Breakthrough: CPS-Security: Towards provably correct distributed attack-resilient control of unmanned-vehicle-operator networks

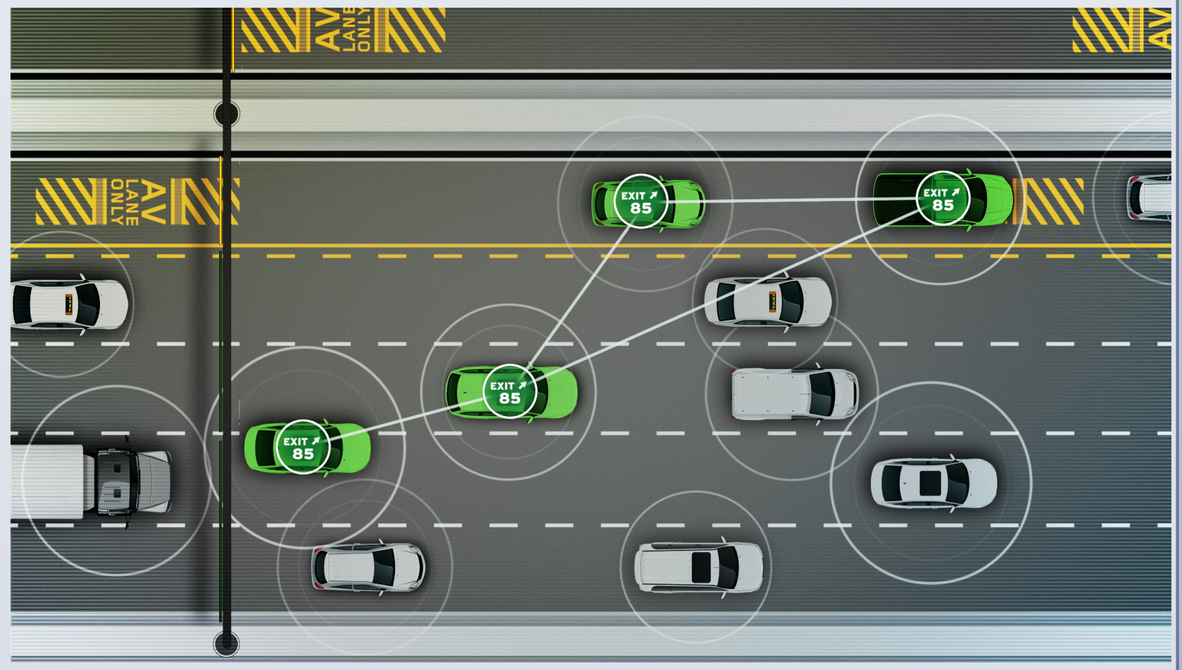
Minghui Zhu (PI), Peng Liu (co-PI), Pennsylvania State University

Background

Recent advances in the technologies of sensing, communication and computing have been boosting the emergence of new generation cyber-physical systems (CPS, for short). Unfortunately, the vulnerabilities of CPS to cyber attacks are evidenced by a number of recent accidents.

1. In 2006, two traffic engineers hacked Los Angeles traffic light control system, lengthened red lights and further snarled traffic.
2. In 2010, the malware Stuxnet attacked industrial programmable logic controllers and reportedly destroyed almost one-fifth of Iran's nuclear centrifuges.
3. In 2011, an American unmanned aerial vehicle (UAV) was brought down by Irian cyber warfare unit.
4. In 2013, the Industrial Control Systems Cyber Emergency Response Team received 181 vulnerability reports about industrial control systems throughout the year in the United States.
5. In 2015, two individuals remotely hacked into a Jeep Cherokee newest model, and were able to control its actuation units such as steering wheels and gas pedals.

These accidents highlight the strong need to guarantee operating functions and performance of CPS under cyber attacks.



Project overview

1. We will develop a distributed attack-resilient control framework to ensure task completion of multiple vehicles despite network attacks and malware attacks.
2. We will develop novel distributed attack-resilient control algorithms; namely high-performance control and network-attack control to deal with network attacks.
3. We will develop so called input-state estimation algorithm to detect malware attacks on vehicles. In addition, we will develop malware-attack control algorithm which allows clean vehicles to avoid the collision with the vehicles compromised by malware.
4. We will employ a principled systematic evaluation plan to validate the cost-effectiveness of our proposed distributed attack-resilient control framework.

