



Concepts of network vulnerability and applications to the identification of critical elements of transport infrastructure

**M A P Taylor, Transport Systems Centre, University of South Australia,
Adelaide and G M D'Este, Parsons Brinckerhoff Pty Ltd, Brisbane**

1. INTRODUCTION

In recent years there has been considerable international research on the concept of network reliability – the ability of degraded transport networks to cope with travel demand. Network degradation may result from infrastructure failure or closure, for example because of natural phenomena, from traffic congestion and other operational factors, and from acts of human error or malevolence. Consideration of the performance of degraded transport systems and networks is assuming new importance, with serious questions being raised about the identification of critical parts of transport infrastructure. Much of the previous research on network reliability has focused on congested urban road networks and the probability that the network will deliver a required standard of performance. Whilst these are important questions, there is also a need to consider regional and national networks. At the national level and outside the major urban centres, accessibility, regional coverage and inter-urban connectivity are the primary considerations. In these sparse networks, ‘vulnerability’ of the network may be more important than ‘reliability’ because of potentially severe consequences to transport services if specific links in the network are cut.

This paper reviews previous research in the field of network reliability, and discusses extensions and adaptations to the reliability concepts that are more appropriate for strategic-level multi-modal transport systems. This leads to the concept and definition of network vulnerability. The paper then discusses the development of techniques to identify specific ‘weak spots’ – critical infrastructure – in a network, where failure of some part of the transport infrastructure would have the most serious effects on access to specific locations and overall system performance. The Australian National Highway System (NHS) network is used as a case study, but the concepts and techniques described in this paper have much wider application.

Transport networks provide access to work, education, business, shopping, socialising and recreation in urban areas; they underpin the national, regional and urban economy; and in rural and remote areas they are vital lifelines connecting isolated communities to essential services. Unfortunately transport networks are not 100 per cent reliable, and as society’s reliance on transport links and its expectations of infrastructure performance grow so do the consequences of network failure. There are many possible sources of degraded network performance, including natural events (such as floods, fires, earthquakes and blizzards); incidents (such as traffic crashes, special events, construction works and civil emergencies); malevolence (which includes industrial disputes, sabotage, acts of war and terrorism); day-to-day congestion; and interruptions to passenger and freight transport services due to breakdowns, commercial failure or other reasons. These disruptions cause delays and detours with potentially severe social, economic and environmental consequences. There are several possible responses to this reduced performance or perceived risk. In some cases, an appropriate response may be to upgrade key transport infrastructure, for instance by raising it above expected maximum flood

levels or by adding more capacity. But sometimes this simply makes the network more reliant on those key links and more vulnerable to their failure. An alternative approach is to add links to the network. These links may normally be redundant but provide alternative routes when key network links are broken. At the urban network level there may already be many such latent alternative routes, but at the regional or national strategic network level this is less likely to be the case. Extra links would make the transport network more robust, but this may add unnecessary cost to the provision of transport infrastructure. The question is where are these locations of potential network vulnerability and what is the best and most cost-effective response. These concerns have led to international research interest in *network vulnerability* (D'Este and Taylor 2001, 2003, Berdica, 2002).

2. RELIABILITY AND VULNERABILITY

Network reliability has been the subject of considerable international research interest (e.g. see Bell and Cassir, 2000 and Bell and Iida, 2003). Much of this research has focused on congested urban road networks and the probability that the network will deliver a required standard of performance. The urban studies are important, but they are not the only areas of concern. At the regional and national strategic level, accessibility, regional coverage and inter-urban connectivity are the primary considerations, because of the potentially severe adverse consequences of network degradation. As noted by BTRE (2002) in its analysis of the effects of flooding on road access, 'the vast distances involved means that access to alternative services (such as hospitals and business) often do not exist ... disruption costs to households, businesses and communities can therefore be more important in rural and remote communities'. In both urban and rural areas, the concept of vulnerability or 'incident audit' – the proactive determination of locations in a transport network which may be most sensitive to failure and where network failure may have the gravest consequences – requires detailed study. The transport planner may seek opportunities to reduce vulnerability, while the community will increasingly expect such action.

Whilst network reliability became a prominent research topic in transport planning during the 1990s, certain elements had been subject to research interest for some time before that (e.g. Lee, 1946, Richardson and Taylor, 1978). The Kobe earthquake of 1995 and its aftermath stimulated an interest in *connective reliability*. This is the probability that a pair of nodes in a network remains connected – i.e. there continues to exist a connected path between them – when one or more links in the network have been cut. Bell and Iida (1997, pp.179-185) and Iida (1999) described an analytical procedure for assessing connective reliability. Subsequent research was directed at degraded networks, usually urban road networks subject to traffic congestion, in which the network remained physically intact but the performance of one or more links could be so severely affected by congestion that their use by traffic is curtailed. This led to the definition of two additional forms of reliability: travel time reliability and capacity reliability, as described below.

Travel time reliability considers the probability that a trip between an origin-destination pair can be completed successfully within a specified time interval (Bell and Iida, 1997, pp.191-192). This can be affected by fluctuating link flows and imperfect knowledge of drivers when making route choice decisions (Lam and Xu, 2000). One measure of link travel time variability is the coefficient of variation of the distribution of individual travel times (Asakura and Kashiwadani, 1991). Measures of travel time variability are useful in assessing network performance in terms of service

quality provided to travellers on a day-to-day basis (Yang *et al*, 2000). Thus travel time variability can be seen as a measure of demand satisfaction under congested conditions (Asakura, 1999).

