UNIVERSITY OF MASSACHUSETTS DARTMOUTH

A Game-Theoretic Method to Efficiently Assess the Vulnerability of a Dynamic Transportation Network

Venkateswaran Shekar[1], Samrat Chatterjee[2], Mahantesh Halappanavar[2], and Lance Fiondella[1]
[1]Department of Electrical and Computer Engineering, University of Massachusetts Dartmouth
[2]Pacific Nortwest National Laboratory

Outline

- Motivation
- Game Theoretic Vulnerability Assessment
- Deterministic Vulnerability Assessment
- Example scenario
- Conclusion
- Future Work

Motivation

- Continuing increase in city populations
  - Expect criticality of transportation infrastructure to increase
- Disaster planning, response, and recovery decision support systems
  - Often assume transportation network completely available
  - Unrealistic assumption may lead to suboptimal strategy

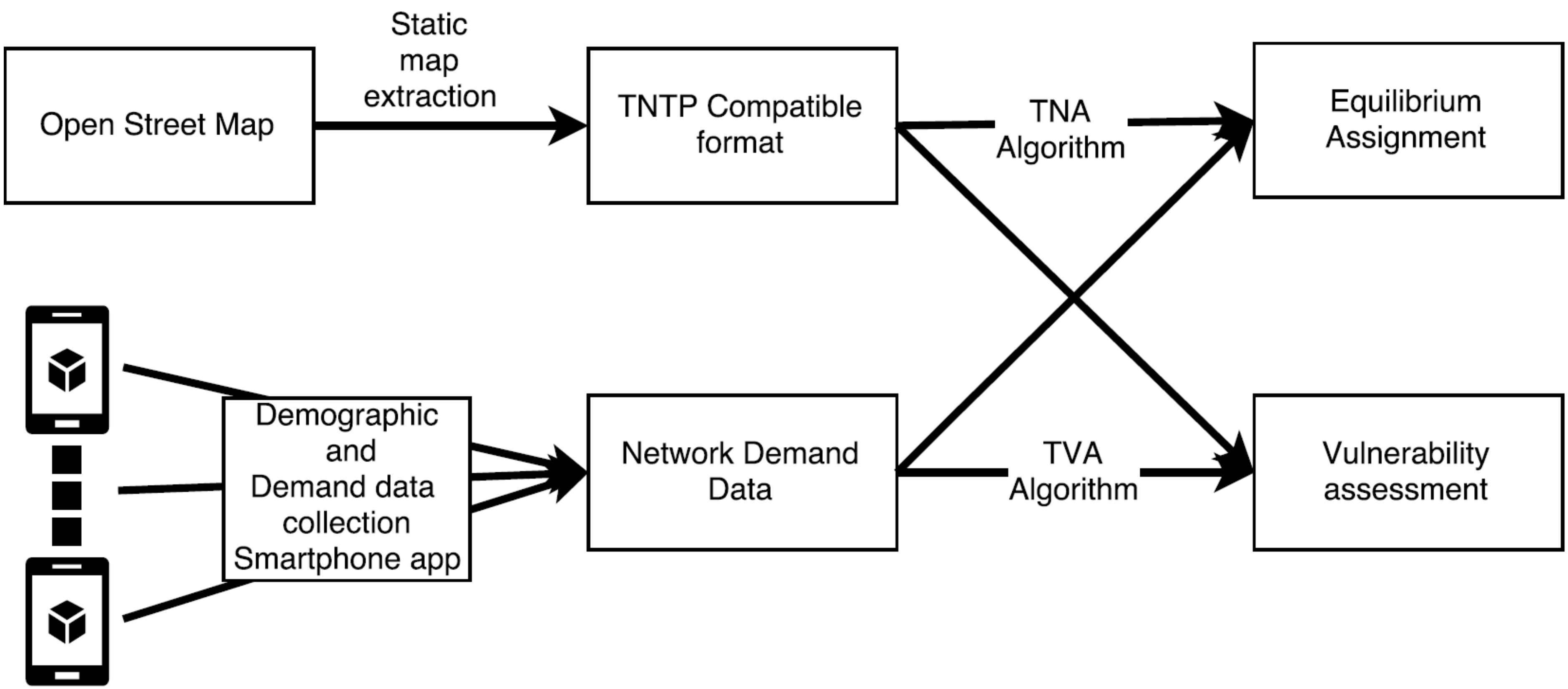
Static Traffic Assignment

- Previous transportation network vulnerability research performed in context of static traffic models
- Simplifies assumptions
  - Travel times of each link on route added together to compute travel time
  - Inflow and Outflow of link equal
  - Congestion occurs if Volume-to-Capacity ratio (V/C) > 1.0

