Assessing and Improving Operational Resilience of Critical Infrastructures and Other Systems

An INFORMS TutORial

Associate Professor David L. Alderson
Distinguished Professor Gerald G. Brown
Professor W. Matthew Carlyle

Operations Research Department
Naval Postgraduate School

INFORMS San Francisco
9 November 2014

Overview

Goal of this TutORial:

Provide a guide to recent work using constrained optimization (along with models of system function) to assess and improve the resilience of (critical infrastructure) systems to disruptive events.

Today's Agenda:

- Motivation and Background
- Modeling
- Algorithms
- Analysis and Insights
- Applications

History: U.S. Policy on Critical Infrastructure

1996 President's Commission on Critical Infrastructure Protection

History: U.S. Policy on Critical Infrastructure

1996 President's Commission on Critical Infrastructure Protection

2001 September 11 terrorist attacks; USA PATRIOT Act

Critical Infrastructure

"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"

History: U.S. Policy on Critical Infrastructure

1996 President's Commission on Critical Infrastructure Protection

2001 September 11 terrorist attacks; USA PATRIOT Act

Critical Infrastructure

"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"

2002 Homeland Security Act establishes DHS with *security* mission

History: U.S. Policy on Critical Infrastructure

- 1996 President's Commission on Critical Infrastructure Protection
- 2001 September 11 terrorist attacks; USA PATRIOT Act

Critical Infrastructure

"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"

- 2002 Homeland Security Act establishes DHS with *security* mission
- 2003 Northeastern Blackout; Homeland Security Presidential Directive (HSPD)-7: "Directive on Critical Infrastructure Identification, Prioritization, and Protection" directs use of *risk-based* strategies
- 2004 Indonesian tsunami
- 2005 Pakistan earthquake; Hurricanes Katrina and Rita in U.S.

History: U.S. Policy on Critical Infrastructure (2)

2007 National Strategy for Homeland Security

"We will not be able to deter all terrorist threats, and it is impossible to deter or prevent natural catastrophes. We can, however, mitigate the Nation's vulnerability to acts of terrorism, other man-made threats, and natural disasters by *ensuring the structural and operational resilience* of our critical infrastructure and key resources" (p.27)

"We must now focus on the resilience of the system as a whole—an approach that centers on investments that make the system better able to absorb the impact of an event without losing the capacity to function" (p.28)

History: U.S. Policy on Critical Infrastructure (2)

2007 National Strategy for Homeland Security

> "We will not be able to deter all terrorist threats, and it is impossible to deter or prevent natural catastrophes. We can, however, mitigate the Nation's vulnerability to acts of terrorism, other man-made threats, and natural disasters by *ensuring the structural and operational resilience* of our critical infrastructure and key resources" (p.27)
>
> "We must now focus on the resilience of the system as a whole—an approach that centers on investments that make the system better able to absorb the impact of an event without losing the capacity to function" (p.28)

2008 Global financial crisis

2010 Haiti Earthquake; Deepwater Horizon Oil Spill

2011 Fukushima Daiichi Nuclear Disaster

2012 Hurricane Superstorm Sandy

History: U.S. Policy on Critical Infrastructure (3)

2013 Presidential Policy Directive (PPD)-21:
"Critical Infrastructure Security and Resilience"

resilience is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents"

History: U.S. Policy on Critical Infrastructure (3)

2013 Presidential Policy Directive (PPD)-21:
"Critical Infrastructure Security and Resilience"

> *resilience* is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents"

2013 Attack on PG&E Metcalf electric substation

2014 Ebola outbreak

History: U.S. Policy on Critical Infrastructure (3)

2013 Presidential Policy Directive (PPD)-21:
"Critical Infrastructure Security and Resilience"

resilience is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents"

2013 Attack on PG&E Metcalf electric substation

2014 Ebola outbreak

Summary: Shift in U.S. Policy on Critical Infrastructure

Security $\rightarrow$ **Risk** $\rightarrow$ **Resilience**

Contribution in context

This TutORial builds on previous work:

- two classes of bi-level programming models in Brown et al. (2005): *attacker-defender*, *defender-attacker*
- tri-level programming models: *defender-attacker-defender* in Brown et al. (2006)
- other recent treatments of *system interdiction models*: Lim and Smith (2007), Alderson et al. (2011, 2013), Wood (2011), and Dimitrov and Morton (2013)

Contribution in context

This TutORial builds on previous work:

- two classes of bi-level programming models in Brown et al. (2005): *attacker-defender*, *defender-attacker*
- tri-level programming models: *defender-attacker-defender* in Brown et al. (2006)
- other recent treatments of *system interdiction models*: Lim and Smith (2007), Alderson et al. (2011, 2013), Wood (2011), and Dimitrov and Morton (2013)

Our contribution in this TutORial:

1. synthesize the most essential material in these many papers,
2. provide a step-by-step explanation of how and why we build these models as we do,
3. introduce a general solution technique for solving them, and
4. establish connections to other related work.

Introduction

Primary Objective

Making critical infrastructure systems and other large systems resilient to a range of accidents, natural disasters, deliberate attacks, and other disruptions.

Introduction

Primary Objective

Making critical infrastructure systems and other large systems resilient to a range of accidents, natural disasters, deliberate attacks, and other disruptions.

Resilience

Introduction

Primary Objective

Making critical infrastructure systems and other large systems resilient to a range of accidents, natural disasters, deliberate attacks, and other disruptions.

Resilience

- What is resilience?

Introduction

Primary Objective

Making critical infrastructure systems and other large systems resilient to a range of accidents, natural disasters, deliberate attacks, and other disruptions.

Resilience

- What is resilience?
- How can we measure it?

Introduction

Primary Objective

Making critical infrastructure systems and other large systems resilient to a range of accidents, natural disasters, deliberate attacks, and other disruptions.

Resilience

- What is resilience?
- How can we measure it?
- How can we improve it?

Introduction

Primary Objective

Making critical infrastructure systems and other large systems resilient to a range of accidents, natural disasters, deliberate attacks, and other disruptions.

