This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

G-DPS: A Game-theoretical Decision-making Framework for Physical Surveillance Games

Ali Alshawish, Hermann de Meer
University of Passau
Faculty of Computer Science
and Mathematics,
Passau, Germany

Stefan Rass
Universitaet Klagenfurt
Institute of Applied Informatics
System Security Group
Klagenfurt, Austria

CIP Workshop
Vienna, 19.-20.09.2016

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Agenda

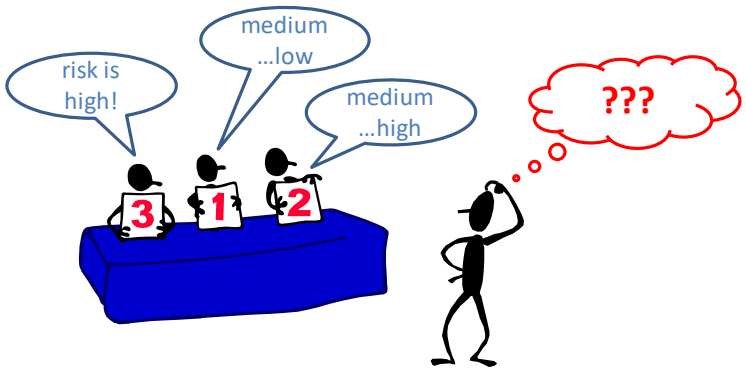
- Introduction
- Game-Theoretic Modeling using Uncertainty
- Decision-Making Framework and Physical Surveillance Games
- Example: Risk of Physical Intrusion in Critical Infrastructure Environment
- Conclusion

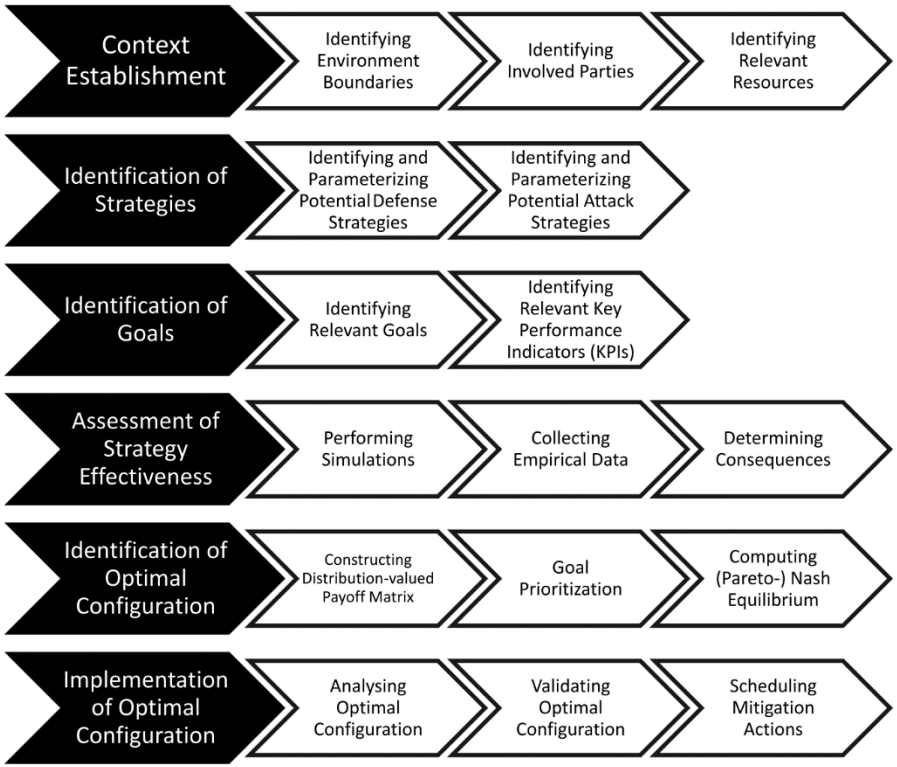
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Introduction

- Risk Management Approaches are typically generic and leave degrees of freedom in the „how“ to accomplish individual steps
- Input in each step relies on domain expertise
- Asking experts is occasionally problematic:

