IPSN 2020

Electric Vehicle Battery Energy Information is Enough to Track You

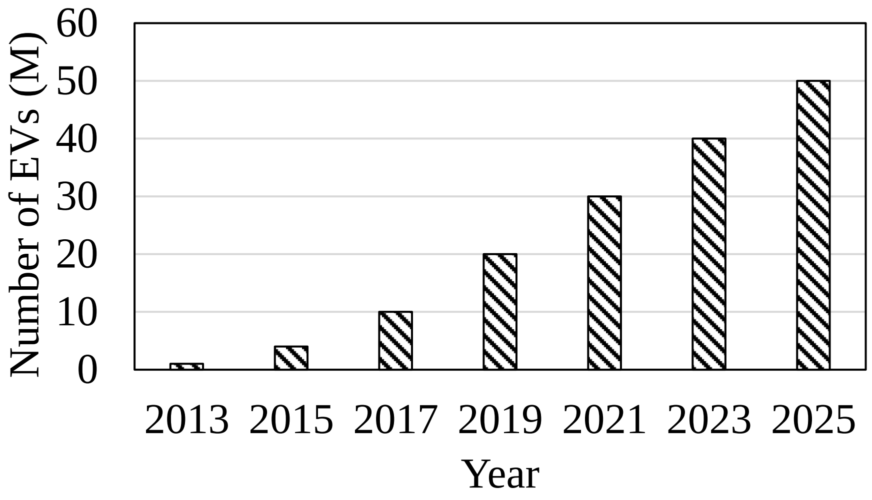
Liuwang Kang and Haiying Shen
Department of Computer Science, University of Virginia

Background

Pure electric vehicles (EVs) become popular in current automotive markets:

Advantages of EVs

- No air pollution emission
- High energy efficiency



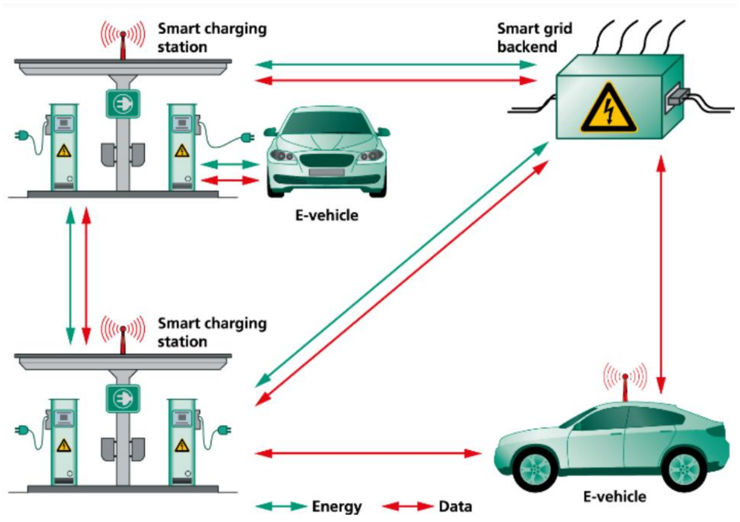
Prediction of global EV sales

Background

Remotely obtaining energy consumption time series of EVs is possible:

Background

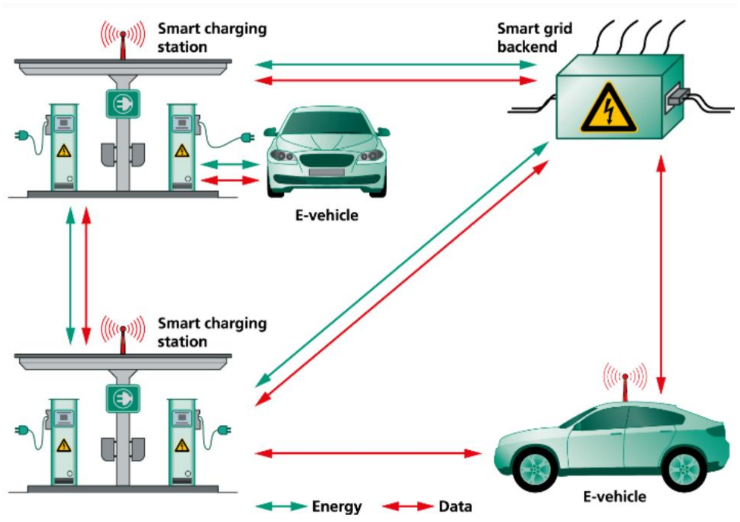
Remotely obtaining energy consumption time series of EVs is possible:



Smart battery charging systems

Background

Remotely obtaining energy consumption time series of EVs is possible:



Smart battery charging systems

Battery Apps

Related Work

- Methods [JCS’17, INFOCOM’18] use anonymous certification technologies to ensure communication security between EVs and smart battery charging systems

➢ Result in heavy certification data management loads on EVs during the EV communication process [TCPS’17]

- Methods [SECURITY’11, NDSS’14] try to remove malicious Apps from centralized mobile marketplaces

➢ Malware authors keep developing new methods to help malicious Apps penetrate into marketplaces [CS’18]

Energy consumption time series become vulnerable

Challenges

Propose a battery energy based path inference attack (Bepath) to infer an EV's driving paths based on its energy consumption time series data

Challenge 1: How to estimate appliance states (i.e., vehicle speed, AC state and intersection turn state)?

