

# Detecting Nuclear Materials Smuggling: Performance Evaluation of Container Inspection Policies

Gary M. Gaukler,<sup>1,\*</sup> Chenhua Li,<sup>1</sup> Yu Ding,<sup>1</sup> and Sunil S. Chirayath<sup>2</sup>

---

In recent years, the United States, along with many other countries, has significantly increased its detection and defense mechanisms against terrorist attacks. A potential attack with a nuclear weapon, using nuclear materials smuggled into the country, has been identified as a particularly grave threat. The system for detecting illicit nuclear materials that is currently in place at U.S. ports of entry relies heavily on passive radiation detectors and a risk-scoring approach using the Automated Targeting System (ATS). In this article we analyze this existing inspection system and demonstrate its performance for several smuggling scenarios. We provide evidence that the current inspection system is inherently incapable of reliably detecting sophisticated smuggling attempts that use small quantities of well-shielded nuclear material. To counter the weaknesses of the current ATS-based inspection system, we propose two new inspection systems: the Hardness Control System (HCS) and the Hybrid Inspection system (HYB). The HCS uses radiography information to classify incoming containers based on their cargo content into “hard” or “soft” containers, which then go through different inspection treatment. The HYB combines the radiography information with the intelligence information from the ATS. We compare and contrast the relative performance of these two new inspection systems with the existing ATS-based system. Our studies indicate that the HCS and HYB policies outperform the ATS-based policy for a wide range of realistic smuggling scenarios. We also examine the impact of changes in adversary behavior on the new inspection systems and find that they effectively preclude strategic gaming behavior of the adversary.

---

**KEY WORDS:** Inspection systems; intelligence information; nuclear materials; radiography information; smuggling interdiction

## 1. INTRODUCTION

Large-scale terrorist attacks remain among the most alarming threat situations in the world today. Arguably the most disquieting scenario is

presented by the possibility of an attack using a nuclear device.

While the worldwide arsenal of nuclear weapons (in the form of warheads and fully assembled devices) is generally believed to be well secured and accounted for,<sup>(1)</sup> the same claim unfortunately cannot be made for stockpiles of weapons-usable nuclear materials, such as plutonium and highly enriched uranium (HEU), the so-called special nuclear materials (SNM). In the wake of the turmoil surrounding the disintegration of the Soviet Union, for example, nuclear material from Soviet reactors may

<sup>1</sup>Department of Industrial and Systems Engineering, TAMU 3131, Texas A&M University, College Station, TX 77843, USA.

<sup>2</sup>Nuclear Security Science & Policy Institute, TAMU 3473, Texas A&M University, College Station, TX 77843, USA.

\*Address correspondence to Gary M. Gaukler, Department of Industrial and Systems Engineering, TAMU 3131, Texas A&M University, College Station, TX 77843, USA; gaukler@tamu.edu.

have been diverted into illegal channels in unknown quantities.<sup>(2)</sup>

The danger, then, is that a terrorist group may acquire sufficient quantities of these nuclear materials, smuggle them into the United States, assemble them into a nuclear device, and use this device on a target on U.S. soil.

Illicit trade and smuggling of nuclear materials occur remarkably often: according to the International Atomic Energy Agency (IAEA), between 1993 and 2006, there were 1,080 confirmed incidents of illicit trafficking and unauthorized activities involving nuclear and radiological materials worldwide. Eighteen of these cases involved weapons-usable materials, which could be used to produce a nuclear weapon.<sup>(3)</sup>

Nuclear material could be smuggled into the United States in a variety of ways: hidden in a vehicle, in cargo containers, sent through mail, or carried in personal luggage through an airport. Among these, standard cargo container shipping is particularly vulnerable to smuggling nuclear materials. More than 15 million cargo containers arrive in the United States each year,<sup>(4)</sup> and combined they carry more than 95% of U.S. imports by weight and 75% by value.<sup>(5)</sup>

Detecting nuclear smuggling, whether it be at a domestic or a foreign port, is difficult due to a number of reasons. First, compared to many other natural and man-made sources of radiation, HEU and plutonium are relatively “low-brightness” materials.<sup>(6,7)</sup> This means that there is a low level of gamma and neutron particles being emitted by a unit quantity of plutonium and, in particular, HEU. The lower the amount of particles emitted, the more difficult it is to detect the presence of the material using detectors.

Compounding this difficulty is the expectation that a smart adversary may try to minimize chances of detection by smuggling very small amounts of material. Approximately 15 kg of HEU are necessary to fuel a nuclear weapon,<sup>(8)</sup> but an adversary could conceivably attempt to smuggle this total amount in much smaller quantities, perhaps down to 1 kg. For reference, 1 kg of HEU in solid form is approximately the size of a tennis ball. The smaller the quantity smuggled, the lower the number of particles emitted. In addition, both the gamma and neutron emissions from HEU and plutonium are easily shielded by large amounts of high-density metal, such as lead.

Furthermore, there are many sources of neutron and gamma radiation everywhere—from cosmic rays to emissions from concrete floors, ceramic tiles, fertilizer, bananas, cat litter, etc. Thus, the detection equipment needs to be able to differentiate at some level between radiation coming from background or from benign sources, and radiation coming from smuggled HEU or plutonium. Therefore, at any inspection station, an essential trade-off exists between time and accuracy: inspecting more stringently tends to cost more and delays the cargo longer, but has a better chance of detecting smuggled nuclear material, if it is present. There are several detector technologies available, and each technology has limitations in its ability to detect and identify nuclear materials. Thus, the U.S. government needs to develop useful inspection policies to decide which technology to use for which container, the sequence of detector use, and the detector operational parameters.

The inspection system currently in use at U.S. and foreign ports is a layered system, which relies heavily on intelligence information supplied by a rule-based software system that attaches risk scores to individual cargo containers. This software system is called the Automated Targeting System (ATS). We mathematically analyze this layered inspection system in this article and demonstrate its performance for several smuggling scenarios. Based on the results of our study, we argue that this current layered inspection system is inherently incapable of reliably detecting sophisticated smuggling attempts that use small quantities of well-shielded nuclear material.

To counter the weaknesses of the pure ATS-based inspection system, we develop and analyze two new inspection systems in this article. The first such system (initially proposed in Gaukler *et al.*,<sup>(9)</sup> see also Section 2), which we call the Hardness Control System (HCS), uses information obtained from radiographic imaging to determine whether a given cargo container contains a large amount of shielding material (a “hard” container), or not (a “soft” container). Then, based on this classification, containers undergo different inspection treatment. The second new inspection system, referred to as the Hybrid Inspection System (HYB), integrates both this radiographic imaging as well as the current ATS approach into a single inspection system. We analyze and contrast these two inspection systems with the ATS-based system and evaluate their response

to several possible adversary strategies. Our study indicates that for a wide range of scenarios, both the HCS and the HYB significantly outperform the ATS-based system, especially against sophisticated adversary strategies.

The remainder of the article is organized as follows. Section 2 provides a literature review of related research on preventing the smuggling of illicit nuclear materials or nuclear weapons. The current ATS-based inspection system is modeled in Section 3, and Section 4 contains an analysis of the ATS-based inspection system. Sections 5, 6, and 7 present and evaluate the proposed Hybrid inspection model. Overall conclusions and discussion are provided in Section 8.

## 2. RELATED WORK

Our article expands on the work done by Gaukler *et al.*,<sup>(9)</sup> in which the authors propose replacing the current ATS-based detection system with a detection system that is radiography based. Rather than relying on intelligence information, the proposed system relies on calculated hardness measures obtained from radiographic images taken of each incoming container. From these images, a set of possible “container scenarios” is formed. A container scenario reflects the densities, positions, sizes, etc. of the items inside the container. The system is evaluated with respect to detection probabilities and inspection delay times, and both of these values are conditioned on the distribution of container types. A fundamental weakness of this radiography-based system is the dismissal of the intelligence information provided by ATS. A container’s path through the detection system is determined solely by the data gathered from that container’s radiographic image with no consideration of intelligence information in the manifest data that may suggest an alternative path.

In this article, we seek to eliminate this weakness by proposing a hybrid system that combines the use of both radiography imaging and the ATS system. Another major difference is that in Gaukler *et al.*,<sup>(9)</sup> the objective of the inspection policy optimization is to maximize a weighted average of detection probabilities for different container types. Such an objective formulation makes it potentially easier for adversaries to game the system if they are able to select a container type that has a low detection probability (DP). Instead, in our current work, we use an objective of maximizing the minimum DP. This gives assurance that independent of the adversaries’ gaming

abilities, the lower bound on DP is maximized. Finally, in our current model we allow for container-type-specific false alarm rates, whereas in Gaukler *et al.*,<sup>(9)</sup> there was a single false alarm rate applied to all containers types.

Other research that has focused on the inspection system of shipping containers with an emphasis on the threat of nuclear materials includes that of Wein *et al.*,<sup>(10)</sup> Elsayed *et al.*,<sup>(11)</sup> and Young *et al.*<sup>(12)</sup> The approach of Wein *et al.*<sup>(10)</sup> is an 11-layer security system that calls for shipper certification, container seals, and a targeting software system. Additionally, passive, active, and manual inspection of the containers is performed both at foreign and domestic ports. A Stackelberg game is used to formulate the attacker-defender strategies and ultimately obtain the optimal inspection strategy with respect to budget constraints and port congestion. Unlike this 11-layer system, our hybrid model incorporates radiography information along with the notion of container types. This allows for differentiation between containers laden with different materials, an important factor in measuring the effects of container loads on inspection system performance. Elsayed *et al.*<sup>(11)</sup> formulate a constrained optimization problem by modeling the inspection system at the port of entry as a sequential problem in which both the threshold levels and the sequence of the sensors must be determined. They employ the enumeration method to solve the optimization problem, minimizing total cost subject to given budget constraints. Young *et al.*<sup>(12)</sup> introduce to this model the additional objective of minimizing the total expected time in the system. The optimal sensor arrangement and optimal threshold levels are determined with a multiobjective optimization approach.

Much research is comparable to our own in that it focuses on the threat of nuclear materials smuggling but differs from our work in that it does not examine the tactical problem of deciding the specific inspection policy at a given location. Similarly, other research works do propose an inspection policy at a given location but the threat in question is not necessarily that of nuclear materials.

The problem explored by Pan<sup>(13)</sup> and Morton *et al.*<sup>(14)</sup> as part of the second line of defense is the strategic, rather than tactical, problem of locating inspection stations and nuclear materials detectors along a long border when the inspection policy is assumed to be given. In order to determine these optimal locations, Pan<sup>(13)</sup> and Morton *et al.*<sup>(14)</sup> develop a class of stochastic network interdiction

models. The threat of nuclear materials is also the subject of the work done by Wein *et al.*,<sup>(15)</sup> Atkinson *et al.*,<sup>(16)</sup> and Atkinson and Wein,<sup>(17)</sup> however, in their work, it is assumed that nuclear materials have already been successfully smuggled beyond the border in question. In particular, they focus on the situation in which a terrorist is attempting to drive an already-assembled nuclear or radiological weapon toward a target in a city center. Wein *et al.*,<sup>(15)</sup> Atkinson *et al.*,<sup>(16)</sup> and Atkinson and Wein<sup>(17)</sup> investigate the last line of defense from different points of view, and formulate and solve the corresponding optimization problems. They apply stochastic dynamic programming, queuing theory, and game theory in order to model the behavior of the terrorist and the government both individually and together.

Boros *et al.*,<sup>(2,18)</sup> Stroud,<sup>(19)</sup> and Madigan *et al.*,<sup>(20)</sup> have all provided research on container inspection systems at the port of entry, but, in this research, special attention is not paid to nuclear materials. Boros *et al.*<sup>(18)</sup> seek to determine an optimal inspection strategy for sequential container inspection. To do so, they develop a large-scale linear programming model that includes various constraints pertaining to factors such as budget, sensor capacity, and time limits. Stroud<sup>(19)</sup> and Madigan *et al.*,<sup>(20)</sup> on the other hand, seek the optimal policy by formulating the inspection sequencing task as a problem of finding an optimal binary decision tree for an appropriate Boolean decision function. The work of Boros *et al.*<sup>(21)</sup> reviews and presents the research work that has been conducted for improving container inspection procedures using various optimization techniques.

