Commentary on paper [P3] Asif Salekin

[P3] Jingyu Xin, Vir V. Phoha, **Asif Salekin**, "Combating False Data Injection Attacks on Human-Centric Sensing Applications", Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), 2022. https://doi.org/10.1145/3534577

Problem and Motivation: Human-centric sensing applications on smart wearables are vulnerable to false data injection attacks (FDIA) that alter a portion of the victim's sensory signal with forged data comprising a targeted trait. Such a mixture of forged and valid signals successfully deceives the continuous authentication system to accept it as an authentic signal. Simultaneously, introducing a targeted trait in the signal misleads human-centric applications to generate specific targeted inferences; that may cause adverse outcomes. Take a health monitoring system as an example that utilizes smartwatch physiological sensory data to assess a patient's health. Suppose the FDIA attacker injects other unhealthy individuals' physiological signals into the genuine healthy user's physiological sensory signals. In that case, it can cause wrong health assessment that may lead to unnecessary interventions and harm the patient's health. This paper evaluates false data injection attack (FDIA), its deception efficacy on sensor-based authentication and human-centric sensing applications simultaneously, and presents a novel attack detection approach.

Paper's Novelty and Contribution: FDIA modifies the sensory data such that the sensory data stream of another user is injected into the target user's sensory stream (victim), so no knowledge of the victim is assumed. If the attacker wants to generate a specific output, they can use signals with targeting information to influence the application's outcome. This paper particularly focuses on such targeting FDIAs aiming to misinform human-centric sensing applications with certain forged information.
However, several continuous authentication approaches have been proposed in the literature for human sensing applications. Hence, this paper's threat model considers a harder situation where a continuous authentication system is working in the background to protect the smart device. Other sensing applications can further accept only the signal verified by the authentication system. Hence, a successful FDIA sample must deceive the authentication system into thinking it is an authentic signal and the human-centric application to generate a misled inference. We evaluated a wide variety of FDIA samples and showed that an equal proportion of forged and legit signals mixed could deceive both the authentication and human event detection approaches.

Notably, we developed a novel FDIA detection approach from a single sensor stream. Literature shows that, in human-centric sensing, the sensory streams convey the user's unique traits. This paper's novelty comes from formulating the FDIA detection problem as a multiple instance learning (MIL) problem. The FDIA detection identifies if a signal sample (subject to inspection) comprises at least a pair of segments belonging to different individuals. This paper performs this task through a novel framework named Siamese-MIL that leverages the MIL paradigms, Siamese network structure, and a unique sensor data representation. The Siamese-MIL segments a signal sample into a set of all possible segment pairs. A Siamese neural network (SNN) is trained to identify any segment pair that contains signals from different individuals. If the trained SNN identifies at least one mismatched segment pair in a set, the respective signal sample is considered an FDIA sample. The approach differs from supervised learning or voting mechanisms on how the SNN is trained. Following the MIL training paradigm, SNN is tailored to be highly effective in detecting matched (legit) segment pairs (i.e., high recall) where mismatched segment pair detection accuracy (true negative rate) can be lower. Such characteristics ensure high FDIA detection accuracy. The Siamese-MIL FDIA detection approach is designed to extend the conventional authentication systems, prohibiting any attack signal from reaching human-centric applications. Importantly, the approach is generalizable to detect FDIA in any single human-centric sensing data stream.

Professional Significance: This paper was published in csranking.org listed top conference Ubicomp/IMWUT 2022. The work is funded by my NSF SCH Medium grant, and my Ph.D. student Jingyu Xin is the first author, and I am the corresponding author. I am preparing an NSF SaTC proposal based on this work.