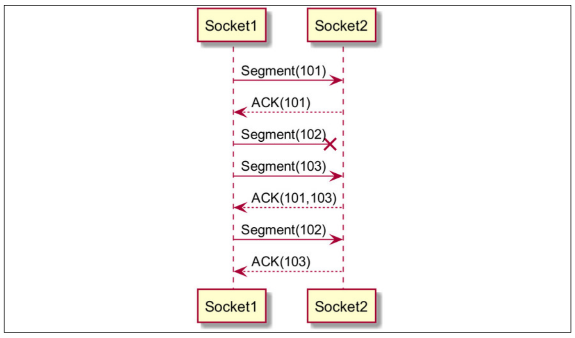
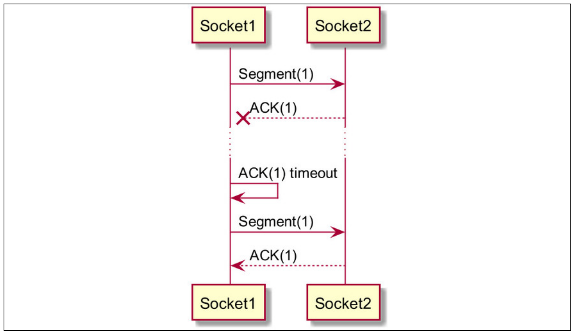
Students	Nico Stalder, Thomas Elsensohn
Examiner	Dr. Thomas Bocek
Subject Area	Internet Technologies and Applications

ATP: A 0-RTT network protocol

Secure and reliable network transmission protocol in Golang



After data loss, an out-of-order segment is detected and the sender is informed accordingly.
Own presentment



Timeout on segments will also lead to a retransmission, further ensuring all data reaches its destination
Own presentment

Introduction: TomP2P is a distributed hash table equipped with additional features, such as storing multiple values for a key. For the planned rewrite in Golang a reliable and secure protocol is required.

Due to the various problems of TCP (handshake, port binding, differences in implementation) and its focus on client-server applications, an alternative is needed. However, the two most likely candidates, QUIC and KCP, have problems of their own, which led to the decision to develop a new network protocol that is tailored for P2P systems.

Approach / Technology: The main goal of ATP was to define and implement a network protocol that closely resembles other widely used protocols in terms of usage. The following sections summarize how the key points of ATP were approached and implemented.

- Connectivity: Like QUIC and KCP, ATP uses UDP as its underlying connection interface. This forgoes the need for a specific handshake and port binding that were mentioned above as TCP's caveats. Implementation-wise, each ATP socket consists of a two-way UDP connection that is connected to another socket's endpoint.
- Reliability: To ensure data arrives in the order it was sent, most protocol implement some form of the sliding window protocol. ATP uses selective repeat ARQ (Automatic Repeat Request). Data transmitted over ATP is split into segments, each of which is assigned a sequence number. Each segment needs to be acknowledged by the receiver. In this version of ARQ, out-of-order segments are not dropped, but buffered, while the discrepancy in ordering is transmitted to the original sender. The latter will then re-transmit any (potentially) lost segments.
- Security: To ensure all data transmitted is kept private, ATP implements security features according to industry standards and with the help of proven encryption libraries and algorithms. More specifically, the main framework used is the "Noise Protocol Framework", a library that makes use of the Diffie-Hellmann key exchange as well as AES-GCM to encrypt data.

Result: The implemented protocol uses well-known industry standards to achieve reliable and secure connections between two endpoints, providing developers with appropriate tools for the communication in peer-to-peer applications.

Future work includes NAT hole punching, which, in today's network environments, is an important feature of any P2P network protocol.

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz