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

Venkateswaran Shekar[a], Lance Fiondella[a],
Samrat Chatterjee[b], and Mahantesh Halappanavar[b]
[a] University of Massachusetts Dartmouth, USA
[b] Pacific Northwest National Laboratory, Richland, USA

Abstract: Many transportation network vulnerability assessment methods are based on the static traffic assignment problem, which determines the distribution of traffic demand over a network for a static snapshot in time. However, transportation networks are dynamic because demand is time-varying. This paper proposes a mixed strategy, stochastic game-theoretic approach to determine the relative criticality of links in different time intervals. We quantitatively compare the results of the proposed approach with deterministic methods that do not scale efficiently. Our results indicate that the criticalities identified by the game-theoretic approach are strongly correlated with the slower deterministic method, suggesting that the proposed approach will enable efficient vulnerability assessment of dynamic transportation networks.
Keywords: Transportation Network, Vulnerability Assessment, Game Theory, Modeling and Simulation.

1. INTRODUCTION

Transportation networks play a critical role in the smooth functioning of a nation's economy and ensuring its security. Moreover, these networks are critical to the Emergency Services Sector (ESS), which includes a system of prevention, preparedness, response, and recovery from natural and man-made disasters. Areas with high population densities are of particular concern due to the effect of disruptions on continuity of services and the well-being of the population. Thus, to prevent major disruptions, quantifying transportation network vulnerability and identifying critical links that may be the prime targets for attacks is essential. Transportation networks are complex because their utilization throughout a 24-hour period is dynamic, suggesting that vulnerability is a function of both location and time. Several previous studies have proposed transportation network vulnerability assessment methods [1] and strategies to quantitatively enhance resilience. Commonly used techniques include traditional optimization methods and game theoretic approaches. However, most previous approaches treat transportation networks as static graphs, assessing structural vulnerability, but do not consider their time-varying dynamics.

Optimization methods include the work of Jenelius *et al*. [2] who proposed methods to answer questions such as "Which regions are most susceptible to disruption in the transportation system?" by defining "exposure," where a node is vulnerable if the loss of a small number of links significantly reduces the accessibility to that node. Murray-Tuite and Mahmassani [3] developed a vulnerability index to consider traffic flow, link capacities, travel times, and the availability of alternate routes. Scott *et al*. [4] proposed a network robustness index (NRI), which is computed as the increase in user equilibrium travel time when a specific link is closed. Sullivan *et al*. [5] extended this NRI to the case where links are only partially degraded. Nagurney and Qiang [6] also studied network robustness but focused on the travel cost implications. In [7], Demšar *et al*. combined graph modeling with connectivity analysis as well as topological measures to quantify the vulnerability of a network's elements and identify critical locations within the network.

Examples of game theoretic approaches include Bell and Cassir [8] who presented a deterministic user equilibrium traffic assignment that is equivalent to the mixed-strategy Nash equilibrium of an n-player, non-cooperative game. Bell [9] proposed a mixed strategy stochastic game between a router seeking minimum cost paths for vehicles and a tester attempting to maximize the cost of these trips. Murray-Tuite and Mahmassani [3] developed a bi-level non-zero-sum game between an attacker and the traffic

management agency to quantify vulnerability. Wang *et al*. [10] incorporated static traffic assignment and the corresponding concepts of network congestion into a two player attacker-defender game, sorting link attack and defense strategies and interpreting them as priority lists of the most critical links. Fiondella *et al*. [11] combine game theoretic vulnerability assessment and metaheuristic optimization to allocate limited resources to defend the U.S. high-speed rail network as it expands in a discrete sequence of times steps.

The past research discussed above was performed in the context of Static Traffic Assignment (STA) methods, which only consider a snapshot of the network in time and does not account for the time-varying nature of traffic demand. To study the criticality of links as a function of time Dynamic Traffic Assignment (DTA) methods explicitly model travel demand as a function of time which allow dynamic vulnerability mitigation strategies that consider where and when to deploy defenses within the network. Compared to STA research, relatively few studies have considered dynamic vulnerability strategies. For example, Duanmu *et al*. [12] assessed the utility of effective information dissemination on evacuation, but limited analysis to a case study with three primary evacuation routes. Shekar *et al*. [13] employed dynamic transportation simulation methods as the basis of a systematic approach, which disconnects one link at a time to measure the increase in network travel time over a nominal scenario where all links work. However, this approach was difficult to scale because a simulation is required for each edge of a network. Moreover, individual simulations require additional time for larger networks.

To advance dynamic transportation network vulnerability research, this paper presents a game-theoretic method that uses dynamic transportation simulation. Game theory enables the consideration of each link/time interval in a single simulation, effectively achieving parallelism that scales arbitrarily with the size of the network. To avoid the complexity associated with games on graphs, we implemented the method of successive averages to ensure that the game converges. Moreover, we quantitatively compare the proposed approach with the deterministic method [13]. Our results indicate that the game-theoretic approach achieves strong correlation with the deterministic approach, suggesting that it may be a viable alternative to improving the scalability of dynamic transportation network vulnerability assessment without compromising accuracy.