Another area that lends itself to research very similar to our own is that of aviation security. For instance, Kobza and Jacobson<sup>(22)</sup> examine an inspection system with different layers of detection by considering bags entering an aviation security system, taking several subpaths with different detection technologies. Unlike our work and the work done by Wein *et al.*,<sup>(10)</sup> however, they do not consider any queuing results. Additional research on the inspection of aviation passenger baggage for explosives has been done by Kobza and Jacobson<sup>(23)</sup> and McLay *et al.*<sup>(24,25)</sup> Specifically, Kobza and Jacobson<sup>(23)</sup> present a method to quantify the effect of dependence in security system architectures. They examine the Type I and Type II errors of a multidevice system and present probability models for access control security system architectures. McLay *et al.*<sup>(24)</sup> focus on risk-based issues in the detection of explosives in aviation security baggage screening models.

A cost-benefit analysis is performed in order to quantify the tradeoff between intelligence and screening technology capabilities. Finally, McLay *et al.*<sup>(25)</sup> introduce a new problem, the Sequential Stochastic Passenger Screening Problem, which utilizes passengers' perceived risk levels in order to determine an optimal passenger screening policy that maximizes the expected number of true alarms, subject to capacity and assignment constraints. Typically, the main targeted threat in these cases is the presence of explosives rather than nuclear materials.

### 3. THE CURRENT ATS-BASED INSPECTION SYSTEM

The current inspection system at a given port is a layered system comprised of the ATS, as well as other detection hardware.

The first layer of security is the ATS, an expert system that identifies suspicious containers based on their manifest and customs entry document. The ATS is a decision-support tool used by the Customs and Border Protection that compares available information regarding incoming containers with additional intelligence data in order to assign a risk score to each container.<sup>(26)</sup> It does this by considering information about the origin of the container, its destination, and its declared content. This information is available through the shipping manifest, the bill of lading, and other means. This risk score is meant to communicate whether or not a given container is likely to contain dangerous or smuggled materials. If a container receives a risk score above a predetermined cutoff point, it is considered "high risk" and sent directly to a manual inspection station where its contents are emptied and reviewed. Containers with risk scores falling below the cutoff point are considered "low risk" and proceed to an additional layer of detection.

This additional layer of detection involves passive radiation inspection. Passive detectors (such as the current radiation portal monitors (RPMs) deployed at U.S. borders<sup>(27)</sup>) measure the emission of gamma rays as the containers pass through. If a container fails at this stage of the screening (i.e., it exhibits too large an emissions level), it is sent to manual inspection, where the container is opened up and examined. Passive tests are the fastest means of radiation detection, with a complete container scan taking on the order of 30–60 seconds. Manual inspection, on the other hand, can take several hours per container. However, manual inspection is much

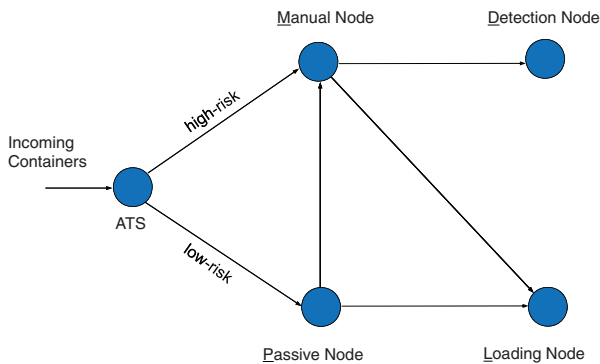


Fig. 1. ATS-based inspection system.

more capable in detecting nuclear materials, if they are present. A note regarding the use of terminology: manual inspection is generally referred to as the *secondary* inspection, while RPM inspection is part of the *primary* inspection.

In addition to RPMs, there also exist active radiation detectors. Active detectors emit gamma or neutron particles that pass through the container, while monitoring the particle counts being emitted from the container. This particle bombardment excites a reaction in nuclear material, if such material is present. This reaction produces a significantly higher particle emissions count when nuclear materials are present, which can then be used to ascertain the presence of nuclear materials.<sup>(28)</sup> Failure at active screening would send a container to be inspected manually. However, apart from radiography, active detector technology is, at the time of writing of this article, only available in laboratory testbed settings and is not in use at ports of entry in the United States or abroad. We therefore do not include an active detector node in our analysis.

A flow graph of the current inspection system is given in Fig. 1. We point out that this inspection system could either represent a domestic (U.S.) port, or a foreign port. In the case of a foreign port where containers are shipped to the United States, the loading node represents the actual loading of containers onto a ship, whereas in the case of a domestic port, the loading node represents the pick up of a container via truck or rail.

From Fig. 1, it is immediately clear that the performance of the ATS-based detection system is a direct function of (1) the reliability of container risk scores, and (2) the capability of the passive RPMs. (We assume from here on that when a container with SNM is manually inspected, the DP is 1.)

#### 4. EXAMINING THE RELIABILITY OF THE ATS-BASED SYSTEM

The performance of the ATS-based system is predicated on two components: the ability to assign “correct” risk scores to incoming containers, and the capability of passive detectors in detecting any infiltrated containers that the ATS may have missed.

Problems arise in the ATS system whenever one considers the possibility of “incorrect” risk score calculations. Imperfect intelligence may easily lead to the misclassification of a container as either “high” or “low” risk. If a container is misclassified, it may lead to one of two issues: (1) unnecessary congestion of the system or (2) undetected nuclear materials. The first would arise if a nondangerous container is classified as “high risk” and manually inspected and the second if a dangerous container is sent directly to passive inspection where the nuclear materials may go undetected.

It is important to understand that the ATS system was not created exclusively to aid in detecting nuclear materials smuggling. Rather, it is a comprehensive tool, developed to aid in the detection of all types of smuggling attempts, such as intercepting counterfeit goods, weapons smuggling, and illegal narcotics trafficking. As such, the container traits that the ATS system is checking against to ascertain a compromised container exhibit a wide variety and are necessarily of a general nature. Moreover, there is no historical data on nuclear smuggling events that targeted the United States, and thus it is not clear what signs of nuclear smuggling one would look for. Machine learning algorithms are not applicable due to this same lack of data. One might be inclined to use other smuggling data as a substitute, but commercial smuggling of drugs and even weapons is presumably significantly different from smuggling nuclear materials, in that there is a large flow of these goods. Thus, smugglers are prepared to see a fraction of these goods be detected, as long as the bulk of the contraband passes through. Given the extreme scarcity of special nuclear materials such as plutonium and HEU, it is unlikely that an adversary would treat smuggling them the same way as smuggling commodities. Note that the confirmed smuggling incidents reported by the IAEA<sup>(3)</sup> took place in (Eastern) Europe and the states of the former Soviet Union. These reflect attempts to sell nuclear materials by “smugglers of opportunity.” We argue that terrorist groups trying to smuggle SNM into the United States



represent a significantly different, more sophisticated adversary.

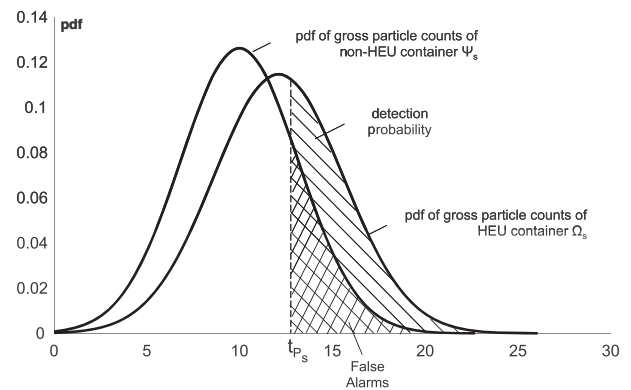
Thus, it appears questionable that the ATS system will be able to reliably identify nuclear materials smuggling attempts, and therefore there is a perceived high likelihood that a container with SNM may not enter secondary inspection directly, but will rather be relegated to an RPM inspection. Indeed, congressional testimony as cited in Cirincione *et al.*<sup>(29)</sup> indicates that the capability of the ATS with respect to nuclear materials smuggling has “not been proven to be any better than selecting containers at random.”

Most existing passive detectors, including the RPMs currently installed at sea ports and land border crossings, operate by counting gamma or neutron particles across a predefined energy range (energy bins). For example, a particular RPM may count all gamma particles across the range 0.8–1.1 MeV. Based on the particle counts recorded by the detector, a decision is then made whether these count data correspond to “normal” emissions, or whether this is due to the presence of SNM. To implement this decision making, a threshold policy is used: if particle counts are above a threshold, perform additional inspection.

Statistically, the number of particles of a certain energy range, emitted over a time window, follows a Poisson distribution. For large enough particle counts, this Poisson distribution can be approximated by the Normal.<sup>(10)</sup> Thus, the fundamental problem of detecting special nuclear materials in a container using a single passive detector can be described as follows.

For a particular container type  $s$ , let  $\Psi_s$  (mean  $\mu_{\Psi_s}$ , standard deviation  $\sigma_{\Psi_s} = \sqrt{\mu_{\Psi_s}}$ ) be the normal random variable describing particle incidence at a detector when no SNM is present; and let  $\Omega_s$  (mean  $\mu_{\Omega_s} \geq \mu_{\Psi_s}$ , standard deviation  $\sigma_{\Omega_s} = \sqrt{\mu_{\Omega_s}}$ ) be the normal random variable describing particle incidence at a detector when SNM is present. Find the threshold  $t_{P_s}$  such that the probability of detection of SNM (the area under the probability density function (pdf) of  $\Omega_s$  to the right of  $t_{P_s}$ ) is maximized, subject to the probability of false alarm (the area under the pdf of  $\Psi_s$  to the right of  $t_{P_s}$ ) being less than some predetermined number.

What makes this problem challenging is the degree of overlap between the two pdfs. For any threshold that we stipulate for the detector operation, there is a probability that the container with the HEU will be let pass by the system. The lower the threshold is



**Fig. 2.** Detection probability, false alarm probability, and distribution overlap.

set, the higher the DP, but also the higher the percentage of undesirable false alarms.

Fig. 2 shows these two pdfs for a particular shipping container that we simulated using MCNP.<sup>(30)</sup> MCNP is a software package developed at Los Alamos National Lab. This software is the *de facto* industry standard for performing nuclear transport calculations for particles such as photons, neutrons, and electrons. The software simulates the creation of particle emissions, particle trajectories, and particle interactions with surrounding materials, including absorption, reflection, scattering, and attenuation. The container modeled here is loaded with textiles, plastics, and some metal items. Background radiation is modeled coming primarily from the concrete floor on which the container sits. Two passive detectors were simulated, on both sides of the container, similar to an RPM. We inserted a 1 kg sphere of HEU into this container as the special nuclear material.

Fig. 2 demonstrates the significant overlap between the two distributions. The tradeoff between DP and false alarms is dire. In order to attain a reasonable DP, one would have to accept an unreasonable number of false alarms; more than any secondary inspection installation would likely be able to process.

We can conclude from this discussion that a system that relies only on the capabilities of passive radiation detection will necessarily be severely limited in its performance. This limitation exists because the gross counts of gamma or neutron particles from containers with shielded HEU are only slightly higher than normal background emissions.

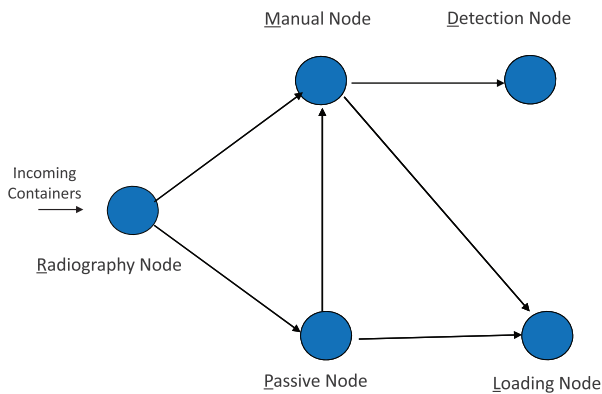


Fig. 3. Hardness control system.

Thus, the two major determinants of the performance of the ATS-based system, the “correctness” of the ATS risk scores and the capability of the passive detectors, both appear unsuited to defending against a sophisticated and determined adversary who uses shielding to his advantage.

### 5. IMPROVED INSPECTION POLICIES

In order to improve on the systemic weaknesses of the ATS-based system, we here develop two inspection policies that incorporate the use of radiographic imaging.

#### 5.1. The Hardness Control Policy

The HCS inspection policy is a refined version of the model described and analyzed in Gaukler *et al.*<sup>(9)</sup> Fig. 3 shows the flow diagram for this system.

