Networks of Critical Infrastructures: Cost Estimation and Defense of Attacks

Reinhard Bürgy

1 Introduction

Critical infrastructures (CIs) are systems that provide vital services to society, such as the supply of drinking water, electricity, or transportation. Any significant disruption of these services directly threatens the security and the economic system of a society, public health and safety, or any combination of the above [5]. Even small disruptions and component failures can strongly reduce performance and cause major economic damage. Hence, a physical or cyber-attack on a CI generates massive negative externalities, especially because of the increasing interdependency and technical interconnectedness of different CIs. Particularly, the cascading effect of failures among CIs could pose a serious threat to society [2, 10]. Therefore, CIs are an ideal target for terrorist, politically motivated, or criminal attacks.

Such attacks constitute the most dangerous asymmetric threat CIs have to face today and in the future [5]. Hence, there is the need to develop applied models that can evaluate the costs and consequences of intentional attacks on CIs. In this work, infrastructure networks are investigated, and a specific method for evaluating the cost of attacks on CIs is presented. A generic theoretical model is suggested that can account for different network types and attack patterns. The practical application of the model allows the reader to identify weak spots within the network.

R. Bürgy (✉)
Department of Informatics, University of Fribourg, Fribourg, Switzerland
e-mail: reinhard.buergy@unifr.ch

M. M. Keupp (ed.), *The Security of Critical Infrastructures*, International Series
in Operations Research & Management Science 288,
https://doi.org/10.1007/978-3-030-41826-7_2

2 Background

The model is grounded in solid scientific work from the operations research domain. The model builds on prior work by Brown et al. [6], Golany et al. [9], and Alderson et al. [3] who have all modeled and evaluated attacks on CIs. It employs linear programming and network flow theory [1, 8] and applies prior research on network interdiction [7]. To date, this research resonates little in the communities of experts responsible for CI protection. Attempts to prioritize efforts for critical infrastructure protection typically produce descriptive lists and planning instruments. For instance, both the Swiss Federal Office for Civil Protection, the U.S. Department of Defense, and the U.S. Department of Homeland Security have all prioritized critical infrastructure elements in an attempt to produce comprehensive protection. However, this practice is questionable from a scientific perspective since particular components cannot be prioritized by criticality [2]. The model in this chapter is proposed as an alternative.

3 Methods

3.1 Operator Model

The model assumes that a homogeneous good or service is transported across a network. The network contains supply nodes that provide the good or service, demand nodes that consume it, and transit nodes that transfer it to other nodes.

In order to graphically represent the model, a simple directed graph $G = (V, E)$ is given, where V represents a set of nodes (the circles in Fig. 1 and all following figures), and E a set of arcs (the arrows in Fig. 1 and all following figures). The set of nodes is partitioned into $V = V_A \cup V_N \cup V_T$, where V_A is the set of "supply nodes", V_N the set of "demand nodes" and V_T the set of "transit nodes". The set of

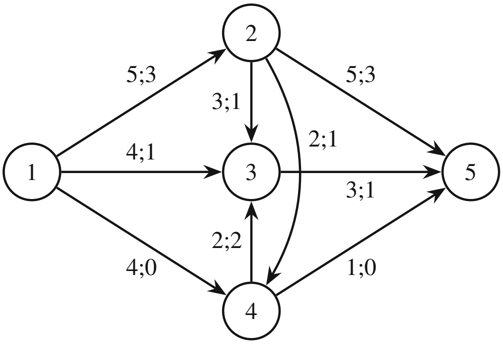


Fig. 1 A small operator network with five nodes

arcs E represents the connections between the objects. In this paper, an arc $e \in E$ is either indicated as e or by its end nodes $e = (v, w)$.

For each node $v \in V$, if $v \in V_A$, it can provide a (non-negative) supply a_v, and if $v \in V_N$, it has a (non-negative) demand n_v. Each arc $e \in E$ has an arc capacity u_e, which is the maximal flow of a good or service through the arc (for a given time span), and cost c_e for each unit of the good or service transported by this arc.

Figure 1 illustrates this setting for a system with five nodes. In this specific example, node 1 is a supply node with a supply of $a_v = 7$ and node 5 is a demand node with a demand of $n_v = 5$. All other nodes are transit nodes. Each arc $e \in E$ is represented by an arrow and a pair of numbers u_e; c_e which indicate the capacity and the unit cost of the arc.

