \Omega_3^2 + \Omega_4^2\right) \\ U_\phi = bl\left(\Omega_2^2 - \Omega_4^2\right) \\ U_\theta = bl\left(\Omega_3^2 - \Omega_1^2\right) \\ U_\psi = d\left(\Omega_1^2 + \Omega_2^4 - \Omega_3^2 - \Omega_2^2\right) \end{cases}$$

Parameter Estimation Block

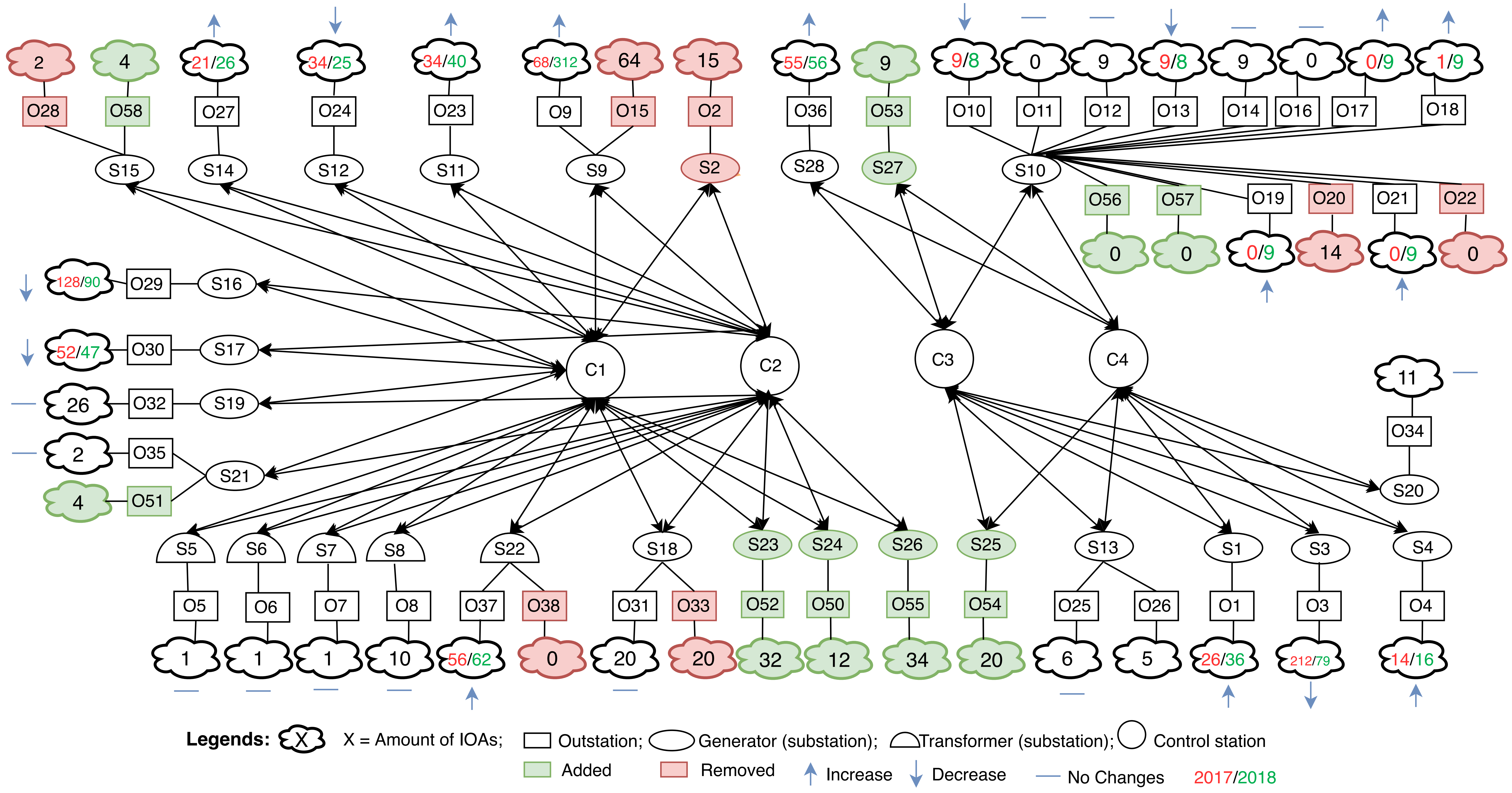


SAVIOR: Securing Autonomous Vehicles with Robust Physical Invariants 11 2020