Dynamic Traffic Assignment

- Travel demand function of time
- Explicit modeling of traffic flow dynamics
  – Ensures direct link between travel time and congestion
- Application of dynamic transportation models
  – Congestion and vulnerability assessment

Framework


Open Street Map
Static map extraction
TNTP Compatible format
TNA Algorithm
Equilibrium Assignment
Demographic and Demand data collection Smartphone app
Network Demand Data
TVA Algorithm
Vulnerability assessment

Deterministic Method

- For every edge e in network G
- For every time interval Δt_i in ΔT
  - Disable edge e during interval Δt_i
  - Record travel times of vehicles
  - Calculate ratio of disrupted travel time with undisrupted travel time
- **Problem**: Method is not scalable

Game Theory

- The analysis of competitive situations (or situations of conflicts) using mathematical models
- Involves one or more **players**
- Actions taken by players called **moves**
- A set of **outcomes** for each move
- An amount received for each outcome called **payoff**

Approach

- Two-player mixed strategy stochastic game
- Router vs Tester
- Router – Seeks strategy to distribute traffic over roads to minimize risk
- Tester – Develops attack strategy to maximally disrupt smooth flow of traffic
- Perfect knowledge – Strategy of adversary is immediately known

Simulation setup

- Transportation network represented as a graph $G(V, E)$, with V vertices and E edges
- Trips are characterized by demand $D_{|V|\times|V|}(t)$
- Simulation divided into k time intervals $\Delta T = < \Delta t_1 \ldots \Delta \mathrm{t_k} >$
- Disrupting a link renders it unavailable for interval Δt_i and is fully restored at Δt_{i+1}

Mini-max Formulation

$$\min_{\gamma} \max_{\rho} \mu^n(\gamma, \rho) = \sum_{i \in \Delta T} \sum_{e \in E} \gamma_{e,i}^n \rho_{e,i}^n \tau_{e,i}^n$$

μ^n system vulnerability in the n^{th} iteration
$\gamma_{e,i}^n$ usage probability of edge e in interval i and iteration n
$\rho_{e,i}^n$ link attack probability
$\tau_{e,i}^n$ heuristic link travel cost

Product is summed over all edges and intervals
to quantify system vulnerability

Probabilities

Link usage probability

$$\gamma_{e,i}^{n} = \frac{f_{e,i}^{n}}{\sum_{i \in \Delta T} \sum_{e \in E} f_{e,i}^{n}}$$

Tester attack probability

$$\rho_{e,i}^{n} = \frac{\tau_{e,i}^{n} \times \gamma_{e,i}^{n}}{\sum_{i \in \Delta T} \sum_{e \in E} (\tau_{e,i}^{n} \times \gamma_{e,i}^{n})}$$

$f_{e,i}^{n}$ traffic on edge e, interval i, in n^{th} iteration

Link costs

Link cost

$$C_e^n = \begin{cases} C_e^- & \text{if } \rho_e^n = 0 \\ C_e^+ = \beta \times |E| \times C_e^- & \text{if } \rho_e^n > 0 \end{cases}$$

S-expected link cost

$$S_{e,i}^{n+1} = \left(\left(1 - \rho_{e,i}^n\right) \times C_e^-\right) + \left(\rho_{e,i}^n \times C_e^+\right)$$

S-expected link costs with Method of Successive Averages (MSA)

$$\tau_{e,i}^{n+1} = \frac{1}{n^\alpha} S_{e,i}^{n+1} + \left(1 - \frac{1}{n^\alpha}\right) \tau_{e,i}^n$$

$\alpha > 1.0$ rate of convergence

Algorithm Initialization

Require: Road network G with v vertices and e edges
Require: Dynamic traffic demand data profile $D_{|V|\times|V|}(t)$
Require: Array of time intervals ΔT
Require: Maximum iterations N_{max}
1: Initialize iteration $n = 0$
2: Initialize system vulnerability $\mu^0 = 0$
3: **for** $i = 1$ to k **do**
4: **for** $e = 1$ to $|E|$ **do**
5: $\tau_{e,i}^1 = C_e^-$
6: **end for**
7: **end for**

