

Traffic Assignment Based on Individual Risk-Attitude

Victor L. Knoop, Michael G.H. Bell, Henk J. van Zuylen

Abstract— Incidents whose frequencies are unknown cause a large part of the unreliability of road networks. Especially risk-averse road users avoid the possibility of large travel times under a disruption. This paper proposes a traffic assignment which accounts for risk-averseness. Scenarios for all possible disruptions are simulated. The risk-averseness of a user is generalized in a two-parameter route choice formulation. Depending on the parameters, users assign a weight on the travel times for each scenario. This is the basis for their route choice. The simulator can handle a traffic flow composed from different user classes simultaneously in the same network. In the presented case study, the link loads depend on the parameter settings of the users. The route choice for a user class also depends on the risk-averseness of the other users in the network.

I. INTRODUCTION

Road users are interested in reliable routes, sometimes even more than in fast routes[1]. Often, one needs to be certain that one arrives before a certain time, regardless of the road conditions. That is the reason that road authorities are switching their attention to reliability, see for instance [2].

If people want reliable routes, they will tend to avoid the routes that can have long delays, even if it were incidentally. This paper discusses a traffic assignment which takes that risk into account. On beforehand, however, the probability of travel times on links is not known. The concept of risk-averse behaviour, introduced to traffic by [3], assumes that risk-averse drivers are likely to count on the worst cases to happen.

In the literature the risk-averse assignment has just been combined with static models. This paper combines route advice with risk-averse behaviour. It introduces a new journey planner for individuals, taking risk-averseness into account. To implement the model, it is first of all needed that journey planners have an estimation of the OD-matrix and travel times.

Paper submitted for presentation at the International Conference of Infrastructure systems, March 15, 2008. This work was supported by the research program Next Generation Infrastructures and the Transport Research Center Delft.

V. L. Knoop and H. J. van Zuylen are with the Delft University of Technology; Transport & Planning; P.O. Box 5048; 2600 GA Delft; The Netherlands; Tel. +31 15 27 89 341 and TRAIL Research School; e-mail v.l.knoop@tudelft.nl or h.j.vanzuylen@tudelft.nl

M. G. H. Bell is with Imperial College London, Room 608, Skempton Bldg. Imperial College London SW7 2AZ, United Kingdom, e-mail: m.g.h.bell@imperial.ac.uk

It is useful for planning purposes. In the future, it can be implemented in a journey planner. Then, one can imagine a journey planner to have a slide bar for risk-averseness. In general, risk-minimizing behaviour is relevant for transport of special goods or persons, such as hazardous materials or VIPs. Also for just-in-time deliveries, the consequences of arriving late are high. The risk-averseness can depend on the purpose of the trip. When trying to catch an airplane, one is likely to be more risk-averse than when making a family trip.

The paper is set-up as follows. First, there is a review of the literature about network robustness and risk-averse traffic assignment. Section III describes how a dynamic traffic simulator can be fitted into a framework of risk-averse traffic assignment. The model is applied to a case study which is presented in section IV. Section V shows the results of the case study and the last section gives the general conclusions of the modelling framework.

II. LITERATURE REVIEW

The issue of reliability has become a subject of research over the last decade. Users value reliability highly [4]. It can be posed that one minute of standard deviation in travel time is be equally valued as two minutes of travel time [1]. Also, experiences of extreme travel times influence the route choice[5]. These extreme travel times can for instance be caused by the blocking of a link.

Reliability and vulnerability are closely related. We use vulnerability in the following way. Parts of a network are called vulnerable if the consequences of a blocking are severe for the travel time for that link and for other links. Given that, a network with many vulnerable links is likely to give unreliable travel times.

Extreme travel times can be caused not only by accidents on the link itself, but also by the blocking of a link by spillback from another link. One can assess the impacts of blocking links in a real-world network using intensive computation [6]. That paper uses two types of routes. First, there are routes independent of the blocking based on a network without a risk of a blocking. Then, there are routes with en-route assignment: dependent on the location of the blocking, people will take another route. Jenelius et al. present measures for the importance of links for a network performance [7]. He defines an importance and exposure for a link, based on the flows and the delays if the link is blocked. This also takes intensive computation. More than the work by Knoop et al. [6], their measures focus on the connectivity of the road network. This method can be used to improve network planning.