The remainder of the paper is organized as follows. Section II describes a game-theoretic method to assess the vulnerability of a dynamic transportation network, including its formulation and algorithm. Section III illustrates the method through a simple network representing an evacuation scenario. Section IV provides conclusions and identifies future research.

2. GAME THEORETIC APPROACH

This section presents a two-player game to assess the vulnerability of a dynamic transportation network, where the traffic management authority and attacker are referred to as the "router" and "tester" respectively. The game is iterative with the router and tester revising their strategies in odd and even turns. The router seeks to identify a strategy to distribute traffic over the links of the network in a manner that ensures the vehicles reach their destinations in a timely fashion but also minimizes their risk exposure. Conversely, the tester wishes to develop an attack strategy that maximally disrupts the smooth flow of traffic.

The game is one of perfect knowledge in which the latest strategy of the adversary becomes immediately available to its opponent. For the sake of analysis, this is pessimistic with respect to the defender's goals in the sense that the tester has all inside information in real time and is therefore able to counteract the router's most recent attempt to work around the tester. Similarly, the assumption of perfect knowledge is optimistic in the sense that the router is aware of how the tester will revise its attack strategy. In practice, this game can be thought of as an objective exercise between the defender and how they believe a rational adversary would behave. This requires accurate characterization of the tester. The combination of alternating turns and perfect knowledge can lead to cycles in the strategies selected by the router and tester, which results in lack of convergence in the sequence of revisions to the strategies of the adversaries. To avoid this, the game implements the method of successive averages in which greater

emphasis is placed on earlier iterations. This places greater weight on earlier iterations that reflect the most likely strategies, including those that are most likely to be repeated because of the alternating game play.

2.1. Game Formulation

The transportation network is represented as a directed graph $G(V, E)$, where $V$and E are the sets of vertices and edges which respectively represent the intersections and road segments. Trips are characterized by the demand profile $D_{|V|\times|V|}(t)$, which is a $|V| \times |V|$ dimension matrix and entry $D_{i,j}(t)$ indicates the number of vehicles commencing travel at integer time steps $t \in (0, T_{\max})$ from vertex i with destination j. For the sake of analysis, the simulation is divided into k time intervals of equal length

$$\Delta T = \langle \Delta t_1, \Delta t_2, \dots, \Delta t_i, \dots, \Delta t_k \rangle,$$

which represent the times at which the tester can disable a particular link.

Disrupting a link renders it unavailable for the entire duration of the time interval Δt_i and the link is restored to full capacity at the beginning of the next interval Δt_{i+1}. This approach allows us to objectively compare disruptions of equal length at different times and locations to assess their relative criticality with respect to the resulting increase in travel time. It also allows for direct comparison with our past method [13] which implemented a deterministic approach that disabled each link individually and simulated the network to identify the increase in travel time over a baseline where all links are available. The reader may note that the assumption of a single disruption at uniform and non-overlapping time intervals imposed on the deterministic and proposed game-theoretic approach can be relaxed and that it is possible to consider more complex scenarios in which there is more than one disruption and these disruptions are of non-uniform length with arbitrary recovery profile back the nominal case, where the link returns to the state where it is capable of conveying the volume of traffic prior to disruption.
Equation (1) represents the mini-max formulation between the router and the tester.

$$\min_{\gamma} \max_{\rho} \mu^n(\gamma, \rho) = \sum_{i\in\Delta T} \sum_{e\in E} \gamma^n_{e,i} \rho^n_{e,i} \tau^n_{e,i} \tag{1}$$

where μ^n represents the system vulnerability in the n^{th} iteration, which is computed as the product of (i) the usage probability of edge e in interval i and iteration n ($\gamma^n_{e,i}$) (ii) the corresponding link attack probability ($\rho^n_{e,i}$), and (iii) heuristic link travel cost ($\tau^n_{e,i}$). This product is summed over all edges and time intervals, which quantifies the contribution of each combination of location and time to network vulnerability.
Equation (1) is subject to the following constraints

$$\sum_{i\in\Delta T} \sum_{e\in E} \gamma_{e,i} = 1 \tag{2}$$

$$\sum_{i\in\Delta T} \sum_{e\in E} \rho_{e,i} = 1 \tag{3}$$

which may be interpreted as the router and tester strategies respectively because these vectors quantify the probability that the router and attacker use or attack each link in any one of the specified time intervals. Thus, these strategies consider both *where* potential vulnerabilities may exist as well as *when* they arise.

2.2. Algorithm

Algorithm 1 provides the pseudo code of the proposed game-theoretic approach to assess the vulnerability of a dynamic transportation network. The router begins the game by assigning vehicles to the network in a manner that minimizes travel time. This approach represents the ideal scenario in which

the router attempts to solve the standard dynamic transportation network traffic assignment problem, but disregards the presence of a malicious tester. To maximize disruption, the tester observes the state of the network under these nominal conditions and then determines attack probabilities. In subsequent iterations, the router and tester revise their path selection and attack strategies until convergence is achieved.