A solution is sought for a feasible flow $x \in \mathbb{R}^E$ that minimizes total cost (a so-called cost-optimal flow). Thus, a respective flow x_e has to be found for every arc $e \in E$. For a given node $v \in V$ the net inflow $f_x(v)$ is defined as total inflow less total outflow, formally:

$$f_x(v) = \sum_{w:(w,v)\in E} x_{wv} - \sum_{w:(v,w)\in E} x_{vw}$$

A flow is feasible if the flow constraints as well as the capacity constraints are satisfied. The flow constraints state that a supply node cannot provide more than its supply, a demand node must satisfy demand, and a transit node has to relay the flow without losses:

$$\begin{aligned} f_x(v) &\leq a_v \text{ for all } v \in V_A, \\ f_x(v) &= n_v \text{ for all } v \in V_N, \\ f_x(v) &= 0 \text{ for all } v \in V_T. \end{aligned}$$

The capacity constraints guarantee that the capacity of the arcs is not exceeded:

$$0 \leq x_e \leq u_e \text{ for all } e \in E.$$

Among all feasible flows, we seek to find a minimum-cost flow x, i.e. $\sum_{e\in E} c_e x_e$. Together, these conditions yield the following minimum-cost flow problem (P1):

$$\min \sum_{e\in E} c_e x_e$$

subject to:

$$\begin{aligned} f_x(v) &\leq a_v \text{ for all } v \in V_A, \\ f_x(v) &= n_v \text{ for all } v \in V_N, \\ f_x(v) &= 0 \text{ for all } v \in V_T, \\ 0 \leq x_e &\leq u_e \text{ for all } e \in E. \end{aligned} \tag{P1}$$

Fig. 2 Cost optimal flow for the network given by Fig. 1

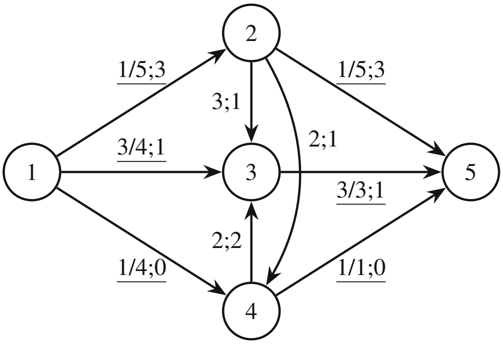


Figure 2 gives an optimal solution for the example specified by Fig. 1. For each arc with a positive flow, the calculated flow value is given next to the arc and before the slash. For example, the flow from node 1 to node 2 equals $x_{12} = 1$. In this example, the total cost of this optimal solution is 12.

3.2 *Inclusion of Shortage and Formulation in Standard Form*

The above model is now extended and applied to a situation where the network cannot or not completely satisfy all demands. This is done by assigning a penalty cost p_v to each demand node $v \in V$. Additionally, all flow constraints are now described by equations in order to formulate the problem in a standard form. Hence, the following elements are added to graph $G = (V, E)$:

(a) A pseudo supply node v_a with supply $a_{v_a} = \sum_{v \in V_N} n_v$
(b) For every demand node $v \in V_N$, an arc (v_a, v) with cost p_v and capacity n_v
(c) A pseudo demand node v_n with demand $n_{v_n} = \sum_{v \in V_A} a_v$
(d) For every supply node $v \in V_A \cup \{v_a\}$, an arc (v, v_n) with zero cost and capacity a_v

The pseudo supply node can deliver missing units to demand nodes at penalty cost p_v. The resulting graph is denoted by $G' = (V', E')$. For every node $v' \in V'$ the demand b_v is defined as:

$$b_v = \begin{cases} -a_v & \text{if } v \in V_A \cup \{v_a\} \\ n_v & \text{if } v \in V_N \cup \{v_n\} \\ 0 & \text{else.} \end{cases}$$

