Contribution ID: **84** Type: **Študenti informatika**

Explainable Malware Detection via Relational Graph Neural Networks with Bidirectional Relations

Wednesday, November 26, 2025 3:26 PM (1 minute)

Graph Neural Networks (GNNs) are increasingly applied to cybersecurity tasks such as malware detection, intrusion detection, and program analysis, as they can model structured program representations and capture relational dependencies beyond flat feature vectors. However, their black-box nature poses challenges in security-critical do- mains, where analysts and stakeholders require explanations for trust and forensic analysis. This has motivated growing interest in explainable GNNs (XGNNs), which aim to provide interpretable insights into model decisions. In this work, we investigate Relational Graph Convolutional Networks (R-GCNs) for ontology-based malware detection. We introduce a proof-of-concept framework that incorporates bidirectional relations through edge reversal to strengthen semantic representation.
Experimental results on the numeric subset of the Ontology–Knowledge Graph EMBER dataset (1,000 binaries) show that bidirectional relations substantially improve performance: R-GCN with edge reversal (RGCN2) achieved 98% accuracy and true positive rate (TPR), compared to 67% in baseline models, and delivered 87% fidelity with the Captum explainer. These findings demonstrate the effectiveness of relational GNNs in leveraging semantic structures for robust and interpretable malware detection.

Pracovisko fakulty (katedra)/ Department of Faculty

Department of Applied Informatics

Tlač postru/ Print poster

Budem požadovať tlač /I hereby required to print the poster in faculty

Author: ONOJA, Monday (Department of Applied Informatics, Faculty of Mathematics Physic and informatics Comenius University in Bratislava)

Co-authors: HOMOLA, Martin; ANTHONY, Peter; Mr ADAMS, Zekeri (Department of Applied Informatics, Faculty of Mathematics Physic and informatics Comenius University in Bratislava)

Session Classification: Poster session + káva: prezentácie vedeckých výsledkov FMFI UK Zamestnanci Informatika

Track Classification: Poster session + káva: prezentácie študentov: Poster session + káva: prezentácie študentov informatika