

COMPARISON OF POTENTIAL PATHS SELECTED BY A MALICIOUS ENTITY WITH HAZARDOUS MATERIALS : MINIMIZATION OF TIME VS. MINIMIZATION OF DISTANCE

Rakesh Nune
Pamela Murray-Tuite

Virginia Polytechnic Institute and State University
7054 Haycock Road
Falls Church, VA 22043,USA

ABSTRACT

Security of hazardous materials (hazmat) shipments is a growing concern for many governments and private companies due to their potential use as weapons. This paper identifies a methodology for obtaining the paths taken by a malicious entity when he/she hijacks a hazmat truck based on conditional consequence and a measure of cost (either distance or travel time). The work compares the routes obtained by travel time and distance for a sample network and suggests the need for travel time to be considered in urban areas, especially in peak hours.

1 INTRODUCTION

Hazardous materials (hazmat) are generally substances required for industrial production or a byproduct of the same. These materials should be safely transported to and from the industrial areas owing to their potential hazardous behavior. For example, in 1977 alone, the United States transported 2.8 million tons of ammonia by highway over 476 million ton-miles (Brown et al. 2001). Thus, hazmat routing is a source of concern for government and private agencies.

The major concern about hazmat transportation is the potential damage done to society and the environment when accidents or spills occur (Taboada et al. 2006). Hence, there is considerable pressure on authorities to formulate guidelines for routing hazmats. Such dangerous shipments pose risk both at individual and societal levels and was calculated by previous authors (Saccomanno and Shortreed 1993).

The probability of occurrence of such accidents is generally very low, but when they do occur, they could cause wide-spread damage to both human lives and infrastructure. Such behavior classifies these events in to a low probability and high consequence (lphc) group. Thus, the paths chosen by the hazmat trucks should minimize the

possible consequences and also minimize the distance traveled in order to reduce shipments costs.

These shipments could become targets for terrorists and other malicious entities and could be used as weapons. Terrorist-related risk involved in hazmat transportation is very difficult to calculate, due to its low probability of occurrence and potential high consequence. Risk is generally estimated with probability and consequence of the event as a whole (Volpe Center 2003; Haimes 2004). Consequence is measured in terms of causalities or economic loss (Bush 2003; Crowther and Haimes 2005). Previous authors (Huang and Fery 2005; Huang et al. 2004) have worked on the integration of hazmat routing and security concerns but did not consider the decisions hijackers might make to reach their targets.

1.1 Travel Time and Simulation

Changing traffic conditions and congestion patterns actually force the general commuters and hazmat vehicle owners to choose routes according to travel time rather than the distance (Haghani and Jung 2005). Chang and Mahmassani (1998) described a heuristic rule with which daily commuters recall the travel times under limited information and their cumulative experience for choosing the best routes to reach their destination. Wunderlich (1998) conducted a study by simulating route guidance under variable network congestion conditions and concluded that guidance actually improves the travel by 8-26% in peak time. The same rule applies to hazmat vehicle owners and more importantly for the malicious entities.

Previous work (Murray-Tuite et al. 2006) focused on developing routes taken by the hazmat driver and also the possible routes taken by the malicious entities. The present work considers travel time, rather than distance, in route determination. The travel time coupled with possible consequence on network links is used for the estimating the multiple paths of the malicious entities in this work. The

paper compares the results between the routes of the malicious entities by considering travel distance and travel time.

The remainder of this paper consists of three sections. First, the problem is defined and the mathematical model is described. Second, the model is applied to a sample network and the simulation is described. Finally, conclusions are presented.

2 PROBLEM DEFINITION

This paper identifies possible paths taken by the hijacker once he/she captures the hazmat truck at any point in its normal route. Since the malicious entity’s target is often located in an urban area and the objective is often to cause the maximum damage, the entity is assumed to time a hazmat release during or near the peak traffic hours. The hijacker is further assumed to eliminate paths with high congestion levels to reduce his/her travel time. The network on which he/she hijacks the truck and causes damage is denoted by $G(N, A)$ which consists of a set of nodes N and directed arcs A . Each link i has the attributes of law enforcement interception probability P_i , consequence C_i , distance d_i , and travel time t_i .

The malicious entity intercepts the truck at node O' and moves towards target T . Table 1 summarizes the notation used in the paper.

The path chosen by the hijacker should maximize consequence with consideration of the probability of being intercepted by authorities and minimize travel time. The route taken by the malicious entity may be determined by the distance traveled (Murray-Tuite et al. 2006), but in urban areas, travel times are not necessarily proportional to distance due to congestion.

2.1 Procedure

The magnitude of the probability of an accident on any particular link is sufficiently small that the probability of accident along a path can be approximated as in equation (1) (Sherali et al. 1997).

$$P_{AQ} = \sum_{i \in A} p_{ai} x_i \quad (1)$$

Where

P_{AQ} is the probability of accident on path Q

p_{ai} is the probability of accident on a particular link i

x_i is the variable denoting link i whose value becomes 1 if link is chosen and 0 if not.

The expression can be similarly extended to probability of hijack since the probability of hijack is also comparatively very low which gives rise to equation (2)

$$P_Q = \sum_{i \in A} p_i x_i \quad (2)$$

Where

P_Q is the probability of hijack along path Q

p_i is probability of interception by law authorities on link i

x_i is the variable denoting link i whose value becomes 1 if link is chosen and 0 if not.

Table 1: Notation summary

Notation	Interpretation
Sets and Indices	
$G(N,A)$	Road network consisting of a set N of nodes and set A of directed arcs
A	Set of directed arcs, indexed by a
N	Set of nodes, indexed by j
O'	Origin node of the malicious entity’s path
T	Possible target for the malicious entity
Parameters	
C_i	Consequence of a hazmat incident on link i
D_i	Length of link i
P_{hj}	Probability of a successful hijack at node j
P_i	Probability of interception by law enforcement
λ	Weight associated with conditional expected consequence
t_{min}	Minimum time for the malicious entity’s path
t_{max}	Maximum time for the malicious entity’s path
v_{min}	Minimum conditional expected consequence for the malicious entity’s path
v_{max}	Maximum conditional expected consequence for the malicious entity’s path
w_{min}	Minimum conditional expected consequence for original path
w_{max}	Maximum conditional expected consequence for original path
t_i	Travel time on a link i
Variables	
x_i	Binary integer decision variable taking the value 1 if the link is chosen by the hijacker and 0 otherwise
z_1	Value of objective function for malicious entity’s path selection using distance of the network
z_2	Value of objective function for malicious entity’s path selection using travel time of the network

The methodology developed in the following sections for identifying the most likely paths taken by the malicious entities is based on a few assumptions. First, it is certain that a hijacking will occur somewhere in the network. Sec-

ond, once a truck is hijacked, it is directly moved towards the target. Multiple paths are estimated for a single target given the most possible hijack node.

The method in the present work obtains routes based on the trade off between consequence and estimated travel time. Previous works have considered use of distance as cost, but travel time might be a better measure during peak hours. Since congestion causes considerable changes in travel time, it is often necessary to recalculate the paths, especially estimating the paths taken by malicious entities.

2.2 Preferred Paths By The Malicious Entity

The different paths preferred paths by the malicious entity are obtained from the formulation gives from equations (3-5)

$$\min z_1 = -\lambda_1 \frac{\sum_{i \in A} p_i C_i x_i}{\sum_{i \in A} \rho_i x_i - v_{\min}} + (1 - \lambda_1) \frac{\sum_{i \in A} d_i x_i - u_{\min}}{u_{\max} - u_{\min}} \quad (3)$$

Subject to

$$\sum_{i \in F(j)} x_i - \sum_{i \in H(j)} x_i = \begin{cases} 1 & \text{if } j = O \\ -1 & \text{if } j = T \\ 0 & \text{Otherwise} \end{cases} \quad (4)$$

$$x_i \in \{0,1\} \forall i \in A \quad (5)$$

the objective function in equation 3 should be minimized for different values of λ_1 . Equation 4 represents the continuity of the flow in the network and equation 5 ensures the integer constraint of the variables.

$$z_2 = -\lambda_2 \frac{\sum_{a \in A} \rho_a C_a x_a}{\sum_{a \in A} \rho_a x_a - v_{\min}} + (1 - \lambda_2) \frac{\sum_{i \in A} t_i x_i - t_{\min}}{t_{\max} - t_{\min}} \quad (6)$$

Equation 6 is obtained by replacing the travel distance term with travel time t_i in equation (3). The methodology for obtaining the values of obtaining $v_{\max}, v_{\min}, t_{\max}, t_{\min}$ and procedure for solving is used as described by (Murray-Tuite et al. 2006)

3 SAMPLE APPLICATION

The above descried routing methodology is applied to a network based on Reston, Virginia. The network, shown in Figure 1, has 354 links and 147 nodes and is divided into

14 zones. Reston has population of 56,407 according to the 2000 US Census (Citydata.com 2000). In addition to the residents, people move through Reston going to/ coming from Washington, DC. The network has both freeways and arterials, including Route 7 and the Dulles Toll Road indicated by arrows in Figure 1. Approximately 60,000 total vehicles were loaded on the network in 120 minutes, with an incremental increase up to 75 minutes followed by a gradual reduction in new demand. The exact demand for any particular fifteen minute increment was based on a random number and a base origin-destination matrix. The travel time was found by simulating the given environment with the traffic assignment-simulation tool DYNASMART-P version 1.2. Traffic was assigned according to user equilibrium. Simulation time was set to 1000 minutes and 50 iterations were performed. The parameters used for the simulation are given in Table 2.

Consequences were generated randomly and distributed among the zones depending on the zone characteristics. The areas inside Reston with residential areas and office space were given high consequence values and zones containing only routes and freeways were given lower values.

The probability of capture by law authorities was also randomly generated and distributed differently in residential areas and highways, as it is easier to be caught in arterials due to lower capacity, low speeds and higher density of law agencies. The hazmat truck was assumed to be hijacked at the northern most point in Figure 1 on Route 7. The hijacker then proceeds towards the airport, which is the selected target.

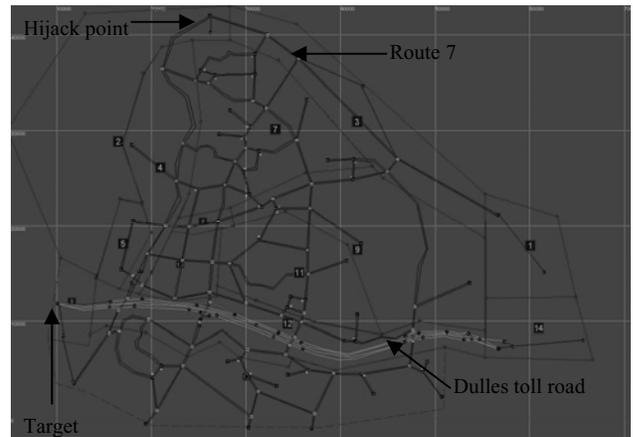


Figure 1: The map of Reston used for simulation

The traffic condition simulated was the peak hour, which is when heavy congestion is experienced and when the malicious entity might prefer to attack so that he/she can cause maximum damage. Congestion and queues can be observed from the simulation software outputs for the first 400 minutes which can be observed from the Figures 2-7.

Table 2: Parameters used for simulation

Total number of vehicles	58425
Max Simulation Time (min)	1000
Number of Nodes	147
Number of Links	354
Total number of iterations	20
Start Time in Which Vehicle Statistics are Collected	30
End Time in Which Vehicle Statistics are Collected	1000

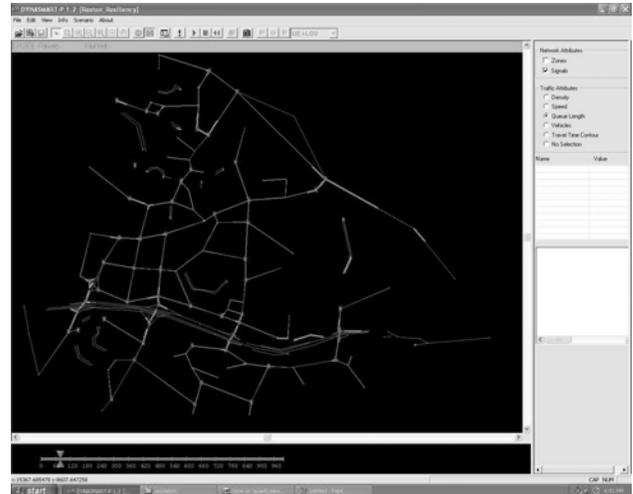


Figure 4: Queue length at traffic signals after 90 min.

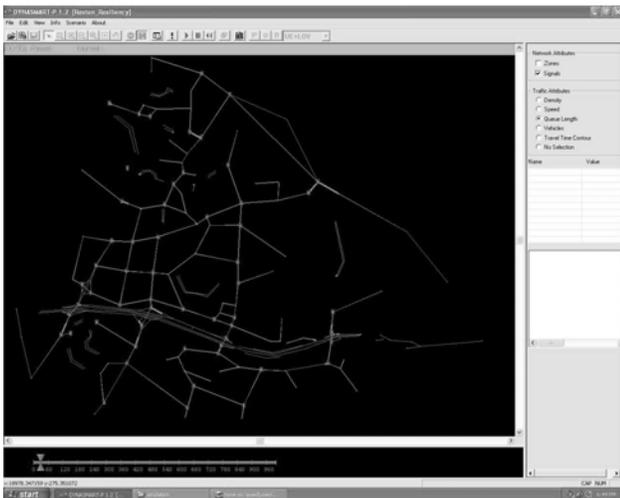


Figure 2: Queue length at traffic signals after 30 min.

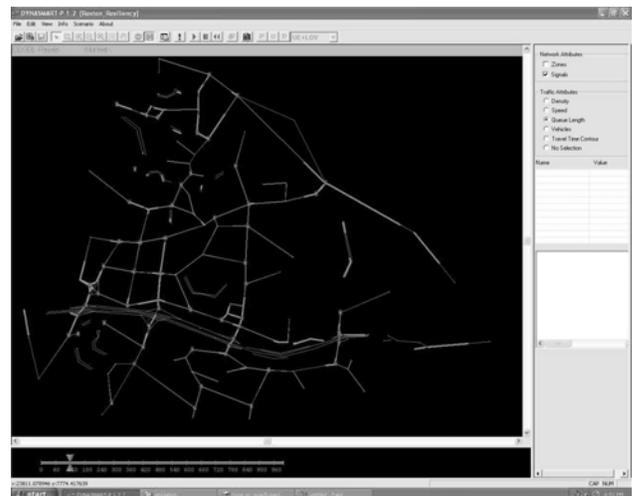


Figure 5: Queue length at traffic signals after 120 min.

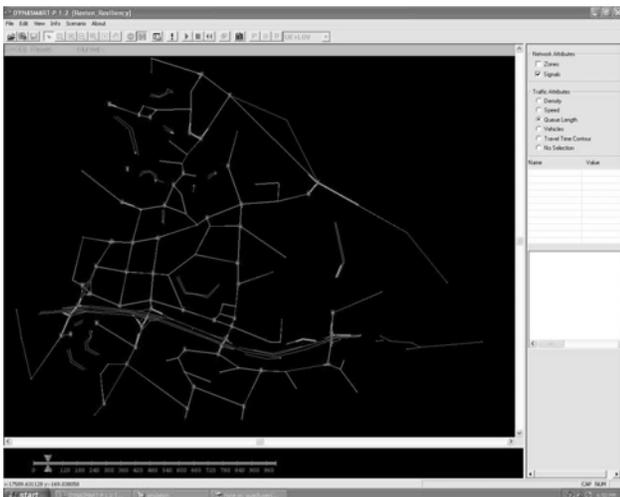


Figure 3: Queue length at traffic signals after 60 min.

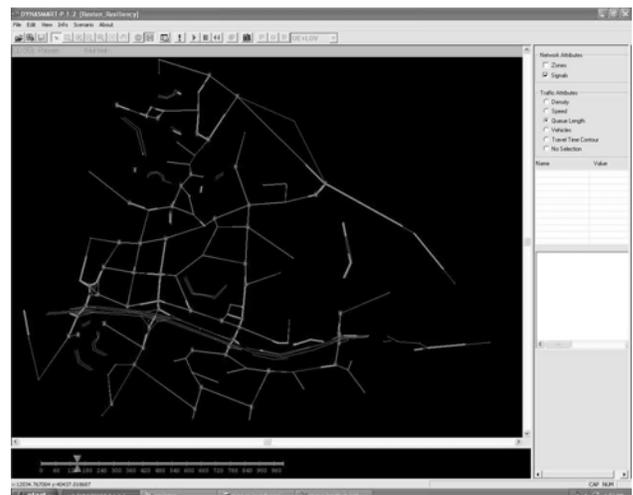


Figure 6: Queue length at traffic signals after 150 min.

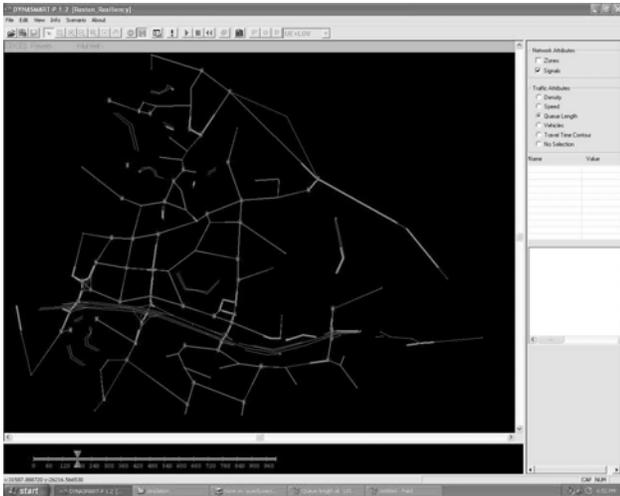


Figure 7: Queue length at traffic signals after 180 min.

The darker lines on the links indicate the length of the queues and the blue dots indicate the traffic signals. Mean travel time for first 180 minutes is considered starting from 30 minutes. This represents the peak time of loading and which is of primary interest here.

3.1 Different Preferred Paths

Using the described optimization formulation in equations (3-6) various paths were calculated for different values of λ . The different paths can be observed in the Figures 8-10 when distance is considered and in Figures 11-13 when travel time is considered. The highlighted line indicates the path taken by the malicious entities.

3.2 Results

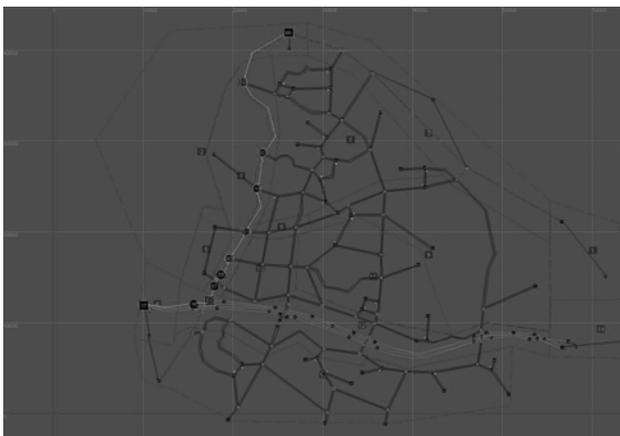


Figure 8: Path obtained when $\lambda = 0.1$ for distance

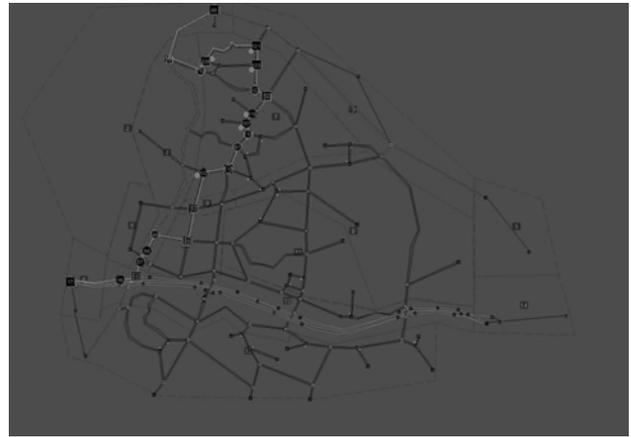


Figure 9: Path obtained when $\lambda = 0.5$ for distance

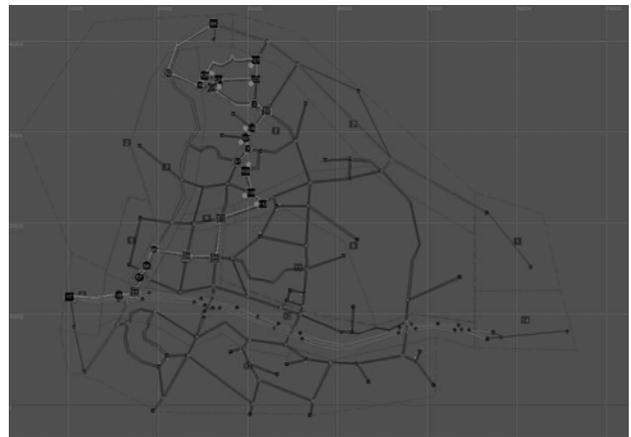


Figure 10: Path obtained when $\lambda = 0.9$ for distance

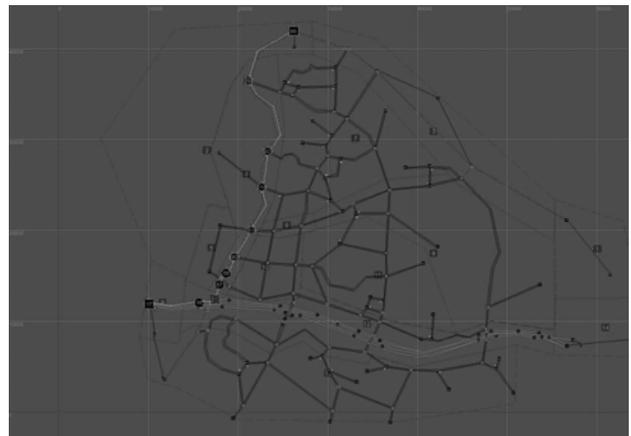
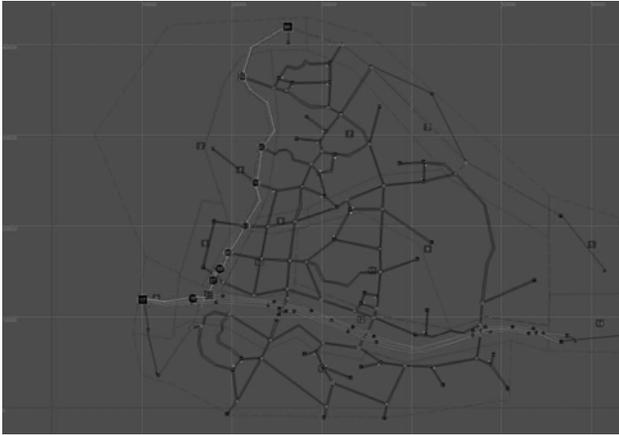
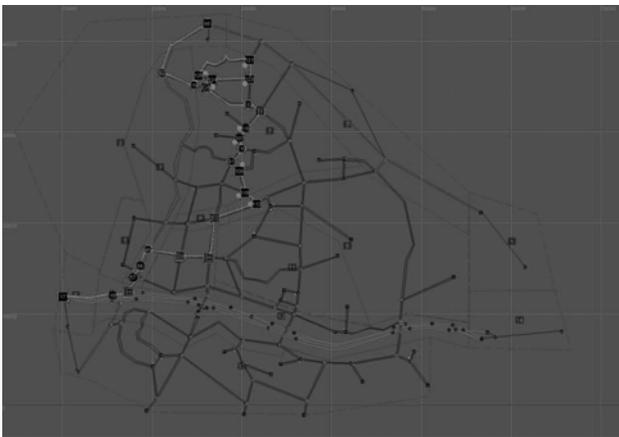


Figure 11: Path obtained when $\lambda = 0.1$ for travel time

Figure 12: Path obtained when $\lambda = 0.5$ for travel timeFigure 13: Path obtained when $\lambda = 0.9$ for travel time

4 CONCLUSIONS

As Reston is both a residential and working area the consequence to human lives and private property that can be caused by any possible hazmat incident in those areas is relatively high compared to more open roadways. But from the queuing pictures it can be observed that these areas also have relatively high congestion and hence high travel time. Thus we can see that for $\lambda = 0.1$ which would give preference (greatest weight) to shortest travel distance or time, the routes obtained by distance and travel time criteria are the same whereas at $\lambda = 0.5$ (figure 9 and 12) differences exist. The time criteria yields a path traveling on the highway (Fairfax County Parkway) where there is less congestion whereas the distance criteria gives a path through Reston which has higher consequences since the distance factor and consequence factor are now given equal weight and the distance factor is not as dominating as the travel time factor which is very high in the Reston area during the peak hour. This implies that though the malicious entity might want to travel in a path where he/she can also cause a high degree of damage and also lower travel

time, he/she might not prefer the path through Reston because of high travel time unless and until he/she gives a very high preference to only the damage factor. Figures 10 and 13 obtained at $\lambda = 0.9$ are similar except in the last few links of the routes because the distance and travel time factor is reduced to a small amount.

Using distance for determining the routes taken by the malicious entities after hijacking might not give the correct estimate of the path especially in networks which are coupled with freeways and toll roads. The travel time factor dominates more in peak hours when congestion is very high and hence could give different answers if travel time is not used. The travel time might be proportional to distance at off peak hours and in areas where all the links face similar kinds of congestion. The present results are specific to networks when there is surrounding freeways which provide a relatively low travel time at peak hours. The selected hijacking point and target also influence the potential variability in routing.

Future work will include the larger networks. In the present work consequence is considered from the residential and office space, the consequence actually changes with increases in traffic and queue length as the damage at that point could take more lives; including this criterion would further increase the results' accuracy.

REFERENCES

- Brown, D. F., S. Hwang, J. O. Steen, A. J. Policastro, and W. E. Dunn. 2001. A risk assessment for national transportation of selected hazardous materials. *80th Annual Meeting of the Transportation Research Board*, Washington, D.C., Transportation Research Board.
- Bush, G. W. 2003. Homeland Security Presidential Directive / HSPD-7. The White House, Office of the Press Secretary.
- Citydata.com. (2000). Reston, Virginia. Retrieved 2 April, 2007, from <http://www.city-data.com/city/Reston-Virginia.html#top>.
- Crowther, K. G. and Y. Y. Haimes. 2005. Application of the inoperability input-output model (IIM) for systemic risk assessment and management of interdependent infrastructures. *Systems Engineering* 8(4): 323-341.
- Saccomanno, F. F. and J. H. Shortreed. 1993. Hazmat transport risks: societal and individual perspectives. *ASCE Journal of Transportation Engineering* 119(2): 11.
- Chang, G.L., and H. S. Mahmassani. 1998. Travel time prediction and departure time adjustment behavior dynamics in a congested traffic system. *Transportation Research* 22B(3): 217-232.
- Haghani, A. and S. Jung. 2005. A dynamic vehicle routing problem with time-dependent travel times. *Computers & Operations Research* 32:2959-2986.

- Haimes, Y. Y. 2004. Risk modeling, assessment, and management of terrorism. *Risk Modeling, Assessment, and Management*. John Wiley & Sons. Hoboken, John Wiley & Sons, Inc: 684-716.
- Huang, B. and P. Fery 2005. Aiding route decision for hazardous material transportation. *Transportation Research Board*.
- Huang, B., C. R. Long and Y. S. Liew. 2004. GIS and genetic algorithms for HAZMAT route planning with security considerations. *International Journal of Geographical Information Science* **18**(8): 769-787.
- Murray-Tuite, P., R. H. Garrido and R. Nune. 2006. Path prediction methodology for hazardous materials transported by malicious entities. In *11th World Conference on Transport Research* Berkeley, California.
- Sherali, H. D., L. D. Brizedine, T. S. Glickman and S. Subramanian. 1997. Low probability-high consequence considerations in routing hazardous material shipments. *Transportation Science* 31:14.
- Taboada, J., J. M. Matias, A. Saavedra, C. Ordonez and R. Martinez-Algeria 2006. Risk communication: around the world neural networks models for assessing road suitability for dangerous goods transport. *Human and Ecological Risk Assessment* 12:17.
- Volpe Center. (2003). Risk assessment and prioritization. Retrieved July 14, 2006, from <http://www.volpe.dot.gov/infosrc/journal/2003/chap1.html>.
- Wunderlich, K. 1998. A simulation-based assessment of route guidance benefits under variable network congestion conditions. *Mathematical and Computer Modeling* 27(9-11): 87-101.

AUTHOR BIOGRAPHIES

RAKESH NUNE is a graduate research assistants presently pursuing his masters from Virginia Tech in transportation engineering. He has completed his undergrad studies in Indian Institute of technology Guwahati INDIA. His research interests include optimization algorithms, modeling and AI. His email id is nune@vt.edu

PAMELA M. MURRAY-TUITE is an Assistant Professor of Civil and Environmental Engineering at Virginia Polytechnic Institute and State University (Virginia Tech). She was previously a senior consultant with Booz Allen Hamilton. She received a BS degree in Civil Engineering from Duke University and an MS and a PhD in Civil Engineering from The University of Texas at Austin. Her current research interests focus on transportation network analysis, modeling, and simulation; security, reliability, risk, and resilience analysis; evacuation modeling; disaster recovery modeling; and congestion mitigation. Her e-mail address is murraytu@vt.edu.