

Routing for Autonomous Vehicles

Yixuan Liu¹

yixuan.liu@utexas.edu

Andrew B. Whinston^{1,2}

abw@uts.cc.utexas.edu

¹ McCombs School of Business, University of Texas at Austin

² Department of Computer Science, University of Texas at Austin

TPI's Artificial Intelligence conference

February 2018

Washington, D.C.

A modern interpretation of Pigou Paradox

live**mint**

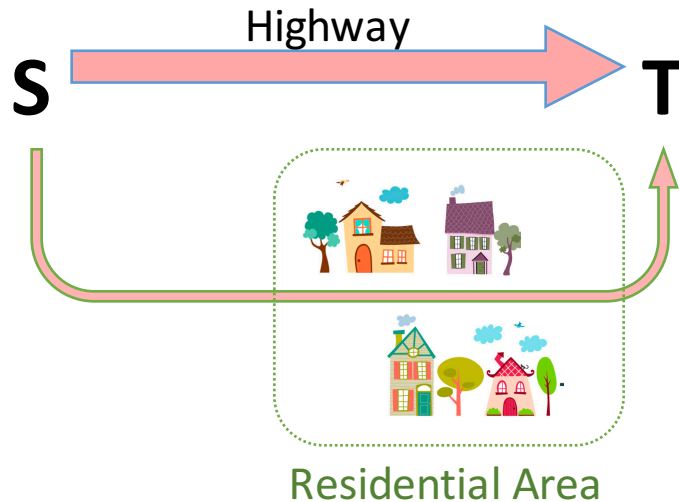
Home » Opinion » IT Matters

Of Map Apps and Traffic Jams

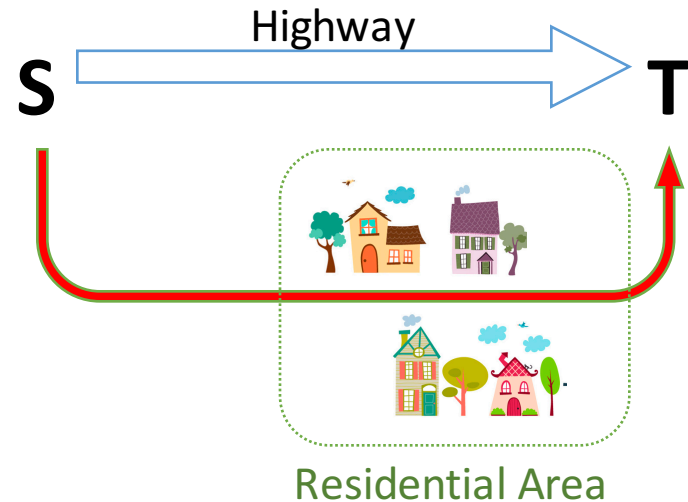
Real-time updates to traffic congestion now find their way on to apps such as Google Maps and this information is then used by the programme to re-route traffic through quieter areas

