JUNO2: US-Japan Collaborative Project

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

PI Meeting (August 2021)

Our Super Team

MISSOURI S&T

Sajal K. Das

WESTERN MICHIGAN UNIVERSITY

Shameek Bhattacharjee

VANDERBILT

Abhishek Dubey

Hayato Yamana

Waseda University

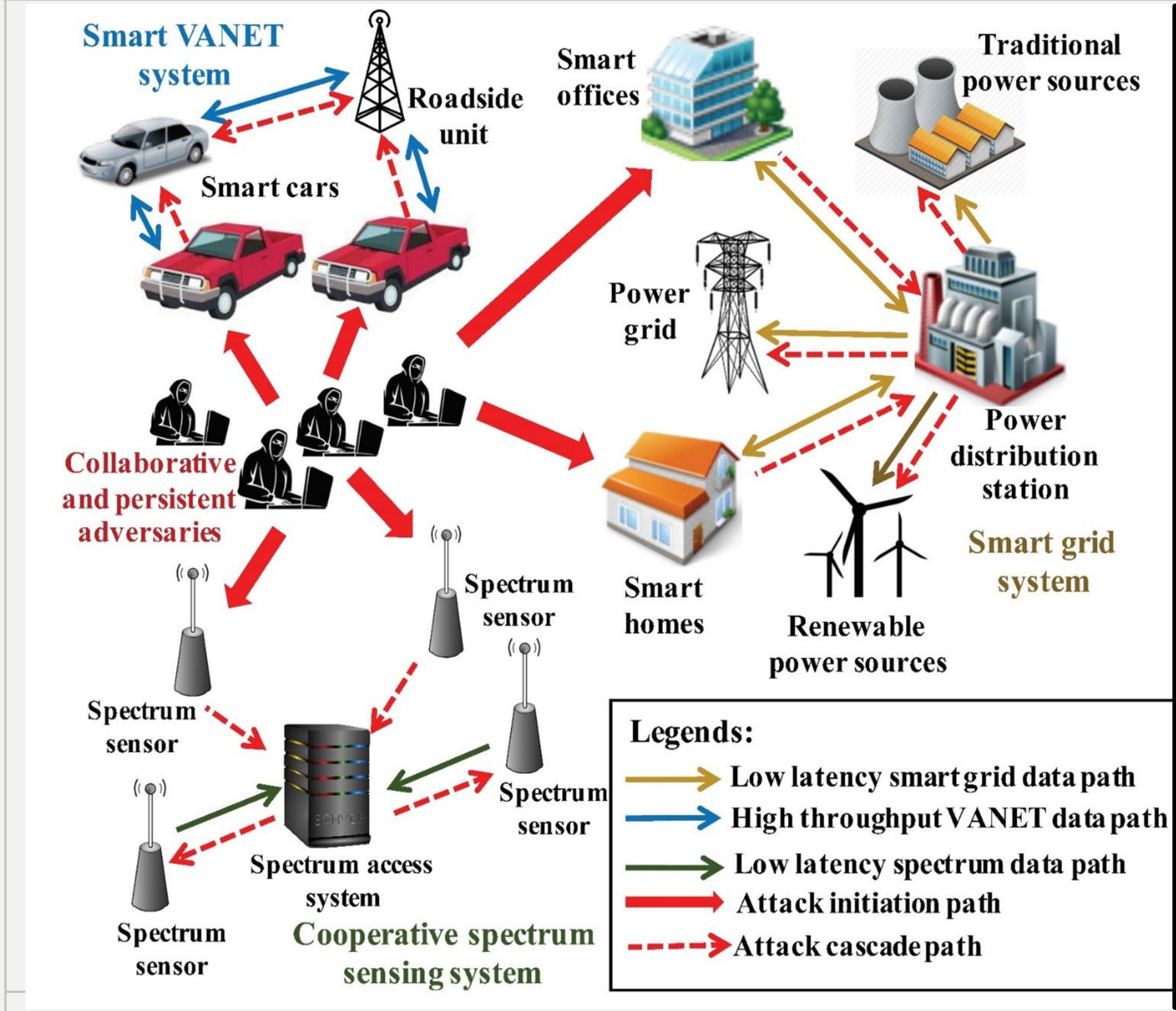
Hirozumi Yamaguchi

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, resilience and privacy preservation

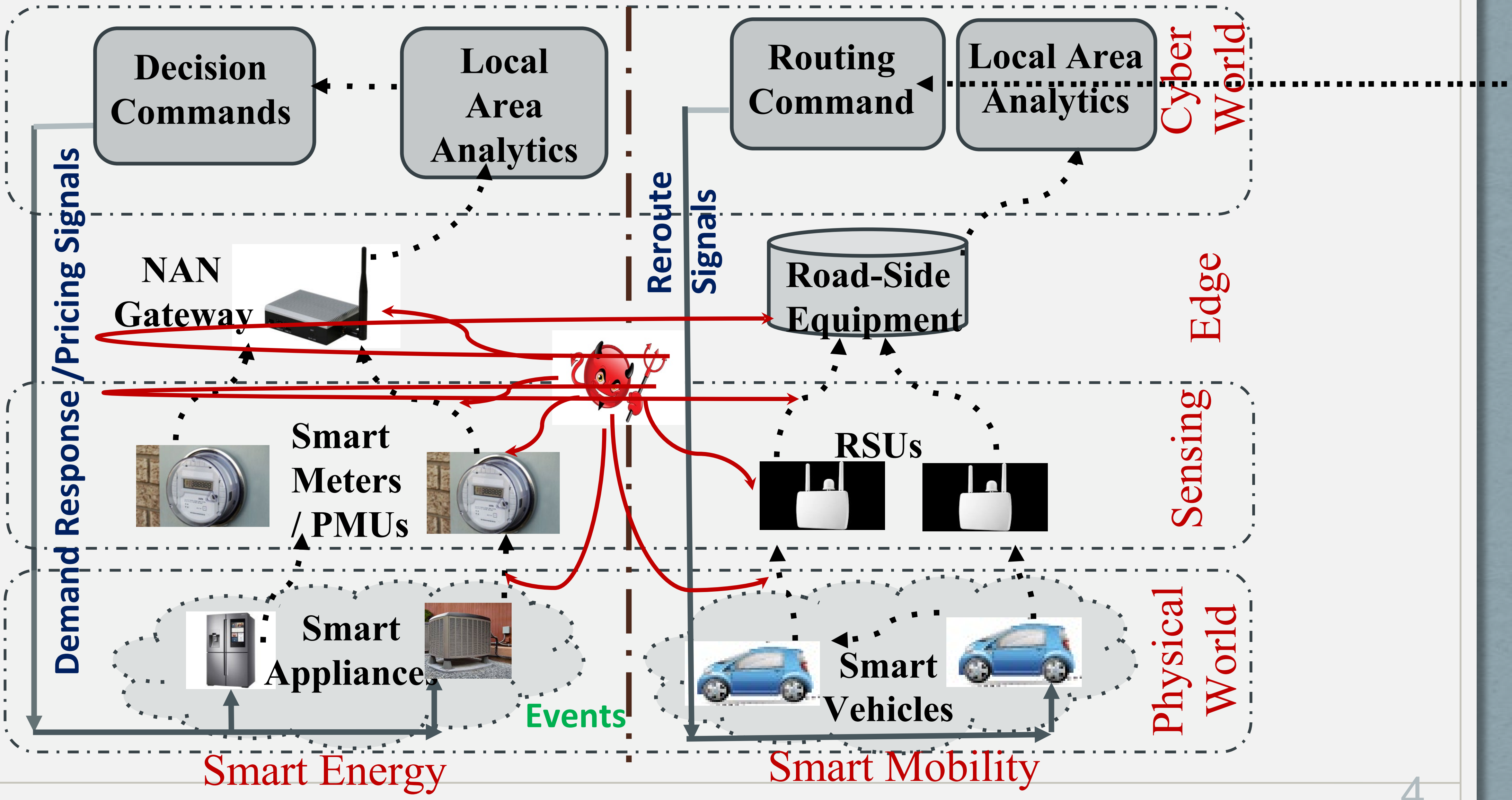
Unique Challenges in Securing S & CC

- Large variations in individual endpoint data due to human behavior 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.

Energy and Mobility: Integrated CPS View



STEAM Project: Intellectual Merit

Thrust 1: Secure and Trustworthy Decision Making under Uncertainty (Bhattacharjee, Das)

- **Task 1.1: Lightweight Anomaly Detection:** Fast, efficient and accurate decentralized anomaly detection for compromised smart meters and transportation sensors under stealthy attacks, using Pythagorean means and long short-term memory (LSTM) networks.
- **Task 1.2 Trust Models:** Trust scoring models for diagnosing device compromisation with attack margins much below standard deviation.
- **Task 1.3: Trustworthy Decision Making:** Dependable decisions

Thrust 2: Privacy-Preserving Computations using FHE (Yamana, Bhattacharjee, Das)

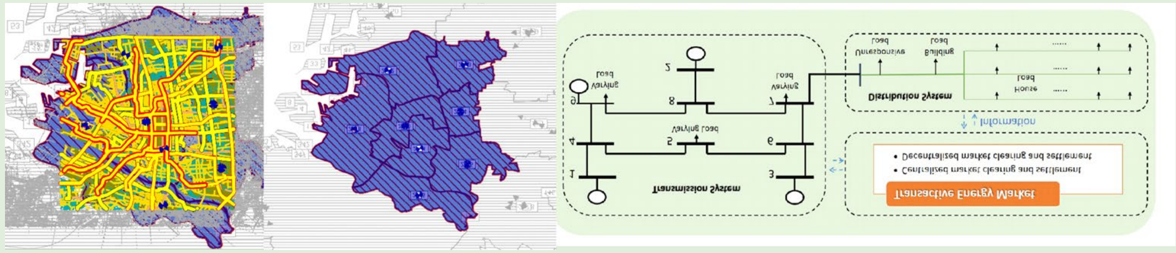
- **Task 2.1: FHE (Complex) Calculations:** Efficient schemes to compute FHE for privacy preserving decisions
- **Task 2.2: Handling Range Search:** Table lookup with non-colluding server for calculations at aggregator for higher speed-up;
- **Task 2.3: Applying FHE to Secure Decisions:** Approximate Homomorphic Encryption (HE) to leverage floating-point arithmetic (e.g., log computation) over encrypted data.

Thrust 4: Developing a Secure and Trustworthy Middleware Architecture (Dubey, Yasumoto)

- **Task 4.1: Distributed Aggregation:** Developed a middleware platform for SCC apps via distributed processing at edge nodes
- **Task 4.2: Secure Anonymization:** Developed a secure anonymization mechanism for smart mobility apps
- **Task 4.3: Decision Making under Trade-offs:** Balance query throughput, route accuracy, and privacy protection level

Thrust 5: Validation With Real Datasets for Smart Mobility and Energy (Yamaguchi, Dubey)

- **Task 5.1: Smart Transportation Application:** Large scale road traffic data collected from Osaka, Japan and Nashville, USA.
- **Task 5.2: Smart Energy Application:** Transactive energy testbed.



