JUNO2: US-Japan Collaborative Project

STEAM: Secure and Trustworthy Framework for Integrated Energy and Mobility in Smart Connected Communities

PI Meeting – Chicago, October 11, 2019

Our US-Japan Team

MISSOURI S&T

Sajal K. Das

WESTERN MICHIGAN UNIVERSITY

Shameek Bhattacharjee

VANDERBILT

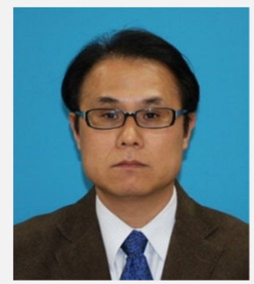
Abhishek Dubey

Hayato Yamana

Waseda University

Hirozumi Yamaguchi

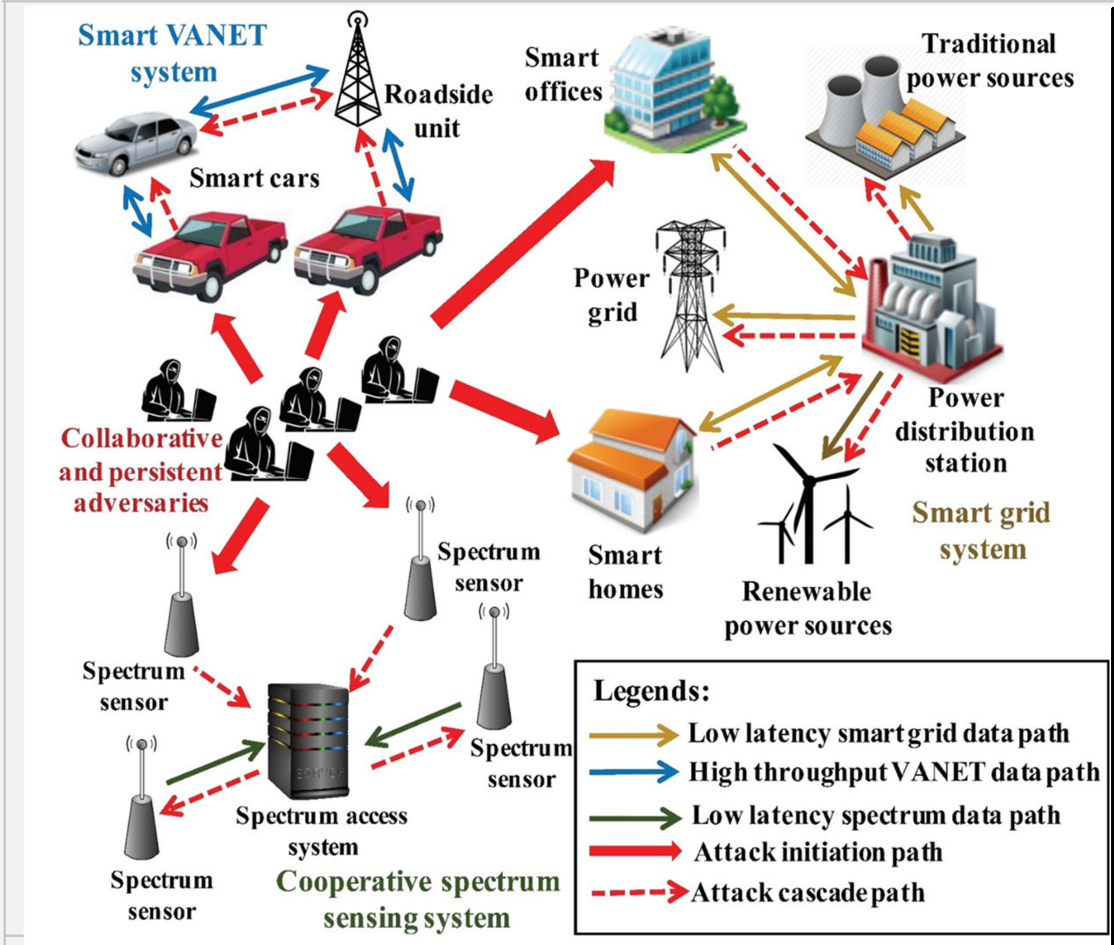
大阪大学
OSAKA UNIVERSITY



Keiichi Yasumoto

Nara Institute of Science and Technology
NAIST

Security in a Smart City Scenario



Smart Mobility and Smart Energy:

- Interdependent, societally critical CPS networks
- Ensuring safety, resiliency and privacy preservation

Unique Challenges in Securing S & CC

- Large variations in individual end point data due to behavioral and activity differences.
- No strict stationarity over time or space.
- Heterogeneous time granularities of sensing and network sizes.

Goals and Novelty of STEAM Project:

- Develop integrated frameworks, algorithms and models to address security, dependability and trustworthiness challenges in mobility and energy under various threats.
- Design lightweight resilient anomaly detection and privacy preserving encryption schemes & middleware architecture.
- Trust building in S & CC applications; efficient mechanisms to handle conflicting goals of identifying anomalies; trade-off between security, privacy and integrity at scale.
- Efficient co-design and calibration of encryption and robust anomaly detection schemes.

STEAM Project: Year 1 Progress Report

Thrust 1: Secure and Trustworthy Decision Making under Uncertainty

- Fast, hierarchical, efficient, and accurate decentralized anomaly detection methodology for streaming transportation sensors using Pythagorean means and long short-term memory (LSTM) networks
- Fast and accurate detection of compromised smart meters under temporally distributed stealthy attacks for smart energy networks
- Algorithms for detecting components with attack margins much below the standard deviation of data with high accuracy.

Thrust 2: Privacy Preserving Computations using Fully Homomorphic Encryption (FHE)

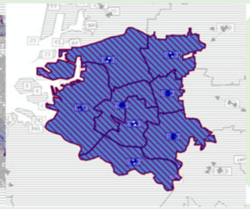
- Developed efficient approaches for enhancing FHE to execute privacy preserving decisions that require complex calculations.
- **Approach 1:** Table lookup with a non-colluding server to adopt any kinds of calculations at aggregators for higher speed-up
- **Approach 2:** Approximate Homomorphic Encryption scheme (HEAAN) to leverage floating-point arithmetic (e.g., log computation) over encrypted data

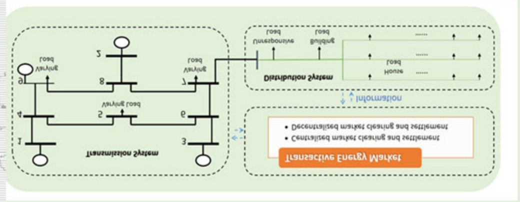
Thrust 4: Developing a Secure and Trustworthy Middleware Architecture

- A novel middleware architecture to assign tasks over IoT devices (e.g., RSUs, smart meters) taking into account the required quality of service (QoS) levels
- Implementation and evaluation of a prototype middleware using Docker technology for easy deployment
- Development of a Smart Transportation Service Emulation Testbed
- Defining an optimal task assignment problem and developing an algorithm with federated learning

Thrust 5: Validation With Real Datasets for Smart Mobility and Energy

- Large scale road traffic data collection from Osaka and Nashville
- An integrated energy simulation testbed development for experimenting with integrated mobility and energy scenarios





Progress on Thrust 1:

(Shameek Bhattacharjee, Sajal Das, Abhishek Dubey)

Secure and Trustworthy Decision Making under Uncertainty

Tasks:

1.1 Lightweight Anomaly Detection
1.2 Stochastic Trust Models
1.3 Dependable Decision Making

Trustworthy and Efficient Anomaly Detection

Threat Model: Orchestrated attacks on a collection of sensors to maximize the effect of attack on the global transportation system

Tried on real data from Nashville, TN

Optimal RSU Placement: designed for optimal anomaly detection using ROC curves

Macro Model: designed for large scale decentralized anomaly detection in real time

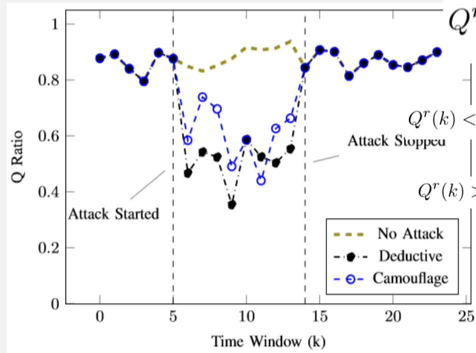
Micro Model: highly accurate and fine grained-anomaly detection. Computationally intensive