R Quinonez, J Giraldo, L Salazar, E Bauman, AA Cardenas, Z Lin

USENIX Security

Uncharted Networks: A First Measurement Study of the Bulk Power System



Uncharted Networks: A First Measurement Study of the Bulk Power System

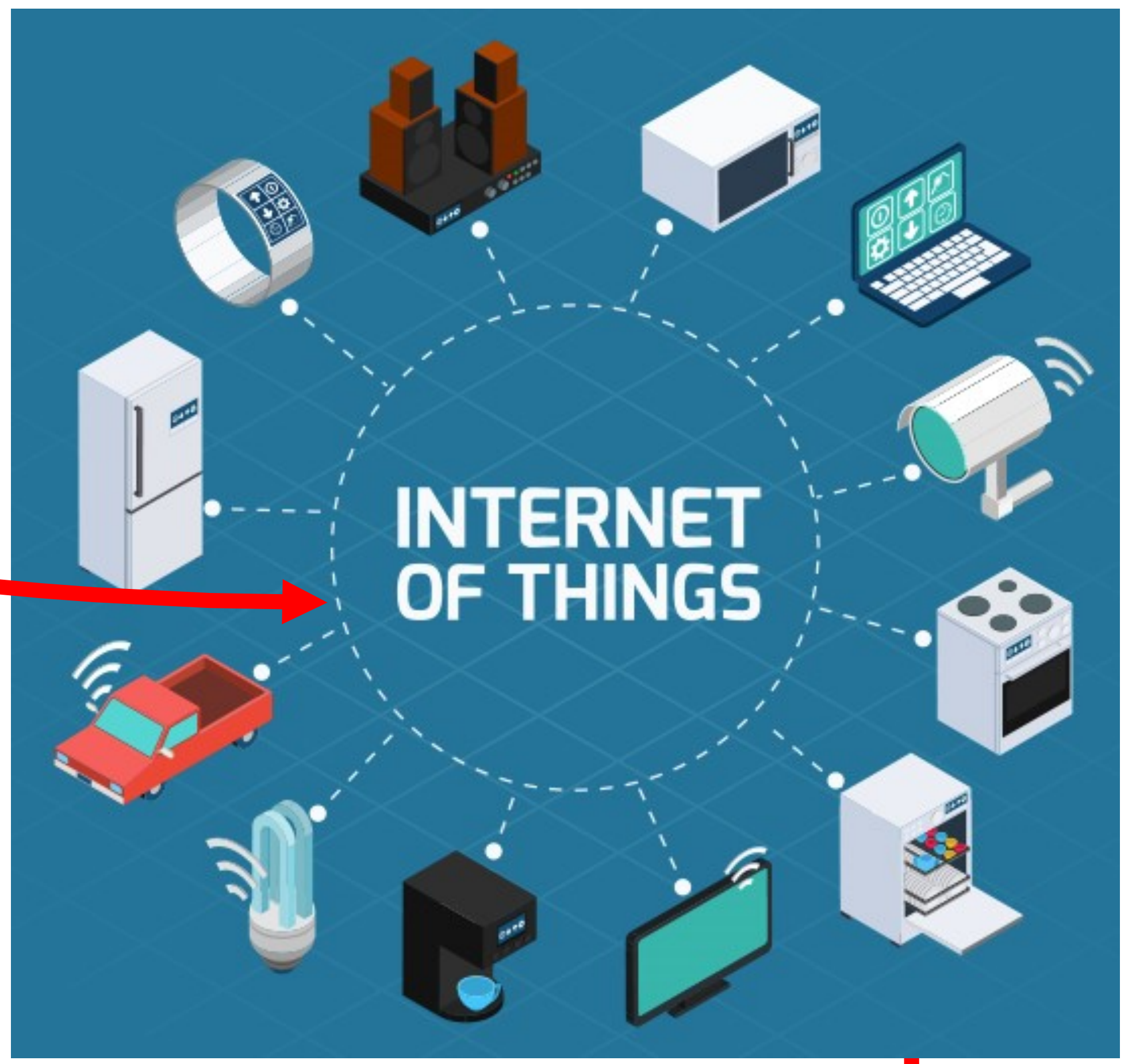
2020

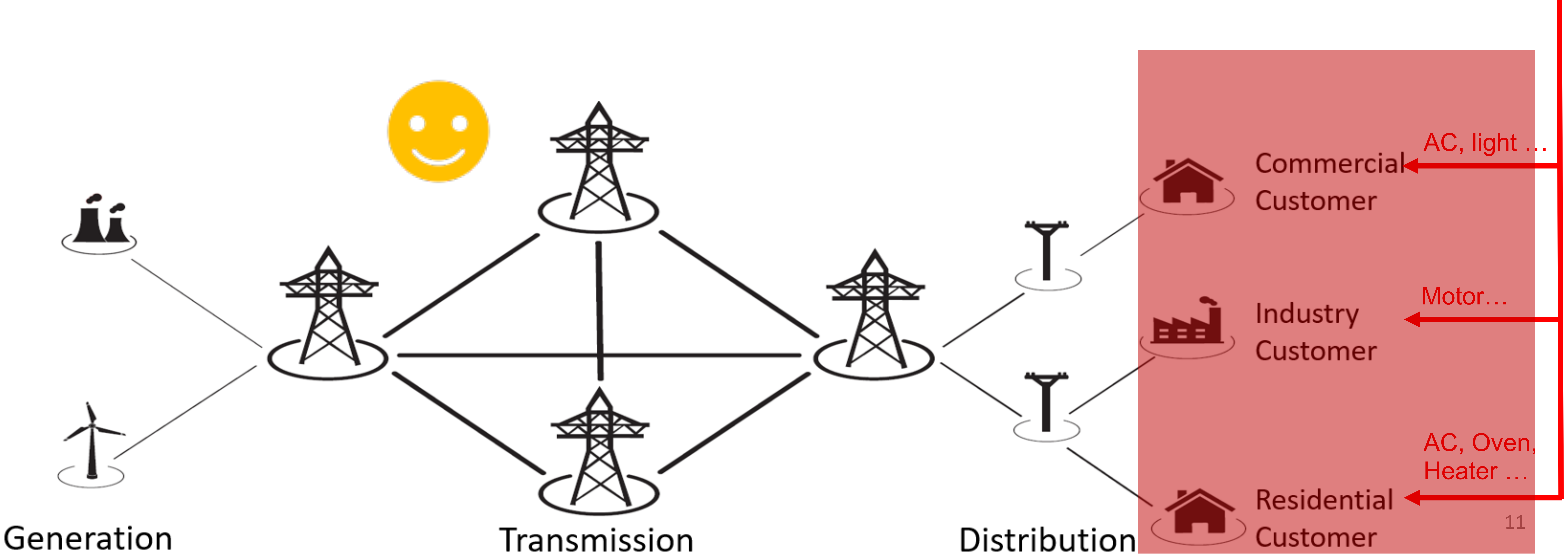
K Mai, X Qin, N Ortiz, J Molina, AA Cardenas

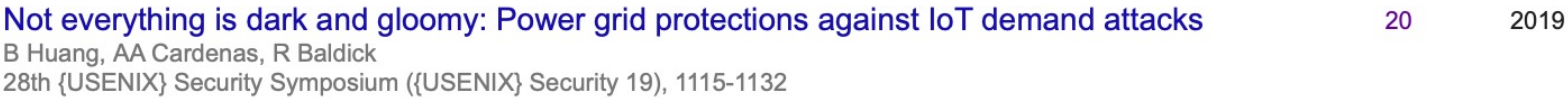
Proceedings of the ACM Internet Measurement Conference, 201-213

Can a High Wattage IoT Botnet Bring Down the Power Grid?

Our paper:
Not as easy as previously thought







Not everything is dark and gloomy: Power grid protections against IoT demand attacks 20 2019
B Huang, AA Cardenas, R Baldick
28th {USENIX} Security Symposium ({USENIX} Security 19), 1115-1132

- MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets. CCS 2021