Thrust 1 Results:

(Shameek Bhattacharjee, S. K. Das)

Secure and Trustworthy Decision Making under Uncertainty

Tasks:

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

Task 1.1 Anomaly Detection

Threat Model:

- Attacks from sensing layer affect operations in smart energy and mobility systems
- Special Events such as
  data omission □ energy
  traffic accidents □ mobility

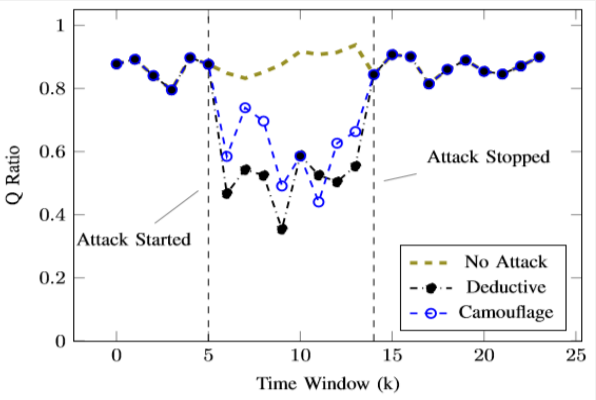
Macro Level: designed for large scale decentralized anomaly detection in real time for energy and transportation □ *Pythagorean Mean*

Micro Model: highly accurate and fine grained-anomaly detection □ *LSTM, Folded Gaussian Trust Models*

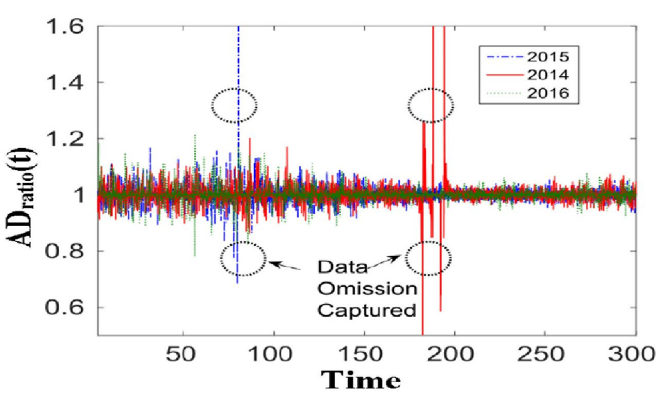
Key Theory → Schur Ostrowski Criterion

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

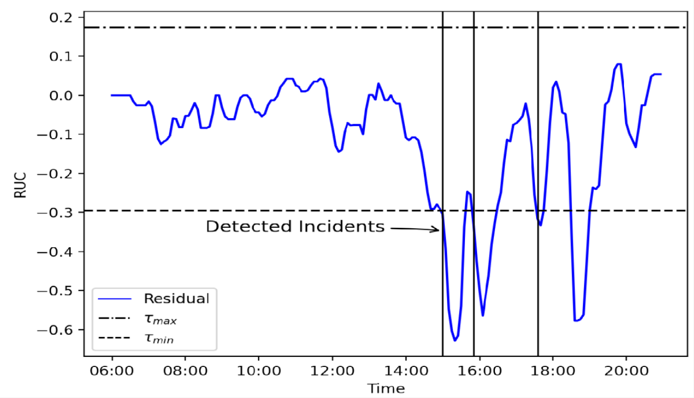
Validation:
Mobility: real data from Nashville, TN
Energy: real data from TX and Ireland



Anomaly under attacks



Anomaly under data omission



Anomaly under accidents

Metrics:

- Q ratio
- AD_{ratio}
- RUC

Derived from Pythagorean Means

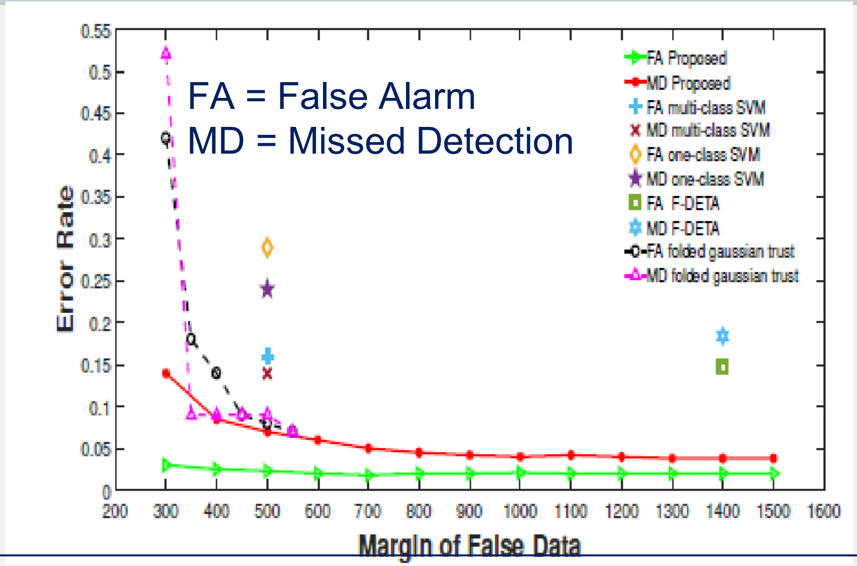
Products:

(1) IEEE Trans. on Dependable and Secure Computing 2021
(2) ACM Trans. on Privacy and Security 2021
(3) IEEE Smart Computing Conference 2019
(4) IEEE Big Data and IoT Security Workshop 2019
(5) IEEE Big Data Conference (in preparation)

Task 1.2: Trust Scoring Models

Challenge: *Fast* and *accurate* detection of Compromised Smart Meters, RSUs, users of distributed data falsification attacks.

- **Introduction of Attack Responses as Robust Statistical Measures**
  - Pythagorean Means and Real Analysis
  - 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 threshold design indicates attack responses**



Key Theory:

- *Folded Gaussian Trust Model (Density based)*
- *Response Enhanced KL Divergence (Distance based)*
- *Neuro-cognitive models (Behavioral AI based)*

Key improvement over existing works

- *Detects meters with attack margin > 300W*
- *FA < 10% for large sized grid*
- *Compared with existing works*
- *Detects malicious users in vehicular crowdsensing applications*

Products:

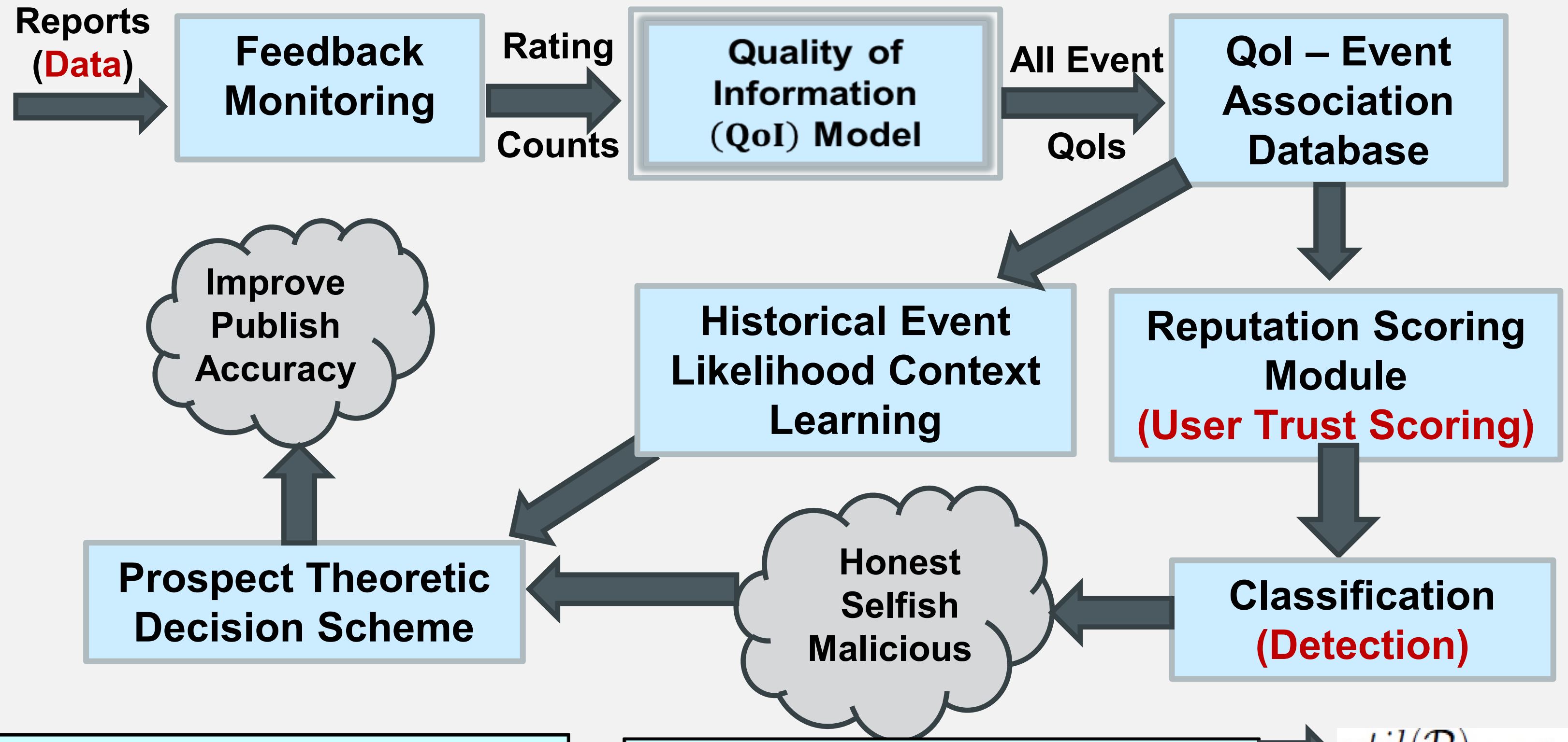
(1) *ACM Trans. on Privacy and Security, '21* ***(2)*** *IEEE Trans. on Mobile Computing, '21*

(3) *Journal (in preparation for IEEE TIFS)* ***(4)*** *IEEE MASS '20*

Broader Impacts:

- Includes closed form approximations and performance limits under attacks
- Validated across big datasets from Texas (800 meters) and Ireland (5000 meters)
- Preliminary efforts show success with other IoT domains (e.g., smart home)

Task 1.3: Trustworthy Decision Making



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

Compare with classical decision tree with expected utility maximization

Modified Tversky-Kahneman Utility Function

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

Modified Dual Prob. Weighing Function

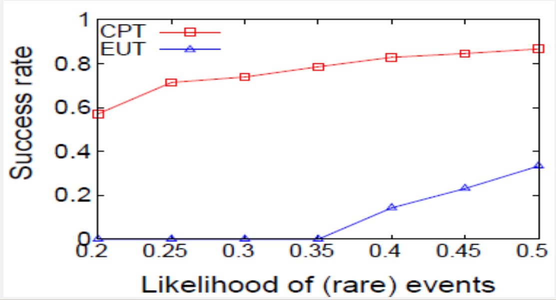
$$\pi^+(p_j) = \frac{p_j^{\delta_1}}{(p_j^{\delta_1} + (1-p_j)^{\delta_1})^{\frac{1}{\delta_1}}},$$

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

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

g_1 = publish given event j occurred (gain)

l_1 = publish given event j occurred (loss)



Products: **(1)** *IEEE Trans. on Mobile Computing '20* **(2)** *ACM Trans. on CPS '20,* **(3)** *IEEE WoWMoM '21*

Result on Thrust 2:

(S. Bhattacharjee, S. K. Das, H. Yamana)

Privacy-preserving Computations using Fully Homomorphic Encryption (FHE)

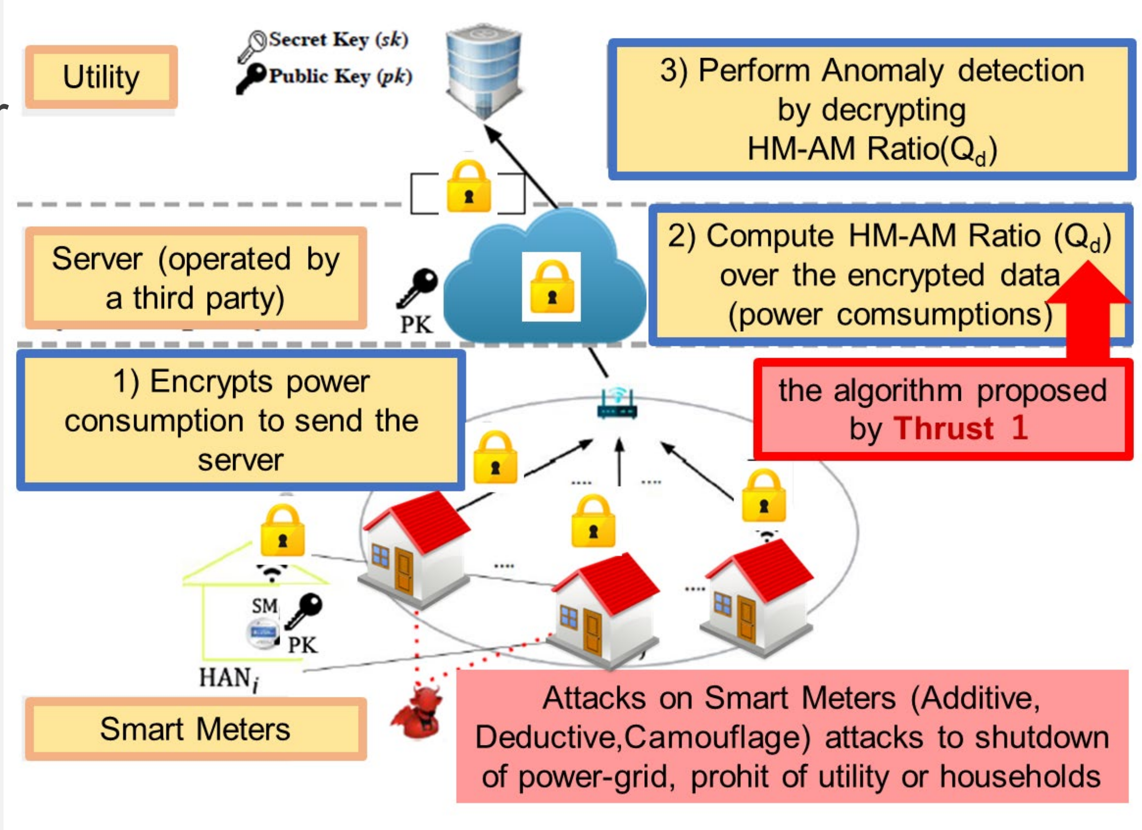
Tasks:

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

Preserving Privacy – Goal and Results

- Goal
  - Establishing a **privacy-preserving anomaly detection** method by adopting both Thrust 1 and "fully homomorphic encryption(FHE)," which has not been possible in the past.