Last Published: Mon, Feb 05 2018. 10 23 PM IST

Without a truthful Waze

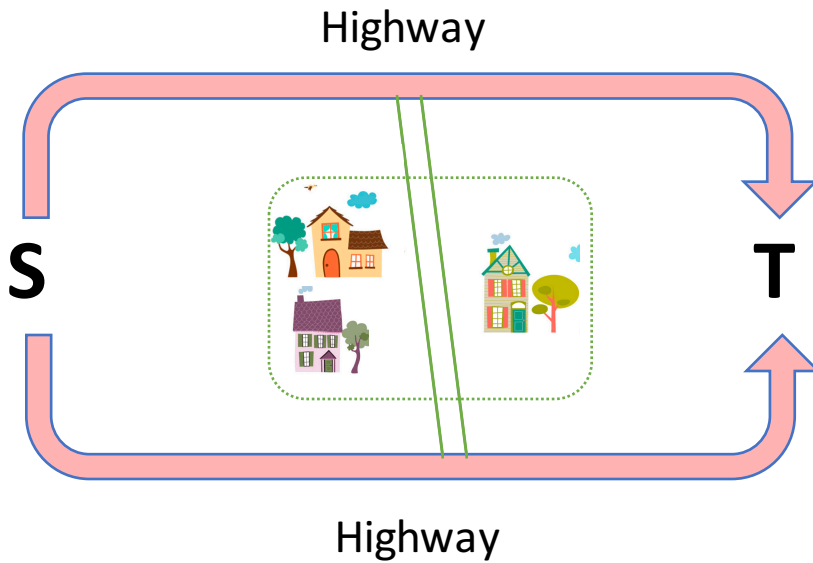


With a truthful Waze

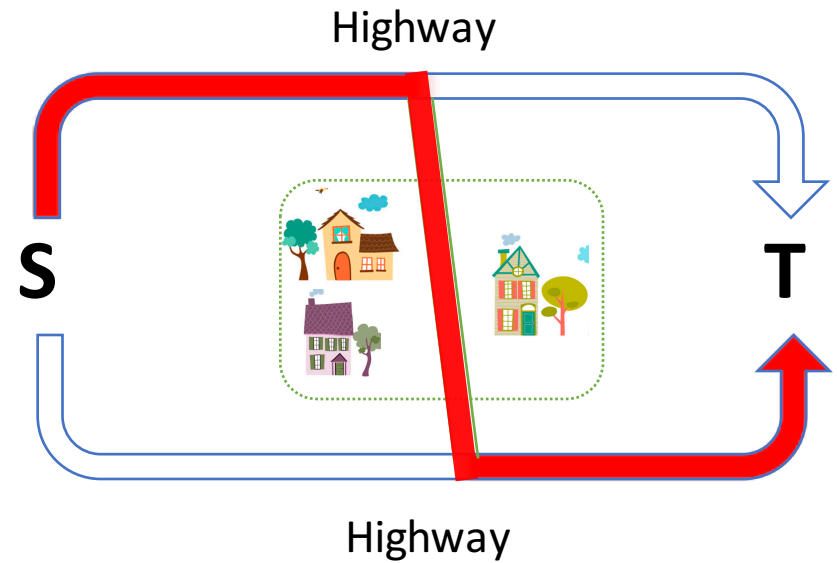


A modern interpretation of Braess Paradox

Without a truthful Waze



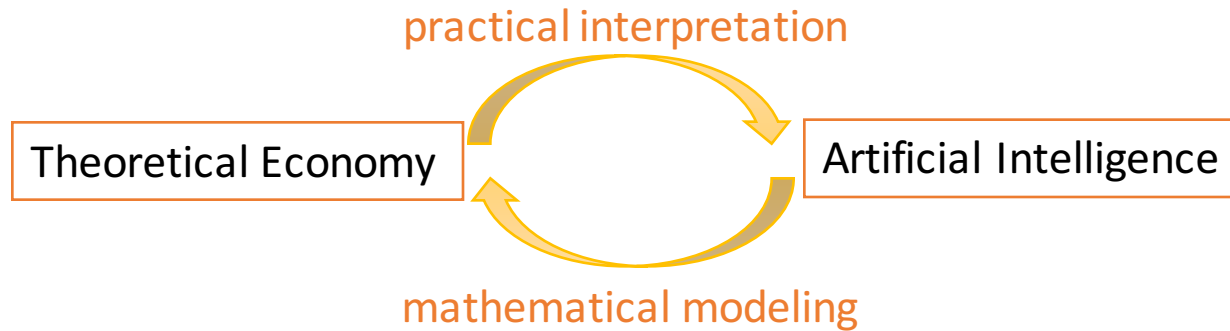
With a truthful Waze



Shall we *lie* to autonomous vehicles?

