SECONOMICS

Adversarial and Non-Adversarial Risk Analysis for Security over Multiples Sites

J. Cano[1] D. Ríos Insua[2]

[1]URJC

[2]Royal Academy of Sciences, Spain

XXVI EURO. Rome. July 2, 2013

SEVENTH FRAMEWORK PROGRAMME

Security Economics: Socio economics meets security

Outline

- Fare evasion
  - Solving only for standard evaders
  - Solving only for colluders
  - Solving both problems simultaneously
- Pickpocketing
- Fare evasion and pickpocketing over multiple stations

General overview

- One station
- Two threats.
  - Fare evasion
  - Pickpocketing by a team.
  - Both threats simultaneously.
- Extension to more than one station.

1. Fare evasion

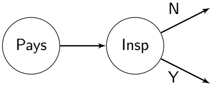
Description of problem

- Two types of evaders:
  - Standard (standard random process).
  - Colluders (ARA; explicitly modelling intentionality).
- Five countermeasures.
  - Inspectors (preventive/recovery), (x_1, c_1).
  - Security guards (*bouncers*), usually outsourced (preventive), (x_2, c_2).
  - Guards, working solo or in pairs (preventive/recovery), (x_3, c_3).
  - Automatic access doors (preventive), $(x_4 \leq n_4, c_4)$.
  - Metro officers (preventive), $(x_5,$ negotiation$)$.
- In general, the more resources, the less fare evasion will be. Also, the more inspectors, the more customers checked and, possibly, the more fines collected.

Three types of customers

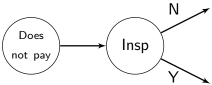
SECONOMICS

1. Civic customers.



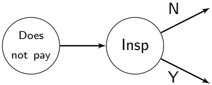
+ Metro	− Metro
Ticket	
Ticket	Annoyed customer

2. Standard fare evaders.



+ Metro	− Metro
	Ticket
Fine	

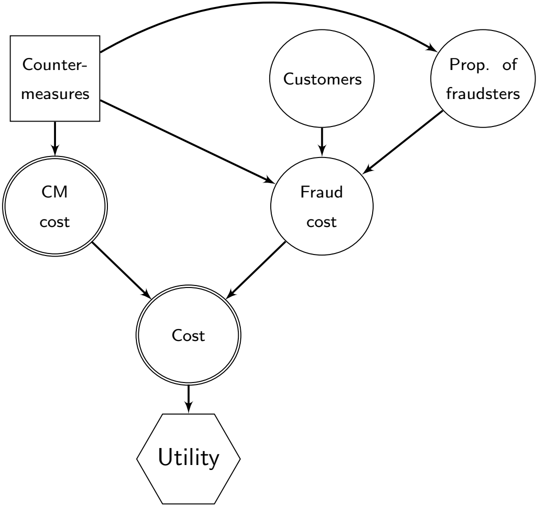
3. Colluding fare evaders.



+ Metro	− Metro	+ Customer	− Customer
	Ticket	Ticket	Cost
Fine			Cost, fine

Solving only for standard evaders

- This is a 'standard' risk management problem



Solving only for standard evaders (cont.)

- Operator invests $c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + x_5$. (Constraints)
- $p(x)$ proportion of standard evaders. $q(x_1)$ proportion of customers inspected.
  - $1 - p(x) \longrightarrow N_1$ civic customers pay ticket.
  - $p(x)[1 - q(x_1)] \longrightarrow N_2$ not pay ticket, not caught (loss t).
  - $p(x)q(x_1) \longrightarrow N_3$ do not pay ticket but are caught (income f).

$$c_D(N_1, N_2, N_3) = 0 \times N_1 - t \times N_2 + f \times N_3 - \sum_{i=1}^{4} c_4x_4 - x_5.$$

- Evaluate security plan x maximising expected utility

$$\max_{x \in \mathscr{B}_1} \psi(x) = \sum_{N_1,N_2,N_3} u_D(c_D(N_1, N_2, N_3))p^1_{N_1x}\, p^2_{N_2x}\, p^3_{N_3x}.$$

Typical assumptions

SECONOMICS

$$N_1 \sim \mathscr{P}ois\,(\lambda_1 = N[1-p(x)])$$
$$N_2 \sim \mathscr{P}ois\,(\lambda_2 = Np(x)[1-q(x_1)])$$
$$N_3 \sim \mathscr{P}ois\,(\lambda_3 = Np(x)q(x_1))$$

