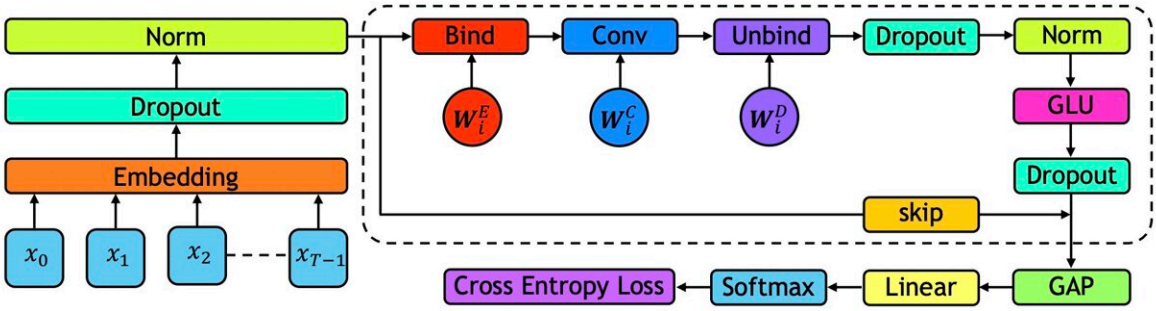
Tackling long-range malware detection tasks using holographic global convolutional networks

May 21 2024, by Ingrid Fadelli



Block diagram of the proposed method. The dotted region shows a single layer of the proposed network which is repeated N times. In the figure, prenorm is applied. In the case of postnorm, normalization is applied after the GLU layer before the skip connection. Credit: Alam et al.

Over the past few decades, cyber-attackers have devised increasingly sophisticated malware that can disrupt the functioning of computer systems or grant them access to sensitive data. The development of techniques that can reliably detect the presence of malware and determine the "family" to which they belong could be highly advantageous, as it could help to neutralize them rapidly, before they cause significant damage.

Researchers at University of Maryland and Booz Allen Hamilton have recently introduced a new computational model designed to complete long-range malware detection tasks. These are tasks that entail the identification and analysis of sophisticated malware designed to circumvent traditional security measures, typically by looking at anomalies or subtle indicators of a system being compromised.

The team's new model, introduced in a paper pre-published on *arXiv*, leverages the capabilities of a particular class of machine learning algorithms, known as holographic global convolutional networks (HGConv). HGConv networks are particularly well-suited for capturing long-range dependencies and the general context in which an event occurs, thus gathering deeper insight about the relationships between various elements in data.

As part of their study, the researchers first reviewed previous efforts at long-range malware detection, examining the results achieved by existing techniques and benchmark approaches. Overall, they found that previously proposed methods are not particularly well-suited for long-range malware detection, which inspired them to devise an alternative technique.

"We introduce HGConv that utilize the properties of Holographic Reduced Representations (HRR) to encode and decode features from sequence elements," Mohammad Mahmudul Alam, Edward Raff, and their collaborators wrote in their paper. "Unlike other global convolutional methods, our method does not require any intricate kernel computation or crafted kernel design. HGConv kernels are defined as simple parameters learned through backpropagation."

The researchers have so far evaluated their proposed method for long-range malware detection in a series of tests, focusing on practical malware classification problems. They used common malware

classification benchmarks, including Microsoft Windows Malware, Android application packages, the Drebin dataset's malware benchmark, and the EMBER benchmark.

The team compared their model's performance to both baseline methods and other recently developed machine learning techniques for malware classification. Their findings were highly promising, with their model outperforming other techniques in terms of execution time and attaining an accuracy of 99.3% on the Kaggle dataset and 91.0% on the Drebin dataset.

"The proposed method has achieved new state-of-the-art results on Microsoft Malware Classification Challenge, Drebin, and EMBER malware benchmarks," the team wrote in their paper. "With log-linear complexity in sequence length, the empirical results demonstrate substantially faster run-time by HGConv compared to other methods achieving far more efficient scaling even with sequence length ≥ 100,000."

The new HGConv-based method for long-range malware detection developed by Alam, Raff and their colleagues could soon be improved further and tested on a wider range of malware detection tasks. In the future, it could be deployed in real-world settings, helping users to rapidly spot malware on computer systems and mitigate their adverse impact.

More information: Mohammad Mahmudul Alam et al, Holographic Global Convolutional Networks for Long-Range Prediction Tasks in Malware Detection, *arXiv* (2024). DOI: 10.48550/arxiv.2403.17978

© 2024 Science X Network

Citation: Tackling long-range malware detection tasks using holographic global convolutional networks (2024, May 21) retrieved 17 July 2024 from https://techxplore.com/news/2024-05-tackling-range-malware-tasks-holographic.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.