NPS-OR-10-007

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

The Effect of Decoys in IED Warfare

by

Kyle Y. Lin and Alan R. Washburn

September 2010

Approved for public release; distribution is unlimited

Prepared for: Joint IED Defeat Organization
5000 Army Pentagon, Washington, D.C. 20301-5000

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CA 93943-5001

Daniel T. Oliver
President

Leonard A. Ferrari
Executive Vice President and
Provost

This report was prepared for and funded by the Joint IED Defeat Organization, 5000 Army Pentagon, Washington, D.C. 20301-5000.

This report was prepared by:

KYLE Y. LIN
Associate Professor of
Operations Research

ALAN R. WASHBURN
Distinguished Professor Emeritus of
Operations Research

Reviewed by:

RONALD D. FRICKER
Associate Chairman for Research
Department of Operations Research

ROBERT F. DELL
Chairman
Department of Operations Research

Released by:

KARL VAN BIBBER
Vice President and
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE					*Form Approved* *OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**					
1. REPORT DATE *(DD-MM-YYYY)* 09-2010	**2. REPORT TYPE** Technical Report				**3. DATES COVERED** *(From - To)*
4. TITLE AND SUBTITLE The Effect of Decoys in IED Warfare					**5a. CONTRACT NUMBER**
					5b. GRANT NUMBER
					5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Kyle Y. Lin and Alan R. Washburn					**5d. PROJECT NUMBER**
					5e. TASK NUMBER
					5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000					**8. PERFORMING ORGANIZATION REPORT NUMBER** NPS-OR-10-007
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Joint IED Defeat Organization, 5000 Army Pentagon, Washington, D.C. 20301-5000					**10. SPONSOR/MONITOR'S ACRONYM(S)**
					11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited					
13. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.					
14. ABSTRACT This report examines two forms of decoy that may arise in warfare involving improvised explosive devices (IEDs). The first is a fake IED, which costs less than a real IED and wastes the time of route-clearing patrols that investigate it. The second is an understaffed surveillance tower, which may provide some deterrence to insurgent activities, as from the outside the tower appears to be fully operational. For each form of decoy, we formulate mathematical models to study the optimal strategies for both the insurgents and the government forces. We use numerical examples to demonstrate our models, and to point out the situations when these decoys may play a significant role in IED warfare.					
15. SUBJECT TERMS IED, decoy, game theory, red teaming					
16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	UU	38	**19b. TELEPHONE NUMBER** *(include area code)*

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This report examines two forms of decoy that may arise in warfare involving improvised explosive devices (IEDs). The first is a fake IED, which costs less than a real IED and wastes the time of route-clearing patrols that investigate it. The second is an understaffed surveillance tower, which may provide some deterrence to insurgent activities, as from the outside the tower appears to be fully operational. For each form of decoy, we formulate mathematical models to study the optimal strategies for both the insurgents and the government forces. We use numerical examples to demonstrate our models, and to point out the situations when these decoys may play a significant role in IED warfare.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

The authors thank Che Shiung Lin for conducting the numerical experiments in Section 3.5.

THIS PAGE INTENTIONALLY LEFT BLANK

1. INTRODUCTION

Our subject is prolonged warfare involving Improvised Explosive Devices (IEDs). There are two sides, Blue and Red, with Blue (usually government forces) trying to maintain regional stability and Red (usually insurgents) using IEDs to disrupt and undermine Blue's effort. This report examines two forms of decoy that may arise in IED warfare. The first is the use of fake IEDs by Red in order to delay Blue's route clearance patrols, and the second is the use of understaffed surveillance towers by Blue to deter Red's IED attacks.

Although decoys are widely used and can, at times, be very effective, there is surprisingly little academic research to mathematically analyze their effectiveness in combat models. Hershaft (1968) analyzed how imperfect decoys affect the survival probability, and Lu, Yang, and Yang (2008) conducted a cost benefit analysis. Washburn (2005) has studied the effects of decoys in decreasing the effectiveness of antiballistic missiles. In search theory, there are studies on imperfect classification of targets (false positive and false negative); for example, see Stone (2004) and Kress, Lin, and Szechtman (2008). However, the false positive is technically not a result of decoys, because the neutral targets are random noise in the field, as opposed to fake targets deployed purposely to mislead the opponent. All these earlier works focus on single-person decision models by assuming one can predict the enemy's behavior.

In this report, we use mathematical models to analyze two forms of decoy that may arise in IED warfare. In Section 2, we investigate Red's potential use of objects that appear to be IEDs, but which are actually nonfunctional fakes. Red's idea is that Blue's IED clearance forces will be delayed just as much by a fake IED as by a real one, and that fake IEDs are much easier to produce and deploy. We consider questions of how Red's fake and real IEDs and Blue's clearance forces should be allocated to a network of roads, with Blue's object being to minimize the total rate at which IEDs cause damage. We find an algorithm for optimizing Blue's allocations in the face of known Red tactics, and suggest how it might be employed in a long contest, where Blue is given a sequence of opportunities to adjust his allocations. We also consider the cost/effectiveness question from Red's standpoint. Qualitatively speaking, we find that Red's use of fakes should either be null or large, with intermediate usage being unattractive from his standpoint. Thus, while systematic use of fake IEDs has not been observed so far in either Iraq or Afghanistan, the United States and its allies should remain alert to the possibility of suddenly encountering them in numbers large enough to strongly affect the efficiency of route clearance efforts.

In Section 3, we consider a situation where Blue sets up two surveillance towers in two different locations, but does not have enough manpower to staff both towers. Although an understaffed surveillance tower has poor detection capability, it may still be able to deter Red's insurgent activities, as long as Red does not know that the tower is understaffed. We assume that Red gets a reward for each undetected attack, but incurs a penalty for each detected one. Blue's goal is to maintain peace and ideally to eliminate Red's attacks altogether, so a detected attack is bad, while an undetected attack is worse. We study whether Blue can lower the region's insurgent activities by switching its manpower between the two towers in a random manner. We formulate the problem as a two-person, non-zero-sum game. Qualitatively speaking, we find that a dynamic allocation strategy is useful to Blue, unless Red's penalty for a detected attack is small and Blue's penalty for an undetected attack is huge. As the Ground-Based Operational Surveillance Systems are being deployed to Iraq and Afghanistan, our findings may provide some guidance on how to operate these systems when the number of trained operators is limited.

2. FAKE IMPROVISED EXPLOSIVE DEVICES

Antitank mines are expensive, dangerous, and heavy. If one anticipates that the main effect of such a mine will be to cause a delay while the mine is found and cleared, it will be tempting to occasionally substitute fake mines, which are cheap, safe, and light. This was, in fact, the case in World War Two (United States Department of War, 1942)—a large fraction of the antitank "mines" employed in that war were actually fakes.

The same issue is present in IED warfare where IEDs are employed over a long time period to disrupt transport on a road network. The main counter to such warfare is to find and remove the IEDs using Route Clearance Patrols (RCPs) that are usually in short supply. If the associated time delays are significant, it will be tempting to disrupt RCP operations by including some fake IEDs in the mix.

Fake IEDs have, in fact, been occasionally employed by insurgents (hereafter "Red") in recent warfare, albeit not for the simple purpose of delaying RCPs. Red's purpose instead is usually to enable a supplementary attack during the delay that ensues after the fake IED is discovered (United States Army, 2010). There are no publicly available records recounting the use of fake IEDs in the same manner as the fake antitank mines of World War Two. Perhaps one reason for this is that Red typically places IEDs on a road network that Red does not control, so that the main perceived "cost" of an IED is the cost of the emplacement itself, which does not depend on whether the IED is real or fake. This situation could change if the materials for real IEDs become harder to acquire, or for other reasons. In any case, it is important to understand the potential influence of fake IEDs on the efficiency of RCP operations. The model described below has the purpose of enabling that understanding.

The reader may wish to have available the Microsoft Excel ™ workbook *IEDFake.xls*, which can be downloaded from http://faculty.nps.edu/awashburn/ .

2.1 ASSUMPTIONS

We model IED warfare as a prolonged contest between Red and Blue. Blue convoys of various kinds attempt to use a road network, while Red attempts to interdict that traffic using IEDs. Except for the additional feature of fake IEDs and the delays that they cause, we make the same assumptions about IED warfare as do Washburn and Ewing (2010), the essential ones being the following four:

- **Indefiniteness.** The battle is assumed to proceed indefinitely, with no time limit. Every mine placed on a road will eventually be involved in an incident with some kind of Blue convoy, possibly an RCP convoy. An "incident" by definition removes the mine, one way or another.

