Asian Transport Studies, Volume 3, Issue 4 (2015), 362–377.

Decision Principles for Routing Strategies: Games against Nature and Demons

Jan-Dirk SCHMÖCKER [a], Achille FONZONE [b*]

[a] *Department of Urban Management, Kyoto University, Kyoto,* 615-8540, Japan*; E-mail:* schmoecker@trans.kuciv.kyoto-u.ac.jp
[b] *Transport Research Institute, Edinburgh Napier University, Edinburgh,* EH10 5DT, UK*; E-mail:* a.fonzone@napier.ac.uk

Abstract: In this paper we firstly review general decision principles under uncertainty and apply them to route choice decisions. Risk-averse behaviour leads to the description of route choice a game. The difference between games against demons and nature are pointed out by distinguishing when disruptions on the chosen route might be related to the traveller's behaviour or not. It is argued that in many cases the traveller has some (limited) information about the connection between attack likelihood and routing, meaning that pure games against demons are rare for practical applications. The paper therefore extends the game theoretic literature on route choice by formulating a generalised model. The model allows for games against multiple demons and consideration that some links might be safer than others. It is shown that games against nature and the Bell (2007) model can be derived as limiting cases. Results are illustrated with an example network.

Keywords: Risk-aversion, Game Theory, Route Choice, Incident Information

1. INTRODUCTION

Decision making under uncertainty is a topic of wide interest, from philosophical questions to mathematical problems with a very diverse range of applications (e.g., Binmark, 2008; Gilboa, 2010). Applied to transport, and more specifically route choice in a network, uncertainty arises as travellers and dispatchers often have to consider a number of risks when choosing a route. There might be congestion, accidents, vehicle-break downs or natural disasters. These risks could result in delays or, worse, loss of goods and life. Therefore the nominally shortest or most attractive route may no longer be chosen if the fear of such incidents dominates decision maker's concerns. The more a traveller is unwilling to experience such risks the more "risk averse" he is considered. Whereas a risk-neutral traveller would try to balance the potential risks and the risk-independent minimum operational costs of a route, for an extremely risk-averse traveller the possible consequences of incidents outweigh the fixed costs.

The strategy of the traveller to counter the risk will therefore depend on the feared consequences as well as the likelihood of the incidents. In particular, he has to judge whether the likelihood of incidents will depend in any way on his route choice. If he/she assumes that this is not the case, route choice under risk can be considered a "game against nature". The fear of natural disasters or generally unpredictable events are examples. For such games against nature different decision principles have been proposed, in particular aiming to

* Corresponding author.

minimise the risk, the expected value or the possible regret (Straffin, 1993).
However, if incident likelihood and route usage might be related, a risk averse traveller can consider the route choice as a game against a "demon" or "evil entity" (Bell, 2000). A prime example for such a scenario is the transportation of highly valuable or hazardous materials, where the router fears that any information about his chosen route could enable an opponent, such as a thief or terrorist, to plan an attack. The router therefore aims to find a routing strategy that is safest independent of what the attack plans could be.

The implicit assumption of this zero-sum game is that the traveller has no information about incident likelihood and hence fears the worst. In many situations, however, the likelihood of an incident may be at least partially predictable as a function of the route usage. Based on past statistics or other additional information one may remain risk averse but also conclude that certain scenarios are too unlikely to be worth considering. Hence we deal with incidents whose probabilities are known to be disproportionally increasing with resource usage. There are also several examples for these types of failures: Human errors are likely to increase under more stress, or, in the case of repeated transportation of hazardous goods, the annoyance of residents along the route can cause the incident probability to increase with more frequent use of the route.

The reminder of the paper is organised as follows. The next section will review the decision principles used for routing under uncertainty, distinguishing games against nature and demons. Section 3 introduces the notation used that is required to describe such games. Section 4 then reviews mixed routing strategies in more detail highlighting some practical issues with existing approaches. Section 5 sets up our revised model formulation that allows for games against nature, demons and intermediate cases. We discuss some model properties and limiting cases and apply the model to a small example network in Section 6. Section 7 then concludes this study by summarising some of the observation and discussing possible applications as well as further work issues.

2. LITERATURE REVIEW

2.1. Games against Nature

Let us first assume that a single optimal route has to be chosen, either because the decision has to be made only once or because previous decisions have no influence on the current decision. One might argue that the latter assumption is typical for games against nature. Nature is not considered to have a *strategy* but rather specific *scenarios* are feared by the traveller. When the probabilities of incident scenarios are known, one can base an estimation of the risk on this information (using the expected value principle) and choose a route that is perceived as a good trade-off between the risk and the operational costs associated with the choice. The more risk averse the traveller, the higher weight will be attached to the potential consequences and the lower to the operational costs. If the probabilities of incidents are unknown alternative principles will have to be used by the decision maker. Following Straffin (1993), Schmöcker (2010) distinguishes a number of general decision principles which could also be applied to route choice:

The Laplace principle, also referred to as *criterion of insufficient reason*, recommends in the absence of further information to assume equal probabilities of all possible incidents. Applied to route choice this means assuming equal probabilities for all possible failure scenarios, and applying the expected value principle to find the route with the least expected cost. Especially if incidents are known to be rare, this clearly overestimates failure scenarios

though. If such additional information is available, the likelihood of particular scenarios can be weighted accordingly.

An alternative decision criteria, mostly associated with risk-averseness, is Wald's minmax principle (Wald, 1950). Wald's suggestion is to choose the route that has the lowest cost in the worst case scenario. This is equivalent to ignoring the incident probabilities altogether, and in the literature on network reliability and route choice is referred to as "vulnerability analysis" (Berdica, 2002; D'Este and Taylor, 2003; Taylor and D'Este, 2007). Vulnerability analysis is focused only on consequences and understanding which links in a network can potentially cause most disruption if affected by an incident, and usually is based on the assumption that link usage and incident probability are unrelated.

The opposite of a risk-averse is an optimistic traveller who always chooses the shortest path. This is known as minmin principle (or maxmax principle if utilities instead of costs are considered). Hurwicz introduces a "level of risk-averseness" by mixing the minmin (optimistic) and minmax (pessimistic) approaches (see Milnor, 1951). He introduces a "coefficient of optimism" bounded between 0, when one is only pessimistic, and 1, when one is only optimistic. With this coefficient one can describe route choice considering the trade-off between optimism and pessimism (or risk-aversion). Especially if these coefficients become route or link specific this approach can then also be described as the expected value approach.

Alternatively a traveller might base his decision on the principle of minimising regret proposed originally by Savage (1954). In this case the decision maker aims to choose an alternative which will never be too far off from the best possible option without paying too much avoidable costs if the worst scenarios do not occur. Application of regret to mode and route choice decisions has recently found growing interest in the transport literature (Chorus, 2012; Fonzone *et al.*, 2012).

It is important to emphasise that under the assumption of "independent scenarios" all these decisions principles lead to single route decisions. Others have suggested that even for games against nature mixed routing decisions might be used. In particular Milnor (1951) illustrates with a family of game scenarios that mixed strategies might be employed for all decision principles. The argument might be summarised with the proverb "don't put all your eggs into one basket". The difference whether it is useful to employ a mixed strategies or single strategies should be based on the assumption of "independent scenarios". Straffin (1993) summarises the discussion on the "Jamaican fishing problem" which illustrates this problem: Davenport (1960) observes optimal fishing strategies for fishermen in a Jamaican village who are confronted with uncertainty of currents in the sea. It happens that nature is employing a near optimal mixed strategy as if it would be an intelligent demon. The fishermen respond by employing their optimal mixed strategy, which is taken by Davenport as evidence that the solution to this kind of game against nature should be the resulting mixed strategy Nash equilibrium. Kozelka (1969) and Read and Read (1970) have pointed out though that the strategy of nature can be observed and that the fishermen could maximise their profit by treating this as an expected value problem with a single strategy solution since nature will not react to changes in the fishermens' strategies. In turn Bagnato (1974) responds that this ignores risks associated with the potential uncertainty of nature's strategy. For example it might happen that over a certain time period currents do not follow the observed probabilities.

It is precisely the property that the mixed strategy guarantees a certain payoff over time, irrespective of nature's strategy, in this case the actual currents occurring, that make it attractive to the fisherman. This argument, however, implicitly assumes that the decisions are not made independently of previous outcomes. The fishermen might have to ensure a certain

amount of pay-off at all time to sustain their living instead of maximising their profit over the long term as also pointed out by Straffen (1993). Therefore, the fishermen compensate for potential loss during one fishing day by employing a more conservative strategy on the next day. If, however, the gain or loss encountered on a previous day does not have an influence on the current decision this argument obviously does not hold and one might employ the same strategy at all times. One might call this the Markov property of games against nature.

2.2. Games against Single and Multiple Demons

In contrast to the type of scenarios discussed before, in this section situations are considered when incident probabilities cannot be assumed to be independent from the route choice and the Markov property in decision making does not hold for at least one player. The prime example for games against a single demon is fear of a terrorist attack en route.

The risk-averse routing strategy in this kind of situation is found using a game-theoretic approach proposed in Bell (2000). If the game is played only once, the resulting route will be the same as the one suggested by Wald's minmax principle. However, if the game is played repeatedly, a mix of routes rather than a single route will be optimal in most cases. This mix of routes is a Nash equilibrium mixed strategy, in which using both shorter (but potentially more expensive if an incident occurs) and longer (but less expensive if an incident occurs) routes leads to a reduction in the maximum expected cost. This reduction in the expected cost is owing to the traveller leaving the attacker uncertain which route will actually be chosen. Bell (2007) emphasises that this mixed strategy should be implemented by randomly choosing the route according to the probabilities found at equilibrium. This sort of game theoretic analysis requires that an assumption is made regarding the number of expected incidents, and subsequent papers by Bell and his co-authors assume that one should plan for exactly one (major) incident, since the occurrence of multiple incidents is too unlikely. Finding optimal routes if one considers that n (minor or major) independent incidents might occur is considered by Szeto *et al.* (2007). Bell (2008) and Schmöcker *et al.* (2009) examine the case of fear for one incident on each link downstream from a decision node ("local demon problem"). The solution is a "hyperpath" that gives the traveller optimal path split probabilities at each decision point.

3. NOTATION

Throughout the paper following notation will be used which largely follows Bell (2007). In this paper "link" might be interpreted not only as a road link but more generally as any element of a journey or process that might be subject to an incident.

A	Set of all links, with $\bar{A}$ denoting the number of links
O	Set of links emanating from the origin
D	Set of links leading into the destination
γ_{ij}	1 if link j precedes link i and 0 otherwise
L_i	Feared "loss" on link i if in failed (delayed) condition
c_i	Fixed travel cost on link i (optimistic travel time)
p_i	Probability that link i is used

q_i	Perceived risk of experiencing L_i due to link usage (demon game)
z_i	Perceived unavoidable risk of experiencing L_i (link usage independent risk, game against nature)
C	Expected cost for selected route set (strategy)
M	Total exposure to loss on route set
N	Number of links feared to be in failed (delayed) condition

4. PROBLEM FORMULATION

4.1. Route Sets for Risk Dispersion

There is a larger set of literature, in particular related to the routing of hazmats, on generating path sets rather than a single path as a means to reduce exposure to risk without developing optimal path split probabilities: Batta and Chiu (1998) or Erkut and Ingolfsson (2000) discuss in which circumstances it might be worth considering additional less risky routes for hazmats transported on road networks and Glickmann *et al.* (2007) discuss that the same might also be true for public transport networks. Akgün *et al.* (2000) discuss several algorithms to generate a set of dissimilar paths or generally to create a "*k*-paths" set out of which one will be chosen. Obviously the more dissimilar the paths, the higher the chance that an alternative path is not affected by the same incident. Kurauchi *et al.* (2009) therefore extend the literature on network vulnerability analysis by providing a solution to generate *k* non-overlapping paths. To avoid the inclusion of unrealistically long routes the sets are restricted to paths for which the increase in length, compared to the non-disrupted base case, does not exceed a predetermined factor.

Compared to this set of literature, the attractiveness of the approach in Bell (2007) is that it generates a path set as well as route choice probabilities. Furthermore, these probabilities can be behavioural justified to provide a risk-minimising solution. The game is set up between a traveller and a single fictive network demon. The reasoning is as follows: The traveller, being risk averse, expects exactly one incident (link failure or in general any adverse event) to occur. Such an adverse event is so unlikely that the occurrence of more than one incident (multiple attacks) is not considered. The router has no information where the attack might occur. The decision maker's objective is to find a routing strategy that minimises total cost *C*. Therefore the problem is formulated as P0:

$$\text{P0:} \quad Min_{\boldsymbol{p}} Max_{\boldsymbol{q}}\ C = \sum_{i \in A} p_i L_i q_i + p_i c_i \tag{1}$$

Subject to

$$\sum_{i \in A} q_i = 1 \tag{2}$$

as well as

flow conservation and non-negativity of link choice and link attack probabilities.