Resilience

- What is resilience?
- How can we measure it?
- How can we improve it?

Basic Assumption

Everything we propose is based on having an *operational model* of system performance

Operational Model

Modeling system operation:

- system components provide function
- the operation of the system is a coordinated operation of its components
- the operational setting describes the working state of the components, and determines the cost of operating them
- the system design specifies existence of and connections between components, and determines feasible operation
- performance is measured by a scalar function of the design, setting, and operation of the system.

Example performance measures: total shipping cost, barrels of fuel delivered, total vehicle-hours of commuting traffic, megawatt-hours of power shed (not delivered), total weighted rewards for delivering medical supplies.

Optimizing System Performance

Using an operational model to determine a maximum-performance operation of the system:

$$z^* = \max_{y \in Y(\hat{w})} f(\hat{w}, \hat{x}, y)$$

Optimizing System Performance

Using an operational model to determine a maximum-performance operation of the system:

$$z^* = \max_{y \in Y(\hat{w})} f(\hat{w}, \hat{x}, y)$$

- $f(\cdot)$ measures system performance

Optimizing System Performance

Using an operational model to determine a maximum-performance operation of the system:

$$z^* = \max_{y \in Y(\hat{w})} f(\hat{w}, \hat{x}, y)$$

- $f(\cdot)$ measures system performance
- $\hat{w}$ is the design of the system

Optimizing System Performance

Using an operational model to determine a maximum-performance operation of the system:

$$z^* = \max_{y \in Y(\hat{w})} f(\hat{w}, \hat{x}, y)$$

- $f(\cdot)$ measures system performance
- $\hat{w}$ is the design of the system
- $\hat{x}$ is the operational setting

Optimizing System Performance

Using an operational model to determine a maximum-performance operation of the system:

$$z^* = \max_{y \in Y(\hat{w})} f(\hat{w}, \hat{x}, y)$$

- $f(\cdot)$ measures system performance
- $\hat{w}$ is the design of the system
- $\hat{x}$ is the operational setting
- $y \in Y(\hat{w})$ indicates activities y depend on design $\hat{w}$

Optimizing System Performance

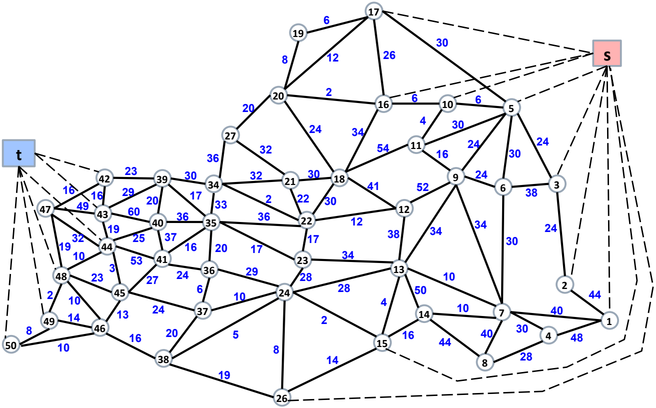
Using an operational model to determine a maximum-performance operation of the system:

$$z^* = \max_{y \in Y(\hat{w})} f(\hat{w}, \hat{x}, y)$$

- $f(\cdot)$ measures system performance
- $\hat{w}$ is the design of the system
- $\hat{x}$ is the operational setting
- $y \in Y(\hat{w})$ indicates activities y depend on design $\hat{w}$

y^* is an optimal way to operate the system for design $\hat{w}$ under operational setting $\hat{x}$, and results in performance z^*.

Example Infrastructure: Russian Rail Network



Soviet Rail system, c.1955 (from Alderson et al. (2013), adapted from Harris and Ross (1955)). Capacities in 1,000s of tons. Max *s*-*t* flow is 163,000 tons.

Events, Disruptions, and Resilience

Building a model of system operation:

- an event is a change to the operational setting
- the consequence of an event is the change in system performance resulting from that event
- a disruption is an event that hurts performance
- the resilence of the system to an event is quantified by the consequence resulting from the event; designs that have lower consequence to an event are more resilient to it
- system resilience to a specific set of events is measured by a scalar function of the resilence of the system to each of the events in the set.

Examples of disruptive events: Port of Long Beach closed by oil spill, explosion destroys two collocated pipes, flooding closes all New Orleans roads below sea level, three electrical substations are shut down by snipers, two key hospitals placed under complete quarantine from rampant infections.

Modeling and Analysis Script

1. Formulate *Operator Model*: operational model that determines optimal system operation and performance,
2. Define set of events and identify how each event modifies operational setting,
3. Modify Operator Model: include events and their impact on operational setting,
4. Formulate bi-level *Attacker Model*: identify worst-case events that minimize optimal performance,
5. Define design decisions that change the feasible operation of the system,
6. Modify Operator and Attacker Models: include design and its effect on operations,
7. Formulate tri-level *Defender Model*: choose best design *in anticipation of* a worst-case event.

Example Applications: Operator Models

	Electric power transmission grid	Highway network	Undersea comms cables
System components	Generators; buses; transmission lines; transformers; substations	Road segments; tunnels; bridges; interchanges	Landing stations; branching units; repeaters; fiber-optic cables ("links")
System configuration	Inter-component connections; line thermal capacities; generating capacities	Inter-component connections; component lengths, capacities, and speed limits	Inter-component connections; router capacities; link capacities
Relevant operating environment	During one or more weekday time periods: generation costs; customer classes; load-shedding costs; demands at each bus	During one or more peak travel periods: demands for vehicular travel between origin-destination pairs	During one or more periods of high demand: user requirements for end-to-end communications
Operator	Independent System Operator makes centralized, near-real-time generating decisions to balance supply with demand	Drivers select routes in a decentralized but "smart" fashion (implicitly following the tenets of game-theoretic, equilibrium model)	Undersea Cable Operator establishes end-to-end "lightpath" connections, and "grooms" network traffic (e.g., Zhu and Mukherjee, 2002)
Operator's model	A "DC optimal power-flow model" (a linear program) that system operators use to optimize generation to meet demands (e.g., Wood and Wollenberg, 1996, pp.108–111)	A traffic-equilibrium model (solved as a nonlinear program) for origin-destination routing decisions and travel times (e.g., Beckmann et al., 1956)	A multicommodity transportation model to route customer traffic (e.g., Mukherjee et al., 1996)
System performance metric	Minimize: generation costs plus the economic cost of unserved demand over the course of a typical work day (e.g., Salmerón et al., 2004)	Minimize: average travel time during for network users during a peak commute period	Minimize: traffic delays and shortage penalties for unmet end-to-end traffic demands (e.g., Crain, 2012)

