Nuclear Engineering and Technology 52 (2020) 626–632

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

A strategic analysis of stationary radiation portal monitors and mobile detection systems in border monitoring

Ryan Coogan [a], Craig Marianno [a, *], William Charlton [b]

[a] Department of Nuclear Engineering, Texas A&M University, United States
[b] Department of Mechanical Engineering, University of Texas at Austin, United States

ARTICLE INFO

Article history:
Received 30 December 2018
Received in revised form
8 April 2019
Accepted 16 August 2019
Available online 21 August 2019

Keywords:
Terrorism
Smuggling
Second line of defense
Transportation
Border
RPM

ABSTRACT

Radiation Portal Monitors (RPMs) are our primary border defense against nuclear smuggling, but are they still the best way to spend limited funds? The purpose of this research is to strategically compare RPM defense at the border with state-side mobile detectors. Limiting the problem to a comparison of two technologies, a decision-maker can prioritize how to best allocate resources, by reinforcing the border with stationary overt RPMs, or by investing in Mobile Radiation Detection Systems (MRDs) which are harder for an adversary to detect but may have other weaknesses. An abstract, symmetric network was studied to understand the impact of initial conditions on a network. An asymmetric network, loosely modeled on a state transportation system, is then examined for the technology that will maximally suppress the adversary's success rate. We conclude that MRDs, which have the advantage of discrete operation, outperform RPMs deployed to a border. We also conclude that MRDs maintain this strategic advantage if they operate with one-tenth the relative efficiency of their stationary counter-parts or better.

1. Introduction

The theft and trafficking of nuclear material is a significant concern in counter terrorism strategies and to the international nonproliferation regime which has demonstrated that nuclear smuggling is real, albeit rare, and primarily the work of organized groups rather than lone-wolf actors [1,2].

U.S. nuclear security is a multi-stage process that begins with enhancing security of foreign nuclear material and continues to U.S. borders where radiation portal monitors (RPMs) can detect nuclear materials moving through the border. RPMs are passive systems that can detect nuclear and radiological materials in vehicles, containers, and on persons passing through them. There are a few different configurations for portal monitors; however, the most common configuration is double-sided where two detectors are placed on opposite sides of a controlled lane to scan objects of interest for both gamma and neutron radiation. Improvements in technology and the commercialization of radiation detectors have made mobile radiation detection systems (MRDs) another option that can support security. Mobile systems are housed in trucks, vans, or SUVs that can be deployed to major thoroughfares or surged to protect a potential target, interdicting actors that have breached the border.

A number of network interdiction models have been developed and studied over the last decade. Wood developed a deterministic model for analyzing commodity smuggling wherein an interdictor with limited resources seeks to minimize an adversary's commodity trafficking across a capacitated network [3]. Wood demonstrated that even this basic problem, solving for the interdictor's cost-effective investment, is computationally exhaustive. Dimitrov copes with the computational challenge that Wood discovered by inverting the data stream, turning the unknown resources into a known input instead [4]. Under a known threat scenario, with known detection probabilities, this stochastic model plots the most effective deployment of detectors. Cheng et al. demonstrated the viability of a mobile sensor network where simple radiation detectors are mounted in vehicles [5]. Israeli and Wood acknowledge that adversaries may have access to pathways that are immune to the influence of an interdictor [6]. The number of cross-border tunnels that have been discovered to smuggle narcotics into the United States is evidence enough that Israeli and Wood were correct [7]. A practical model must consider that there may be nodes and pathways that the interdictor cannot influence or may not even know exist.

* Corresponding author.
E-mail address: marianno@tamu.edu (C. Marianno).

https://doi.org/10.1016/j.net.2019.08.010
1738-5733/

A comprehensive model may be intractable, however, a model that examines a particular scenario can be sufficiently limited to provide a solution that is informative for decision makers [8]. The research presented here makes several assumptions and simplifications, justified by the narrow scope of the research objective, and by the computational limits of comprehensive network modeling. We assume that the adversary is a group that is technically sophisticated, conventionally capable, and well-funded. These assumptions include a network model where the adversary has access to routes which are immune to the interdictor's influence, where the interdictor's detection capabilities are known with certainty, but the adversary's success is uncertain and expressed as a probability. These assumptions make for a simplistic model, but one that is well justified by the research presented above.

