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

Challenge:

High randomness in Smart living CPS data patterns

Low profile data integrity attacks hide behind such randomness

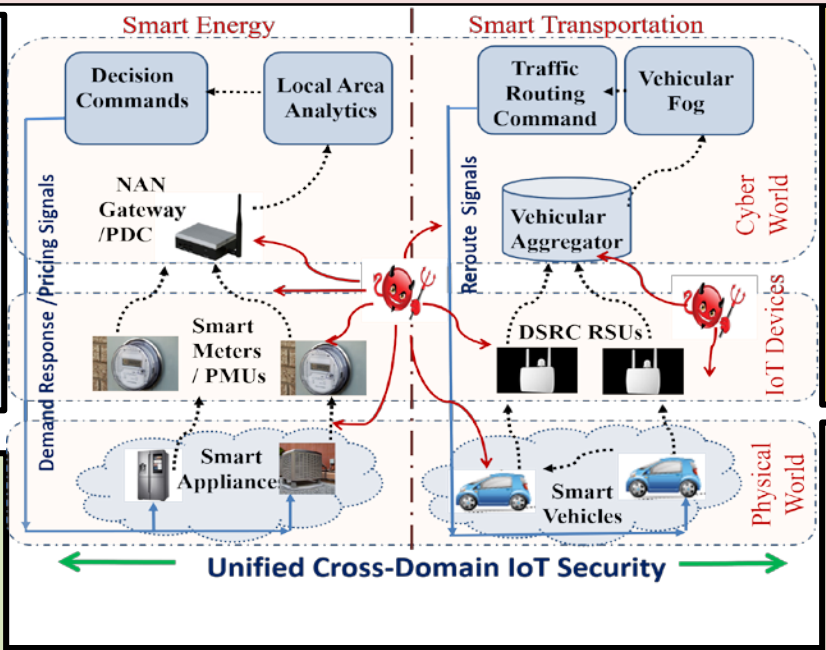
Both cyber and physical exploits cause to data integrity attacks

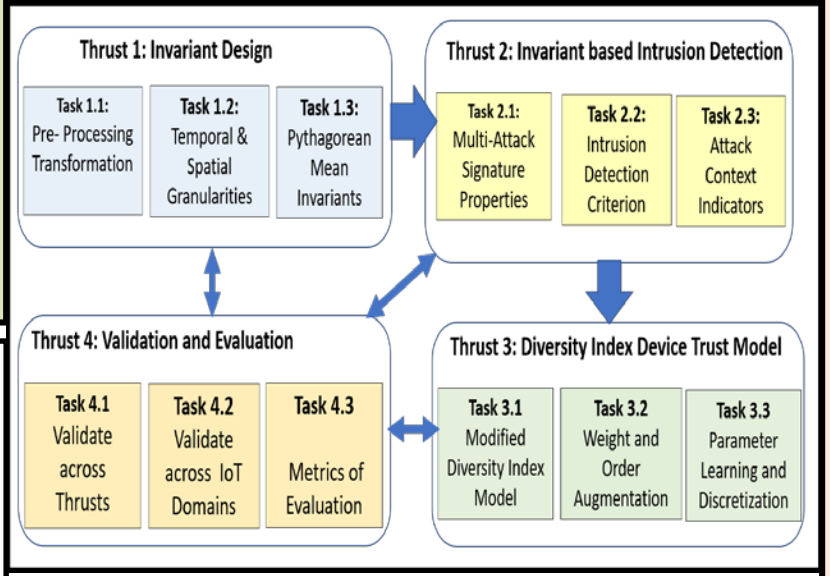
Solution:

- Behavioral invariant design as anomaly detection metric at decentralized cluster level

- Attack Context Generation from invariant's produced signatures

- Trust scoring based on Bio-inspired information theory





Scientific Impact:

- Unified approach for data integrity attack detection is feasible in smart living CPS.

- Theory for low margin attacks

- Common framework works against multiple attack types and strategies.

Broader Impact and Broader Participation:

Utilities, Smart City consumers of Smart Living IoT and CPS applications

Validated with real datasets and testbeds

K-12 & senior design projects,, Workshop on IoT Security for Smart Living

4 PhDs. partially supported, 2 undergraduates trained, 3 science projects for K-12 students

SATC-2030611, Western Michigan Univ.,
PI Contact: Shameek Bhattacharjee
Email: shameek.bhattacharjee@wmich.edu
SATC- 2030624, Missouri Sc & Tech
PI Contact: Sajal K. Das
Email: sdas@mst.edu