INTERDICTION MODELING FOR SMUGGLED NUCLEAR MATERIAL

Nedialko B. Dimitrov, Marc A. Gonzalez, Dennis P. Michalopoulos, David P. Morton,
Michael V. Nehme, Elmira Popova, Erich A. Schneider and Gregory G. Thoreson
The University of Texas at Austin, Austin, TX 78712 USA

ABSTRACT

We describe a stochastic interdiction model on a transportation network consisting of two adversaries: a nuclear-material smuggler and an interdictor. The interdictor first installs radiation detectors on the network. These installations are transparent to the smuggler, and are made under an uncertain threat scenario, which specifies the smuggler's origin and destination, the nature of the material being smuggled, the manner in which it is shielded, and the mechanism by which the smuggler will select a route. The interdictor's goal is to minimize the probability the smuggler avoids detection. The performance of the detection equipment depends on the material being sensed, geometric attenuation, shielding, cargo and container type, background, time allotted for sensing and a number of other factors. Using a stochastic radiation transport code (MCNPX), we estimate detection probabilities for a specific set of such parameters, and inform the interdiction model with these estimates.

INTRODUCTION

The Department of Homeland Security (DHS) has been installing portal detectors in the US and these installations will likely continue [8]. The Second Line of Defense (SLD) program of the US Department of Energy (DOE) seeks to reduce the risk of illicit trafficking of nuclear material through international airports, seaports and border crossings. The program's initial efforts were in Russia but have grown to include other key transit states in Eurasia.

The DHS and DOE are addressing a real threat. In the early 1990s, Russia inherited roughly 600-850 metric tons of highly-enriched uranium (HEU) and plutonium [9], and the nuclear ambitions of rogue nations make daily news. An International Atomic Energy Agency (IAEA) database includes over 1000 incidents of trafficking of nuclear and radioactive material from 1993-2006 [10]. 55% of these involved nuclear material and 18 involved weapons-grade uranium or plutonium. Sometimes a smuggler's intent is difficult to discern, but according to the IAEA report, many of the thefts of material were motivated by profit and a perceived demand on the illegal market. Other smuggling attempts were apparently motivated by malicious intent. US efforts to assist the Former Soviet Union in securing nuclear material are ongoing, but by themselves, insufficient. An accurate inventory of the nuclear material that existed at the beginning of the 1990s seems impossible.

SLD's first detector installation was at Moscow's Sheremetyevo International Airport in September 1998. The equipment's installation was dedicated with a ribbon-cutting ceremony [4]. According to the DOE, such detector installations have two purposes: (i) to deter potential theft and smuggling of nuclear material and (ii) to detect and therefore prevent actual smuggling attempts.

Importantly, considerable effort is being devoted to developing more sophisticated radiation detectors. Less attention is devoted to how to best deploy these detectors over a system-wide network to deter and interdict the smuggling of nuclear material. Well-designed deployment can significantly improve system performance, and in this paper, we describe a stochastic network interdiction model for locating radiation detectors. A key input to our interdiction model is the ability of radiation detectors to sense nuclear material. Using plastic scintillator radiation portal monitors (RPMs) as a baseline detector, we employ the stochastic radiation transport code MCNPX (Monte Carlo N-Particle Extended) [3] to estimate detection probabilities (DPs) under specific threat scenarios.

STOCHASTIC NETWORK INTERDICTION PROBLEM

First, we describe our stochastic network interdiction problem (SNIP) on a general transportation network, which could involve multiple countries. Then, we specialize to the computationally simpler case of placing detectors on the border of one country. We call this model BiSNIP, as it is SNIP specialized to a bipartite network, which we describe in detail below.

We model two adversaries, an interdictor and a smuggler, and an underlying transportation network $G(N,A)$. The smuggler starts at source node $s \in N$ and wishes to reach terminal node $t \in N$. The probability that the smuggler will be detected while traversing arc $(i,j) \in A$ is q_{ij} if (i,j) has a detector and $p_{ij} < q_{ij}$ if not. A smuggler can be caught by indigenous law enforcement without detection equipment, and so $p_{ij} > 0$. Detection events on distinct arcs are assumed to be mutually independent. The smuggler chooses an *s*-*t* path to maximize his evasion probability. With limited resources, the interdictor must select arcs on which to install detectors in order to minimize this probability.