Heuristic travel cost is initialized to free flow travel time

Algorithm

do

  $n = n + 1$

  $f_{e,i}^{n} = Simulate(G, \tau_{e,i}^{n})$

  for $i = 1$ to k **do**

    for $e = 1$ to $|E|$ **do**

      Calculate usage probability $\gamma_{e,i}^{n}$

      Calculate attack probability $\rho_{e,i}^{n}$

      Calculate link vulnerability

$$\mu_{e,i}^{n} = \gamma_{e,i}^{n} \times \rho_{e,i}^{n} \times \tau_{e,i}^{n}$$

      Update system vulnerability $\mu^{n} = \mu^{n} + \mu_{e,i}{}^{n}$

      Update s-Expected link cost $S_{e,i}^{n}$

      $\tau_{e,i}^{n+1} = MSA(S_{e,i}^{n+1}, \tau_{e,i}^{n})$

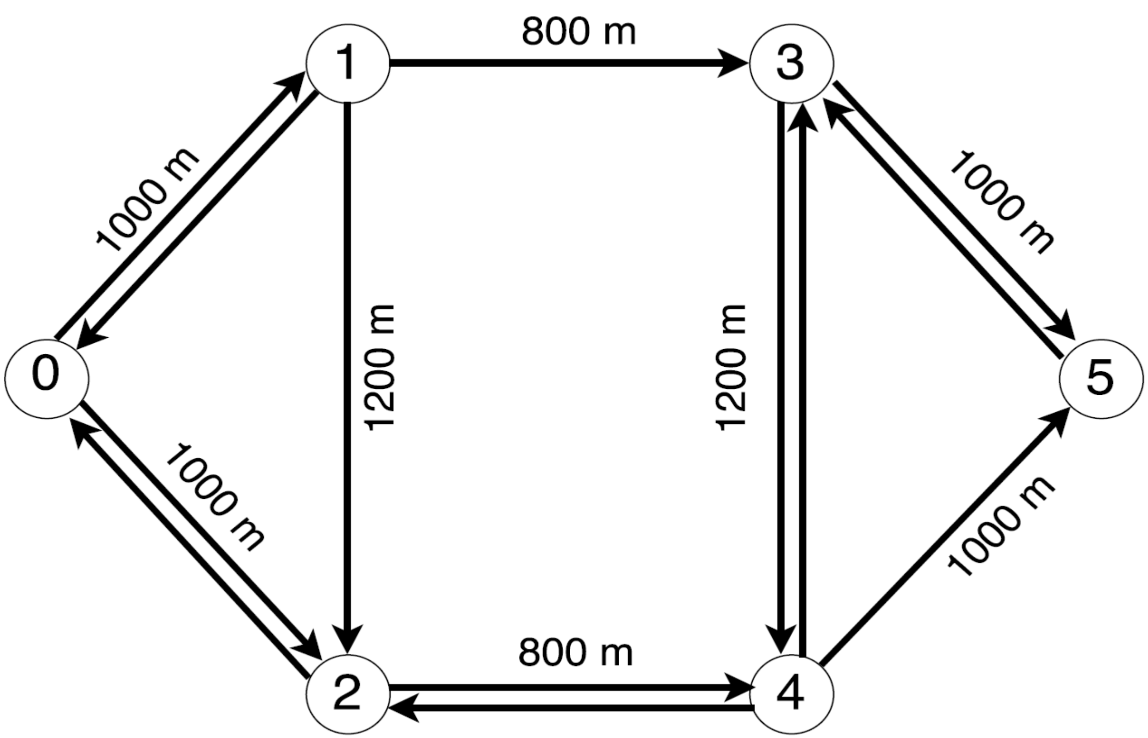
    end for

  end for

while $(|\mu^{n} - \mu^{n-1}| > \varepsilon)$ **or** $(n < N_{max})$

Algorithm terminates if convergence criterion is met or number of iterations exceeds N_{max}