2. Methods

The strategic problem of analyzing a transportation network can be examined with a modeled network composed of nodes and pathways [4]. Nodes represent specific physical locations such as airports, border crossings, seaports, etc. Whereas pathways represent a transportation path available to an adversary vis-à-vis roadways, rail, boat, etc. that connects two nodes. Nodes are the end-points and midpoints for all pathways, representing entry points into the network, the target destination, and midpoint opportunities (such as junctions or a change in transport). A simple network is illustrated in Fig. 1.

SHIELD is a code developed by Jun Luo, Alexander Solodov, and William Charlton at the Center for Nuclear Security Science and Policy Initiatives (NSSPI) to analyze the strategic problem of nuclear smuggling using a network composed of nodes and pathways. An input deck provided by the user generates a network with a starting node, a target node, and a network of intermediary nodes and pathways. Each node and pathway has a perceived non-detection probability, which is used to calculate the adversary's preferences in routes; the actual non-detection probability is used in calculating the adversary's expected success in traversing the network.

SHIELD linearizes all routes across the network, eliminating low probability and zero-success routes in favor of high success routes until the code has the user-defined maximum number of routes. A Monte Carlo method is used to determine the adversary's successes and failures across multiple routes. SHIELD then aggregates the successes and failures of the adversary across all routes and calculates the adversary's overall success. SHIELD does track distance and time across different routes, however, these are not variables on the network's output.

In this work, RPMs are modeled as nodes in a border region with a static detection probability. It is assumed that all RPMs have the same detection probability and that real differences in the lab are insignificant to the strategic problem of determining adversary preferences. For all RPMs, the non-detection probability is 0.02, based on ANSI standards [9]. MRDs are modeled as pathways with a detection probability greater than zero (since we assume that the indigenous probability of detection for each pathway is zero). The MRD's non-detection probability is assumed to be the same as RPMs, because ANSI standards for both systems are identical for the purposes of evaluating non-detection probability [9,10]. MRDs have significantly less control over geometry and implementation than RPMs because of the way they are used, which may include discrete operations. This work also considers a range of possible values for MRD efficiencies relative to RPMs, such that:

$$P_{MRD} = P_{RPM} * \varepsilon$$

where P_{MRD} is the detection probability of the MRD unit, P_{RPM} is the detection probability of the RPM unit, and ε is the fractional difference in efficiency between an RPM, which operates in practically ideal circumstances, and the MRD which does not. Initial simulations would assume that the fractional difference in efficiency is unity, the fractional difference in efficiency of MRDs would later be perturbed and simulations rerun for scenarios where ε was less than unity.

MRDs are modeled as a detection capability on pathways of the network. MRDs are centered on a node inside the border and traverse adjacent pathways feeding in or out of this node. It is assumed that there is an equal probability that the MRD unit will be positioned to any of its adjacent pathways. The probability (p) that a MRD unit is on any given pathway at any given time is $p = \frac{1}{n}$ where n is the number of adjacent pathways. Therefore, the non-detection probability for a pathway is:

$$\beta_{i,j} = 1 - \frac{P_{MRD}}{n_i}$$

where $\beta_{i,j}$ is the non-detection probability of a pathway connected to deployment node i and node j, n_i is the number of paths connected to deployment node i, and P_{MRD} is the detection probability of the MRD unit.

An illustration of MRD modeling is provided in Fig. 1. Node 2 is the deployment node (i). The adversary can only move forward toward the target (denoted by arrows), but the mobile unit can be positioned on any connected pathway. All pathways moving in or out of the deployment node are potential routes (n) for the MRD and will have a non-detection probability determined by the formula given above. For an ideal system where the MRD has perfect detection capabilities (i.e., where $\varepsilon = 1$), $\beta_{1,2} = 0.333$. A demonstration of how SHIELD analyzes a simple network like the one below can be found in the Appendix.

This work is a comparative assessment of two technologies (RPMs and MRDS), and therefore our primary focus is how these technologies impact the strategic problem of nuclear smuggling