A supply-side measure of network performance in congested networks is *capacity reliability*, introduced by Chen *et al* (1999) and applied by Yang *et al* (2000). Capacity reliability is defined as the probability that a network can successfully accommodate a given level of travel demand. The network may be in its normal state or in a degraded state (say due to incidents or road works). Chen *et al* (1999) defined this probability as equal to the probability that the reserve capacity of the network is greater than or equal to the required demand for a given capacity loss due to degradation. Yang *et al* (2000) indicated that capacity reliability and travel time reliability together could provide a valuable network design tool. Taylor (1999ab) demonstrated how the concepts of travel time reliability and capacity reliability could be used in evaluating traffic management plans in an urban area.

Current reliability research is attempting to properly specify travellers' responses to uncertainty (e.g. Bonsall, 2000, Van Zuylen and Kikuchi, 2003) so that reliability research can be used to properly inform developments of new driver information systems and to influence the design of traffic control systems.

The current international situation and new concerns about national security, including preservation of the integrity and operation of critical infrastructure, lead to a heightened interest in the vulnerability of transport systems and networks.

Berdica (2003) proposed that vulnerability analysis should be regarded as an overall framework through which different transport studies could be conducted to determine how well a transport system would perform when exposed to different kinds and intensities of disturbances. From her study of the road network in central Stockholm she suggested three main questions that might be posed in these studies:

1. how do interruptions of different critical links affect system performance, and to what extent?
2. how is network performance affected by general capacity reductions and possible changes to traffic management and road space allocation in a subregion of the network?
3. how is the system affected by variations in travel demand?

These questions provide a starting point from which to build a methodology for studies of vulnerability of transport networks and infrastructure. They highlight the key issue of the identification of critical components of the networks. This study will address these questions and the perhaps more important questions that flow from them – when we know where the vulnerable elements (the 'weakest links') of a transport network are, what is the best response, and what can we do about it?

3. METHODOLOGY FOR VULNERABILITY ANALYSIS

Standard approaches to transport network reliability focus on network connectivity and travel time and capacity reliability. Whilst this provides valuable insights into certain aspects of network performance, reliability arguments based on probabilities and absolute connectivity may obscure potential network problems. For example, D'Este and Taylor (2001) used the example of the Australian land transport system to illustrate the potential consequences of the severance of certain transport connections in this multimodal network. In this example the system reliability was

considered, in terms of a cut to the Eyre Highway and transcontinental rail line between Perth and Adelaide – for instance by flood. The overall national land transport network remains connected and the probability that the route in question is cut by flood or other natural cause is extremely small (but not zero since it has happened), so the travel time and capacity reliability is high. Therefore the established standard measures of network reliability may not indicate any major problem with the network. However the consequences of network failure are substantial – in this case the next best feasible path through the network involved a detour of some 6000 km! In reality the alternative route via Broome would not be used – it is more likely that shipments would be delayed or cancelled thereby producing a different but no less significant economic impact. Nicholson and Dalziell (2003) pointed to similar circumstances in their study of the regional highway network in the centre of the North Island of New Zealand, a region subject to both snowstorms and volcanic eruptions.

These examples illustrate the concept of network vulnerability and the difference between network reliability and vulnerability. The concept of vulnerability is more strongly related to the consequences of link failure, irrespective of the probability of failure. In some cases, link failure may be statistically unlikely but the resulting adverse social and economic impacts on the community may be sufficiently large to indicate a major problem warranting remedial action – akin to taking out an insurance policy for an extremely unlikely yet potentially catastrophic event. For example, consider the impact on a rural community of loss of access to markets for its produce and to vital human services (such as a hospital). Low probability of occurrence and network performance elsewhere does not offset the consequences of a network failure. Thus network reliability and vulnerability are related concepts but while reliability focuses on connectivity and probability, vulnerability is more closely aligned with network weakness and consequences of failure.

Transport networks are potentially vulnerable to a wide range of potential sources of degraded network performance. Sources include fluctuations in traffic conditions ('recurrent congestion') and fluctuations in capacity due to abnormal events (referred to as incidents, or in the case of road traffic, as 'non-recurrent congestion'). Previous research (e.g. Nicholson and Du, 1997) has identified a wide range of potential threats to transport infrastructure from the occurrence of natural disasters, adverse weather, technical error, human error, acts of war, and acts of terrorism. Berdica (2003) suggests that these threats may also be viewed in terms of a level of malevolence, as shown in Figure 1. A level of malevolence may readily be ascribed to human behaviour, but the concept has also been applied in more general terms in network reliability studies. Bell (2000) used game theory involving two players, one a traveller attempting to use the network and the other an 'evil entity' who attempts to disrupt the progress of the traveller.

Whilst there is now a strong international recognition of the need for vulnerability analysis of transport systems, there has been very little research explicitly directed at vulnerability studies. For a start, there is still no internationally accepted definition of 'vulnerability' or theoretical basis on which to build. D'Este and Taylor (2001, 2003) suggested that the best starting point is the existing body of research into network reliability and risk assessment, and have offered working definitions of vulnerability (in terms of either network connectivity or accessibility to services and facilities) to help stimulate research effort. But many important research questions remain unanswered – especially in relation to diagnosing transport system weaknesses, targeting detailed risk assessments, and formulating the best response (such as reducing the potential for network degradation from a given incident, reducing its likelihood, or reducing the consequences should the incident occur). The study of

transport network vulnerability is a comparatively new field, with substantial scope for innovation and substantial scope for delivering major benefits to Australia, New Zealand and internationally.

