Multithreat Multisite Protection: An Adversarial Risk Analysis Approach

J. Cano\textsuperscript{1} D. Ríos Insua\textsuperscript{2}

\textsuperscript{1}URJC
\textsuperscript{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.
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 $u_D(d,s_1,\ldots,s_m)$. 

![Diagram of the multithreat protection problem with nodes and arrows representing the interactions between attackers, defense, and consequences.](SECONOMICS)
Optimal solution

- Assume cond. ind. \( S_i \mid d, a_i \rightarrow p_D(s_i \mid d, a_i) \).
  - Obtain expected utility, given the attacks
    \[
    \psi_D(d \mid a_1, \ldots, a_m) = \int \cdots \int u_D(d, s_1, \ldots, s_m) p_D(s_1 \mid d, a_1) \cdots p_D(s_m \mid d, a_m) \, ds_1 \cdots ds_m.
    \]
  - Suppose Defender able to build models \( p_D(a_i \mid d) \).
  - Assume cond. ind. of \( a_1, \ldots, a_m \) given \( d \). Compute
    \[
    \psi_D(d) = \int \cdots \int \psi_D(d \mid a_1, \ldots, a_m) p_D(a_1 \mid d) \cdots p_D(a_m \mid d) \, da_1 \cdots da_m,
    \]
    and solve
    \[
    d^* \leftarrow \max_{d \in \mathcal{D}} \psi_D(d).
    \]
Assessment of Attacker’s intentions

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

$$a_1^*(d) = \arg \max_{a_1 \in \mathcal{A}_1} \int u_{A_1}(a_1, s_1) p_{A_1}(s_1|d, a_1) ds_1.$$  

- Defender lacks knowledge $(u_{A_1}(\cdot), p_{A_1}(s_1|\cdot)) \rightarrow (U_{A_1}, P_{A_1})$.

- Approximate $\hat{p}_D(a_i|d)$ 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 $g(d_1, \ldots, d_n) \in \mathcal{D}$.
5. $i$-th Attacker performs $a_{ij}$ over $j$-th site, satisfying $h_i(a_i) \in \mathcal{A}_i$.
6. Interaction yields random results $S_{ij} \in \mathcal{S}_{ij}$.
7. Defender aggregates results through $u_D(d, s_1, \ldots, s_m)$.
8. To find optimal defense strategy $d^*$, compute

$$
\psi_D(d|a_1, \ldots, a_m) = \int \cdots \int u_D(d, s_1, \ldots, s_m) p_D(s_{11}|d_1, a_{11}) \cdots p_D(s_{mn}|d_n, a_{mn}) ds_1 \cdots ds_m.
$$

$$
\psi_D(d) = \int \cdots \int \psi_D(d|a_{11}, \ldots, a_{mn}) p_D(a_{11}|d_1) \cdots p_D(a_{mn}|d_n) da_{11} \cdots da_{mn}.
$$
3. Case study
Influence diagram

Colluders decision
- Prop. of colluders
- Prop. of fraudsters

Cost colluders

Cost operator

Fraud cost

Counter-measures

Theft level

Costs

Num. of customers

Business level

Number of thefts

Loot

Cost pick-pockets

$u_{A_1}$

$u_D$

$u_{A_2}$
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).

<table>
<thead>
<tr>
<th>Role</th>
<th>Fare</th>
<th>Pick</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>$d_1$ Inspector</td>
<td>Prev./rec.</td>
<td>—</td>
<td>Inspect customers. Collect fines</td>
</tr>
<tr>
<td>$d_2$ Door guard</td>
<td>Prev.</td>
<td>—</td>
<td>Control access points</td>
</tr>
<tr>
<td>$d_3$ Door</td>
<td>Prev.</td>
<td>—</td>
<td>New secured automatic access doors</td>
</tr>
<tr>
<td>$d_4$ Ticket clerk</td>
<td>Prev.</td>
<td>—</td>
<td>Current little implication in security</td>
</tr>
<tr>
<td>$d_5$ Guard</td>
<td>Prev.</td>
<td>Prev./rec.</td>
<td>Patrol along the facility</td>
</tr>
<tr>
<td>$d_6$ Patrol</td>
<td>—</td>
<td>Prev./rec.</td>
<td>Trained guard+security dog</td>
</tr>
<tr>
<td>$d_7$ Camera</td>
<td>—</td>
<td>Prev.</td>
<td>Complicate pickpocket actions</td>
</tr>
<tr>
<td>$d_8$ Campaign</td>
<td>—</td>
<td>Prev.</td>
<td>Alert users about pickpockets</td>
</tr>
</tbody>
</table>
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 $q_8$).