Intrusion detection system

Dynamic system model

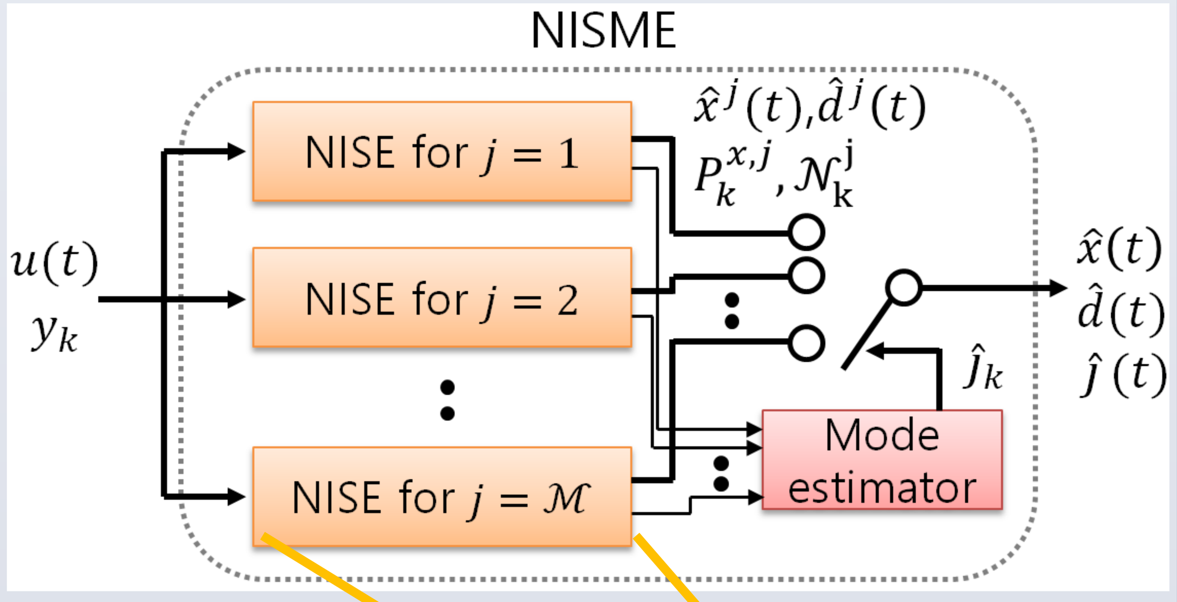
$$\dot{x}(t) = f(x(t), u(t), d^{j(t)}(t), w^{j(t)}(t), j(t), t), \quad x(t) \in \mathcal{C}^{j(t)}$$
$$(x(t), j(t))^{+} = \Omega(x(t), j(t)), \quad x(t) \in \mathcal{D}^{j(t)}$$
$$y_k = h\left(x_k, u_k, v_k^{j_k}, j_k, t_k\right) + H_k^{j_k} d_k^{j_k}$$