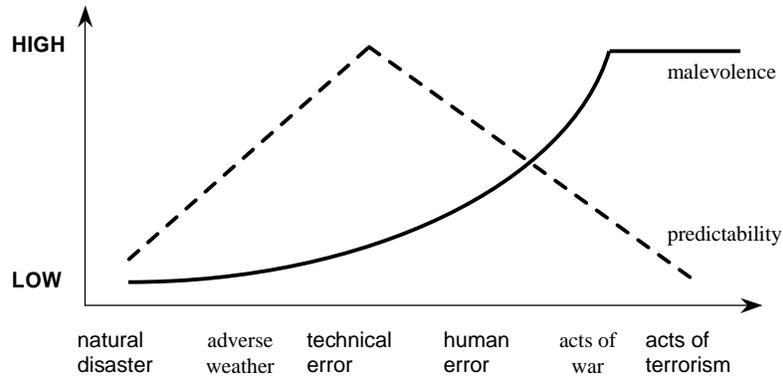


Figure 1: A possible range of threats to infrastructure (source: Berdica, 2003)

We note that considerable research effort has already occurred in relation to reliability and vulnerability of communications networks (most notably the internet). While these studies provide valuable insights into the inherent reliability and attack tolerance of different types of network topologies (Albert, Jeong and Barabasi, 2000) and into techniques for constructing robust networks, they are not directly transferable to transport networks because of the added complication of the comparatively 'snail pace' travel speeds on transport networks. For a communications network, connectivity is critical – but any alternative route is acceptable, even if it involves a 6000 km detour!

Vulnerability, reliability and risk are closely linked concepts. In broad terms, risk is something associated with negative outcomes for life, health, or economic or environmental condition. Risk can be defined in many different ways, but most definitions focus on two factors: the probability that an event with negative impacts will occur, and the extent and severity of the resultant consequences of that event. This is shown schematically as a 'risk matrix' in Figure 2.

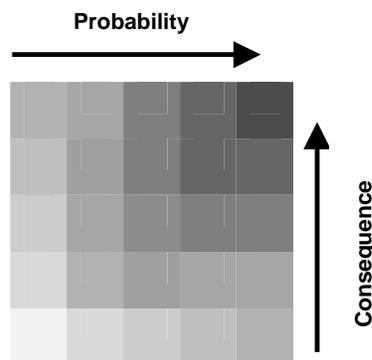


Figure 2: Conceptual risk matrix

Risk and reliability analysis is mostly concerned with the top-right sector of the matrix where increasing probability and increasing consequences combine. Nicholson and

Dalziell (2003) applied this framework to the risk assessment of transport networks in New Zealand. They measured risk as the sum of the products of the event probabilities and the economic costs of the event (e.g. the expected annual economic cost of a given event). Their risk evaluation process involved the following steps:

- establish the context (i.e. the technical, financial, legal, social and other criteria for assessing the acceptability of risk)
- identify the hazards (i.e. the potential causes of closure)
- analyse the risks (i.e. identify the probabilities, consequences and expectations)
- assess the risks (i.e. decide which risks are acceptable and which are unacceptable).

If any risk is found unacceptable, it needs to be managed. This generally involves either (1) treating the unacceptable risks, using the most cost-effective treatment options, or (2) monitoring and reviewing the risks (i.e. evaluating and revising treatments).

The study of vulnerability extends this risk assessment framework in several important ways. Firstly it extends the region of interest to areas of high consequences and low or unquantifiable (but non-zero) probability of occurrence – on the basis that measurement of occurrence probability and consequences (human and economic) is imprecise for many types of incidents, and society may consider some consequences to be unacceptable and worthy of safeguarding against, despite uncertainty about their probability of occurrence. Secondly, vulnerability analysis provides a framework for targeting risk assessment. One of the key conclusions (Nicholson, private communication) of the Nicholson and Dalziell (2003) risk assessment of the New Zealand highway network was that it is impractical and financially infeasible to conduct detailed geophysical and other risk assessment across an entire transport network. The costs of deriving accurate location-specific risk probabilities across a range of risk factors are too high to make it viable – what is needed is a way of targeting risk assessment resources to get best value from them. Vulnerability analysis provides an alternative approach to this problem. It can be used to find structural weaknesses in the network topology that render the network vulnerable to consequences of failure or degradation. Resources can then be targeted at assessing these 'weak links' where there is potential for significant adverse implications for the community if the link is broken. Thirdly, vulnerability auditing admits a more proactive and targeted approach to the issue of transport network risk assessment and mitigation.

Our current working definition of vulnerability is to consider the connection between a particular origin and destination; or to access from a particular location to other parts of the network; or to the network as a whole. The following definition provides a starting point for applying the concept to network analysis and diagnosis: *a network node is vulnerable if loss (or substantial degradation) of a small number of links significantly diminishes the accessibility of the node, as measured by a standard index of accessibility*. Therefore vulnerability can be defined in terms of the overall quality of access from a given node to other parts of the network. In earlier work (D'Este and Taylor, 2001) a second definition, in terms of network connectivity and generalised cost of travel, was also proposed. The above definition encompasses the earlier one, as generalised cost may be used as a measure of the difficulty of access.

