A Robust Approach for Network Protection Games [1]

Melike Baykal-Gürsoy

Department of I&S Engineering, CAIT
Rutgers University

SAMSI - Games and Decisions in Reliability and Risk Workshop
May 16 - 20, 2016, NC

Joint work with A. Yolmeh

[1] This material is based upon work supported by the National Science Foundation under Grant Numbers CMMI-1436288 and CMMI-1435778.

Outline

Network Protection Under Uncertainty

- Sources of uncertainty
  - Parameter Uncertainty
  - Attack type uncertainty
- How to deal with uncertainty
  - Bayesian Approach
  - Robust Approach

Problem Description

- Static Single Defender - Single Adversary Zero-Sum game,
- N potential targets,
- $\tilde{C}_i$, uncertain asset value of site i with support $\left[\underline{C}_i, \overline{C}_i\right]$,
- If the defender defends site i and the adversary attacks site $j, j \neq i$, a successful attack on site j will be launched.
  Adversary's payoff: $\tilde{C}_j$.
- If both players choose the same site i, the attack will be detected with probability d_i,
  Adversary's payoff: $\left(1 - \tilde{d}_j\right) \tilde{C}_j$.

Problem Description

- The probability of detection, $\tilde{d}_i$, is also uncertain with support $\left[\underline{d}_i, \overline{d}_i\right]$,
- Attack type uncertainty:
  - Maximum damage adversary: The MD adversary aims at maximizing his/her expected payoff.
  - Infiltration adversary: all sites are the same and the aim is to increase the probability of a successful attack regardless of its value.

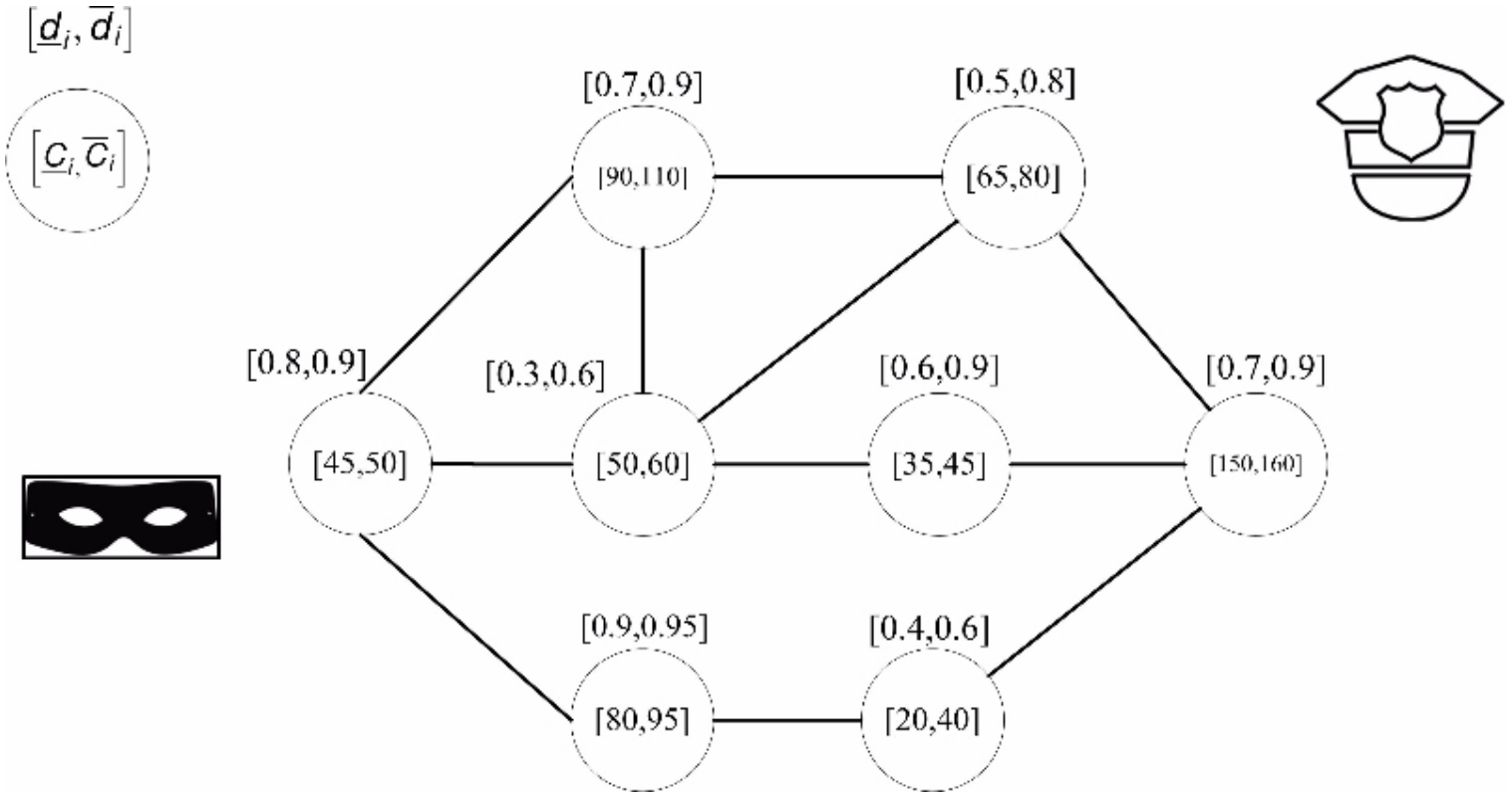

Figure: Example of a maximum damage game

RUTGERS

Notations and Assumptions

- N: number of nodes,
- $\tilde{C}_i$: value of assets at node i, $\forall i = 1, 2, \ldots, N$,
- $\tilde{d}_i \in (0, 1)$: detection probability at node i,