3 People asked → 4 opinions told



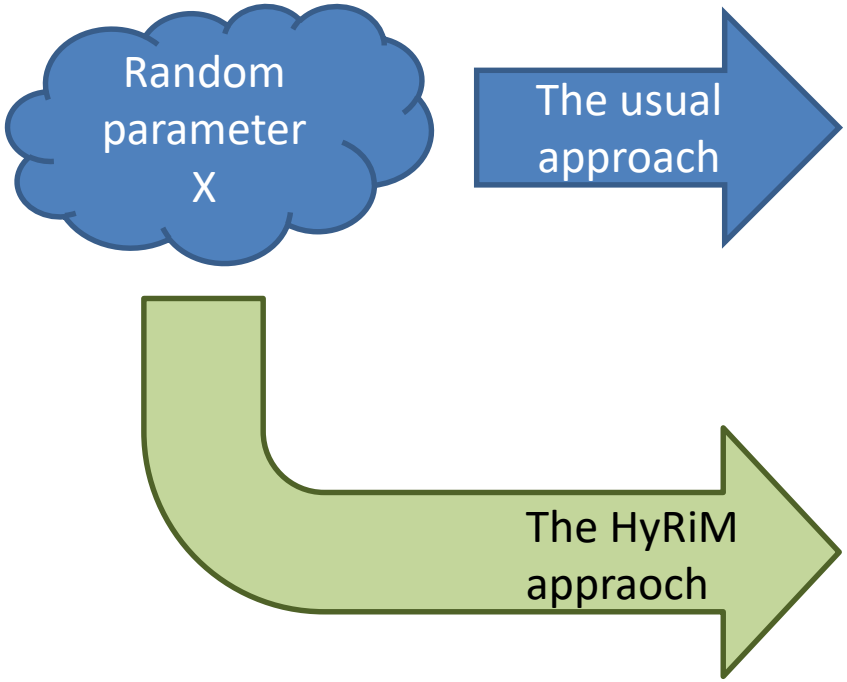


G-DPS Framework

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Uncertainty Modeling

- Suppose we have a random parameter or quantity X to deal with (such as „risk“ for decision making)



- „Average out the randomness“ (talk only about means, not concrete outcomes)
- Simplifies matters, as we are back at familiar numbers
- But burns lot of information

- Work with the full-featured random variable
- Theoretically more involved
- Yet preserves the available information (that is scarce anyway)

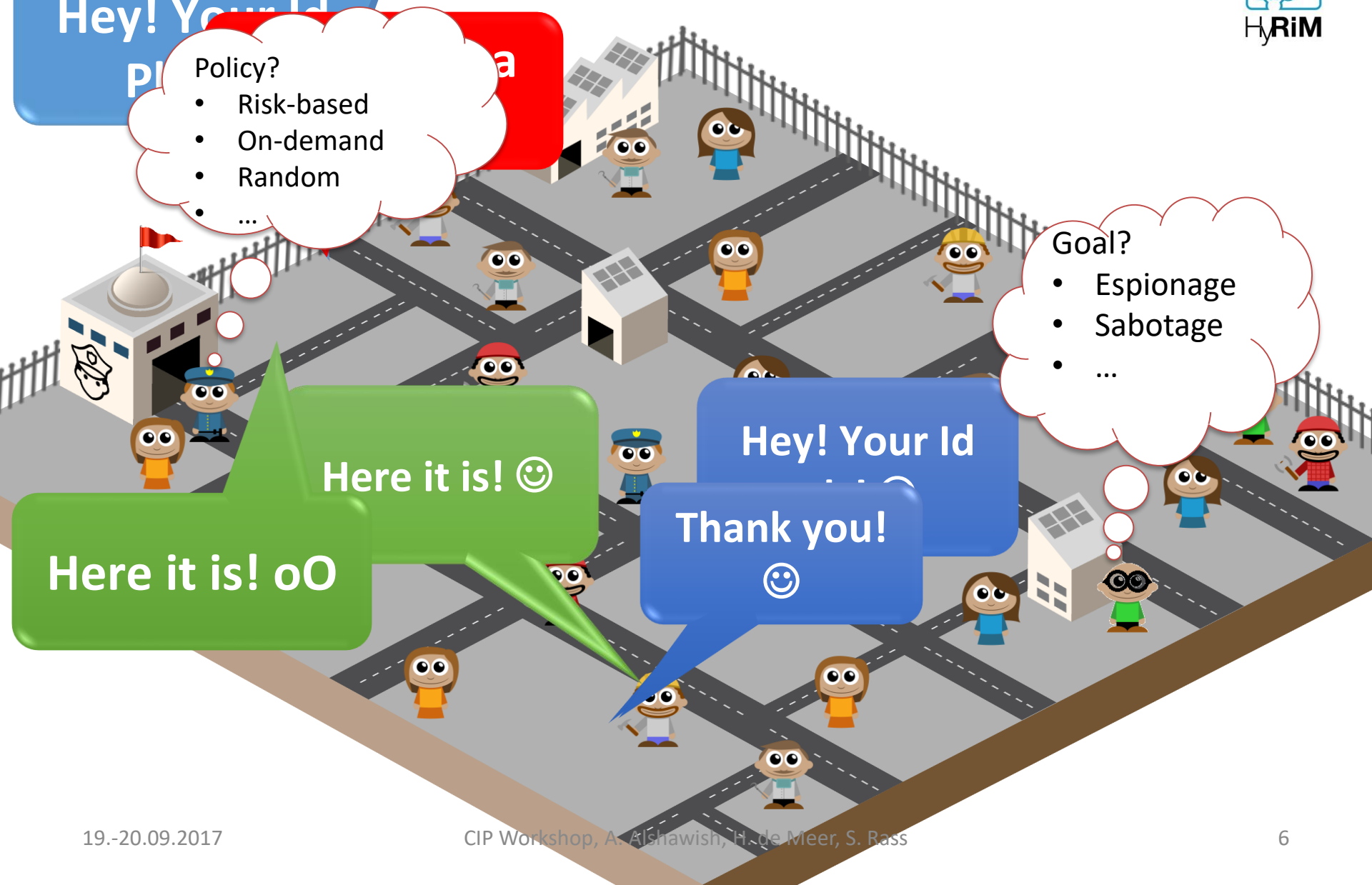
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Uncertainty in Games

