Multi-Level Resilience: Reconciling Robustness, Recovery and Adaptability from a Network Science Perspective

Mehdi Khoury, School of Electronics and Computer Science, University of Southampton, Southampton, UK

Seth Bullock, School of Electronics and Computer Science, University of Southampton, Southampton, UK

ABSTRACT

From a multi-disciplinary point of view, research on resilience focuses on robustness, recovery, and adaptive capacity. Robustness quantifies how much damage a system can take before it breaks, whereas recovery refers to the ability of a system to recuperate within limits of time and resources, and adaptability requires a system to be able to structurally reorganize throughout time so as to improve its chances of survival when facing disturbances. In this paper, after discussing examples of models of robustness, recovery and adaptability from different scientific disciplines, is a discussion on the relationship between these three aspects of resilience, introducing a multi-level resilience hierarchy with which to relate them to each other which is termed the resilience pyramid. This paper then exemplifies this multi-level view of resilience through discussing the resilience of symbiotic networks to cascading failure in the context of modern infrastructures, and considers the introduction of infrastructure nodes with permutable roles as a possible solution.

Keywords: Adaptability, Recovery, Resilience, Robustness, Symbiotic Interdependency

1. INTRODUCTION

Resilience can be broadly defined as the ability of systems to survive and thrive under adverse conditions. However, a general understanding of the mechanisms underpinning resilience is still elusive (Deffuant & Gilbert, 2011; Hollnagel, Woods, & Leveson, 2006). Domain-specific research has tended to consider many different measures of resilience, which ultimately involve three primary aspects: robustness, recovery, and adaptive capacity. Robustness quantifies how much damage a system can withstand before it breaks. It is often characterised in terms of a threshold or limit beyond which a system fails to function. Recovery refers to the ability of a system to recuperate, heal or self-repair, within some limits of time and resources. It is usually quantified in terms of the speed with which a system recovers from a disturbance, and sometimes also the cost of this recovery. Adaptability requires a system to be able to structurally change or reorganise over time such that it tends to improve its chances of

DOI: 10.4018/ijaras.2014100103

Copyright © 2014, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
surviving further disturbances. These three primary aspects of resilience are first presented, and then linked by a generalizable hierarchical relationship defined in this paper as the resilience pyramid. This multi-disciplinary view of resilience is exemplified through a discussion introducing the resilience of symbiotic interdependent networks to cascading failure in the context of modern infrastructures featuring elements with permutable roles.

2. ROBUSTNESS, RECOVERY AND ADAPTABILITY AS BUILDING BLOCKS OF RESILIENCE

The idea of resilience originates from disparate fields and is not yet clearly defined in a trans-disciplinary fashion (Deffuant & Gilbert, 2011; Hollnagel et al., 2006). This lack of conceptual cohesion can be problematic when trying to understand the resilience of, e.g., heterogeneous infrastructures which themselves reflect an amalgam of different engineering, economic and social science paradigms. Although the models and definitions employed across these disciplines vary widely, they can be organised along thematic lines that reveal core aspects of resilience at a basic conceptual level. In this section, we list some examples of resilience language used by different disciplines, highlighting a degree of conceptual resonance that distinguishes three specific aspects of resilience: robustness, recovery and adaptability.

2.1. Models of Robustness

Robustness is the most studied aspect of resilience, and is a measure used by default across many different disciplines. In materials science, resilience is defined in terms of elastic potential energy, i.e., the ability of a material to store energy when it is stretched or compressed. This approach equates resilience with a notion of robustness, an ability to withstand stress without failing, which can be represented by the area under the stress-strain curve (Avallone, Baumeister, & Sadegh, 2006) as shown in Figure 1. Under this reading of resilience, more resilient materials will be able to tolerate a greater degree of stress or compression before breaking. Resilience is associated with a threshold: the material’s elastic limit. By contrast, the process of successful elastic recovery that takes place when some previously stressed material regains its original shape is at best only implicit in the resilience story and is consequently downplayed under this picture of resilience. Moreover, a notion of material adaptation where materials reorganise such that they are better prepared for future stress or compression events is entirely absent from this account, at least in its typical, basic formulation.