Congestion Progression: how the effects of anomalies propagate through the network

Optimized (for detection) RSU Deployment

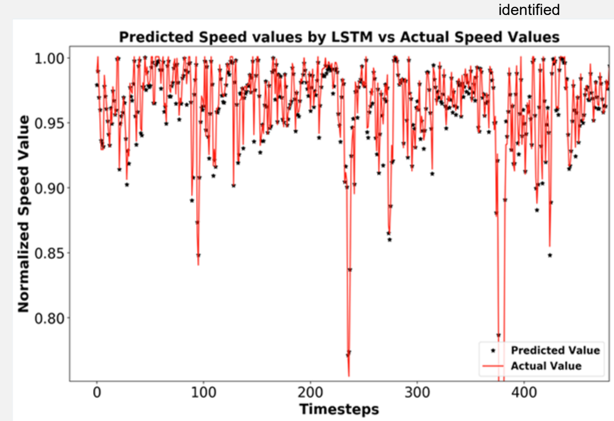
Data Collection	Zone Level Detection	Sensor Level Detection	Network Level State Estimation
Speed data sent from sensor to its corresponding RSU.	Light-weight anomaly detection run at the RSU level. Statistical means approach. Purpose: identify orchestrated data-integrity attacks.	LSTM based detection run at the centrally located cloud on high-capacity detection nodes. Identify which sensors are compromised by data-integrity attack. Only runs when attack is identified at the zone level.	If a real-incident is detected then then congestion propagation framework is used to identify the future affects in short-term. Then the state of the transportation network can be used for optimal routing. LSTM Networks are used to mitigate the anomalous information if no physical incident was identified

$$Q^r(k) = \frac{HM^r(k)}{AM^r(k)}$$



$$Q^r(k) < Q^r_{ave}(k) - \epsilon^r * Q^r_{std}(k)$$

$$Q^r(k) > Q^r_{ave}(k) + \epsilon^r * Q^r_{std}(k)$$



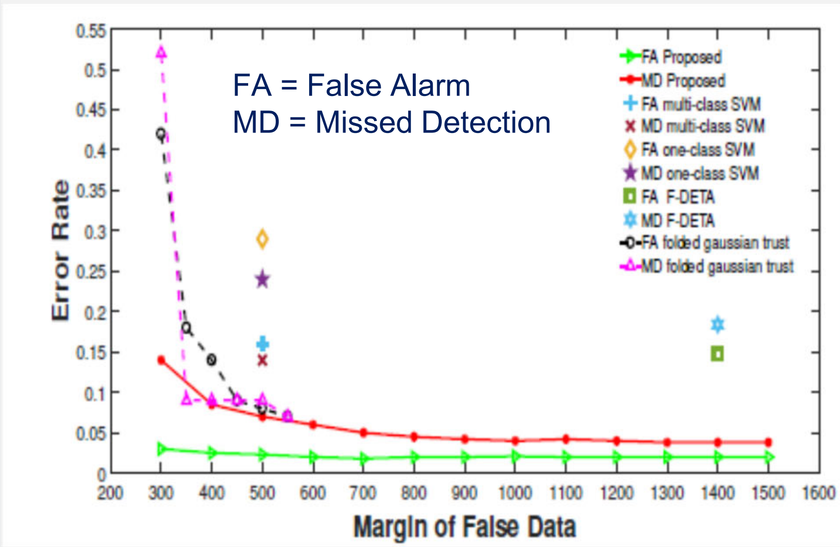
Macro-Level Detection: Built efficient streaming statistical algorithm

Micro-Level Detection: Efficient long short-term memory (LSTM) based traffic predictor by modeling each road segment in large scale traffic network as a function of neighboring roads.

Attack Context Embedded Trust Scoring Models

Challenge: *Fast* and *accurate* detection of <u>Compromised Smart Meters</u> under temporally distributed stealthy data falsification attacks.

- **Introduction of Attack Responses as Robust Statistical Measures**
  - Pythagorean Means and Real Analysis
  - Median Absolute Deviation
  - Location Parameter Correction
  - Attack Probability Time Ratio
- **Embedding of Responses** → magnify divergence in probability space for information theoretic detection
- **Magnified Divergence** → high detection accuracy, reduced false alarms, decreased convergence time under stealthy attacks
- **Multi-granular anomaly based attack detector → across temporal scales → better unsupervised threshold design**



Key improvement over existing works

- *Detects meters with attack margin > 300W*
- *FA < 10% for large sized grid*
- *Micro-grid level detection of attack presence ~ 100W*

Key Theory → Schur Ostrowski Criterion

$(x_i - y_i)\left(\frac{\partial f}{dx_i} - \frac{\partial f}{dy_i}\right) \geq 0$ → *Schur Convexity*

Products: (1) *ACM Trans. on Privacy and Security,* minor revision, Oct 2019
(2) *IEEE Trans. on Dependable and Secure Computing,* to appear

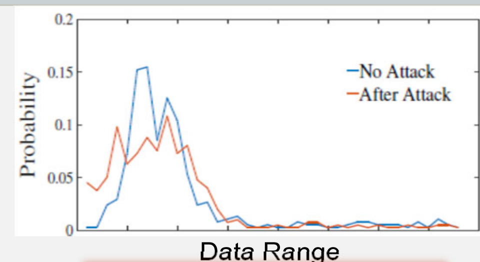
Broader Impacts:

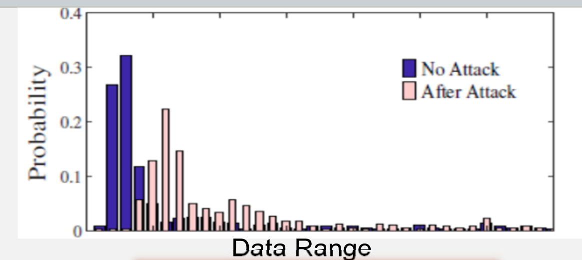
- Includes closed form approximations and performance limits of robust statistics under various attacks
- Validated across big datasets from Texas (800 meters) and Ireland (5000 meters)

Diversity Index Trust Scoring

Problem and Challenges: Detect Components with attack margins much below the standard deviation of data and minimal shape parameter change with high accuracy

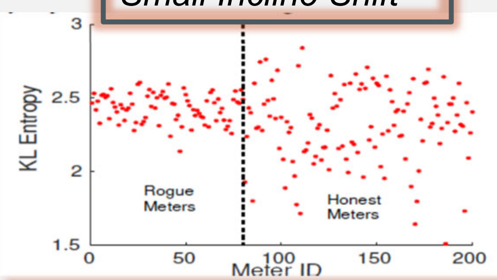
- **Introduced a new approach towards information theoretic trust scores using**
  - *Modified Hill's Diversity Index*
  - *Weighted Version of Renyi Entropy*
- **Captured horizontal, vertical, and incline shifts in statistical distributions**
- **Introduced the notion of Expected Temporal Self Similarity**
- **Optimized Model Parameters**
- **Higher Scores means more dishonest**