Illustration

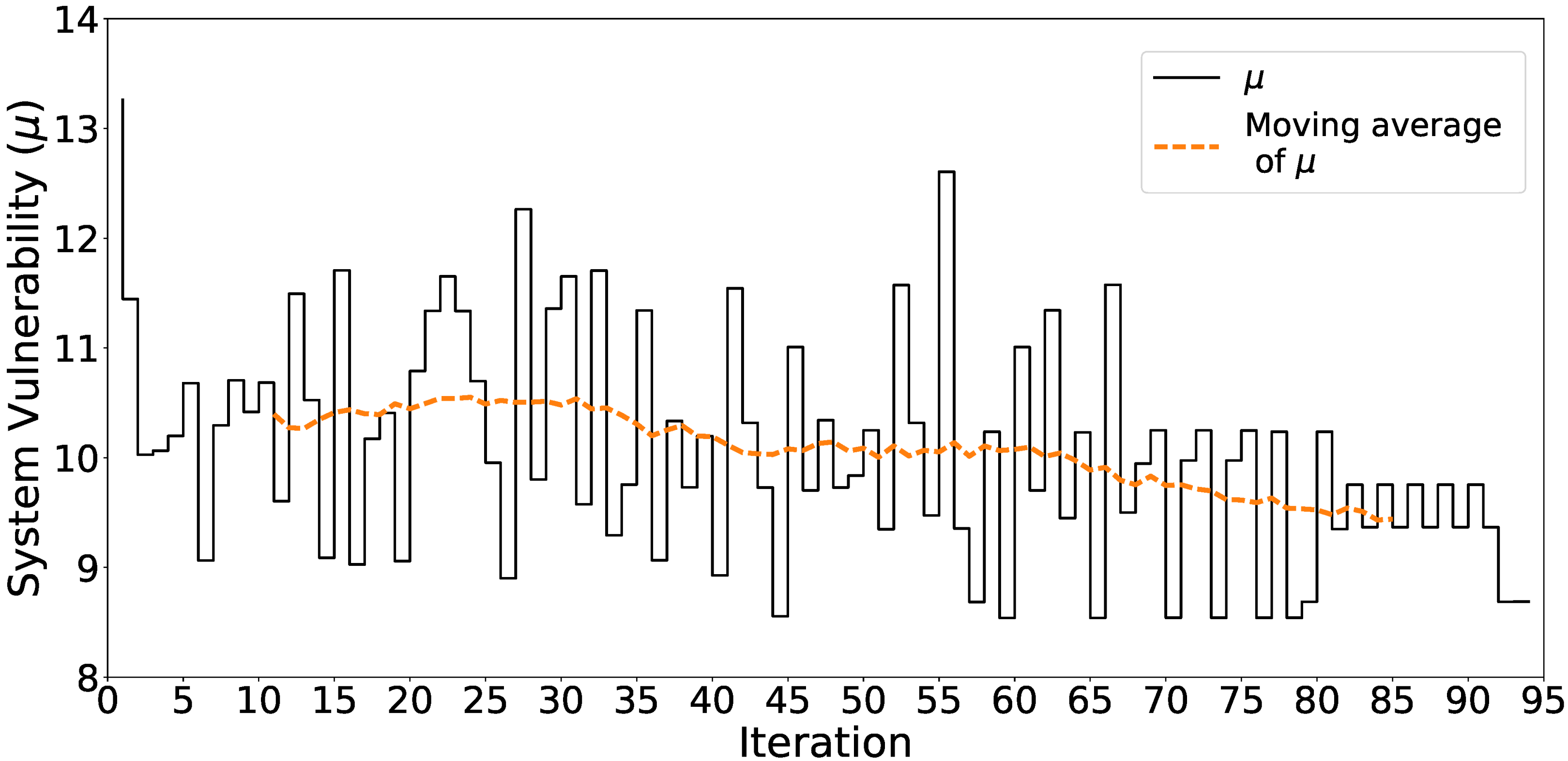


- Network Structure
  - 6 Nodes
  - 13 Links
- Speed Limit
  - 30 miles/hour
- Time intervals
  - Δt_1 = 0 – 500 sec
  - Δt_2 = 500 – 1000 sec
  - Δt_3 = 1000 – 1500 sec
- 500 vehicles depart node zero
- Destination is node five
- Simulator: SUMO