For the HCS, the ATS node is replaced by a new inspection step, the radiographic imaging node. All incoming containers arrive at this radiography node. At the radiography node, x-ray equipment, similar to the Z portal systems currently deployed at the San Ysidro, CA border checkpoint,<sup>(31)</sup> is used to scan every container. The  $z$ -values (or atomic numbers) of the materials inside the container determine the scattering and absorption of the x-ray radiation as the container is scanned. High  $z$ -value materials (having high density) absorb more x-ray radiation and leave a dark area in the resulting radiographic image, while a low  $z$ -value material (having low density) leaves a bright area. From the darkness of the items (or areas) in the radiography image(s), it is possible to infer the  $z$ -value of the corresponding contents in the container. Thus, the radiographic images can be used

to determine the distribution of the  $z$ -values of materials stored inside the container.

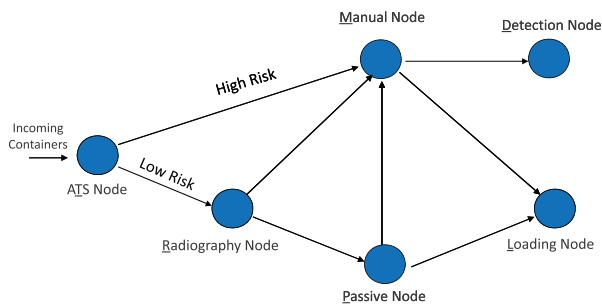
This distribution of the  $z$ -values is then used to determine a measure of how hard it would be for a given passive detector to detect HEU inside that particular container. We call this measure the hardness of the container, and denote it by  $h_s$ . For example, a container that is empty, or loaded with low  $z$ -value materials like textiles, has a low hardness; meaning that even an unsophisticated passive detector has a reasonable chance to detect HEU inside, if there is any. On the other hand, for a container that is loaded with high  $z$  metal items, a passive detector would not be able to discriminate, and therefore this container would be sent to manual inspection directly. Thus, the radiography information is used to determine whether to send a container to passive inspection, or to manual inspection directly. As in the ATS-based inspection system, containers that are flagged at the passive inspection node are sent to manual inspection.

Different from the simpler model in Gaukler *et al.*,<sup>(9)</sup> we apply a randomization treatment at the radiography node as follows: if the hardness measure for container type  $s$  is higher than a threshold  $t_R$ , then a randomly selected proportion  $a$ ,  $0 \leq a \leq 1$ , of container type  $s$  is elevated to manual inspection. If a container is not selected for manual inspection, it will be sent to passive inspection. The idea behind the randomization treatment is to reduce congestion and to allow for more effective use of manual inspection. The randomization parameter  $a$  is a decision variable in our new model. Hence our formulation is a generalization of the HCS policy presented in Gaukler *et al.*<sup>(9)</sup>

#### 5.2. The Hybrid Policy

In major contrast to the HCS, this new inspection policy also incorporates the use of intelligence data, as seen in the pure ATS-based system. We therefore call this new inspection policy the hybrid policy (HYB).

Fig. 4 shows the flow diagram for this hybrid system. As with the current inspection system, the first inspection of the proposed hybrid system is still the ATS, which considers the manifest data and intelligence information and classifies containers as either “high-risk” or “low-risk” containers. The high-risk containers are routed directly to manual inspection. For low-risk containers, a new inspection node, the radiography node, is added to the system. Low-risk



**Fig. 4.** Hybrid inspection system.

containers are sent to this radiography node, instead of the passive inspection in the ATS-based inspection system. The radiography information is then used in the same manner as in the HCS system to determine whether to send the container to passive inspection, or to manual inspection directly. Containers that are flagged at the passive inspection node are always sent to manual inspection. The radiography node in the hybrid system works the same way as in the HCS system.

Thus, the basic ideas behind the hybrid policy are (1) to use intelligence information whenever it is indicated that a container is “suspicious,” and (2) for those containers that are “unsuspicious,” make their treatment dependent on how difficult it is for the passive detector to differentiate between HEU inside or not for that particular container.

In the following section, we describe the modeling aspects for the ATS-based system, as well as the HCS and HYB systems. The detailed model formulations are provided in Appendices B–E.

## 6. MODELING THE INSPECTION SYSTEMS

In order to realistically model and analyze the behavior of the inspection systems, we need to be able to describe five aspects:

- (1) the level of emissions of gamma and neutron particles from shipping containers, dependent on differing contents of the containers;
- (2) the performance of differing types of radiation detectors with respect to the emissions from (1), and the natural background radiation;
- (3) the “hardness” of containers;
- (4) the intrinsic “accuracy” of the risk scores that the ATS system is built upon;

- (5) an inspection policy that describes (as a function of the inputs from (1)–(4) when to escalate a container from passive inspection to manual inspection, and when to let a container pass.

### 6.1. Emissions and Detector Modeling

We choose to model aspects (1) and (2) using MCNP. We model both shipping containers (with their contents), as well as the nuclear detector performance. For our purpose of evaluating nuclear radiation emitted from a shipping container, we provide MCNP with the geometric and structural properties of a shipping container, as well as the  $z$ -value matrix representing the contents of the container. The  $z$ -value, also called atomic number, describes the number of protons in an atomic nucleus. The information on the  $z$ -values of the materials inside the container is crucial because both gamma and neutron emissions from SNM are easily attenuated (shielded) by high  $z$ -value materials. Hence the material contents of a container strongly influence the emissions that a detector can register outside the container.

Based on the container model, radiation fluxes are computed by MCNP for defined regions around the container, and the flux values are then incorporated into a detector model to arrive at gross particle counts.

Thus, the MCNP code takes the  $z$ -value matrix associated with a container type as its input, and simulates the detection performance of a given type of detector. The MCNP code counts how many particle hits (i.e., influx) the simulated detector will register for a specified exposure time, and outputs the average influx per unit time per unit detector area. In our work, we only model gamma radiation fluxes because neutron emissions in the case of HEU are extremely low (at the rate of roughly 1/s/kg),<sup>(6,32)</sup> and thus not useful for the relatively short detection exposure times attainable at a port of entry.

Fig. 5 is a 3-D view of a sample 20-foot cargo container model used in the MCNP code. The large boxes shown in the figure that make up the container represent areas of different  $z$ -value materials (i.e., the cargo material) inside the container. The small boxes, along the outside of the container, represent the volumes in which the radiation flux is captured in MCNP. The detectors are located on both long sides of the container at a distance of 1 foot from the container walls. The natural radiation background is



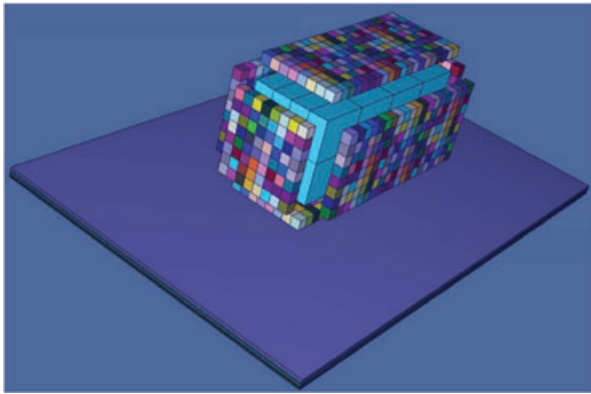


Fig. 5. 3-D image of container model in MCNP.

modeled by putting a sandstone concrete floor under the container, with thickness of 1 foot, and length and width five times that of the container. For modeling situations where HEU is present, a 1 kg HEU sphere (60% U-238, and 40% U-235) with 1 cm lead shielding is placed in the center of the highest  $z$ -value box in the container. This placement of the HEU represents the hardest possible case for detection, and thus is likely to be an adversary’s best choice.

The gamma emissions registered by the passive detector can come from two sources: the first component is the naturally occurring background level. This background level is influenced by the container and its cargo (e.g., the presence of NORM); by the container surroundings; and by the amount of shielding that is present at the detector to keep background radiation from being registered. The second component is the actual radiation emitted by the SNM, attenuated by the container cargo and any shielding material that may be present.

The gamma emissions stemming from natural background radiation, denoted by  $\Psi_s$ , are modeled as a normal random variable with a standard deviation equal to the square root of the mean. Similarly, the gamma emissions when HEU is present (including both the HEU emission component and the background radiation component), is another normal random variable, denoted by  $\Omega_s$ .

**6.2. Hardness Determination**

To quantify the hardness ( $h_s$ ) of a container type, we also utilize MCNP. The MCNP code takes the  $z$ -value matrix associated with a container type as its input, and simulates the performance of a given type of passive detector. It counts how many photon parti-

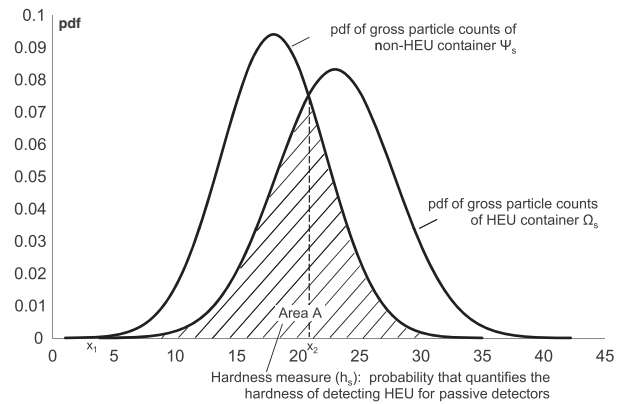


Fig. 6. Determination of the hardness measure.

cle hits the simulated detector will receive for a specified exposure time. The MNCNP code outputs the average photon counts per unit time per unit detector area. From this information, we construct the pdfs of particle counts for that container, with and without a given quantity of HEU placed inside. The hardness is then computed as the area of overlap between the two pdfs; see Area A in Fig. 6.

The higher this overlap between the distributions, the larger the hardness measure. Details on the mathematical derivation of the hardness measure are given in Appendix A.

**6.3. Reliability of Risk Scores**

To address the fourth aspect—the reliability or accuracy of ATS risk scores—we assign a measure of reliability to the risk scores. As we argued before, if the ATS was perfectly accurate, then it would be (from a DP standpoint) the optimal system, since it would always assign any container with HEU to the set of high-risk containers. In reality, the intelligence used in the ATS is likely less ideal. Thus, we need to assess and model how reliable the ATS classification can be.

To create this reliability measure, we adopt the “trust” concept ( $\delta_{ATS}$ ) that was introduced in McLay *et al.*<sup>(24)</sup> This trust measure is defined as the ratio of the probability that a container labeled “high-risk” contains HEU versus the probability that a container labeled “low-risk” contains HEU. Thus,

$$\delta_{ATS} = \frac{P(\text{HEU} | \text{HR})}{P(\text{HEU} | \text{LR})}. \tag{1}$$

If this ratio is one, this indicates that the intelligence is no better than random sampling. High

values of  $\delta_{\text{ATS}}$ , on the other hand, indicate that the high-risk containers are significantly more likely to contain HEU than the low-risk containers, and thus the reliability of the ATS risk scoring is great. It is possible that  $\delta_{\text{ATS}} < 1$ , and risk scoring could be worse than random sampling in the presence of sophisticated adversaries.

#### 6.4. Optimization of Inspection Policies

Modeling the inspection policy is handled in our approach by treating the inspection system as a queueing network. In this queueing network, the individual inspection stations correspond to servers, and the containers line up for service. A threshold policy is used to decide when to escalate a container to the next inspection step, or let the container pass. This means that there is a critical number  $t_{P_s}$  such that if the emissions registered at the passive detector are higher than  $t_{P_s}$ , then the container is going to be escalated to manual inspection; else the container is cleared and leaves the system.

For any choice of thresholds, we can calculate the probability that a particular container, if it has SNM inside, will be escalated to manual inspection, and during manual inspection will be found to have SNM inside. This quantity then is the DP. The DP is, strictly speaking, a conditional probability because it is conditioned on the event that a particular container contains a quantity of SNM. Besides the DP, we are also interested in the time delay that is experienced by a particular container as it moves through this inspection system. Since the more reliable detection method, manual inspection, takes significantly longer time to complete than passive inspection, there is a tradeoff between DP and the time delay experienced by containers.

Thus, the inspection system can be formulated as an optimization problem, in which the U.S. government chooses an inspection policy that maximizes DP, subject to a constraint on the average delay time a container may experience in the system. For the ATS-based inspection system, the decision variables for the government are the threshold  $t_{P_s}$ , and the fraction of containers to label as “high risk,” denoted  $\beta$ . In reality, the quantity  $\beta$  is implicitly chosen by the system operators through specifying a critical risk score: any container with a risk score above this critical value would be treated as a “high-risk” container.