- Game Theory: …the (natural) model for the non-cooperative competition between the defender and the adversary
- Game Theory in HyRiM:
  - In practice: Play a worst-case game (what is the best defense against any action of the adversary? What are the worst case attack scenarios?)
  - In theory: lift games to abstract spaces of probability distributions, and use stochastic orders for optimization
- In this talk:
  - Two-Player game: Surveillance people (player 1) vs. Intruders (player 2)
  - Outcome: Intruders either get caught or get missed
  - Uncertainty: …several kinds of…
    - Blind spots of cameras (static surveillance system)
    - Coincidental misses upon location visitations (adversary was „just not seen“)
    - …

Example

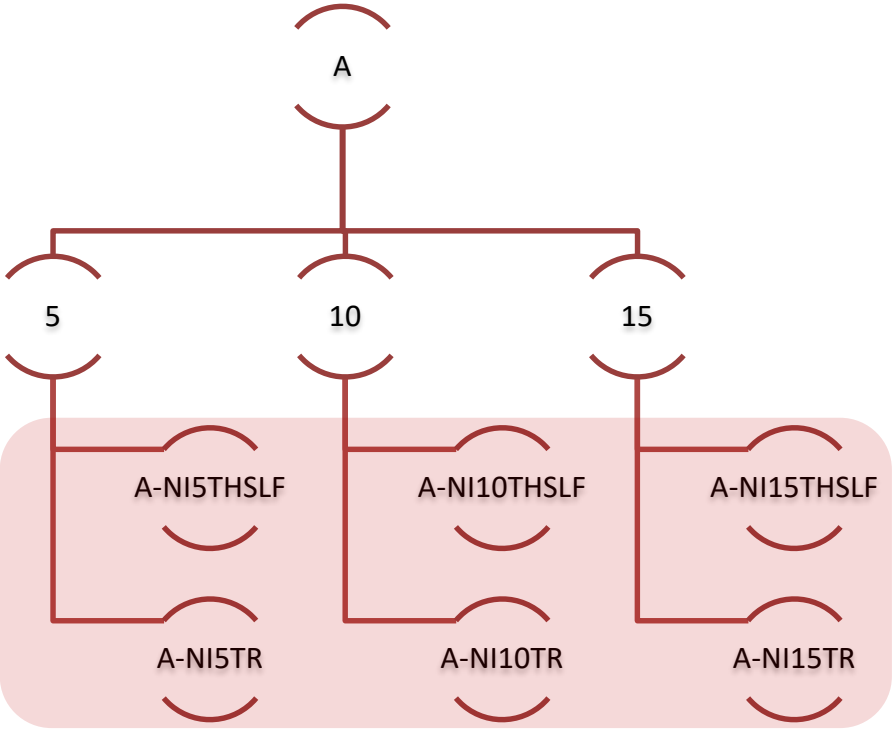
Physical Surveillance Games

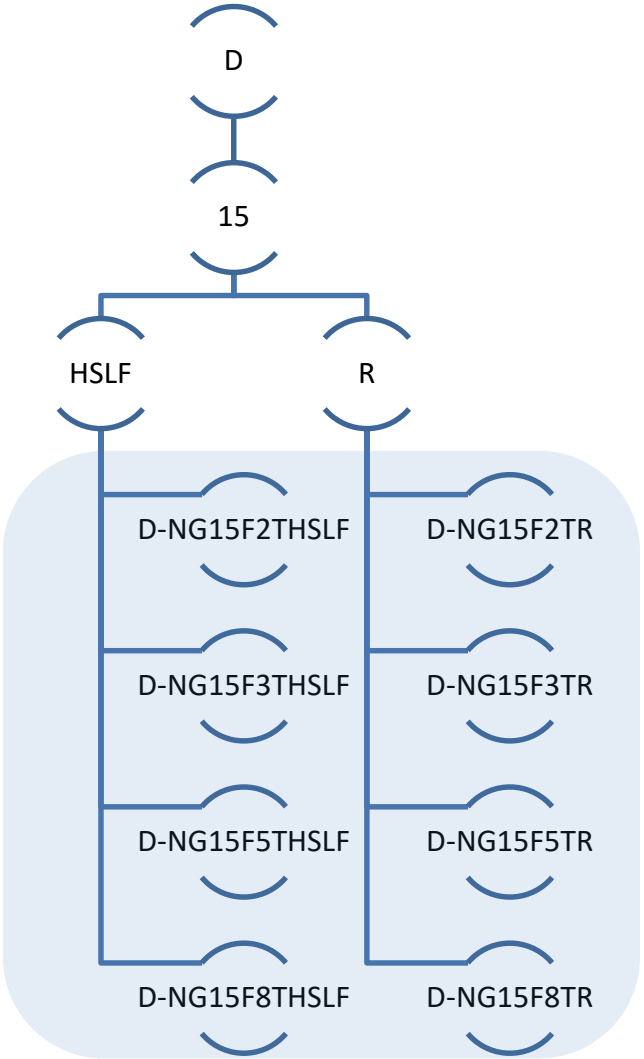


