Combining Agent-Based Simulation and Adversarial Learning to Detect Market Manipulation

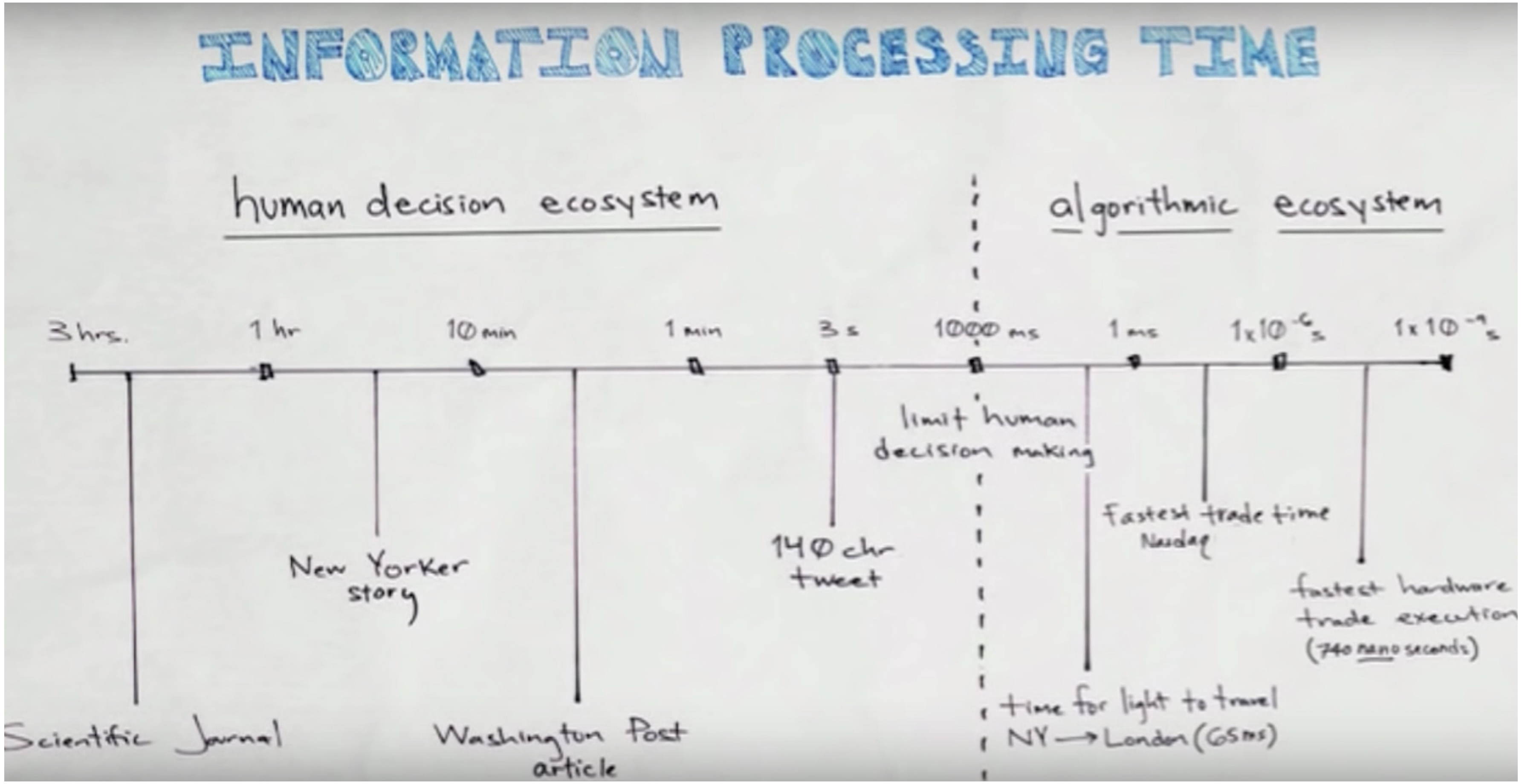
Xintong Wang

Jan 27, 2023 @ FINRA

COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY OF MICHIGAN

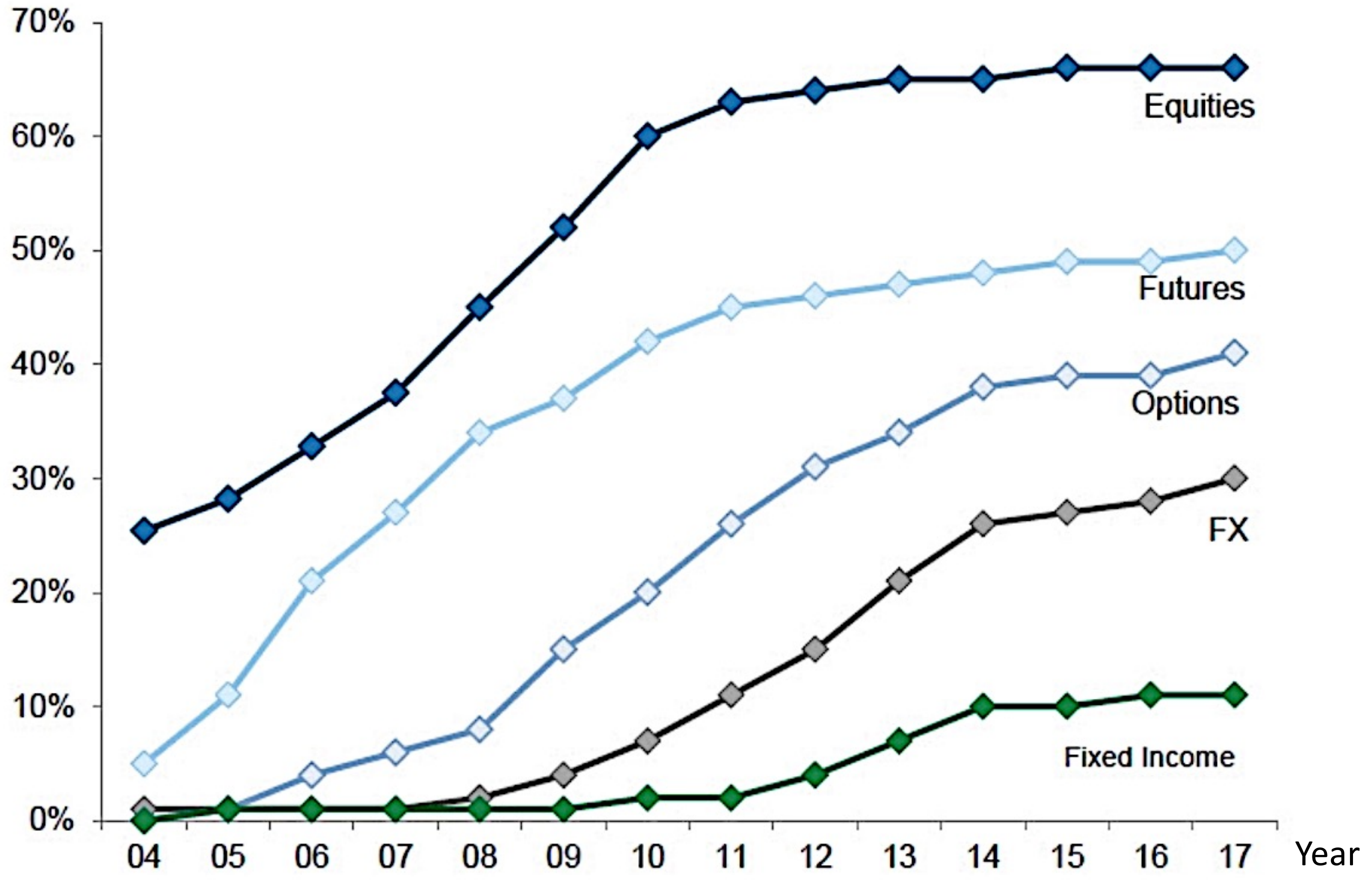
Harvard John A. Paulson School of Engineering and Applied Sciences

Financial Markets – An Algorithmic Ecosystem

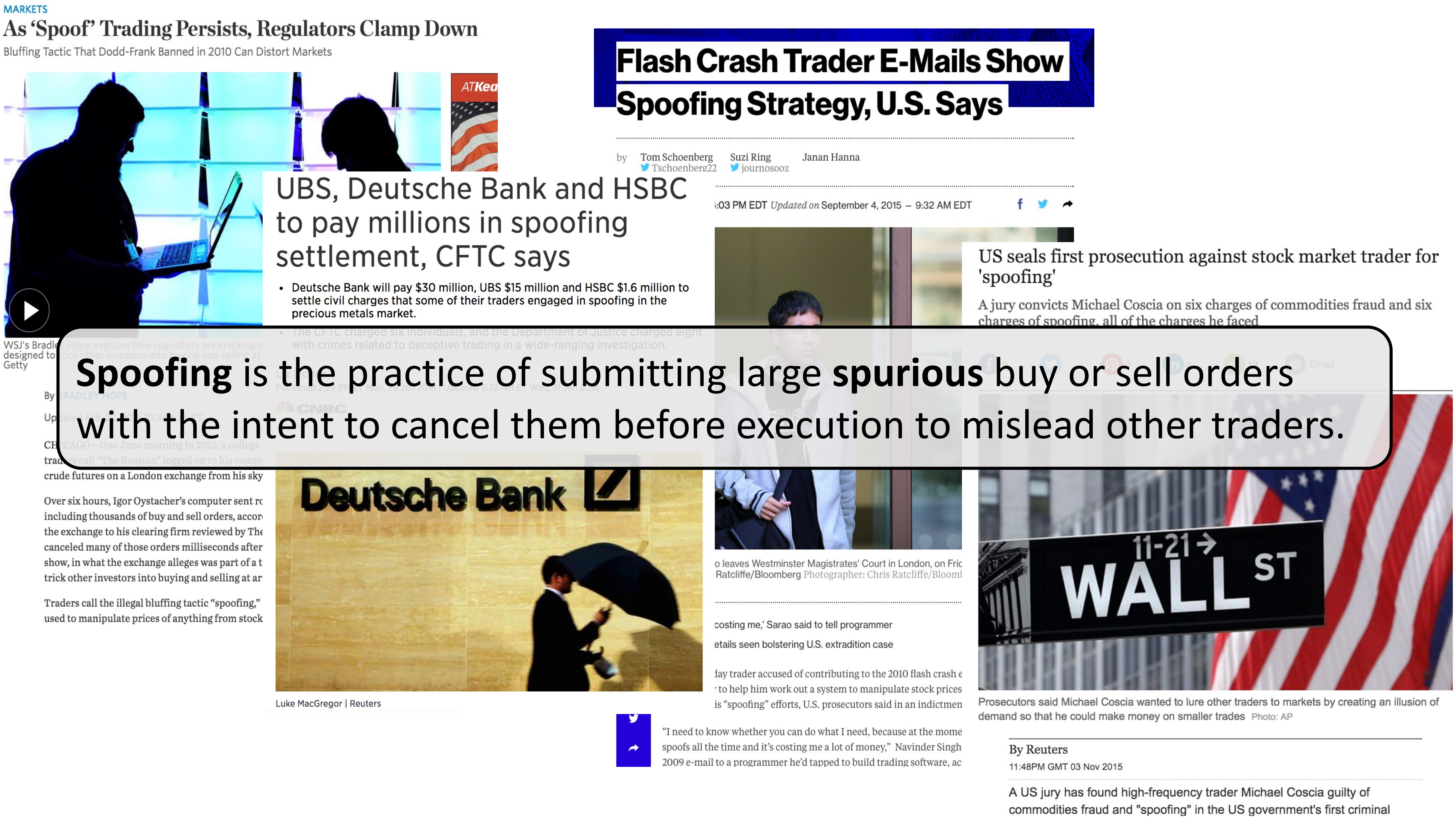

INFORMATION PROCESSING TIME
human decision ecosystem
algorithmic ecosystem
3 hrs.
1 hr
10 min
1 min
3 s
1000 ms
1 ms
1x10^-6 s
1x10^-9 s
limit human decision making
Scientific Journal
New Yorker story
Washington Post article
140 chr tweet
time for light to travel NY → London (65ms)
fastest trade time Nasdaq
fastest hardware trade execution (740 nano seconds)

Source: TEDxNewWallStreet by Sean Gourley.

