SAND2018-9861PE

Modeling Network Efficiency and Resilience

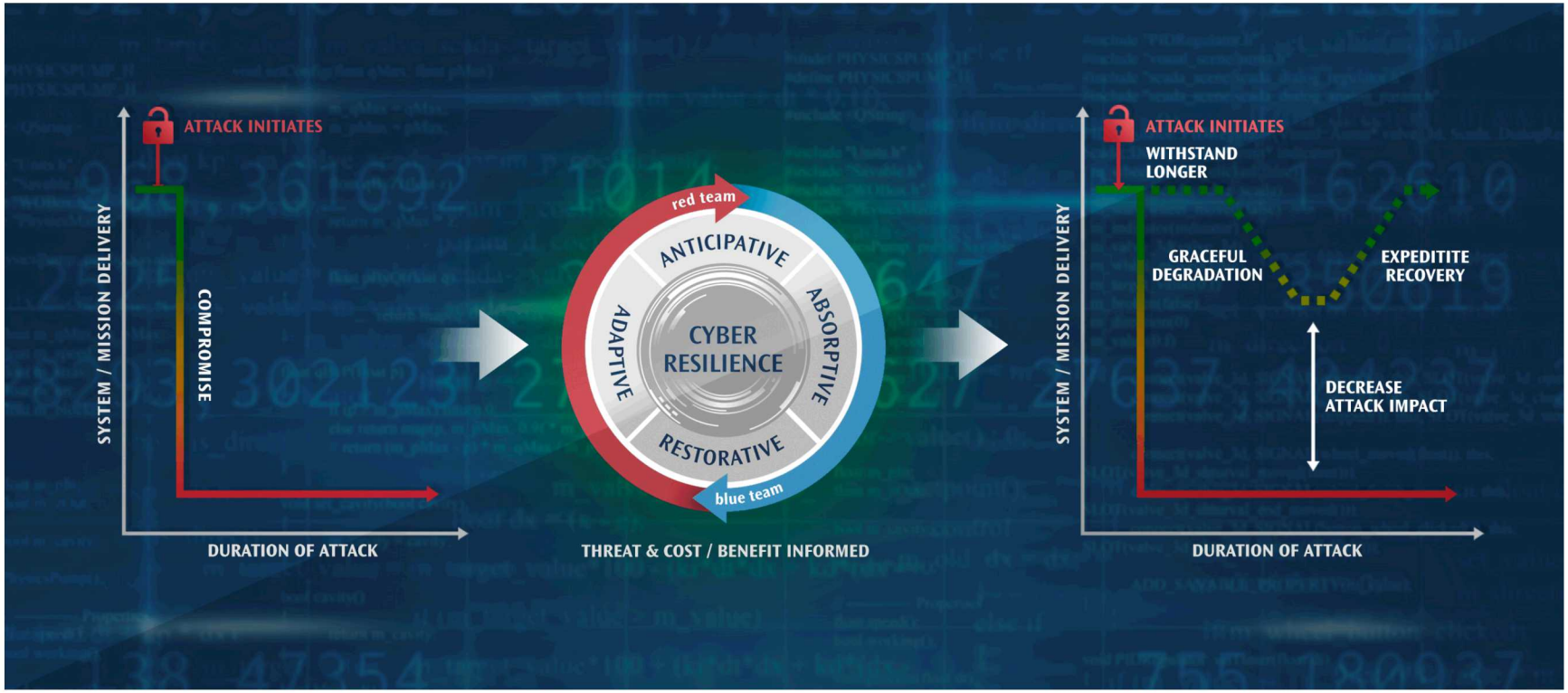
PRESENTED BY

Jamie Thorpe

Outline

- Introduction and Goal
- Methods
  - Metrics
  - Innovations
- Results
- Conclusions

Cyber Resilience



Defining Metrics

- Ulanowicz et al.* (2009) Previously Defined a Set of Metrics for Ecological Networks:
  - Ascendency (Efficiency)

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

  - Reserve (Resilience)

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

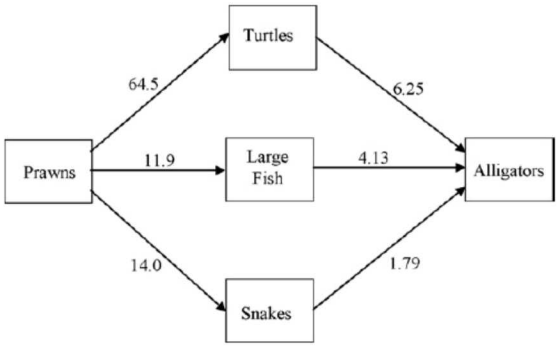
  - Capacity for Development/Sustainability

$$C = A + \phi$$

*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.