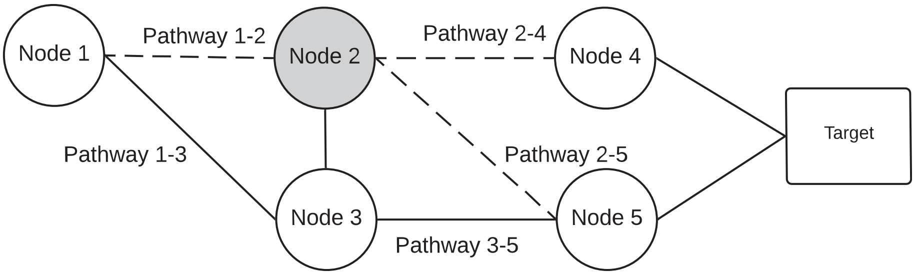

Fig. 1. Node 2 is the deployment node for a MRD unit. Pathways 1–2; 2–4; and 2–5 will have an increased detection capability as a result. See Appendix for a more thorough breakdown.

relative to each other. Therefore, it is assumed that RPMs and MRDs dominate the non-detection probabilities associated with the network. Indigenous detection probabilities, such as local law enforcement which may contribute to detection and interdiction, are not considered in this model.

This work considers the conservative case – an intelligent adversary that is technically sophisticated, capable, and well-funded. Intelligence is modeled as the ability to accurately identify RPMs and assess their non-detection capabilities, and therefore,

$$\beta_j^{Per} = \beta_j^{Act}$$

where β_j^{Per} is the adversary's perceived non-detection probability for node j and β_j^{Act} is the actual non-detection probability of node j. Intelligence and conventional capabilities are modeled in the adversary's ability to perceive and rank-order routes across the whole network rather than traversing the network step-by-step. The adversary's perceived non-detection probability for any given route is a product of that route's non-detection probabilities.

It is also assumed that an intelligent adversary may be informed to the presence of MRDs on the network, but is not capable of identifying placement because MRDs can be housed in low-profile automobiles that would make identification very difficult. Further, MRDs may be deployed to several potential sites and thoroughfares that can be challenging to scout and plan around. For pathways that do house MRD capability, the perceived non-detection probability ($\beta_{i,j}^{Per}$) will always be less than the actual non-detection probability ($\beta_{i,j}^{Act}$). Therefore,

$$\beta_{i,j}^{Per} < \beta_{i,j}^{Act}$$

A strategic analysis was conducted on two networks – a simple symmetrical network and a more complicated asymmetrical network. Each network was composed of four different regions – pre-border, border, principality, and target – see Fig. 2.

The pre-border region represents materials outside the border and is used strictly to position material for movement across the border region. The border region represents entry points into the state and is composed of legal border crossings with simulated RPMs and illegal “holes” which have zero-detection capability. The default network has 80% coverage across the border, and legal entry points are nodes with a perceived and actual non-detection capability of two percent:

$$\beta_j^{Per} = \beta_j^{Act} = 0.02$$

The principality region represents pathways and opportunities available inside the border en-route to the target. The default non-detection probability for all pathways and nodes in the principality region is unity. The target region is composed of a single node that the adversary must reach. The target node does not change.

An asymmetric network was inspired by a state roadway system. Previous simulation, using a simplified and symmetric network, was used to test the code's sensitivity to different initial conditions. We eliminated distance, time, and the distribution of illegal entry points as variables in the network's output. For simplicity, we distributed illegal entry points randomly throughout the network. The asymmetric network, with the initial distribution of holes and RPMs, is shown in Fig. 3. The principality region was further divided into two parts – roadways and major thoroughfares. Major thoroughfares were identified as pathways that fed into or out of major transportation hubs on the network, effectively creating choke points. MRD assignments were restricted to nodes on thoroughfares. This restriction on MRDs was designed to better simulate an intelligent and strategic deployment, exploiting the natural bottlenecks that exist in a transportation system. The network's thoroughfares are shown in Fig. 4.

3. Results and discussion

The network initially tested only the impact of additional RPMs. RPMs were added piece-wise to the border region and tested, until all holes in the border region were closed by RPMs. As shown in Table 1, RPMs had a negligible impact on adversary success until they achieved full coverage of the border region, when there are zero holes. However, this is not realistic, as the adversary will always have access to pathways which the state cannot perceive [6,7].

MRDs were then tested on the asymmetric network, with a baseline of 34 entry points and 8 illegal holes (Fig. 3). MRDs were initially tested with comparable efficiency to RPMs. MRDs were based out of major transportation hubs and deployed strictly to the major thoroughfares previously identified (Fig. 4). Additional MRDs were added to the network and tested as well. MRDs were never assigned to the same node but could overlap in the pathways that they covered. Overlapping routes were treated as independent probabilities. Eight trials using 100,000 simulations were run, one for each MRD deployment position in the network.