The *threat scenario*, indexed by $\omega \in \Omega$, is unknown when detectors are installed, but is governed by a probability mass function, $p^{\omega}, \omega \in \Omega$. A threat scenario specifies the origin-destination pair, (s^{ω}, t^{ω}), as well as other details about the material being smuggled and the manner in which it is shielded. So, we have scenario-dependent DPs, q_{ij}^{ω} and p_{ij}^{ω}. The probability the smuggler traverses the network undetected is a sum of (conditional) evasion probabilities, each weighted by p^{ω}, over all threat scenarios. The timing of decisions and realizations is as follows: First, the interdictor installs detectors on a subset of the network's arcs subject to a budget constraint. Then, a threat scenario reveals and the smuggler selects an s^{ω}-t^{ω} path. We conservatively assume the smuggler selects a path with full knowledge of the detector locations and evasion probabilities.

Transparency of detector locations is reasonable in Russia as the initial installation was accompanied by a ribbon-cutting ceremony, and subsequent installations were reported in the news. Completely sealing Russia's 12,500 miles of borders is impractical, and so, in addition to catching nuclear smugglers, the SLD program seeks to deter would-be smugglers, e.g., who seek financial gain.

Further notation and the SNIP formulation follow:

Network and sets:	
$FS(i)$	set of arcs leaving node i
$RS(i)$	set of arcs entering node i
$AD \subset A$	arcs on which detectors may be placed
Data:	
b	total budget for installing detectors
c_{ij}	cost of installing a detector on arc $(i,j) \in AD$
Decision variables:	
x_{ij}	1 if a detector is installed on arc (i,j) and 0 otherwise
Smuggler's decision variables:	
y_{ij}	positive only if smuggler traverses (i,j) and no detector is installed
z_{ij}	positive only if smuggler traverses (i,j) and a detector is installed

Formulation:

$$\min_{x \in X} \sum_{\omega \in \Omega} p^{\omega} h(x,\omega), \tag{1}$$

where $X = \{x : \sum_{(i,j)\in AD} c_{ij}x_{ij} \le b, x_{ij} \in \{0,1\}, (i,j) \in AD\}$, and where

$$\begin{aligned}
h(x,\omega) = \max_{y,z} \;& y_{t^{\omega}} && \text{(2a)}\\
\text{s.t.} \;& \sum_{(s^{\omega},j)\in FS(s^{\omega})} \big(y_{s^{\omega}j} + z_{s^{\omega}j}\big) = 1 && \text{(2b)}\\
& \sum_{(i,j)\in FS(i)} (y_{ij} + z_{ij}) = \sum_{(j,i)\in RS(i)} \big((1-p^{\omega}_{ji})y_{ji} + (1-q^{\omega}_{ji})z_{ji}\big), \quad i \in N \setminus \{s^{\omega}, t^{\omega}\} && \text{(2c)}\\
& y_{t^{\omega}} = \sum_{(j,t^{\omega})\in RS(t^{\omega})} \Big((1-p^{\omega}_{jt^{\omega}})y_{jt^{\omega}} + (1-q^{\omega}_{jt^{\omega}})z_{jt^{\omega}}\Big) && \text{(2d)}\\
& 0 \le y_{ij} \le 1 - x_{ij}, \quad (i,j) \in A && \text{(2e)}\\
& 0 \le z_{ij} \le x_{ij}, \qquad (i,j) \in AD. && \text{(2f)}
\end{aligned}$$

The value, $h(x,\omega)$, is the conditional evasion probability, given ω. The goal is to install detectors via $x \in X$ to minimize the evasion probability over all threat scenarios, i.e., to minimize the objective function in (1). SNIP with h defined in (2) is a bilevel stochastic mixed-integer program (MIP).

A simplified version of SNIP arises when we restrict attention to placing detectors at border crossings of a single country. In SLD, the initial goal was to deter smuggling out of Russia. Another single-country model would install detectors to minimize the probability a smuggler could enter the US with nuclear material. The key to simplifying the formulation for the single-country case is that each s^{ω}-t^{ω} path has exactly one arc on which the smuggler could encounter a detector. For a smuggler under threat scenario ω, let AD^{ω} be the set of such *checkpoint* arcs. For each ω, we compute the values of the maximum-reliability paths from s^{ω} to the tail of each checkpoint arc and from the head of each checkpoint arc to t^{ω}. Call the product of these two probabilities γ^{ω}_k, $k = (i,j) \in AD^{\omega}$. Then,

