

VE453 Quiz 2 Summary Questions

Routing

What are the demand and supply for a queuing network?

Given a time step Δt , at each time step

demand λ is a probability denoting whether one car will come into the network through the origin

supply μ is a probability denoting whether one car will finish its service through the destination

Why queues can build up in a network?

Each queue can be regarded as one node

We can build the network by connecting the queuing nodes in series and in parallel

The route can be represented as a sequence of nodes from the origin to the destination

What are static routing and dynamic routing?

| static routing | dynamic routing |
|--|---|
| traffic assigned with time-invariant fractions | traffic assigned with time-variant fractions |
| depends on model data (open-loop policy-free) | depends on model and environment (closed-loop policy-based) |
| not adaptive to disruptions | can respond to disruptions |
| only calculation at the beginning | real-time sensing and calculating abilities |

When is network stable?

The steady state size (or long-time average size) of the network has an upper bound

$$\bar{X} = \lim_{T \rightarrow \infty} \left[\frac{1}{T} \sum_{t=1}^T X(t) \right] < \infty$$

What is Bernoulli routing?

The probability of vehicle distribution β_{ij} are time-invariant (equivalent to policy-free)

Why dynamic routing can adapt to disruptions, such as demand surge and capacity drop?

Dynamic routing uses both the model data and the real-time environment data to make decisions. Compared with static routing, dynamic routing can receive the information of disruptions during the process and accordingly modify the routing behaviors to fit the new situations.

Air Traffic Control

What are some similarities and differences between road and air transportation?

similarities

- microscopic — each object transports from its origin to its destination
- macroscopic — flows of objects with safety constraints

differences

| road traffic | air traffic |
|--------------------------|--------------------------------|
| highly distributed | highly centralized |
| primary cost — time | primary cost — fuel |
| not sensitive to weather | extremely sensitive to weather |
| low automation level | high automation level |

Why are aircraft trajectory optimization more challenging than CAV trajectory optimization?

More complex process. Aircraft trajectory optimization including taking off and landing.

More complicated control. It is much harder to control an aircraft.

More difficult analysis. Parameters such as air drag is ineligible caused by its great speed.

More dimension. Aircraft trajectory is three-dimensional.

More constraints. Aircraft needs to follow more constraints to ensure its safety.

Smart Grid

What are the difference between a smart grid and conventional grids?

| old grid | smart grid |
|------------------------|------------------------|
| electromechanical | digital |
| one-way communication | two-way communication |
| centralized generation | distributed generation |
| few sensors | sensors throughout |
| manual monitoring | self-monitoring |
| manual restoring | self-healing |
| failures and blackouts | adaptive and islanding |
| limited control | pervasive control |
| few customer choices | many customer choices |

How to model a distribution network?

- Constraints
 - power conservation — $\widehat{S}_j = \sum_{k \in E} [\widehat{S}_k + \widehat{\mathbf{sc}}_j - \widehat{\mathbf{sg}}_j]$
 - voltage drop — $\widehat{v}_j = \widehat{v}_i - 2\text{Re}(\widehat{z}_j \widehat{S}_j)$
 - current-voltage-power — $\widehat{l}_j = \frac{|\widehat{S}_j|^2}{\widehat{v}_j}$
 - demand curtailment — $\mathbf{sc}_i = \gamma_i \mathbf{sc}_i^{\text{nominal}}$ where $0 \leq \gamma_i \leq 1$
 - soft bounds — $\underline{v}_i \leq v_i \leq \overline{v}_i$
 - hard bounds — $\underline{\mu} \leq v_i \leq \overline{\mu}$
- Objective functions
 - minimize $J = L_{\text{VR}}(x) + L_{\text{LC}}(x) + L_{\text{LL}}(x)$
 - $L_{\text{VR}}(x) = \max_i [W_i(v_i - \underline{v}_i)H(v_i - \underline{v}_i)]$
 - $L_{\text{LC}}(x) = \sum_i [C_i(1 - \gamma_i)\mathbf{pc}_i^{\text{nominal}}]$
 - $L_{\text{LL}}(x) = \sum_i [r_i l_i]$

What are DERs?

Distributed Energy Resources (DER) are electric generation units located within the electric distribution system at or near the end user.

What is demand curtailment?