Generally, the exposure *M* to loss on given a route set can be defined as:

$$M = \sum_{i \in A} p_i L_i \tag{3}$$

and Bell (2007) shows that this problem is equivalent to a minimisation problem with respect

to **p** where $L_i p_i < M^* \; \forall i$, with assumption (2), side constraints (3) – (7), where M^* is the maximum exposure on any single link.

4.2. Discussion and Extension

The game described in previous section obtains its mathematical simplicity due to two behavioural stringent assumptions. Firstly, **p** and **q** are independent in the sense that both traveller and demon can choose links freely only considering the constraints on maximum attack, flow conversation and non-negativity. From both players' point of view this is equivalent to a no-information scenario. Secondly, (2) assumes that the decision maker expects exactly one incident to occur. In the following both assumptions are generalised in order to obtain insights in how far mixed routing strategies are still valid under such relaxed conditions.

We consider that the traveller might have some limited information about the relationship between incident probabilities and link usage. The more risk averse, the less he will trust this information, so that P0 should be a limiting case. In the case of terrorist attacks often potentially dangerous spots in a network are anticipated and other system elements are believed to be less threatened. Furthermore, also for other situations with fictive demons in which P0 might be envisaged to be applied the no-information case often does not hold true. Consider transportation of hazardous goods through populated areas. The dispatcher might fear incidents as well as annoyance of residents due to their exposure to risk. Frank *et al.* (2000) suggests limiting the amount of hazardous materials transported on the same route for equality reasons in order not to overexpose some populations. Accordingly, dispatchers of nuclear waste or other hazardous material might choose not to rely too heavily on one specific route to avoid demonstrations along the route by annoyed residents. While a certain level of usage might be deemed acceptable (or unavoidable), overreliance on a single route might be perceived as unfair. Similarly, the transport routes of high value shipments, e.g. money, are often altered in order to reduce the likelihood of being attacked on a particular link.

The list of examples might be extended by infrastructure failures due to overstrain or fatigue. Further, an accident at an airport, shipping port or a rail line is more likely if the facility is used up to, or, in particular, above capacity. Similarly, concern about accident likelihood increasing with long driving times is reflected by legislation limiting truck drivers' working hours, in particular if they transport hazardous goods. The common point of all these examples is that incident likelihood is disproportionally increasing with higher usage of the resource.[1] Though it might be difficult to obtain accurate data on incident probabilities it seems likely that decision makers can at least to some degree estimate how "loss probability" depends on link usage in many cases.

Secondly, we modify (2) to consider that the traveller might not only fear a single incident. Terrorists might strike at several network points simultaneously as some tragic events in the last decade have shown. In the case of other events and games against nature such as natural disasters also the simultaneous failure of several links in the network is frequently. For example Jelenius and Mattson (2012) discuss the case of all roads in some parts of Sweden being not operational due to snow fall. The area wide impacts of earthquakes and tsunamis are also obvious. Alternatively, the decision maker might not be certain that an incident occurs at all, in which case it will be more beneficial to stick even more often to the shorter route than in the route mix suggested by P0. In conclusion, a more general model

[1] Note that also the converse might be true, i.e. that the likelihood of an incident might be decreasing with higher usage of a resource; for example if familiarity of the driver with the route is a key aspect. In this case obviously sticking to the same route all time will be the best option, which will also be illustrated in the following analysis.

description than n=1 as in problem P0 is desirable.

5. GENERALISED MODEL FORMULATION

5.1. Formulation

Given the attractiveness of P0 to provide risk-averse route sets we seek a similarly simple model formulation that overcomes the above discussed possible shortcomings for practical routing applications. We derive following modification of P0 which we argue also clarifies the relationship between games against nature versus games against demons:

$$\text{P1: } Min_{\boldsymbol{p}} Max_{\boldsymbol{q}}\ C = \sum_{i \in A} p_i L_i (z_i + q_i - z_i q_i) + p_i c_i \tag{3}$$

Subject to following constraints for $\forall i \in A$:

$$\sum_{i \in A} q_i \leq n \tag{4}$$

$$q_i \leq Min\{f(p_i), 1\} \tag{5}$$

as well as

flow conservation and non-negativity of link choice and link attack probabilities.

Firstly note that we introduce a new set of parameters **z**. These are not optimized but describe the general perceived risk of being exposed to losses. This part of the cost function can hence be described as "game against nature". The risk of travelling on link i is linearly dependent on z_i which can be described as the general (usage-independent) scenario likelihood of an incident occurring. For example on links known to be accident hotspots the dispatcher of hazmat transports might set this value to non-zero.

In addition to "scenarios" the traveler might fear strategies of a fictional demon. As in P0 this is expressed with **q**. We firstly replace (2) with (4) to allow for various attacks. Constraint (5) specifies the relationship between **p** and **q** which might take various forms and is here hence just described as a general functional form. Being risk averse, the decision maker considers the maximum likelihood of attacks on links. For example for links presumed to be the likely target of a terrorist one might set $f(p_i)$ close to 1, on other links that are perceived to be safe from attacks or where one is certain that one has enough information to avoid attacks the function might take values close to zero. In general the functional value will depend on a) the general perceived likelihood on the link and b) the perceived available information that allows avoiding the impact of an attack.

5.2. Limiting Cases

From the model formulation we can immediately establish some limiting cases. Firstly, P1 reduces to P0 for n = 1, **z** = 0 and $f(p_i) \geq 1\ \forall i$. This is as expected as it means that exactly one attack is feared, the risk is perceived to only derive from an intelligent demon and no information is available on whether the attack can be avoided or defused.

Secondly, the demon part of the game is not relevant and the game reduces to a pure game against nature when the demon is not active or "powerless" ($n \to 0$, $f(p_i) \to 0\ \forall i$) or when the traveler already considers the worst case on all links ($z_i \to 1$). In the case of $n \to 0$ or $f(p_i) \to 0\ \forall i$ no malevolent incidents are feared and the route suggested by P1 tends to be similar to that obtained by applying the expected value principle considering the general

incident likelihood z_i. Accordingly also the case of $z_i \rightarrow 1$ leads to Wald's minmax decision principle ("choose the safest route considering the worst case on each link").

