Nonnegative matrix factorization and metamorphic malware detection

ABSTRACT

Metamorphic malware change their internal code structure by adopting code obfuscation technique while maintaining their malicious functionality during each infection. This causes change of their signature pattern across each infection and makes signature based detection particularly difficult. In this paper, through static analysis, we use similarity score from matrix factorization technique called Nonnegative Matrix Factorization for detecting challenging metamorphic malware. We apply this technique using structural compression ratio and entropy features and compare our results with previous eigenvector-based techniques. Experimental results from three malware datasets show this is a promising technique as the accuracy detection is more than 95%.

Keyword: Metamorphic malware; Nonnegative matrix factorization; Dimension reduction; Structural analysis