Example Applications: Attacker and Defender Models

	Electric power transmission grid	Highway network	Undersea comms cables
Operator's model	A "DC optimal power-flow model" (a linear program) that system operators use to optimize generation to meet demands (e.g., Wood and Wollenberg, 1996, pp.108–111)	A traffic-equilibrium model (solved as a nonlinear program) for origin-destination routing decisions and travel times (e.g., Beckmann et al., 1956)	A multicommodity transportation model to route customer traffic (e.g., Mukherjee et al., 1996)
System performance metric	Minimize: generation costs plus the economic cost of unserved demand over the course of a typical work day (e.g., Salmerón et al., 2004)	Minimize: average travel time during for network users during a peak commute period	Minimize: traffic delays and shortage penalties for unmet end-to-end traffic demands (e.g., Crain, 2012)
Attacks on components	Generators, buses, etc., damaged or destroyed by explosives, gunfire, etc.	Road segments, tunnels, etc., damaged or destroyed by explosives, burning liquids, etc.	Cables severed by accident, natural disaster, or deliberate attack; landing stations attacked
Design (defenses)	Offset fencing at substations; physical or electro-magnetic shielding; surplus component capacity (e.g., new generators, upgraded transmission lines)	Vehicle inspections at bridge entrances; structural reinforcement; increased police patrols; surplus component capacity (e.g., new bridges, widened roads)	Construction of addtional redundant pathways; Enhanced physical security at landing stations

Modeling and Analysis Script

1. Formulate *Operator Model*: operational model that determines optimal system operation and performance,
2. Define set of events and identify how each event modifies operational setting,
3. Modify Operator Model: include events and their impact on operational setting,
4. Formulate bi-level *Attacker Model*: identify worst-case events that minimize optimal performance,
5. Define design decisions that change the feasible operation of the system,
6. Modify Operator and Attacker Models: include design and its effect on operations,
7. Formulate tri-level *Defender Model*: choose best design *in anticipation of* a worst-case event.

Step 1: Formulate the Operator Model

Indices and Sets

$n, i, j \in N$	stations (ordered set of nodes)
$s, t \in N$	distinguished start and end stations
$[i, j] \in E$	undirected edge between nodes i and j; where $i < j, \forall [i, j] \in E$
$(i, j) \in A$	directed arc from i to node j; $[i, j] \in E \Leftrightarrow i < j \wedge ((i, j) \in A \wedge (j, i) \in A)$

Data [units]

u_{ij}	upper bound on (undirected) flow on edge $[i, j] \in E$ [tons]

Decision Variables [units]

y_{ij}	directional flow of cargo on arc $(i, j) \in A$ [tons]
y_{ts}	total flow through network from s to t [tons]

Step 1: Formulate the Operator Model

RAIL-NET-CAPACITY

$$\max_{y} \quad y_{ts} \tag{1}$$

$$\text{s.t.} \quad \sum_{j:(n,j)\in A} y_{nj} - \sum_{i:(i,n)\in A} y_{in} = \begin{cases} y_{ts} & n = s \\ 0 & n \neq s,t \\ -y_{ts} & n = t \end{cases} \quad \forall n \in N \tag{2}$$

$$y_{ij} + y_{ji} \leq u_{ij} \quad \forall [i,j] \in E \tag{3}$$

$$y_{ij} \geq 0 \quad \forall (i,j) \in A \tag{4}$$

$$y_{ts} \geq 0 \tag{5}$$

Step 2: Define the Events

Event:

The simultaneous damage of one or more edges.

$\hat{x} = \{\hat{x}_{ij}\}, [i,j] \in E$, where
$\hat{x}_{ij} = 1$ if edge $[i,j] \in E$ has been damaged, and is zero otherwise.

Example Sets of Events:

Step 2: Define the Events

Event:

The simultaneous damage of one or more edges.

$\hat{x} = \{\hat{x}_{ij}\}, [i,j] \in E$, where
$\hat{x}_{ij} = 1$ if edge $[i,j] \in E$ has been damaged, and is zero otherwise.

Example Sets of Events:

Defined by enumeration:

$$S_1 = \{\hat{x}^1, \hat{x}^2, \ldots, \hat{x}^p\}$$

Step 2: Define the Events

Event:

The simultaneous damage of one or more edges.

$\hat{x} = \{\hat{x}_{ij}\}, [i,j] \in E$, where
$\hat{x}_{ij} = 1$ if edge $[i,j] \in E$ has been damaged, and is zero otherwise.

Example Sets of Events:

Defined by enumeration:

$$S_1 = \{\hat{x}^1, \hat{x}^2, \ldots, \hat{x}^p\}$$

Defined by constraint(s):

$$S_2 = \{\hat{x} : \hat{x} \in \{0,1\}^{|E|}, \sum_{(i,j)\in A} \hat{x}_{ij} \leq atk\_budget\}$$

Step 3: Incorporate Events into the Operator Model

Step 3: Incorporate Events into the Operator Model

Obvious, but computationally difficult:

$$y_{ij} + y_{ji} \leq (1 - \hat{x}_{ij})u_{ij}, \qquad \forall [i,j] \in E.$$

Step 3: Incorporate Events into the Operator Model

Obvious, but computationally difficult:

$$y_{ij} + y_{ji} \leq (1 - \hat{x}_{ij})u_{ij}, \qquad \forall [i,j] \in E.$$

This leads to difficulty in maintaining linearity of the models.