- **Logistic Ineffectiveness.** Red's efforts are assumed to have a negligible effect on Blue's logistic operations. While the damage done to Blue logistic convoys may be a significant issue for Blue, the convoys perform their logistic function regardless of damage. When attacked by a mine, a Blue convoy simply continues with its mission, and may even be attacked on multiple occasions. The analytical effect of this assumption is that, in quantifying the probability that a particular mine damages a particular Blue convoy, we will pay no attention to the possibility that other mines might have already damaged the convoy.
- **Independence.** The various types of Blue traffic and the Red process of placing mines on roads are all assumed to be time-homogeneous Poisson processes, with all Red processes being independent of all Blue processes, and with all processes of any color being independent of each other on any given segment. While Red knows from experience the general levels of Blue traffic, he does not know the schedule of movements, so he cannot, for example, rush out and put an IED right in front of a Blue logistic convoy before the RCPs can get to it.
- **Scalar Damage.** We assume that all types of damage due to mines (vehicles lost, vehicles damaged, cargo lost, men killed, men wounded, and so on) can be put on one scale called "damage". Blue's goal is to minimize it, and Red's the opposite.

To these four we add the assumptions that fake mines interact only with RCPs, and that every mine cleared by an RCP results in a time delay during which the RCP is not searching for additional IEDs. This time delay is what Red is trying to exploit in using fake IEDs.

2.2. A 2×2 MODEL

Although our ultimate goal is to optimally assign RCP effort to a road network, we first examine a single road segment. Given assumption 2, extension to a network composed of multiple segments will not be difficult. We will refer to "mines", rather than IEDs, to emphasize the essential features of the object involved: a mine does not move once planted, instead relying on its victim's need to move, and destroys itself along with its intended victim. The thing that distinguishes IED warfare from ordinary mine warfare is not that the explosive devices are improvised, but rather the assumptions listed above in Section 2.1.

For simplicity, we consider only two types of Red mine, fake and real, and only two kinds of Blue traffic, logistic and RCP. The unit of Blue traffic will be called a "convoy" for both types. Red plants mines on the road segment at given rates (in Poisson processes, to be exact), and Blue traffic passes over the segment at given rates. Logistic convoys are never delayed by mines of either type, but RCP convoys are delayed by any mine that they discover. When a real mine is discovered by either type of traffic, it disappears, possibly causing damage in the process. The parameters required to describe this are:

$x_F\,(x_R) =$ rate at which fake (real) mines are planted on the segment

$k =$ rate at which logistic convoys actuate each real mine on the segment

$y =$ base rate at which RCP convoys pass over the segment

$\beta_F\,(\beta_R) =$ probability that a fake (real) mine is discovered in one RCP pass

$\Delta_F\,(\Delta_R) =$ delay to an RCP convoy when it discovers a fake (real) mine

$d_L\,(d_{RCP}) =$ damage to a logistics (RCP) convoy when a real mine is discovered

The discovery probabilities should be understood to apply to each interaction between a convoy and a mine. Thus, if the segment happens to have five real mines on it when an RCP convoy passes over it, and if $\beta_R = 1$, then all five mines will be discovered by the convoy. All five might also cause damage to the convoy, since none of them (by assumption) would halt it.

Parameter y should be understood to be the base rate at which RCPs assigned to the segment pass over it, where by "base" we mean the rate not counting any delays caused by discovery. The base rate has nothing to do with the numbers of mines present, and will be subject to natural constraints when multiple segments are considered later. The actual rate at which RCPs pass over the segment may be smaller than y due to delays caused by mine discovery and clearance; indeed, causing this decrease is the only function of fake mines, since fake mines do not damage anything.

Let z be Blue's total rate of loss, counting damage to both kinds of convoy. Our object is to determine z as a function of the tactical allocations x_F, x_R, and y, as well as other parameters. The fact that the actual RCP pass rate (as opposed to the base rate y) depends on x_F and x_R, as well as y, is a significant complication that forces us to first dispose of some special cases. Some of these special cases are tactical nonsense for one side or the other, but we nonetheless include them for the sake of completeness. Let $h = y\beta_R$.

<u>Case 1 ($k = 0$ and $h = 0$)</u>: In this case, neither logistic nor RCP convoys are capable of discovering real mines. If $x_R > 0$, real mines will accumulate indefinitely on the road segment. Regardless of whether that happens, we take $z = 0$.

<u>Case 2 ($k > 0$ and $h = 0$)</u>: In this case, RCP convoys are ineffective at discovering real mines, but logistics convoys are effective. Real mines do not accumulate, but nonetheless all real mines are discovered by logistics convoys, so $z = x_R d_L$.

<u>Case 3 ($k = 0$ and $h > 0$)</u>: In this case, logistic convoys do not interact with mines of either type, so RCPs are the only effective traffic. Every real mine will eventually be discovered by an RCP, so $z = x_R d_{RCP}$.

<u>Case 4 ($k > 0$ and $h > 0$)</u>: This is the general case, where both types of convoy are present and interact with real mines. Real mines will not accumulate because the logistic convoys alone will prevent it, but it is possible that fake mines will accumulate in spite of the efforts of the RCPs. If this happens, RCPs will become completely saturated with fake mines, and will therefore be ineffective at removing real mines, so we are back to Case 2. Thus, our first task is to determine when saturation happens.

We suppose that RCP convoys come from a base somewhere, that each sortie from the base spends a total time T working on the segment, and that each pass over the segment requires a transit time of τ, not counting any delays caused by mines. The length of each sortie may be longer than T because of travel time getting to and from the segment, but need not concern us for the moment. Let λ be the rate at which sorties leave the base with a mission to clear mines on the subject segment. According to Little's Law, the average number of RCP convoys that are active on the segment is λT. The rate of RCP passages over the segment without consideration of clearance time delays is therefore $y = \lambda T / \tau$. Now, the average number of active RCP convoys required merely to deal with fake mines placed on the segment by Red is $x_F \Delta_F$. Fake mines will therefore accumulate, unless $\lambda T > x_F \Delta_F$, which is equivalent to $y\tau > x_F \Delta_F$. If this inequality is not true, we are back to Case 2, so we assume in the sequel that it holds. It is a distinguishing feature of this problem that there is no point in Blue's making y anything smaller than $x_F \Delta_F / \tau$, since the effect is the same as assigning no RCPs at all to the segment.

As long as saturation is avoided, we expect an equilibrium where the number of mines of each type on the road segment fluctuates with time in a stationary manner. Let m_F and m_R be the average numbers of fake and real mines that are present on the segment. The average time τ' for an RCP convoy to make one pass of the segment is the travel time τ plus the average time required to deal with any mines discovered:

$$\tau' = \tau + m_F \beta_F \Delta_F + m_R \beta_R \Delta_R \tag{2.1}$$

Let $\delta_F = \Delta_F / \tau$ be the dimensionless delay time for fake mines, and similarly let $\delta_R = \Delta_R / \tau$. Also, let

$$c = \tau' / \tau = 1 + m_F \beta_F \delta_F + m_R \beta_R \delta_R . \tag{2.2}$$

The actual rate of making RCP convoy passes is y/c, which is smaller than the nominal rate y because c exceeds 1. The total rate at which each real mine is removed from the segment is the sum of the removal rates by the two types of Blue convoys: $k + y\beta_R / c$. The word "each" is underlined to emphasize that every individual real mine on the segment is subject to removal at this rate; that is, the number of real mines on the segment is an M/M/∞ queue, and the average number of real mines present is therefore simply the ratio of the planting rate to the removal rate:

$$m_R = \frac{x_R}{k + y\beta_R / c} . \tag{2.3}$$

A similar argument leads to

$$m_F = \frac{x_F}{y\beta_F / c} , \tag{2.4}$$

where in (2.4) there is no term involving logistic convoys because logistic convoys do not interact with fake mines.

Substituting (2.3) and (2.4) into (2.2), we obtain a single equation in c:

$$c = 1 + \frac{x_F \beta_F \delta_F}{y \beta_F} c + \frac{x_R \beta_R \delta_R}{k + y\beta_R / c}. \tag{2.5}$$

Parameter β_F cancels in (2.5), and therefore cannot affect the calculation of c. This usually makes sense—if you halve β_F, you will also double m_F (the equilibrium number of fakes on the road), and therefore not affect $\beta_F m_F$ (the average number of fakes discovered by an RCP pass). If $\beta_F = 0$, however, there will be no equilibrium. The number of fakes will increase indefinitely as long as $x_F > 0$, but RCP operations will not be affected because none of the fakes will be discovered. One reasonable analytic alternative is to simply require that $\beta_F > 0$, since otherwise the use of fakes by Red is silly. Another alternative would be to set δ_F to 0 when $\beta_F = 0$, as doing so will eliminate the delaying effects of fakes. In the following, we assume $\beta_F > 0$.