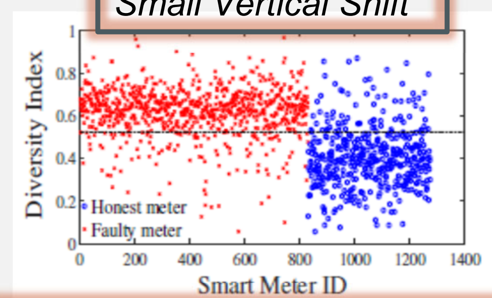




Small Incline Shift

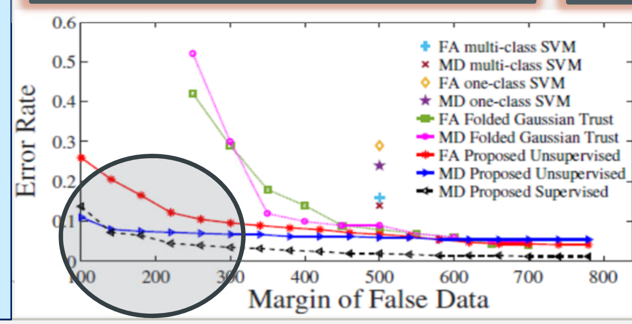
Small Vertical Shift





KL Divergence fails to classify

Our method classifies the same

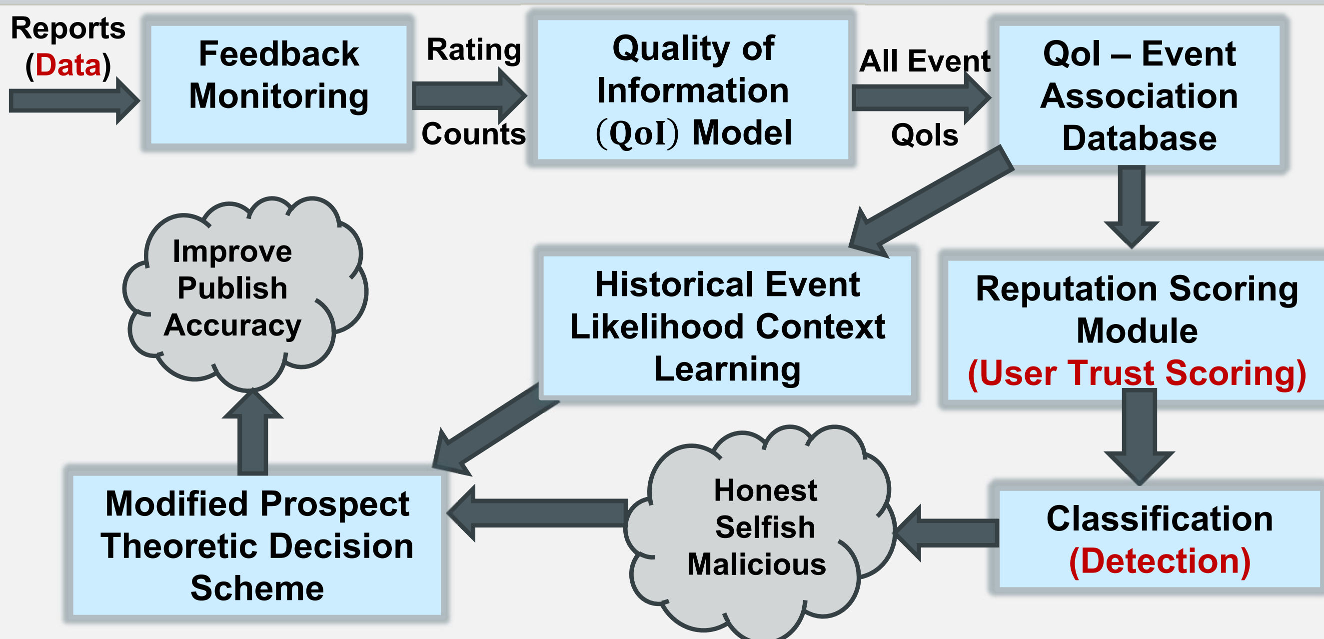


Broader Impacts:

- Applied to mobility data
- Validated by real datasets

(Product: Under double blind review in a conference)

Robust Decision Making under Attacks and Uncertainty



Problem and Challenges: Improve publish decision accuracy in vehicular social sensing under attacks and observation uncertainty

Two Level Decision Tree Formulation

- Which event type ?
- What event confidence ?

Key Theory for Tree Design

- Modified Prospect Theory (CPT)
- Tversky Kahneman Function
- Dual Prob. Weighing Function

Compare with classical decision tree with expected utility maximization

Modified Tversky-Kahneman Utility Function

$$v(\mathcal{C}_j) = \begin{cases} (\mathcal{C}_j)^{\theta_2}, & \text{if } \mathcal{C}_j \geq 0.5 \\ -\lambda_2.(0.5 - \mathcal{C}_j)^{\phi_2}, & \text{if } \mathcal{C}_j < 0.5 \end{cases}$$

Modified Dual Prob. Weighing Function

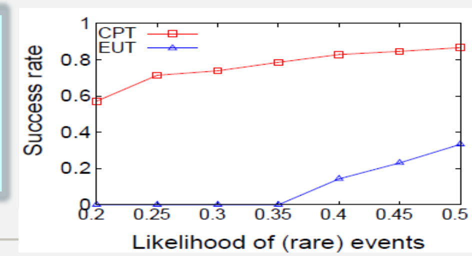
$$\pi^+(p_j) = \frac{p_j^{\delta_1}}{(p_j^{\delta_1} + (1-p_j)^{\delta_1})^{\frac{1}{\delta_1}}},$$

$$\pi^-(\overline{p_j}) = \frac{(\overline{p_j})^{\delta_2}}{((\overline{p_j})^{\delta_2} + (1-\overline{p_j})^{\delta_2})^{\frac{1}{\delta_2}}}$$

$$util(\mathcal{P}) = g_1 * v(\mathcal{C}_j) * \pi^+(p_j) + l_1 * v(\mathcal{C}_j) * \pi^-(\overline{p_j})$$

g_1 = publish given event j occurred **(gain)**

l_1 = publish given event j occurred **(loss)**



(**Products:** IEEE Transactions on Mobile Computing, and ACM Transactions on CPS)

Progress on Thrust 2:

(Shameek Bhattacharjee, Sajal Das, Hayato Yamana)

Privacy-preserving Computations using Fully Homomorphic Encryption (FHE)

Tasks:

2.1 FHE Calculations with Table Search
2.2 Handling Range Search
2.3 Applying FHE to Secure Decisions

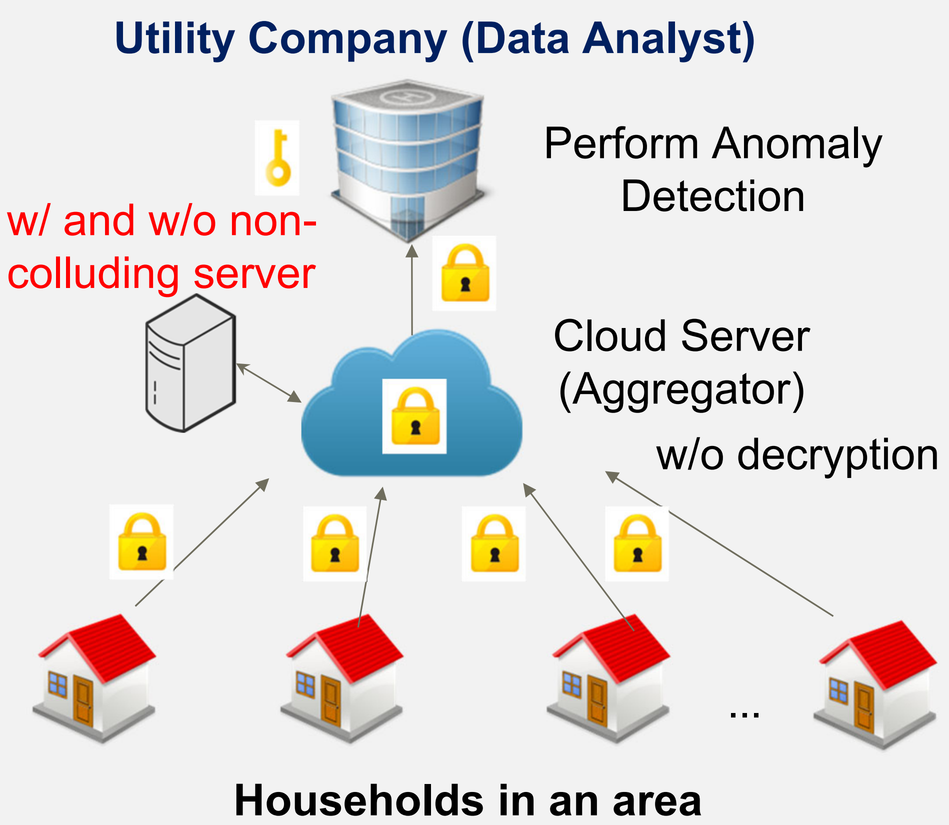
Preserving Privacy

Motivation

- Ensure secure and trustworthy decisions across integrated domains of smart energy and smart mobility networks
- Preserve privacy of each data output by IoT