As noted above, the purpose of analysing network vulnerability is firstly, to anticipate points of weakness where the transport network is vulnerable and network failures will have substantial adverse effects; and secondly, to suggest cost-effective remedial measures such as 'protecting' vulnerable links or adding links to the network to make it more robust. It is tempting to believe that a transport network is

most vulnerable simply where link flows are greatest but: (1) alternative routes may be available providing a new equilibrium pattern of flows at little reduction in overall network performance, and (2) considering aggregate flows may obscure significant vulnerabilities in connections between particular origins and destinations. Therefore the key to diagnosing network vulnerability is the development of analytical tools for identifying network weaknesses because network vulnerabilities may exist that are not obvious from a scan of network activity patterns under normal operating conditions. The scale of demand for travel on these vulnerable links can then be taken into account in determining what level of resources can be justified for remedial actions.

Our definition of network vulnerability emphasises the consequences of degradation of the network. In other words, if the 'best' path through the network is no longer available, how much worse is the second-best option, or the third best, and so on. This suggests an approach based on n th best paths through the network or on constrained shortest path algorithms, but in general, algorithms for these problems are inefficient and are not included in standard transport network modelling software packages. For a review of algorithms for n th-best and constrained path problems, see D'Este (1997).

An alternative starting point is probabilistic route choice algorithms, such as those based on the logit model. According to this model, a traveller will choose a particular path from the set of available paths from the required origin to destination on the basis of the utility of that path compared to the alternatives. The measure of utility is travel time or other appropriate generalised cost. The probability of using a particular path will then depend on its relative utility. This argument can be extended to individual links. The probability of using a particular link is a measure of the utility of paths through that link compared to paths through alternative links. Note that for a network without loops, the probabilities for links that comprise a network cut will sum to unity. Therefore if the probability of using a particular link is low then there exist other links with similar or 'better' paths. However if the probability is high then paths through alternative links are inferior. The higher the probability of using a particular link, the greater is the difference between its utility and the utility of paths through alternative links. If that link is cut then the network performance will degrade significantly. In other words, the link probabilities provide a measure of the relative performance of alternative paths and hence of the consequences of network failure. Hence logit-based assignment algorithms, as discussed in D'Este and Taylor (2003), can form the basis of a method for identifying vulnerable links in a transport network, as follows.

Assume that the probability of use of path $R(i, j)$ connecting origin i to destination j is directly proportional to the likelihood of use of all links e in the path. The directional link e connects node r to node s , i.e. $e = (r, s)$. Then:

$$\Pr\{R(i, j)\} = K \prod_{e \in R(i, j)} g(e) = KG(R(i, j)) \quad (1)$$

where K is a constant, $g(e)$ is the *link likelihood function*, $G(R)$ is the *path likelihood function* and $0 \leq g(e) \leq 1$. A suitable functional form for $g(e)$ is

$$\begin{aligned} g(e) &= \exp(-az(e)) && \text{if } e \text{ is on an acceptable path} \\ g(e) &= 0 && \text{otherwise} \end{aligned}$$

where $a \geq 0$ is the path dispersion factor for the network, reflecting the level of usage of paths longer than the minimum cost path. A value of zero for a means that all alternative paths are equiprobable. A value of a of infinity means that only the minimum cost path will be used. The function $z(e) \geq 0$ is the difference between the travel cost incurred in using link e to travel from r to s and the minimum cost path between r and s . If $z(e) = 0$ then link e is on a minimum path. Taylor (1979) defined an acceptable path to be one on which each succeeding node is closer to the destination than its predecessor. If $V(r, j)$ is the minimum path potential of node r with respect to destination j , i.e. the minimum travel cost from r to j , then the link e will be on an acceptable path if $V(r, j) > V(s, j)$. The cost difference $z(e)$ is given by $z(e) = V(s, j) + c(e) - V(r, j)$ where $c(e)$ is the travel cost on link e . If e is on a minimum path from i to j then $z(e) = 0$ as $V(r, j) = V(s, j) + c(e)$ by definition.

Equation (1) provides a conceptual definition of the probability of use of a path $R(i, j)$ between i and j . The probability that link e will be used for travel between i and j is given by summing the path probabilities of all paths from i to j that use e , i.e.

$$\Pr\{e, (i, j)\} = \sum_{R(i, j): e \in R(i, j)} \Pr\{R(i, j)\}.$$

This result is conceptually simple but difficult to use in practice, because it requires definition of all of the acceptable paths between i and j . However, the conditional probability of a trip from i to j using e given that it passes through node r ($\Pr\{e, (i, j) | r\}$) may be found using an efficient recursive algorithm without the need for explicit determination of all acceptable paths. This conditional probability may be computed recursively using the link weight function $w(e)$ (Taylor, 1979):

$$\begin{aligned} w(e) &= g(e) && \text{if } s = j, \text{ the destination node} \\ w(e) &= g(e) \sum_{l \in b(s)} w(l) && \text{for all other } s \end{aligned}$$

where the summation $\sum_{l \in b(s)} w(l)$ is the sum of the weight functions of all links l in the

set $b(s)$, i.e. those links that can be used to leave node s . It can then be shown (Taylor, 1979) that $\Pr\{e, (i, j) | r\} = \frac{w(e)}{\sum_{l \in b(r)} w(l)}$, given that $w(e)$ may be computed

recursively by considering each node s in forward topological order (i.e. increasing value of path potential $V(s, j)$) from the destination j .

Link probabilities may be used in network scans for the identification of critical network components (links, nodes, routes or subnetworks). The probability that a trip from i to j uses the link e is $\Pr\{e, (i, j)\}$, which may be determined as above. This probability can be used to indicate where to look for the key links where the connection is most vulnerable. In general, the higher the link probability, the greater the adverse impact if that link is broken. This suggests that candidates for the source of network vulnerability can be identified by setting a probability threshold λ (with $\lambda \geq 0.5$) then looking for links with probability higher than this threshold. Recommendations for efficient values of the threshold λ and the choice parameter α are topics for further research, as discussed in D'Este and Taylor (2003).