In Gaukler *et al.*,<sup>(9)</sup> the objective function of this optimization problem is formulated as maximizing a weighted average of the detection probabili-

ties for the individual container types. That is, the objective function is  $\max \text{DP} = \sum_s \omega_s \cdot \text{DP}_s$ , where  $\omega_s$  are weights assigned exogenously to the individual container types. These weights represent the exogenous likelihood that an adversary would infiltrate a particular container type. The drawback to this formulation is that it potentially allows adversaries to game the system: the objective function tends to disregard the influence of the DP for container types of low weighting  $\omega_s$ . Thus, the optimal detection probabilities for these container types tend to be very low. A sophisticated adversary can exploit this weakness by targeting exactly those container types for a smuggling attempt. Thus, using a weighted-average maximization approach may lead to a significant overstatement of actual detection probabilities and to system configurations that are decidedly suboptimal. We circumvent this problem in our current models by implementing an objective function that maximizes the minimum DP over all container types ( $\max \min_s \text{DP}_s$ ). This objective is also used, for example, in Wein *et al.*<sup>(10)</sup>

Furthermore, in our current models we allow the use of container-type-dependent false alarm rates. In Gaukler *et al.*,<sup>(9)</sup> the critical number thresholds are set such that each container type has the same false alarm rate. This is achieved by setting, for example, the threshold for the passive node for container type  $s$  to  $t_{P_s} = \mu_{\psi_s} + \gamma \cdot \sigma_{\psi_s}$ , but the same constant  $\gamma$  is used for all container types. We relax this in our current model and allow for individual false alarm rates by setting thresholds for container type  $s$  based on  $t_{P_s} = \mu_{\psi_s} + \gamma_s \cdot \sigma_{\psi_s}$ , where  $\gamma_s$  differs for different  $s$ . Since the container-type information that is necessary to have for this relaxation is available only through radiographic imaging, we only apply the individual false alarm rate concept to the HCS and HYB models. The ATS model necessarily still uses a common  $\gamma$  for all container types.

Since in all three inspection systems the manual inspection is the most discriminating inspection step, and also the most expensive one in terms of time and effort, any inspection policy will at optimality attempt to utilize manual inspection as much as possible. However, this extreme capacity utilization behavior would make the system very sensitive to even the smallest unanticipated changes to the arrival stream, such as a slight arrival rate increase, or container composition change, etc. In order to obtain a more robust and practicable system, we add a constraint on the utilization rate at the manual node, denoted as  $\rho_M$ , and set  $\rho_M \leq r$ , where 0

$< r < 1$  is an exogenously given capacity utilization limit.

In our models, we calculate two main performance measures: the DP and the expected delay time of containers (DT). In terms of the underlying queueing network, the expected delay time corresponds to the expected delay time of containers within the system; that is, the sum of expected waiting and service (inspection) times. In order to better illustrate the tradeoff between the two conflicting performance measures (DP and DT), we choose to present efficient frontiers rather than provide a set of optimized decision variables. These efficient frontiers are generated by solving a sequence of optimization problems for discrete choices of a delay time limit  $t$ . Table I summarizes the decision variables used in the inspection systems.

For the HYB, the optimization problem for obtaining the efficient frontier is:

$$\begin{aligned} \max_{\beta, t_R, a, \gamma_s} \min_s DP_s^{\text{HYB}}, \\ \text{s.t. } DT^{\text{HYB}} \leq t, \\ \rho_M^{\text{HYB}} \leq r. \end{aligned} \quad (2)$$

Since the ATS system, as shown in Fig. 1, does not use a radiography node, the decision variables of the ATS system are  $\beta$ ,  $\gamma$ , and the optimization problem becomes:

$$\begin{aligned} \max_{\beta, \gamma} \min_s DP_s^{\text{ATS}}, \\ \text{s.t. } DT^{\text{ATS}} \leq t, \\ \rho_M^{\text{ATS}} \leq r. \end{aligned} \quad (3)$$

Note that the  $\gamma$  in Equation (3) is not container-type specific (it does not have the subscript  $s$ ) because the pure ATS system, without the radiographic node, does not have the container scenario information.

For the HCS system without the ATS node, as shown in Fig. 3, the decision variables are  $t_R$ ,  $a$ ,  $\gamma_s$ ,

and the optimization problem is:

$$\begin{aligned} \max_{t_R, a, \gamma_s} \min_s DP_s^{\text{HCS}}, \\ \text{s.t. } DT^{\text{HCS}} \leq t, \\ \rho_M^{\text{HCS}} \leq r. \end{aligned} \quad (4)$$

Details of the derivation of  $DP_s$  and DT for HYB, ATS, and HCS systems are given in Appendices B–E.

One can also add other constraints to the above optimization problem in order to confine the length of queueing at each node if the waiting space is limited. In this article, the waiting area is assumed to be unconstrained.

## 7. ANALYSIS OF THE INSPECTION SYSTEMS

A genetic algorithm (GA) is used to solve the max-min optimization problem. To simplify the coding of the GA, we turn the original constrained optimization problem into an unconstrained optimization problem by changing the nonlinear constraint into a penalty function. The new unconstrained optimization problem for the HYB system is:

$$\begin{aligned} \min_{\beta, t_R, a, \gamma_s} (-\min_s DP_s^{\text{HYB}} + \eta \cdot (\max\{0, (DT^{\text{HYB}} - t)\} \\ + \max\{0, (\rho_M^{\text{HYB}} - r)\})), \end{aligned} \quad (5)$$

where  $\eta$  is the penalty coefficient, and is set to  $10^{12}$  in our numerical study. The optimization problems for the ATS and HCS models are transformed similarly.

### 7.1. Experiment Setup

The GA is implemented using the MATLAB<sup>®</sup> GA toolbox, with default options for uniform creation, rank fitness scaling, stochastic uniform selection, Gaussian mutation, and scattered cross-over.<sup>(33)</sup>

After initial experimentation, we ran each replication for 100 generations, using a cross-over fraction of 0.6 and an elite count (i.e., the number of

**Table I.** Summary of Decision Variables

Name	Description	Systems Used
$\beta$	Proportion of containers labeled as “high risk”	HYB, ATS
$t_R$	Hardness threshold at $R$ -node	HYB, HCS
$a$	Proportion of hard containers sent from $R$ -node to $M$ -node	HYB, HCS
$\gamma_s$	Escalation threshold at $P$ -node for container-type $s$	HYB, HCS
$\gamma$	Escalation threshold at $P$ -node (same for all container types)	ATS

**Table II.** Container Information and Simulated Gross Counts of Passive Detection

$s$	$p_s$	$\mu_{\Psi_s}$	$\sigma_{\Psi_s}$	$\mu_{\Omega_s}$	$\sigma_{\Omega_s}$	$h_s$
1	0.60	9.99	3.16	29.52	5.43	0.02
2	0.30	9.99	3.16	15.75	3.97	0.41
3	0.08	9.99	3.16	12.10	3.48	0.75
4	0.02	49.95	7.07	52.06	7.21	0.88

unchanged chromosomes from one generation to the next) of 4. The population size was 600 for the HCS and 2,000 for the hybrid system.

With these settings, the computation time for obtaining one point on the efficient frontier was approximately 35 seconds for the HCS system, and 2 minutes for the HYB system, on a 3.2 GHz dual core processor.

For our numerical example, we define four container types. The first container type consists of only low  $z$ -value materials, whose  $z$ -value is less than 10 (e.g., textiles, plastic, wood). The contents of the second container type is a mixture of medium  $z$ -value materials, whose  $z$ -value is between 10 and 20 (e.g., aluminum), and low  $z$ -value materials. The third container type has high  $z$ -value materials, whose  $z$ -value is greater than 20 (e.g., steel), and low  $z$ -value materials. The fourth and last scenario considers the case where other particle emissions (from NORM) exist. To account for the effect of NORM, the natural background emission level of the fourth scenario is set to be five times that of the third scenario.

Table II lists the container information and count data obtained from the MCNP simulations. The first column, labeled  $p_s$ , is the proportion of each container type among all the containers. We assume that there are relatively fewer hard containers than there are soft containers. This assumption is based on a 2007 listing of the top 100 U.S. container importers and the industry (and thus cargo) segments represented by these top 100 importers.<sup>(34)</sup> For all four container types, MCNP is used to obtain the background count data and the HEU count data. The last column is the hardness corresponding to each container type, calculated based on the description in Section 6 and Appendix A.

The model parameters that describe the port operations are summarized in Table III. We assume that the arrival rate of containers at the port is 90 per hour, which is the same arrival rate used in Wein *et al.*<sup>(10)</sup> The scan time for each of the three radiography machines is taken to be exponentially dis-

**Table III.** Values for the Model Parameters

Parameter	Description	Value
$\lambda$	Arrival rate of container	90/hour
$\mu_R$	Service rate at radiography node ( $R$ -node)	40/hour
$m_R$	Number of servers at $R$ -node	3
$\mu_P$	Service rate at passive detection node ( $P$ -node)	80/hour
$m_P$	Number of servers at $P$ -node	2
$\mu_M$	Service rate at manual detection node ( $M$ -node)	1/hour
$m_M$	Number of servers at $M$ -node	6

tributed with a mean of 90 seconds. For each of the two passive detectors, the scan time is assumed to be exponentially distributed with a mean of 45 seconds. The inspection time at the manual detection stage is also an exponential distribution with a mean time of 1 hour, and we assume that there are six manual inspection teams that can work in parallel. We set the maximum allowable capacity utilization for the manual inspection stage to be  $\rho_M \leq 0.95$  for all inspection models.

We further assume that when a container with HEU is manually inspected, the probability that the HEU is discovered is  $d_M = 1$ . If in reality there is a possibility that manual inspection is unable to discover the HEU in an infiltrated container, then  $d_M < 1$ , and the detection probabilities and efficient frontiers that we report need to be scaled by  $d_M$ .

This choice of parameters is consistent with earlier work in Gaukler *et al.*,<sup>(9)</sup> and also with Wein *et al.*<sup>(10)</sup>

## 7.2. System Comparison

In this section, we compare the performance of the three inspection policies. For the purposes of this comparison, the ATS-based system is evaluated for  $\delta_{ATS}$  values between 1 and 50. For simplicity of exposition, the hybrid system is evaluated only for two choices of  $\delta_{ATS}$  values: 2 and 20.

The range of the  $\gamma_s$  values in the example (which determine the escalation thresholds) is  $\gamma_s \in [0, 3.5]$ . The upper bound of  $\gamma_s$  is conservatively set to be 3.5, such that the lowest possible false alarm rate is 0.02%. This false alarm rate is low enough for any practical purposes, especially compared to current practice, where false alarm rates are typically around 10–30%.<sup>(24)</sup>

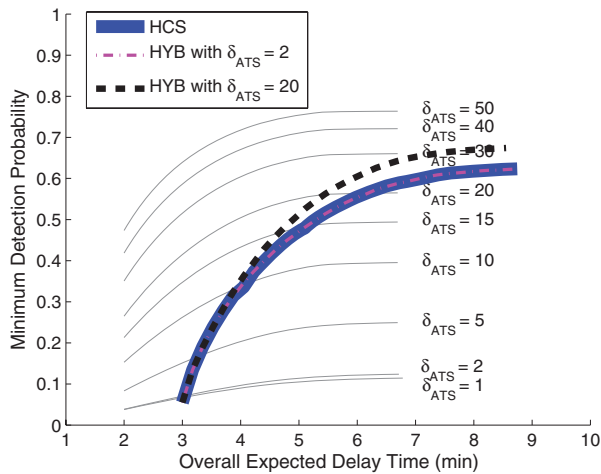


Fig. 7. System performance comparison.

Fig. 7 summarizes the system performance of the HCS system, the HYB system, and the ATS system for different  $\delta_{ATS}$  values.

Fig. 7 shows that for our sample data, the performance of the HCS system alone (without using intelligence information) is roughly equivalent to the performance of an ATS-based system with intelligence reliability of  $\delta_{ATS} = 20$  at an overall delay time of about 6 minutes, and about  $\delta_{ATS} = 25$  at a delay time limit of 8 minutes. The higher the acceptable delay time, the better the HCS system performs relative to the ATS. Thus, if a decisionmaker accepts an overall delay time of 6 minutes or more, and if the decisionmaker believes that the reliability of available intelligence information is less than  $\delta_{ATS} = 20$ , the HCS will outperform an ATS-based system.