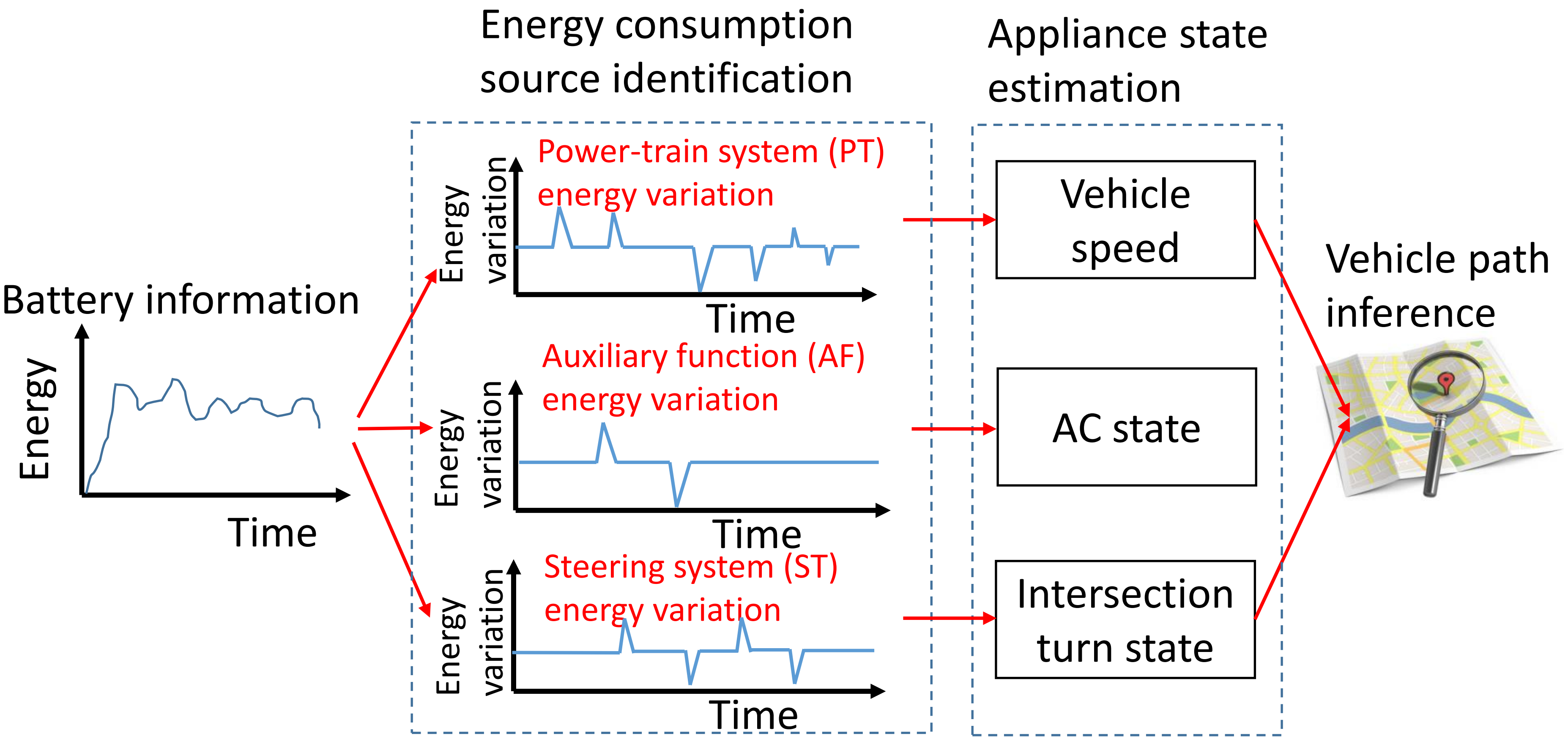
- Battery energy is consumed to drive both vehicle movement and auxiliary functions

Challenge 2: How to infer a driving path of an EV based on its estimated appliance states?

- The estimated appliance states only contain absolute speed values but not driving direction

Battery Energy based Path Inference Attack (Bepath)

Bepath infers an EV’s driving paths based on its energy consumption time series data



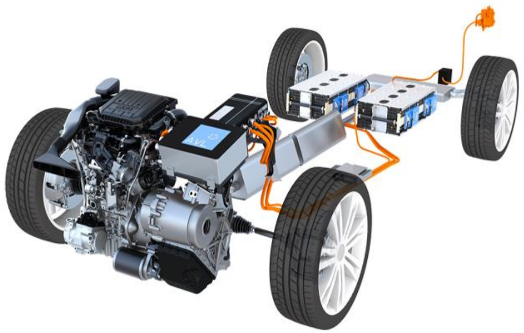
Challenge 1

How to estimate appliance states (i.e., vehicle speed, AC state and intersection turn state)?

Energy Consumption Source Identification

Energy consumption source types

- Statistically analyze one real-life daily EV driving data
- Power-train system, steering system and air condition (AC) consume around 95% of total battery energy



Power-train system

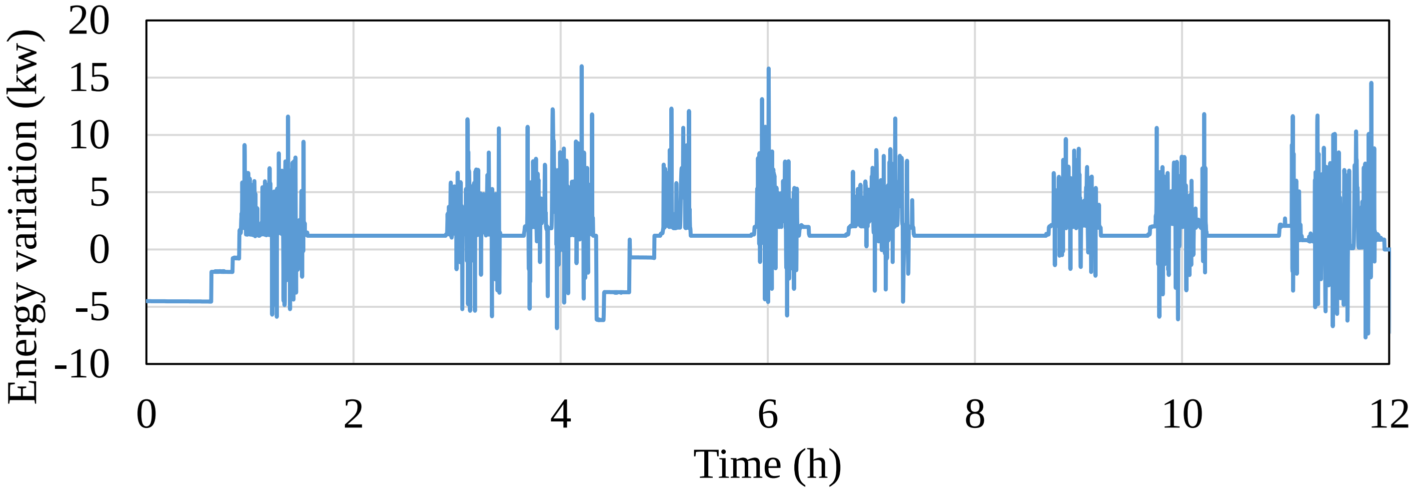
Steering system

Auxiliary functions (Air condition)

Energy Consumption Source Identification

Energy variation time series

Represent a set of energy variations and each energy variation ($\Delta E_t = E_t - E_{t-1}$) is caused by an appliance state change