Liu et al. [8] looked at the route choice process as determined by a stochastic perception of the travel time and its variability by users. Uncertainty of travel time is in their model a part of the route disutility. They assume that the travel time and travel time uncertainty are terms in a utility function and solve the stochastic network (SN) combined with stochastic perception dynamic user optimum (SDUO). The disutility in their model is depends on the travel time, observation error, uncertainty of the travel time and the risk attitude of the traveller. They took a normally distributed travel time function without specifying the mechanism that causes the travel time uncertainty.

Bell was the first to take a game-theoretical approach towards link-vulnerability[3]. He assumes the road users do not know the chances of blocking a link. They will, however, count on the worst case scenario. The users change their route for this scenario and then the worst case scenario changes. Bell allows for a mixed strategy for the worst case, i.e. there is a distribution of blocking probabilities over different links, adding up to 1. The opposite would be to require a pure strategy: the blocking probability is either 1 or 0. This pure strategy is for instance applied for a network of oil supply and an electrical transmission system [9].

In the concept by Bell there are just two costs for a link possible: when it is unblocked the costs are low and when it is blocked the costs are high [3]. Bell and Cassir extend the concept [10]. In their paper, a blocked link has a lower capacity than an unblocked link. The traffic demand then determines the travel costs, using a link-based relationship between flow and travel time.

Nagae and Akamatsu continue on this line of research [11]. They point out that it might be too extreme to expect the worst case situation to happen. They relax the assumption of people being completely risk-averse. They add an extra (“entropy”) term to spread the breakdown chances over the different scenarios. Such an entropy term is added to the choice of the scenarios and the route choice. This changes the perspective on route choice behaviour slightly, but it also makes the mathematical framework much easier to solve (see also section III.A). Bell et al. use the same, but, compared to the strictly risk-averse simulation, just relaxes the perception of link failure probabilities (and not the route choice) [12]. The mathematical advantage then still holds.

All papers that handle risk-averseness in a game-theoretical way so far assume that all people have the same route choice. This paper deals with users having an individual route choice. As opposed to Liu et al. [8], we continue the game-theoretical approach and suppose that risk-averse users will expect the worst traffic conditions and thus base the probabilities on the possible consequences of a blocking.

In this paper, the methodology of routing is that routes are optimal, but not in the sense of system optimal. The model introduced here does not aim at controlling traffic and reaching a system optimum as Hoogendoorn et al. [13] do by using VMS to control routes. This paper develops a method to provide users with a service for an individually optimized route advice.

Note that if one individual changes its route according to the route advice, the link loads will only change marginally. Link costs will not change and therefore routing of the others will not change.

III. METHODOLOGY

This section points out how users are routed when one accounts for risks. This can be done at two levels: first, the total demand can be assigned using a suitable composition of the user classes. When this is finished, an individual driver can get personalized route advice, based on his attitude towards risk, using vulnerable links. The model is described in the first paragraph. Section B indicates how the system is solved and then an implementation of the model is shown.

A. Mathematical formulation

Bell was the first to introduce a risk-averse route formulation [3]. We extend their formulation with an extra parameter. Table 1 lists the symbols used in the formulation of the game.

Table 1 The symbols used

C	User class
k	Path
q_{Cj}	Perceived failure probability of link j for user class C
h_{kC}	Probabilities to choose path k for user class C
TC	Total travel cost (vector for each scenario j)
i	Link number
j	Scenario number
B	Set of scenarios with a blocking
a_{ik}	Link incidence, 1 if link i is on path k , 0 otherwise
c_{ij}	Cost of travelling on link i under scenario j
g_{jk}	Travelling costs of path k under scenario j
θ	Constant indicating the risk-averseness of a user class
D	Operator for the distance between 2 vectors
th	Threshold value for converging algorithm
p	Probability assigned to the blocking scenarios for the risk-neutral users ($0 < p < 1$)
n	Iteration number

