Modelling Robustness of Critical Infrastructure Networks

Srinath Pinnaka, Rajgopal Yarlagadda, and Egemen K. Çetinkaya
Department of Electrical and Computer Engineering
Missouri University of Science and Technology, Rolla, MO 65409, USA
{sp4h9, rywd5, cetinkayae}@mst.edu
http://web.mst.edu/~mstconets

Abstract—Critical infrastructure networks are becoming increasingly interdependent. An attack or disaster in a network or on a single node in a network will affect the other networks dependent on it. Therefore, it is important to assess and understand the vulnerability of interdependent networks in the presence of natural disasters and malicious attacks that lead to cascading failures. We develop a framework to analyse the robustness of interdependent networks. Nodes and links in the interdependent networks are attacked based on the graph centrality metrics. We apply our framework on critical infrastructure network data. Our results indicate that the importance of critical infrastructure varies depending on the attack strategy.

Keywords—critical infrastructure, interdependent networks, directed graph, cascading failures, resilience, robustness, centrality.

I. INTRODUCTION AND MOTIVATION

The structure of a network of networks is comprised of complex infrastructures emphasising the importance of interdependency. An interdependency is a mutual relationship between two networks, which means the functionality of one network is influenced by another network. Critical infrastructures, such as transportation systems, communications, and power grid are some of the examples of networks that are mutually dependent on the connectivity of each other [1]. In such interdependent networks, when nodes in one network fail, they may lead to the failure of dependent nodes in both the same network as well as other networks, leading to a cascade of failures [2]. The 2003 Northeast US power blackout [3] and the 2003 Italy power blackout [4] are canonical examples of cascading failures in which failure of a critical infrastructure results in cascading effect of failures on other critical infrastructures. For interdependent networks to be resilient and survivable to attacks, the design of such infrastructure must optimise principles such as heterogeneity and diversity [5], [6].

An important property that one should consider in analysing and designing interdependent systems, is their robustness to cascading failures. Many tools have already been developed to study cascading failures, thus providing insight into the behaviour of individual infrastructure networks. A far more neglected area is that of the interdependency among multiple infrastructure networks, including potential cascading effects [7], [8]. Attackers can exploit potential vulnerabilities, causing a cascade of failures in interdependent networks.

Despite extensive research on cascading failures in such complex networks, the dynamic behaviour of such attacks and random failures is not well understood [9]. The existing approaches for single networks are based on various metrics, such as the degree of suspected nodes or edges, global clustering coefficients, and pairwise conductivity. However, the performance of the existing approaches drop tremendously when interdependent networks are considered. This is because the approaches are proposed in such a way that they are meant for individual networks or configuration models since these metrics fail to capture the cascading failures in interdependent networks [10].

In this paper, we develop a graph-theoretic framework to analyse robustness of interdependent networks. We model interdependencies between nodes in a network as a directional graph. We apply US critical infrastructure network data to our framework to analyse the robustness under targeted attacks. The important nodes and links in interdependent networks are determined using graph centrality metrics. We show that the rankings of critical nodes vary over different attack strategies. This framework can help us understand and study the resilience of complex interdependent networks.

The paper is organised as follows: The framework on the critical infrastructure is presented in Section II. The topological dataset is presented in Section III. In Section IV, we present our experimental results to understand the effect of elemental removal in an interdependent network, then we conclude and showcase some probable future work in Section V.

II. FRAMEWORK

In this section, we explain the methodology to analyse the interdependent networks. We build our framework using the Python NetworkX library [11]. We consider the flow robustness to evaluate the resilience of interdependent networks. Flow robustness of a network is a measure to compute the connectivity of the network [8] and it is the ratio of number of flows to the total number of possible flows in a network. Every time a node is removed from the network, the flow robustness is calculated and normalised with the total number of flows of the network, which is \( n(n - 1) \), where \( n \) is the number of nodes in a network. However, calculating the flow robustness also depends on the node that is being removed from the
network. That is, after removing a node, if the entire network is connected, the aforementioned method will act. If the network is not connected, then the possible number of flows in each subnetwork are calculated separately and are summed up in order to get the aggregate number of flows in the network. In our framework, the calculation of robustness is adaptive [2], which means after every attack, the flow robustness of the network is recalculated considering the centrality values at each iteration. Attacks on a network can either be on a node or on an edge.