Market Share of Algorithmic Trading



Source: Aite Group, Goldman Sachs Global Investment Research.



MARKETS

As ‘Spoof’ Trading Persists, Regulators Clamp Down

Bluffing Tactic That Dodd-Frank Banned in 2010 Can Distort Markets

WSJ's Bradley Hope explains how regulators are cracking d designed to trick other investors into buying and selling at Getty

By BRADLEY HOPE

Updated Feb

CHICAGO—One June morning in 2012, a college traders call “The Russian” logged on to his compu crude futures on a London exchange from his sky

Over six hours, Igor Oystacher’s computer sent ro including thousands of buy and sell orders, accor the exchange to his clearing firm reviewed by The canceled many of those orders milliseconds after show, in what the exchange alleges was part of a t trick other investors into buying and selling at ar

Traders call the illegal bluffing tactic “spoofing,” used to manipulate prices of anything from stock

Flash Crash Trader E-Mails Show Spoofing Strategy, U.S. Says

by Tom Schoenberg Tschoenberg22 Suzi Ring journosooz Janan Hanna

:03 PM EDT *Updated on* September 4, 2015 – 9:32 AM EDT

o leaves Westminster Magistrates' Court in London, on Fric Ratcliffe/Bloomberg Photographer: Chris Ratcliffe/Blooml

costing me,' Sarao said to tell programmer

etails seen bolstering U.S. extradition case

day trader accused of contributing to the 2010 flash crash e to help him work out a system to manipulate stock prices is “spoofing” efforts, U.S. prosecutors said in an indictmen

“I need to know whether you can do what I need, because at the mome spoofs all the time and it’s costing me a lot of money,” Navinder Singh 2009 e-mail to a programmer he’d tapped to build trading software, ac

UBS, Deutsche Bank and HSBC to pay millions in spoofing settlement, CFTC says

- Deutsche Bank will pay $30 million, UBS $15 million and HSBC $1.6 million to settle civil charges that some of their traders engaged in spoofing in the precious metals market.
- The CFTC charged six individuals, and the Department of Justice charged eight with crimes related to deceptive trading in a wide-ranging investigation.

Published 2:29 PM ET Mon, 29 Jan 2018 | Updated 8:32 AM ET Wed, 31 Jan 2018

CNBC

Luke MacGregor | Reuters

US seals first prosecution against stock market trader for 'spoofing'

A jury convicts Michael Coscia on six charges of commodities fraud and six charges of spoofing, all of the charges he faced

Email

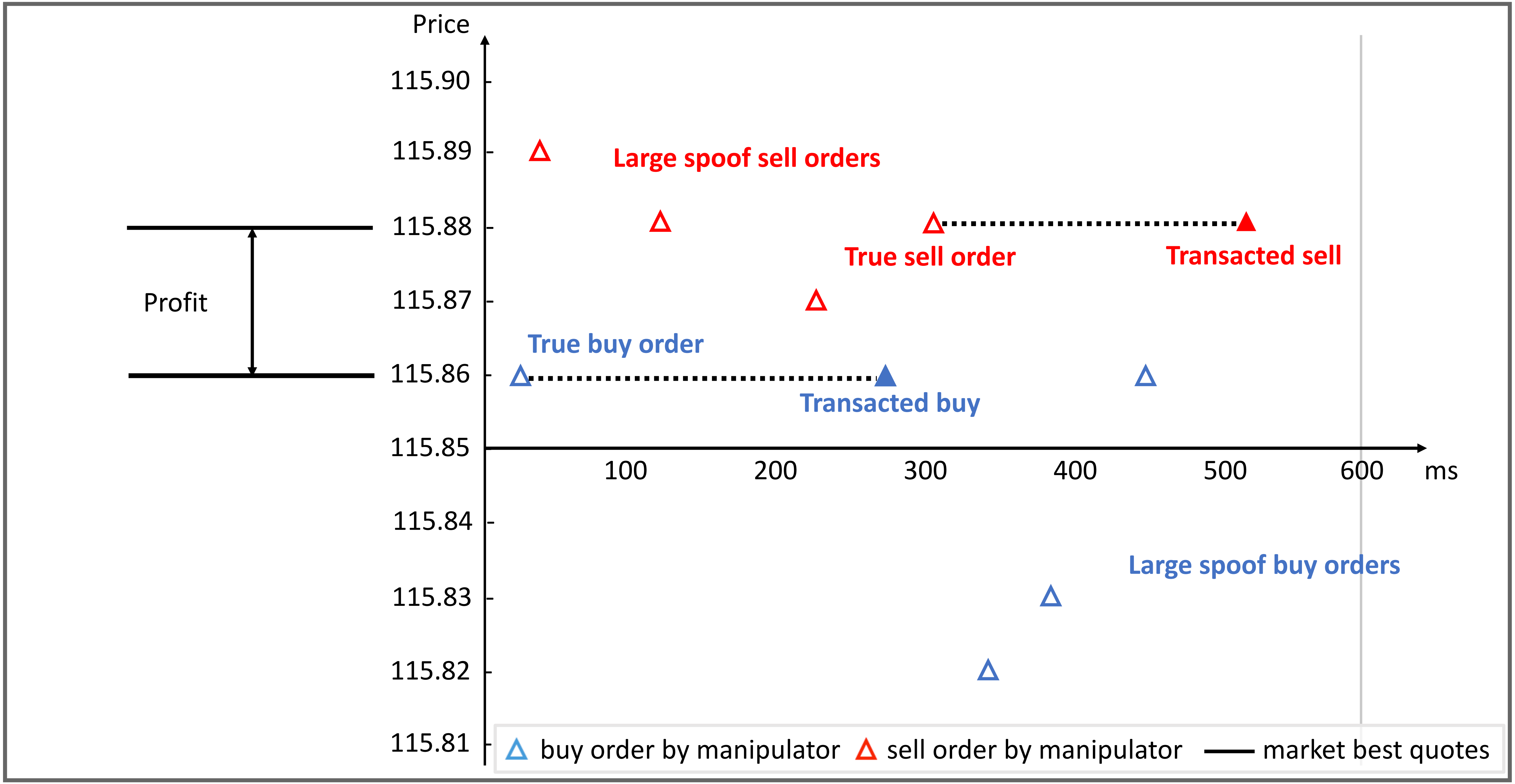
Prosecutors said Michael Coscia wanted to lure other traders to markets by creating an illusion of demand so that he could make money on smaller trades Photo: AP

By Reuters

11:48PM GMT 03 Nov 2015

A US jury has found high-frequency trader Michael Coscia guilty of commodities fraud and "spoofing" in the US government's first criminal

Spoofing is the practice of submitting large **spurious** buy or sell orders with the intent to cancel them before execution to mislead other traders.



Source: Financial Conduct Authority, Animated Example of Mr. Coscia's Trading

Key Elements in Spoofing

- The intent to falsely signal supply and demand with spoof orders
- The effect of misleading other traders about the market condition
- The connection to adversarial attacks on machine learning algorithms
    - ❑ Inference-level attack on deployed trading algorithm
    - ❑ Poisoning attack on future algorithm training

To what extent are the other traders misled by the spoof orders?

What would happen if the spoof orders are not placed?

This Talk

Towards Manipulation-Resistant Markets

❑ *A computational agent-based model*

Strategic dynamics between a manipulator and market participants.

❑ *Design of deterrent mechanisms and trading strategies (briefly)*

Mitigating manipulation effects.

❑ *An adversarial learning framework*

Strategic dynamics between a manipulator and a regulator.

This Talk

Towards Manipulation-Resistant Markets

❑ *A computational agent-based model*

Strategic dynamics between a manipulator and market participants.

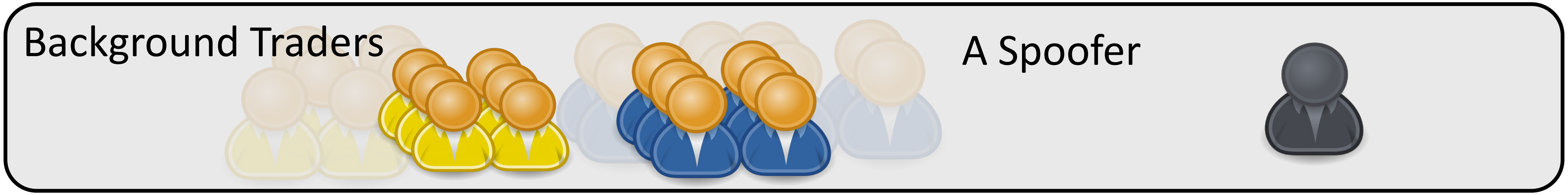
❑ *Design of deterrent mechanisms and trading strategies (briefly)*

Mitigating manipulation effects.

❑ *An adversarial learning framework*

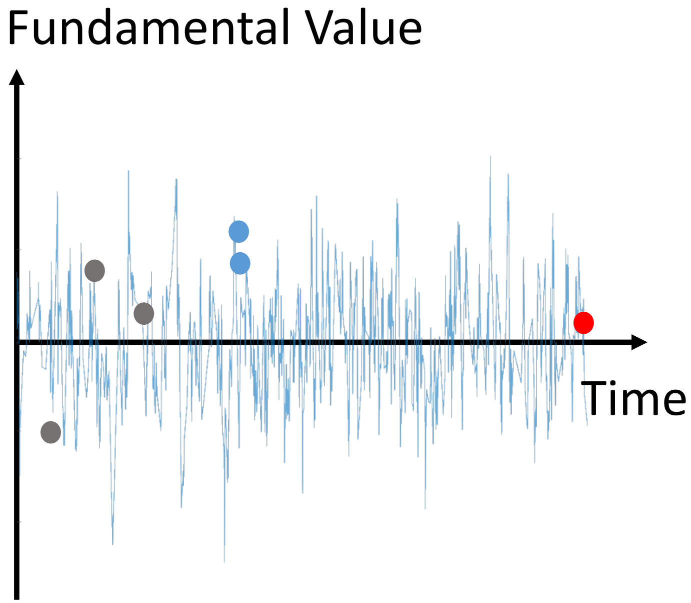
Strategic dynamics between a manipulator and a regulator.

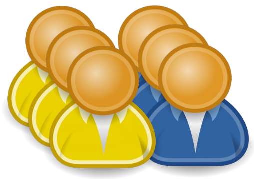
Agent-Based Modeling & Empirical Game-Theoretic Analysis



- Agent-Based Modeling (ABM)
  - Simulate financial market as a complex multi-agent system;
  - Lay out strategic choices faced by trading agents;
  - ✓ Reproduce manipulation effect through agent interactions.
- Empirical Game-Theoretic Analysis (EGTA)
  - Induce a normal-form game and identify Nash equilibria;
  - ✓ Characterize agent interactions and market performance in equilibrium.