Let $\varepsilon_F = x_F \delta_F$, $\varepsilon_R = x_R \delta_R$, and $j = k / \beta_R$. We note that $\varepsilon_F < y$ by assumption, and also that β_R cannot be 0 in the current case. Equation (2.5) can be expressed as

$$\left(1 - \frac{\varepsilon_F}{y}\right) c - 1 = \frac{\varepsilon_R c}{jc + y}. \tag{2.6}$$

The left-hand side of (2.6) is negative when $c = 1$, and strictly increases linearly with c. The right-hand side is positive when $c = 1$, and is a concave, increasing function of c that is bounded above. There is, therefore, exactly one solution of the equation for c, and it must exceed 1. This solution can be found by reducing (2.6) to a quadratic equation. Specifically, let $a = j(y - \varepsilon_F)$ and $b = (y - \varepsilon_F - \varepsilon_R - j)$. Then the unique solution of (2.6) is

$$c = \frac{2y}{b + \sqrt{b^2 + 4a}}. \tag{2.7}$$

Once c is determined, m_R and m_F are determined by (2.3) and (2.4), and finally the total loss rate is

$$z = k m_R d_L + y \beta_R m_R d_{RCP} / c. \tag{2.8}$$

Let

$$g \equiv \frac{k}{k + y\beta_R / c} = \frac{jc}{jc + y}, \text{ and also } g_{RCP} \equiv 1 - g. \tag{2.9}$$

Then (2.8) can be expressed as

$$z = x_R (g d_L + g_{RCP} d_{RCP}). \tag{2.10}$$

The number g is the fraction of real mines that are removed by logistics convoys, with the rest being removed by RCP convoys. Only real mines cause damage, and (2.10) simply conditions on the cause of each real mine's removal. Parameter x_F is not explicitly present in (2.10), but still influences z because it influences c.

2.3. PARAMETER QUANTIFICATION

The model described above requires several parameters to be measured before it can be used to predict how damage depends on the tactical variables. One might design a separate experiment to measure each of them. To estimate β_F, for example, one might deliberately plant some fake mines at locations known to the experimenter but not the RCP forces, and then observe how many fake mines are detected in repeated passes by RCP convoys. However, other experiments of this type, especially those involving damage, might prove difficult, unrealistic, or expensive. We therefore consider a scheme where the required parameters can be estimated from current operations.

Assume that operations have been continuing at a stationary level over some interval of significant length (weeks or months), and that the following records about results have been kept:

T = length of the time interval
N_L = number of real mines removed by logistics convoys
N_{RCP} = number of real mines removed by RCP convoys
F = number of fake mines removed by RCP convoys
D_L = damage to logistic convoys caused by real mines
D_{RCP} = damage to RCP convoys caused by real mines
T_F = total time spent clearing fake mines by RCP convoys
T_R = total time spent clearing real mines by RCP convoys
T_S = total time spent searching by RCP convoys
Y = base rate of RCP passes over the segment

Note that it is the base rate of RCP passes that is assumed to be measured, rather than the actual rate. We prefer not to deal with the actual rate on account of our suspicion that many RCP passes will actually be incomplete or redundant, as the RCP moves one way or another over the road segment. The base rate would not be measured by the RCPs themselves, but rather by the commander who assigns RCPs to road segments. The base rate is proportional to the rate at which RCP sorties are assigned to the road segment, with the same proportionality factor in all time intervals. That factor involves the distance of the segment from the RCP base, the segment length and other parameters, but need not concern us for the moment.

Based on these measurements, we desire to estimate the parameters required to predict total damage over a similar interval of time where everything except for the base rate of RCP passes remains constant. The easy estimates are simple ratios of totals to trials:

$$\begin{aligned} d_L &= D_L / N_L \\ d_{RCP} &= D_{RCP} / N_{RCP} \\ \Delta_F &= T_F / N_{RCP} \\ \Delta_R &= T_R / N_{RCP} \end{aligned} \quad . \qquad (2.11)$$

We assume, of course, that neither denominator is zero. Avoidance of this possibility is the reason for our insistence that T should be of "significant length".

Since the operation is assumed stationary, the rate of removing mines is the same as the rate of planting them, so we have

$$\begin{aligned} x_F &= F / T \\ x_R &= (N_L + N_{RCP}) / T \end{aligned} \quad . \qquad (2.12)$$

The total time spent on the segment by RCP convoys is $T_F + T_R + T_S$, of which only T_S is spent searching for mines. The fraction of the time that RCP convoys have spent searching for mines is therefore

$$1/C = T_S/(T_F + T_R + T_S) \tag{2.13}$$

We use an uppercase C here to emphasize that the ratio c cannot be expected to remain constant if the base level changes from Y to some other value, so C is not one of the fundamental parameters to be used in future predictions. It is nonetheless useful to employ C in making other computations.

We can also determine τ, the time required for an RCP convoy to make one complete pass of the road segment if distractions due to clearing mines are ignored. Since RCP convoys move only when they are searching for mines, the total number of RCP passes is YT/C, during which a total time of T_S is spent moving and searching. Therefore

$$\tau = \frac{T_S C}{YT} = \frac{T_F + T_R + T_S}{YT}. \tag{2.14}$$

While the numerator and denominator of (2.14) both depend on Y, the ratio does not. An alternative way to estimate τ would be to divide the segment length by the average RCP searching speed. Our method avoids needing to know the latter.

With τ known, we can also estimate

$$\begin{aligned} \varepsilon_F &= x_F \Delta_F / \tau \\ \varepsilon_R &= x_R \Delta_R / \tau \end{aligned}. \tag{2.15}$$

We can estimate the ratio j by solving (1.6) for j:

$$j = \frac{\varepsilon_R Y}{(Y - \varepsilon_F)C - Y} - \frac{Y}{C}. \tag{2.16}$$

As in the case of τ, j does not actually depend on Y in spite of the appearance of Y in (2.16). With j known, we are now prepared to predict the total loss rate as a function of y. We first employ (2.7) to determine c, then (2.9) to determine g and g_{RCP}, and finally (2.10) to determine z.

An example of the above data estimation technique is shown on page "DataEst" of the workbook *IEDFake.xls*.

2.4. MULTIPLE ROAD SEGMENTS

Now assume that a single Blue commander is responsible for all RCP actions on some road network; that he can generate RCP convoys from some base at a fixed rate b; and that the commander's goal is to minimize total damage over the whole network. Introduce a subscript k for road segment, and assume for the moment that every RCP convoy works on exactly one segment. If λ_k is the rate at which sorties bound for segment k are generated, then the commander's constraint is $\sum_k \lambda_k \le b$.

Segments far from the base will be hard to clear because much of the assigned convoy's time will be spent in travel to the segment. Let T_k be the total time that a sortie bound for k can actually spend working on segment k, whether searching for mines or clearing them, and let τ_k be the time required to make one pass (not counting clearance delays) of segment k. For example, sorties might be a standard four hours long, but T_k might be only two hours because of time spent in transit, and τ_k might be one hour because segment k is 15 miles long and RCPs travel at 15 mph when not dealing with mines. The implied base passage rate for RCPs on segment k is $y_k = \lambda_k T_k / \tau_k$. Letting $\alpha_k = \tau_k / T_k$, we can eliminate further reference to λ_k and say that the Blue commander's constraint is

$$\sum \alpha_k y_k \le b. \tag{2.17}$$

In the example, α_k would (1 hr)/(2 hr) = 0.5. From Blue's standpoint, small values of α_k are preferable to large ones.

Other parameters such as d_L can also depend on k, so we write $d_{L,k}$ for the average damage to a logistics convoy when it actuates a real mine on segment k, etc. After applying (2.7), (2.9), and (2.10) for each segment, we finally obtain the total damage over all segments

$$z = \sum_k x_{R,k} (g_k d_{L,k} + g_{RCP,k} d_{RCP,k}), \tag{2.18}$$

to be minimized by the Blue commander. The minimization is potentially difficult, especially if the RCP convoys are not immune to damage, but having an analytical expression for total damage as a function of RCP allocation is still useful. Small problems can be solved by exhaustion. Page "TwoSeg" of *IEDFake.xls* finds the optimal distribution of RCP effort between two identical segments by simply plotting total damage versus the allocation to the first segment. Figure 2.1 displays the resulting graph.

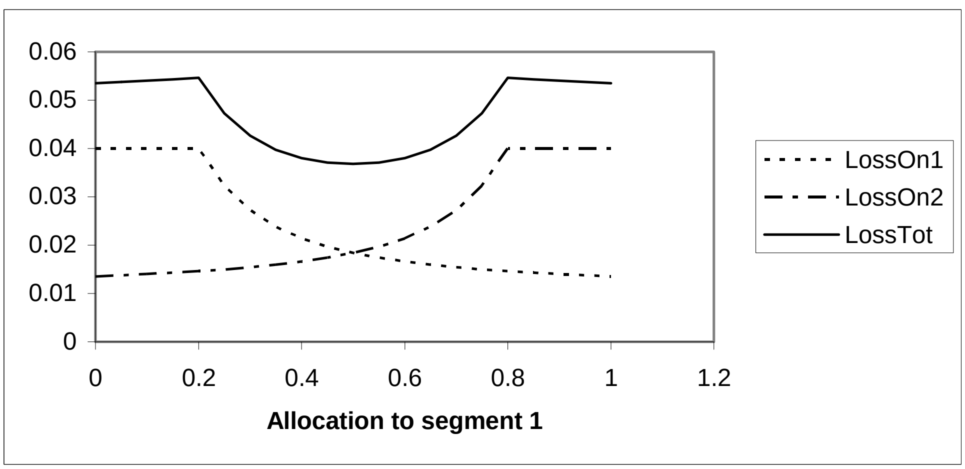

Figure 2.1: Losses on two road segments as a function of the RCP allocation.

