Quantitative Assessment of Transportation Network Vulnerability with Dynamic Traffic Simulation Methods

Venkateswaran Shekar*, Lance Fiondella*
*Department of Electrical & Computer Engineering
University of Massachusetts
285 Old Westport Road
North Dartmouth, MA 02747–2300
Email: {vshekar,lfiondella}@umassd.edu

Samrat Chatterjee†, Mahantesh Halappanavar†
†Pacific Northwest National Laboratory
902 Battelle Blvd,
P.O. Box 999, MSIN K7-20
Richland, WA 99352
Email: {samrat.chatterjee,mahantesh.halappanavar}@pnnl.gov

***Abstract*—Transportation networks are critical to the social and economic function of nations. Given the continuing increase in the populations of cities throughout the world, the criticality of transportation infrastructure is expected to increase. Thus, it is ever more important to mitigate congestion as well as to assess the impact disruptions would have on individuals who depend on transportation for their work and livelihood. Moreover, several government organizations are responsible for ensuring transportation networks are available despite the constant threat of natural disasters and terrorist activities. Most of the previous transportation network vulnerability research has been performed in the context of static traffic models, many of which are formulated as traditional optimization problems. However, transportation networks are dynamic because their usage varies over time. Thus, more appropriate methods to characterize the vulnerability of transportation networks should consider their dynamic properties. This paper presents a quantitative approach to assess the vulnerability of a transportation network to disruptions with methods from traffic simulation. Our approach can prioritize the critical links over time and is generalizable to the case where both link and node disruptions are of concern. We illustrate the approach through a series of examples. Our results demonstrate that the approach provides quantitative insight into the time varying criticality of links. Such an approach could be used as the objective function of less traditional optimization methods that use simulation and other techniques to evaluate the relative utility of a particular network defense to reduce vulnerability and increase resilience.**

I. Introduction

The Department of Homeland Security (DHS) identifies the Transportation Systems Sector (TSS) as one of 16 critical infrastructure sectors, which are considered so essential to the United States that their degradation or unavailability would have a serious impact on a combination of security, national economic security, and national public health or safety. The Transportation Systems Sector is critical to national economic security because the majority of citizens utilize the ground transportation network to commute to work on a daily basis and is also a medium by which domestic and international tourist move about. Thus, the United States and other nations are critically dependent on transportation for both work and leisure activities and the corresponding economic stability that such activities bring. Moreover, the Transportation Systems Sector is a fundamental enabler of the Emergency Services Sector (ESS), which is defined as a system of prevention, preparedness, response, and recovery elements to mitigate risk from terrorist attacks [1], man made incidents, and natural disasters [2]. This dependence among critical infrastructures makes the Transportation Systems Sector even more important because of its role in ensuring communal safety and well-being of the population.

The Federal Emergency Management Agency (FEMA) administers the Urban Areas Security Initiative (UASI), which invests nearly $600 million annually to assist high-threat, high-density Urban Areas build and sustain the capabilities necessary to prevent, protect against, mitigate, respond to, and recover from acts of terrorism as well as related preparedness capabilities for other hazards. High-density areas include New York City, Los Angeles, Miami, and Boston. Washington, DC and cities with major international airports such as Chicago and Charlotte as well as many of these high-density areas are also high-threat areas Thus, quantitative methodologies to characterize vulnerability and risk can guide defensive strategies to enable greater resilience have gained significant attention in recent years. Decision support tools based on such methods to systematically reduce the consequences of disruptions and preserve the continuity of activities enabled by transportation are therefore highly desirable.

Several previous studies have proposed transportation network vulnerability assessment methods [3] and strategies to quantitatively enhance resilience. Commonly used techniques include traditional optimization methods and game theoretic approaches. Examples of game theoretic approaches include Bell [4] who 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 [5] developed a bi-level non-zero-sum game between an attacker and the traffic management agency to quantify vulnerability. An example of an optimization-based

approach is the work of Ukkusuri and Yushimito [6] who proposed a heuristic procedure that draws upon concepts from network science to assess the importance of transportation networks using increased travel time as a measure of criticality. Wang *et al.* [7] 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.* [8] 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.

