Optimal routing against ambushes: a first approach

Roy Lindelauf[1]

NL-ARMS, 2009, 179-196

Introduction

The Israeli Defense Force (IDF) encountered numerous problems during the invasion of southern Lebanon in 2006. Division 162, for instance, experienced serious difficulties while approaching the village of Ghandouriyeh.[2] Even though multiple axes of approach were available the IDF took the route along Wadi Saluki (other possibilities were to approach either from the south or north). Hezbollah launched a successful ambush resulting in the death of several IDF soldiers.[3] This action stands as an example of IDF's failure to obtain accurate tactical ground intelligence during this conflict.[4] Ambushes, raids and IED attacks have been, and still are, tactics most often employed by irregular fighters.[5] Counter-measures consist of physical protection of men and materiel, and methods to detect, predict and neutralise possible attacks.[6] Game theory, the mathematical analysis of the strategic interaction between actors, offers a coherent analytical framework that can be used to systematically analyse problems related to counter-insurgency.[7] In addition, it offers a framework that helps understand the influence of assumptions on outcomes of an analytical process.[8] Game theory has been used extensively in modeling military operations as well as in modeling problems of a more strategic nature.[9] We argue that game theory can also be useful in predicting and preventing attacks with improvised explosive devices by reducing the predictability of traffic patterns.

The goal of this chapter is to present an analytical framework that can be used to optimise routing schemes, knowing that the enemy employs ambushes and IED attacks. This will be done by considering the possible strategies each player in this `ambush game' can employ. Simply put, one player has to choose among the possible routes between a source and destination, and the other player has to choose the location of an attack. Game theory is perfectly equipped to analyse such strategic interactions.

Clearly, mathematical modeling always comes at the cost of making simplifying assumptions. We recognise that other considerations also play a role in deciding what route to take (such as geography, available time, etc.). However, a game-theoretical approach can certainly aid in maximizing the unpredictability of routing schemes, consequently minimizing the expected loss to allied forces.

The layout of this chapter is as follows. A game-theoretical model that captures the strategic interaction between the player that conducts the ambush and the player that moves from source to destination on risk-homogeneous networks will be introduced first. Next, a discussion on approximating the risk of an attack on edges in the network will be presented. Finally, optimal routing on heterogeneous networks will be presented in the last section.

Optimal routing on risk-homogeneous networks

In the remainder of this chapter the player that conducts the ambush will be called `Red', and the other player will be called `Blue'. The following restrictions can be made to simplify the analysis:

1. Red conducts exactly one ambush each iteration.
2. Red conducts exactly k ambushes each iteration.
3. Red knows the source and destination of the Blue forces.
4. Red knows the probability distribution of Blue's source and destination.
5. The edges in the network are risk-homogeneous.
6. The edges in the network are risk-heterogeneous.
7. Blue does not have data on possible ambush locations.
8. Blue has several sources and destinations in the network.

Multiple extensions of the above-mentioned restrictions are possible. In this chapter we will present an analysis of the case that Red conducts one ambush and is aware of Blue's source and destination in the network. Next, we will extend the analysis by giving Red the option to conduct several ambushes. This section will be concerned with networks in which the edges are considered to be homogenous with respect to risk. The heterogeneous case will be dealt with in later sections. More complex situations are subject of future research.

A homogeneous network is a network in which the risk of an attack at an edge in the network is equal over all edges. We assume that during each iteration Blue will move from source to destination and that Red conducts an ambush. Consider the following example.

Example 1

Suppose Blue has to move regularly from source S to destination T, see figure 1.

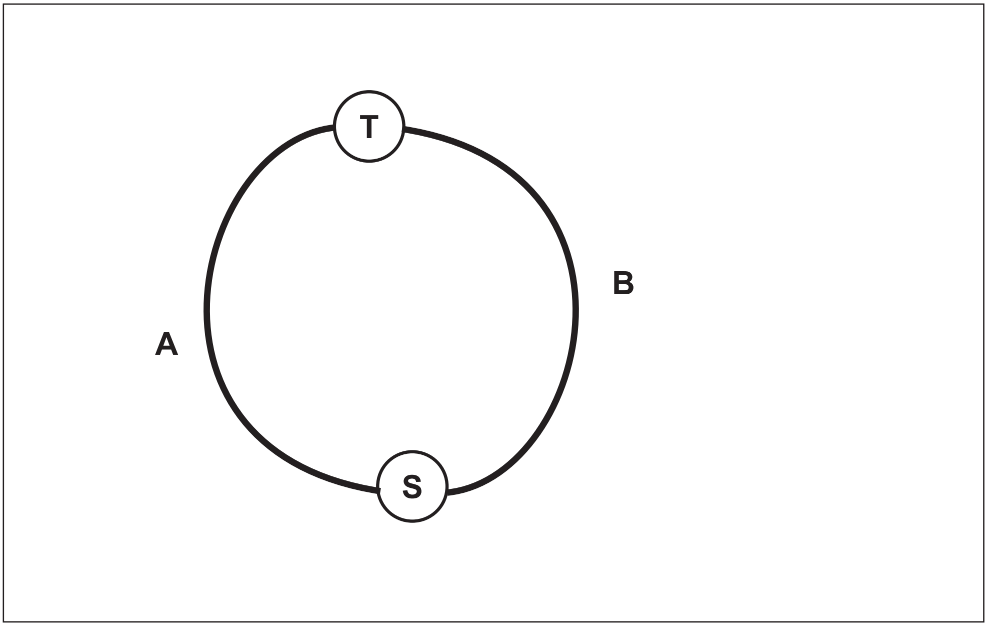

Figure 1: A simplified transportation network

To do this Blue has two options at his disposal, route A and route B. How should Blue assign his routing scheme?