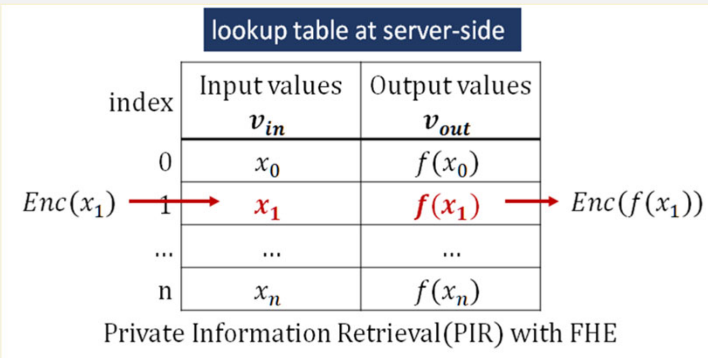
Objectives

- Enhance *Fully Homomorphic Encryption* (FHE) to execute privacy preserving decisions that require complex calculations - TWO TECHNICAL APPROACHES
- Speed-up the FHE execution to satisfy the required performance



Preserving Privacy – Approach 1

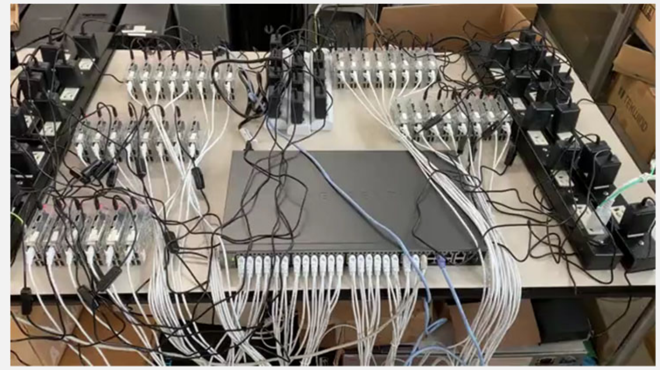
- Table lookup with a non-colluding server to adopt any kinds of calculations at aggregators and to speed-up.



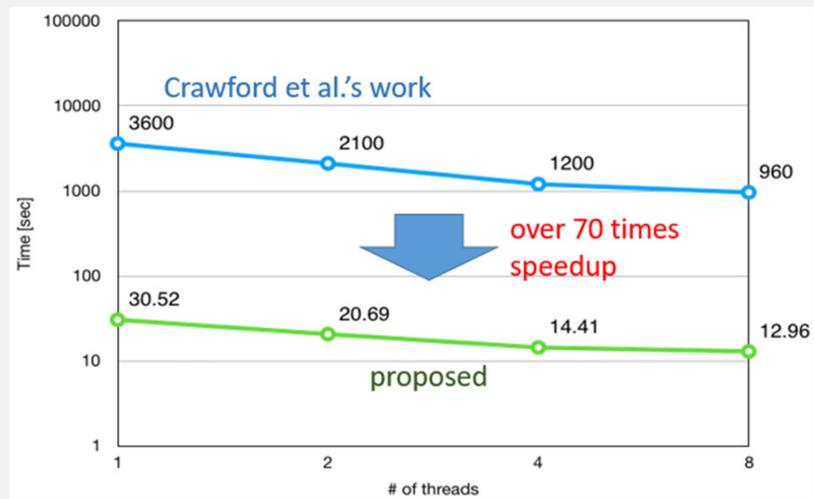
Novelty

- Any kinds of calculations can be adopted
- Integer-based encoding for further speedup in comparison with state-of-the-art research [Crawford et al. 2018] adopting bitwise-based encoding.

R. Li, Y. Ishimaki and H. Yamana, "Fully Homomorphic Encryption with Table Lookup for Privacy-Preserving Smart Grid," *3rd IEEE International Workshop on Big Data and IoT Security in Smart Computing* (BITS), June 2019.



35 working Raspberry Pi's to emulate power meters



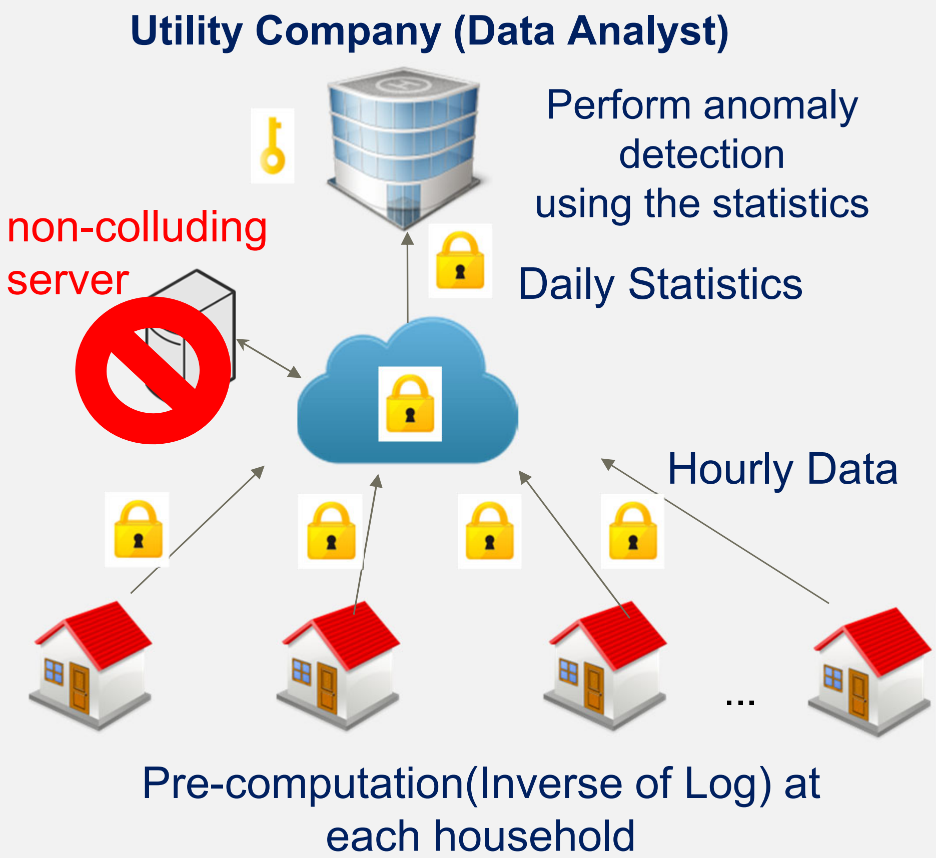
Execution time of one table lookup (Intel Core i7-8700 @3.2 GHz)

Preserving Privacy – Approach 2

- Adopted Approximate Homomorphic Encryption scheme (HEAAN) to leverage floating-point arithmetic (log computation) over encrypted data

Novelty

- Anomaly detection algorithm over encrypted data w/o using non-colluding servers (more secure than Approach 1)
- Pre-computations of logarithm and its inverse at each household
- Optimized for FHE-friendly anomaly detection
- Homomorphic evaluation up to daily statistics that hide individual power consumption



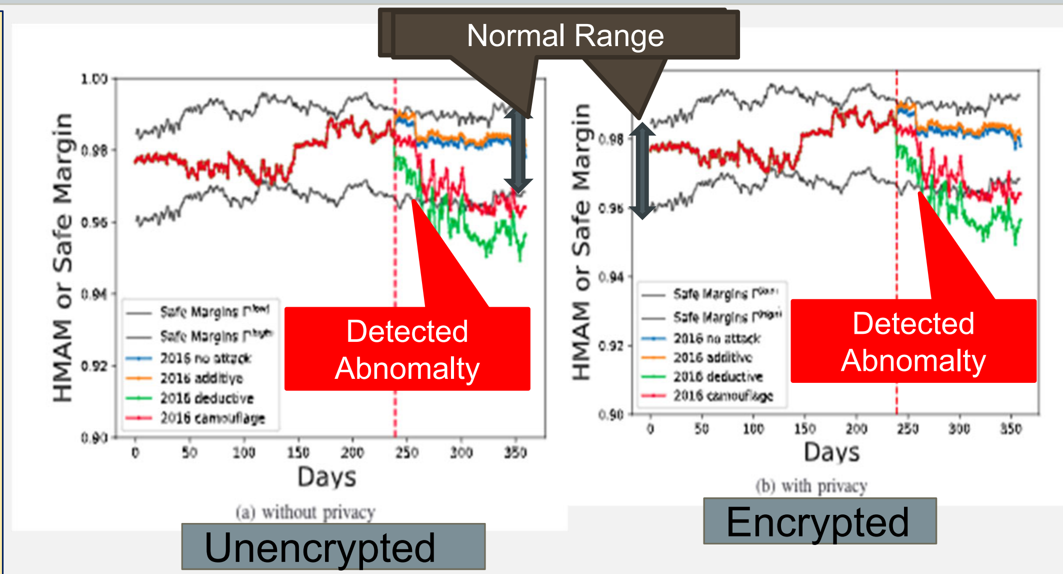
Preserving Privacy: Results and Conclusions

Findings

- Almost same accuracy over both encrypted and unencrypted methods (possible to mitigate small accuracy error via post-processing)
- Server-side computation is feasible: 3.303 s/hour (each hourly time-slot)

Next Challenges

- Enhance table lookup method to adopt multiple values, and propose less-than comparison for input values to handle wide range of inputs
- Balance Privacy-Performance trade-off with quantification (e.g., FHE with Differential Privacy)



Ciphertext Size:
Household → Server: 2,270KB/hour
Server → Utility: 224KB/date

All experiments are with 136 households. Experiment is done with Intel Xeon CPU E5-1620 v4 @ 3.50GHz in single-threaded mode.