Most of the previous research and all of the references cited above are restricted to static traffic assignment (STA) problems which only consider a static snapshot of the network at a single point in time. Static vulnerability and resilience methods can characterize structural risk within a transportation network and mitigation strategies. However, they are unable to consider how traffic demand changes over time and the corresponding impact of both location and timing of a disruption on vulnerability. Unlike static traffic assignment, dynamic traffic assignment (DTA) considers the time-varying nature of network congestion. This means that the criticality of a link can be studied as a function of time. Given that most vulnerability quantification approaches account for the number of individuals at risk or the increase in system travel time computed as the sum of the times of the individual trips, more realistic vulnerability assessment should consider DTA methods which explicitly model travel demand as a function of time such as the morning and evening rush hours and activities such as sporting events and other large social gatherings. This would enable dynamic vulnerability mitigation strategies that consider not only where but also when to deploy defenses that either deter attack or reduce the effectiveness of an attack. However, relatively few studies consider dynamic methods such as simulation. For example, Duanmu *et al.* [9] assessed the utility of effective information dissemination on evacuation, but limited analysis to a case study with three primary evacuation routes.

This paper presents an approach to assess the dynamic vulnerability of transportation network using simulation techniques. We employ a microscopic road traffic simulator to compute baseline measures of congestion within a fully operational network and systematically compare these measures with results obtained when individual links within the network are disrupted at specific times. Thus, unlike static methods that only consider network demand at a single point in time to identify structural vulnerabilities, the proposed approach can consider both the network structure as well as time varying demand to assess the relative criticality of the impact of timed disruptions. The dynamic network vulnerability assessment method is illustrated through a series of examples. A small example provides details of the mechanics of the approach and inferences enabled. A university campus-level example is given to illustrate the potential for application to evacuation. Our results demonstrate that the approach can quantify the time varying criticality of links, which can inform network defense and resilience planning. Because pervasive deployment of defenses is prohibitively expensive, identifying how the vulnerability of links change over time will provide greater insight, enabling quantitative assessment of competing defense strategies to preserve continuity of travel time reliability within a transportation network despite disruptions.

The remainder of the paper is organized as followed. Section II proposes an algorithmic approach to assess the dynamic vulnerability of a transportation network. Section III illustrates the approach through examples. Section IV summarizes with conclusions and possible directions for future research.

II. Dynamic Transportation Network Vulnerability Assessment

Travel demand within a network is a function of time, meaning that trips are generated in discrete epochs to approximate continuous time activities such as the morning and evening rush to commute to and from work or school. Dynamic equilibrium routes this and existing demand flowing within the network to achieve equilibrium that characterizes individual traveler's natural desire to minimize their travel time. A link outage will disrupt this equilibrium necessitating rerouting to achieve a new equilibrium. Some disruptions will increase overall and individual travel times more significantly than others. Thus, a simple yet systematic strategy to assess the vulnerability of a dynamic transportation network is to consider the relative impact of disruptions on specific links for a specified duration. Such an approach can answer the question, "*When* **and** *where* would a disabled link be the most disruptive to the network?" In doing so, one can identify both when and where would an intentional attack or accidental incident be most harmful to network travel times, there by suggesting how to prioritize the time and location of defensive strategies. This is substantially more detailed than static approaches that only consider where to defend and thus require permanent deployment of defenses to locations within the network.

To enable a dynamic transportation network vulnerability approach that is both methodical and scalable, a transportation simulator that allows interaction with the network during simulation through a programming interface is desirable. The strengths and weaknesses of several simulators were assessed to determine suitability for use as the driver of dynamic transportation network vulnerability studies. Proprietary tools such as Visum [10] and VISSIM [11] are used to study traffic demands and traffic flow optimizations. However, the closed source nature of these tools prevents the independent verification of models and the simulation results produced. MATSim [12] is an open source multi-agent traffic simulator that was designed to simulate individual vehicles but ignores the physics behind the behavior of vehicles. We ultimately selected the open source simulator SUMO (Simulator of Urban MObility) [13], which is also a microscopic simulator. In addition to allowing programmatic interaction with the network during simulation, SUMO can import OpenStreetMap (OSM) data for use in simulations. The Dynamic Traffic

Assignment algorithm is based on Gawron's algorithm [14] and the shortest path to the destination is calculated with Dijkstra's algorithm [15].

Algorithm 1 shows the pseudo code of our approach to assess the vulnerability of a dynamic transportation network using SUMO as a black box function to quantify the impact of temporary link disruptions in order to quantify their relative criticality. While SUMO is used for the analysis presented here, we note that our approach is general and could utilize another traffic simulator to perform vulnerability assessment.