Thirdly, in general the demon's reaction is assumed not predictable when $f(p_i) = y \ \forall i$, where y is a constant, i.e. when it is not possible to consider the influence of p_i on the (maximum) probability of attack. Assuming $z_i = 0$, the demon will attack in each iteration the m links with the highest loss exposure $L_i p_i$ with this constant y where m is n/c rounded down to the nearest integer and the link with the m+1-th highest loss exposure with $q_i = (n - m \cdot c)$ In line with this is again our observation that $f(p_i) \rightarrow 1$ is assumed in the risk-averse case of P0.

Fourthly, it is worth pointing out that for $n \rightarrow A$, the traveler expects that the demon can strike on each link. This means that constraints (4) are inactive and the problem reduces to a minimization problem of **p** with given **q**. Therefore this case can also be described as game against nature with the decision principle "risk-averse expected value", where the traveler fears that on each link the loss L_i might occur with probability $Min\{f(pi), 1\}$. It therefore describes Hurwicz decision principle where (5) describes the coefficient of pessimism.

Following this and the argumentation in Section 2 we expect that in the second and third limiting case single route strategies are optimal and mixed routing strategies are optimal in the first limiting case as well as intermediate cases.

5.3. Solution Algorithm

We firstly note that the traveller problem remains a linear program of the form Min C subject to demon attack scenario costs, flow conversation and non-negativity constraints as discussed in Bell (2003). The formulation of the constraints in P0 further illustrates that direct LP solver methods can be applied (Bell, 2007). For large network applications and to avoid path enumeration we propose though to solve the problem with an MSA heuristic instead as proposed in Bell (2000) and applied in Bell (2003). Convergence and uniqueness of the single traveller problem follow immediately from LP theorems.

Further following Bell (2000) who in turn refers to iterative game solution approaches used in Hillier and Liebermans (1990) the Nash equilibrium of P0 can be found if the demon problem is solved within each MSA iteration, given the current traveller route choice scenario. In both P0 and P1 also the demon problem is a linear problem with identical objective function though different constraints. Bell (2003) solves the problem by letting the demon attack the single link with the highest exposure $L_i p_i$ in each MSA iteration. This solution approach is not feasible anymore for P1 due to link specific constraints (4) and (5). Furthermore (4) implies that the demon has wider attack options if $n > 1$, meaning that an optimal set of attacked links needs to be found. We propose that this problem can be solved with the following variation of the MSA. It is worth noting that averaging of **q** is not required due to the fixed point nature of this problem. This is similar to the Bell (2007) contribution that the Minmax game can be converted into a minimisation problem for the traveller considering the worst case attack combination for the demon.

1. Set $m \leftarrow 1$, $\mathbf{p}^m \leftarrow 0$ and $\mathbf{q} \leftarrow 0$.
2. Select the shortest route and find auxiliary link choice probabilities $\boldsymbol{v}$ by setting $v_i \leftarrow 1$ for all used links and $v_i \leftarrow 0$ for all unused links.
3. Update the link choice probabilities **p** by MSA: $p_i \leftarrow (1/m)\ v_i + (\ (1- (1/m))\ p_i$
4. Attack the links with highest loss as much as possible considering constraints (9) to (11) in order to find attack probabilities **q** by performing following steps:
    a. Set $x \leftarrow n$.

   b. Choose link i with highest exposure $L_i p_i$ not chosen so far.
   c. $q_i \leftarrow$ Min $\{ x , 1, f(p_i) \}$.
   d. Reduce x by attack on link i: $x \leftarrow x - q_i$.
   e. Return to Step 4b until all links are chosen or $x = 0$.
5. Check convergence, if $\forall i \; |p_i^m - p_i^{m-1}| < \varepsilon$ then stop, otherwise $m \leftarrow m + 1$ and return to Step 2.

The main difference compared to the previous MSA suggested by Bell (2000) that solves the zero sum game P0 is in Step 4. Previously the (auxiliary) attack probabilities would be binary with 1 for the link that increase the path costs most and 0 on all other links. In this game with additional side constraints Step 4 is implemented as follows: Step 4a initialises the algorithm with an auxiliary variable x defining the total possible link failures. The reasoning of Step 4b is that, being risk-averse, the traveller fears that the links with highest potential damage are subject to an incident. Step 4c finds therefore these incident probabilities considering constraints (4) and (5).

Proposition 1: Steps 4a to 4e also find the optimal demon strategy in each iteration:

Proof: Assume not, i.e. a link $j \neq i$ with $L_j p_j < L_i p_i$ is chosen in iteration 4b ahead of link i and C increases. Choosing a different choice order leads to **q'** with $p_j L_j q'_j \geq p_j L_j q_j$ and $p_i L_i q'_i \leq p_i L_i q_i$ since x might reduce to be less than Max $\{ 1, f(p_i) \}$ by the time i is chosen. This means that the cost function has changed by $p_j L_j (q'_j - q_j) - p_i L_i (q'_i - q_i)$. Due to maximisation in 4c as well as constraint (4) it follows however, that $(q'_j - q_j) \leq (q'_i - q_i)$. Even assuming equality due to $L_j p_j < L_i p_i$ it follows that $p_j L_j (q'_j - q_j) \leq p_i L_i (q'_i - q_i)$ so that the cost function cannot have increased.

Similarly argumentation leads to a contradiction for the assumption that not the maximum possible q_i is chosen in Step 4c which completes the proof as the other steps in the demon problem simply ensure the constraints are kept. Qed.

