Multithreat multisite protection:

A case study in metro security

D. Ríos Insua, RAC and ICMAT-CSIC

J. Cano, URJC

M. Pellot, R. Ortega, TMB

Washington, June ’14

Supported by SECONOMICS and AXA Research Fund

Outline

- **Motivation**
- Multithreat protection
- Case study
- Multisite Multithreat protection
- Case study (cont)
- Discussion

Motivation: Security

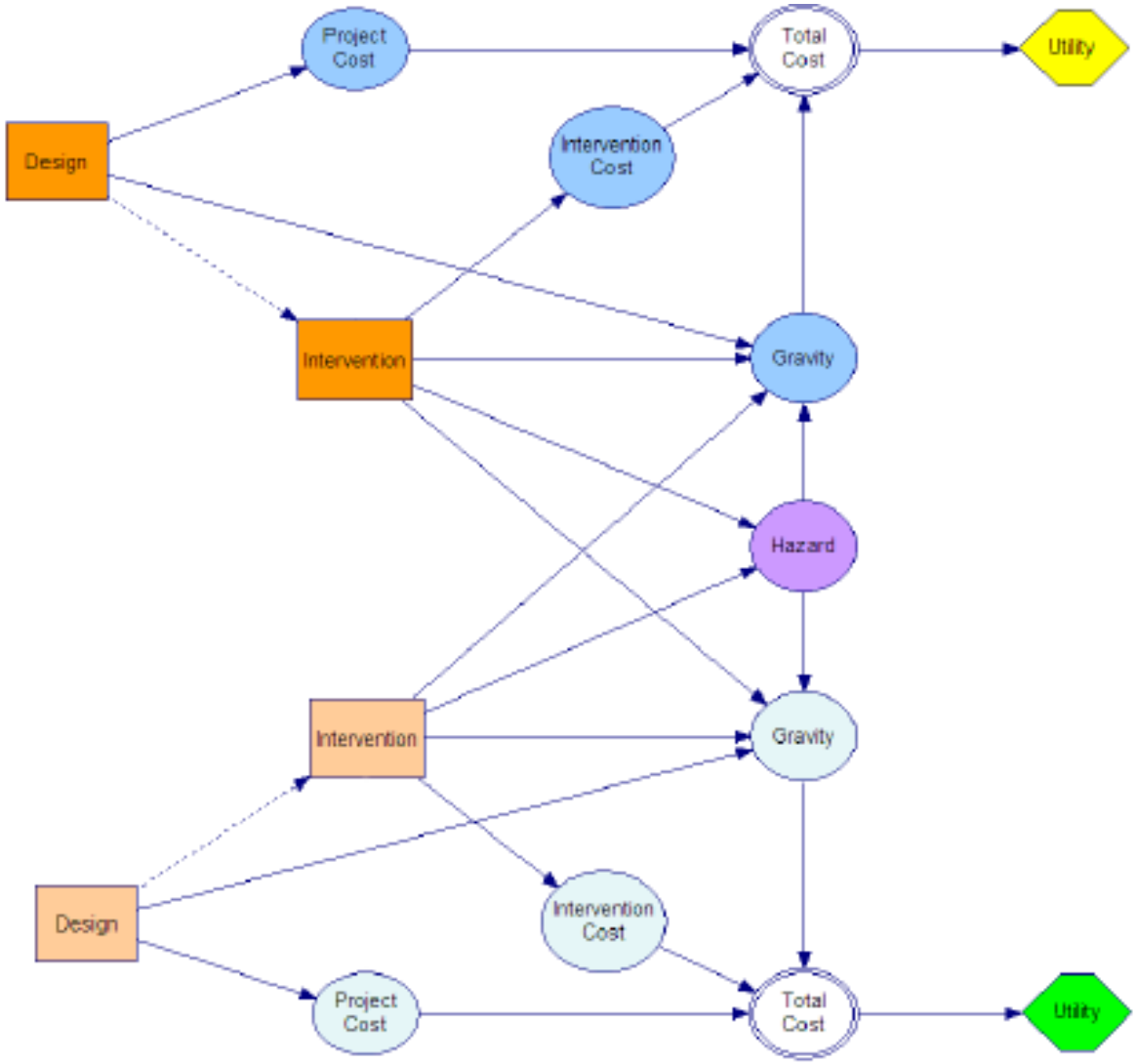
- Several of ‘The World’s (23) Biggest Problems´ (Lomborg, 2008)
- Global Risks Report WEF (2014)
- One of (8) Horizon 2020 pillars
- SECONOMICS (2012-2015) FP7
  - Anadulu Airport
  - Barcelona metro
  - National Grid, UK