Algorithm 1 Pseudo code for transportation network vulnerability assessment

Require: Road network G with n nodes and e edges
Require: Traffic demand data **D**
Require: Array of time intervals $\mathbf{T} = \langle \Delta t_1, \Delta t_2, \ldots, \Delta t_i, \ldots, \Delta t_k \rangle$
  $V_o =$ Run simulation without disabling links
  for Each edge $e \in G$ **do**
    for For each interval $\Delta t_i \in \mathbf{T}$ **do**
      $V_{e,i} =$ Run simulation, disabling edge e in interval Δt_i
    end for
    $\Delta V_{e,i} = V_{e,i}/V_o$
  end for

Inputs include the static graph G of the road network containing n nodes to represent road junctions and e edges for the roads that convey vehicles through the network from source to destination. The origin-destination (OD) demand matrix is a discrete sequence of matrices **D**, where $D(i)$ is the $n \times n$ OD demand matrix of the trips wishing to travel between distinct pairs of nodes generated in the ith of k epochs in the simulation. To establish a baseline, the simulation is first run under the scenario where all links are available at all time steps to produce the nominal vulnerability V_o. Next, a single link is disabled for a single time period to determine $V_{e,i}$ and the simulation rerun with no change to the demand matrix to determine the vulnerability edge e poses to the network at time i. The increase in vulnerability incurred by this transient disruption $\Delta V_{e,i}$ is calculated by dividing the nominal vulnerability V_o by the elevated vulnerability $V_{e,i}$ that results from this disruption. The larger the ratio the greater the impact such a disruption would have because it could increase congestion, thereby slowing evacuation and response times.

The asymptotic run time required to perform dynamic transportation network vulnerability assessment based on this approach is $O(eks)$, where e is the number of edges, k the number of time intervals, and s the time needed to execute a single DTA simulation. Therefore, runtime increases linearly with respect to the number of edges within the network, but increasing e also increases s in larger networks. As a result, efficient DTA simulation techniques that can accurately characterize network behavior will have a large influence on the run time of the approach. Increasing the number of intervals k will also increase the run time, but could enable additional applications such as identification of the value of fast restoration. While the approached described here uses disruptions of uniform duration on a single link, the approach could also be generalized to non-uniform disruption of one or more links on potentially overlapping intervals. Such and approach could characterize the impact of staggered attacks, cascading failures, and many other complex scenarios to disrupt multiple links over time.

A. Sources of input for dynamic transportation network vulnerability assessment

This section describes the inputs required for simulation simulation and potential sources for this data. Figure 1 indicates traffic simulators require the network structure and traffic demand data.

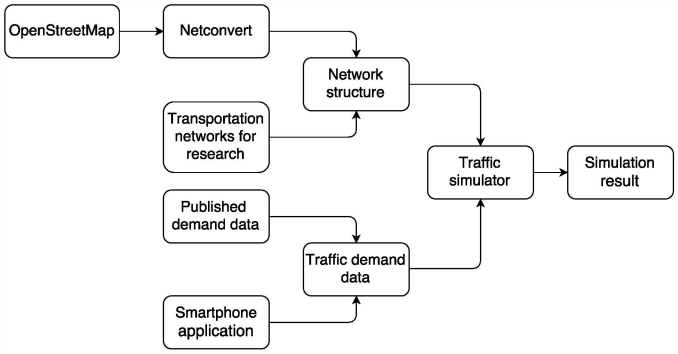


Fig. 1: Overview of data sources and simulation

The sources of these data can vary. For example, many static traffic assignment studies use the network structure and traffic demand data provided by the Transportation Networks for Research [16] website, now hosted on Github. An emerging source of road network data is OpenStreetMap (OSM) [17], a freely available crowdsourced map of the world. We used the NETCONVERT application [18] which can extract network data from a variety of sources including OSM and convert it into other usable formats including SUMO simulator input. Similarly, traffic simulation studies can use traffic demand data feeds from a variety of sources. Smartphones have become increasingly popular, both as a data collection and delivery platform. Our ongoing research [19] is developing an open source smartphone app to enable data collection for transportation network studies that do not charge a fee, thereby promoting novel modeling and analysis. A second motivation of our work is to attract transportation researchers to network vulnerability research of interest to the Department of Homeland Security and other organizations. As pervasive real-time traffic demand data feeds become available, high-fidelity dynamic network vulnerability should become feasible.

III. Illustrations

To demonstrate the utility of the proposed approach, we apply our dynamic transportation network vulnerability assessment algorithm to a number of road networks. The first example uses a simple test network as a pedagogical tool to easily highlight the benefits of the methodology. The second

example uses the University of Massachusetts Dartmouth road network, which was evacuated after the April 15, 2013 Boston Marathon bombing when it was discovered that one of the bombers was a student there.