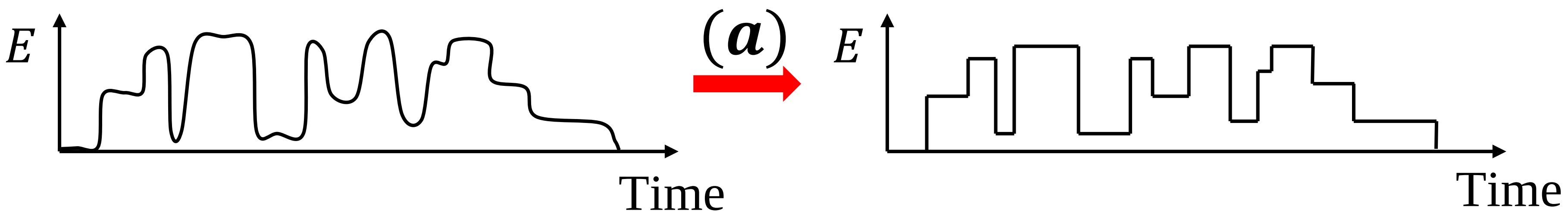
Identify energy consumption sources

- Energy variation clustering
- Energy variation matching

Energy Consumption Source Identification

Energy variation clustering

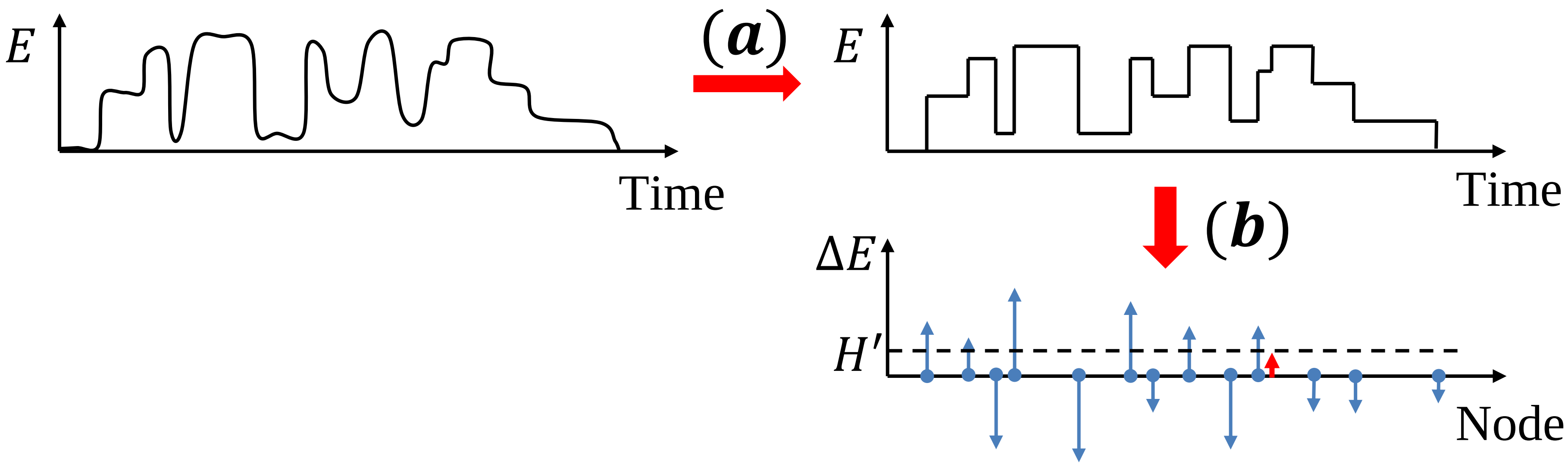
- Pre-process energy consumption data



Energy Consumption Source Identification

Energy variation clustering

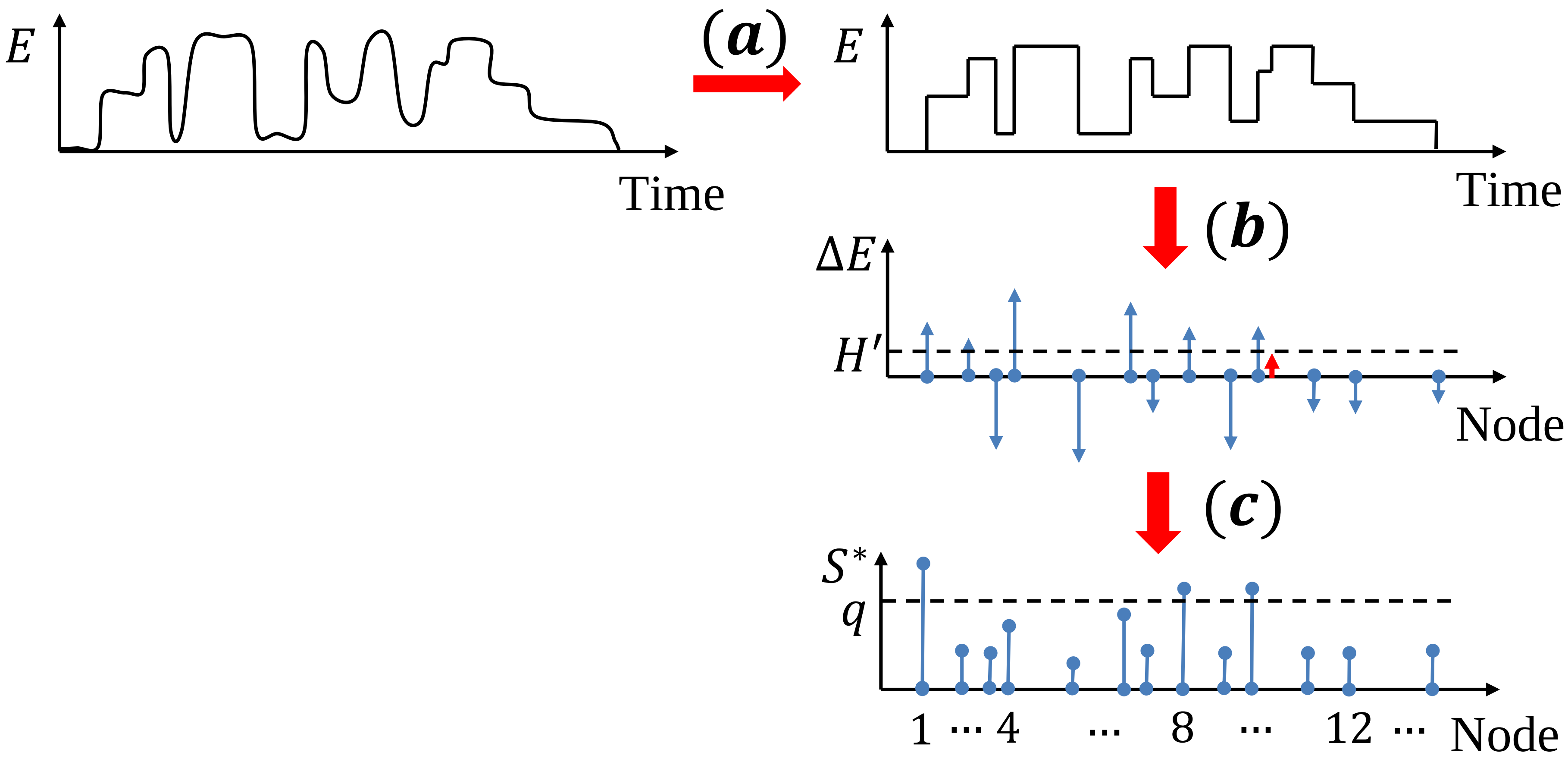
- Calculate energy variation ΔE and make comparisons with H' to form a new graph



