Defending Transportation Networks Against Random and Targeted Attacks

Yingyan Lou and Lihui Zhang

This paper explores several reliability and vulnerability measures for transportation networks and proposes three models for optimal resource allocation for transportation network design or defense to minimize the disruption caused by both random and targeted attacks. The common day-to-day disturbances with less severe consequences are referred to as random attacks, but targeted attacks include both coordinated terrorist strikes and large-scale natural disasters. For random attacks, the major concern would be the reliability of the total system travel time. A robust discrete network design problem is formulated to take into account random attacks in the planning stage. The transport capacity or the unsatisfied demand would be critical in case of emergency evacuation, and law enforcement forces could be deployed to prevent malicious attacks in the first place or to ensure a smooth evacuation operation. The proposed models feature an intrinsic trilevel game structure of the network users, the attacker, and the defender (planner). By exploring the unique properties of the proposed measures and reformulating the problems, the trilevel structure models are reduced to mixed-integer semi-infinite optimization programs. This paper further applies an active-set algorithm, combined with a cutting-plane scheme to solve the proposed models. Numerical examples indicate that the proposed formulations are valid and that the solution algorithm can solve the problems effectively and efficiently. The models for targeted attacks provide practical implications on identifying critical infrastructures for evacuation.

Transportation has been identified as one of 17 critical infrastructure sectors in the national strategy for homeland security (*1*). Transportation systems are vulnerable not only to planned attacks, but also to natural disasters and random disturbances. More than 1,000 catalogued terrorist attacks and acts of violence worldwide that involved surface transportation have occurred in the past 100 years (*2*). For example, the public transportation systems in Madrid, Spain (March 2004), London (July 2005), and Mumbai, India (July 2006), were effectively crippled by a series of targeted attacks. Transportation network operations also face numerous natural sources of disruptions, such as earthquakes, hurricanes, adverse weather, traffic accidents, vehicle breakdowns, signal failures, and roadwork. The scales, impacts, frequencies, and predictability of these attacks vary significantly. The eruption of a volcano in Iceland in April 2010 caused a massive shutdown of air traffic, whereas daily traffic disruptions cause less earth-shattering but chronic pains, such as congestion.

Y. Lou, Department of Civil, Construction, and Environmental Engineering, University of Alabama, A127K Bevill Building, Box 870205, Tuscaloosa, AL 35487. L. Zhang, School of Transportation and Logistics, Dalian University of Technology, Dalian 116024, China. Corresponding author: Y. Lou, ylou@eng.ua.edu.

Transportation Research Record: Journal of the Transportation Research Board, No. 2234, Transportation Research Board of the National Academies, Washington, D.C., 2011, pp. 31–40.
DOI: 10.3141/2234-04

How to maintain or improve the ability of transportation systems to handle day-to-day, small-scale disturbances and at the same time, protect the systems from natural disasters and targeted attacks, remains a challenge. Although little can be done about their scales, frequencies, or predictability, particularly for natural disasters, it is possible to allocate resources in advance to design or defend transportation networks to minimize the negative effects that such attacks may cause.

In view of the distinct nature of these two groups of disruptive events, the corresponding criteria for assessing vulnerability as well as the countermeasures for minimizing their consequences should be different. For small-scale disruptions, which are called "random attacks" in this article, the connectivity of a transportation network often remains intact, and the major concern would be the reliability of the total system travel time. This reliability issue can be incorporated into the network planning stage by allocating more capacity to accommodate a possible reduction of system performance caused by random attacks.

The transport capacity, or the unsatisfied demand, would be critical in case of an emergency evacuation, because of both malicious attacks and large-scale natural disasters, in which part of the network may be destroyed and connectivity may be lost. Such large-scale disruptive events are referred to as "targeted attacks" in this article. One possible countermeasure is deployment of law enforcement forces to prevent malicious attacks in the first place or to ensure a smooth evacuation operation.

On the basis of these considerations, the study described here investigates different reliability and vulnerability measures for random and targeted attacks and develops several optimization models that may serve as guidance to resource allocation in defending transportation networks.

A variety of network reliability and vulnerability measures have been proposed in the literature. However, no measure for transportation networks is dominant because of the difficulty of defining their reliability or vulnerability. In systems engineering, reliability is generally defined as the ability of a system to perform its desired function to an acceptable level for some given period of time. However, in the case of transportation networks, neither the desired function nor the corresponding acceptable level of performance lends itself to straightforward and unambiguous definition (*3*). So far, the following aspects of reliability have been considered: connectivity, travel time, terminal capacity, network reserved capacity, and user and demand satisfaction. For a recent review on transportation network reliability assessment, readers are referred to the work of Heydecker et al. (*4*) and Yin (*5*).

With emphasis on both the adverse consequences and the probabilities of occurrence of disruptive events, recent studies have shifted the focus to assessment of the vulnerability or robustness of transportation networks. Vulnerability is defined as susceptibility to attacks that result in a considerable reduction in transportation network

serviceability (*6*). Various vulnerability measures include robustness and accessibility indicators that quantify the difference in system performance or social welfare before and after network degradation (*7–9*).

The ultimate goal of reliability or vulnerability analysis of transportation networks is to allocate limited resources in an optimal manner to improve network resilience after these attacks. Some have applied the notion of reliability-based design and attempt to obtain a transportation network characterized by a low probability of failure. The approaches adopted are either to maximize a reliability measure directly (*10–12*) or to incorporate reliability as chance constraints while maximizing system efficiency (*13, 14*). All these studies focus on random attacks, and the corresponding network design problems are mostly continuous, although capacity expansion is usually discrete (in number of lanes).

More recently, Lou et al. proposed a discrete robust network design problem against disturbances in travel demands (*15*). The formulation does not require knowledge of the probabilities of occurrence of uncertain events but is able to achieve a satisfactory reliability level, according to both the mean and the standard deviation of system performance. Another stream of research focuses on defending transportation networks against targeted attacks in various scenarios (*16*). Rather than resource allocation, Bell et al. optimize routing strategies to minimize the expected loss caused by random and targeted attacks (*17*).

In the study described here, several optimization models are developed to increase the resilience of transportation systems to random and targeted attacks on the basis of the proposed reliability and vulnerability measures for the two distinct groups of disruptive events. To cope with random attacks, the study considers a discrete robust network design problem. The uncertainty is also represented in a discrete manner on the basis of the observation that incidents often shut down an integer number of lanes on a road segment. For targeted attacks, remaining network transport capacity and unsatisfied demand are proposed to be two vulnerability measures. Optimal defense plans that allocate patrol personnel and surveillance resources to protect existing networks against malicious terrorist attacks are determined to minimize the vulnerability. All problems are formulated as mixed-integer minimum–maximum (or maximum–minimum) problems and are solved by use of an active-set algorithm first proposed by Zhang et al. (*18*), together with a cutting-plane scheme. The solution quality of the active-set algorithm is also discussed.