Figure 2.1 shows that the best allocation is an even split between the two segments. It also shows that the *worst* allocation is to use just enough RCP patrols on a segment so that they are saturated by clearing fakes, which accomplishes nothing for the chosen segment, while starving the other segment of patrols.

Other problems, including problems where the segments are not identical, can be similarly solved by adjusting the input parameters on page “TwoSeg”.

The road “network” modeled above is merely a set of road segments, with the topological connections between the segments being irrelevant. This is partly because of the assumption of logistic ineffectiveness, which implies that mines on any given segment do not need to worry about being robbed of opportunities by mines on other segments. Another reason is our assumption that every RCP convoy works on exactly one segment, which ignores the possibility that an RCP convoy might do some clearance on segments that it must travel over, even if they are not assigned. An alternative would be to introduce “missions” for RCP convoys indexed by m, and an additional array of input data T_{km} = “average amount of time that an RCP convoy on mission m spends on segment k”. If u_m is the rate of generating missions of type m, then these become the decision variables for Blue, with the constraint now being $\sum_m u_m \le b$. The intermediate variables y_k are computed from

$$y_k = \sum_m u_m T_{km} / \tau_k , \qquad (2.19)$$

and z is computed as in (2.18). This is still a potentially difficult nonlinear minimization problem, but no more so than the problem with direct assignments of sorties to segments. The essential feature of both is that Blue’s constraint set is a collection of linear inequalities.

2.5. GAMING ASPECTS

Parameters x_F and x_R have so far been treated as known inputs that can be measured in one period and successfully extrapolated to the next. One of our goals, however, is to describe circumstances where the introduction of fake IEDs can be expected, and to do that we need to introduce some flexibility into Red’s strategy. Therefore, we now suppose that Red has a budget b measured in units of what real IEDs cost, and that fake IEDs cost only f on that scale, where $0 < f < 1$. Red can divide his budget as he wishes between real and fake IEDs; that is, he can have any (x_F, x_R) pair he wishes as long as $x_R + fx_F \le b$.

Figure 2.2 shows losses on a segment in an example where f = 1/4. This is the same example considered in Section 2.4, except that (x_F, x_R) is now controllable, and each point on the curve has been calculated for a specific budget division. The figure shows that the best option for Red is to spend half of his budget on fakes. This is the amount required to overwhelm the RCP forces, which end up doing nothing but fake clearance. The rest of Red’s budget is spent on real IEDs, all of which engage logistic traffic and damage some of it. The presence of the RCP forces is in effect a tax that Red must pay in order to employ his real IEDs. Note that the curve ultimately decreases, which should be expected because additional fakes accomplish nothing once RCP saturation occurs, and also note that the curve is convex before the RCP saturation point—the only competitor to saturation is to use no fakes at all. Indeed, if f is increased to 1/3, Red ignores fakes and uses only real IEDs. We should not conclude from this that there is anything special about fractions like 1/4 and 1/3, which depend on other parameters that have been arbitrarily assigned. However, the convexity of the curve is perhaps significant. If fake

IEDs suddenly appear on the battlefield, it may be in quantities large enough to seriously hamper RCP forces. The appearance of fakes could make a significant difference—the damage level when fakes are used optimally (0.10) is significantly higher than the damage without fakes (0.08). Sheet "TwoSegGame" of *IEDFake.xls* performs all of these calculations, and the reader is, of course, free to change the green inputs to see the effect on tactics and outcome.

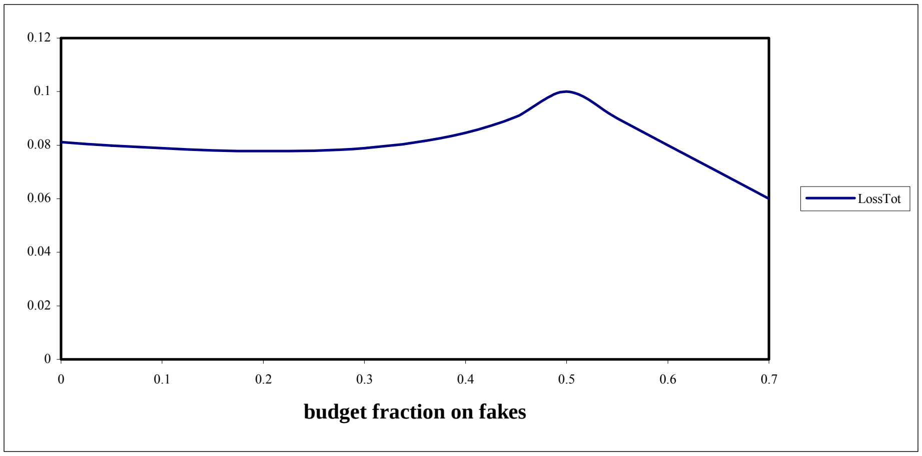

Figure 2.2: Damage on a segment as a function of how Red splits his budget between fake and real IEDs.

New issues arise when there are multiple segments. The most favorable case for Red is when he can freely divide his budget over the segments in the knowledge of Blue's RCP allocations, possibly using different fake/real divisions in different segments. In the same example considered above, but with two identical segments, Blue's best option is to split his RCP forces evenly. The damage level will then be 0.10 if Red splits his budget evenly, but Red would be ill-advised to do that. The damage level can be made as high as 0.15 if Red spends the entirety of his budget on one of the two segments, ignoring the other. On the one segment that he attacks, Red employs sufficient fakes to saturate the RCP forces, together with real IEDs that are in no danger of being cleared. These claims can be verified using *IEDFake.xls*.

Of course, once Blue observes that Red's fake IEDs have saturated his RCP forces, he can be expected to change the distribution of his RCP forces, or even, if the network permits, change the routing of logistic traffic. A multistage game results where each side is continually adapting to the actions of the other. The advantage can be expected to accrue to the side with the best information system. A quantitative analysis of this situation will be the object of a future study.

3. DECOY SURVEILLANCE TOWERS

The Ground-Based Operational Surveillance System (G-BOSS) is being deployed to Iraq and Afghanistan to provide persistent surveillance for the U.S.-led coalition forces. The G-BOSS consists of a tower that is about 100 feet tall, with two infrared cameras on the top. The cameras feed real-time videos to a control room, where the operators monitor the tower's surroundings through computer screens. Because the operators sit inside a control room, from the outside it is almost impossible to tell whether there is indeed an operator sitting inside. A research question arises naturally: When the coalition forces are short of manpower, does an understaffed surveillance tower provide any deterrence to insurgency?

If a surveillance tower is not staffed for a prolonged period of time, then sooner or later the insurgents will realize it, perhaps by spying on the coalition forces' operations, by talking to people who work for the coalition forces, or by probing the surveillance system in some way. If, on the other hand, the surveillance tower is understaffed only intermittently, then it may be difficult for the insurgents to know the tower's surveillance capability at any given time. The purpose of this section is to study the possible deterrence effect provided by understaffed surveillance towers.

3.1. A MODEL WITH TWO SURVEILLANCE TOWERS

Consider a situation where Blue has established military bases in two towns. Blue's goal is to maintain peace and eliminate insurgent activities in these two towns. Insurgent activities include shooting, hostage taking, planting IEDs, etc. From now on, we will refer insurgent activities as *attacks* for brevity. Blue has one surveillance tower set up in each base, but Blue cannot detect all attacks in both towns at all times due to lack of resources (manpower, equipment, etc.). Denote by s ($s \le 2$) the total resource available to Blue, such that Blue can allocate detection probability p_i to tower i, as long as $p_1 + p_2 \le s$ and $0 \le p_i \le 1$, for $i = 1,2$. The problem facing Blue is how to allocate s between the two surveillance towers.

In each town, an insurgent group attempts to carry out attacks for its own gain. We refer to the insurgent group operating in town i as Red i, for $i = 1,2$. Red 1 and Red 2 operate independently from each other. For each Red team, the status quo is not to attack, in which case neither Red nor Blue receives a reward or a penalty. If a Red team launches an attack, there are two possible outcomes: (1) the attack is detected by the surveillance tower; or (2) the attack is not detected. The Red team earns reward of +1 for each undetected attack, and incurs a penalty $r > 0$ (reward $-r$) for each detected attack. Because Blue's goal is to maintain peace and ideally to eliminate attacks altogether, there is a penalty for each attack, regardless of whether or not the attack is detected. However, detecting an attack is better than not detecting it, so Blue incurs a penalty 1 (reward -1) for an undetected attack and a smaller penalty $b \in (0,1)$ (reward $-b$) for a detected attack. Table 3.1 summarizes the reward for Blue and each Red team, respectively.

Table 3.1: Reward table. Parameter *r* is positive, while parameter *b* lies between 0 and 1.