First three iterations for Δt_1

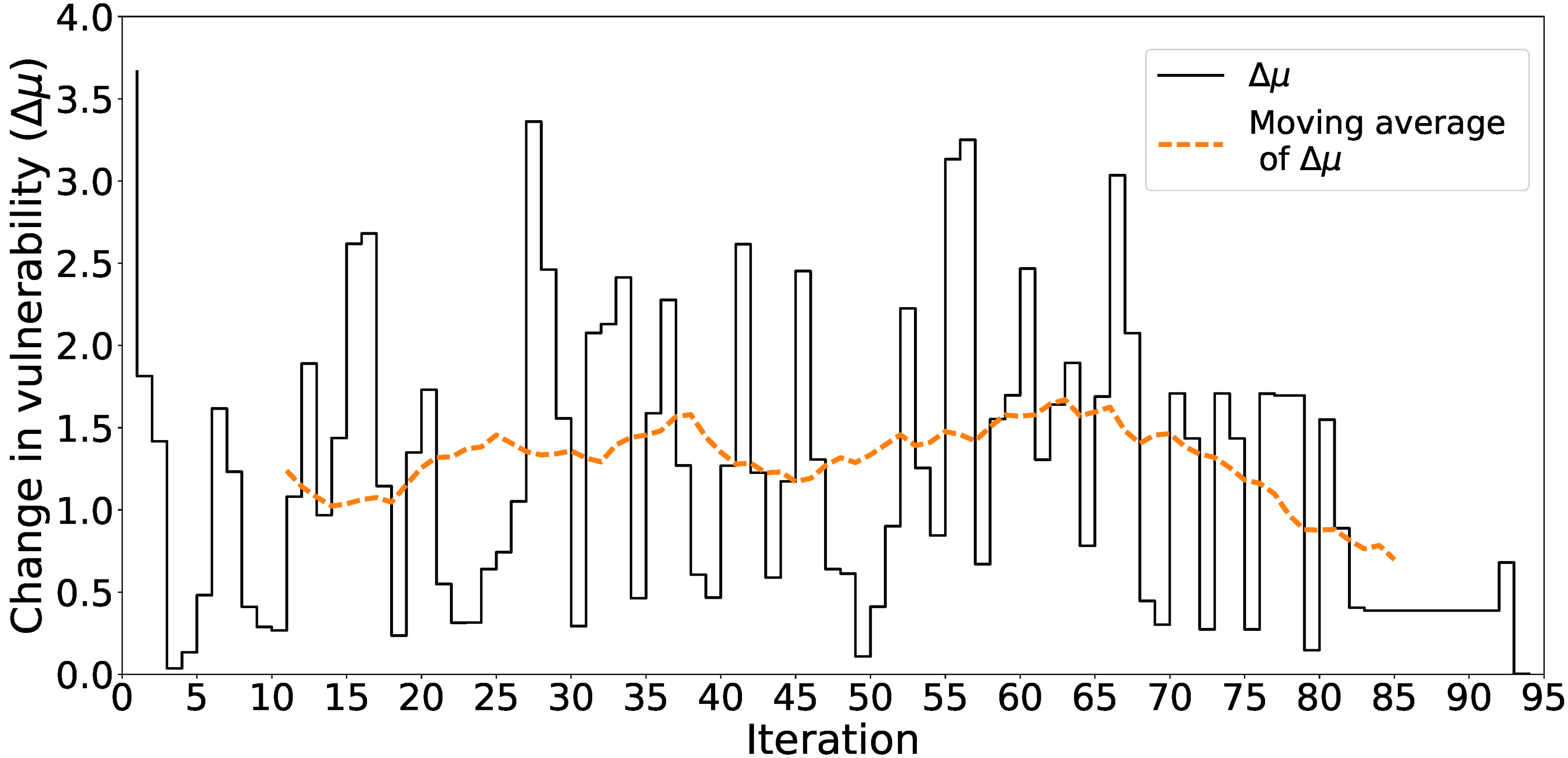
Link	Iteration 1			Iteration 2			Iteration 3		
Name	$\tau_{e,1}^{1}$	$\gamma_{e,1}^{1}$	$\rho_{e,1}^{1}$	$\tau_{e,1}^{2}$	$\gamma_{e,1}^{2}$	$\rho_{e,1}^{2}$	$\tau_{e,1}^{3}$	$\gamma_{e,1}^{3}$	$\rho_{e,1}^{3}$
*L*0,1	73.5399	0.0499	0.0528	120.1637	**0.1141**	**0.1380**	**138.9500**	0.0188	0.0231
*L*0,2	73.5399	**0.0717**	**0.0758**	**140.4437**	0.0000	0.0000	123.7100	**0.1017**	**0.1116**
*L*1,0	73.5399	0.0000	0.0000	73.5399	0.0000	0.0000	73.5400	0.0000	0.0000
*L*1,2	**88.5347**	0.0000	0.0000	88.2923	0.0000	0.0000	88.2900	0.0000	0.0000
*L*1,3	59.1946	0.0374	0.0319	81.8295	0.0794	0.0654	87.7800	0.0220	0.0171
*L*2,0	73.5399	0.0000	0.0000	73.5399	0.0000	0.0000	73.5400	0.0000	0.0000
*L*2,4	59.1946	0.0443	0.0377	85.9972	0.0034	0.0030	79.8300	0.0733	0.0520
*L*3,4	**88.5347**	0.0000	0.0000	88.5347	0.0000	0.0000	88.5300	0.0000	0.0000
*L*3,5	73.7957	0.0458	0.0486	116.8651	0.0892	0.1049	129.3300	0.0451	0.0518
*L*4,2	59.1946	0.0000	0.0000	59.1946	0.0000	0.0000	59.1900	0.0000	0.0000
*L*4,3	**88.5347**	0.0000	0.0000	88.5347	0.0000	0.0000	88.5300	0.0000	0.0000
*L*4,5	73.7957	0.0403	0.0428	111.6604	0.0172	0.0193	106.4700	0.0749	0.0708
*L*5,3	73.7957	0.0000	0.0000	73.7957	0.0000	0.0000	73.8000	0.0000	0.0000

Network Vulnerability (μ)