Case 1

Assume that both edges in the network are homogeneous with respect to the risk of an ambush. We will show that the choice of either route A or B according to the flip of a coin minimises the maximum number of *expected* encounters with IED's. To do this, assume without loss of generality that Blue chooses route A with probability *p* and hence route B with probability *1-p*. Also note that Blue is not aware of the location of Red's ambush (IED). If Red plans the ambush at route A and Blue chooses to use route A, it follows that Red `wins' 1 convoy. If Red plans to ambush at route B and Blue chooses route A, then Red `wins' nothing. We model this strategic interaction as a two person zero-sum game, i.e., whatever Red's gains equals Blue's losses. The expected payoff of this game in case of an ambush at route A and Blue choosing a mixed strategy (p,1-p) equals $p \cdot 1 + (1-p) \cdot 0 = p$. In case of Red conducting an ambush at edge B the expected payoff to Blue equals $p \cdot 0 + (1-p) \cdot 1 = 1-p$. Clearly, Blue will adopt that strategy (a value for *p*) such that the expected number of encountered ambushes will be minimised. Since Blue does not know the location of Red's ambush it can be argued that adopting a strategy that minimises the maximum expected payoff is preferable. Hence, Blue will choose a value of *p* such that $\max\{p, 1-p\}$ is minimal. Therefore, Blue will choose $p = {}^{1}/_{2}$. This strategy corresponds to Blue tossing a fair coin each time he has to move from his source S to his destination T. In case of Heads he will move along route A and in case of tails he will move along route B.

Clearly the previous analysis consists of an oversimplified transportation network because Blue only had two options available in transporting from A to B. In reality this network can be more complex. Therefore, we generalise the previous example.

Case 2

Consider the following transportation network, see figure 2.

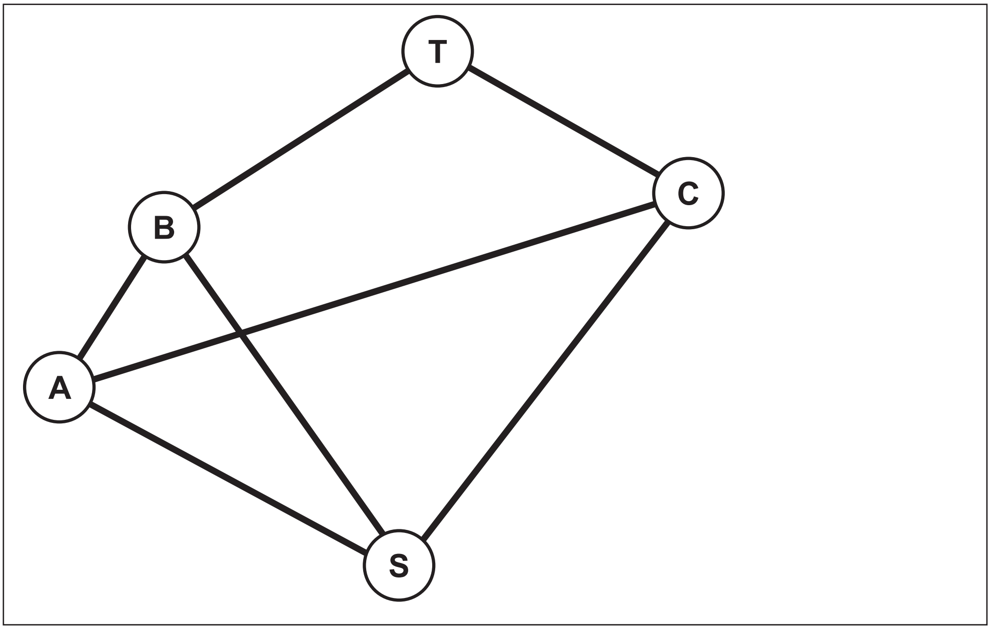

Figure 2: A transportation network between S and T

Assume Blue has to move from S to T regularly. We determine the payoff for each strategy combination of Red and Blue and present the resulting information in table 1.

	SBT	SCT	SABT	SACT	SCABT
SA	0	0	1	1	0
SB	1	0	0	0	0
SC	0	1	0	0	1
AB	0	0	1	0	1
AC	0	0	0	1	1
BT	1	0	1	0	1
CT	0	1	0	1	0

Table 1: Strategic payoff (encounter: 1, no encounter: 0) corresponding to each choice of strategy for Blue and Red.

Table 1 should be read as follows. Each row corresponds to the options available to Red (the location of a possible ambush) and the columns correspond with the options (routes) available to Blue. For instance, in case of Red planning an ambush at the edge indicated by ‘CT’, he will encounter Blue if he either chooses route ‘SCT’ or route ‘SACT’. Clearly, Red wants to maximise the possible number of encounters with Blue. On the other hand, Blue wants to minimise his number of encounters with Red.

