Empirical Comparisons of Descriptive Adversary Models in Stackelberg Security Games

Jinshu Cui, Richard S. John
Department of Psychology
Center for Risk and Economic Analysis of Terrorism Events (CREATE)
University of Southern California

AAAI Spring Symposium on Applied Computation Game Theory
Palo Alto, CA
March 23-25, 2015
Acknowledgement

• Grant # ARO MURI (P59733-NS-MUR), Scalable, Stochastic and Spatiotemporal Game Theory for Real-World Human Adversarial Behavior

• TEAMCORE at USC
Adversary Decision Making in a SSG setting

• Stackelberg Security Games (SSG)
• Security resource allocation literature has focused on generating algorithms that are optimal and efficient for defenders (prescriptive)
  – Adversary Modeling
    • BRQR (Yang et al., 2012), SUQR (Nguyen et al., 2013)
  – Robust Methods
    • COBRA (Pita et al., 2009), MATCH (Pita et al., 2012)
• Little has been done to investigate how comparable those models are capturing adversary choices (descriptive)
• Evaluate Adversary Choices varying Utility Functions
Risk Attitude

- Power utility function
- The curve of utility function \( w^\alpha \) is concave if risk averse (\( \alpha < 1 \)), linear if risk neutral (\( \alpha = 1 \)), and convex if risk seeking (\( \alpha > 1 \))

- Model
  \[ U_{A_i} = p_i P_{A_i}^\alpha + (1 - p_i) R_{A_i}^\alpha \]
**Lens Model** (Brunswik, 1952; Hammond, 1955)

- Framework for modeling judge’s prediction based on observable cues and to help decision maker reach better judgments
- \( Y_s' = a + \sum_{i=1}^{k} b_i X_i \)

- Cues in SSG for an attacker: \( p(\text{guard}) \), reward, penalty, defender’s reward and penalty
- Models (Nguyen et al., 2013)
  - \( Y_s' = w_1 p_i + w_2 P_{Ai} + w_3 R_{Ai} \)
  - \( Y_s' = w_1 p_i + w_2 P_{Ai} + w_3 R_{Ai} + w_4 P_{Di} + w_5 R_{Di} \)
Multi-Attribute Utility Theory (MAUT) (Keeney & Raiffa, 1976)

- Framework handling tradeoffs among multiple objectives for making decisions
  
  \[ U(x_1, x_2, \ldots, x_m) = \sum_{i=1}^{m} k_i U_i(x_i) \]

  \[ \sum_{i=1}^{m} k_i = 1, \quad 0 \leq U(x_1, x_2, \ldots, x_m) \leq 1, \quad U_i(x_i) = \frac{x_i - \text{worst}}{\text{best} - \text{worst}} \]

- Target selection
  - Objectives: maximize probability of success, maximize EV (attacker), minimize EV (defender)

- Model
  
  \[ U_{Ai} = w_1 p_i + w_2 EV_{Ai} + w_3 EV_{Di} \]
  
  \[ = w_1 p_i + w_2 [p_i P_{Ai} + (1 - p_i) R_{Ai}] + w_3 [p_i P_{Di} + (1 - p_i) R_{Di}] \]
Models

• Attacker’s expected value
  - $U_{A_i} = p_i P_{A_i} + (1 - p_i)R_{A_i}$

• Accounting for risk attitude
  - $U_{A_i} = p_i P_{A_i}^\alpha + (1 - p_i)R_{A_i}^\alpha$

• Lens model
  - $U_{A_i} = w_1 p_i + w_2 P_{A_i} + w_3 R_{A_i}$
  - $U_{A_i} = w_1 p_i + w_2 P_{A_i} + w_3 R_{A_i} + w_4 P_{D_i} + w_5 R_{D_i}$

• Lens model accounting for risk attitude
  - $U_{A_i} = w_1 p_i + w_2 P_{A_i}^\alpha + w_3 R_{A_i}^\alpha$
  - $U_{A_i} = w_1 p_i + w_2 (P_{A_i}^\alpha + R_{A_i}^\alpha) + w_3 (P_{D_i} + R_{D_i})$

• Multi-attribute utility model
  - $U_{A_i} = w_1 p_i + w_2 EV_{A_i} + w_3 EV_{D_i}$
Probabilistic Choice

• Luce’s Choice Axiom (Luce, 1959)
  – Probabilistic choice
  – \( P_S(x) = \frac{v(x)}{\sum_{y \in S} v(y)} \)