Figure 3 illustrates these modifications for a unit penalty cost of 100.
This extended problem can now be described as follows in $G' = (V', E')$:

$$z = min \sum_{e \in E'} c_e x_e$$

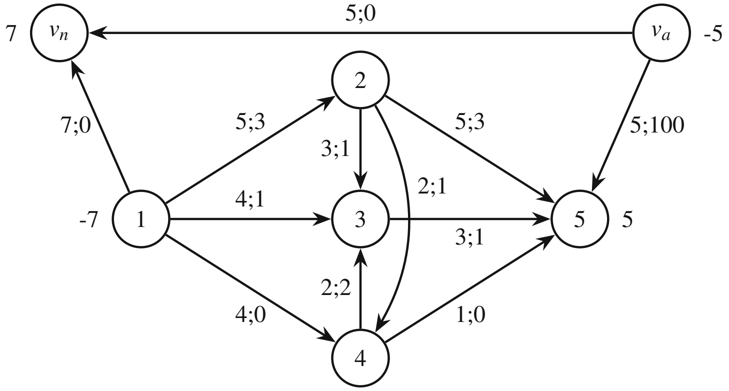


Fig. 3 Modified model in standard form

subject to:

$$f_x(v) = b_v \text{ for all } v \in V', \tag{P2}$$
$$0 \leq x_e \leq u_e \text{ for all } e \in E'.$$

It is assumed that the operator runs the network at optimal cost. In this case the value of the optimized solution of the following model simply indicates the "regular" operating costs.

3.3 Modeling an Attack Scenario

It is assumed that an attack on a network can target both nodes and arcs. If an arc is attacked, it becomes inoperative, i.e. its capacity is reduced to zero. If a node is attacked, it cannot deliver supply nor serve as a transit node, but its demand remains unchanged. This situation is modeled by reducing the capacity of all arcs interrupted as a consequence of the attack to zero.

An attack scenario $U = (V_u, E_u)$ is defined by the sets of attacked nodes $V_u \subseteq V$ and arcs $E_u \subseteq E$. Pseudo nodes and pseudo arcs cannot be attacked. A valid solution for this attack scenario must satisfy the following constraints:

$$x_e = 0 \text{ for all } e \in E_u,$$
$$x_{vw} = 0 \text{ for all } v \in V_u,$$
$$x_{vw} = 0 \text{ for all } w \in V_u.$$

Once these constraints are added to the model, a given attack scenario $U = (V_u, E_u)$ can be described as:

$$z_U = min \sum_{e \in E'} c_e x_e$$

subject to:

$$\begin{aligned} f_x(v) &= b_v \text{ for all } v \in V', \\ 0 \le x_e &\le u_e \text{ for all } e \in E', \\ x_e &= 0 \text{ for all } e \in E_u, \\ x_{vw} &= 0 \text{ for all } v \in V_u, \\ x_{vw} &= 0 \text{ for all } w \in V_u. \end{aligned} \tag{P3}$$

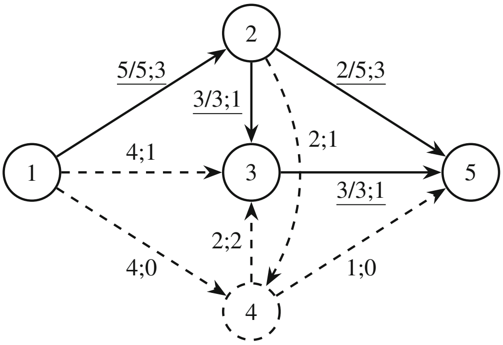
If $V_u = \varnothing$ and $E_u = \varnothing$ then (P3) is equivalent to (P2). Problem (P3) is also a minimum cost flow problem, implying that it can be solved efficiently and that integer input vectors b and u yield integer solutions. This is an important characteristic of network flow problems.

Again, it is assumed that the network is run at optimal cost after an attack. Hence, the target variable z_U of an optimal solution of (P3) indicates the operating cost after an attack $U = (V_u, E_u)$. For every attack U the costs K_U are defined as:

$$K_U = z_u - z.$$

Hence, the operating costs after an attack exceed those of normal operations, i.e. $z_U \geq z$ and hence $K_U \geq 0$ for any attack U. Figure 4 illustrates an attack scenario $U = (V_u, E_u)$ with $V_u = \{4\}$ and $E_u = \{(1, 3)\}$. Only graph G instead of G' is shown. Dashed arcs are unavailable after the attack. Arcs with a positive flow are underlined. The demand of node 5 can still be met. Total operating cost after the attack is 27, implying the cost K_U of the attack is $K_U = 27 - 12 = 15$.