Motivation: ARA

- Traditional RA extended to include adversaries ready to increase our risks

- S-11, M-11,… lead to large security investments globally, some of them criticised
- Many modelling efforts to efficiently allocate such resources
- Parnell et al (2008) NAS review
  - Standard reliability/risk approaches not take into acocunt intentionality
  - Game theoretic approaches. Common knowledge assumption…
  - Decision analytic approaches. Forecasting the adversary action…

Motivation: ARA



Motivation: ARA

- A framework to manage risks from actions of intelligent adversaries (DRI, Rios, Banks, JASA 2009)
- One-sided prescriptive support
  - Use a SEU model
  - Treat the adversary's decision as uncertainties
- Method to predict adversary's actions
  - We assume the adversary is a *expected utility maximizer*
    - Model his decision problem
    - Assess his probabilities and utilities
    - Find his action of maximum expected utility
  - But other *descriptive* models are possible
- Uncertainty in the Attacker's decision stems from
  - *our* uncertainty about his probabilities and utilities
  - but this may lead to a hierarchy of nested decision problems

(random, noninformative, k-level, heuristic, mirroring argument) vs (common knowledge)

Motivation: Which is the best security resource allocation in a metro network?

Metro Network as nodes, (links)

Threats: Pickpocketing, Fare evasion, (Graffitti, Terrorism)

Each node has a value

For each node, each threat, a predictive model of acts

Allocate security resources (constraints)

For each cell predict the impact of resource allocation

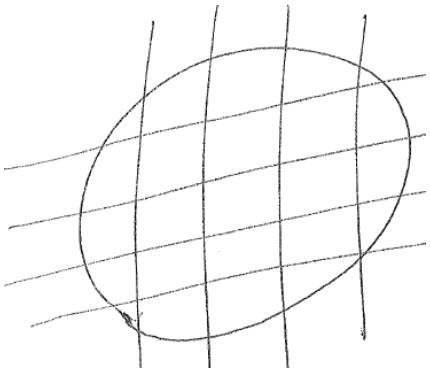
Optimal resource allocation

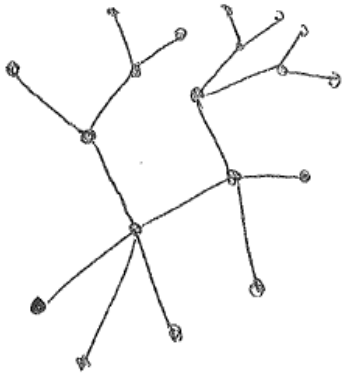
NB1: Bad guys operate intelligent and organisedly!!!

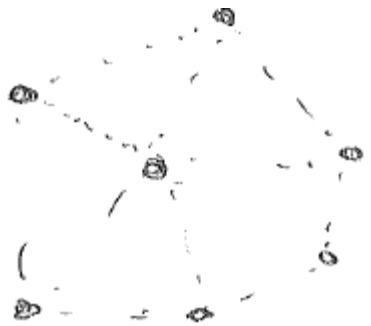
NB3: Different bad guys uncoordinated…

NB2: (Strategic) Tactical (Operational)