Progress on Thrust 4:

(Abhishek Dubey, Keiichi Yasumoto)

Developing Secure and Trustworthy Middleware Architecture

Tasks:

4.1 Distributed Aggregation
4.2 Secure Anonymization
4.3 Decision Making under Trade-offs

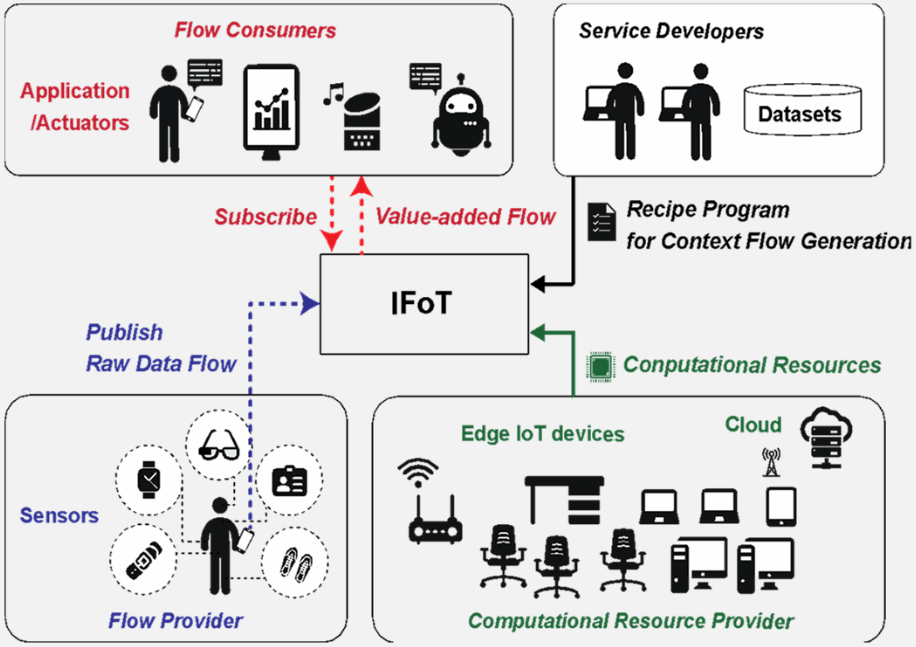
Middleware for Smart and Connected Communities

Challenges

- How to build multi-domain architecture for smart mobility and smart energy?
- How and where to implement computations related to privacy, security, and trust?
- What are computational/resource challenges for scalability?

Goal

Propose a novel middleware framework that distributes security features across multiple tasks and incorporates privacy, trustworthiness, resource constraints, and distributed decision support.



We have designed and developed IFoT middleware [SEC2018]

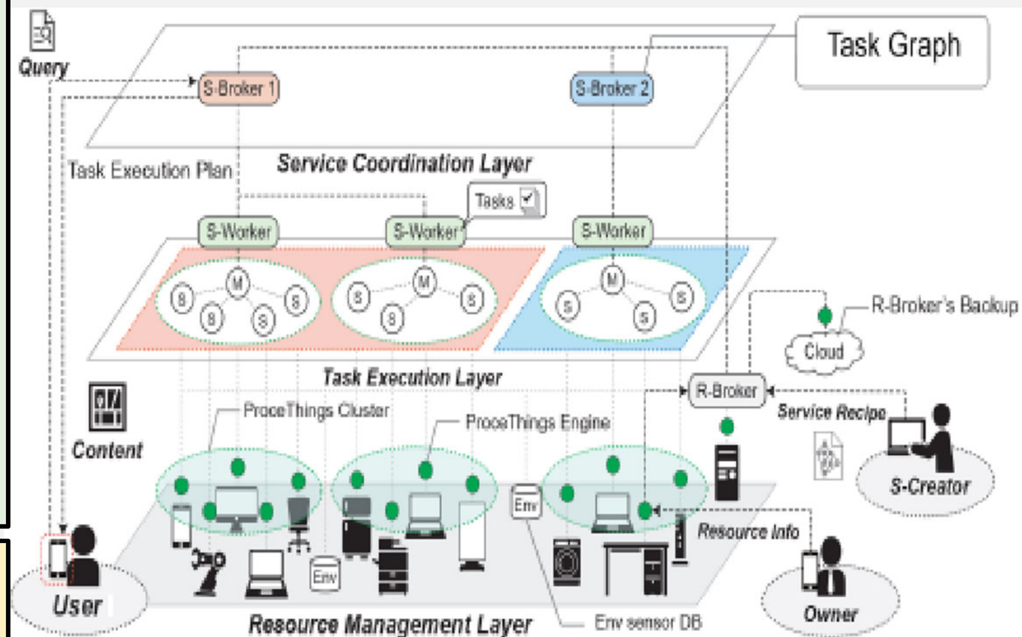
In-situ Distributed Computation and Aggregation

Innovation:

1. Designed a middleware architecture to assign tasks over IoT devices (e.g., RSUs, smart meters) taking into account required QoS level
2. Implemented/ evaluated a prototype middleware
   - Used Docker technology for easy deployment
   - Implemented a smart workspace use case (occupancy level of multiple rooms is queried)
3. Developed Smart Transportation Service Emulation Testbed

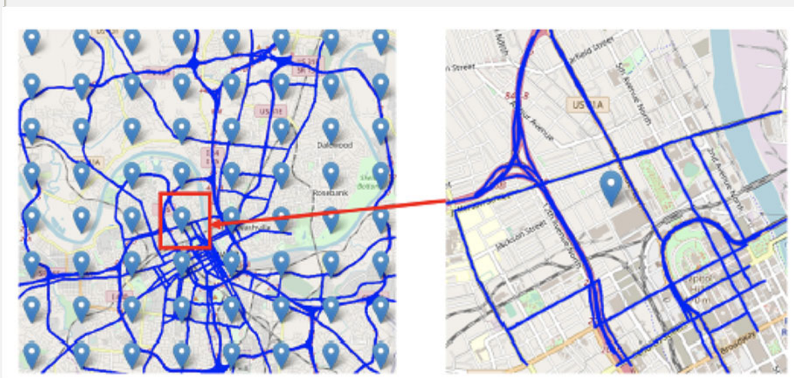
Findings:

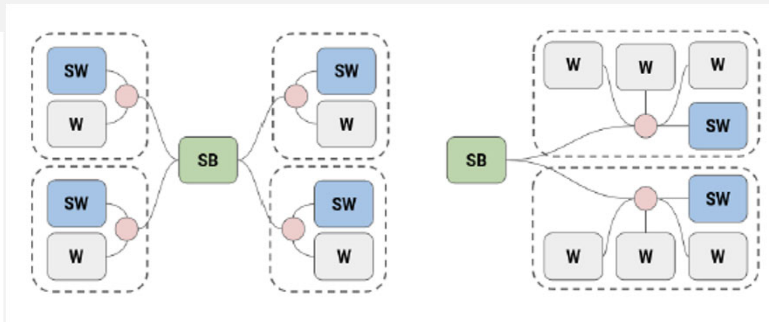
- Smart and Connected Community services can be realized by distributed execution of tasks assigned over IoT devices
- Query response time can be reduced by distributing tasks over IoT devices



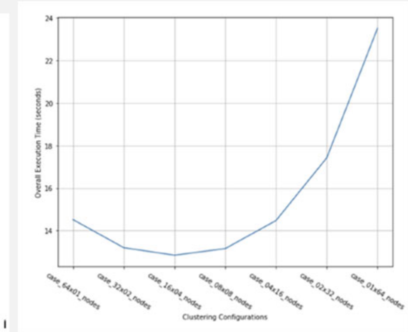
J. P. Talusan, K. Yasumoto, et al., “Evaluating Performance of In-Situ Distributed Processing on IoT Devices by Developing a Workspace Context Recognition Service," *IEEE PerCom Workshops,* 2019.