A. Example I: Simple network

This example uses the simple test network show in Figure 2 to illustrate inferences enabled by the Algorithm 1 to assess dynamic transportation network vulnerability.

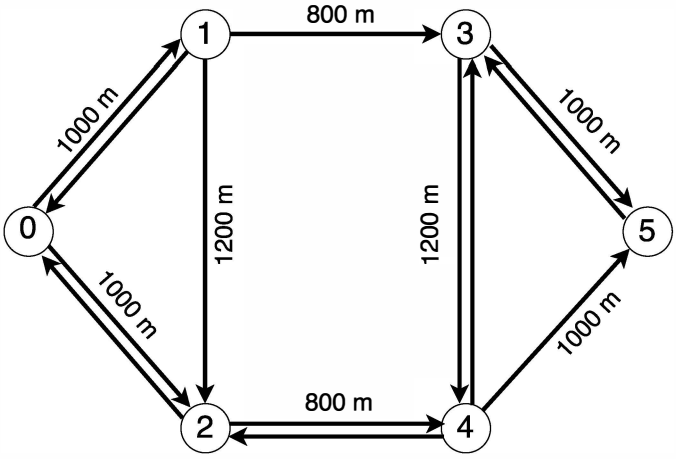


Fig. 2: Structure of simple network

The network consists of $n = 6$ 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).

In the scenario we created for the sake of illustration, the array of time intervals in which link disruption could occur were $\mathbf{T} = \{\Delta t_1 = (0, 500), \Delta t_2 = (500, 1000), \Delta t_3 = (1000, 1500)\}$. 500 vehicles depart node zero at the beginning of each of these three time steps with the objective of reaching node five. Since there are eight (i, j) pairs of adjacent nodes with links between them and three disconnection intervals, a total of 24 $(= 8 \times 3)$ simulations were performed. A 25th simulation where none of the links were disconnected was performed to quantify the baseline vulnerability of the network.

Figure 3 provides a visual summary of the results of our dynamic network vulnerability assessment for the simple network.
The x-axis indicates the direct link from node i to j that was disrupted as well as the time interval in which the disruption occurred. The y-axis denotes the ratio of the simulation time when that link is disabled divided by the simulation time taken for the nominal case.

Figure 3 indicates that a disruption to the link between nodes two and four in the time interval $\Delta t_3 = (1000, 1500)$ would elevate the total time by over 10%. This agrees with intuition and can be explained based on the structure of the network given in Figure 2 where it can be seen that either $(1, 3)$ or $(2, 4)$ is needed to cross from the left to right side of the

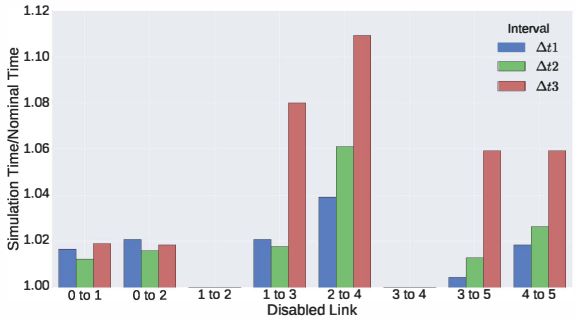
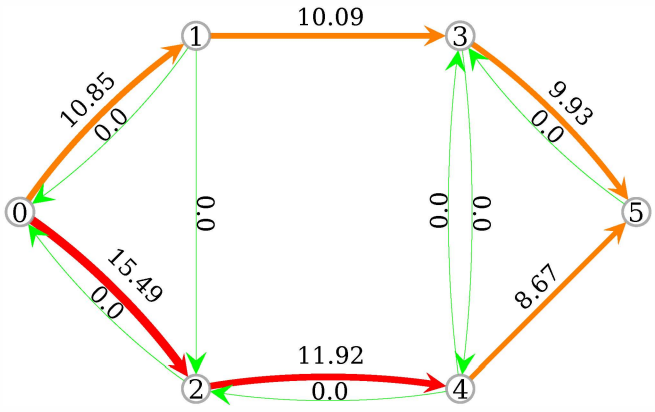