The expected network performance for user class C is

$$TC_C(\mathbf{q}, \mathbf{h}) = \sum_j \sum_k q_{Cj} h_{Ck} g_{jk} \quad (1)$$

with $g_{jk} = \sum_i a_{ik} c_{ij}$, the cost of travelling on path k under scenario j . Users choose their routes to minimize the expected travel cost:

$$\mathbf{h}_C = \underset{\mathbf{h}}{\operatorname{argmin}} (TC_C(\mathbf{q}, \mathbf{h})) \quad (2)$$

In this formula, q_{jC} is the probability that a class C counts on scenario j to happen. A risk-averse user (subscript ra) would count on the worst scenario to happen most likely. This leads to

$$\mathbf{q}_{ra} = \underset{\mathbf{q}}{\operatorname{argmax}} (TC_{ra}(\mathbf{q}, \mathbf{h})) \quad (3)$$

Nagae and Akamatsu pose that a worst case set of is perhaps too extreme and add an entropy term to give a higher probability to the non-extreme cases[11]. In our formulation, the maximization process now changes from equation (3) to:

$$\mathbf{q}_{ra} = \underset{\mathbf{q}_{ra}}{\operatorname{argmax}} \sum_i \sum_j h_{ra,i} c_{ij} q_{ra,j} - 1/\theta \sum_j q_{ra,j} \ln q_{ra,j} \quad (4)$$

θ indicates the influence of the entropy term. A low θ means that more weight is given to the entropy term and therefore one scenario is less likely to get a very high probability. Equation (4) has a closed solution for q_j [11]

$$q_{ra,j} = e^{\theta TC_j} / \sum_j e^{\theta TC_j} \quad (5)$$

Note that $\theta = 0$ gives an equal probability to each scenario and an infinite θ gives only weight to the scenario with the highest disruption.

We generalize this formula. It is argued that not every user does always consider an incident to happen. In contrary, optimistic users will assign a probability 0 to all scenarios with a blocking. We therefore introduce a two-parameter model.

$$q_j = p e^{\theta TC_j} / \sum_j e^{\theta TC_j} \quad \forall j \in B$$

$$q_j = 1 - p \quad \forall j \notin B \quad (6)$$

This is a generalised form of equation (5).

Parameter θ indicates the distribution of the incident chance over different scenarios. The risk-averse users expect the worst case to happen: the scenarios where the disruption is the biggest (the total cost is the highest) are taken more likely. A user group with $\theta = 0$ considers each scenario with a blocking even likely. The newly introduced parameter p indicates the total weight that is given to any incident scenario. If $p = 0$, users assume there will be no disruption in the network. Setting $p = 1$ gives back the formulation by Nagae and Akamatsu [11]. Setting $p = 1$ and $\theta = \infty$ gives back the original formulation of Bell [3].

By adapting the parameters, different user classes can be introduced. These different user classes share the same network and thus interact with each other. The interaction of the different travellers comes from the travel times. Traffic load on a link will be the sum of the traffic of all classes.

For the sake of simplicity, we formulated the model for one destination. A multi-destination network is easily fit into this model. All route-related variables as well as \mathbf{q} should then be considered for each destination separately.

B. Solving the system

To solve the equations, we use an iterative method based on the method described by Bell et al. [12]. The main difference is that the load on the links, V , is now composed of the different user classes.

We implemented this iterative process as follows. Initially, the traffic is assigned in a free flow network. The iterative loop starts with computing travel times out of link loads. Then, for each scenario, the total cost is computed and

the link travel times are stored. Following equation (6), the total cost for the scenarios determines the anticipated probability that a scenario occurs, depending on parameters θ and p . After the computation of these probabilities, an expectation value for the travel time on each link can now be determined. Based on these travel times, traffic is assigned along possible paths. This gives the link loads which completes one iteration. One iteration of the game is the combined move of two “players”: the setting of the link failure probability vector \mathbf{q} by an “evil entity” and the route choice for the travellers, vector \mathbf{h} . A graphical representation of the solving algorithm can be found in Fig. 1.