Analogously, within network science, a network’s resilience is typically associated with the maximum amount of disruption that it can withstand before its largest connected component disappears (i.e., the number of nodes in the largest surviving network fragment approaches unity). This view from percolation theory (Albert, Jeong, & Barabási, 2000; Callaway, Newman, Strogatz, & Watts, 2000; Cohen & Havlin, 2002; Latora & Marchiori, 2005) understands resilience in terms of the fraction of the system that survives a shock or attack. It assumes that the larger the size of the largest surviving connected component, the higher the chances of the network performing as required and therefore the greater its resilience (Najjar & Gaudiot, 1990). If we measure the area under the curve representing how the average size of the largest connected network component varies with the size of the disturbance suffered by the network (in terms of the percentage of nodes attacked) we obtain a model of resilience as robustness to perturbation that is strongly analogous to the materials science view discussed above (see Figure 1).

Resilience is again associated with the failure threshold of a static structure. Again, there is little attention given to some process of recovery that could reconnect the network, or to processes of adaptive reorganisation that could lead to the configuration of a more resilient network (a reorganised network would likely
be treated as simply a different static network structure).

Resilience is also framed in terms of robustness across many other fields and disciplines, such as controllability theory, ecology, social sciences, economics, and the study of transport and power transmission systems, although the models employed are different in many respects. In controllability theory, robustness is the maximum amount of disruption a network can take before the remaining number of controller or “driver” nodes needed to maintain full-control of the network is insufficient. Identifying how many driver nodes are needed and where they are in the network ensures controllability (Liu, Slotine, & Barabási, 2011). In ecological modelling, robustness is defined as the size of a disturbance needed to dislodge a system from a stability domain (Holling, 1973). Similarly, socio-ecological models define robustness as “latitude”: the maximum amount by which a system can be changed before losing its ability to recover (Walker, Holling, Carpenter, & Kinzig, 2004). In economics, robustness is the maximum amount of perturbation caused by the loss of a particular type of local industry or employer that the local economy can take before losing function, employment, and prosperity (Jansen et al., 2007). Analogously, in the study of transport systems robustness is quantified as the maximum disturbance from which the system can recover (Berdica, 2002). A final example of the conceptual resonance of robustness can be found in the study of power transmission systems where resilience is assimilated to robustness in quantifying the maximum amount of disturbance a system can take before submitting to the effects of cascading failure (Albert, Albert, & Nakarado, 2004; Baldick et al., 2009).

2.2. Models of Recovery

Recovery is an aspect of resilience found in various domains within the natural and social sciences such as ecological modelling, economics, and epidemiology. In ecological modelling, resilience has been defined in terms of recovery: “how fast the variables return towards their equilibrium following perturbation” (Pimm, 1984). The faster the system returns to normal, the greater the system’s resilience. Within work on understanding regime shifts (Scheffer et al., 2001), a system’s speed of recovery from perturbation is associated with the steepness of the slopes of its “basin of attraction”, i.e., a region in state space within which the system tends to remain. For economists, an analogous

---

Figure 1. Two similar models of robustness encountered in materials science and network percolation theory

![Diagram showing stress-strain relationship with Young's modulus and fracture point](image-url)
resilience concept involves the time it takes for a business to recover from perturbation and resume its operations (Janssen et al., 2007). Within epidemiology, the Susceptible-Infected-Susceptible (SIS) model explores cases where members of a vulnerable population can be infected, recover and be re-infected again (individuals have no immunity to the disease and are immediately susceptible to infection). In the kind of compartmental models (where individuals flow from one state to another) of disease propagation, parameters such as the speed of recovery of individuals following infection determine whether the population as a whole recovers and survives (Moreno, Pastor-Satorras, & Vespignani, 2002). Notice that, by contrast with accounts of resilience defined in terms of robustness, we are now interested, not in failure thresholds associated with essentially static systems under unwithstandable stress. Rather, a focus on recovery foregrounds the dynamic processes involved in response to withstandable perturbations. We become interested in rates and propensities rather than thresholds and breaking points, and can become interested in the differential response of system components (e.g., individuals) rather than gross measurements of the system as a whole.

