Summary - Efficient Point-to-Multipoint Data Reconciliation

Bowen Song[1]

August 28, 2018

***Abstract*— This report is a part of an independent study for set and string reconciliation problems in distributed systems. The patent [1] describes a solution to the problem of set reconciliation based on levels of hash hierarchy. The reconciliation scheme broadcasts top level hashes and transmits lower level hash hierarchy as encoding streams on respective communication channels. The reconciliation protocol uses decomposable hashes to make use of all parts of encoding streams.**

I. Introduction

The paper considers the problem of set reconciliation in a distributed system with a central authority server. The distributed nodes wish to receive data updates and change their local data according to the central server. The system exists in a radio broadcast environment, and most distributed nodes are user-controlled devices connected via wireless network. These devices have different receiving intervals for accepting packages at different activation period. For example, cell phones may have shorter receiving intervals than a laptop regarding battery consumption, and different users may turn on their device at different times. These varieties may cause devices to hold different versions of data. The proposed protocol hopes to broadcast the same information of the newest data version to reconcile all distributed nodes in the system.

II. Algorithm Overview

The paper proposes a protocol broadcasting *Erasure hashes* of the newest version of the entire data to update all distributed node in the network. The receiving nodes decode the *Erasure hashes* and use the *decomposing property* of the hashes to extract more information. After finding the hashes of data update at the lowest level of the hash hierarchy, the receiving nodes request to download the list of missing information from the central server.

A. Erasure Hash

The *Erasure hashing* is an encoding scheme that randomly combines hashes through linear operation in $\mathcal{F}_{16}$. An *Erasure hash* is the cross product of a *hash block* and a vector of random coefficients.

B. Decomposable Hash

Each *hash block* is a part of a hash hierarchy that can be divided into two sub-blocks in the next level. These sub-blocks have the same dimension as their parent block, but each hash represents half of the values from its corresponding parent hash. By using *decomposable homomorphic hashes*, the *hash block* a and its two sub-blocks b and c hold the property that $h(a) = h(b) + h(c)$. Therefore, for each level of the hash hierarchy, the central server only needs to send out information for half of the *hash blocks*.

C. Encoding Process

In the encoding process, the central server generates *hash blocks* for levels of increasingly smaller subdivisions of the dataset using *decomposable homomorphic hashes* to form a hash hierarchy. At each level of the hash hierarchy, the central server repeatedly computes the *Erasure Hashes* of each *hash block* based on a vector of random coefficients and broadcasts in a unique communication channel with the seed of the random coefficients. The number of communication channels is, therefore, equal to the levels of hash hierarchy.

D. Decoding Process

Based on these repeating broadcasts, the receiver node can reconcile its data in increasing order of hash hierarchy level to find out and download the smallest partition of data update at any time.

III. Algorithm Performance Analysis

There is a trade-off between the amount of bandwidth utilization and levels of hash hierarchy. With only one level of a hash hierarchy, almost all of the bandwidth utilization is from data download. As more levels of hash hierarchy are computed, the less bandwidth is spent on downloading data; however, the bandwidth for downloading hashes gradually increases.

IV. Conclusion

The protocol efficiently reconciles dataset on different hosts in a system with a central authority server by combining hierarchical, Erasure, and decomposable hashing techniques. The protocol can update all nodes in the system by repeatedly broadcasting the information. The receiving nodes are not required to be in the same state, and the communication cost on each receiving node is reduced to the minimum. The protocol is designed for radio broadcast environment and applicable in other general point-to-multipoint systems.

References

[1] P. Rodriguez and J. Chesterfield, "Efficient point-to-multipoint data reconciliation," Jul. 19 2011, uS Patent 7,984,018.

[1] B. Song is with Department of Electrical and Computer Engineering, Boston University, Boston MA, `sbowen@bu.edu`