Decision Variables

- $\boldsymbol{x} = (x_1, x_2, \ldots, x_N)$: strategy of the defender, $x_i \geq 0 \ \forall i, \ \sum_{i=1}^{N} x_i = 1$,
- $\boldsymbol{y} = (y_1, y_2, \ldots, y_N)$: strategy of the adversary, $y_i \geq 0 \ \forall i, \ \sum_{i=1}^{N} y_i = 1$,

Performance Measure

- $R_i(x_i, y_i)$: damage to node i under x_i and y_i,

Payoff to the Adversary: $R_i(x_i, y_i) = (1 - \tilde{d}_i x_i)\tilde{C}_i y_i$.

RUTGERS

Maximum Damage Game

Payoff Matrix

$$R = \begin{array}{c} i \setminus j \\ 1 \\ 2 \\ \vdots \\ N \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & \cdots & N \end{array} \\ \begin{pmatrix} -(1-\tilde{d}_1)\tilde{C}_1 & -\tilde{C}_2 & \cdots & -\tilde{C}_N \\ -\tilde{C}_1 & -(1-\tilde{d}_2)\tilde{C}_2 & \cdots & -\tilde{C}_N \\ \vdots & \vdots & \ddots & \vdots \\ -\tilde{C}_1 & -\tilde{C}_2 & \cdots & -(1-\tilde{d}_N)\tilde{C}_N \end{pmatrix} \end{array},$$

Defender's Payoff

$$u_D^1(x,y) = \min_{\substack{\tilde{d}_i \in [\underline{d}_i, \overline{d}_i] \\ \tilde{C}_i \in [\underline{C}_i, \overline{C}_i]}} \left(-\sum_{i=1}^{n} \left(1 - \tilde{d}_i x_i\right) \tilde{C}_i y_i \right) = -\sum_{i=1}^{n} \left(1 - \underline{d}_i x_i\right) \overline{C}_i y_i$$

Maximum Damage Game

Adversary's Payoff

$$u_A^1(x,y) = \min_{\substack{\tilde{d}_i \in [\underline{d}_i, \overline{d}_i] \\ \tilde{C}_i \in [\underline{C}_i, \overline{C}_i]}} \left(\sum_{i=1}^{n} \left(1 - \tilde{d}_i x_i\right) \tilde{C}_i y_i \right) = \sum_{i=1}^{n} \left(1 - \overline{d}_i x_i\right) \underline{C}_i y_i$$

RUTGERS

Nash Equilibrium

$(\boldsymbol{x}_*, \boldsymbol{y}_*)$ is a Nash equilibrium for the non-zero-sum game iff

$$u_D^1(\boldsymbol{x}, \boldsymbol{y}_*) \leq u_D^1(\boldsymbol{x}_*, \boldsymbol{y}_*) \text{ and } u_A^1(\boldsymbol{x}_*, \boldsymbol{y}) \leq u_A^1(\boldsymbol{x}_*, \boldsymbol{y}_*) \text{ for any } (\boldsymbol{x}, \boldsymbol{y}).$$

Assume

$$\underline{C}_1 > \underline{C}_2 > \cdots > \underline{C}_N.$$

Theorem

The game has the unique equilibrium $(\boldsymbol{x}_*, \boldsymbol{y}_*)$ *with* $k \in \{1, \ldots, N\}$ *such that*

$$\varphi_k \leq 1 < \varphi_{k+1},$$

where $\{\varphi_i\}$ *is a strictly increasing sequence defined as*

$$\varphi_i = \sum_{j=1}^{i} (\underline{C}_j - \underline{C}_i)/\overline{d}_j \underline{C}_j, \text{ for } i \in \{1, \ldots, N\}$$

and $\varphi_{N+1} = \infty$.

Theorem cont'd

Defender's strategy

$$x_{*i} = \begin{cases} \dfrac{1/(\overline{d}_i \underline{C}_i)}{\sum_{j=1}^{k} 1/(\overline{d}_j \underline{C}_j)} \left(1 - \sum_{j=1}^{k} \dfrac{\underline{C}_j - \underline{C}_i}{\overline{d}_j \underline{C}_j}\right), & i \le k, \\ 0, & i \ge k+1. \end{cases}$$

Adversary's strategy

$$y^1_{*i} = \begin{cases} \dfrac{1/(\underline{d}_i \overline{C}_i)}{\sum_{j=1}^{k} 1/(\underline{d}_j \overline{C}_j)}, & i \le k, \\ 0, & i \ge k+1. \end{cases}$$

Remark

Remark 1

If all the nodes have the same detection probability, i.e. $\overline{d}_i = d, \ \forall i$, then x_i's are decreasing in i, i.e. $x_1 > x_2 > \ldots > x_k$.

