NSF SaTC CORE: Small: TAURUS: Towards a Unified Robust and Secure Data Driven Approach for Attack Detection in Smart Living

Shameek Bhattacharjee, Western Michigan Univ., PI (# 2030611) Sajal K. Das, Missouri Univ. Sc & Tech., PI Lead (#2030624)

Project URL: https://sites.google.com/view/satc-project-tauras/home

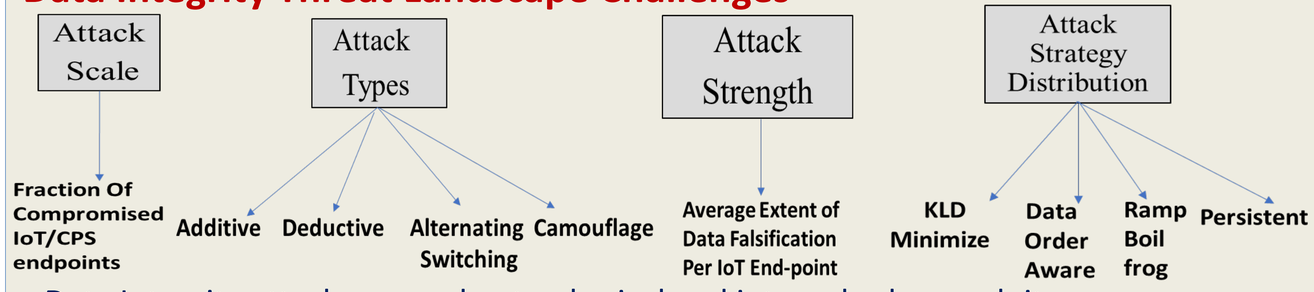
Summary of Hypothesis

- For IoT/CPS domains, some unified structure in the data can be used to *derive* invariants
- Invariants characterize a latent space that is highly stable under benign conditions
- Invariants have math properties that *show sharp deviations* under data integrity threats
- Invariants have the power to indicate what type of threat → Attack Context
- *Attack Context informs device level anomaly classifiers that are bio-inspired*

Smart Living IoT and CPS domain Challenges

- How to model human behavior & physics of process affecting sensory data?
- How to reduce false alarms while detecting anomalies due to attacks?
- How to distinguish legitimate changes from attacks and unsafe incidents?
- How to detect low profile attacks hiding behind randomness?
- Is co-location of many security mechanisms for each service burdensome?
- How to design plug and play type unified approaches that generalize?

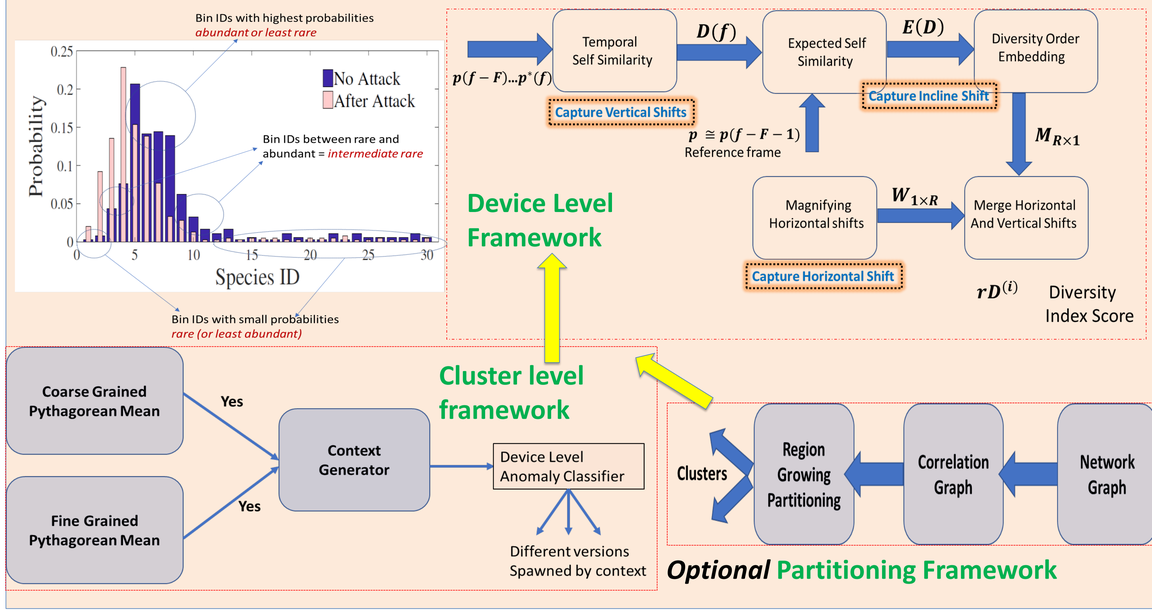
Data Integrity Threat Landscape Challenges