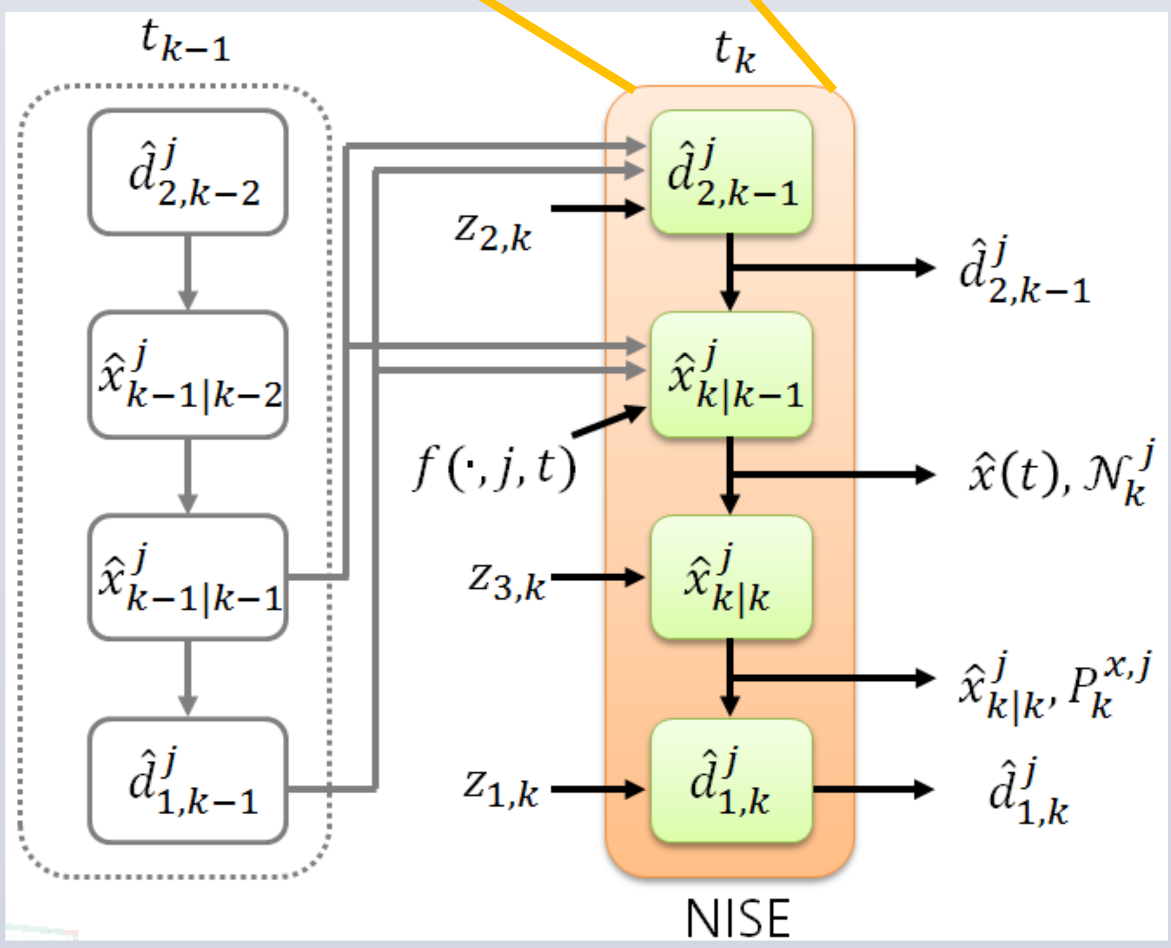
Output decomposition

$$y_k \begin{cases} z_{1,k} = h_1(x_k, u_k, v_{1,k}, t_k) + H_{1,k} d_{1,k} \\ z_{2,k} = h_2(x_k, u_k, v_{1,k}, t_k) = \cdots + G_{2,k-1} d_{2,k-1} \\ z_{3,k} = h_3(x_k, u_k, v_{1,k}, t_k) \end{cases}$$

Where $d_k = G_{1,k} d_{1,k} + G_{2,k} d_{2,k}$ and directly measureable $d_{1,k}$, and indirectly measureable $d_{2,k}$ are orthogonal.