Algorithm 1 Game-theoretic transportation network vulnerability assessment algorithm

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**
8: **do**
9: $n = n + 1$
10: $f_{e,i}^n = Simulate(G, \tau_{e,i}^n)$
11: **for** $i = 1\ to\ k$ **do**
12: **for** $e = 1\ to\ |E|$ **do**
13: Calculate usage probability $\gamma_{e,i}^n$ // Eq (4)
14: Calculate attack probability $\rho_{e,i}^n$// Eq (5)
15: Calculate link vulnerability
$$\mu_{e,i}^n = \gamma_{e,i}^n \times \rho_{e,i}^n \times \tau_{e,i}^n$$
16: Update system vulnerability $\mu^n = \mu^n + \mu_{e,i}{}^n$
17: Update s-Expected link cost $S_{e,i}^n$ // Eq (6)
18: $\tau_{e,i}^{n+1} = MSA(S_{e,i}^{n+1}, \tau_{e,i}^n)$ // Eq (8)
19: **end for**
20: **end for**
21: **while** $(|\mu^n - \mu^{n-1}| > \varepsilon)\ or\ (n < N_{\max})$

Algorithm Input

Inputs to the algorithm include the graph of the road network, $G(V, E)$ with v vertices and e edges, dynamic traffic demand profile $D_{|V|\times|V|}(t)$, an array of time intervals ΔT, and the maximum number of turns to play the game, N.

Steps 1-7: Initialization

Before starting the game, all parameters are initialized as shown in steps one through seven. System vulnerability in the zeroth iteration μ_i^0 is initialized to zero to prevent the game from converging prematurely after the first iteration. For each time interval i and edge e, the link costs, $\tau_{e,i}^1$ are initialized to the free flow travel time denoted C_e^-.

Steps 9-10: Run simulation

The network is simulated using the present link weights, $\tau_{e,i}^n$, which produces the traffic (number of vehicles per second) on edge e during time interval i in the n^{th} iteration ($f_{e,i}^n$).

Step 13: Calculate link usage probabilities

The link usage probability is

$$\gamma_{e,i}^{n} = \frac{f_{e,i}^{n}}{\sum_{i \in \Delta T} \sum_{e \in E} f_{e,i}^{n}} \tag{4}$$

which is the ratio of traffic on edge e during time interval i in the n^{th} iteration over the sum of the traffic on all edges in all time intervals in the n^{th} iteration.

Step 14: Calculate tester attack probabilities

Based on the link usage probabilities determined in the previous step, the tester formulates a plan of attack by assigning link failure probabilities to maximize travel time disruption. Thus, the link attack probability is

$$\rho_{e,i}^{n} = \frac{\tau_{e,i}^{n} \times \gamma_{e,i}^{n}}{\sum_{i \in \Delta T} \sum_{e \in E} (\tau_{e,i}^{n} \times \gamma_{e,i}^{n})} \tag{5}$$

which is the ratio of the product of link cost ($\tau_{e,i}^{n}$) and link usage ($\gamma_{e,i}^{n}$) on edge e during time interval i in the n^{th} iteration over the sum of these terms on all edges in all time intervals in the n^{th} iteration.

Step 15, 16: Update system vulnerability

The vulnerability for link e during interval i in iteration n ($\mu_{e,i}^{n}$) is computed according to Equation (1) as the product of link usage, attack probability, and link cost.

Step 17: Calculate s-Expected link cost

The s-expected cost of each link and time interval is revised for use in iteration $n + 1$ according to the attack probabilities determined by Equation (5).

$$S_{e,i}^{n+1} = ((1 - \rho_{e,i}^{n}) \times C_{e}^{-}) + (\rho_{e,i}^{n} \times C_{e}^{+}) \tag{6}$$

where C_{e}^{-} is the free flow travel time cost and C_{e}^{+} is the link's cost in the disrupted state

$$C_{e}^{n} = \begin{cases} C_{e}^{-} & if \rho_{e}^{n} = 0 \\ C_{e}^{+} = \beta \times |E| \times C_{e}^{-} & if \rho_{e}^{n} > 0 \end{cases} \tag{7}$$

Here, β is a penalty coefficient (risk aversion factor) and $|E|$ is the number of links in the network. The term $|E|$ is included to normalize across graphs of different sizes and $\beta > 1/|E|$ ensures that $C_{e}^{+} > C_{e}^{-}$.

Step 18: Calculate s-Expected Link Cost with Method of Successive Averages

To ensure that convergence, it is necessary to reduce the impact of periodically cycling through a sequence of attack and defense strategies. This is accomplished by applying the method of successive averages (MSA), which assigns greater weight to the tester's earlier strategies and the router's response.

$$\tau_{e,i}^{n+1} = \frac{1}{n^{\alpha}} S_{e,i}^{n+1} + \left(1 - \frac{1}{n^{\alpha}}\right) \tau_{e,i}^{n} \tag{8}$$

where a value of $\alpha > 1.0$ accelerates the rate of convergence. Note $\lim_{n \to \infty} \tau_{e,i}^{n+1} - \tau_{e,i}^{n} = 0$, and convergence will occur for some finite $n > N$.