We introduce the concept of domination to analyse this situation. A pure strategy ‘A’ is *dominated* by another pure strategy 'B’ if and only if the payoff corresponding to option ‘B’ is always equal to or better than option ‘A’, irrespective of one’s opponent strategy. A pure strategy that is dominated will never be an option to a rational player, simply because he has a better strategy available, irrespective of his opponent’s choice. Looking at the payoffs in table 1 it can be seen that pure strategy ‘BT’ dominates pure strategy ‘AB’. In addition, it can be seen that option ‘BT’ also dominates ‘SB’. The game can therefore be simplified by removing these pure strategy options from the table, resulting in table 2. Note that intuitively this is also clear: if Blue transported over SB or AB he would have to choose BT next to end up in T. Locating the ambush at BT always ensures Red of encountering Blue in these cases.

	SBT	SCT	SABT	SACT	SCABT
SA	0	0	1	1	0
SC	0	1	0	0	1
AC	0	0	0	1	1
BT	1	0	1	0	1
CT	0	1	0	1	0

Table 2

In a similar fashion we analyse the options available to Blue. It can be seen that his pure strategy ‘SBT’ dominates ‘SABT’ and ‘SCABT’. Taking these considerations into account yields table 3.

	SBT	SCT	SACT
SA	0	0	1
SC	0	1	0
AC	0	0	1
BT	1	0	0
CT	0	1	1

Table 3

Due to the elimination of Blue’s dominated strategies it becomes possible to restrict the rational options to Red once more. Analysing table 3, it can be seen that option ‘CT’ dominates ‘SA’, ‘SC’ and ‘AC’, resulting in:

	SBT	SCT	SACT
BT	1	0	0
CT	0	1	1

Table 4

Table 4 cannot be reduced any further using the concept of dominance. Assume that Blue adopts the strategy $(p, q, 1\text{-}p\text{-}q)$, i.e, Blue chooses route SBT with probability p, route SCT with probability q and hence route SACT with probability $1\text{-}p\text{-}q$. This yields an expected payoff of p against Red’s first option, and a payoff of $q+1\text{-}p\text{-}q=1\text{-}p$ against Red’s second option. Hence, Blue’s optimal strategy consists of choosing either route SBT *or* routes SCT and SACT according to the flip of a coin, where it does not matter how he chooses between SCT and SACT (his choice of q does not affect the outcomes against either of Red’s strategies). In addition, Red will decide to ambush BT or CT according to the flip of a coin.

The previous situations consisted of Red being able to conduct exactly *one* ambush (IED attack). We will extend this analysis by allowing Red to be able to conduct more than one ambush attack.

Example 2:

Assume that Blue's transportation network can be simplified as shown in figure 3.

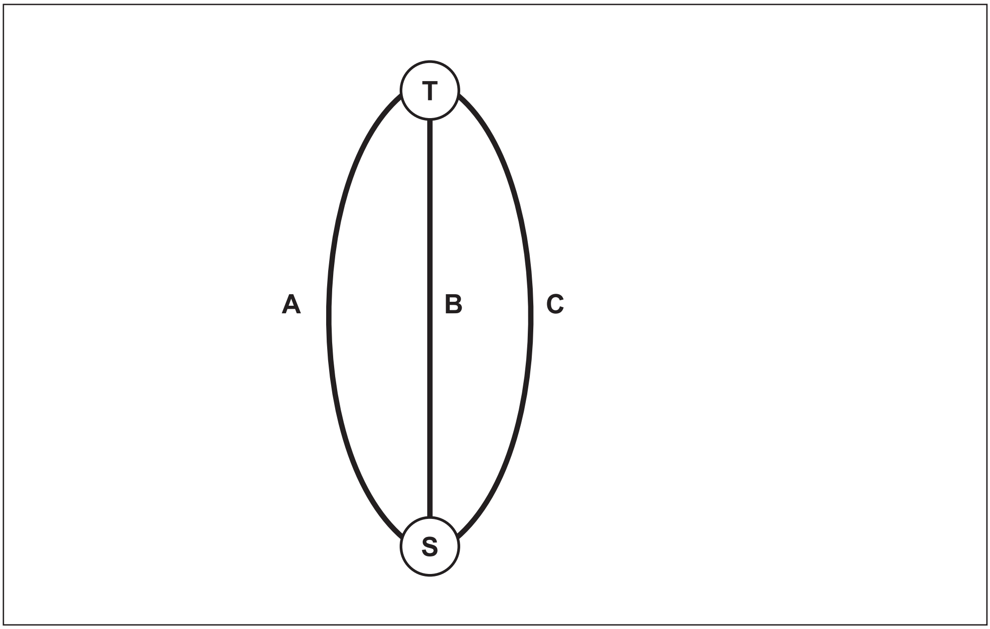

Figure 3: A simple transportation network between source S and destination T

In addition, assume that Red can conduct two ambushes. We present all possible combinations of strategy in table 5:

	A	B	C
A:2	2	0	0
B:2	0	2	0
C:2	0	0	2
A:1, B:1	1	1	0
A:1, C:1	1	0	1
B:1, C:1	0	1	1
A:2	2	0	0

Table 5

Table 5 presents the number of encounters between Blue and Red for each possible strategy combination. For instance, if Red conducts two ambushes along edge A (and consequently zero at B and C), and Blue chooses to use route A, it follows that there will be two encounters. A similar analysis as done in the previous section (using software package MAPLE) yields the following optimal (maximin) strategies:

1. Red chooses uniformly over options A:2, B:2, C:2.
2. Blue chooses uniformly over his three options.

Thus, it can be seen that the game-theoretical analysis can easily be extended to cases of multiple possible ambushes by use of software packages.