$\underline{C}_i = \underline{C}, \overline{C}_i = \overline{C}$

Defender's Payoff

$$u_D^2(x,y) = \sum_{i=1}^{n} (1 - \underline{d}_i x_i)\, \overline{C}_i y_i$$

Adversary's Payoff

$$u_A^2(x,y) = \underline{C} \sum_{i=1}^{n} (1 - \overline{d}_i x_i)\, y_i$$

Theorem

The Infiltration/Harassment game has the unique equilibrium $(\boldsymbol{x}_*, \boldsymbol{y}_*)$

$$x_{*i} = \frac{1/\overline{d}_i}{\sum_{j=1}^{N} 1/\overline{d}_j}, \quad y_{*i}^2 = \frac{1/(\underline{d}_i \overline{C}_i)}{\sum_{j=1}^{N} 1/(\underline{d}_j \overline{C}_j)}, \quad i = 1, \ldots, N.$$

Remark

Remark 2

NE does not depend on the value of $\overline{C}$ or $\underline{C}$. This is natural because for the infiltrating adversary all sites are equal and the value of these sites does not affect his behavior. Moreover, the defender has his own valuation of the sites independent of $\overline{C}$ and $\underline{C}$.

Uncertainty about the Attack Type

Defender does not know the adversary's goal:

(1) Maximum Damage Attack with probability q

(2) Harassment/Infiltration Attack with probability $1-q$

Adversary's strategies towards each goal: $\boldsymbol{y}^1$ and $\boldsymbol{y}^2$ respectively

The expected payoff to the defender under $\boldsymbol{x}$, and $(\boldsymbol{y}^1, \boldsymbol{y}^2)$

$$u_D(\boldsymbol{x}, (\boldsymbol{y}^1, \boldsymbol{y}^2)) = q u_D^1(\boldsymbol{x}, \boldsymbol{y}^1) + (1-q) u_D^2(\boldsymbol{x}, \boldsymbol{y}^2).$$

Payoff to type k Adversary

$u_A^k(\boldsymbol{x}, \boldsymbol{y}^k)$ for $k = 1, 2$

Bayesian Equilibrium for the Incomplete Information Game

Theorem

The following strategy pair is a Bayesian Equilibrium: Let k be an integer such that: $\phi_k \leq 1 < \phi_{k+1}$ *where* $\phi_i = \sum_{j=1}^{i} \frac{\underline{C}_j - \underline{C}_i}{\overline{d}_j \underline{C}_j}$

Let m be an integer such that: $\psi_{m-1} < q \leq \psi_m$ *where* $\psi_i = \frac{\left(\sum_{j=1}^{i} \frac{1}{\underline{d}_j \overline{C}_j}\right)}{\left(\sum_{j=1}^{n} \frac{1}{\underline{d}_j \overline{C}_j}\right)}$

Theorem cont'd

If $m \leq k$ then:

$$x_j = \begin{cases} \dfrac{1+\sum_{j=1}^{m} \frac{\underline{c}_1 - \underline{c}_j}{\underline{c}_j \overline{d}_j} + \frac{\underline{c}_1 - \underline{c}_m}{\underline{c}_m} \sum_{j=m+1}^{n} \frac{1}{\overline{d}_j}}{\left(\sum_{j=1}^{m} \frac{\underline{c}_1 \overline{d}_1}{\underline{c}_j \overline{d}_j} + \frac{\underline{c}_1 \overline{d}_1}{\underline{c}_m} \sum_{j=m+1}^{n} \frac{1}{\overline{d}_j} \right)}, & j = 1, \\ \dfrac{\underline{c}_1 \overline{d}_1}{\underline{c}_j \overline{d}_j} x_1 - \dfrac{\underline{c}_1 - \underline{c}_j}{\underline{c}_j \overline{d}_j}, & 2 \leq j \leq m, \\ \dfrac{x_m \overline{d}_m}{\overline{d}_j}, & j > m \end{cases}$$

Theorem cont'd

If $m \leq k$ then:

$$y_j^2 = \begin{cases} 0, & j < m, \\ \dfrac{\left(\sum_{j=1}^{m} \frac{1}{\underline{d}_j \overline{c}_j}\right) - q\left(\sum_{j=1}^{n} \frac{1}{\underline{d}_j \overline{c}_j}\right)}{(1-q)\left(\sum_{j=1}^{n} \frac{1}{\underline{d}_j \overline{c}_j}\right)}, & j = m, \\ \dfrac{\frac{1}{\underline{d}_j \overline{c}_j}}{(1-q)\left(\sum_{j=1}^{n} \frac{1}{\underline{d}_j \overline{c}_j}\right)}, & j > m \end{cases}$$

Theorem cont'd

If $m \leq k$ then:

$$y_j^1 = \begin{cases} \frac{\underline{d}_{j+1}\overline{C}_{j+1}}{\underline{d}_j\overline{C}_j} y_{j+1}^1, & j < m-1, \\ \frac{\underline{d}_m\overline{C}_m}{\underline{d}_{m-1}\overline{C}_{m-1}} \left(\frac{q y_m^1 + (1-q) y_m^2}{q} \right), & j = m-1, \\ \frac{(1-q)}{q} \left(\frac{\underline{d}_{m+1}\overline{C}_{m+1}}{\underline{d}_m\overline{C}_m} y_{m+1}^2 - y_m^2 \right), & j = m \\ 0, & j > m \end{cases}$$