2.3. Models of Adaptability

Models of resilience that focus on adaptability are developed in fields with long time-scale, organic problems such as biological, environmental, and social sciences. Here there is an accent on the ability of systems not just to recover the status quo that existed before a perturbation but to reorganise, reconfigure, learn or evolve such that new organisational forms arise that may be increasingly able to cope with perturbations. Ecosystem resilience research (Walker et al., 2004) describes resilience in terms of adaptability, the “ability to absorb disturbances, to be changed and then to reorganize and still have the same identity, while the basic structure and ways of functioning of the ecosystem retains the same”. Socio-ecological systems research also associates resilience with adaptability. It focuses on transformability, learning, and innovation because social systems involve the capacity of humans to anticipate and plan for the future (Janssen et al., 2007; Walker et al., 2002). The social-ecological model makes use of the adaptive cycle (Folke, 2006) that alternates between periods of destruction and reorganization and periods of growth and conservation. In the emerging field of biologistics (Helbing, Armbruster, Mikhailov, & Lefeber, 2006), fungal networks are studied for their adaptive capacities. Fungal systems develop and adapt a transport network by over-producing links and nodes during exploration and then selecting and positively reinforcing some links while recycling the remainder during a consolidation phase (Tero, Kobayashi, & Nakagaki, 2006). Economics also includes an adaptive view of resilience in crisis situations requiring ingenuity and extra efforts (Rose, 2004). In ethnology, community or cultural resilience is viewed as adaptive and defined as: “the capacity of a distinct community or cultural system to absorb disturbance and reorganize while undergoing change so as to retain key elements of structure and identity that preserve its distinctness” (Luthar, Cicchetti, & Becker, 2000). In psychology, some researchers have distinguished resilience from “resiliency” (Richardson, 2002) in the sense of adaptability. The former is a character trait and the latter is a dynamic developmental process. While resilience requires the presence of substantial risk or adversity, resiliency does not.

2.4. Relationships Between Robustness, Recovery and Adaptability

Robustness, recovery, and adaptability are not mutually independent properties of a resilient system. A system cannot exhibit recovery or adaptability, for example, without some form of robustness because recovery and reorganisation are only possible if a system is capable of withstanding some perturbations. Similarly, recovery is to some extent undermined by adaptability since recovery processes re-establish the pre-perturbation status quo whereas adaptation
sacrifices old organisations in favour of new ones. The purpose of the resilience pyramid (see Figure 2) is to capture more complex nuances and subtle dependencies that tend to be domain specific. It represents a cumulative relationship where robustness stands at the base, adaptive capacity at the apex, and recovery in between.

This hierarchical arrangement also captures the different time scales at which the three aspects operate. Robustness is generally expressed as an a-temporal threshold associated with a static system, and can be seen as either an instantaneous property, the product of extremely fast acting structural dynamics, or as a timeless parameter of the system. By contrast, the concept of recovery is inherently dynamic, positing an unfolding process that takes place on the same timescale as individual perturbation events. For example, a city recovers from each extreme weather event that it is subjected to, a football team recovers from each match that it loses, and an individual recovers from each virus that it contracts. Adaptability involves a longer-term perspective because it invokes a series of perturbations and requires a system that can adapt to generic properties of this sequence of perturbations over an undetermined length of time.

The three aspects of resilience also differ in terms of the degree of abstraction that they encourage in modellers and analysts. As we ascend the hierarchy, models, measurements and accounts become less abstract and more specific, i.e., domains such as ecosystems modelling or psychology which combine complex considerations of robustness, recovery, and adaptability, present highly system-specific accounts, reliant on the particular details of processes and components, that tend to preclude quantitative analysis. By contrast, quantitative models of resilience flourish in the context of robustness at the base of the pyramid, often invoking a generic idealised system (a network, a material) and treating it as a homogeneous or structureless assembly of interchangeable parts that could represent many real-world situations. In order to present a single simple model of resilience that has the capacity to represent all three aspects of resilience in a concrete manner, in the next section we propose a generalized model of cascading failure in networks that contain permutable nodes. These nodes may be thought of as system elements that are able to respond to perturbation by changing the role that they play within the system of systems that contains them. By keeping the model fairly generic, we resist the tendency in the resilience literature to fully associate high-level resilience aspects with detailed accounts of specific real-world systems. However, by casting the model in

Figure 2. The pyramid of resilience formed by robustness, recovery and adaptability. The three aspects form a hierarchy with different properties of resilience foregrounded depending on the level at which an account is formulated.
terms of an explicit network simulation we are able to provide a concrete mechanistic account of each aspect of resilience.