Having assessed the vulnerability of connections between a particular origin and destination (relative accessibility), the vulnerability of overall access of a particular node (integral accessibility) can then be evaluated by repeating the process for all destinations reachable from that node. Thus calculating link probabilities using a logit-based multi-path assignment algorithm provides a heuristic technique for identifying link and node vulnerabilities. Collections of vulnerable links and nodes may then be considered in the identification of vulnerable routes or sub-networks. D'Este and Taylor (2003) reported the application of this method to a study of the UK intercity railway network.

Vulnerability analysis should be regarded as an overall framework within which different transport analyses can be performed to indicate how well a given transport system will function when exposed to different kinds of disturbances and associated levels of risk. Figure 3 shows our proposed general schematic for vulnerability analysis, derived from the specific method for road safety vulnerability studies suggested by Berdica, Bergh and Carlsson (2003). The proposed general schematic works as follows. Given a set of standards ('goals and objectives') for system operation, a set of definitions for the existence of vulnerability problems can be assembled. Travel demand and transport systems performance data, coupled with other data sources such as environmental or meteorological data or land use and activity data, may then be analysed using suitable vulnerability assessment tools to compare a specific incident situation with normal operation. Reduced system performance leading to reduced levels of serviceability below a pre-defined threshold indicate the existence of a vulnerability condition. Suitable plans and actions may then be devised to reduce the level of vulnerability. This schematic process model is providing the basis for further research.

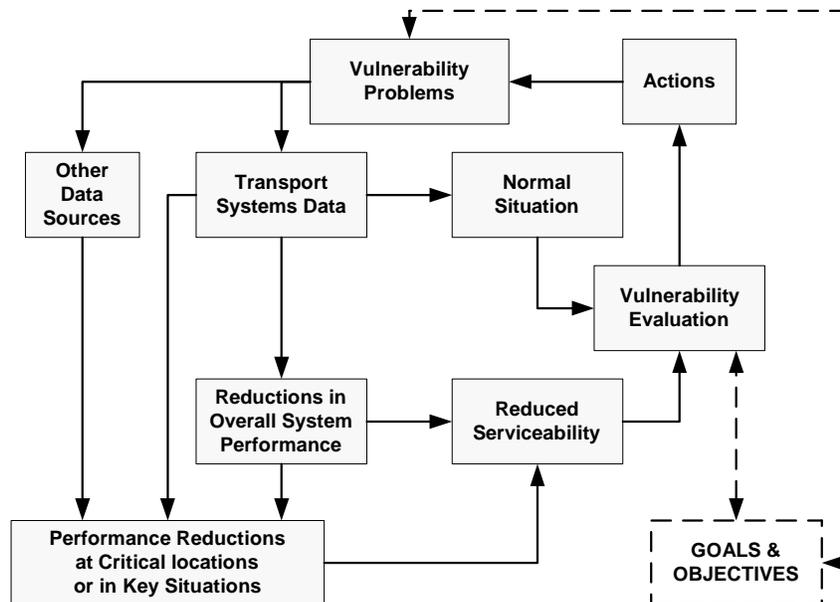


Figure 3: Schematic for general vulnerability studies in transport networks (derived from the road safety vulnerability model proposed by Berdica, Bergh and Carlsson, 2003)

4. SAMPLE APPLICATION

To illustrate the proposed method, consider the following application to the Australian National Highway Systems (NHS) network, as shown in Figure 4. This network provides a basic, sparse skeleton of the nation's road network.

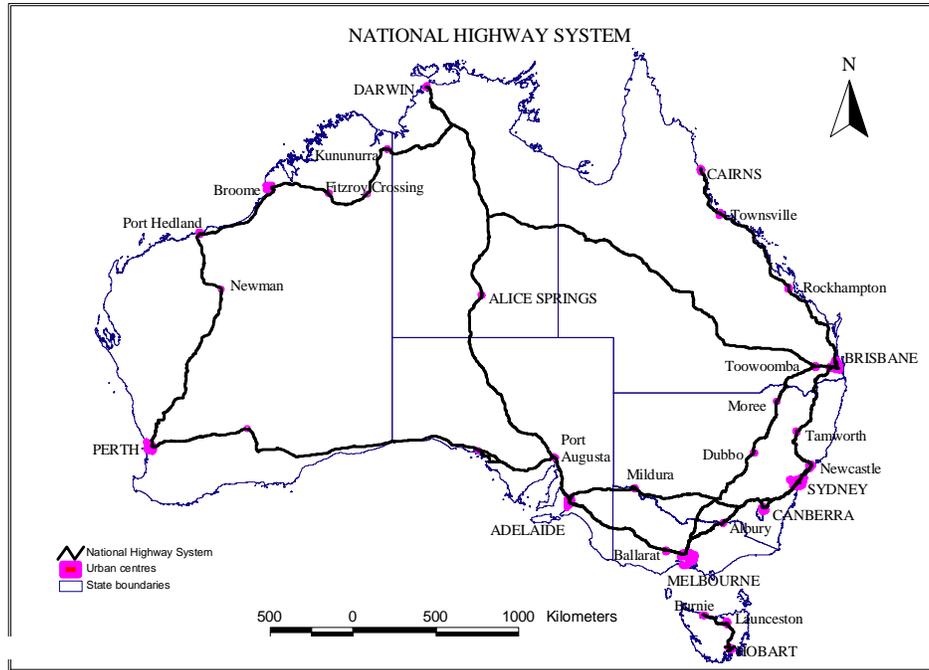


Figure 4: The Australian National Highway System (NHS)

A model of the NHS network was developed for illustrative purposes to demonstrate the concepts of network vulnerability studies, and a trial analysis is presented here. This analysis considers the vulnerability of the NHS network for travel between two selected pairs of capital cities: Perth and Sydney and Darwin and Sydney. Table 1 provides a summary of a vulnerability analysis for the NHS route between Perth and Sydney.