Fig. 4 Modified model with an attack on node 4



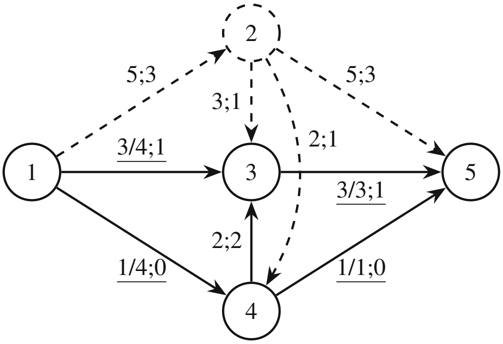


Fig. 5 Modified model with an attack on node 2

Figure 5 illustrates an attack scenario where only node 2 is attacked, i.e. $U_2 = (V_{u_2}, E_{u_2})$ with $V_{u_2} = \{2\}$ and $E_{u_2} = \emptyset$:

The demand at node 5 cannot be fully satisfied. One unit cannot be delivered, implying a penalty cost of 100. The total operating cost of the network is now 106, such that attack has caused a damage of $106 - 12 = 94$ monetary units.

3.4 The Attacker-Defender Model

While the CI operators may not know how exactly the network will be attacked in the future, they can assume that a well-informed attacker will likely attempt to maximize any damage, i.e. to maximize the network's total operating cost. In the following, the model is modified further to reflect this intention. An attacker has a given budget B. Every element of the network has a certain strength, which represents the resources an attacker must invest to disable this element. Specifically, the attacker incurs a cost of p_v units for an attack on any node $v \in V$, and a cost of p_e units for an attack on any arc $e \in E$. The following decision variables are introduced to model the attack decision:

y_e for all $e \in E$: y_e is 1 if arc e is attacked and 0 otherwise,

y_v for all $v \in V$: y_v is 1 if node v is attacked and 0 otherwise.

Further, the attacker is subject to the budget constraint:

$$\sum_{e \in E} p_e y_e + \sum_{v \in V} p_v y_v \leq B.$$

In a first step, the attack is modeled by adjusting the arc capacities:

$$
\begin{aligned}
&0 \leq x_e \leq u_e \text{ for all } e \in E' - E,\\
&0 \leq x_e \leq u_e\left(1 - y_e\right) \text{ for all } e \in E,\\
&0 \leq x_{vw} \leq u_{vw}\left(1 - y_v\right) \text{ for all } (v, w) \in E,\\
&0 \leq x_{vw} \leq u_{vw}\left(1 - y_w\right) \text{ for all } (v, w) \in E.
\end{aligned}
$$

The constraints in the first line address those pseudo arcs whose capacities remain unchanged. For an arc $e = (v, w) \in E$, the capacity is u_e unless either arc e or node v or w are attacked. In any of these cases, the constraints in lines 2 to 4 specify that the capacity of any such node or arc is reduced to zero. Hence, the following model results:

$$\max_y \min_x \sum_{e \in E'} c_e x_e$$

subject to:

$$
\begin{aligned}
&f_x(v) = b_v \text{ for all } v \in V', \qquad \text{(P4)}\\
&0 \leq x_e \leq u_e \text{ for all } e \in E' - E,\\
&0 \leq x_e \leq u_e\left(1 - y_e\right) \text{ for all } e \in E,\\
&0 \leq x_{vw} \leq u_{vw}\left(1 - y_v\right) \text{ for all } (v, w) \in E,\\
&0 \leq x_{vw} \leq u_{vw}\left(1 - y_w\right) \text{ for all } (v, w) \in E,
\end{aligned}
$$

$$\sum_{e \in E} p_e y_e + \sum_{v \in V} p_v y_v \leq B,$$

$$
\begin{aligned}
&y_e \in \{0, 1\} \text{ for all } e \in E,\\
&y_v \in \{0, 1\} \text{ for all } v \in V.
\end{aligned}
$$

Problem (P4) is a bi-level optimization problem to which standard mathematical solvers such as CPLEX or Gurobi cannot be applied directly. To transform this bi-level into a single-level optimization problem, (P4) is reformulated by following the approach described in Brown et al. [6]. Flows over attacked arcs are penalized, letting M denote a sufficiently high penalty cost. Hence, (P4) can be rewritten as:

$$\max_y \min_x \sum_{e \in E' - E} c_e x_e + \sum_{e = (v, w) \in E} \left(c_e + M\left(y_e + y_v + y_w\right)\right) x_e$$

subject to:

$$
\begin{aligned}
& f_x(v) = b_v \text{ for all } v \in V', \\
& 0 \le x_e \le u_e \text{ for all } e \in E', \\
& \sum_{e \in E} p_e y_e + \sum_{v \in V} p_v y_v \le B, \\
& y_e \in \{0, 1\} \text{ for all } e \in E \\
& y_v \in \{0, 1\} \text{ for all } v \in V.
\end{aligned}
\tag{P5}
$$

