Universität des Saarlandes
MI Fakultät für Mathematik und Informatik
Department of Computer Science

Bachelor's Thesis

Link Stealing Attacks on Inductive Trained Graph Neural Networks

submitted by

Philipp Zimmermann

on

15. June 2021

Reviewers

asdf

asdf

Abstract

Acknowledgment

Contents

Chapter 1

Introduction

Chapter 2

Technical Background

2.1 Neural Networks

2.2 Graphs

Chapter 3

Graph Neural Networks

3.1 Transductive Learning

3.2 Inductive Learning

3.3 GraphSAGE

3.4 Graph Attention Network

3.5 Graph Convolution Networks

Chapter 4

Privacy Issues on GNNs

4.1 Link Stealing Attack

Chapter 5

Experiment

5.1 Setup

5.1.1 Target Models

5.1.2 Attacker Model

5.2 Datasets

5.2.1 Attacker Sampled Dataset

5.3 Attacks

5.3.1 Attack 1

Description

5.3.2 Attack 2

Description

5.4 Evaluation

Chapter 6

Conclusion

6.1 Consequences in Machine Learning

6.2 Consequences in Society