$$h(x,\omega) = \max_{k \in AD^{\omega}} \{\gamma^{\omega}_k(1-p^{\omega}_k)(1-x_k), \gamma^{\omega}_k(1-q^{\omega}_k)x_k\} \tag{3}$$

is the probability the smuggler under ω avoids detection. Linearizing (3), we obtain the MIP:

$$\begin{aligned}
\min_{x,\theta} \quad & \sum_{\omega\in\Omega} p^{\omega}\theta^{\omega}\\
\text{s.t.} \quad & x \in X\\
& \theta^{\omega} \ge \gamma^{\omega}_k(1-p^{\omega}_k)(1-x_k), \; k \in AD^{\omega}, \omega \in \Omega \qquad (4)\\
& \theta^{\omega} \ge \gamma^{\omega}_k(1-q^{\omega}_k)x_k, \qquad k \in AD^{\omega}, \omega \in \Omega.
\end{aligned}$$

BiSNIP (4) may be viewed on a bipartite network with arcs (ω,k) linking each threat scenario with its checkpoints. Excluding the checkpoint, γ^{ω}_k is the smuggler's probability of traveling from s^{ω} to t^{ω}, via k, undetected. This is multiplied by $1-q^{\omega}_k$ or $1-p^{\omega}_k$ depending on whether a detector is installed at k. Model (4) again minimizes the (unconditional) probability the smuggler avoids detection.

There is a modest but growing literature on network interdiction. The base model we describe in this section was first proposed in [14] and more fully developed in [15] as is its bipartite special case in [13]. See [1] for further related work.

DETECTION PROBABILITIES

The probability that a smuggler ω will be sensed by a radiation detector installed on $(i,j) \in A$ is $1-q_{ij}^{\omega}$. These are key model parameters, and we now turn to estimating the detection probability (DP) associated with each detector, under various threat scenarios ω. In this section we first discuss detection modeling and DP calculation in a general sense. We then describe DP calculations for a specific example, which is used in the next section to analyze a specific BiSNIP model instance.

In addition to specifying the smuggler's origin-destination pair, a threat scenario includes: (i) the type of special nuclear material (SNM), i.e., weapons-grade plutonium (WGPu), reactor-grade plutonium, natural uranium, low-enriched uranium, highly-enriched uranium (HEU), fresh nuclear fuel, and spent nuclear fuel; (ii) SNM mass, where we consider masses of nuclear materials from milligrams to IAEA significant quantities; (iii) shielding, e.g., lead, borated-polyethylene and steel in different geometries and thicknesses; and, (iv) vehicle in which the material is concealed, e.g., personal luggage, truck-trailers, passenger cars, rail-cars, ships, and shipping containers. The DP can be derived as a function of (i)-(iv) and the detection equipment, survey strategy, and alarm algorithm.

We derive DPs by simulating detector response to a radioactive source via MCNPX. Alarm algorithms are applied to these results to translate count rate probability density functions (PDFs) into detection probabilities. Multiple issues complicate DP computation. NORM (naturally occurring radioactive material) and other authorized radionuclide-bearing cargos can induce false or "nuisance" alarms at detection portals. NORM-bearing payloads include fertilizer, cat litter, granite and marble. Compared to background, radiation from most NORM increases detector count rates but does not dramatically alter spectra. This can aid in alarm algorithm design to mitigate nuisance alarms, but it can also be used to conceal special nuclear material (SNM). A smuggler might use NORM, e.g., actinide-bearing NORM such as granite, to obfuscate an SNM radiation field. We obtain spectra for selected NORM from published data (e.g., [6] provides spectra for tile and fertilizer) where available.

Nuisance alarms occur when NORM causes the count rate to exceed the alarm threshold. Statistical false alarms, on the other hand, arise when this threshold is exceeded in the absence of any radioactive source, NORM or otherwise. Alarm thresholds are typically selected to control the false alarm probability (FAP). That said, alarm thresholds are parameters we can control. The FAP also depends on interrogation time, which is a primary concern for portal detectors, where many short measurements generate a spatial spectrum profile. Checkpoints with portal detectors therefore employ a two-tier screening process where the primary detector's alarm produces a secondary inspection. Our focus is on the primary detector as opposed to detailed modeling of the two-tiered system.