A Market Model of Spoofing

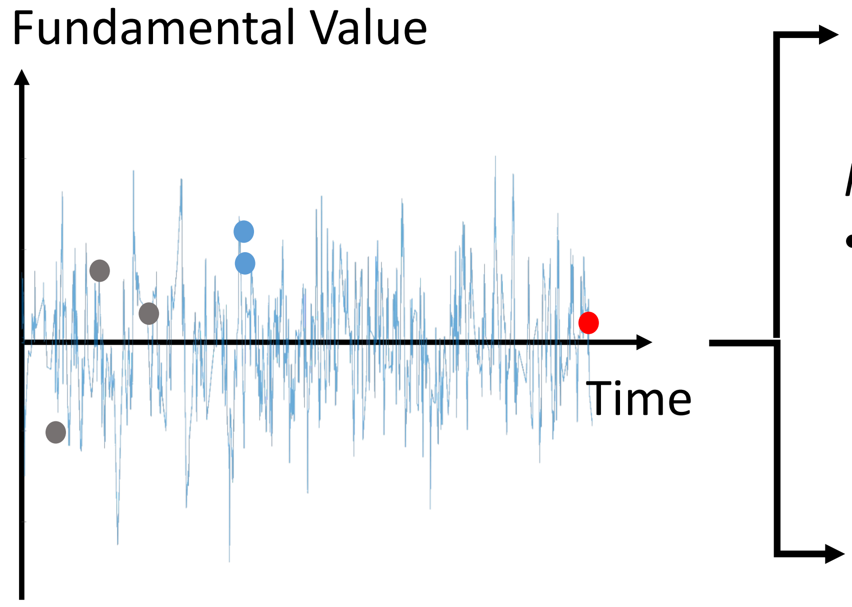


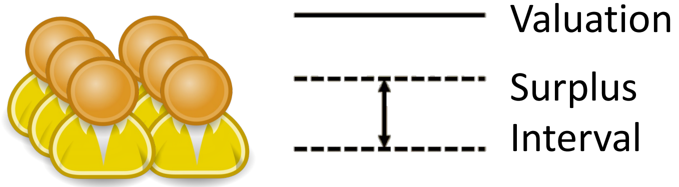


Background Traders

- Continuous Double Auction (CDA)
- Market Environments
  - Fundamental Shocks;
  - Observation Noise;
  - {LS, MS, HS} × {LN, MN, HN};

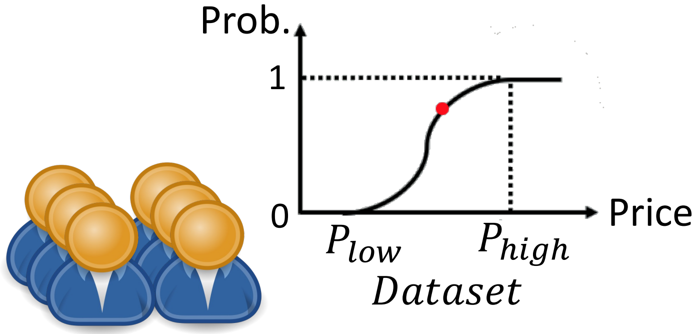
A Market Model of Spoofing





Non-Learning Agents [Gode & Sunder 1993, Wah & Wellman 2015]

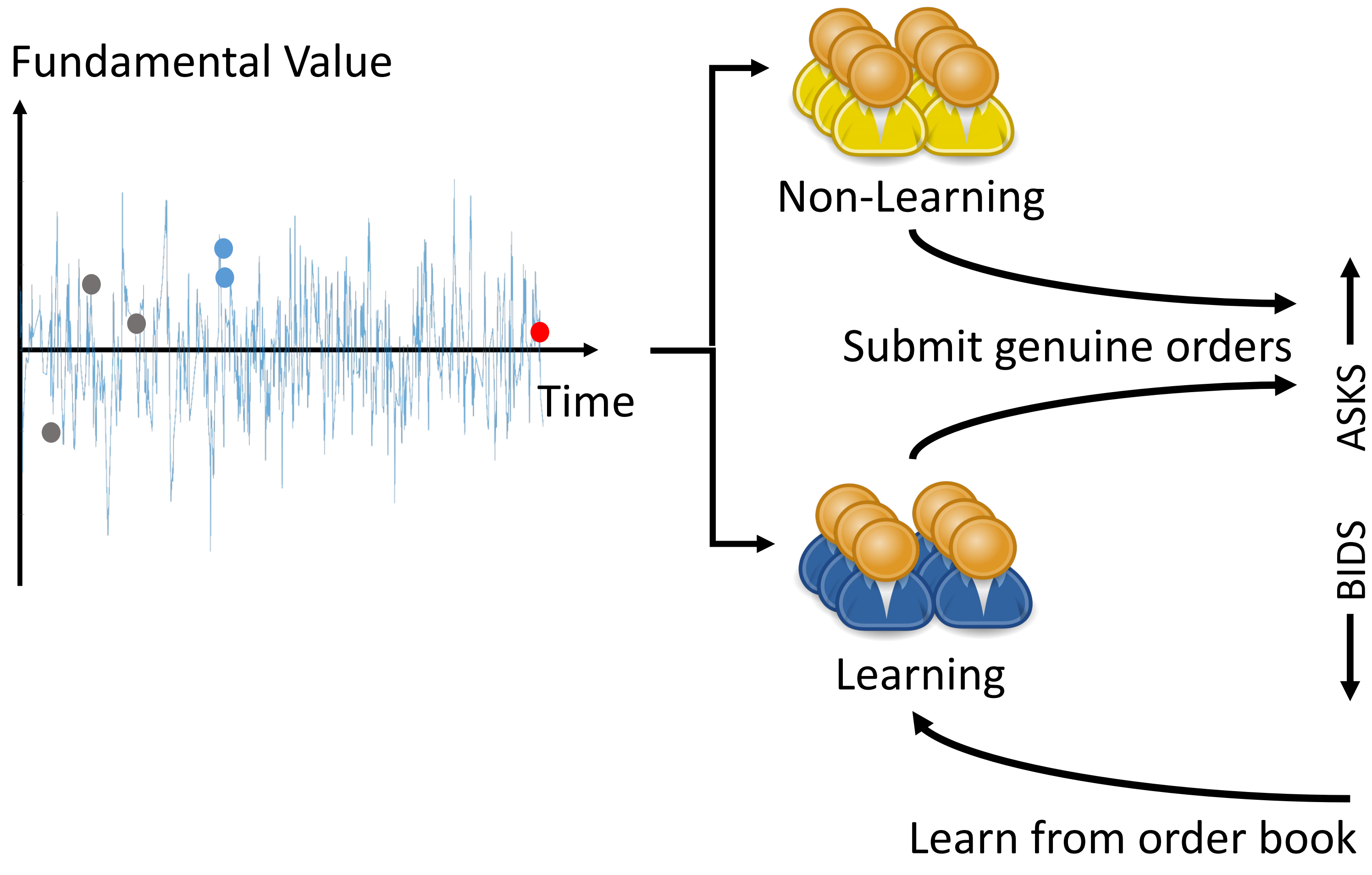
- Choose a price based on its valuation and a requested surplus.



Learning Agents [Gjerstad & Dickhaut 1998, Wang & Wellman 2017]

- Learn from the limit order book in its memory to approximate the probability of an order being transacted;
- Choose a price to maximize expected surplus.

A Market Model of Spoofing



Non-Learning

Submit genuine orders

Learning

Learn from order book

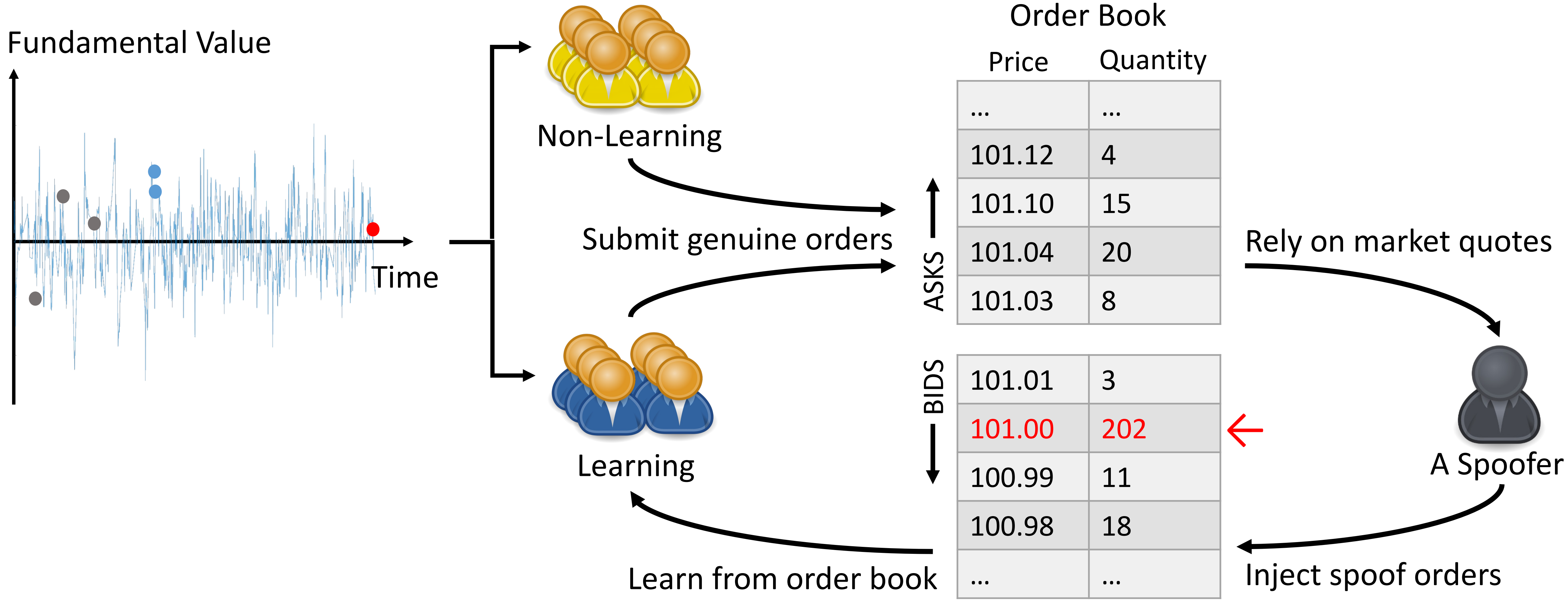
ASKS

BIDS

Order Book

Price	Quantity
…	…
101.12	4
101.10	15
101.04	20
101.03	8
101.01	3
101.00	2
100.99	11
100.98	18
…	…

A Market Model of Spoofing



Fundamental Value

Time

Non-Learning

Learning

Submit genuine orders

Learn from order book

Order Book

	Price	Quantity
ASKS	…	…
	101.12	4
	101.10	15
	101.04	20
	101.03	8
BIDS	101.01	3
	101.00	202
	100.99	11
	100.98	18
	…	…

Rely on market quotes

A Spoofer

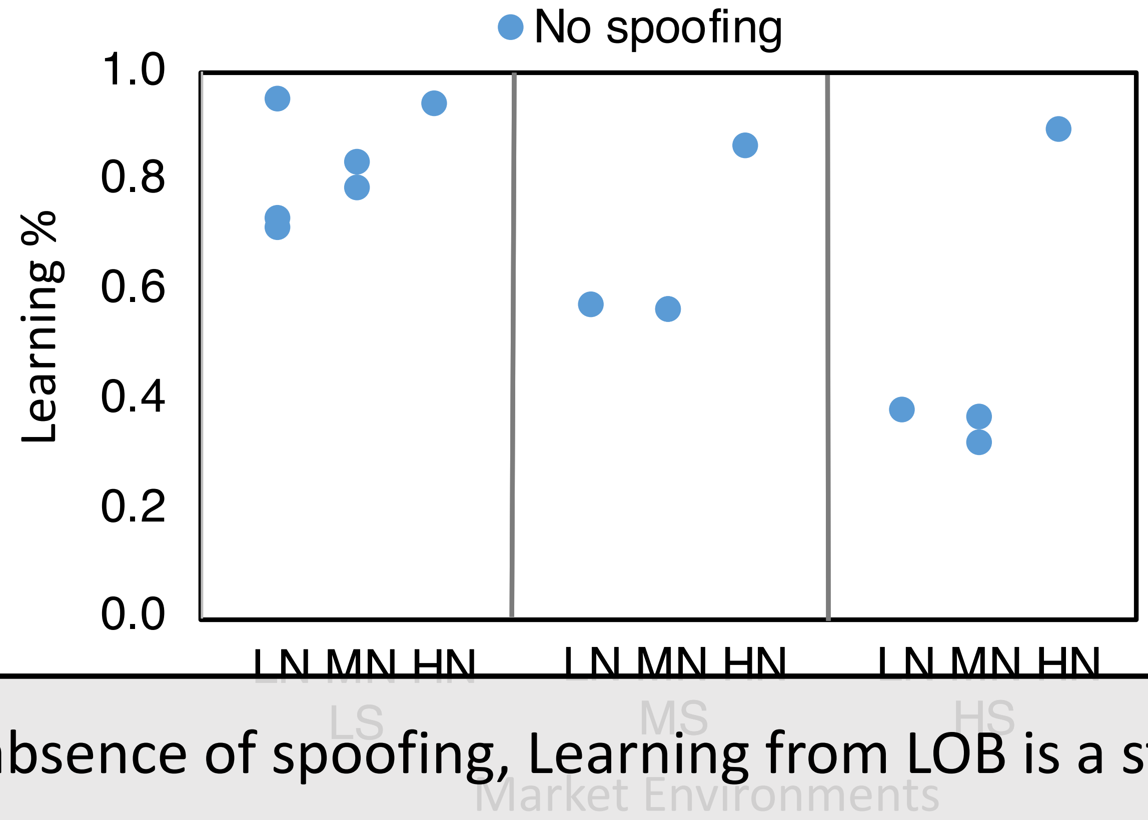
Inject spoof orders

What is the effect of spoofing on agent behavior and market performance?