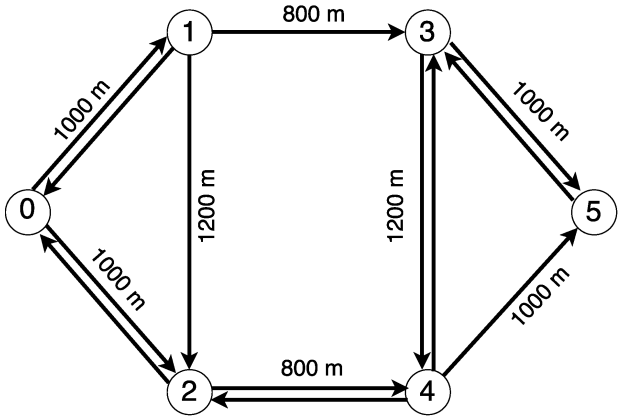
Step 21: Convergence Criteria

The game stops when the difference in system vulnerability of two consecutive iterations determined by Equation (1) is less than a specified threshold $\Delta\mu = |\mu^{n} - \mu^{n-1}| < \varepsilon$ or if the number of iterations exceeds a user defined value N_{max}.

3. ILLUSTRATION

The game theoretic dynamic vulnerability assessment model is demonstrated through a case study of a simple network accompanied by a detailed description of the algorithm. Figure 1 shows the structure of the simple network used to demonstrate the approach.

Figure 1 Structure of simple network



The network G consists of $v = 6$ vertices (nodes) and $e = 13$ directed edges (links), which are labeled with their distance in meters. The speed limit on each edge was set to 30 miles/hour (13.41 m/s).

To simulate an evacuation scenario, a total of 500 vehicles are considered in which trips are generated at the rate of one vehicle every two time steps ($t < 1{,}000$) originating from node zero with the goal of reaching node five. Thus, the nonzero entries of the demand matrix are $d_{0,5}(2t) = 1, (0 \leq t \leq 998)$. The array of time intervals is $\Delta T = (\Delta t_1 = (0, 500), \Delta t_2 = (500, 1000), \Delta t_3 = (1000, 1500))$. The risk aversion factor is set to $\beta = 1$, the convergence criterion $\varepsilon = 0.01$, maximum number of iterations $N_{max} = 250$, and convergence factor $\alpha = 2.0$.

3.1. Iterations one to three

Table 1 shows the values of the link cost τ_e, router's link use probability γ_e, and tester's attack probability ρ_e in the first time interval Δt_1 through the first three iterations. Table 1 indicates that the link travel time in the first iteration (τ_e) is simply the free flow travel time, as noted in Section 2. The reader may note that the calculations are computed over each time interval Δt_1 through Δt_3, which is necessary for the method to quantify the relative criticality of each pair of link and time interval. However, the table and discussion have been limited to Δt_1 for detailed explanation of the algorithm.

Simulation with these link travel times produces the number of vehicles on edge e during the first time interval of the first iteration ($f_{e,1}^1$), which are subsequently used to compute the router probabilities and attacker probabilities with Equations (4) and (5) respectively. For example, both links $L_{0,1}$ and $L_{0,2}$ possess travel cost 73.5399. However, during simulation, structural asymmetry in the graph produces unequal amounts of traffic on these two edges in the interval Δt_1 such that $f_{(0,1),\Delta t_1}^1 = 10.626$ vehicles/sec and $f_{(0,2),\Delta t_1}^1 = 15.254$ vehicles/sec respectively. Moreover, the total flow over all intervals and links in the network is $f^1 = 212.752$. Thus, $\gamma_{(0,1),\Delta t_1}^1 = \frac{10.626}{212.752} = 0.0499$ and $\gamma_{(0,2),\Delta t_1}^1 = \frac{15.254}{212.752} = 0.0717$, while $\rho_{(0,1),\Delta t_1}^1 = \frac{73.5399 \times 0.0499}{69.52} = 0.0528$ and $\rho_{(0,2),\Delta t_1}^1 = \frac{73.5399 \times 0.0717}{69.52} = 0.0758$. This is followed by the computation of system vulnerability shown in Equation (1). Therefore the vulnerability of link $L_{0,1}$ becomes $\mu_{(0,1),\Delta t_1}^1 = \tau_{(0,1),\Delta t_1}^1 \times \gamma_{(0,1),\Delta t_1}^1 \times \rho_{(0,1),\Delta t_1}^1 = 73.5399 \times 0.0499 \times 0.0528 = 0.3997$.

Equation (6) is used to calculate the s-expected link costs for the next iteration. For example, for the link from zero to one, $S^2_{(0,1),\Delta t_1} = (1 - 0.0528) \times 73.5399 + 0.0528 \times 1 \times 13 \times 73.5399 = 120.1637$ and $S^2_{(0,2),\Delta t_1} = 140.4437$ for the link from zero to two. Subsequently, the MSA of the s-expected cost is calculated according to Equation (8) such that $\tau^2_{(0,1),\Delta t_1} = \left(\frac{1}{1^2}\right) \times 120.1637 \left(1 - \frac{1}{1^2}\right) \times 73.5399 = 120.1637$ and $\tau^2_{(0,2),\Delta t_1} = 140.4437$. Thus, the router's preference to utilize $L_{0,1}$ and the attacker's interest in attacking this link coupled with the router's risk aversion increases the cost of $L_{0,1}$, but not as much as the router's aversion to $L_{0,2}$.