The fundamental approach of our framework is to analyse the cascading failures of nodes and edges based on graph metrics. To compute the robustness of the critical infrastructure, we attack the nodes based on the graph centrality metrics. We model interdependent networks as directed graphs. After each attack, we calculate the flow robustness, compare with the result of the previous attack, and analyse the remaining flows of the interdependent networks. This shows the best possible way for an attacker to attack the network. There are several metrics to characterise the structure of a network; however, the targeted attacks on the critical infrastructure are based on the centrality metrics since centrality explains how important a node is in a network [12]. We use degree centrality, closeness centrality, betweenness centrality, and eigenvector centrality to explain node characteristics in a network as these centralities—when combined effectively—discover the critical nodes in a network. Next, we explain the four centrality metrics that are used in our framework:

1) **Degree Centrality**: The degree of a node refers to the number of incident edges it has. Degree centrality is the normalised node degree. The node degree is normalised with \( n - 1 \), where \( n \) is the total number of nodes in the network. However, in directed graphs, there will be in-degree centrality and out-degree centrality. The in-degree centrality is the normalised value of the total number of incoming connections to that particular node. Similarly, out-degree centrality is the normalised value of the total number of outgoing connections from that particular node. We consider the normalised value of node degree for degree centrality because there is a difference between the degree of a node and the degree centrality of a node. We choose degree centrality over degree because it enables us to evaluate different order and size networks in our future work.

2) **Closeness Centrality**: Closeness centrality describes how close a node is to all other nodes in the network. It is measured as a reciprocal of fairness. The fairness is the sum of the shortest paths from that particular node to all other nodes in the network. As the sum of the distances from all other nodes depends on number of nodes in the network, closeness centrality is normalised with \( n - 1 \) [13].

3) **Betweenness Centrality**: This metric describes how central a node is, compared with all other nodes in the network. It is...
the ratio of shortest path through a node or through an edge over the total number of shortest paths in that network. It is also a normalised value [13].

4) Eigenvector Centrality: Eigenvector centrality is based on the concept that a node is important if it has richly connected neighbours. It measures the importance of a node based on its connections to the high degree nodes in the network.

III. TOPOLOGICAL DATASET

We apply our framework on the US critical infrastructure network in which critical sectors are dependent on each other. Interdependency means the sectors are mutually dependent on each other i.e., there is a bidirectional relationship between two sectors, whereas dependency is a unidirectional relationship. We construct the interdependency graph based on the designated critical sectors by the Department of Homeland Security (DHS) [14]. In this graph, we designate each sector as a node and the connectivity between the sectors as directed links. If there is an interdependency (i.e. mutual dependency) between two sectors, then we designate this as a bidirectional link. If a sector is dependent on another, but this dependency is not mutual then we designate this relation via an unidirectional link. The US critical infrastructure network is shown in Figure 1 with 16 nodes (i.e. sectors) and 113 links including unidirectional and bidirectional links. The red arrows indicate mutual interdependency of the sectors whereas the black arrows indicate dependency of one sector on another sector, as shown in Figure 1. For example, there is a mutual dependency between the “communications” and “energy” sectors. The “transportation systems” sector depends on “communications” sector, but this dependency is unidirectional (i.e. communications does not rely on the transportation systems).

IV. RESULTS

We apply the critical infrastructure graph on our framework that analyses interdependent networks. Nodes and links are removed adaptively based on the centrality metrics. We evaluate robustness as a measure of network resilience.

The effect of attacks on the nodes based on their degree, closeness, betweenness, and eigenvector centrality is shown in Figure 2. We see that all the node centrality attacks have an equal impact on the critical infrastructure for the first eight node attacks. Degree centrality and betweenness centrality equally eliminates the total flows completely in the critical infrastructure with the fewest number of attacks (11 sectors needed to be removed). Although both degree centrality and betweenness centrality eliminate the total critical infrastructure with equal number of attacks, degree centrality has a greater effect because removing a node with higher interdependencies results in the removal of a large number of flows.

We also rank the 16 critical infrastructure sectors based on the centrality measure as they are being removed from the interdependent network, as shown in Table I. For example, based on the degree centrality (shown in Column 2 in Table I), energy is removed first since this sector has the highest degree centrality measure. Then in the remaining graph, we calculate the degree-centralities again and remove the water systems next. The ranking process continues until all 16 sectors are ranked based on a centrality measure. The ranking of sectors based on closeness, betweenness, and eigenvector centralities are shown in columns 3, 4, 5 of the Table I, respectively.

Based on the degree centrality and eigenvector centrality, we have observed that energy, water and wastewater systems, communications, IT, and transportation systems are more critical than the other infrastructures. However, we see a different result when closeness and betweenness centralities are analysed. The ranks of the sectors differed quite significantly when compared with the other centrality results. We believe that this phenomenon is explained by their definitions where degree centrality and eigenvector centrality refer directly to number of nodes and the popularity of nodes to which a particular node is connected. Closeness centrality describes how close a node is to the other nodes which does not necessarily mean it is dependent on majority of the nodes in the network. Betweenness centrality is the fraction of shortest
paths between all the nodes in a network, which does not mean it is linked to most of the nodes. We plan to investigate these centralities further and present the results in our future work.

