Towards more robust internetworks:  
an application of graph theory

Authors
Jamie Greenwood, MSc (Royal Holloway, 2016)  
Stephen Wolthusen, ISG, Royal Holloway

Abstract
As networks become increasingly connected to and dependent upon one another, the size and complexity of the resulting internetworks are increasing. This poses a threat to the security and functionality of these networks. In this article we explain how graph theory can be used to model internetworks and improve their resilience against failures and attacks. We evaluate the robustness of various internetwork configurations when subject to targeted attacks. Our results show that one configuration more successfully retains network functionality, whereas another retains close connectivity. This trade-off between functionality and connectivity is particularly relevant to the specific application of the network.

Introduction
In a world where technology is becoming more abundant than ever before and convenience is sought after in everyday life, consumers and services are becoming increasingly connected to provide a better all-round experience. These services are provided via networks where information or physical resources are exchanged. For example, an online message is relayed through a network of routers and cables before arriving at its destination, just like water is distributed through a network of reservoirs and pipelines. Where a network may have once operated independently of other networks, it is now common to have a collection of interacting networks, also known as an internetwork.

Networks can range from biological processes (such as neural networks) to economic systems and transportation networks. They also include, perhaps most importantly, utilities such as electricity, telecommunications, water, oil and gas supply networks. These networks can interact with one another in a variety of different ways. Connections between them result in complex internetworks where the successful operation of one network may implicitly depend on that of another.

In the modern day individuals and businesses rely on the constant functioning of internetworks to provide a range of services at all times. However, as internetworks expand, so does the possibility of failure, and these failures can have severe repercussions across the entire internetwork. It is frightening to see how easily these large internetworks can be disrupted by a simple attack or a random failure. Because of this, there is a desire to find ways of constructing more robust internetworks - those that can more successfully continue to operate in adverse circumstances - in order to minimise the number of disruptions and security issues, along with their associated costs.

Using a branch of mathematics known as graph theory, we can model these complex internetworks, predict attack scenarios and failures, realise the potential damages to the networks and explore methods of strengthening them. This article discusses how we can do this by outlining the process behind
our investigation, and summarising some of the key results.

**What is graph theory and why is it relevant?**

Simply put, graph theory is the study of mathematical graphs consisting of nodes. These nodes are connected via links, which define relations between the nodes.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nodes</strong></td>
<td><strong>Links</strong></td>
</tr>
<tr>
<td>Customers</td>
<td>Internet connections</td>
</tr>
<tr>
<td>Processing facilities</td>
<td>Telephone lines</td>
</tr>
<tr>
<td>Servers and databases</td>
<td>Virtual connections</td>
</tr>
<tr>
<td>PCs and mobile phones</td>
<td>Electricity, water and gas supplies</td>
</tr>
<tr>
<td>Residences and buildings</td>
<td>Flow of resources</td>
</tr>
<tr>
<td></td>
<td>Dependencies on a service</td>
</tr>
</tbody>
</table>

Table 1: *Real-world examples of nodes and links.*

We use two distinct types of link: connectivity links and dependency links. Connectivity links are undirected, representing a two-way connection between components. Dependency links are directed and indicate a dependency between nodes - node A is said to depend on node B if a link is directed from node B towards node A. Using graphs, we can represent real-world networks and their interactions. An example can be seen in Figure 1.

![Internetwork showing the dependencies between simplified electricity and water networks](image)

Figure 1: *An internetwork showing the dependencies between simplified electricity and water networks, illustrated as a graph model with directed dependency links.*

By abstracting these networks, we can then calculate various graph metrics over the network. This allows us to quantify desirable network properties and, most importantly, determine the robustness of the network.

One of the simplest ways to measure network robustness is to observe the number of nodes that remain operational after a failure or attack. This measure of network functionality gives a global per-
spective of how resilient the network is. Likewise, the number of connections that each node has can be compared before and after an attack. This can be calculated as an average node degree across the network. If a network retains most of its degree then it could be considered robust.

Other key metrics make use of the distances between nodes - the minimum number of links that must be traversed from one node to the other. The average distance for a single node can be calculated by taking the mean of the distances to reach every other node. Typically, a network is considered more robust if the average distance for each node remains small in adverse circumstances. This shows that nodes are still tightly connected, whilst larger values indicate that the network has become fragmented and alternative routes must be taken.

We have only highlighted a few simple metrics here but there are many more of varying complexities. There is no single best graph metric to measure network robustness - each can be used to evaluate a different aspect of network robustness, and some may be more relevant than others depending on the network in question.