- Results
  - Enabling **10 sec** anomaly detection for by our proposed special optimization (**Method 1**)
  - Enabling **5 min** anomaly detection for power-grid by adopting "table search mechanism," which is applicable in various anomaly detection algorithms. (**Method 2**)



[Note]

- Used 2014 to 2016 power consumption data of 200 households in Texas.
- The requirement for power-grid is every 10 min detection.
- Experiments on single core execution on the server (Intel Xeon E5-1620v4)

Preserving Privacy – Method 1

Calculation for the anomaly detection

timeslot

$$\begin{pmatrix} p_1^{(1)} & p_1^{(2)} & \cdots & p_1^{(N)} \\ p_2^{(1)} & p_2^{(2)} & \cdots & p_2^{(N)} \\ \vdots & \cdots & \cdots & \vdots \\ p_T^{(1)} & p_T^{(2)} & \cdots & p_T^{(N)} \end{pmatrix} \longrightarrow$$

Daily HM-AM ratio

$$Q_d = \frac{\sum_{t=1}^{T} HM_t}{\sum_{t=1}^{T} AM_t}$$

$$HM_t = \frac{N}{\sum_{i=1}^{N}(1/\log(p_t^{(i)}+2))}$$

$$AM_t = \frac{\sum_{i=1}^{N}\log(p_t^{(i)}+2)}{N}$$

HM_t: harmonic mean of all households' power consumption at time t

AM_t: arithmetic mean of all households' power consumption at time t

$p_i^{(j)}$: **power consumption** of household **i** at time **j**

Problems to adopt FHE（HE）

1) Logarithm cannot be implemented with FHE (only addition/multiplication are adopted)
2) Division with a variable cannot be implemented (cannot calculate inverse)

before → after

$p_i^{(j)}$ is sent to the server

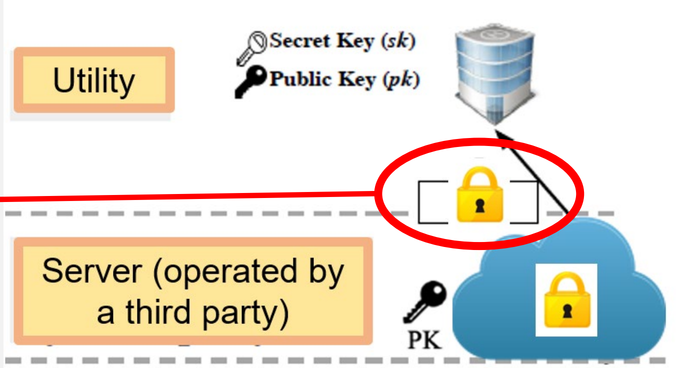
- Logarithms and divisions are required to calculate Q_d

idea 1) eliminating the calculation of logarithms at the server

Besides $p_t^{(i)}$, $\log(p_t^{(i)}+2)$ and $1/\log(p_t^{(i)}+2)$ are sent to the server

idea 2) eliminating the calculation of divisions at the server

Instead of sending $Enc(Q_d)$, $Enc(AM_t)$ and $Enc(HM_t)$ from the server to the utility, separately. Then, the utility will decrypt them to calculate Q_d



[1]Y. Ishimaki, S. Bhattacharjee, H. Yamana and S. K. Das, "**Towards Privacy-preserving Anomaly-based Attack Detection against Data Falsification in Smart Grid**," *2020 IEEE Int'l Conf. on Communications, Control, and Computing Tech. for Smart Grids*, pp. 1-6, 2020. Int'l co-authorship Method1 Proposal
[2] Y. Ishimaki and H. Yamana, "**Faster Homomorphic Trace-Type Function Evaluation**," in IEEE Access, vol. 9, pp. 53061-53077, 2021 Speedup methods

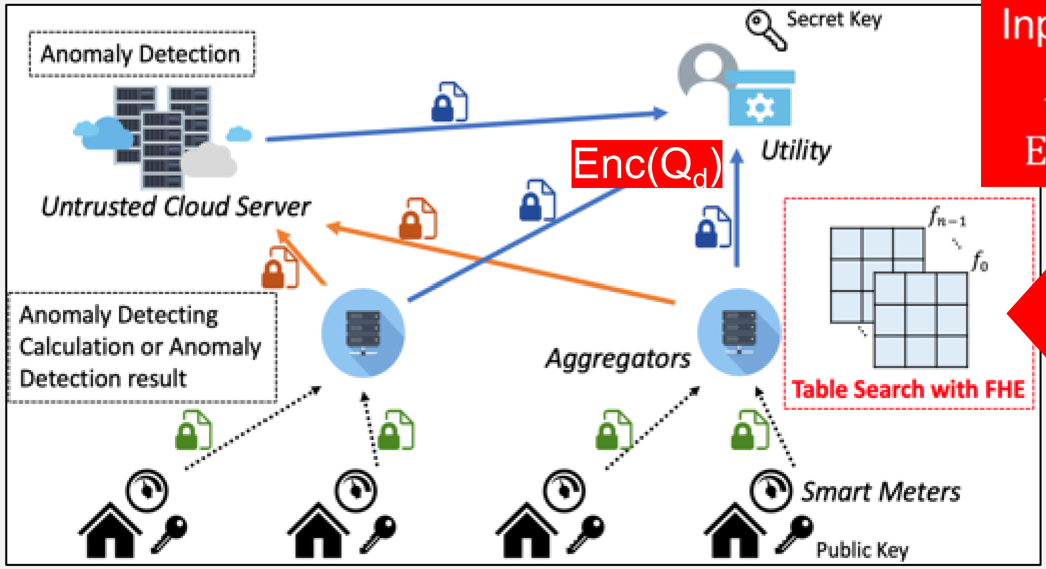
Preserving Privacy – Method 2

Problems to adopt FHE（HE）

1) Logarithm cannot be implemented with FHE (only addition/multiplication are adopted)
2) Division with a variable cannot be implemented (cannot calculate inverse)

idea : replacing $f(x, y, \ldots.)$ to calculate Q_d to table lookup

Table lookup with a non-colluding server to adopt any kinds of calculations at the server (aggregators).

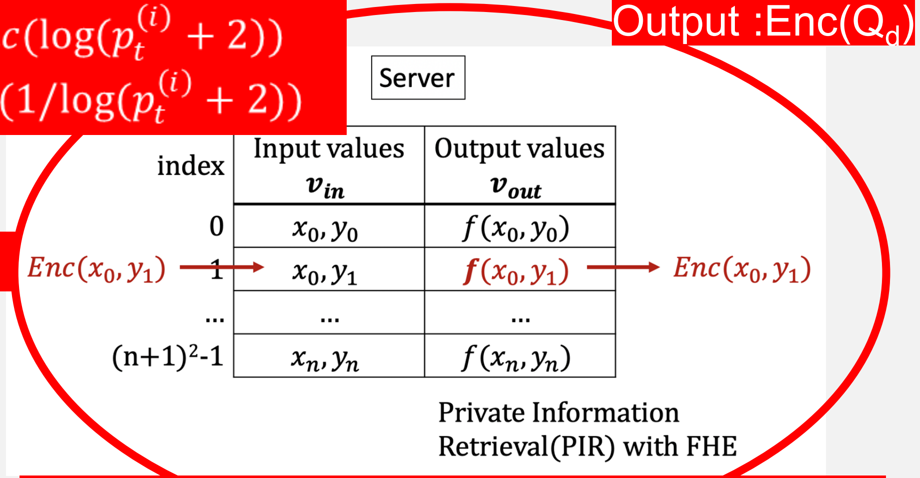


Inputs:

$Enc(\log(p_t^{(i)} + 2))$

$Enc(1/\log(p_t^{(i)} + 2))$

Output :Enc(Q_d)



index	Input values v_{in}	Output values v_{out}
0	x_0, y_0	$f(x_0, y_0)$
1	x_0, y_1	$f(x_0, y_1)$
…	…	…
$(n+1)^2$-1	x_n, y_n	$f(x_n, y_n)$

Private Information Retrieval(PIR) with FHE

Division is implemented by table lookup

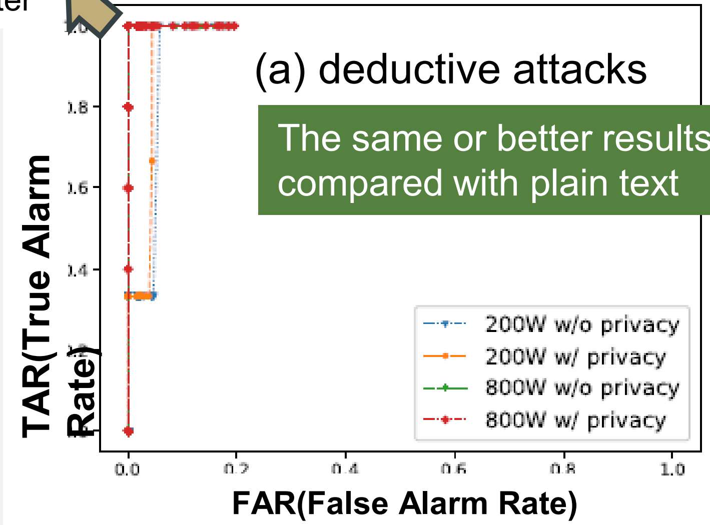
[3] Ruixiao Li, Yu Ishimaki and Hayato Yamana, "**Fully Homomorphic Encryption with Table Lookup for Privacy-Preserving Smart Grid**," Proc. of the 3rd IEEE International Workshop on Big Data and IoT Security in Smart Computing, pp.19-24 (2019.6) supported one input version

[4] Ruixiao Li, Yu Ishimaki, Hayato Yamana, "***Privacy Preserving Calculation in Cloud using Fully Homomorphic Encryption with Table Lookup***," Proc. of the 5th IEEE International Conference on Big Data Analytics (ICBDA2020), pp.315-322 (2020.05) supported any number of inputs version

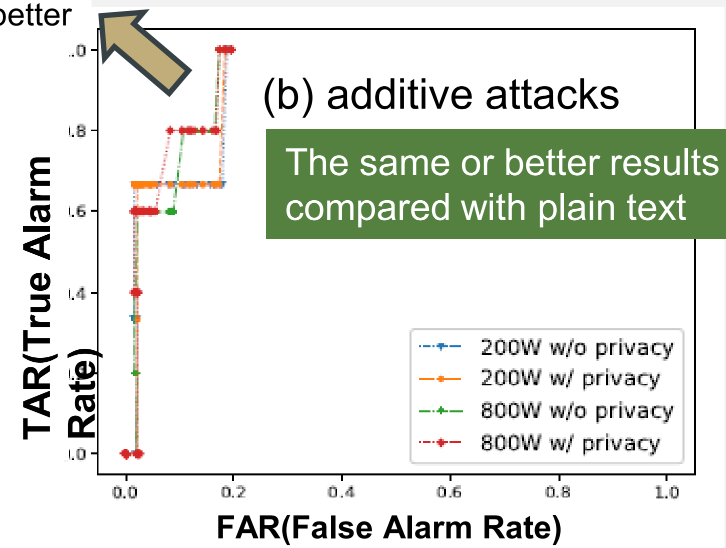
[5] Ruixiao Li and Hayato Yamana, ***Fast and Accurate Function Evaluation with LUT over Integer-based Fully Homomorphic Encryption***, Proc. of the 35th International Conference on Advanced Information Networking and Applications (AINA-2021), pp.620-633 (2021.5) supported any input value version / adopting approximation for inputs to select the best entry in the table