Vehicle-specific factors affect FAP. Setting aside shielding by cargo space, vehicle profiles must be considered because they shield background radiation. This baseline depression due to the vehicle profile can be approximately compensated for in real-time detection. An alarm algorithm can adjust alarm thresholds based on baseline depression by vehicle type predicted using a particle transport model or empirical data. Lo Presti has developed an extensive library of depressions by vehicle type and detector location [12]. A second method [6] bins detector signals into energy windows. This method is viable because most baseline depression does not strongly affect count ratios between energy bins. This approach can increase detector sensitivity by a factor of up to five [5].

Given the threshold, count rates and spectra and alarm algorithm, we compute the DP using the method of Geelhood [7], which applies to both active and passive detection systems and involves three steps. First, the expected value of the detection metric for a vehicle containing no source, NORM or otherwise, is established. The metric may be gross count rate with or without baseline suppression correction, photopeak count rate, or energy bin count ratio, depending on the alarm algorithm. Second, a PDF for the detection metric for the fleet of vehicles to be screened—vehicles without any source and those carrying NORM—is established. Third, the detection metric PDF for the smuggled cargo is calculated. The latter two calculations reflect both statistical and systematic variability; sampling the position of the smuggled cargo from multiple possible locations within a cargo container exemplifies the systematic component. With these PDFs in hand, the alarm threshold is chosen so the FAP is acceptable in view of traffic flow and secondary screening capacity.

We now turn to our example calculation, involving WGP smuggled in a truck-trailer. We use a standard 53-foot truck-trailer, and the background radiation is that of the U.S. average terrestrial. The detector consists of two PVT panels with dimensions 3.8 cm × 36 cm × 173 cm. The SNM is chosen as one IAEA significant quantity of WGPu: an 8 kg sphere, aged 10 years. As we describe below, the shielding is a lead shell whose thickness we vary parametrically. The source spectrum is generated using the RadSrc code package [11]. the detection interval is 0.1 sec. with a vehicle speed of 2.2 mph. We compute detection probabilities using a false alarm probability of 1%.

For simplicity, we drop the ω and (i,j) dependency and denote the detection probability as q. The false alarm probability is denoted, $\underline{q}$, the observation time, t, and the alarm threshold count rate is D. The normal background has count rate B, and variance σ^2_B. The analogous parameters for the suppressed count rate, i.e., suppressed by the concealing vehicle, are $\underline{B}$ and $\sigma^2_{\underline{B}}$. The count rate for the SNM source is denoted S_0 and the variance of the combined process of SNM signal and background is σ^2_s. While a measurement is being taken, the detector measures a superposition of the suppressed background and SNM signals. We employ MCNPX to compute, in three separate radiation transport calculations, the parameters S_0, B and $\underline{B}$. The background calculation assumes typical radionuclide concentrations in soil and concrete. The baseline suppressed background is found to be 13% lower than the unsuppressed background, consistent with experimentally observed values [12].

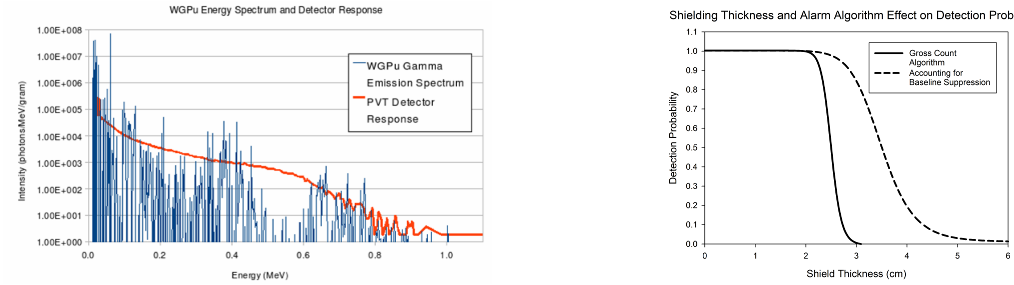
We denote by $F(\cdot,\sigma^2,\mu)$ the cumulative distribution function of a normal random variable with mean μ and variance σ^2. With this notation, we can represent the detection and false alarm probabilities using the standard gross-count algorithm as

$$\begin{aligned} q &= 1 - F(Dt, \sigma^2_s, (S_0 + \underline{B})t) && \text{(5a)} \\ \underline{q} &= 1 - F(Dt, \sigma^2_B, Bt). && \text{(5b)} \end{aligned}$$