In the second iteration, the router sends all traffic through $L_{0,1}$, avoiding $L_{0,2}$ altogether. This occurs because the shortest path from node zero to five through $L_{0,1}$ is lower than the shortest path through $L_{0,2}$ and the demand pattern $D(t)$ generates a single trip every two time steps. Thus, the combination of link cost and travel demand pattern leads the router to prefer $L_{0,1}$ over $L_{0,2}$ and the attacker revises their strategy accordingly, concentrating their attack probability on $L_{0,1}$. However, the method of successive averages retains memory of the threat to $L_{0,2}$ in the first iteration such that $\tau^3_{(0,2),\Delta t_1}$ does not simply revert to the free flow travel time. As a result, in iteration three the router shifts most but not all of the traffic from $L_{0,1}$ to $L_{0,2}$.

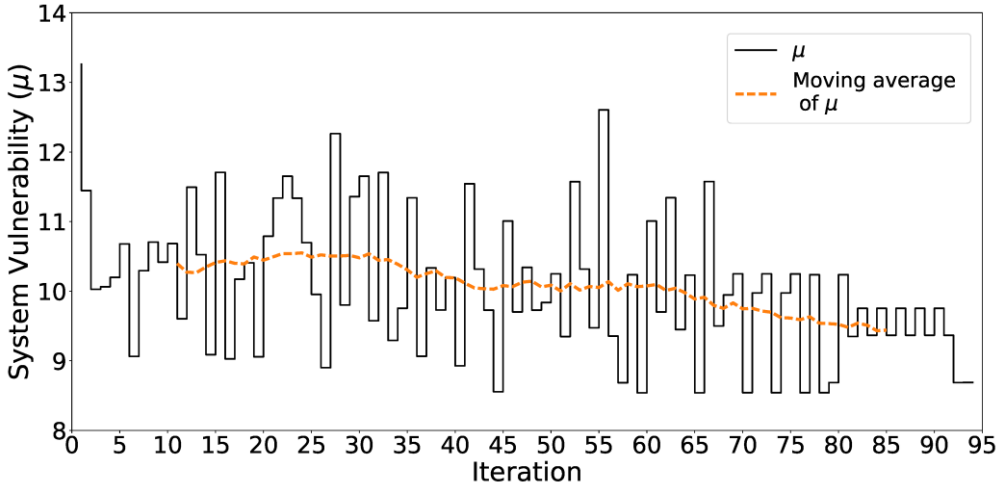
Table 1: Link cost, link use probability, and link failure probability, in time interval t1

Link	Iteration 1			Iteration 2			Iteration 3		
Name	$\tau^1_{e,1}$	$\gamma^1_{e,1}$	$\rho^1_{e,1}$	$\tau^2_{e,1}$	$\gamma^2_{e,1}$	$\rho^2_{e,1}$	$\tau^3_{e,1}$	$\gamma^3_{e,1}$	$\rho^3_{e,1}$
$L0,1$	73.539	0.0499	0.0528	120.1637	**0.1141**	**0.1380**	**138.9500**	0.0188	0.0231
$L0,2$	73.539	**0.0717**	**0.0758**	**140.4437**	0.0000	0.0000	123.7100	**0.1017**	**0.1116**
$L1,0$	73.539	0.0000	0.0000	73.5399	0.0000	0.0000	73.5400	0.0000	0.0000
$L1,2$	**88.534**	0.0000	0.0000	88.2923	0.0000	0.0000	88.2900	0.0000	0.0000
$L1,3$	59.194	0.0374	0.0319	81.8295	0.0794	0.0654	87.7800	0.0220	0.0171
$L2,0$	73.539	0.0000	0.0000	73.5399	0.0000	0.0000	73.5400	0.0000	0.0000
$L2,4$	59.194	0.0443	0.0377	85.9972	0.0034	0.0030	79.8300	0.0733	0.0520
$L3,4$	**88.534**	0.0000	0.0000	88.5347	0.0000	0.0000	88.5300	0.0000	0.0000
$L3,5$	73.795	0.0458	0.0486	116.8651	0.0892	0.1049	129.3300	0.0451	0.0518
$L4,2$	59.194	0.0000	0.0000	59.1946	0.0000	0.0000	59.1900	0.0000	0.0000
$L4,3$	**88.534**	0.0000	0.0000	88.5347	0.0000	0.0000	88.5300	0.0000	0.0000
$L4,5$	73.795	0.0403	0.0428	111.6604	0.0172	0.0193	106.4700	0.0749	0.0708
$L5,3$	73.795	0.0000	0.0000	73.7957	0.0000	0.0000	73.8000	0.0000	0.0000

3.2. Iterations through convergence

Figure 2 shows the network vulnerability in each iteration as a step function as well as a moving average to illustrate the trend.

Figure 2 Network vulnerability of simple network



While there are large variations in system vulnerability in successive iterations, the fluctuations become smaller after approximately the 80^{th} iteration and the moving average indicates the underlying trend is decreasing.