The paper is organized as follows. The next section formulates a discrete robust network design problem and two optimal defense planning problems for random and targeted attacks, respectively. The solution algorithm and procedures are then provided. Discussions of the solution quality of the active-set algorithm are also provided. Numerical experiments are then conducted to validate the formulations and demonstrate their effectiveness. The final section provides conclusions.

MODEL FORMULATIONS

In view of the differences in the nature of the two types of attacks and the levels of their corresponding consequences, different reliability and vulnerability measures are investigated for the two groups. The following problems are considered in this section: a robust discrete network design problem against random attacks (DA-R) and two problems for optimal defense planning against targeted attacks (DA-T1 and DA-T2). Subject to a given budget, the robust discrete network design problem is to determine a plan to add new roads or increase the capacities of the existing ones of a transportation network to achieve a satisfactory level of robustness of total system travel time against random attacks. The defense objective against targeted attacks is to minimize the adverse consequence of the attacks, such as unsatisfied demand, or to ensure the remaining transport capacity of the networks for postdisaster relief work.

The proposed models feature a game structure involving at least two players: the defender (planners) and the attacker (terrorists or nature). In the first level, the defender determines a network design or defense plan; the attacker then responds by interdicting the network to maximize the damage or disruption in the second level. In the case of the robust network design problem against random attacks, network users are also involved as other players who make their own travel plans in the third level. Game theory approaches have previously been adopted in the literature for transportation network reliability measures (*19–21*), in which the attackers (terrorists or nature) are modeled as demons to interdict the transportation network as much as possible. Although previous studies consider only the network users and the attackers in their models, this study explicitly includes the defender in the problem to provide transportation planners with more straightforward practical suggestions about where to allocate their resources. Another unique feature of this study is its way of modeling uncertainties by using a discrete uncertainty budget, in which some previous studies, such as the study of Szeto (*21*), have considered cooperation among multiple demons to reach a reasonable representative of the worst-case scenario.

To formulate the problem mathematically, a transportation network is represented as a directed graph, $G(N, A)$, where N and A are the sets of nodes and links, respectively. The latter are represented as a node pair (i, j), where $i, j \in N$, and $i \neq j$. Also, let W denote the set of origin–destination (O-D) pairs. For each O-D pair, $w \in W$, the travel demand is assumed to be fixed and is denoted d^w. Let d denote the demand vector for the network, and let V denote the set of all feasible flow distributions. V can be mathematically expressed as follows:

$$V = \left\{ v \middle| v = \sum_w x^w,\ \Delta x^w = E^w d^w,\ x^w \geq 0 \qquad \forall w \in W \right\}$$

where

v = aggregated link flow vector,
x^w = link flow vector for O-D pair w,
Δ = node–link incidence matrix, and
E^w = a vector in $R^{|N|}$ (where $|\bullet|$ represents the cardinality of a set) with only two nonzero components: one has a value of 1 in the component corresponding to the origin node of O-D pair w and the other has a value of −1 in the component corresponding to the destination.

Robust Discrete Network Design Against Random Attacks

For the discrete network design problem against random attacks, users' route choices are part of the system and cannot be excluded. Therefore, the problem is inherently a trilevel problem.

Attacker's Problem

It is assumed that day-to-day disruptive events may randomly occur at the link level. Once an event occurs, one lane would be blocked

and the capacity of the link would drop accordingly. Note that random attacks refer to small-scale disruptive events. It is assumed that these disruptions are not able to shut down a link completely for the entire planning horizon. Therefore, the network remains connected and a feasible flow pattern that satisfies the travel demand exists. Although it is generally difficult to obtain the probabilities of occurrence of those events, it is often possible to identify a subset of links with a higher frequency of traffic incidents through historical data. More generally, let $A_1, A_2, \ldots, A_L$ denote L subsets of links with different random attack frequency levels. Because of the lack of detailed probability information, a risk-averse perspective is taken and nature is viewed as a demon attempting to damage the network to the greatest extent possible. To avoid being overly conservative, it is further assumed that the small-scale disruptions have a limited uncertainty budget (Γ_l) for each group $l \in \{1, 2, \ldots, \text{and } L\}$; that is, only up to Γ_l disruptive events can occur simultaneously in subset A_l. Consequently, the attacker's problem becomes one of deciding where to block the lanes to maximize the total system travel time. Note that this is not a behavioral assumption for the attackers; rather, it is a way to identify a reasonable worst-case scenario for the planner's optimal network design problem.

This modeling approach is based on the idea that the decision maker should account for the risks neither too optimistically nor too conservatively. This notion follows the concept of discrete robust optimization (*22*), in which discrete random events are modeled by an uncertainty set whose size is restricted by an uncertainty budget. The uncertainty budget is selected by the defender as part of the robust network design model. It actually reflects the defender's attitudes toward risk. The larger that the uncertainty budget is, the more conservative that the defender is.

Mathematically, let z_{ij} be a binary variable indicating whether a disruptive event occurs on link $(i, j) \in A$. If z_{ij} is equal to 1, the link capacity drops by one lane. The actual random attacks can now be represented by the discrete uncertainty set as follows:

$$\sum_{(i,j)\in A_l} z_{ij} \le \Gamma_l \qquad \forall l = 1, 2, \ldots, L$$

The binary variable z_{ij} can be treated as a continuous variable when two additional constraints, $z_{ij}(1 - z_{ij}) = 0$ and $0 \le z_{ij} \le 1$, are added to the formulation. As usual, link travel time t_{ij} is considered a function of the aggregated link flow and the link capacity. The function is strictly increasing in the former and decreasing in the latter. It is assumed that traffic condition is in user equilibrium (UE), when it is considered that the attacks are mild day-to-day disruptions.

Defender's Problem

The defender's problem is to determine a capacity expansion plan to minimize the total travel time on the damaged network (without a loss of generality, the construction of new links can be treated as adding capacity to existing links with no lane). A capacity expansion (in the unit of one lane) can always be represented in binary digits. Let y_{ij}^k be a 0–1 variable in the kth bit of the binary number corresponding to the capacity expansion of link $(i, j) \in A$. Let K be the number of bits, and then the number of additional lanes is $\sum_{k=1}^{K} 2^{k-1} y_{ij}^k$, an integer between zero and 2^{K-1}. Similarly, y_{ij}^k can be treated as a continuous variable with two additional constraints: $y_{ij}^k(1 - y_{ij}^k) = 0$ and $0 \le y_{ij}^k \le 1$. As previously assumed, the link travel time function can be represented as $t_{ij}(v_{ij}, y_{ij}, z_{ij})$, where v_{ij} is the aggregated link flow and y_{ij} is a vector in the set of all real numbers R^K whose element is y_{ij}^k.

