Robust Dynamic Distribution of Security Assets in Transit Systems
ROBUST DYNAMIC DISTRIBUTION OF SECURITY ASSETS IN TRANSIT SYSTEMS

FINAL REPORT

DTRT07-G-0003

Prepared for

U.S. Department of Transportation
Research and Innovative Technology Administration

By

Principal Investigator
Dr. Elise Miller-Hooks

Faculty and Undergraduate Research Assistants
Dr. Rahul Nair
Jonathan Kumi
Kevin Denny

Department of Civil & Environmental Engineering
University of Maryland
College Park, MD 20742

July, 2012

UMD-2010-05

This work was sponsored by the U.S. Department of Transportation, Federal Highway Administration. The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of either the Federal Highway Administration or U.S. Department of Transportation at the time of publication. This report does not constitute a standard, specification, or regulation.
A robust, mixed-integer, multi-stage program is presented that seeks to effectively secure a transit system where risk is considered to be dynamic and varies over time. A time-varying risk measure reflects the unique nature of transit systems, where accumulation of passengers at transfer facilities, stations and transit vehicles is dynamic and increases the vulnerability of transit users and system to adverse events. The model is robust under uncertainty and better matches security assets at stations in the face of time-varying risk by redistributing them. The volume-dependent risk measure and subsequent deployment of security assets are developed for the transit system in Washington, D.C. demonstrating the variable nature of risk and response. The value of considering a robust solution is demonstrated by comparing the robust approach to an expected value approach. Five scenarios, designed on recent events on the system, replicate the operational conditions of the transit system for the morning rush hour period and show the effectiveness of the developed deployment strategies.
Contents

1 Executive Summary 2

2 Introduction 3

3 Model Formulation 6

4 Evolving Risk 11
  4.1 Illustrative Example ........................................ 12

5 Application to Washington, D.C. 14
  5.1 Risk Computation ............................................. 15
  5.2 Scenario Development ........................................ 16
  5.3 Robust Deployments .......................................... 17

6 Summary and Conclusions 17

7 Acknowledgments 20
1 Executive Summary

A robust, mixed-integer, multi-stage program is presented that seeks to effectively secure a transit system where risk is considered to be dynamic and varies over time. A time-varying risk measure reflects the unique nature of transit systems, where accumulation of passengers at transfer facilities, stations and transit vehicles is dynamic and increases the vulnerability of transit users and system to adverse events. The model is robust under uncertainty and better matches security assets at stations in the face of time-varying risk by redistributing them. The volume-dependent risk measure and subsequent deployment of security assets are developed for the transit system in Washington, D.C. demonstrating the variable nature of risk and response. The value of considering a robust solution is demonstrated by comparing the robust approach to an expected value approach. Five scenarios, designed on recent events on the system, replicate the operational conditions of the transit system for the morning rush hour period and show the effectiveness of the developed deployment strategies.
2 Introduction

Transit systems serve a key role in providing urban mobility. Through high occupancy and throughput, transit is a sustainable and efficient mode of travel. However, the compact congregation of people at stations, transfer facilities, and transit vehicles offers an attractive target for terrorist attack. Over the past 10 years alone, attacks on public transit systems have occurred in Moscow, Madrid, London, and India, causing significant loss of life and material damage. Overall, between 1901 and 2002, the surface transportation system was involved in 25% of terrorist attacks (Balog et al., 2005). A key challenge for transit operators is to maintain a secure transit system. Security needs, however, need to be balanced with mobility requirements of the traveling public. By their nature, transit systems are open and allow for free movement of large volumes of people. Security protocols that seek to screen every passenger or monitor every point of entry are expensive and, from the perspective of users, onerous. Faced with fewer resources, transit operators need to target their security assets to specific facilities where their presence can make the greatest impact.

Security assets can be fixed (monitoring equipment like CCTVs, alarm systems, physical barriers) or mobile (security personnel, first responders, and monitors). To better understand the impact of operator decisions on security and evaluate competing deployment plans of security assets, a quantitative risk assessment framework is needed. Several definitions of risk on transportation networks have been proposed in the literature. These measures can be either qualitative or quantitative and aim to capture the likelihood of adverse events and their consequences (Murray-Tuite and Fei, 2010; Kaplan and Garrick, 1981). The consequences can be quantified by fatalities, economic impacts of events, loss of service, and service quality.