Energy Consumption Source Identification

Energy variation clustering

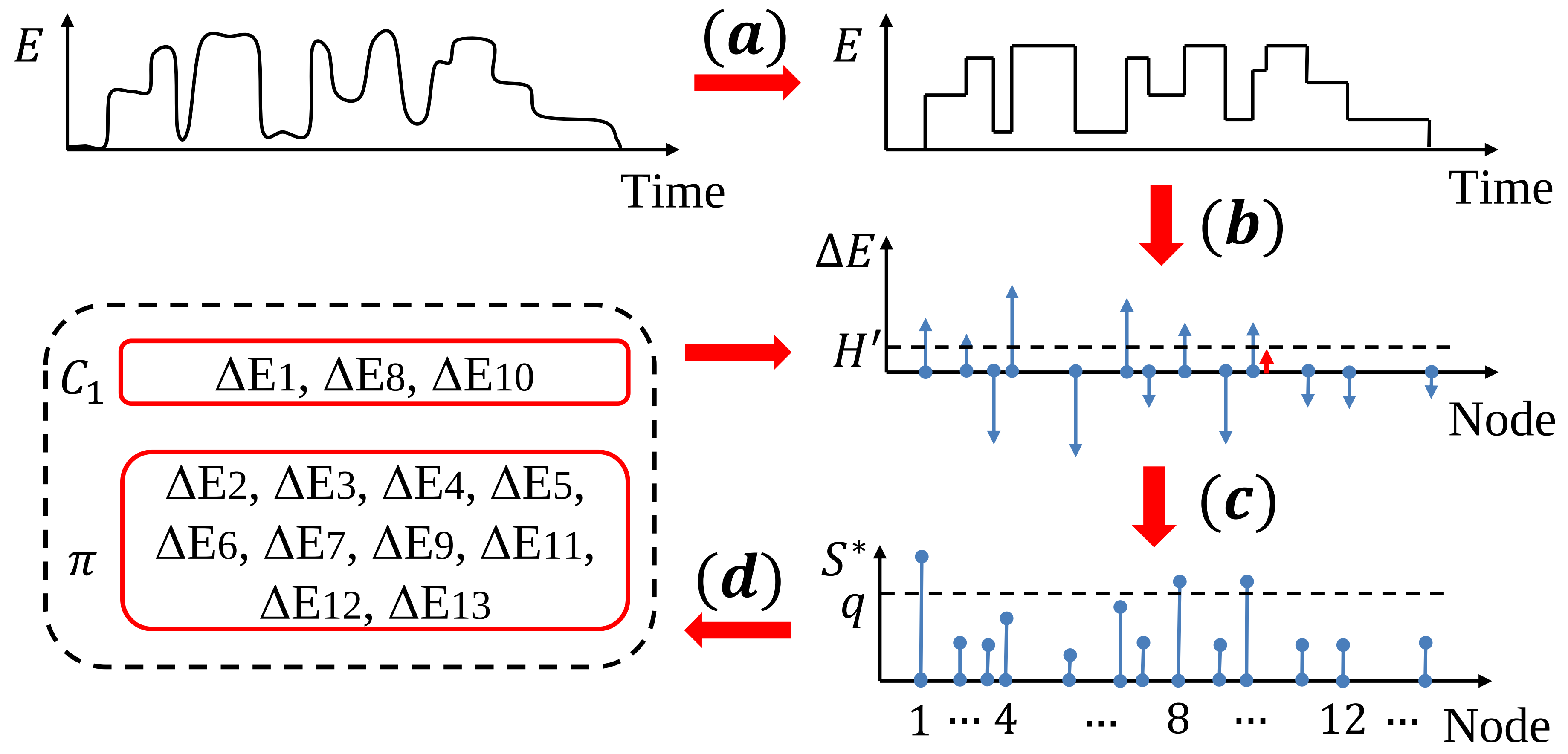
- Calculate global note states s^* and compare them with threshold q



Energy Consumption Source Identification

Energy variation clustering

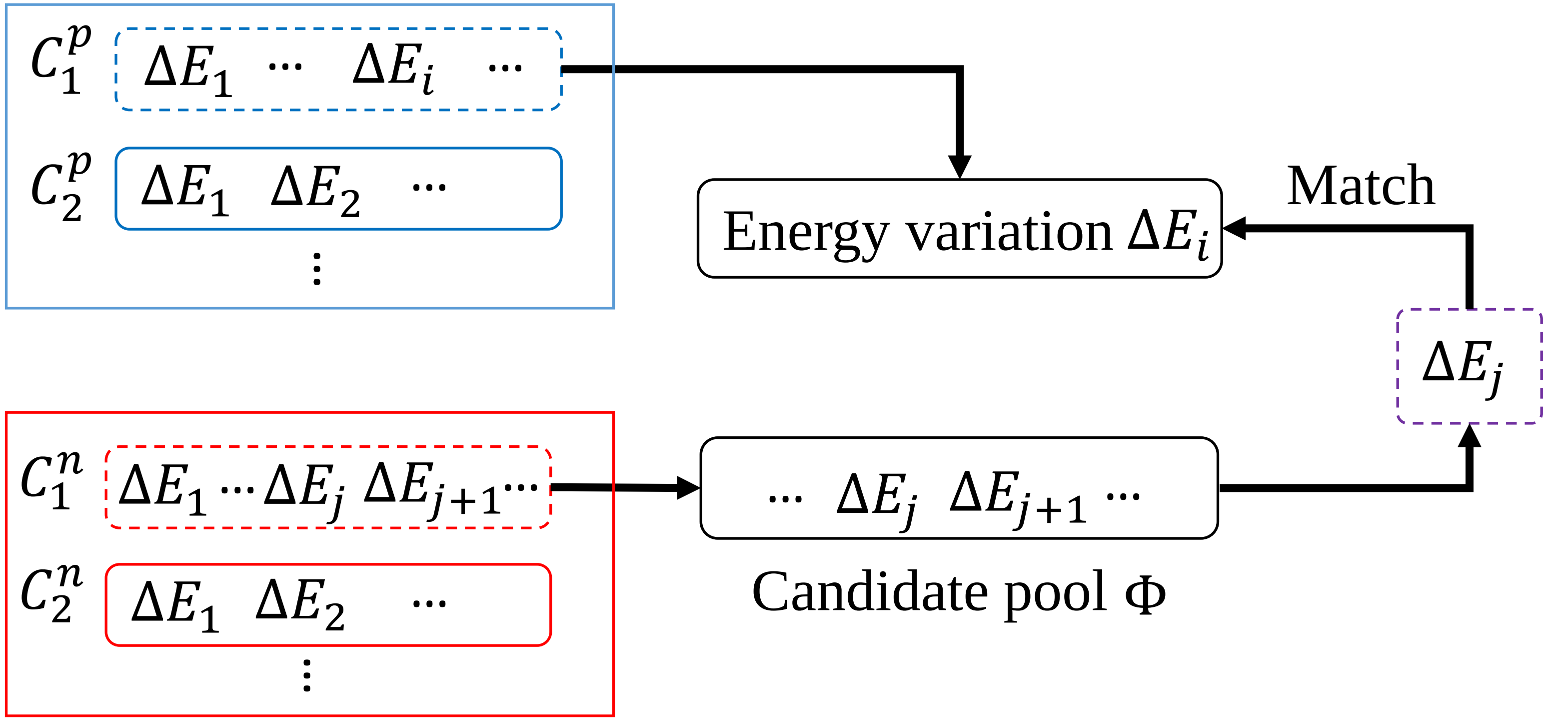
- Assign energy variations with higher s^* together into one cluster and other left energy variations to form a new graph



