Fractal Dimensionality of Network Traffic as a Feature for Intrusion Detection

Viktoras Bulavas

Institute of Data Science and Digital Technologies
Vilnius University
viktoras.bulavas@itpc.vu.lt

Cyber threats are an evolving aspect of our daily lives, intrusion detection being one of the remedies to address information security breach. Intrusion detection relies on observation of network traffic features and their dynamics in time, which allows intrusion detection systems to prevent certain types of attacks upon detection. While rule based systems are following decision trees of prescribed conditions, anomaly recognition systems await for deviation from usual behavior of network users. While multiple event counters help rule-based recognition, various aggregates are calculated in order to detect anomalies. Based on the analogy of successful use of fractal features to recognize patterns in other fields of application including signal analysis, an experiment with network traffic dataset CSE-CIC-IDS2018 was setup to study fractal dimension features of network traffic as a possible indication of a cyber-attack. Network traffic aggregates were represented as two-dimensional images, further presented as an animation, allowing real time observation of the development of an attack. To support cyber-attack detection, Box-Counting calculation according to T. Higuchi algorithm was performed to extract fractal dimension of a given timeframe traffic block. Maximum values were observed at the time of an attack and minimum following the successful attack. These results are in line with dataset events, confirming a possibility to use this feature for supporting real time detection of cyber-attack.