Fig. 3: Dynamic network vulnerability assessment of simple network

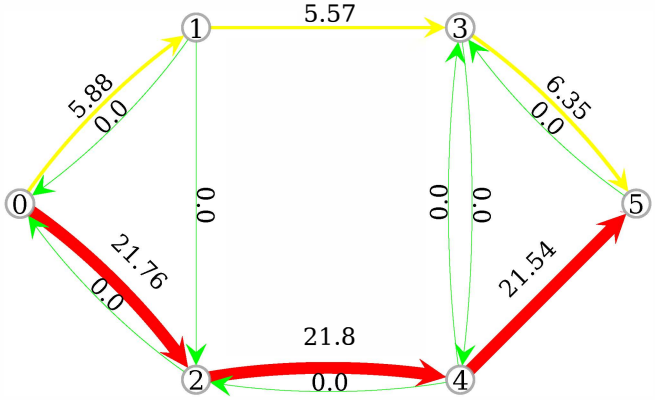
graph. However, $(1, 3)$ is not of equal structural importance because there exist a $(1, 2)$ link, but no $(2, 1)$ link. Thus, vehicles that traveled along $(0, 2)$ would be trapped until $(2, 4)$ was restored. Hence, a later disruption to $(2, 4)$ would increase total travel time most significantly.

The results suggest that the pairs $(1, 2)$ and $(3, 4)$ would have virtually no impact on network vulnerability because Figure 2 indicates that these links do not lie on shortest paths from the source to destination. Moreover, our analysis only considers a single disruption in isolation. Therefore, disabling these links are of little importance to the simple network case study representative of an evacuation scenario and would not be identified as priority links for defense to ensure that they remain open during a crisis. However, scenarios where multiple links are simultaneously disabled or are disabled at different periods of time may change the criticality of these links. Pairwise link failures would require a quadratic number of simulations and the possibility of link unavailability in the same or different time intervals adds additional complexity to the pairwise problem $O(\binom{e}{2}|\mathbf{T}|^2)$, where $|\mathbf{T}|$ is the cardinality of the number of time intervals considered. Three-way failures impose cubic complexity $(O(\binom{e}{3}|\mathbf{T}|^3))$ and an exhaustive approach to assess all subsets of links would require at least time exponential in the number of links comprising the network. Thus, when the network is large, exhaustive analysis must be tempered with common sense that considers a core set of links that are likely to be critical in isolation or in conjunction with a small number of other edges.

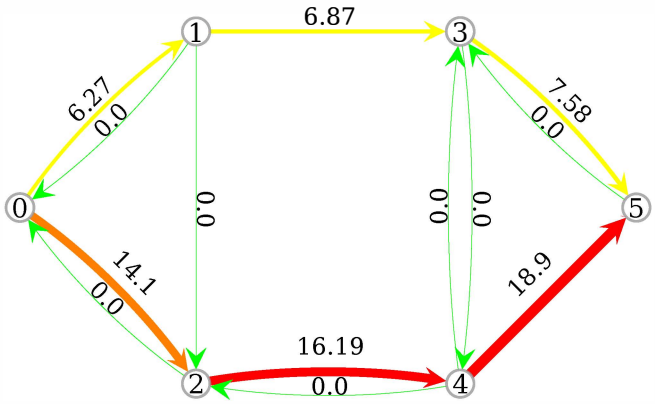
Figure 4 provides an intuitive view of dynamic vulnerability. Figure 4a, 4b, and 4a correspond to the nominal case when none of the links are disabled for the respective time periods Δt_1, Δt_2, and Δt_3. Edges of the graph are labeled with numbers indicating the density of vehicles (vehicles/km). The most critical links with the highest densities are colored red, followed by orange, yellow, and green. Alternative heat maps with a larger number of distinct colors are also possible. Figure 4a indicates that $(0, 2)$ is most heavily utilized in Δt_1, while 4b shows $(0, 2)$, $(2, 4)$, and $(4, 5)$ form a critical path from source to destination as traffic flows through the network. Figure 4c shows that criticality of earlier stages



(a) Time interval Δt_1



(b) Time interval Δt_2



(c) Time interval Δt_3

Fig. 4: Vehicle densities in fully functioning network

such as $(0, 2)$ decrease as trips generated at the beginning of the first two time intervals approach their destination, but $(0, 2)$ remains elevated (orange) because of the trips departing from node zero in this final time interval. Thus, the dynamic transportation network vulnerability assessment approach can intuitively visualize the time varying criticality of links within a network for emergency scenarios such as evacuation as well as other more commonly occurring events such as delays due to rush hour and traffic accidents. Animating a sequence of color coded graphs such as those shown in Figure (4a-4c) can provide decision makers with a criticality "weather map" to easily understand how link criticality can change as a scenario progresses.

