Multithreat Multisite Protection: An Adversarial Risk Analysis Approach

J. Cano[1] D. Ríos Insua[2]

[1]URJC

[2]Royal Academy of Sciences, Spain

XXIII SRA. Istanbul. June 17, 2014

Outline

Multithreat protection for one site

Multithreat multisite protection

Case study

General overview

- ARA (Ríos Insua et al., 2009) approach for multithreat problem over one site
  - Uncoordinated attacks.
  - Outcome of attacks might affect each other.
- Extension to multiple sites (Ríos Insua et al., 2014b)
  - Sequential Defend-Attack for each site/threat.
  - Models related by resource constraints and value aggregation.
  - No particular spatial structure.
- Case study: metro network protection against
  - Fare evasion. (Ríos Insua et al., 2014a)
  - Pickpocketing by a team.

SECONOMICS

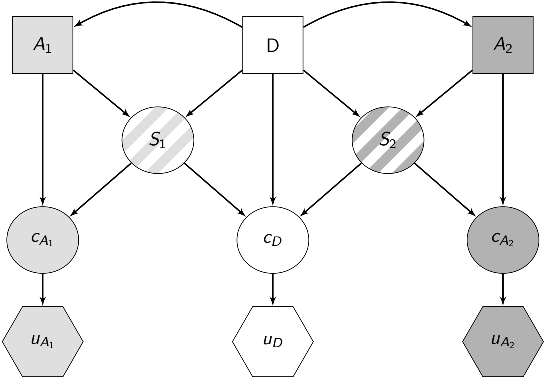
1. Multithreat protection for one site

What is ARA?

- ARA builds decision analysis model for Defender, who forecasts actions of her intentional adversaries.
- Once with this knowledge, she decides optimal defense against attacks.
- Sequential Defend-Attack model.
  - Defender first chooses a portfolio of countermeasures
  - After observing it, Attacker decides his attack.

Description of problem

- Basic multithreat protection problem



- Defender aims at finding optimal defense d^*.
  - Consequences evaluated through utility $u_D(d, s_1, \ldots, s_m)$.

Optimal solution

SECONOMICS

- Assume cond. ind. $S_i|d, a_i \longrightarrow p_D(s_i|d, a_i)$.
  - Obtain expected utility, given the attacks

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

- Suppose Defender able to build models $p_D(a_i|d)$.
- Assume cond. ind. of $a_1, \ldots, a_m$ given d. Compute

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

and solve

$$d^* \longleftarrow \max_{d \in \mathscr{D}} \quad \psi_D(d).$$

Assessment of Attacker's intentions

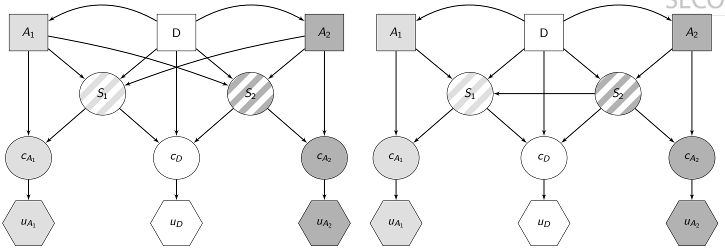
SECONOMICS

- To obtain $p_D(a_i|d)$, solve each attacker's problem (E.U. max.)

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

- Defender lacks knowledge $\left(u_{A_1}(\cdot), p_{A_1}(s_1|\cdot)\right) \to \left(U_{A_1}, P_{A_1}\right)$.
- Approximate $\widehat{p_D}(a_i|d)$ through Monte Carlo simulation.
  - Assessment of $P_{A_1}(\cdot)$ typically based on $p_D(\cdot)$
    - Dirichlet distribution (process) for discrete (continuous).
  - For U_A, information about Attacker's interests
    - Aggregate with weighted measurable value function.
    - Assume risk proneness.
    - Distributions over weights and risk proneness coefficients.

Possible generalizations



- *(left)* If simultaneous, but uncoordinated attacks $a_1, \ldots, a_m$ jointly detrimental in face of d

$$p_D(s_1|d, a_1) \cdots p_D(s_m|d, a_m) \rightarrow p_D(s_1|d, a_1, \ldots, a_m) \cdots p_D(s_m|d, a_1, \ldots, a_m).$$

- *(right)* Cascading effect between results of attacks

$$p_D(s_1|d, a_1)\, p_D(s_2|d, a_2) \rightarrow p_D(s_1|d, a_1, s_2)\, p_D(s_2|d, a_2).$$

