

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

1	Introduction	7
2	Technical Background	9
2.1	Machine Learning	9
2.1.1	Neural Networks	9
2.2	Graphs	9
3	Graph Neural Networks	11
3.1	Transductive Learning	11
3.2	Inductive Learning	11
3.3	Different Types	11
3.3.1	GraphSAGE	11
3.3.2	Graph Attention Network	11
3.3.3	Graph Convolution Networks	11
4	Privacy Issues on GNNs	13
4.1	Link Stealing Attack	13
5	Experiment	15
5.1	Setup	15
5.1.1	Target Models	15
5.1.2	Attacker Model	15
5.2	Datasets	15
5.2.1	Attacker Sampled Dataset	15
5.3	Attacks	15
5.3.1	Attack 1	15
5.3.2	Attack 2	15
5.4	Evaluation	15

6	Conclusion	17
6.1	Consequences in Machine Learning	17
6.2	Consequences for Society	17

Chapter 1

Introduction

Chapter 2

Technical Background

2.1 Machine Learning

Machine Learning is a branch of Artificial Intelligence (AI), where so called Machine Learning Models try to improve their accuracy, based on given data, that was used for training earlier [2]. In that way, Machine Learning (ML) Models try to predict future behavior given unseen data, while considering prior learned knowledge.

This is done by first finding a mathematical / formal description of the problem. [1]

2.1.1 Neural Networks

2.2 Graphs

Chapter 3

Graph Neural Networks

3.1 Transductive Learning

3.2 Inductive Learning

3.3 Different Types

3.3.1 GraphSAGE

3.3.2 Graph Attention Network

3.3.3 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 for Society

References

Bibliography

- [1] Alex Kozlenkov. *PROVA a Language for Rule-based Java Scripting, Data and Computation Integration, and Agent Programming*. City University, London, May 2005. User's Guide, Version 1.8. 9
- [2] Osvaldo Simeone. A brief introduction to machine learning for engineers, 2018. 9