A Game-Theoretic Analysis

Stage 1: Is Learning from LOB Competitive?

In the absence of spoofing, how will agents choose between Learning and Non-Learning?



In the absence of spoofing, Learning from LOB is a strategic choice.

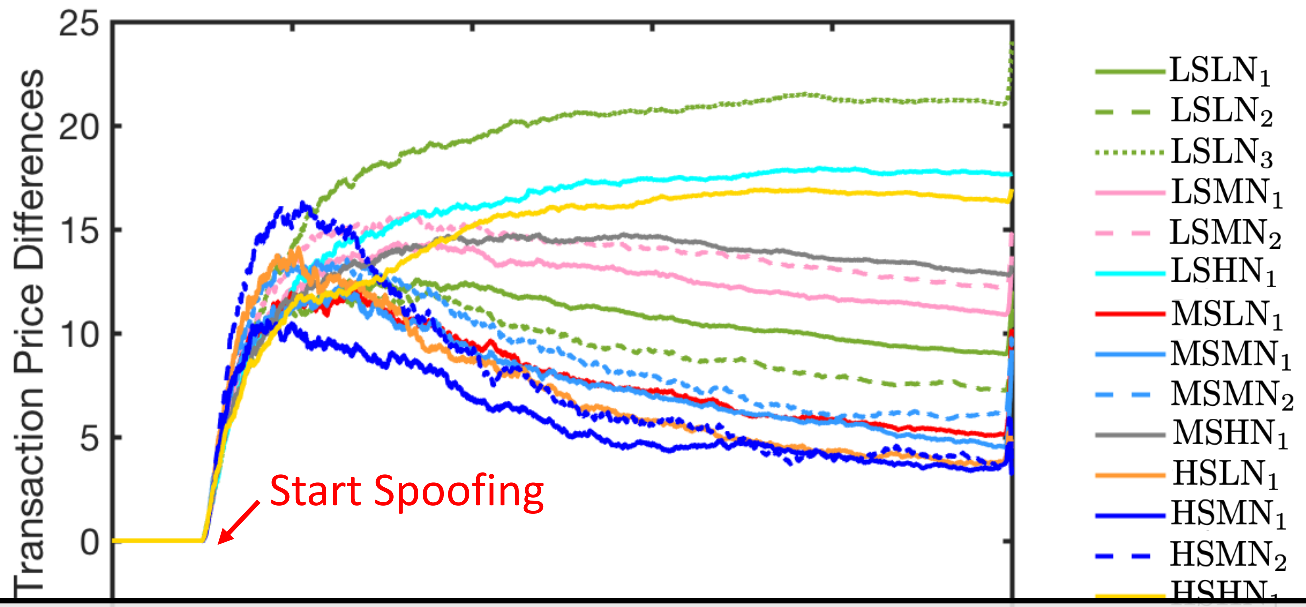
Stage 1: Is Learning from LOB Competitive?

In the absence of spoofing, how will agents choose between Learning and Non-Learning?

Learning from LOB improves market efficiency and price discovery.

Stage 2: Is Spoofing Effective?

- Price Deviation: prices in market with spoofing – prices in market without spoofing



Start Spoofing

Markets with learning traders are vulnerable to spoofing.
Spoofing causes learning surplus ↓ & non-learning surplus ↑.
Learning tends to amplify spoofing effects.

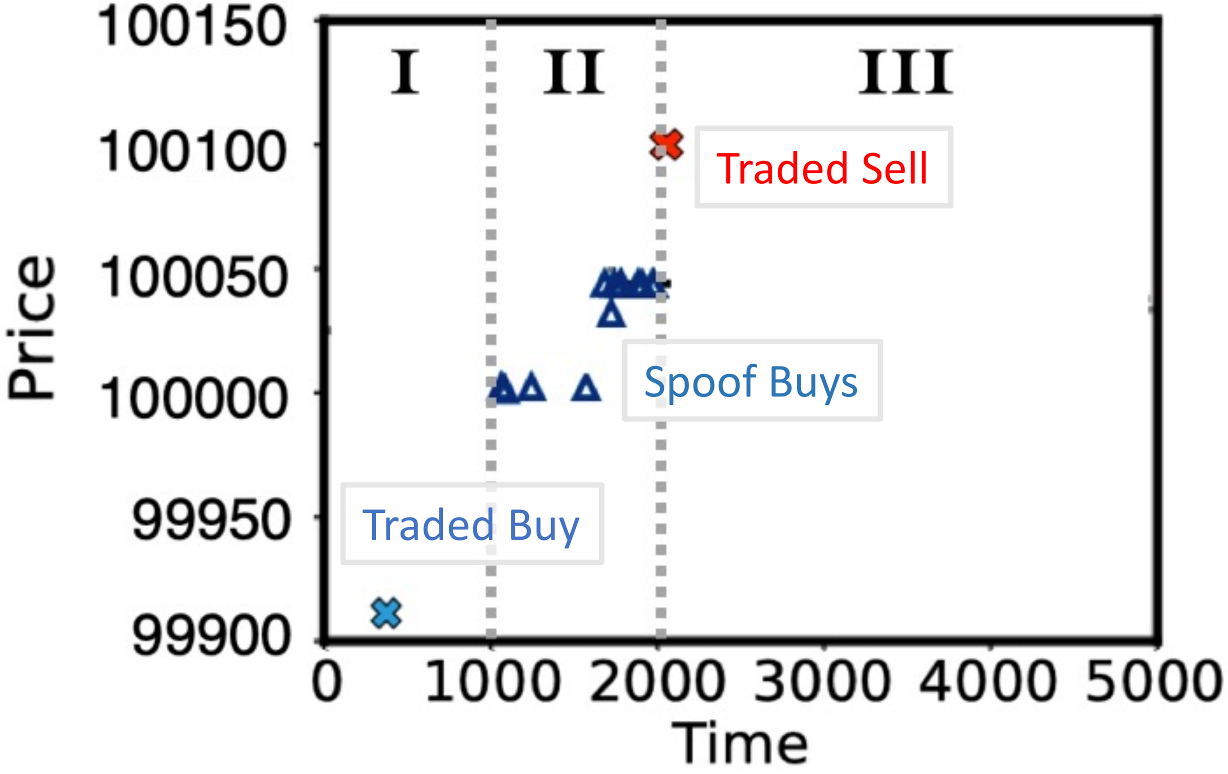
Stage 2: Is Spoofing Effective?

- Profitable Spoofing

I: Buy at prices lower than a threshold

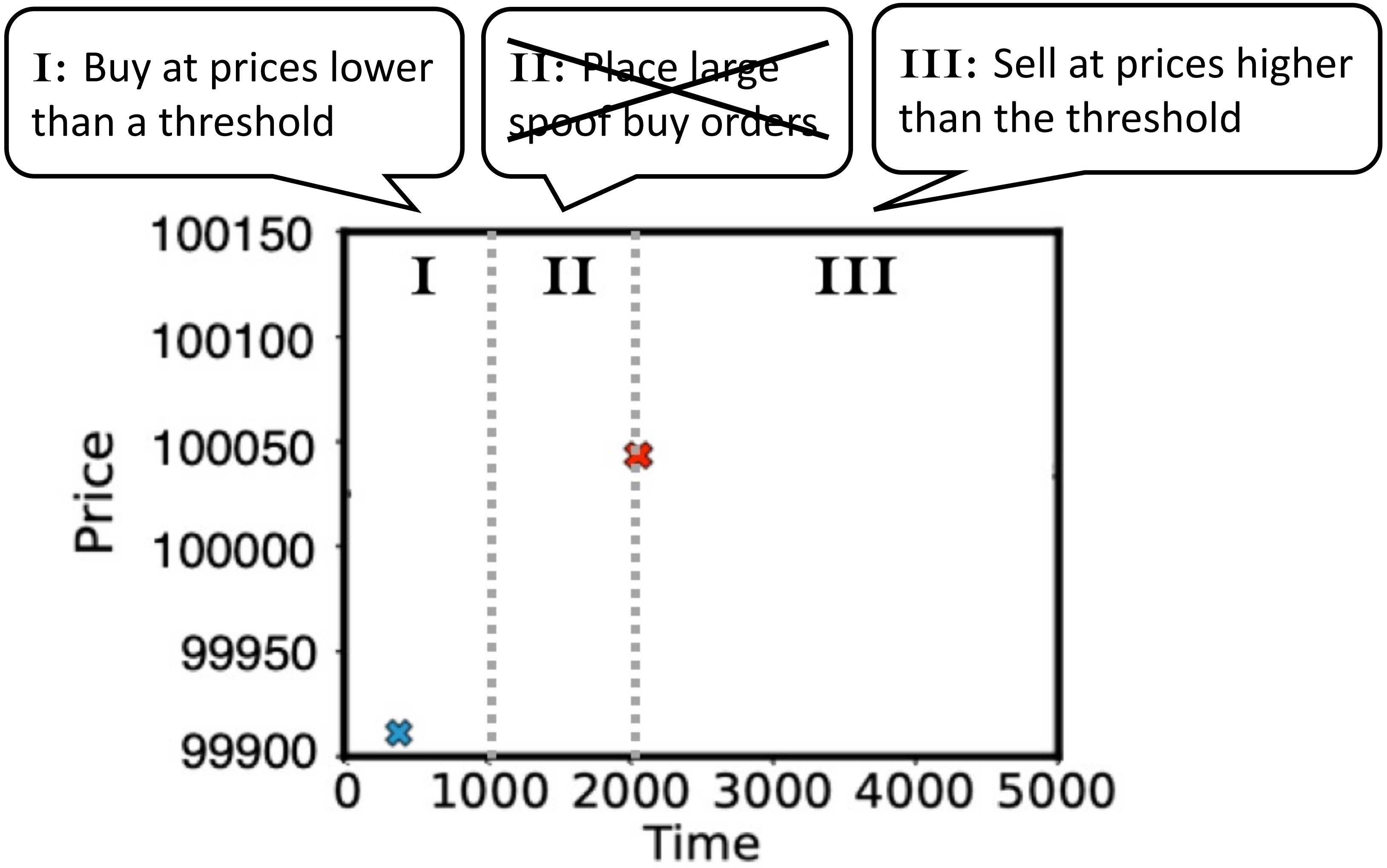
II: Place large spoof buy orders

III: Sell at prices higher than the threshold



Stage 2: Is Spoofing Effective?