Energy Consumption Source Identification

Energy variation matching

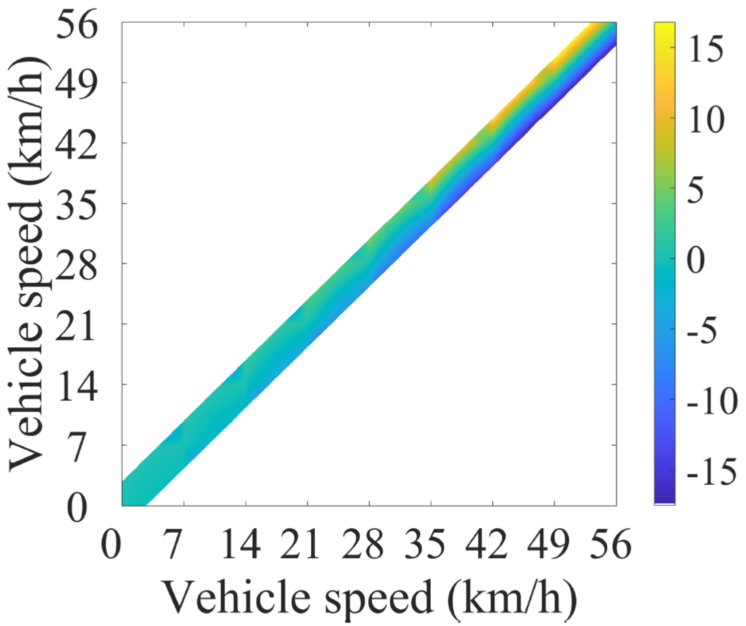
- The number of positive clusters equals to the number of negative clusters
- Match each positive energy variation with a negative energy variation having similar absolute values



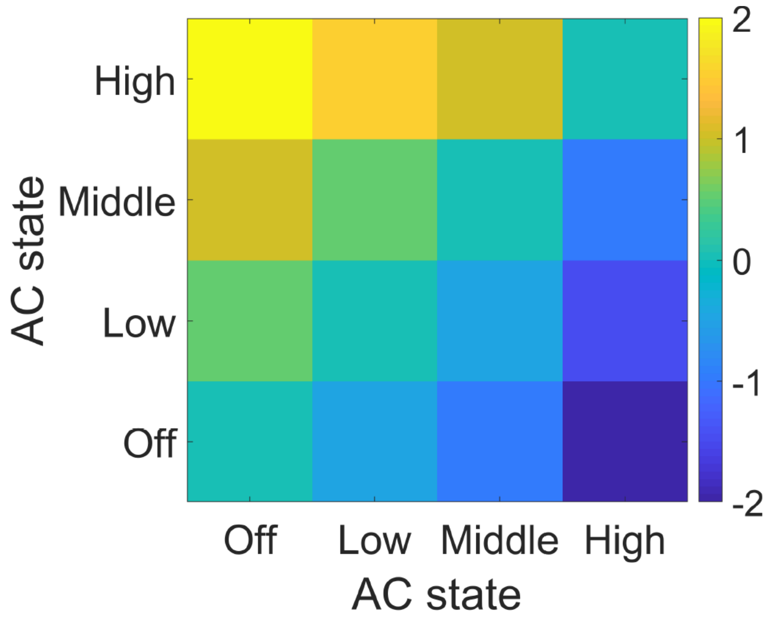
Appliance State Estimation

State change energy variation (SCEV)

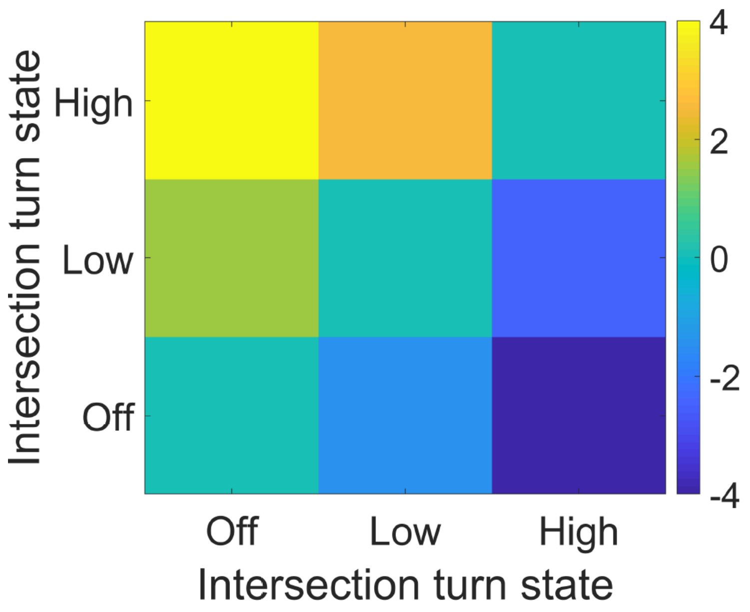
Energy variation value when an EV's state changes from one appliance state to another appliance state



SCEV (kw) of vehicle speed



SCEV (kw) of AC state



SCEV (kw) of intersection turn state

Appliance State Estimation

Appliance state estimation problem

Given total J energy variations and their corresponding time stamps, Bepath estimates appliance states by minimizing the sum of energy consumption differences:

$$argmin \sum_{j=1}^{J} \left(f\left(a_{t_{j-1}} \to a_{t_j}\right) - \Delta E_j \right)^2$$

Where $f(a_{t_{j-1}} \to a_{t_{j-1}})$ represents SCEV for appliance state change $a_{t_{j-1}} \to a_{t_j}$

Challenge 2

How to infer a driving path of an EV based on its estimated appliance states?

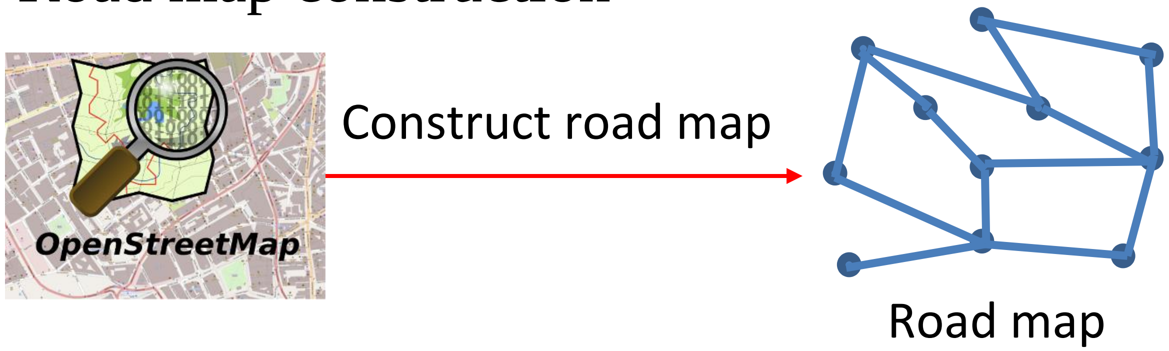
Vehicle Path Inference

Bepath infers possible paths of an EV based on the estimated appliance states (vehicle speed and intersection turns)