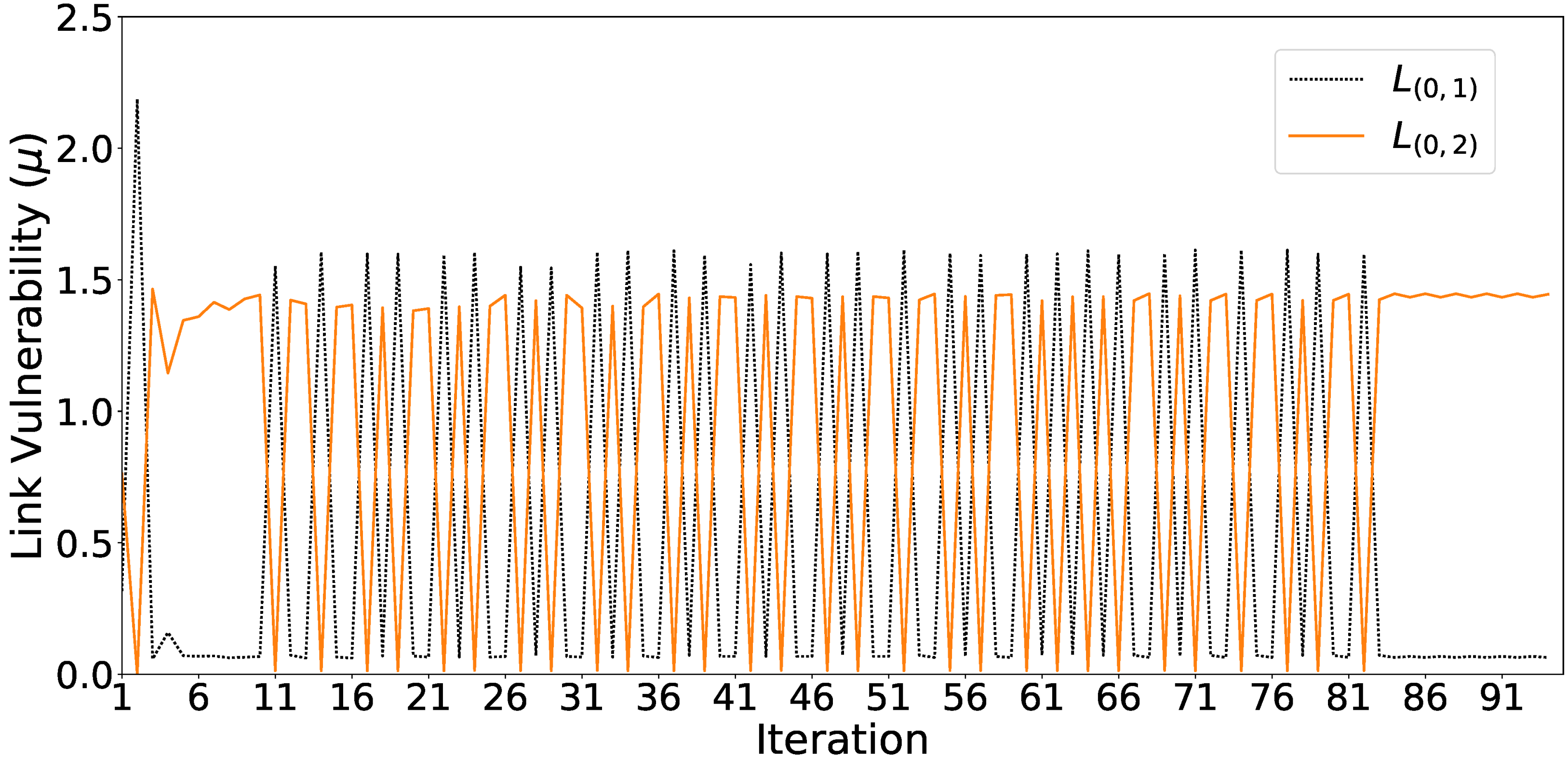
Variations in vulnerability decrease after 80th iteration

Change in vulnerability ($\Delta\mu$)



