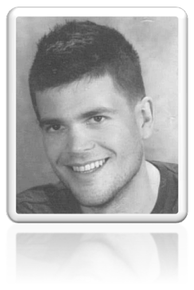
MEDNARODNA PODIPLOMSKA ŠOLA JOŽEFA STEFANA

JOŽEF STEFAN INTERNATIONAL POSTGRADUATE SCHOOL

# Identifying Suspicious Behavior from Multiple Events




**BOŠTJAN KALUŽA**

Department of Intelligent Systems, Jožef Stefan Institute, Jamova cesta 39, 1000 Ljubljana

Jožef Stefan International Postgraduate School, study program New Media and E-Science

Advisors:

**Prof. Milind Tambe**, Teamcore Research Group, University of Southern California, Los Angeles, California

**Prof. Gal Kaminka**, Bar Ilan University, Ramat Gan, Israel


## Problem Statement

**Goal:**

**Detect suspicious behavior from a collection of individual trigger events**

- No single event is enough to decide (no incidents)
- Combination of events enables reasoning

**Main challenges:**

- Trigger events are noisy
- Trigger events involve interactions of multiple agents making recognition under noise difficult
- Our belief that person is acting suspiciously increases with the number of suspicious events non-linearly
- Subject's behavior in the past affects current evaluation

## Where Can It Be Applied?

- Adversary has a motivating goal
- His/her behavior deviates from behavior of regular subjects

**Detect Server Attack**
Observe users' actions to identify individuals who misuse server access.

**Find Pirate Vessel**
Observe how vessels interact with security patrols to identify pirates.

**Catch Dangerous Drivers**
Observe driving maneuvers to identify dangerous/reckless drivers.

**Catch Shoplifter**
Automatize video surveillance in shopping center to detect shoplifting from a series of events.

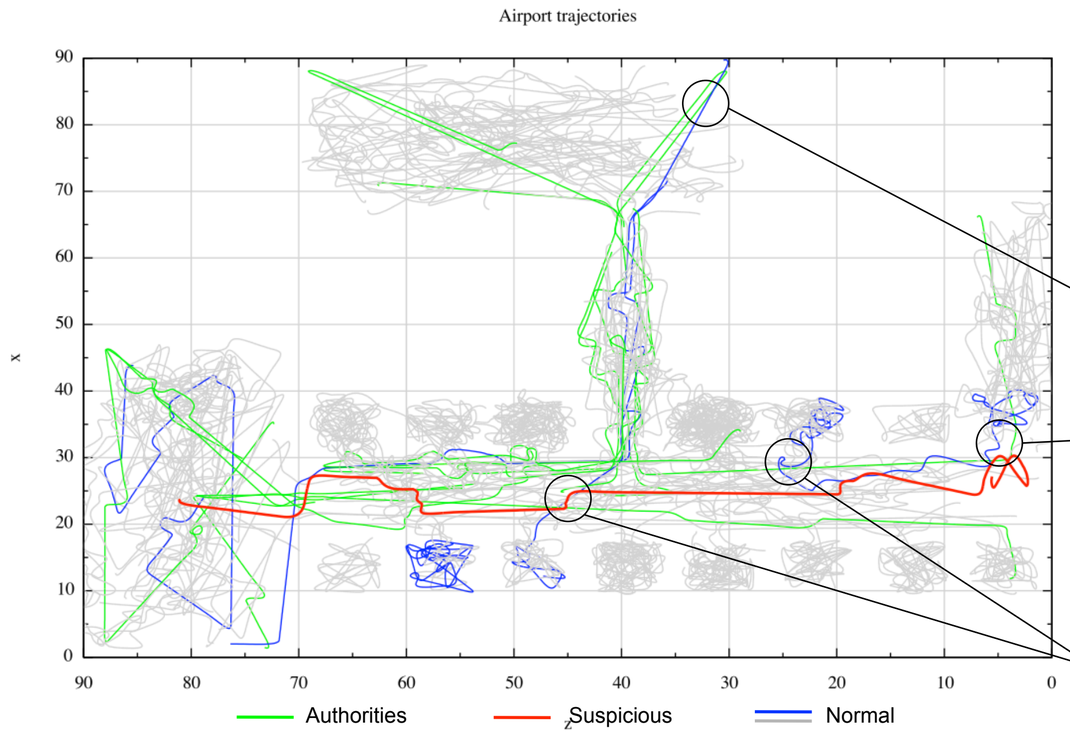
## Example: Detecting Suspicious Passenger at the Airport

**Goal: detect passengers that try to achieve a secured point**

- Go from point A to B (e.g., to smuggle drugs, plant a bomb, gain access…)
- Keep contacts with authorities at minimum
- Scenario defined by airport security experts

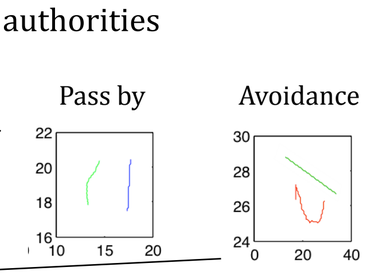
**Input: 2D traces of all passengers**

- Produced by multiagent simulator ESCAPES
- Find suspicious passenger (red trace)




**Trigger events**

Interactions with authorities




Detected with Coupled Hidden Markov Models

Turns

Turns in absence of authority


Detected with trajectory curvature

**Results**

- Naïve Bayes detector: recall 90%, precision 41%
- Scoring function: recall 90%, precision 90%

## Detectors

**Bayes-Optimal Detector**

- Optimal detector!
- We have no direct knowledge to estimate parameters
- We need approximate approaches

**Naïve-Bayes Detector**

- Assumes event independence
- Assumes that events are generated by stationary processes
- Model is over-simplified

**Scoring Function**

- Class of *well-behaved* functions
- Well-behaved heuristic function
  - Considers behavior in the past
  - Exponential increase in suspicion
  - Exponential time decay


ACKNOWLEDGMENTS: The authors would like to thank Zhengyu Yin for valuable discussion and suggestions, and Jason Tsai and Matthew Brown for their help with implementation challenges in the ESCAPES simulator. This research was done during Boštjan Kaluža's extended visit to Teamcore Research Group at University of Southern California. His work was supported partly by the Slovene Human Resources Development and Scholarship Fund and partly by the Slovenian Research Agency.