The solution spaces of (P4) and (P5) are not identical but if M is chosen correctly, the optimal solutions and the optimal objective values are the same in both problems. (P5) is still a bi-level optimization problem, but the inner optimization problem can be transformed using duality theory [8]. Informally speaking, the inner optimization problem (P5) is transformed into a maximization problem while the value of the optimal solution stays the same. Two types of dual variables are introduced: α_v for each flow constraint of node $v \in V'$ in (P5) and β_{vw} for each capacity constraint of arc $(v, w) \in E'$ in (P5). Developing the corresponding dual constraints for all primal variables and the dual objective function, the following dual problem is obtained:

$$
\max \sum_{v \in V'} b_v \alpha_v - \sum_{e \in E'} u_e \beta_e
$$

subject to:

$$
\begin{aligned}
& \alpha_w - \alpha_v + \beta_{vw} \le c_{vw} \text{ for all } (v, w) \in E' - E, \\
& \alpha_w - \alpha_v + \beta_{vw} \le c_{vw} + M\,(y_e + y_v + y_w) \text{ for all } e = (v, w) \in E, \\
& \beta_e \ge 0 \text{ for all } e \in E'.
\end{aligned}
\tag{P6}
$$

The inner optimization problem of (P5) always has a solution and the optimum is limited since all cost factors c_e are positive. In this case, the objective value of the optimal solution of (P6) equals the objective value of (P5). Hence, the inner optimization problem (P5) can be replaced by (P6), which yields the following reformulation of (P5):

$$
\max \sum_{v \in V'} b_v \alpha_v - \sum_{e \in E'} u_e \beta_e
$$

subject to:

$$\alpha_w - \alpha_v + \beta_{vw} \leq c_{vw} \text{ for all } (v, w) \in E' - E, \tag{P7}$$

$$\alpha_w - \alpha_v + \beta_{vw} \leq c_{vw} + M\,(y_e + y_v + y_w) \text{ for all } e = (v, w) \in E,$$

$$\beta_e \geq 0 \text{ for all } e \in E',$$

$$\sum_{e \in E} p_e y_e + \sum_{v \in V} p_v y_v \leq B,$$

$$y_e \in \{0, 1\} \text{ for all } e \in E,$$

$$y_v \in \{0, 1\} \text{ for all } v \in V.$$

Problem (P7) is a mixed-integer linear program. While we specify this problem here, we also note that current optimization solvers, such as CPLEX and GUROBI, are not able to find optimal solutions for large-size instances of this problem in acceptable computation time. Future research may focus on improving the numerical analysis and compatibility of this linear program.

3.5 Application to a Small Example

The attacker-defender model is now applied to the operator network example. The strength p_e of each arc $e \in E$ is indicated at the third position of the respective data lines next to the arcs. Nodes are considered infinitely resilient, i.e. $p_v = \infty$ for all $v \in V$:

Table 1 below gives optimal attack strategies for different attack budgets B. It demonstrates that there is no straightforward correlation between the attack budget and the number of attacked arcs.

To illustrate this fact, Figs. 6, 7 and 8 give the respective graphs for attack budgets of $B = 1$ and $B = 13$. Although the cost of the attack increases by a factor of more than 81 in the latter scenario, only two more arcs are attacked.

Table 1 Optimal attacks and cost of these attacks for all attack budgets

Attack budget B	Optimal attack	Cost of attack
$B = 1$	(4,5)	$6 = (18 - 12)$
$B = 2$	(3,5)	$6 = (18 - 12)$
$3 \leq B \leq 9$	(3,5),(4,5)	$18 = (30 - 12)$
$B = 10$	(2,5)	$94 = (106 - 12)$
$B = 11$	(2,5),(4,5)	$194 = (206 - 12)$
$B = 12$	(2,5),(3,5)	$388 = (400 - 12)$
$B \geq 13$	(1,2),(1,4),(3,5)	$488 = (500 - 12)$