Among qualitative methods, Haimes et al. (2002) assess risk through a framework that seeks to identify, prioritize, and assess risk scenarios for large scale systems. Their method, termed risk filtering, ranking and management (RFRM), builds a hierarchical holistic model to first identify risk, then filters the sources of risk that are critical. A scenario-based likelihood is used to evaluate risk mitigation actions. Luyten and Barr (2011) study risk assessment on bus and subway networks. They provide a matrix of threats and targets along with
associated probabilities. Their systematic, step-by-step approach is aimed at transit operators and provides a clear and concise manner to determine mitigation strategies. Abkowitz (2002) introduces a paradigm for transportation risk management that actively considers the consequences of a broad set of human-made and natural incidents. The author evaluates consequences by taking into account contingent and societal effects. Risks are prioritized by identification of critical facilities, performing risk assessments, formulating control strategies, and monitoring performance.

Several quantitative risk metrics have been proposed in the literature. While details of these metrics are presented elsewhere for specific domains (for example see Erkut et al., 2007, for applications in hazardous materials), two studies that form the basis for the work in this paper are highlighted. Xia et al. (2005) develop a risk metric for road networks that considers static and dynamic factors. Static risk components remain unchanged over long periods of time. Dynamic factors, including flow, speed, vehicles, weather, and accident rates, vary over time and are also considered in the overall risk measure. The methods to combine these disparate criteria and adjust their respective weights can be adjusted to reflect the type of network being studied. French and O’Mahony (2008) extend the concept of static and dynamic factors to evaluate the risk of attacks on bus networks in Dublin, Ireland. The static and dynamic factors are normalized and weighted using the analytic hierarchy process. Pairs of factors, both static and dynamic, are compared so that their relative importance can be calculated. A value is assigned to describe the relationship between the factors. They demonstrate their risk assessment on five scenarios and show that higher risk scores are associated with rush hours and high volume passenger movement. During off-peak hours, static factors such as attractiveness of targets, conditions, and frequency are most critical.

Both qualitative and quantitative risk measures inform decisions made by transit operators. Different options within the operators’ security toolkit can be examined to determine good security strategies. These options can be strategic in nature, such as blast hardening of critical assets, policies to restrict access to key service cores and facilities, installation of monitoring equipment, and modifying passenger movement patterns within transit facilities.
Operational strategies, such as real-time monitoring of CCTVs and deployment of security assets that are implemented on a day-to-day basis, can also be developed. Several agencies also deploy teams to conduct randomized checks across the network. The variability and visibility of such strategies serve as a deterrent. The focus of this work is on deployment strategies for mobile security assets. Such strategies can be developed using risk-coverage based optimization models as proposed herein.

Several works have considered optimization models that seek to maximize coverage of risk for the protection of critical facilities. These models have been applied in several application domains, including hazmat transport, the location and relocation of emergency medical service (EMS) vehicles, and mobile service facilities. Models dealing with asset relocation deployment in dynamic models are addressed in (Berman and LeBlanc, 1984; Daskin and Dean, 2005), where a Markov Decision Process is used to address the desirability of repositioning facilities on a network. Relocation of EMS vehicles is considered in several works (Brotcorne et al., 2003; Rajagopalan et al., 2008; Gendreau et al., 2005), where the aim is to provide a faster response to anticipated calls. Previous work by the authors studied the location and relocation of assets to guard critical facilities (Sathe and Miller-Hooks, 2005), and evaluated the benefit of relocation using EMS data from Montreal (Nair and Miller-Hooks, 2009). There is considerable literature on the role of uncertainty in asset location models (see Snyder, 2006, for a comprehensive review). Several methods have been presented to generate robust strategies in the face of uncertainty. Snyder and Daskin (2006) developed the concept of $p$-robustness, where the robust solution is within a certain fraction of the optimal solution for each and every possible scenario, where scenarios are a sample of discrete realizations that describe all potential future states. Since risk across the transit system cannot be determined exactly, the uncertainty in the risk measure is captured using the $p$-robustness measure.

The main contributions of this paper are the following. A dynamic, volume-dependent, time-varying risk measure, adapted from French and O’Mahony (2008), that accounts for the unique characteristics of urban transit systems is developed. A mixed-integer, multi-period, stochastic model for the robust deployment of security assets is developed that aims
to maximize coverage of risk across the system. The deployment strategy calls for security assets to be relocated over time to respond to changes in risk. This dynamic distribution of security assets aims to provide better security outcomes by better matching security coverage to evolving risk. The volume-dependent risk measure and subsequent deployment of security assets are generated for the transit system in Washington, D.C. demonstrating the variable nature of risk and response. The value of considering a robust solution is demonstrated. Five scenarios, designed on recent events on the system, replicate the operational conditions of the transit system for the morning rush hour period and show the effectiveness of the developed deployment strategies.

The next section presents the robust optimization model and framework. Section 4 presents the notion of evolving risk and the need for a robust deployment through an illustrative example. Finally, the model is applied to Washington, D.C.

3 Model Formulation

Given (a) the existing transit network with travel times and network structure, (b) a probabilistic, time-varying risk estimate for all transit facilities, and (c) the number of security assets available and their characteristics, we seek to find a deployment strategy that maximizes the risk coverage and maintains coverage over all realizations of risk.