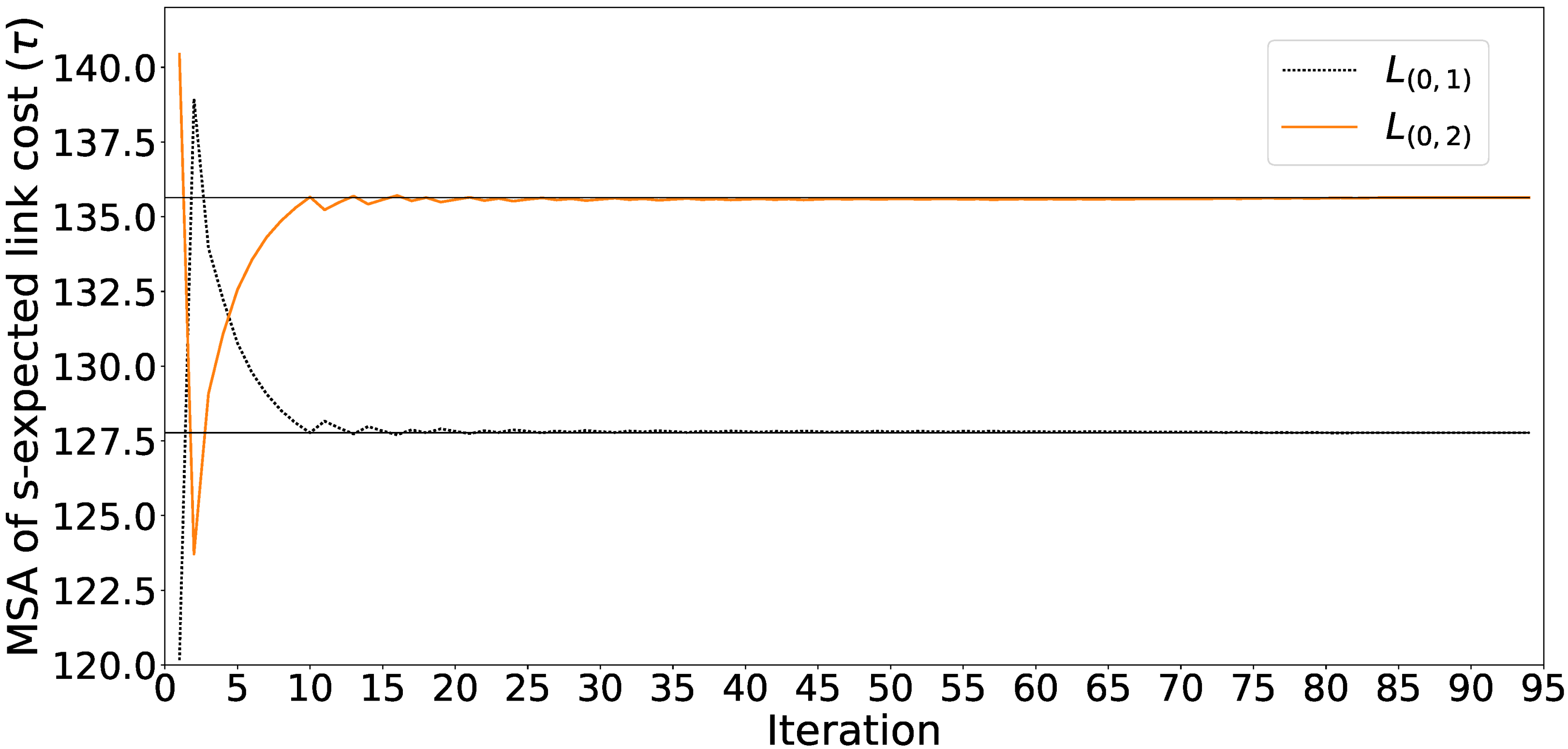
MSA places less emphasis on later strategies, forcing convergence

Link vulnerability in interval Δt_1



Link level vulnerability oscillates until a stable solution is found

MSA in interval Δt_1



Crossing link cost at convergence explains oscillation

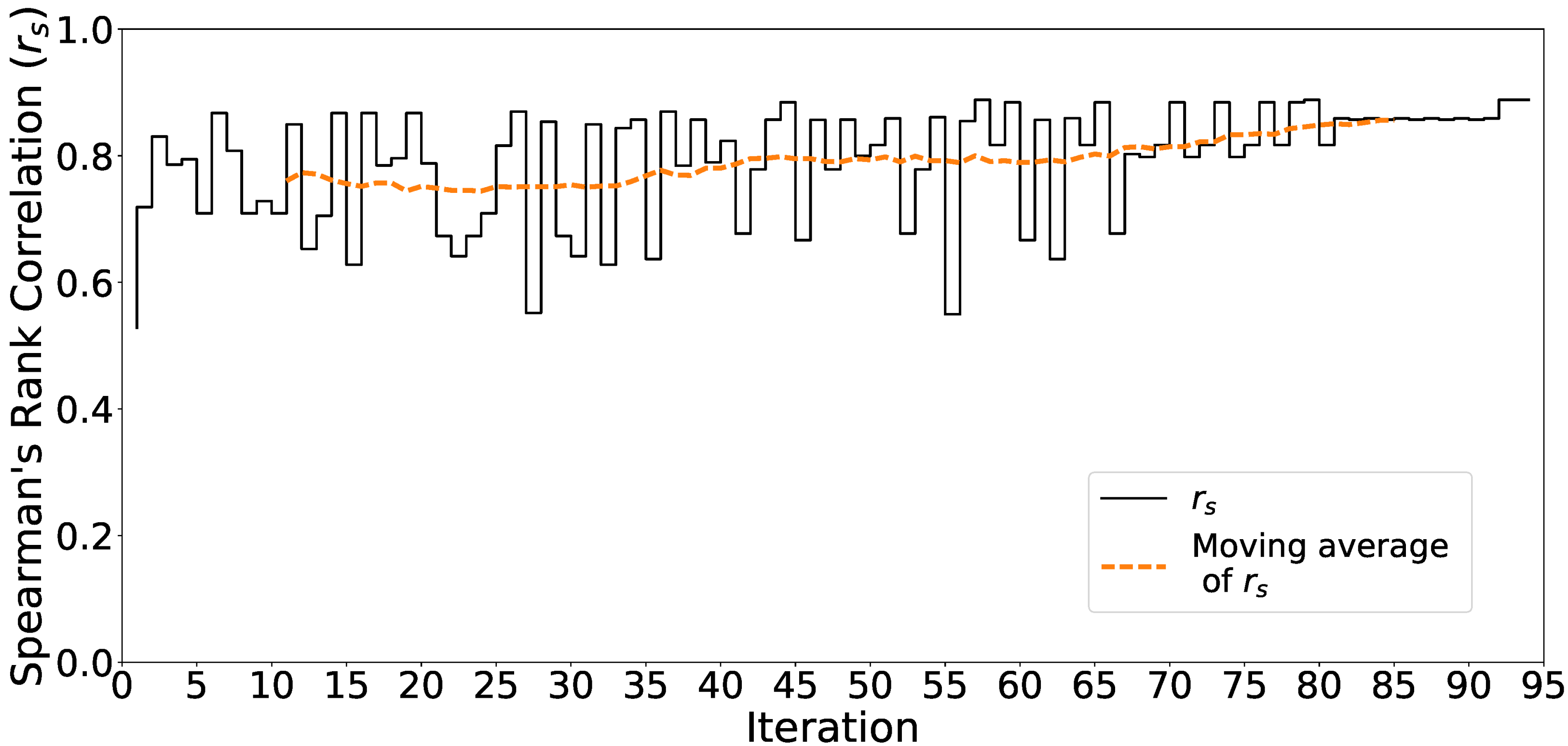
Comparison of game-theoretic and deterministic methods

