SAND2018-8596D

Modelling Network Efficiency and Resilience

Jamie Thorpe
Carnegie Mellon University
MS Information Security, Spring 2019

iSAFE
Interns for Security, Arms control and Force protection Engineering

Managers:
Shawn Taylor (iSAFE), 5829
Derek Hart, 5821
Project Mentors:
Meghan Galiardi, 5821
Eric Vugrin, 5821

Goal: To create a modelling tool which uses graph analysis and metrics for network efficiency and resilience to quantify network topologies. The tool should allow for the simulation of network attacks and attack response.

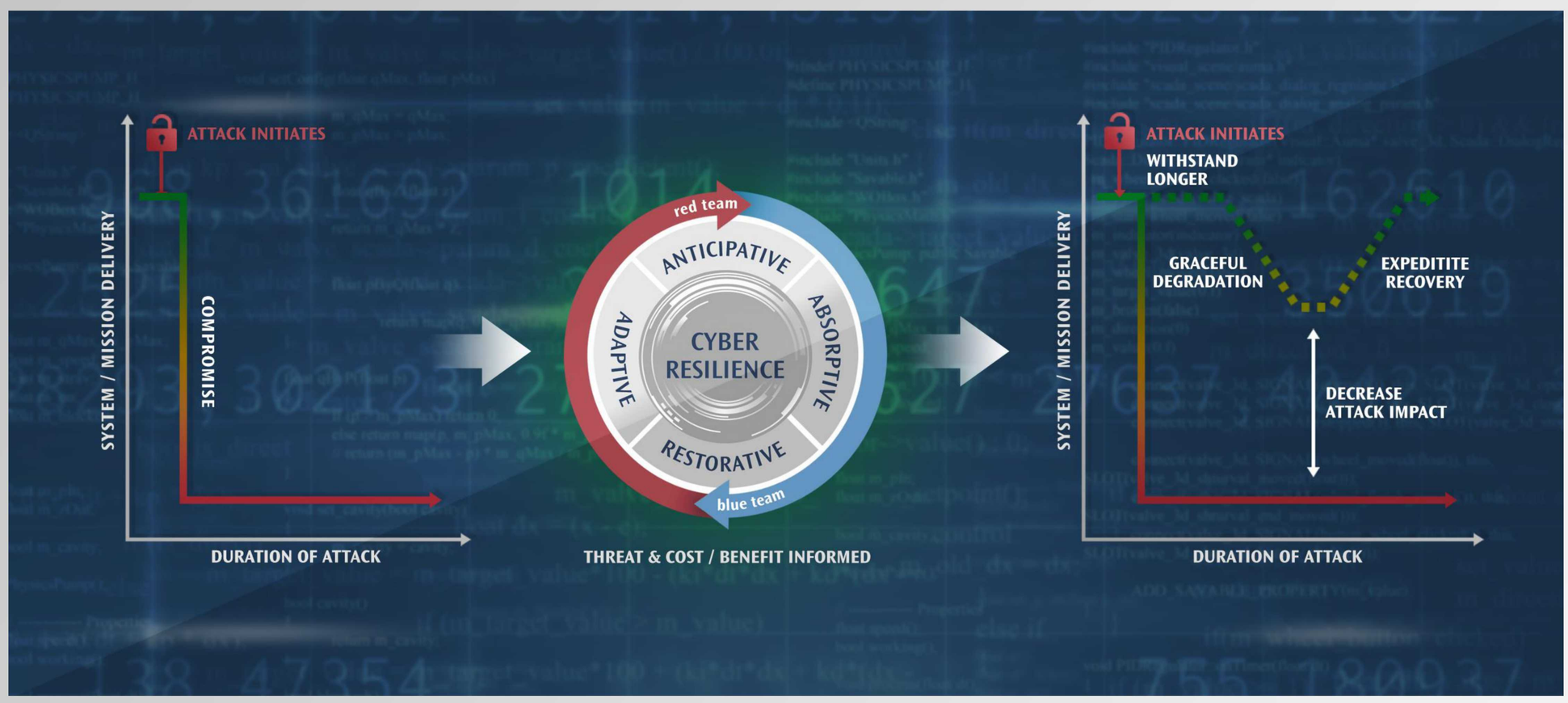

Figure 1: Foundations of Cyber Resilience

Cyber Resilience

- Cyber security focuses on preventing an adversary from accessing a system
  - "How do we *avoid* being compromised?"
- Cyber resilience focuses on how prepared a system is to withstand and cope with an attack
  - "What happens when we *are* compromised?"
  - There are currently no universally-accepted metrics for cyber resilience