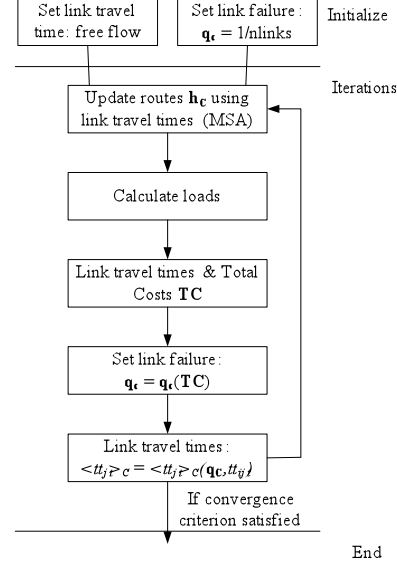


Fig. 1 The solving algorithm

We implement a Method of Successive Averages [14]. This means that the distribution of the new routes is always the weighted average of the old route distribution and a newly computed distribution. The weight of the new distribution reduces proportionally with the inverse of the iteration number. Mathematically, it can be expressed as follows:

$$\mathbf{h}_n = \left(1 - \frac{1}{n}\right) \mathbf{h}_{n-1} + \frac{1}{n} \mathbf{h}_n^{opt} \quad (7)$$

In this equation, \mathbf{h}_n^{opt} is the optimal route choice determined in the n th iteration. When n increases, the total route choice after the n th iteration, \mathbf{h}_n , depends less on the optimal routes in iteration n .

In the proposed algorithm, the fraction of the traffic that is reassigned to a route reduces and thus the route choice \mathbf{h} converges. \mathbf{q} depends only on \mathbf{h} , so a converging \mathbf{h} means \mathbf{q} will converge too. For one user class, this converges to the optimum [12]. Here, multiple user classes can use the network in the same time. There is an interaction of the route choice from one user class to the other (in the next iteration, via the assignment and \mathbf{q}). If another user class then user class C has the largest influence on \mathbf{q}_C , the solution, although convergent, is not unique.

When the convergence criterion is satisfied, the assignment stops. We define the change of a vector as the difference in Euclidian space.

$$D(\mathbf{z}_1, \mathbf{z}_2) = \|\mathbf{z}\| = \sqrt{\sum_j (z_{1j} - z_{2j})^2} \quad (8)$$

The most fluctuating behaviour is found in the risk-averse user group. For convergence we require that 2 subsequent vectors (for both q and h) do not more than a threshold value. The threshold values can be chosen different. This can be useful if the number of routes is much larger than the number of scenarios.

C. Application possibilities

The result of the methodology presented above, is route assignment procedure for different user classes. When applied on a network, the link flows can be predicted. First of all, the composition of the traffic demand then needs to be calibrated.

The calibrated assignment can thus be used as an estimation of travel times. In the view of the total network flows, the route choice of one individual is negligible. The most interesting application of the framework is a journey planner.

Bogers et al state that people take the risk into account when choosing their route [5]. The journey planner based on the ideas in this paper, gives the optimal route for a specific user. In the framework, the user optimal path for an individual user can be determined. A user can now give its own attitude towards risk, indicated by parameters θ and p .

The use of a numerical value by users to indicate their risk averseness might be unsuited in practice, but any interval scale can be used by transforming verbal expressions to numerical values. “No risk acceptable” can be transformed in $p = 1$ and $\theta = \infty$, via $p=1$ and $\theta = 0$ for “risk neutral” to $p = 0$ for “optimistic”.

The concept can also be applied also for cases with $p > 1$. It needs care then that the incident probability of one link does not exceed one. $q_j \leq 1$ is a boundary condition for j in each iteration.. Large networks, the effects of multiple incidents (a combination of scenarios) can be estimated as the combined effect of the two incidents separately. However, with smaller networks the interaction can be larger (one might suffer from both incidents) and all combinations should be simulated.

IV. CASE STUDY

This section presents an application of the method presented in section III. The case study describes an accident happening somewhere in the network. It shows the trade-off between speed and reliability in a grid network. The first section introduces the scenarios. Section B presents the network and discusses its characteristics. Then section C describes the traffic simulation model used and the way how the method presented in this paper is modelled in this simulator.