Link			The image part with relationship ID rId2 was				The image part with relationship ID rId2 was				The image part with relationship ID rId2 was	
Name	The image part with relationship ID rId2 was not found in the file.	The image part with relationship ID rId2 was not found in the file.	TT	TT rank	The image part with relationship ID rId2 was not found in the file.	The image part with relationship ID rId2 was not found in the file.	TT	TT rank	The image part with relationship ID rId2 was not found in the file.	The image part with relationship ID rId2 was not found in the file.	TT	TT rank
$L_{0,1}$	0.0639	15	1665	11	0.1394	12	1658	14	0.0817	14	1669	8
$L_{0,2}$	1.4447	1	1672	7	1.0896	5	1664	12	1.2558	2	1668	9
$L_{1,0}$	0.0000	20	1638	16	0.0000	20	1638	16	0.0000	20	1638	16
$L_{1,2}$	0.0000	20	1638	16	0.0000	20	1638	16	0.0000	20	1638	16
$L_{1,3}$	0.0071	19	1672	7	0.0380	17	1667	10	0.0390	16	1769	2
$L_{2,0}$	0.0000	20	1638	16	0.0000	20	1638	16	0.0000	20	1638	16
$L_{2,4}$	0.4149	7	1702	5	0.3081	9	1738	3	0.3085	8	1817	1
$L_{3,4}$	0.0000	20	1638	16	0.0000	20	1638	16	0.0000	20	1638	16
$L_{3,5}$	0.1323	13	1645	15	0.1475	11	1659	13	0.1489	10	1735	4
$L_{4,2}$	0.0000	20	1638	16	0.0000	20	1638	16	0.0000	20	1638	16
$L_{4,3}$	0.0306	18	1638	16	0.0000	20	1638	16	0.0000	20	1638	16
$L_{4,5}$	0.8295	6	1668	9	1.1028	4	1681	6	1.1038	3	1735	4
$L_{5,3}$	0.0000	20	1638	16	0.0000	20	1638	16	0	20	1638	16

Comparison of game-theoretic and deterministic methods (2)

- Spearman's rank correlation
  - Correlation $r_s = 0.8882$ at convergence
  - p-value = 4.63×10^{-14}
    - Strong correlation between approaches
- As size of network increases, number of simulations will decrease

Comparison of game-theoretic and deterministic methods (3)



Correlation never below $r_s = 0.8$ and trend increases

Conclusion

- Presented a game-theoretic approach to assess dynamic vulnerability of transportation network
- Considers relative vulnerability of all links and time intervals in parallel
- Results indicate that game-theoretic approach achieves strong correlation to slower deterministic method

Future Research

- Address performance and accuracy challenges to scale game- theoretic approach to larger networks
- Utilize game-theoretic dynamic transportation network vulnerability approach to allocate limited defensive resources to links at specified times to mitigate vulnerability most effectively