Risk and Uncertainty in Bio-surveillance having Imperfect Detection Rates

David R. Fox
Colin Thompson
University of Melbourne, Australian Centre of Excellence for Risk Analysis
Parkville, Australia 3010
david.fox@unimelb.edu.au

1. Introduction

Since the events of September 11 2001, there has been increased emphasis on monitoring and surveillance to detect and prevent further terrorist attacks. While significant resources have been devoted to the *mechanics* of screening, far less attention has been paid to quantifying the efficacy of these surveillance programs. Unlike the industrial setting where there is generally good information on the performance of the manufacturing process (eg. percent defective; proportion of non-conforming or 'out-of-spec' items), monitoring in the context of bio / homeland security is characterised by extreme uncertainty.

In contrast to traditional methods of (constrained) optimisation, Ben-Haim (2006) developed Info-Gap theory to identify robust solutions to decision-making problems under extreme uncertainty. Info-gap theory has recently been applied to assessing the performance of counter-terrorism surveillance programs (Moffitt et al. 2005) and the identification of robust strategies to deal with bioterrorism attacks (Yoffe and Ben-Haim 2006). Thompson (unpublished) examined the general sampling problem associated with inspecting a random sample of *n* items (containers, flights, people, etc.) from a finite population of *N* such items in a biosecurity context using an info-gap approach. The basic situation considered is that there is a probability $p(n)$ of a catastrophic outcome (eg. terrorist attack) given that *n* events / items out of *N* have been inspected. Thompson's (unpublished) info-gap formulation of the problem permitted the identification of a sample size n such that $p(n)$ did not exceed a nominal threshold, π_c when severe uncertainty about $p(n)$ existed. Implicit in this formulation was the assumption that the detection probability (ie. the probability of detecting a weapon, adverse event, anomalous behaviour etc.) once having observed or inspected the relevant item / event / behaviour was unity. In the context of counter-terrorism, our uncertainties (or info-gaps) will most certainly extend to a lack of certitude in detection.

In the following sections we describe the general surveillance problem for which the probability of detection is less than unity. We then provide an info-gap formulation to help identify sampling strategies that are robust to multiple sources of uncertainty – including the detection probability.

2. Surveillance with imperfect detection

Following Thompson (unpublished), we assume that there is a finite population of *N* objects, events, people, or behaviours that are potentially subject to inspection. From this population of *N* 'objects' a random sample of size *n* is to be inspected. We define the following events:

I – the event that an object is inspected;
W – the event that an object is a security threat (eg. the object is a weapon, the person is a terrorist, the behaviour is indicative of malicious intent);
D – the event that the security breach is identified / detected.

Furthermore, we assume that only inspected objects are classified as either belonging to D or $\overline{D}$.
In a biosecurity / counter-terrorism context, arguably, the most important probability is *not* $P[W]$ (the probability of a security threat) but rather it is the *conditional probability* $P\left[W \middle| \overline{D}\right]$ ie. the probability of a security threat *given* that no breach of security was detected.

The lack of detection of a security breach is due to: (i) the absence of a security threat; and/or (ii) imperfections of the detection equipment / method/ process. Our inability to distinguish between (i) and (ii) is an info-gap.

Problem formulation

From elementary probability theory:

$$P\left[W\left|\overline{D}\right.\right]=\frac{P\left[W\cap\overline{D}\right]}{P\left[\overline{D}\right]} \tag{1}$$

Now, $P\left[W\cap\overline{D}\right]=P[I]-P\left[D\middle|W\right]P[W]-P\left[\overline{D}\middle|\overline{W}\right]P\left[\overline{W}\right]-P\left[D\middle|\overline{W}\right]P\left[\overline{W}\right]$ (2)

Note that $P\left[\overline{D}\middle|\overline{W}\right]=1$ and $P\left[D\middle|\overline{W}\right]=0$.