Step 3: Incorporate Events into the Operator Model

Obvious, but computationally difficult:

$$y_{ij} + y_{ji} \leq (1 - \hat{x}_{ij}) u_{ij}, \qquad \forall [i,j] \in E.$$

This leads to difficulty in maintaining linearity of the models.

Penalty-costs in the objective:

$$\max_{y} \quad y_{ts} - \sum_{[i,j] \in E} 2\,(y_{ij} + y_{ji})\,\hat{x}_{ij}.$$

Step 3: Incorporate Events into the Operator Model

Obvious, but computationally difficult:

$$y_{ij} + y_{ji} \leq (1 - \hat{x}_{ij}) u_{ij}, \qquad \forall [i,j] \in E.$$

This leads to difficulty in maintaining linearity of the models.

Penalty-costs in the objective:

$$\max_{y} \quad y_{ts} - \sum_{[i,j] \in E} 2 \left(y_{ij} + y_{ji} \right) \hat{x}_{ij}.$$

If an edge has been damaged, any flow is penalized *twice* what it would eventually contribute to the objective via y_{ts}.

Step 4: Formulate the Attacker Model

New Data

atk_budget	max #edges targeted in an attack

New Decision Variables [units]

x_{ij}	$=$1 if track section $[i, j] \in E$ is attacked, $=$0 otherwise [binary]

The simple cardinality-based attack budget generalizes easily to multiple resource costs and budgets.

Step 4: Formulate the Attacker Model

ATTACK-RAIL-NET

$$\min_{x} \max_{y} \quad y_{ts} - \sum_{[i,j]\in E} 2\,(y_{ij} + y_{ji})\, x_{ij} \tag{6}$$

$$\text{s.t.} \quad (2), (3), (4), (5)$$

$$\sum_{[i,j]\in E} x_{ij} \leq atk\_budget \tag{7}$$

$$x_{ij} \in \{0, 1\} \qquad \forall [i,j] \in E \tag{8}$$

Step 5: Define the Design Decisions

$\hat{w}$: build edges (rail sections) or not

$\hat{w}_{ij} = 1$ if edge $[i, j] \in E$ has been built, and zero otherwise.

def_cost$_{ij}$ cost to build track section $[i, j] \in E$
def_budget total budget for design

Example set of feasible designs

$$\Delta = \{\hat{w} : \hat{w} \in \{0,1\}^{|E|}, \sum_{[i,j] \in E} \mathit{def\_cost}_{ij} \hat{w}_{ij} \leq \mathit{def\_budget}\},$$

def_cost$_{ij} = 0$ for edges that already exist.

Step 6: Incorporate Design Decisions into the Models

For any $\hat{w} \in \Delta$, we restrict the flows in the network to edges that have been built:

Step 6: Incorporate Design Decisions into the Models

For any $\hat{w} \in \Delta$, we restrict the flows in the network to edges that have been built:

$$y_{ij} + y_{ji} \leq u_{ij}\hat{w}_{ij} \qquad \forall [i,j] \in E.$$

Step 6: Incorporate Design Decisions into the Models

For any $\hat{w} \in \Delta$, we restrict the flows in the network to edges that have been built:

$$y_{ij} + y_{ji} \leq u_{ij}\hat{w}_{ij} \qquad \forall [i,j] \in E.$$

Implementation Note:

For a fixed $\hat{w}$, this set of constraints is a restriction on the operator's flow variables, and we can simply fix flows on unbuilt arcs to zero

Step 7: Formulate the Defender Model

New Data [units]

def_budget	defense construction budget [$]
def_cost_{ij}	defense construction cost of track section $[i, j] \in E$ [$]

New Decision Variables [units]

w_{ij}	$=1$ if we decide to build track section $[i, j] \in E$, $=0$ otherwise [binary]

Step 7: Formulate the Defender Model

DEFEND-RAIL-NET

$$\max_{w} \min_{x} \max_{y} \quad y_{ts} - \sum_{[i,j] \in E} 2\,(y_{ij} + y_{ji})\, x_{ij} \tag{9}$$

$$\text{s.t.} \quad (2), (4), (5), (7), (8)$$

$$y_{ij} + y_{ji} \leq u_{ij} w_{ij} \qquad \forall [i,j] \in E \tag{10}$$

$$\sum_{[i,j] \in E} \mathit{def\_cost}_{ij} w_{ij} \leq \mathit{def\_budget} \tag{11}$$

$$w_{ij} \in \{0, 1\} \qquad \forall [i,j] \in E \tag{12}$$

Extension to Include Defense Options

What if we can defend an *existing* arc?
(And change its properties...)

Extension to Include Defense Options

What if we can defend an *existing* arc?
(And change its properties...)

New Indices and Sets

$d \in D$ defense option (for each configuration of an edge)

New Data [units]

v_{ij}^d vulnerability of option d for edge $[i,j] \in E$
u_{ij}^d capacity of edge $[i,j] \in E$ for option d [tons]
$def\_cost_{ij}^d$ construction cost of option d for edge $[i,j] \in E$ [$]

New Decision Variables [units]

y_{ij}^d flow across directed arc $(i,j) \in A$ under option d [tons]

w_{ij}^d $=1$ if we select option d for edge $[i,j] \in E$,
$=0$ otherwise [binary]

Illustration of Defense Options

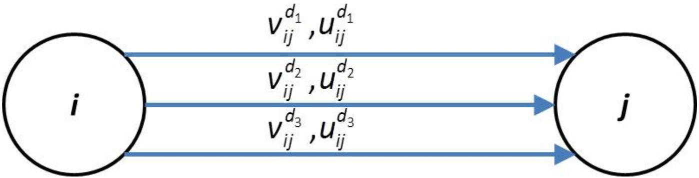
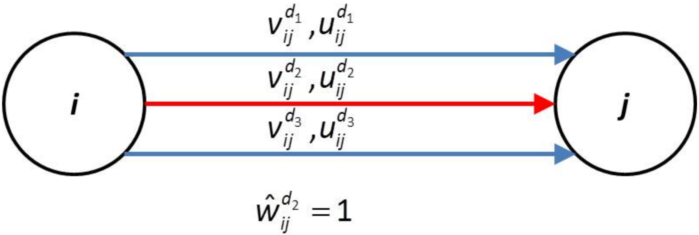


Illustration of an edge with three defense options (arcs shown in one direction only).