Mobile units were highly effective in decreasing the adversary's success rate (Table 2). A single mobile unit of comparable efficiency to an RPM decreased the adversary's success by 20.12% on average. However, the variance in the adversary's success rate tells us that MRD performance is highly sensitive to placement. Mobile units decreased adversary success by as much as 33.44% and as little as 5.56%. In a one-to-one comparison, this is significantly more

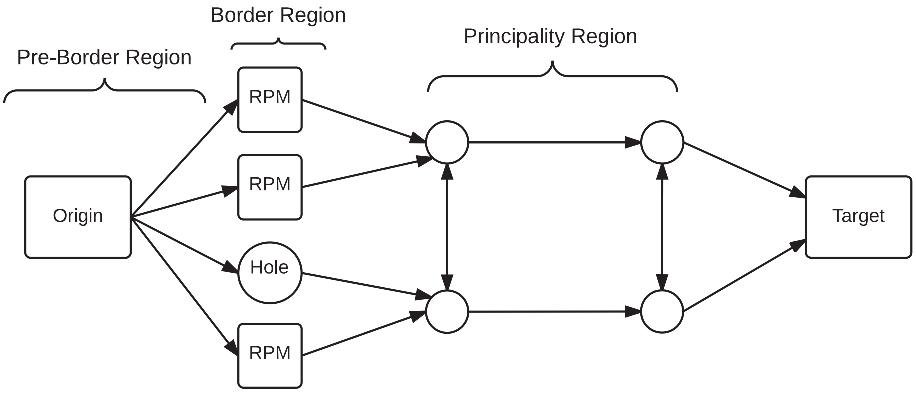

Fig. 2. A sample network with a pre-border, border, principality, and target regions.