6. ILLUSTRATION WITH EXAMPLE NETWORK

To illustrate the model and the limiting cases the solution algorithm has been implemented in Matlab with the stopping criteria in Step 5 of the solution algorithm as in (6).

$$\varepsilon = 10^{-3} \cdot \sqrt{\bar{A}} \tag{6}$$

We further assume a linear in log odds relationship between link usage and the perceived upper bound for the attack risk.

$$f(p_i) = \frac{\alpha \cdot p_i^{\delta}}{\alpha \cdot p_i^{\delta} + (1 - p_i)^{\delta}}, \alpha, \delta \geq 0 \quad \forall i \in A \tag{7}$$

This type of function represents a wide range of situations in which objective probabilities are somehow interpreted within decision making processes and other tasks related to cognition (Zhang and Maloney, 2012). Figure 1 shows how the upper bound of the perceived probability of a malevolent attack $f(p_i)$ – i.e. his inclination to attack a link – varies with the link choice probability p_i for different values of the parameters α and δ. These

parameters can be easily interpreted as demon's "aggressiveness" and "discrimination" respectively. Given a certain link choice probability p_i, the higher α the more likely the demon attacks (or is thought to attack) the link. For instance, in Figure 1c, a link used in 60% of cases has a maximum probability of being attacked of 60% if α =1, but the same probability becomes 90% if α=6. Parameter δ regulates the demon reactiveness. The higher δ the more the demon is sensitive to differences of link choice probability: For low values of δ, the demon reaction tends to become unpredictable, i.e. his strategy does not depend on the traveler's strategy (Figure 1a). On the contrary, for high values of δ, even a small increase in a link choice probability can dramatically increase the probability that the demon targets that link (Figure 1d). For $\alpha \to 0$ P1 degenerates into a pure game against nature, whereas for $\delta \to 0$ and $\alpha \to \infty$ P1 becomes a Wald's minmax-like problem regulated by n as described in 5.2. In particular P0 is obtained if $\delta \to 0$, $\alpha \to \infty$ and $n = 1$.

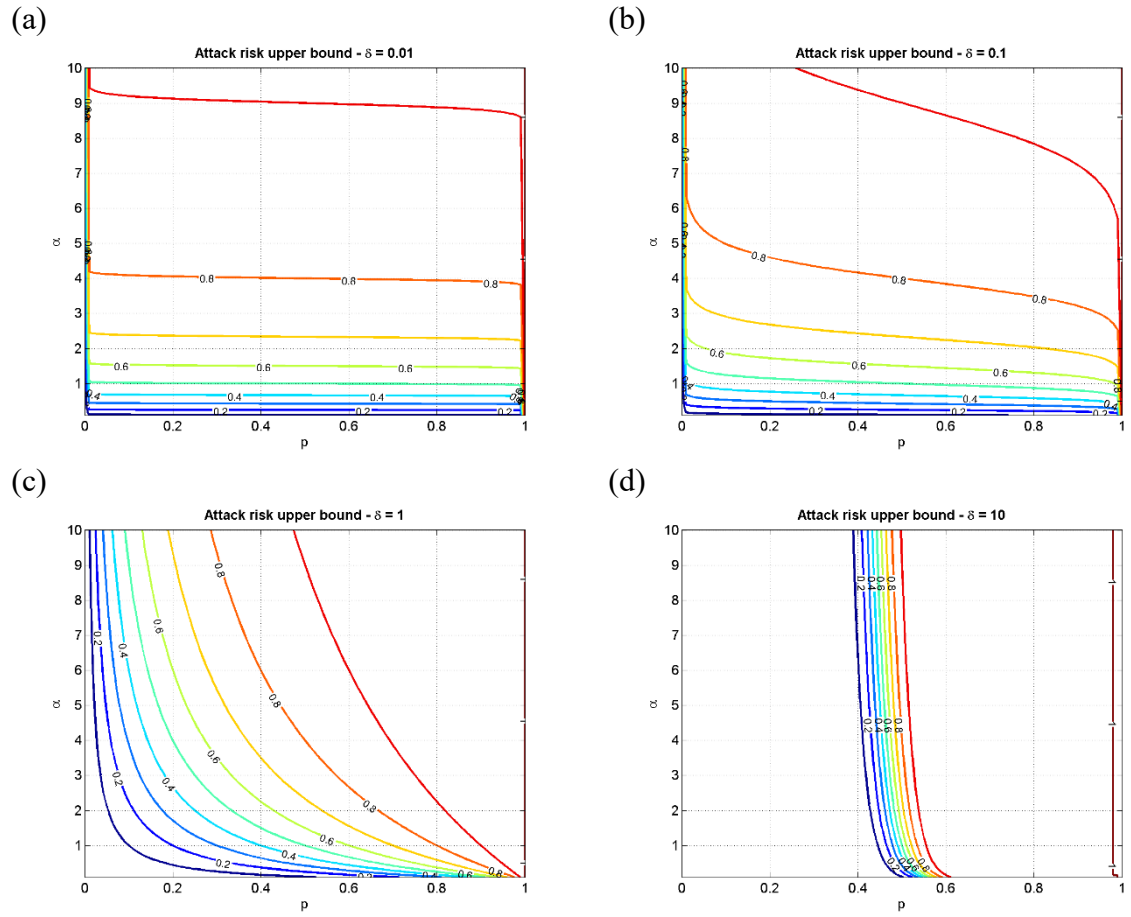
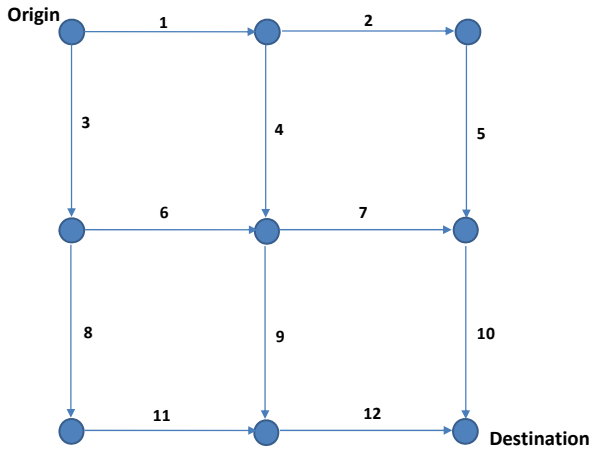


Figure 1. Attack risk upper bound function

In this section the small example network shown in Figure 2 is used. Table 1 illustrates the 6 potential paths the traveller might take between the OD pair as well as the fixed (optimistic) path costs and the loss exposure on paths. Path 1 exposes the traveller to the least potential loss whereas path 4 is the nominally shortest path if no incident occurs but also the path with potentially highest cost in case all links are in failed condition.