The optimal deployment provides a better match between available security assets and changing risk profiles in the network. However, operators only know the risk at each facility in a probabilistic sense. The optimal deployment must therefore be robust to uncertainty in the risk measure. One method, amongst several, is to account for uncertainty using $p$-robustness (Snyder and Daskin, 2006). The main idea is to bound the worst-case coverage resulting from the deployment over all possible realizations of risk. All possible realizations are depicted in a finite set of scenarios over which the deployment decisions are optimized. The notion of $p$-robustness relates the optimal decisions for the individual scenarios to the optimal decision for all scenarios combined. It does so by restricting the ratio of coverage resulting from the joint decision to the individual decisions to a fraction $p$. Effectively, this
ensures that the deployment decision performs at acceptable levels for all scenarios.

There are two types of deployment decisions that transit operators can pursue to maximize the utility of their security assets. The first decision is to locate security teams at facilities, such as transit stops, transfer facilities, and transit vehicles. Since the risk is assumed to change over time, the security assets can be mobilized to change locations in response to the new risk states. This redistribution forms the second type of deployment decision. Through the location and redistribution of security assets, the transit operator aims to manage the system-wide covered risk.

The deployment problem is defined on a network \( G = (V, A) \), where \( V \) is the set of facilities in the transit network that need to be covered and is indexed by \( i \) or \( j \). The set \( A \) represents the physical connections between the facilities. The problem is defined for a set of discrete time periods \( T \) indexed by \( t \). Let \( t_n \) denote the last time period. Risk at facility \( i \) during time period \( t \) is denoted by \( \vartheta_{it} \) which is a random variable. The realizations of risk are assumed to be discrete and referred to as a scenario, indexed by \( s \). The set of scenarios \( S \) reflects all potential realizations of risk for the entire network. While the risk is associated with different assets at nodes (e.g., stations) and mobile assets, such as vehicles, in this paper risk is considered explicitly at nodes. Each scenario is assumed to be realized with a probability \( q_s \). The risk measure for a particular scenario \( s \) at node \( i \) and period \( t \) is denoted by \( \theta_{its} \), which is not random.

The operator is limited to \( k \) security assets that need to be located on the network. The cost of relocating one asset from node \( i \) to node \( j \) is a linear function of the distance between the two nodes \( d_{ij} \). Let \( \delta \) be a small penalty incurred by the operator to limit relocation of security assets. The model needs additional parameters to represent the notion of coverage and limit the mobility of security teams within the network from one period to the next. If an asset is within \( c_1 \) distance of a security asset, it is considered to be covered. Denote \( c_2 \) as the maximum distance that a security asset can relocate in one time period. Define two binary indicator parameters, \( \gamma_{ij} \) and \( \beta_{ij} \), as
Three sets of binary decision variables define the operator actions. Two sets of deployment actions are independent of risk realizations, while the third depends on the individual scenarios. Let \( y_{it} \) denote a binary decision variable that indicates when a security asset is located at facility \( i \) during time period \( t \). Let \( w_{ijt} \) denote a binary decision variable indicating if a security asset is relocated from facility \( i \) to \( j \) in preparation for time period \( t \). Based on these deployment decisions, the coverage variables \( x_{its} \) are binary variables indicating if facility \( i \) is covered during scenario \( s \) during time period \( t \). In addition to the operator decision variable, a slack variable \( \xi_s \) is employed to ensure that the robustness measure constrained in the deployment problem formulation can be relaxed but only by incurring a large penalty \( \Delta \).

To generate a robust deployment under a wide range of scenarios, the optimal decisions are constrained such that the performance under any single scenario is bounded. This bound is defined to be relative to the optimal strategy had the operator planned for a particular scenario. Denote \( z^*_s \) to be the optimal coverage for scenario \( s \). This is the coverage if the operator were to plan only for scenario \( s \). Given a value of \( p_s \), the robust coverage is constrained to be within \( p_s z^*_s \) over the set of scenarios \( S \). The solution is therefore referred to as \( p \)-robust (Snyder and Daskin, 2006). The value of \( p_s \) is scenario specific and can be adjusted to reflect low-probability scenarios. Alternatively, a general value \( p \) can be used for all scenarios, in which case the robust deployment is more sensitive to extreme events.

