Adversarial Risk Analysis Models for Urban Security Resource Allocation

David Ríos Insua, Royal Academy
Cesar Gil, U. Rey Juan Carlos
Jesús Ríos, IBM Research YH

COST Smart Cities Wshop
Paris, September 2011
ARA for Urban Security Resource Allocation

- Security
- Urban security and modelling
- Adversarial Risk Analysis
- ARA for Urban Security Resource Allocation
- Discussion
Security

• One of ‘The World’s Biggest Problems’ (Lomborg, 2008)
  – Arms proliferation
  – Conflicts
  – Corruption
  – Terrorism
  – Drugs
  – Money laundering

• One of the FP7 topics!!!
Urban Security and Modelling

- Criminology
- Becker (1968) Economic theory of delict
- Clarke and Cornish (1986) Situational crime prevention. The reasoning criminal
  - Rational Choice in criminology
  - Routine activities theory
  - Delictive pattern theory
  - Problem-oriented policing
- Displacement theory
- Policing performance measures
Urban Security and Modelling

- COMPSTAT (1994)
- Crime Mapping
- Patrol Car Allocation Models (Tongo, 2010)
- Police Patrol Area Covering Models (Curtin et al, 2007)
- Police Patrol Routes Models (Chawathe, 2007)
- ARMOR (CREATE, 2007)
- The Numbers behind NUMB3RS (Devlin, Lorden, 2007)
Adversarial Risk Analysis

- S-11, M-11 led to large security investments globally, some of them criticised
- Many modelling efforts to efficiently allocate such resources
- Parnell et al (2008) NAS review of bioterr assessment
  - Fault tree not accounting for intentionality
  - Game theoretic approaches. Common knowledge assumption...
  - Decision analytic approaches. Forecasting the adversary action...
- Merrick, Parnell (2011) review approaches commenting favourably on Adversarial Risk Analysis
Adversarial Risk Analysis

• 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 leads to a hierarchy of nested decision problems (k level thinking)

    (noninformative, heuristic, mirroring argument) vs (common knowledge)
Adversarial Risk Analysis

- ARA applications to counterterrorism models (Rios, DRI, 2009, 2012) (ESF-COST ALGODEC)
  - Sequential Defend-Attack
  - Simultaneous Defend-Attack
  - Sequential Defend-Attack-Defend
  - Sequential Defend-Attack with private information
  - General coupled influence diagrams? Koller, Milsch
- Somali pirates case (Sevillano, Rios, DRI, 2012)
- Routing games (anti IED war) (Wang, Banks, 2011)
- Borel games (Banks, Petralia, Wang, 2011)
- Auctions (DRI, Rios, Banks, 2009; Rothkopf, 2007)
ARA for Urban Security. Basics

- City divided into cells $(i,j)$ with value $c_{ij}$
- Each cell has a value $v_{ij}$
- Agents
  1. Defender, $D$, Police. Aims at maintaining value
  2. Attacker, $A$, Mob. Aims at gaining value

- $D$ allocates resources to prevent
- $A$ performs attacks
- $D$ allocates resources to recover

\[
\sum_{ij} a_{ij} \leq A \\
\sum_{ij} d_{ij}^1 \leq D_1 \\
\sum_{ij} d_{ij}^2 \leq D_2
\]
**ARA for Urban Security. Basics**

The map and the values:

\[ \sum_{ij} d_{ij}^1 \leq 11 \quad \text{and} \quad d_{ij}^1 \geq 0, \quad d_{ij}^1 \text{ integer} \]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \text{ } & \text{ } & 1.0 & 0.8 & 0.6 \\
2 & \text{ } & \text{ } & 0.4 & 0.2 & 0.5 \\
3 & \text{ } & \text{ } & 0.7 & 0.9 & 1.0 \\
\end{array}
\]