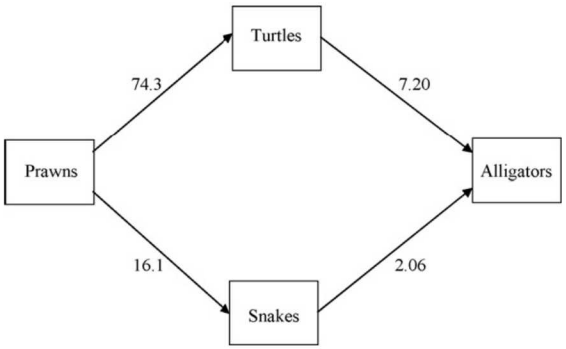
Ulanowicz and Ecological Networks

Carbon Flow Through an Ecosystem*



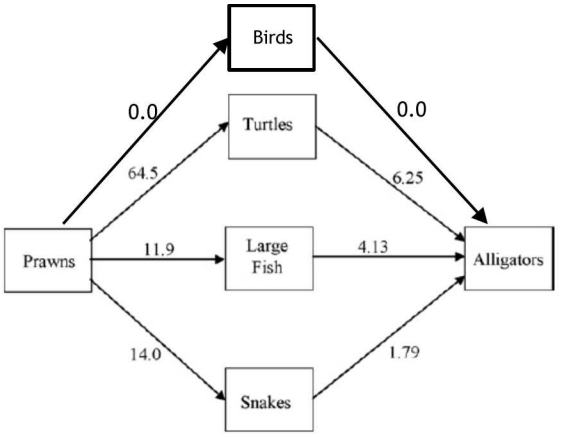
Efficiency = 53.9
Resilience = 121.3

Disrupt the Large Fish Population*



Efficiency = 44.5
Resilience = 68.2

Additional Link with No Flow



Efficiency = 53.9
Resilience = 121.3

Problem: when there is an Unused Path on the Network, the Ulanowicz Metric is the Same as if that Path weren't there at all.

Innovations to Ulanowicz Metrics

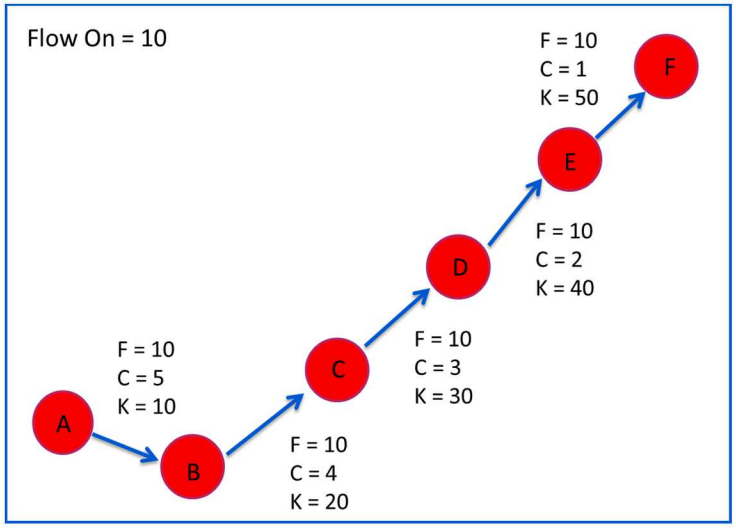
- Adapt Ecology Metrics to the Cyber Domain
- Integrate Flow and Capacity

$$\phi = -\sum_{i,j} T_{ij} \log\left(\frac{T_{ij}^2}{T_{i\cdot}T_{\cdot j}}\right), \text{ such that } T = \text{LinkFlow}$$

$$\phi' = -\left(\frac{SuccessfulFlow}{DesiredFlow}\right)\sum_{i,j} K_{ij} \log\left(\frac{K_{ij}^2}{K_{i\cdot}K_{\cdot j}}\right), \text{ such that } K = \left(\frac{LinkCapacity}{LinkCost}\right)$$

- Include Temporal Dynamics
- Visualization

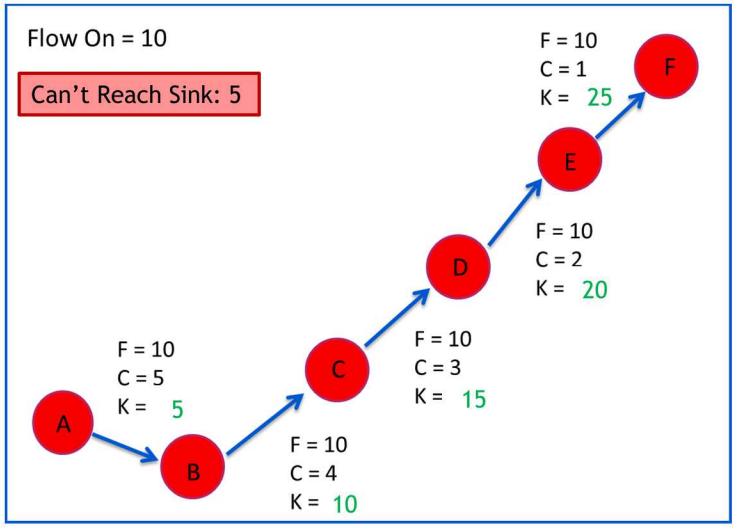
Results: Chain Link Before Disruption



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

Problem: when there is an Unused Path on the Network, the Ulanowicz Metric is the Same as if that Path weren't there at all.