A. Scenarios

The scenarios present in our case study are related to accidents. Each scenario is a link at which the accident can happen.

The cost of a link i only consists of travel time. In this paper, we use a BPR-function to compute the times.

$$c_{ij} = TT_0 \cdot \left(1 + \left(V_i / C_{ij}\right)^4\right) \quad (9)$$

In this formula, TT_0 is the free flow travel time, defined by the length of the link divided by the free flow speed.

A complete blocking is impossible in this formulation. To indicate the effects of a capacity reduction, a severe reduction is modelled. If a scenario consists of a blocking of a link, the capacity of that link will reduce to 1% of the original capacity. Consequently, the travel time will increase much.

B. Network and OD-matrix

The network we use is based on a grid network. Fig. 2 shows the network we use; the width of the lines is the capacity of the links. The traffic flows from origin in node 1 to destination in node 9. Basic idea is to have a network with three types of routes. One can interpret the network as follows. In the centre, there is a city centre. There are just local roads (low capacity, low speed limit) through there. The roads at the bottom and right hand side are 80 km/h highways with a capacity of 1750 veh/h.

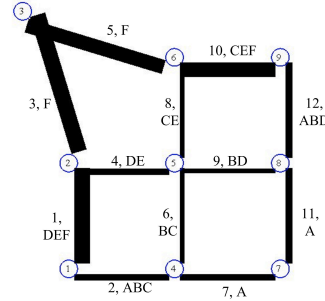


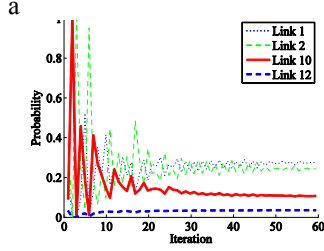
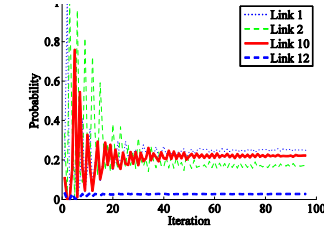
Fig. 2 The used network with link numbers and paths letters

The motorway around the city (left and top) is a bit longer, but quicker (100 km/h) and has a higher capacity. This is probably the link that is also avoided by the risk-averse people: a demon will probably attack here. Link 1 and 3 have a higher capacity (4200) than link 5 and 10 (3800 veh/h).

The total demand is set to 2000 veh/h. The users use the total link cost as input for an update of the route choice. Three user groups are introduced: a risk-averse user group, $\theta = 5 \times 10^{-8}$ h/veh) and $p = 1$, a group with neutral risk behaviour, $\theta = 0$ and $p = 1$, and an optimistic group which does not consider any risk at all, $p = 0$.

The value of θ is chosen to match the performance of the network. A too low θ would lead to an equal spread of anticipation of link failure.

The total demand is spread over the three different user classes. Classifying all travellers as risk-averse would be the same as in [3].



b

Fig. 3 Convergence of risk-averse link failure probabilities for (a) traffic composed only of risk-averse travellers and (b) traffic composed of 50% risk-averse and 50% risk-neutral travellers

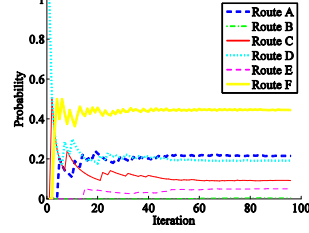
Once the risk-averseness of all travellers is known and fitted into numbers, the model can be implemented in a journey planner. For this purpose, route choices made for user classes not present in the traffic composition are also relevant. An individual user does not contribute much to congestion, so has zero weight in the traffic assignment.

C. Route choice model

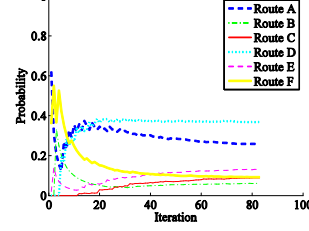
In each iteration of the game, we do a stochastic static probit assignment. The travel times used for this assignment are the travel times of the past period. In this way, congestion on routes has effect on the assignment. Within one iteration, the assignment does not result in equilibrium. But, since there is the iterative loop of the game, equilibrium will realized in the converged state. In each iteration of the game, a smaller part of the travellers is assigned to the new route. This is the same as would happen in an equilibrium assignment.