Table 1: Vulnerability scan for NHS network, Perth-Sydney

Origin: Perth (1)	Destination: Sydney (109)	$\alpha = 0.1 \text{ (km}^{-1}\text{)}$	$\lambda = 0.5$		
Travel distance (km)	Minimum path cost (MP) = 3999	Expected path cost (EP) = 4002			
Vulnerability scan: degrade network by cutting link					
Links (node1-node2- ... -nodeN)	Link prob	Minimum path cost (MPD)	Expected path cost (EPD)	MPD/M P	EPD/EP
1-75-74- ... -55-54-76-77-78-79 Grt Eastern Hwy – Eyre Hwy – Stuart Hwy	1.000	6835	6835	1.709	1.708
79-80- ... -86-87-103 Sturt Hwy	1.000	4225	4227	1.056	1.056
103-104-105 and 107-108-109 Hume Fwy	1.000	5413	5416	1.354	1.353
105-107 Hume Fwy	1.000	4060	4063	1.015	1.015

The analysis in Table 1 was performed for travel distance taken to represent travel cost. A threshold link probability value of $\lambda = 0.5$ was set, although in this case there is a sole path (consequently with probability of once of one) determined from the reasonable path analysis, with path dispersion factor $\alpha = 0.1$ (km^{-1}). The table shows the minimum path cost (MP) and the expected path cost (EP) in the full network, and the minimum and expected path costs (MPD and EPD respectively) in the degraded network, i.e. when a specific link is cut. The table also shows the ratios MPD/MP and EPD/EP, thus indicating the proportionate increases in travel costs resulting from the loss of a given link. The links tend to fall into clusters, better seen as route segments, as indicated in the table. For the journey from Perth to Sydney there are four clusters, as seen in Table 1. One is the route segment from Perth to Adelaide. A cut at any point along this segment leads to an increase in minimum travel distance of 71 per cent ($\text{MPD}/\text{MP} = 1.709$). The next segment, from Adelaide taking the Sturt Highway to the Hume Freeway, has an MPD/MP ratio of 1.056, indicating that there is at least one reasonable alternative path available. The section of the Hume Freeway near Canberra forms a third route segment, with $\text{MDP}/\text{MP} = 1.015$. This reflects the small detour available in the NHS via Canberra at this point. The fourth segment is a composite, consisting of the section of the Hume Freeway between the Sturt and Barton Highways and the section of the freeway from the Federal Highway into Sydney. This composite segment has $\text{MDP}/\text{MP} = 1.354$, implying an increase in travel distance *via the NHS network* of 35 per cent should any link in the segment be cut.

Figure 5 provides a picture of the network model, displaying travel paths between Darwin and Sydney and the probabilities of use of those paths. Table 2 summarises the analysis for this path using travel time as the measure of travel cost.

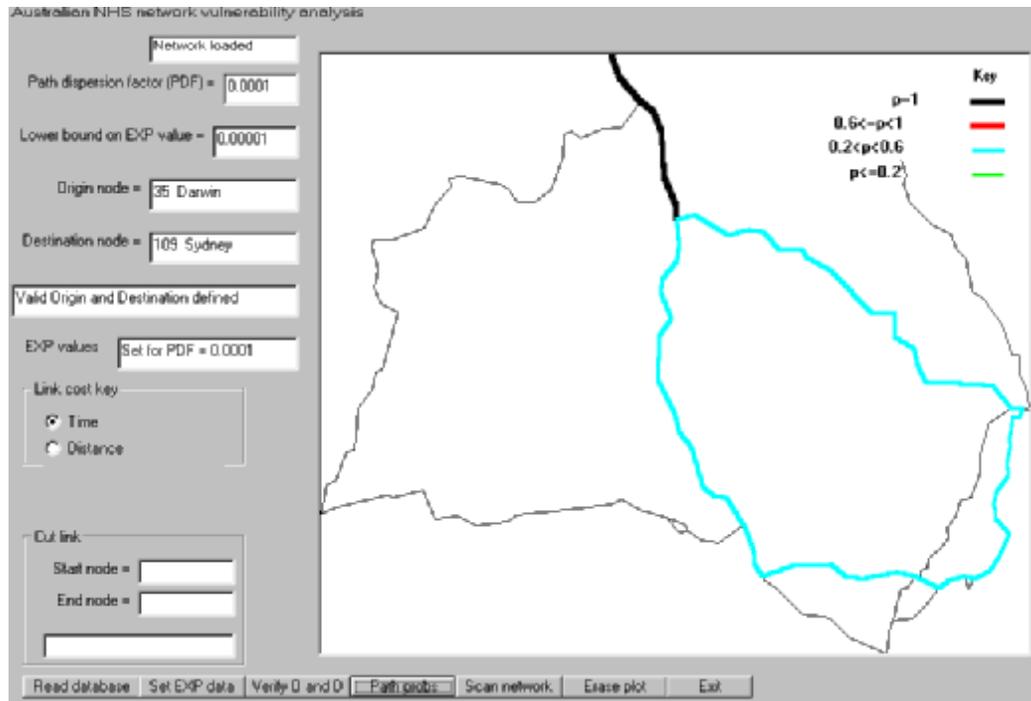


Figure 5: Alternative paths between Darwin and Sydney in the Australian NHS network, for vulnerability analysis based on travel distance and path dispersion factor $\alpha = 0.0001$ (min^{-1})