- Each additional inspector inspects fraction ρ of tickets

$$q\,(x_1) = \rho x_1\,.$$

- Each additional measure has a (dampened) deterrent effect

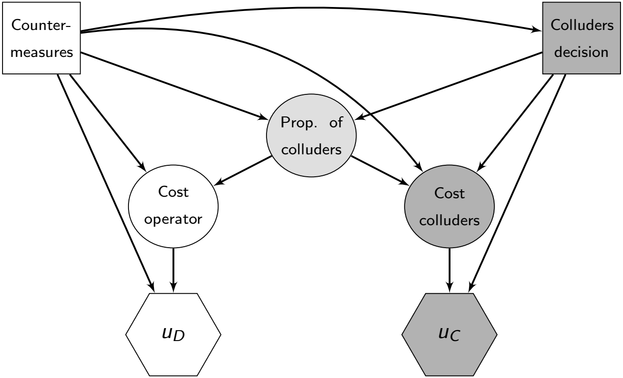
$$p\,(x) = p(x_1, x_2, x_3, x_4, x_5) = p_0 \exp(-\gamma_1 x_1 - \gamma_2 x_2 - \gamma_3 x_3 - \gamma_4 x_4 - \gamma_5) + p_r\,.$$

- u_D risk averse, u_D strategically equivalent to

$$u_D(c_D) = -\exp(-k_D c_D),\ k_D > 0.$$

Solving only for colluders

- This is an adversarial problem



Colluders dynamics

- "Club" entailing M operations over incumbent planning period.
  - They see security investments x (Sequential Defend-Attack).
  - They decide proportion r of fare evasion
  - Actual proportion r' depends also on $(x_1, x_2, x_3, x_4, x_5)$.
  - Operational costs, including preparation costs c_e

$$c = t(M_2 - M_1) - fM_3 - rc_e M.$$

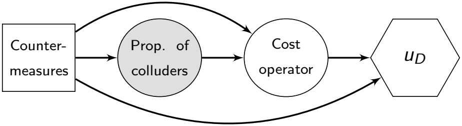
    - M_1 evaders pay (abortion).
    - M_2 not pay, not caught.
    - M_3 not pay, caught.

$$(M_1, M_2, M_3) \sim \mathscr{M}\left(M; (1-r'), r'(1-q_A(x_1)), r' q_A(x_1)\right).$$

  - Their utility (risk prone)

$$u_C(c - rc_e M).$$

Operator's problem



- Relevant revenues and costs

Concept	Revenue
Security costs	$-(c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + x_5)$
Tickets lost	$-tM_2$
Fines won	fM_3

- Total increase in outcome is

$$c_D = fM_3 - tM_2 - (c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + x_5).$$

Operator's problem (cont.)

SECONOMICS

- $u_D \longrightarrow$ utility, $h(r|x)$ models their beliefs over r given x, then

$$\psi(x) = \int \left[\sum_{M_1, M_2, M_3} p_{M_1 M_2 M_3 x}\, u_D \left(fM_3 - tM_2 - \sum_{i=1}^{4} c_i x_i - x_5 \right) \right] \times h(r|x) dr,$$

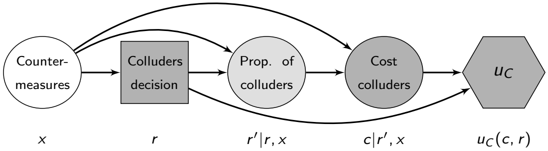
$p_{M_1 M_2 M_3 x} = \Pr(M_i \text{ type } i \text{ colluders} | x \text{ invested}),\ \sum_{i=1}^{3} M_i = M.$

- They must solve

$$\max_{x \in \mathscr{B}_1} \psi(x_1, x_2, x_3, x_4, x_5),$$

but $h(r|x)$ not directly available ($\longrightarrow$ Attacker's problem).

Attacker's problem



- x, security investment by Operator. We may consider $p_A(x)$ (Attacker's beliefs over x), although not necessary (is seen).
- r, decision made by Attacker.
- r', effective fare evasion proportion.
  - One possible model $r' = r(1 - s(x_1))$, $s(x_1)$ proportion of evasion abortions.
  - $p_A(s(x_1)) = p_A(s|x_1)$ induces $p_A(r'|r, x)$.
- c, global costs of evasion operation.
- u_C, utility over consequences $u_C(c - rc_e M)$.