Underlying topology





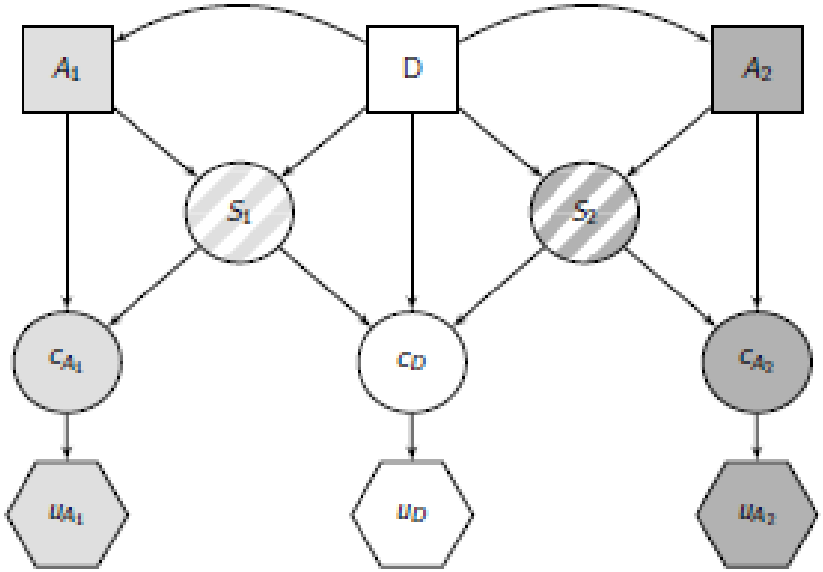


Hausken and Levitin classification

Outline

- Motivation
- **Multithreat protection**
- Case study
- Multisite Multithreat protection
- Case study (cont)
- Discussion

Multithreat protection



$$\psi_D(d|a_1,\ldots,a_m) = \int \cdots \int u_D(d,s_1,\ldots,s_m)\, p_D(s_1|d,a_1)\cdots p_D(s_m|d,a_m)\,\mathrm{d}s_1\ldots\mathrm{d}s_m$$

$$\psi_D(d) = \int \cdots \int \psi_D(d|a_1,\ldots,a_m)\, p_D(a_1|d)\cdots p_D(a_m|d)\,\mathrm{d}a_1\ldots\mathrm{d}a_m$$

$$\max_{d\in\mathcal{D}} \quad \psi_D(d)$$

Multithreat protection

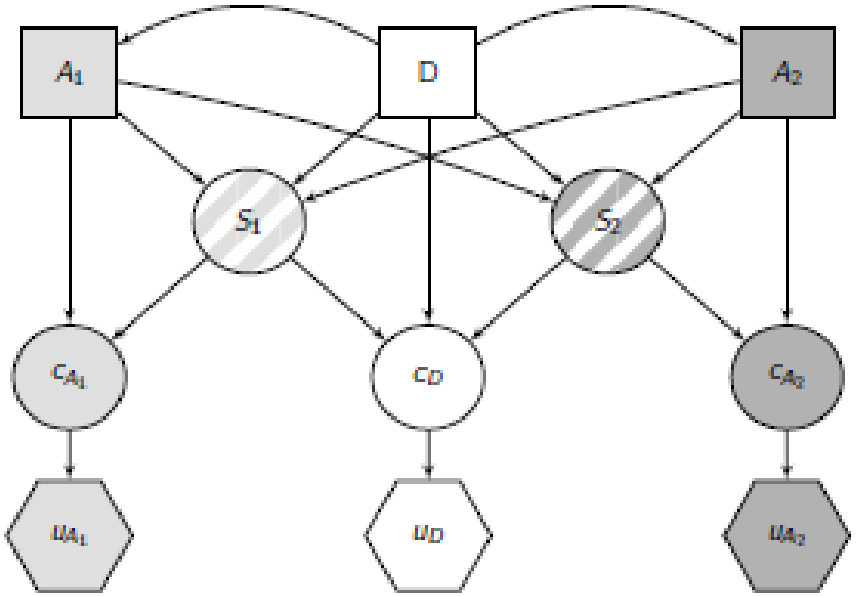
$$a_1^*(d) = \arg\max_{a_1 \in \mathcal{A}_1} \int u_{A_1}(a_1, s_1)\, p_{A_1}(s_1 | d, a_1)\, \mathrm{d}s_1$$

$$A_1^*(d) = \arg\max_{a_1 \in \mathcal{A}_1} \int U_{A_1}(a_1, s_1)\, P_{A_1}(s_1 | d, a_1)\, \mathrm{d}s_1$$

