Malware spreading and critical nodes in multi-layered networks under computer viruses attack

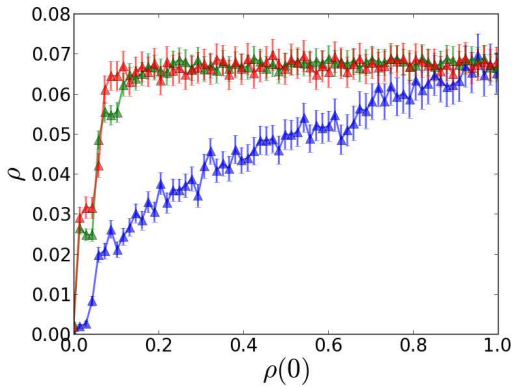
Rafael Vida[†], Javier Galeano, Sara Cuenda[‡]
Complex System Group (GSC), Universidad Politécnica de Madrid

Computer viruses are evolving by developing spreading mechanisms based on the use of multiple vectors of propagation adapted to different kinds of vulnerabilities. The use of the social network as an extra vector of attack to penetrate the security measures in IP networks is improving the effectiveness of the malware, and have therefore been used by new and most aggressive viruses, like Conficker and Stuxnet[1]. These multi-vector viruses can be modeled in multi-layered networks in which each node belongs simultaneously to different layers, adapting the spreading vector to the properties of the layer.

In particular, we study the propagation of a SIS model on a multi-layer network where the state of each node is layer-independent and the dynamics in each network follows either a contact process or a reactive process, with different propagation rates. We show that the interplay between the layers leads to a non-trivial contagion matrix[2].

As an example, we apply this study to a multi-layered network formed by two layers: the social network of collaboration of the Spanish scientific community of Statistical Physics, FisEs, and the telecommunication network of each institution.

We also analyze the spreading of a virus in a multi-layered network formed by M layers for different network couplings. In the figure we show the density of infected nodes in the quasi stationary state, ρ, vs. the density of infected nodes in the initial seed, $\rho(0)$, in the FisEs network. The infection strategy is based on the strength of nodes in the contagion matrix. The contagion rates are $\beta_1 = 1.0$, $\beta_2 = 0.0$ (blue); $\beta_1 = 0.0$, $\beta_2 = 0.027$ (green) and $\beta_1 = 0.18$, $\beta_2 = 0.02$ (red).



[†] Dept. de Sistemas Informáticos, E. T. S. de Ingeniería (ICAI), Univ. Pontificia de Comillas.
[‡] Dept. Economía Cuantitativa, Universidad Autónoma de Madrid.

[1] V. Antoine, R. Bongiorni, A. Borza, P. Bosmajian, D. Duesterhaus, M. Dransfield, B. Eppinger, K. Gallicchio, J. Houser, A. Kim, et al. Router security configuration guide, version 1.1 b. Technical Report C4-040R-02, System and Network Attack Center (SNAC), National Security Agency (NSA) (2003).
[2] R. Vida, J. Galeano and S. Cuenda. ArXiv:1310.0741 [physics.soc-ph].