The resource allocations:

\[ \sum_{ij} a_{ij} \leq 3 \quad \text{and} \quad a_{ij} \geq 0, \quad a_{ij} \text{ integer} \]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & 1 & 0 & 1 \\
2 & 1 & 3 & 1 \\
3 & 1 & 1 & 2 \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & 11 & 0 & 0 \\
2 & 0 & 0 & 0 \\
3 & 0 & 0 & 0 \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 \\
3 & 0 & 0 & 3 \\
\end{array}
\]

\[ \sum_{ij} d_{ij}^2 \leq 11, \quad d_{ij}^2 \geq 0, \quad d_{ij}^2 \text{ integer} \]

\[ \sum_{ij} d_{ij}^2 \leq \sum_{(k,h)\in (i,j)_m} d_{kh}^1 \]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & d_{11}^1 & d_{12}^1 & d_{13}^1 \\
2 & d_{21}^1 & d_{22}^1 & d_{23}^1 \\
3 & d_{31}^1 & d_{32}^1 & d_{33}^1 \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & d_{11}^2 & d_{12}^2 & d_{13}^2 \\
2 & d_{21}^2 & d_{22}^2 & d_{23}^2 \\
3 & d_{31}^2 & d_{32}^2 & d_{33}^2 \\
\end{array}
\]
ARA for Urban Security. Basics

At each cell, a coupled influence diagram

Cell decision making coordinated by constraints on resources
ARA for Urban Security. Police dynamics

At each cell:

- Makes resource allocation $d_{ij}^1$
- Faces a level of delinquency $a_{ij}$ with impact $s_{ij}^1$
- Recovers as much as she can with resources $d_{ij}^2$ with a level of success $s_{ij}^2$
- Gets a utility $U_{ij}^D = U_{ij}^D(d_{ij}^1, s_{ij}^2, d_{ij}^2, v_{ij})$
- Aggregates utilities/Aggregates consequences
ARA for Urban Security. Police dynamics

The assessments required from the defender are

- $p_D(a|d_1)$
- $p_D(s_1|a, d_1)$
- $p_D(s_2|s_1, d_2)$
- $u_D(d_1, s_2, d_2, v)$
ARA for Urban Security. Police dynamics

The assessments required from the defender are

\[
P_D(s_2 | s_1, d_2)
\]

\[
P_D(s_1 | a, d_1)
\]

\[
u_{ij}^D = -\exp(cv_{ij} (1 - \rho)), \quad \rho = 0,1 \text{ si } s_{ij} = 1 \quad y \quad \rho = 0 \text{ si } s_{ij} = 0
\]

\[
P_D(a | d_1)
\]
ARA for Urban Security. Police dynamics

The Police solves sequentially

- At node $U_D$, $u_D(d_1, s_2, d_2, v)$.
- At node $S_2$, compute $\psi_D(d_1, s_1, d_2, v) = \int u_D(d_1, s_2, d_2, v)p_D(s_2|s_1, d_2)ds_2$.
- At node $D_2$, compute $\psi_D(d_1, s_1, v) = \max \sum d_3^{ij} < D_2 \psi_D(d_1, s_1, d_2, v)$ and store optimal allocation.
- At node $S_1$, compute $\psi_D(d_1, v, a) = \int \psi_D(d_1, s_1, v)p_D(s_1|a, d_1)ds_1$.
- At node $A$, compute $\psi_D(d_1, v) = \int \psi_D(d_1, v, a)p_D(a|d_1)da$
- At node $D$, compute $\psi_D(v) = \max \sum d_1^{ij} < D_1 \psi_D(d_1, v)$ and store optimal allocation.

$$\max \sum d_1^{ij} < D_1 \max \sum d_3^{ij} < D_2 \int \int u_D(d_1, s_2, d_2, v)p_D(s_2|s_1, d_2)p_D(s_1|a, d_1)p_D(a|d_1)ds_2ds_1da$$

Augmented probability simulation (Bielza, Muller, DRI, ManSci1999)
ARA for Urban Security. Mob dynamics

At each cell:

- Observes resource allocation $d_{ij}^1$
- Undertakes attack $a_{ij}$, with impact $s_{ij}^1$
- Observes recovery with resources $d_{ij}^2$ with a level of success $s_{ij}^2$
- Gets a utility $U_{ij}^A(a_{ij}, s_{ij}^2, v_{ij})$
- Aggregates utilities/Aggregates consequences
ARA for Urban Security. Mob Dynamics

