ICOSSAR 2021
The 13th International Conference on Structural Safety and Reliability (ICOSSAR 2021), June 21-25, 2021, Shanghai, P.R. China
J. Li, Pol D. Spanos, J.B. Chen & Y.B. Peng (Eds)

Comparing Topology-based and Flow-based Resilience Assessment of Interdependent Infrastructure Networks

Jin-Zhu Yu[a], Yu Wang[b], and Hiba Baroud[c]

[a]*Interdisciplinary Studies of Systems Engineering, Vanderbilt University, E-mail: jinzhu.yu@vanderbilt.edu.*
[b]*Department of Civil and Environmental Engineering, Vanderbilt University, E-mail: yu.wang.1@vanderbilt.edu.*
[c]*Department of Civil and Environmental Engineering, Vanderbilt University, E-mail: hiba.baroud@vanderbilt.edu.*

ABSTRACT: Infrastructure networks are vulnerable to a wide range of disruptions due to natural hazards or man-made attacks. The ability of such networks to respond to and recover from disruptions is characterized by their resilience which influences the impact of disruptions and corresponding resource allocation. Therefore, the accurate assessment of infrastructure resilience is critical to inform the restoration process. This study investigates the resilience assessment of interdependent infrastructure systems using topology- and flow-based approaches. The objective of the research is to compare the two classes of models in order to determine the importance of incorporating flow in resilience assessment methods, and to explore the applicability of topology-based methods in assessing infrastructure resilience. In order to conduct the comparison, we propose a mixed-integer program (MIP) to optimize the resilience of coupled infrastructure networks, and we adapt the MIP to model the topology-based problem by modifying the objective function and linearizing the constraints required for calculating topology-based resilience. The proposed models and the comparative analysis are illustrated with a case study of a 49-node coupled power-gas system.

1 Introduction

Interdependencies across critical infrastructure networks improve their operational efficiency. However, interdependent connections increase the vulnerability of infrastructure systems during disruptions due to the cascading effect of failures (Vespignani, 2010; Buldyrev et al 2010). Understanding systems resilience, the ability of a systems to recover from disruptions (Hosseini et al 2016), has been recognized by academics, practitioners, and government agencies (Goldbeck et al. 2017). As infrastructure networks become increasingly interdependent, the resilience of interdependent critical infrastructures (ICIs), which is determined by the vulnerability and recoverability of a system, has recently garnered attention (Ouyang & Wang 2015; Zou & Chen 2017; Nan & Sansavini 2017; Goldbeck et al. 2017; Yu 2020). Many approaches have been developed to assess the resilience of ICIs, such as agent-based models, network-based methods, system dynamics, and reinforcement learning (Ouyang 2014; Sun & Zhang 2020). Among these approaches, network-based methods have been widely applied due to their ability to mathematically represent the network characteristics of critical infrastructures, which then enables researchers to leverage powerful network-based modeling and optimization techniques (Ouyang & Wang 2015; González et al. 2016; Fang & Zio 2019; Karakoc et al. 2019; Yu & Baroud 2020). Network-based approaches for the

resilience assessment of infrastructure networks can be divided into two categories: topology-based models and flow-based models (Ouyang 2014). Each of the two classes of models has been used widely and separately for resilience assessment (Johansson & Hassel 2010; Gao et al. 2016; Goldbeck et al. 2017; Sun & Zhang 2020; Ahangar et al. 2020). However, different types of models may lead to different conclusions about resilience assessment and subsequently different restoration plans of damaged ICIs. Few studies have examined the differences between the resilience assessment using these two classes of models. This study conducts a comparative analysis of resilience assessment methods using topology- and flow-based approaches.

1.1 *Relevant Background*

Topology-based models only consider the topology in representing the ICIs, thus nodes can become inoperable due to direct physical damage or the loss of connectivity to the supply. In contrast, flow-based models also include the flow in modeling ICIs. Each link is associated with a flow and a flow capacity, therefore node can lose functionality when the required amount of flow is not provided even though the node is still connected to the supply source. Some studies have explored the difference between the two class of models with a focus on the vulnerability of a single network. By comparing the vulnerability assessment using topological model and direct current optimal power flow model (DCOPF) for the venerability assessment of power grids, Hines et al. (2010) conclude that although topology-based models can reveal general trends of vulnerability, they can underestimate the vulnerability of power systems. Ouyang (2013) evaluates the vulnerability of synthetic power systems in which the cascading failures are described using the topological model, betweenness-based model, and the DCOPF model. Ouyang finds that the three models can produce almost identical topology-based vulnerability at a high failure probability and the topology-based vulnerability results can provide a good approximation for flow-based vulnerability when the failure probability of components is high. Goldbeck et al. (2017) point out that topological models cannot capture the characteristics beyond network connectivity and develop a dynamic network flow model to assess the resilience of ICIs. While several studies have investigated the applicability of topology-based models in the context of vulnerability assessment, few studies compare the two classes of models for the resilience assessment of ICIs following different types of disturbances.

1.2 *Contributions*

The objective of our study is to evaluate the ability of flow-based and topology-based models in assessing the resilience of ICIs following cascading failures triggered by different types of initial attacks. The contributions of this study are three-fold. First, we evaluate the cascading failures of ICIs under different types of attacks where the cascading dynamics are simulated using the dynamic network flow redistribution model. Second, we develop a mixed-integer program (MIP) to optimize flow-based resilience and adapt the program to model the topology-based resilience optimization problem. Non-linear constraints are linearized such that the programs can be solved efficiently. Finally, we demonstrate shortcomings of the topology-based resilience assessment by comparing the resilience of coupled infrastructure networks after different types of initial attacks.

The rest of this paper is structured as follows. Section 2 introduces the mathematical representation of ICIs, the method for simulating the cascading dynamics using the DFR algorithm, and the MIP for flow-based and topology-based resilience optimization. Section 3.1 introduces the synthetic power-gas networks used for illustrating the proposed methods. The results from the case study are shown in Section 3.2. Finally, the conclusion and discussions about future work are pre-

sented in Section 4.

2 Methodology

2.1 *Mathematical Representation of Interdependent Critical Infrastructures*

ICI networks are represented as a directed graph $G(N,A)$ where N is the set of nodes and A is the set of arcs. For ICI networks, the node set N is the union of sets of nodes in each network N^m, $\forall m \in M$, i.e. $N = N^1 \cup N^2 ... \cup N^{|M|}$. Nodes represent the facilities in each network, e.g. the power station and substations in power systems and gas processing plants and storage stations in gas distribution systems. The link set A is the union of sets of links in each network A^m, $\forall m \in M$, i.e. $A = A^1 \cup A^2 ... \cup A^{|M|}$ and the interdependency links between the networks $A^{m \to l}$, $\forall m,l \in M$. Each node is associated with a demand value and supply value. Each link is associated with a flow value and a value of flow conservation rate. Note that for links within a network, the value of flow conservation rate is 1.

2.2 *Attack Types*

In order to simulate the damaged state of the ICIs, four types of exogenous disturbances to the networks are considered.

The first type of disturbance is *random failure*, which models the impact of natural hazards. In this study, we consider that attacks impact nodes only. In simulating the random failure, nodes of the ICIs are removed randomly from the networks. The random failures are repeated many times to average out the impact of randomness. As critical infrastructure systems may also be subject to intentional attacks that aim to maximize the damage to the networks, we consider two types of targeted attacks, including *degree-based*, *betweenness-based*, and *closeness-based* attacks. Degree centrality (D) is the number of edges of a node. Betweenness centrality (B) of a node is defined as the ratio between the number of shortest paths between each pair of nodes passing through the node under study to the total number of shortest paths between each pair of nodes, which is given by

$$B(v) = \sum_{i \neq v \neq j} \frac{\sigma_{ij}(v)}{\sigma_{ij}} \tag{1}$$

where σ_{ij} is the total number of shortest paths between node pair i and j and $\sigma_{ij}(v)$ is the number of those paths passing through node v. The closeness centrality (C) measures how close a node is to the other nodes in the network, which is expressed as

$$C(i) = \frac{N-1}{\sum_{j=1}^{N-1} d(i,j)} \tag{2}$$

where N is the total number of nodes in the network and $d(i,j)$ is the shortest path between node i and j (Hagberg et al. 2008). For each type of targeted attack, nodes are incrementally removed beginning with the ones having the highest value of the respective centrality.