With these definitions, the Robust Asset Deployment problem (RAD-\( p \)) can be defined for a value of \( p \) as follows.

\[
\max \sum_{s \in S} \sum_{t \in T} \sum_{i \in V} q_s \theta_{its} x_{its} - \sum_{t \in T} \sum_{i \in V} \sum_{j \in V} \delta d_{ij} w_{ijt} - \sum_{s \in S} \Delta \xi_s
\]
subject to

\[ \sum_{i \in T} \sum_{i \in V} \theta_{its} x_{its} - \xi_s \geq p_s z^*_s \quad \forall s \in S \] (3)

\[ \sum_{i \in V} y_{it} \leq k \quad \forall t \in T \] (4)

\[ \sum_{j \in V} \gamma_{ij} y_{it} \geq x_{its} \quad \forall i \in V, t \in T, s \in S \] (5)

\[ \sum_{j \in V} w_{ijt} \leq y_{it+1} \quad \forall i \in V, t \in T \setminus t_n \] (6)

\[ \sum_{i \in V} w_{ijt} \geq y_{jt} \quad \forall j \in V, t \in T \] (7)

\[ w_{ijt} \leq \beta_{ij} \quad \forall i, j \in V, t \in T \] (8)

\[ x_{its}, y_{it}, w_{ijt} \in \{0, 1\} \quad \forall i, j \in V, t \in T, s \in S \] (9)

\[ \xi_s \in \mathbb{R}_+ \quad \forall s \in S \] (10)

The first term of the objective (2) maximizes the covered risk over the system for all scenarios, while the second imposes a small penalty on relocation to minimize excessive relocation of assets. The third term in the objective is a large penalty for using slack variables that relax the robustness constraint. Constraints (3) ensure that the coverage for each scenario is within \( p_s \) fraction of the optimal coverage for that scenario \( z^*_s \). If this is not feasible, the slack variable has a non-negative value to make the constraint feasible. In this case, the resulting solution is no longer \( p \)-robust, but has a lower effective \( p \). This is described in greater detail below. Constraints (4) limit the number of assets deployed on the network to the ones available. Constraints (5) relate coverage variables in each scenario to the location variables. Constraints (6) state that an asset cannot be located at a particular node if it did not relocate there. Constraints (7) limits the relocations from a node to facilities with assets. Constraints (8) restrict relocation variables such that all relocations between two time periods are feasible, i.e. within \( c_2 \) time units. Constraints (9) limit the decision variables to be binary integer and constraints (10) limit the slack variable to be non-negative.

The above model is parameterized in \( p_s \) which ensures a minimum coverage is met for all
scenarios. The value of $z^*_s$ represents the optimal coverage for a particular scenario and is defined as

$$z^*_s = \sum_{i \in V} \sum_{t \in T} \theta_{its} x^*_{it},$$

(11)

where $x^*_{it}$ is the optimal coverage vector determined from solving the following program.

$$\max \sum_{t \in T} \sum_{i \in V} \theta_{its} x_{it} - \sum_{t \in T} \sum_{i \in V} \sum_{j \in V} \delta d_{ij} w_{ijt}$$

subject to

Eqns. (4), (6), (7), (8), and,

$$\sum_{j \in V} \gamma_{ij} y_{it} \geq x_{it} \quad \forall i \in V, t \in T$$

(13)

$$x_{it}, y_{it}, w_{ijt} \in \{0, 1\} \quad \forall i, j \in V, t \in T$$

(14)

This model is a scenario-specific variant of RAD-p, where the objective is to maximize coverage while reducing relocation penalties for a specific scenario. This program needs to be solved for each scenario to generate values of $z^*_s$ for all $s$. When the number of scenarios is large, solving RAD-p can become problematic. To reduce the size of the program, scenarios can be sampled to provide a representative set that would yield sufficient robustness in the deployment decisions.

If extreme scenarios are included in set $S$, the model RAD-p can no longer achieve $p$-robustness for any deployment decisions that the operator can implement. In this case, the model uses the set of slack variables $\xi_s$ to relax the robustness constraint. This mechanism results in partial robustness, where deployment decisions are unlikely to satisfy particular scenarios within the specified bound. In order to evaluate the efficacy of the implemented solution, the ‘true’ robustness measure can be evaluated as follows. If $x^*_{its}$ and $\xi^*_s$ are optimal solutions to RAD-p, the effective robustness value is
\[ \hat{p} = \frac{q_s}{z_s^*} \sum_{s \in S} \sum_{i \in V} \theta_{its} x_{its} - \xi_s^* \] (15)

where \( q_s \) is the probability of realizing scenario \( s \).

To quantify the benefits of accounting for the distribution of risk, a variant of the model that disregards the distributional information is constructed. The Expected Value (EV) model constructs deployment decisions based on the expected value of risk. The EV solution can be generated by solving the following program.

\[
\max \sum_{t \in T} \sum_{i \in V} E[\vartheta_{it}] x_{it} - \sum_{t \in T} \sum_{i \in V} \sum_{j \in V} \delta d_{ij} w_{ijt} 
\] (16)

subject to

Eqns. (4), (6), (7), (8), (13), (14).

