A framework for optimizing the deployment of intrusion detection systems in social networks and within the telecom infrastructure. The framework includes a variety of optimization algorithms and a network simulator. The former are used to analyze the topology of a network and suggest optimal inspection points to collect forensic data and filter out malware. The latter simulates propagation of malicious software, evaluates the effectiveness of the deployment and performs what-if analysis.


