Network Vulnerability and High-Speed Rail

Presented by
Nicholas Lownes, Ph.D., P.E.

Co-Authors:

Reda Ammar, Ph.D
Sanguthevar Rajasekaran, Ph.D.
Lance Fiondella
Qixing Wang

Organization

- Introduction
- Research Objective
- Solution Approach
- Sioux Falls Network Application
- Conclusion

Introduction

- The vulnerability of a transportation network is strongly correlated with the ability of the network to withstand shocks and disruptions.
- High-volume edges with limited alternative paths represent obvious system vulnerabilities.
- Can be modeled as a traffic assignment problem.
- High-speed rail (HSR) introduces a bi-modal element – increases complexity in modeling and algorithmic approaches.

Objective

- Create a model of network vulnerability that:
  - Has the flexibility to include HSR
  - Has a high degree of behavioral realism
  - Can be utilized as a decision-support system for technology deployment
  - Uses theoretically sound framework

Background Review

- Bell et al. (2002, 2003, 2008), Murray-Tuite and Mahmassani (2004) , Laporte et al. (2010) applied the game theory to analysis the network vulnerability.

- Ukkusuri and Yushimito (2009) propose a heuristic method incorporating a user equilibrium assignment procedure to assess the importance of highway transportation networks

- Bar-Noy et al. (1995), Latora and Marchiori (2005), Scott et al. (2006), Hollander and Prasjka (2006), Murray-Tuite (2008), propose different approach to identify critical links and evaluate network performance

Context: Mixed strategy adversarial game

- We adopt Bell (2003) the game-base approach to: Establish a vulnerability metric for all O-D pairs.
- Two-Player Game
  - Assumes perfect information
  - Non-cooperative

Role:	Router	Tester
Goal	Seeking shortest paths for all travelers	Disable Link(s) that most harm of network
Tool	Route assignment strategy	Link failure strategies

Formulation

The objective of the game between router and tester can be represented as a minimax formulation

$$\min_{\gamma}\max_{\rho} V(\boldsymbol{\gamma},\boldsymbol{\rho}) = \sum_{e\in E}\gamma_e^n \rho_e^n C_e^{F,n}$$

subject to

$$\sum_{e\in E}\rho_e = 1,\quad \rho \geq 0$$
$$\sum_{k_p\in K_p} h_{k_p} = 1,\quad h > 0$$
$$\sum_{k_p\in K_p} h_{k_p} a_{e,k_p} = \gamma_e$$

h_{k_p}	Path choice probability between O-D pair, p
a_{e,k_p}	Parameter that takes value 1 if $e \in k_p$ and 0 otherwise
d_p	Travel demand between O-D pair, p
C_e^F	Cost of edge e in failure scenario F
x_e^n	Edge use probability differential of edge e at iteration n
ρ_e^n	Probability the tester disables edge e at iteration n
γ_e^n	Probability the router chooses edge e at iteration n

Solution Approach

Step 0: Initialize network

Step 1: Update edge costs under Tester's failure scenario,

Step 2: Calculate *s*-expected edge costs,

Router

Step 3: Identify shortest path(s) for all *O-D pairs*

Step 4: Calculate Router's edge use probability differential

Step 5: Update Router's edge use probability using MSA

Tester

Step 6: Calculate Tester's edge failure probability,

Step 7: Calculate Network Vulnerability

Step 8: If no change, stop. Otherwise, go to Step 1

Calculate edge failure probability

To calculate edge failure probability, Bell (2008) proposes introducing an entropy function to the tester's level of this problem. Adding a weighted entropy function, the tester's problem has an explicit solution that is unique in edge failure probability. The modified objective function :

$$\min_{\gamma}\max_{\rho} V^{n}(\boldsymbol{\gamma},\boldsymbol{\rho}) = \sum_{e\in E}\gamma_e^n \rho_e^n C_e^{F,n} - \left(\frac{1}{\theta}\right)\sum_{e\in E}\rho_e^n \ln \rho_e^n$$