This paragraph explains the implementation of the probit route choice model. Six different paths are possible, see Fig. 2. In each iteration the time on these routes is determined. The basis for this assignment is the expected flow in the previous assignment. The travel time of the link is determined from this flow in the previous iteration and disturbed with a random error term to obtain a stochastic user equilibrium to get a realistic traffic assignment. The average expected link travel time in the previous period is determined for all links. Note that this expectation value is different for all scenarios, since the capacities of the links differ. Then, the fastest path is selected. This is repeated multiple times with different draws for the link travel time errors.

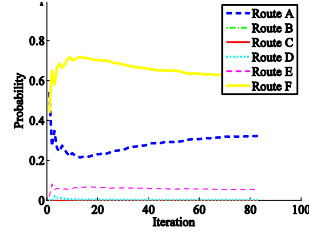
V. RESULTS



a



b



c

Fig. 4 Convergence of route choice probabilities for (a) risk-averse users in a traffic composition of just risk-averse users; (b) risk-averse users in a traffic equally composed from all 3 classes and (c) optimistic users in traffic composed equally from all 3 classes

In the network of the cast study, the fastest route is the route passing over the motorway, route G followed by the alternative route around the city, route 1. One of these two routes is assigned to almost all traffic in the optimistic user class will take. Fig. 5b shows the routes of these users: the width of a line indicates the load of the link. The urban links are hardly used. So even in the case that there is no other traffic, the optimistic users do not deviate from the two main routes. For the study in this paper, it is more interesting to focus on the risk-averse user group, which has a more varied route choice.

Fig. 3a shows how the probabilities for the scenarios for the risk-averse user classes converge. There are just a few links that are vulnerable. These are the links that are closest to the origins and destinations for the reason that there is no alternative yet. The traffic from node 1 has to

pass either link 1 or link 2 as well as link 10 or link 12. For all other links, there are more alternative routes.

Compositions with just risk-neutral or just optimistic travellers, however, differ considerably. There is no feedback loop from the risk to the route choice since there are no risk-averse travellers. This means that risk-averse users anticipate most on the failure of links which are most used by *other* user classes. This is illustrated in Fig. 3b.

The resulting routes can be found in Fig. 4. This is the result of a probit route assignment. In a traffic composition which consists of all three classes in equal proportions optimistic travellers would be advised to take route G (see Fig. 4a). In the same composition, risk-averse users consider it too risky to take that busy motorway with large possible delays. The majority would therefore take route F (Fig. 4b).

The assigned routes also depends on the other users. Consider the same demand as above, but composed differently. Now all users are risk-averse. This means that the links are used differently, and thus the traffic is assigned to other routes. As shown in Fig. 4c, a majority of the risk-averse travellers is now assigned to route G. This difference shows that it is important to calibrate the model behind the journey planner well. Not only the OD-matrix needs to be calibrated, but also the risk-averseness of the travellers needs calibration.

The total link flows are plotted in Fig. 5: For a complete risk-averse traffic composition (plotted in Fig. 5a), the traffic is almost evenly spread over the links. This holds also for the urban links which would yield a longer travel time under free flow conditions. The risk of taking the motorway and facing a very long travel time makes the risk-averse users decide to spread more evenly over the network. Fig. 5b indicates that if all users are optimistic and do not anticipate any incident, the urban part of the network is hardly used.

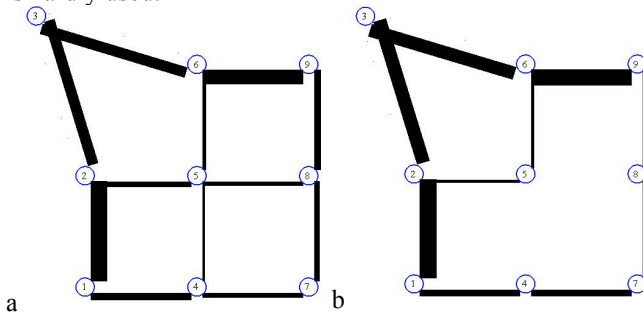


Fig. 5 The final intensities (width of the link) in different traffic compositions: a) just risk-averse travellers and b) optimistic travellers

VI. CONCLUSIONS & FUTURE WORK

This paper introduces a traffic assignment model which can cope with user classes with different attitude towards risk. The model computes the consequences of pre-defined scenarios. In this paper, each scenario is a blocking at one of the links. Risk-averse users avoid routes

with a possibility of high travel costs. The possible delays depend on the assignment, and the assignment on the possible delays. This is solved iteratively.