	No Attack	Attack Undetected	Attack Detected
Red	0	+1	$-r$
Blue	0	-1	$-b$

We model the interaction between Blue and two Red teams as a non-zero-sum game, where Blue moves first, and then each Red team moves second, independently, after observing Blue's strategy. The objective of each player is to maximize his own long-run average reward.

If the detection probability is p in a town, Blue's expected reward for each attack is

$$(-1)(1-p)+(-b)p=-1+(1-b)p, \tag{3.1}$$

and Red's expected reward for each attack is

$$(+1)(1-p)+(-r)p=1-(1+r)p. \tag{3.2}$$

By setting Equation (3.2) to 0, we can solve

$$\hat{p}\equiv\frac{1}{1+r}. \tag{3.3}$$

If $p>\hat{p}$, Equation (3.2) is negative, so it is optimal for a Red team to shut down his operation altogether. In the special case when $p=\hat{p}$, Red's expected reward for each attack is 0, so Red feels indifferent between attacking or not. For mathematical completeness, however, we assume that Red will continue to attack if $p=\hat{p}$, as it gives Blue a negative expected reward.

Suppose each Red team can carry out attacks at a maximum rate *x*. Consider three cases for *s*:

1. $s\in\left(2\hat{p},2\right]$. If Blue allocates $p_1=p_2=s/2>\hat{p}$, then both Red teams will stop their operations. The long-run reward rate is 0 for all three players.

2. $s\in\left[0,\hat{p}\right]$. No matter how Blue allocates *s*, both Red teams will continue to attack at the maximum rate *x*. The total long-run reward rate for both Red teams is

$$x(1-(1+r)p_1+1-(1+r)p_2)=x(2-(1+r)s). \tag{3.4}$$

Blue's long-run reward rate is

$$x(-1+(1-b)p_1-1+(1-b)p_2)=x(-2+(1-b)s). \tag{3.5}$$

3. $s\in\left(\hat{p},2\hat{p}\right]$. In this case, it is possible for Blue to allocate the detection probability such that it is optimal for one Red team to stop his operation.

For the rest of this section, we will focus on the case when $s\in(\hat{p},2\hat{p}]$. In particular, we will study two strategies for Blue: stationary allocation and dynamic allocation.

3.2. STATIONARY ALLOCATION

With a stationary allocation, Blue assigns p_i to surveillance tower *i*, *i* = 1, 2, on a permanent basis. It is reasonable to assume that each Red team will find out this allocation sooner or later, whether by intelligence or by computing his own success rate. Without loss of generality, assume $p_1\geq p_2$. First, it does not help to set $p_1\leq\hat{p}$, with which the optimal strategy for each Red team is to attack at the maximum rate *x*. If Blue sets $p_1=\hat{p}+\varepsilon$, for some $\varepsilon>0$, then it is optimal for Red 1 to cease the operation, and for Red 2 to attack at rate *x*. Using Equation (2), Red 2's long-run reward rate is

$$x(1-(1+r)(s-\hat{p}-\varepsilon)) = x(2-(1+r)(s-\varepsilon)),$$

which converges to

$$x(2-(1+r)s) \tag{3.6}$$

as $\varepsilon \downarrow 0$. Using Equation (3.1), Blue's long-run reward rate is

$$x(-1+(1-b)(s-\hat{p}-\varepsilon)) = x\left(-1+(1-b)\left(s-\frac{1}{1+r}-\varepsilon\right)\right),$$

which converges to

$$x\left(-1+(1-b)\left(s-\frac{1}{1+r}\right)\right), \tag{3.7}$$

as $\varepsilon \downarrow 0$.

3.3. DYNAMIC ALLOCATION

With a dynamic allocation, Blue first assigns p to a tower and $s-p$ to the other tower, and then swaps these allocations from time to time. Without loss of generality, assume $p > s-p$. The idea of dynamic allocation is to make $p > \hat{p}$ so that sometimes it is optimal for a Red team to pause the attacks, but each Red team needs to guess when to resume the attacks. The tower with detection probability $s-p$ can be viewed as a decoy, which may provide deterrence effect if a Red team does not know the detection probability has dropped from p to $s-p$.

Blue has two decision variables, p and y, such that Blue allocates detection probability p to one tower and $s-p$ to the other, and swaps these allocations at a Poisson rate y. Because the two Red teams do not interact with each other, and because the parameters are identical in the two towns, from now on, the analysis will focus on the interaction between Blue and one Red team (henceforth, Red for brevity).

One feasible strategy for Red is to attack at a Poisson rate x. Alternatively, Red can set aside some effort to learn about the detection probability at a Poisson rate z. Red can do this by sending a spy, bribing Blue's people, or probing the system in some way. We will impose a constraint that requires $x + \alpha z \le c$, where $\alpha > 0$ models the trade-off between the *attack rate* x and the *learning rate* z, and where c is the maximum attack rate if Red sets the learning rate to 0. With a learning rate $z > 0$, Red would learn about the detection probability at time moments that constitute a Poisson process with rate z. In other words, the time between two consecutive learning points follows an exponential distribution with rate z, independent of everything else.

Recall that $p > s-p$. We say the surveillance tower (or Blue) is in state 1 if its detection probability is p, and in state 0 if its detection probability is $s-p$. In other words, each tower remains in state 1 for a random time that is exponentially distributed with mean $1/y$, and then switches to state 0 and stays in state 0 for another random time, also exponentially distributed with mean $1/y$, and so on. In the long run, each tower will be in each state 50% of the time. We say Red is in state 1 if Red is carrying out attacks at a Poisson rate x, and in state 0 if Red pauses the attacks. Red decides when he wants to move from one state to the other.

Because $p > \hat{p}$, when Red learns the tower is in state 1, Red should pause the attacks. Let $P_{jk}(t)$ denote the probability that the tower will be in state k after t time units if it is currently in state j, $j,k = 0,1$. Using the result in Ross (1996), we can compute

$$P_{11}(t) = \frac{1}{2} + \frac{1}{2}e^{-2yt} = 1 - P_{10}(t).$$

Red can compute the probability of detection after t time units once he learns that Blue is in state 1, if Red does not having a learning point in the next t time units, as

$$P_{11}(t) \cdot p + P_{10}(t) \cdot (s - p) = \left(\frac{1}{2} + \frac{1}{2}e^{-2yt}\right)p + \left(\frac{1}{2} - \frac{1}{2}e^{-2yt}\right)(s - p).$$

Red should attack if this detection probability is less than $\hat{p}$. After some algebra, we can show that Red should wait for another

$$\hat{t} \equiv \frac{\ln\left(\frac{2p - s}{2\hat{p} - s}\right)}{2y} \tag{3.8}$$

time units before resuming the attacks, if Red does not have another learning point in this time period. Consequently, Red's optimal strategy takes the following form: Whenever Red learns that Blue's tower is in state 1, Red pauses the attacks until the next learning point or until $\hat{t}$ time units have elapsed. If Red learns Blue's state is 0 within the next $\hat{t}$ time units, Red should resume the attacks immediately; if Red does not have a learning point within the next $\hat{t}$ time units, then Red resumes the attacks after $\hat{t}$ time units. With this strategy, we can define a renewal reward process, where a renewal is a time moment when Red learns that Blue's tower is in state 1. Figure 3.1 depicts this renewal reward process.

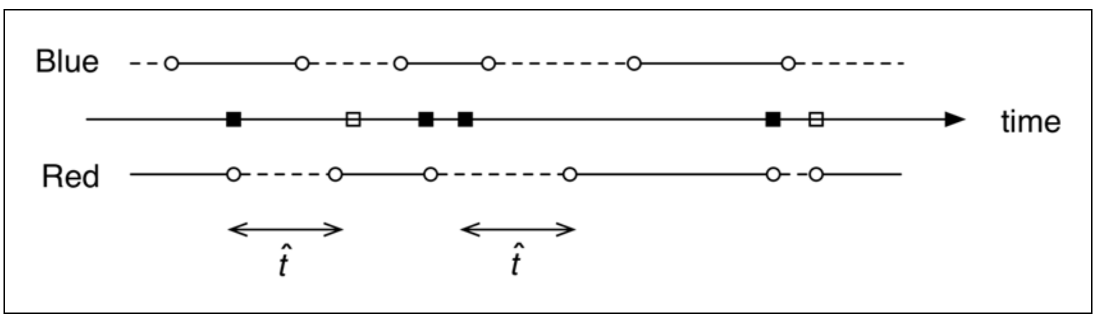

Figure 3.1: Renewal reward process. This diagram depicts the renewal reward process if Blue dynamically allocates its resource. For Blue, each circle represents a switch point, with solid lines indicating state 1 (detection probability *p*) and dashed lines indicating state 0 (detection probability $s - p$). For Red, solid lines indicate state 1 (attacking) and dashed lines indicate state 0 (not attacking). For the time line, each square represents a Red's learning point, with a solid square being a renewal (Blue in state 1).