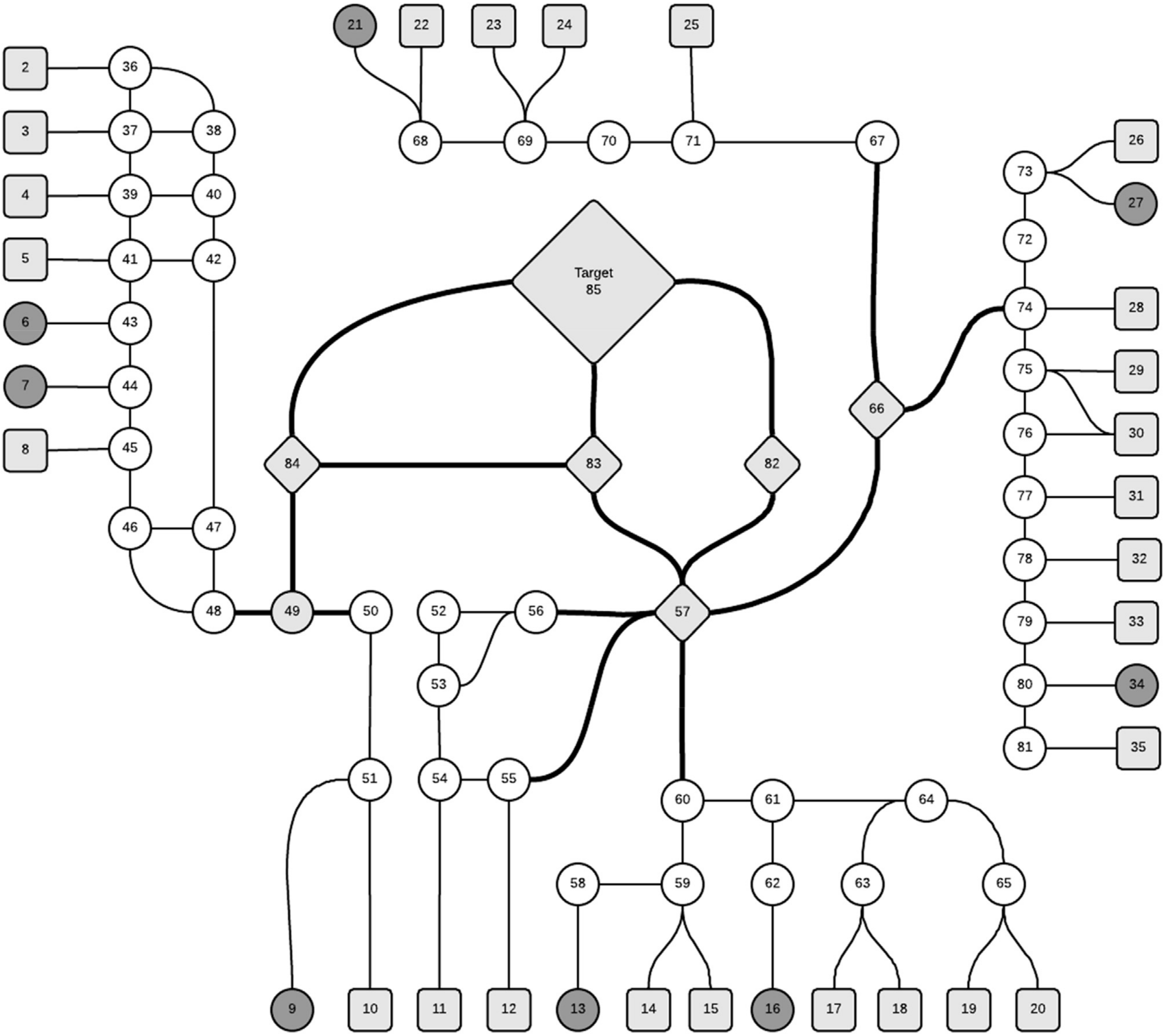

Fig. 3. The complete asymmetric network. RPMs are denoted by grey boxes and illegal holes are denoted by dark grey circles. Through-fares are denoted by bold pathways. MRD deployment nodes are marked by diamonds.

effective than stationary RPMs. The most effective MRDs were those positioned close to target or that had connection to all border entry points, even if there were alternative routes. Position 84 and 83 were close to target. Both had routes to every illegal entry point. While there were also alternative routes where an adversary could have avoided the MRDs, this large footprint seems to be the key to the high impact on adversary success. Position 85, the Target, also had minimal adversary success for the same reasons. Conversely, position 49 and position 66 had the smallest impact on the adversary. These positions covered only some of the illegal entry points into the network. Given the robust number of entry points and routes the adversary could take, these deployment positions simply did not have the kind of footprint that other deployment positions did.

Additional mobile units were then added to the model, such that every deployment position was tested in combination with a secondary deployment position. This process was repeated, to test three MRDs on a single network. Additional mobile units provided smaller returns, which is to be expected, but still had a large impact, upwards of 2.5 times the standard deviation, on the adversary's ability to successfully negotiate the network. Additional mobile units on the network have a measurable impact on the adversary's success (see Table 3). This research does not measure the impact of more than three mobile units on the network but does predict that as the population of MRDs grows, the adversary's success will drop off logarithmically until approaching a minimum where every thoroughfare has been blanketed with multiple MRDs. As with RPMs, this may not be realistic as we ought to assume that in such a circumstance the actor has access to pathways which the interdictor cannot perceive or influence [6].

The relative efficiency of MRDs was perturbed and the simulations duplicated for a system in which MRDs possessed one-half, one-third, and one-tenth the detection capability of their RPM counterpart (See Table 4). At one-tenth relative efficiency, the MRDs still reduced the adversary's expected success rate to 97.63%. However, the uncertainty included in this number (0.91%), overlaps with our results of a very effective RPM regime creating a conservative equilibrium point between these technologies.