Solving Attacker's problem

1. Integrate out uncertainty over c, getting expected utility

$$\psi_A(r', r, x) = \int \left[\sum_{M_1, M_2, M_3} p_{M_1 M_2 M_3 x} \right.$$

$$\left. \times \; u_C\left(t(M_2 - M_1) - fM_3 - rc_e M\right) \right] \times g_A(q_A | x_1) dq_A.$$

   $g_A(q_A|x_1)$ density over $q_A|x_1$, inducing $p_A(c|r', x)$.

2. Integrate out uncertainty over r', obtaining expected utility

$$\psi_A(r, x) = \int \psi_A(r', r, x) p_A(s|x_1) ds.$$

3. Find Attacker's optimal strategy

$$r(x) = \arg\max_r \psi_A(r, x).$$

Simulation scheme for estimating $h(r|x)$

- Uncertainty about $u_C(\cdot)$, $g_A(q_A|\cdot)$, $p_A(s|\cdot)$, modelled through $U_C(\cdot)$, $G_A(q_A|\cdot)$, $P_A(s|\cdot)$, has to be propagated.

```
For each x
  For i = 1 to K
    Sample U_C^i, G_A^i(q_A|·), P_A^i(s|·). Compute
```

$$\psi_A^i(r',r,x) =$$

$$\int \left[\sum_{M_1,M_2,M_3} p_{M_1M_2M_3x} U_C^i\left(t(M_2 - M_1) - fM_3 - rc_eM\right) \times G_A^i(q_A|x_1) \right] dq_A.$$

Compute

$$\psi_A^i(r,x) = \int \psi_A^i(r',r,x) P_A^i(s|x_1) ds.$$

Compute random optimal alternative

$$R^i = \arg\max_r \psi_A^i(r,x).$$

Approximate $p_A(R(x) \leq r) \approx \#\{1 \leq i \leq K : R^i \leq r\}/K$.

Typical assumptions

- Colluders risk prone in benefits $\longrightarrow u_C$ strategically equivalent

$$u_C(c) = \exp(k_C c),\ k_C > 0.$$

  - A random utility model could be

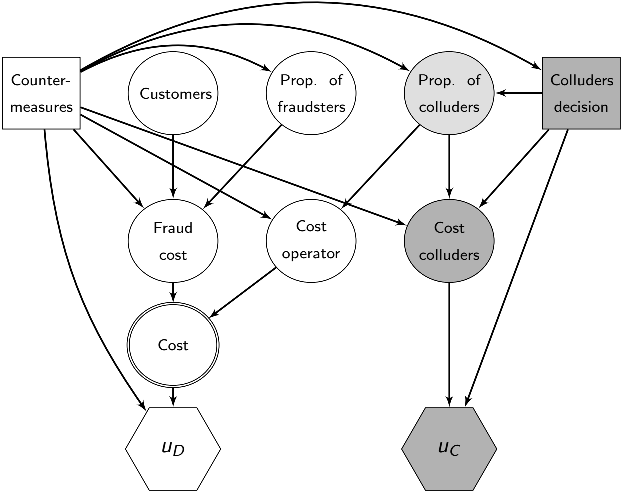
$$U_C(c) = \exp(k_C c),\ k_C \sim \mathscr{U}(0, K_C).$$

- Evaders proportion $s \sim \mathscr{B}e(\alpha, \beta)$. Dirichlet process with base $\mathscr{B}e(\alpha, \beta)$ for P_A

$$P_A \sim \mathscr{D}\mathscr{P}(\mathscr{B}e(\alpha, \beta), \delta_1).$$

  - If we consider $r' > r$, we could use an error model $r' = r + s$, s described by $p_A(s)$ and $P_A \sim \mathscr{D}\mathscr{P}(p_A, \delta_2)$.
- Proportion of inspections $q_A(x_1) \sim \mathscr{B}e(\alpha, \beta)$ with $\frac{\alpha}{\alpha+\beta} = \delta x_1$ and small variance.
  - Then, $G_A \sim \mathscr{D}\mathscr{P}(\mathscr{B}e(\alpha, \beta), \delta_3)$.

