Fraud Risk Mitigation in Real-Time Payments: A Strategic Agent-Based Analysis

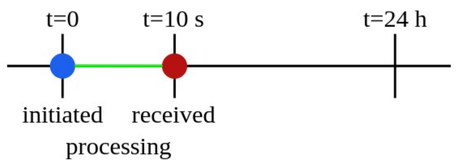
Katherine Mayo, Nicholas Grabill, and Michael P. Wellman

By analyzing an agent-based model of the real-time payments scenario, we find:

- Banks liable for fraud are more likely to employ restrictions and a high level of fraud detection
- Restricting customer use is an important initial mitigation technique for banks
- Strategic measures of banks negatively affect fraudsters while minimally impacting customers

Motivation

Real-time payment (RTP): a payment characterized by immediate or near-immediate (~10 sec) receipt of funds



Fraud Risk in RTPs

- Manual fraud detection averages 5 - 10 minutes
- Fraudsters exploit the limited ability for fraud detection systems to handle the required speed
  - Faster Payment Service introduction led to 132% increase in fraud in the UK
  - Authorized Push Payments largest fraud in the UK in 2018

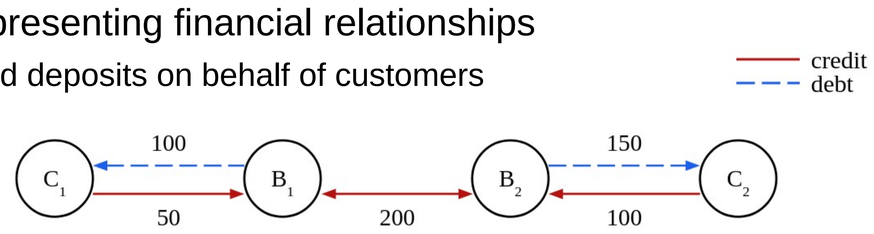
Studying Strategic Mitigation of Fraud Risk

- Define an RTP fraud game played by banks and a fraudster in an agent-based model of the payments system
- Analyze using empirical game-theoretic analysis to identify Nash equilibria

Payments Network Model

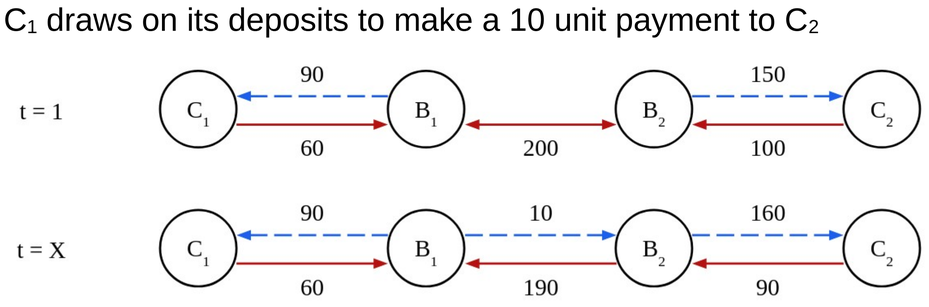
Idea: Banks and customers are nodes connected by directed edges representing financial relationships

- Banks hold deposits on behalf of customers



Standard Payment:

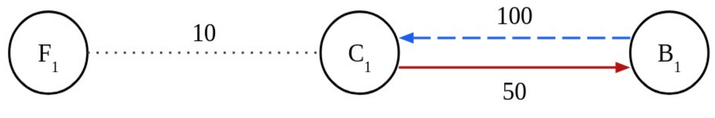
- C_1 draws on its deposits to make a 10 unit payment to C_2



- A real-time payment updates all edge values in t = 1

Fraudster:

- Connected to victim by a fraud edge
- Remaining payment steps are the same as non-fraudulent payments



UNIVERSITY OF MICHIGAN

Contact: kamayo@umich.edu

RTP Fraud Game

Strategies:

- Banks: max threshold and investment level in fraud detection for RTPs
- Fraudster: payment type and rule for choosing banks to target for fraud

Game Steps:

- Assign customers to banks assuming they prefer a bank that meets their RTP preferences
- Generate random customer and fraudster payments over T time steps
  - Type determined by value, sender and receiver, and bank strategy
- All payments go through black-box fraud detectors defined by accuracy
  - Accuracy: probability the payment is correctly labeled

Payoffs:

- Banks: initial deposits attracted, liability for fraud, detection costs
- Fraudster: amount of fraud successfully committed

Strategic Feature Gains Assessment

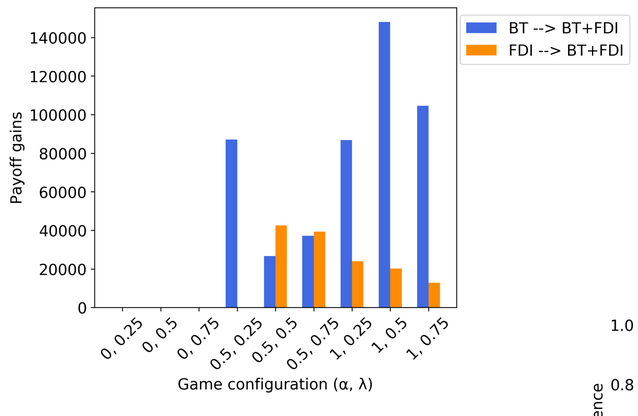
Idea: calculate payoff gain to agents for access to a deviation set of strategies (Δ) in reference to some base set of strategies (Ω)

1. Define Δ,Ω as disjoint subsets of S
2. Obtain the Nash equilibrium $\sigma^*(\Omega)$ using empirical game-theoretic analysis
3. Calculate the gain of Δ as: $max_{s \in \Delta \cup \Omega} \; u_i(\sigma^*_{-i}, s_i) - u_i(\sigma^*)$

Findings

Nash equilibria:

- Banks: balance restricting RTPs with investment in fraud detection
- Fraudster: target all payment types and select banks based on historical success



Strategic Feature Gains Assessment

Gain from one mitigation technique given prior access to the other

No mitigation measures vs NE

Number of successful payment attempts with no measures compared to under equilibrium