Graph community metrics as a reliable and time robust tool to detect cyber-attacks

Julien Michel*[1] and Pierre Parrend

[1]Laboratoire des sciences de l'ingénieur, de l'informatique et de l'imagerie – Ecole Nationale du Génie de l'Eau et de l'Environnement de Strasbourg, université de Strasbourg, Institut National des Sciences Appliquées - Strasbourg, Centre National de la Recherche Scientifique, Matériaux et nanosciences d'Alsace, Réseau nanophotonique et optique – France

Résumé

Attack detection in internet traffic networks proves to be a challenge as detection systems aim to detect different and evolving types of attacks in an ever changing environment of detection. In this paper we propose to build dynamic graph representations of the traffic dataset to represent the topology of the network from IP addresses or ports on different time windows. Those graph representations are then partitioned as communities of nodes and graph community metrics are computed from each community. The information contained in those metrics is highly related to the topology of the network in the corresponding time windows which is not accessible from net flow base features. Those communities and graph community metrics are then matched between all the states of the dynamic graphs corresponding to a time window to compute dynamic graph community metrics which add information about the evolution in the topology of the network. The set of our features leads to an increase in the detection performances across all types of attack in the UGR16 dataset while trying to use minimal amount of knowledge an attacker could use to mitigate the detection performance.

*Intervenant