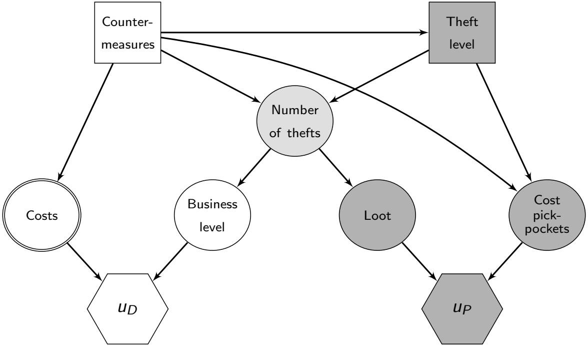
Solving the problem when both evaders are present



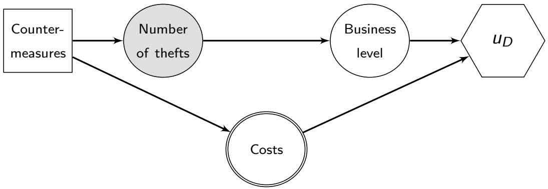
2. Pickpocketing

Description of problem

- Four countermeasures.
  - Patrols (preventive/recovery), (y_1, d_1).
  - Cameras (preventive), (y_2, d_2).
  - Guards (preventive/recovery), (x_3, c_3).
  - Public awareness plans (preventive), (y_3).



Defender's problem



- Operator invests y_1, y_2, x_3 (units) and y_3 (in the plan).
- Faces a delinquency level.
- Sees a decrease in business.
- Gets her utility (depends on business level and operator costs).

Defender's problem (cont.)

- Security costs

$$c'_D(y_1, y_2, x_3, y_3) = d_1 y_1 + d_2 y_2 + c_3 x_3 + y_3.$$

- b, business level, T theft level, $u_D(c'_D, b)$ Defender's utility

$$\max_{y \in \mathscr{B}_2} \iint u_D(c'_D, b) p(b|T) p(T|y) \, \mathrm{d}T \, \mathrm{d}y.$$

- $u_D(c'_D, b)$ includes costs and reduction in business level

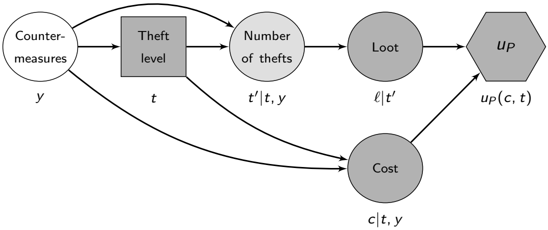
$$c'_D + (b_0 - b).$$

- Operator typically risk averse with respect to costs

$$u_D(c'_D, b) = -\exp\left(k'_D \cdot [c'_D + (b_0 - b)]\right), \; k'_D > 0.$$

- To assess $p(T|y) \longrightarrow$ Attacker's problem.

Attacker's problem



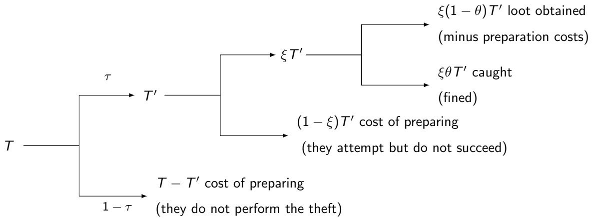
- See Defender's investment (y_1, y_2, x_3, y_3).
- Decide on target theft level T.
- Implement actual number of theft operations, $T' = \tau T$.
- Costs (of implementing) their actions is $c_p T$.

Attacker's problem (cont.)

- Face operational costs.
  - With prob. $(1-\xi)$, unsuccessful attempt. No consequences.
  - With prob. $\xi\theta$, succeed but caught. Fine g.
  - With prob. $\xi(1-\theta)$, succeed and not caught. Loot L.
- Total cost/benefit balance

$$c = \left[-c_p \times T_1\right] - \left[(g+c_p)\times T_2\right] + \left[(L-c_p)\times T_3\right] = -c_p T - g T_2 + L T_3.$$

- Get utility $u_P(-c_p T - g T_2 + L T_3)$.