We use equations (5) as follows: We first select a value for $\underline{q}$ and then use equation (5b) to determine the alarm threshold count rate, D. Using this value of D in equation (5a) we can determine the detection probability, q. So, the above equations assume that D is computed via equation (5b) using the standard background count process. However, we can refine the alarm algorithm for a given false alarm probability if we instead use the suppressed background process. That is, we use equations:

$$\begin{aligned} q &= 1 - F(Dt, \sigma^2_s, (S_0 + \underline{B})t) && \text{(6a)} \\ \underline{q} &= 1 - F(Dt, \sigma^2_{\underline{B}}, \underline{B}t). && \text{(6b)} \end{aligned}$$

Following the same steps described above with the same initial value of $\underline{q}$, we will find a smaller value of D from equation (6b) and hence a larger detection probability, q from equation (6a). In the analysis of the next section, we view this simple adjustment of the alarm algorithm as a surrogate for a more general situation in which we have a higher-fidelity detector or improved detection algorithm. More extensive MCNPX simulations to be conducted in the future will allow us to address such situations.



(a) Energy spectrum and detector response

(b) Detection Probability

Figure 1: Part (a) of the figure shows the energy spectrum and associated PVT detector response. The detection probabilities as a function of lead shielding thickness, under the algorithms that ignore, and account, for baseline suppression are shown in part (b) of the figure.

NETWORK INTERDICTION RESULTS

We form and solve two sets of BiSNIP models using the type of physics-based DP estimates described in the previous section. Our model is based on a transportation network in Russia, and includes 33 storage sites of SNM, which we model as being vulnerable to theft. We model eight destinations outside of Russia to where a smuggler may wish to travel. We consider five equally-likely lead shielding scenarios of the SNM, and we view these scenarios as surrogates for the smuggler's level of sophistication. This leads to $|\Omega| = 33 \cdot 8 \cdot 5 = 1320$ threat scenarios. In the problem instances we consider we restrict attention to motor vehicle crossings, and model 231 such customs checkpoints departing Russia. A subset of these checkpoints will receive SAIC Exploranium AT-900 PVT detectors, i.e., the type of detector for which we presented DP calculations in the previous section. The transportation network covers 79 Russian oblasts. Since all detectors are identical, we use a cardinality-constrained special case (i.e., in constraint set X) of the BiSNIP model. Our two sets of models are based on two detection algorithms. The first is the standard gross-count algorithm, which does not account for baseline suppression; see equations (5) and the associated discussion. The second detection algorithm accounts for baseline suppression of the transporting cargo truck-trailer; see equations (6). Instead of WGPu, the results presented here are based on HEU, and we again use an 8 kg sphere shielded in a concentric sphere of lead. The indigenous DPs, as well as the probabilities of the threat scenarios, are based on a multi-attribute factor model that uses expert elicitation and is described in detail in [16]. Our MIPs were solved via the commercially-available CPLEX software [2].

Figure 2 shows the evasion probability as a function of the number of detectors we install, and it does so for both alarm algorithms, i.e., with, and without, accounting for baseline suppression. The former alarm algorithm yields smaller evasion probabilities and the gap between the evasion probabilities for the two systems grows with the number of detectors installed. Generally speaking, both sets of results exhibit diminishing returns with respect to decreasing the evasion probability as the number of detectors grows. That said, there are some interesting features, such as the larger drop in evasion probability as we go from 20 to 25 detectors under the baseline suppression alarm algorithm.

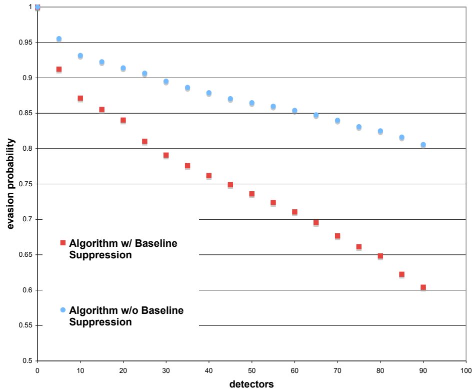


Figure 2: The figure shows the evasion probability as a function of the number of detectors installed for two alarm algorithms, one with and the other without accounting for baseline suppression. The results come from the BiSNIP model restricted to motor crossings in Russia. The objective function value has been scaled so that the evasion probability has value one, if no detectors are installed.