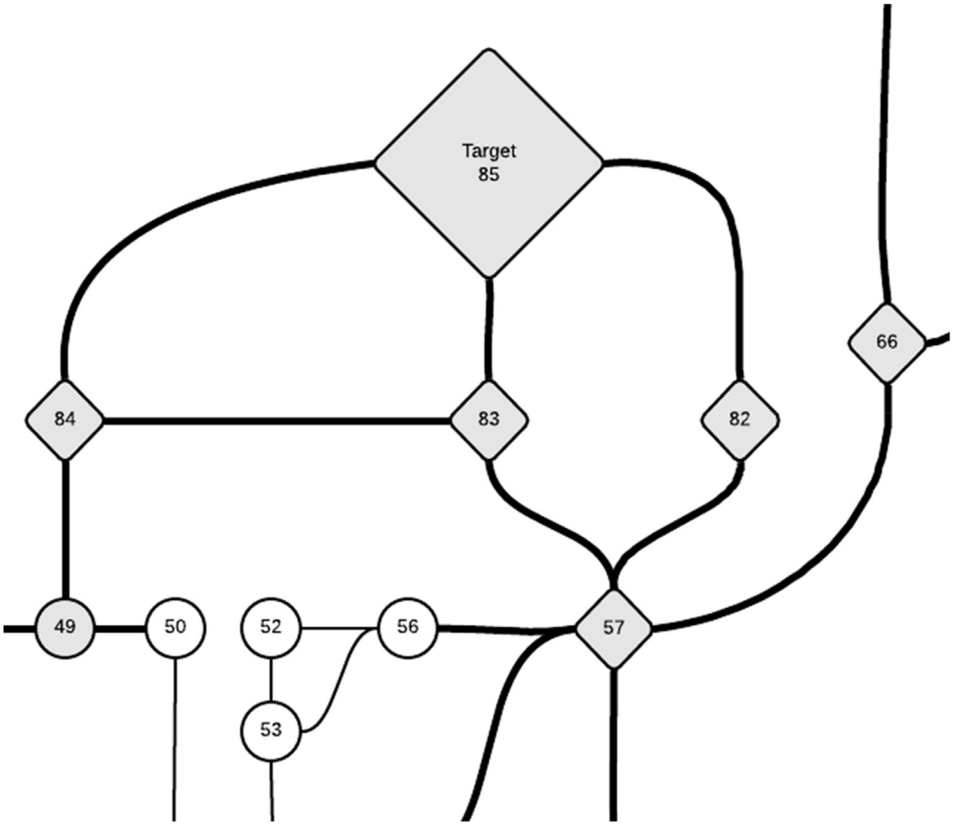

Fig. 4. Major thoroughfares feed into or out of critical transportation nodes on the network. These nodes connect the border region to the larger network and to each other. MRDs deployments nodes are grey diamonds.

Table 1
RPMs have a negligible impact on the adversary's success rate until they are ubiquitous.

Illegal Holes	Adversary Success Rate (Percent)
8	100.00
7	100.00
6	100.00
5	100.00
4	100.00
3	99.55
2	98.74
1	97.18
0	1.92

Table 2
MRDs have a significant impact on the asymmetric network, decreasing the adversary's success rate by 20.12% in the aggregate. Eight trials were run to cover all eight deployment positions, with 100,000 simulations per trial.

Position	Adversary Success Rate
Position 49	94.37
Position 57	79.17
Position 66	94.44
Position 82	85.12
Position 83	72.49
Position 84	66.56
Position 85	66.98
MIN	66.56
MAX	94.44
AVERAGE	79.88
Std. Dev	11.01

Table 3
Additional MRDs provide diminishing returns but have a profound impact on the adversary's failure rating.

	Adversary Success Rate		
	1 MRD	2 MRDs	3 MRDs
MIN	66.56	44.76	34.00
MAX	94.44	79.71	64.87
AVERAGE	79.88	62.54	48.53
Std. Dev	5.28	5.91	5.56

Table 4
The average success rate for a single MRD of varying relative efficiencies on the asymmetrical network.

Position	$\varepsilon = 1$	$\varepsilon = 1/2$	$\varepsilon = 1/3$	$\varepsilon = 1/10$
Position 49	94.37	91.34	93.96	98.24
Position 57	79.17	89.12	93.21	97.26
Position 66	94.44	97.00	97.93	99.38
Position 82	85.12	91.48	94.19	97.98
Position 83	72.49	85.06	89.61	97.07
Position 84	66.56	82.41	87.59	96.43
Position 85	66.98	84.13	88.99	97.02
MIN	66.56	82.41	87.59	96.43
MAX	94.44	97.00	97.93	99.38
AVERAGE	79.88	88.65	92.21	97.63
Std. Dev.	11.01	4.74	3.36	0.91

Unfortunately, it is very difficult to identify if we possess a highly effective RPM regime – one where a smuggler has very limited options for moving through illegal entry points – because the smuggler's pathways cannot be fully known [6]. We can say that a conservative equilibrium point exists where neither technology can be said to outperform the other with certainty. A MRD with a relative efficiency greater than one-tenth would outperform a RPM. At one-tenth it cannot be said that one system outperforms the other on average. Below one-tenth relative efficiency, there does not appear to be a strategic benefit to MRDs.