Link	Cost c_i	Loss L_i
L1	11	25
L2	2	25
L3	3	40
L4	8	25
L5	9	10
L6	3	50
L7	10	35
L8	9	25
L9	6	25
L10	5	35
L11	2	25
L12	10	25

Figure 2. Network structure and link costs

Table 1. Possible paths of example network

	Links of Paths				**Fixed travel cost** $\sum_{i \in Path} c_i$	**Exposure** $\sum_{i \in Path} L_i$
Path 1	1	2	5	10	27	95
Path 2	1	4	7	10	34	120
Path 3	1	4	9	12	35	100
Path 4	3	6	7	10	21	160
Path 5	3	6	9	12	22	140
Path 6	3	8	11	12	24	115

Table 2 shows the optimal link split strategies for four specific cases. In the first three cases $\delta \to 0$ that is $f(p_i) \to$ const, i.e. decreasing the choice probability of a link does not reduce the (maximum) probability that the link is attacked. In the first column we set $\alpha \to 0$ which means that the game transforms into a game against nature. Since $\mathbf{z} = \mathbf{0}$ no failure at all is expected and the traveller tends to select the optimistic shortest path (path 4). Setting $\alpha \to \infty$ in the second column leads to maximum attack probabilities equal to 1. With n=1 the scenario resembles the P0 game of a single demon against a traveller, where the demon has the capability to fail exactly one link. Since the attack probability are not limited by the choice probability, the demon concentrates its firepower on the link that maximise the cost for the risk-aware traveller. As explained in previous literature and illustrated in the example in this case it is best not to focus on one specific route. In column 3 we set n = 12, meaning that the demon can attack each link. In this case constraints (4) tend to become redundant, in other words the demon, having the possibility, will attack each link independent from the probability of hitting travellers. The solution of P1 approximates Wald's minmax route choice. It is assumed that every link fails and therefore path 1 is picked because it has the minimum sum of travel cost and exposure. Finally, in column 4 we illustrate the effect of high discrimination. With high δ (and high α) Eq. (7) becomes a step function with $f(p_i) \approx 1$ for $p_i \geq 0.5$ and $f(p_i) = 0$ for other values of p_i. Since n =12 the demon will surely attack any link which has a usage probability greater than 0.5, but he will not attack a link if he has less than 1 chances out of 2 of hitting travelers. Therefore, the traveler tends to keep all link usage probabilities below this critical value, and only 5 links are potentially subject to attacks despite the demon having the firework to strike all of them.

Table 2. Link Split (Attack) probabilities for 12 link network for four specific cases, **z** = **0**

Link	**α=0, δ=10^{-3}, n=1 P1 → Optimistic**	**α=10^3, δ=10^{-3}, n=1 P1 → P0**	**α=10^3, δ=10^{-3}, n=12 P1 → Wald minmax**	**α=10^3, δ=10^3, n=12 "Choosy" demon**
1	0.03 (0)	0.53 (0)	0.95 (1)	0.50 (1)
2	0.03 (0)	0.53 (0)	0.93 (1)	0.45 (0)
3	0.97 (0)	0.47 (0)	0.04 (1)	0.50 (0.95)
4	0 (0)	0 (0)	0.04 (1)	0.05 (0)
5	0.03 (0)	0.53 (0)	0.93 (1)	0.45 (0)
6	0.94 (0)	0.37 (0)	0.02 (1)	0.50 (0)
7	0.94 (0)	0 (0)	0.02 (1)	0.05 (0)
8	0.03 (0)	0.09 (0)	0.02 (1)	0 (0)
9	0 (0)	0.37 (0)	0.02 (1)	0.50 (0.04)
10	0.97 (0)	0.53 (1)	0.95 (1)	0.50 (0.95)
11	0.03 (0)	0.09 (0)	0.02 (1)	0 (0)
12	0.03 (0)	0.47 (0)	0.04 (1)	0.50 (1)
Risk averse cost	21.26	43.60	123.92	86.08
Exposure	156.86	113.688	97.04	118.61

Figures 2 to 5 illustrate more generally the solution to P1 for different α, δ and n; in all cases **z** = 0 is assumed. Figure 3 shows optimal path splits in case the demon attack strategy is not understood (low discernibility) and cannot provoke more than 1 incident. Low values of α indicate that the demon is not likely to attack hence a mix of routes with a preference for the shortest path (Path 4) is the best solution. When links become attractive for the demon (large α) the optimal solution coincides with that of P0 and Path 4 is abandoned because of its high exposure. Note that Path 2 is never used because 1) for $\alpha \to 0$ the risk averse link costs coincide with the optimistic travel times and Path 2 has the second highest optimistic cost and 2) for $\alpha \to \infty$ all flows arriving at the central node prefer the subpath {L9, L12} because it has an exposure considerably lower than {L7, L10}.

Figure 4 shows the path split depending on δ considering a very large value of α and no more than 1 incident. P1 and P0 have the same solution for a wide range of δ values, meaning that the risk-averse approach proposed by Bell provides the optimal solution for all the situations in which attack probabilities cannot be well predicted. Even for high δ the path split suggested by P1 is not too far from that suggested by P0, with paths 1 and 5 still carrying overall almost the same flows, though differently distributed, between the two paths. Therefore it can be concluded that the risk-averse mixed strategy *a la* Bell is sound as far as it is known that the demon is determined and can cause at most 1 strike.

This is not always the case when the number of expected attacks increases. To illustrate this, we define two indicators measuring the similarity of two solutions given by different sets of route choice parameters, defined as follows: Given two path splits, let A_1 and A_2 be the respective sets of used links and p_{i1} and p_{i2} the probabilities of link i usage. Let further $A_U = A_1 \cup A_2$, $A_I = A_1 \cap A_2$. We define

$$A_{12} = \frac{|A_I|}{|A_U|} \quad \forall i \in A \tag{8}$$

$$P_{12} = \frac{\sqrt{\sum_{i \in A_U} (p_{i2} - p_{i1})^2}}{\sqrt{\sum_{i \in A_U} (max\{p_{i1}, 1 - p_{1i}\})^2}} \quad \forall i \in A \tag{9}$$

A_{12} is a measure of how many links are used by both path splits (overlap). P_{12} quantifies how different the flows are assigned in the two path splits (path split similarity). Both indicators vary between 0 and 1. In Figure 5 it can be seen that when the demon has the capacity to attack all links, the flow distributions suggested by P0 and P1 are rather different for low/medium demon strategy discernibility. Note that since the P0 solution uses 10 links out of 12, high values of overlap are expected with any other mixed strategy solution. Overlap and similarity with the optimistic route choice (single path) are also reported for reference.