The models RAD-p and EV were solved using CPLEX and results for a real-world network in Washington, D.C. are presented in Section 5. The next section presents the concept of evolving risk in transit systems and how it can be computed for real-world systems.

4 Evolving Risk

Following the risk assessment framework proposed by French and O'Mahony (2008), various factors are assumed to contribute to the overall risk of a facility. These can be classified as static and dynamic and total risk is assumed to be additive.

\[ \text{Risk} = \text{static factors} + \text{dynamic factors.} \] (17)

Static factors account for inherent qualities of transit facilities that do not change over time. This measure can include variables for type of facility and its importance, the symbolic nature of the facility and its surroundings, the level of service offered by the facility through proxies such as the number of feeder bus routes, existing number of service lines, and auxiliary services. Dynamic factors can include time-varying passenger flows through stations, service
frequency, passenger transfer volumes at transfer facilities, estimates of number of passengers waiting at a station, and maximum throughput of the station. Several transit systems track users for fare-collection. This can serve as a data source for some of the dynamic metrics or real-time operations. Other monitoring equipment, such as CCTV and dispatch communications, can be used to augment data on the users in the system. The overall metric is a weighted combination of various sources of risk. The risk at facility $i$ during time $t$ can therefore be expressed as

$$\vartheta_{it} = \alpha \left( \sum_l w_l a_l \right) + (1 - \alpha) \left( \sum_m w_m a_m \right),$$

where $w_l$ and $w_m$ are weights for individual static and dynamic factors, respectively, and $a_l$ and $a_m$ are the risk metrics for each risk component. The risk metrics can be normalized.

While several of the component measures can be determined precisely through data, the overall risk measure is uncertain, since the analyst cannot account for all sources of risk and some components may be only known probabilistically. For example, dynamic factors that are dependent on passenger volumes may rely on an estimate of the mean and variance which may be imprecise. The actual risk itself is uncertain. The evolving risk is viewed as a distribution that evolves over time. Assumptions on the nature of the distribution can be made to account for the uncertainty of $\vartheta_{it}$.

### 4.1 Illustrative Example

An example to demonstrate key concepts of evolving risk and the nature of the robust solution is presented. Consider the 4-node network with 2 time periods and two risk scenarios shown in Figure 1. Scenario 1, is a low-probability realization with 0.1 probability of occurring, and Scenario 2 occurs with a probability of 0.9. The risk measures are summarized in Table 1.

Assume the coverage distance $c_1 = 0$, which implies that only nodes that have security assets are covered. Deploying two security assets on this 4-node network can be done in several ways. If risk realizations were known in advance, the operator can optimize the deployment based on the realization. This yields the value of $z^*_s$, the optimal coverage under individual
Figure 1: Risk profiles for two scenarios and two time periods

(a) Scenario 1, $t = 1$  (b) Scenario 1, $t = 2$  (c) Scenario 2, $t = 1$  (d) Scenario 2, $t = 2$

Table 1: Summary of risk metrics

<table>
<thead>
<tr>
<th>Node</th>
<th>Scenarios</th>
<th>EV $0.1s_1 + 0.9s_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$s = 1$</td>
<td>$s = 2$</td>
</tr>
<tr>
<td></td>
<td>$t = 1$</td>
<td>$t = 2$</td>
</tr>
<tr>
<td>1</td>
<td>0.4</td>
<td>0.1</td>
</tr>
<tr>
<td>2</td>
<td>0.2</td>
<td>0.8</td>
</tr>
<tr>
<td>3</td>
<td>0.2</td>
<td>0.1</td>
</tr>
<tr>
<td>4</td>
<td>0.5</td>
<td>0.9</td>
</tr>
</tbody>
</table>

Figure 2: Optimal deployment under individual scenarios

(a) $s = 1, z^*_1 = 0.9 + 1.7 = 2.6$  (b) $s = 2, z^*_2 = 0.7 + 0.6 = 1.3$

However, the operator cannot pursue both deployment strategies and must determine an appropriate tradeoff between robustness and good performance for the average case. The average case is determined by the EV model based on the expected values. Figure 3(a) shows the deployment based on expected values. When the strategy is determined using the average case, the coverage works well for some scenarios (in this case Scenario 2), but not for others (Scenario 1). To observe this, compute the coverage resulting from the EV model, had scenario 1 been realized. The coverage for time period 1 is 0.4 (risk covered at nodes 2 and 3) and for time period 2 is 0.9 (risk covered at nodes 1 and 2). Therefore, the total coverage for
the expected value approach would be \( z_{EV} = 1.3 \) had scenario 1 been realized. In contrast, consider the robust solution in Figure 3(b). If Scenario 1 is realized, the coverage for time period 1 is 0.7 and for time period 2 is 1.7, so the total coverage for both time periods is 2.4, which is closer to the optimal value \( z_1^* = 2.6 \). The trade-off is a minor degradation in coverage should the scenario 2 be realized. In this case, the coverage is 0.6 for time period 1, and 0.5 for time period 2 resulting in a coverage of 1.1, which is below the optimal solution of 1.3 for the expected value model had scenario 2 been realized.