Illustration of Defense Options



One defense option, d_2, has been selected for this edge (arcs shown in one direction only). $\hat{w}_{ij}^{d_1}$ and $\hat{w}_{ij}^{d_3}$ are both zero. All flows on this edge in either direction will use the second set of parameters.

Defense Options Formulation

DEFEND-RAIL-NET

$$\max_{w} \min_{x} \max_{y} \quad y_{ts} - \sum_{[i,j]\in E} \sum_{d\in D} \left(v_{ij}^d y_{ij}^d + v_{ij}^d y_{ji}^d \right) x_{ij} \tag{13}$$

$$\text{s.t.} \quad \sum_{d\in D} \left[\sum_{j:(n,j)\in A} y_{nj}^d - \sum_{i:(i,n)\in A} y_{in}^d \right] = \begin{cases} y_{ts} & n = s \\ 0 & n \neq s, t \\ -y_{ts} & n = t \end{cases} \quad \forall n \in N \tag{14}$$

$$(5), (7), (8)$$

$$y_{ij}^d + y_{ji}^d \leq u_{ij}^d w_{ij}^d \qquad \forall [i,j] \in E, d \in D \tag{15}$$

$$y_{ij}^d \geq 0 \qquad \forall (i,j) \in A, d \in D \tag{16}$$

$$\sum_{d\in D} \sum_{[i,j]\in E} def\_cost_{ij}^d w_{ij}^d \leq def\_budget \tag{17}$$

$$\sum_{d\in D} w_{ij}^d = 1 \qquad \forall [i,j] \in E \tag{18}$$

$$w_{ij}^d \in \{0,1\} \qquad \forall [i,j] \in E, d \in D \tag{19}$$

Resilience Curves

The points about resilience we want to emphasize in our systems:

Resilience Curves

The points about resilience we want to emphasize in our systems:

Resilience of a system is more than a single number,

and

Resilience Curves

The points about resilience we want to emphasize in our systems:

Resilience of a system is more than a single number,

and

A resilient system can handle a *range* of events.

Resilience Curves

The points about resilience we want to emphasize in our systems:

Resilience of a system is more than a single number,

and

A resilient system can handle a *range* of events.

With our models, we conduct a parametric analysis on:

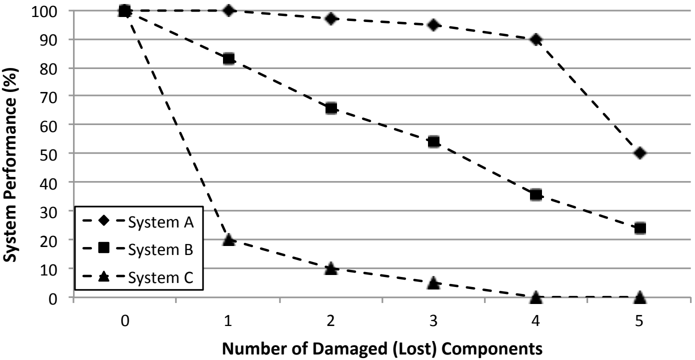
- the number of defenses we can afford (or the defense budget, more generally)
- the number of attacks our opponent can afford

These analyses give a richer representation of how a system adapts its operations to respond to a variety of attacks, and how we can *improve* those responses.

Parameterizing the Number of Attacks

Given competing designs, we can use a parametric analysis of the attacker model to compare those designs to each other.

Comparing the Resilience of Systems

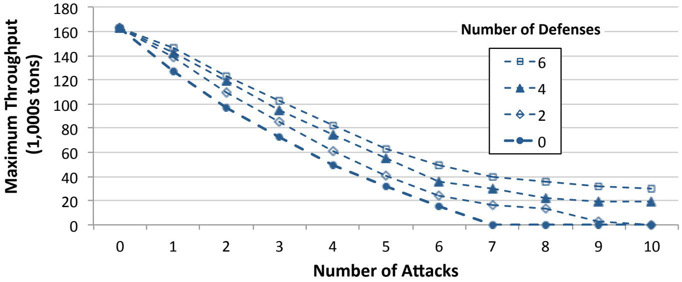


Resilience curves for three notional systems, and for disruptions that include the loss of up to 5 components. System A is “more resilient” than System B, while System C is “less resilient,” for this range of disruption.

Parameterizing the Number of Defenses and Attacks

Each level of defense yields a different resilience curve, and we can plot multiple curves to evaluate the effectiveness of increased defensive effort.

Resilience Curves for Russian Rail



Resilience curves showing throughput as a function of the number of attacks for varying numbers of defended rail sections.

Analysis

Once we have the models built, we can exercise them in a number of ways, and present the results graphically, or in a table, or even using a sequence of maps.

We represent the multidimensional nature of “resilience” for a range of defender and attacker capabilities in the hopes that we can inform better decision making.

Attacker Model Results: Power System

Component Name	*atk_cost*	*atk_budget* 1	2	3	4	5	6	7	8	9	10	11	12
Line1	1	X		X									
Line2	1										X		
Substation 1	2		X	X	X	X			X			X	
Substation 2	2				X								
Substation 3	3					X	X		X				
Substation 4	3						X	X	X	X	X	X	X
Substation 5	4							X		X	X	X	X
Substation 6	2									X	X	X	X
Substation 7	3												X

Most-disruptive interdictions by attack budget.

Defender Model Results: Power System

Component Name	*atk_cost*	*def_budget* 0	1	2	3	4	5
Substation 1	4	X					
Substation 2	3	X	O	O	O	O	O
Substation 3	2	X					
Substation 4	3		X	X	X	X	X
Substation 5	2		X	O	O	O	O
Substation 6	3		X	X	X	X	O
Substation 7	2		X	X	X	O	O
Substation 8	2			X	O	O	O
Substation 9	2				X	X	X
Substation 10	2					X	X
Substation 11	3						X

Optimal defensive "hardening" of links.
'O' = defense,'X' = attack.