- Exploitation



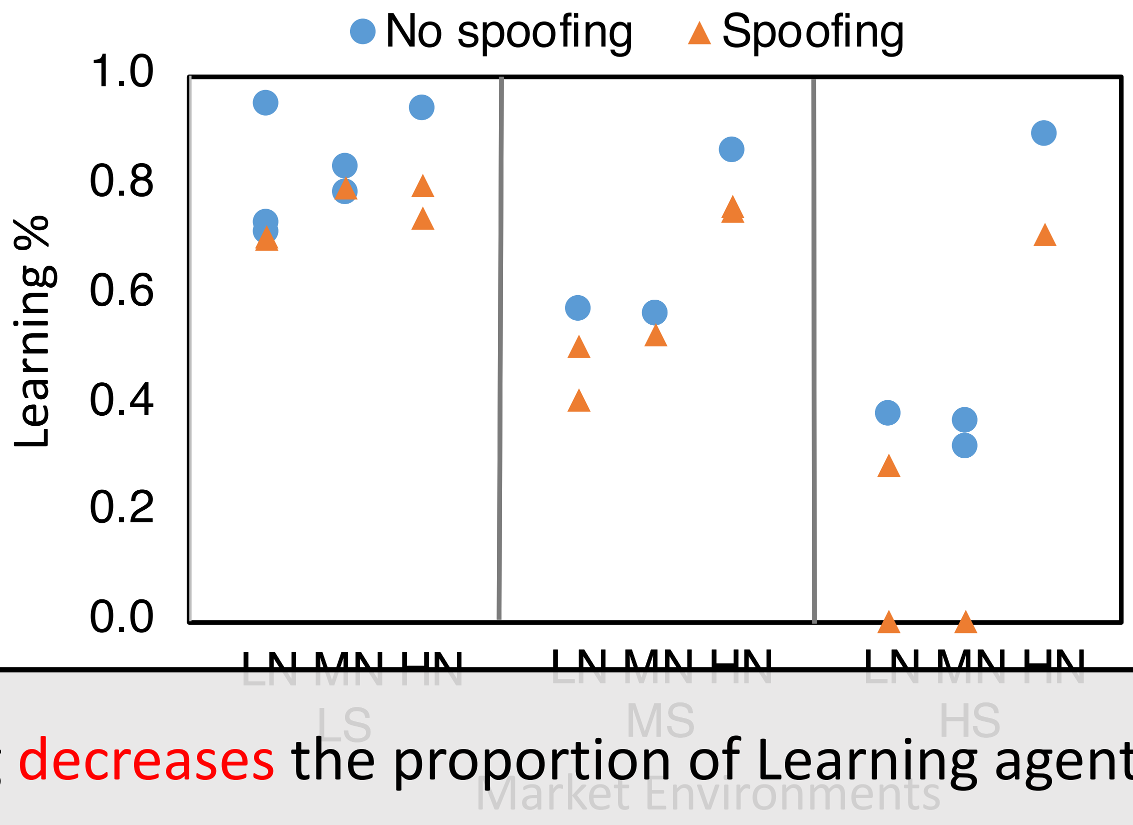
I: Buy at prices lower than a threshold

~~**II:** Place large spoof buy orders~~

III: Sell at prices higher than the threshold

Stage 3: What is the Effect of Spoofing?

In the presence of spoofing, how will agents adapt by re-equilibrating?



Spoofing decreases the proportion of Learning agents in equilibrium.

Stage 3: What is the Effect of Spoofing?

In the presence of spoofing, how will agents adapt by re-equilibrating?

Spoofing harms market efficiency and price discovery.

Spoofing the Limit Order Book:
A Strategic Agent-Based Analysis

Modeling strategic dynamics between a manipulator and market participants

- Reproduce spoofing in a dynamic limit-order market mechanism.
- Demonstrate the effectiveness of spoofing against approximate-equilibrium traders.

  Spoofing distorts prices, decreases learning proportion, and hurts market surplus.
- Provide a model to quantify the effect of manipulation practices and evaluate any deterrent proposal under strategic settings.

This Talk

Towards Manipulation-Resistant Markets

❑ *A computational agent-based model*

Strategic dynamics between a manipulator and market participants.

❑ *Design of deterrent mechanisms and trading strategies (briefly)*

Mitigating manipulation effects.

❑ *An adversarial learning framework*

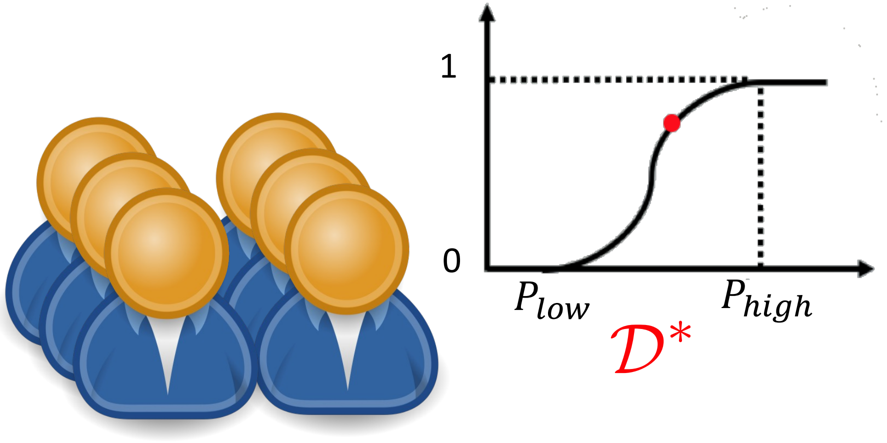
Strategic dynamics between a manipulator and a regulator.

Two Variations of CDA Mechanisms

- "Cloaking" Mechanisms: strategically cloak price levels and disclose part of the order book
  - Mitigate manipulation effect
  - Introduce transaction risk to the manipulator
  - X. Wang, Y. Vorobeychik, M. P. Wellman. *A Cloaking Mechanism to Mitigate Market Manipulation*. IJCAI 2018.
- Frequent Call Markets
  - Reduce manipulation frequency and impact
  - B. Liu, M. Polukarov, C. Ventre, L. Li, L. Kanthan, F. Wu, and M. Basios. *The Spoofing Resistance of Frequent Call Markets*. AAMAS 2022.

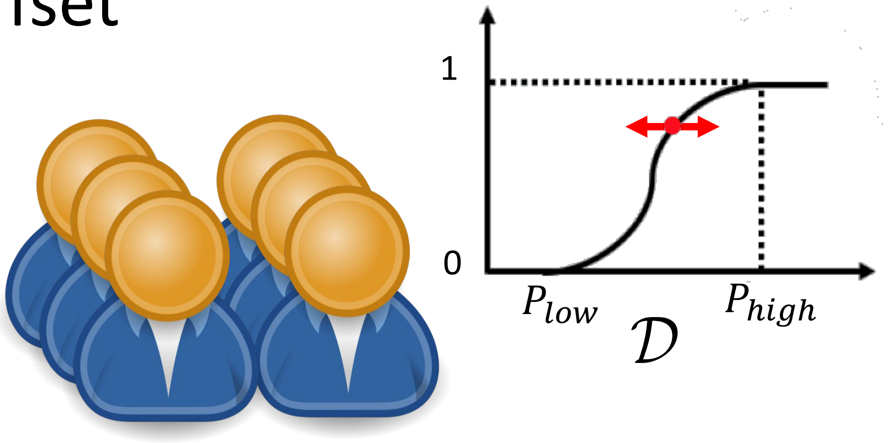
Two Variations of Learning-Based Strategies

- Learning with order blocking



Improve robustness against spoofing and remain competitive in non-manipulated markets.

- Learning with stochastic price offset



Improve general performance over the baseline learning strategy; combine with the first proposal to gain robustness.

This Talk

Towards Manipulation-Resistant Markets

❑ *A computational agent-based model*

Strategic dynamics between a manipulator and market participants.

❑ *Design of deterrent mechanisms and trading strategies (briefly)*

Mitigating manipulation effects.

❑ *An adversarial learning framework*

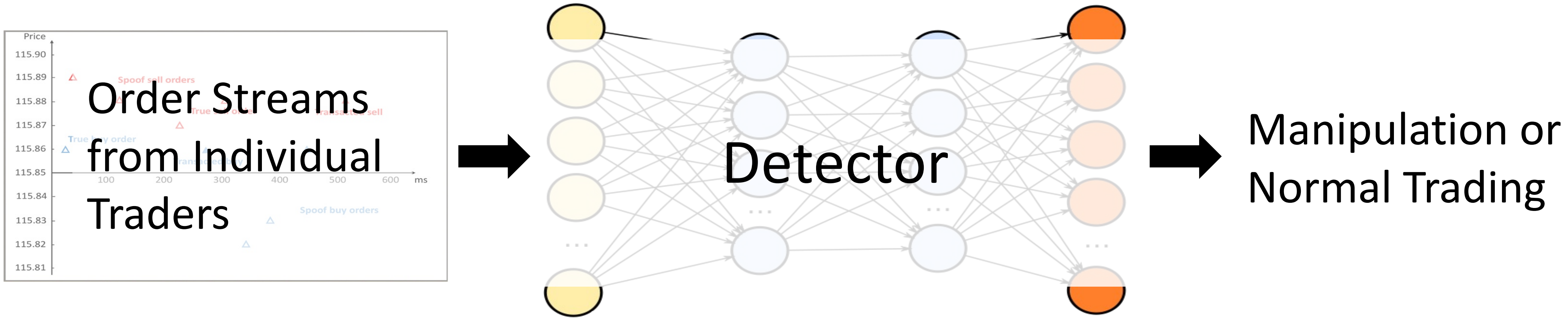
Strategic dynamics between a manipulator and a regulator.

Detect Market Manipulation

- The ideal case: adopt supervised learning approaches

  - Use order streams associated with a verified manipulator and normal traders;

  - Represent an order stream as a variable-length sequence of bidding actions (e.g., submit/cancel, buy/sell, price, and quantity)