Smart Transportation Middleware





Processing time of a query (travel time b/w points) for different network configurations are tested



Processing time

80 km^2 map of Nashville, TN is divided into 8 x 8 grids, where each grid deploys an RSU which receives/stores traffic data (vehicle speed data) within the grid.

J. P. Talusan, K. Yasumoto, A. Dubey, S. Bhattacharjee, et al: Smart Transportation Delay and Resiliency Testbed based on Information Flow of Things Middleware. *IEEE BITS* 2019.

Ongoing work

- Develop federated learning on RSUs
- Optimal task assignment problem and algorithm with federated learning
- Develop and test anomaly detection algorithm (Target: submit to IoTDI 2020)

Progress on Thrust 5:

(Abhishek Dubay, Hirozumi Yamaguchi)

Validation with Real Datasets

Tasks:

5.1 Smart Transportation Application
5.2 Smart Energy Application

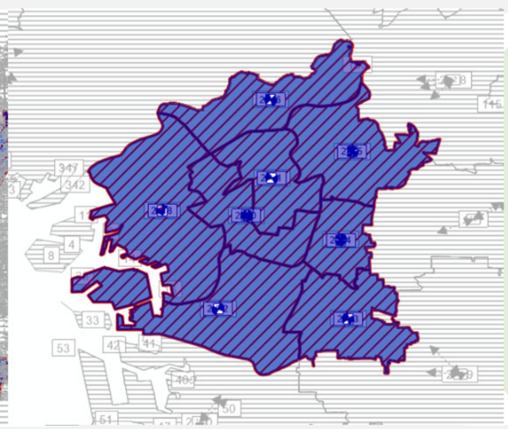
Validation with Real Datasets

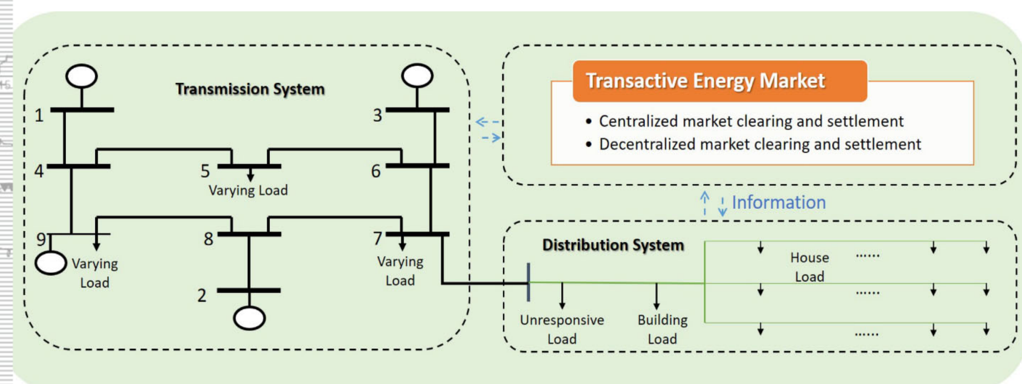
Objective: Validate the proposed models and approaches using smart mobility and smart energy distribution / consumption scenarios with real-world datasets

Approach:

- Generate large-scale mobility data from real datasets in Osaka

- Design a transactive energy testbed that can integrate energy market data

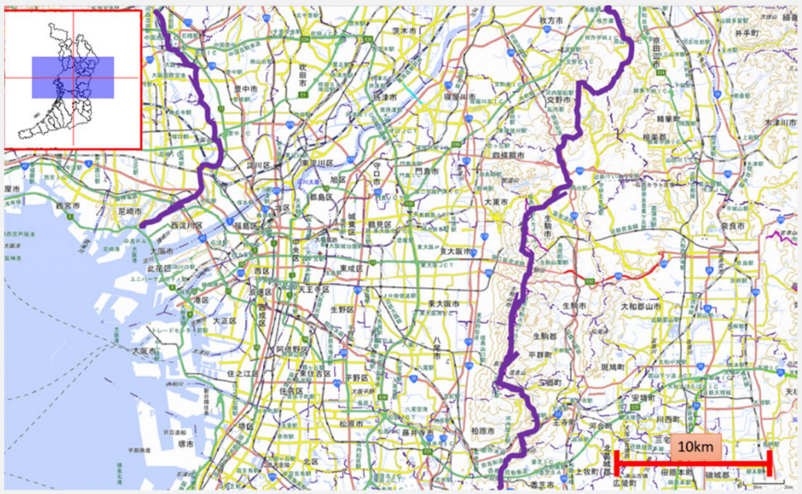


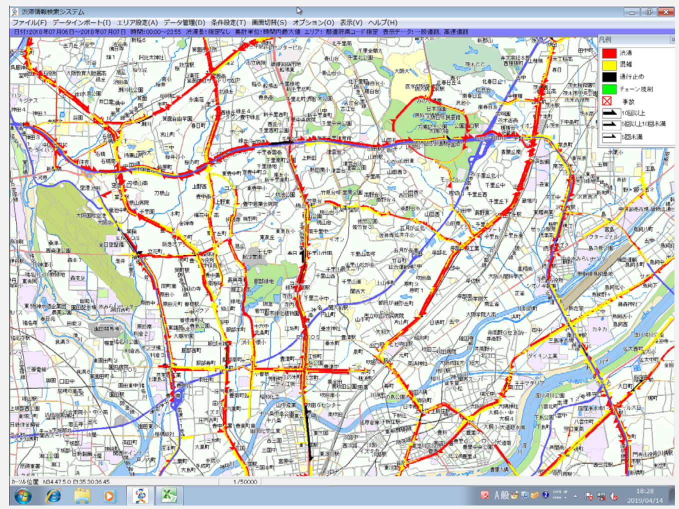


Real World Data Sets

Road Traffic Census data (obtained by nation-wide survey by Ministry Road Bureau) : contains traffic volume & velocity and OD of a particular day

VICS (obtained via IR beacons) : contains queue length of major city roads and highways for 3months (Osaka prefecture whole region)





Infrared beacons (Ordinary trunk roads)

Infrared beacons are installed on the ordinary trunk roads and provide information covering about 30 km in the forward direction and about 1 km in the rear direction.

- Traffic congestion and travel time information.
- Information on restrictions due to accidents, construction, disasters, and weather conditions.
- Parking availability.