Figure 6 shows the exposure for various n as well as δ. As expected the higher the attacking capacity of the demon the less the traveller uses links with high loss, i.e. the exposure reduces. When δ increases the information the traveller has got becomes richer in the sense that it allows a better prediction of demon's behaviour. Therefore the traveller can dare using paths with higher exposure and the solutions merge. For very high δ values, case 4 in Table 3 is obtained. The traveller understands the "choosy" behaviour of the demon well and the solution is determined by finding the route choice set with the lowest cost and the constraint that the usage probability on each link is below 0.5.

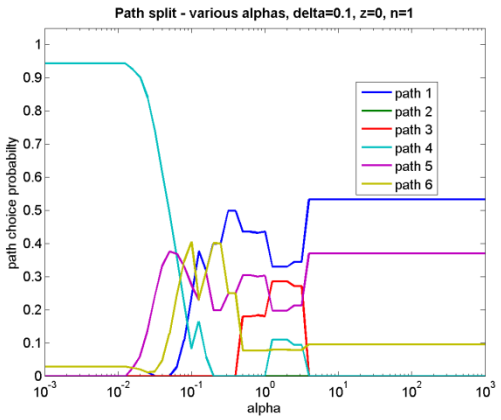


Figure 3. Path splits for different α

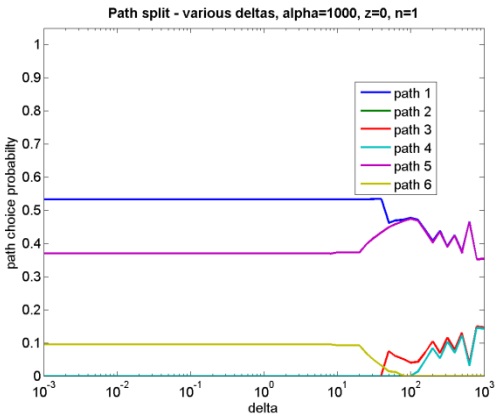


Figure 4. Path splits for different δ

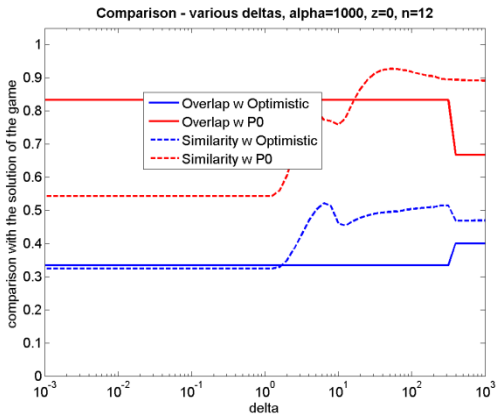


Figure 5. Comparison with special cases for different δ

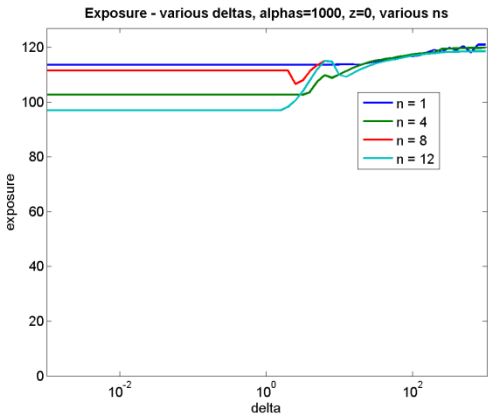


Figure 6. Exposure for different δ and n

7. CONCLUSIONS

This paper started by reviewing the in the literature common decision principles for games against nature and how these might be applied to route choice. If information about incident probabilities is not available (or reliable) the traveller will have to decide in how far the risk of such incidents influences routing decisions. Travellers will have to decide between optimism, pessimism or a mixture between the two. A fourth decision principle mentioned but not focused on this paper is regret. Regret will be especially important to travellers who can gain information about actual travel costs on a set of routes. Fonzone *et al.* (2012) further argue that in the context of dynamic route guidance regret becomes important if travellers obtain information on best and worst case travel times on links.

This paper focused on the trade-off between optimism, i.e. choosing shorter but potentially more risky routes, and pessimism. We argue that even in case of extreme pessimism and games against nature mixed routing decisions are not useful if decisions are made independently of the results of past routes taken. The situation differs if one believes that the incident likelihood might, at least to some degree, depend on one's own behaviour, i.e. if one fears that the risk is caused by a reactive "demon". Such a demon might be fictional ("just in case if nature might be malevolent") or a real threat. Bell (2003) further argues that the demon game is valuable to understand network vulnerability to find the worst links in the network.

The main contribution of this paper is the formulation of P1 in Section 5 and the insights gained from this formulation of game theory and routing decisions. In particular we show that optimism, nature game pessimism and the Bell (2000) game are limiting cases. We believe P1 allows for the combination of pessimism and optimism even in a demon game context. A purely pessimistic traveller without any information about what may occur in the network is, in most circumstances, unrealistic. It is worth pointing out though, that P1 does not cover two specific games also proposed in the literature: Szeto *et al.* (2007) discuss route choice if there are *n* uncoordinated demons. Schmöcker *et al.* (2009) discuss the case of "local demons", i.e. the fear of independent incidents at specific nodes in the network.

We illustrate our model with a small example network as well as the Chicago sketch network. Our results show the existence of the predicted limiting cases and a number of observations can be made: Firstly, with an increase in the number of feared link attacks the number of routes does not necessarily increase. Secondly, with good discernibility, i.e. understanding of the demon behaviour, the traveller focuses on a single route with one or more "back-up routes" that he might use with low probability. This is the case even if he fears that multiple incidents might occur. Thirdly, whereas a perceived change in demon attraction to some links only changes the size and probability of alternative routes being used, a change in the perceived general risk of link failure can change the entire link set being used by the traveller.

To our knowledge game theoretic routing has so far been seldom applied in practice and we believe that one reason is the lack of realism of the pure demon game. Recently there is though increasing interest in applying multi-path routing based on game theory to navigation systems and general traffic demand management (Ma *et al.*, 2012; Bell *et al.*, 2012). We hope that the game proposed here might help to encapsulate some of the behavioural perceptions of the risk-averse travellers better. For this clearly the parameters that describe the side-constraints of the P1 game as well as the potential losses would have to be estimated. This might be achievable partly through past data on incident statistics. The evaluation of such statistics as well as the demon fear will be person and situation specific though. To find the personalised route set the future routing device might hence ask a traveller some questions

to understand his/her willingness to take risks as well as whether he believes certain links in the network are safe before giving a route suggestion.