Nonlinear unknown input, state, and mode estimation





Formal analysis

Filter convergence

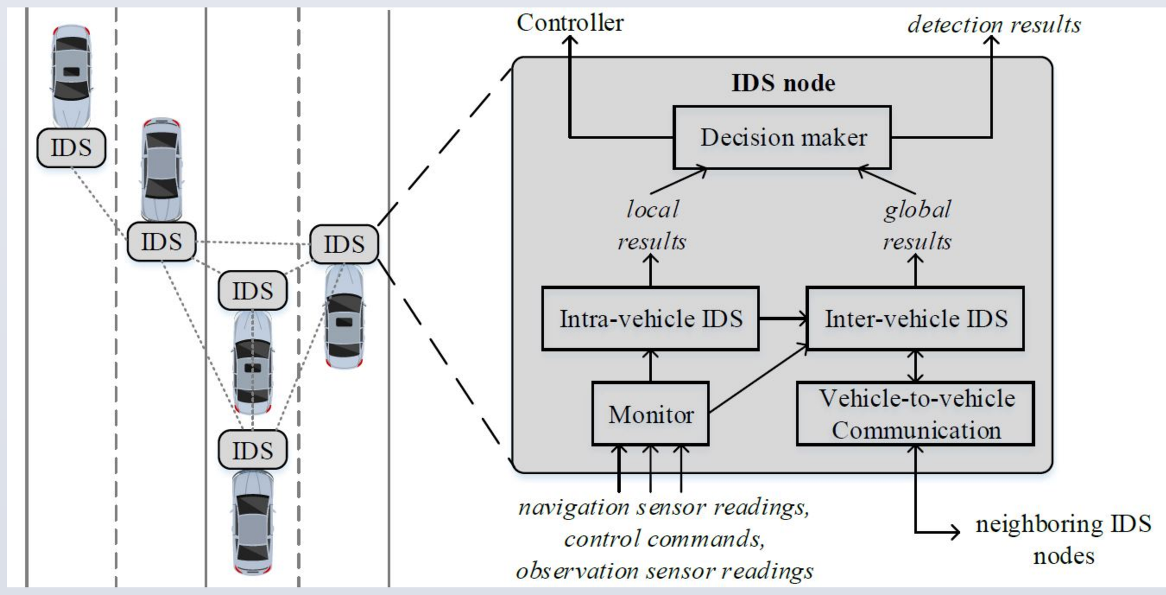
There exist constants a_0, a_1, a_2, a_3, a_4 such that if $Q_k \leq a_0 I, R_{1,k} \leq a_1 I, R_{2,k} \leq a_2 I, R_{3,k} \leq a_3 I$, $\varepsilon \leq a_4$, then it holds that

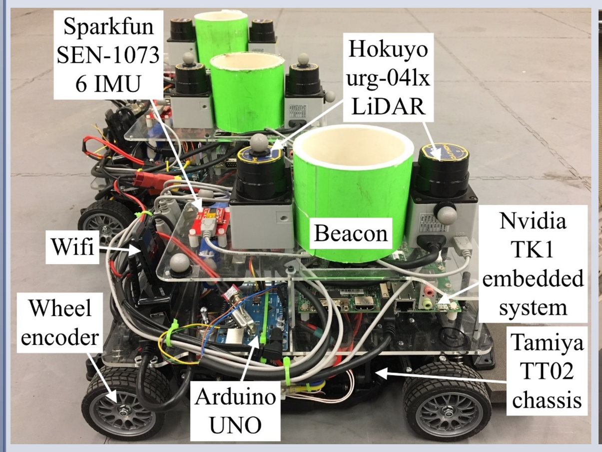
1. $E[\| \tilde{x}_{k|k} \|^2] = \alpha_1 E[\| \tilde{x}_{0|0} \|^2] e^{-\beta_1 t} + \gamma_1$
   $E[\| \tilde{x}_{k|k} \|^2] < \infty$ with probability 1
2. $E[\| \tilde{x}(t) \|^2] = \alpha_2 E[\| \tilde{x}_{0|0} \|^2] e^{-\beta_2 t} + \gamma_2$
   $E[\| \tilde{x}(t) \|^2] < \infty$ with probability 1
3. $E[\| \tilde{d}_1(t) \|^2] = \alpha_3 E[\| \tilde{x}_{0|0} \|^2] e^{-\beta_3 t} + \gamma_3$
4. $E[\| \tilde{d}_2(t) \|^2] = \alpha_4 E[\| \tilde{x}_{0|0} \|^2] e^{-\beta_4 t} + \gamma_4$