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

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

$d_1, d_2, d_3, d_5, d_6, d_7$ integer,

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

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

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

- 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.
  - $1 - \phi(d_c) \rightarrow N_1$ civic customers pay ticket.
  - $\phi(d_c)[1 - q(d_1)] \rightarrow N_2$ not pay, not caught (loss $v_c$).
  - $\phi(d_c)q(d_1) \rightarrow N_3$ do not pay but caught (income $f_c$).

- **Colluders** see security investments $d_c$ (Seq D-A).
- Fare evasion proportion $r \rightarrow r'$, inspection proportion $q_A(d_1)$
  - $1 - r' \rightarrow M_1$ pay, abortion (income $v_c$).
  - $r'(1 - q_A(d_1)) \rightarrow M_2$ not pay, not caught (loss $v_c$).
  - $r'q_A(d_1) \rightarrow M_3$ not pay, caught (income $f_c$).

- Operational costs, including preparation costs $q_c$
  \[
c_{A_1} = v_c(M_2 - M_1) - f_cM_3 - rq_cM.
\]
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 $t \rightarrow t'$, abortion $\tau$, success $\xi$, detention $\theta$
  - $1 - (1 - \tau)\xi \rightarrow t_1$ not succeed.
  - $(1 - \tau)\xi \theta \rightarrow t_2$ succeed, but caught (fine $f_p$).
  - $(1 - \tau)\xi (1 - \theta) \rightarrow t_3$ succeed, not caught (loot $\ell$).
- 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
  \[ u_{A_i}(c_{A_i}) = \exp(k_{A_i} \cdot c_{A_i}), \quad k_{A_i} > 0, \quad i = 1, 2. \]
Solving the bithreat problem

- Operator benefit/cost balance

\[
c_D(N_1, N_2, N_3, M_1, M_2, M_3, d, b) =
\]
\[
- \nu_c(N_2 + M_2) + f_c(N_3 + M_3) - \sum_{k=1}^{8} q_k d_k - (b_0 - b).
\]

- Operator risk averse to increase in income,

\[
u_D(c_D) = -\exp(-k_D \cdot c_D).
\]

- Evaluate security plan \( d \) maximizing expected utility

\[
\psi_D(d) = \int \left\{ \int \int \left[ \sum_{N_1, N_2, N_3, M_1, M_2, M_3} p_{M_1 M_2 M_3 d_c} \cdot p_{N_1 d_c} p_{N_2 d_c} p_{N_3 d_c} \cdot u_D(c_D) \right] p_D(t|d_p) p_D(b|t) dt db \right\} \times p_D(r|d_c) dr.
\]
A case study

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

<table>
<thead>
<tr>
<th>Station</th>
<th>Passengers</th>
<th>Budget (k€)</th>
<th>Fare evasion</th>
<th>Pickpocketing</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1,000,000</td>
<td>30–100</td>
<td>Moderate</td>
<td>Moderate</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>1,000,000</td>
<td>30–100</td>
<td>Moderate</td>
<td>Moderate</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>1,000,000</td>
<td>30–100</td>
<td>High</td>
<td>Moderate</td>
<td>1 inspector</td>
</tr>
<tr>
<td>4</td>
<td>5,000,000</td>
<td>50–100</td>
<td>Moderate</td>
<td>High</td>
<td>1 guard</td>
</tr>
<tr>
<td>Total</td>
<td>8,000,000</td>
<td>120–200</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

- 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

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

- 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

- 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 → fare evasion and pickpocketing (cascading effect).
Future research

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

▶ 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.