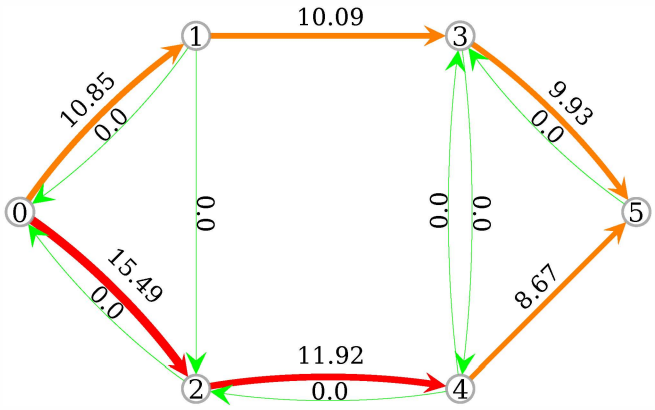
To illustrate the effect of link unavailability, Figure 5 shows the vehicle density map when the link between two and four is disabled in the interval Δt_2. In this scenario, Figures 4a and 5a are identical. However, when $(2, 4)$ is disabled at the beginning of the second time interval, traffic that was moving in that direction must turn around because there is no alternative path and backtracking becomes necessary. As a result, the criticality $(0, 1)$ during Δt_2 is significantly higher in Figure 5b than it was in 4b. Moreover, the $(1, 3)$ and $(3, 5)$ links along the upper path from zero to five also increase, while the $(2, 4)$ and $(4, 5)$ links decrease because they become inaccessible. However, in the final time step, access to the lower path is restored and vulnerability increases, but not to the level observed in Figure 4c. It can also be observed from Figure 5c that the traffic that rerouted itself through the upper path when $(2, 4)$ was disrupted during Δt_2 drastically increasing $(3, 5)$ during the final time step. Thus, the dynamic transportation network vulnerability assessment indicates the importance of ensuring safe passage of travelers on link $(3, 5)$ during Δt_3 despite restoration of $(2, 4)$.

B. Example II: University of Massachusetts Dartmouth evacuation

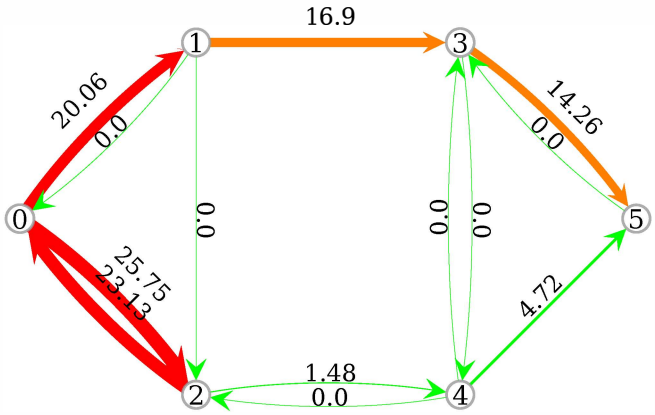
On April 15, 2013, the Boston Marathon bombing killed three civilians and injured approximately 250 others. The University of Massachusetts (UMass) Dartmouth was evacuated only a few days later when it was discovered that one of the suspects was a student there. This example applies our dynamic network vulnerability assessment algorithm to the UMass Dartmouth campus road network.

Figure 6 shows the campus map imported from OpenStreetMaps. All traffic entering and leaving campus must pass through the entrance at the north (top of Figure 6), which is connected to Ring Road encircling the library, classroom, and administrative buildings. Dormitories and facilities are located to the east, the Fitness Center to the south, and additional dormitories are located in the south west. The main parking lots P_1 through P_10 are located on the interior of the ring and are the source of vehicles seeking to evacuate in this example. Twelve distinct link S_1 through S_{12} are considered. Due to the circular nature of the road, any single disruption would require that vehicles reverse direction to reach the campus exit.

