Annotated bibliography on complex networks

Jose M Sallan

References

[1] Liang Dai, Ben Derudder, and Xingjian Liu. The evolving structure of the Southeast Asian air transport network through the lens of complex networks, 1979–2012. *Journal of Transport Geography*, 68(October 2017):67–77, apr 2018.

> The article explores the structural evolution of the Southeast Asian air transport network (SAAN) during 1979-2004 from a complex network perspective. First, authors study the evolution of network metrics (scale-free properties, dissotative mixing and small-world properties), and compare them with other major regional blocs. Second, they unveil the core-bridge-periphery structure of the SANN, and its temporal evolution. This multilayer structure has experienced significant changes in the studied period, as the core of the network shifts towards the north. Additionnally, the introduction contains an geographical and historical analysis of Southeast Asia, and discuss the opportunity of defining region boundarys to analyze transportation networks.

[2] Shuliang Wang, Liu Hong, Min Ouyang, Jianhua Zhang, and Xueguang Chen. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. *Safety Science*, 51(1):328–337, jan 2013.

> This paper analyzes the vulnerability of a two interdependent networked systems to cascading failures: a power grid and a gas network. The cascading failure model of the power grid is the defined in Wang et al. (2008), where edge load is proportional to the power of product of edge's nodes. The model for the gas network is the generalized betweenness centrality model defined in Carvalho et al. (2009). Network interdependence is modeled through a specific interdependence function. Nodes that lead to interdependence are detected using spatial proximity criteria. Authors define three categories of network disturbance: random failures, deliberate attacks and natural disasters.

Deliberate attacks are defined as suppression of edges of high load and nodes of high degree. The results of the vulnerability metrics are global vulnerability analysis and critical component analysis. Global vulnerability is measured with network efficiency and damaging rate. Critical component analysis reports the network components whose damage would lead to larger vulnerability.