Defining Metrics

- Adapting ecology metrics to the cyber domain
- Integrating flow and capacity
- Inclusion of temporal dynamics
- Visualization

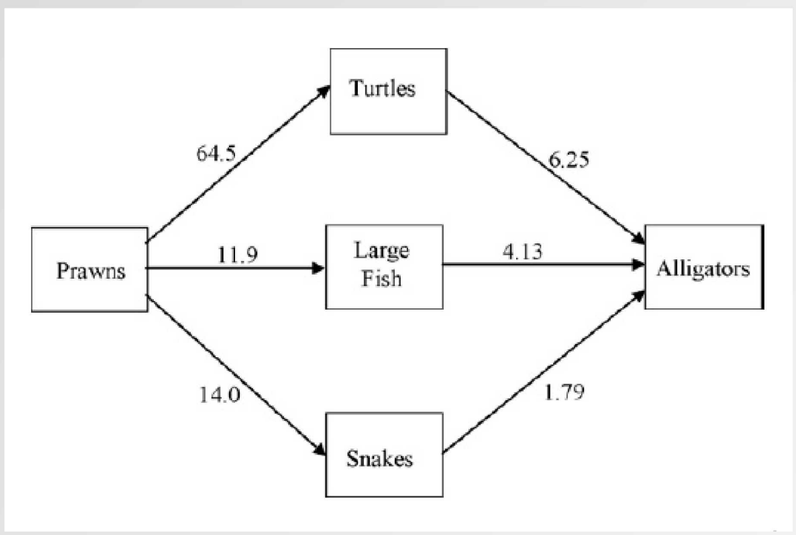

Figure 2: Example of a carbon flow through an ecosystem*

Innovations to Ulanowicz Metrics

- Ulanowicz et al.* (2009) previously defined a set of metrics for ecological networks:
  - Ascendency

$$A = \sum_{i,j} T_{ij} \log\left(\frac{T_{ij}T_{..}}{T_{i.}T_{.j}}\right)$$

  - Reserve

$$\phi = -\sum_{i,j} T_{ij} \log\left(\frac{T_{ij}^2}{T_{i.}T_{.j}}\right)$$

- Capacity for development / Sustainability

$$C = A + \phi$$

*R. Ulanowicz et al., *Quantifying sustainability: Resilience, efficiency and the return of information theory,* Ecological Complexity, An International Journal on Biocomplexity in the Enviornment and Theoretical Ecology, vol. 6 issue 1, March 2009.