Figure 3 Change in network vulnerability ($\Delta\mu$)

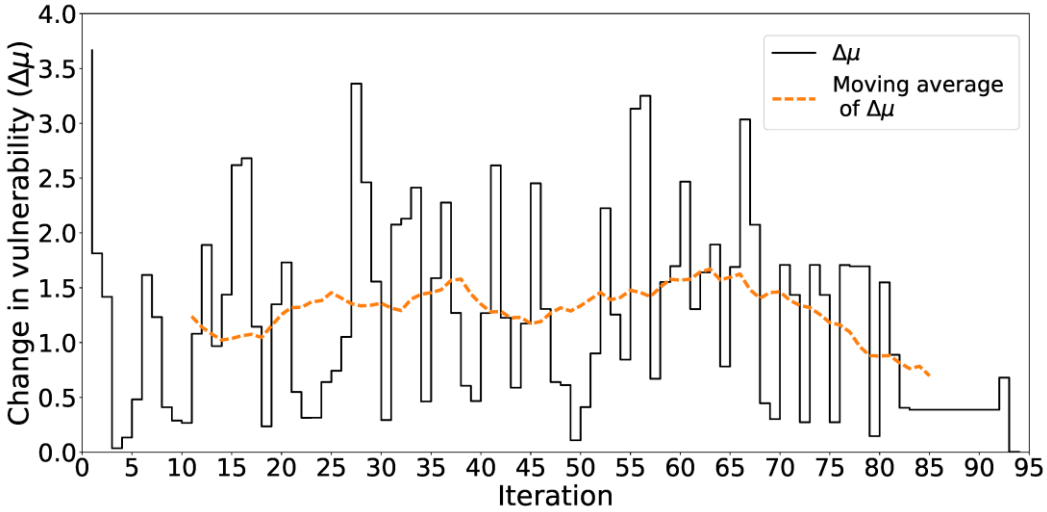
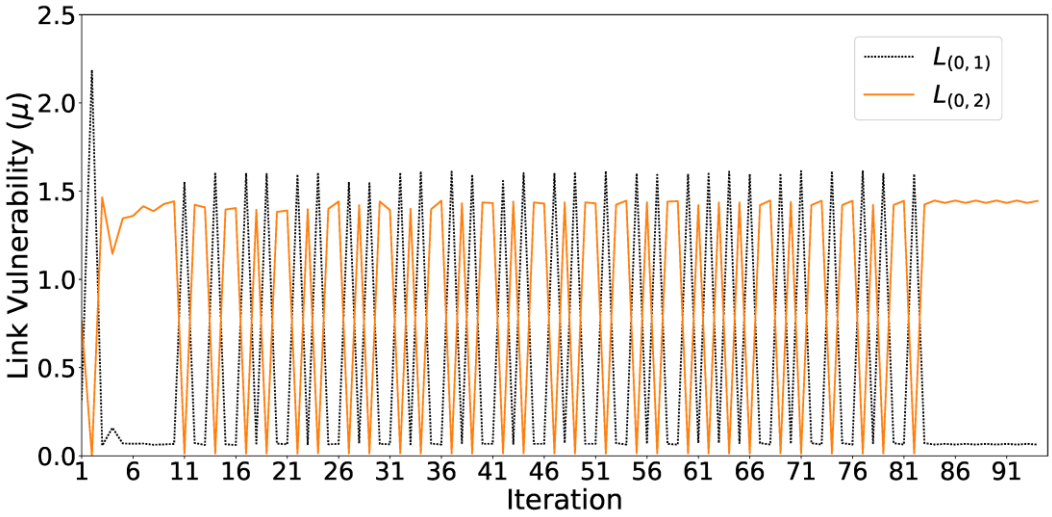


Figure 3 provides an alternative view, showing the change in system vulnerability ($\Delta\mu$) between successive iterations as well as a moving average. Similar to Figure 2, $\Delta\mu$ fluctuates significantly. However, after the 60^{th} iteration, this difference never exceeds 2.0 and after the 80^{th} it never exceeds 1.0, converging in the 94^{th} iteration when $\Delta\mu < \varepsilon = 0.01$. The moving average illustrates this more clearly, indicating a visibly decreasing trend after the 60^{th} iteration. Convergence occurs because applying the method of successive averages to the s-expected costs places less emphasis on the later defense strategies, producing smaller changes in network vulnerability.

To provide a more detailed view of the iterations of the game and the influence of the method of successive averages on convergence, Figure 4 shows a plot of the vulnerability of links $L_{0,1}$ and $L_{0,2}$.