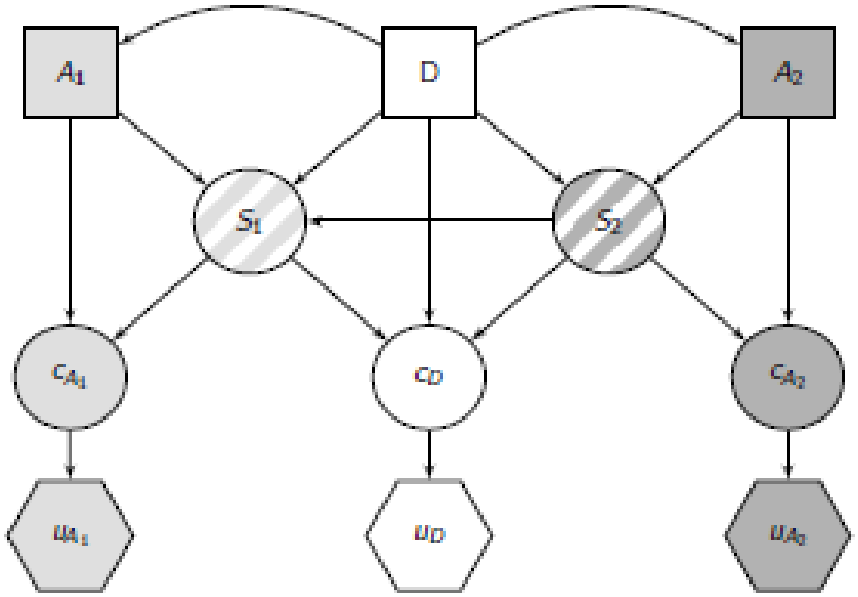
Algorithm 1: Simulating the problem for attacker $\mathtt{A}_1$

For $\mathtt{d} \in \mathcal{D}$
  For $\mathtt{k} = 1$ to $\mathtt{K}$
    For $\mathtt{a}_1 \in \mathcal{A}_1$
      Draw $(\mathtt{u}^{\mathtt{k}}_{\mathtt{A}_1}, \mathtt{p}^{\mathtt{k}}_{\mathtt{A}_1}) \sim (\mathtt{U}_{\mathtt{A}_1}, \mathtt{P}_{\mathtt{A}_1})$
      Compute $\psi^{\mathtt{k}}_{\mathtt{A}_1}(\mathtt{d}, \mathtt{a}_1) = \int \mathtt{u}^{\mathtt{k}}_{\mathtt{A}_1}(\mathtt{a}_1, \mathtt{s}_1)\, \mathtt{p}^{\mathtt{k}}_{\mathtt{A}_1}(\mathtt{s}_1 | \mathtt{d}, \mathtt{a}_1)\, \mathrm{d}\mathtt{s}_1$
    Compute $\mathtt{a}^{\mathtt{k}}_1(\mathtt{d}) = \arg\max_{\mathtt{a}_1 \in \mathcal{A}_1} \psi^{\mathtt{k}}_{\mathtt{A}_1}(\mathtt{d}, \mathtt{a}_1)$
  Approximate $\widehat{\mathtt{p}}_{\mathtt{D}}(\mathtt{a}_1 | \mathtt{d}) \approx \#\{1 \le \mathtt{k} \le \mathtt{K} : \mathtt{a}^{\mathtt{k}}_1(\mathtt{d}) \le \mathtt{a}_1\} / \mathtt{K}$

Multithreat protection



(a) Detrimental effect.



(b) Cascading effect.