- The assessments for the Mob are

- We model our uncertainty about them through

\[
\begin{align*}
p_A(d_2|s_1) \\
p_A(s_1|a, d_1) \\
p_A(s_2|s_1, d_2) \\
u_A(a, s_2, v) \\
\end{align*}
\]

\[
\begin{align*}
P_A(d_2|s_1) \\
P_A(s_1|a, d_1) \\
P_A(s_2|s_1, d_2) \\
U_A(a, s_2, v) \\
\end{align*}
\]
ARA for Urban Security. Mob Dynamics

\[
P_A(s_1 | a, d_1) \approx \beta e(\alpha, \beta)
\]

\[
E(P_A(s_1 | a, d_1)) = P_D(s_1 | a, d_1)
\]

\[
\sigma(P_A(s_1 | a, d_1)) = 0.05
\]

\[
P_A(s_2 | s_1, d_2) \approx Be(\alpha, \beta)
\]

\[
E(P_A(s_2 | s_1, d_2)) = P_D(s_1 | a, d_1)
\]

\[
\sigma(P_A(s_2 | s_1, d_2)) = 0.05
\]

\[
s_{ij}^1 = 0 \quad d_{ij}^2 = d_{ij}^1
\]

\[
d_{ij}^2 = a_{ij} \text{ con probabilidad } 0.5
\]

\[
s_{ij}^1 = 1 \quad d_{ij}^2 \geq a_{ij}
\]

\[
d_{ij}^2 = a_{ij} + 1 \text{ con probabilidad } 0.25
\]

\[
d_{ij}^2 = a_{ij} + 2 \text{ con probabilidad } 0.125
\]

\[
P_A(d_2 | s_1, d_1) = \prod_{ij} P_A(d_{ij}^2 | s_{ij}^1, d_{ij}^1)
\]

Generate all feasible allocations, comp probabs, normalise, add some uncertainty

\[
\exp(c(\rho v_{ij} - k a_{ij})), \quad \rho = 0.1 \text{ si } s_{ij} = 1 \quad \text{y} \quad \rho = 0 \text{ si } s_{ij} = 0
\]

\[
c \sim U(0, C)
\]
ARA for Urban Security. Mob dynamics

- We propagate such uncertainty through the scheme

- At node $U_A$, $U_A(a, s_2, v)$.
- At node $S_2$, compute $\Psi_D(a, s_1, d_2, v) = \int U_A(a, s_2, v) P_A(s_2|s_1, d_2) ds_2$.
- At node $D_2$, compute $\Psi_D(a, s_1, v) = \int \Psi_D(a, s_1, d_2, v) P_A(d_2|s_1) dd_2$
- At node $S_1$, compute $\Psi_D(d_1, v, a) = \int \Psi_D(a, s_1, v) P_A(s_1|a, d_1) ds_1$.
- At node $A$, compute $\Psi_D(d_1, v) = \max \sum_{a^{ij} \leq A} \Psi_D(d_1, v, a)$ and stores optimal random allocation $A^*(d_1, v)$.

$$\int_{\{x \leq a\}} p_D(A = x|d_1, v) dx = Pr(A^*(d_1, v) \leq a)$$
ARA for Urban Security. Mob dynamics

• We can estimate it by Monte Carlo

• Sample from

\[ F = \{ U_A(a, s_2, v), P_A(s_1 | a, d_1), P_A(d_2 | s_1), P_A(s_2 | s_1, d_2) \} \]

• Solve for maximum expected utility attack (EU computed in one step+ augmented prob. Simulation)

\[
\hat{P}_D(A \leq a | d_1) = \frac{\# \{ A_k^*(v, d_1) \leq a \}}{n}
\]
Discussion

• SECONOMICS FP7 project (Feb 2012)
  • UK energy grid
  • Ankara airport
  • Barcelona underground

• Forthcoming proposal on urban security
Discussion

- Multiple Defenders to be coordinated (risk sharing).
- Multiple Attackers possibly coordinated
- Various types of resources (people, cars, cameras,...)
- Various types of delinquency (terrorism, thefts, drugs,...)
- Multivalued cells.
- The perception of security (concern analysis)
- Multiperiod planning
- Time and space effects (Displacement of delicts)
- Insurance
- Private security
- Structural measures
- Sensor info to update dynamically allocations