COMP2410/6340
Automated Decision Making & Cyber (Physical) Security – Part 1

Hanna Kurniawati

http://users.cecs.anu.edu.au/~hannakur/
Fun video (if you’re not the driver…)

Source: https://www.youtube.com/watch?v=MK0SrxBc1xs
Cyber Security in Physical Systems

• Is important

• Interestingly, the same methods that made autonomous robot operate robustly can be used to improve cyber security (for physical and non-physical systems)

→ Decision-making under uncertainty
This set of videos

- **Part-1: Intro**
  - Automated decision-making
- **Part-2: Intro to POMDP**
  - Framework for decision-making under uncertainty
  - Solving, aka. generating strategic decisions
- **Part-3: Example of POMDP in Cyber security**
  - Autonomous pen-testing
What is automated decision-making?

• Intuitively, a mechanism to enable computers make decision on what to do now, so as to get good (long term) outcomes

• Where is it used? Lots of places

Robot

Computer network (router, web crawler, security, etc.)

Email (spam filter)
How do we model the problem?

• As an agent that:
  • Gathers information about an environment
  • Decide what to do autonomously based on that information, to achieve a good outcome
An agent is defined as a tuple \(<S, A, O, T, Z, U>\):

- **State space** (S)
  - Properties of the agent & the environment that matter for the interaction between the agent & the environment in achieving a pre-specified outcome.

- **Action space** (A)
  - The set of all actions the agent can do.

- **Observation space** (O)
  - The set of all things the agent can perceive about its state.
A bit more formal…

• System dynamics (T: SXA → S)
  • A mapping from the current state and the action the agent performs to the next state.
  • Often called transition function
• Observation function (Z: S → O)
  • A mapping from the current state or state-action pairs to observations that can be perceived by the agent
• Utility function (U: S → real number)
  • A function that assigns a value to each state (or sequence of states or state-action or state-action-observation), to indicate the desirability of being in such a (sequence of) state with respect to the agent’s task.
Solving means…

• Finding a mapping from from a state to an action the agent will perform from the state \( (S \rightarrow A) \), so as to maximize a pre-specified utility function
• Often called policy or strategy
• Can be thought of as a “rule book”.
• Can also be mapping from histories of action—observation pairs that have been performed and perceived by the agent to the next action \( ((AXO)^* \rightarrow A) \)
The agent as defined earlier is called rational agent in Artificial Intelligence
Classes of problems …

• Properties about the environment itself or the agent’s knowledge about the environment
  • **Discrete vs continuous (space and time)**
    • Are the state / action / observation discrete set?
    • Are the time discrete?
  • **Deterministic vs non-deterministic**
    • Does the agent always know exactly which state it will be in after it performing an action from a state?
    • Is the system dynamics (T) a function (i.e., does it map each state—action pair to exactly one next state)?
  • **Fully observable vs partially observable**
    • Can the agent infer its exact state exactly from an observation?
• **Static vs dynamic**
  • Can the world change while the agent is “thinking”?
This set of videos

✓ Part-1: Intro
  ✓ Automated decision-making

• Part-2: Intro to POMDP
  • Framework for decision-making under uncertainty
  • Solving, aka. generating strategic decisions

• Part-3: Example of POMDP in Cyber security
  • Autonomous pen-testing