Estimating risk-heterogeneity

It can be argued that the assumption of network homogeneity with respect to risk is too restrictive. After all, some edges in the network are 'more dangerous' than others. The probability of attack at some locations may be assumed to be higher than at others. A network is called risk-heterogeneous if the likelihood of an attack is not distributed uniformly over its edges. The first step in determining an optimal routing strategy along such a heterogeneous network is the estimation of the risk of attack at each edge. Risk is clearly an abstract concept and the critic will argue that it is difficult to quantify. However, when choosing a routing scheme, in practice one already intuitively uses the concept of risk: after all, there is a tendency to choose that route that minimises the probability of attack. Instinctively, one avoids routes along which attacks often take place, or are `likely' to occur.

An extremely simple method of attributing risk to edges is by setting the likelihood of an attack to occur at a certain edge equal to the fraction of successful attacks on that edge. Intuitively, this is a good initial approach and the complexity of this method is nil.

Of course it is also possible to develop more elaborate analyses. Amongst others, this can be done with the help of expert data, statistical analyses and graph-theoretical analyses. When there are no historical data with regard to attacks it is possible to attribute risks to edges based on centrality principles commonly used in mathematical network analysis. If there is data available on previous attacks, it will be possible to attribute risks by use of point pattern analysis.[10] Here, we will give an initial illustrative discussion of several graph-theoretical methods useful in attributing risk to edges.

Centrality

If no data concerning previous attacks is available, other methods must be developed in order to attribute risks to edges in the network. Intuitively, edges in the network that are near major traffic junctions pose a higher risk, simply because these are assumed to be Red's most likely locations for locating roadside bombs (red assessing the probabilities of a transport passing there the highest).

It suffices to say that there are many ways of determining central nodes in a network.[11] With regard to transport over a network the 'betweenness-centrality' is an important centrality measure, as it attributes a value to a node which reflects its importance with regard to the exchange of information (transport) in the network. Calculating the centrality index of each node in the network and attributing a risk value to an edge by taking the sum of the values of its end nodes, seems to be a good starting point. Let $g = (V, E)$ indicate the network, with source $s \in V$ and destination $t \in V$. The amount of 's-t betweenness' of node $i \in V$ equals the fraction of shortest paths between s and t that node *i* occupies. We present an educative example:

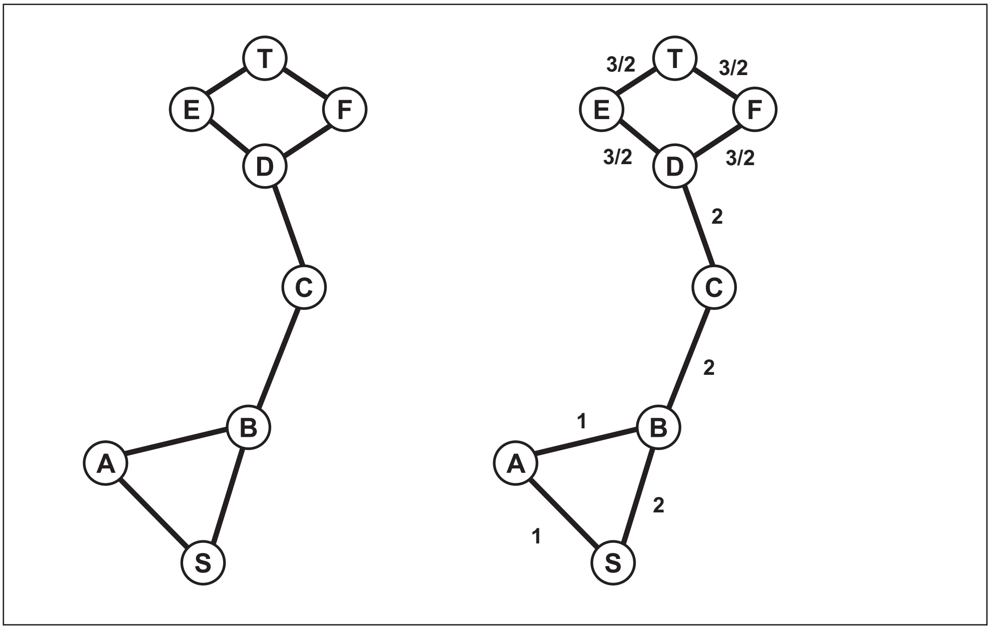

Figure 4: Example of 'betweenness centrality' (Left) and attribution of risks (Right)

Consider the network given in figure 4, with source S and destination T. Clearly, it can be seen that there are two shortest paths between S and T (SBCDET, SBCDFT). The nodes B, C and D are elements in both paths and hence score a betweenness centrality value of 1, i.e., $c_B = c_C = c_D = 1$. Node A does not occupy any shortest S-T path, hence $c_A = 0$. Similarly we obtain $c_E = c_F = {}^1/_2$. Since the source of the transport equals 'S' and the destination 'T' we let $c_S = c_T = 1$. Next, we attribute risk to each edge in the network by taking the sum of the centrality measures adjacent to the respective edge. The resulting network, including risk attributed to the edges is given in figure 4 Right. It can be seen that the results correspond to intuition: the highest risk is attributed to edges BC and CD and lowest to edge AS. This method can easily be implemented in standard software and hence complement standard network analysis in optimizing routing schemes.