This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608990.

G-DPS Framework

Identification of Strategies





HSLF: **H**igher **S**ecurity **L**evel **F**irst

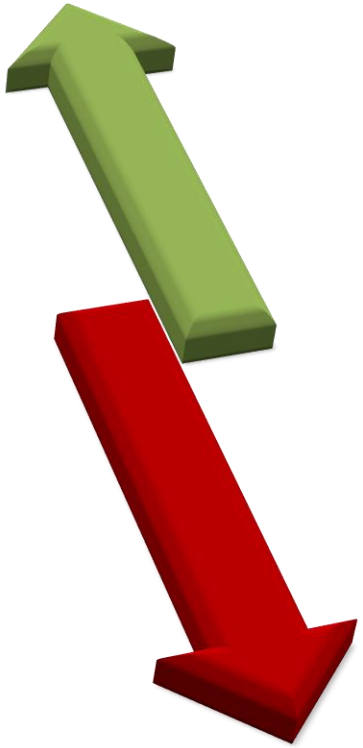
R : **R**andom

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

G-DPS Framework

Identification of Goals

- Detection Rate:
  - Number of detected intruders/Total number of intruders (NI)
- Minimum Privacy preservation:
  - Inversely related to the maximum possible disclosure of employees' locations
- Average Caused Damage
  - $\frac{1}{NI}\sum_i \sum_j timeSpent(intruder_i, area_j) \times secLevel(area_j)$
  - where $secLevel(area_j)$ gives the security level of area j
- Maximum Comfort Breach
  - The maximum comfort breach experienced by the employees
- **The multi-objective security game (MOSG): 8 Def. Strategies x 6 Atk. Strategies x 4 goals**