• Quantal Response Equilibrium (McKelvey & Palfrey, 1995 & 1998)
  – \( P_S(x) = \frac{e^{\lambda u(x)}}{\sum_{y \in S} e^{\lambda u(y)}}, \lambda \to \infty \), player maximizes expected utility
  • \( U_{A_i}(x_i) = x_i P_{A_i} + (1 - x_i) R_{A_i} \) (Yang et al., 2012)
  • \( U_{A_i}(x_i) = w_1 x_i + w_2 P_{A_i} + w_3 R_{A_i} \) (Nguyen et al., 2013)

• Comparing adversary models (softmax)
  – \( P_S(x) = \frac{e^{u(x)/\lambda}}{\sum_{y \in S} e^{u(y)/\lambda}}, \lambda \to 0^+, \) player maximizes expected utility
## Models

<table>
<thead>
<tr>
<th>Category</th>
<th>Model</th>
<th>Abbreviation</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacker’s expected value models</td>
<td>Attacker’s expected value model</td>
<td>EV</td>
<td>( q_i = \frac{e^{[p_i P_{A_i} + (1-p_i)R_{A_i}]/\lambda}}{\sum_{k \in T} e^{[p_k P_{A_k} + (1-p_k)R_{A_k}]/\lambda}} )</td>
</tr>
<tr>
<td>Attacker’s expected utility model accounting</td>
<td>Attacker’s expected utility model accounting</td>
<td>EU–( \alpha )</td>
<td>( q_i = \frac{e^{[p_i P_{A_i} + (1-p_i)R_{A_i}]/\lambda}}{\sum_{k \in T} e^{[p_k P_{A_k} + (1-p_k)R_{A_k}]/\lambda}} )</td>
</tr>
<tr>
<td>Lens models</td>
<td>Lens model – three parameters</td>
<td>Lens–3</td>
<td>( q_i = \frac{e^{(w_1 P_{A_i} + w_2 P_{A_k} + w_3 R_{A_i})/\lambda}}{\sum_{k \in T} e^{(w_1 P_{A_i} + w_2 P_{A_k} + w_3 R_{A_k})/\lambda}} )</td>
</tr>
<tr>
<td>Lens models</td>
<td>Lens model – five parameters</td>
<td>Lens–5</td>
<td>( q_i = \frac{e^{(w_1 P_{A_i} + w_2 P_{A_k} + w_3 R_{A_i} + w_4 P_{D_i} + w_5 R_{D_i})/\lambda}}{\sum_{k \in T} e^{(w_1 P_{A_i} + w_2 P_{A_k} + w_3 R_{A_i} + w_4 P_{D_i} + w_5 R_{D_i})/\lambda}} )</td>
</tr>
<tr>
<td>Lens models accounting for risk attitude</td>
<td>Lens model – three attributes accounting for risk attitude</td>
<td>Lens–3–( \alpha )</td>
<td>( q_i = \frac{e^{(w_1 P_{A_i} + w_2 P_{A_k} + w_3 R_{A_i})/\lambda}}{\sum_{k \in T} e^{(w_1 P_{A_i} + w_2 P_{A_k} + w_3 R_{A_i})/\lambda}} )</td>
</tr>
<tr>
<td>Lens models accounting for risk attitude</td>
<td>Lens model – five attributes accounting for risk attitude</td>
<td>Lens–5–( \alpha )</td>
<td>( q_i = \frac{e^{(w_1 P_{A_i} + w_2 P_{A_k} + w_3 R_{A_i} + w_4 P_{D_i} + w_5 R_{D_i})/\lambda}}{\sum_{k \in T} e^{(w_1 P_{A_i} + w_2 P_{A_k} + w_3 R_{A_i} + w_4 P_{D_i} + w_5 R_{D_i})/\lambda}} )</td>
</tr>
<tr>
<td>Multi-attribute utility model</td>
<td>Multi-attribute utility model</td>
<td>MAU</td>
<td>( q_i = \frac{e^{[w_1 P_{A_i} + w_2 P_{A_k} + (1-p_i)R_{A_i} + w_3 p_i P_{D_i} + (1-p_i)R_{D_i})/\lambda}}{\sum_{k \in T} e^{[w_1 P_{A_i} + w_2 P_{A_k} + (1-p_i)R_{A_i} + w_3 p_i P_{D_i} + (1-p_i)R_{D_i})/\lambda}} )</td>
</tr>
</tbody>
</table>
The Guards and The Treasure

- 8 gates protected by 3 guards
- Gate attacked not guarded, attacker receives a reward and defender receives a penalty
- Gate attacked guarded, attacker receives a penalty and defender receives a reward
Experiment I (Yang et al., 2012)