Results: Chain Link After Disruption

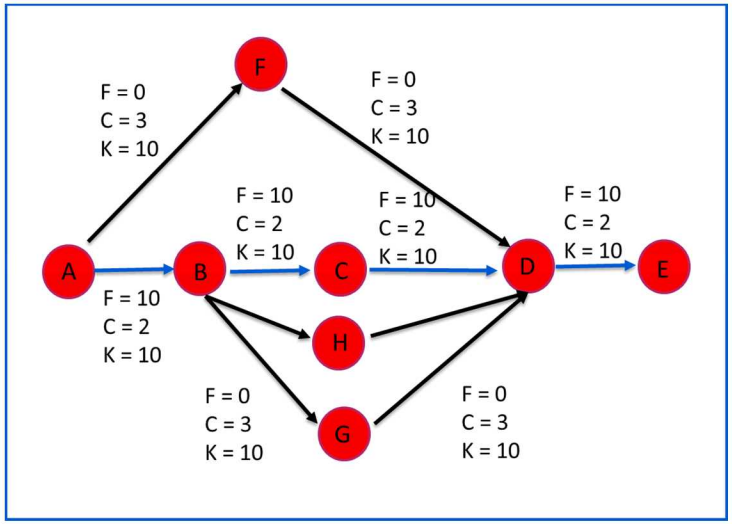


Disruption: A Denial of Service attack reduces bandwidth to 50% on all links

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

Summary: a Chain Link Network, while very Efficient, is not Resilient to Disruptions (Attack, Natural Disaster, etc.).

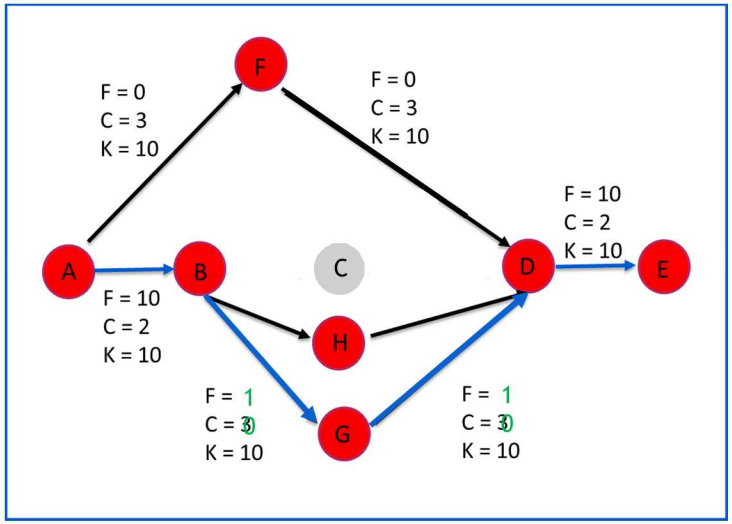
Results: Redundant Network Before Disruption



	Efficiency, No Disruption	Resilience, No Disruption
Ulanowicz, et al.	24.08	0
Thorpe, et al.	24.08	5.33

Summary: a more Redundant Network is Less Efficient, but should be more Resilient. The Ulanowicz Resilience Metric sees a Non-Utilized Link the same as a Non-Existent Link, and the Resilience of the Network is not Accurately Reflected.

Results: Redundant Network After Disruption



Disruption: An attacker breaches Node C, preventing traffic from flowing in or out

	Efficiency, No Disruption	Efficiency, With Disruption	Resilience, No Disruption	Resilience, With Disruption
Ulanowicz, et al.	24.08	14.31	0	0
Thorpe, et al.	24.08	14.31	5.33	2.92

Summary: a more Redundant Network is Less Efficient, but should be more Resilient. The Ulanowicz Resilience Metric sees a Non-Utilized Link the same as a Non-Existent Link, and the Resilience of the Network is not Accurately Reflected.

Conclusion

- Metrics that only Consider Flows without Capacities Miss some Key Resilience Features
- Future Work ought to Consider:
  - Continue to Refine New Resilience Metric
  - Multiple Flow Types
    - Power and Information
    - Sensitive and Non-Sensitive Flows
  - Run with real traffic and routing protocols