Solving the Tri-Level Model

How do we unwind the min-max-min structure in $\mathbf{DAD}(w, x, y)$?

$$\min_{w \in W} \max_{x \in X} \min_{y \in Y(w)} f(w, x, y)$$

Solving the Tri-Level Model

How do we unwind the min-max-min structure in $\mathbf{DAD}(w, x, y)$?

$$\min_{w \in W} \max_{x \in X} \min_{y \in Y(w)} f(w, x, y)$$

Observation

X is a finite set of attacks

Solving the Tri-Level Model

How do we unwind the min-max-min structure in $\mathbf{DAD}(w, x, y)$?

$$\min_{w \in W} \max_{x \in X} \min_{y \in Y(w)} f(w, x, y)$$

Observation

X is a finite set of attacks

Recourse-based Reformulation

Define vectors $\{y^k\}$, where each y^k is operator's response (recourse!) to a particular $\hat{x}^k \in X$.

Unwinding The Tri-Level Model

Reformulated **DAD**(w, x, y):

$$z^* = \min_{w \in W} \max_{\hat{x}^k \in X} \min_{y^k \in Y(w)} f(w, \hat{x}^k, y^k),$$

- The set X, though finite, can be enormous. We'll overlook that for now...
- The max operator is over the (finite) enumeration of all attacks, and each attack $\hat{x}^k$ has a separate response, y^k.

Insight

For any $\hat{w}$, we can pick the optimal response, y^k, for each $\hat{x}^k$, *in advance*.

From Tri-Level to Bi-Level

Practically speaking, this means we can *exchange the order of the inner two operators*, at the cost of a significant increase in the number of variables.

Rewritten, reformulated DAD(w, x, y):

$$z^* = \min_{\substack{w \in W \\ y^k \in Y(w)}} \max_{\hat{x}^k \in X} f(w, \hat{x}^k, y^k),$$

Decomposition Master Problem

If we only enumerate a *subset* of the attacks, $\hat{x}^1, \hat{x}^2, \ldots, \hat{x}^K$, where $K << |X|$, we can state the:

Decomposition Master Problem

If we only enumerate a *subset* of the attacks, $\hat{x}^1, \hat{x}^2, \ldots, \hat{x}^K$, where $K << |X|$, we can state the:

Relaxed master problem

DAD-Master:

$$z* = \min_{\substack{z, w \in W \\ y^k \in Y(w)}} \quad z$$

$$\text{s.t.} \quad z \geq f(w, \hat{x}^k, y^k) \qquad \forall k = 1, \ldots, K. \quad \text{(DADC1)}$$

Decomposition Master Problem

If we only enumerate a *subset* of the attacks, $\hat{x}^1, \hat{x}^2, \ldots, \hat{x}^K$, where $K << |X|$, we can state the:

Relaxed master problem

DAD-Master:

$$z* = \min_{\substack{z, w \in W \\ y^k \in Y(w)}} z$$

$$\text{s.t. } z \geq f(w, \hat{x}^k, y^k) \qquad \forall k = 1, \ldots, K. \quad \text{(DADC1)}$$

- Optimal solution provides a lower bound for **DAD**(w, x, y), a feasible design $\hat{w}^K$, and the optimal responses, $\hat{y}^k$, for each attack $\hat{x}^k$, under that design.

Decomposition Master Problem

If we only enumerate a *subset* of the attacks, $\hat{x}^1, \hat{x}^2, \ldots, \hat{x}^K$, where $K << |X|$, we can state the:

Relaxed master problem

DAD-Master:

$$z* = \min_{\substack{z, w \in W \\ y^k \in Y(w)}} \quad z$$

$$\text{s.t.} \quad z \geq f(w, \hat{x}^k, y^k) \qquad \forall k = 1, \ldots, K. \quad \text{(DADC1)}$$

- Optimal solution provides a lower bound for **DAD**(w, x, y), a feasible design $\hat{w}^K$, and the optimal responses, $\hat{y}^k$, for each attack $\hat{x}^k$, under that design.
- For any fixed design, $\hat{w}^K$, solve **DAD**$(\hat{w}^K, x, y)$ for an upper bound on **DAD**(w, x, y), the resulting optimal attack, $\hat{x}^{K+1}$, in response to $\hat{w}^K$, and a new cut (DADC1).

Solving the Attacker (Sub)problem

Given feasible defense $\hat{w}$ from **DAD-Master**, we need

- the optimal (worst-case) attack in response, and
- the resulting operating cost.

Solving the Attacker (Sub)problem

Given feasible defense $\hat{w}$ from **DAD-Master**, we need

- the optimal (worst-case) attack in response, and
- the resulting operating cost.

DAD$(\hat{w}, x, y)$ is the subproblem for our decomposition approach.

Attacker Subproblem

$$\max_{x \in X} \min_{y \in Y(\hat{w})} f(\hat{w}, x, y)$$

Solving the Attacker Subproblem

If the Operator Problem is a Linear Program:

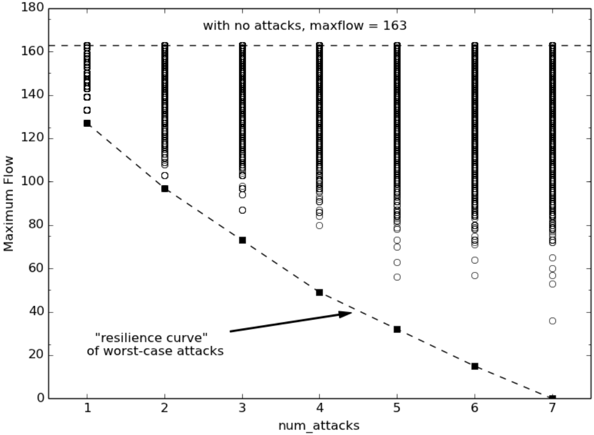
- Benders Decomposition
- taking the dual of the Operator Problem (Yielding a pure max ILP)

Otherwise

- Decomposition similar to DAD
- Heuristic search for attacks (Operator Problem to evaluate)

As a specific example of the latter, we could use random sampling to generate disruptive events (attacks)...