The robust discrete network design problem under random attack (DA-R) can now be formulated as follows. The objective of DA-R is to minimize the maximum system travel time incurred by disruptive events. The decision variables of the outer problem (the defender's minimization problem) compose a capacity expansion plan, and those of the inner problem (the attacker's maximization problem) are the attack plan and the associated UE flow distributions. Constraints 1 to 3 ensure that, for a given network design y and an attack plan z, the feasible flow distribution satisfies UE conditions, where variable π_i^w is the node potential of node i for O-D pair w. Constraints 4 to 6 ensure the feasibility of an attack plan, and Constraints 7 and 8 ensure that capacity expansion is discrete. Finally, Constraint 9 guarantees that the total cost of the expansion plan do not exceed B, the construction budget, where $h_{ij}(y_{ij})$ is the construction cost for link $(i, j) \in A$.

$$\min_{y} \max_{x,v,z,\pi} \sum_{(i,j)\in A} t_{ij}(v_{ij}, y_{ij}, z_{ij}) \cdot v_{ij}$$

subject to

$$x_{ij}^w\left(t_{ij}(v_{ij}, y_{ij}, z_{ij}) + \pi_i^w - \pi_j^w\right) = 0 \qquad \forall (i, j) \in A, \forall w \in W \tag{1}$$

$$t_{ij}(v_{ij}, y_{ij}, z_{ij}) + \pi_i^w - \pi_j^w \ge 0 \qquad \forall (i, j) \in A, \forall w \in W \tag{2}$$

$$v \in V \tag{3}$$

$$\sum_{(i,j)\in A_l} z_{ij} \le \Gamma_l \qquad \forall l = 1, 2, \ldots, L \tag{4}$$

$$z_{ij}(1 - z_{ij}) = 0 \qquad \forall (i, j) \in A \tag{5}$$

$$0 \le z_{ij} \le 1 \qquad \forall (i, j) \in A \tag{6}$$

$$y_{ij}^k(1 - y_{ij}^k) = 0 \qquad \forall (i, j) \in A, \forall k \in K \tag{7}$$

$$0 \le y_{ij}^k \le 1 \qquad \forall (i, j) \in A, \forall k \in K \tag{8}$$

$$\sum_{(i,j)\in A} h_{ij}(y_{ij}) \le B \tag{9}$$

As formulated, DA-R is a mathematical program with complementarity constraints (MPCCs), consisting of three sets of complementarity constraints: one set is associated with Constraints 1 and 2, and the other two are due to the conversion of the binary variables y_{ij}^k and z_{ij} to continuous ones. Note that this formulation does not alter the trilevel nature of the problem, as the inner problem cannot be solved as an ordinary nonlinear program because constraint qualifications may not hold for the complementarity constraints. The formulation appears to be a generalized semi-infinite minimum–maximum problem (*23*), in which the feasible set of the inner problem depends on the decision variable of the outer problem through Conditions 1 and 2. In fact, it is only an ordinary minimum–maximum problem because UE link flow is unique for a given set of y_{ij} and z_{ij}. In other words, the actual decision for the inner problem is z_{ij}, whose feasible region does not vary with y_{ij}. All the other variables can be viewed as ones auxiliary to calculation of the objective function. The problem can be solved efficiently by use of the active-set algorithm and a cutting-plane scheme.

Optimal Defense Planning Against Targeted Attacks

Optimal defense problems are formulated in this subsection to allocate patrol personnel and surveillance resources to protect existing networks against malicious terrorist attacks or to help with evacuation after a natural disaster. When it is considered that connectivity and serviceability are more critical than total system travel time in the case of evacuation and postdisaster relief, two vulnerability measures are proposed: one deals with the remaining transport capacity, and the other considers the unsatisfied demand of the transportation network. The proposed vulnerability measures and corresponding optimal resource allocation models do not consider congestion in the network because when part of the network may be destroyed under targeted attacks, the question of how many people can be evacuated safely becomes more important than how congested the network is. The two vulnerability measures also enable the problems to be simplified as ordinary minimum–maximum or maximum–minimum problems.

Binary variable y_{ij} is used to indicate whether a link is protected, and another binary variable, z_{ij}, is used to represent whether a link is a terrorist target. $h_{ij}(y_{ij})$ is now the cost for protecting link $\forall(i, j) \in A$, and B is the resource limit. The other notations remain the same as in DA-R. It is assumed that if a link is protected, terrorists will not be able to select it as a target. If a link is targeted, it will be completely destroyed. In the case of a large-scale natural disaster, the assumption becomes that a protected link will be fully restored shortly after the strike. Mathematically, the new link capacity can be written $C_{ij}(1 - z_{ij}(1 - y_{ij}))$. When y_{ij} is equal to 1, that is, when a link is protected, its capacity will remain at the original level, C_{ij}, regardless of the attacker's actions. When y_{ij} is equal to 0, the new link capacity is then subject to the targeted attack.

Attacker's Problem

With limited resources, the terrorists attempt to interdict the network as much as possible. When a large-scale natural disaster is considered, the resources limit can be viewed as the uncertainty budget, as discussed earlier. When transport capacity is considered a vulnerability measure, the objective of the attacker is to minimize the transport capacity, which can be represented by F^w, the maximum flow between each O-D pair. Let E_i^w denote the ith component of the vector E^w, and the attacker's problem can be formulated as follows:

$$\min_{z} \max_{x,F} \sum_{w} F^w$$

subject to

$$\sum_{w} x_{ij}^w \le C_{ij}\left(1 - z_{ij}\left(1 - y_{ij}\right)\right) \qquad \forall\left(i, j\right) \in A \tag{10}$$

$$\sum_{(i,j)\in A} x_{ij}^w - \sum_{(j,i)\in A} x_{ji}^w = E_i^w F^w \qquad \forall i \in N, \forall w \in W \tag{11}$$

$$x_{ij}^w \ge 0 \qquad \forall\left(i, j\right) \in A, \forall w \in W$$

$$\sum_{(i,j)\in A} z_{ij} \le \Gamma$$

$$z_{ij}\left(1 - z_{ij}\right) = 0 \qquad \forall\left(i, j\right) \in A$$

$$0 \le z_{ij} \le 1 \qquad \forall\left(i, j\right) \in A$$

This problem is itself a generalized minimum–maximum problem and will lead to a trilevel minimum–maximum–minimum formulation when the defender's problem is considered. When y_{ij} and z_{ij} are given, the inner maximum-flow problem reduces to a linear program (LP). Therefore, the strong duality theory was applied to transform the maximum-flow problem into its LP dual, a minimum-cut problem. Let λ_{ij} and π_i^w denote the multiplier for Conditions 10 and 11, respectively. Let $s(w)$ and $t(w)$ denote the origin and destination nodes for O-D pair w, respectively. The attacker's problem can now be written as a single-level problem.