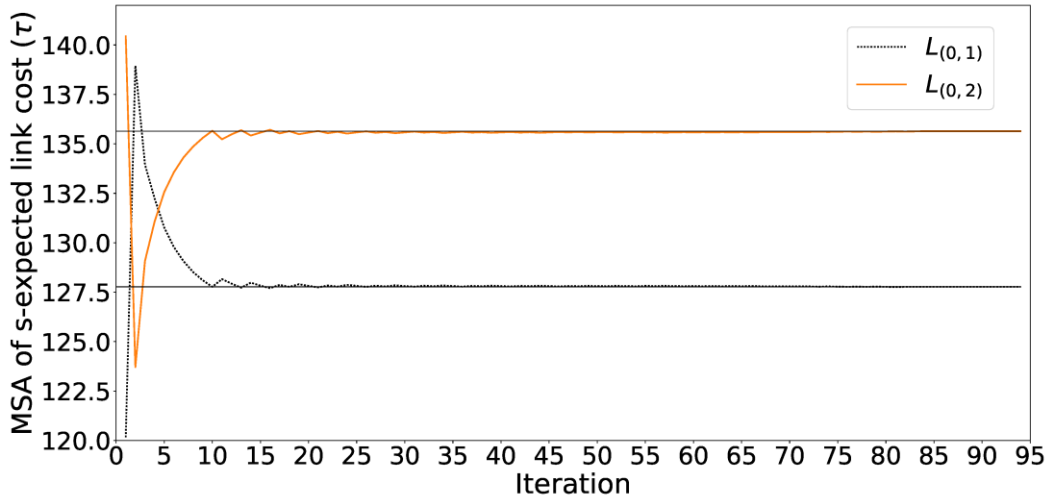
Figure 4 Link Vulnerability at interval Δt_1



Link vulnerability oscillates, in the first few iterations because the link cost lacks sufficient memory of the attacker's alternating strategy. There is greater stability between iterations four and ten because the router has observed the alternating attacker strategy enough to avoid subsequent oscillation. However, oscillation begins again at iteration 11 and continues to iteration 80 after which the vulnerability stabilizes until convergence.

To explain the oscillatory behavior in the link vulnerability, recall that link cost τ is a term in vulnerability, $\mu = \tau \times \gamma \times \rho$. Figure 5 shows the MSA of the s-expected links cost $\tau^n_{(0,1),\Delta t_1}$ and $\tau^n_{(0,2),\Delta t_1}$.

Figure 5 MSA of s-expected link costs at interval Δt_1



The black horizontal lines at $\mu = 127.77$ and $\mu = 135.64$ indicate the value of link costs at convergence for links $L_{0,1}$ and $L_{0,2}$ respectively. In the first iteration the router overcompensates by shifting all traffic from $L_{0,2}$ to $L_{0,1}$ and the attacker reacts accordingly. In subsequent iterations, the attacker observes the lack of change in the router's strategy and progressively increases the probability of attack on $L_{0,2}$ until a tipping point is reached because the router's risk aversion threshold has been exceeded and it calibrates its routing strategy to reduce risk. Thus, every reversal in Figure 4 corresponds to occasions in Figure 5 where the black lines (risk aversion thresholds) are crossed and the router

responds to the provocations of the attacker. While not visible in Figure 5, iteration 82 to convergence do not cross the black lines, explaining why there is substantially less fluctuation in the corresponding vulnerabilities in Figure 4.

3.3 Comparison between deterministic and game theoretic approach

To assess the quality of the proposed method, we compared it to the deterministic approach described in [13], which also divided the simulation into time intervals ΔT, but ran $|E| \times |\Delta T|$ simulations, computed the travel time, and difference between this travel time and the travel time for the fully operational network. In the deterministic approach, the criticality of a link is proportional to the travel time, whereas relative criticality in the game-theoretic approach is the sorted values of the link vulnerabilities. Thus, it is possible to directly compare the agreement between the rankings produced by the deterministic and game-theoretic approaches.

Table 2 compares the outputs of the game-theoretic and deterministic methods. Columns two and three report the vulnerability determined by the game-theoretic approach on the 94th iteration (μ^{94}) and the corresponding ranking over all combinations of time interval (Δt_i) and link($L_{(i,j)}$), while columns four and five provide the corresponding travel times (TT) and ranks produced by the deterministic approach for time interval Δt_1. Similarly, the values for intervals Δt_2 and Δt_3 are shown in columns six through thirteen.

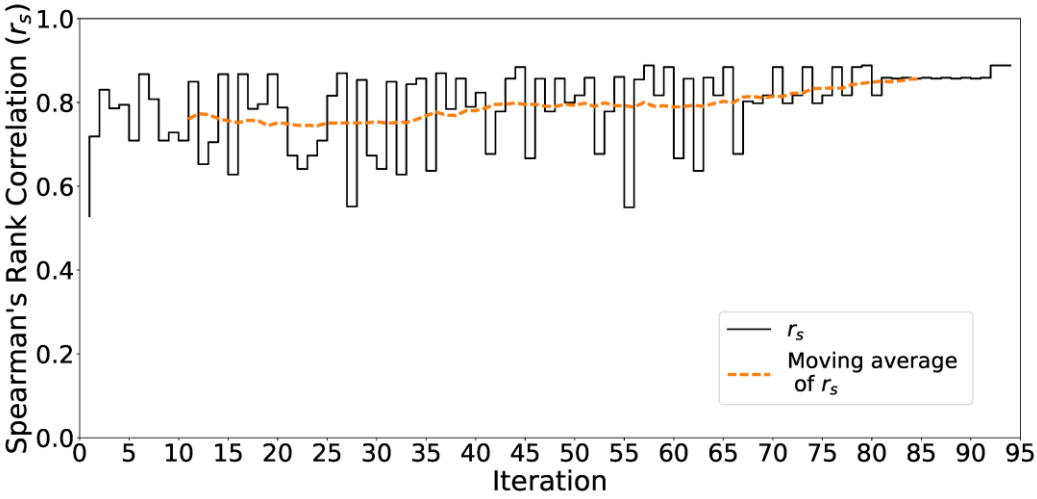
Table 2 Comparison of game-theoretic and deterministic methods