![Deployment based on EV and RAD-p models](image)

Figure 3: Optimal deployment for EV and RAD-p models

The example illustrates the value of pursuing a robust strategy. When there is significant uncertainty in the input risk measures, robust strategies perform more consistently and are likely to significantly outperform strategies based on average risk measures for some scenarios. However, robust strategies may marginally under-perform for some scenarios. The value of providing consistent coverage in the face of uncertainty should outweigh the cost of lower coverage for some scenarios.

5 Application to Washington, D.C.

The transit system in Washington, D.C. includes rail and bus systems operated by the Washington Metropolitan Area Transit Authority (WMATA). The focus of this case study is on the rail system that is comprised of five service lines with 86 stations. Of these 86 stations, 5 serve as transfer stations between rail lines. The rail system carries roughly 800,000 people on a typical weekday. In recent years, the system has been prone to severe events, both human-made and natural, that have severely impacted performance. These adverse events include earthquakes, flooding, equipment failures leading to delays, and construction delays.
A scenario-based analysis of these events is conducted. Based on studies by the Washington Metropolitan Area Transit Authority (WMATA), data on passenger volumes, bus routes, and transfer volumes were utilized to compute the risk measures outlined earlier. The RAD-$p$ and EV models were run to establish optimal coverage of transit assets in the system.

### 5.1 Risk Computation

The static and dynamic risk components were calculated based on data available for the system on daily boardings (WMATA, 2011), transfer volumes observed, peak half-hour loading, and station access modes (P2D, 2008; WMATA, 2008). Additionally, the bus system, that serves as a feeder system to rail, was analyzed to determine the combined peak-hour frequency and the number of bus routes that serve each station. This was done by parsing the schedule information from WMATA. Each station was also assigned a symbolic score representing its visibility, importance, and proximity to sensitive areas. The symbolic score was between 1 and 5 with 5 indicating greatest sensitivity. Dynamic factors are harder to compute due to lack of operational data (for example the SmartTrip fare cards used in the system were not readily available for this study). To overcome this, the dynamic factors were sampled from the peak half-hour passenger volumes and perturbed to incorporate variability as it exists on real systems. Table 2 summarizes the parameters used to compute risk factors.

Once data for each station on the system was collected, each risk component was normalized and added. The contribution of dynamic factors $1 - \alpha$ was considered to be 0.3 to emphasize the effects of the dynamic characteristics on the results. Four time periods of half an hour each from 8am to 10am were considered. As an alternative, the static risk values

<table>
<thead>
<tr>
<th>Factor</th>
<th>Source</th>
<th>Category</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symbolic score</td>
<td>Assigned</td>
<td>Static</td>
<td>Between 1 (lowest) to 5 (highest)</td>
</tr>
<tr>
<td>Rail frequency</td>
<td>Schedule</td>
<td>Static</td>
<td>Trains/hour</td>
</tr>
<tr>
<td>Line ridership</td>
<td>WMATA</td>
<td>Static</td>
<td>Passengers/line</td>
</tr>
<tr>
<td>Bus service</td>
<td>Schedule</td>
<td>Static</td>
<td>Number of routes/ peak hour</td>
</tr>
<tr>
<td>Transfer volume</td>
<td>Sampled</td>
<td>Dynamic</td>
<td>Passengers/hour</td>
</tr>
<tr>
<td>Passengers</td>
<td>Sampled</td>
<td>Dynamic</td>
<td>Passengers/half hour</td>
</tr>
</tbody>
</table>

Table 2: Summary of risk factors computed
can come from the risk assessment process that transit agencies are likely to have and the dynamic values for real-time operational data, such as data generated from automatic fare card readers.

5.2 Scenario Development

Five scenarios were generated based on recent events on the transit system. These are graphically summarized in Figure 4. Scenario 1 shows a typical weekday morning commute from 8-10 am in four time periods, with the highest dynamic risk values typically moving from outlying suburban stations to centrally located transfer points. This scenario serves as a base-case. Scenario 2 involves minor delays on the Red Line westbound in the center of the city, and all nodes upstream of the delay show a spike in dynamic risk values. Scenario 3 represents significant delays on the Red Line, and subsequent increases in dynamic risk effect the entire line. Scenario 4 focuses on an event causing significant disruption in the Yellow Line, causing diversion of passengers to alternate lines, and a subsequent increase in dynamic risk effect on other lines that are used as alternatives, particularly at transfer stations on these lines. Scenario 5 models the recent 2011 earthquake in the DC region, causing all trains to run at 15 mph, causing delays along all lines and increase in dynamic risks. Scenario 5 is considered a low probability event.