Solving Attacker's problem

For each y
  For i = 1 to K
    Sample $U_P^i, P_A^i(\tau|\cdot), P_A^i(\xi|\cdot), P_A^i(\theta|\cdot)$.
    Compute

$$\psi_P^i(t', t, y) = \iint \left[\sum_{T_1, T_2, T_3} p_{T_1 T_2 T_3 y} \int U_P^i\left(-c_p T - g T_2 + L T_3\right) dU_P \right] \times P_A^i(\xi | y_1, x_3, y_3) P_A^i(\theta | y_1, x_3) d\xi d\theta.$$

    Compute

$$\psi_P^i = \int \psi_P^i(t', t, y) P_A^i(\tau | y_1, x_3) d\tau.$$

    Compute (and register) the optimal alternative

$$T^i = \text{argmax}_t \; \psi_P^i(t, y).$$

  Approximate $p_A(T(y) \leq t) \approx \#\{1 \leq i \leq K : T^i \leq t\}/K$.

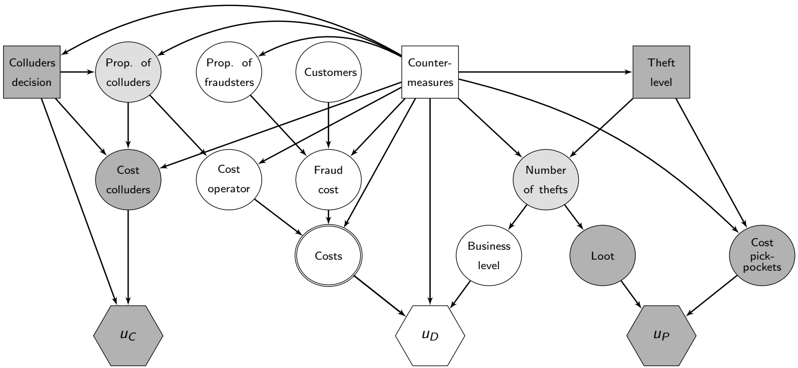
Model assumptions and uncertainties

SECONOMICS

- $\ell \sim \mathscr{U}(\ell_a, \ell_b)$, loot obtained when:
  - t', effective theft level $t' = t\tau(y_1, x_3)$.
    - $p_A(\tau(y_1, x_3)) = p_A(\tau | y_1, x_3)$ induces $p_A(t' | t, y)$.
  - ξ, success rate
    $\xi(y_1, x_3, y_3) = \xi_0 \exp(-\mu_1 y_1 - \mu_2 x_3 - \mu_3 y_3) + \xi_r$.
    - $p_A(\xi(y_1, x_3, y_3)) = p_A(\xi | y_1, x_3, y_3)$ induces $p_A(\ell | t')$.
  - θ, detention rate $\theta(y_1, x_3) = \rho_1 y_1 + \rho_2 x_3$.
    - $p_A(\theta(y_1, x_3)) = p_A(\theta | y_1, x_3)$ induces $p_A(c | t, y)$.
- $u_P(c) = \exp(k_P c)$, $k_P > 0$, $U_P(c) = \exp(k_P c)$, $k_P \sim \mathscr{U}(0, K_P)$.

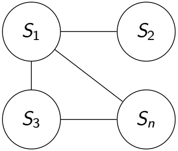
3. Fare evasion and pickpocketing over multiple stations

Joint influence diagram



Multiple sites problem

- Colluders and pickpockets do not make common cause.
- We can solve their problems separately.
- A network of n interconnected stations



- For each station a model like above is applicable, with mobile resources subject to global and specific budget and mobility constraints.

Mobility rules

- Fare evaders
  - If too many security measures in entering station i, move to adjacent station i'.
  - If inspectors in intermediate station k, an alternative route.
- Pickpockets
  - If too many security measures in station i, move to adjacent station i'.
- Some personnel (inspectors, patrols, guards) are mobile.

Main results

- A DSS is being currently devised to help decision makers.
- Upon perceived low-level threats, authorities tend to underestimate risk.
  - Attackers see a breach in security (more attackers).
  - Great impact can be caused even with low-profile attacks.
  - Low-cost preventive measures and well-trained personnel could deter attackers or minimize their number.
- Under scenario of high probability of attack.
  - Authorities tend to invest on expensive (sometimes sensationalist and ineffective) measures.
  - Set up security and mobility protocols for personnel increase their efficiency.

Conclusions

- For fare evasion, a mixed non adversarial - adversarial problem has been tackled.
- For pickpockets, not only direct economic impact considered (also image costs).
- General model over multiple sites has been devised.
  - Resources are constrained by budget and mobility.
  - Some countermeasures have to be shared for both threats.