Fig. 7 also shows that if intelligence reliability is very low, such as  $\delta_{ATS} = 2$ , the performance of the hybrid system is equivalent to that of the HCS system (the efficient frontier curves are identical). In fact, since there is very limited value to the intelligence information when  $\delta_{ATS} = 2$ , the hybrid system actually does not use this information at all, and the proportion of containers labeled as “high risk” is virtually zero in this case (compare Table IV).

If, on the other hand, intelligence reliability is fairly high, such as  $\delta_{ATS} = 20$ , the hybrid system performs better than the HCS system. In this case, combining the radiography information and the intelligence information is roughly equivalent to an ATS system with  $\delta_{ATS} = 30$  at the overall delay time of 7 minutes.

Table IV. Route Selections with Overall Delay Time of 6 Minutes

	$\delta_{ATS}$	$s$	P-L	ATS-M-L	R-M-L	P-M-L
ATS	1	1	0.938	0		0.062
		2	0.938	0		0.062
		3	0.938	0		0.062
		4	0.938	0		0.062
	2	1	0.938	0.046		0.017
		2	0.938	0.046		0.017
		3	0.938	0.046		0.017
		4	0.938	0.046		0.017
	20	1	0.938	0.060		0.002
		2	0.938	0.060		0.002
		3	0.938	0.060		0.002
		4	0.938	0.060		0.002
	50	1	0.938	0.060		0.002
		2	0.938	0.060		0.002
		3	0.938	0.060		0.002
		4	0.938	0.060		0.002
HCS		1	1		0	0
		2	0.951		0	0.049
		3	0.698		0	0.302
		4	0.560		0.031	0.409
HYB	2	1	1	0.0001	0	0
		2	0.951	0.0001	0	0.049
		3	0.699	0.0001	0	0.301
		4	0.554	0.0001	0.091	0.355
	20	1	0.967	0.033	0	0
		2	0.958	0.033	0	0.009
		3	0.844	0.033	0.0001	0.123
		4	0.744	0.033	0.0001	0.223

Table IV shows the probabilities of a particular incoming container going through different inspection steps when the delay time is 6 minutes. The notation P-L represents the probability of a container going through the passive detector and then leaving the inspection system. As such, for the ATS system this notation represents the path ATS-P-L; for the HCS system the path R-P-L; and for the hybrid system the path ATS-R-P-L. Similarly, the notation P-M-L represents the path ATS-P-M-L for the ATS system, R-P-M-L for the HCS system, and ATS-R-P-M-L for the hybrid system, respectively.

From Table IV we can observe that for the ATS system, as the reliability of intelligence information increases, the system in optimality uses this information to send containers directly to manual inspection. However, since capacity at manual inspection is finite, this reduces the chance to send containers to manual inspection following a reading at the passive radiation detection stage: the higher the reliability of intelligence information, the higher the passive radiation emission threshold ( $\mu + \sigma \cdot \gamma$ )



**Table V.** Optimal Thresholds with Overall Delay Time Limit of 6 Minutes

		$\gamma_1$	$\gamma_2$	$\gamma_3$	$\gamma_4$
ATS	$\delta_{\text{ATS}} = 1$	1.54	1.54	1.54	1.54
	$\delta_{\text{ATS}} = 2$	2.11	2.11	2.11	2.11
	$\delta_{\text{ATS}} = 20$	2.85	2.85	2.85	2.85
HCS		3.50	2.09	0.90	0.53
HYB	$\delta_{\text{ATS}} = 2$	3.50	1.66	0.52	0.28
	$\delta_{\text{ATS}} = 20$	3.50	2.36	1.14	0.74

that needs to be exceeded for a container to be escalated to manual inspection at the passive radiation detection stage. When  $\delta_{\text{ATS}} = 50$ , the threshold at passive inspection is set so high that only 0.2% of containers will be escalated from passive inspection directly to manual. For comparison, the HCS system escalates between 0% (for the “softest” container type) and 40.9% (for the hardest container type) of the containers from passive detection directly to manual inspection.

This observation underscores the earlier discussion in Section 4 on the fundamental weakness of the ATS-based system: if a sophisticated adversary manages to infiltrate a container that will not be flagged as high risk, the chance of SNM being detected at the passive radiation detection stage is exceedingly small, even when the system parameters are set optimally.

Additionally, the HCS and hybrid systems are able to use container-type-specific false alarm rates by selecting different passive detector thresholds ( $\mu + \sigma \cdot \gamma_s$ ). For example, Table V shows that the HCS and hybrid systems attach higher false alarm rates to harder containers, and lower false alarm rates to softer containers. This makes sense because soft containers have low shielding ability, and thus SNM, if present, will have a more obvious emissions signature. Hence a higher threshold at passive inspection can be used, with resulting lower false alarm rate. Thus, knowing the container type aids in fine-tuning the escalation logic of the inspection system. The ATS-based system is unable to do this because it lacks the container-type information (i.e., the distribution of  $z$ -values) that comes from the radiography step. Thus, the ATS-based system uses one “overall” false alarm rate for all container types.

This is visible in Table IV as well. One can observe that the ATS system treats all container types in the same manner, regardless of their cargo content; the inspection path probabilities are identical for all container types. The HCS and hybrid sys-

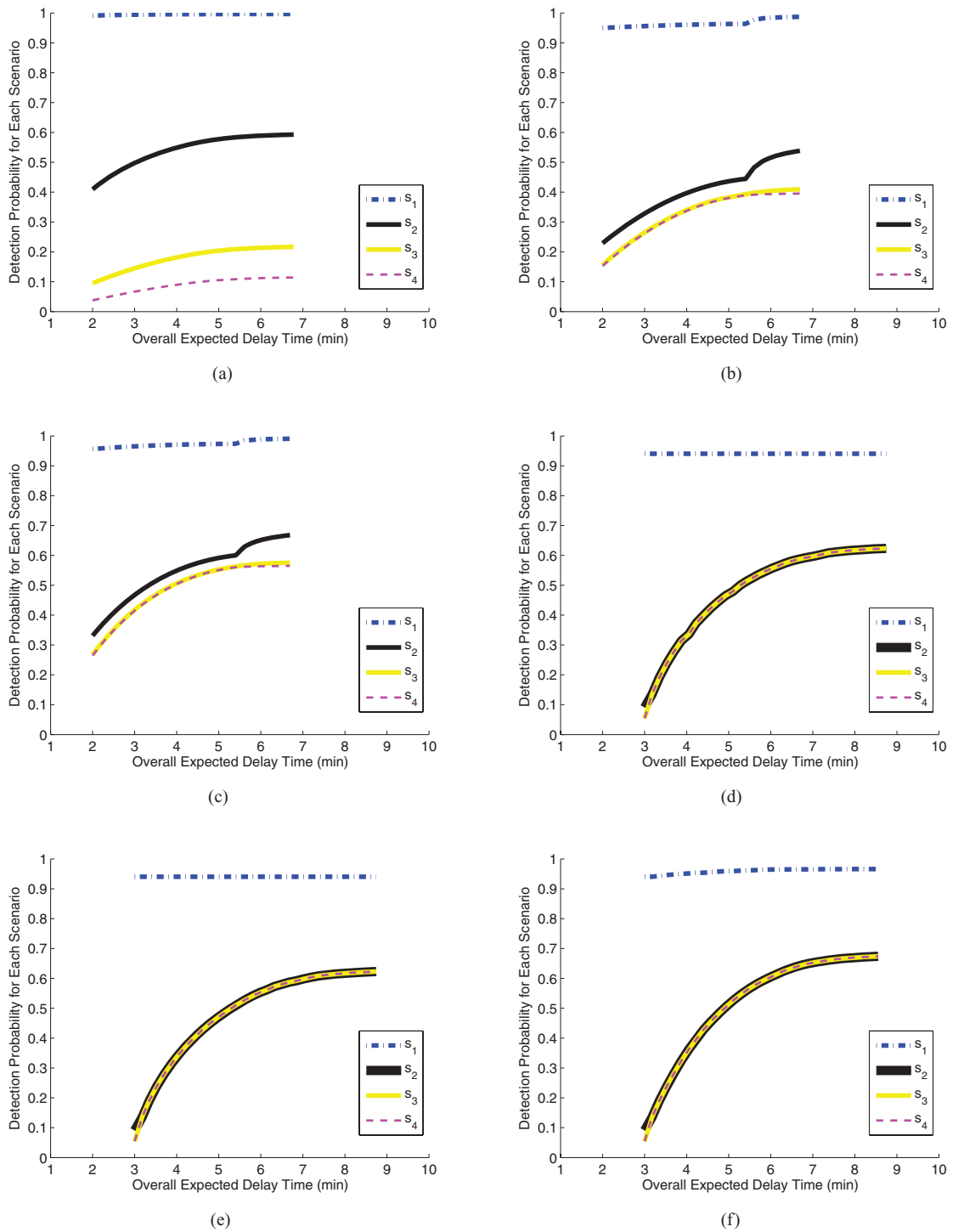
tems, on the other hand, are able to select inspection paths for containers based on knowledge of the cargo contents. In the hybrid system for  $\delta_{\text{ATS}} = 2$ , for example, none of the “soft” containers are escalated to manual inspection directly from the radiography node, but 9.1% of containers of the hardest container type are. As the reliability of intelligence increases to  $\delta_{\text{ATS}} = 20$ , more containers are escalated to manual inspection using this intelligence information (3.3% vs. 1/100 of a percent), and fewer containers are escalated to manual due to radiography (1/100 of a percent vs. 9.1%).

We point out that inclusion of the radiography node does cause extra time in the processing of containers; this is the price to pay to obtain the container hardness information. As a result, the percentage of containers handled by the manual node in a HCS or a hybrid system, the most time-consuming yet most capable node in the whole inspection process, is smaller than that in the pure ATS system. This can be easily verified by inspecting Table IV. The percentage of containers handled by the manual node can be calculated as  $1 - \sum_{s=1}^4 (\text{P-L})_s \cdot p_s$ , where  $(\text{P-L})_s$ ,  $s = 1, 2, 3, 4$ , represent the probability values in the P-L column of Table IV. A simple calculation reveals that for the pure ATS system, this percentage is 6.2%, while for the HCS or the hybrid system, the percentages are 4.766% (HCS), 4.77% (HYB with  $\delta_{\text{ATS}} = 2$ ), and 5% (HYB with  $\delta_{\text{ATS}} = 20$ ). However on the other hand, the analysis we made so far suggests that the HCS and hybrid systems are able to utilize the existing capacity at the manual inspection stage more effectively than the ATS-based system. This more intelligent utilization of existing capacity in the end can lead to a dramatic improvement in DP, despite the slight decrease in container percentages processed by the manual node.

Fig. 8 shows the detection probabilities individually for each container type.

For the ATS system, three different  $\delta_{\text{ATS}}$  values are considered:  $\delta_{\text{ATS}} = 1, 10$ , and 20. When  $\delta_{\text{ATS}} = 1$ , there is no value to the intelligence information, and the system is equivalent to a layered system of passive detection and manual inspection only. In this case, the DP for the softest container type is approaching 1. However, the DP for the hardest container type reaches only approximately 0.1.

Notice also that as  $\delta_{\text{ATS}}$  increases, the DP for the softest container type decreases. This happens because with better intelligence, in optimality (based on maximizing the minimum DP) one will send a higher percentage of containers directly to manual



**Fig. 8.** Detection probability of each container type: (a) ATS with  $\delta_{ATS} = 1$ ; (b) ATS with  $\delta_{ATS} = 10$ ; (c) ATS with  $\delta_{ATS} = 20$ ; (d) HCS system; (e) HYB with  $\delta_{ATS} = 2$ ; (f) HYB with  $\delta_{ATS} = 20$ .

inspection based on intelligence information alone (compare Table IV). However, increasing this direct escalation percentage comes at the expense of higher thresholds at passive inspection, and thus a lower escalation percentage from passive inspection to manual inspection, which lowers the DP for soft container types.

For the HCS and hybrid systems, the DP for the softest container type is above 0.9, but not as high as in the ATS system. The other three container types have essentially identical efficient frontiers. The minimum detection probabilities for the HCS and HYB systems, as expected, are superior compared to the ATS-based system.

Independent of container type, the ATS system escalates a constant percentage of containers from passive detection to manual inspection. Thus, the ATS sets an escalation threshold (see Table IV) that yields an “average” false alarm probability for all container types. By doing this, the ATS-based system achieves very high detection probabilities for the softest container types because emissions from unshielded SNM have a high likelihood of exceeding this “average” threshold. However, the detection probabilities for hard container types are very low because the well-shielded SNM in the higher hardness containers has a low likelihood of exceeding this “average” threshold. As  $\delta_{\text{ATS}}$  increases, the detection probabilities for all scenarios increase, but the hardest container type remains the one with the lowest DP.