The impact of adaptive attacks on the critical infrastructure network based on node and edge centrality metrics is shown in Figure 3. The node-centrality attacks impact the flow robustness at a much higher rate compare to edge betweenness attack since removing a node disconnects all the incident edges connected to that node. Moreover, as soon as a node is removed, we can see the degradation in flow robustness immediately, whereas it takes 51 links to be removed to see flow robustness degradation in this critical infrastructure network. However, in some cases, removing a targeted link can degrade the flow robustness more drastically than removing a node.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we developed a framework to analyse interdependent networks. We have modelled the interdependent US critical infrastructure graph as a directed graph and studied its robustness under targeted attacks. Based on the four centrality metrics, we conclude that energy is the most critical sector in this interdependent network. However, the critical node of a network varies depending on the centrality metric we choose. An attack on the sectors in the critical infrastructure graph impacts the robustness more than an attack on the links between the sectors.

Our framework focuses on the analysis of critical infrastructure network with 16 nodes, it is flexible and can be applicable to any network with any number of nodes and edges. Our future work aims to design and optimise these critical infrastructure networks.

ACKNOWLEDGMENT

We would like to acknowledge members of the CoNetS group for discussions on this work. We thank Rebecca J. Crosthwait for feedback on an early draft of this paper.

REFERENCES


TABLE I

<table>
<thead>
<tr>
<th>Rank</th>
<th>Degree Centrality</th>
<th>Closeness Centrality</th>
<th>Betweenness Centrality</th>
<th>Eigenvector Centrality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Energy</td>
<td>Food and agriculture</td>
<td>Energy</td>
<td>Energy</td>
</tr>
<tr>
<td>2</td>
<td>Water and wastewater systems</td>
<td>Energy</td>
<td>Water and wastewater systems</td>
<td>Communications</td>
</tr>
<tr>
<td>3</td>
<td>Communications</td>
<td>Emergency services</td>
<td>Critical Manufacturing</td>
<td>IT</td>
</tr>
<tr>
<td>4</td>
<td>IT</td>
<td>Healthcare and public health</td>
<td>Commercial facilities</td>
<td>Water and wastewater systems</td>
</tr>
<tr>
<td>5</td>
<td>Transportation systems</td>
<td>Commercial facilities</td>
<td>Food and agriculture</td>
<td>Critical Manufacturing</td>
</tr>
<tr>
<td>6</td>
<td>Food and agriculture</td>
<td>Critical manufacturing</td>
<td>Chemicals</td>
<td>Transportation systems</td>
</tr>
<tr>
<td>7</td>
<td>Critical manufacturing</td>
<td>Defense industrial base</td>
<td>Transportation systems</td>
<td>Chemicals</td>
</tr>
<tr>
<td>8</td>
<td>Chemicals</td>
<td>Chemicals</td>
<td>Healthcare and public health</td>
<td>Dams</td>
</tr>
<tr>
<td>9</td>
<td>Emergency services</td>
<td>Financial services</td>
<td>Emergency services</td>
<td>Food and agriculture</td>
</tr>
<tr>
<td>10</td>
<td>Healthcare and public health</td>
<td>Nuclear</td>
<td>IT</td>
<td>Healthcare and public health</td>
</tr>
<tr>
<td>11</td>
<td>Commercial facilities</td>
<td>Transportation systems</td>
<td>Communications</td>
<td>Emergency services</td>
</tr>
<tr>
<td>12</td>
<td>Dams</td>
<td>Government facilities</td>
<td>Financial services</td>
<td>Financial services</td>
</tr>
<tr>
<td>13</td>
<td>Financial services</td>
<td>Water and wastewater systems</td>
<td>Government facilities</td>
<td>Government Facilities</td>
</tr>
<tr>
<td>14</td>
<td>Nuclear</td>
<td>Dams</td>
<td>Nuclear</td>
<td>Nuclear</td>
</tr>
<tr>
<td>15</td>
<td>Government facilities</td>
<td>Communications</td>
<td>Dams</td>
<td>Commercial facilities</td>
</tr>
<tr>
<td>16</td>
<td>Defense industrial base</td>
<td>IT</td>
<td>Defense industrial base</td>
<td>Defense industrial base</td>
</tr>
</tbody>
</table>