3. PRESENT STATE OF MODERN INFRASTRUCTURE NETWORKS: THE DANGER OF SYMBIOTIC INTERDEPENDENCY

In this section, we illustrate the problem of the resilience of modern interdependent infrastructure networks using a very simple abstract setting. We proceed to explore robustness, recovery, adaptation and their interplay in this context.

Let us assume that two different infrastructure networks rely on being mutually connected in order to be viable. For example, a power network, A, relying on smart meters needs to be connected to an ICT network, B, in order to work properly, while, reflexively, ICT network, B, itself also relies on its connections to power network, A. In this scenario, a connected component (i.e., a network fragment) in one infrastructure network is viable only if a minimum fraction of its nodes are connected to a surviving network component from the other infrastructure network. Connected components in both infrastructure networks are subject to this survival constraint. So, in our example, a connected component of the power network needs to have at least some minimum fraction of its nodes linked to functioning ICT nodes in order to function properly. Similarly, while our imaginary ICT network has some degree of energy autonomy, each connected component of the ICT network requires that some minimum proportion of its nodes are directly linked to a network A power supply in order for the network B component to function properly as a whole. This symbiotic requirement for the viability of a network component can be expressed by a dependency threshold, \( \Gamma \), that is to say, the minimum ratio of nodes in a network component that must be connected to functioning nodes in the complementary infrastructure network.

We have presented this notion of symbiosis in the context of infrastructure systems, but it has relevance much more broadly. Ecosystem resilience might implicate mutually dependent species that cannot exist in isolation. The resilience of an industrial complex to energy threats implicates inter-network symbiosis when its day-to-day operations depend on the availability of multiple energy sources. The concept can also be applicable to models of mutually dependent transport networks, and likely many other systems (Buldyrev, Parshani, Paul, Stanley, & Havlin, 2010).

Figure 3 shows the robustness of pairs of coupled symbiotic networks. The different types of network topology explored are: Erdős– Rényi (Erdős & Rényi, 1976) (each pair of nodes is connected with some fixed probability such that the average number of neighbours, or degree, for each node is Poison distributed with mean, \( k \)), Barabási–Albert (Albert & Barabasi, 2002) networks (where a network with mean degree \( k \) has a degree distribution that is scale free, featuring a few well-connected hubs with far more than \( k \) neighbours, but also many nodes with very few connections), Watts-Strogatz or small-world networks (Watts & Strogatz, 1998) (whose structure is close to social networks in the sense that the network exhibits significant clustering and any node is just a small number of connections away from all others), and ring lattices (regular networks where all nodes have the same number of neighbours, i.e., every node has degree \( k \)). These network types were chosen as they are well known and are affected in distinctive ways when confronted by attacks (Albert, Jeong, & Barabasi, 2000).

Here we generate two networks from the same class and establish dependencies between nodes in one network and nodes in the other. We consider two coupled networks A and B of N nodes each (N typically equal to 500), each with average degree \( k \). The degree of coupling between the two networks is defined by the fraction \( q \) of nodes in network A that are each dependent on at least one randomly selected node in network B. These inter-network dependencies are undirected (i.e., if a node in A depends on a node in B, then each will fail to operate if the other is disabled). Where a node
in one network depends on multiple nodes in the other network, it will fail to operate in the event that any of the nodes that it depends upon fails.

The robustness of these interdependent network pairs is evaluated by attacking one network directly and then by establishing the extent of the post-attack viability of both networks after any cascading failure has run its course. The initial attack is carried out by directly disabling a fraction, p, of randomly chosen nodes in network A. Here we consider nodes to fail if they are attacked directly in this way, if the component that they are part of falls below some critical size, or if a node in the complementary network upon which they depend fails. Consequently, whenever a single node fails there is the potential for it to cause further nodes to fail, which in turn may bring down yet further nodes. This process of cascading node failure iterates until no further node failures occur. The robustness of the system is expressed as the area under the curve defined by the fraction of nodes still alive in each network after cascading failure as a function of attack size, p, varying from 0 to 1. For each network topology and each level of intra-network connectivity, k, and each level of inter-network connectivity, average robustness is evaluated for 25 independently generated network pairs.