'Chokepoints'

Another method to assign risk to edges is to determine those edges in the network that are critical in the connectivity of the network. For instance, Blue, in transporting from a source to a destination, will have certain edges in the network that he cannot avoid. Locating an ambush at such an edge seems profitable to Red. To determine such chokepoints in transporting between source S and destination T can easily be done by the graph theoretical concept of connectivity. This boils down to determining the minimum number of edges in the network, when omitted, disconnects source S from destination T. Such a cut is also called an S-T cut. We attribute a value to an edge by determining the minimum capacity of all S-T cuts that this respective edge occupies. The higher this value, the more alternatives are available in the S-T path with respect to this edge. Hence, the value of risk attributed to this edge equals 1 over this minimum capacity (the more alternatives available the lower the risk). We illustrate such a chokepoint analysis by an example.

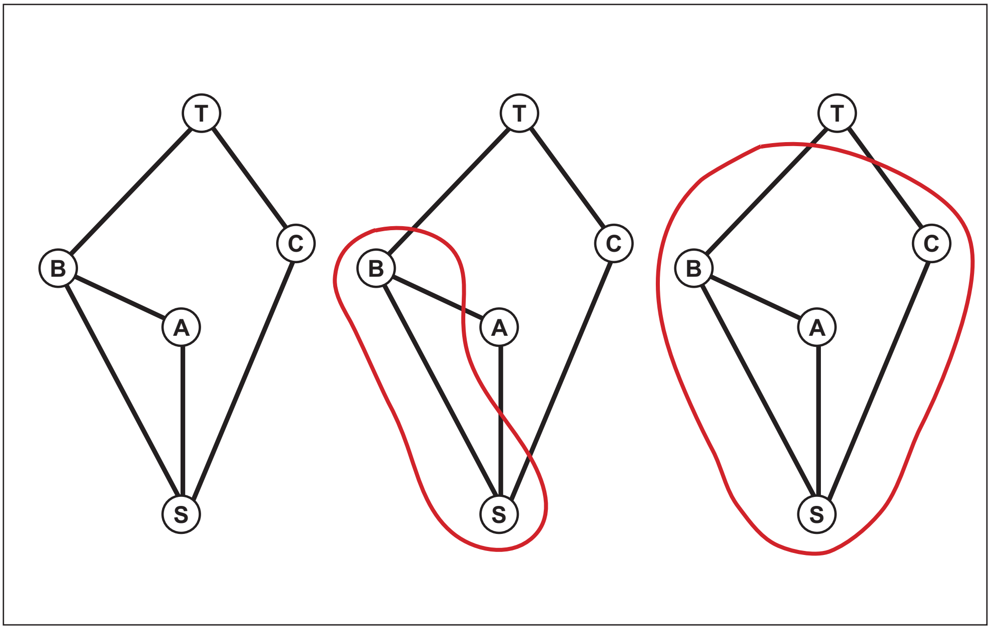

Figure 5: routing network (Left), with cut SB (Middle) and cut SABC (Right)

In Figure 5 two S-T cuts are presented: cut SB and cut SABC. Consider edge BT. Clearly this edge is a member of both S-T cut sets SB and SABC. All possible cut sets corresponding to S-T cuts containing BT are: SB(4), SAB(2), SABC(2) and SBC(6). The minimum number of edges that have to be cut (including BT) to isolate S from T equals 2. Hence, the corresponding risk attributed to edge BT equals ½. A similar analysis in case of edge SA shows that its risk equals $^1/_3$, as expected lower than that of BT.

Optimal routing on risk-heterogeneous networks

The preceding sections have shown that with the help of game theory it is possible to optimise routing schemes on risk homogenous networks. In addition, two methods of assigning risks to edges have been briefly discussed. Below, an analysis will be presented of optimal route allocation in case of such risk heterogeneous networks. This is done by using an example in which it is assumed that data on previous attacks is available.

Example:

Consider the simple network as presented in the first section, example 1. Assume that blue has the following data:

1. On route A 100 transports have taken place, against which 5 attacks have been committed.
2. On route B 200 transports have taken place, against which 2 attacks have been committed.

The risk of a successful attack on route A is therefore estimated at 5% (5/100) and the risk of a successful attack on route B at 1% (2/200). A naive routing scheme for blue would consist of always taking that route that has the lowest risk of attack, in this case route B. However, Red, aware of this reasoning, will always ambush route B. If Blue extends his reasoning by taking Red's deliberations into account, he will always pick route A. A game-theoretic analysis can easily break this kind of circular reasoning. Such a simple two-person zero-sum game is solved again in terms of minimax and maximin strategies.[12] It is customary to define a pay-off matrix, in which the rows correspond to the pure strategies of player I (Red, who wants to maximise the number of 'hits') and the columns with the pure strategies of player II (Blue, who wants to minimise), as we have already demonstrated using tables in the previous sections. The ensuing pay-off matrix is as follows,