SUMMARY

We have presented a stochastic network interdiction model, which can provide decision support for locating radiation detectors to thwart nuclear smuggling. The model takes as input detection probabilities, which we estimate via physics-based simulations using MCNPX. We compare two alarm algorithms, one which ignores baseline suppression associated with the vehicle used to smuggle SNM, and a second algorithm which accounts for this suppression. We view this as two alternative systems and compare their relative performance. Our aim is not to focus on the benefits of using the baseline suppression algorithm, per se, but rather to show how our interdiction model can compare the merits of alternative systems. For example, we could compare the potential benefits of a novel detector with that of an existing system. The example problem instance we develop is of limited scope: We use a small number of lead shielding scenarios; we restrict attention to motor crossings; we assume a single type of SNM is smuggled in a 53-foot truck trailer; we model only a single type of PVT detector; and, we restrict attention to Russia, as opposed to a more global transportation network. In future work, we will improve the model's scope and fidelity in multiple ways. Our goal in this paper is to demonstrate the type of analyses that can be performed with our interdiction model, and indicate how high-fidelity detection probability calculations can be employed in such a model.

ACKNOWLEDGMENTS

This research was supported by the National Science Foundation through grants CMMI-0653916 and CBET-0736231.

REFERENCES

[1] M. P. Atkinson and L. M. Wein. Spatial queueing analysis of an interdiction system to protect cities from a nuclear terrorist attack. *Operations Research*, 56:247–254, 2008.

[2] ILOG CPLEX 9.0 User's Manual, 2008.

[3] MCNPX User's Manual. Technical Report LA-CP-05-0369, Los Alamos National Laboratory, Los Alamos, New Mexico, 2005.

[4] Department of Energy Press Release: Bill Richardson, Russian Federation Dedicate "Second Line of Defense", US Nuclear Detection Technology to Help Secure Russian Borders, September 2, 1998.

[5] J. Ely and R. Kouzes. Spies, lies and nuclear threats. Technical report, Health Physics Society, Homeland Security Committee, McLean, Virginia, 2005.

[6] J. Ely, R. Kouzes, J. Schweppe, E. Siciliano, D. Strachan, and D. Weier. The use of energy windowing to discriminate SNM from NORM in radiation portal monitors. *Nuclear Instruments and Methods in Physics Research A,*, 560:373–387, 2006.

[7] B. Geelhood. Evaluation of the use of energy thresholds to enhance detection sensitivity using data from Detroit's Fort Street cargo facility. Technical Report PNNL-14282 TM-054, Pacific Northwest National Laboratory, Richland, Washington, 2003.

[8] General Accounting Office, Combatting Nuclear Smuggling: DHS's Decision to Procure and Deploy the Next Generation of Radiation Detection Equipment Is Not Supported by Its Cost-Benefit Analysis, GAO-07-581T, March 2007.

[9] General Accounting Office, Nuclear Nonproliferation: US Efforts to Help Other Countries Combat Nuclear Smuggling Need Strengthened Coordination and Planning, Report to the Ranking Minority Member, Subcommittee on Emerging Threats, and Capabilities, Committee on Armed Services, US Senate, GAO-02-426, May 2002.

[10] International Atomic Energy Agency, Illicit Trafficking Database, Fact Sheet: January 1993–December 2006.

[11] J. Gronberg L. Hiller, T. Gosnell and D. Wright. Calculating gamma-ray signatures from aged mixtures of heavy nuclides. In *IEEE Nuclear Science Symposium Conference Record, NSS '07*, volume 2, pages 1138–1142, Honolulu, HI, 2007.

[12] C. Lo Presti, D. Weier, R. Kouzes, and J. Schweppe. Baseline suppression of vehicle portal monitor gamma count profiles: A characterization study. *Nuclear Instruments and Methods in Physics Research A,*, 562:281–297, 2006.

[13] D. P. Morton, F. Pan, and K. J. Saeger. Models for nuclear smuggling interdiction. *IIE Transactions on Operations Engineering*, 38:3–14, 2007.

[14] F. Pan, W. Charlton, and D. P. Morton. Interdicting smuggled nuclear material. In D.L. Woodruff, editor, *Network Interdiction and Stochastic Integer Programming*, pages 1–20. Kluwer Academic Publishers, Boston, 2003.

[15] F. Pan and D. P. Morton. Minimizing a stochastic maximum-reliability path. *Networks*. To appear.

[16] K. M. Witt. Development of a probabilistic network model to simulate the smuggling of nuclear materials, 2003. Nuclear and Radiation Engineering, The University of Texas at Austin, M.S. Thesis.