**ACKNOWLEDGMENT**

I would like to express my sincere gratitude for my family and friends for their support throughout the thesis process. I am also grateful to Professor Tran Hai Anh for his kind and thoughtful feedback during thesis process.

**ABSTRACT**

The ever-evolving cybersecurity landscape presents significant challenges for Intrusion Detection Systems (IDS), necessitating the ability to continually adapt to novel attacks and shifting attack patterns. Traditional IDS models often rely on complete retraining when encountering new attack types, a resource-intensive and inefficient process. This thesis proposes a novel Class Incremental Learning (CIL) approach to IDS, allowing the model to dynamically learn new attack classes while preserving previously acquired knowledge. Inspired by cutting-edge image classification CIL models, this method leverages a knowledge distillation framework. This framework facilitates the transfer of knowledge from a robust pre-trained model to a dynamically expanding network dedicated to handling new attack classes. Two dynamic networks from image classification CIL (DER and MEMO) are implemented and their performance compared across multiple IDS datasets. The thesis demonstrates the potential of model-centric CIL in constructing adaptive and robust IDS capable of effectively addressing the dynamic threat landscape.

Table of Contents

[Chapter 1. Introduction 2](#_Toc155124144)

# Chapter 1. Introduction

* 1. Problem statement
  2. Background and Problems of Research
  3. Research Objectives and Conceptual Framework
  4. Contributions

In summary, we make the following contributions in this paper:

1. We apply DER, MEMO model from Image Classification field to Network Intrusion Detection domain.
2. We compare the results of those model in 4 dataset KDD99, UNSW\_NB15, TON\_IOT\_NETWORK, CIC-IDS2017.
3. We test the performance of these dataset in custom dataset and analyze the result.
   1. Organization of Thesis

The remainder of this paper is arranged as follows: Section II presents related work; Section III describes our proposed incremental learning algorithm; Section IV explains the experimental setup of this research, Section V presents a summary of the experimental results. Section VI discusses the challenges of implementing the proposed incremental algorithm in the network intrusion detection problem; and Section VII provides our conclusion and future work.

Chapter 2. Literature Review

2.1 Scope of Research

2.2 Related Work

Chapter 3. Methodology

Methodology

1. Overview

Trong phần này mình sẽ giới thiệu các kiến trúc dynamic model dùng trong bài toán Class Incremental Learning. Đầu tiên mình sẽ nói qua về các kiến trúc mình dùng. Tuy nhiên các kiến trúc này được có nguồn gốc từ domain phân loại ảnh trong CIL. Nên mình sẽ trình bày về kiến trúc mình dùng đối với bài toán Network Intrusion Detection Problem.

1. DER Model

DER model

* 1. The paper DER: Dynamic Expandable Representation for Class Incremental Learning introduces expandable representation. At step , the model is composed of a super feature extractor is build by expanding the feature extractor with a newly created extractor . Specifically, given an image , the feature extracted by is obtained by concatenation as follows

Here reuse the previous and encourage the new extractor to learn only the novel aspect of new classes. The feature u is then fed into the classifier to make predictions as follows

= Softmax())

Then the prediction y = argmaxp\_h\_t(y|x). The classifier is designed to match its new input and output dimension for step t. The parameters of H\_t for the old features are inherited from H\_t-1 to retain old knowledge and its newly added parameters are randomly initialized.

To reduce catastrophic forgetting, we freeze the learned function at step t, as it captures the intrinsic structure of previous data. In detail, the parameters of last step super-feature extractor , and the statistics of Batch Normalization are not updated. Besides, we instantiate Ft with Ft-1 as initialization to reuse previous knowledge for fast adaptation and forward transfer.

1. MEMO Model

MEMO Model: (Memory-Efficient Expandable Model)

The model from Paper A Model or 603 Exemplars: Toward Memory-Efficient Class-Incremental Learning try to solve the problem of expanding memory by answering the question: Given the same memory budget, if we share the generalized block and only extend specialized blocks for new tasks, can we further improve the performance?

Concretely, we redefine the model structure by decomposing the embedding module into specialized and generalized blocks. Specialized blocks correspond to the deep layers in the network, while generalized blocks corresponds to the rest shallow layers. We argue that the features of shallow layers can be shared across different incremental stages, i.e., there is no need to create an extra model.