• Design overview
  – 7 payoff structures, 10 defender strategies
  – each played 40 games

• Participants
  – 102 participants
  – 40 (39%) from the US, 48 (47%) from India
  – Age ranged from 18 to 74, median age 30
  – 36 (35%) female

• Procedure
  – Feedback given after finishing all 40 games
  – Paid with base rate $0.50 and a bonus of $0.01 multiplied by the total points received from the 40 games
Experiment II (Pita et al., 2012)

- **Design overview**
  - 104 payoff structures, 2 defender strategies
  - each played 25 games

- **Participants**
  - 653 participants
  - All from the US
  - Age ranged from 18 to 68, median age 26
  - 272 (42%) female

- **Procedure**
  - Feedback following each round
  - Paid with base rate $1.50 and a bonus of $0.15 multiplied by the total points received from 4 randomly selected games
Experiment III (Nguyen et al., 2013)

- **Design overview**
  - 22 payoff structures, 4 defender strategies
  - each played 25 to 33 games

- **Participants**
  - 294 participants
  - All from the US
  - Age ranged from 18 to 60, median age 26
  - 89 (30%) female

- **Procedure**
  - Feedback given after finishing all games played
  - Paid with base rate $1.50 and a bonus of $0.15 multiplied by the total points received from 3 randomly selected games
Results – Nomothetic Analysis

• Maximum Likelihood Estimation over all games in an experiment (R, optim)

\[ L = \prod_{i=1,2,\ldots,N} q_i(x_i) \]
\[ \log(L) = \log \prod_{i=1,2,\ldots,N} q_i(x_i) \]
\[ \max \log L \quad \text{s.t.} \quad \lambda \geq 0 \text{ and/or } \alpha > 0 \]

• Akaike Information Criterion (AIC) (Akaike, 1974)

\[ \text{AIC} = -2 \log L + 2k \]

– An estimate of the distance between the fitted model and the unknown true mechanism that generated the observed data (Burnham & Anderson, 2002)

– Tradeoff between goodness of fit and the complexity of the model which has a built-in penalty for models with more parameters

– The model with the minimum AIC is the best among the alternatives, however, AIC cannot tell the quality of the model in an absolute sense
Results – Nomothetic Analysis

<table>
<thead>
<tr>
<th>Model</th>
<th>Experiment I</th>
<th></th>
<th>Experiment II</th>
<th></th>
<th>Experiment III</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AIC</td>
<td>parameters estimation</td>
<td>AIC</td>
<td>parameters estimation</td>
<td>AIC</td>
<td>parameters estimation</td>
</tr>
<tr>
<td>EV</td>
<td>15036</td>
<td>(\lambda=0.09)</td>
<td>33334</td>
<td>(\lambda=0.20)</td>
<td>60674</td>
<td>(\lambda=0.08)</td>
</tr>
<tr>
<td>EU−(\alpha)</td>
<td>15012</td>
<td>(\lambda=0.08, \alpha=0.86)</td>
<td>31065</td>
<td>(\lambda=0.08, \alpha=0.33)</td>
<td>59169</td>
<td>(\lambda=0.06, \alpha=0.7)</td>
</tr>
<tr>
<td>Lens−3</td>
<td>14670</td>
<td>(\lambda=0.05, w=(-0.32,0.44,0.24))</td>
<td>25445</td>
<td>(\lambda=0.07, w=(-0.16,0.18,0.67))</td>
<td>52014</td>
<td>(\lambda=0.04, w=(-0.42,0.35,0.23))</td>
</tr>
<tr>
<td>Lens−5</td>
<td>14658</td>
<td>(\lambda=0.05, w=(-0.30,0.43,0.23,0.02,0.02))</td>
<td>22592</td>
<td>(\lambda=0.04, w=(-0.44,-0.01,0.04,0.30,0.21))</td>
<td>43265</td>
<td>(\lambda=0.02, w=(-0.31,0.26,0.17,0.04,0.20))</td>
</tr>
<tr>
<td>Lens−3−(\alpha)</td>
<td>14645</td>
<td>(\lambda=0.05, w=(-0.32,0.35,0.34), \alpha=1.47)</td>
<td>25159</td>
<td>(\lambda=0.07, w=(-0.09,0.11,0.80), \alpha=1.86)</td>
<td>51929</td>
<td>(\lambda=0.04,w=(-0.42,0.30,0.28), \alpha=1.25)</td>
</tr>
<tr>
<td>Lens−5−(\alpha)</td>
<td>14624</td>
<td>(\lambda=0.08, w=(-0.46,0.5,0.04), \alpha=1.51)</td>
<td>23228</td>
<td>(\lambda=0.05, w=(-0.58,0.07,0.35), \alpha=0.47)</td>
<td>48121</td>
<td>(\lambda=0.04,w=(-0.45,0.32,0.18), \alpha=1.32)</td>
</tr>
<tr>
<td>MAU</td>
<td>14973</td>
<td>(\lambda=0.08, w=(-0.06,0.84,0.10))</td>
<td>26540</td>
<td>(\lambda=0.07, w=(-0.66,-0.01,0.33))</td>
<td>45335</td>
<td>(\lambda=0.03, w=(-0.32,0.39,0.29))</td>
</tr>
</tbody>
</table>