For all symbiotic network pairs considered here, no matter what their individual topology type is, the higher the level of symbiotic in-

---

Figure 3. The robustness of a pair of interdependent 500-node networks as a function of their dependency threshold, $\Gamma$. Each robustness score corresponds to the average of the robustness values over all attack sizes, and over a range of average node degree, $k$, between 4 and 24, obtained for different degrees of inter-network random coupling between 5% and 100%.
terdependency, the lower their robustness (see Figure 3). The level of the symbiotic dependency threshold strongly influences the optimal level of coupling between networks, and this level of coupling is also influenced by network topology.

This result may have wide implications, because it demonstrates that the dynamic process of fragmentation that may decouple interdependent networks during a cascading failure may be as important as the process of percolating failure within each network when it comes to quantifying and predicting the robustness of interdependent networks. This implies that systems built to rely on the combined availability of different resources such as transport, power, ICT, and water networks may become increasingly vulnerable to catastrophic failure. Consistent with much previous work on modelling infrastructure networks, the above analysis adopts an account of resilience that highlights robustness rather than recovery or adaptation. To date, little attention has been paid to the capacity of networks and individual network nodes to dynamically respond to perturbation in order to reorganise or self-heal (Hollnagel et al., 2006). In the context of the resilience of symbiotic networks, we suggest the introduction of permutable nodes as an example of recovery and adaptability that fits within a fairly generalizable model of resilience that takes into account symbiotic interdependency. In the following section we explore one example of how recovery/adaptation capacities might influence system resilience.

4. INFRASTRUCTURE NODES WITH PERMUTABLE ROLES

In domain such as organizational resilience, permutation can be seen as the key operator (De Florio et al., 2012; Serugendo, Coronato, & Bakhoura, 2012) selected to represent how social groups form and collapse as a response to change. Similarly, in network communication, permuting roles is a way to tune the algorithmic complexity and achieve control of the emergence of events like collisions (De Florio & Blondia, 2012), which may also be used as an additional example of exchange between complementary networks. Within the idealized framing introduced above, in order to ensure the post-attack viability of symbiotic clusters, it is important to maintain the fraction of coupled nodes in each connected component above a critical threshold. The symbiotic viability condition for a given component can be defined in its simplest form as maintaining the coupling ratio of the components above an interdependency threshold, \( \Gamma \), and can be expressed as:

\[
\frac{q}{q + \bar{q}} \geq \Gamma
\]

Where \( q + \bar{q} = N \) is the number of nodes in a component, \( q \) is the number of nodes that are directly coupled to nodes within viable components from a different complementary network, \( \bar{q} \) is the number of uncoupled nodes, \( \Gamma \) is the interdependency threshold below which the component is not viable. There are only two ways to increase a component’s coupling ratio: either add extra coupled nodes to the component to increase the weighted sum in the numerator, or remove uncoupled nodes to reduce the weighted sum in the denominator.

The opportunity for improving post-attack viability of the coupled networks provided by the presence of permutable nodes is significant. The number of different possible component configurations resulting from permutations can be computed as \( 2^{s^p} \), where \( s \) is the size of the component, and \( p \) is the fraction of permutable nodes randomly distributed in the system. A system with, for example, only 10 permutable nodes in a surviving component, would still present \( 2^{10} = 1024 \) possible configurations, each potentially associated with different numbers of surviving nodes in the network as a whole, and each therefore potentially associated with different levels of post-attack quality of service.

However, while in the last section our focus was restricted to interpreting resilience in terms of the robustness of networks to attacks, in this section so far we have been considering
permutation only in the context of recovery. After an attack and the resulting cascading failure, permutation of the roles of some surviving nodes can increase the number and/or size of viable network components, bringing additional capacity and functionality back online. An alternative paradigm involves permuting node functions during, or even in advance of, the perturbation or attack. Where the timescales of permutation are sufficiently fast with respect to the timescales of cascading failure, it is possible to dynamically reconfigure the network in an effort to stem the spread of the problem, e.g., re-routing traffic in the case of accidents or road outages, repurposing office space or computational resources in the case of malicious attack, etc. Key here is the capacity to quickly identify the permutations that will minimise the spread of failure and maximise the functionality of the remaining systems. The exponential number of possible reconfigurations ensures that neither random choices, nor exhaustive search for the best configuration, are feasible. Sophisticated planning may be required in order to manage effective real-time permutation of this type, but implementing such planning risks slowing the system’s response time, which may render dynamic resilience ineffective.