Preserving Privacy: Evaluation

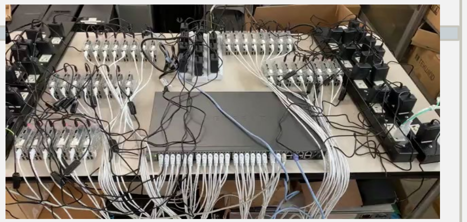
Method 1) eliminating FHE unfriendly calculations



The same or better results compared with plain text



The same or better results compared with plain text



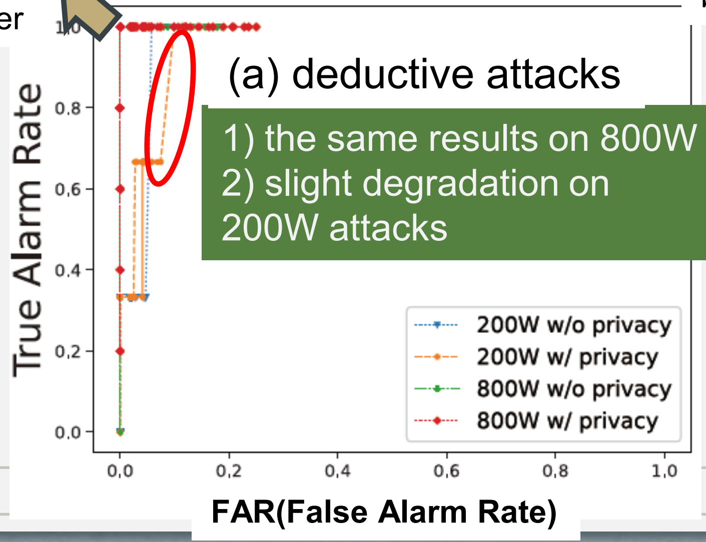
Execution time

	time [sec]
1) Aggregator	9.935
2) Utility	0.022
Total time	9.957

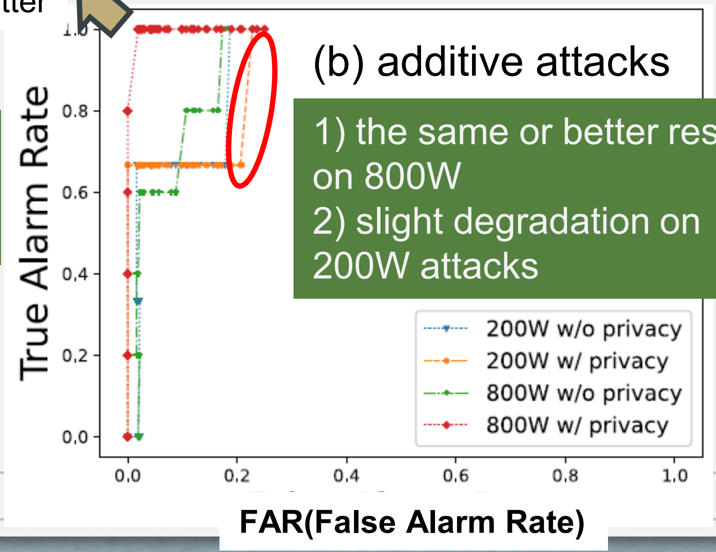
Aggregator：Intel Xeon E5-1620v4 3.5GHz(single thread)
Encrypted data size: 11,784KB(household→aggregator)
288KB(aggregator→utility)

※execution time at power meter is 0.112 sec/data

Method 2) adopting FHE table lookup



1) the same results on 800W
2) slight degradation on 200W attacks



1) the same or better results on 800W
2) slight degradation on 200W attacks

Execution time

	time
1) Aggregator	5 min

Input table size: 22,795 x 663
Output table size： 15,113,085
average power consumption is 1kWh/household)

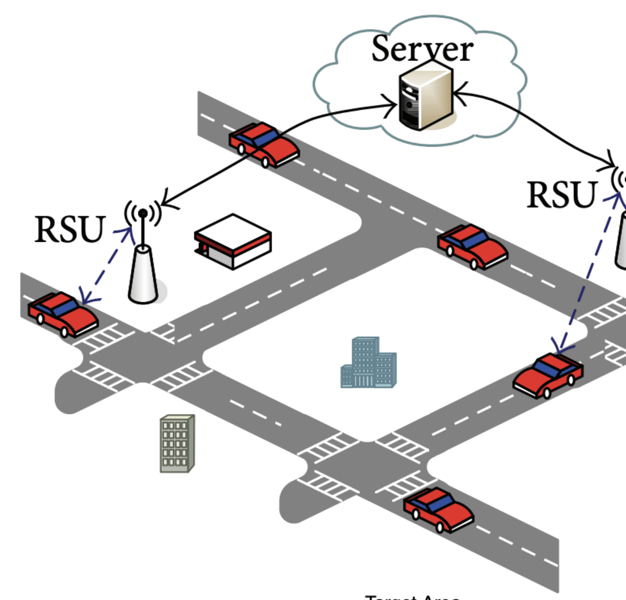
1) confirmed **the same results** with plain text implementation w/ **800W attacks**
2 depending on table size, TAR/FAR will vary especially for small attacks.

Thrust 3 Results:
(Abhishek Dubey, S. K. Das, S. Bhattacharjee, K. Yasumoto)

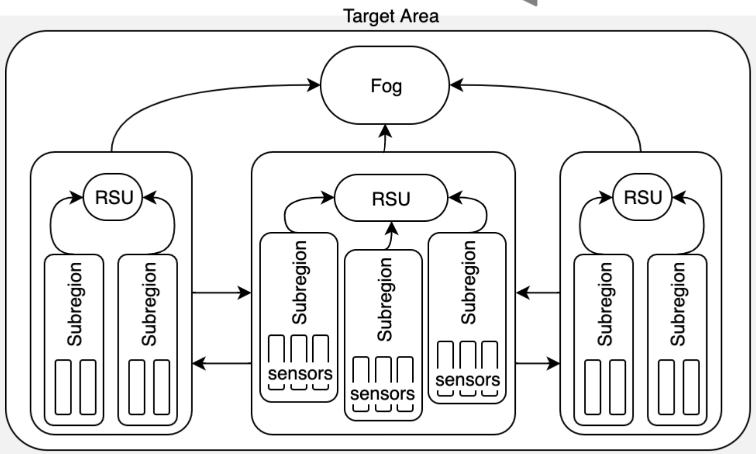
Security and Performance Tradeoff

Thrust 3 : Anomaly Detection & Performance Tradeoff

- Detect anomalies in real-time in transportation and energy data collected from urban areas.
- Correlated anomalies with incidents in urban transportation network.
- Data used:
  - Road segment and traffic mobility data
  - Traffic incidents: Nashville Police, Fire department data and Waze data
  - Weather data



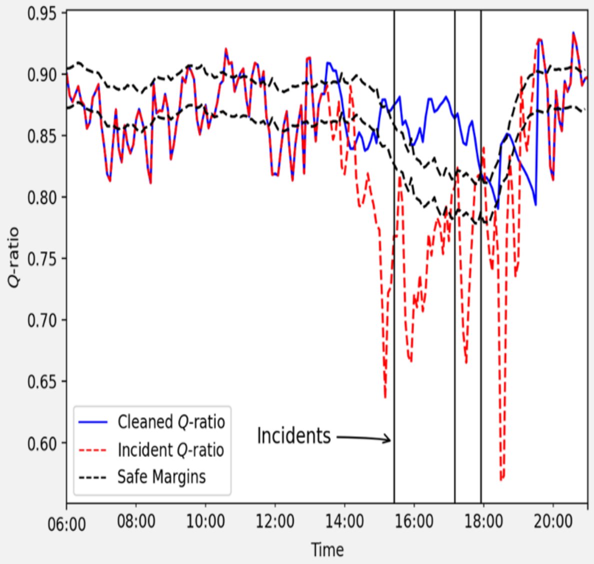
Y. Xiong, J. Ma, Jian, W. Wang, Wendong , and D. Tu, "RoadGate: Mobility-Centric Roadside Units Deployment for Vehicular Networks," *International Journal of Distributed Sensor Networks*, 2013.

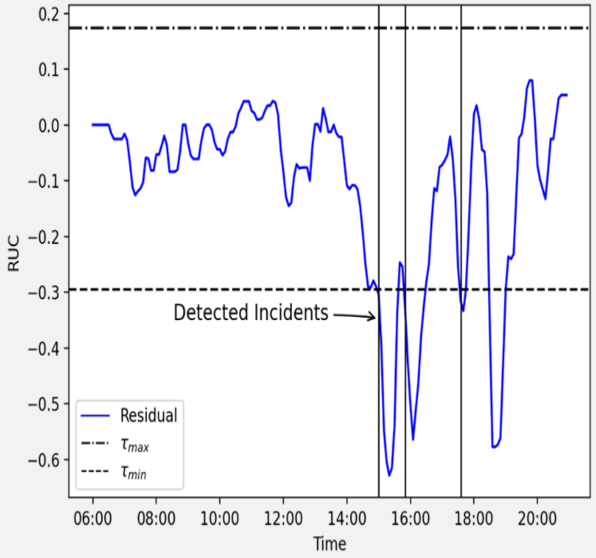


Proposed architecture for distributed anomaly detection

Thrust 3: Clustering Approach

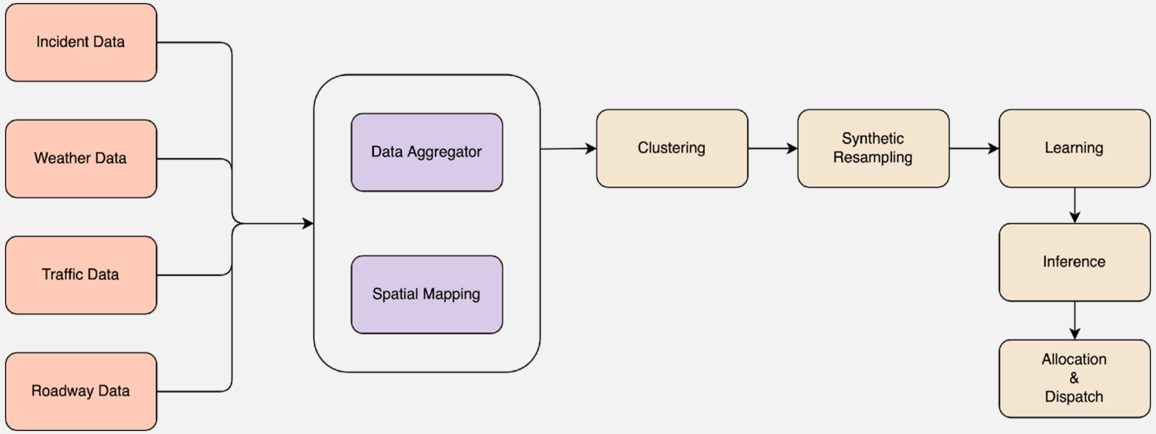
- Use clustering and statistical ratios to identify sudden changes.
- Averaged 2019 speed data into 7 day of week data and used only weekends
- Cluster segments using different spatio-temporal granularities
  - *Spatial*: Max distance between segments
  - *Temporal*: Resampling speed data