Fig. 6 Application of the model to an attack on arcs

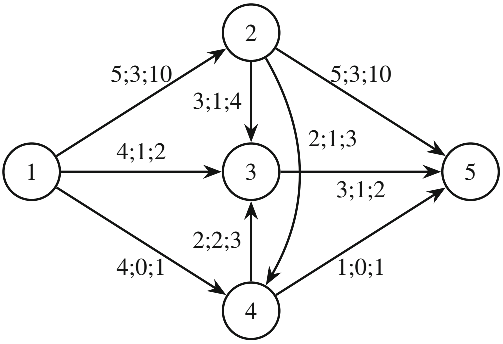


Fig. 7 Optimal attack strategy for $B = 1$

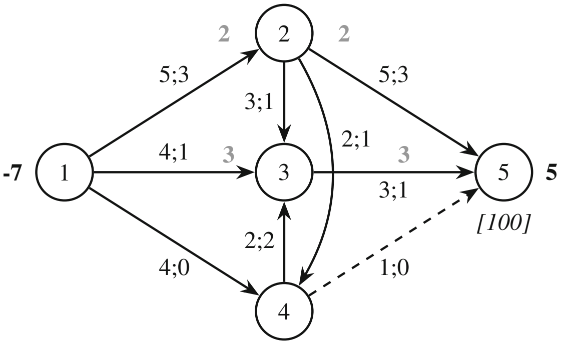
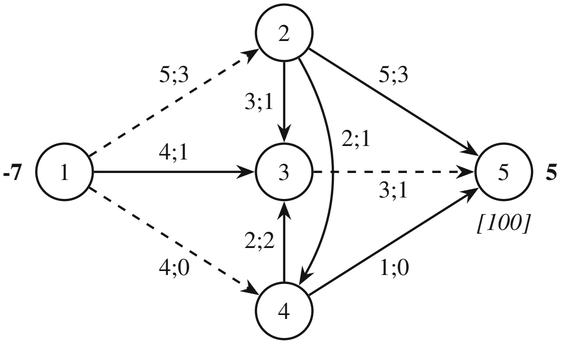


Fig. 8 Optimal attack strategy for $B = 13$



Further, a particular arc need not constitute an attractive target in an optimal strategy anymore as the attack budget increases. This effect shows as B is increased from 1 to 2 and from 9 to 10. Hence, optimal attacking strategies are not nested with respect to an increase in B. This implies that network elements cannot be prioritized by criticality, which confirms the initial criticism of [3].

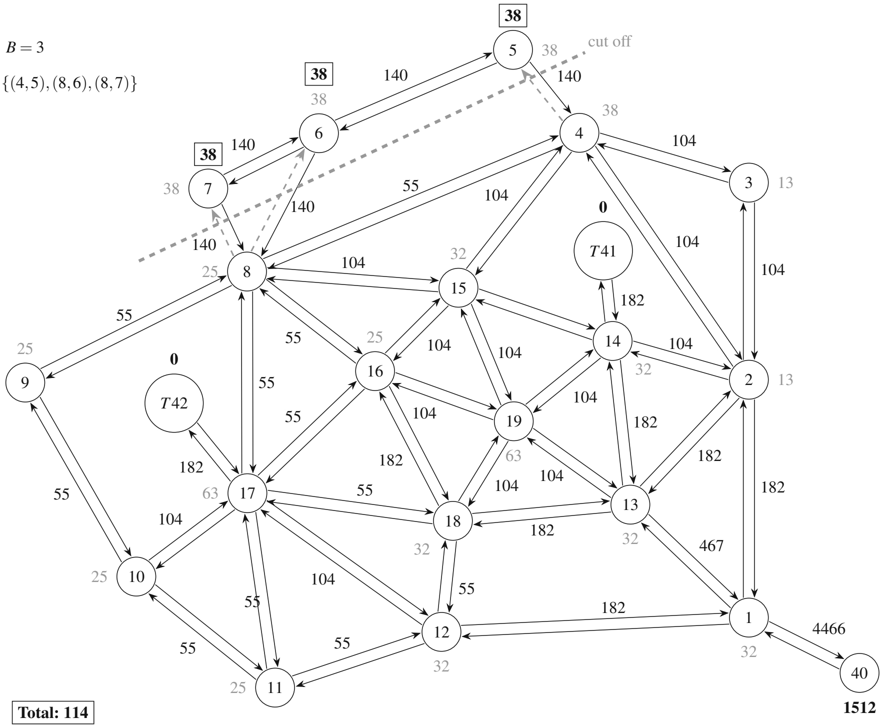


Fig. 9 Attack on the Anytown network for $B = 3$

3.6 *Application to the Anytown Network*

The Anytown Network is a modeling tool for diverse problems in network design. To apply it, I used data from the University of Exeter Centre for Water Systems.[1] In all following diagrams, nodes T41 and T42 are water reservoirs whose analysis is not required for the purposes of our model.