We next define the *detection efficiency,* θ as $P\left[D\middle|W\right]$ i.e. the probability that a security breach will be detected given a threat actually exists. Furthermore, we let $\phi=P[W]$ be the *unconditional* probability that an object is a security threat and $\lambda=P[I]=n/N$ the inspection fraction or probability. It can be shown that equation (1) can be written as

$$P\left[W\left|\overline{D}\right.\right]=\frac{\phi(\lambda-\theta)}{\phi(\lambda-\theta)+(1-\phi)}=p(\lambda,\theta,\phi) \tag{3}$$

Notice that for the probability in equation (3) to be non-negative $\lambda\geq\theta$ i.e the sampling fraction must be at least as large as the detection efficiency. Note, that when 100% inspections are performed, the conditional probability in equation (3) becomes

$$P\left[W\left|\overline{D}\right.\right]=\frac{\phi(1-\theta)}{1-\theta\phi}=p(1,\theta,\phi) \tag{4}$$

and under these conditions, this probability is only zero when the detection efficiency is 100%. For 0% detection efficiency $p(1,0,\phi)$ is ϕ - the unconditional probability that the object is a security threat. Furthermore, whenever the inspection rate is $\leq 100\%$, $p(\lambda,\theta,\phi)$ *underestimates* $p(1,\theta,\phi)$. This underestimation may be regarded as the 'cost' associated with less than complete inspection. We thus define our performance criterion Ψ to be the ratio $\frac{p(\lambda,\theta,\phi)}{p(1,\theta,\phi)}$, thus

$$\Psi(\lambda,\theta,\phi)=\frac{\phi(\lambda-\theta)}{\phi(\lambda-\theta)+(1-\phi)}\cdot\frac{1-\theta\phi}{\phi(1-\theta)} \tag{5}$$

We next consider an info-gap formulation to assess the effects of uncertainty in key parameters (namely θ and ϕ) on the performance criterion given by equation (5).

3. An Info-Gap model for surveillance performance

Information-gap (hereafter referred to as info-gap) theory is a recent development designed to assist decision makers faced with severe uncertainty (Ben-Haim 2006, Regan et al. 2005, Carmel and Ben-Haim 2005). Info-gap theory aims to address the "robustness" of decision making under uncertainty. It asks the question: how wrong can a model and its parameters be without jeopardising the quality of decisions made on the basis of this model?

Info-gap theory derives its robustness functions from three elements: a performance measure, a process model and a non-probabilistic model of uncertainty. The performance measure is a statistical, economic or bio-physical metric of value to the decision maker. The decision maker may wish to increase the performance measure (e.g. dollar value of a share portfolio) or reduce it (e.g. probability of not detecting a terrorist attack). In each case there is often a critical performance value which defines a change in decision. In our case, the performance measure is Ψ - effectively the reduction in surveillance efficacy when less than 100% inspection is employed.

The process model is a mathematical summary of the system in question. It describes the relationship between the performance measure and the important characteristics of the system in question. In this example the performance threshold is the maximum tolerable reduction in surveillance efficacy and the process model is given by equation (8).

The info-gap model of uncertainty for the uncertain quantities Θ in the process model is the unbounded family of nested sets $U\left(\alpha,\tilde{\Theta}\right)$ of possible realisations Θ, where α represents the unknown "horizon of uncertainty" and $\tilde{\Theta}$ our best or initial estimate of Θ. This model satisfies two axioms:

contraction: $$U\left(0,\tilde{\Theta}\right)=\left\{\tilde{\Theta}\right\} \tag{6}$$

nesting: $$\alpha<\alpha' \Rightarrow U\left(\alpha,\tilde{\Theta}\right)\subset U\left(\alpha',\tilde{\Theta}\right) \tag{7}$$

The contraction axiom states that in the absence of uncertainty $\left(\alpha=0\right)$, our best estimate $\tilde{\Theta}$ is correct, while the nesting axiom states that the range of uncertain variation increases as the horizon of uncertainty increases. In all cases α is unknown and unbounded with $\alpha\geq 0$. In this example the uncertain quantities are the detection efficiency θ and ϕ, the probability that an object is a security threat. Thus, $\Theta=\left(\theta,\phi\right)$ and our initial or best estimate of these parameters is denoted $\tilde{\Theta}=\left\{\tilde{\theta},\tilde{\phi}\right\}$.

