Commentary on paper [P5] Asif Salekin

[P5] Tianjia He, Lin Zhang, Fanxin Kong, and **Asif Salekin**. Exploring Inherent Sensor Redundancy for Automotive Anomaly Detection, The 57th Design Automation Conference (DAC), 2020. https://doi.org/10.1109/DAC18072.2020.9218557

*Problem and Motivation*: Modern automobiles follow open architectures enabling various promising services and applications such as vehicle-to-vehicle communication and self-driving. However, it also introduces potential security vulnerabilities to malicious attacks that are beyond conventional cyber-attacks, such as spoofing attacks on GPS sensors, noninvasive attacks on Antilock Braking Systems, cameras, and LiDAR systems, etc. These attacks can spoof the automobile controllers to perform actions that may result in adverse outcomes. Hence, there is a need to validate sensor data before the automobile controller act on them. This paper addresses the task of detecting anomalous sensory streams by exploiting inherent redundancy among heterogeneous sensors.

*Paper's Novelty and Contribution*: The paper's threat model considers that the attacker can maliciously alter a subset of all sensors and control their measurements given to the controller, and the training data is trustful.

This paper investigates and leverages the inherent redundancy among heterogeneous sensors to detect anomalies. Inherent sensor redundancy is defined as multiple sensors simultaneously responding to the same physical aspect in a related manner. For example, pressing the accelerator will increase engine RPM and vehicle speed as well as affect GPS readings.

The developed anomaly detection approach's primary idea is first to identify the consistency among sensor data and then utilize it to detect anomalous behaviors of sensor measurements. To realize this idea, we developed a deep autoencoder-based anomaly detection method.

The developed deep-autoencoder learns a consistent pattern from vehicle sensor data in normal states and utilizes it as the nominal behavior for the detection. We define a threshold based on the reconstruction error (of the autoencoder), where corrupted sensor measurements will result in higher reconstruction errors than the threshold, while normal data will not. The approach only relies on normal sensor data and does not restrict the existence of multiple clusters in the training data set. The proposed method is independent of anomalous data for training and the calculation of pairwise correlation among sensors. We use a real-world dataset to demonstrate the feasibility of our approach.

The developed approach is generalizable and extendible on multi-sensor systems, where multiple sensors measure the same event, conveying inherent redundancy.

*Professional Significance:* The paper was published in csranking.org listed top-tier conference DAC 2020. This paper was first authored by Tianjia He, a master's student at Syracuse University. After joining Syracuse University, I co-mentored the student with Dr. Fanxin Kong, and this is the first paper resulting from my mentorship of a Syracuse University student. The paper received 20 citations.