Thus, in order to improve the minimum DP, the HCS and hybrid systems sacrifice some of the potential detection capability for the softest containers, to instead use the available capacity to elevate the DP for hard containers.

### 7.3. Impact of Adversary Behavior

In real situations, the decisionmaker typically does not know ahead of time which container type an adversary might choose to infiltrate. Thus, to the decisionmaker, the adversary’s choice in selecting a container type for infiltration is stochastic.

For example, the adversary may prefer to select a “hard” container (with larger  $h_s$  value) to transport HEU in order to take advantage of the added shielding from the container contents. Alternatively, if an adversary is aware of the principles of hardness-based inspection policies, he might choose to select a low-hardness container to reduce the likelihood to

**Table VI.** Various Prior Probability Distribution of  $\omega_s$

		$\omega_s$			
$s$	$h_s$	Uniform Quadratic		Bell	Inv-Quadratic
		$1/n_s$	$0.66 \cdot h_s^2$	$0.53 \cdot \exp\left(-\frac{(h_s-h_2)^2}{2 \cdot 0.25^2}\right)$	$0.73 \cdot (1-h_s)^2$
1	0.02	0.25	0.0003	0.1555	0.6950
2	0.41	0.25	0.1137	0.5333	0.2490
3	0.75	0.25	0.3706	0.2187	0.0460
4	0.88	0.25	0.5153	0.0925	0.0100

be singled out for more stringent inspection, or a medium-hardness container to combine both effects.

For the decisionmaker, then, an important question is whether the hardness-based inspection policies may inadvertently open an avenue for the adversary through which he can game the inspection system.

In this section, we model various types of adversary behavior through characterizing probability distributions, and we evaluate the performance of the inspection systems in response to these adversary types.

Let  $\omega_s$  denote the prior probability that the adversary selects container-type  $s$  to infiltrate. We model four different types of adversaries, each with a distinct distribution of  $\omega_s$ . To model a wide range of adversary types, we use uniform, quadratic, bell, and inverse quadratic distributions to characterize the adversary.

For the uniform type, the adversary has no preference over the container type; thus all container types have the same probability of being selected for infiltration.

For the quadratic type, the container type with the highest  $h_s$  value has the highest probability of being selected; the functional relationship is such that  $\omega_s$  is a quadratic function of the hardness value  $h_s$ .

The inverse quadratic type is the opposite of the quadratic type: soft containers have a higher probability of being selected than hard containers, and the functional relationship between hardness and selection probability is inverse quadratic.

For the bell type, the adversary prefers to choose medium hardness containers, producing a bell-shaped distribution.

Table VI lists the parameters for the different distributions  $\omega_s$  we consider in our analysis, and Fig. 9 shows the distributions graphically.

Fig. 10 shows the efficient frontier of the overall DP versus the overall expected delay time for the

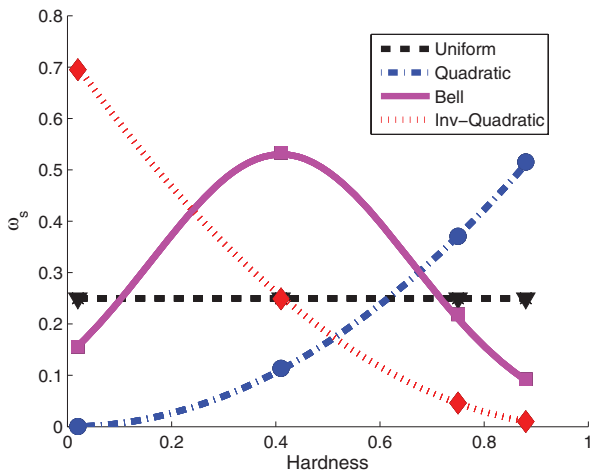


Fig. 9. Adversary behavior type.

ATS, HCS, and hybrid systems, under different adversary behavior. Multiple levels of  $\delta_{ATS}$  are plotted for the ATS system, such as:  $\delta_{ATS} = 1, 5, 10, 15, 20, 30, 40, 50$ . Two levels of intelligence information reliability in the hybrid system are considered,  $\delta_{ATS} = 2$ , and  $\delta_{ATS} = 20$ .

Notice that Fig. 10, different from Fig. 7, does not show the efficient frontier that corresponds to the container type that exhibits the minimum DP. Instead, Fig. 10 displays the weighted detection probability  $DP = \sum DP_s \cdot \omega_s$ , so that the impact of the adversary’s decision can be studied. This weighting is also the reason why in some of the figures the efficient frontiers of the ATS-based system intersect for different values of  $\delta_{ATS}$ : recall that the DP for the softest container types tends to be higher for low values of  $\delta_{ATS}$  than for high values of  $\delta_{ATS}$  (compare Fig. 8). Thus, if an adversary is more likely to infiltrate a soft container, a lower intelligence reliability can be, counterintuitively, actually an asset.

From the sequence of figures, we can observe that compared to the ATS, the HCS system is most competitive in the case of quadratic adversary behavior, where it performs better than  $\delta_{ATS} = 22$ . Conversely, the HCS is least competitive in case of inv-quadratic behavior, worse than  $\delta_{ATS} = 10$ .

This behavior results because the HCS system focuses the inspection efforts on the hardest container types, and therefore works best when the adversary has a high likelihood of infiltrating hard containers; it performs worst (relatively speaking) when the adversary has a high likelihood of infiltrating soft containers.

The hybrid system with  $\delta_{ATS} = 2$  performs equivalent to the HCS system. For  $\delta_{ATS} = 20$ , the performance of the hybrid system is similar to the HCS system with respect to the different adversary types, but at a significantly higher level of DP.

Compared to the ATS system, the hybrid system performs best when the adversary is of the quadratic type, equivalent to approximately  $\delta_{ATS} = 28$ . Similar to the HCS system, the worst case happens when the adversary is of the inv-quadratic type, where the equivalent  $\delta_{ATS} = 15$ .

However, these observations do not translate into an opportunity for the adversary to game the system. Note that the absolute values of overall DP are very high ( $>0.8$ ) for the inv-quadratic case, whereas the overall detection probabilities for the quadratic case are lower. Thus, it is not in the interest of the adversary to prefer to infiltrate soft containers. Instead, if behaving rationally, the adversary, even with knowledge of the new hardness-based inspection policies, will try to avoid selecting soft containers. Indeed, the adversary’s best choice is still to target hard containers for infiltration because this choice minimizes his probability of being detected.

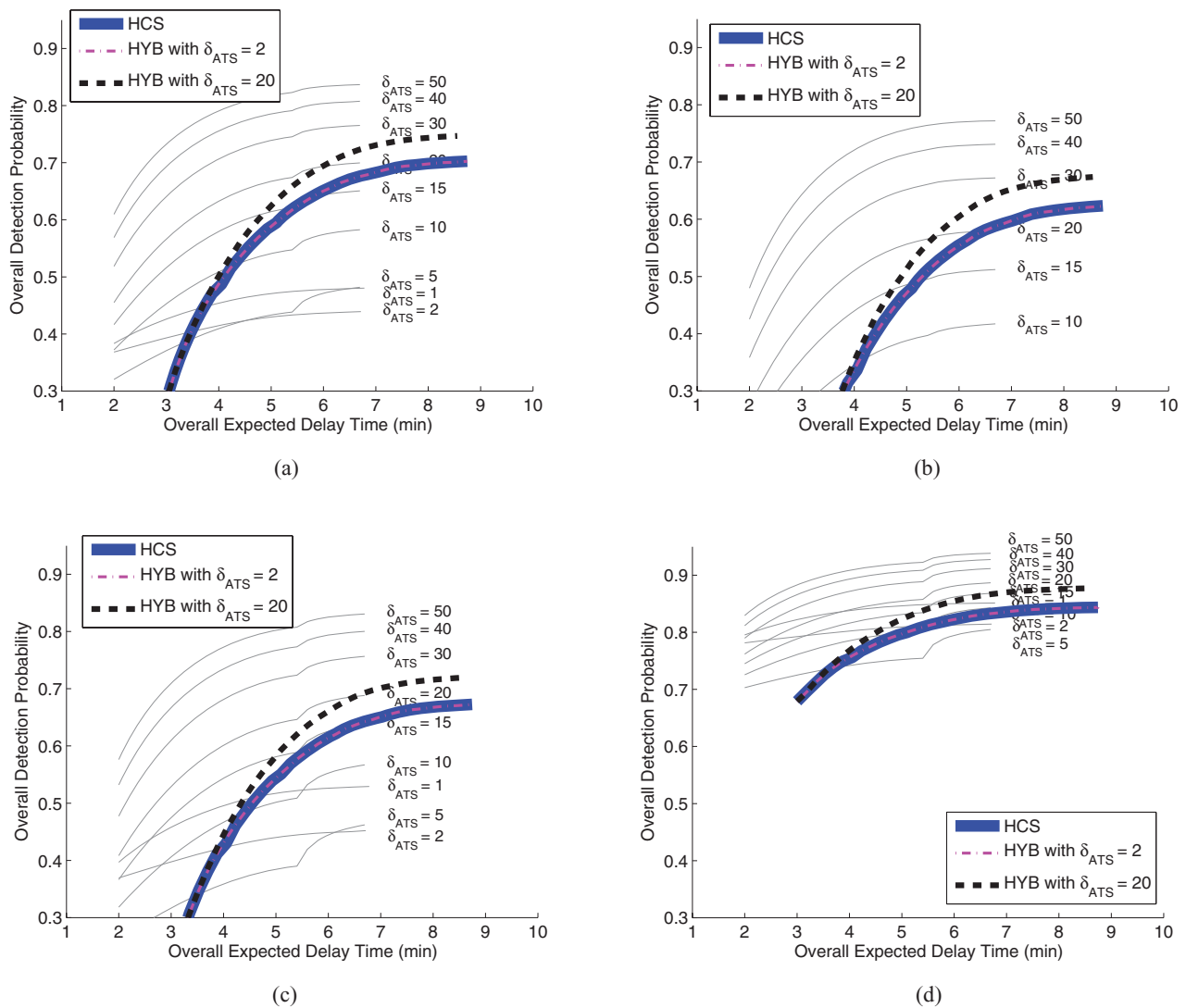
Thus, since the HCS and hybrid systems focus on maximizing the DP of the worst case, the choice of either of these inspection policies by the defender prevents the adversary from being able to game the inspection system.

## 8. CONCLUSION AND DISCUSSION

In this article we present a model framework for studying the problem of inspecting container traffic at sea ports for special nuclear materials. We model the port operations relevant to inspection efforts via a queuing network, where the servers correspond to individual inspection stages such as RPMs, radiography, and manual inspection. This basic framework is easily extensible to port operations in which other inspection steps are performed by adding inspection stages such as active inspection to the queuing network.

We also explicitly model the content of containers, and the impact of container content on shielding emissions from SNM in the container, using realistic detector models via simulation in MCNP. This allows us to obtain realistic estimates of actual detection probabilities.

Using this framework, we compare the performance of three basic inspection policies. One is the ATS-based inspection policy as it is in use currently



**Fig. 10.** Terrorist behavior analysis: (a) with uniform selection; (b) with quadratic selection; (c) with bell selection; (d) with inv-quadratic selection.

at domestic and foreign ports. The second inspection policy is a container content-dependent policy known as the HCS, which is a variant of a policy first described in Gaukler *et al.*<sup>(9)</sup> The third policy is a hybrid policy that combines elements of the ATS and HCS policies. The second and third policies rely on calculated hardness measures obtained from radiographic images taken of each incoming container. From these images, a “container type” is formed that reflects the densities, positions, and sizes of the items inside the container.

Our numerical studies show that the HCS and hybrid policies typically outperform the ATS-based

policy under realistic assumptions of allowable inspection delay time and reliability of intelligence information. In general, we find that if the reliability of intelligence information is low, a decisionmaker ought to use the HCS policy. If the reliability of intelligence information is high, the decision maker should make use of it via the hybrid policy. Only in instances where the reliability of intelligence is deemed extremely high ( $\delta_{ATS} > 30$  in our study), should a decisionmaker use the ATS-based policy.

Our study also shows that under an ATS-based inspection policy, if a sophisticated adversary manages to infiltrate a container that subsequently is not



flagged as high risk, then the chance of SNM being detected at the passive radiation detection stage is exceedingly small, even when the system parameters are set optimally. The HCS and hybrid policies are able to yield a significantly better DP in this case.