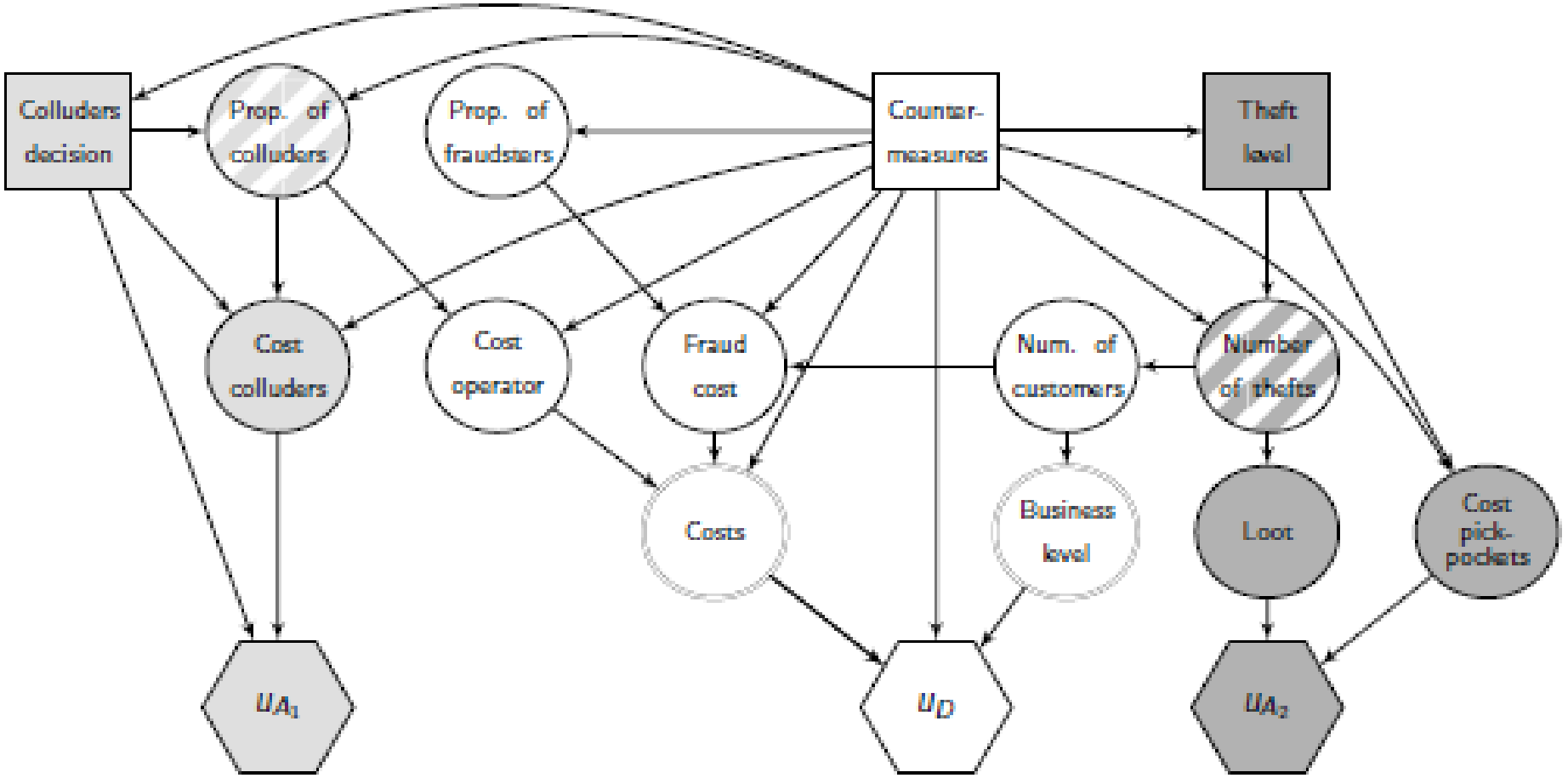
Multithreat protection

- If S_2 is discrete, $P_{A_2}(s_2|d,a_2)$ could be modeled as a Dirichlet distribution with mean $p_D(s_2|d,a_2)$ and variance accounting for the incumbent uncertainty. Note that, in particular, when S_2 is binary $P_{A_2}(s_2|d,a_2)$ would be modeled as a beta distribution.
- If S_2 is continuous, then $P_{A_2}(s_2|d,a_2)$ could be a Dirichlet process with base distribution $p_D(s_2|d,a_2)$ and concentration parameter δ, expressing our uncertainty about such base, see Ferguson (1973).

Outline

- Motivation
- Multithreat protection
- **Case study**
- Multisite Multithreat protection
- Case study (cont)
- Discussion

Case study: Pickpocketing and fare evasion



Case study

	Role		Features
	Fare evasion	Pickpocketing	
Inspectors	Preventive/recovery	—	Inspect customers. Collect fines
Door guards	Preventive	—	Control access points
Doors	Preventive	—	New secured automatic access doors
Ticket clerks	Preventive	—	Current little implication in security
Guards	Preventive	Preventive/recovery	Patrol along the facility
Patrols	—	Preventive/recovery	Trained guard+security dog
Cameras	—	Preventive	Complicate pickpocket actions
Awareness plans	—	Preventive	Alert users about pickpockets