ACKNOWLEDGEMENTS

Sincere thanks to Michael Bell, Fumitaka Kurauchi and Satoshi Fujii for comments on earlier drafts of this paper.

REFERENCES

Akgün, V. Erkut, E. and Batta, R. (2000). On finding dissimilar paths. *European Journal of Operational Research*, 121, 232-246.

Bagnato, R. (1974). A Reinterpretation of Davenport's game theory analysis. *American Anthropologist*, 76, 65-66.

Batta, R. and Chiu, S.S. (1988). Optimal obnoxious paths on a network – transportation of hazardous materials. *Operations Research*, 36(1), 84-92.

Bell, M. G. H. (2000). A game theory approach to measuring the performance reliability of transport networks, *Transportation Research Part B*, 34, 533–545.

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

Bell, M. G. H. (2007). Mixed routing strategies for hazardous materials: Decision-making under complete uncertainty. *International Journal of Sustainable Transport*, 1(2), 133-142.

Bell, M. G. H. (2008). Hyperstar: A multi-path Astar algorithm for risk averse vehicle navigation. *Transportation Research Part B*, 43, 97-107.

Bell, M.G.H., Kanturska, U., Schmöcker, J.-D. and Fonzone, A. (2008). Attacker-Defender Models and Road Network Vulnerability. *Philosophical Transactions of the Royal Society A*, 366, 1893-1906.

Bell, M.G.H., Solmaz, H.H. and Fonzone, A. (2012). Dynamic risk-averse system optimal traffic assignment, Submitted for Publication at the 20th ISTTT.

Berdica, K. (2002). An introduction to road vulnerability: what has been done, is done and should be done. *Transport Policy* 9, 117-127.

Binmark, K. (2008). Rational decisions. Princeton University Press.

Chorus, C.G. (2012) Regret theory-based route choices and traffic equilibria. *Transportmetrica*, 8(4), 1-15.

Davenport, W.C. (1960) Jamaican fishing: A game theory analysis. In Rouse, I. (ed.) Papers in Caribbean Anthropology, 59, 3-11, Yale University Press.

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 Iida, Y. and Bell, M.G.H. (eds.) *The Network Reliability of Transport*. Elsevier, Oxford, 23-44.

Erkut, E. and Ingolfsson, A. (2000). Catastophe avoidance models for hazardous materials route planning. *Transportation Science*, 34(2), 165-179.

Fonzone, A., Schmöcker, J.-D., Ma, J.S. and Fukuda, D. (2012). Link-based Route Choice Considering Risk Aversion and Regret. *Transportation Research Record*, 2322, 119-128.

Frank, W. C., Thill, J.-C. and Batta, R. (2000). A Decision Support System for hazardous material truck routing. *Transportation Research Part C*, 8, 337-359.

Gilboa, I. (2010). *Rational Choice*. The Massachusetts Institute of Technology Press.

Glickman, T.S., Erkut, E. and Zschocke, M.S. (2007). The cost and risk impacts of

re-routing railroad shipments of hazardous materials. *Accident Analysis and Prevention* 39, 1015-1025.

Jelenius, E. and Mattsson, L.-G. (2012). Road network vulnerability analysis of area-covering disruptions: A grid-based approach with case study. *Transportation Research Part A*, 46(5), 746-760.

Kozelka, R. (1969) A Bayesian Approach to Jamaican fishing. In Buchler and Nutini (eds): *Game Theory in the Behavioral Sciences*. University of Pittsburgh Press.

Hillier, F.S. and Lieberman, G.J. (1990) Introduction to Operations Research. McGraw Hill.

Ma, J.S., Fukuda, D. and Schmöcker, J.-D. (In press). Faster hyperpath generating algorithms for vehicle navigation. *Transportmetrica A*, 9(10), 925-948.

Milnor, J.W. (1951) Games against nature. Rand Research Memorandum. Available from <http://www.rand.org/pubs/research_memoranda/RM0679/> . Accessed Sept. 2010.

Nicholson, A., Schmöcker, J.-D., Bell, M.G.H. and Iida, Y. (2003). Assessing Transport Reliability: Malevolence and User Knowledge, In M.G.H. Bell and Y.Iida (eds): *The Network Reliability of Transport*. Pergamon, 1-22.Read, D.W. and Read, C.E. (1970). A Critique of Davenport's game theory analysis. *American Anthropologist*, 72, 351-355.

Savage, L.J. (1954). *The Foundations of Statistics*, Wiley.

Straffin, P.D. (1993). *Game Theory and Strategy*. The Mathematical Association of America. New Mathematical Library, 24-27 and 56-61.

Taylor, M.A.P and D'Este, G.M. (2007). Transport network vulnerability: A method for diagnosis of critical locations in transport infrastructure systems. In Murray, A.T. and Grubesic, T.H. (eds.) *Critical Infrastructure: Reliability and Vulnerability*. Springer-Verlag, New York, 9-30.

Schmöcker, J.-D. (2010) On Decision Principles for Routing Strategies Under Various Types of Risks. In Bell, M.G.H., Hosseinloo, S.H. and Kanturska, U. (eds): *Security and Environmental Sustainability of Multimodal Transport*. NATO Science for Peace and Security Series – C: Environmental Security. Springer, Dordrecht, The Netherlands, 57-72.

Schmöcker, J-D., Bell, M.G.H., Kurauchi, F. and Shimamoto, H. (2009). A game theoretic approach to the determination of hyperpaths in transportation networks. Proceedings of the *18th International Symposium on Transportation and Traffic Theory* (ISTTT), Hong Kong, July 2009.

Spiess, H. and Florian, M. (1989). Optimal strategies: A new assignment model for transit networks, *Transportation Research Part B*, 23(2), 83-102.

Szeto, W. Y., O'Brien, L., O'Mahony, M.(2007). Generalisation of the risk-averse traffic assignment, Proceedings of the *17th International Symposium on Transportation and Traffic Theory (ISTTT)*, Elsevier: Oxford, 127-155.

Wald, A. (1950). *Statistical Decision Functions*. Wiley.

Zhang, H. and Maloney, L.T. (2012) Ubiquitous log odds: A common representation of probability and frequency distortion in perception, action, and cognition. Hypothesis and Theory Article. *Frontiers in Neuroscience*, 6, 1-14.