The main reason for the improvement in DP under the HCS and hybrid policies is due to the fact that these two policies are container-type-specific. As type-specific policies, they are able to set individual detection thresholds and thus optimize the allowance of false alarm rates for each container type. In particular, the HCS and hybrid policies are able to focus the inspection effort on “hard” containers that present particular problems to existing RPMs. In contrast, the ATS-based policy yields one “average” false alarm rate for all container types. Thus, the HCS and hybrid systems are able to utilize the existing capacity at the manual inspection stage better and more effectively than the ATS-based system. This more intelligent utilization of existing capacity leads to a dramatic improvement in DP.

We also study the potential of an adversary being able to game the inspection policies. For example, if the adversary knows that a container hardness-based policy is in place at a particular port, does this allow him to game the system by smuggling SNM into “softer” containers that may be under less scrutiny than hard containers? To address this concern, we model several different adversary types, each characterized by a different preference distribution for container types to infiltrate. Our numerical results suggest that there is no gaming opportunity for the adversary. If he opts for infiltrating a “soft” container, his success probability is actually minimized. Hence the adversary’s best choice, even knowing a hardness-based policy is in place, is to try to infiltrate a “hard” container and take advantage of the inherent shielding that this container offers. The defender’s best strategies against this adversary then are the HCS and Hybrid inspection policies. Thus, the choice of either of these inspection policies by the defender prevents the adversary from being able to game the inspection system.

We believe that our combination of queueing network analysis, policy evaluation and optimization, and detector and particle emissions modeling in MCNP makes this the to-date most realistic treatment of special nuclear materials interdiction at ports.

For future work, we are interested in extending this analysis to the international transportation net-

work level, where more than one port is involved. For example, it is of interest to investigate how inspection policies at foreign ports might affect the inspection at domestic ports. How should a decisionmaker at a domestic port use inspection results from foreign ports in his decision making, if at all? How is this affected by the possibility of container infiltration in-transit between ports? Another interesting research direction is to investigate which detection equipment is most useful at what node in the transportation network. For example, given a limited budget that does not allow all ports to have the same level of detection equipment, is there more benefit to install radiography equipment at foreign ports, or at domestic ports? We believe that our current single-port effort is a stepping stone toward, and likely a necessary component of, a model formulation that can investigate these additional questions.

**ACKNOWLEDGMENTS**

The authors gratefully acknowledge financial support for this research provided by the Domestic Nuclear Detection Office (DNDO) under Grant ARI-LA 2007. We thank our colleagues Wolfgang Bangerth, David Boyle, Bill Charlton, Craig Marianno, Pete Miller, Paul Nelson, and Arnold Vedlitz for many fruitful discussions that have contributed to enhancing this article.

**APPENDIX A. DERIVATION OF HARDNESS MEASURE**

The hardness measure  $h_s$  of container-type  $s$  is defined as the misclassification error that is determined by the two distribution functions, as area A in Fig. 6, namely:

$$h_s = P(\text{conclude that HEU exists} \mid \text{HEU is absent}) + P(\text{conclude that HEU does not exist} \mid \text{HEU is present}).$$

In the absence of HEU, we assume that the natural background emission for container-type  $s$  is a normally distributed random variable  $\Psi_s$  with mean  $\mu_{\Psi_s}$  and standard deviation  $\sigma_{\Psi_s} = \sqrt{\mu_{\Psi_s}}$ . The normal distribution is the result of the normal approximation to the Poisson distributed particle counts. The pdf is:

$$f_{\Psi_s}(x) = \frac{1}{\sqrt{2\pi}\sigma_{\Psi_s}} e^{-(x-\mu_{\Psi_s})^2/2\sigma_{\Psi_s}^2}.$$

In the presence of a quantity of HEU, it is also assumed that the radiation emission for that container type is a normally distributed random variable  $\Omega_s$  with mean  $\mu_{\Omega_s}$ , standard deviation  $\sigma_{\Omega_s} = \sqrt{\mu_{\Omega_s}}$ , and pdf:

$$f_{\Omega_s}(x) = \frac{1}{\sqrt{2\pi}\sigma_{\Omega_s}} e^{-(x-\mu_{\Omega_s})^2/2\sigma_{\Omega_s}^2}.$$

Since  $\mu_{\Psi_s} < \mu_{\Omega_s}$ , and  $\sigma_{\Psi_s} < \sigma_{\Omega_s}$ , the intersection points can be obtained as the solution to:

$$\text{Find } x \text{ such that } f_{\Psi_s}(x) = f_{\Omega_s}(x).$$

The intersection points are given by:

$$x_{1,2} = \frac{-R_1 \mp \sqrt{R_1^2 - R_2}}{2(\sigma_{\Omega_s}^2 - \sigma_{\Psi_s}^2)},$$

where  $R_1 = 2\mu_{\Omega_s}\sigma_{\Psi_s}^2 - 2\mu_{\Psi_s}\sigma_{\Omega_s}^2$ , and  $R_2 = 4(\sigma_{\Omega_s}^2 - \sigma_{\Psi_s}^2) \cdot (\mu_{\Psi_s}^2\sigma_{\Omega_s}^2 - \mu_{\Omega_s}^2\sigma_{\Psi_s}^2 + 2\sigma_{\Psi_s}^2\sigma_{\Omega_s}^2(\ln(\sigma_{\Psi_s}) - \ln(\sigma_{\Omega_s})))$ .

The hardness of container-type  $s$  is then obtained as:

$$h_s = 1 - \int_{x_1}^{x_2} (f_{\Psi_s} - f_{\Omega_s}) dx.$$

## APPENDIX B. SYSTEM COMPONENTS

In this section, we analyze the system flow and provide the node-to-node transition probabilities for containers entering the inspection network. These probabilities are then used to derive the system DP and the queuing network delay times.

### B.1. Probabilities at the T-Node

In the ATS and the HYB, all containers first go through the ATS-node (T-node). Information submitted by shipping companies as well as any additional intelligence information gathered regarding incoming containers will be evaluated by the ATS prior to the onsite arrival of the containers, and then categorized as either “low risk” (LR) or “high risk” (HR). Containers classified as HR are sent to the M-node directly, and LR containers are sent either to the P-node (for ATS), or to the R-node (for HYB), respectively.

Then, the probability that a container will travel from  $T$  to  $M$  is:

$$P(TM) = P(HR) = \beta,$$

and the probability that a container will take the other path or be classified as “low risk” is:

$$\begin{aligned} P(LR) &= P(TP) \text{ (for ATS)} \\ &= P(TR) \text{ (for HYB)} = 1 - \beta. \end{aligned}$$

With the definition of the intelligence information reliability measure  $\delta_{ATS}$  in Equation (1), and an application of Bayes’s theorem, the probability that a container with HEU is classified as HR at this T-node of the network is obtained as:

$$P(TM | \text{HEU}) = P(HR | \text{HEU}) = \frac{\delta_{ATS} \cdot \beta}{(1 - \beta) + \delta_{ATS} \cdot \beta}.$$

In the proposed inspection system, the fraction of containers that are directly escalated to manual inspection based on intelligence information, namely,  $\beta$ , is a decision variable.

### B.2. Probabilities at the R-Node

Both HCS and the hybrid system utilize the R-node, where radiography information is used. Different from the treatment in Ref. 9, we apply a randomization policy at the R-node. Instead of sending all the container types with hardness values greater than the threshold value  $t_R$  to manual detection, we randomly select a fraction  $a$  of those scenarios. This  $a$  is a new decision variable in our model. For a given container-type  $s$ , the probability of going from the R-node directly to the M-node, denoted by  $P(RM|s)$  for non-HEU containers, or  $P(RM|s^{\text{HEU}})$  for HEU containers, is:

$$P(RM|s) = P(RM|s^{\text{HEU}}) = \begin{cases} a & h_s \geq t_R \\ 0 & h_s < t_R, \end{cases}$$

and the probability of going from the R-node directly to the P-node, denoted by  $P(RP|s)$ , is  $P(RP|s) = 1 - P(RM|s)$ .

### B.3. Probabilities at the P-Node

The P-node and M-node are the common inspection nodes for all three inspection systems. At the P-node, containers undergo passive radiation screening. The results of the screening will be compared against the predetermined threshold at the passive node  $t_{P_s}$ , where  $t_{P_s} = \mu_{\Psi_s} + \sigma_{\Psi_s} \cdot \gamma_s$ , and  $\gamma_s$ s are determined through the optimization. Containers with passive screening results that fall below the threshold will proceed to the loading node. Containers with passive screening results that fall at or above the

threshold will proceed to secondary screening at the manual node.

For a container of type  $s$ , the probability that this container will travel from  $P$  to  $M$  is:

$$P(PM|s) = P(\Psi_s > t_{P_s}) = 1 - \Phi(\gamma_s).$$

Here,  $\Phi(\cdot)$  represents the cumulative distribution function of a standard normal distribution. We can then use this probability to define the proportion of containers that go from  $P$  to  $M$  as:

$$P(PM) = \sum_s P(PM|s)P(s|RP),$$

$$\text{where } P(s|RP) = \frac{P(s) \cdot P(RP|s)}{\sum_s P(s) \cdot P(RP|s)}.$$

Containers screened at the passive node may contain HEU. Hence, the probability that such containers will be successfully detected and will continue to the  $M$ -node from the  $P$ -node is:

$$P(PM|s^{\text{HEU}}) = P(\Omega_s > t_{P_s}) = 1 - \Phi_{\mu_{\Omega_s}, \sigma_{\Omega_s}}(t_{P_s}).$$

Here,  $\Phi_{\mu, \sigma}(\cdot)$  represents the cumulative distribution function of a normal distribution that has mean  $\mu$  and standard deviation  $\sigma$ .

#### B.4. Probabilities at the M-Node

The  $M$ -node is the location in our network at which the final decision will be made whether or not a container in fact contains HEU. We denote by  $d_M$  the probability that HEU will be successfully detected at  $M$  when it is present in a container. In this article, we assume that  $d_M = 1$ .

### APPENDIX C. HYB MODELING

This section contains the mathematical models for the HYB. By analyzing the flow diagram in Fig. 4, the DP and the expected delay time of the hybrid system are obtained. Here the DP is the probability that an HEU container will be successfully escalated to the manual detection.

#### C.1. Hybrid DP

For the HYB, a container may arrive at this node in one of three ways. Either the container is identified as ‘‘high risk’’ by the ATS, or it is identified as ‘‘low risk’’ and travels from  $R$  to  $M$ , or it is identified as ‘‘low risk’’ and travels from  $R$  to  $P$  to  $M$ . Then the probability that a container that contains HEU

arrives at  $M$  for HYB system is expressed as:

$$P(M|s^{\text{HEU}})^{\text{HYB}} = \begin{cases} P(TM|s^{\text{HEU}}) & \text{T-M} \\ P(TR|s^{\text{HEU}})P(RM|s^{\text{HEU}}) & \text{T-R-M} \\ P(TR|s^{\text{HEU}})P(RP|s^{\text{HEU}}) & \\ P(PM|s^{\text{HEU}}) & \text{T-R-P-M.} \end{cases}$$

The DP for container-type  $s$ , denoted as  $\text{DP}_s^{\text{HYB}}$ , is then defined as the HEU container of type  $s$  successfully arriving the detection node in the HYB. We can calculate the  $\text{DP}_s$  as follows:

$$\begin{aligned} \text{DP}_s^{\text{HYB}} &= d_M \cdot [P(TM|s^{\text{HEU}}) \\ &\quad + P(TR|s^{\text{HEU}})P(RM|s^{\text{HEU}}) \\ &\quad + P(TR|s^{\text{HEU}})P(RP|s^{\text{HEU}})P(PM|s^{\text{HEU}})]. \end{aligned}$$

#### C.2. Hybrid System Queuing Network Model

The second performance measure, that is, the expected delay time, represents the average time a container spends in the system. To calculate the expected delay time, we need to know the expected time spent at each node  $i$ ,  $T_i$ ,  $i \in \{R, P, M\}$ .  $T_i$  is the summation of the expected waiting time, which is found using a queueing network model. The queueing model uses the expected service time (which is the reciprocal of  $\mu_i$ ) and the number of servers at each node, denoted as  $m_i$ .