Modelling Network Efficiency and Resilience

Jamie Thorpe
Carnegie Mellon University
MS Information Security, Spring 2019

iSAFE
Interns for Security, Arms control and Force protection Engineering

Managers:
Shawn Taylor (iSAFE), 5829
Derek Hart, 5821

Project Mentors:
Meghan Galiardi, 5821
Eric Vugrin, 5821

Results

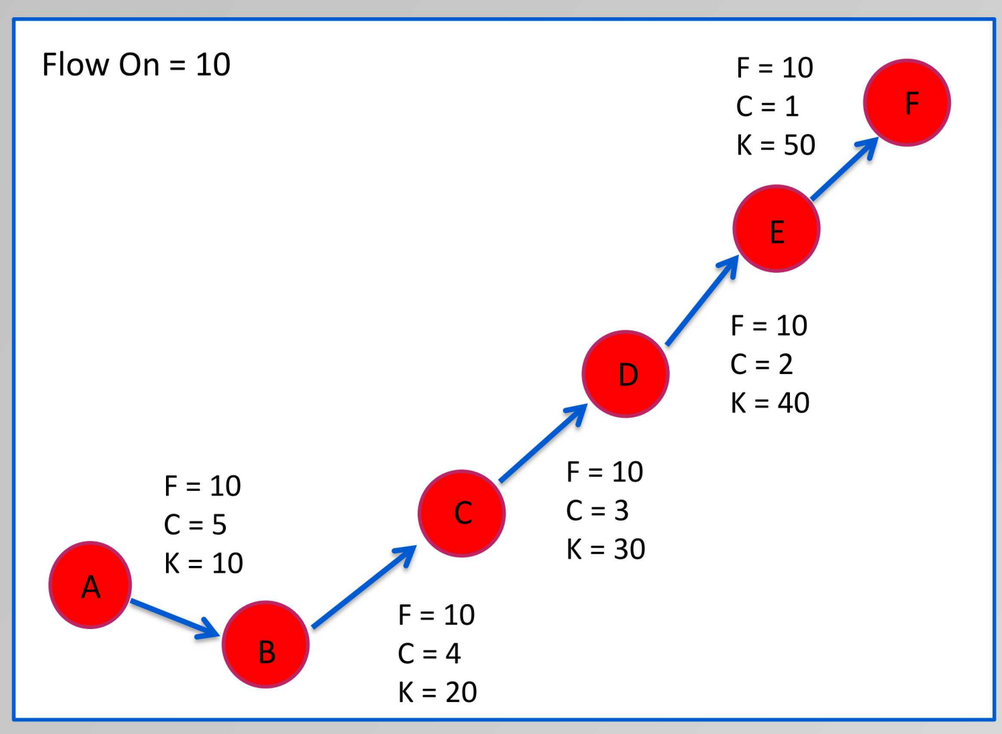

Figure 4: Chain Link topology

Simulation: Denial of Service attack reduces the capacity of every link by 50%. Note that the efficiency is severely reduced.

	Efficiency, No Disruption	Efficiency, With Disruption	Resilience, No Disruption	Resilience, With Disruption
Ulanowicz, et al.	34.95	17.47	0	0
Thorpe, et al.	-	-	0	0

