الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي - 08 ماي 1945 – بسيدي بلعباس
Ecole Supérieure en Informatique
- 08 Mai 1945 - Sidi Bel Abbes

Mémoire de Fin d'étude

En Vue de l'obtention du diplôme d'**Ingénieur d'Etat**

Filière : **Informatique**

Spécialité : Ingénierie des Systèmes Informatiques (ISI)

Thème

E-GNNExplainer: Single-Instance Explanation of Edge-Classification Graph Neural Networks-based Network Intrusion Detection Systems

Présenté par :

Mr. **BAAHMED Ahmed-Rafik-El Mehdi**

Soutenu le : 04/07/2023 Devant le jury composé de :

Dr. BENDAOUD Fayssal	Président
Dr. KHALDI Belkacem	Examinateur
Prof. RAHMOUN Abdellatif	Encadrant
Prof. ROBARDET Céline	Co-Encadrante

Année Universitaire : 2022/2023

Abstract

The ever-increasing evolution of deep learning methods has made it possible to apply them in all fields, more specifically in the field of cybersecurity. With the exponential growth of the volume of data circulating in the global network, network security becomes a paramount necessity, by applying different security mechanisms such as Network Intrusion Detection Systems.

The intersection between deep learning and network intrusion detection systems has achieved much success, in particular, by considering the topological data structure of the networks to secure them by applying Graph Neural Networks, an emerging sub-field of deep learning, based on the study of the graph structure. Recently, explaining artificial intelligence methods has become an important task, especially when working on a sensitive area such as cybersecurity, however, there is a lack of study for the explainability on Graph Neural Networks.

In this Engineering degree report, we introduced the main aspects of network intrusion detection systems, and the graph neural networks approach. Then we introduced the notions of explainable artificial intelligence and presented the state of the art of explainability methods employed to explain graph neural networks. Finally, we presented an experimental work that consists of explaining graph neural networks working on the edge-classification task, and we proposed our developed approach that allows explaining this type of graph neural networks.

Keywords : Explainable Artificial Intelligence, Graph Neural Networks, Machine Learning, Deep Learning, Network Intrusion Detection Systems, Cybersecurity.

Ackowledgements

Thank you ALLAH for giving me the blessings, good health, strength, courage and the patience to accomplish this work and achieve this valuable success that brings the happiness to everyone around me.

To begin my dedications and thanks, I would like to present my deepest gratitude and appreciation to my dearest loved ones who have never said no to my exigences, my lovely parents BENALLAL Khadidja and BAAHMED Mohamed Amine Kadda. They gave me the best motivation, support and advices that allows me to improve and achieve all the successes in my life.

To my sisters, Amira Ghizlene and Ferdous Yasmine, that always believed in me and gave me all the positive energy, thank you for your moral and physical support.

At the end of this work, I would like to thank my supervisors Prof. RAHMOUN Abdellatif and Prof. ROBARDET Céline for their efforts and great advices for performing this research. Working under their direction was such an honor for me and they gave me a great experience. I would also like to thank Prof. APPICE Annalisa and Prof. ANDRESINI Giuseppina for their valuable assistance and domain knowledge to achieve this work.

I would like to express my sincere and deepest thanks to my dear friends HARIRI Ali, DELANDA Lahcen, SMATI Meriem, BENGUEDDA Ilhem, GREBICI Nour and LOUADJ Rania. Thank you for providing the best atmosphere and good mood that help us to overcome all the obstacles. Without forgetting my professors who, with the help of their learning and teaching, I passed all the steps to become an engineer.

Special thanks to Prof. RAHMOUN Abdellatif, Mr. ACED Mohamed Réda, Prof. BENSLIMANE Sidi Mohammed and Prof. AMAR BENSABER Djamel, for having given me the best of them throughout my five years of study, for always considering me as their son and always pushing me for the best.

I would like to express, through these few lines of thanks, my gratitude to my ESI-SBA family, my Alphabit Family, for giving me the best educational path and the best five years of my life, and ll those in whom, through their presence, their support and their advice, I found the enthusiasm to accomplish this project.

List of abbreviations and acronyms

XAI	*eXplainable Artificial Intelligence*
GNN	*Graph Neural Networks*
CSRC	*Computer Security Resource Center*
NIST	*National Institute of Standards and Technology*
IDS	*Intrusion Detection System*
NIDS	*Network-based IDS*
HIDS	*Host-based IDS*
AIDS	*Anomaly-based IDS*
SIDS	*Signature-based IDS*
IPS	*Intrusion Prevention System*
NIST	*National Institute of Standards and Technology*
AI	*Artificial Intelligence*

ML	*Machine Learning*
DL	*Deep Learning*
DR	*Detection Rate*
FPR	*False Positive Rate*
LIME	*Local Interpretable Model Agnostic Explanation*
SP-LIME	*Submodular Pick Local Interpretable Model Agnostic Explanation*
SHAP	*SHapley Additive exPlanations*
LOCO	*Leave One Covariate Out*
DeepLIFT	*Deep Learning Important FeaTure*
LRP	*LayerWise Relevance Propagation*
TCAV	*Testing with Concept Activation Vector*
GIRP	*Global Interpretation via Recursive Partitioning*
GIRP	*Global Interpretation via Recursive Partitioning*