Table 2: Vulnerability scan for NHS network, Darwin-Sydney

Origin: Darwin (35) Travel time (min)	Destination: Sydney (109) Minimum path cost (MP) = 2510	$\alpha = 0.0001 \text{ (min}^{-1}\text{)}$ Expected path cost (EP) = 2535.9	$\lambda = 0.5$	Vulnerability scan: degrade network by cutting link		
Links (node1-node2- ... -nodeN)	Link prob	Minimum path cost (MPD)	Expected path cost (EPD)	MPD/M P	EPD/EP	
35-34-33 Stuart Hwy	1.00	∞	∞	∞	∞	
33-34- ... -39-40 Stuart Hwy	1.00	4873	4875	1.941	1.922	
40-152-151- ... -139-138-137- ... -124-123-122- ... -110-109 Hume Fwy	0.51	2562	2562	1.021	1.010	

In this case there are a pair of reasonable paths, as shown in Figure 5. One path has a probability of use of 0.51, the other has a probability of use of 0.49, which means that they have similar costs and offer viable alternatives. Given that in general, higher probability indicates potential for greater adverse impacts if a link is broken, the path with higher probability has been analysed to demonstrate the vulnerability scan.

The results of the scan are shown in Table 2. Three route segments emerge. The first is the section of the Stuart Highway south of Darwin to the intersection with the Victoria Highway. This segment has no alternative in the NHS network (it is the only way in and out of Darwin in that network) and thus a cut to the network in this segment has an infinite MPD/MP cost ratio. The second segment is the Stuart Highway between the Victoria Highway and the Barkley Highway. A cut in this segment means a journey by the next best route some 94 per cent longer than the preferred path (MPD/MP = 1.941). The final segment takes the Barkley, Matilda and Warrego Highways to Brisbane, and the New England Highway to Sydney. There are good alternatives to this route segment, and the MPD/MP ratio for it is 1.021.

These two examples indicate a number of the features to be expected in a network vulnerability analysis. Some route segments provide unique connections and are thus vulnerable. As in the case of the Stuart Highway out of Darwin in the NHS network, they will tend to be readily identifiable. There are no alternatives to them in the defined network. Other segments have ready alternatives in the network and thus these may be seen as effectively invulnerable. Of most interest is the third type of route segment found in the scan. This segment type has alternatives, but these require substantial detours. Such links are of most interest in a vulnerability scan.

The simple NHS network used in this study is intended for illustration of the basic concepts of vulnerability analysis only. In reality, even the national road network is more complex than the NHS and thus offers more alternatives. In our present research we are considering similar analyses to these reported here but based on the more comprehensive strategic national road network. It is in the field of such studies that more fruitful vulnerability results will be found.

5. FURTHER RESEARCH

Our research to date has yielded a potential method for analysis of network vulnerability in terms of the spatial or topological configuration of the network. Further research is needed to:

- develop better and more comprehensive vulnerability metrics
- refine techniques for identifying network weaknesses
- extend and refine the use of network vulnerability indicators for use in studies of critical infrastructure and the implications of network degradation
- develop techniques for recommending and evaluating cost-effective risk management and remedial responses (such as reducing risk profile, upgrading existing infrastructure, adding alternative routes, and so on). This may involve trading off the level of resources put into managing the risk against a measure of vulnerability that takes into account the implications of network failures as well as path probabilities
- develop visualisation tools for interpreting and communicating results

Candidate vulnerability metrics belong to a composite set including:

- indices of network connectivity and accessibility
- probability distributions for travel times and costs to specified destinations
- measures of change in the utility of travel
- spatial distributions of changes in the above metrics
- indices of risk, including expected values of costs, changes in these values under different network conditions, propensity for component failure, and performance thresholds.

This set of measures is being designed to reflect both the intensity of vulnerability and its extent, both spatially and demographically, across a study region. The techniques to apply these measures to vulnerability analysis will be based on the complex system paradigm, thus focusing the research on the required methodology, process and tools. Validation of the techniques will require careful appraisal of the modelled consequences of network failure for real world systems.

Research on the general assessment of consequences and risks is also required. We envisage the development of a general method of 'vulnerability audit', perhaps akin to road safety audit, which can be used in conjunction with assessment of risk of network infrastructure degradation and failure.

Our research plan includes the development, testing, validation and refinement of analytic tools that will be applied to real world assessment of Australia's transport network. The plan includes consideration of urban, regional, state and national networks by all land transport modes, and will extend to regional, interstate (and possibly international) aviation networks. The impact on regional communities of recent airline collapses has highlighted the potential vulnerability of access by air to regional Australia.

6. CONCLUSIONS

Considerations of critical infrastructure are now a major concern in Australia and New Zealand, amongst other countries. The concern stems from a variety of causes, including the state of development and condition and level of use of existing transport infrastructure; difficulties associated with public sector provision of new infrastructure; public-private partnership arrangement for infrastructure provision; and perceptions

of risks and threats to infrastructure through malevolence such as acts of war, sabotage or terrorism. Thus there are great potential benefits from the development and application of a methodology to assess risk and vulnerability of transport systems, that allows planners and policy makers to make rational assessments of threats to facilities and infrastructure; the consequences of network degradation and failure at various locations and under different circumstances; and what to do about it. Social and economic benefits immediately flow from the ability to plan for and manage the impacts of transport network degradation to minimise wider consequences on economic, employment, trade and social activities in cities and regions.