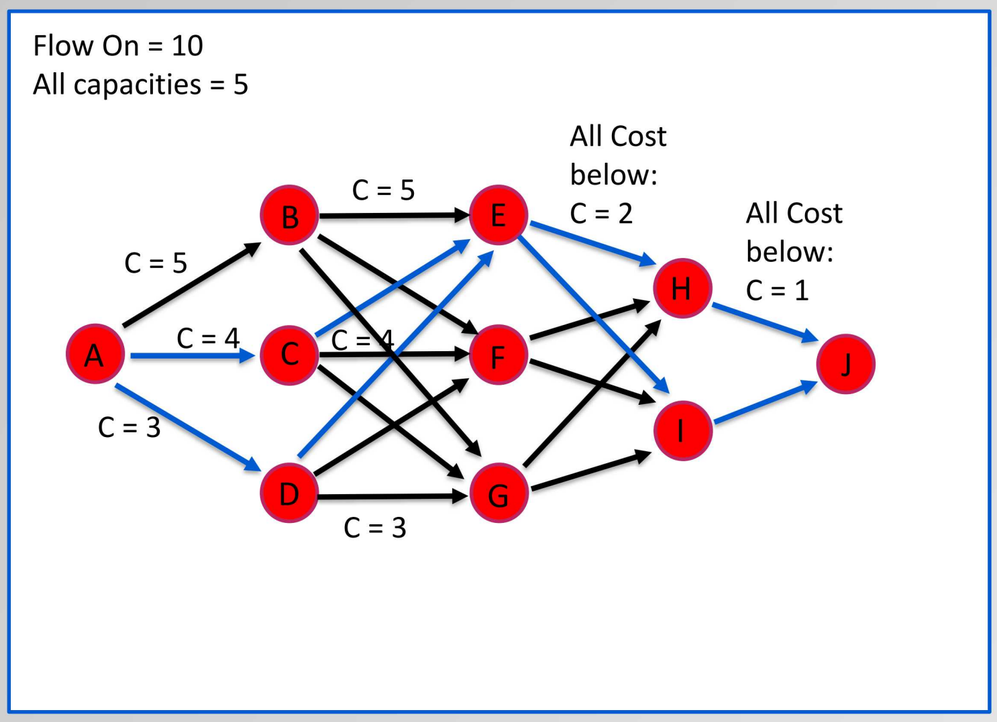

Figure 5: Full Web topology

Simulation: Major natural disaster takes out nodes C, F, and I. Note that in a fully networked topology, all the information can still traverse the full network.

	Efficiency, No Disruption	Efficiency, With Disruption	Resilience, No Disruption	Resilience, With Disruption
Ulanowicz, et al.	24.08	12.04	12.04	0
Thorpe, et al.	-	-	10.76	1.93

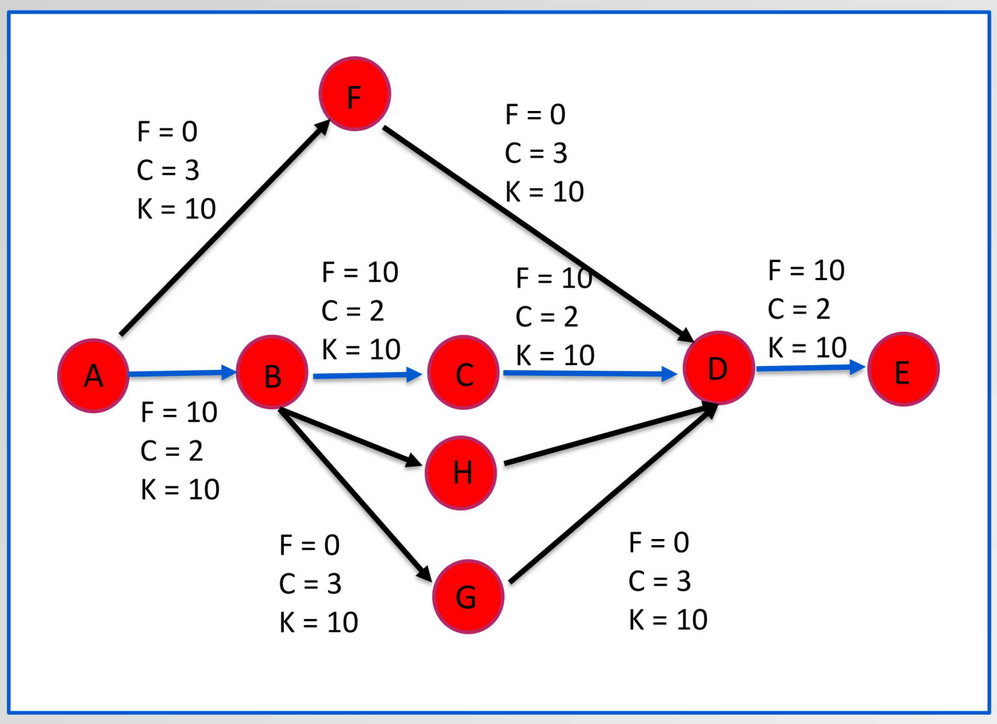

Figure 6: Mixed topology

Simulation: An attacker breaches node C, breaking all links in or out. Note the difference in resilience score depending on the metric used.

	Efficiency, No Disruption	Efficiency, With Disruption	Resilience, No Disruption	Resilience, With Disruption
Ulanowicz, et al.	24.08	14.31	0	0
Thorpe, et al.	-	-	5.90	2.33

Conclusions and Future Work

- Metrics that only consider flows without capacities miss some key resilience features
- Future work ought to consider
  - Network flows and capacities
  - Multiple flow types (power and information, sensitive and non-sensitive flows)

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

XX

U.S. DEPARTMENT OF ENERGY