In a case study it is shown that the route choice for different groups in the same network is different. It is also shown that route choice for the same user class can differ depending on composition of the rest of the traffic (with the same total demand).

The concept described in this paper can be used for planning purposes. Once there is a well calibrated model (both the OD-matrix and the risk-averseness of the travellers), it can also be used in a journey planner. Travellers can then get a personalised route advice, based on their individual attitude towards risk.

This paper describes the concept of a two-parameter risk-averseness function. It is applied on a static network assignment model. In the future, this will be changed into a time-dependent, dynamic formulation of the traffic state. Also influences of jams from one link to another can then taken into account.

REFERENCES

- [1] J. Bates, J. Polak, P. Jones, and A. Cook, "The valuation of reliability for personal travel," *Transportation Research Part E: Logistics and Transportation Review*, vol. 37, pp. 191-229, 2001.
- [2] "Nota Mobiliteit," Ministerie van Verkeer en Waterstaat & VROM 2005.
- [3] M. G. H. Bell, "A game theory approach to measure the performance reliability of transport networks," *Transportation Research Part B*, vol. 34, pp. 533-545, 2000.
- [4] H. X. Liu, W. Recker, and A. Chen, "Uncovering the contribution of travel time reliability to dynamic route choice using real-time loop data," *Transportation Research Part A: Policy and Practice* vol. 38, pp. 435-453, 2004.
- [5] E. A. I. Bogers and H. J. Van Zuylen, "The importance of reliability in route choices in freight transport for various actors on various levels," in *the European Transport Conference*, Strasbourg, 2004.
- [6] V. L. Knoop, S. P. Hoogendoorn, and H. J. van Zuylen, "Approach to Critical Link Analysis of Robustness for Dynamical Road Networks," in *Traffic & Granular Flow*, Berlin, 2005, pp. 393-402.
- [7] E. Jenelius, T. Petersen, and L.-G. Mattsson, "Importance and exposure in road network vulnerability analysis," *Transportation Research Part A: Policy and Practice*, vol. 40, pp. 537-560, 2006.
- [8] H. X. Liu, X. Ban, B. Ran, and P. Mirchandani, "An Analytical Dynamic Traffic Assignment Model with Probabilistic Travel Times and Perceptions," in *the 81st Annual Meeting of the Transportation Research Board*, Washington D.C., 2002.
- [9] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending Critical Infrastructure," *Interfaces*, vol. 36, pp. 530 - 544, 2006.
- [10] M. G. H. Bell and C. Cassir, "Risk-adverse user equilibrium traffic assignment: an application of game theory," *Transportation Research Part B*, vol. 36, pp. 671-681, 2002.
- [11] T. Nagae and T. Akamatsu, "An Efficient Algorithm for a Maxmin Routing Model for Hazardous Materials," in *the Third International Symposium on Transport Network Reliability*, The Hague, the Netherlands, 2007.
- [12] M. G. H. Bell, U. Kanturska, J.-D. Smöcker, and A. Fonzone, "Attacker-Defender Models and Road Network Vulnerability," *Royal Society of London Philosophical Transactions*, 2008.
- [13] S. P. Hoogendoorn, V. L. Knoop, and H. J. van Zuylen, "Model-based Stochastic Control of Traffic Networks," in *the Third International Symposium on Transportation Network Reliability*, Den Haag, the Netherlands, 2007.

- [14] Y. Sheffi, *Urban transportation networks: Equilibrium analysis with mathematical programming methods*. Englewood Cliffs, New Jersey: Prentice-Hall, 1985.