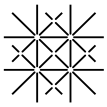

University of Basel

Secure and History-Aware Peer-to-Peer Set Synchronization on Android

Bachelors Thesis)

Faculty of Science of the University of Basel
Department of Mathematics and Computer Science
Computer Networks Research Group
https://cn.dmi.unibas.ch/

Examiner: Examiner: Prof. Dr. Christian Tschudin)
Supervisor: Supervisor: Claudio Marxer, MSc.

David Seger
david.seger@stud.unibas.ch
17-054-693

Hand-In-Date

Abstract

Hier könnte ihre Werbung stehen

Table of Contents

1 Introduction

In an infrastructure less environment, such as a peer-to-peer(p2p) network, there is no regulating body that manages the synchronization of content between devices. While this type of network has advantages such as scalability and reliability, it does require different protocols than the more commonly used server based architecture. One of the challenges posed by decentralized networks is the synchronization of content across the participants, especially considering that in a peer-to-peer environment, data can take different paths to arrive at its destination, contrary to the single-distributer concept of server/client networks. As efficiency is key in the growth of new technologies, the need for a fast and secure commmunication protocol between peers arises.

1.1 Append Only Set Synchronization

Many usages of network communication can be broken down to a set synchronization problem, meaning we have to synchronize a dataset across multiple participants, that each might have added things to the set, bringing them all up to the correct state. A subcategory of this problem is the append only set synchronization, this simplifies the problem setting, since in an append only set new elements must always be inserted at the end of a dataset, removing the need to check the whole collection every time a synchronization is to be done. Append only sets can be found in many different network-related uses, for example social media or games.

1.2 History Awareness

Due to the abscence of a central device that regulates all network activity, a decentralized environment needs to self-regulate, effectively transforming every peer into both a server and a client. As every device has to regulate its own connection, the performance of a synchronization can be greatly increased by adding meta-data about past connections with peers, this is called history awareness. While this approach uses more storage space, it has the potential to greatly improve efficiency and therefore user friendliness.

1.3 Security

As there are many risks in any kind of wireless communication, a direct connection between two peers must ensure that the devices are connected to the right partner and that the messages between these partner can not be read or altered by any, potentially malicious, third party.

1.4 The Goal of this Thesis and the general outline

The aim of this work is to design a protocol allowing participants in a p2p network to efficiently synchronize an append only set, by utilizing history awareness. Furthermore the protocol will be securely implemented in an android app as prove of concept.

This thesis will first take a look at related work that will be the basis for the practical part of the project, mainly the scuttlebutt protocol and the work of Gowthaman Gobalasingam, who built the app that will function as the starting point for the implementation. After this, the protocol and how it came to be will be explained in detail. Next, the implementation of the designed protocol in the android app will be discussed, which will lead into an evaluation of the advantages and disadvantages of the method. Finally, possible future work and usages of the created app will be explored.

A

Appendix

Declaration on Scientific Integrity
Erklärung zur wissenschaftlichen Redlichkeit

includes Declaration on Plagiarism and Fraud
beinhaltet Erklärung zu Plagiat und Betrug

Author — Autor
David Seger

Matriculation number — Matrikelnummer
17-054-693

Title of work — Titel der Arbeit
Secure and History-Aware Peer-to-Peer Set Synchronization on Android

Type of work — Typ der Arbeit
Bachelors Thesis)

Declaration — Erklärung
I hereby declare that this submission is my own work and that I have fully acknowledged the assistance received in completing this work and that it contains no material that has not been formally acknowledged. I have mentioned all source materials used and have cited these in accordance with recognised scientific rules.

Hiermit erkläre ich, dass mir bei der Abfassung dieser Arbeit nur die darin angegebene Hilfe zuteil wurde und dass ich sie nur mit den in der Arbeit angegebenen Hilfsmitteln verfasst habe. Ich habe sämtliche verwendeten Quellen erwähnt und gemäss anerkannten wissenschaftlichen Regeln zitiert.

Basel, Hand-In-Date

Signature — Unterschrift