2. Multithreat multisite protection

General methodology

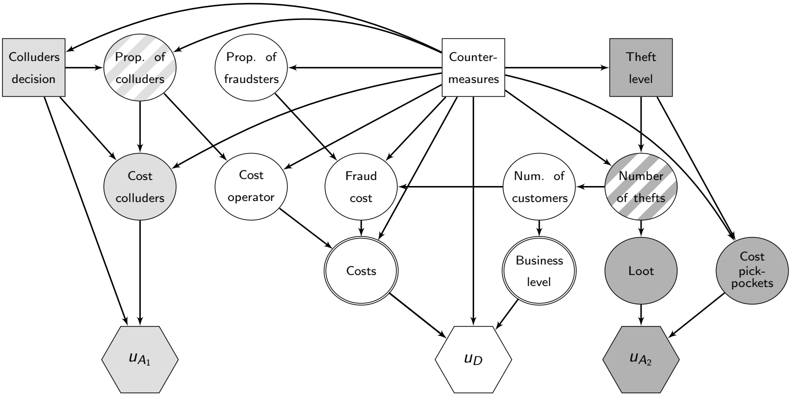
1. Deploy one of previous models over each site.
2. Resource constraints coordinate models.
3. Aggregate value at nodes applying utility function.
4. Defender deploys d_j over site j, fulfilling $g(d_1, \ldots, d_n) \in \mathscr{D}$.
5. i-th Attacker performs a_{ij} over j-th site, satisfying $h_i(\boldsymbol{a}_i) \in \mathscr{A}_i$.
6. Interaction yields random results $S_{ij} \in \mathscr{S}_{ij}$.
7. Defender aggregates results through $u_D(\boldsymbol{d}, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_m)$.
8. To find optimal defense strategy $\boldsymbol{d}^*$, compute

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

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

3. Case study

Influence diagram



Description of problem

- Metro operator D protecting from:
  - Fare evasion. Two types of evaders:
    - Standard (standard random process).
    - Colluders A_1 (ARA; explicitly modeling intentionality).
  - Pickpockets A_2. Organized group. Security & image costs.

		Role		Features
		Fare	Pick	
d_1	Inspector	Prev./rec.	—	Inspect customers. Collect fines
d_2	Door guard	Prev.	—	Control access points
d_3	Door	Prev.	—	New secured automatic access doors
d_4	Ticket clerk	Prev.	—	Current little implication in security
d_5	Guard	Prev.	Prev./rec.	Patrol along the facility
d_6	Patrol	—	Prev./rec.	Trained guard+security dog
d_7	Camera	—	Prev.	Complicate pickpocket actions
d_8	Campaign	—	Prev.	Alert users about pickpockets

Feasible portfolios

- Associated unit costs $q_1, q_2, q_3, q_5, q_6.q_7$.
- $d_4 \in \{0,1\}$ ($d_4 = 1 \rightarrow$ clerks involved, incurred costs q_4).
- $d_8 \in \{0,1\}$, ($d_8 = 1 \rightarrow$ operator invests q_8).

$$
\begin{gathered}
q_1 d_1 + q_2 d_2 + q_3 d_3 + q_5 d_5 + q_6 d_6 + q_7 d_7 + q_8 d_8 \leq B, \\
d_1, d_2, d_3, d_5, d_6, d_7 \geq 0, \\
d_1, d_2, d_3, d_5, d_6, d_7 \text{ integer}, \\
d_3 \leq \bar{d}_3, \\
d_4, d_8 \in \{0,1\},
\end{gathered}
$$

$\bar{d}_3$ maximum # of doors that may be replaced.

Fare evasion

SECONOMICS

- Operator invests $d_c = (d_1, d_2, d_3, d_4, d_5)$. (Constraints)
  - Fare evasion costs (partly mitigated by fines).
- $\phi(d_c)$ evaders proportion. $q(d_1)$ inspection proportion.
  - $1 - \phi(d_c) \longrightarrow N_1$ civic customers pay ticket.
  - $\phi(d_c)[1 - q(d_1)] \longrightarrow N_2$ not pay, not caught (loss v_c).
  - $\phi(d_c)q(d_1) \longrightarrow N_3$ do not pay but caught (income f_c).
- **Colluders** see security investments d_c (Seq D-A).
- Fare evasion proportion $r \to r'$, inspection proportion $q_A(d_1)$
  - $1 - r' \to M_1$ pay, abortion (income v_c).
  - $r'(1 - q_A(d_1)) \to M_2$ not pay, not caught (loss v_c).
  - $r' q_A(d_1) \to M_3$ not pay, caught (income f_c).
- Operational costs, including preparation costs q_c