Vehicle Path Inference

Bepath infers possible paths of an EV based on the estimated appliance states (vehicle speed and intersection turns)

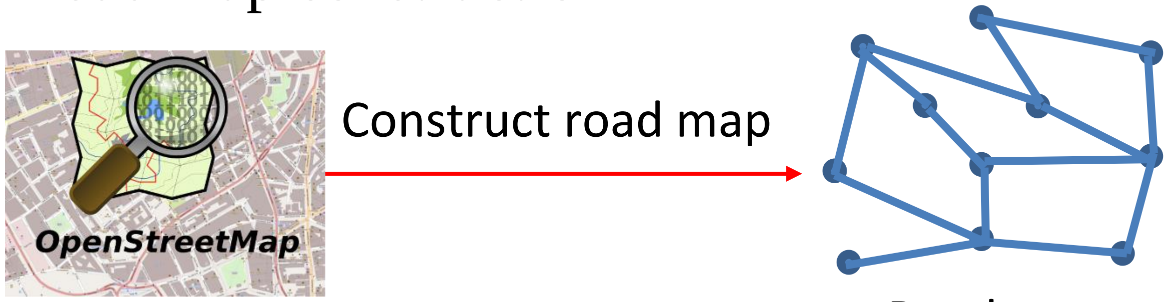
- Road map construction



Vehicle Path Inference

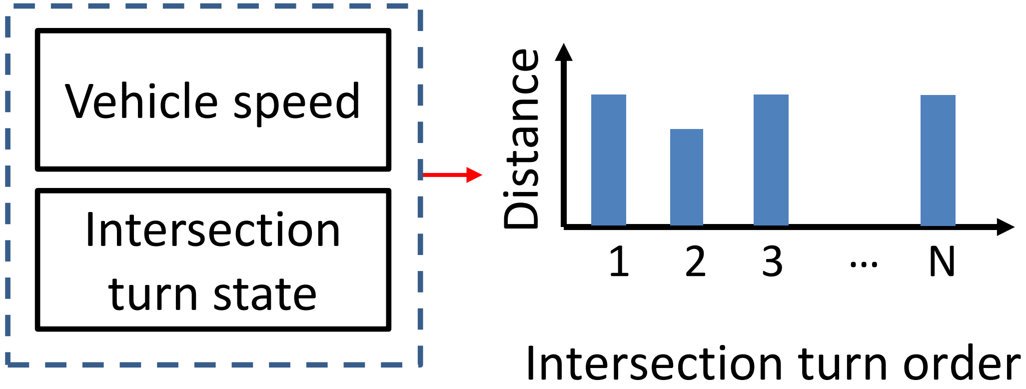
Bepath infers possible paths of an EV based on the estimated appliance states (vehicle speed and intersection turns)

- Road map construction



Road map

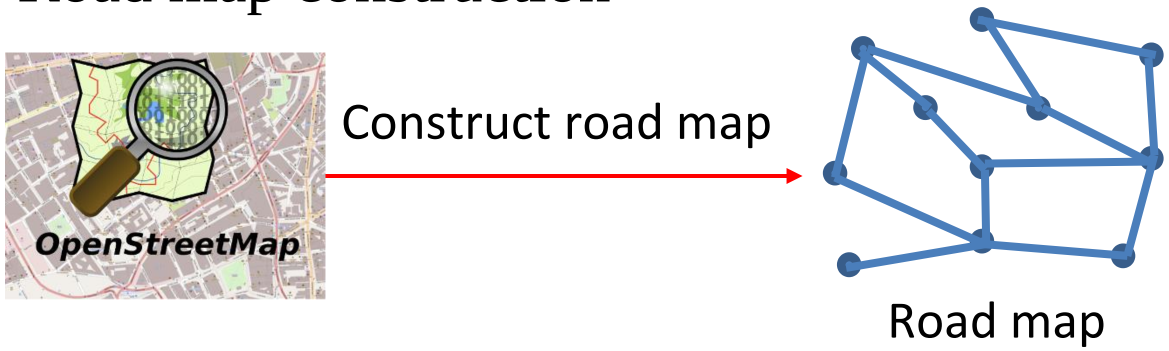
- Path candidate determination



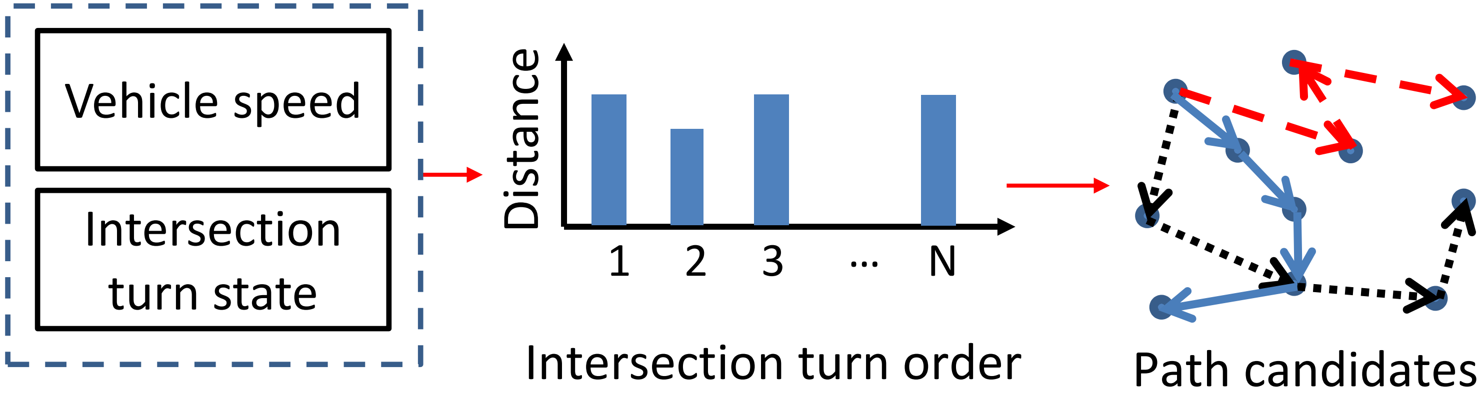
Vehicle Path Inference

Bepath infers possible paths of an EV based on the estimated appliance states (vehicle speed and intersection turns)

- Road map construction



- Path candidate determination

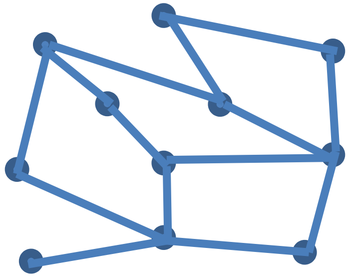


Vehicle Path Inference

Bepath infers possible paths of an EV based on the estimated appliance states (vehicle speed and intersection turns)