7. REFERENCES

- Albert, R, Jeong, H and Barabási, A-L (2000) Error and attack tolerance in complex networks. *Nature* 406, pp.378.
- Asakura, Y (1999). Evaluation of network reliability using stochastic user equilibrium. *Journal of Advanced Transportation* 33 (2), pp.147-158.
- Asakura, Y and Kashiwadani, M (1991). Road network reliability caused by daily fluctuation of traffic flows. *Proc 19th PTRC Summer Annual Meeting*, University of Sussex, Brighton, July (PTRC Ltd: London), pp.73-84.
- Bell, M G H (2000). A game theory approach to measuring the performance reliability of transportation networks. *Transportation Research B* 34B (6), pp.533-545.
- Bell, M G H and Cassir, C (eds) (2000). *Reliability of Transport Networks* (Research Studies Press: Baldock).
- Bell, M G H and Iida, Y (1997). *Transportation Network Analysis*. (John Wiley and Sons: Chichester)
- Bell, M G H and Iida, Y (eds) (2003). *The Network Reliability of Transport*. (Pergamon-Elsevier: Oxford).
- Berdica, K (2002). An introduction to road vulnerability: what has been done, is done and should be done. *Transport Policy* 9, pp.117-127.
- Berdica, K (2003). Vulnerability: a model-based case study of the road network in Stockholm. *Transportation* (in press).
- Berdica, K, Bergh, T and Carlsson, A (2003). 2+1 roads with cable barriers – traffic safety and transport quality effects. *Accident Analysis and Prevention* (in press).
- BTRE (2002) *Benefits of Flood Mitigation in Australia*. Bureau of Transport and Regional Economics report 106, AGPS, Canberra.
- Bonsall, P W (2000). Travellers' response to uncertainty. In Bell, M G H and Cassir, C (eds), *Reliability of Transport Networks* (Research Studies Press: Baldock), pp.1-10.
- Chen, A, Yang, H, Lo, H K and Tang, W H (1999). A capacity related reliability for transportation networks. *Journal of Advanced Transportation* 33 (2), pp.183-200.
- D'Este, G M (1997). Implementing a hybrid route choice procedure in a network modelling context. *Journal of the Eastern Asia Society for Transportation Studies* 2 (3), pp.737-720.
- D'Este, G M and Taylor, M A P (2001). Modelling network vulnerability at the level of the national strategic transport network. *Journal of the Eastern Asia Society for Transportation Studies* 4 (2), pp.1-14.
- D'Este, G M and Taylor, M A P (2003). Network vulnerability: an approach to reliability analysis at the level of national strategic transport networks. In Bell, M G H and Iida, Y (eds). *The Network Reliability of Transport*. (Pergamon-Elsevier: Oxford), pp.23-44.
- Evans, A W (1994). Evaluating public transport and road safety measures. *Accident Analysis and Prevention* 26, pp.411-428.

- Iida, Y (1999). Basic concepts and future directions of road network reliability analysis. *Journal of Advanced Transportation* 33 (2), pp.125-134.
- Lam, W H K and Xu, G (2000). Calibration of traffic flow simulator for network reliability assessment. In Bell, M G H and Cassir, C (eds), *Reliability of Transport Networks* (Research Studies Press: Baldock), pp.139-157.
- Lee, C E (1946). New works for wartime traffic – 2. *The Railway Magazine* Vol 92 No 563, May/June, pp.177-183.
- Nicholson, A J and Dalziell, E (2003). Risk evaluation and management: a road network reliability study. In Bell, M G H and Iida, Y (eds). *The Network Reliability of Transport*. (Pergamon-Elsevier: Oxford), pp.45-59..
- Nicholson, A J and Du, Z P (1997). Degradable transportation systems: an integrated equilibrium model. *Transportation Research B* 31B (3), pp.209-223.
- Richardson, A J and Taylor, M A P (1978). A study of travel time variability on commuter journeys. *High Speed Ground Transportation Journal* 12 (1), pp.77-99.
- Taylor, M A P (1982). Travel time variability – the case of two public modes. *Transportation Science* 16 (2), pp.517-521.
- Taylor, M A P (1999a). Dense network traffic models, travel time reliability and traffic management. I: General introduction. *Journal of Advanced Transportation* 33 (2), pp.218-233.
- Taylor, M A P (1999b). Dense network traffic models, travel time reliability and traffic management II: Application to reliability. *Journal of Advanced Transportation* 33 (2), pp.235-251.
- Taylor, M A P (2000). Using network reliability concepts for traffic calming - permeability, approachability and tortuosity - in network design. In Bell, M G H and Cassir, C (eds), *Reliability of Transport Networks*. (Research Studies Press: Baldock), pp.217-242.
- Van Zuylen, H and Kikuchi, S (2003). Travellers' behaviour under uncertain conditions. In Bell, M G H and Iida, Y (eds). *The Network Reliability of Transport*. (Pergamon-Elsevier: Oxford), pp.155-170.
- Yang, H, Lo, H K and Tang, W H (2000). Travel time versus capacity reliability of a road network. In Bell, M G H and Cassir, C (eds), *Reliability of Transport Networks*. (Research Studies Press: Baldock), pp.191-138.