Let T denote the cycle time (the random amount of time between two consecutive renewals) in this renewal reward process. In addition, denote by T_k the time until the next renewal if Blue's current state is $k, k = 0,1$. We denote the expected value of random variable X by E[X]. To compute $E[T_1]$, consider the next event. If Blue's current state is 1, then the next event can either be Blue's switch to state 0, or Red's learning Blue's state. Because the time to each event is exponentially distributed, the time to *either* event, whichever occurs first, is also exponentially distributed with rate equal to the sum of the two individual rates $y + z$. With probability $y / (y + z)$, the next event will be Blue's switch to state 0, in which case the additional time until a renewal is distributed as T_0. With probability $z / (y + z)$, the next event will be Red's learning Blue's state to be 1, which constitutes a renewal. Therefore, we can write

$$E[T_1] = \frac{1}{y+z} + \frac{y}{y+z} E[T_0].$$

With a similar argument, we can write

$$E[T_0] = \frac{1}{y} + E[T_1].$$

Solving the preceding yields $E[T_1] = 2/z$, and $E[T_0] = 1/y + 2/z$. By definition, T and T_1 have the same distribution, so $E[T] = 2/z$.

Let X denote the number of detected attacks in a cycle, and Y the number of undetected attacks in a cycle. If Blue is in state k (k = 0, 1) and Red is in state 1 (attacking), then let X_k denote the number of detected attacks until the next renewal, and Y_k the number of undetected attacks until the next renewal.

To compute $E[X_1]$, consider whether Blue switches to state 0 first or Red learns Blue's state first. The time until either event occurs follows an exponential distribution with rate $y + z$, so the expected number of detections during this time period is $px/(y+z)$. Moreover, with probability $y/(y+z)$, Blue will switch to state 0 first, in which case the additional number of detected attacks in the cycle is distributed as X_0. With probability $z/(y+z)$, Red will learn that Blue is in state 1 first, which constitutes a renewal. Therefore, we can write

$$E[X_1] = \frac{x}{y+z} p + \frac{y}{y+z} E[X_0].$$

With a similar argument, we can write

$$E[X_0] = \frac{x}{y}(s-p) + E[X_1].$$

Solving from the preceding yields,

$$E[X_1] = \frac{x}{z} s \text{ and } E[X_0] = \frac{x}{y}(s-p) + \frac{x}{z} s.$$

In a similar way, we can set up two linear equations involving $E[Y_1]$ and $E[Y_0]$ as

$$E[Y_1] = \frac{x}{y+z}(1-p) + \frac{y}{y+z}E[Y_0],$$

$$E[Y_0] = \frac{x}{y}(1-(s-p)) + E[Y_1].$$

Solving from these two linear equations yields,

$$E[Y_1] = \frac{x}{z}(2-s) \text{ and } E[Y_0] = \frac{x}{y}(1-(s-p)) + \frac{x}{z}(2-s).$$

Now we proceed to compute $E[X]$ and $E[Y]$. Let Z denote the time of the first learning point after the renewal, which follows an exponential distribution with rate z. To compute $E[X]$, condition on the event $Z = t$. If $t < \hat{t}$, then at time *t*, either (1) the cycle ends if Blue is in state 1, or (2) Red resumes the attacks (moves to state 1) if Blue is in state 0. If $t > \hat{t}$, then Red resumes the attacks at time $\hat{t}$. Therefore,

$$\begin{aligned} E[X] &= \int_0^{\hat{t}} P_{10}(t)E[X_0]ze^{-zt}dt + e^{-z\hat{t}}(P_{11}(\hat{t})E[X_1] + P_{10}(\hat{t})E[X_0]) \\ &= \int_0^{\hat{t}} \left(\frac{1}{2} - \frac{1}{2}e^{-2yt}\right) ze^{-zt}dt\, E[X_0] + e^{-z\hat{t}}\left(\frac{1}{2} + \frac{1}{2}e^{-2y\hat{t}}\right)E[X_1] + e^{-z\hat{t}}\left(\frac{1}{2} - \frac{1}{2}e^{-2y\hat{t}}\right)E[X_0]\text{w} \\ &= \frac{1}{2}\frac{x}{z}s(1+e^{-z\hat{t}}) - \frac{1}{2}\frac{x}{z+2y}(2p-s)(1-e^{-(z+2y)\hat{t}}), \end{aligned}$$

here $\hat{t}$ is given in Equation (3.8). Similarly,

$$\begin{aligned} E[Y] &= \int_0^{\hat{t}} P_{10}(t)E[Y_0]ze^{-zt}dt + e^{-z\hat{t}}(P_{11}(\hat{t})E[Y_1] + P_{10}(\hat{t})E[Y_0]) \\ &= \frac{1}{2}\frac{x}{z}(2-s)(1+e^{-z\hat{t}}) + \frac{1}{2}\frac{x}{z+2y}(2p-s)(1-e^{-(z+2y)\hat{t}}). \end{aligned}$$

Red's long-run reward rate is equal to (renewal reward theory)

$$\begin{aligned} R(p,y,x,z) &= (+1)\frac{E[Y]}{E[T]} + (-r)\frac{E[X]}{E[T]} \\ &= \frac{x}{4}\left((2-(1+r)s)(1+e^{-z\hat{t}}) + (1+r)(2p-s)\frac{z}{z+2y}(1-e^{-(z+2y)\hat{t}})\right). \end{aligned} \tag{3.9}$$

Red's decision variables are x and z, subject to $x + \alpha z \le c$. Blue's long-run reward rate is

$$\begin{aligned} B(p,y,x,z) &= (-1)\frac{E[Y]}{E[T]} + (-b)\frac{E[X]}{E[T]} \\ &= \frac{x}{4}\left((-2+(1-b)s)(1+e^{-z\hat{t}}) - (1-b)(2p-s)\frac{z}{z+2y}(1-e^{-(z+2y)\hat{t}})\right), \end{aligned} \tag{3.10}$$

with decision variables p and y.

We assume that the two Red teams operate independently, without any coordination. That is, when the Red team in one town learns the tower's detection probability, he does not give this information to the Red team in the other town. In the case when the two Red teams maintain a real-time communication, the learning rate at each town is essentially doubled and the same analysis applies.

3.4. COMPUTING THE OPTIMAL STRATEGIES IN DYNAMIC ALLOCATION

When Blue dynamically allocates his resource between the two surveillance towers, each player has two decision variables, as shown in Equations (3.9) and (3.10). In our model, Blue moves first and Red moves seconds, with each player trying to maximize his own long-run average reward. To compute this equilibrium, we first solve Red's optimization problem for given p and y.

Although Red has two decision variables, at the optimality the constraint $x + \alpha z \le c$ must be equality, because $R(p, y, x, z)$ strictly increases in x when z is held constant. Substituting $x = c - \alpha z$ into Equation (3.9), Red's objective function involves a single variable z as follows:

$$R(z) \equiv \frac{c - \alpha z}{4}\left(\left(2-(1+r)s\right)\left(1+e^{-z\hat{t}}\right)+(1+r)(2p-s)\frac{z}{z+2y}\left(1-e^{-(z+2y)\hat{t}}\right)\right).$$

Proposition 3.1. The function $R(z)$ is concave in z.
Proof: See Appendix.

Red's objective is to choose $z \in [0, c/\alpha]$ to maximize $R(z)$. Because $R(z)$ is concave in z, to maximize $R(z)$, first compute

$$R'(0) = \frac{2-(1+r)s}{4}\left(-2\alpha - c\hat{t}\right) + \frac{(1+r)(2p-s)}{4}\frac{c}{2y}\left(1-e^{-2y\hat{t}}\right). \tag{3.11}$$

Consider two cases:

1. $R'(0) > 0$: In this case, it is optimal to set $z^* = 0$.
2. $R'(0) < 0$: Red wants to maximize $R(z)$ for $z \in [0, c/\alpha]$. Because $R(z)$ is concave and $R'(c/\alpha) < 0$, to maximize $R(z)$ it is equivalent to solving $R'(z) = 0$. A simple bisection algorithm can compute the solution.

Denote the optimal learning rate derived from the preceding algorithm by $z^*(p, y)$, and let $x^*(p, y) = c - \alpha z^*(p, y)$. Define

$$\hat{B}(p, y) \equiv B(p, y, x^*(p, y), z^*(p, y)),$$

which Blue wishes to maximize by choosing p and y. To compute Blue's optimal strategy, we first plot $\hat{B}(p, y)$ and observe that the function is unimodal in each variable. We use the following algorithm to compute Blue's optimal strategy.

1. Let $i \leftarrow 0$, and $p_i \leftarrow \min(1, (s + \hat{p})/2)$. Use the golden section search to compute $y_i \leftarrow \arg\max_y \hat{B}(p_i, y)$.

2. Use the golden section search to compute $p_{i+1} \leftarrow \arg\max_p \hat{B}(p, y_i)$.

3. Use the golden section search to compute $y_{i+1} \leftarrow \arg\max_y \hat{B}(p_{i+1}, y)$.

4. If $\hat{B}(p_{i+1}, y_{i+1}) - \hat{B}(p_i, y_i) > \delta$, then let $i \leftarrow i+1$ and go to step 2. The parameter δ is the error bound.