Systems capable of longer-term adaptation have the potential to meet the challenge of quickly identifying the most appropriate adaptive reconfigurations. Over the course of multiple attacks or perturbations, adaptively resilient systems can come to learn or adapt such that they are organised in ways that naturally facilitate the right spontaneous permutations when attacks or perturbations arise.

Robustness and recovery are thus just the tip of the iceberg when looking at the resilience of modern infrastructure networks. Adaptability refers to a range of more sophisticated processes analogous to those operating within the human brain (a system able to cope with some forms of injury because its sub-components can adopt new roles and assume each other’s tasks) or in an evolving population (where constant random variation at the level of individuals gives rise of adaptive capacity at the level of the population). While the presence of infrastructure nodes that can switch between different roles across distinct interdependent networks does not automatically imply infrastructure systems with resilience stemming from their adaptive capacity, the addition of longer-timescale processes of learning or reconfiguration could do.

Cascading failure being inherent to symbiotic interdependency, the more an infrastructure depends on connections between multiple different types of services in order to function properly, the more likely failure is to spread iteratively through different parts of the system during periods of stress or perturbation. Unfortunately, this propensity of modern infrastructure systems to require an increasing number of services to function together is not likely to reverse. Considerations presented here indicate that one way to reduce the impact of the resulting symbiotic interdependency is to design infrastructure nodes that can switch between different roles across distinct interdependent networks, such that they have the capacity to be functionally permutable. This does not mean that these nodes are required to fulfil simultaneously multiple roles (e.g., dual infrastructures), but rather that they would have the ability to perform only one type of service at any particular time. These reconfigurational capabilities provide infrastructure networks with the capacity to adapt while limiting the risks associated with symbiotic interdependency. One way to achieve this is to treat coupled and uncoupled nodes like valuable resources that can be exchanged between complementary networks in the form of permutable infrastructure nodes. Examples of such a mechanism are: roads convertible to landing strips (M2 motorway in Pakistan, PAF exercise High Mark, 2010), the Stormwater Management and Road Tunnel (SMART) in Kuala Lumpur (a tunnel that can alternate between traffic and storm water management) (Abdullah, 2004), and energy storage devices on board electric vehicles that can be plugged to the power grid when not in use so as to store and produce energy whenever needed (Vehicle-to-Grid) (Kempton & Tomić, 2005).

Here we assume that if a permutable node of this kind is active as part of a component within one network, A, it cannot simultaneously
be active as part of a component within another network, B. That is, permutable nodes can only play one role at a time. When permutation occurs, a node’s role swaps, potentially allowing the allocation of a node from a non-essential role in one network to a potentially critical role in another (see Figure 4).

5. CONCLUSION

We have presented a hierarchical framework for considering system resilience that relates systems robustness, recovery and adaptability. While the former is associated with resilience thinking in many disciplines, tends to take an a-temporal perspective and can be used as a generic and quantitative tool for describing arbitrary systems, the latter is associated with longer timescales that span multiple episodes of perturbation and tends to be domain specific and harder to quantify or formalise. Here we have used the example of permutable nodes in interdependent infrastructure networks to exemplify the three related perspectives on resilience and point the way to a genuinely transdisciplinary account of resilient systems.

Figure 4. Using a permutable node where $\Gamma = 1/3$, i.e., a component in either network is only viable if at least 1/3 of its nodes are directly connected to a viable component in the complementary network. The network diagram in (i) represents the pluripotent network before the permutable node has been assigned a role. Dashed lines represent inter-network links, while solid lines are edges within a network. Black nodes belong to network A, white nodes to network B, and the black and white node is permutable. In the first alternative scenario (ii), the black role is activated. In the second alternative situation (iii), the white role is activated. After cascading failure, alternative (ii) leaves a larger viable network than alternative (iii).
ACKNOWLEDGMENT

This research was funded by the EPSRC under grant reference number EP/I005943/1.

REFERENCES


ENDNOTES

1 Here we are using the term component in the sense employed by network science to mean a set of network nodes that are part of the same connected network fragment. While not all nodes in a component need to be directly connected to each other, every node in a network component can be reached from every other node in the same component by taking a route through nodes that are directly connected. Conversely, there is no path of connected nodes that links a pair of nodes that are in different components.