$$\boldsymbol{d} = (d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8)$$

$$q_1 d_1 + q_2 d_2 + q_3 d_3 + q_5 d_5 + q_6 d_6 + q_7 d_7 + q_8 d_8 \leq B,$$

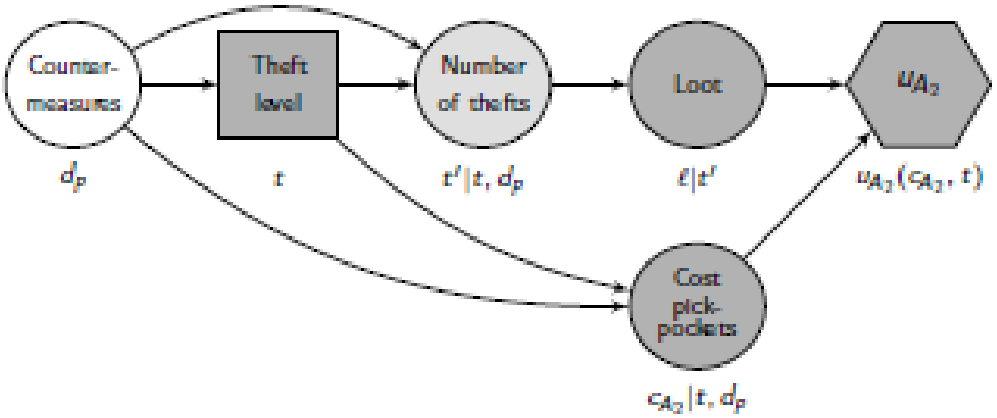
$$d_1, d_2, d_3, d_5, d_6, d_7 \geq 0,$$

$$d_1, d_2, d_3, d_5, d_6, d_7 \text{ integer},$$

$$d_3 \leq \bar{d}_3,$$

$$d_4, d_8 \in \{0, 1\},$$

Case study: Pickpocketers' problem



$$\Psi_{A_2}(t', t, d_p) = \iint \left[\sum_{t_1, t_2, t_3} p_{t_1 t_2 t_3 d_p} U_{A_2}(-q_p t - g t_2 + \ell t_3) \right] \times P_{A_2}(\xi | d_5, d_6, d_8)\, P_{A_2}(\theta | d_5, d_6)\, \mathrm{d}\xi\, \mathrm{d}\theta.$$

We integrate out the uncertainty over t' to get the random expected utility

$$\Psi_{A_2}(t, d_p) = \int \Psi_{A_2}(t', t, d_p) P_{A_2}(t' | t, d_p)\, \mathrm{d}t'.$$

$$p_D(T \leq t | d_p) = \Pr(T^*(d_p) \leq t).$$

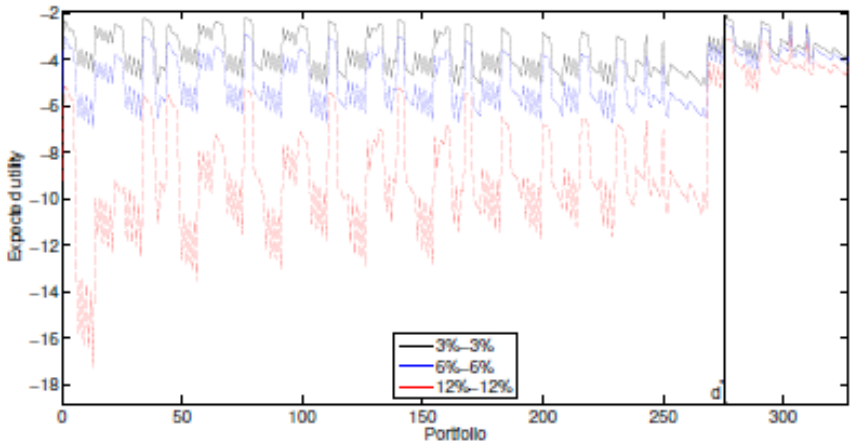
Then, the pickpockets find the random optimal theft level, given the defense d_p, through

$$T^*(d_p) = \arg\max_{t \in A_2} \Psi_{A_2}(t, d_p).$$

$$p_D(r | d_c).$$

Case study

$$\psi_D(d) = \int \left\{ \iint \left[\sum_{\substack{N_1,N_2,N_3 \\ M_1,M_2,M_3}} p_{M_1M_2M_3d_c} \cdot p_{N_1d_c}\, p_{N_2d_c}\, p_{N_3d_c} \cdot u_D(c_D) \right] p_D(t|d_p)\, p_D(b|t)\, \mathrm{d}t\, \mathrm{d}b \right\} \times p_D(r|d_c)\, \mathrm{d}r$$



$\phi_0 + \phi_r = 0.03$			
d	Invest.	$\psi(d)$	Income
$(1,0,0,0,0,1,0,0)$	85000	−2.36	−171585
$(0,4,0,0,0,0,0,0)$	100000	−4.72	−310277
$(0,0,1,0,0,0,0,0)$	15000	−3.32	−239770
$(0,0,0,0,0,0,3,0)$	13500	−3.54	−252791
$(0,0,0,0,0,0,0,1)$	40000	−4.07	−280640
$(0,4,0,1,0,0,0,0)$	100000	−5.09	−325518
$(0,1,1,1,2,0,0,0)$	100000	−6.82	−383989
$(0,0,0,1,2,0,0,1)$	100000	−6.86	−385086

- App. 1000000 passengers/year
- 100000 € additonal budget/year
- 324 feasible portfolios. Minutes.
- Expert assessment. Validation wshop.