$$\min_{z,\lambda,\pi} \sum_{(i,j)\in A} \lambda_{ij} C_{ij}\left(1 - z_{ij}\left(1 - y_{ij}\right)\right)$$

subject to

$$\lambda_{ij} + \pi_i^w - \pi_j^w \ge 0 \qquad \forall\left(i, j\right) \in A, \forall w \in W$$

$$\pi_{t(w)}^w = 1 + \pi_{s(w)}^w \qquad \forall w \in W$$

$$\lambda_{ij} \ge 0 \qquad \forall\left(i, j\right) \in A$$

$$\sum_{(i,j)\in A} z_{ij} \le \Gamma$$

$$z_{ij}\left(1 - z_{ij}\right) = 0 \qquad \forall\left(i, j\right) \in A$$

$$0 \le z_{ij} \le 1 \qquad \forall\left(i, j\right) \in A$$

When the unsatisfied demand of the network is considered to be the vulnerability measure for a transit-based evacuation operation, the flow distribution is likely to be coordinated by transportation authorities to minimize the total or weighted unsatisfied demand, in which more important O-D pairs, such as hospital, school, and residential zones, may have higher priorities in evacuation. The attacker's objective is then to maximize this value. With the introduction of two auxiliary variables d_+ and d_- to represent the excess transport ability and the unsatisfied demand, respectively, the problem can be formulated as follows:

$$\max_{z} \min_{x,d_+,d_-} \sum_{w} g^w d_-^w$$

subject to

$$\sum_{(i,j)\in A} x_{ij}^w - \sum_{(j,i)\in A} x_{ji}^w = E_i^w\left(d^w + d_+^w - d_-^w\right) \qquad \forall i \in N, \forall w \in W$$

$$\sum_{w} x_{ij}^w \le C_{ij}\left(1 - z_{ij}\left(1 - y_{ij}\right)\right) \qquad \forall\left(i, j\right) \in A$$

$$x_{ij}^w \ge 0 \qquad \forall\left(i, j\right) \in A, \forall w \in W$$

$$d_+,\ d_- \ge 0$$

$$\sum_{(i,j)\in A} z_{ij} \le \Gamma$$

$$z_{ij}\left(1 - z_{ij}\right) = 0 \qquad \forall\left(i, j\right) \in A$$

$$0 \le z_{ij} \le 1 \qquad \forall\left(i, j\right) \in A$$

where g^w terms are predetermined weights for each O-D pair.

Similarly, this problem can be converted to a single-level problem by taking the LP dual of the inner problem. The attacker's problem can be equivalently formulated as

$$\max_{z,\lambda,\pi} \sum_{(i,j)\in A} \lambda_{ij} C_{ij}\left(1 - z_{ij}\left(1 - y_{ij}\right)\right) + \sum_{w\in W} d^w \left(\pi^w_{s(w)} - \pi^w_{t(w)}\right)$$

subject to

$$\lambda_j + \pi^w_i - \pi^w_j \geq 0 \qquad \forall (i,j) \in A, \forall w \in W$$

$$0 \leq \pi^w_{s(w)} - \pi^w_{t(w)} \leq g^w \qquad \forall w \in W$$

$$\lambda_j \geq 0 \qquad \forall (i,j) \in A$$

$$\sum_{(i,j)\in A} z_{ij} \leq \Gamma$$

$$z_{ij}\left(1 - z_{ij}\right) = 0 \qquad \forall (i,j) \in A$$

$$0 \leq z_{ij} \leq 1 \qquad \forall (i,j) \in A$$

Defender's Problem

The defender's objective is to increase the maximum flow of the attacked network or to reduce the unsatisfied demand under targeted attacks. Two formulations for the two vulnerability measures are presented below.

The first formulation of the robust discrete network design problem under targeted attack (DA-T1) adopts the transport capacity (maximum flow) as a connectivity vulnerability measure.

$$\max_{y} \min_{z,\lambda,\pi} \sum_{(i,j)\in A} \lambda_{ij} C_{ij}\left(1 - z_{ij}\left(1 - y_{ij}\right)\right)$$

subject to

$$\lambda_{ij} + \pi^w_i - \pi^w_j \geq 0 \qquad \forall (i,j) \in A, \forall w \in W \tag{12}$$

$$\pi^w_{t(w)} = 1 + \pi^w_{s(w)} \qquad \forall w \in W \tag{13}$$

$$\lambda_{ij} \geq 0 \qquad \forall (i,j) \in A \tag{14}$$

$$\sum_{(i,j)\in A} z_{ij} \leq \Gamma \tag{15}$$

$$z_{ij}\left(1 - z_{ij}\right) = 0 \qquad \forall (i,j) \in A \tag{16}$$

$$0 \leq z_{ij} \leq 1 \qquad \forall (i,j) \in A \tag{17}$$

$$y_{ij}\left(1 - y_{ij}\right) = 0 \qquad \forall (i,j) \in A \tag{18}$$

$$0 \leq y_{ij} \leq 1 \qquad \forall (i,j) \in A \tag{19}$$

$$\sum_{(i,j)\in A} h_{ij}\left(y_{ij}\right) \leq B \tag{20}$$

DA-T2 features the (weighted) unsatisfied demand as the serviceability measure.

$$\min_{y} \max_{z,\lambda,\pi} \sum_{(i,j)\in A} \lambda_{ij} C_{ij}\left(1 - z_{ij}\left(1 - y_{ij}\right)\right) + \sum_{w\in W} d^w \left(\pi^w_{s(w)} - \pi^w_{t(w)}\right)$$

subject to

$$\lambda_{ij} + \pi^w_i - \pi^w_j \geq 0 \qquad \forall (i,j) \in A, \forall w \in W \tag{21}$$

$$0 \leq \pi^w_{s(w)} - \pi^w_{t(w)} \leq g^w \qquad \forall w \in W \tag{22}$$

$$\lambda_{ij} \geq 0 \qquad \forall (i,j) \in A \tag{23}$$

$$\sum_{(i,j)\in A} z_{ij} \leq \Gamma \tag{24}$$

$$z_{ij}\left(1 - z_{ij}\right) = 0 \qquad \forall (i,j) \in A \tag{25}$$

$$0 \leq z_{ij} \leq 1 \qquad \forall (i,j) \in A \tag{26}$$

$$y_{ij}\left(1 - y_{ij}\right) = 0 \qquad \forall (i,j) \in A$$

$$0 \leq y_{ij} \leq 1 \qquad \forall (i,j) \in A$$

$$\sum_{(i,j)\in A} h_{ij}\left(y_{ij}\right) \leq B$$

The two DA-T models actually provide practical implications on defense strategies against targeted attacks. As the performance measure, these two models consider how many people can (and cannot) be moved to safe zones after certain targeted attack. They are particularly suitable for identifying critical infrastructures in a network in the event of large-scale disruption and emergency evacuation. Practitioners may allocate resources, such as patrol vehicles, directly according to the modeling result to prevent malicious attacks in the first place or, in the event of evacuation, deploy more personnel to those critical links to ensure an efficient operation.