In this section we consider uncertain parameter values – the detection efficiency θ and the probability that an object is a security threat, ϕ. The fractional errors $\left|\left(\theta-\tilde{\theta}\right)/\tilde{\theta}\right|$ and $\left|\left(\phi-\tilde{\phi}\right)/\tilde{\phi}\right|$ are unknown. With this prior information we formulate the following fractional-error info-gap model:

$$U\left(\alpha,\tilde{\theta},\tilde{\phi}\right)=\left\{\begin{array}{ll}(\theta,\phi): & \max\left[0,\left(1-\alpha\right)\tilde{\theta}\right]\leq\theta\leq\min\left[1,\left(1+\alpha\right)\tilde{\theta}\right] \\ & \max\left[0,\left(1-\alpha\right)\tilde{\phi}\right]\leq\phi\leq\min\left[1,\left(1+\alpha\right)\tilde{\phi}\right]\end{array}\right\},\quad \alpha\geq 0 \tag{8}$$

This is a bounded family of nested sets of $\left\{\tilde{\theta},\tilde{\phi}\right\}$ values with the sets becoming more inclusive as the horizon of uncertainty, α increases. The definition of the performance measure, process model and uncertainty model(s) completes the specification of the formulation of the info-gap analysis.

We now turn to the derivation of the robustness function. In info-gap parlance "robustness" is defined as the greatest horizon of uncertainty, across all uncertain model components, such that the performance measure still meets the pre-defined requirement. In our application the robustness of a surveillance regime in which λ x100% of the target population is inspected, is the greatest horizon of uncertainty $\hat{\alpha}$ for which all combinations of the uncertain parameters $\tilde{\Theta}=\left\{\tilde{\theta},\tilde{\phi}\right\}$ the minimum required inspection performance is achieved, that is

$$\hat{\alpha}\left(\lambda,\gamma_d\right)=\max\left\{\alpha:\left(\min_{(\theta,\phi)\in U\left(\alpha,\tilde{\theta},\tilde{\phi}\right)}\Psi\left(\lambda,\theta,\phi\right)\geq\ \gamma_d\right)\right\} \tag{9}$$

where γ_d is the required value of Ψ. Equation (9) is the robustness function for this application of the info-gap model. The strategy of robust-satisficing (Ben-Haim 2006) is to attempt to guarantee an adequate level of surveillance performance, by choosing a value of λ which is highly robust to uncertainty. Thus, for any inspection fraction λ, the robustness function indicates the confidence in attaining the minimum performance requirement with that λ. Examination of the process model (equation 5) reveals that it is a monotonic decreasing function with respect to θ and a monotonic increasing function with respect to ϕ. Combining this observation with the uncertainty model (equation 8) allows us to write the inner minimum of the robustness function (equation 9) as

$$h\left(\alpha,\lambda,\theta,\phi\right)\geq\gamma_d \tag{10}$$

where $$h\left(\alpha,\lambda,\theta,\phi\right)=\frac{\left(1-\alpha\right)\phi\left[\lambda-\left(1+\alpha\right)\theta\right]}{\left(1-\alpha\right)\phi\left[\lambda-\left(1+\alpha\right)\theta\right]+\left[1-\left(1-\alpha\right)\phi\right]}\cdot\frac{1-\left(1-\alpha^2\right)\theta\phi}{\left(1-\alpha\right)\phi\left[1-\left(1+\alpha\right)\theta\right]} \tag{11}$$

4. Illustrative Example

Suppose new intelligence suggested that a terrorist attack of an aircraft was imminent and that the mode of attack was thought to involve a previously undetected chemical woven into the fabric of a passenger's clothes. The exact nature of the chemical is unknown and hence no test is available to detect it. Airport security staff have no clear idea what they are looking for except that the have been instructed to closely monitor the appearance, texture, and integrity of passengers' clothes. Our best guess of the parameters $\tilde{\Theta} = \left\{\tilde{\theta}, \tilde{\phi}\right\}$ is $\tilde{\phi} = 0.7$ and $\tilde{\theta} = 0.05$ although considerable uncertainty exists around these figures. Figure 1 plots the performance function $\Psi\left(\lambda, \theta, \phi\right)$ as a function of robustness for a range of λ values.