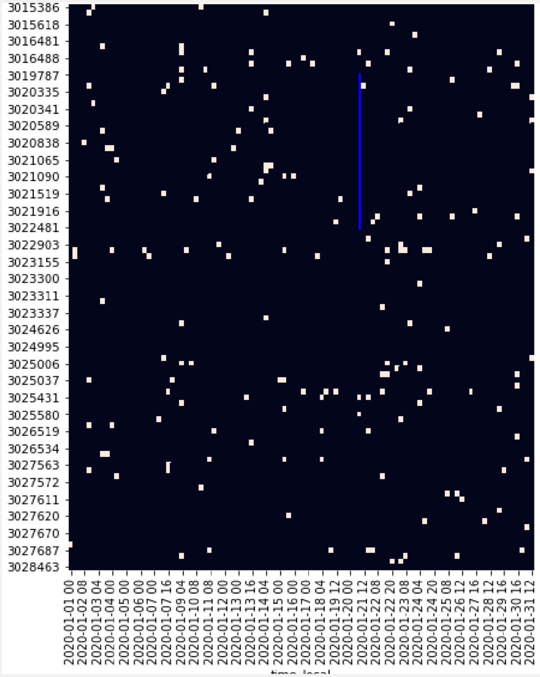




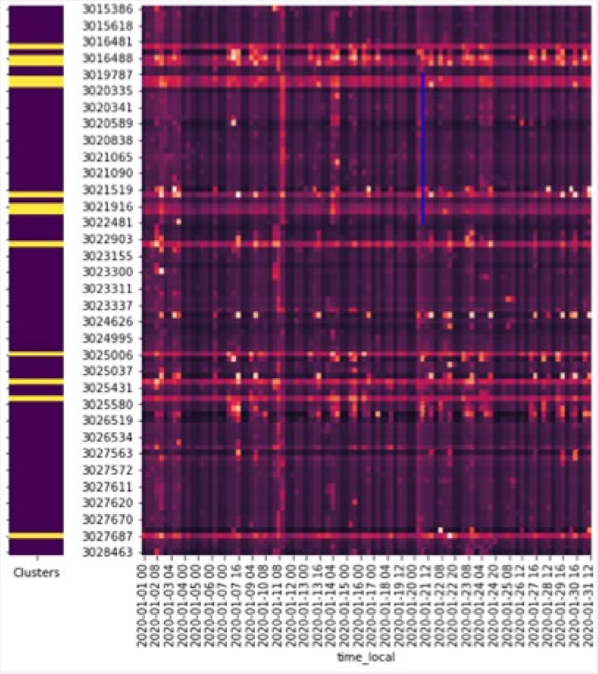
Thrust 3: Predicting Anomalies

- **Challenges**
  - **Big Data:** Many factors are involved in road accidents, which requires collecting various types of data from assorted resources with different resolution and quality.
  - **Sparsity:** Although frequency of road accidents is high, when viewed from the perspective of total time and space, incidents are rare events.
  - **Irregularity:** Accidents are random in nature, especially in high spatial-temporal resolution





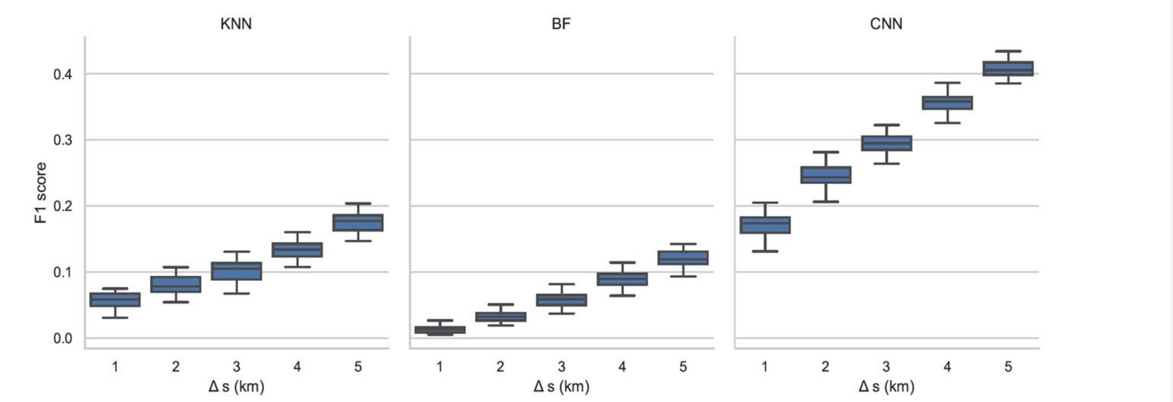
Test data over 4-hour window

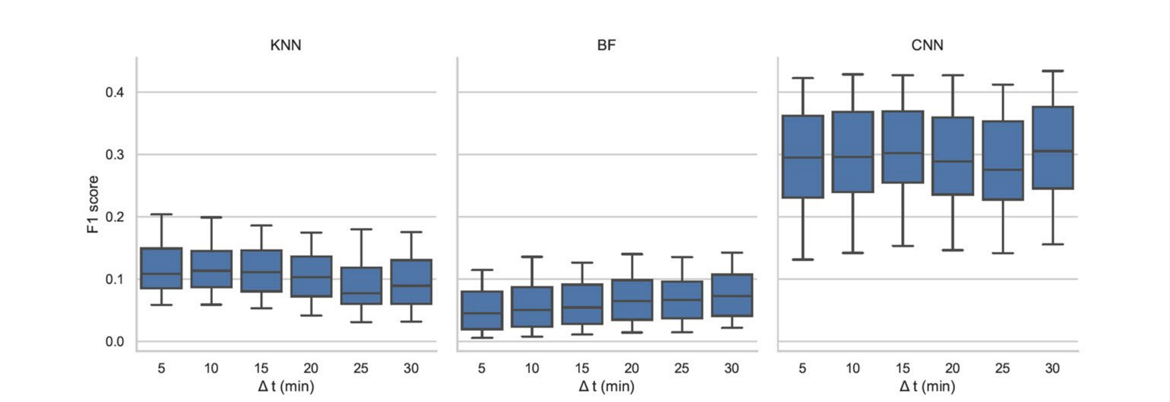


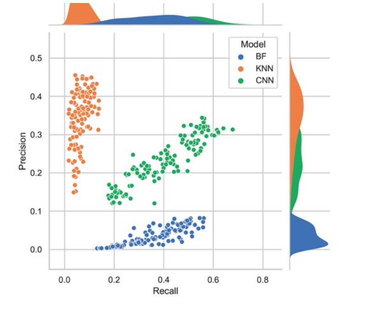
Prediction over 4-hour window

Thrust 3: Uncertainty Handling

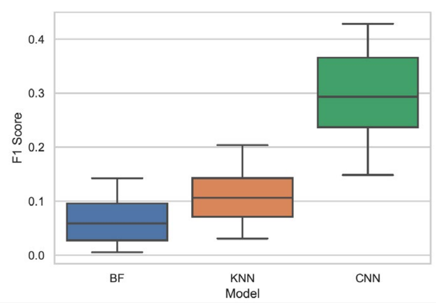
- **Challenge** – Uncertainty of data. This requires fine tuning of the detection thresholds.
- **Spatial discretization** – Reduces precision but improves robustness
- **Temporal discretization** – Reduces usefulness of detection metric. But high temporal resolution reduces recall.
- **Solution** – Uses pareto optimization with CNNs (convolutional neural networks)







CNN model can balance precision and recall to achieve higher F-1 scores.



Thrust 4 Results:

(Abhishek Dubey, Keiichi Yasumoto)

Developing Secure and Trustworthy Middleware Architecture

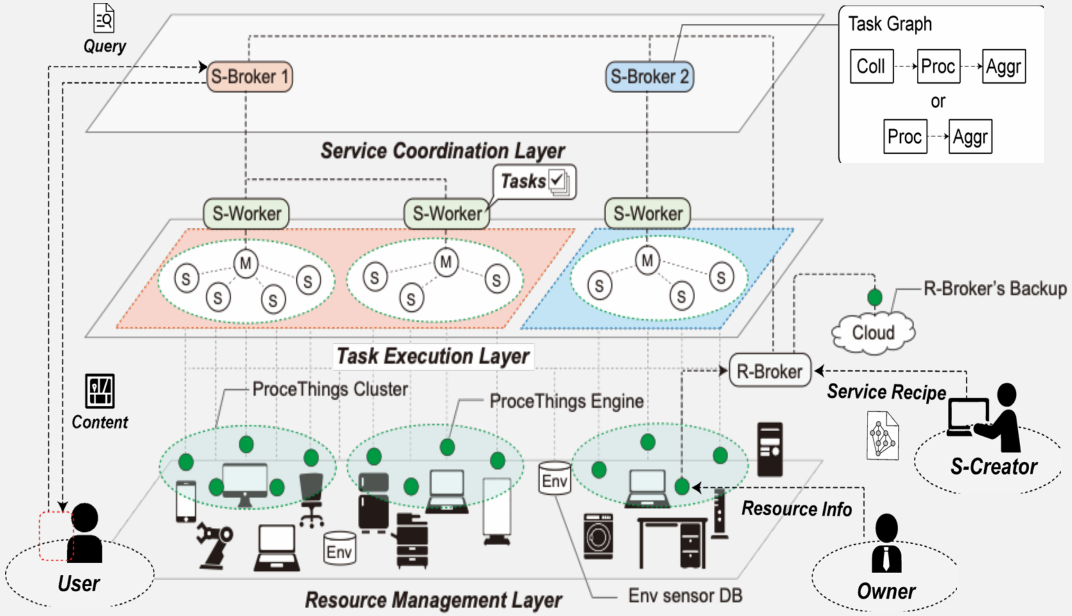
Tasks:

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

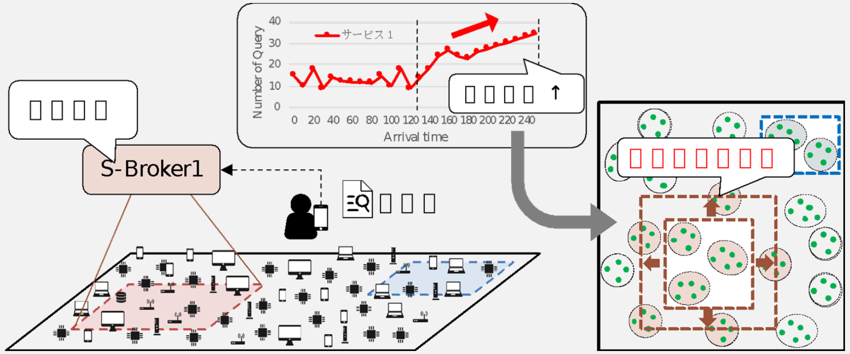
Task 4.1: Distributed Aggregation

Proposed a novel middleware framework for Smart and Connected Communities that distributes security features across proposed tasks and incorporates privacy, trustworthiness, resource constraints, and distributed decision support.

Developed a middleware platform for SCC apps through distributed processing among edge nodes [MUSICAL 2021]



Middleware Platform [MUSICAL2021]



Adaptive scale-out mechanism

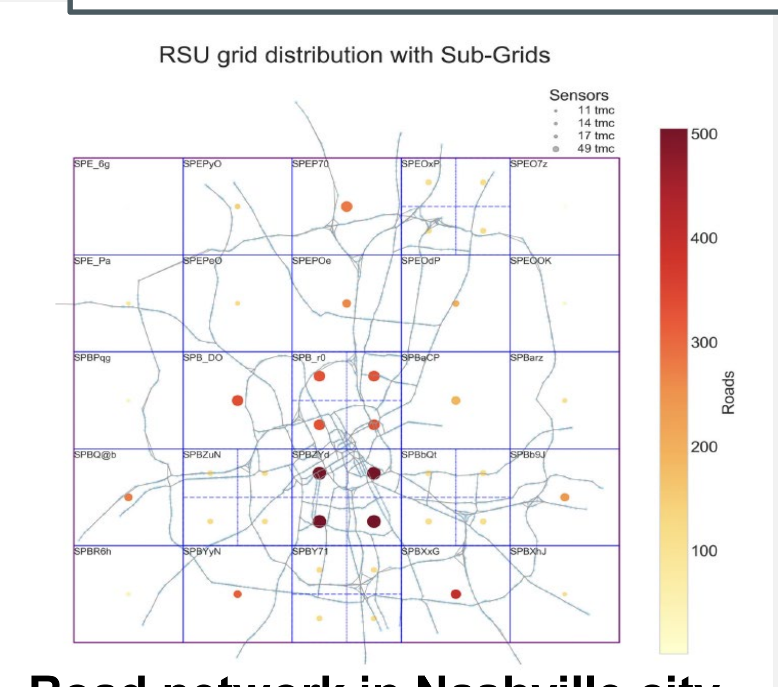
the number of edge nodes is increased as necessary

Smart Mobility App Developed on Middleware

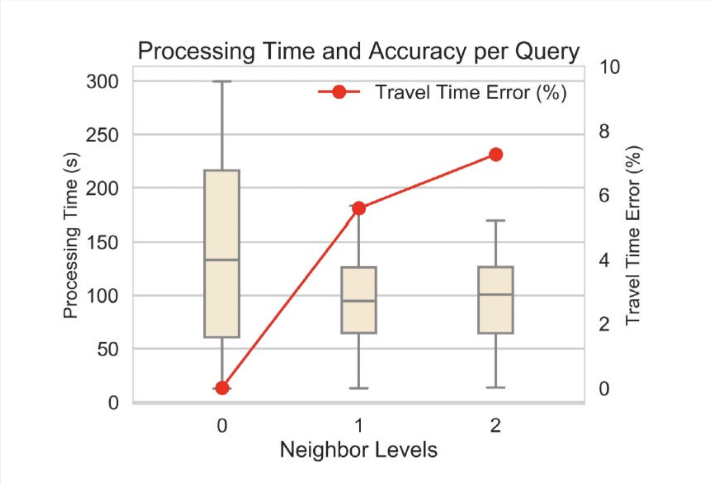
Distributed route planning was implemented on the middleware [IEEE Access 2021]