Theorem cont'd

if $m > k$ then:

$$x_j = \begin{cases} \dfrac{\frac{1}{\overline{d}_j \underline{C}_j}}{\sum_{i=1}^{k} \frac{1}{\overline{d}_i \underline{C}_i}} \left(1 - \sum_{i=1}^{k} \dfrac{\underline{C}_i - \underline{C}_j}{\overline{d}_i \underline{C}_i}\right), & j \le k, \\ 0, & j > k \end{cases}$$

$$y_j^1 = \begin{cases} \dfrac{\frac{1}{\underline{d}_j \overline{C}_j}}{\sum_{l=1}^{k} \frac{1}{\underline{d}_l \overline{C}_l}}, & j \le k \\ 0, & j > k \end{cases}$$

$$\sum_{j=k+1}^{n} y_j^2 = 1, \quad y_i^2 < \frac{q}{(1-q)} \left(\frac{\frac{1}{\underline{d}_i \overline{C}_i}}{\sum_{l=1}^{k} \frac{1}{\underline{d}_l \overline{C}_l}} \right), \forall i > k,$$

Remark

Remark 3

- Similar to the infiltration game, NE does not depend on the value of $\overline{C}$ or $\underline{C}$.
- For the case $m > k$, there is a continuum of NE strategies for the infiltrating adversary.

Numerical Example

Table: Expected damage data for the 10 urban areas with the highest losses

Urban Area	Property loss ($million)	Fatalities & Injuries	Air Departures (Major & Minor Airports)
NY	413	5350	23599
CH	115	1212	39949
SF	57	472	19142
WDC	36	681	17253
LA	34	402	28816
PHL	21	199	13640
BSTN	18	225	11625
HSTN	11	160	20979
NW	7.3	74	12827
STL	6.7	88	13578
Total	719	8863	201408