The benefits of *fake* information

Challenges of Converting Econ to AI



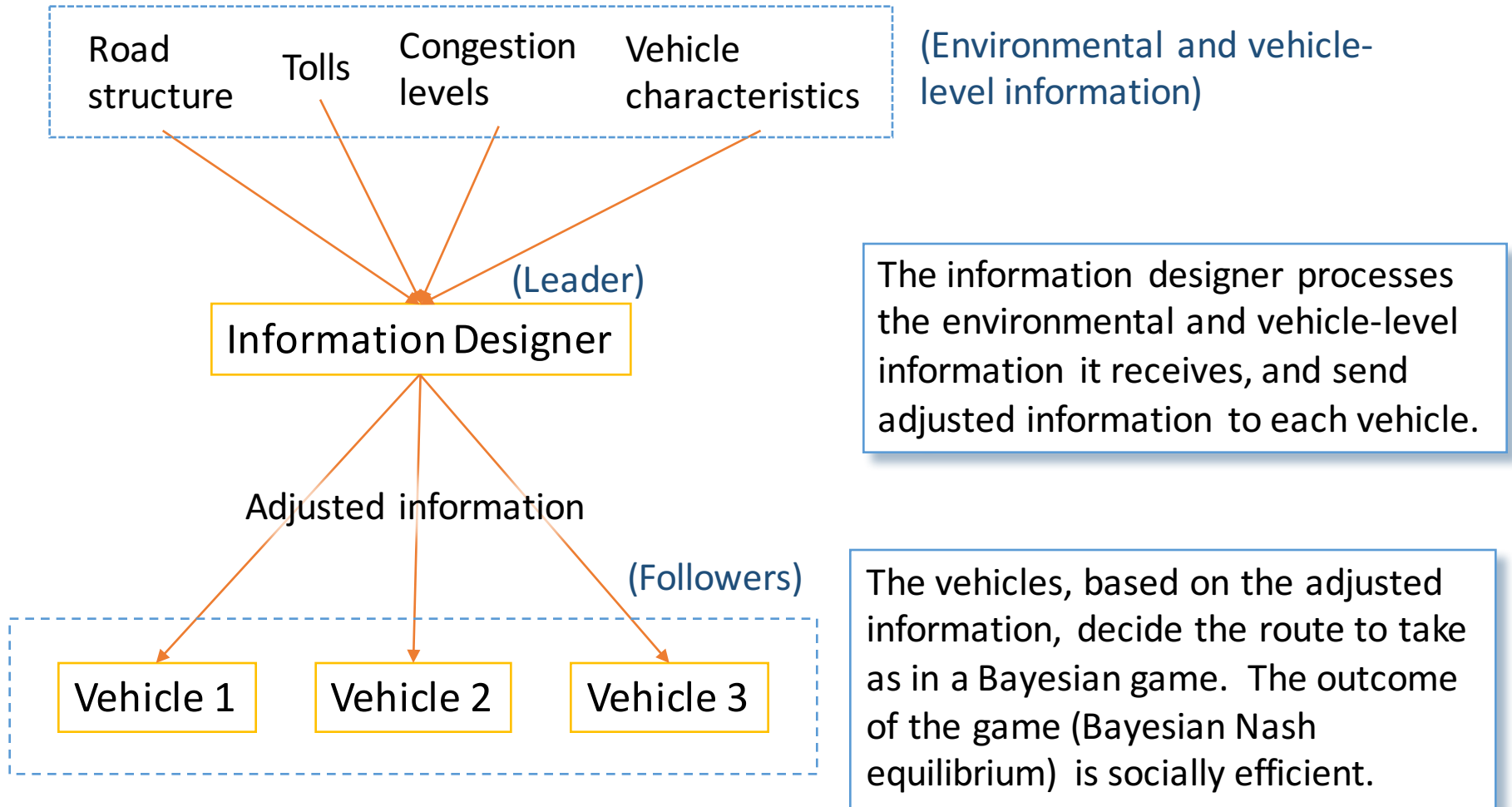
Technology

- Autonomous vehicles
- Vehicle-to-Vehicle (V2V) communication
- sensor data

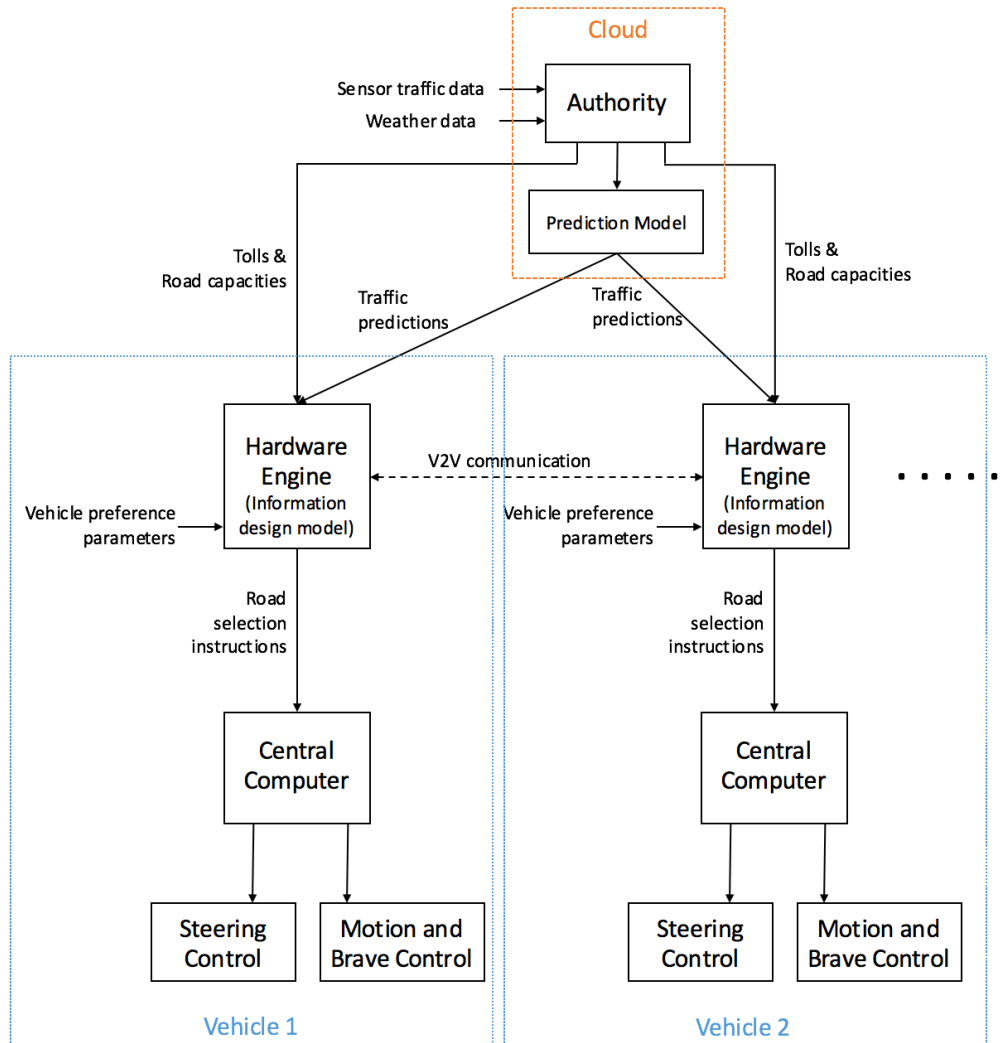
Economic theory

- Bayesian persuasion

Diagram



Institutional Arrangement and ASIC



Impact on Future Labor Market

Displacement effect

- substitute drivers

FINANCIAL TIMES

Driverless vehicles

Out of road: driverless vehicles and the end of the trucker

New self-driving technology threatens an American way of life

Leslie Hook

MARCH 29, 2017

Productivity effect

- provide transportation service to people
- increase demand for labor in sensor engineers, data scientists, urban designers, etc.

Reference: Acemoglu, D., & Restrepo, P. (2018). *Artificial Intelligence, Automation and Work* (No. w24196). National Bureau of Economic Research.

Impact on Environment

The greatest environmental challenge: Global warming

- greenhouse gas emissions

An efficient transportation system of autonomous vehicles could potentially push the movement forward towards a carbon-free economy.

- path optimization \Rightarrow decrease the aggregate miles traveled by vehicles
- less congestion on roads \Rightarrow decrease the idle time vehicles spend

Security

Application Specific Integrated Circuits (ASICs) are less vulnerable to security-related attacks than general-purpose solutions, but they can still be compromised via certain methods.

- Not vulnerable to attacks that exploit security vulnerabilities in operating systems or certain software running on computers
- Vulnerable to attacks targeted at communication between the ASIC and the cloud
 - The Internet protocols and standards (e.g. HTTPS, SSL, etc.) can be implemented in hardware to provide encryption, data integrity, authentication, and non-repudiation.
- Vulnerable to attacks that are related to how they are manufactured (or programmed)
 - Trojans
 - reverse engineer integrated chips provided physical access