**Modelling a realistic internetwork**

Theoretical results from graph theory can provide precise information on how resilient an isolated network is from a particular type of attack, though unfortunately many of these results are not applicable to internetworks. However, due to the computing power that is available nowadays, we can instead run large scale simulations on these abstract networks to test their robustness in various scenarios.

But why bother with this when we can evaluate network security and put safeguards in place? Securing a network is a task in itself, but securing other networks within the internetwork may be impossible, depending on who has control and ownership of them. For this reason, it is best to assume that attacks will happen, and failures will always occur - no matter how secure the individual components are, they are always prone to mechanical failures or operator errors. When a component in a network does fail for whatever reason, ideally the structure of the internetwork will limit the amount of damage done.

Simulations on graph models can provide an insight into how similar, real-world networks may react to these attacks or failures. By tweaking these model and repeating simulations, we can identify changes to the network that may increase its overall resilience or safeguard specific components.

In order to run these simulations, we require realistic network models such that any improvements to their robustness remains applicable to real-world networks. One of the key observations found throughout academic literature is that the majority of real-world networks tend to be scale-free. An illustration of a scale-free network can be seen in Figure 2.

In order to create graph models of networks on a large scale, an algorithm is needed to procedurally add new nodes and links - this governs the properties of the graph model, which ideally need to closely match those observed in real-world networks. A preferential attachment method is incorporated to generate scale-free models with hub nodes - those nodes with a larger number of links are more likely to attain future connections than those with a small degree.

Once sufficiently realistic isolated networks have been produced, they must be connected to each other to form an internetwork. These interconnections may be in the form of connectivity and/or dependency links. This leads onto the main part of our investigation, where we experiment with ways in which we
Figure 2: Graph model of a scale-free network with clearly visible hub nodes.

can connect these scale-free networks together to form an internetwork.

Investigating internetwork configurations

An ideal internetwork, in terms of robustness at least, would require that every node wishing to connect to nodes in other networks does so via a direct link. This would allow for maximum functionality. However, this is clearly not viable due to geographical, technological, virtual and financial constraints. Instead, it is more common that nodes are connected via multiple intermediary nodes. This poses the risk that if any of the intermediary nodes are disrupted, two interconnecting nodes will no longer be connected.

To investigate how best to create interconnections between networks, we consider two distinct problems: designing suitable structures in which networks within the internetwork are connected, and choosing which nodes from a network to interconnect.

For the first problem we design four internetwork configurations, each one able to scale up to a larger number of networks within the internetwork, with some inspiration drawn from real-world internetworks. Figure 3 shows a graphical representation of the four configurations, with \( n \) networks represented by the indices of \( G \). Black links are direct interconnecting links, whereas coloured links indicate the use of an intermediary network.

1. **Direct configuration**: A typical internetwork with no formal structure, resulting in a complex network with unpredictable behaviour.

2. **Ring configuration**: Only neighbouring networks interconnect. This can represent network connections limited by geographical distance, for example.

3. **Star configuration**: Taking inspiration from the Internet, which is commonly a central network for other networks to interact with, this star-like configuration results in all interconnections passing through the central network \( (G_1) \).

4. **\((n-1)\)-regular configuration**: We define a secure intermediary network \( (G_r) \) without any dependencies, such that it always remains functional and acts as a bridge between the other \( n \) networks. This secure, central network consists of only \( n \) nodes, each with \( n-1 \) links connecting to the other nodes in the network. This configuration reduces the average distances between nodes, as there always exists a direct route through the intermediary network.
To address the second problem, three different methods of choosing interconnecting nodes are considered:

- Random - interconnecting nodes are chosen at random.
- Degree-similar - randomly chosen nodes are linked to nodes sharing a similar degree.
- Preferential attachment - hub nodes are more likely to be chosen.

The final method is most relatable to real-world internetworks, where hub nodes are a likely point of interconnection, since they can provide a more direct link to a larger number of nodes on that network.

Attacking an internetwork model

There are many ways of removing nodes and links in an attack. For example, in a mobile data network, the nodes may represent satellites and mobile phones that can be remotely controlled, whilst in a physical network such as a water pipeline infrastructure, the pipes could be physically damaged or tampered with. When nodes are removed on a graph model, this does not necessarily mean they stop functioning. Instead, the model can be used to simulate how a hacker can take control of a computer network, where nodes that are removed indicate computers or servers that the hacker has access to.

