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

Since nowadays graphs are a common way to store and visualize data, Machine Learning algorithms have been improved to directly operate on them. In most cases the graph itself can be deemed confidential, since the owner of the data often spends much time and resources collecting and preparing the data. In our work, we show, that so called Graph Neural Networks can reveal sensitive information about their training graph. We focused on extracting information about the edges of the underlaying graph by observing the predictions of the target model in so called link stealing attacks. present results

Acknowledgment

write at the end

Contents

Chapter 1

Introduction

1.1 Motivation

A graph is a datastructure which is used to model large data and the relationships between entities. It consists of nodes and edges and can be used to model data in almost every domain. For example in social networks, healthcare analytics or protein-protein interactions. In a social network, the nodes would be the users that are registered and the edges would represent whether the users know each other or not by connecting them or not. A graph itself can be deemed as intellectual property of the data owner, since she may spent lots of time and resources collecting and preparing the data. In most cases the graph is also highly confidential because it contains sensitive information like private social relationships between users in a social network or medical information about specific people in healthcare-analytic datasets.

1.2 Outline

write at the end

Chapter 2

Related Work

Chapter 3

Technical Background

3.1 Neural Networks

3.2 Graphs

As Graph we denote a data structure that contains nodes and edges. A node can have multiple attributes describing it and an edge describes the relationship between them. The most popular example where graphs are used are social networks. The nodes represent the users that have multiple attributes like location, gender, work place etc. In a directed graph user A will have an outgoing edge and user B an ingoing edge if A follows B and vice versa. In an undirected graph the edge won't have a direction. Which means that either A follows B, B follows A or both will lead to the same result, namely only one edge that is drawn, describing their relationship.

3.3 Graph Neural Networks

Bibliography