2.3 *Cascading Failure*

To obtain accurate damage state of the interdependent networks following different attacks, it is necessary to simulate cascading failures. In this study, we adapt the *local flow redistribution model* (Wang & Chen 2008; Wang et al. 2019) to simulate the cascading failures triggered by initial attacks. The model in Wang & Chen (2008) only works for undirected networks, and we adapt their model for directed networks. In each step during the failure propagation, link k and node i will be overloaded and thus fail if the flow or supply exceed the respective capacity, which is assumed to be $(1+\alpha)$ times the respective initial value (Eqs. (3) and (4)) (Motter & Lai 2002).

$$u_k = (1+\alpha) f_{k0}, \ \forall k \in A \tag{3}$$

$$c_i = (1+\alpha) q_{i0}, \ \forall i \in N \tag{4}$$

The additional flow assigned to each adjacent link of the failed edge is proportional to the

ICOSSAR 2021
The 13th International Conference on Structural Safety and Reliability (ICOSSAR 2021), June 21-25, 2021, Shanghai, P.R. China
J. Li, Pol D. Spanos, J.B. Chen & Y.B. Peng (Eds)

Algorithm 1: Simulating cascading failures

Input: ID of attacked nodes N_0^d, tolerance rate α, supply capacity of each node c_i, and supply capacity of each link u_k.

Output: ID of damaged components N_t^d and A_t^d after cascading failures

$t \leftarrow 1$
while True **do**
  Redistribute the flow to the failed nodes to the remaining functional links
  Check if each of the remaining links fails using Eq. (3) and store the ID of all failed links in A_t^d
  Check if each of the remaining nodes fails using Eq. (4) and store the ID of all failed nodes in N_t^d
  $t \leftarrow t+1$
  if $|N_{t+1}^d| = |N_t^d|$ & $|A_{t+1}^d| = |A_t^d|$ **then**
    Break
  end if
end while

initial flow of the adjacent link. For example, if link (i,j) fails, the flow redistributed to the adjacent link (i,v), Δf_{iv}, is given by

$$\Delta f_{iv} = \frac{f_{iv}}{\sum_{a \in V_i} f_{ia}} f_{ij}, \ \forall v \in V_i \tag{5}$$

where V_i is the set of outgoing neighbors of node i, i.e. nodes that have a link from node i; f_{ia} and f_{ij} are the flow along link (i,a) and (i,j), respectively. For each type of targeted attacks, the nodes are sorted in descending order according to the respective centrality and are attacked (removed) incrementally from the network. The procedure for simulating the cascading failures is described in Algorithm 1.

2.4 *Resilience Optimization*

2.4.1 *Resilience Measure*

Resilience of the interdependent networks at a time period t during the recovery, denoted as R_t, is defined as the weighted average of the percentage of satisfied demand in each individual network. Formally, R_t is given by Eq. (6).

$$R_t = \sum_{m \in M} w_m \left(\sum_{i \in N^m} 1 - \frac{s_{it}}{d_i} \right) \tag{6}$$

In Eq. (6), s_{it} is the slack (unmet demand) at node i at time t, d_i is the demand at node i, and w_m is the weight of network m. In our study, we assume an equal weight of each network (i.e., $w_m = \frac{1}{|M|}$, $\forall m \in M$).

Table 1. Notations

	Sets and indices
T	set of time periods, $t \in T$
M	Set of networks, $m \in M$
N, A	Set of all nodes and links respectively $i \in N$ and $k \in A$
N_{d+}	set of demand nodes
N^d, A^d	Set of damaged nodes and links respectively
$A^{m \to l}$	Set of interlinks from network m to l
N^m_{iter}	Set of nodes $\in N^l$ that require supply from N^m
	Parameters
c_i	Supply capacity of node i
d_i	Demand of node i
w_m	Weight of the resilience of network m
u_k	Flow capacity on link k
N_r	Maximum number of components repaired in a single time period
η_k	Conversion rate of resource flow from i to j on link $k = (i,j)$
ε	A sufficiently small positive number
	Decision variables
f_{kt}	Flow on link k at time t
q_{it}	Supply at node i at time t
s_{it}	Unmet demand at node i at time t
x_{it}	=1 if the repair of node i starts at time t; 0 otherwise
x_{kt}	=1 if the repair of link k starts at time t; 0 otherwise
y_{i0}	=1 if node i is not damaged; 0 otherwise
y_{k0}	=1 if link k is not damaged; 0 otherwise
y_{it}	=1 if node i functions at time t; 0 otherwise
y_{kt}	=1 if link k functions at time t; 0 otherwise
z_{it}	=1 if node i can receive supply at time t; 0 otherwise
z_{kt}	=1 if the start and end nodes of k and link k itself functions at time t; 0 otherwise
R_t	The resilience of ICIs at time t

2.4.2 *Notation*

The notations in Table 1 are used in formulating the resilience optimization problem.