Link	Δt_1				Δt_2				Δt_3			
Name	μ^{94}	μ^{94} rank	TT	TT rank	μ^{94}	μ^{94} rank	TT	TT rank	μ^{94}	μ^{94} rank	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

To compare the deterministic and game-theoretic approaches, we applied Spearman's rank correlation coefficient to the ranks reported in Table 2, producing a correlation $r_s = 0.8882$ with a p-value of 4.63×10^{-14}, demonstrating the strong correlation between the two approaches.

To further illustrate the value of the game-theoretic approach, Figure 6 shows the correlation attained in each iteration as well as a moving average. Not only does the game produce vulnerabilities that correlate well with the deterministic ranks, the correlation never falls below 0.8 after iteration 65 and the moving average demonstrates the increasing trend.

Figure 6 Spearman's rank correlation coefficient



4. CONCLUSION AND FUTURE RESEARCH

This paper presents a game theoretic approach to assess the dynamic vulnerability of a transportation network. The technique implements a mixed-strategy game between an attacker that seeks to disrupt the normal flow of traffic and a defender that attempts to minimize the risk posed by such an adversary. The method of successive averages was implemented to ensure convergence. Unlike our previous deterministic approach, this technique can consider the relative vulnerability of all links and time intervals in parallel. Moreover, computing Spearman's rank correlation coefficient on the relative criticality of link/time interval pairs determined by the deterministic and game- theoretic methods demonstrated strong correlation, suggesting that the proposed game-theoretic approach produces a reasonable approximation to the exact but slower deterministic method.

Future research will seek to overcome performance and accuracy challenges encountered when scaling the game- theoretic approach to larger networks to enable fast identification of vulnerable links. We will also utilize the game-theoretic dynamic transportation network vulnerability approach to allocate limited defensive resources to links at specified times to mitigate vulnerability most effectively.

References

[1] K. Berdica. "*An introduction to road vulnerability: what has been done, is done and should be done."* Transport Policy, 9(2):117–127, 2002.

[2] E. Jenelius, T. Petersen, and L. Mattsson. *"Importance and exposure in road network vulnerability analysis."* Transportation Research Part A: Policy and Practice, 40(7):537–560, 2006.

[3] P. Murray-Tuite and H. Mahmassani. *"Methodology for determining vulnerable links in a transportation network."* Transportation Research Record: Journal of the Transportation Research Board, (1882):88–96, 2004.

[4] D.M. Scott, D.C. Novak, L. Aultman-Hall, and F. Guo. *"Network robustness index: a new method for identifying critical links and evaluating the performance of transportation networks."* Journal of Transport Geography, 14(3):215–227, 2006.

[5] J.L. Sullivan, D.C. Novak, L. Aultman-Hall, and D.M. Scott. "*Identifying critical road segments and measuring system-wide robustness in transportation networks with isolating links: a link-based capacity-reduction approach."* Transportation Research Part A: Policy and Practice, 44(5):323–336, 2010.

[6] A. Nagurney and Q. Qiang. *"Fragile networks: identifying vulnerabilities and synergies in an uncertain age."* International Transactions in Operational Research, 19(1-2):123–160, 2012.

[7] U. Demšar, O. Spatenkova, and K Virrantaus. *"Identifying critical locations in a spatial network with graph theory."* Transactionsin GIS, 12(1):61–82, 2008.

[8] M.G.H. Bell and C. Cassir. *"Risk-averse user equilibrium traffic assignment: an application of game theory."* Transportation Research Part B: Methodological, 36(8):671–681, 2002.

[9] M.G.H. Bell. *"The use of game theory to measure the vulnerability of stochastic networks."* IEEE Transactions on Reliability, 52(1):63–68, 2003.
[10] Q. Wang, L. Fiondella, N. Lownes, J. Ivan, R. Ammar, S. Rajasekaran, and S. Tolba. *"Integrating equilibrium assignment in game-theoretic approach to measure many-to-many transportation network vulnerability."* In Proc. IEEE International Conference on Technologies for Homeland Security, pages 351–357, 2011.
[11] L. Fiondella, A. Rahman, N. Lownes, and V. Basavaraj. *"Deployment of high speed rail: An evolutionary algorithm guided by game theory."* IEEE Transactions on Reliability, 65(2):674–686, 2016.
[12] J. Duanmu, K.M. Taaffe, M. Chowdhury, and R M. Robinson. *"Simulation analysis for evacuation under congested traffic scenarios: a case study."* Simulation, 88(11):1379–1389, 2012.
[13] V. Shekar, L. Fiondella, S. Chatterjee, and M. Halappanavar. *"Quantitative assessment of transportation network vulnerability with dynamic traffic simulation methods."* In Proc. IEEE International Symposium on Technologies for Homeland Security, pages 1–7, 2017.