1000+ road sections

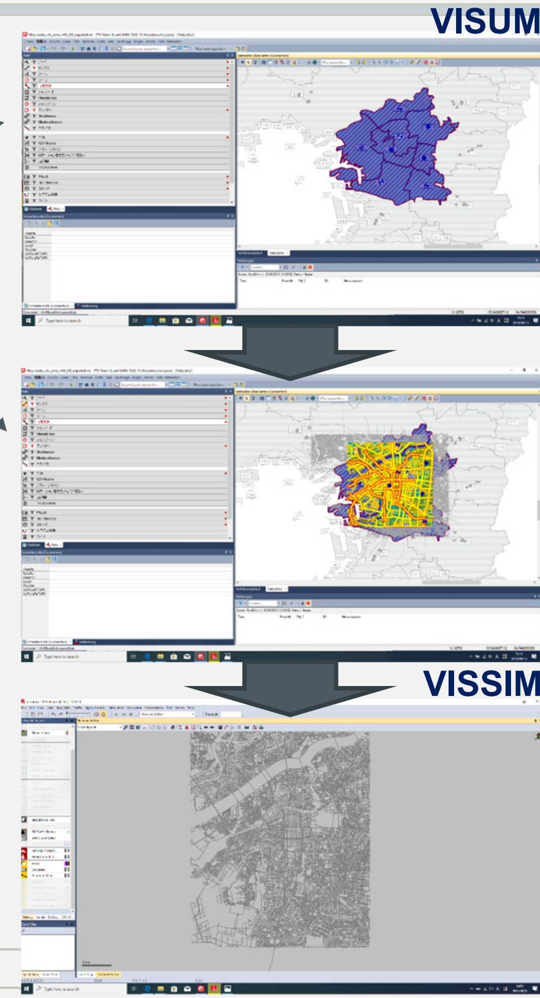
two vehicle types

hourly traffic volume

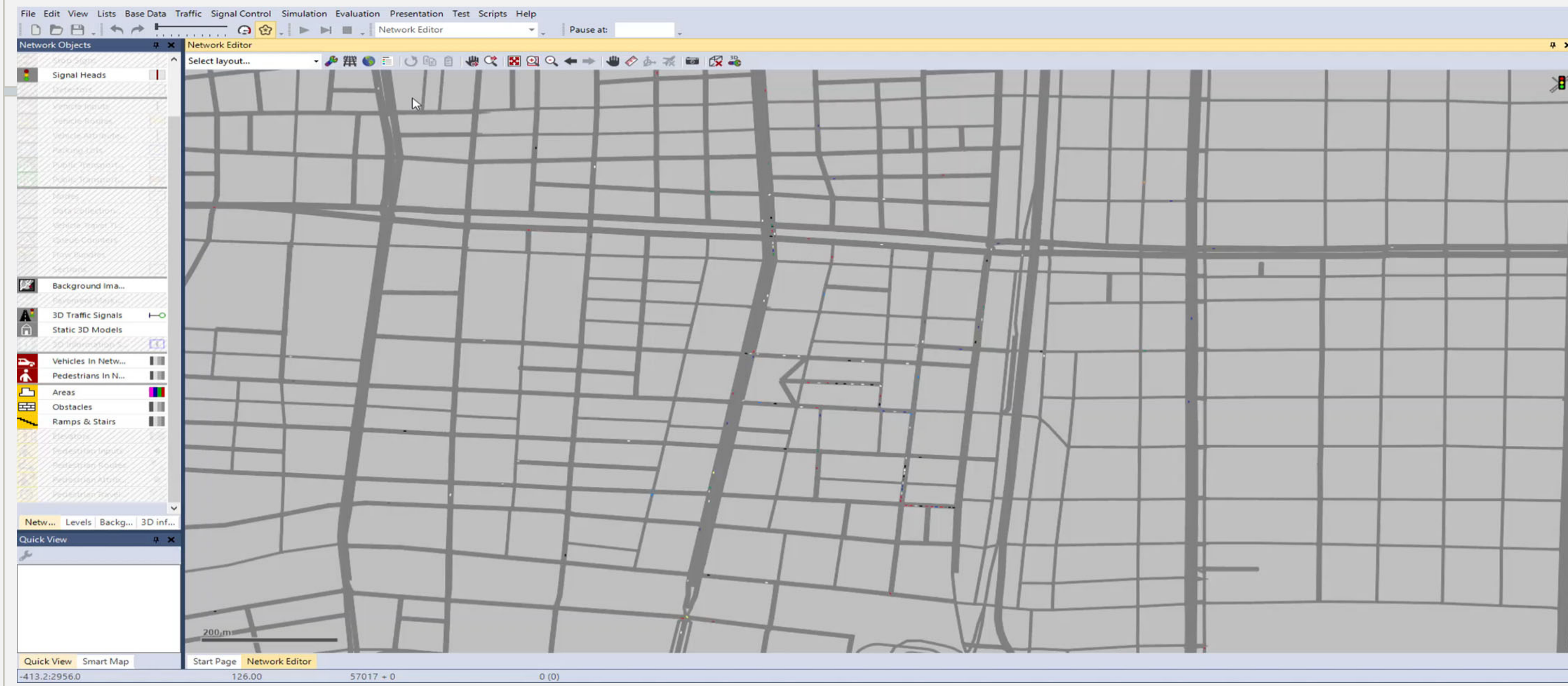
都道府県指定市コード	交通量調査単位区間番号	道路種別	路線番号	平成27年度交通量調査観測・非観測の別	個別調査観測値活用の別	12・24時間観測の別	交通量観測年月日	天候	上り・下りの別	車種区分	交通量（台/時） 7時台	8時台	9時台	10時台	11時台	12時台	13時台	14時台	15時台	16時台	17時台	18時台	19時台	20時台	21時台	22時台	23時台	0時台	1時台	2時台	3時台	4時台	5時台	6時台	昼間12時間自動車類交通量（台）	24時間自動車類交通量（台）
27140	10	1	1720	1	0	2	20151008	6	1	1	2981	2237	1821	1709	1583	1644	1674	1934	2122	2419	2886	2204	1432	1014	770	545	364	265	181	128	101	172	413	2254	25214	32853
27140	10	1	1720	1	0	2	20151008	6	1	2	668	626	945	930	858	750	731	877	794	736	536	404	305	333	260	186	151	151	197	176	219	248	418	697	8855	12196
27140	10	1	1720	1	0	2	20151008	6	2	1	2751	2459	2101	2098	2059	1766	1721	1777	2064	2090	2662	2622	1590	1177	929	638	368	297	210	161	176	191	345	1353	26170	33605
27140	10	1	1720	1	0	2	20151008	6	2	2	751	701	811	1103	982	816	668	809	764	592	606	389	325	209	182	150	154	198	225	205	262	245	430	613	8992	12190
27140	20	1	1720	1	0	2	20151008	6	1	1	2652	1962	1573	1441	1318	1426	1444	1666	1842	2088	2582	1918	1254	885	675	483	317	229	159	107	90	158	368	2035	21912	28672
27140	20	1	1720	1	0	2	20151008	6	1	2	614	574	873	860	793	686	668	805	723	666	488	378	273	311	250	179	144	143	189	163	203	234	392	639	8128	11248

Osaka City Vehicle Mobility Generation

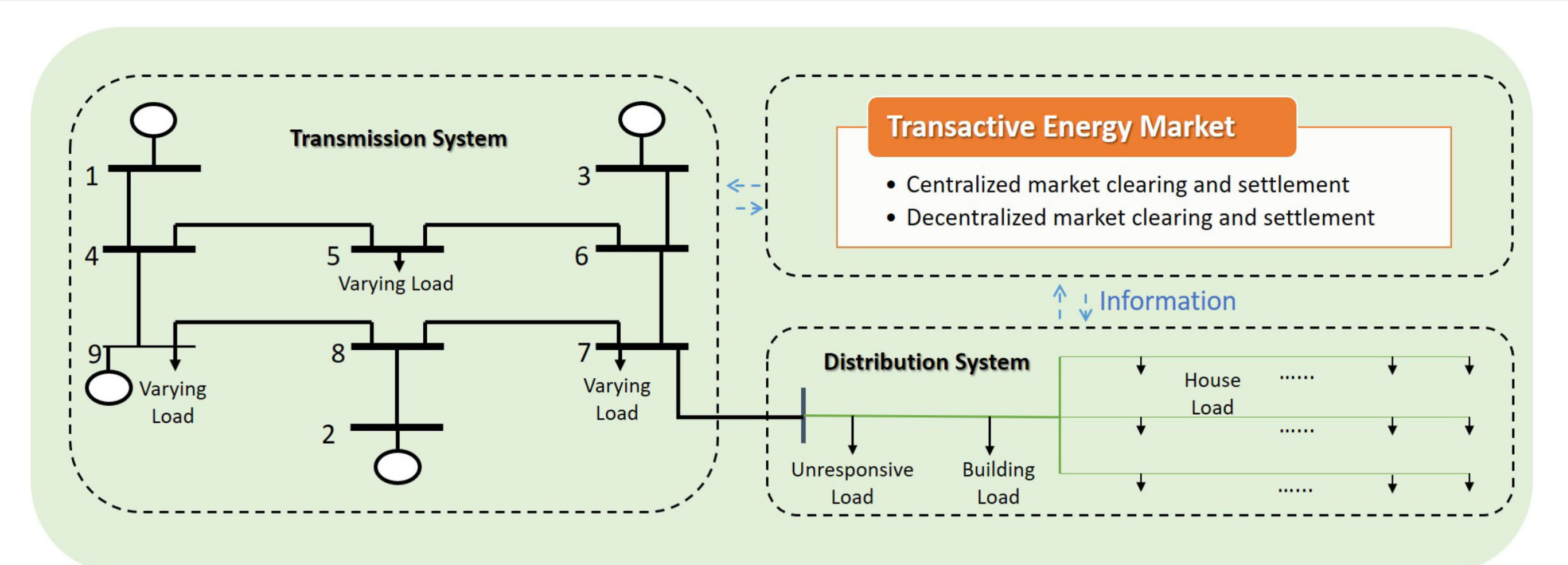
- **Procedure**
  - Arrange map (Open Street Map)
  - Set ODs (Census Survey Data)
  - Calculate route for each OD (by Traffic Simulator)
  - Determine OD volumes (Census Survey Data)
  - Adjust link-level traffic volume (VICS)
- **The generated mobility data includes**
  - 10K – 60K vehicles in Osaka city region
  - 90 days (will include data of the day of “big rain disaster” in July 2018)
- **Next Challenges:**
  - RSU placement design in 5G realistic situations
  - Evaluation of the impact of anomaly data on decision making using Osaka and Nashville data