The model allows for bidirectional flows and hence specifies bidirectional arcs whose capacity is identical. All arcs have unit cost 1 and the penalty cost for all demand nodes is 1000 per missing unit. It is assumed that all nodes and arcs incident to node 1 cannot be attacked, while all other arcs have a strength of 1. We calculated models and generated their corresponding graphs for all attack budgets. For reasons of space only a selection of the results is discussed here. The full set of graphs is available on request.

[1] http://emps.exeter.ac.uk/engineering/research/cws/.

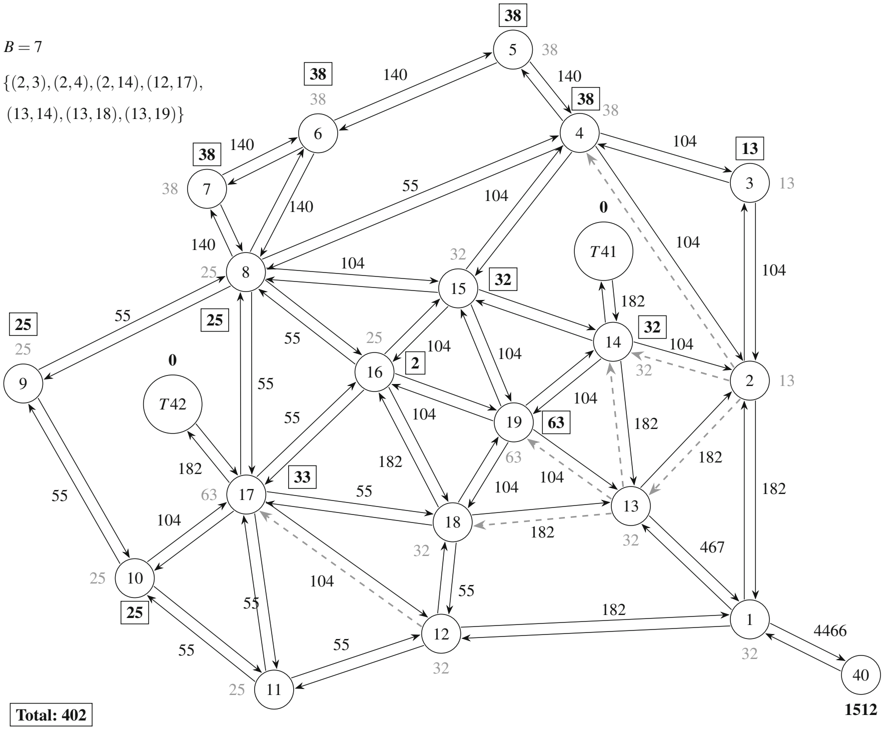


Fig. 10 Attack on the Anytown network for $B = 7$

Figure 9 shows the results of an attack on the network for $B = 3$. A subsection of the graph (nodes 5, 6 and 7) is cut off from both the remaining nodes and from the source, as illustrated by the bold dashed line.

Figure 10 illustrates an attack for $B = 7$. While the graph remains strongly-connected, several central elements are attacked, and bidirectional flow is significantly reduced, implying a significant increase in operating cost.

Figure 11 shows the results for an attack budget of $B = 9$. The graph is split into two sub-graphs, and no other nodes than those directly linked to node 1 can be operated.