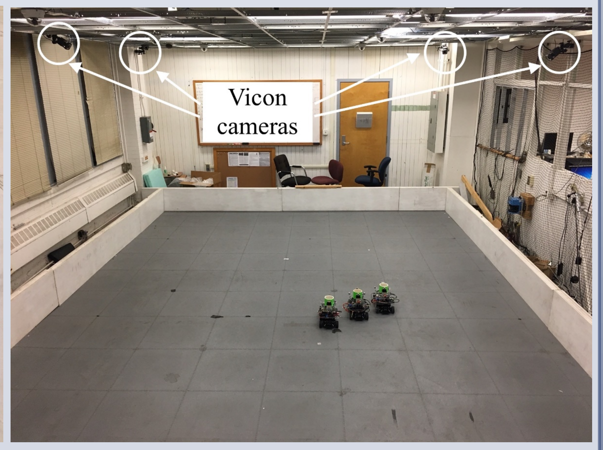
Covariance boundedness

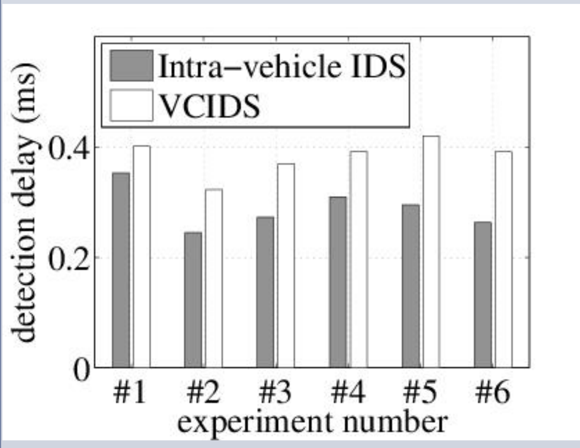
There exist constants $\bar{p}, \underline{p}$ such that $\underline{p} I \leq P_{k|k} \leq \bar{p} I$.

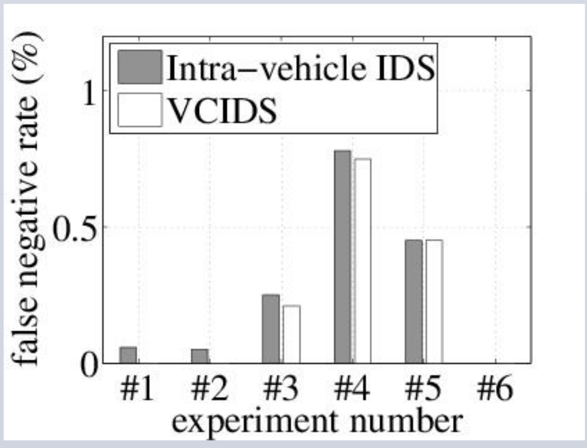
Collaborative intrusion detection of connected vehicles