4. Conclusions

Decision makers who wish to increase our capabilities against nuclear smuggling threats must weigh the payoffs of investing further into RPMs or diversifying into MRDs. This paper does not examine the costs associated with these choices, but it does examine the impact measured as a decrease in the success rate of a simulated adversary. This research demonstrates that MRDs have a significantly higher impact on adversary success rate per unit deployed given some assumptions and simplifications to constraint uncertainty. Mobile units are discrete and while the adversary may be able to anticipate their presence, they cannot have the same confidence in their placement as a stationary (and fairly obvious) RPM. This manifests in decreased adversary success in a range of scenarios and MRD efficiencies. The overall results of this work demonstrate that MRDs can be more effective than RPMs when considering an intelligent adversary that is technically sophisticated, capable, and well-funded.

Perturbing the efficiencies of MRDs on the network presents a target threshold for manufacturers. This work examined MRDs with a relative efficiency of as low as 10% compared to RPMs. Although ANSI standards make the two systems practically identical, execution in a real-world scenario may drop MRD non-detection probabilities. At one-tenth relative efficiency, MRDs are comparable to RPMs. Below this value, the effectiveness of the MRDs are too small and the uncertainties too large to say with confidence how it performs compared to a robust RPM program with limited pathways for an adversary. There may still be tactical advantage to MRDs at this efficiency because of mobility, especially when complimented with actionable intelligence, but that is beyond the scope of this work. We recommend that manufacturers aim for a system which has a non-detection probability one-third of an RPM or better in a real-world application scenario. Even a system that performs at one-tenth the efficiency of an RPM in a real world scenario will have a larger impact than one RPM, but the impact is quite low.

MRDs have a higher impact on adversary success rate per unite deployed than RPMs and are likely worth the investment. While the costs associated with each system is not the focus of this work, it is worth acknowledging that there already exists an infrastructure for RPM deployment and use. RPMs have been well adapted into Customs and Border Protection and there is established protocol and norms for secondary screenings, clearing an alarm, etc [11]. MRDs have no such infrastructure. More importantly, their mobility creates additional complications which do not exist for stationary RPMs operating at a site that is heavily controlled and monitored. A comprehensive MRD program must consider the following challenges:

1. Procedure for a vehicle stop.
2. Secondary screening procedure.
3. Clearing an alarm.
4. Jurisdiction.

Investing into additional RPMs will aid against opportunist adversaries, because the opportunist (by definition) has a limited capability to detect and avoid RPMs. Against an intelligent and capable adversary, further investment into RPMs will have a negligible impact on adversary success until they become ubiquitous. However, this is not a practical solution for the real world where illegal entry points can be manufactured and discovered by resourceful adversaries. MRDs have a measurable impact on adversary success without being omnipresent; they can be surged to protect a target when actionable intelligence is present, and they can be operated in a discrete fashion that will hinder the adversary's ability to make rational choices about successful movement.

APPENDIX

SHIELD linearizes all possible routes on the network, eliminates low probably and zero-success routes based on the user's preferences, and then uses a Monte Carlo method to determine the adversary's successes and failures across multiple routes. In a simple network (see Fig. 1 on page 4), the adversary would begin at the origin node (1) and traverse the network to reach the target (T). In this sample network there are no RPMs and one MRD. Pathways 1–2, 2–4, and 2–5 each have a non-detection probability of 0.6733 for the case where $\varepsilon = 1$. All other pathways have a non-detection probability of unity since we do not account for any indigenous detection capability on the network.

SHIELD linearizes the complete network into all possible routes from the origin node to the target. For the network in Fig. 1, there are six complete routes available to the adversary. Those six pathways are given in Table 5. As the adversary travels across a route from origin to target, SHIELD will calculate a random number at each node and each pathway and sample from a distribution (in this case a uniform distribution based on the non-detection probability for that node or pathway) to determine if the adversary is detected along that node or pathway. The adversary then moves to the next node or pathway and this process is repeated until the adversary is either detected or reaches the target. For this simple network where time, distance, and indigenous detection are neglected, the adversary's expected total non-detection probability on any given route is equal to the product of the individual non-detection probabilities (which gives the probability that the adversary is not detected when traveling from the origin all the way to the target).

One potential route for the adversary is Node 1 to Node 3 to Node 5 to Target (the last route listed in Table 5). For this route, the non-detection probability for all nodes and all pathways is unity, therefore the expected success rate for this particular route is 100%.

The adversary might also take a route from Node 1 to Node 2 to Node 3 to Node 5 to Target. Pathway 1–2 has an MRD present. The non-detection probability for this pathway is 0.6733. All other nodes and pathways have a non-detection probability of unity. Again, SHIELD will calculate a random number and sample from a distribution for all nodes and all pathways, but on this route pathway 1–2 is the only pathway that matters for interdiction, and we would expect that across a large number of simulations the adversary will be interdicted 32.667% of the time and be successful 67.333% of the time. So the expected adversary success rate along this route is 67.33%.