SOLUTION ALGORITHM

As discussed above, all three formulations can be viewed as ordinary semi-infinite minimum–maximum (or maximum–minimum) problems with complementarity constraints for the two sets of decision variables y and z. More generally, all three proposed models can be written in the following format:

$$\min_{y} \max_{\xi} f\left(y, \xi\right)$$

or

$$\max_{y} \min_{\xi} f\left(y, \xi\right)$$

subject to

$$\xi \in \Xi$$

$$y \in Y$$

where ξ denotes the decision variables of the inner problem, including the attacker's decision z. For DA-R, $\xi = \{z\}$, Ξ is defined by Conditions 4 to 6, and Y is characterized by Conditions 7 to 9. Again, note that $f(y, \xi)$ is uniquely determined for a given y and z through Conditions 1 to 3. For DA-T1, $\xi = \{z, \lambda, \pi\}$, Ξ is defined by Conditions 12 to 17, and Y is characterized by Conditions 18 to 20.

DA-T2 is similar to DA-T1, with the exception that Ξ is now defined by Conditions 21 to 26.

Without a loss of generality, the minimum–maximum problem will be used to demonstrate the solution procedure in this section. To reveal its semi-infinite property, the general formulation can be further transformed into the following equivalent problems:

$$\min_{y} \eta$$

subject to

$$f(y, \xi) \le \eta \qquad \forall \xi \in \Xi \tag{27}$$

$$y \in Y$$

Therefore, all three proposed problems can be solved by use of a cutting-plane scheme for the minimum–maximum (or maximum–minimum) structure, together with the active-set algorithm to handle the complementarity constraints in Ξ and Y.

Combined Cutting-Plane and Active-Set Algorithm

Consider the minimum–maximum problem as an example. The essential idea of the cutting-plane scheme is to approximate Constraint 27 by a finite subset $\tilde{\Xi} \subset \Xi$. The approximated or the relaxed problem (R-DA) can be written as

$$\min_{y} \eta$$

subject to

$$f(y, \xi^i) \le \eta \qquad \forall \xi^1, \xi^2, \ldots, \xi^n \in \tilde{\Xi}$$

$$y \in Y$$

Additional points in Ξ are generated by solving the inner maximization problem as needed to enlarge $\tilde{\Xi}$. The solution procedure is briefly summarized in the following.

Step 0. Select a feasible point ξ^1 to the inner problem. Set $n = 1$ and $\tilde{\Xi}^1 = \{\xi^1\}$.

Step 1. Solve the R-DA problem with the discrete set $\tilde{\Xi}^n$. Let y^n denote the resulting optimal solution and η^n the optimal objective value.

Step 2. Solve the inner maximization problem and let ξ^{n+1} denote the resulting optimal solution.

Step 3. If $f(y^n, \xi^{n+1}) \le \eta^n$, stop and y^n is an optimal robust network design or defense plan. Otherwise, set $\tilde{\Xi}^{n+1} = \tilde{\Xi}^n + \{\xi^{n+1}\}$ and $n = n + 1$. Go to Step 1.

If both Steps 1 and 2 can be solved to global optimality, the solution procedure is able to result in a true optimum solution to the original problem. However, because both the inner and the relaxed outer problems are essentially mixed-integer or integer problems, it is difficult to obtain their global optimal solutions. Although it is possible to apply branch-and-bound algorithms (*24, 25*) to achieve a nearly optimal solution, the computational cost is usually high and it may not be practical to do so for real-size networks. Instead, this study treats the binary variable as continuous by introducing corresponding complementarity constraints. In this way, both the R-DA and the inner maximization problem can be solved by the active-set algorithm (*18*). Similar to previous work (*26*), it can be proved that each feasible integer solution is a point strongly stationary (*27*) to MPCCs. In this sense, the basic idea of the active-set algorithm is to strategically update a given feasible design or defense plan by making use of the dual information associated with an index-set-based relaxation of the original problem. For a more elaborate description of the cutting-plane scheme with active-set algorithm, readers are referred to other work (*15, 18*). The algorithm is heuristic but efficient. The solution quality of the algorithm is further discussed in the next subsection.

Further Discussion on Active-Set Algorithm

In their numerical study, Zhang et al. illustrated that the active-set algorithm is able to generate global optimal or nearly optimal solutions for a group of small problems (*18*). Recently, Wang and Lo proposed a linearization scheme to convert the network design problem into a mixed-integer linear program by approximating the nonlinear travel time function using a set of piecewise linear functions (*28*). The finer that the approximation resolution is, the closer that the problem is to the original one. In this way, they were able to find the global optimal solution to the original network design problem. To further test the solution quality of the active-set algorithm for larger networks, this subsection compares the solutions obtained by the active-set algorithm with those reported by Wang and Lo (*28*).

The testing network consists of six nodes and 16 links. All the links are subject to expansion to up to three lanes. For the active-set algorithm, this results in 32 binary variables. Two demand scenarios are tested. The corresponding settings and parameters can be found elsewhere (*28, 29*). For the low-demand scenario, the active-set algorithm leads to a local optimal solution with an objective value of 213.42. The expansion plan differs by one link from the global optimal solution reported by Wang and Lo (*28*), and the objective value is 6.47% more than the global optimum. For the high-demand scenario, the active-set algorithm produces the exact global optimal solution, as reported previously (*28*). The active-set algorithm is far more efficient than the linearization scheme. Wang and Lo reported computation times of 3 min and 2.6 h for the two scenarios, respectively, whereas the times for the active-set algorithm are only 5.16 and 39.34 s, respectively, on a Dell E6400 laptop computer with a 2.10-GHz Intel Core Duo central processing unit (CPU) and 1.95 GB of random access memory (RAM). This indicates that the active-set algorithm is efficient and may be able to achieve solutions with satisfactory qualities.