Demand curtailment shows the relationship between actual transmitted power and the original demand represented by $\mathbf{sc}_i = \gamma_i \mathbf{sc}_i^{\text{nominal}}$ where γ_i is the load curtailment

What are smart meters? How are they different from conventional meters?

the electric device that can record information with the following features

- support two-way communication between the meters and the central system
- nearly real-time record information and sent to the Utility for monitoring and billing purpose
- be able to disconnect/reconnect remotely and control the users' appliances and devices to manage loads and demands

needs additional hardware investment and faces cyber security concerns

Smart Meters

What are linear regression & linear classification?

linear regression — use a linear function to predict the actual value of y given x

linear classification — use a linear function to predict the category $P[y \in G_1]$ of y given x

linear classification is a special case of linear regression

What are the inputs & outputs to the smart meter problem?

- input — load power curve
 - edge signatures
 - sequence signatures
 - trend signatures
 - time/duration signatures
 - phase signatures
- output — whether an appliance should be active

Why linear regression cannot be used to multiple (more than two) classes?

Linear regression can only generate a linear function, dividing the domain into two parts, which is impossible to predict multiple classes

How to convert power consumption data to input of a linear classification model?

Identifying different signatures for each appliance

For each appliance, collect all its signatures as a vector and multiply it with a weight vector

Input all the vectors as the power consumption import data to train a linear classification model

Smart Grid Balancing

stage-1 formulation

- Constraints
 - $E_i^t \leq s_i^t \leq E_i^t + \frac{\alpha_i^t}{\beta_i}$
- Objective function
 - minimize $J = \sum_{t=1}^T \sum_{i=1}^N \left[\theta C_i (r_i^t)^2 + (1 - \theta) \beta_i (s_i^t - E_i^t) E_i^t \right]$
 - $r_i^t = \frac{E_i^t + \beta_i}{C_i}$

stage-2 formulation

- Constraints
 - workload constraint — $\sum_{i=1}^N [\lambda_i^t] = L^t$ and $\lambda_i^t \geq 0$
 - QoS constraint — $d_i^t + \frac{1}{\mu x_i^t - \lambda_i^t} \leq D$ and $\mu x_i^t - \lambda_i^t > 0$
 - server constraint — $0 \leq x_i^t \leq M_i$
 - Energy consumption constraint — $a \lambda_i^t + b x_i^t + c = E_i^t \leq q_i^t$
- Objective function
 - minimize $J = \sum_{t=1}^T \sum_{i=1}^N \left[(\alpha_i^t + \beta_i (E_i^t - s_i^t)) E_i^t \right]$

CAV Security

What types of attacks do CAVs face?

- Application-layer attack — directly attack the application itself
 - Flasification attack
 - Spoofing attack
 - Replay attack
- Network-layer attack — affect the functioning of user applications
 - DDoS

- System-level attack — attack the vehicle hardware or software
- privacy leakage attack — collect privacy data for attackers' own benefits

For CAVs, how does cyber security influence physical safety?

If cyber security cannot be ensured, then the CAV application may malfunction, and provide wrong instructions based on fake information. Then the vehicles may not be controlled correctly, or even crash with each other.

What are the actions and objectives for CAV attackers and defenders?

attackers

- Actions
 - DDoS — erase certain pieces of information
 - Spoofing — modify certain pieces of information
 - Manipulations — modify instructions
- Objectives
 - create safety issues or even accidents
 - maximize efficiency loss

defenders

- Actions
 - increase security investment
 - improve encryption technology
 - maintain safety margins
 - isolate detected malicious information
 - switch to or activate redundant information sources
 - intervene the trajectories with the neighboring vehicles
- Objectives
 - ensure safety and security
 - improve efficiency

Network Security

Why is game theory relevant to cyber-physical security problems?

Game theory can be regarded as the analysis of multi-agents performing actions over one problem for their own benefits.

In cyber-physical security problems, attackers can be viewed as an agent intended to create safety issues and maximize efficiency loss, and defenders can be viewed as an agent intended to protect the application and improve the efficiency. Moreover, current attack over cyber-physical applications becomes more organized, and it can show that both attackers and defenders want to achieve the best goal for them respectively. It is reasonable to apply game theory to analyze cyber-physical security problems.

What are players, strategies, utilities, and equilibria?

- players — the agents that can perform action in the problem
- strategies — the function for one player to output an action by inputting the current state
- utilities — the expected gain one player could get if he choose the action or follow the strategy
- equilibria — a specific state that all players prefer (no utility can be improved by any unilaterally changed action)