Sensitivity analysis

- 1 inspector, 1 patrol

Outline

- Motivation
- Multithreat protection
- Case study
- **Multisite Multithreat protection**
- Case study (cont)
- Discussion

Multisite Multithreat protection

- One of the previous models per site
- Relate models by resource constraints and value aggregation. No spacial effects,…

$$\psi_D(\boldsymbol{d}|\boldsymbol{a}_1,\ldots,\boldsymbol{a}_m) = \int \cdots \int u_D(\boldsymbol{d},\boldsymbol{s}_1,\ldots,\boldsymbol{s}_m)\, p_D(s_{11}|d_1,a_{11}) \cdots p_D(s_{mn}|d_n,a_{mn})\, \mathrm{d}\boldsymbol{s}_1 \ldots \mathrm{d}\boldsymbol{s}_m$$

$$\psi_D(\boldsymbol{d}) = \int \cdots \int \psi_D(\boldsymbol{d}|a_{11},\ldots,a_{mn})\, p_D(a_{11}|d_1) \cdots p_D(a_{mn}|d_n)\, \mathrm{d}a_{11} \ldots \mathrm{d}a_{mn},$$

$$\begin{aligned} \max \quad & \psi_D(\boldsymbol{d}) \\ \text{s.t.} \quad & g(\boldsymbol{d}) \in \mathcal{D}. \end{aligned}$$

$$\boldsymbol{A}_1^*(\boldsymbol{d}) = \underset{h_1(\boldsymbol{a}_1)\in\mathcal{A}_1}{\arg\max} \int \cdots \int U_{A_1}(\boldsymbol{a}_1,\boldsymbol{s}_1)\, P_{A_1}(s_{11}|d_1,a_{11}) \cdots P_{A_1}(s_{1n}|d_n,a_{1n})\, \mathrm{d}s_{11} \ldots \mathrm{d}s_{1n}.$$

Outline

- Motivation
- Multithreat protection
- Case study
- Multisite Multithreat protection
- **Case study (cont)**
- Discussion

Case study

- 4 stations (different size, traffic, problems)

$$\sum_{j=1}^{4}\left(\sum_{\substack{k=1\\k\neq 4}}^{7} q_k d_{jk}\right) + q_8 d_8 \leq B,$$

$$0 \leq \sum_{j=1}^{4} d_{jk} \leq \bar{d}_k,\ k = 1,\ldots,7,\ k \neq 4,$$

$$d_{jk}\ \text{integer},\ j = 1,\ldots,4,\ k = 1,\ldots,7,\ k \neq 4,$$

$$d_{j3} \leq \bar{d}_{j3},\ j = 1,\ldots,4,$$

$$d_4, d_8 \in \{0,1\}.$$

Case study

- 26 decision variables, portfolios….
- Genetic algorithm, A few hours

Table 4 Optimal portfolio for the bithreat problem in four stations

	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	Invest. $(-)$	Fines $(+)$	Loss fare $(-)$	Loss pick. $(-)$
S_1	0	0	0	—	0	1	0	—	35,000	—	101,938	42,595
S_2	0	0	0	—	0	1	0	—	35,000	—	114,280	33,757
S_3	1	0	1	—	0	0	0	—	65,000	162,688	234,401	127,994
S_4	0	0	2	—	0	1	0	—	65,000	—	394,731	78,290
Total	1	0	3	1	0	3	0	0	200,000	162,688	845,170	282,636

- 1.2 M loss vs 2.5 M loss
- 165 stations, 662 decision variables, a few days..

Outline

- Motivation
- Multithreat protection
- Case study
- Multisite Multithreat protection
- Case study
- **Discussion**

Discussion

- Coordinated attackers
- Several defenders (coordinated)
- Less static D-A-D ….
- … Or afterwards, work on patroling schedule
- SECONOMICS tool
- General strategy

Thanks!!!

david.rios.insua@gmail.com

Supported by SECONOMICS and AXA Research Fund