4 Conclusion and Outlook

In this chapter, the cost of an attack on critical infrastructure networks was assessed with a generic model. This model was implemented as a mixed-integer linear program and applied to several small-scale examples. Future work could use this operationalization to analyze actual infrastructures, such as energy or drinking water

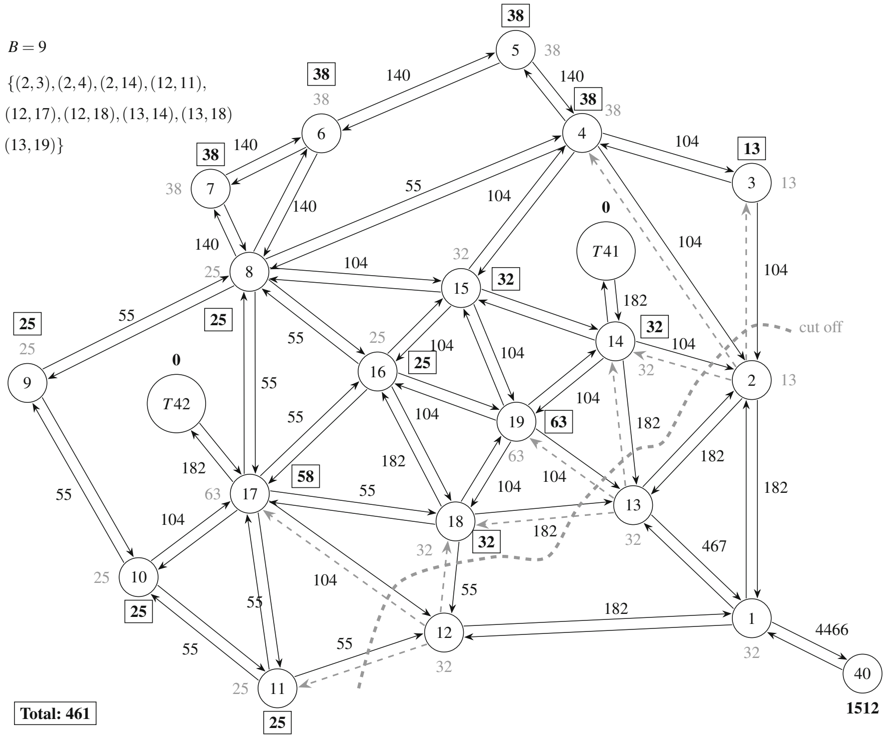


Fig. 11 Attack on the Anytown network for $B = 9$

networks. While the challenges of modeling such real networks are anything but trivial, related work may draw on some of the ideas presented here.

Further, the attacker-defender model considered here could be extended to scenarios where the operator attempts to protect the infrastructure in question by investing into the strength of the network. Such an operator would use a particular defence budget to invest in measures that minimize the maximum costs of an attack (e.g., by increasing the robustness or redundancy of critical components). Future work may analyze optimal investment strategies for this defence budget. While the analysis of such defender-attacker-defender models [4, 6] builds on the basic scenarios we have illustrated here, it is significantly more complex.

References

1. Ahuja, R.K., Magnanti, T.L., Orlin, J.B.: Network Flows: Theory, Algorithms and Applications. Prentice Hall, Englewood Cliffs (1993)
2. Alcaraz, C., Lopez, J.: Wide-area situational awareness for critical infrastructure protection. Computer **46**(4), 30–37 (2013)

3. Alderson, D.L., Brown, G.G., Carlyle, W.M., Cox Jr, L.A.: Sometimes there is no “most-vital” arc: assessing and improving the operational resilience of systems. Mil. Oper. Res. **18**(1), 21–37 (2013)
4. Alderson, D.L., Brown, G.G., Carlyle, W.M., Wood, R.K.: Solving defender-attacker-defender models for infrastructure defense. Technical Report, Naval Postgraduate School Monterey CA Department of Operations Research (2011)
5. Anderson, R., Fuloria, S.: Security economics and critical national infrastructure. In: Economics of Information Security and Privacy, pp. 55–66. Springer, Berlin (2010)
6. Brown, G., Carlyle, M., Salmerón, J., Wood, K.: Defending critical infrastructure. Interfaces **36**(6), 530–544 (2006)
7. Collado, R.A., Papp, D.: Network Interdiction–Models, Applications, Unexplored Directions. Rutcor Res Rep, RRR4, Rutgers University, New Brunswick (2012)
8. Frederick, S., Hillier, L., Gerald, J.: Introduction to Operations Research. McGraw-Hill Education, New York (2014)
9. Golany, B., Kaplan, E.H., Marmur, A., Rothblum, U.G.: Nature plays with dice–terrorists do not: allocating resources to counter strategic versus probabilistic risks. Eur. J. Oper. Res. **192**(1), 198–208 (2009)
10. Gordon, L.A., Loeb, M.P., Lucyshyn, W., Zhou, L.: Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. J. Inf. Secur. **6**(1), 24 (2015)