

In this paper, the problem of detecting adversarial methods on the basis of mimicry against locality-based classifiers has been studied in detail. In particular, the locality-based mimicry by noise generation slightly outperformed the padding-based method, but both approaches strengthened the importance of acquiring a representative set of observations for building a more robust adversarial model. An exhaustive revision of the state-of-the-art has been conducted, from which locality-based mimicry by action pruning and noise generation were presented as effective methods for thwarting conventional machine-learning-based masquerade detection capabilities.