In this section, we explore the queueing results for all the nodes in the network. Since ATS decisions are made while the containers are still en route, the expected time spent at the ATS node is considered to be negligible. Therefore only the queues at the  $R$ -node,  $P$ -node, and  $M$ -node are considered. We assume that containers arrive at the port according to a Poisson process with rate  $\lambda$ , and the service rate at each of those nodes are also Markov processes. Thus, the  $R$ -node,  $P$ -node, and the  $M$ -node are modeled as  $M/M/C$  queues, where the first  $M$  denotes the Markov arrival process, the second  $M$  denotes the Markov service process, and  $C$  denotes multiple servers. The general  $M/M/C$  queue results can be applied to obtain the expected response time at those nodes, denoted as  $T_i$ ,  $i \in \{R, P, M\}$ , shown as follows:

$$T_i = \frac{1}{\mu_i} + \frac{\rho_i}{\lambda_i(1 - \rho_i)} \cdot \frac{(m_i \rho_i)_i^m}{m_i!(1 - \rho_i)} \cdot \pi_0,$$

where  $\rho_i = \frac{\lambda_i}{m_i \mu_i}$ , and  $\pi_0 = \frac{1}{\sum_{j=0}^{m_i-1} \frac{(m_i \rho_i)^j}{j!} + \frac{(m_i \rho_i)^{m_i}}{m_i!(1-\rho_i)}}$ . Here,  $\rho_i$  represents the utilization rate at node  $i$ . The utilization rate at the manual node is  $\rho_M = \frac{\lambda_M}{m_M \mu_M}$ , which is one of the constraints to the optimization problem.

An incoming cargo container can take one of four paths through the system:

$$\text{ATS} \rightarrow M \rightarrow L$$

$$\text{ATS} \rightarrow R \rightarrow M \rightarrow L$$

$$\text{ATS} \rightarrow R \rightarrow P \rightarrow M \rightarrow L$$

$$\text{ATS} \rightarrow R \rightarrow P \rightarrow L$$

Because the decisions at the ATS node ( $T$ -node) are made prior to the container's arrival and the loading node ( $L$ -node) is not considered part of the container inspection policy, we do not include the time spent at these nodes. As such, the time spent in the system for each container type is:

$$T_s^{\text{HYB}} = \begin{cases} T_M & \text{with } P(TM) \\ T_R + T_M & \text{with } P(TR)P(RM|s) \\ T_R + T_P + T_M & \text{with } P(TR)P(RP|s)P(PM|s) \\ T_R + T_P & \text{with } P(TR)P(RP|s)(1 - P(PM|s)) \end{cases}$$

Consequently, the expected delay time of all container types for the hybrid system is:

$$DT^{\text{HYB}} = \sum_{s \in S} T_s^{\text{HYB}} \cdot p_s,$$

where  $p_s$  is the proportion of each container type and listed in Table II.

## APPENDIX D. ATS INSPECTION SYSTEM MODELING

This section contains the mathematical models for the ATS-based inspection system, shown in Fig. 1. Compared to the hybrid system in Fig. 4, the ATS system does not have the  $R$  node. Thus, a container can arrive at the  $M$  node through two paths: either from the  $T$  node directly to the  $M$  node, or from the  $T$  node to the  $P$  node and then to the  $M$  node.

### D.1. ATS DP

The probability of a container with HEU inside arriving at the  $M$  node for the ATS system:

$$P(M|s^{\text{HEU}})^{\text{ATS}} = \begin{cases} P(TM|s^{\text{HEU}}) & \text{T-M} \\ (1 - P(TM|s^{\text{HEU}}))P(PM|s^{\text{HEU}}) & \text{T-P-M} \end{cases}$$

The DP for container type  $s$  for the ATS system is then:

$$DP_s^{\text{ATS}} = d_M \cdot [P(TM|s^{\text{HEU}}) + (1 - P(TM|s^{\text{HEU}}))P(PM|s^{\text{HEU}})].$$

## D.2. ATS System Queuing Network Model

The expected delay time for container-type  $s$  is:

$$T_s^{\text{ATS}} = \begin{cases} T_M & \text{with } P(TM) \\ T_P + T_M & \text{with } (1 - P(TM))P(PM|s) \\ T_P & \text{with } (1 - P(TM))(1 - P(PM|s)) \end{cases}$$

Therefore, the expected delay time of all container types for the ATS system is obtained as:

$$DT^{\text{ATS}} = \sum_{s \in S} T_s^{\text{ATS}} \cdot p_s.$$

## APPENDIX E. HCS INSPECTION SYSTEM MODELING

Similarly, the mathematical formulation for the HCS inspection system is obtained by analyzing the system flow shown in Fig. 3. Containers can arrive at the  $M$ -node through two paths: either from the  $R$ -node directly to the  $M$ -node, or from the  $R$ -node to the  $P$ -node and then to the  $M$ -node.

### E.1. HCS DP

The probability of a container with HEU inside arriving at the  $M$ -node for the HCS system is:

$$P(M|s^{\text{HEU}})^{\text{HCS}} = \begin{cases} P(RM|s^{\text{HEU}}) & \text{R-M} \\ (1 - P(RM|s^{\text{HEU}}))P(PM|s^{\text{HEU}}) & \text{R-P-M.} \end{cases}$$

The DP for container-type  $s$  for the HCS system is:

$$DP_s^{\text{HCS}} = d_M \cdot [P(RM|s^{\text{HEU}}) + (1 - P(RM|s^{\text{HEU}}))P(PM|s^{\text{HEU}})].$$

**E.2. HCS System Queuing Network Model**

Since the HCS inspection system has queuing at the *R*-node, *P*-node, and the *M*-node, the expected delay time for container-type *s* is:

$$T_s^{\text{HCS}} = \begin{cases} T_R + T_M & \text{with } P(RM) \\ T_R + T_P + T_M & \text{with } (1 - P(RM))P(PM|s) \\ T_R + T_P & \text{with } (1 - P(RM))(1 - P(PM|s)) \end{cases}$$

The expected delay time for all container types for the HCS system is then obtained as

$$DT^{\text{HCS}} = \sum_{s \in S} T_s^{\text{HCS}} \cdot p_s.$$

**REFERENCES**

1. Medalia J. Terrorist Nuclear Attacks on SeaPorts: Threat and Response. Congressional Research Service Report, CRS 21293, August 2002.
2. Woolf AF. Nuclear Weapons in Russia: Safety, Security, and Control Issues. Congressional Research Service Report, CRS IB98038, August 2003.
3. International Atomic Energy Agency. Illicit Trafficking and Other Unauthorized Activities Involving Nuclear and Radioactive Materials Fact Sheet. International Atomic Energy Agency Report, January 2006.
4. U.S. Department of Transportation. America’s Container Ports: Freight Hubs that Connect Our Nation to Global Markets. U.S. Department of Transportation, June, 2009.
5. Frittelli JF. Port and Maritime Security: Backgrounded and Issues for Congress. CRS Report for Congress, Congressional Research Services, RL 31722, May 2005.
6. Fetter S, Frolov VA, Miller M, Mozley R, Prilutsky OF, Rodionov SN. Detecting nuclear warheads. Science & Global Security, 1990; 1:225–302.
7. International Atomic Energy Agency. Detection of Radioactive Materials at Borders. International Atomic Energy Agency Report, September 2002.
8. Union of Concerned Scientists. Weapon Material Basics. Union of Concerned Scientists, 2004. Available at: [http://www.ucsusa.org/assets/documents/nwgs/nuclear\\_terrorism\\_fissile\\_materials.pdf](http://www.ucsusa.org/assets/documents/nwgs/nuclear_terrorism_fissile_materials.pdf)
9. Gaukler GM, Li C, Cannaday R, Chirayath SS, Ding Y. Detecting nuclear materials smuggling: Using radiography to improve container inspection policies. Annals of Operations Research, 2011; 187(1): 65–87.
10. Wein LM, Wilkins AH, Baveja M, Flynn SE. Preventing the importation of illicit nuclear materials in shipping containers. Risk Analysis, 2006; 25(5):1377–1393.
11. Elsayed EA, Young CM, Xie M, Zhang H, Zhu Y. Port-of-entry inspection: Sensor deployment policy optimization.

- IEEE Transactions on Automation Science and Engineering, 2009; 6(2):265–276.
12. Young CM, Li M, Zhu Y, Xie M, Elsayed EA, Asamov T. Multiobjective optimization of a port-of-entry inspection policy. IEEE Transactions on Automation Science and Engineering, 2010; 7(2):392–400.
13. Pan F. Stochastic network interdiction: Models and methods. PhD thesis, University of Texas, Austin, TX, May 2005.
14. Morton DP, Pan F, Saeger KJ. Models for nuclear smuggling interdiction. IIE Transactions, 2007; 39:3–14.
15. Wein LM, Liu Y, Cao Z, Flynn SE. The optimal spatiotemporal deployment of radiation portal monitors can improve nuclear detection at overseas ports. Science and Global Security, 2007; 15:211–233.
16. Atkinson MP, Cao Z, Wein LM. Optimal stopping analysis of a radiation detection system to protect cities from a nuclear terrorist attack. Risk Analysis, 2008; 28(2):353–370.
17. Atkinson MP, Wein LM. Spatial queueing analysis of an interdiction system to protect cities from a nuclear terrorist attack. Operations Research, 2008; 56(1):247–254.
18. Boros E, Fedzhora L, Kantor PB, Saeger K, Stround P. A large-scale linear programming model for finding optimal container inspection strategies. Naval Research Logistics, 2009; 56(5):404–420.
19. Stroud PD. Enumeration of increasing boolean expressions and alternative digraph implementations for diagnostic applications. Pp. 318–333 in Chu H, Ferrer J, Nguyen T, Yu Y (eds). Proceedings Volumn IV, Computer, Communication and Control Technologies. Orlando, FL: International Institute of Informatics and Systematics, August 2003.
20. Madigan D, Mittal S, Roberts F. Sequential decision making algorithms for port of entry inspection: Overcoming computational challenges. Pp. 1–7 in Muresan G, Altiok T, Melamed B, Zeng D (eds). Proceedings of IEEE International Conference on Intelligence and Security Informatics. New Jersey: IEEE Press, 2007.
21. Boros E, Elsayed E, Kantor P, Robert F, Xie M. Intelligence and security informatics: Techniques and applications. In Optimization Problems for Port-of-Entry Detection Systems. Studies in Computational Intelligence. Berlin Heidelberg: Springer, 2008.
22. Kobza JE, Jacobson SH. Probability models for access security system architectures. Journal of the Operational Research Society, 1997; 48(3):255–263.
23. Kobza JE, Jacobson SH. Addressing the dependency problem in access security system architecture design. Risk Analysis, 1996; 16(6):801–812.
24. McLay LA, Jacobson SH, Kobza JE. The tradeoff between technology and prescreening intelligence in checked baggage screening for aviation security. Journal of Transportation Security, 2008; 1:107–126.
25. McLay LA, Jacobson SH, Nikolaev AG. A sequential stochastic passenger screening problem for aviation security. IIE Transactions, 2009; 41:575–591.
26. Stana RM. Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System. U.S. Government Accountability Office Report, GAO-06-591T, March 2006.
27. Aloise G. Combating nuclear smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, But Preliminary Results Show Limits of the New Technology. U.S. Government Accountability Office Report, GAO-09-655, May 2009.
28. Moss CE, Hollas CL, McKinney GW, Myers WL. Comparison of active interrogation techniques. IEEE Transactions on Nuclear Science, 2006; 53(4):2242–2246.
29. Cirincione R, Cosmas A, Low C, Peck J, Wilds J. Barriers to the Success of 100 Percent Maritime Cargo Container Scanning. Massachusetts Institute of Technology



- Engineering Systems Division Report, ESD-WP-2007-05, January 2007.
30. X-5 Monte Carlo Team. MCNP-a General Monte Carlo N-Particle Transport Code, Version 5, 2003.
  31. Defense File. AS&E's Z Portal Vehicle Screening System at USA Southwest Border, October 2009. Available at: <http://www.defensefile.com>, Accessed December 2010.
  32. Srikrishna D, Chari AN, Tisch T. Nuclear Detection: Fixed Detectors, Portals, and NEST Teams Won't Work for Shielded HEU on a National Scale; a Distributed Network of In-Vehicle Detectors Is also Necessary to Deter Nuclear Terrorism, October 2005. Available at: <http://www.devabhaktuni.us/research/disarm.pdf>, Accessed December 2010.
  33. MATLAB. R2010b Documentation, Global Optimization Toolbox: Using the Genetic Algorithm, 2010. Available at: <http://www.mathworks.com/help/toolbox/gads/f6010df3.html>, Accessed December 2010.
  34. PIERS. Top 100 U.S. importers via ocean container transport-2007. *Manufacturing & Technology News*, 2008; 15(14):6.