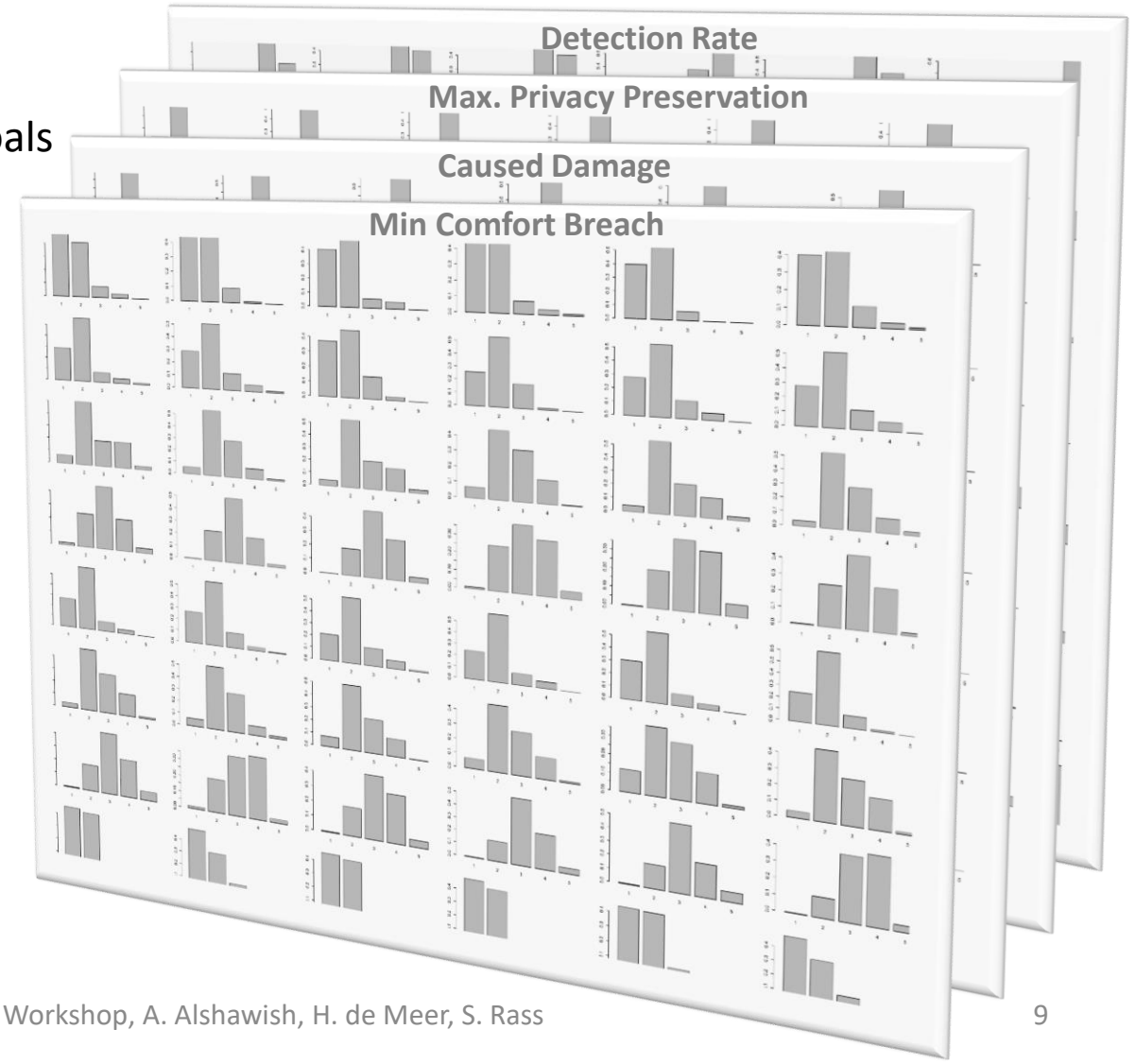
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

G-DPS Framework

Assessment of Strategies

- Strategy assessment
  - w.r.t. the identified goals
  - Classical surveys
  - Expert opinions
  - Statistical data
  - Simulation