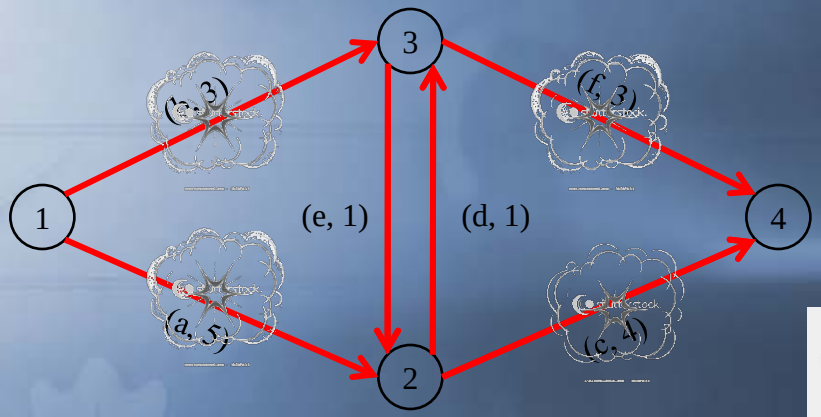
The explicit solution is:

$$\rho_e^{n+1} = \frac{\exp\left(\theta\gamma_e^n C_e^{F,n}\right)}{\sum_{s\epsilon E}\exp\left(\theta\gamma_s^n C_s^{F,n}\right)}$$

The parameter θ been called the aggressiveness of the tester, could also be interpreted as the confidence of their strategy.

Sample Demonstration

Figure below depicts the example network it contains four nodes and six edges, with the edge identifier and edge cost noted in parenthesis above each edge.

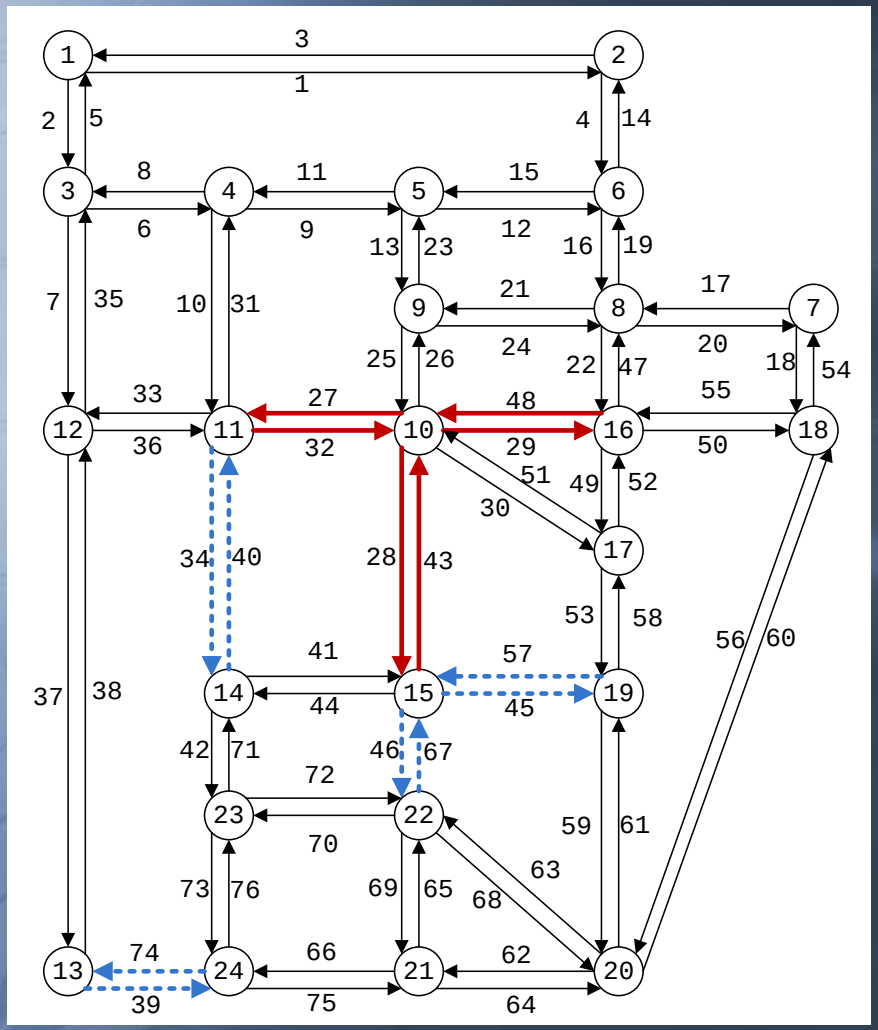


O-D Pair	Demand
(1, 2)	1
(1, 3)	1
(1, 4)	1
(2, 3)	1
(2, 4)	2
(3, 4)	1

	1st Iteration		2nd Iteration	
O-D Pair	SP	Cost	SP	Cost
(1, 2)	b-e	4	a	5
(1, 3)	b	3	a-d	6
(1, 4)	b-f	6	a-c	9
(2, 3)	d	1	d	1
(2, 4)	d-f, c	4	c	4
(3, 4)	f	3	e-c	5