$$H = \begin{bmatrix} 5 & 0 \\ 0 & 1 \end{bmatrix}$$

Consider the payoff in the first row and first column: 5. This equals the number of expected 'hits' if the ambush is located on route A (first row) and the transport goes along route A (first column), i.e., 100*0.05 = 5. Therefore, it can be argued that the risk on this edge in the network equals 5, bearing in mind that there are more ways of determining such a risk. In a similar way, if the ambush is placed on route A and the transport goes along route B, the transport will reach its target safely. Given this matrix, the optimal strategy for blue can be determined similarly to that in the previous sections. Blue's optimal strategy consists of transporting over route A with probability 1/6 and over B with probability 5/6. The expected number of losses equals 5/6. If blue were to take another strategy, for instance, according to the flip of a coin, it can be seen that the expected number of losses could be even lower (a half if Red chooses to ambush B) but also higher: 2.5 if red chooses A. Since blue does not know red's choice of strategy he best opts for the 1/6 probability A strategy, this *guarantees* a maximum number of losses of 5/6, irrespective of red's strategy! It is also easy to show that Red's optimal strategy equals: with probability $^1/_6$ ambush route A and with probability $^5/_6$ ambush route B.

We assumed that Blue will choose a routing scheme taking historical data on attacks into account, and consequently that Red will take this also into account. Red cannot predict the route Blue will pick, but he can assume that Blue will allocate his routes based on historic trends. Therefore, Red's goal is to attain a payoff as high as possible against Blue. The strength of the optimal strategy based on minimax principles is that a deviation of Red from his optimal strategy will only benefit Blue.

In reality optimal route allocation is not as easy as the above example suggests. After all, the transport takes place along a network of roads and the number of possible routes will increase drastically with the number of routes in the network. As was shown above, the method employed can be generalised fairly easily. Determining the optimal strategy in a two-person zero-sum game setting does not depend on the number of (finite) strategies. In practice, however, one resorts to computer simulation as computations become cumbersome. In addition, it must be remarked that the method can be made more user-friendly by implementing it in software. In principle, the analyst only needs to make the choice of network to analyse and attribute risks to edges (this could be done for instance by attributing a scale of 1 to 10 for risk to each side of by automating some of the above-mentioned methods).

Therefore, in general, consider a route map as given. In other words, blue has a network and he knows what the source and destination of the transport are. Such a network can easily be converted into a mathematical graph, see figure 6 for an illustration. A mathematical graph is nothing more than a set of dots and lines: a dot corresponds to a node in reality and a line to an edge between the respective junctions. Such a graph is presented as $g = (V,E)$, where V is the set of nodes and E the set of edges.

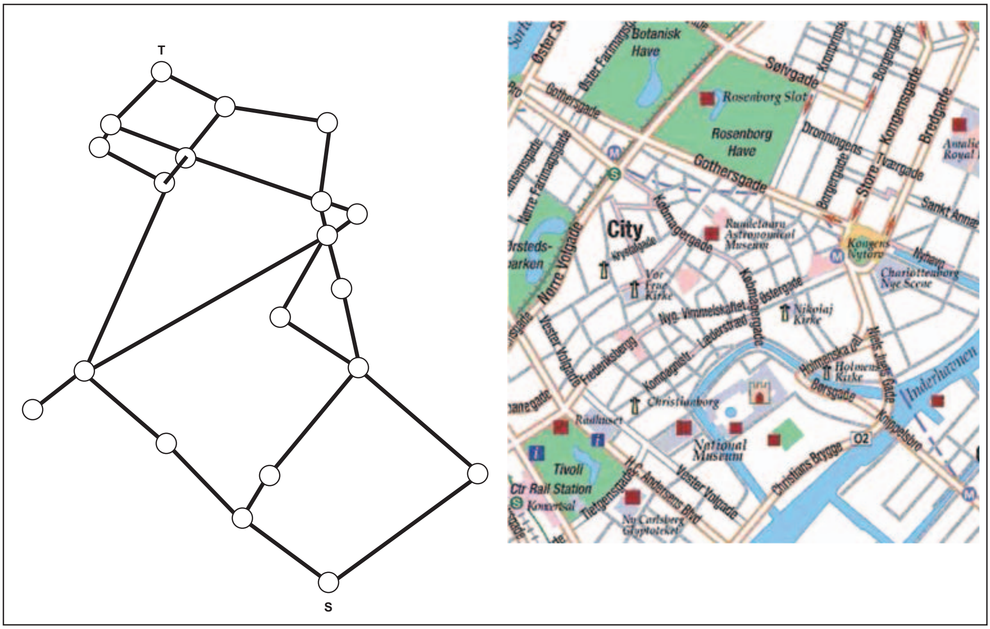

Figure 6: a mathematical graph (left) representing a routing network (right)

In addition, there is information with regard to the risk of attacks corresponding to each edge in the network. Such information might be available from a point pattern analysis, a centrality analysis, expert information or a combination of all three. This information is modelled using a function that attributes weights to the edges. For instance, denote this function by $w : E \rightarrow (\ 1, \infty\ )$. Hence $w_{ij} > w_{kl},\ ij,\ kl \in E$ implies that the risk of a successful attack on edge *ij* is greater than on edge *kl*. This risk depends on geographic circumstances, the condition of the roads, et cetera, as discussed above. Given this network with weights assigned to the edges, the question remains how to rationally determine unpredictable routing schemes. A first approach to the answer to this question has been given in the previous sections.

In principle, there is an infinite number of possible routes from source to target. Therefore, the restriction is imposed that each route must be a *path* in the network (not a single edge may occur more than once in a route).

A routing scheme consists of multiple edges risk weights w_{ij} attributed to each edge. Blue’s pure strategies consist of paths (from source to target) and red’s pure strategies correspond to edges where ambushes will take place.

