NETWORK ATTACKS BASED ON VERTEX COVERINGS

EDUARDO SÁENZ-DE-CABEZÓN AND HENRY P. WYNN

Extended Abstract

The robustness of networks is an important problem that has been studied in a variety of situations, see for instance [3] or the survey [5] and the references therein. A milestone in the study of this problem was the discovery by Albert *et al.* of the dramatic effect of targeted attacks on networks whose vertex degrees follow a power-law distribution, like the Internet and the World Wide Web [1].

Attack strategies are often described as vertex or edge deletion strategies. We focus in this paper on vertex deletion. The vertices (also called nodes) of the network are sorted according to some property such as degree and are removed from the network according to this property. The resilience of a network to such vertex removal is important in areas ranging from vaccination strategies in epidemiology to fighting criminal organizations.

In this paper we propose two vertex deletion strategies based on the structure of vertex covers of the network. Given a simple graph, e.g. a network N, a vertex cover C of N is a set of vertices such that each edge of N is incident to at least one vertex of C. We say that C is *minimal* if it does not contain another vertex cover. C is said to be *minimum* if it is of minimal cardinality among all vertex covers of N.

For a given vertex v of a network N we define its covering degree, $\mathrm{cd}(v)$ as the number of *minimal* vertex covers of N that contain v. We also define the covering index of v, $\mathrm{ci}(v)$ as the number of *minimum* vertex covers of N that contain v plus the quotient of $\mathrm{cd}(v)$ divided by the total number of minimal vertex covers of N.

We study these degrees and indices in several network models, such as Erdös-Renyi random graphs, Albert-Barabasi networks and the Watts-Strogatz small world model.

In our experiments we found that the covering degree of a vertex was correlated to other widely used properties like vertex degree and betweeness centrality, but surprisingly we found that the covering index was not correlated to any of the other measures, including covering degree. We used the connectivity of the network to measure the resilience of the network to attacks based on covering degree and index and found that the covering index broke the studied networks in a bigger number of smaller disconnected components than any of the other strategies studied.

A strong concern about the use of this strategy is its high computational complexity, which makes it impractical for use in large complex networks. We show, however, that it is usable for networks of less than 100 nodes, which allows us to use it in some social organizations or industrial systems. The strategy we propose is targeted to relatively small networks, where we can use techniques that are unusable for large scale complex networks.

The main computational bottleneck for the use of this strategy is the large number of the collection of vertex covers of a sparse network. Also, in order to compute this collection, the available implementations of graph-theoretic algorithms are very slow. We propose here a different approach to this computation using computational commutative algebra algorithms. Given any simple graph (such as a network), the minimal vertex covers of the graph are in one to one correspondence to the generators of the Alexander dual of its edge ideal, cf. [4, 6]. We use this correspondence and compute covering degrees and indices of networks using algorithms for computing the Alexander dual of monomial ideals, in particular those implemented in the software Frobby [2]. This shows better performance than the graph-theoretic algorithms and can be highly improved, for the algorithms we used are designed for general monomial ideals.

One can take clear advantage of the fact that edge ideals are squarefree. Previous experience shows that a multiplying factor can be expected in the size of the networks that can be studied using these algorithms. This is work in progress.

The paper describes the proposed strategies, gives account of extensive experimentation on model networks and application to actual real world social networks and describes details on algorithmic considerations.

References

[1] R. Albert, H. Jeong and A.L. Barabási, Attack and error tolerance of complex networks, *Nature* 406:378-382, 2000

[2] B. H. Roune, *Frobby version 0.9 - a software system for computations with monomial ideals*, available at `http://www.broune.com/frobby`

[3] P. Holme, B.J. Kim, C.N. Yoon and S.K. Han, Attack vulnerability of complex networks, *Phys. Rev. E* 65, 14 pages, 2002

[4] E. Miller and B. Sturmfels, *Combinatorial Commutative Algebra*, Springer Verlag, 2004

[5] M.E.J. Newman, The structure and function of complex networks *SIAM Review* 45:167-256, 2003

[6] R. Villarreal, *Monomial Algebras*, Marcel Dekker, 2001

Universidad de La Rioja
E-mail address: `eduardo.saenz-de-cabezon@unirioja.es`

London School of Economics
E-mail address: `H.Wynn@lse.ac.uk`