Simulator Video



Transactive Energy Testbed



Architecture of TESST

Physical System

Transactive Energy Market

Network Simulator

Centralized Market Option

Decentralized Market Option

STEAM Project: Broader Impacts

➢ Interdisciplinary Education and Experiential Learning for Students:

- Praveen Madhavarapu; Prithwiraj Roy (Missouri S&T and Western Michigan Univ., USA)
- Michael Wilbur; Geoff Pettet (Vanderbilt Univ., USA)
- Yu Ishimaki; Ruixiao Li (Waseda Univ., Japan)
- Jose Paolo Talusan; Francis Tiausas (NAIST, Japan)
- S. Choochotkaew; Yuki Akura (Osaka Univ. Japan)

➢ Student Visit Exchanges:

- Y. Ishimaki (Waseda) visited MST in Aug-Sep 2018 for one month, and WMU for 2 weeks in June and Oct 2019
- P. Madhavarapu and P. Roy (Missouri S&T) respectively visited WMU for 4 weeks in July 2019 and Aug 2019
- J.P. Talusan (NAIST) visited Vanderbilt for 3 weeks in June 2019.
- M. Wilbur (Vanderbilt) visited WMU for 1 week.

➢ Integration of Research into Courses:

- Dubey (Vanderbilt Univ.) integrated anomaly detection module in his course on *Reliable Distributed Systems*, fall 2019.
- Shameek (WMU) incorporated CPS security challenges and smart grid security solutions in his course *Science of Cybersecurity*, spring 2019.

➢ Outreach (Workshop Organization):

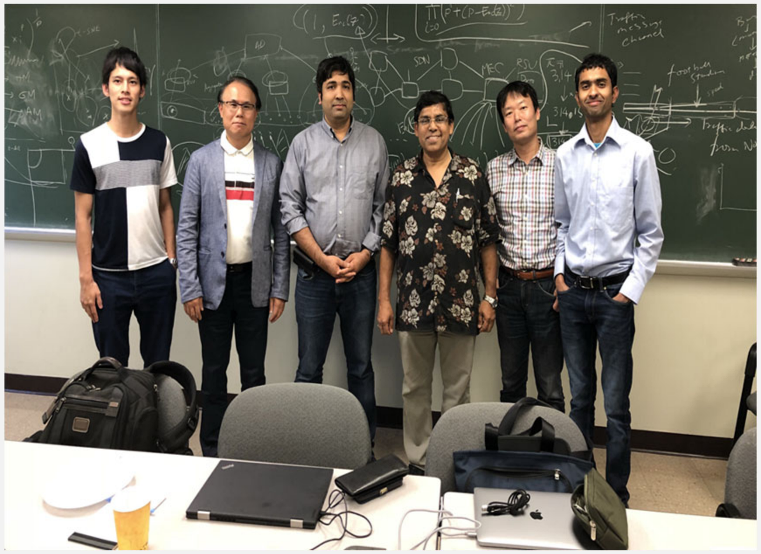
- Big Data and IoT Security (BITS), in conjunction with IEEE SmartComp 2019, Washington, DC, June 2019.
- Science of Smart City Operations and Platforms Engineering (SCOPE), during CPS-IoT Week, Montreal, Canada, April 2019.

Coordination and Collaboration

- Weekly Skype meeting; Very coherent group
- Joint publications by PIs and their students
- Co-organization of BITS and SCOPE workshops in 2019
- Planned Vision Paper: Security in Integrated Energy and Mobility
- Planned Special Issue Editing: Magazine and/or Journal

All Hands Meeting:

- Missouri S&T: Sept 14-15, 2018
- Tokyo: Oct 26-27, 2018 (JUNO2 Kick-off)
- Kyoto: March 11-14, 2019 (IEEE PerCom)
- Washington, DC: June 12-14, 2019 (IEEE SmartComp)
- Chicago: Oct 11, 2019 (JUNO2 PI Meeting)
- Bologna: June 20-23, 2020 (IEEE SmartComp)
- Nara: January 5-8, 2021 (ACM ICDCN)



September 14-15, 2018 meeting (Missouri S&T)

Collaborative Publications

1. S. Roy, N. Ghosh, and S. K. Das, "bioSmartSense: A Bio-inspired Data Collection Framework for Energy-efficient, QoI-aware Smart City Applications," *17th Annual IEEE International Conference on Pervasive Computing and Communications* (PerCom), Kyoto, Mar 2019.
2. Y. Nishimura, A. Fujita, A. Hiromori, H. Yamaguchi, T. Higashino, A. Suwa, H. Urayama, S. Takeshima and M. Takai, "A Study on Behavior of Autonomous Vehicles Cooperating with Manually-Driven Vehicles," *17th Annual IEEE PerCom*, pp. 212-219, Kyoto, Mar 2019.
3. J. P. Talusan, K. Yasumoto, et al, "Evaluating Performance of In-Situ Distributed Processing on IoT Devices by Developing a Workspace Context Recognition Service," *IEEE PerCom Workshop*, Kyoto, Mar 2019.
4. H. Yamaguchi, "Toward Urban Vehicle Mobility Modeling in Japan," *4th International Science of Smart City Operations and Platforms Engineering Workshop* (SCOPE), pp. 1-6, Apr 2019.
5. R. Li, Y. Ishimaki and H. Yamana, "Fully Homomorphic Encryption with Table Lookup for Privacy-Preserving Smart Grid," *IEEE BITS2019 Workshop*, pp. 19-24, June 2019.
6. M. Wilbur, A. Dubey, B. Leão and S. Bhattacharjee, "A Decentralized Approach for Real Time Anomaly Detection in Transportation Networks," *4th IEEE International Conference on Smart Computing* (SMARTCOMP), Washington, DC, pp. 274-282, June 2019.
7. J. P. Talusan, K. Yasumoto, A. Dubey, and S. Bhattacharjee, "Smart Transportation Delay and Resiliency Testbed based on Information Flow of Things Middleware," *IEEE BITS Workshop*, June 2019.
8. Y. Ishimaki, H. Yamana, "Non-Interactive and Fully Output Expressive Private Comparison," *INDOCRYPT*: 355-374, 2018.
9. S. Bhattacharjee and S. K. Das, "Detection and Forensics against Stealthy Data Falsification in Smart Metering Infrastructure," *IEEE Transactions on Dependable and Secure Computing*, to appear, 2019.
10. R. P. Barnwal, N. Ghosh, S. K. Ghosh, and S. K. Das, "Publish or Drop Traffic Event Alerts? Quality-aware Decision Making in Participatory Sensing-based Vehicular CPS," *ACM Transactions on Cyber-Physical Systems*, to appear, 2019.
11. S. Bhattacharjee, N. Ghosh, V. K. Shah, S. K. Das, "QnQ: A Quality and Quantity Unified Approach for Secure and Trustworthy Crowdsensing, *IEEE Transactions on Mobile Computing*, to appear, 2019.
12. A. Sturaro, S. Silvestri, M. Conti, and S. K. Das, "A Realistic Model for Failure Propagation in Interdependent Cyber-Physical Systems," *IEEE Transactions on Network Science and Engineering*, to appear, 2019.
13. S. Bhattacharjee, V. P. Madhavarapu, S. Silvestri, and S. K. Das, "Attach Context Embedded Data Driven Trust Diagnostics in Smart Metering Infrastructure," *ACM Transactions on Privacy and Security*, under minor revision, Oct 2019.

JUNO2: US-Japan Collaborative Project

STEAM: Secure and Trustworthy Framework for Integrated Energy and Mobility in Smart Connected Communities

PI Meeting – Chicago, October 11, 2019

Thank You