2.5 *MIP for Resilience Optimization*

The model for optimizing the restoration of damaged ICIs is provided in Model (7). The objective function is to maximize the sum of resilience during the restoration horizon. The major decision variables include the dynamic network flow on links, supply at nodes, and the repair schedule.

$$\text{Max} \sum_{t\in T} R_t \tag{7a}$$

s.t.

$$\sum_{t\in T} x_{it} = 1,\ \forall i \in N^d \tag{7b}$$

$$\sum_{t\in T} x_{kt} = 1,\ \forall k \in A^d \tag{7c}$$

$$\sum_{i\in N} x_{it} + \sum_{k\in A} x_{kt} \le N_r,\ \forall t \in T \tag{7d}$$

$$\sum_{k=(i,j)\in A^m} f_{kt} - \sum_{k=(j,i)\in A^m} f_{kt} = q_{it} + s_{it} - d_i,\ \forall m \in M, i \in N^m, t \in T \tag{7e}$$

$$q^m_{it} \le \sum_{k=(j,i)\in A^{l\to m}} \eta_k f_{kt},\ \forall m \in M, i \in N^m_{\text{iter}}, t \in T \tag{7f}$$

$$0 \le f_{kt} \le y_{it} y_{jt} y_{kt} u_k,\ \forall k = (i,j) \in A, t \in T \tag{7g}$$

$$0 \le q_{it} \le y_{it} c_i,\ \forall i \in N, t \in T \tag{7h}$$

$$0 \le s_{it} \le d_i,\ \forall i \in N, t \in T \tag{7i}$$

$$x_{kt} \le x_{it},\ \forall i \in N, k = (i,j) \in A, t \in T \tag{7j}$$

$$y_{it} \le y_{i(t-1)} + x_{i(t-1)},\ \forall i \in N, t \in T\backslash\{1\} \tag{7k}$$

$$y_{kt} \le y_{k(t-1)} + x_{k(t-1)},\ \forall k \in A, t \in T\backslash\{1\} \tag{7l}$$

$$y_{i(t-1)} \le y_{it},\ \forall i \in N, t \in T \tag{7m}$$

$$y_{k(t-1)} \le y_{kt},\ \forall k \in A, t \in T \tag{7n}$$

$$y_{i1} = y_{i0},\ \forall i \in N \tag{7o}$$

$$y_{k1} = y_{k0},\ \forall k \in A \tag{7p}$$

$$y_{it}, y_{kt} \in \{0,1\},\ \forall i \in N, k \in A, t \in T \tag{7q}$$

$$x_{it}, x_{kt} \in \{0,1\},\ \forall i \in N, k \in A, t \in T \tag{7r}$$

In this model, constraints (7b) and (7c) ensure that damaged nodes N^d or links A^d will certainly be restored at one of the time periods. Constraint (7d) ensures that at most N_r damaged components can be restored at one time period. Constraint (7e) enforces flow conservation. Constraint (7f) guarantees that the supply at nodes dependent on another network is less than the converted supply. N^m_{iter} represents the set of nodes in network m that requires supply from another network. Formally, N^m_{iter} is given by

$$N^m_{\text{iter}} = \{i \in N^m \cap \{i' \mid \exists l \in M, (j,i') \in A^{l\to m}\}\} \tag{8}$$

Constraint (7g) ensures that the flow on each functional link is capped and the flow on a link will be zero unless the start node, end node, and the link itself are all functional. Constraints (7h) and (7i) define the range of supply and slack, respectively. Constraint (7j) states that an arc will not be restored until its start node is restored. Constraints (7k) and (7l) guarantee that nodes or links will be functional if it is repaired. Constraints (7m) and (7n) state that the functional state of components is non-deteriorating over the recovery process. Constraints (7o) to (7r) force the respective decision variables to be binary variables.

In constraint (7g), $f_{kt} \le y_{it} y_{jt} y_{kt} u_k,\ \forall k = (i,j) \in A, t \in T$ is non-linear. We linearize it using an auxiliary variable $z_{kt}, \forall k \in A, t \in T$. The equivalent linear constraints are given by

$$z_{kt} \le y_{it}, \forall k = (i,j) \in A, t \in T \tag{9a}$$

$$z_{kt} \le y_{jt}, \forall k = (i,j) \in A, t \in T \tag{9b}$$

$$z_{kt} \le y_{kt}, \forall k \in A, t \in T \tag{9c}$$

$$z_{kt} \ge y_{it} + y_{jt} + y_{kt}, \forall k = (i,j) \in A, t \in T \tag{9d}$$

For simplicity, we assume that only N_r damaged components can be repaired during a time period. Thus, the total time periods for

restoration is given by

$$|T| = \left\lceil \frac{\sum_{i\in N}(1-y_{it}) + \sum_{k\in A}(1-y_{kt})}{N_r} \right\rceil + 1 \tag{10}$$

where $\sum_{i\in N}(1-y_{it}) + \sum_{k\in A}(1-y_{kt})$ represents the total number of damaged components as $1-y_{it}=1$ or $1-y_{kt}=1$ if node i or link k is damaged, and 0 otherwise. $\lceil\cdot\rceil$ is the ceiling function that returns the least integer greater or equal to the input number. The additional one time period is added to ensure that the slack is zero, i.e. the resilience returns to 1, at the last time period. In this study, $N_r = 2$ is assumed for simplicity. In practice, a more accurate value of N_r can be determined based on information on the resources available to perform the repairs.