Example cont'd

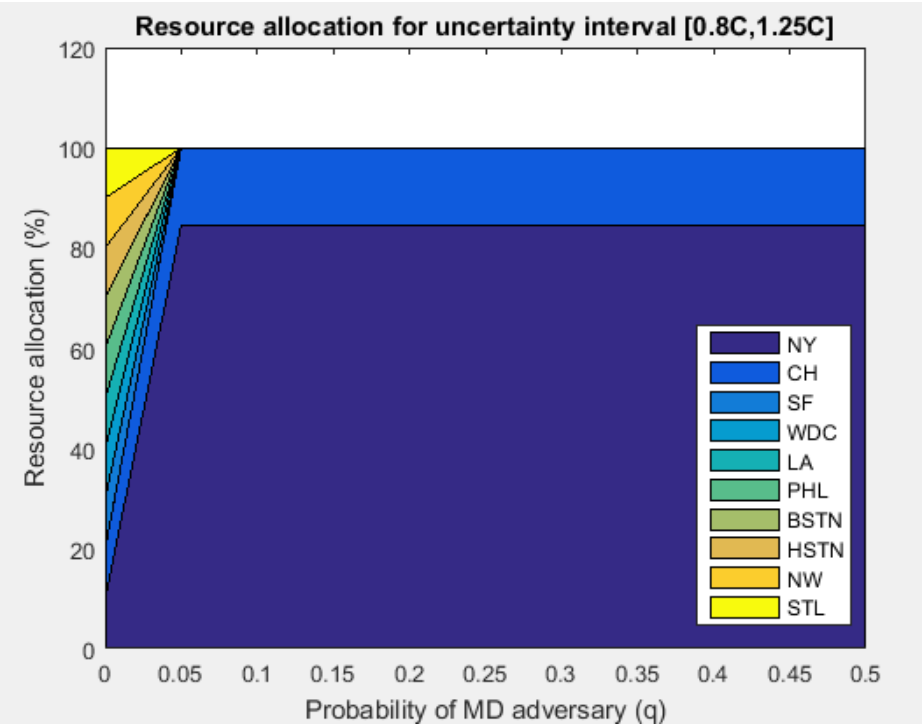

Figure: Allocation of defensive resources to reduce monetary losses

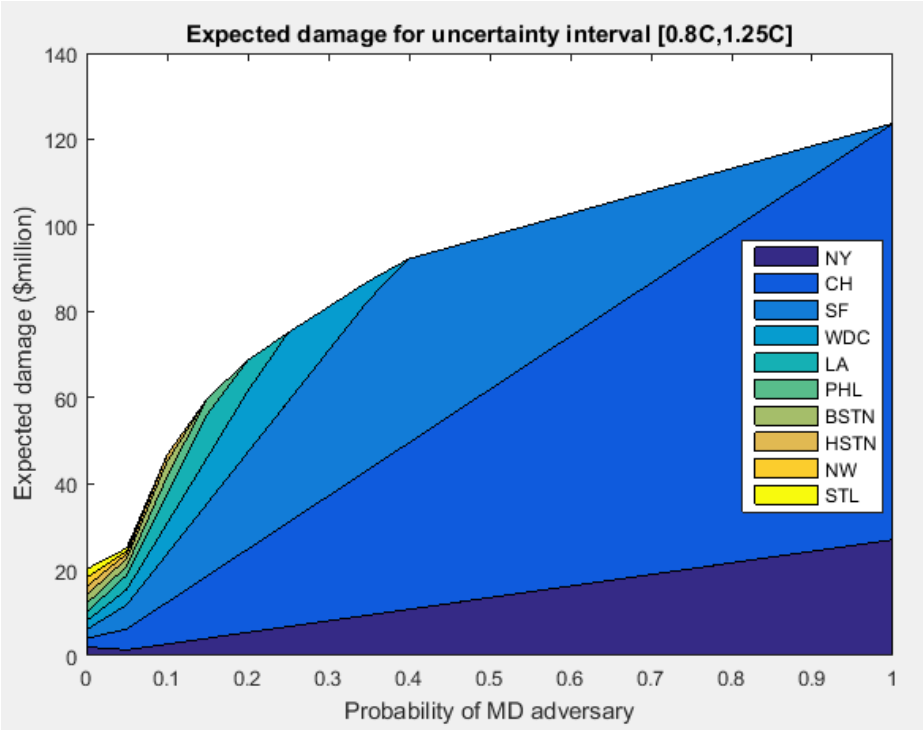

Figure: Expected damage under monetary considerations

Example cont'd

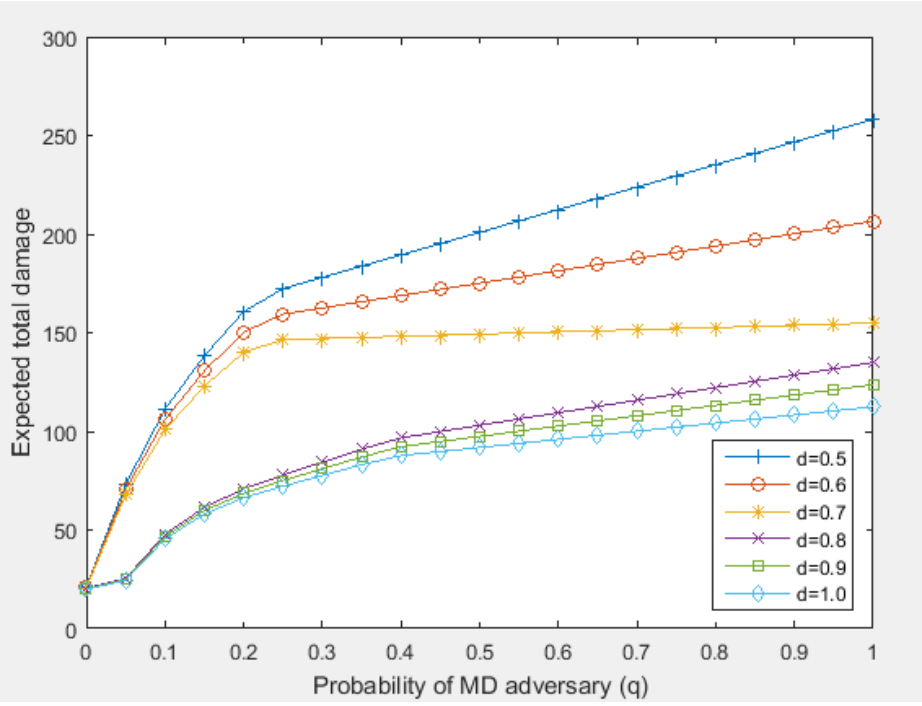

Figure: Expected damage under different detection probabilities

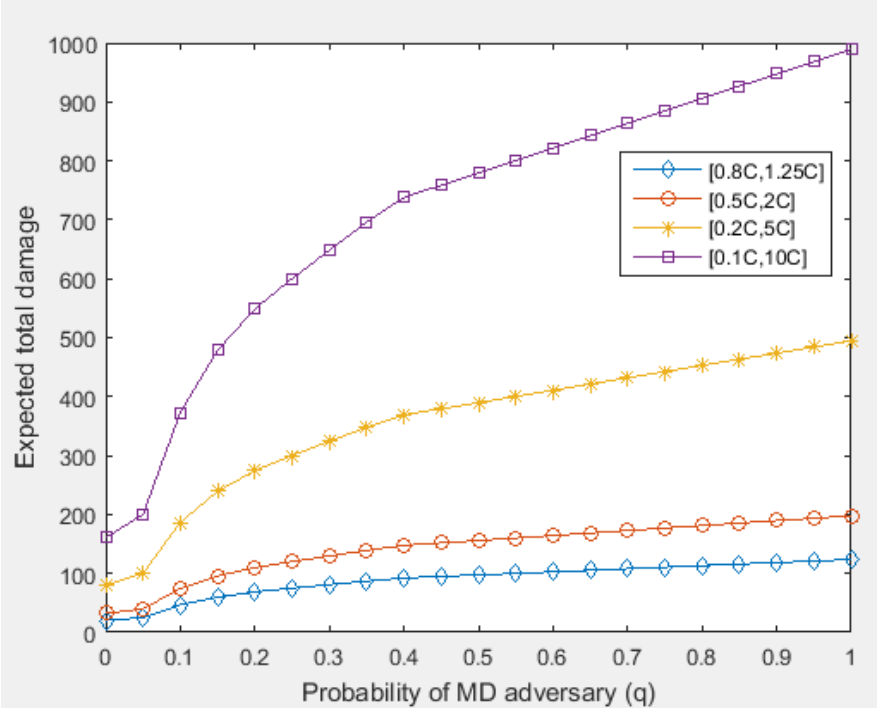

Figure: Expected damage under different uncertainty ranges