Another potential route the adversary might takes if from Node 1 to Node 2 to Node 4 to the Target. Along this route there is an MRD present on pathway 1–2 and one on 2–4. Each of these pathways has a non-detection probability of 0.6733. The pathway from 4-T has a non-detection probability of unity. Thus, the non-detection probability for this route is the product of 0.6733 and 0.6733 and unity which is 45.33%.

If we similarly analyze the remaining routes for Fig. 1, then we will find the results shown in Table 5 for all of the six possible routes through the network.

SHIELD will rank order the linearized routes by the adversary's

Table 5
All potential routes for the simple network in Fig. 1 on page 4. Routes are notated by the nodes in the network, where T stands for Target.

Route	Expected Adversary Success Rate
1-2-4-T	45.33%
1-2-5-T	45.33%
1-2-3-5-T	67.33%
1-3-2-4-T	67.33%
1-3-2-5-T	67.33%
1-3-5-T	100.00%

perceived expected success rate. SHIELD will then aggregate the number of successes across all sampled routes to create the adversary's success rate across the complete network. SHIELD does not account for an adversary that moves backwards. Lateral movements which do not progress closer to target are possible but most be coded explicitly. Routes 1-2-3-5-T and 1-3-2-5-T are an example of such a lateral movement. These routes are identical mathematically, but they will be identified as independent routes. The number of routes which are sampled is determined by the user, with the default being 10. In the simple case provided, there are only six possible routes, so successes and failures will be aggregated for all routes. The adversary will not exhibit any preference or prioritization, because each route is perceived the same to the adversary. SHIELD will sample across all six of these routes, and aggregate the number of successes (and failures) to generate the adversary's success rate for the complete network. In this simple case, the aggregate is a simple average of the expected adversary success rate for each route and thus the expected success rate for the adversary across the complete network is 65.44%.

If this simple network included a route with an RPM which is apparent to the adversary, then the adversary will prioritize routes that circumvent the RPM. These routes are often culled. In the scenario where there are simply not enough perceived high-success routes to sample from, then SHIELD will sample from low probability routes as well.

References

[1] White House, National Strategy on Counterterrorism, 2011.

[2] IAEA, IAEA incident and traficking database (ITDB). https://www.iaea.org/resources/databases/itdb, 2017.

[3] K.R. Wood, Deterministic network interdiction, Math. Comput. Model. 17 (1993) 1–18.

[4] N. Dimitrov, D. Michalopoulos, D. Morton, M. Nehme, F. Pan, E. Popova, E. Schneider, G. Thoreson, Network deployment of radiation detectors with physics-based detection probability calculations, Ann. Oper. Res. 187 (2011) 207–228.

[5] J.Q. Cheng, M. Xie, R. Chen, F. Roberts, A latent source model to detect multiple spatial clusters with application in a mobile sensor network for surveillance of nuclear materials, J. Am. Stat. Assoc. 108 (2013) 902–913, https://doi.org/10.1080/01621459.2013.808945.

[6] E. Israeli, R.K. Wood, Shortest-path network interdiction, Networks. 40 (n.d.) 97–111. doi:10.1002/net.10039.

[7] DHS, CBP's Strategy to Address Illicit Cross-Border Tunnels, OIG, 2012, pp. 12–132.

[8] N. Haphuriwat, V.M. Bier, H.H. Willis, Deterring the smuggling of nuclear weapons in container freight through detection and retaliation, Decis. Anal. 8 (2011) 88–102, https://doi.org/10.1287/deca.1110.0199.

[9] IEEE, American National Standard Performance Criteria for Spectroscopy-Based Portal Monitors Used for Homeland Security, vols. 38–2015, 2016, pp. 1–45, https://doi.org/10.1109/IEEESTD.2016.7394937. ANSI N42.

[10] IEEE, American National Standard Performance Criteria for Handheld Instruments for the Detection and Identification of Radionuclides, ANSI N42.34-2015, 2016, pp. 1–60, https://doi.org/10.1109/IEEESTD.2016.7551091 (Revision ANSI N42.34-2006).

[11] DHS, United States Customs and Border Protection's Radiation Portal Monitors at Seaports, 2013.