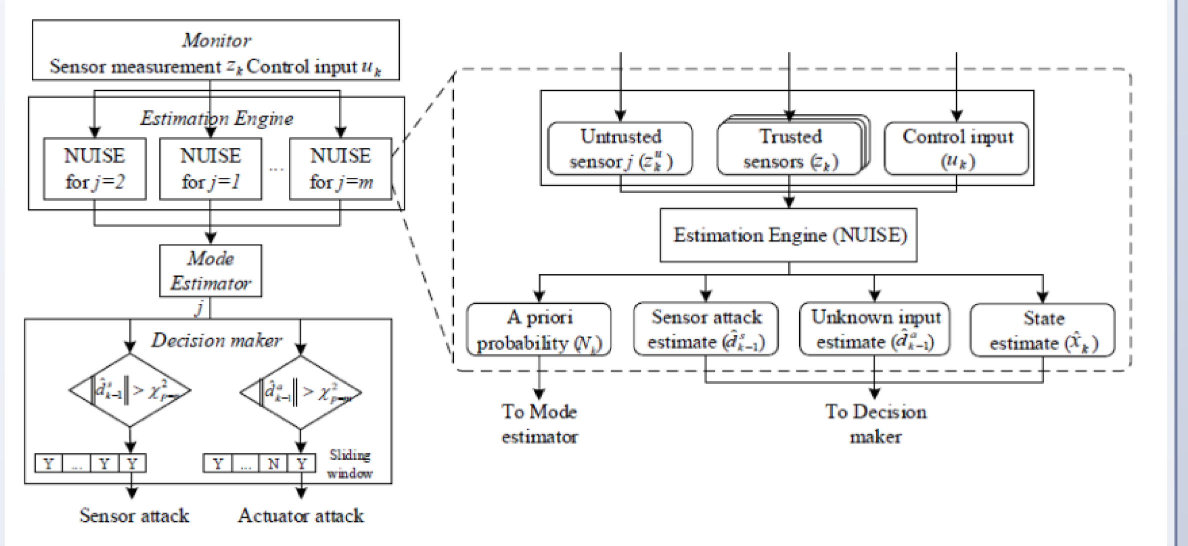


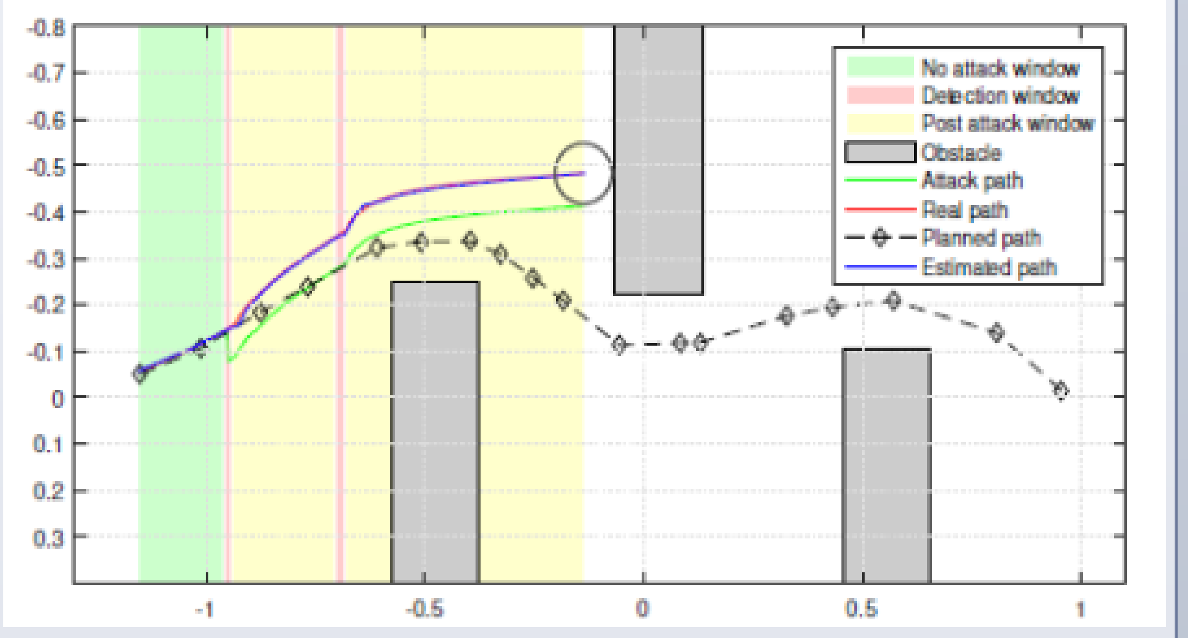






Intrusion detection of a single mobile robot





#	Attack Type	Launch Time (s)	Attack Description	Detection Result	Detection Delay (s)
1	Wheel controller logic bomb	16.0	-6000 unit on v_l +6000 unit on v_r	Actuator attack	0.49
2	Wheel controller logic bomb	4.0	(Override[2]) 7000 unit on v_l 6500 unit on v_r	Actuator attack	2.32
3	Wheel jamming	5.3	0 unit on v_l no change on v_r	Actuator attack	0.76
4	IPS logic bomb	19.0	Shift $+0.07m$ on X Shift $0m$ on Y	Sensor attack (mode 1)	0.30
5	IPS spoofing	26.0	Shift $-0.1m$ on X Shift $0m$ on Y	Sensor attack (mode 1)	0.24
6	Wheel encoder logic bomb	16.0	increment 100 steps on left wheel encoder	Sensor attack (mode 2)	0.43
7	LiDAR denial of service	0.0	distance measurement as $0m$ on each direction	Sensor attack (mode 3)	0.23
8	LiDAR sensor blocking	7.0	faulty distance to the left wall	Sensor attack (mode 3)	0.55

References

1. P. Guo, H. Kim, L. Guan, M. Zhu and P. Liu. **VCIDS: Collaborative intrusion detection of actuator and sensor attacks on connected vehicles.** *13th International Conference on Security and Privacy in Communication Networks*, Oct 2017.
2. H. Kim, P. Guo, M. Zhu and P. Liu. **On attack-resilient estimation of switched nonlinear cyber-physical systems.** *2017 American Control Conference*, Seattle, pages:4328-4333, May 2017.
3. S. Yong, M. Zhu and E. Frazzoli. **Resilient state estimation against switching attacks on stochastic cyber-physical systems.** *2015 IEEE Conference on Decision and Control*, Osaka, Japan, pages:5162-5169, Dec 2015.
4. S. Yong, M. Zhu and E. Frazzoli. **Switching and data injection attacks on stochastic cyber-physical systems: Modeling, resilient estimation and attack mitigation.** *ACM Transactions on Cyber-Physical Systems*, 2016, Submitted.