  → Distribution-valued payoff matrix
  - Demo *„Simulation Framework to Assess Physical Surveillance Strategies “* on Wednesday at 10:00



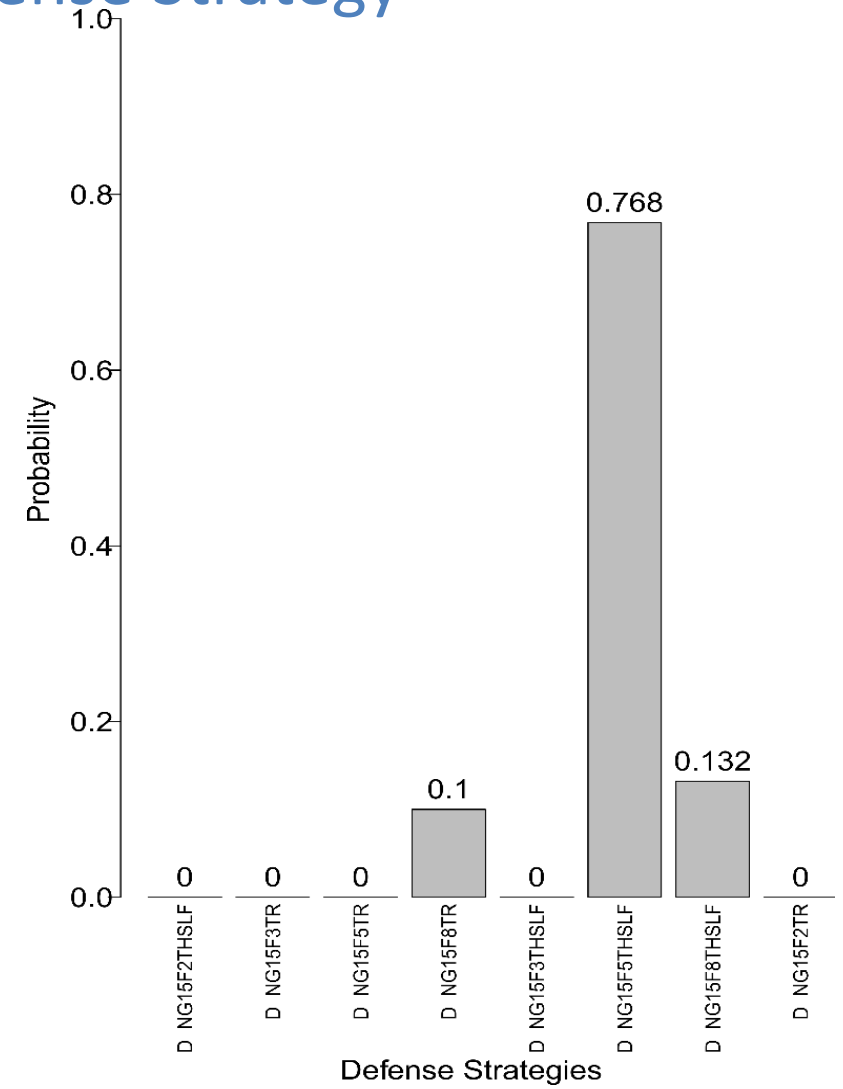
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

G-DPS Framework

Optimal Defense Strategy

Applying HyRiM R-package

- Optimal defense strategy
  - No single optimal defense precaution
  - The best is a „mix“ of defense measures