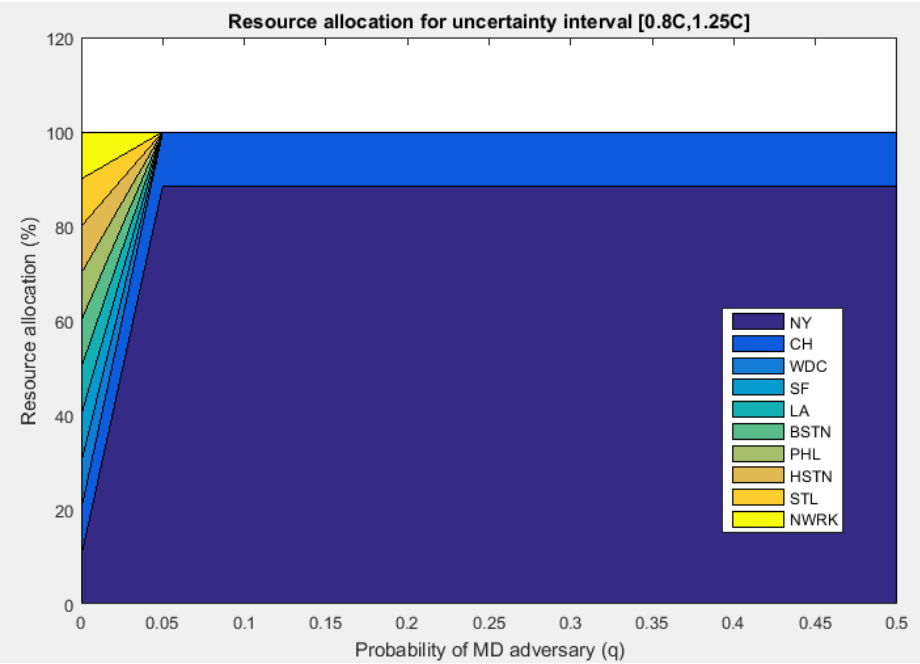

Figure: Allocation of defensive resources to reduce mortality

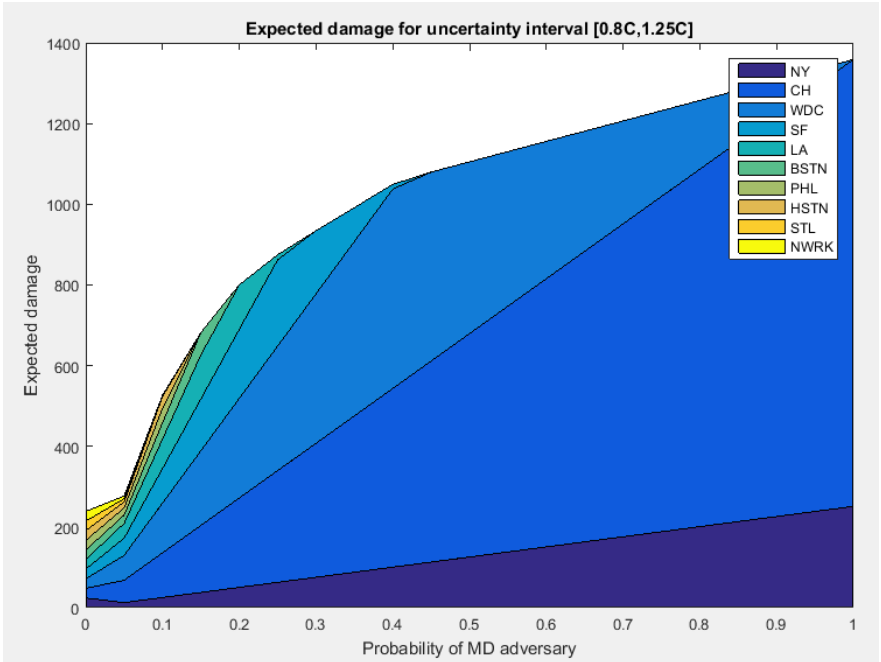

Figure: Expected damage under mortality considerations

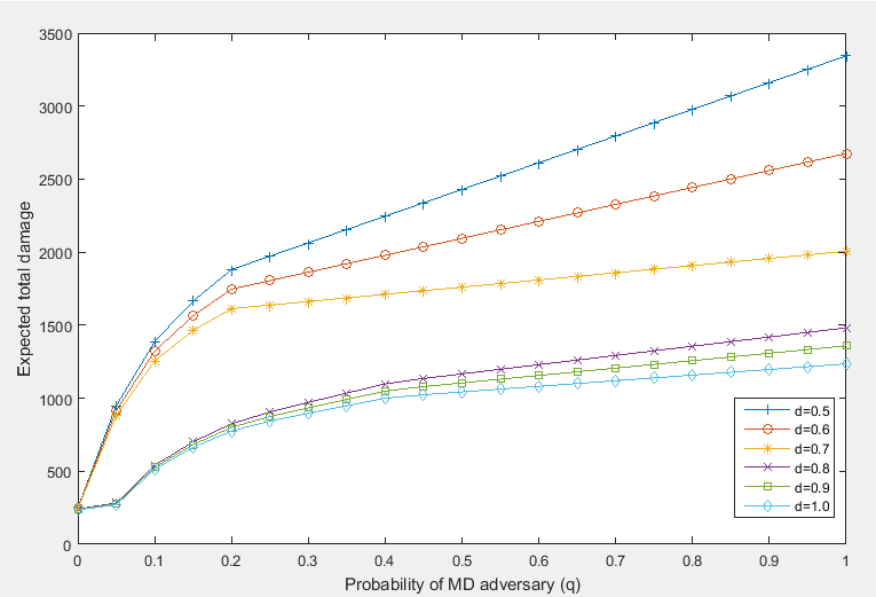

Figure: Expected total damage under different detection probabilities

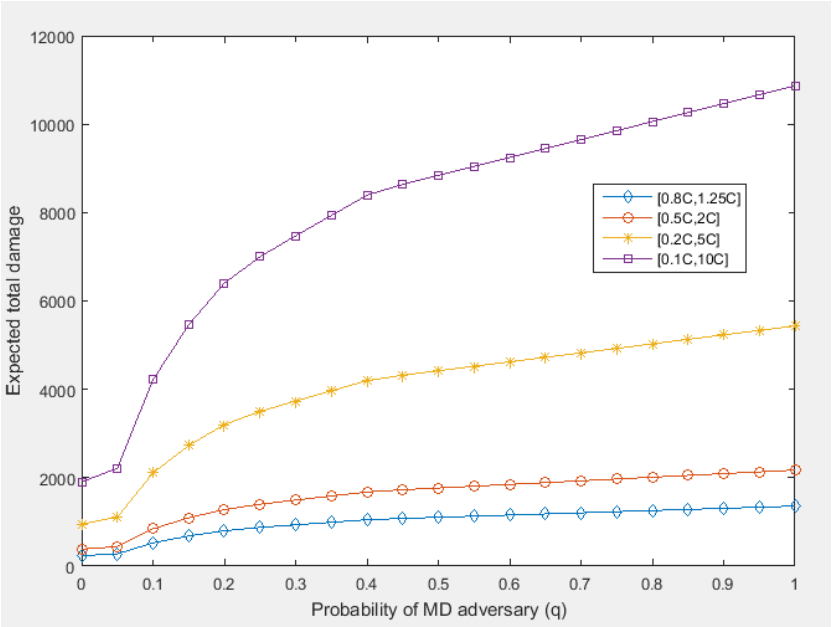

Figure: Expected total damage under different uncertainty ranges

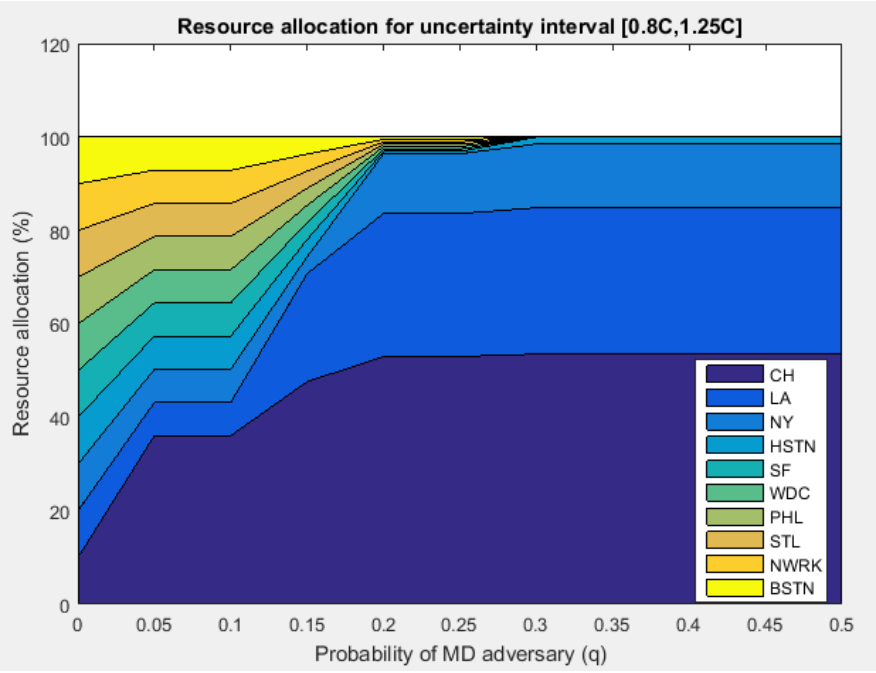