Solving the Attacker Problem via Random Sampling



10,000 random attacks on the Soviet railway compared with a worst-case attack, for each of $num\_attacks = 1, 2, \ldots, 7$. (Figure from Alderson *et al.* Alderson et al. (2013), Figure 5.)

Decomposition Details

- The master problem is an ILP (binary design variables)
- The subproblem is equivalent to an ILP (binary attack variables)

Decomposition Details

- The master problem is an ILP (binary design variables)
- The subproblem is equivalent to an ILP (binary attack variables)

Standard Benders decomposition might cycle.

But with only a finite number of attacks...

Decomposition Details

- The master problem is an ILP (binary design variables)
- The subproblem is equivalent to an ILP (binary attack variables)

Standard Benders decomposition might cycle.

But with only a finite number of attacks...

Solution elimination constraints

$$\sum_{(i,j):\hat{x}_{ij}^k=0} x_{ij} + \sum_{(i,j):\hat{x}_{ij}^k=1} (1 - x_{ij}) \geq 1 \qquad \forall k = 1, \ldots, K$$

- Add these to the subproblem, and you are guaranteed to get a new (possibly suboptimal) attack in each iteration...
- ... and therefore (eventually) generate every cut in the master.

Other Solution Options

For a "small" number of feasible defenses we can enumerate:

Other Solution Options

For a “small” number of feasible defenses we can enumerate:

- can also enumerate attacks to solve the subproblem

Other Solution Options

For a "small" number of feasible defenses we can enumerate:

- can also enumerate attacks to solve the subproblem
- be careful with $\binom{m}{k}$

Other Solution Options

For a "small" number of feasible defenses we can enumerate:

- can also enumerate attacks to solve the subproblem
- be careful with $\begin{pmatrix} m \\ k \end{pmatrix}$

We can use brute-force enumeration and just solve a large number of Attacker Problems (and Operator Problems), or we can try to implement special master problems that implicitly enumerate defenses (or attacks).

Other Solution Options

For a "small" number of feasible defenses we can enumerate:

- can also enumerate attacks to solve the subproblem
- be careful with $\binom{m}{k}$

We can use brute-force enumeration and just solve a large number of Attacker Problems (and Operator Problems), or we can try to implement special master problems that implicitly enumerate defenses (or attacks).

- Solution elimination constraints (try a new defense at each iteration)

Other Solution Options

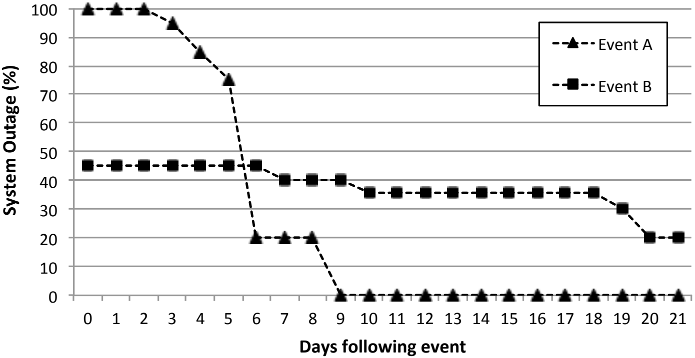
For a "small" number of feasible defenses we can enumerate:

- can also enumerate attacks to solve the subproblem
- be careful with $\binom{m}{k}$

We can use brute-force enumeration and just solve a large number of Attacker Problems (and Operator Problems), or we can try to implement special master problems that implicitly enumerate defenses (or attacks).

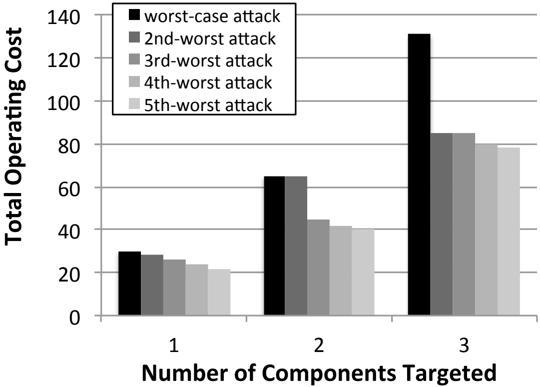
- Solution elimination constraints (try a new defense at each iteration)
- Set covering constraints (defend at least one attacked component in each attack)

Time-phased Reconstitution of Components



Reconstitution of a notional system following two different events.

Best k attacks



Top five rank-ordered attacks for target lists containing one to three components.

Stochastic “Attacker” Model

If events that modify the operational setting are not deliberate attacks, but random events, then for any fixed design we can evaluate the resilience of the system via:

$$\mathbb{E}_{\tilde{x}}\left[\min_{y \in Y(\hat{w})} f(\hat{w}, \tilde{x}, y)\right],$$

where $\tilde{x} \in X$ is a random event drawn from the set of events, X, and the expectation is taken over a known distribution.

The set X can be parameterized by magnitude of the events (similar to earthquakes, hurricanes, etc.), and resilience curves can be plotted for these models, too.

Stochastic Programs with Recourse

If we wish to design the system to be resilient to the distribution of events from X, then we have

$$\min_{w \in W} \mathbb{E}_{\tilde{x}} \left[\min_{y \in Y(w)} f(w, \tilde{x}, y) \right],$$

a two-stage stochastic program with recourse, with design w as the first stage decisions, the “attack” $\tilde{x}$ as the random realization, and the operations y as the recourse.