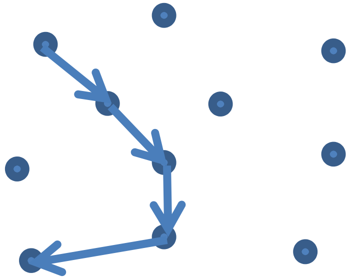
- Road map construction

Construct road map



Road map

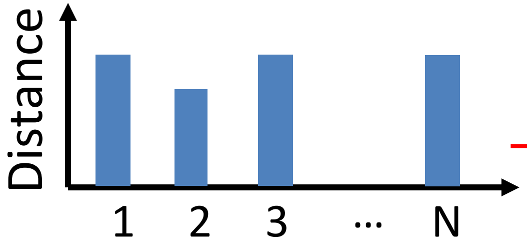
Final inference path



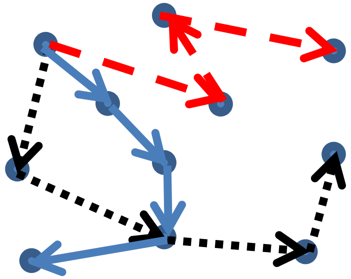
- Path candidate determination

Vehicle speed

Intersection turn state



Intersection turn order



Path candidates

$$argmin \sum_{j=1}^{K} \left(D\left(V_{j-1}, E_j, V_j\right) - D_j\right)^2$$

Performance Evaluation

Experiment settings

- Obtain real-world EV driving data from [National Big Data Alliance of New Energy Vehicle]
  - Total 8 EVs for 7 days in Beijing city
  - Average driving distance per EV per day is more than 100 km
  - Covers driving actions including parking, turn, acceleration and deceleration
- Implement Bepath in a laptop (Intel i5 CPU and 16 gigabyte memory)

Comparison method

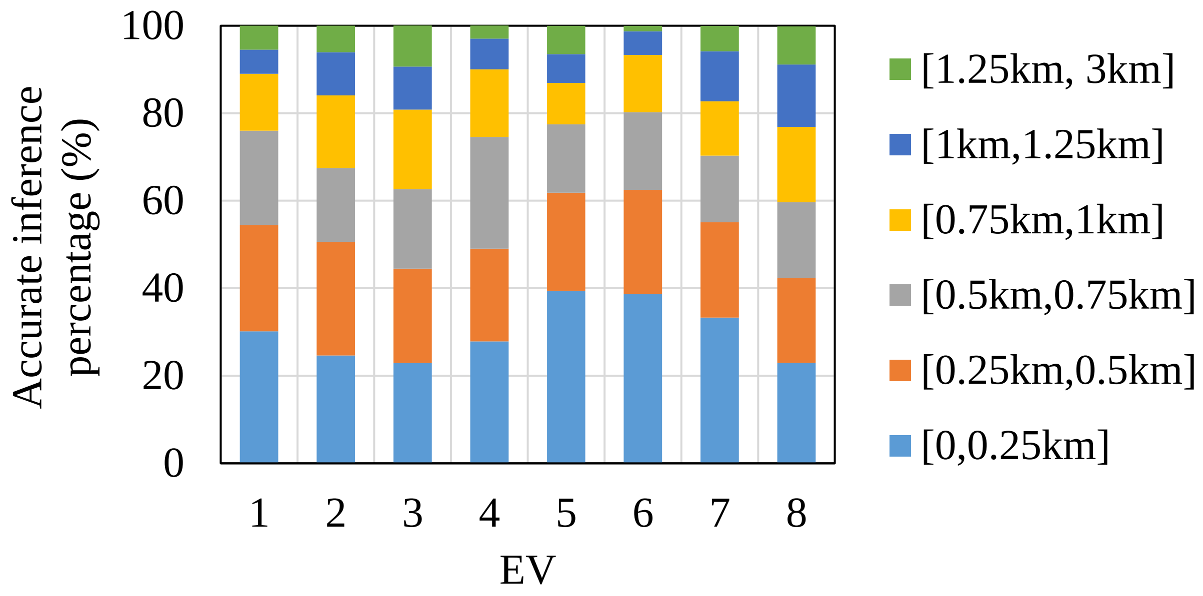
- Elastic path [Ubicomp'14] infers a vehicle path based on driving speed and starting point of the path

Performance Evaluation

Path inference accuracy evaluation

Infer driving paths of 8 EVs and compare path inference results with true paths:

- Around 50% of trips are inferred accurately by Bepath if Γ equals to 0.5km



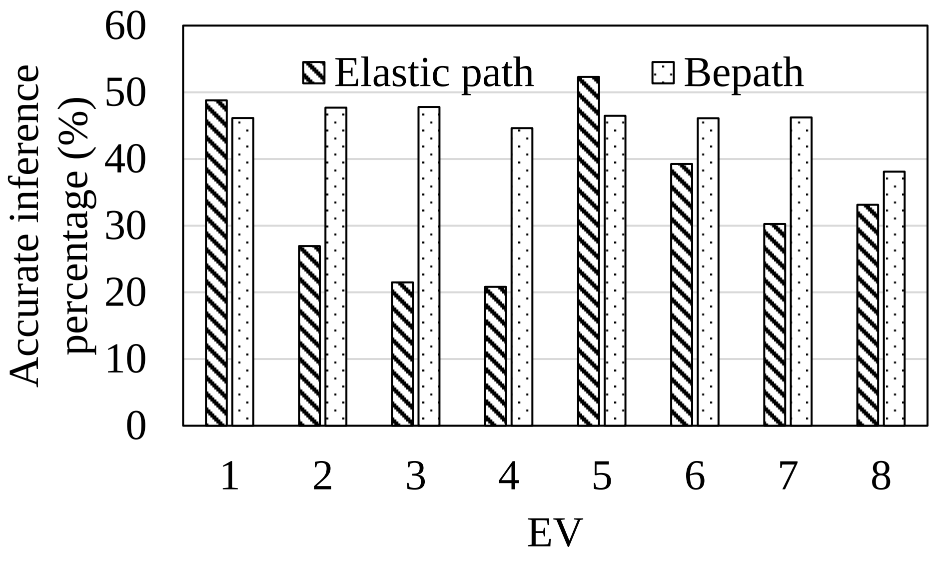
Accurate inference percentages of Bepath when the maximum distance error is located at different error ranges

Performance Evaluation

Path inference accuracy evaluation

Compare path inference accuracies between Bepath and Elastic path

- Has higher path inference accuracies than Elastic path
- Most of path inference accuracies are larger than 40% for Bepath