A variety of different attack scenarios can be considered - these can range from random component failures to targeted attacks. These attack models can be specifically tailored depending on who the attacker is, what intelligence they possess and what their objectives are. We only consider two simple attack strategies here: removing a random fraction of nodes and removing a fraction of nodes with the highest degree. In both cases, when a node is removed so are all of its incident links. More complex attack models could include simultaneous attacks and logical decisions based on the outcome of previous attacks.

In general, a node is considered operational if it remains connected at least one other node - the exception to this is when a node is dependent upon another node. If the dependency link is broken, the dependent node becomes inoperable and loses all other incident links. The removal of such dependency links can cause widespread cascading failures over an internetwork, where a single well-chosen removal may propagate disruption across the internetwork. An example of this can be seen on a small scale in Figure 4, where two networks are connected via a connectivity link and a dependency link (where the right-hand node depends on the left-hand node) before being disrupted.

For each network configuration and attack model considered, a number of metrics are measured before and after the attack, giving an indication of the resulting internetwork robustness. This entire process is repeated for multiple simulations of the same scenario, in order to produce meaningful results.
Experimental results

Analysis of the robustness metrics produce interesting results, some of which have not been previously documented. When investigating internetwork configurations, the star configuration displays a consistently higher network functionality than other configurations when subject to degree-based node removal (see Figure 5). After repeating these simulations with a larger number of networks within the internetwork, we observe that network functionality does not significantly differ in the star configuration, whereas in all others it significantly deceased. This result is particularly important because the number of networks within the internetwork usually has a drastic effect on internetwork robustness, since there are more points of failure. Consequently, this internetwork design may be a preferred choice if connectivity between network components is of utmost importance, especially in a growing internetwork.

Although the \((n - 1)\)-regular configuration appears to be less functional than others, it does display significantly lower average path lengths than all other configurations. Also, the resulting \((n - 1)\)-regular internetworks appear to be far more densely connected. This design may be preferable if maintaining a number of nodes within a set distance is more important than the overall number of connected nodes - for example, if the application require a very small latency.

For the second part of the investigation, statistical analysis shows that the choice of interconnecting nodes does not significantly affect overall internetwork robustness when subject to degree-based node removal. However, the preferential attachment method leads to a larger network functionality in some specific simulations. In these simulations, the models possess slightly more hub nodes, and so after the attack more of these nodes remain operational. This results in a greater number of functional interconnecting nodes, which contributes to higher network functionality and shorter average path lengths. From this we can hypothesise that a preferential attachment method would produce more robust internetworks, as long as the highly connected hub nodes are sufficiently protected such that they are not removed in an attack.

Our results show the benefits of both the star configuration and the \((n - 1)\)-regular configuration. We also highlighted the apparent trade-off between network functionality and dense network connectivity. This should be of consideration when designing networks and their applications. It is hoped that future research in this area will help to design internetworks that remain both highly functional and densely connected after an attack.

Closing remarks

As we become increasingly reliant on instant access to everyday services and worldwide communication, it is important to consider the potential vulnerabilities of expanding these already complex
internetworks. Where organisations once had to secure only their own network, they now heavily rely on other networks that they are connected to and/or depend upon - this means that vulnerabilities outside of their control can directly or indirectly affect their service. Attacks and unforeseen failures on these large internetworks can have knock-on effects that ultimately disrupt more people and services than ever before, so it is in our best interest to protect these networks wherever possible.

Although it is not economically or physically viable to alter most internetwork structures, the implications of graph theory can still help to strengthen these existing networks, whilst providing more robust designs for future internetworks. The design of robust internetworks is crucial to the smooth and successful operation of everyday processes and services, and the development and application of graph-based modelling will continue to contribute to such designs.

**Biographies**

*Jamie Greenwood* received his BSc (Hons) degree in Mathematics and its Applications from Cardiff University in 2015, and went on to graduate from Royal Holloway, University of London in 2016 with an MSc in Information Security with distinction. His interests include cryptography, network security and attack modelling. He is currently exploring options to embark on a career in the cyber security industry.

*Stephen Wolthusen* received his Dipl.-Inform. degree in computer science in 1999 and completed his Ph.D. in theoretical computer science in 2003, both at TU Darmstadt. He is currently a Reader with the ISG, and also Full Professor of Information Security (part-time) at the Norwegian University of Science and Technology, Norway. His research focuses on models of adversaries and resilient networks, with applications in defence networks and particularly in critical infrastructure networks and control systems security. He has led a number of national and European projects, including the Internet of Energy project. He is author and editor of several books, as well as over 130 peer-reviewed publications, and is currently vice-chair of the IEEE Task Force on Network Science.