Next we extend our example even more, see figure 7. Assume blue has the following route network for movement from location S to location *T*.

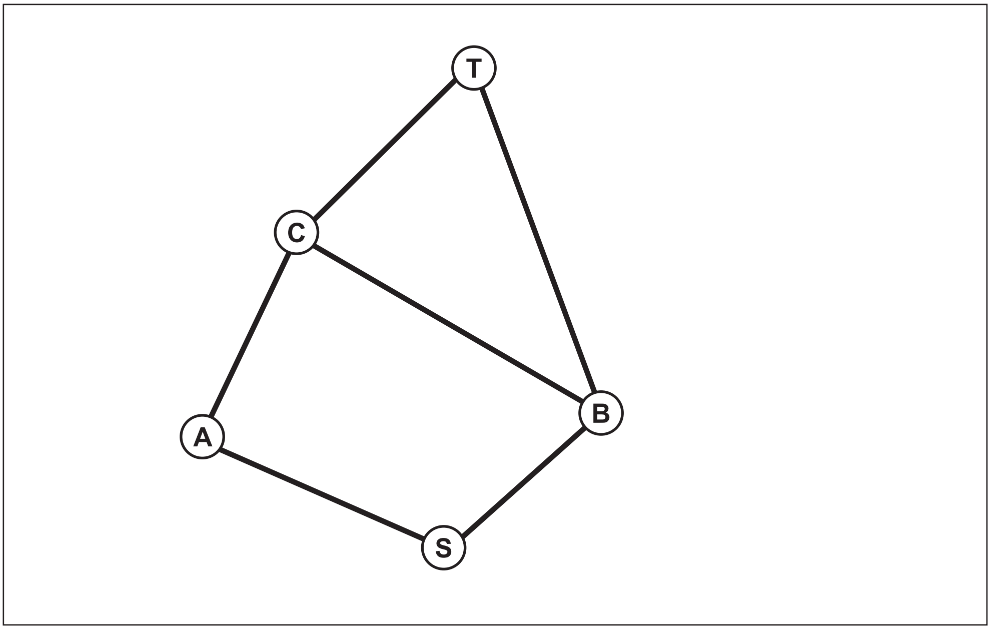

Figure 7: Routing network between source (S) and destination (T).

Clearly, there are four possible paths between source S and destination T, i.e., SACT, SACBT, SBT and SBCT. Notice, for instance, that SACBSACT is not a path because several edges (AC) occur more than once. In addition, assume that Blue has data available on previous transportations and attacks see table 6. We assign risk values to each edge corresponding to the fraction of attacks that occurred on the respective edge.

	Nr. of times passed	Nr. of attacks
AS	160	10
SB	48	9
AC	32	10
CB	48	6
CT	32	2
BT	4	1

Table 6

Compare edge AS and edge AC. The risk attributed to edge AS is set equal to $^1/_{16}$, this because of all 160 times this edge was traversed 10 attacks occurred. The risk attributed to edge AC equals $^5/_{16}$, i.e., of all 32 passages there have been 10 attacks. Assigning risks to all edges in a similar way, and normalising, we end up with risks as shown in figure 8.

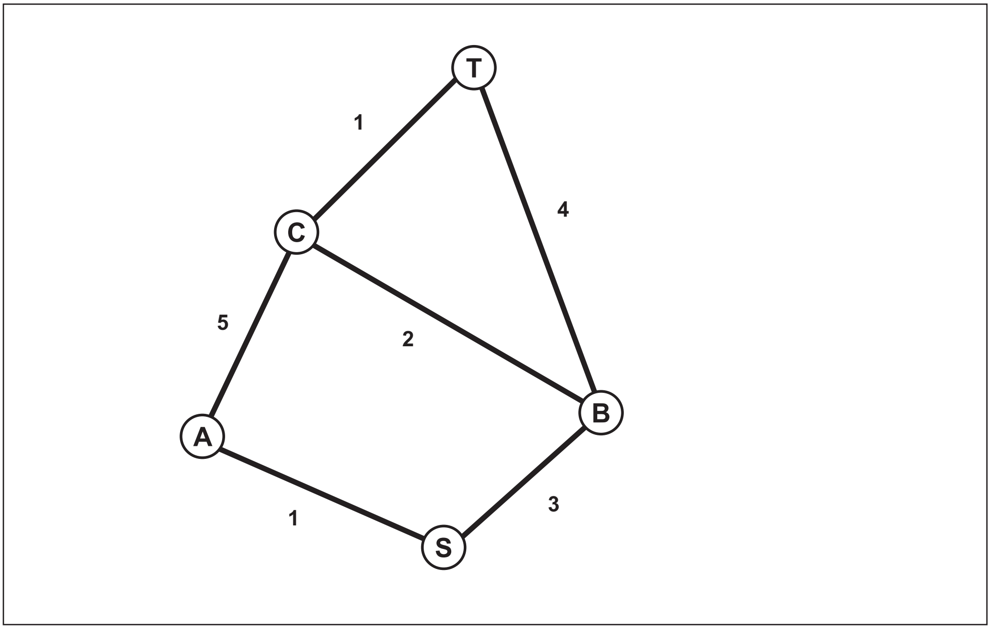

Figure 8: Network with risks attributed to the edges.