For evaluation, emulation environment was constructed

- 49 Docker containers corr. to RSUs were virtually deployed over the 25 grids
- Each RSU running the middleware uses real traffic data to compute the shortest time paths
- "adaptive scale-out" is applied to the heavy-loaded grids (tasks are off-loaded to neighboring grids)

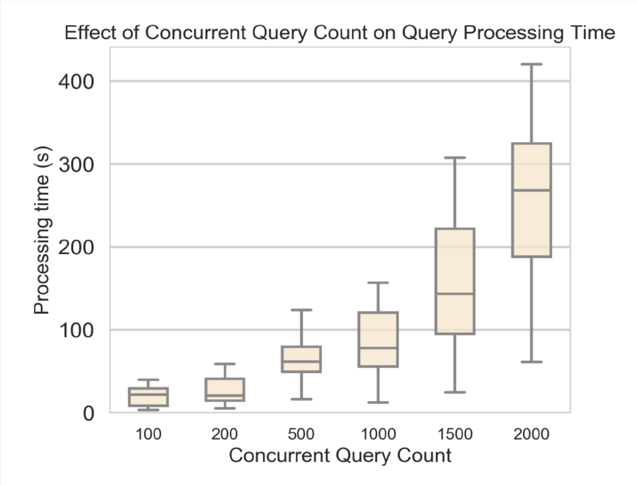


Road network in Nashville city
divided into 25 grids



Query response time for 1000 queries
(neighbor level means # hops for offloading tasks)

Offloading (adaptive scale-out) enabled a great reduction of resp. time

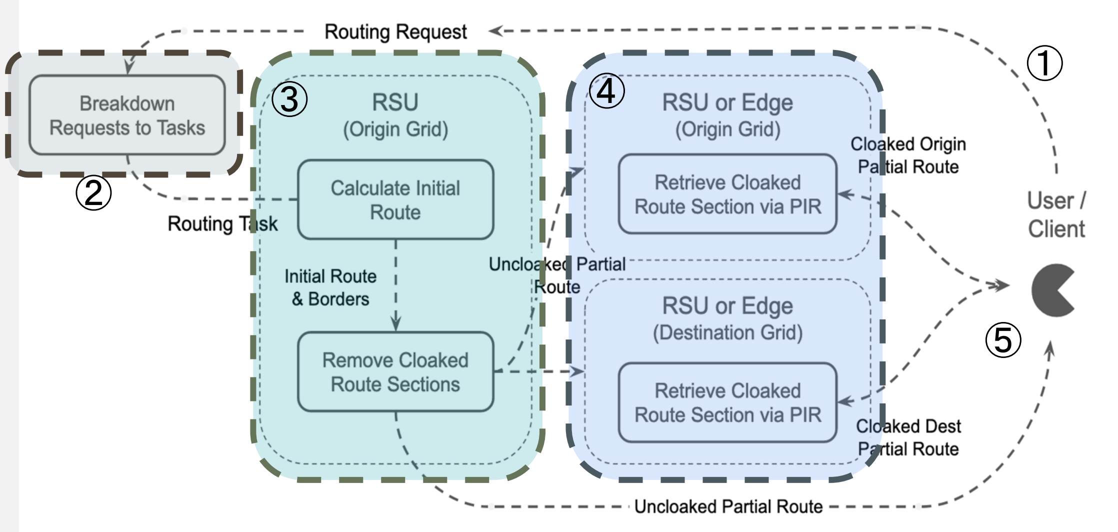


Response time for 100 to 2000 queries
(Neighbor level = 1)

Up to 2000 queries can be processed in practical time

Task 4.2: Secure Anonymization

Developed a secure anonymization mechanism based on APSP/PIR for smart mobility apps that allows users to get a query result securely without revealing origin/dest. points [SmartComp2021]



(i) User sends a query with blurred origin & dest. points (in grid level) to S-broker

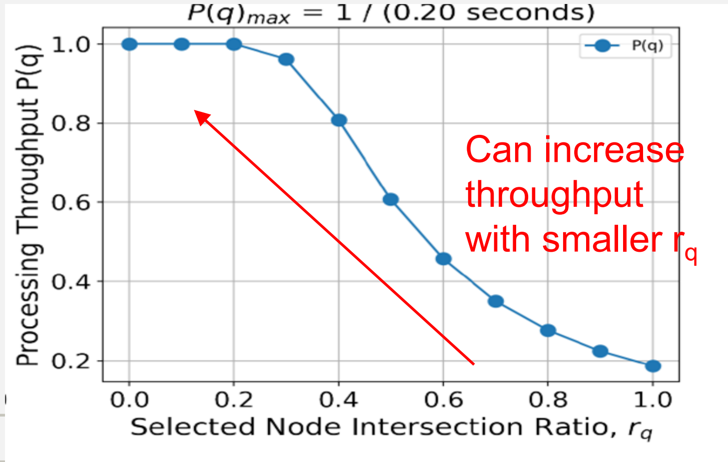
(ii) S-broker assign tasks for computing sub-shortest-paths to grids (RSUs) along the grid sequence

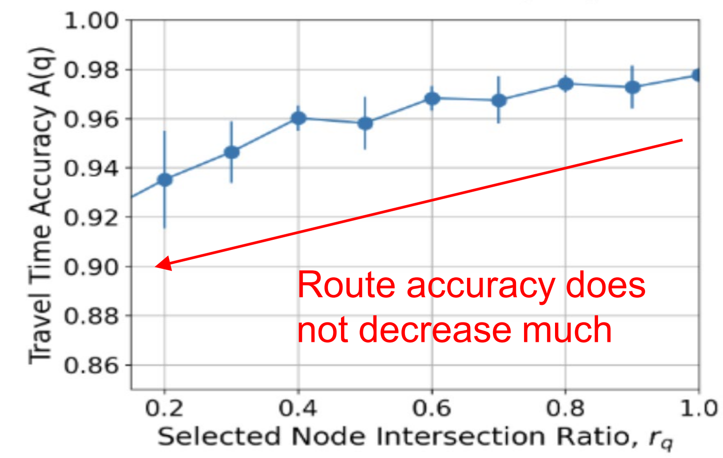
(iii) Each intermediate grid computes the shortest paths between border intersections

(iv) Source & dest. grids compute APSP (all-pairs-shortest-paths) between all intersections

(v) User gets sub-shortest paths (PIR is used to retrieve the paths for the source and destination grids) and concatenate them

- Applying APSP/PIR to all queries could cause some edge nodes (e.g., center grids) to be heavily loaded
- Reducing num. intersections can improve the throughput while keeping accuracy high enough.





Task4.3: Decision Making under Trade-offs

Developed a tradeoff mechanism that balances query throughput, route accuracy and privacy protection level [SmartComp2021]

Conducted simulations using Osaka city traffic data from T5.1

We formulated multi-objective optimization problem and developed NSGA-II based algorithm

Set of queries at time slot t

$$Maximize\ (P(Q_t), V(Q_t), A(Q_t))\ s.t.\ (3)$$

Query throughput   Privacy level   Route accuracy

$$\forall g \in G, |\{q \mid q \in Q_t, src(q) = g \vee dst(q) = g\}| \leq Cap(g) \quad (3)$$

#queries processed at each RSU is limited

$$\mathcal{P}(q) = \frac{1}{\mathbf{1^T} \cdot [R(\mathbf{g_q}) + I(\mathbf{g_q}) + C(\mathbf{g_q})]}$$

Throughput = 1÷(route calc. + PIR calc. + delay)

$$\mathcal{V}(q) = \mathbf{1^T} \cdot [(\mathbf{a_q}^{\gamma} \odot \mathbf{v'_q}) \cdot C_{lp}]$$

Privacy level = area size x cover rate x coefficient

$$\mathcal{A}(q) = \mathbf{1^T} \cdot M(\mathbf{v_q}, \mathbf{r_q})$$

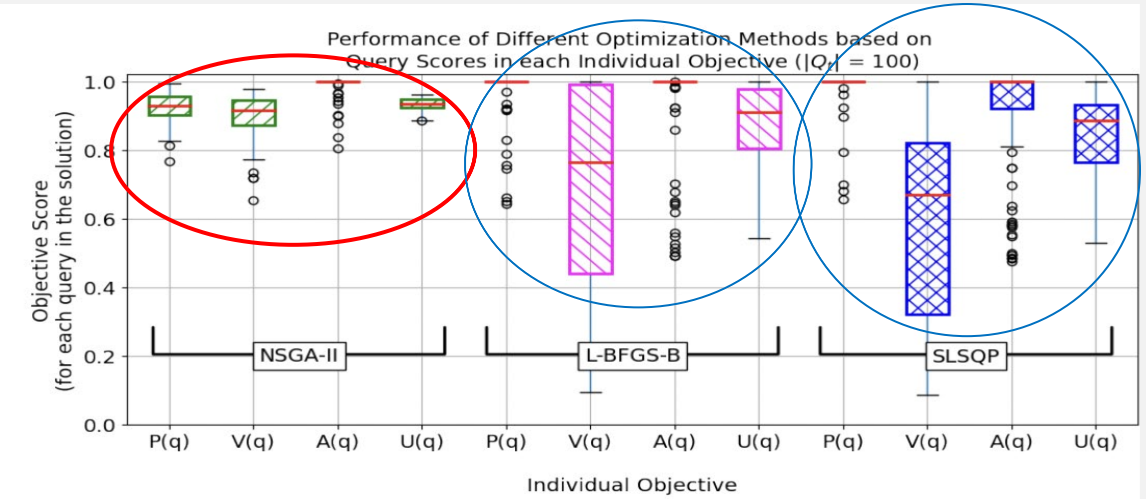
Accuracy = computed by #intersections and cover rate

$$P(Q_t) = \frac{\sum_{q \in Q_t} \mathcal{P}(q) \cdot H_P(q)}{|Q_t|}$$

$$V(Q_t) = \frac{\sum_{q \in Q_t} \mathcal{V}(q) \cdot H_V(q)}{|Q_t|}$$

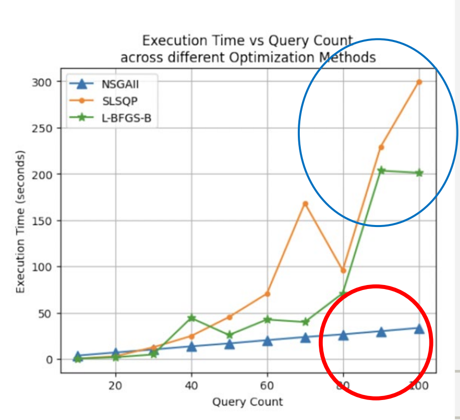
$$A(Q_t) = \frac{\sum_{q \in Q_t} \mathcal{A}(q) \cdot H_A(q)}{|Q_t|}$$

Aggregate by multiplying User preference Hx



Ours (NSGA-II) outperforms others in all objectives: P, V, A, U

P: throughput, V: privacy level, A: accuracy, U: average utility



Our method outperforms others in execution time

Thrust 5 Results:

(A. Dubay, Hirozumi Yamaguchi)

Validation with Real Datasets

Tasks:

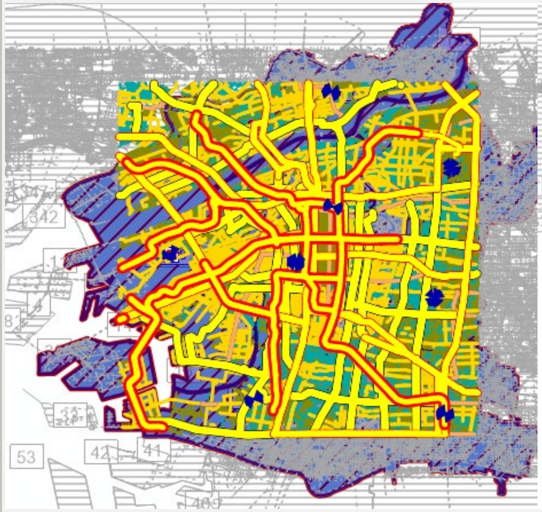
5.1 Smart Transportation Application
5.2 Smart Energy Application

