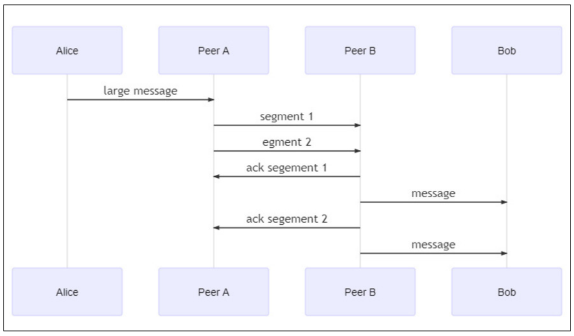
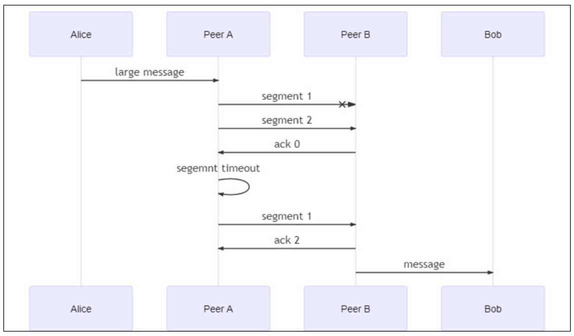
Graduate Candidate	Nico Stalder
Examiner	Prof. Laurent Metzger
Co-Examiner	Dr. Guilherme Sperb Machado, Swisscom (Schweiz) AG, Zürich, ZH
Subject Area	Networks, Security & Cloud Infrastructure

ATP: ARQ Transmission Protocol

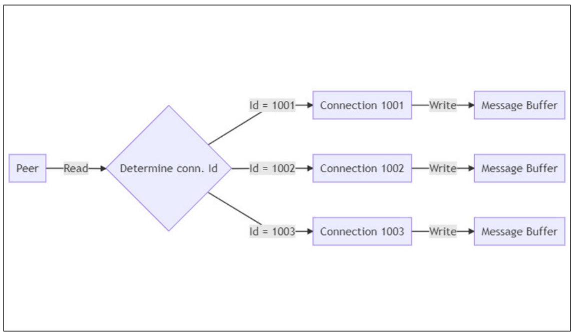
Secure and reliable peer-to-peer network protocol



Long messages are segmented and sent/acknowledged in sequence
Own presentment



Segment 1 is lost on the way to Peer B and is retransmitted after segment timeout
Own presentment



A peer reading from three separate connections with ATP's multiplexing
Own presentment

Initial Situation: ATP is designed and optimized for peer-to-peer networks.
The main features are reliability and built-in security.
It originally started as a term project in fall 2019 that resulted in a Go-lang prototype version hosted as MIT-licensed GitHub project.
This prototype already had encryption using the Noise Protocol Framework. It also featured a basic version of the selective repeat ARQ algorithm that ensured packets always arrived correctly despite potential losses and packet reordering.

Approach / Technology: The aim of this bachelor thesis was to expand the pre-existing code base with stability improvements and advanced features.

ATP's selective repeat ARQ implementation required extensive refactoring, and ended up being rewritten from scratch to completely eliminate some of the original's design flaws.
The new implementation stayed more closely to TCP's RFC description of ARQ and prepared it for the most prominent feature of this bachelor thesis: Congestion control. This mechanism is required for a network protocol of this kind to ensure connections remain as stable as possible. To achieve this, a window is maintained on every sender side that determines how much data may be in transit without acknowledging its arrival.
After examining existing standards, CUBIC was chosen as congestion control standard, a relatively new extension to the current TCP standards. As the name implies, it uses a cubic function to calculate the congestion window every time a packet is either acknowledged, or congestion event occurs (timeout, duplicate ACKs). It is especially powerful in high latency networks, but falls short of other standards in networks with very low latency. To rectify this, CUBIC uses an additional function as well as standard slow start to increase overall performance.
Next to the big features described above, ATP was extended with various smaller improvements. These include
- Cleaner interface for establishing connections and communicating with peers
- Built-in multiplexing function for communicating with multiple endpoints over the same socket
- Improved Diffie-Hellmann handshake procedure

Result: The current state of ATP can hardly be compared to the initial project and now much more closely resembles other network protocols in functionality.
With the improved flow and added congestion control, ATP is now ready to be used in actual projects.
Thanks to various performance improvements, ATP can now match industry standard protocols in speed and reliance.
All that being said, there is still room for improvement, with specialized features (e.g. NAT hole-punching) planned for future work.

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz