Attacker–defender models and road network vulnerability

BY M. G. H. BELL¹,*, U. KANTURSKA², J.-D. SCHMÖCKER¹
AND A. FONZONE³

¹Centre for Transport Studies, Imperial College London, London SW7 2BU, UK
²Arup, 13 Fitzroy Street, London W1T 4BQ, UK
³Dipartimento di Vie e Trasporti, Politecnico di Bari, Bari 70125, Italy

The reliability of road networks depends directly on their vulnerability to disruptive incidents, ranging in severity from minor disruptions to terrorist attacks. This paper presents a game theoretic approach to the analysis of road network vulnerability. The approach posits predefined disruption, attack or failure scenarios and then considers how to use the road network so as to minimize the maximum expected loss in the event of one of these scenarios coming to fruition. A mixed route strategy is adopted, meaning that the use of the road network is determined by the worst scenario probabilities. This is equivalent to risk-averse route choice. A solution algorithm suitable for use with standard traffic assignment software is presented, thereby enabling the use of electronic road navigation networks. A variant of this algorithm suitable for risk-averse assignment is developed. A numerical example relating to the central London road network is presented. The results highlight points of vulnerability in the road network. Applications of this form of network vulnerability analysis together with improved solution methods are discussed.

Keywords: transport network vulnerability; defender–attacker–defender; risk-averse routing; game theory; networks under attack

1. Introduction

Uncertainty is a pervasive feature of decision making in general, and decisions regarding the use of road networks are no exception. Where probabilities for events (disruptions, failures and attacks) that affect the use of road networks are known, it is possible to base decisions on expectations. However, a feature of uncertainty is that the probabilities corresponding to such events may be unknown. This paper presents an approach to decision making under uncertainty whereby the unknown event probabilities are replaced by event probabilities that constitute a worst case from the network user perspective. It is assumed that no more than one such event can occur and that the loss arising from any event, if the network user is involved, is known to the user. The network user can therefore reduce his/her exposure to the loss arising from any event by

* Author for correspondence (m.g.h.bell@imperial.ac.uk).

One contribution of 16 to a Discussion Meeting Issue ‘Networks: modelling and control’.
reducing the use of the link or area affected. This pessimistic view of event probabilities is then relaxed to allow consideration of less extreme versions of risk aversion.

In parallel security-related work, attacker–defender (AD) models have been applied to electricity supply networks and oil supply chains (see Brown et al. 2006). These have the structure of a game, whereby an attacker attempts to inflict maximum damage by supply interdiction and the defender seeks to route supplies in a way that minimizes the damage inflicted by supply interdiction. This is a zero sum game of pure strategies between an attacker and a defender. This paper, by contrast, focuses on the mixed strategy case where the next decisions of the attacker and defender are not known with certainty by each other. This is equivalent to finding the worst set of probabilities for failure, disruption or attack scenarios and using these to base decisions on network use. The outcome is a set of optimal path-use probabilities, with the implication that if the scenario probabilities are not known with certainty the network user should not ‘place all his eggs in one basket’ but rather spread usage across a number of paths so that his/her exposure to any given scenario is minimized.

The paper briefly considers a number of applications categorized into planning and prediction. The planning applications include the shipment of very important persons (VIPs) and hazardous materials in hostile (or potentially hostile) environments. The mixed strategy solution tells the shipper, who chooses routes randomly, how often to select each route. The prediction application relates to risk-averse traffic assignment. Here it is noted that not all drivers will base route choices on the worst scenario probabilities, so a relaxation is formulated to allow the assumed scenario probabilities to lie between risk neutral and the worst case.

Road networks are characterized by their large size. Excellent electronic road navigation networks are available from firms such as Navteq and Teleatlas. These can be ported directly into traffic assignment software. Practical applications of AD models should make use of existing networks and software wherever possible. A solution algorithm using a commercial traffic assignment tool and the Python scripting language together with the method of successive averages is presented. It is noted that at the solution neither the worst scenario probabilities nor the optimal path usage probabilities are in general unique. However, under a relaxation designed for risk-averse traffic assignment, the scenario probabilities, but not necessarily the path-use probabilities, are unique. The paper concludes with a numerical example relating to the movement of VIPs across London.

2. Literature review

The quality of service offered by transport systems has been subject to extensive research in recent years. Immers et al. (2004) highlight that a transport system is seen as reliable when the experienced travel time is not very different from the expected travel time. In general, divergences are brought about by changes in demand and supply, whether expected or unexpected, frequent or exceptional. Given an incident, its impact will depend on network topology (is there sufficient redundancy and spare capacity in the residual network?), the state of network information (are users informed about the location and duration of a blockage as
well as the propagation and dissipation of congestion resulting from the blockage?) and the reactions of network users (are users aware of alternative routes?). Clearly, the propagation and dissipation of congestion will be determined in part by the reactions of network users. Nicholson et al. (2003) emphasize that the loss of performance following an incident also depends on the degree of malevolence involved in the incidents and on the level of user knowledge regarding malevolence.

One response to malevolence is to focus on the potential consequences and minimize these (Berdica 2002). Bell (2000, 2003) estimates the potential benefit from a routing strategy involving multiple routes in situations where incident probabilities are not known, following the ‘don’t place all your eggs in one basket’ principle. Jenelius et al. (2006) put forward the concepts of link importance and site exposure to deal with very rare events, proposing measures based on the increase in generalized travel cost caused by rerouting when some links are removed. A similar approach can be found in Scott et al. (2006), who present case studies implementing an equilibrium assignment and show that their measure of link importance, called the network robustness index, can improve the effectiveness of highway planning. Their index ranks link importance according to the increase in travel cost if the link is blocked.

The literature concerning transport networks under attack can be classified according to the degree of complexity in representing flows. The simplest (zero-degree models) consider empty networks and examine just their topological features. An example of such an approach is that of Angeloudis & Fisk (2006), who inspect the topology and robustness of large subway systems in the case of targeted attacks, following the approach of Albert et al. (2000). The most studied problem is that of a flow between a single origin and destination (OD) pair (one-degree models), known in the operations research literature as network interdiction problems (see Pan (2005) for a comprehensive bibliography). Situations are studied in which an attacker tries to thwart mobility in a network by interdicting a given number of links with the intent of maximizing the shortest path (e.g. Israeli & Wood 2002) or minimizing the maximum flow between two nodes. The interdiction problem has been studied in two ways: deterministic, in which there is no uncertainty related to network features and attack effectiveness (Wood 1993; Washburn & Wood 1995; Royset & Wood 2007); and stochastic, in which arc capacities and/or attack outcomes are random variables (see Cormican et al. 1998; Pan 2005). Recently, interest has been growing in analysing networks with many OD pairs (n-degree models), as in the Scott et al. (2006) paper.

The interdiction model is an AD model, which, as in Brown et al. (2006), can be used as a procedure for identifying a near-optimal, budget limited defence plan to efficiently protect infrastructure against terrorist attack. Such models lead to bi-level optimization problems in which an attacker maximizes the defender’s minimum operating cost. Only heuristics are available to identify the critical infrastructure. Brown et al. (2006), therefore, propose to embed an AD model in a tri-level optimization problem called a defender–attacker–defender (DAD) model, in which the defender has limited resources to protect the system and must decide where to deploy them to minimize the damage the attacker can cause.

An example of the DAD approach is provided by Church & Scaparra (2005), dealing with the r-interdiction median problem with fortification, the objective of which is to find the interdiction set (r of p supply locations) which, when
removed, yields the highest level of weighted distance’. The authors show that the subset of the \( q \) facilities ‘which when fortified, provides the best protection to a subsequent optimal \( r \)-interdiction strike’ must contain at least one element of the interdiction set, but does not necessarily coincide with it. Smith et al. (2005) implement a DAD model for the design of survivable networks. The paper considers two-player games under three different attack strategies: in the first, the demon destroys the links with the largest capacities; in the second, the links with the highest initial flows; and in the third, those links whose failure minimizes the benefits generated by the flows.

3. Game theory approach to vulnerability

The theory of games, initially developed by von Neumann (see Osborne (2003) for an exhaustive introduction to the topic), is a study of the interaction between rational decision makers. Each player has a number of strategies (feasible actions), which determine the outcome of the game and the pay-off to each player. The conflict arises when particular players value their outcomes differently. A pure conflict occurs when two players aim to achieve opposite outcomes. Such a situation is called a ‘zero-sum game’. An equilibrium outcome of a game is achieved when each player has chosen a strategy, either pure or mixed, and neither has any incentive to move to a different strategy. This happens only when a maxmin strategy of one player gives the same outcome as a minmax strategy of another player.

Game theory has been applied in many contexts; Hollander & Prashker (2006) provide a review of non-cooperative game theory applications in the transport field. Games are classified into four groups; against a ‘demon’, between travellers, between authorities, and between travellers and authorities. Games against a demon are zero-sum games, in which one or more demons try to maximize user costs. The solution describes optimal network usage from the perspective of a pessimistic user, highlighting points of vulnerability.