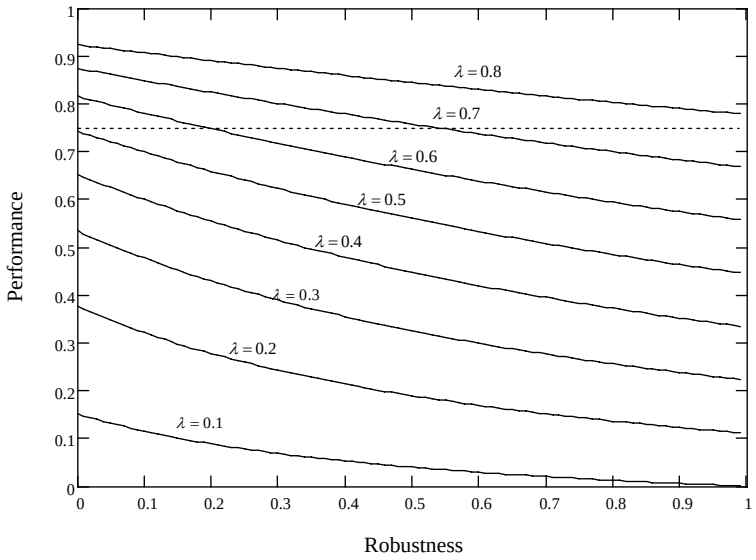

Figure 1. Robustness of surveillance performance for various sampling fractions (lambda).

In recognition that 100% detailed inspection of all passengers is not feasible, a reduced level of surveillance will be tolerated provided the reduction in performance (relative to complete inspection) is no less than 25%. The dashed horizontal line in Figure 1 is thus our minimum performance requirement. To meet this performance requirement a minimum of 50% of passengers will have to be screened. At this level of screening, the robustness to uncertainty is zero and hence, if our initial estimates of the probability of an attack or of the detection probability are wrong, the performance requirement will not be met. Increasing the surveillance rate to 60% results in 20% robustness, while a surveillance rate of 70% will guarantee the performance requirement is met even if our initial guesses for the parameters are in error by 50%.

REFERENCES

Ben-Haim, Y. (2006). *Information-gap decision theory: Decisions under severe uncertainty*. 2nd. edition, Academic Press, San Diego.

Carmel, Y. and Ben-Haim, Y. (2005) , Info-gap robust-satisficing model of foraging behavior: Do foragers optimize or satisfice? American Naturalist, 166: 633-641.

Moffitt, L.J., Stranlund, J.K., and Field, B.C. (2005). Inspections to Avert Terrorism: Robustness Under Severe Uncertainty. Journal of Homeland security and Emergency Management, 2(3), 1-17.

Regan, H.M, Ben-Haim, Y., Langford, W., Wilson, W.G., Lundberg, P., Andelman, S.J, and Burgman, M.A. 2005, Robust decision making under severe uncertainty for conservation management, Ecological Applications, 15(4) ,1471-1477.

Thompson, C.J. (unpublished) Modelling Risk and Uncertainty in Bio- and Homeland security. Presented at Australian and New Zealand Society for Risk Analysis Conference, University of Melbourne, July 17-19, 2006.

Yoffe, A. and Ben-Haim, Y. (2006) An Info-Gap Approach to Policy Selection for Bio-Terror Response. IEEE International Conference on Intelligence and Security Informatics, ISI 2006, San Diego, CA, USA May 23-24 2006, pp.554-559.