5. Output $y^* = y_{i+1}$ and $p^* = p_{i+1}$ as Blue's optimal strategy.

3.5. NUMERICAL EXPERIMENTS

This section presents numerical experiments to demonstrate our model. First, we set $c = 1$ without loss of generality, because using the other values is equivalent to rescaling the clock to a different unit. Second, we set $\alpha = 1$, which—although not as intuitive—is also without loss of generality. To understand why it is the case, rewrite Equaiton (3.9) as $R(p, x, y, z, \alpha)$ and Equation (3.10) as $B(p, x, y, z, \alpha)$ to signify its dependence on α, and note that

$$\begin{aligned} R(p, y, x, z, \alpha) &= R(p, \alpha y, x, \alpha z, 1) \\ B(p, y, x, z, \alpha) &= B(p, \alpha y, x, \alpha z, 1) \end{aligned}.$$

In other words, if we treat αz (instead of *z*) as Red's decision variable and αy (instead of *y*) as Blue's decision variable, then we convert the original problem to an equivalent problem with $\alpha = 1$. This transformation is possible mainly because there is no cost or constraint associated with Blue's choice of *y*. The optimal choice of *y* involves a delicate balance. If *y* is too small (say once a year), then Red can easily take advantage of it by setting a moderate learning rate without much sacrifice to the attack rate. If *y* is too large (say once an hour), then Red might as well give up learning altogether and attack at the maximum rate 1, which defeats the purpose of fake surveillance towers. In other words, Blue's choice of *y* needs to be large enough to keep Red honest, and small enough so Red has incentive to set aside some effort to spy on Blue's operations.

By setting $c = 1$ and $\alpha = 1$, the remaining parameters that we need to consider are *r*, *b*, and *s*. Table 3.2 summarizes the optimal strategies for $r = 4$ and $b = 0.5$ ($\hat{p} = 0.2$), and for different values of *s* between $\hat{p}$ and $2\hat{p}$. The first column gives the total resource available to Blue, and the next four columns give the optimal strategies for Blue and Red, respectively. In this example, it is optimal for Blue to set $p = s$. In other words, when in state 0, the tower has no detection capability at all.

Table 3.2: The optimal strategies when Blue uses dynamic allocation, with $r = 4$ and $b = 0.5$. The corresponding numbers in stationary allocation are given in the parentheses.

s	p	y	x	z	Percentage of Time Red is Attacking	Red's Long-Run Attack Rate	Rate of Undetected Attacks	Rate of Detected Attacks
0.24	0.24	0.002	0.958	0.042	0.504 (0.5)	0.483 (0.5)	0.478 (0.48)	0.005 (0.02)
0.28	0.28	0.011	0.900	0.100	0.510 (0.5)	0.459 (0.5)	0.446 (0.46)	0.013 (0.04)
0.32	0.32	0.034	0.832	0.168	0.516 (0.5)	0.429 (0.5)	0.408 (0.44)	0.022 (0.06)
0.36	0.36	0.090	0.748	0.252	0.523 (0.5)	0.391 (0.5)	0.360 (0.42)	0.031 (0.08)

The 6th column in Table 3.2 gives the long-run proportion of time when Red is attacking. From the definition of the renewal process in Figure 3.1, at the beginning of each cycle, Red will remain in state 0 either until the next learning point, or until $\hat{t}$ time units have elapsed, whichever occurs first. In other words, the amount of time Red is in state 0 in each cycle is $\min(W,\hat{t})$, where W follows an exponential distribution with rate z. In each cycle, the expected time Red is not attacking (state 0) is

$$E[\min(W,\hat{t})] = \int_0^{\hat{t}} w \cdot ze^{-zw} dw + \int_{\hat{t}}^{\infty} \hat{t} \cdot ze^{-zw} dw = \frac{1}{z}(1 - e^{-z\hat{t}}).$$

Consequently, the long-run proportion of time Red is not attacking (state 0) is

$$\frac{E[\min(W,\hat{t})]}{E[T]} = \frac{1}{2}(1 - e^{-z\hat{t}}). \tag{3.12}$$

The long-run proportion of time Red is attacking (state 1) is

$$\frac{1}{2}(1 + e^{-z\hat{t}}), \tag{3.13}$$

which is reported in the 6th column. In addition, $E[Y]/E[T]$ and $E[X]/E[T]$ are reported in the 8th and 9th columns, respectively, with their sum given in the 7th column.

In the last four columns, the corresponding numbers with stationary allocation are given in the parentheses. Recall that with stationary allocation, one Red team attacks at rate 1, while the other Red team shuts down the operation entirely, so the average attack rate between the two towns is 0.5. With dynamic allocation, Red ends up spending more time attacking (state 1), as seen in the 6th column in Table 3.2. The overall attack rate, however, is lower, as seen in the 7th column, because the instantaneous attack rate ($x = 1 - z$) is smaller due to a positive learning rate. With more intelligence, Red is able to attack with a higher success probability. Overall, the rate of undetected attacks decreases, while the rate of detected attacks decreases more.

Figure 3.2 shows the long-run reward rates for both players with $r = 4$ and $b = 0.5$. Because $\hat{p} = 0.2$, dynamic allocation only applies for s between $\hat{p} = 0.2$ and $2\hat{p} = 0.4$. The results for stationary allocation come from Equations (3.4) to (3.7), while those for dynamic allocation come from the algorithm presented in Section 3.4. As shown in the figure, Blue's dynamic allocation strategy increases the long-run reward rates for both players, for $s \in (0.2, 0.4]$. In other words, dynamic allocation provides a way for the two players to cooperate, so both can do better.

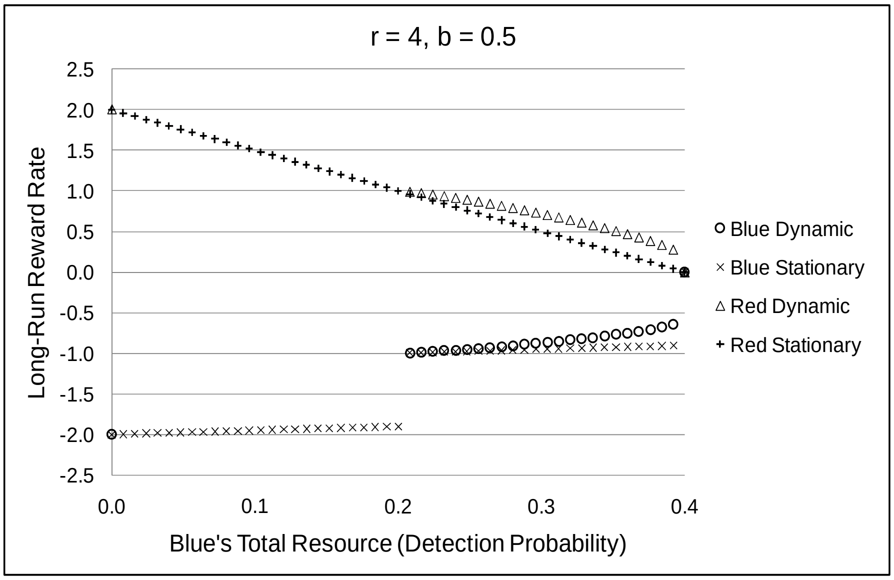

Figure 3.2: The long-run reward rate for Blue and Red with stationary and dynamic allocations, with $r = 4, b = 0.5$.

When is dynamic allocation useful? When *r* becomes larger, a detected attack results in a more serious consequence for Red. Therefore, dynamic allocation becomes more useful, as Red can benefit more from attacking at the right time. When *b* becomes larger (closer to 1), Blue cares less about whether an attack is detected. Instead, Blue should shift his focus to reducing Red's overall attack rate. Therefore, dynamic allocation is also more useful. When both *r* and *b* are small, however, it is possible that dynamic allocation does not provide any benefit at all. Figure 3.3 shows such an example with $r = 1, b = 0.1$. When $s \le 0.8$, the optimal dynamic allocation strategy calls for $y^* = 0$ and $z^* = 0$, which reduces to stationary allocation.