$$c_{A_1} = v_c(M_2 - M_1) - f_c M_3 - r q_c M.$$

Pickpocketing

- Operator invests $d_p = (d_5, d_6, d_7, d_8)$. (Constraints)
  - Decrease in business level $b - b_0$.
- **Pickpockets** see security investment d_p (Seq D-A).
- Theft level $t \to t'$, abortion τ, success ξ, detention θ
  - $1-(1-\tau)\xi \to t_1$ not succeed.
  - $(1-\tau)\xi\theta \to t_2$ succeed, but caught (fine f_p).
  - $(1-\tau)\xi(1-\theta) \to t_3$ succeed, not caught (loot ℓ).
- Operational costs, including preparation costs q_p

$$c_{A_2} = -q_p t - f_p t_2 + \ell t_3.$$

- Both colluders and pickpockets risk prone in benefits

$$u_{A_i}(c_{A_i}) = \exp(k_{A_i} \cdot c_{A_i}),\ k_{A_i} > 0,\ i = 1, 2.$$

Solving the bithreat problem

SECONOMICS

- Operator benefit/cost balance

$$c_D(N_1, N_2, N_3, M_1, M_2, M_3, d, b) =$$

$$- v_c(N_2 + M_2) + f_c(N_3 + M_3) - \sum_{k=1}^{8} q_k d_k - (b_0 - b).$$

- Operator risk averse to increase in income,

$$u_D(c_D) = -\exp(-k_D \cdot c_D).$$

- Evaluate security plan d maximizing expected utility

$$\psi_D(d) = \int \left\{ \iint \left[\sum_{\substack{N_1,N_2,N_3 \\ M_1,M_2,M_3}} p_{M_1 M_2 M_3 d_c} \cdot p_{N_1 d_c} \, p_{N_2 d_c} \, p_{N_3 d_c} \cdot u_D(c_D) \right] \right.$$

$$\left. p_D(t|d_p) \, p_D(b|t) \, \mathrm{d}t \, \mathrm{d}b \right\} \times p_D(r|d_c) \, \mathrm{d}r.$$

A case study

SECONOMICS

- Colluders and pickpockets do not make common cause.
- Cascading effect → N. of customers affected by pickpockets through business level → influence colluder's decision.
- A subnetwork of 4 stations, with models like above, related by resource constraints and value aggregation.

Station	Passengers	Budget (k€)	Fare evasion	Pickpocketing	Constraints
1	1,000,000	30–100	Moderate	Moderate	—
2	1,000,000	30–100	Moderate	Moderate	—
3	1,000,000	30–100	High	Moderate	1 inspector
4	5,000,000	50–100	Moderate	High	1 guard
Total	8,000,000	120–200	—	—	—

- Resource upper bounds $\bar{d}_k = 4$, $k = 1, 2, 3, 5, 6$ and $\bar{d}_7 = 8$.
- At most, two units of each countermeasure at a single station.

Results

	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

- Door guards, cameras and awareness plan not worth it.
- Involve ticket clerks in observation tasks.
- Annual expected losses 1,225,118 € (around 2,5 M€ otherwise).

Conclusions

SECONOMICS

- ARA methodology for protecting multiple sites from multiple uncoordinated threats.
- Sequential Defend-Attack model for each attacker and site.
- Models coordinated by resource constraints and value aggregation over various sites and threats.
- Case study in metro security $\rightarrow$ fare evasion and pickpocketing (cascading effect).

Future research

SECONOMICS

- Multiple defenders and their eventual coordination.
- Coordination of attacks and their rationality type.
- Further interactions among defenders and attackers.
- Mobility of resources.

Acknowledgments

SECONOMICS

- This project has received funding from the **European Union's Seventh Framework Programme for Research, Technological Development and Demonstration under grant agreement no 285223**.
- Work has been also supported by the Spanish Ministry of Economy and Innovation program MTM2011-28983-C03-01 and the Government of Madrid RIESGOS-CM program S2009/ESP-1685.
- We are grateful to TMB experts and stakeholders for fruitful discussion about modeling issues.

Bibliography

SECONOMICS

- Ríos Insua, D., J. Cano, M. Pellot, R. Ortega. 2014. *Current Trends in Bayesian Methodology with Applications*, chap. From Risk Analysis to Adversarial Risk Analysis. CRC Press, To appear.
- Ríos Insua, D., J. Cano, M. Pellot, R. Ortega. 2014. Multithreat Multisite Protection: A Case Study in Metro Security. *In preparation*.
- Ríos Insua, D., J. Ríos, D. Banks. 2009. Adversarial risk analysis. *Journal of the American Statistical Association* 104(486) 841–854.