Building the Tri-Level Model

Our seven-step script simplifies to a sequence of three models:

Building the Tri-Level Model

Our seven-step script simplifies to a sequence of three models:

Operator Model for a fixed defense and setting, $(\hat{w}, \hat{x})$:

$$\textbf{DAD}(\hat{w}, \hat{x}, y) \qquad \min_{y \in Y(\hat{w})} f(\hat{w}, \hat{x}, y)$$

Building the Tri-Level Model

Our seven-step script simplifies to a sequence of three models:

Operator Model for a fixed defense and setting, $(\hat{w}, \hat{x})$:

$$\textbf{DAD}(\hat{w}, \hat{x}, y) \qquad \min_{y \in Y(\hat{w})} f(\hat{w}, \hat{x}, y)$$

Attacker Model for a fixed defense, $(\hat{w})$:

$$\textbf{DAD}(\hat{w}, x, y) \qquad \max_{x \in X} \min_{y \in Y(\hat{w})} f(\hat{w}, x, y)$$

Building the Tri-Level Model

Our seven-step script simplifies to a sequence of three models:

Operator Model for a fixed defense and setting, $(\hat{w}, \hat{x})$:

DAD$(\hat{w}, \hat{x}, y)$ $\quad \min_{y \in Y(\hat{w})} f(\hat{w}, \hat{x}, y)$

Attacker Model for a fixed defense, $(\hat{w})$:

DAD$(\hat{w}, x, y)$ $\quad \max_{x \in X} \min_{y \in Y(\hat{w})} f(\hat{w}, x, y)$

Defender Model:

DAD(w, x, y) $\quad \min_{w \in W} \max_{x \in X} \min_{y \in Y(w)} f(w, x, y)$

Building the Tri-Level Model

Central to all of these models is an operational model of system operation:

$$\min_{y \in Y} f(y).$$

But, if it is built from the start to:

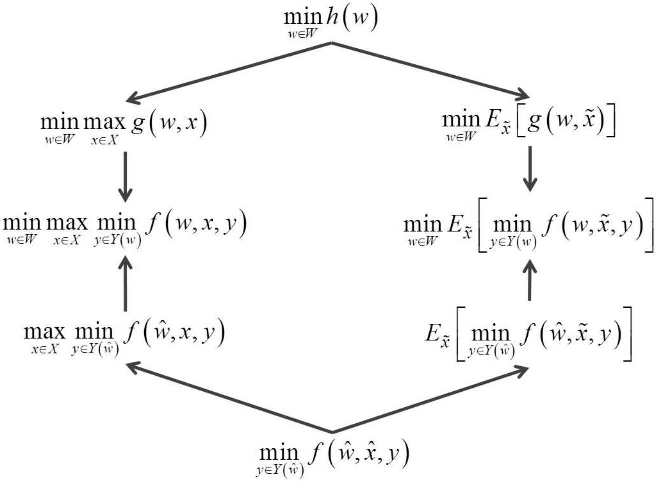
- incorporate design options, $\hat{w}$, and
- incorporate the setting, $\hat{x}$,

To yield:

$$\min_{y \in Y(\hat{w})} f(\hat{w}, \hat{x}, y),$$

then the remaining modeling effort is relatively straightforward.

Some Thoughts on Modeling



We recommend building these models from the bottom up, on this diagram. The "top down" approach, if done carelessly, leads to many (painful) reformulations along the way.

Alderson, D.L., G.G. Brown, W.M. Carlyle. 2014. **Assessing and Improving Operational Resilience of Critical Infrastructures and Other Systems**. A. Newman, J. Leung, eds., *Tutorials in Operations Research: Bridging Data and Decision*. Institute for Operations Research and Management Science, Hanover, MD, 180–215.

Alderson, D.L., G.G. Brown, W.M. Carlyle, L.A. Cox. 2013. Sometimes there is no "most vital" arc: assessing and improving the operational resilience of systems. *Military Operations Research* **18**(1) 21–37.

Alderson, D.L., G.G. Brown, W.M. Carlyle, R.K. Wood. 2011. Solving defender-attacker-defender models for infrastructure defense. K. Wood, R. Dell, eds., *Operations Research, Computing and Homeland Defense*. Institute for Operations Research and the Management Sciences, Hanover, MD, 28–49.

Beckmann, M.J., C.B. McGuire, C.B. Winsten. 1956. *Studies in the Economics of Transportation*. Yale University Press, New Haven, Connecticut.

Brown, G.G., W.M. Carlyle, J. Salmerón, K. Wood. 2006. Defending critical infrastructure. *Interfaces* **36** 530–544.

Brown, G.G., W.M. Carlyle, J. Salmerón, R.K. Wood. 2005. Analyzing the vulnerability of critical infrastructure to attack, and planning defenses. H. Greenberg, J. Smith, eds., *Tutorials in Operations Research: Emerging Theory, Methods, and Applications*. Institute for Operations Research and Management Science, Hanover, MD, 102–123.

Crain, J.K. 2012. Assessing resilience in the global undersea cable infrastructure. Master's thesis, Naval Postgraduate School, Monterey, CA.

Dimitrov, N.B., D.P. Morton. 2013. Interdiction models and applications. J.W. Hermmann, ed., *Handbook of Operations Research for Homeland Security*. Springer, 73–103.

Harris, T.E., F.S. Ross. 1955. Fundamentals of a method for evaluating rail net capacities. The RAND Corporation, Research Memorandum RM-1573.

Lim, C., J. C. Smith. 2007. Algorithms for discrete and continuous multicommodity flow network interdiction problems. *IIE Transactions* **39**(1) 15–26.

Mukherjee, B., B. Banerjee, S. Ramamurthy, A. Mukherjee. 1996. Some principles for designing a wide-area WDM optical network. *IEEE/ACM Transactions on Networking* **4**(5) 684–706.

Salmerón, J., K. Wood, R. Baldick. 2004. Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems* **19** 905–912.

Wood, A. J., B. F. Wollenberg. 1996. *Power generation, operation and control*. 2nd ed. Wiley, New York.

Wood, R.K. 2011. Bilevel network interdiction models: Formulations and solutions. J.J. Cochran, ed., *Wiley Encyclopedia of Operations Research and Management Science*. John Wiley & Sons, 1–11. doi:10.1002/9780470400531.eorms0932.

Zhu, K., B. Mukherjee. 2002. Traffic grooming in an optical WDM mesh network. *IEEE Journal on Selected Areas in Communication* **20**(1) 122–133.