NUMERICAL EXAMPLES

Numerical experiments are conducted and the results are reported in this section to validate and demonstrate the proposed models and algorithms. Two testing networks are used: the nine-node (*30*) and the Sioux Falls, South Dakota (*31*), networks. The former consists of 18 links, nine nodes, and four O-D pairs, whereas the latter comprises 76 links, 24 nodes, and 528 O-D pairs. The proposed models and algorithm are tested in GAMS (*32*), and CONOPT solver (*33*) is used for the nonlinear subproblems generated by the active-set algorithm.

Robust Network Design Against Random Attacks

The results reported in this subsection are from a GAMS implementation on a Dell E6400 laptop computer with a 2.10-GHz Intel Core Duo CPU and 1.95 GB of RAM.

In both networks, all links are candidates for expansion of capacity by up to three additional lanes. For simplicity, the expansion cost is assumed to be 1 for one additional lane, and the additional capacities for one added lane are 5 and 3 in each network, respectively. Links are grouped into two subsets with different probabilities of occurrence of random attacks. Five and 12 links that suffer from higher probabilities of random attacks were selected for the nine-node network and Sioux Falls network, respectively. Links in the high- and low-probability sets were assumed to have 40% and 5% chances of losing one lane of capacity, respectively. It is easy to see that the uncertainty budgets Γ_l in DA-R will have substantial impacts on how well the actual uncertainty is represented and thus will affect the solution quality.

Various uncertainty and expansion budgets were tested for both networks. To compare the robust and nominal plans, a Monte Carlo simulation was conducted on the basis of 500 randomly generated scenarios of different random attacks. The mean, standard deviation, and maximum of the total travel times associated with the UE flows were computed as the performance measures. The average computational time for a robust design (robust plan) was about 2 min for all the numerical experiments.

Table 1 presents the nominal design and three different robust designs (in number of additional lanes) solved with different combinations of the uncertainty budget values for the nine-node network. The expansion budget was set equal to 12. The nominal design is solved with Γ_{high} equal to Γ_{low} equal to 0; that is, it is a deterministic robust design problem. It can be seen that although part of the investment is the same among all four designs, such as Link (5, 7), the remaining investment differs in either the link selection or the number of lanes added. Links (2, 5) and (8, 4) are not selected in the nominal design, although they suffer from a higher probability of random attacks. Link (7, 3) is always chosen in the robust design, even though the associated random attack probability is low: it is a congested link because of the numerical settings of the example.

All three robust designs perform reasonably well for the mean total system travel time. Robust Design 1 even improves the mean value by 1%. The improvement is statistically significant, although not substantial. The standard deviations of all three robust plans outperform the nominal one. The improvements are 12.5%, 21.3%, and 35.17%, respectively. The worst-case total system travel times for Robust Designs 1 and 3 are slightly lower than the travel time of the nominal plan, whereas Robust Design 2 produces a worst-case travel time similar to that of the nominal plan.

The numerical experiments also suggested that the result will be an inferior robust plan if the uncertainty budgets are set too conservatively. One plausible reason for this is that the particular worst-case random attack scenario generated by solving the inner maximization problem of the original formulation is unlikely to be realized. The results validate the formulation and demonstrate that when the uncertainty budgets are set properly, the model is able to produce robust plans that provide superior reliability without impairing the average total system travel time.

Similar results were observed for the Sioux Falls network, as reported in Table 2. The expansion budget was set equal to 15. Links that are subject to higher random attack probabilities are improved only in the robust design. The robust design reduces the standard deviation by 10.4% and at the mean time is able to achieve a level of average total system travel time similar to that of the nominal design. Although the maximum value is higher under the robust design, a closer examination shows that the average value of the distribution's right tail is actually lower under the robust design, indicating that the worst-case scenario is possibly an outlier.

Optimal Defense Planning Against Targeted Attacks

For the purposes of validation and demonstration, this study focused on only one of the two proposed optimal defense planning problems.

TABLE 1 Robust and Nominal Network Designs for Nine-Node Network

Link	High Attack Probability	Nominal Design	Robust Design 1	Robust Design 2	Robust Design 3
(1, 6)	Yes	3	1	3	2
(2, 5)	Yes	—	—	3	1
(5, 7)	No	3	3	3	3
(6, 8)	No	3	3	—	1
(7, 3)	No	3	2	3	3
(8, 4)	Yes	—	3	—	2
Uncertainty Budgets					
Γ_{high}		0	3	1	2
Γ_{low}		0	0	1	1
Simulated Total System Travel Time Statistics					
Mean		2,068.02	2,045.74	2,095.28	2,072.33
SD		25.93	22.68	14.33	16.81
Maximum		2,164.54	2,153.94	2,166.34	2,138.37

NOTE: SD = standard deviation.

TABLE 2 Robust and Nominal Network Designs for Sioux Falls Network

Link	High Attack Probability	Nominal Design	Robust Design
(6, 8)	No	3	3
(8, 6)	No	3	3
(10, 16)	No	3	—
(14, 11)	No	3	—
(16, 10)	No	3	3
(21, 24)	Yes	—	3
(24, 21)	Yes	—	3
Uncertainty Budgets			
Γ_{high}		0	3
Γ_{low}		0	0
Simulated Total System Travel Time Statistics			
Mean		9,336.46	9,414.83
SD		713.57	639.65
Maximum		11,597.57	12,964.11

TABLE 3 Optimal Defense Plans and Targeted Attacks for Sioux Falls Network

Link	S1 $B = 3, \Gamma = 5$		S2 $B = 5, \Gamma = 5$		S3 $B = 10, \Gamma = 5$	
	Defense Plan	Targeted Attack	Defense Plan	Targeted Attack	Defense Plan	Targeted Attack
(1, 2)	1				1	
(1, 3)		1		1	1	
(2, 1)	1				1	
(3, 1)		1	1		1	
(3, 4)						1
(5, 9)				1		
(7, 18)			1		1	
(8, 7)				1		
(9, 5)				1		1
(10, 11)				1		1
(11, 10)						1
(12, 3)			1		1	
(12, 13)	1				1	
(13, 12)		1			1	
(15, 14)		1				
(18, 7)		1				
(18, 20)			1		1	
(20, 18)			1		1	
(22, 15)						1
Maximum Flow						
No defense	651.76		651.76		651.76	
Optimal defense	677.53		717.52		722.05	

All results reported in this subsection are for problem DA-T1 and are from a GAMS implementation on a Dell desktop computer with a 3.19-GHz CPU and 1 GB of RAM.