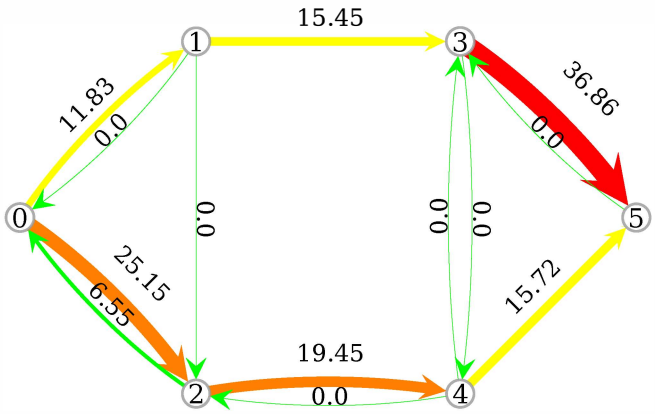
Figure 7 shows the campus network map simplified to nodes and edges with geographic details removed. Four thousand vehicles are generated from P_1-P_{10} with the exit as their destination common destination. Twelve off nominal scenarios



(a) Time interval Δt_1



(b) Time interval Δt_2



(c) Time interval Δt_3

Fig. 5: Impact of disconnecting link from node two to four at Δt_2 on vehicle densities

are considered where links in both directions on one of $S1$-S_{12} are disabled in three possible time intervals $T = \{\Delta t_1 = (0, 3000), \Delta t_2 = (3000, 6000), \Delta t_3 = (6000, 9000)\}$.

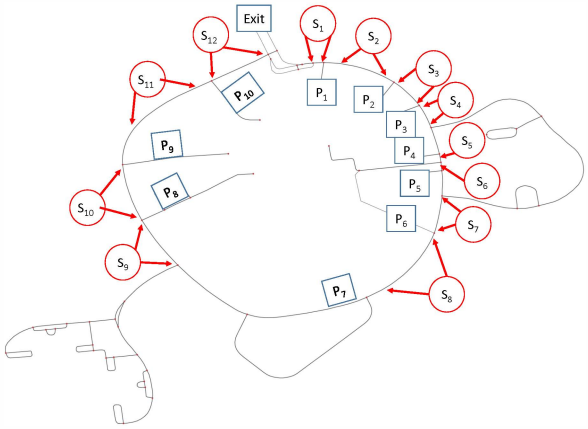


Fig. 6: University of Massachusetts Dartmouth campus map

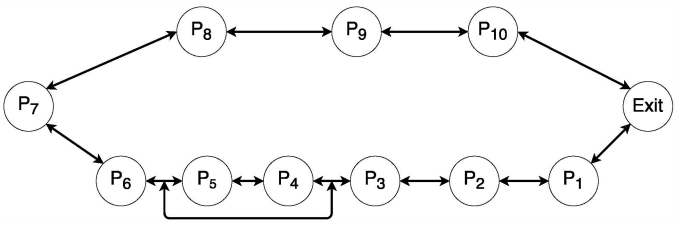


Fig. 7: University of Massachusetts Dartmouth conceptual map

Figure 8 summarizes the results of the dynamic transportation network vulnerability assessment of UMass Dartmouth. The general trend is that lower numbered links such as S_1 as well as higher numbered links like S_{12} are the most critical, which agrees with intuition because these are the links closest to the exit. Thus, vehicles encountering a disrupted link would need to reverse course and drive the entire distance around Ring Road in the opposite direction. While the circular design of the campus appears effective, the lack of a second exit toward the south end of campus poses significant risk. As a result, links closer to the south end of campus are less critical with the single exit in the north because vehicles that would reverse course would only need to travel halfway around campus not all the way. The single largest disruption occurs at S_1 in time interval Δt_3 because there are more parking lots on the east side of campus so many vehicles attempt to exit in a counter clockwise manner. However, many of these vehicles encounter the disrupted S_1 link and must turn around and loop back around Ring Road.

Counterintuitively, the evacuation time is lower when S_5, S_6, S_7, or S_8 is disrupted when compared to the time required of the fully functioning network. In scenarios S_5 and S_6, vehicles traveling counter clockwise bypass the disruption by taking the road that loops around the dorms on the right, while disruptions to S_7 and S_8 require vehicles to exit campus by traveling clockwise around Ring Road. This turns out to be advantageous because the density of vehicles on the west side of campus is lower due to the fewer number of source parking

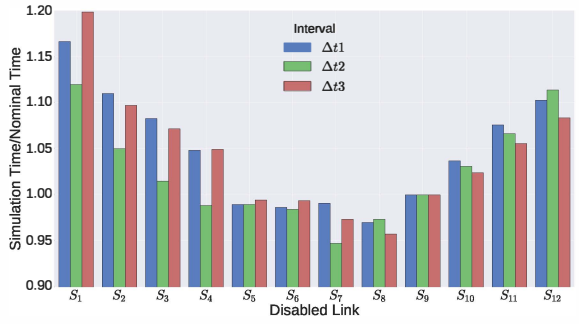


Fig. 8: UMass Dartmouth Simulation Results

lots from which trips originate. Thus, the vehicles originating from P_6 or P_7 exit the campus faster.