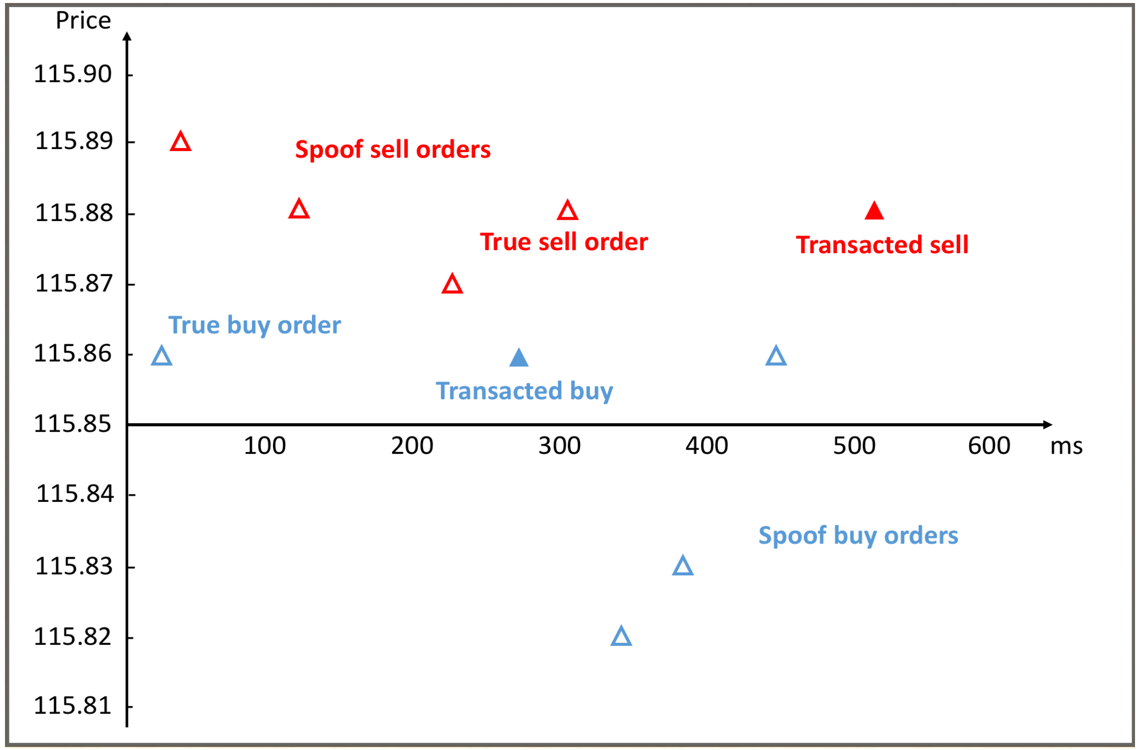
Order Streams from Individual Traders

Detector

Manipulation or Normal Trading

Detect Market Manipulation: The Data Challenge

- Insufficient real-market labeled order streams to serve as training data

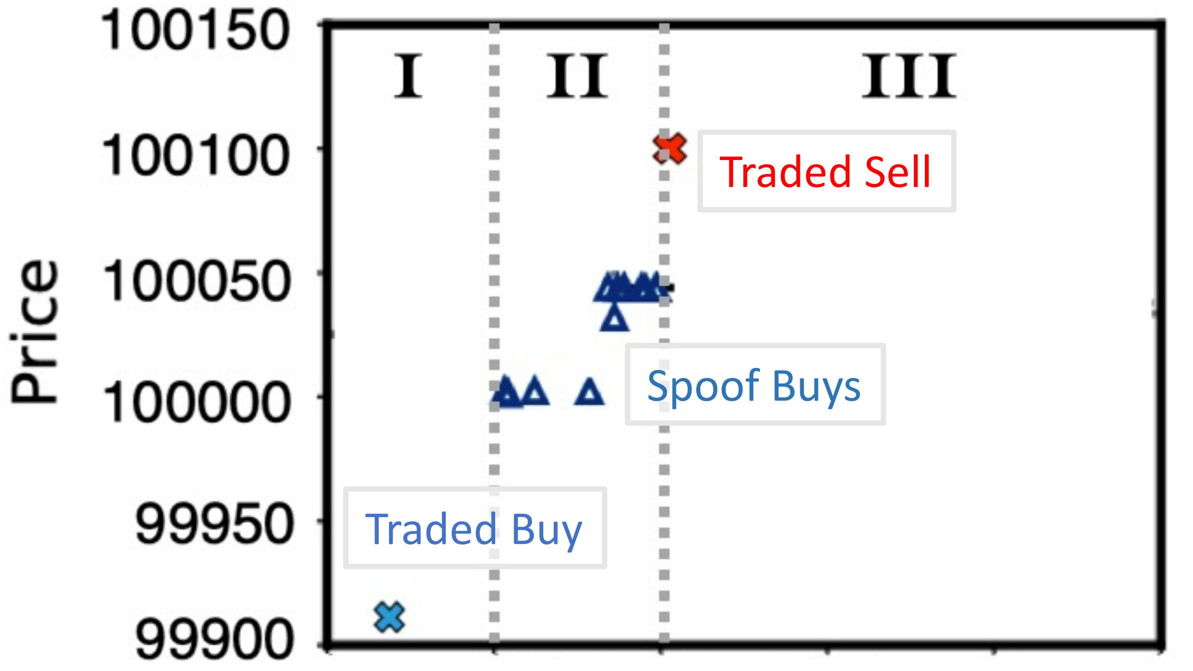


Data: An order stream over a trading period

Label: A manipulator

Detect Market Manipulation: The Data Challenge

- An agent-based market model of spoofing



Data: An order stream over a trading period
Label: A manipulator

Detect Market Manipulation: Challenges

Issue 1: The codified manipulation strategies may not be diverse enough.

Issue 2: The manipulator may adversarially obfuscate actions to evade detection, given a developed classifier.

Detect Market Manipulation

- An adversarial learning framework

Issue 1: The codified manipulation strategies may not be diverse enough.

- ➢ Generate new manipulation patterns through adapting codified spoofing strategies.

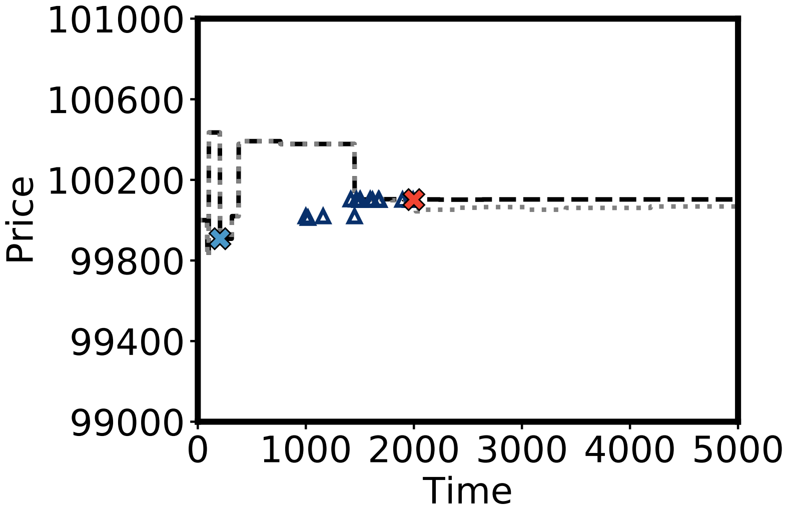
Issue 2: The manipulator may adversarially obfuscate actions to evade detection, given a developed classifier.

- ➢ Reason about how an adversary might mask its behavior to evade detection.

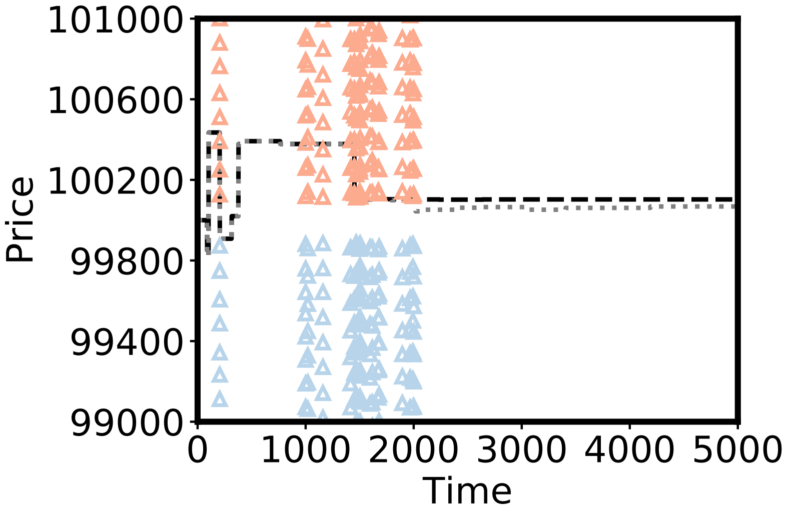
An Adversarial Learning Framework to Evade Detection

- A case study: modify spoofing to resemble market making.

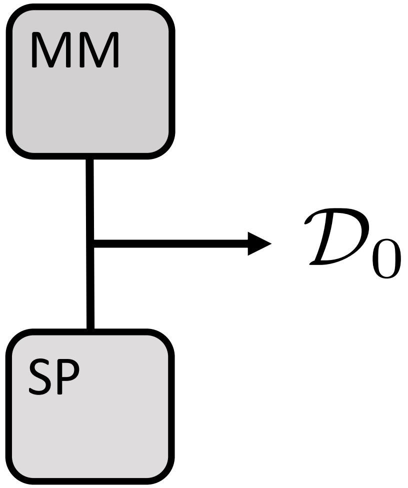
  - A market-making agent (MM) simultaneously submits buy and sell orders to facilitate trading with other investors.



A Manipulation Order Stream (SP)

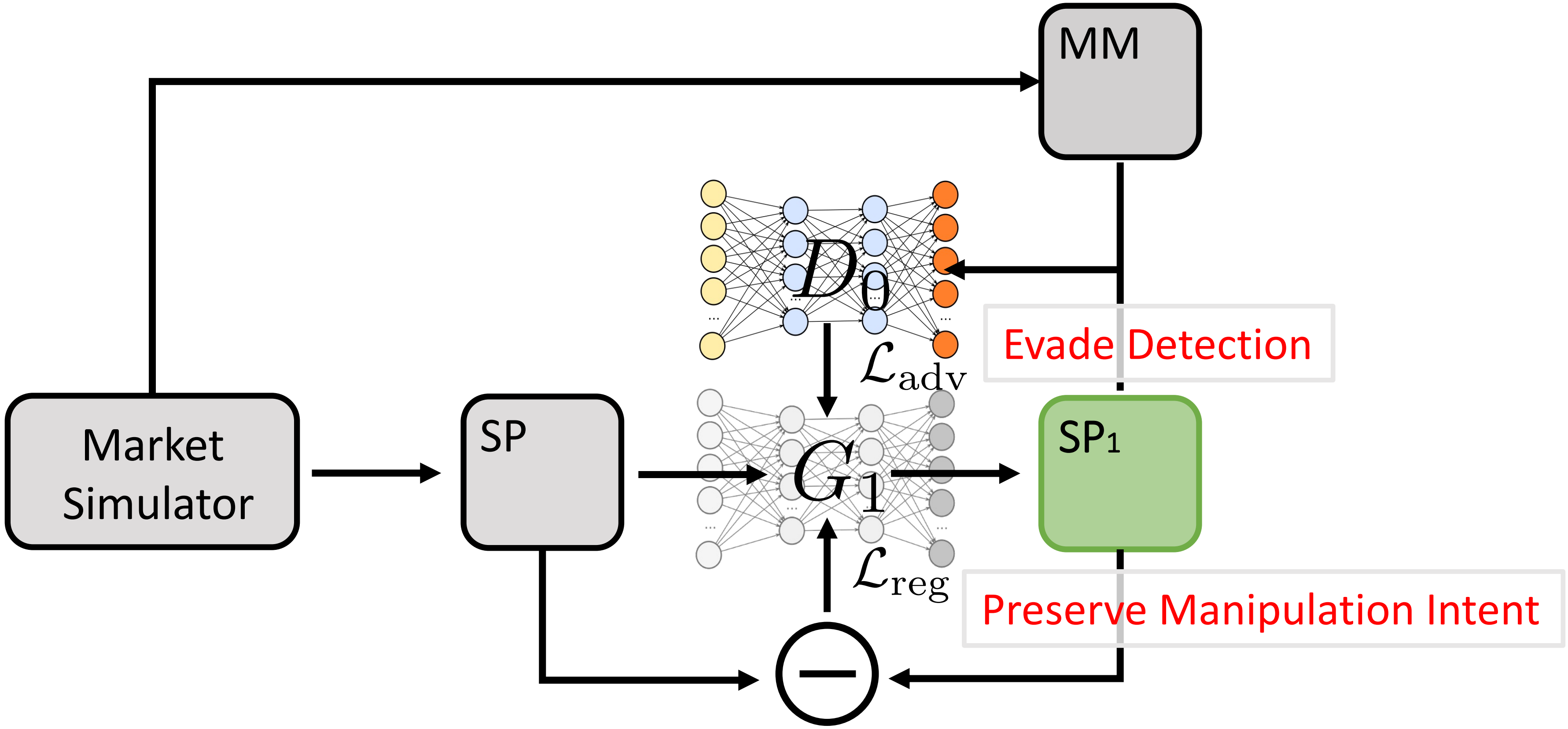


A Market-Making Order Stream (MM)



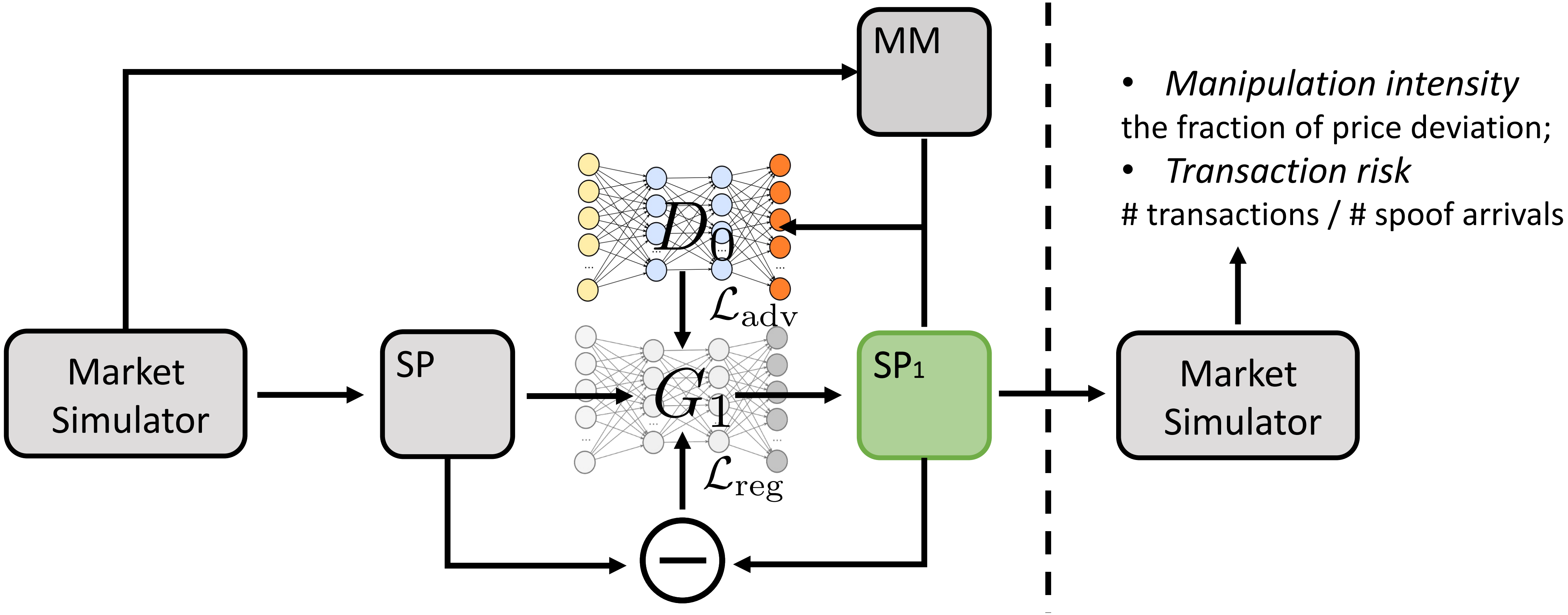
An Adversarial Learning Framework to Evade Detection