For each numerical experiment, 300 instances were sampled from one of these of five scenario sets shown above. Several runs were conducted where parameters were varied including the number of security assets to locate $k$ (5, 10 and 15), the robustness parameter $p$ (0.6, 0.7, 0.8, 0.9 and 1.0), and the coverage distance $c_1$ (0 and 300).
5.3 Robust Deployments

Table 3 summarizes the results from the numerical experiments. The primary measure of effectiveness to demonstrate the performance of the models is the expected covered risk. As shown in Table 3 the risk covered for the Expected Value model \( z_{EV} \) is marginally better in all cases, since it represents the average over all scenarios. However, the purpose of having a robust strategy is to have acceptable coverage for all scenarios. This can be seen by looking at the coverage had a particular scenario been realized. Figure 6 shows the difference of risk measure of expected value and robust models for selected runs. The curves, shown as a cumulative distribution function, show how robust location/relocation outperforms the EV model in extreme scenarios. While the EV model does well marginally in several instances, the magnitude of the improvement for the robust model is greater in these cases.

The start robustness parameter \( p \) impacts the strategy recommended by the program. At low values of \( p \) the system is not constrained therefore providing a closer deployment plan to the expected value (note that in the limiting case when \( p = 0.0 \), the robust model is analogous to the EV model). For higher values of \( p \), the assets are deployed in a manner to weather all scenarios jointly. The effective robustness achieved, \( \hat{p} \), is consequently lower, since the slack variables are employed to meet the robustness constraint.

Figure 6 shows the locations for different time periods studied for a selected scenario. Since two of the scenarios included in the numerical experiments had Red Line delays, several assets are located along this corridor. In the robust variants, the security assets will move from outer suburban areas towards the downtown areas of the network, where passenger volumes are larger. The expected value approach, in contrast, has limited movement to match the passenger volume changes. Figures 7 and 8 show results for 15 assets.