Figure: Allocation of defensive resources to reduce the political effects

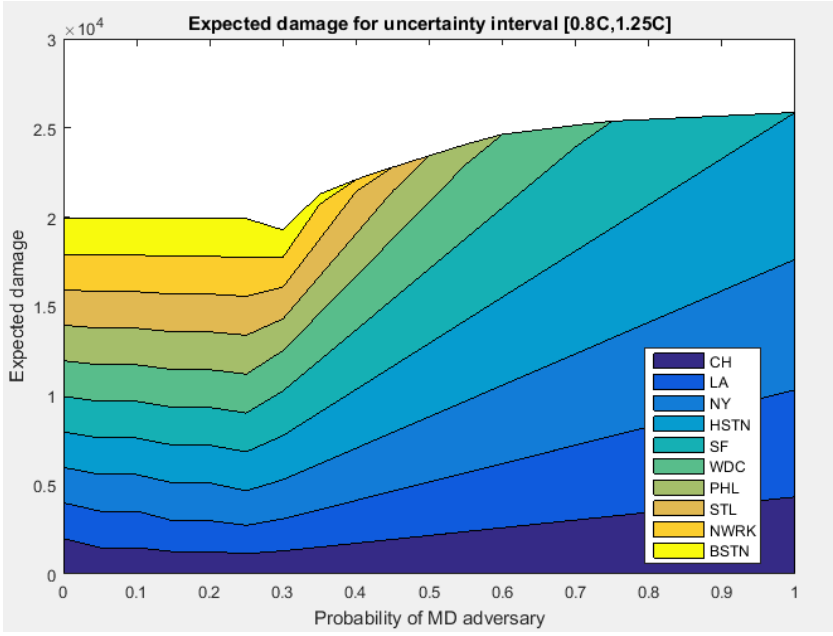

Figure: Expected damage under political considerations

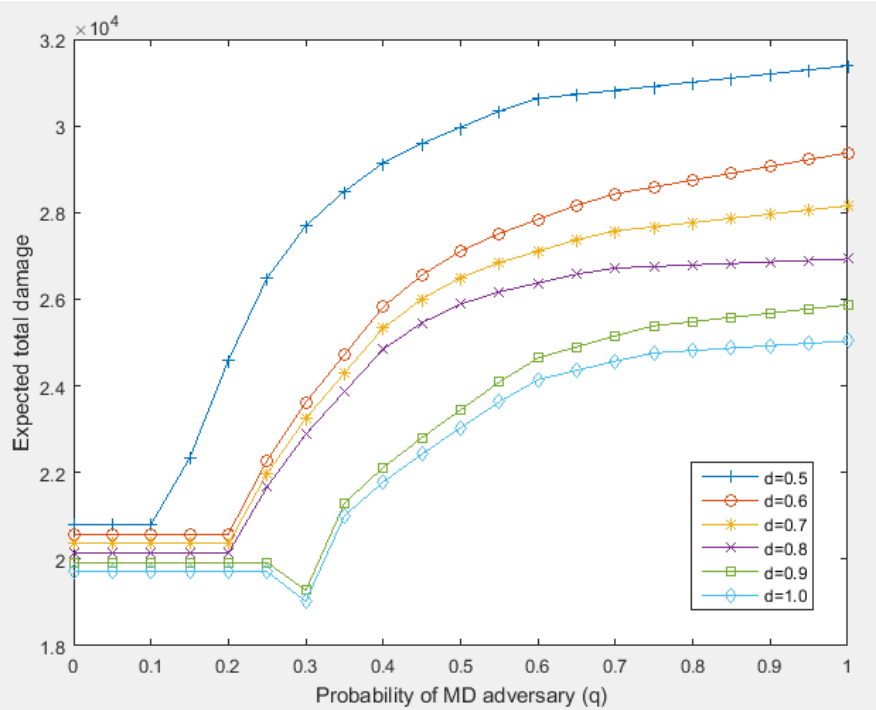

Figure: Expected total damage under different probability of detection

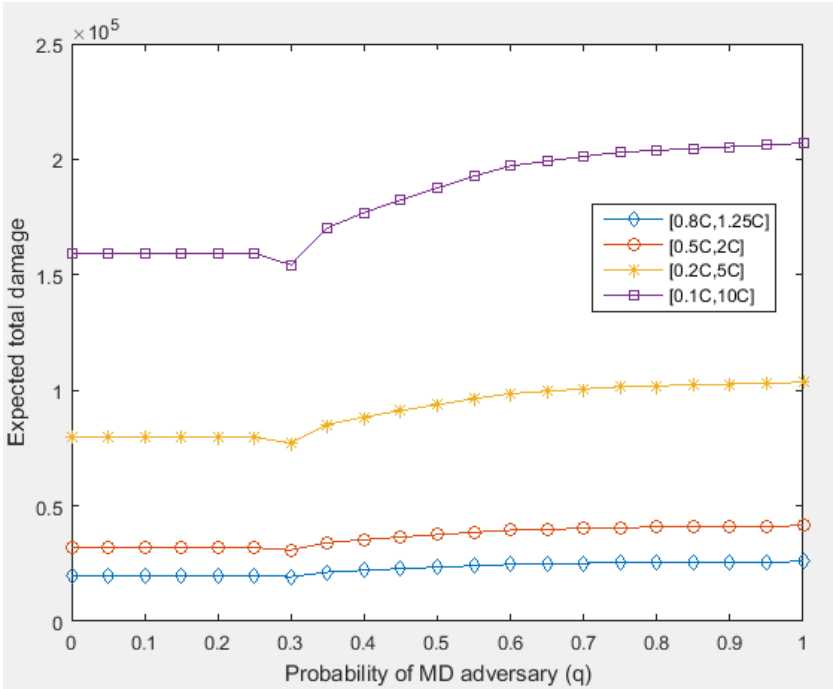

Figure: Expected total damage under different uncertainty ranges

Conclusions

- Maximum damage and harassment attacks against a defender under uncertainty
  - Static Game: Closed form solutions of threshold type policy
  - Defender's Dilemma: Robust-Bayesian Game
    - Accuracy of the estimate range affects the expected damage and optimal defensive strategy
    - Defender's belief about the attack type affects the equilibrium point.
- Future Work
  - Extend the network protection to multi-period dynamic scenarios
  - Incomplete Information Games

Thank you
Comments and Suggestions
gursoy@rci.rutgers.edu