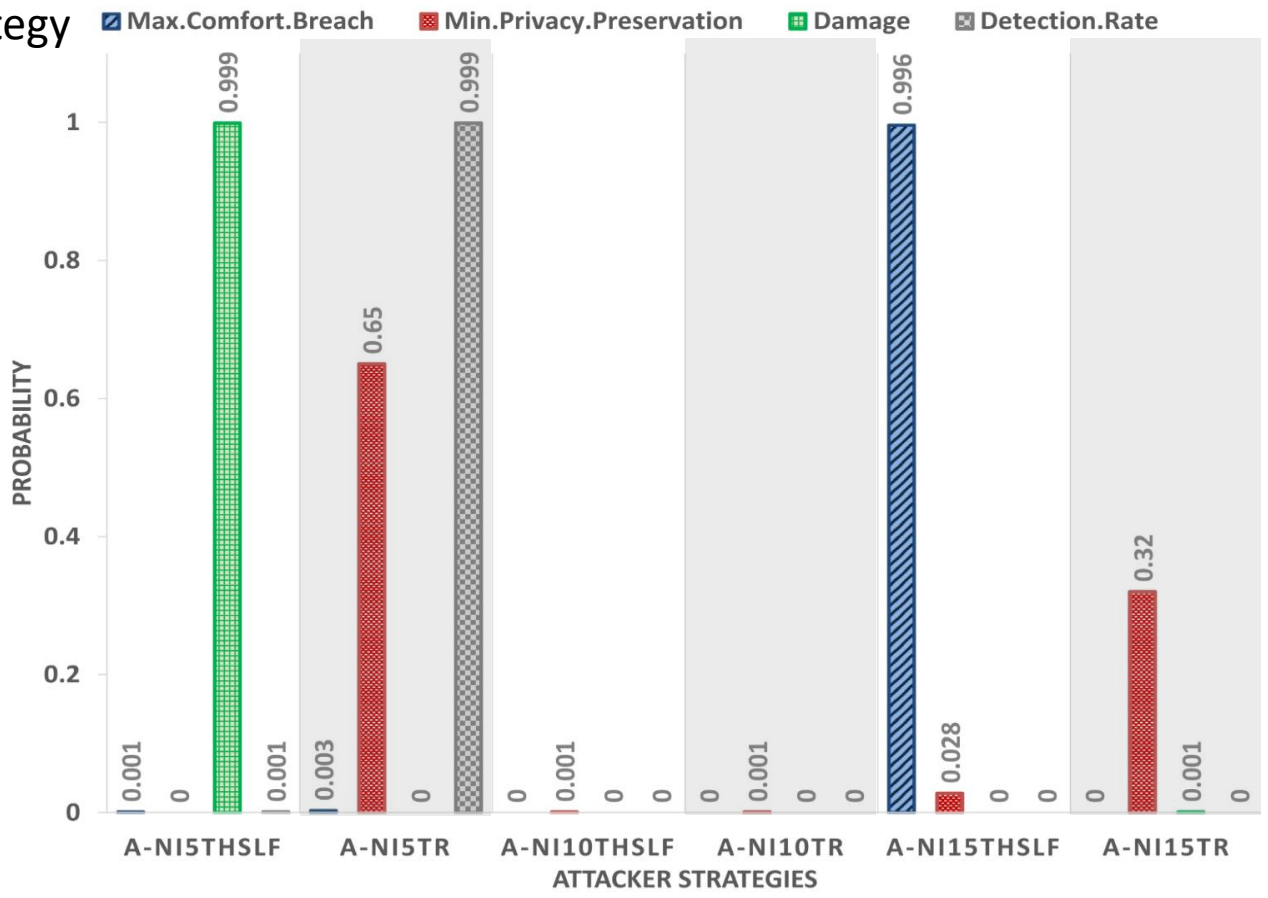
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

G-DPS Framework

Worst-case Attack Strategy

Applying HyRiM R-package

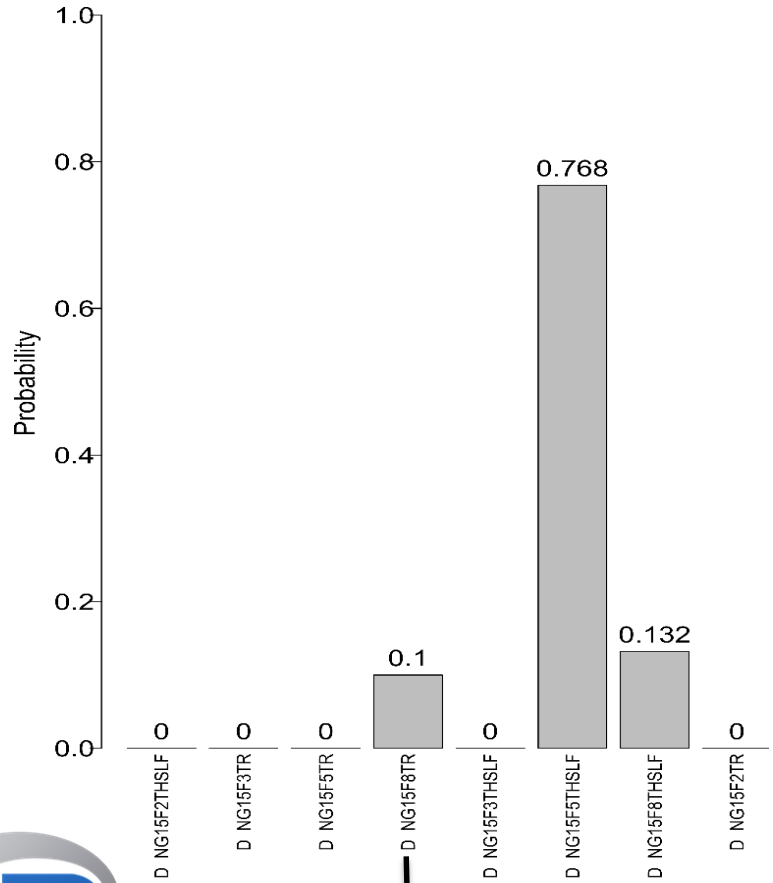
- Worst-case attack strategy
  - No single adversarial plan causes maximal loss in all goals
  - Real losses (in all goals) are less than predicted by the game