6 Summary and Conclusions

A robust dynamic model of distributing mobile security assets on a transit system is presented. The model is robust in that the risk coverage objectives are bounded for all scenarios. The resulting deployments ensure that operator decisions made based on current conditions provide
<table>
<thead>
<tr>
<th># Assets</th>
<th>( r_1^a )</th>
<th>( p^b )</th>
<th>( z_{EV}^c )</th>
<th>( z_{RB}^d )</th>
<th>( \tilde{p}^e )</th>
<th>EV time(^f)</th>
<th>( z^* ) time(^g)</th>
<th>RB time(^h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0</td>
<td>0.6</td>
<td>606.95</td>
<td>606.95</td>
<td>0.780</td>
<td>0.362</td>
<td>118.749</td>
<td>4.492</td>
</tr>
<tr>
<td></td>
<td>0.7</td>
<td>580.50</td>
<td>580.50</td>
<td>0.688</td>
<td>0.306</td>
<td>118.774</td>
<td>4.158</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.8</td>
<td>563.51</td>
<td>562.10</td>
<td>0.583</td>
<td>0.305</td>
<td>118.828</td>
<td>4.147</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.9</td>
<td>595.36</td>
<td>595.29</td>
<td>0.494</td>
<td>0.813</td>
<td>120.224</td>
<td>4.167</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>603.29</td>
<td>601.58</td>
<td>0.399</td>
<td>0.595</td>
<td>118.591</td>
<td>4.108</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>0.6</td>
<td>1044.06</td>
<td>1036.32</td>
<td>0.907</td>
<td>0.307</td>
<td>119.239</td>
<td>178.440</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.7</td>
<td>1039.19</td>
<td>1037.60</td>
<td>0.883</td>
<td>0.574</td>
<td>115.074</td>
<td>134.194</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.8</td>
<td>1047.26</td>
<td>1044.04</td>
<td>0.789</td>
<td>0.567</td>
<td>115.242</td>
<td>91.619</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.9</td>
<td>1050.10</td>
<td>1046.37</td>
<td>0.693</td>
<td>0.810</td>
<td>116.941</td>
<td>80.629</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1030.91</td>
<td>1025.72</td>
<td>0.585</td>
<td>0.804</td>
<td>115.484</td>
<td>76.959</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0.6</td>
<td>801.85</td>
<td>799.35</td>
<td>0.783</td>
<td>0.854</td>
<td>121.758</td>
<td>6.032</td>
</tr>
<tr>
<td></td>
<td>0.7</td>
<td>784.36</td>
<td>782.92</td>
<td>0.715</td>
<td>0.722</td>
<td>120.934</td>
<td>4.763</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.8</td>
<td>784.83</td>
<td>780.72</td>
<td>0.608</td>
<td>0.598</td>
<td>122.429</td>
<td>4.731</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.9</td>
<td>794.26</td>
<td>791.55</td>
<td>0.521</td>
<td>0.606</td>
<td>121.634</td>
<td>5.618</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>777.83</td>
<td>776.82</td>
<td>0.422</td>
<td>0.529</td>
<td>121.092</td>
<td>5.110</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>0.6</td>
<td>1290.10</td>
<td>1282.45</td>
<td>0.935</td>
<td>0.615</td>
<td>130.235</td>
<td>70.908</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.7</td>
<td>1292.18</td>
<td>1290.64</td>
<td>0.908</td>
<td>0.575</td>
<td>129.726</td>
<td>89.709</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.8</td>
<td>1283.95</td>
<td>1280.15</td>
<td>0.823</td>
<td>0.520</td>
<td>130.571</td>
<td>113.723</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.9</td>
<td>1271.41</td>
<td>1266.90</td>
<td>0.715</td>
<td>0.573</td>
<td>129.139</td>
<td>87.331</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1306.56</td>
<td>1302.79</td>
<td>0.627</td>
<td>0.586</td>
<td>128.377</td>
<td>84.998</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0.6</td>
<td>902.40</td>
<td>898.14</td>
<td>0.782</td>
<td>0.843</td>
<td>123.899</td>
<td>5.924</td>
</tr>
<tr>
<td></td>
<td>0.7</td>
<td>905.68</td>
<td>904.25</td>
<td>0.743</td>
<td>0.606</td>
<td>123.913</td>
<td>5.660</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.8</td>
<td>923.46</td>
<td>923.29</td>
<td>0.642</td>
<td>0.548</td>
<td>123.031</td>
<td>4.871</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.9</td>
<td>970.72</td>
<td>970.51</td>
<td>0.561</td>
<td>0.612</td>
<td>124.085</td>
<td>6.059</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>913.50</td>
<td>911.88</td>
<td>0.439</td>
<td>0.656</td>
<td>125.495</td>
<td>5.275</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>0.6</td>
<td>1392.56</td>
<td>1385.82</td>
<td>0.950</td>
<td>1.198</td>
<td>142.251</td>
<td>228.573</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.7</td>
<td>1381.06</td>
<td>1380.86</td>
<td>0.932</td>
<td>1.118</td>
<td>140.803</td>
<td>230.398</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.8</td>
<td>1374.41</td>
<td>1371.10</td>
<td>0.833</td>
<td>1.525</td>
<td>139.576</td>
<td>213.148</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.9</td>
<td>1406.31</td>
<td>1399.96</td>
<td>0.729</td>
<td>1.127</td>
<td>141.749</td>
<td>99.351</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1385.53</td>
<td>1380.36</td>
<td>0.637</td>
<td>1.587</td>
<td>145.553</td>
<td>77.170</td>
<td></td>
</tr>
</tbody>
</table>

\( a \) - Coverage radius  
\( b \) - Robustness bound  
\( c \) - Risk covered under Expected Value model  
\( d \) - Expected risk covered under Robust model  
\( e \) - Achieved robustness bound  
\( f \) - Solution time in seconds for EV model  
\( g \) - Solution time in seconds to compute \( z^* \)  
\( h \) - Solution time in seconds to solve Robust model

Table 3: Summary of results
acceptable outcomes regardless of what scenario is realized. The model is tested using real data from the Washington, D.C. transit system where static and dynamic risk metrics were computed. Based on recent events on the system, five scenarios were developed. Numerical experiments show that while deployment decisions based on average values of risk appear to perform well, in terms of expected risk coverage, they are not well-suited should some extreme scenarios arise. The robust deployment strategies are shown to provide greater coverage in these cases. As further work, dynamic factors that contribute to risk can include the real-time system status, such as infrastructure outage, service levels, and events. The deployment model can be made adaptive to these changes.
Figure 6: Comparison of EV and Robust locations with 10 assets and $c_1 = 300$

7 Acknowledgments

This research was funded through the Mid-Atlantic University Transportation Center (MAUTC), a U.S. Department of Transportation Center, and the National Science Foundation through participation of undergraduate students, Jonathan Kumi and Kevin Denny, on an REU supplement. This support is gratefully acknowledged, but implies no endorsement of its findings.
Figure 7: Comparison of EV and Robust models with 15 assets and $r_1 = 300$
Figure 8: Comparison of EV and Robust locations with 15 assets and $c_1 = 300$
References


URL http://wmata.com/about_metro/planning_dev.cfm


URL http://wmata.com/about_metro/planning_dev.cfm


URL http://wmata.com/about_metro/planning_dev.cfm