		1st Iteration			2nd Iteration		
e	C_e^-	S_e^n	γ_e^n	ρ_e^{n+1}	S_e^n	γ_e^n	ρ_e^{n+1}
a	5	5	0	0.001	5.036	0.214	0.371
b	3	3	0.429	0.490	16.237	0.214	0.044
c	4	4	0.143	0.014	4.496	0.286	0.531
d	1	1	0.286	0.003	1.030	0.286	0.007
e	1	1	0.143	0.002	1.015	0.143	0.004
f	3	3	0.429	0.490	16.237	0.214	0.044

Sioux Falls network Application



The Sioux Falls network is the well-known and well-studied , it has 24 nodes, 76 edges and 552 O-D pairs.

High Critical

Median Critical

Low Critical

$\theta = 0.5$			$\theta = 1$			$\theta = 10$			Ukkusuri & Yushimito (*8*)	
Iter = 9114 RT= 63.5 s			Iter = 3442 RT = 23.0 s			Iter = 5049 RT= 40.3 s				
Edge #	Failure%	Use %	Edge #	Failure%	Use %	Edge #	Failure%	Use %	Edge #	Critical
4	31.51%	27.15%	4	34.08%	24.66%	4	34.78%	23.20%	39	80.34%
6	13.97%	29.87%	39	16.62%	29.03%	39	20.55%	28.87%	4	71.78%
12	13.96%	29.87%	6	15.69%	28.88%	6	17.66%	28.83%	**75**	67.87%
39	10.99%	28.67%	12	15.65%	28.88%	12	16.87%	28.82%	64	50.02%
20	4.93%	32.88%	36	5.23%	17.43%	36	8.32%	19.10%	20	46.23%
7	4.74%	24.46%	20	2.89%	32.87%	64	1.81%	18.84%	16	42.96%
2	2.98%	22.14%	2	2.87%	24.64%				1	30.43%
64	2.89%	14.66%	7	2.68%	24.47%				2	26.19%
75	2.62%	28.67%	64	1.95%	15.78%				60	20.17%
36	2.60%	14.31%	32	0.91%	17.42%				50	19.09%
32	1.27%	14.31%	75	0.91%	29.03%				7	17.61%
68	1.18%	14.01%	29	0.16%	17.43%				54	16.08%
16	0.95%	32.88%	68	0.11%	13.25%				37	12.65%
9	0.70%	29.87%	16	0.11%	32.87%				6	11.02%
29	0.62%	14.31%	9	0.05%	28.88%				**26**	9.02%
37	0.47%	17.24%	37	0.03%	17.25%				12	7.84%
60	0.35%	11.42%	60	0.02%	11.78%				**9**	7.79%
38	0.33%	14.83%	38	0.01%	14.47%				3	7.71%
50	0.20%	11.55%							68	4.63%
56	0.18%	8.20%							**76**	4.61%
18	0.18%	16.08%							**72**	4.48%
35	0.17%	7.73%							**30**	4.06%
65	0.14%	14.01%							**52**	3.99%
1	0.14%	4.51%							**32**	3.84%
47	0.07%	2.77%							**10**	3.30%
All other Failure % < 0.07%			All other Failure < 0.01%			All other Failure < 0.01%				

Bi-Modal Challenges

1. Well-behaved convex performance functions not applicable
2. Modeling access/multi-modal trips
3. Regional scale
4. Non-trivial path choice

Conclusions

- We have described a measure of network vulnerability based on many-to-many demand for a single mode.
- Adopts a game-theoretic framework and applies heuristics to solve both levels of the problem.
- Must be creative in addressing challenges associated with HSR/bi-modal networks.
- Data issues with regional scale.

Acknowledgment

- This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2008-ST-061-TS002. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

Thank you.