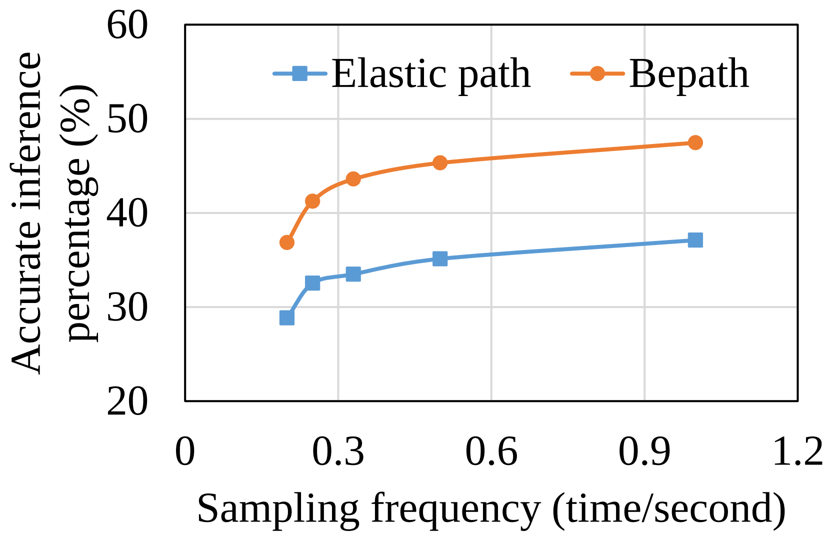
Path inference accuracy comparison

Performance Evaluation

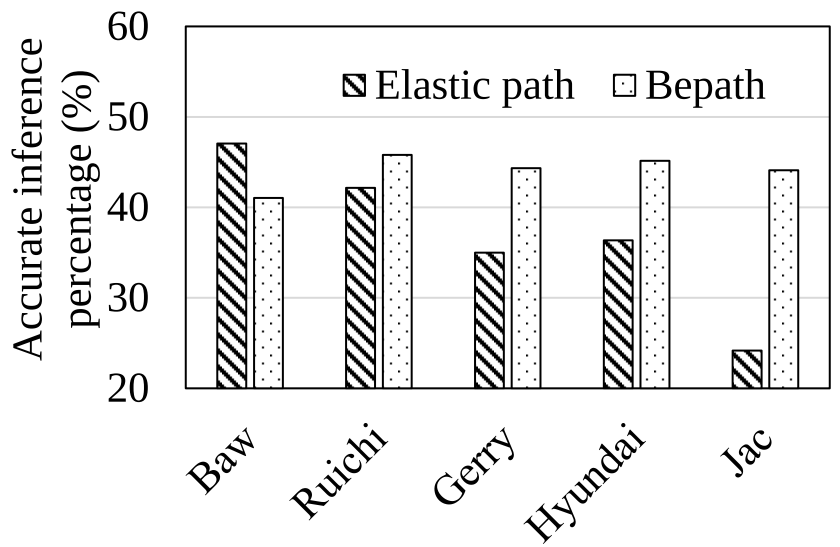
Robustness to sampling frequencies and vehicle types

Test with data including 5 different sampling frequencies and 5 different types

- Higher path inference accuracy as sampling frequency increases
- Bepath keeps almost constant path inference accuracy



Different sampling frequencies



Different vehicle types

Summary

Propose Bepath to infer paths of an EV based on its battery energy information:

- Identify energy consumption sources for appliance state estimation
- Infer paths based on the estimated appliance states
- Apply real-world EV driving datasets to verify Bepath

Future work:

- Consider more energy consumption sources (e.g., music play and light) to improve path inference accuracy

Thank you!

Performance Evaluation

Evaluation metric

- Accurate inference percentage represents the percentage of trips whose maximum distance errors between all inferred locations and all real locations at the same time-stamps are less than threshold Γ among the whole trips

$$\frac{\{n \in N \wedge \max\{g_{1:n}\} \leq \Gamma\}}{N}$$

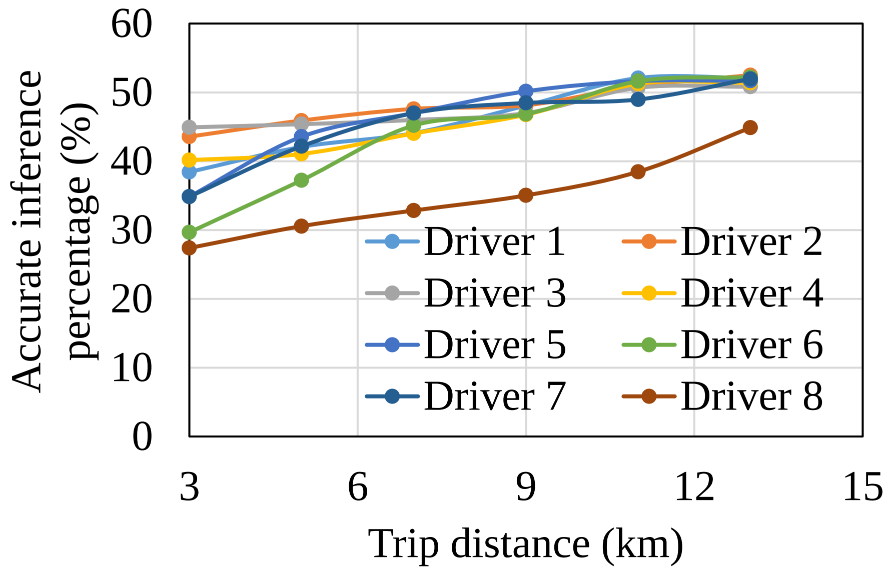
- A trip inference result is acceptable if its maximum distance error is less than 0.5km

Performance Evaluation

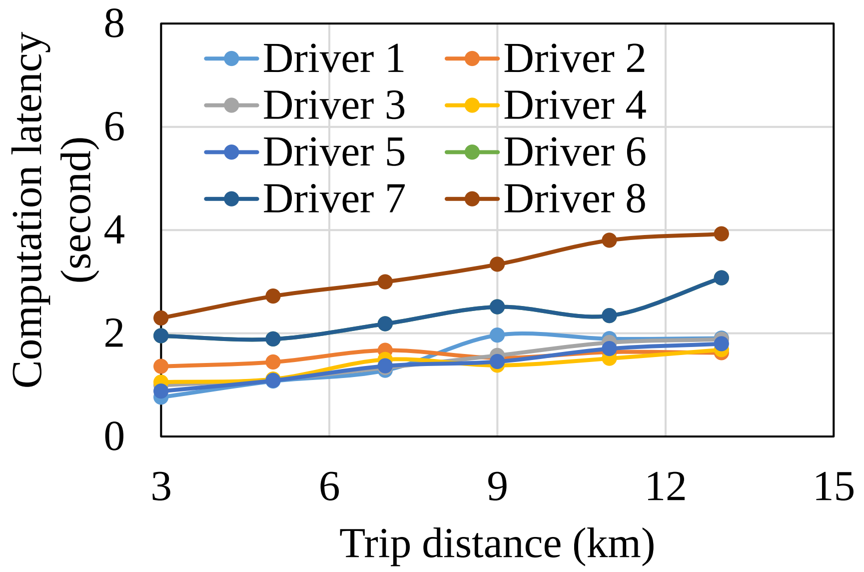
Path inference accuracy evaluation

Test performance of Bepath as trip distance increases from 3km to 13km

- Path inference accuracy increases because of a larger number of intersection turns
- Time latency increases but its maximum value is less than 4 seconds



Path inference performance as trip distance increases



Time latency as trip distance increases