Dynamic counter-measure placements for network security: a hybrid AI/OR approach

Yann Dujardin[1], Nancy Perrot[1], Morgan Chopin[1], Lionel Tailhardat[1]
[1] Orange Innovation, France
{yann.dujardin,nancy.perrot,morgan.chopin,lionel.tailhardat}@orange.com

Mots-clés *: Markov decision processses, ILP, hybrid OR/IA, cybersecurity, communication networks*

Résumé

Telecommunication networks virtualization will facilitate dynamic physical resources allocations to virtual functions and services. Some recent works exploit this capacity in term of counter-measures (CM) placements aiming at stopping/reducing cyber-attacks impacts on networks [1,2]. However the proposed solutions only consider static or bi-level cases, stating that network vulnerabilities are constant (in time). In reality vulnerabilities can evolve in time and dynamic CM placements are more appropriate to get a maximal security. Finding optimal policies of (dynamic) CM placements is very hard (not tractable) since it requires to solve optimization/planning algorithms with very large states space, under uncertainty. However, one can try to reduce the complexity of the problem (so the computing time) when looking only for approximate solutions. In this talk we propose a new approach, hybriding Markov Decision Processes and Linear Programming, that can generate approximate solutions (policies) with performance guarantees, while exploiting the existing static approaches.

Références

[1] Bazgan, C., Beaujean, P., & Gourdin, É. (2018, December). Relaxation and Matrix Randomized Rounding for the Maximum Spectral Subgraph Problem. In International Conference on Combinatorial Optimization and Applications (pp. 108-122). Springer, Cham.

[2] Mahjoub, A. R., Naghmouchi, M. Y., & Perrot, N. (2018). A bilevel programming model for proactive countermeasure selection in complex ICT systems. Electronic Notes in Discrete Mathematics, 64, 295-304