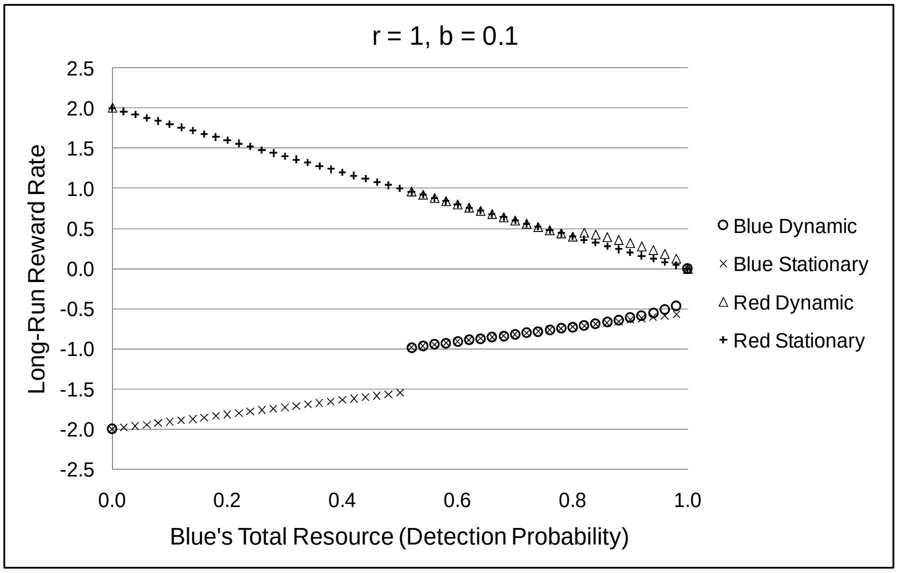

Figure 3.3: The long-run reward rate for Blue and Red with stationary and dynamic allocations, with $r = 1, b = 0.1$.

4. SUMMARY

We have addressed two forms of decoy that may arise in IED warfare. The first is the use of fake IEDs by Red in order to delay Blue's RCPs, and the second is the use of understaffed surveillance towers by Blue to deter Red's IED attacks. In each case, we use a mathematical model to quantify the effect of the decoy. On a tactical level, our models provide the optimal use of decoys, and countermeasures to them, in different scenarios. On a strategic level, our findings provide insights into the circumstances when decoys are expected to play a significant role in IED warfare.

There are many extensions to our models that warrant further research. For fake IEDs, a possible extension is to incorporate more than one type of real IEDs, as real IEDs range from roadside bombs to explosively-formed projectiles. Another extension is to generalize the model to deal with a network of roads, rather than just a collection of independent road segments. RCPs invariably have a base of operations, and have to follow patrol routes that obey network constraints. For decoy surveillance towers, one extension is to allow the two towns to have different parameters to accommodate different levels of insurgent activities. It is also conceivable that detecting an attack in one town is more valuable than that in the other town. Another extension is to study the dynamic allocation when there are more than two surveillance towers.

APPENDIX

Proof of Proposition 3.1.

To facilitate the proof, let

$$K_1 \equiv 2-(1+r)s,$$
$$K_2 \equiv (1+r)(2p-s),$$

and use Equations (3.3) and (3.8) to get

$$\frac{K_1}{K_2} = \frac{\frac{2}{(1+r)} - s}{2p-s} = \frac{2\hat{p}-s}{2p-s} = e^{-2y\hat{t}} < 1 .$$

We can simplify $R(z)$ to

$$\begin{aligned} R(z) &= \frac{c-\alpha z}{4}\left(K_1\left(1+e^{-z\hat{t}}\right) + K_2 \frac{z}{z+2y}\left(1-e^{-(z+2y)\hat{t}}\right)\right) \\ &= \frac{c-\alpha z}{4} K_2 \left(e^{-2y\hat{t}}\left(1+e^{-z\hat{t}}\right) + \frac{z}{z+2y}\left(1-e^{-(z+2y)\hat{t}}\right)\right). \qquad (3.14) \\ &= K_2 \frac{c-\alpha z}{4}\left(e^{-2y\hat{t}} + \frac{z}{z+2y} + \frac{2y}{z+2y} e^{-(z+2y)\hat{t}} \right) \end{aligned}$$

We will show $R''(z) < 0$ to complete the proof. To facilitate the computation, let

$$g(z) = \frac{c-\alpha z}{4},$$
$$h(z) = e^{-2y\hat{t}} + \frac{z}{z+2y} + \frac{2y}{z+2y} e^{-(z+2y)\hat{t}},$$

so $R''(z) = K_2(g''(z)h(z) + 2g'(z)h'(z) + g(z)h''(z))$.

First, compute $g'(z) = -\alpha/4 < 0$ and $g''(z) = 0$. For $h(z)$, taking the first derivative yields

$$\begin{aligned} h'(z) &= \frac{2y}{(z+2y)^2}\left(1 - e^{-(z+2y)\hat{t}} - (z+2y)\hat{t}e^{-(z+2y)\hat{t}}\right) \\ &= \frac{2y}{(z+2y)^2}\left(1 - e^{-(z+2y)\hat{t}}\left(1+(z+2y)\hat{t}\right)\right) \\ &> \frac{2y}{(z+2y)^2}\left(1 - e^{-(z+2y)\hat{t}} e^{(z+2y)\hat{t}}\right) = 0 \end{aligned},$$

where the inequality follows by letting $\Delta = (z+2y)\hat{t} > 0$ in the inequality $1+\Delta \le e^{\Delta}$.

In addition,

$$
\begin{aligned}
h''(z) &= \frac{4y}{(z+2y)^3}\left(-1+e^{-(z+2y)\hat{t}}+(z+2y)\hat{t}e^{-(z+2y)\hat{t}}+\frac{1}{2}\left((z+2y)\hat{t}\right)^2 e^{-(z+2y)\hat{t}}\right) \\
&= \frac{4y}{(z+2y)^3}\left(-1+e^{-(z+2y)\hat{t}}\left(1+(z+2y)\hat{t}+\frac{1}{2}\left((z+2y)\hat{t}\right)^2\right)\right) \\
&< \frac{4y}{(z+2y)^3}\left(-1+e^{-(z+2y)\hat{t}}e^{(z+2y)\hat{t}}\right)=0,
\end{aligned}
$$

where the inequality follows by letting $\Delta=(z+2y)\hat{t}>0$ in the inequality $1+\Delta+\dfrac{\Delta^2}{2}\leq e^{\Delta}$. Consequently, $R''(z)<0$, so $R(z)$ is concave in z.

LIST OF REFERENCES

Hershaft, A. (1968). Effectiveness of imperfect decoys. *Operations Research*, *16*(1), 10-17.

Kress, M., Lin, K.Y., & Szechtman, R. (2008). Optimal discrete search with imperfect specificity. *Mathematical Methods of Operations Research*, *68*(3), 539-549.

Lu, X., Yang, L., & Yang, H. (2008). Decoy's operational jamming effect. *Defense Science Journal*, *58*(3), 405-408.

Ross, S.M. (1996). *Stochastic processes* (2nd ed.). Wiley.

Stone, L. (2004). *Theory of optimal search* (2nd ed.). INFORMS.

United States Army. (2010). Improvised explosive devices, suicide bombers, unexploded ordnance, and mines. In Field Manual 3-21.10, The infantry rifle company, Appendix G. Retrieved (8/18/2010) from https://rdl.train.army.mil/soldierPortal/atia/adlsc/view/public/23168-1/FM/3-21.10/appg.htm .

United States Department of War. (1942). Enemy antitank mine fields and booby traps in Africa. *Tactical and Technical Trends*, 6. Retrieved (8/18/2010) from http://www.lonesentry.com/articles/ttt08/antitank-mine-fields.html .

Washburn, A. (2005). The band-soak theory of missile attack and terminal defense. *Military Operations Research*, *10*(1), 15-23.

Washburn, A., & Ewing, P.L. (2010). Allocation of clearance assets in IED warfare. *Naval Research Logistics* (forthcoming).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Research Office (Code 09)...1
   Naval Postgraduate School
   Monterey, CA 93943-5000

2. Dudley Knox Library (Code 013)...2
   Naval Postgraduate School
   Monterey, CA 93943-5002

3. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

4. Richard Mastowski (Technical Editor)...2
   Graduate School of Operational and Information Sciences (GSOIS)
   Naval Postgraduate School
   Monterey, CA 93943-5219

5. Associate Professor Kyle Y. Lin...1
   Department of Operations Research
   Naval Postgraduate School
   Monterey, CA 93943-5219

6. Distinguished Professor Emeritus Alan Washburn...1
   Department of Operations Research
   Naval Postgraduate School
   Monterey, CA 93940-5219

7. Professor Gordon Bradley...1
   Department of Operations Research
   Naval Postgraduate School
   Monterey, CA 93943-5219

8. Dr. Charles Kimzey 1
   National Security Institute
   Naval Postgraduate School
   777 Dyer Road, Bullard 118
   Monterey, CA 93943

9. Ms. Jane Barreto 1
   Department of Information Sciences
   Naval Postgraduate School
   Bullard Hall, Room 108A
   Monterey, CA 93943

10. Dr. Sue K. Numrich 1
Institute for Defense Analysis
4850 Mark Center Drive
Alexandria, VA 22311-1882

11. Dr. Kathleen Carley 1
Department of Social & Decision Sciences
Carnegie Mellon University
Pittsburgh, PA 15213

12. Mr. Jack Keane 1
Global Management Department
Aviation Systems Engineering Group
Johns Hopkins University Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723-6099

13. Dr. Niki C. Goerger 1
Department of Systems Engineering
Attn: MADN-SE
United States Military Academy
Bldg. 752, 4th Floor, Room 403B
West Point, NY 10996-1905

14. Dr. Jonathan Caulkins...1
Heinz School
Carnegie Mellon University
Pittsburgh, PA 15213-3890