An Introduction to the Special Issue on Network Reliability and Vulnerability Models and their Applications

LOUIS PETINGI
College of Staten Island (CUNY)
Computer Science Department
2800 Victory Boulevard
Staten Island, NY 10314
USA
louis.petingi@csi.cuny.edu

CHARLES SUFFEL
Stevens Institute of Technology
Department of Mathematical Sciences
Castle Point on Hudson
Hoboken, NJ 07030
USA
csuffel@stevens.edu

The main focus of this Special Issue is to present recent developments in network *reliability* and *vulnerability* theories from a theoretical and applied perspective. While network reliability is concerned with how well a topology is expected to operate given that the probabilities of failure of its components (i.e., edges and/or vertices) are known, a topology is said to be less vulnerable than a competing topology if more components than its competitor must fail in order to alter certain graph-theoretic properties of a graph (e.g., *connectivity* [4], *toughness* and *edge-toughness* [3], etc.).

A series of new models and manuscripts have appeared recognizing the importance of network reliability and vulnerability theories to evaluate performance objectives of existing communication networks (e.g., wireless networks, and WDMs optical networks), and, in contrast to the original intention to assess the performance of communication networks (e.g., satellite, Internet and electronic networks), these models are also applicable to measure the performance of a broader range of networks, such as biological and chemical networks.

Within the context of network reliability, in the classical classical model (see [1] for a survey on results and combinatorial properties of this model), given that the edges of a topology $G = (V, E)$ have been assigned independent probabilities of failure (vertices are perfectly reliable), and given a set of terminal nodes $K \subseteq V$, the *K-terminal* reliability, $R_K(G)$, gives the probability that after deletion of the failed edges, each pair of vertices $u, v \in K$ remain connected through operational paths.
In *On Component Order Edge Reliability and the Existence of Uniformly Most Reliable Unicycles*, Gross et al. introduced a generalization of the classical model in which given an integer p, $2 \leq p \leq n$, $n = |V|$, we are interested in determining the probability $R_p(G, \rho)$ of the event that a connected component with at least p vertices will remain after deletion of the failing edges, under the assumption that all edges fail independently with the same probability ρ. From an applied perspective, given a network G, the unreliability $U_p(G, \rho) = 1 - R_p(G, \rho)$ gives the probability that at most $p - 1$ of its vertices will be able to communicate at one time, allowing to assess the quality of communication not contemplated by the classical reliability model.
In the paper *Diameter-related properties of graphs and application to network reliability theory*, Petingi discussed computational complexity issues of the *Diameter-constrained* network reliability measure, $R_K(G, D)$, which is the probability that given a bound D, every pair of vertices $u, v \in K$, are connected by an operational path composed of at most D edges, allowing to assess *QoS* of networks in which delay-constraints must be met. Since in the classical reliability the length of the paths connecting vertices are not under consideration, this measure also represents an important generalization of the traditional reliability.

The section on vulnerability comprises four manuscripts. In the work titled *A Survey of Component Order Connectivity Models of Graph Theoretic Networks*, the authors introduced Component Order Connectivity parameters, which are the minimum number of vertices or edges whose removal results in a disconnected network having all components of order less than some predetermined threshold value p. In vulnerability theory, vertex connectivity and edge connectivity are the minimum number of vertices or edges, respectively, that need to be deleted in order to disconnect the network; in some applications, such as distributed computing or spy networks, the resulting network, while disconnected, may still be viable if there remains a component large enough to complete the network's function.

In *A Modified Measure of Covert Network Performance*, Doty contemplates the performance of Covert Networks in which *secrecy* regarding the existence of its vertices is at odds with the need to optimize communication. To this end, a standard secrecy's parameter is modified to include information about *connectedness* of a graph by using ideas related to the concept of toughness.

When *detectors* (i.e., vertices) are deployed within a network to monitor malfunctioning or intruders, one important graph-theoretic problem is to maintain good surveillance of the topology under the assumption that the detectors may be subject to failures. In the work titled *A framework for faults in detectors within network monitoring systems*, Slater identifies four types of detectors faults and detector-failure parameters for various intruder-detection models.

This section concludes with the work *An Update on Supereulerian Graphs*, by Lai et al. An *Eulerian* graph is a graph that is connected and every vertex is of even degree, and a graph $G = (V, E)$ is Supereulerian if G contains a spanning subgraph that is Eulerian. This paper represents an important update on recent developments in the study of Supereulerian and related families of graphs, of the original survey published by Catlin (see [2]), in 1992.

As both reliability and vulnerability measures were originally intended to assess *QoS* of communication networks, this Special Issue includes a manuscript presenting recent developments in the study of biological networks such as *RNA* secondary structures (2D) modeled as graphs. In the paper titled *Network Theory Tools for RNA modeling*, Kim et al. showed how graph-theoretic representation of RNA structures help to enumerate, predict and design RNA topologies. The connectivity of a graph and *Laplacian* eigenvalues (eigenvectors) relate to biological properties of RNA and help in the process of predicting RNA structures.

Finally, as invited editors for the Special Issue of WSEAS Transactions on Mathematics, we would like to express our sincere gratitude to the authors, reviewers, journal editors and staff. Their support was essential in making this collection of papers, in our modest opinion, a significant contribution to the field of graph theory.

References:

[1] F. T. Boesch, A. Satyanarayana, and C. L. Suffel, A survey of some network reliability analysis and synthesis results. *Networks* 54(2), 2009, pp. 99–107.

[2] P. A. Catlin, Supereulerian graphs: a survey, *J. Graph Theory* 16, 1992, pp. 177–196.

[3] G. Y. Katona, Toughness and edge–toughness, *Discrete Mathematics* 164 (1-3), 1997, pp. 187–196.

[4] K. Thulasiraman, and M. N. S. Swamy, *Graphs: Theory and Algorithms,* John Wiley and Sons, 1992, pp. 200–235.