- Preference on soft targets (neglect of consequence)
  - EV and EU−\(\alpha\) always worse than other alternatives
- Sensitive to defender’s attributes
  - Utility functions with defender’s attributes were better than utility function without defender’s attributes; lens−5−\(\alpha\) was best for experiment I and lens-5 was the best for experiments II and III
- Consistency with maximizing utility function (\(\lambda \to 0^+\))
Results – Idiographic Analysis

- Individual differences in strategy selection
- Maximum Likelihood Estimation over all games played by an individual in an experiment (R, optim)
  \[
  AIC_c = -2 \log L + 2k \left( \frac{N}{N-k-1} \right), \quad N/k<40
  \]
- Akaike’s weights \((w_i)\) (Bozdogan, 1987; Burnham & Anderson, 2001, 2002):
  - the probability that model \(i\) is the best model given a sample of data and \(N\) alternative models.
  \[
  w_i = \frac{\exp(-0.5\Delta_i)}{\sum_{r=1}^{N} \exp(-0.5\Delta_r)}, \quad \text{where} \quad \Delta_i = AIC_i - AIC_{\text{min}}
  \]
  - \(w_i > 0.9\) is an indicator that model \(i\) is the best model among the \(N\) models (Anderson, et al., 2001)
Results – Idiographic Analysis

Number of Times Model i has Minimum AICc for Experiments I, II and III

<table>
<thead>
<tr>
<th>Model</th>
<th>Experiment I</th>
<th>Experiment II</th>
<th>Experiment III</th>
</tr>
</thead>
<tbody>
<tr>
<td>EV</td>
<td>7</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>EU–α</td>
<td>15</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>Lens–3</td>
<td>32</td>
<td>44</td>
<td>42</td>
</tr>
<tr>
<td>Lens–5</td>
<td>5</td>
<td>331</td>
<td>125</td>
</tr>
<tr>
<td>Lens–3–α</td>
<td>7</td>
<td>18</td>
<td>13</td>
</tr>
<tr>
<td>Lens–5–α</td>
<td>15</td>
<td>50</td>
<td>62</td>
</tr>
<tr>
<td>MAU</td>
<td>21</td>
<td>193</td>
<td>51</td>
</tr>
<tr>
<td>Total</td>
<td>102</td>
<td>653</td>
<td>294</td>
</tr>
</tbody>
</table>

Number of Times Model i is the best model for Experiments I, II and III

<table>
<thead>
<tr>
<th>Model</th>
<th>Experiment I</th>
<th>Experiment II</th>
<th>Experiment III</th>
</tr>
</thead>
<tbody>
<tr>
<td>EV</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EU–α</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Lens–3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Lens–5</td>
<td>1</td>
<td>252</td>
<td>54</td>
</tr>
<tr>
<td>Lens–3–α</td>
<td>0</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Lens–5–α</td>
<td>0</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>MAU</td>
<td>8</td>
<td>121</td>
<td>8</td>
</tr>
<tr>
<td>Total</td>
<td>13</td>
<td>380</td>
<td>74</td>
</tr>
</tbody>
</table>

Models with most minAICc:
• Experiment I: lens-3 (31%)
• Experiment II: lens-5 (51%)
• Experiment III: lens-5 (43%)

• 13%, 58%, 25% of subjects in three experiments have best models
• Among those who have best models, MAU is the best model for experiment I (62%), lens-5 is the best model for experiments II (66%) and III (73%)
Conclusion

- EV or EU does not work
  - consider probability of success
- Sensitive to defender’s payoffs
  - give up own rewards
- Using different utility functions to compute the “best” choice
  - differentiate adversaries using different strategies
    - gender, age, education, nationality
    - gender, education, and age do not perform as an indicator of model selection
    - no best model for Americans in experiment I, while lens-3 is the best model for Indians
References


Thank you!