The method developed by Bell (2000) is a game between (i) a traveller, referred to as the ‘router’, who seeks a least-cost path between the OD and (ii) a demon, who strives to maximize the trip cost by failing one link. The equilibrium solution to the game gives the optimal strategy for the traveller to avoid excessive costs, as well as the optimal strategy for the demon to be sure that at least a certain loss will be caused irrespective of the path selected by the traveller. Either pure or mixed strategies may be considered. In the case of pure strategies, the result is an AD model of the kind defined by Brown et al. (2006).

The resulting integer programming problems are typically difficult to solve. In the Bell (2000) formulation, mixed strategies are allowed. As this relaxes the integer constraint, solutions are easier to find. The expected trip cost at equilibrium can be treated as a measure of overall network vulnerability, while the link failure probabilities indicate links that are critical for network performance. The optimal strategy for the traveller in general involves selecting a path from a set of paths having positive probability, where the set has more than one member. Similarly, the optimal demon strategy is to split disruption probabilities over more than one link. The solution delivers the worst link attack probabilities, on the assumption that these are what the traveller is reacting to.

Phil. Trans. R. Soc. A (2008)
4. Mathematical formulation

In Bell & Cassir (2002) and Cassir et al. (2003) link travel cost is indirectly influenced by the link status, because a failed link is defined as a link with reduced capacity and hence more prone to congestion. This paper, however, follows Bell (2000) where it was assumed that link travel cost is directly influenced by link status and is not a function of link flow. Following Cassir et al. (2003), the game described above can be expressed as an optimization problem.

In the following, we assume for simplicity that scenario \( j \) implies a failure, disruption or attack on link \( j \). This is not, however, a limitation of the method. It is possible for a single scenario to encompass multiple link failures, disruptions or attacks. The mathematical notation is summarized in Table 1.

If only movement between a single OD pair is considered, the problem is then to solve the following maximization and minimization in equation (4.1) simultaneously:

\[
\min_h \max_q TC(q, h) = \sum_j q_j h_k g_{jk},
\]  

subject to \( \sum_j q_j = 1, \quad q \geq 0 \) and \( \sum_k h_k = 1, \quad h \geq 0, \) with

\[
g_{jk} = \sum_i a_{ik} c_{ij},
\]

where \( c_{ij} = DCt_{ti} \) if link \( i \) fails in scenario \( j \) and \( c_{ij} = tt_i \) otherwise.

Note the lack of the time dimension: the traveller does not proceed through the network links dynamically. Where routes are pre-planned and not adjusted in the course of the journey, such a static approach is suitable, especially for route pre-planning purposes. At the solution to the above minmax problem, the following conditions must hold: for all scenarios \( j \)

\[
q_j = 0 \iff \sum_k h_k g_{jk} < \max_s \sum_k h_k g_{sk} \quad \text{and} \quad q_j \geq 0 \iff \sum_k h_k g_{jk} = \max_s \sum_k h_k g_{sk}
\]

and for all paths \( k \)

\[
h_k = 0 \iff \sum_j q_j g_{jk} > \min_s \sum_j q_j g_{js} \quad \text{and} \quad h_k \geq 0 \iff \sum_j q_j g_{jk} = \min_s \sum_j q_j g_{js},
\]

Table 1. Notation.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( q )</td>
<td>vector of link failure probabilities</td>
</tr>
<tr>
<td>( h )</td>
<td>vector of path choice probabilities</td>
</tr>
<tr>
<td>TC</td>
<td>total cost to travel between OD pair</td>
</tr>
<tr>
<td>( g_{jk} )</td>
<td>travel cost on route ( k ) under scenario ( j )</td>
</tr>
<tr>
<td>DC</td>
<td>disruption factor indicating the increased cost resulting from a failure/attack</td>
</tr>
<tr>
<td>( tt_i )</td>
<td>non-disrupted travel cost on link ( i )</td>
</tr>
<tr>
<td>( c_{ij} )</td>
<td>travel cost on link ( i ) under scenario ( j )</td>
</tr>
<tr>
<td>( a_{ik} )</td>
<td>link incidence matrix (1 if link ( i ) is on path ( k ), 0 otherwise)</td>
</tr>
</tbody>
</table>
It is well known (e.g. Hillier & Lieberman 1990) that the above minmax problem can be formulated as a linear program as follows:

$$\min_h C \text{ subject to } \sum_k h_k g_{jk} \leq C \text{ and } \sum_k h_k = 1, \ h \geq 0,$$

for which at the solution the dual variables are equal to $q$, and $C$ is equal to $TC$ at the solution to the corresponding maxmin problem (Bell 2000).

5. A solution algorithm

While this problem may be solved very efficiently using a standard linear program solver, this approach requires the prior enumeration of all the relevant paths. The objective here was to solve the problem using standard traffic assignment software which would create the paths as the iterations progress. Standard traffic assignment software is optimized for large road networks, can make use of electronic road navigation networks such as Navteq or Teleatlas, and can display the results efficiently. The software chosen for the numerical example presented later is VISUM from PTV AG.

The algorithm used to solve this problem is based on the method of successive averages (Sheffi 1985). Each player in effect looks at the previous history of the opponent’s strategies and bases the next play on that evidence. After the initialization in step 0, the first sub-problem (find optimal path flows given link failure probabilities) and the second sub-problem (find optimal link failure probabilities given path flows) are solved sequentially in each iteration $m$ until convergence. The algorithm has converged when neither $q$ nor $h$ change significantly between iterations. Though a formal proof of convergence for the method of successive averages (MSA) is missing for this application, experience shows that the solutions obtained are nearly optimal.

— Step 0. Initialize $m=1$ and $q^0 = 1/\text{no. of links}$. Set path flows $h^0$ to 1 for the least non-disrupted cost path and 0 otherwise.

— Step 1. Calculate expected link usage costs for given scenario probabilities $q^{m-1}$ ($\sum_j \sum_i q_i^{m-1} d_{ik} g_{jk}$ for all links $i$).

— Step 2. Obtain auxiliary path probabilities $y^m$ by assigning a unit OD flow to the least cost path. Note that only one path is used so only one element of $y^m$ is non-zero, and that element is one.

— Step 3. Update path probabilities using the MSA:

$$h^m = h^{m-1} + \frac{y^m - h^{m-1}}{m}.$$

— Step 4. Calculate expected scenario losses for given $h^m$ ($\sum_k h_k^m g_{jk}$ for all scenarios $j$).

— Step 5. Obtain auxiliary link failure probabilities $z^m$ by assigning 1 to the scenario with the highest expected loss, and 0 to other scenarios.

— Step 6. Update link failure probabilities by the MSA:

$$q^m = q^{m-1} + \frac{z^m - q^{m-1}}{m}.$$

— Step 7. If convergence criteria are satisfied stop, otherwise set $m := m+1$ and return to step 1.
This algorithm is found to converge rapidly for TC but not necessarily for \( q^m \) and \( h^m \). It should be noted that at the solution, TC is unique but not in general \( q^m \) and \( h^m \), presumably accounting for the slow convergence of these parameters.

An interesting alternative algorithm has been suggested by Nagae & Akamatsu (2007). By adding a weighted entropy term in \( h \) to equation (4.1), the minimization problem gains an explicit solution in the form of a logit path choice model. As the weight applied to the entropy term tends to zero the solution tends to that of the original problem given by equations (4.1)–(4.3). Substituting the logit model solution for \( h \) back into the augmented equation (4.1) leads to a single-level convex programming problem, which may be solved efficiently by an appropriate numerical method. The solution in \( h \) is now unique, as the augmented equation (4.1) is strictly convex in \( h \), although not in general in \( q \). A further extension is proposed which ensures that the solution in \( q \) is also unique. The disadvantage of this approach is that all paths have a non-zero probability of use at the solution, whereas at the solution the linear program partitions the set of paths into those to be used, referred to collectively as a hyperpath, and those not to be used. It is believed that this partition will not in general be unique.

### 6. Applications

A number of application areas for the proposed network vulnerability analysis have been identified. These may be divided into planning and predictive domains. In the planning domain, there is the movement of VIPs and hazardous material (Bell 2006; Kanturska et al. 2007; Nagae & Akamatsu 2007) as well as the design of risk-averse tours for freight distribution (Bell 2004). As mixed strategies are considered, the method indicates how to distribute repeated shipments across a set of paths or, in security applications, what probabilities to use when selecting a path at random. In the predictive domain, there is risk-averse traffic assignment (Bell & Cassir 2002; Szeto et al. 2007). Since drivers are risk averse to varying degrees, basing predictions on the worst set of scenario probabilities is perhaps too extreme. In the planning domain, the emphasis is more on physical threats and low frequency, high loss incidents, while in the predictive domain, the emphasis is more on risk-averse behaviour in response to relatively routine, low loss incidents.