Red's mixed strategy consists of choosing a probability distribution over all edges where ambushes can be placed. Blue's mixed strategy consists of a probability distribution over all possible routes. We present all possible strategy combinations in table 7.

	SACT	SACBT	SBCT	SBT
AS	1	1	0	0
SB	0	0	3	3
AC	5	5	0	0
CB	0	2	2	0
CT	1	0	1	0
BT	0	4	0	4

Table 7.

We analyse this game using two person zero-sum game theory using the software tool MAPLE to solve this linear optimisation problem. It follows that red's optimal strategy equals $(p_{SA}, p_{SB}, p_{AC}, p_{BC}, p_{CT}, p_{BT} = (0, {}^{5}/_{8}, {}^{3}/_{8}, 0, 0, 0)$. The expected payoff equals $\frac{{}^{15}/_{8}}{16} = {}^{15}/_{128}$. Thus red ambushes SB with probability ${}^{5}/_{8}$ and AC with probability ${}^{3}/_{8}$. Another interpretation can be that red distributes his capacity optimally with ${}^{5}/_{8}$ over SB and ${}^{3}/_{8}$ over AC. Blue's optimal strategy equals $(p_{SACT}, p_{SACBT}, p_{SBCT}, p_{SBT}) = ({}^{5}/_{8}, 0, {}^{5}/_{32}, {}^{12}/_{32})$. Again we use the minimax principle: blue opts for that strategy that minimises the maximum expected loss.

Concluding remarks

Inspired by tactical problems that Israel experienced during the incursion into southern Lebanon in 2006, we presented an initial analysis of the optimal allocation of routes against ambush attacks. The methodology thus developed provides an analytical contribution to the prevention and prediction phase in dealing with the IED threat.

The strategic interaction between 'bomb layer' and 'transporter' was modelled as a two-person zero-sum game. The pure strategies for the bomb layer consist of choosing the edges in the network corresponding to ambush locations. The pure strategies available to the transporter consist of all possible routes between source and target. The situation in case of a single ambush was solved for a single source and target. It was also shown that the `multiple ambush' situation can be easily analysed with similar methods. Future research will focus on the multiple sources and targets case, although it must be remarked that the situation seems to be equivalent to multiple transports with one source and target.

In addition risk-heterogeneity of attacks on certain edges in the network was considered. Several methods to estimate these risks were presented. For instance, the probability of an attack on edge was approximated by the fraction of the convoys that encountered an attack. Besides, it was shown that it is possible to develop more complex methods based on graph theory (centrality and 'chokepoint').

Even though the importance of 'unpredictability' is stressed in the military operational literature, the idea of allocating routing schemes according to game-theoretical principles has not received widespread attention in the military community. The analysis in this chapter must therefore be considered as a first step towards the goal of minimizing the expected number of encounters with ambushes. The methods presented in this chapter are standard 'tools' in game theory. Since their implementation in software is straightforward, the operational analyst confronted with allocating routing schemes could greatly benefit from such software.

Notes

[1] R. (Roy) H.A. Lindelauf MSc is a researcher at the Military Operational Arts and Sciences section of the Netherlands Defence Academy and a PhD candidate at the department of Econometrics and Operations Research at Tilburg University.

[2] Cordesman, A.H. et al. (2007), *Lessons of the 2006 Israeli-Hezbollah War*, Washington, D.C: Center for Strategic and International Studies.

[3] Helmer, D. (2007), 'Not Quite Counterinsurgency: A Cautionary Tale for US Forces Based on Israel' Operation Change of Direction', *Armor*, Vol. CXVI(1), pp. 7-11.

[4] Bar-Joseph, U. (2007), 'Israel's Military Intelligence Performance in the Second Lebanon War', *International Journal of Intelligence and Counterintelligence* 20, pp. 583-601.

[5] Alagha, J.E. (2006), *The Shifts in Hizbullah's Ideology, Religious Ideology, Political Ideology, and Political Program*, Amsterdam: Amsterdam University Press; Litaker, E. (2005), 'Efforts to Counter the IED threat', *Marine Corps Gazette* 89(1), p. 29.

[6] Kuznetsov, A.V. and Osetrov, O.I. (2006), 'Detection of Improvised Explosives (IE) and Explosive Devices (IED)', *Detection and Disposal of Improvised Explosives*, NATO Security through Science Series - B: Physics and Biophysics, Springer.

[7] Perry, W.L. and Gordon, J. (2008), *Analytic Support to Intelligence in Counterinsurgencies*, Rand monograph, Rand institute.

[8] Luce, D.L., and Raiffa, H. (1985), *Games and Decisions, Introduction and Critical Survey*, New York: Johny Wiley & Sons.

[9] Aumann, R.J. and Maschler, M.B. (1995), *Repeated Games with Incomplete Information*, Massachusetts Institute of Technology; Hamilton, T. and Mesic, R. (2004), *A Simple Game-Theoretic Approach to Suppression of Enemy Defenses and Other Time Critical Target Analyses*, RAND research report DB-385-AF.

[10] Diggle, P.J. (1983), *Statistical Analysis of Spatial Point Patterns*, London: Academic Press; Stoyan, D. (1987), *Stochastic Geometry and its Applications*, New York: John Wiley & Sons.

[11] Brandes, U. and Erlebach, T. (eds.) (2005), *Network Analysis*, LNCS 3418, Berlin/Heidelberg: Springer.

[12] Luce and Raiffa, op. cit.