IV. Conclusion and Future Research

This paper presents an approach to assess the dynamic vulnerability of a transportation network using simulation techniques. We employed a microscopic road traffic simulator to compute baseline measures of congestion within a fully operational network and systematically compared these measures with results obtained when individual network links are disrupted at specific times. Unlike static methods that only consider network demand at a single point in time, the proposed approach considers both the network structure as well as time varying demand to assess the relative criticality of timed disruptions. The dynamic network vulnerability assessment method was illustrated through two examples. Our results indicate that visualizations provide intuitive interpretation of dynamic vulnerability, enabling insights that could be used to compare competing defense strategies.

Future research will seek practical strategies to manage complexity which will be encountered during large-scale assessments and seek to tailor the approach with additional details that will render it suitable for use in multiple scenario such as emergency response, rerouting of the traveling public, and mass evacuation. To overcome anticipated scalability challenges posed by the deterministic approached given here, we will experiment with randomized defensive strategies identified through game theoretic techniques that can consider the relative vulnerability of all links in a network in parallel.

References

[1] Robert Johnston. Terrorist attacks and related incidents in the united states. http://www.johnstonsarchive.net/terrorism/wrjp255a.html, 2016. Accessed: 2016-05-07.

[2] National Environmental Education Foundation. Transportation disruption. https://www.neefusa.org/nature/land/transportation-disruptions, 2016. Accessed: 2016-05-07.

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

[4] MGF Bell. The use of game theory to measure the vulnerability of stochastic networks. *IEEE Transactions on Reliability*, 52(1):63–68, 2003.

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

[6] Satish V Ukkusuri and Wilfredo F Yushimito. A methodology to assess the criticality of highway transportation networks. *Journal of Transportation Security*, 2(1-2):29–46, 2009.

[7] Qixing Wang, Lance Fiondella, Nicholas Lownes, John Ivan, Reda Ammar, Sanguthevar Rajasekaran, and Sherif 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.

[8] Lance Fiondella, Jun Liu, Sherif Tolba, Sanguthevar Rajasekaran, Reda Ammar, Ashrafur Rahman, Nicholas Lownes, and John Ivan. Game theoretic vulnerability analysis for the optimal defense of high speed rail. In *Proc. IEEE International Conference on Homeland Security*, pages 305–311, 2012.

[9] Jun Duanmu, Kevin M Taaffe, Mashrur Chowdhury, and R Michael Robinson. Simulation analysis for evacuation under congested traffic scenarios: a case study. *Simulation*, 88(11):1379–1389, 2012.

[10] PTV. Ptv visum official website. http://vision-traffic.ptvgroup.com/en-us/products/ptv-visum/, 2016. Accessed: 2016-05-07.

[11] Martin Fellendorf. Vissim: A microscopic simulation tool to evaluate actuated signal control including bus priority. In *Proc. 64th Institute of Transportation Engineers Annual Meeting*, pages 1–9. Springer, 1994.

[12] M Balmer, K Meister, and K Nagel. *Agent-based simulation of travel demand: Structure and computational performance of MATSim-T*. ETH, Eidgenössische Technische Hochschule Zürich, IVT Institut für Verkehrsplanung und Transportsysteme, 2008.

[13] Daniel Krajzewicz, Jakob Erdmann, Michael Behrisch, and Laura Bieker. Recent development and applications of SUMO - Simulation of Urban MObility. *International Journal On Advances in Systems and Measurements*, 5(3&4):128–138, December 2012.

[14] Christian Gawron. An iterative algorithm to determine the dynamic user equilibrium in a traffic simulation model. *International Journal of Modern Physics C*, 9(03):393–407, 1998.

[15] Edsger W Dijkstra. A note on two problems in connexion with graphs. *Numerische mathematik*, 1(1):269–271, 1959.

[16] Hillel Bar-Gera. Transportation network test problems. https://github.com/bstabler/TransportationNetworks, 2016. Accessed: 2016-05-07.

[17] Open street maps. http://www.openstreetmap.org/, 2016. Accessed: 2016-05-07.

[18] Netconvert. http://sumo.dlr.de/wiki/NETCONVERT, 2016. Accessed: 2016-05-07.

[19] V. Shekar and L. Fiondella. Graph extraction and demand profiling applications for transportation network research. In *Proc. Humanitarian Technology: Science, Systems and Global Impact*. Elsevier, 2016.