We have the following problem that may be interesting to other people:

1 There are N

servers out of which less than 1/3N

are Byzantine.

2 We want to save a file F

to these servers, so that a client later can pull the file from the servers.

3 Ideally the client attempts to open N

TCP connections in parallel to all of these servers and starts downloading erasure coded segments. Then nomatter what the bad guys do (they can fail to respond or respond with corrupt data), the client should be able to reconstruct the file and there should be no timeouts in the protocol

A trivial solution without erasure coding is to make N

parallel attempts to pull the entire file from all of the servers, but this will introduce lots of wasteful network traffic.

Ideally you ask each server for a verifiable erasure coded segment, and once you receive 2/3N

segments you verify each of them and reconstruct the file while minimizing the network traffic.

Does anyone know what is the most optimal algorithm/protocol for this?