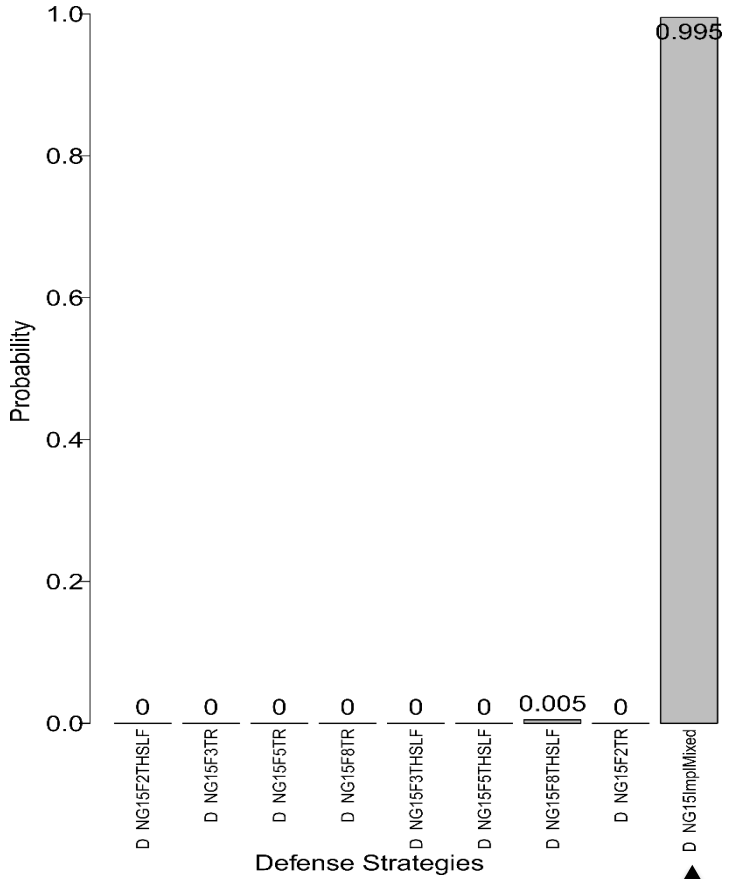


This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

G-DPS Framework

Validation





This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Conclusion

- Risk management in critical infrastructure involves maintaining a high level of situational awareness by means of surveillance and on-site observation.

- The challenge: resource allocation decisions
  - Uncertainty
  - Multiple competing goals

- Therefore, HyRiM approach delivers a tailored framework for game theory that allows:
  - playing games towards risk minimization over stochastic orders, and
  - optimizing over different goals (e.g., damage caused by the adversary, costs for security measures, acceptance of the security measures by the end-users, etc.)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Thank you for your attention

Questions?

A Game-theoretical Decision-making Framework for Physical Surveillance Games

Ali Alshawish, Hermann de Meer
University of Passau
Faculty of Computer Science
and Mathematics,
Passau, Germany

Stefan Rass
Universitaet Klagenfurt
Institute of Applied Informatics
System Security Group
Klagenfurt, Austria

CIP Workshop
Vienna, 19.-20.09.2016