- Adapt SP to evade detection while preserving manipulation effects


MM
D_0
$\mathcal{L}_{\text{adv}}$
Evade Detection
Market Simulator
SP
G_1
SP1
$\mathcal{L}_{\text{reg}}$
Preserve Manipulation Intent

An Adversarial Learning Framework to Evade Detection

- Adapt SP to evade detection while preserving manipulation effects



- *Manipulation intensity*

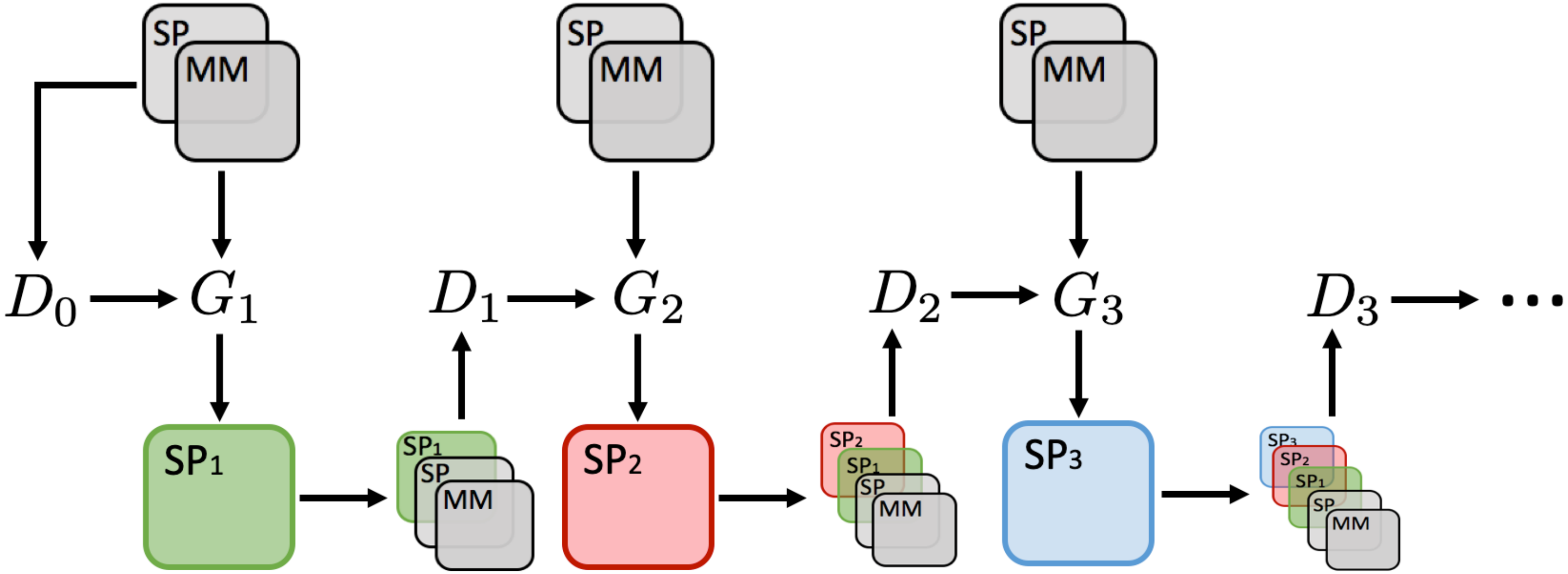
the fraction of price deviation;

- *Transaction risk*

transactions / # spoof arrivals

An Adversarial Learning Framework to Evade Detection

- A recursive training procedure

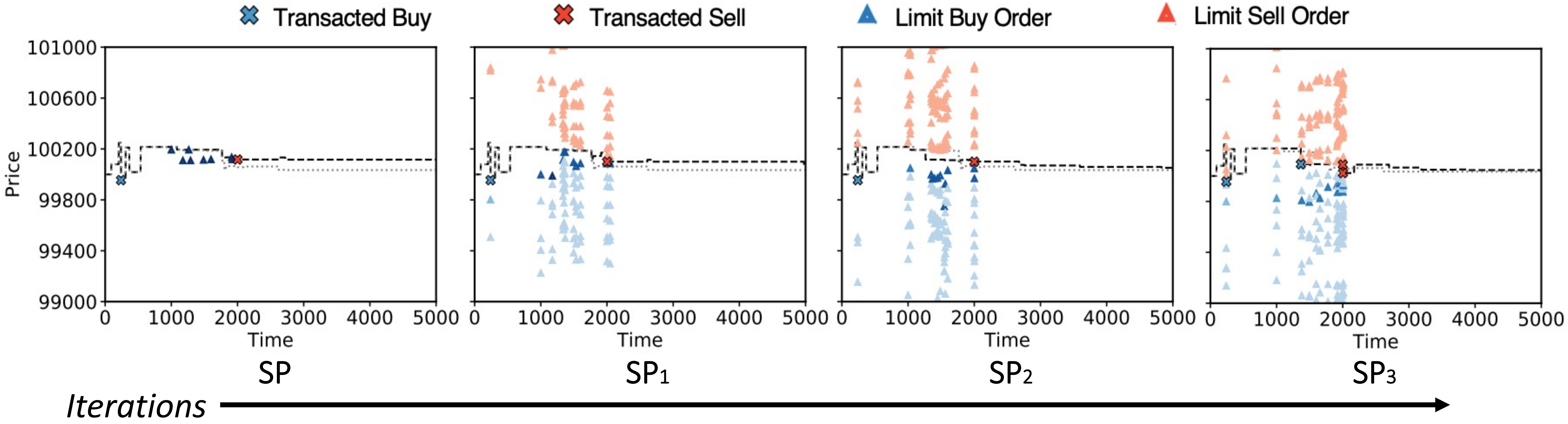


Empirical Evaluation

- Similarity to market making;

- Preservation of manipulation effects.

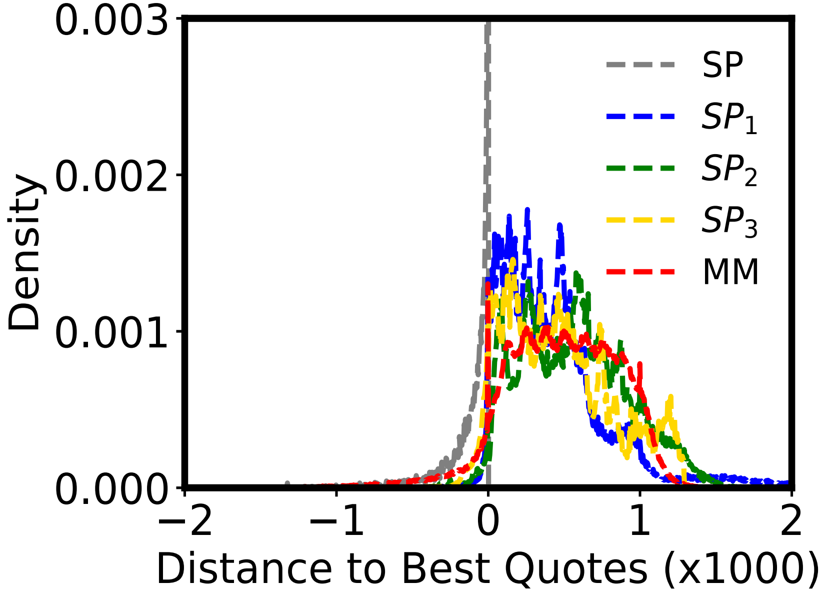
Similarity to Market Making

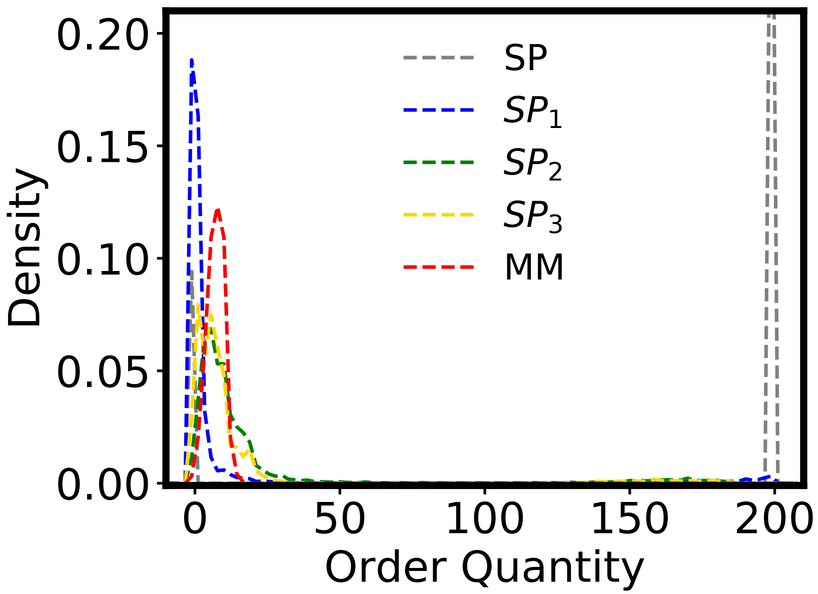


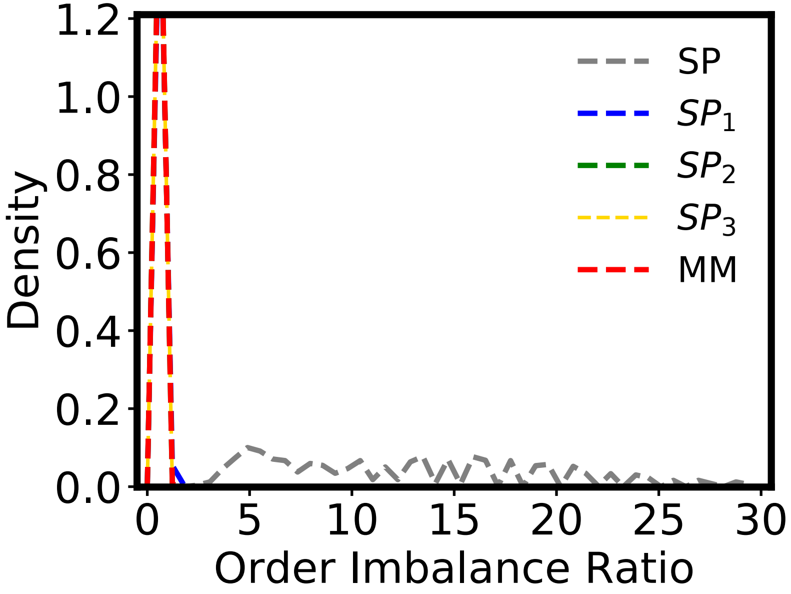
Quote simultaneously on both sides of the market;

Place large orders behind smaller ones.