For the nine-node network, the original transport capacity (maximum flow) is 100. When both the protection and the attacking budgets are set equal to 3, the maximum flow is reduced to 12, and even the three most important links, Links (6, 8), (9, 7), and (9, 8), are protected. When the protection budget B is limited and the attack budget (Γ) is sufficiently large (in this case, B is equal to 3 and Γ is ≥ 5), the network would be totally blocked and no evacuation flow could be sent from any origin to any destination.

Various defending and attacking budgets were tested for the Sioux Falls network. Selected cases are presented in Table 3. All of the attack targets are nonprotected links. This is because of the assumption that the link cannot be destroyed if it is protected. The transport capacity increases with the defense budget. The improvements are as high as 9.2% and 10.8% for B equal to 5 and B equal to 10, respectively. Compared with the original network transport capacity of 778.8, the defense plans reported in Table 3 were able to achieve levels of connectivity ranging from 87.0% to 92.8% of the original value.

This study also investigated three more cases in which Γ was set equal to 10. The resulting network transport capacities under optimal defense and coordinated attacks are reported in Figure 1. Although only limited cases are tested, Figure 1 reveals the general trend that the network transport capacity is an increasing function of B and a decreasing function of Γ.

All six numerical experiments were solved efficiently with less than 10 iterations of the cutting-plane scheme. Take the problem with B equal to 10 and Γ equal to 10, for example. The problem only took 6 iterations and 12 s of CPU time to be solved. Figure 2 shows the evolution of the objective function value at each iteration.

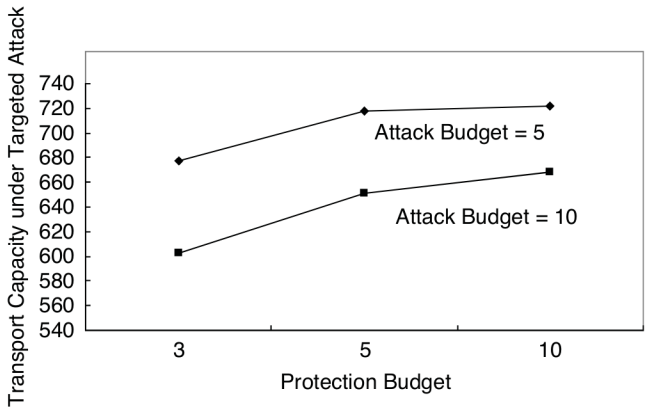

FIGURE 1 Network transport capacities with protection and attack budgets.

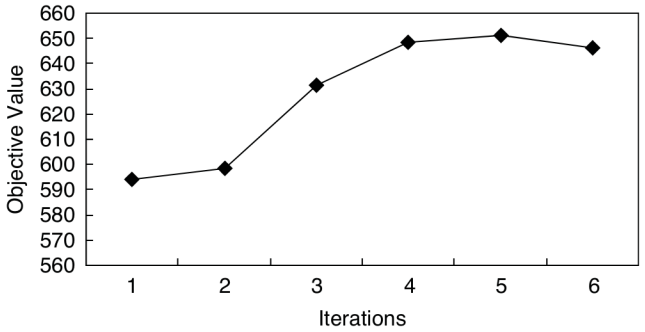

FIGURE 2 Evolution of objective function value.

CONCLUSION

To address reliability and vulnerability issues of transportation networks, this paper investigates multiple resource allocation problems for transportation network design or defense to minimize the disruption caused by both random and targeted attacks. A discrete robust optimization approach is used to model uncertainties associated with the disruptions.

Random attacks refer to day-to-day disturbances such as small-scale adverse weather, traffic incidents, and operation failures. This group of disruptive events often has higher probabilities of occurrence but less severe consequences. Because network connectivity is often unaffected by these disruptions, the reliability of the total system travel time might be one good measure against random attacks and can be addressed in the network planning stage. A robust discrete network design problem is formulated to solve for optimal plans for expansion of capacity that will perform reasonably well against random attacks. The proposed model features a trilevel game structure among the network users, the attacker, and the defender.

Targeted attacks often have lower probabilities of occurrence but disastrous outcomes. This group mainly includes coordinated terrorist strikes and large-scale natural disasters in which part of the network may be destroyed. In this case, risk or vulnerability measures such as connectivity and serviceability become more important. The remaining transport capacity may serve as a measure for network connectivity, and the unsatisfied (weighted) demand would be a critical serviceability measure in case of emergency evacuation.

Two formulations are developed for the two different vulnerability measures to deploy law enforcement forces to prevent malicious attacks in the first place or to ensure a smooth evacuation after or during a natural disaster. By exploring the unique properties of these measures, the trilevel structure can be avoided and these two problems can be reformulated as ordinary minimum–maximum problems. A combination of an active-set algorithm and a cutting-plane scheme is applied to solve the proposed models. The solution quality of the active-set algorithm is briefly investigated. The numerical examples indicate that the proposed formulations are valid and that the solution algorithm is able to solve the problems effectively and efficiently. The resulting robust discrete network design is able to reduce the standard deviation of the total system travel time substantially. The resulting optimal defense plans are able to achieve a reasonably large percentage of the network's original transport capacity even under coordinated attacks.