One feature of the approach so far presented is the extremely pessimistic stance taken with regard to which link will fail. A variation on the Nagae & Akamatsu (2007) approach allows us to relax the degree of pessimism. Rather than seeking the worst \( q \), a logit function is introduced by adding a weighted entropy function in \( q \) to equation (4.1) yielding equation (6.1):

\[
\min_h \max_q \text{TC}(q, h) = \sum_j \sum_k q_j h_k g_{jk} - \left( \frac{1}{\theta} \right) \sum_j q_j \ln q_j. \tag{6.1}
\]

This time the maximization problem has an explicit solution for \( q \), namely

\[
q_j = \frac{\exp \left( \theta \sum_k h_k g_{jk} \right)}{\sum_s \exp \left( \theta \sum_k h_k g_{sk} \right)}, \tag{6.2}
\]
which is a logit choice function describing the probability that the demon chooses scenario \( j \). Parameter \( \theta \) is chosen to represent the degree of aggressiveness of the demon. This logit function can be substituted back into equation (6.1) leading to an alternative convex programming problem

\[
\min_h \ TC(h) = \left( \frac{1}{\theta} \right) \ln \sum_j \exp \left( \theta \sum_k h_k g_{jk} \right),
\]

subject to \( \sum_k h_k = 1, \ h \geq 0, \)

with \( g_{jk} = \sum_i a_{sk} c_{ij}, \)

where \( c_{ij} = DCtt_{i} \) if link \( i \) fails in scenario \( j \) and \( c_{ij} = tt_{i} \) otherwise.

Note that the gradient of the objective function is

\[
\frac{\partial TC(h)}{h_k} = \sum_j q_j g_{jk},
\]

which is the expected usage cost for path \( k \). The path with the least expected usage cost therefore defines the steepest descent direction. Equation (6.3) may thus be minimized subject to the constraints on \( h \) by the following revised and shortened MSA algorithm.

— **Step 0.** Initialize \( m = 1 \) and \( q^0 = 1/\text{no. of links} \). Set path flows \( h^0 \) to 1 for the least non-disrupted cost path and 0 otherwise.

— **Step 1.** Calculate expected link usage costs for given scenario probabilities \( q^m = \frac{1}{m \sum_j \sum_k q_{ijk} a_{sk} g_{jk}} \) for all links \( i \).

— **Step 2.** Obtain auxiliary path probabilities \( y^m \) by assigning a unit OD flow to the least cost path. Note that only one path is used so only one element of \( y^m \) is non-zero, and that element is one.

— **Step 3.** Update path probabilities using the MSA:

\[
h^m = h^{m-1} + \frac{y^m - h^{m-1}}{m}.
\]

— **Step 4.** Calculate \( q^m \) given \( h^m \) via equation (6.2).

— **Step 5.** If convergence criteria are satisfied stop, otherwise set \( m := m + 1 \) and return to step 1.

The solution is now unique in \( q \) rather than \( h \), because equation (6.1) is strictly convex in \( q \). The parameter \( \theta \) could be chosen to reflect the degree of risk aversion present in the population of drivers. When \( \theta \) tends to infinity, the solution tends to that of equation (4.1). Conversely, as \( \theta \) tends to 0, \( q \) becomes insensitive to the size of the expected loss in the event of a disruption, failure or attack, and therefore the traffic assignment is risk neutral. This model has similarities with the approach described in Bell (1999).

*Phil. Trans. R. Soc. A* (2008)
7. Numerical example

The data available for this example comprised the entire Greater London road network including link characteristics, such as permitted speeds, capacities and number of lanes. Traveller path choice was modelled by VISUM macroscopic traffic assignment software, widely used for small- and large-scale traffic assignment problems as well as for multimodal assignment problems. VISUM has been interfaced via the COM interface with Python script to obtain an assignment for the network link costs found in each iteration.

Here we show how the game was applied to determine a risk-averse routing strategy for the shipment of VIPs from Greenwich Park in south London to Victoria Park in north London. The shipper believes there will be disruption and, to be safe, assumes that this disruption will probably occur at a location that is worst for the shipper. In other words, the shipper considers a worst set of link disruption (link failure and link attack) probabilities. The part of the network considered comprises three river crossings: (i) Blackwall Tunnel, (ii) Rotherhithe Tunnel and (iii) Tower Bridge. Figure 1 shows the location of these river crossings and the shortest path for this OD pair obtained in free-flow conditions (light grey) together with the critical link (dark grey). A low disruption cost factor ($DC = 2$) was chosen in this example, meaning that the disruption would cause the cost of the disrupted link to double. Given such a disruption, the total cost of travelling this route would be 847 units.