Similarity to Market Making



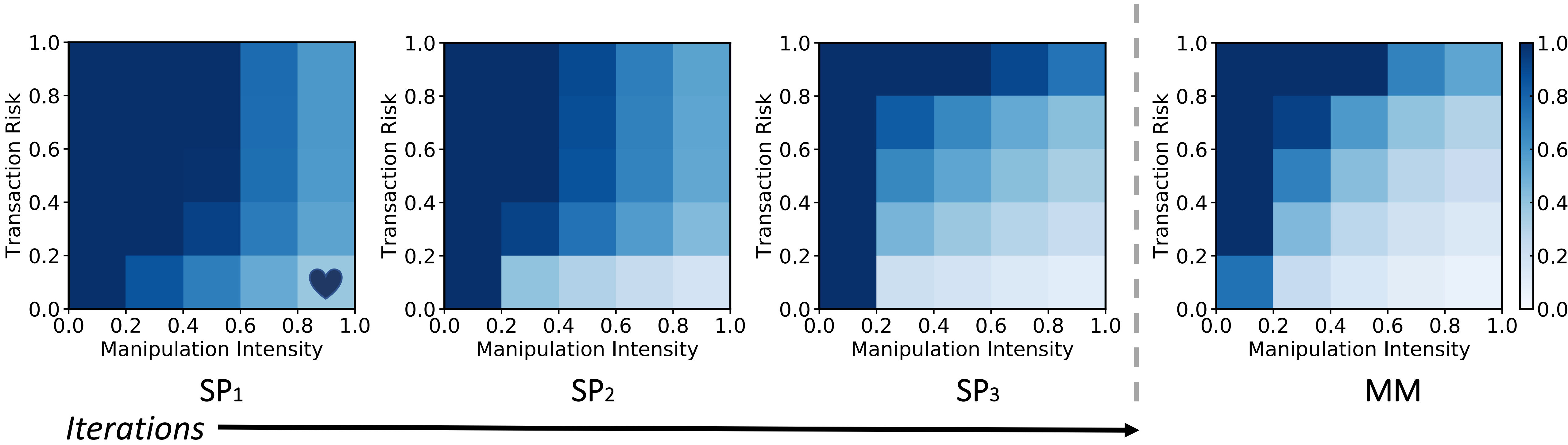




Orders cover a wider range of prices with small quantities;

Buy and sell orders are maintained balanced.

Preservation of Manipulation Effects

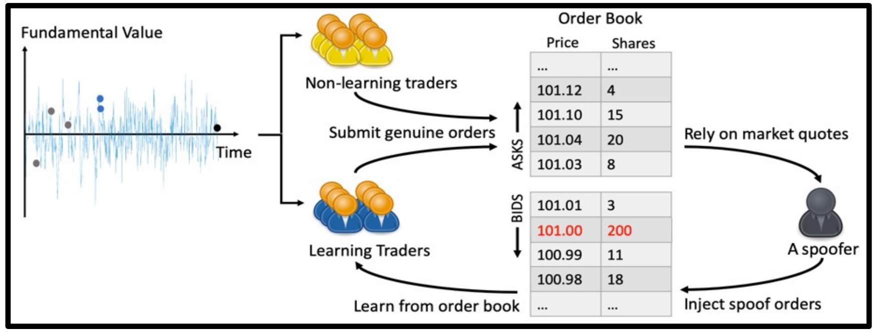


SP$_1$ SP$_2$ SP$_3$ MM

The adaptation comes at the cost of a reduced manipulation intensity and a higher transaction risk.

Modeling the Evasion of Manipulation Detection: An Adversarial Learning Framework

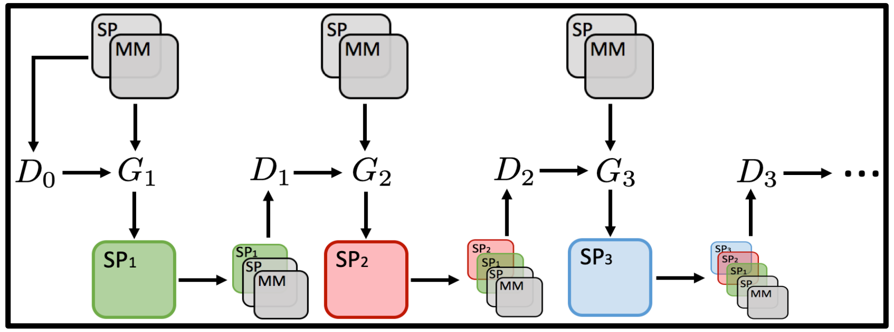
Modeling strategic dynamics between a manipulator and a regulator



Price	Shares
...	...
101.12	4
101.10	15
101.04	20
101.03	8
101.01	3
101.00	200
100.99	11
100.98	18
...	...

Verify Manipulation Effects

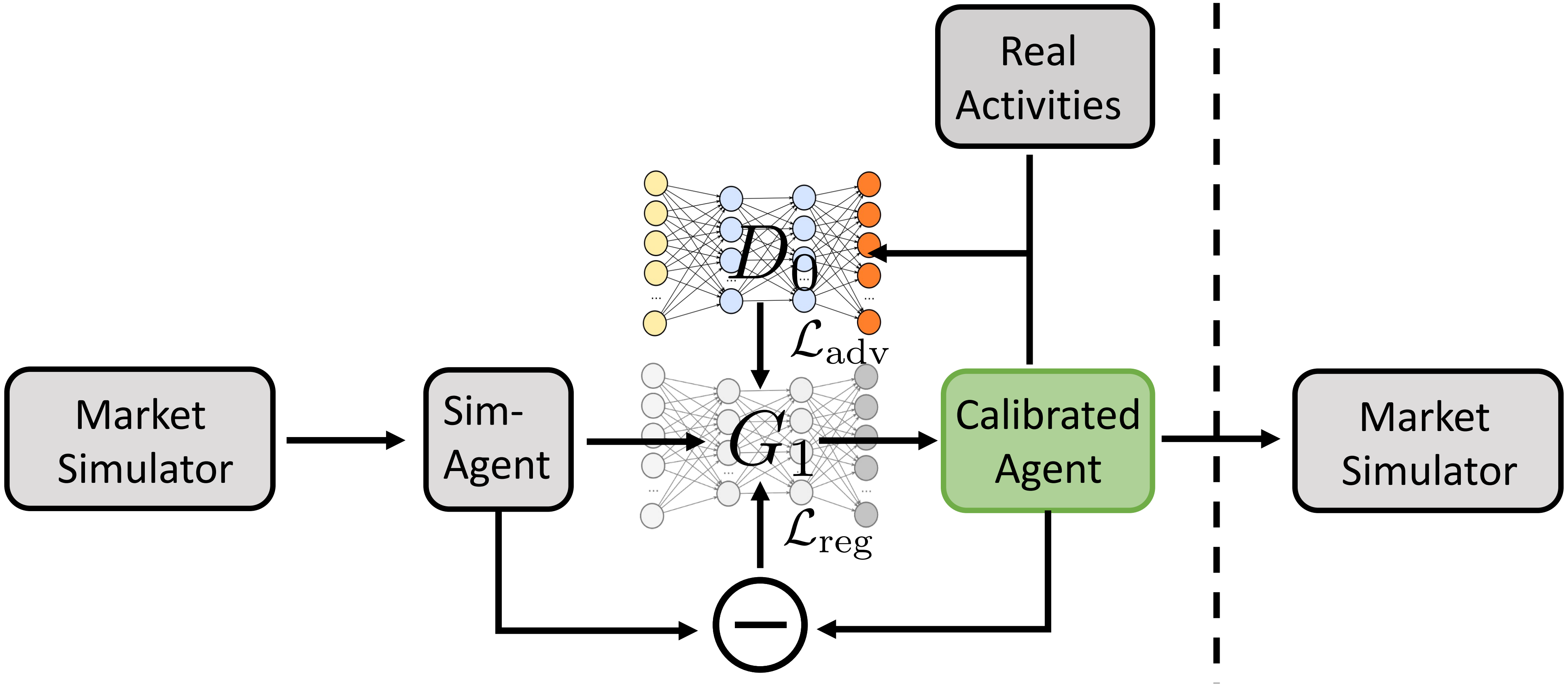
Generate New Manipulative Patterns



Discussions

Integrating model-driven and data-driven approaches

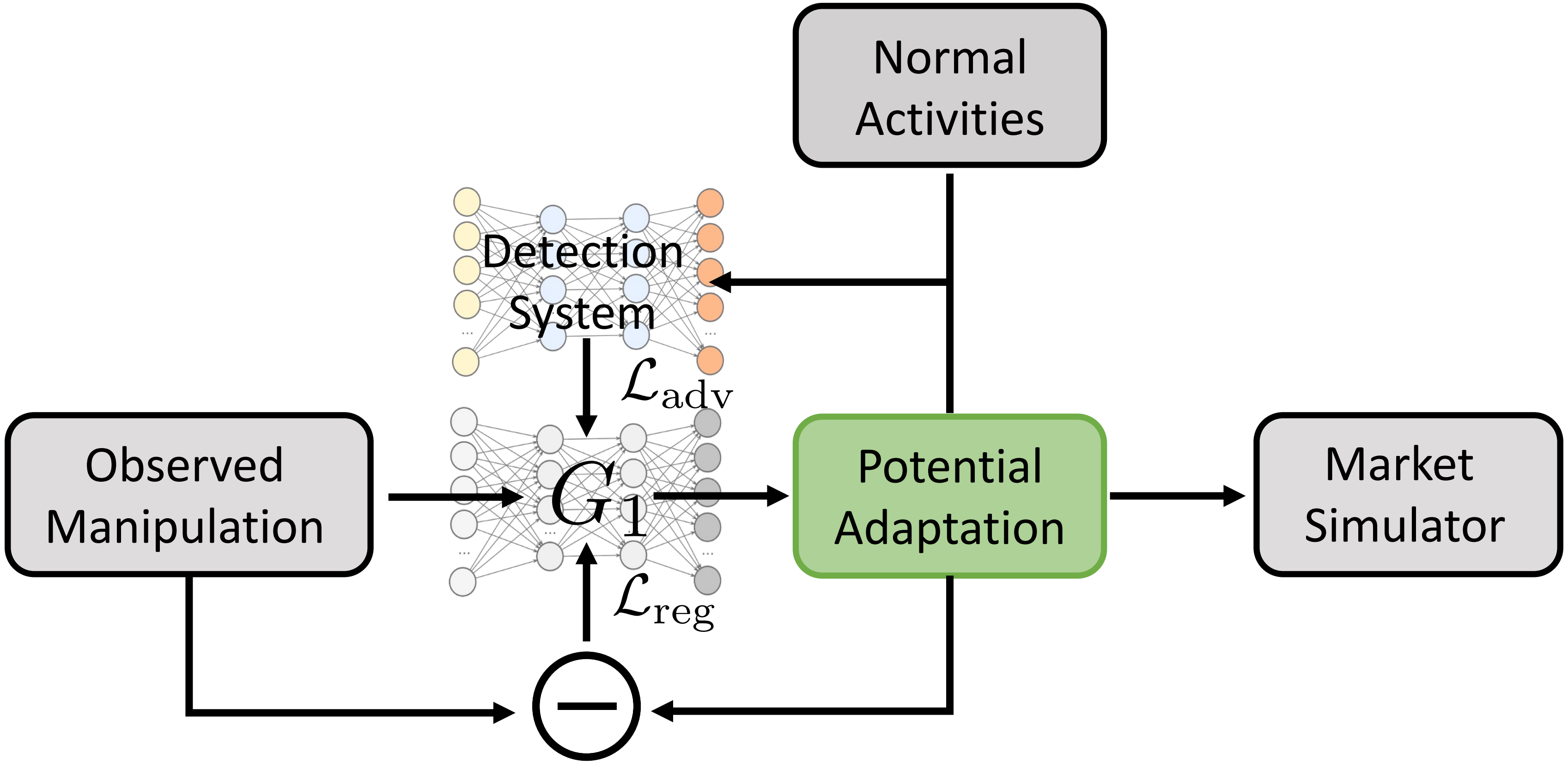
#1 Calibrate model and simulated data using real data



Discussions

Integrating model-driven and data-driven approaches

#2 Proactively reason about adversarial evasion


Normal Activities
Detection System
$\mathcal{L}_{\text{adv}}$
Observed Manipulation
G_1
Potential Adaptation
Market Simulator
$\mathcal{L}_{\text{reg}}$
−