2.5.1 *Topology-based Resilience Assessment*

Topology-based models for resilience assessment only consider connectivity among network components. The topology-based resilience optimization problem is modeled by (i) *setting the capacity of flow and supply to a sufficiently large value in the flow-based optimization model*, and (ii) *modifying the objective function*. For the topology-based optimization problem, the resilience at time t, R'_t, is defined as the proportion of functional demand nodes that can still receive supply. Mathematically, topology-based resilience measure is defined as

$$R'_t = \frac{\sum_{i\in N_{d^+}\cap N_t^f} y_{it}}{|N_{d^+}|} \tag{11}$$

where $|N_{d^+}|$ represents the number of demand nodes (nodes with positive demand), and $\sum_{i\in N_{d^+}\cap N_t^f} y_{it}$ represents the number of functional demand nodes that can receive supply at time t. Because the slack at a functional demand that can receive supply must be lower than the demand, Eq. (11) is equivalent to

$$R'_t = \frac{\sum_{i\in N_{d^+}, s_{it}<d_i} y_{it}}{|N_{d^+}|} \tag{12}$$

In Eq. (12), determining whether or not the slack at a demand node is lower than its demand results in a logical constraint. We transform this logical constraint using an auxiliary variable $z_{it}, \forall i \in N_{d^+}, t \in T$, which is equal to 1 if $s_{it} < d_i$, and 0 otherwise. The equivalent linear constraints are

$$\frac{s_{it}}{d_i} \le 1 - \varepsilon z_{it} \tag{13a}$$

$$\frac{s_{it}}{d_i} \ge 1 - z_{it} \tag{13b}$$

In Eq. (13a), ε is a significantly small positive number. Using the auxiliary variable, the resilience measure for the topology-based model becomes

$$R'_t = \frac{\sum_{i\in N_{d^+}} z_{it}}{|N_{d^+}|} \tag{14}$$

3 Case study

3.1 *Data description*

We illustrate the proposed approaches with a case study of 49-node power-gas networks (Figure 1)[1]. The power-gas networks are generated by coupling the IEEE RTS 24-bus test system (left) with a 25-node gas network (right) through gas-powered generators (G1 to G4) (Zlotnik et al. 2016). Note that not all power generators require gas supply to produce electricity. For instance, the generators at K1, K2, and nodes with generators can have a demand for electricity as well. In the power network, there are 17 demand nodes, 5 supply nodes, and 34 links while in the gas

[1]The case study data and code to implement the models are available at: `https://github.com/jinzhuyu/ICOSSAR2021`

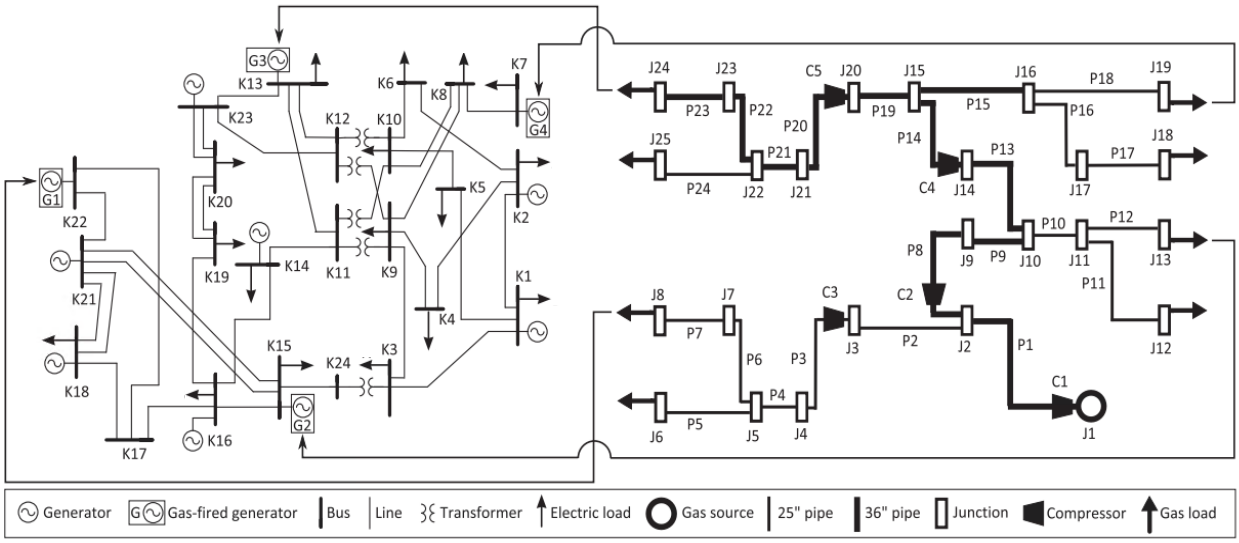


Figure 1. Schematic of 49-node coupled power-gas networks (Zlotnik et al. 2016)

network, there are 4 demand nodes, 1 supply node, and 24 links. The links across the two networks include the links from J8 to K22, J13 to K15, J24 to K13, and J19 to K7. The gas to power energy conversion rate is 172.47 (U.S. EIA 2020).

3.2 *Results*

We first explore the performance of networks, which is defined as the proportion of satisfied demand, after cascading failures (Figure 2). The tolerance rate is arbitrarily assumed to be 40%. Note that depending on the design capacity and the initial value of supply at nodes or flow along the links, the tolerance rate can be any positive number. Random attacks are simulated 50 times to obtain the average performance. As can be observed from Figure 2, random attacks can cause greater damage to network performance than all the targeted attacks when the percentage of nodes attacked is around 15% to 35%. When the proportion of nodes attacked is below 15%, betweenness-based attacks lead to the greatest loss in network performance, followed by random attacks. When more than 35% of nodes are attacked, degree-based attack is the most destructive. These observations indicate that depending on the attack intensity and the networks, ICIs can be more vulnerable to random attacks than intentional attacks. The trend in the deterioration of the performance as additional nodes fail is different for different attacks. The network performance after random and degree-based attacks first declines rapidly before slowing down. A similar trend can be observed for betweenness-based attacks. However, the inflection point occurs at a much lower value of the percentage of nodes attacked. In contrast, the deterioration rate of the performance given closeness-based attacks is more stable as a function of the increase in the percentage of attacked nodes.

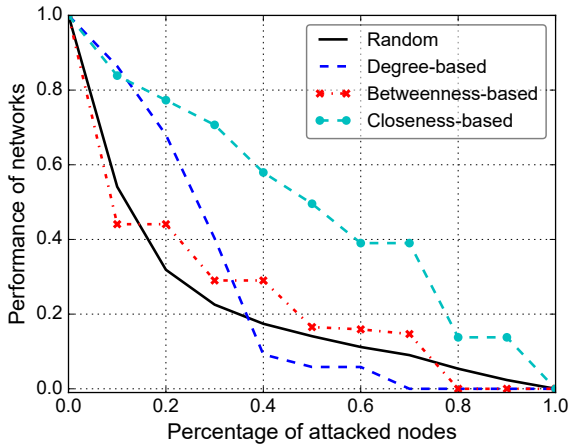
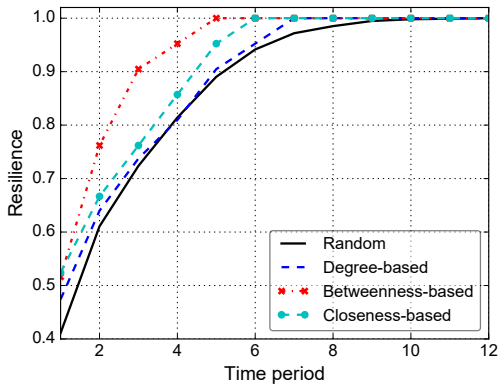
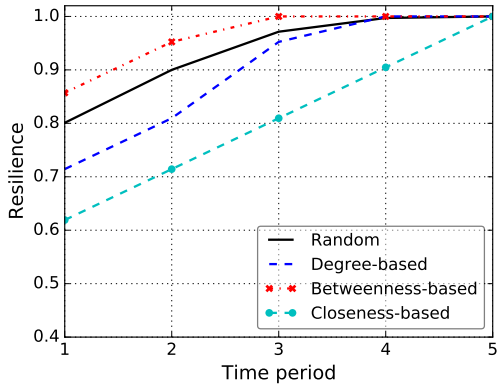


Figure 2. Performance of networks under different types of attacks

The resilience assessment of the 49-node power-gas networks after different types of



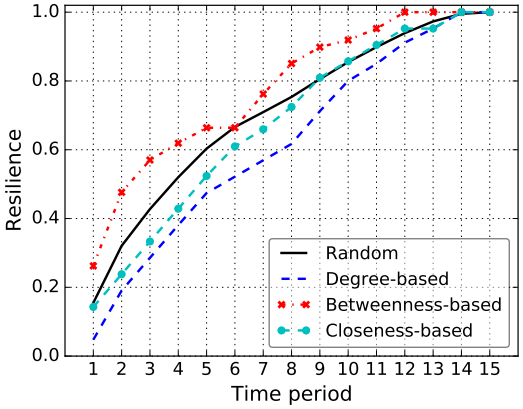
(a)



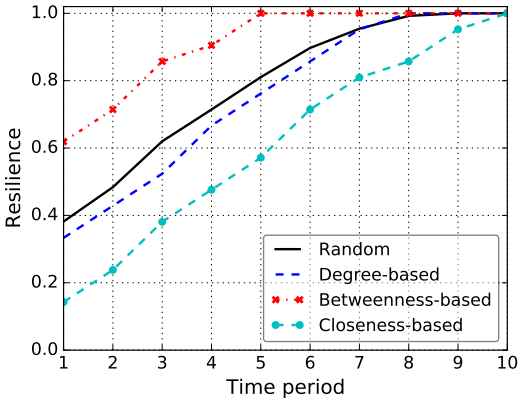
(b)

Figure 3. Restoration over time (a) flow-based and (b) topology-based models with 20% nodes attacked

attacks is depicted in Figure 3 (20% nodes attacked) and Figure 4 (60% nodes attacked). It can be seen that, irrespective of the attack type and percentage of nodes attacked, the resilience obtained using the topological model is consistently higher than the flow-based model and the time to full restoration is much shorter when using the topology-based model. These two observations indicate that topological models can overestimate the resilience and underestimate the time to full restoration of ICIs following disruptions, which may lead to increased restoration costs and even prolonged disruption (Yu & Baroud 2019). This is due to the fact that topological models ignore the network flow, therefore components will be considered to be functional although 1) the required flow is not provided or 2) the flow along a link or into a node exceeds the capacity. Furthermore, using topology-based models, the resilience of ICIs is consistently the highest after betweenness-based attacks, followed by random attacks, degree-based attacks, and closeness-based attacks. However, the ranking of resilience after different types of attacks using flow-based models are different over the percentage of nodes attacked. This observation also indicates that topology-based models can be misleading in the restoration management after the ICIs are damaged by different types of attacks.



(a)



(b)

Figure 4. Restoration over time (a) flow-based and (b) topology-based models with 60% nodes attacked

4 Conclusion

In this paper, we compare the resilience assessment of ICIs using flow-based and topology-based models after ICIs are damaged by different types of attacks. In estimating the damage state of ICIs, cascading failures are simulated using the dynamic flow

redistribution model. In evaluating the resilience of damaged ICIs, a MIP for the flow-based resilience optimization problem is developed and adapted for the topology-based problem. Considering the network performance following different types of attacks, we conclude that while ICIs are generally more vulnerable to targeted attacks than random attacks, ICIs may sometimes be more vulnerable to random attacks than targeted attacks, depending on the percentage of nodes attacked and the structure of the ICIs. By comparing the resilience assessment of ICIs using flow-based and topology-based models, we show that 1) the topology-based model tends to overestimate the resilience of ICIs and underestimate the time to full restoration, and 2) the resilience assessment of ICIs using topology-based models after different types of attacks can be misleading.

Future research can be conducted in several directions. First, since the physical laws on the power system and gas system are not included for simplicity of analysis, future work can incorporate the physical laws into the cascading failure simulation and restoration optimization to obtain a more accurate analysis. As there exist other flow distribution models, e.g. global flow redistribution models (Moreno et al. 2002, Yağan 2015, Scala et al. 2016), future research can also compare the cascading failures and the restoration after those failures using different flow redistribution rules.

5 References

Ahangar, N. E., Sullivan, K. M., & Nurre, S. G. (2020). Modeling interdependencies in infrastructure systems using multi-layered network flows. Computers & Operations Research, 117, 104883.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. Nature, 464(7291), 1025-1028.

Fang, Y. P., & Zio, E. (2019). An adaptive robust framework for the optimization of the resilience of interdependent infrastructures under natural hazards. European Journal of Operational Research, 276(3), 1119-1136.

Gao, J., Barzel, B., & Barabási, A. L. (2016). Universal resilience patterns in complex networks. Nature, 530(7590), 307-312.

González, A. D., DueñasOsorio, L., SánchezSilva, M., & Medaglia, A. L. (2016). The interdependent network design problem for optimal infrastructure system restoration. ComputerAided Civil and Infrastructure Engineering, 31(5), 334-350.

Goldbeck, N., Angeloudis, P., & Ochieng, W. Y. (2019). Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models. Reliability Engineering & System Safety, 188, 62-79.

Hagberg, A., Swart, P. & S Chult, D., 2008. Exploring network structure, dynamics, and function using NetworkX (No. LA-UR-08-05495; LA-UR-08-5495). Los Alamos National Lab.(LANL), Los Alamos, NM (United States).

Hines, P., Cotilla-Sanchez, E., & Blumsack, S. (2010). Do topological models provide good information about electricity infrastructure vulnerability?. Chaos: An Interdisciplinary Journal of Nonlinear Science, 20(3), 033122.

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47-61.

Johansson, J., & Hassel, H. (2010). An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering & System Safety, 95(12), 1335-1344.

Karakoc, D. B., Almoghathawi, Y., Barker, K., González, A. D., & Mohebbi, S. (2019). Community resilience-driven restoration model for interdependent infrastructure networks. International Journal of Disaster Risk Reduction, 38, 101228.

Moreno, Y., Gómez, J. B., & Pacheco, A. F. (2002). Instability of scale-free networks under node-breaking avalanches. EPL (Europhysics Letters), 58(4), 630.

Motter, A. E., & Lai, Y. C. (2002). Cascade-based attacks on complex networks. Physical Review E, 66(6), 065102.

Nan, C., & Sansavini, G. (2017). A quantitative

method for assessing resilience of interdependent infrastructures. Reliability Engineering & System Safety, 157, 35-53.

Ouyang, M. (2013). Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. Chaos: An Interdisciplinary Journal of Nonlinear Science, 23(2), 023114.

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. Reliability engineering & System safety, 121, 43-60.

Ouyang, M., & Wang, Z. (2015). Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. Reliability Engineering & System Safety, 141, 74-82.

Scala, A., Lucentini, P. G. D. S., Caldarelli, G., & DAgostino, G. (2016). Cascades in interdependent flow networks. Physica D: Nonlinear Phenomena, 323, 35-39.

Sun, J., & Zhang, Z. (2020). A post-disaster resource allocation framework for improving resilience of interdependent infrastructure networks. Transportation Research Part D: Transport and Environment, 85, 102455.

U.S. Energy Information Administration (EIA), `https://www.eia.gov/tools/faqs/faq.php?id=107&t=3:%20efficienty%200.4`, accessed: 2021-01-01, 2020.

Vespignani, A. (2010). The fragility of interdependency. Nature, 464(7291), 984-985.

Wang, W. X., & Chen, G. (2008). Universal robustness characteristic of weighted networks against cascading failure. Physical Review E, 77(2), 026101.

Wang, Y., Yu, J. Z., & Baroud, H. (2020). Quantifying the Interdependency Strength Across Infrastructure Systems Using Dynamic Network Flow Redistribution Model. Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference.

Yağan, O. (2015). Robustness of power systems under a democratic-fiber-bundle-like model. Physical Review E, 91(6), 062811.

Yu, J. Z., & Baroud, H. (2019). Quantifying Community Resilience Using Hierarchical Bayesian Kernel Methods: A Case Study on Recovery from Power Outages. Risk Analysis, 39(9), 1930-1948.

Yu, J. Z. (2020). Bayesian and Stochastic Network Methods to Model and Optimize the Resilience of Critical Infrastructure Systems. (Doctoral Dissertation). Vanderbilt University, Nashville, TN, USA.

Yu, J. Z., & Baroud, H. (2020). Modeling Uncertain and Dynamic Interdependencies of Infrastructure Systems Using Stochastic Block Models. ASCE-ASME J Risk and Uncert in Engrg Sys Part B Mech Engrg, 6(2).

Zlotnik, A., Roald, L., Backhaus, S., Chertkov, M., & Andersson, G. (2016). Coordinated scheduling for interdependent electric power and natural gas infrastructures. IEEE Transactions on Power Systems, 32(1), 600-610.

Zou, Q., & Chen, S. (2019). Enhancing resilience of interdependent traffic-electric power system. Reliability Engineering & System Safety, 191, 106557.