By contrast, figure 2 shows the results at equilibrium obtained after 500 iterations. In this case, the risk-averse traveller considers not only the direct route but also allows for the option of re-routing via the nearby Rotherhithe Tunnel. This route
would be taken with a probability of 46%, whereas the route including the Blackwall Tunnel would be used with a probability of 54%. The inclusion of the second route leads to a decrease in the cost expected by a pessimistic driver to 825 units.

Figure 3 shows the equilibrium solution for the case where DC = 1 000 000. Such a high value was chosen in order to demonstrate that the solution obtained depends on the severity of the potential disruption. The scenario shown in figure 2 might correspond to the case of minor disruption whereas the scenario with a very high disruption cost might be used to plan where there is a risk of a life-threatening attack or a terrorist incident. When the disruption cost is high, in addition to the two routes shown in figure 2, a third route via Tower Bridge is added, involving an even longer detour. This route is preferred ($h_k = 62\%$) for two reasons. Firstly, the cost of disruption, being proportional to link travel time (see equation (4.3)), is lower for shorter links, hence the shorter bridge will be favoured. Secondly, the longer travel time with the detour via Tower Bridge is still relatively low compared with the disruption cost.

The above analysis shows that anticipating heavily disruptive incidents the risk-averse shipper should consider a wider spread of routes. Additional analysis with different DC values showed that for DC < 2 multiple paths do not need to be considered.

8. Protection of a critical asset

The solution of the game indicated that river crossings are critical links, which if attacked, would impose the greatest detours. The analysis with a very high disruption cost pointed out that Tower Bridge should be used in most cases from
Greenwich Park to Victoria Park. This evokes a question about what the optimal routing strategy would be when additional security measures were available to assure protection of a chosen asset (e.g. a bridge) from a potential attack. This has been modelled by excluding a link from the set of attack scenarios.

Should Tower Bridge be protected, the frequency of choosing a path across this bridge increases from 0.62 to 0.86 (figure 4). The shortest path leading through the Blackwell Tunnel should be used sometimes, despite the fact that it is indicated as a potential attack target. The route via Tower Bridge is still not regarded as fully safe, as the attacker would now focus on other links that lie on routes using this bridge. The Rotherhithe Tunnel should not be used anymore, because the shorter detour (compared with travelling via Tower Bridge) is not enough to compensate for the perceived risk associated with traversing this tunnel. When Tower Bridge is protected, the critical locations become links located closer to the OD, rather than river crossings.

9. Conclusions

This paper presents an approach to both analysing vulnerability and decision making under uncertainty in the context of using road networks. Where probabilities for predefined disruption, failure or attack scenarios are not known, it is suggested that the worst probabilities, or probabilities that lie between risk
neutral and the worst case, may be used. The methods presented take into account the fact that the worst set of scenario probabilities will in general depend on how the road network is used. Consequently, where some road network users are less risk-averse scenario probabilities should be chosen that lie between risk neutral and the worst case. This paper presents a variation on recent work by Nagae & Akamatsu (2007), which allows scenario probabilities to lie between risk neutral and the worst case. This approach has the beneficial side effect of uniquely defining the scenario probabilities.

The methods presented in this paper are applicable to large road networks as they make use of standard traffic assignment software, which in turn makes use of electronic road navigation networks. However, in the face of serious disruption, a more sophisticated type of model for travel times is required, since there will be congestion and knock-on effects from one link to the next through the formation of long queues. This will probably require the use of time-dependent traffic simulation. Computational efficiency could probably be increased by replacing the fixed step size by a line search or by simplicial decomposition.

We thank PTV Karlsruhe for providing us with VISUM and London road network, Mr Pieter De Beule of Imperial College London for his software assistance and two anonymous referees for their insightful comments.

*Phil. Trans. R. Soc. A* (2008)
References


Berdica, K. 2002 An introduction to road vulnerability: what has been done, is done and should be done. Transp. Pol. 9, 117–127. (doi:10.1016/S0967-070X(02)00011-2)


Pan, F. 2005 Stochastic network interdiction: models and methods. PhD dissertation, University of Texas at Austin, USA.

Phil. Trans. R. Soc. A (2008)