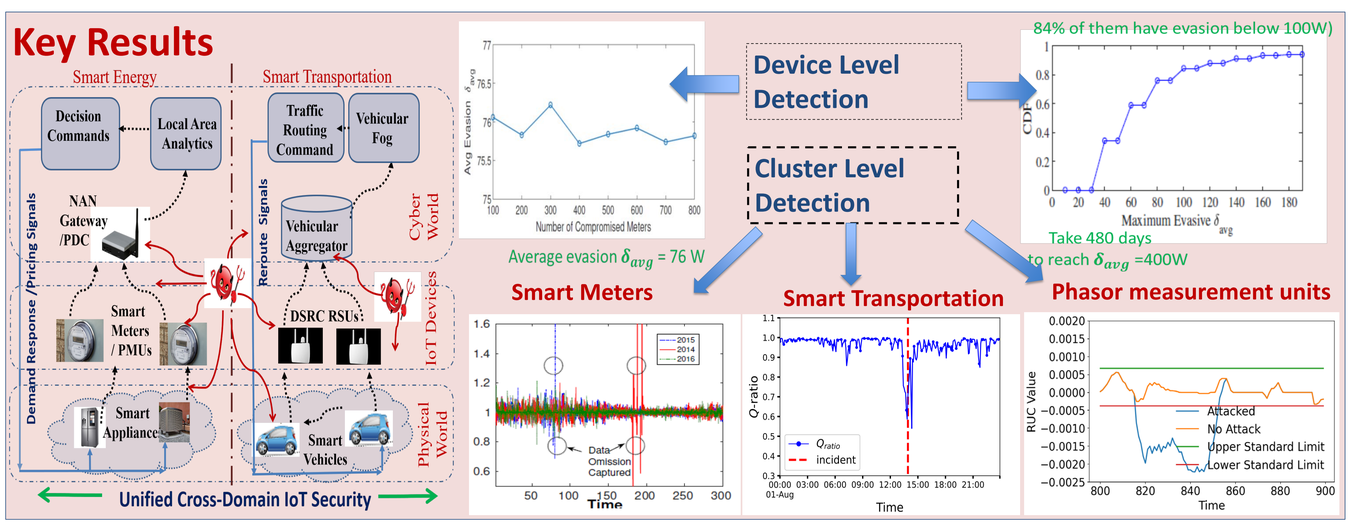
- Data Integrity attacks occur due to physical and internal cyber exploits
- Defender does not know which attack will happen
- Different attacks treated in silos → too many defense solutions
- Attacks are common but have different impacts given a IoT/CPS domain
- *Can we build one framework that works for various attacks and multiple domains?*

Research Contributions

- Novel clustering approach for community scale smart living CPS; each cluster maximizes positive covariance among IoT sensing data
- Pythagorean Mean based Invariant characterizes benign *cluster-level* behavior
- Our Invariant contains properties that deviate under various attack features, and has ability to indicate attack type, strategy, and severity (Context)
- *Context* informs a subsequent *device level anomaly detector*
- Theory for two device level anomaly detectors: (1) context embedded KL divergence; (2) novel *bio inspired information theory* built on Renyi Entropy, better for low margin attacks



Key Results



Broader Scientific Impact

- Generic threat landscape for data integrity attacks in smart living CPS
- Formal Analysis: closed form expressions to predict security performance given any dataset.
- Proved invariant based anomaly detection applies to Smart Energy Metering, Phasor Measurement Units, and Smart Transportation
- Proven compatibility with customer privacy preserving frameworks (e.g., Fully Homomorphic Encryption)
- Closed form approximation of failure/ evasion points of anomaly detector

Education and Outreach

- Bhattacharjee *partnered with Kalamazoo Math Science Center* for yearly advising of high school students who compete in state's school level engineering projects fair.
- Das and Bhattacharjee *co-organized IEEE Big Data and IoT security workshop* co-located with IEEE SmartComp (2021-2022).
- Bhattacharjee offered a new course on *Artificial Intelligence based Security*.
- Das offered a course on Advances in CPS and covered IoT and CPS security in smart grid and smart transportation.
- Das delivered several keynote talks on CPS and IoT security.

Impact of Participation

- 4 PhD students partially funded; 2 at MST and 2 at WMU
- 2 undergrad senior design projects at WMU; two undergrad students at MST
- One women PhD student each recruited at WMU and MST
- Three K-12 student high school research projects in Kalamazoo-Portage school district on WMU
- One BS student at WMU continuing as MS; one BS student at MST continuing PhD.

Publications/Products

1. S. Bhattacharjee, P. Madhavarapu, S. Silvestri, S. K. Das, "Attack Context Embedded Data Driven Trust Diagnostics in Smart Metering Infrastructure" *ACM Trans. Priv. and Sec.*, 2021.

2. S. Bhattacharjee, P. Madhavarapu, S. K. Das, "A Diversity Index Scoring Framework for Identifying Smart Meters Launching Stealthy Data Falsification Attacks", *ACM Asia' CCS,* 2021

3. M. Islam, J. Talusan, S. Bhattacharjee, F. Tiasus, S. Vazirizade, A. Dubey, K. Yasumoto, S. K. Das "Anomaly based Incident Detection in Large Scale Transportation Systems", *IEEE/ACM Intl. Conf. on Cyber Physical Sys. (IEEE ICCPS),* 2022.

4. P. Roy, S. Bhattacharjee, H. Al-Sheakh, S. K. Das, "Resilience against Bad Mouthing Attacks in Mobile Crowdsensing Systems via Cyber Deception" *IEEE WoWMoM, 2021*

5. P. Roy, S. Bhattacharjee, S.K. Das, "Real Time Stream Mining based Attack Detection in Distribution Level PMUs for Smart Grids," *IEEE GlobeCom*, 2020.

6. Y. Ishimaki, S. Bhattacharjee, H. Yamana, S. K. Das, "Towards Privacy-preserving Anomaly-based Attack Detection against Data Falsification in Smart Grid" *IEEE SmartGridComm*, 2020.