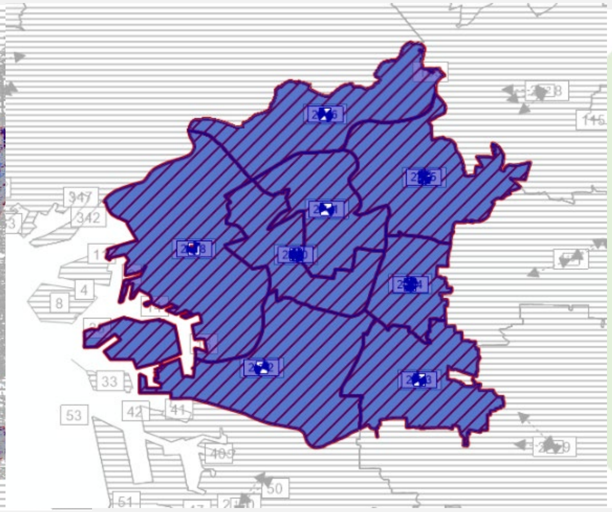
Validation with Real Datasets

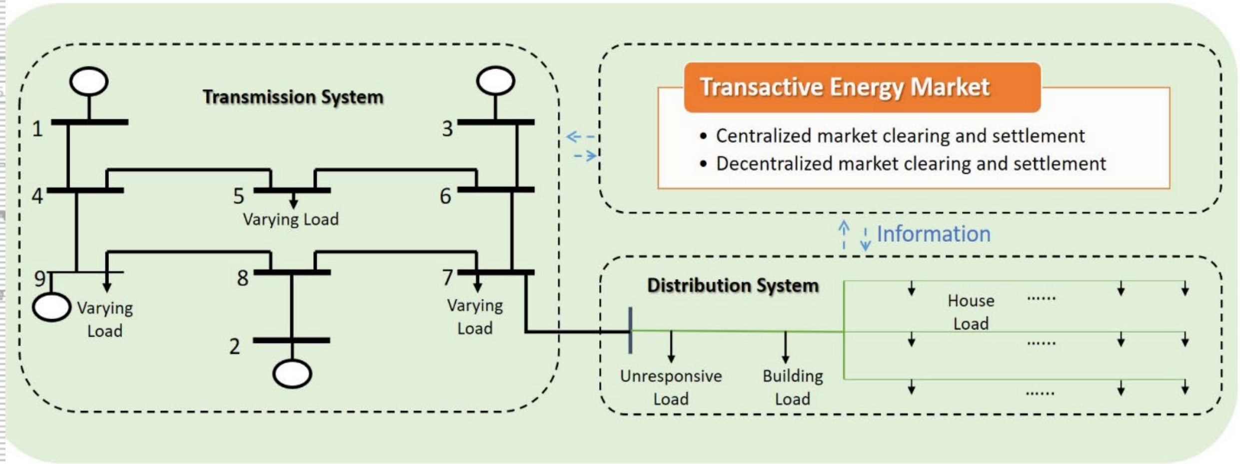
Objective : Validate the proposed models and approaches using smart mobility and smart energy distribution / consumption scenarios with real-world datasets

Approach :

- Generate large-scale mobility data from real datasets in Osaka
- Design a transactive energy testbed that can integrate energy market data







Task 5.1: Smart Transportation Application

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

is simulated using real dataset

Link Traffic

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.

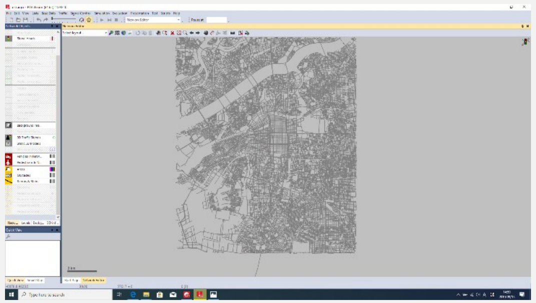
time / road	5:00	6:00	・・・	4:00
road a	a1	a2		a24
road b	b1	b2		b24
・・・				
road z	z1	z2		z24

estimation

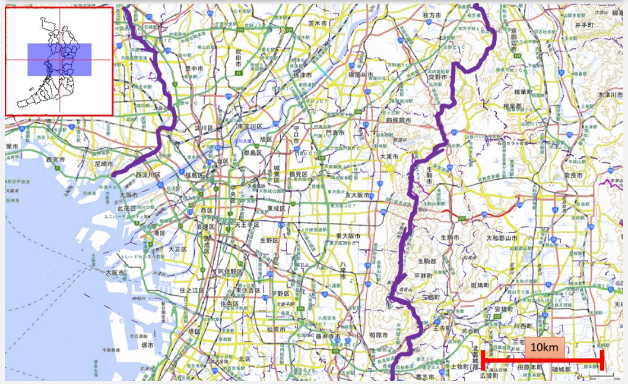
OD Matrix

OD	①	②	③
①	AA	BB	CC
②	DD	EE	FF
③	GG	HH	II

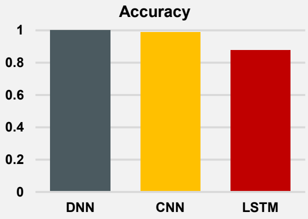
simulation

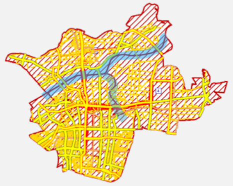


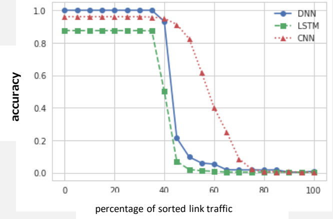
Road Traffic Census data (obtained by nation-wide survey by Ministry Road Bureau)



1. generate possible OD patterns
2. for each OD matrix, simulate vehicles and measure the link traffic to annotate OD matrix label to link traffic data
3. train DNN, LSTM and CNN using this data that predicts OD matrix from link traffic (5,378 links for 24 hours in case of Osaka)



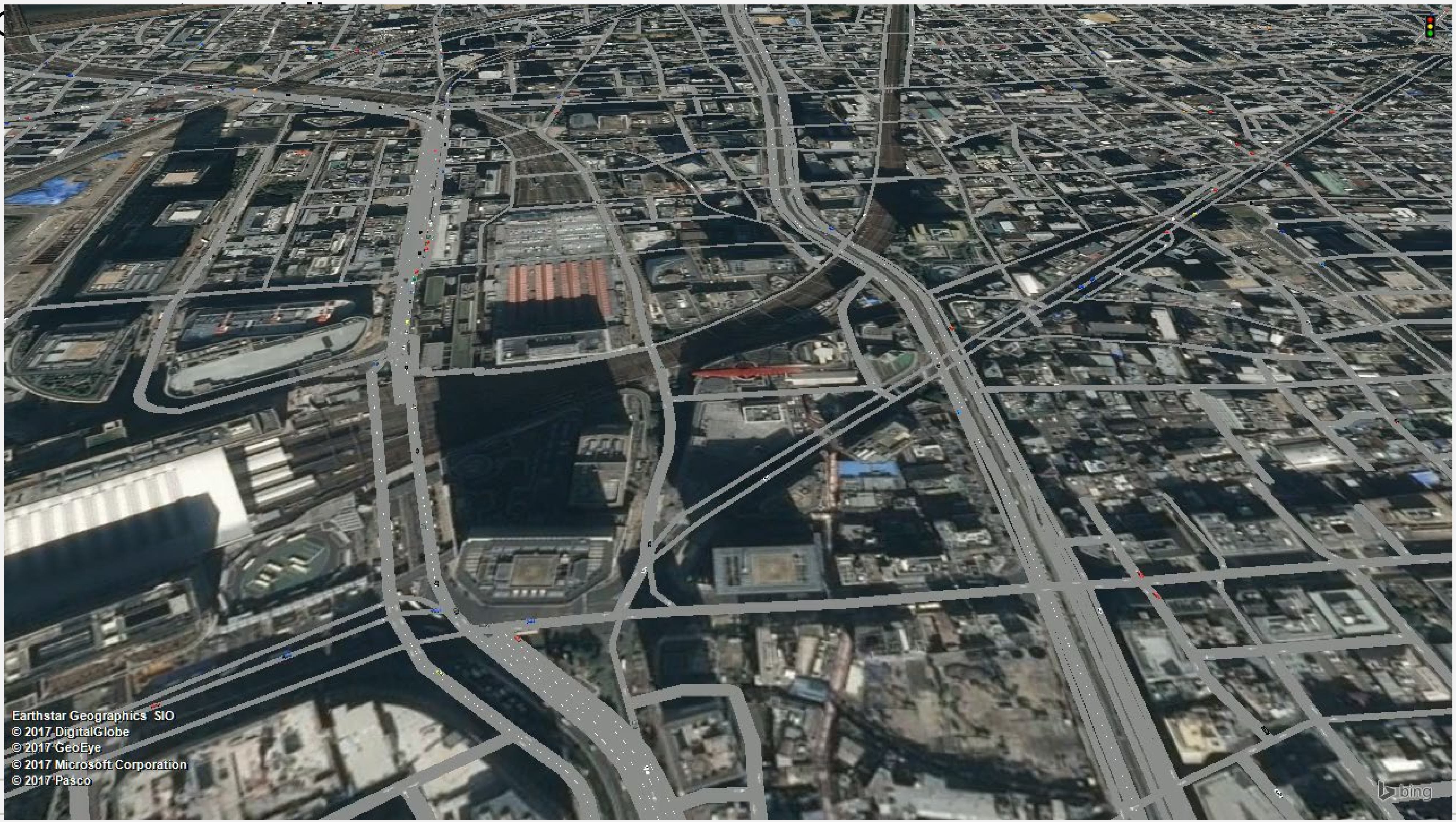




100% accuracy (DNN with all links traffic)
80% accuracy (CNN with 50% link traffic)

Simulated Vehicles in Osaka Downtown

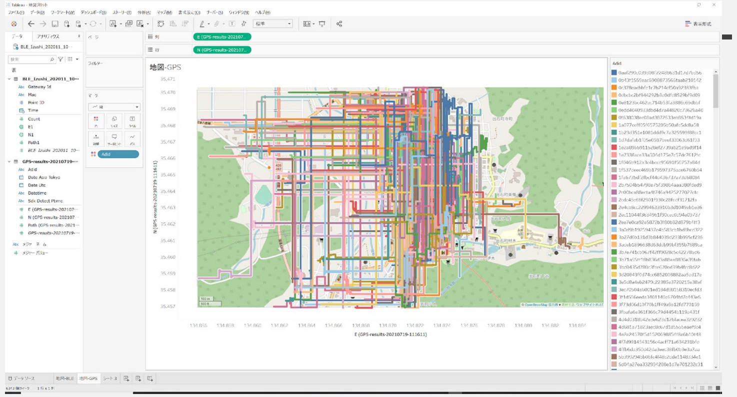
- will b



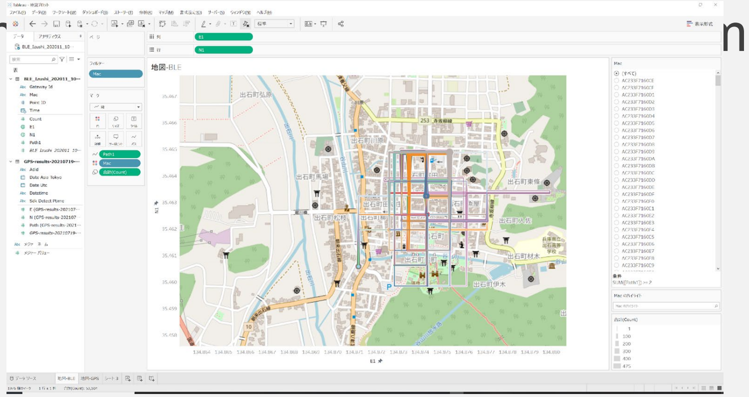
Simulation with Vehicles and Pedestrians

- generating vehicle/human mobility data of Toyooka city (Hyogo prefecture)
  - using anonymized GPS/BLE traces as well as link traffic volume data from the city