REFERENCES

1. *The National Strategy for Homeland Security.* U.S. Department of Homeland Security, Washington, D.C., 2007. http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf. Accessed Oct. 2010.
2. Balog, J. N., A. Boyd, J. Caton, P. N. Bromley, J. B. Strongin, D. Chia, and K. Bagdonas. *TCRP Report 86: Public Transportation Security: Volume 7. Public Transportation Emergency Mobilization and Emergency Operations Guide.* Transportation Research Board of the National Academies, Washington, D.C., 2005.
3. Cassir, C., M. G. H. Bell, and Y. Iida. Introduction. In *Reliability of Transport Networks* (M. G. H. Bell and C. Cassir, eds.), Research Studies Press, Baldock, United Kingdom, 2000, pp. 1–10.
4. Heydecker, B., W. H. K. Lam, and N. Zhang. Use of Travel Demand Satisfaction to Assess Road Network Reliability. *Transportmetrica,* Vol. 3, No. 2, 2007, pp. 139–171.
5. Yin, Y. *Reliability Assessment of Road Networks: Models and Algorithms.* PhD dissertation. Department of Civil Engineering, University of Tokyo, 2002.
6. Berdica, K. An Introduction to Road Vulnerability: What Has Been Done, Is Done and Should Be Done. *Transport Policy,* Vol. 9, No. 2, 2002, pp. 117–127.
7. Chen, A., S. Kongsomsaksakul, Z. Zhou, M. Lee, and W. Recker. Assessing Network Vulnerability of Degradable Transportation Systems: An Accessibility Based Approach. In *Transportation and Traffic Theory 2007* (R. E. Allsop, M. G. H. Bell, and B. G. Heydecker, eds.), Elsevier, Oxford, United Kingdom, 2007, pp. 235–262.
8. Jenelius, E., T. Petersen, and L.-G. Mattsson. Importance and Exposure in Road Network Vulnerability Analysis. *Transportation Research Part A,* Vol. 40, No. 7, 2006, pp. 537–560.
9. Scott, D. M., D. C. Novak, L. Aultman-Hall, and F. Guo. Network Robustness Index: A New Method for Identifying Critical Links and Evaluating the Performance of Transportation Networks. *Journal of Transport Geography,* Vol. 14, No. 3, 2006, pp. 215–227.
10. Yin, Y., and H. Ieda. Optimal Improvement Scheme for Network Reliability. In *Transportation Research Record: Journal of the Transportation Research Board, No. 1783,* Transportation Research Board of the National Academies, Washington, D.C., 2002, pp. 1–6.
11. Chen, A., J. Kim, Z. Zhou, and P. Chootinan. Alpha Reliable Network Design Problem. In *Transportation Research Record: Journal of the Transportation Research Board, No. 2029,* Transportation Research Board of the National Academies, Washington, D.C., 2007, pp. 49–57.
12. Sumalee, A., D. P. Watling, and S. Nakayama. Reliable Network Design Problem: Case with Uncertain Demand and Total Travel Time Reliability. In *Transportation Research Record: Journal of the Transportation Research Board, No. 1964,* Transportation Research Board of the National Academies, Washington, D.C., 2006, pp. 81–90.
13. Lo, H. K. and Y. K. Tung. Network with Degradable Links: Capacity Analysis and Design. *Transportation Research Part B,* Vol. 31, No. 4, 2003, pp. 345–363.
14. Sun, Y. and M. A. Turnquist. Investment in Transportation Network Capacity Under Uncertainty: Simulated Annealing Approach. In *Transportation Research Record: Journal of the Transportation Research Board, No. 2039,* Transportation Research Board of the National Academies, Washington, D.C., 2007, pp. 67–74.
15. Lou, Y., Y. Yin, and S. Lawphongpanich. Robust Approach to Discrete Network Designs with Demand Uncertainty. In *Transportation Research Record: Journal of the Transportation Research Board, No. 2090,* Transportation Research Board of the National Academies, Washington, D.C., 2009, pp. 86–94.
16. Smith, J. C., C. Lim, and F. Sudargho. Survivable Network Design Under Optimal and Heuristic Interdiction Scenarios. *Journal of Global Optimization,* Vol. 38, No. 2, 2007, pp. 181–199.
17. Bell, M. G. H., U. Kanturska, J.-D. Schmocker, and A. Fonzone. Attacker–Defender Models and Road Network Vulnerability. *Philosophical Transactions of the Royal Society A: Mathematical, Physical, and Engineering Sciences,* Vol. 366, No. 1872, 2008, pp. 1893–1906.
18. Zhang, L., S. Laphongpanich, and Y. Yin. An Active-Set Algorithm for Discrete Network Design Problems. In *Transportation and Traffic Theory 2009* (W. H. K. Lam, S. C. Wong. and L. Hong, eds.), Springer, New York, 2009, pp. 283–300.
19. Bell, M. A Game Theory Approach to Measuring the Performance Reliability of Transport Networks. *Transportation Research Part B,* Vol. 34, No. 6, 2002, pp. 533–545.

20. Szeto, W. Y., L. O'Brien, and M. O'Mahony. Measuring Network Reliability Considering Paradoxes: Multiple Network Demon Approach. In *Transportation Research Record: Journal of the Transportation Research Board, No. 2090,* Transportation Research Board of the National Academies, Washington, D.C., 2009, pp. 42–50.
21. Szeto, W. Cooperative Game Approaches to Measuring Network Reliability Considering Paradoxes. *Transportation Research Part C,* Vol. 19, No. 2, 2011, pp. 229–241.
22. Bertismas, D., and M. Sim. Robust Discrete Optimization and Network Flows. *Mathematical Programming,* Vol. 98, No. 1–3, 2003, pp. 49–71.
23. Polak, E., and J. Royset. On the Use of Augmented Lagrangians in the Solution of Generalized Semi-Infinite Min-Max Problems. *Computational Optimization and Applications,* Vol. 31, No. 2, 2005, pp. 173–192.
24. LeBlanc, L. J. An Algorithm for the Discrete Network Design Problem. *Transportation Science,* Vol. 9, No. 3, 1975, pp. 183–199.
25. Poorzahedy, H., and M. A. Turnquist. Approximate Algorithms for the Discrete Network Design Problem. *Transportation Research Part B,* Vol. 16, No. 1, 1982, pp. 44–55.
26. Lou, Y., Y. Yin, and S. Lawphongpanich. Freeway Service Patrol Deployment Planning for Incident Management and Congestion Mitigation. *Transportation Research Part C,* Vol. 19, No. 2, 2011, pp. 283–295.
27. Scheel, H., and S. Scholtes. Mathematical Programs with Complementarity Constraints: Stationarity, Optimality, and Sensitivity. *Mathematics of Operations Research,* Vol. 25, No. 1, 2000, pp. 1–22.
28. Wang, D., and H. Lo. Global Optimum of the Linearized Network Design Problem with Equilibrium Flows. *Transportation Research Part B,* Vol. 44, No. 4, 2010, pp. 482–492.
29. Friesz, T. L., H.-J. Cho, N. J. Metha, R. L. Tobin, and G. Anandalingam. A Simulated Annealing Approach to the Network Design Problem with Variational Inequality Constraints. *Transportation Science,* Vol. 26, No. 1, 1992, pp. 18–26.
30. Hearn, D. W., and M. V. Ramana. Solving Congestion Toll Pricing Models. In *Equilibrium and Advanced Transportation Modeling* (P. Marcotte and S. Nguyen, eds.), Kluwer Academic Publishers, Norwell, Mass., 1998, pp. 109–124.
31. LeBlanc, L. J., E. K. Morlok, and W. P. Pierskalla. An Efficient Approach to Solving the Road Network Equilibrium Traffic Assignment Problem, *Transport Research,* Vol. 9, 1975, pp. 309–318.
32. Brooke, A., D. Kendirck, and A. Meeraus. *GAMS: A User's Guide.* Scientific Press, San Francisco, Calif., 1992.
33. Drud, A. CONOPT—A Large Scale GRG Code. *Operations Research Society of America Journal on Computing,* Vol. 6, 1994, pp. 207–216.

The Critical Transportation Infrastructure Protection Committee peer-reviewed this paper.