Self-adaptive, deep learning model for the detection and classification of Network and Host-level attacks

Nelson Ochieng

Faculty of Information Technology, Strathmore University, Nairobi, Kenya

Intelligent computer and network attack detection is the topic of this study. Existing classification and detection models are built using static and old datasets and hence are not self-adaptive to changing network conditions. The models are also mostly evaluated using accuracy alone. Complexity, appropriateness, execution time and understandability are not considered. It is the argument of this study that these would be quite useful and would help in determining the appropriate model that could be implemented in a vendor product. This study collects and curates its own dataset, and therefore investigates various deep learning techniques on it. The outcome is the dataset which can later be standardized as a benchmark, and a comprehensively evaluated self-adaptive model for classification and detection of network attacks.

Keywords: Deep learning; network and host attacks; network attack detection