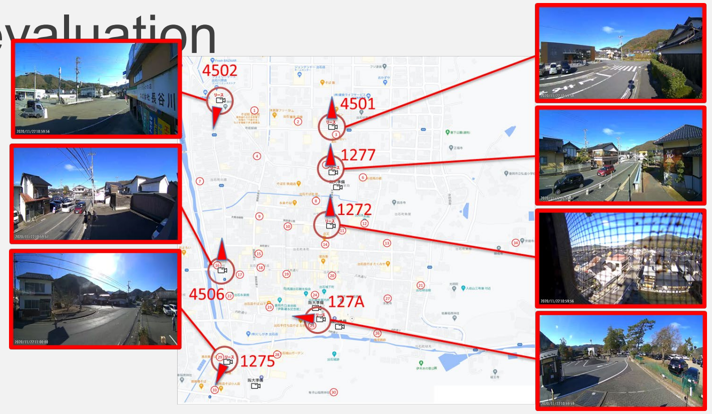
-m … n evaluation



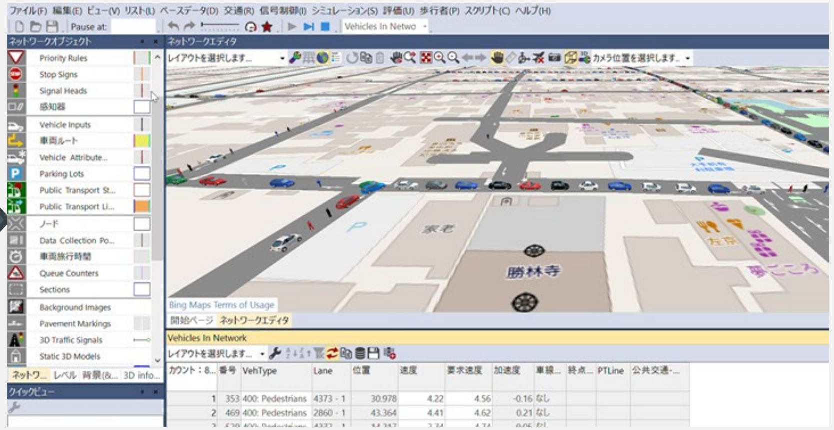
500+ GPS Traces (grid)



170 BLE Traces (grid)

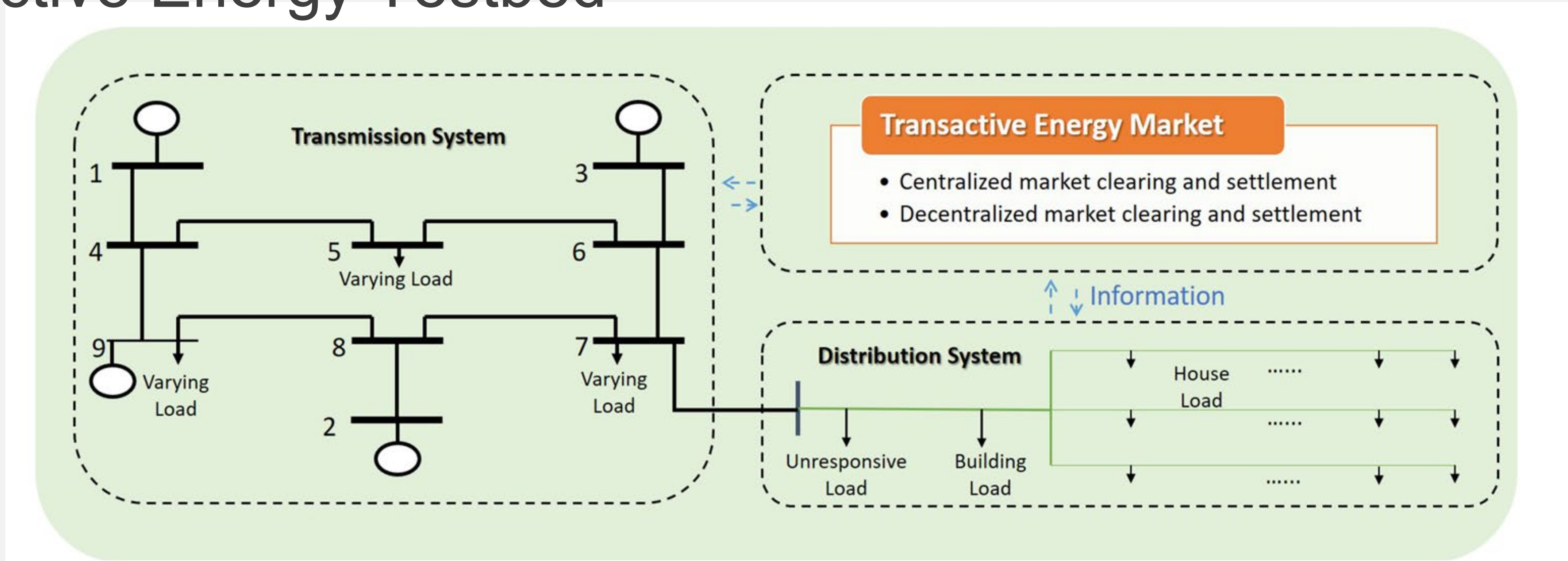


Vehicle/Pedestrian Counting via Roadside Cameras



Task 5.2 Smart Energy Application

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:

- Prithwiraj Roy and Venkata Praveen Madhavarapu (Missouri S&T), PhD - graduating in fall 2021
- Michael Wilbur; Geoff Pettet (Vanderbilt Univ.)
- Yu Ishimaki; Ruixiao Li (Waseda Univ.) - graduated
- Jose Paolo Talusan; Francis Tiausas (NAIST)
- S. Choochotkaew; Yuki Akura (Osaka Univ.)

➢ 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.
- V. P. Madhavarapu and P. Roy (Missouri S&T) visited WMU for 4 weeks in July and Aug 2019, respectively.
- J. P. Talusan (NAIST) visited Vanderbilt for 3 weeks in June 2019.
- M. Wilbur (Vanderbilt) visited WMU for 1 week in 2019.

➢ Integration of Research into Courses:

- Missouri S&T: Developed and taught a new course on *Advances in CPS Security*, spring 2021.
- Vanderbilt Univ.: Incorporated anomaly detection module in *Reliable Distributed Systems*, fall 2019.
- WMU: Covered CPS and smart grid security in *Science of Cybersecurity*, spring 2019.

➢ Outreach Activities:

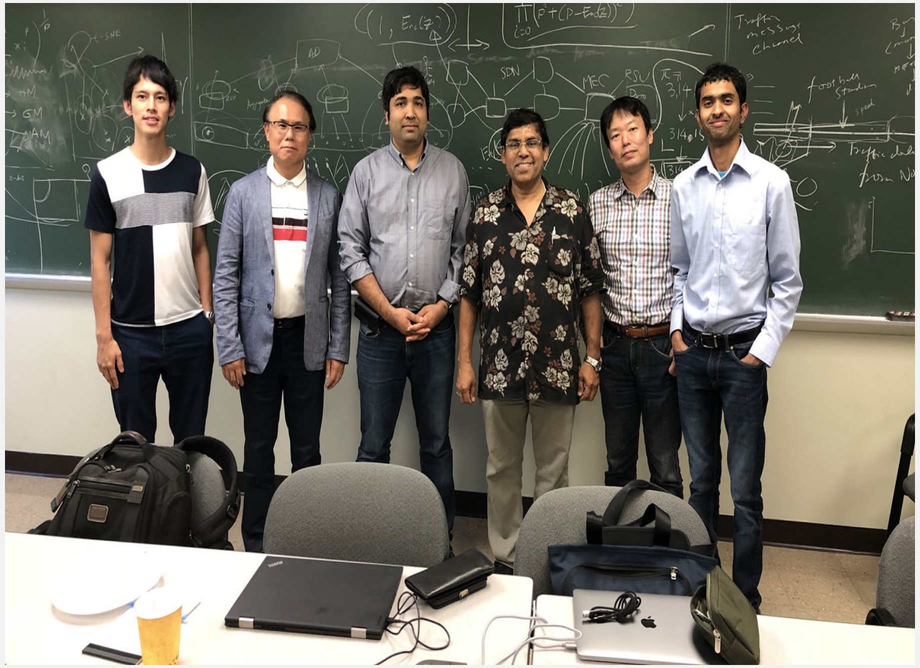
- **Organized** Big Data and IoT Security (BITS) workshop in conjunction with IEEE SmartComp 2019-2021.
- Organized Science of Smart City Operations and Platforms Engineering (SCOPE) workshop during CPS-IoT Week, 2019.
- Led to two NSF projects from CNS and SaTC programs (MST, WMU).
- Supported UG students in research.; mentored high school students.
- Das delivered Keynote Talks at various conferences.

Coordination and Collaboration

- Bi-weekly Skype/Zoom meeting; Very coherent group
- NUmerous joint publications by PIs and their students
- Co-organization of BITS and SCOPE workshops
- 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, Japan: Oct 26-27, 2018 (JUNO2 Kick-off Meeting)
- Kyoto, Japan: March 11-14, 2019 (IEEE PerCom)
- Washington, DC: June 12-14, 2019 (IEEE SmartComp)
- Chicago: Oct 11, 2019 (JUNO2 PI Meeting)
- Bologna, Italy: June 20-23, 2020 (IEEE SmartComp) - NO
- Nara, Japan: January 5-8, 2021 (ACM ICDCN) – NO due to Covid-1



September 2018 (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, 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, S. Bhattacharjee, "Smart Transportation Delay/Resilience Testbed using Information Flow of Things Middleware," *IEEE BITS Workshop*, 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*, 18(1): 356-371, Jan/Feb 2021.
10. S. Bhattacharjee, V. K. P. Madhavarapu, S. Silvestri, and S. K. Das, "Attack Context Embedded Data Driven Trust Model in Smart Metering Infrastructure," *ACM Transactions on Privacy and Security*, 24(2): 9:1-9:36, Apr 2021.
11. 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.
12. 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*, 19(1): 200-216, Jan 2020.
13. J. P. Talusan, M. Wilbur, A. Dubey, K. Yasumoto, "On Decentralized Route Planning Using the Road Side Units as Computing Resources," *IEEE International Conference on Fog Computing (ICFC 2020)*, pp. 1-8, Apr. 2020.
14. 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*, (Special Issue on Network Science for High-Confidence Cyber-Physical Systems), 7(2): 817-831, Apr-Jun 2020.
15. M. Wilbur, C. Samal, J. P. Talusan, K. Yasumoto, A. Dubey, "Time-dependent Decentralized Routing using Federated Learning," *23rd IEEE International Conference on Real-Time Distributed Computing (ISORC 2020)*, pp. 56-64, May 2020.
16. T. Limbasiya, D. Das, and S. K. Das, "MComIoV: Secure and Energy-Efficient Message Communication Protocols for Internet of Vehicles," *IEEE/ACM Transactions on Networking*, 29(3): 1349-1361, June 2021.
17. H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, 69(6): 6709-6717, June 2020.
18. J. P. Talusan, M. Wilbur, A. Dubey, K. Yasumoto, "Route Planning Through Distributed Computing by Road Side Units," *IEEE Access*, Vol. 8, pp. 176134-176148, 2020.
19. S. Bhattacharjee, V. P. Madhavarapu, and S. K. Das, "A Diversity Index based Scoring Framework for Identifying Smart Meters Launching Stealthy Data Falsification Attacks," *ACM Asia Conference on Computer and Communications Security* (ASIACCS), Hong Kong, pp. 26-39, June 2021.
20. P. Roy, S. Bhattacharjee, and S. K. Das, "Real Time Stream Mining based Attack Detection in Distribution Level PMUs for Smart Grids," *IEEE Global Communications Conference (GlobeCom) – Symposium on Smart Grid Communications and Power Line Communications*, Taipei, Taiwan, Dec 2020.
21. Y. Ishimaki, S. Bhattacharjee, H. Yamana, and S. K. Das, "Towards Privacy-Preserving Anomaly-based Attack Detection against Data Falsification in Smart Grid," *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) – Cyber Security and Privacy Symposium*, Nov 2020.
22. F. Tiausas, J. Talusan, Y. Ishimaki, H. Yamana, H. Yamaguchi, S. Bhattacharjee, A. Dubey, K. Yasumoto, and S. K. Das, "User-centric Distributed Route Planning in Smart Cities based on Multi-objective Optimization," *IEEE International Conference on Smart Computing* (SMARTCOMP), Irvine, California, Aug 2021.

JUNO2: US-Japan Collaborative Project

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

PI Meeting: Aug 18 -19, 2021

Thank You