



Implementing a Reliable Data Transport Protocol

1 Objectives

Since you've learned about the socket interface and how it is used by an application; by now, you're pretty much an expert in how to use the socket interface over a reliable transport layer, so now seems like a good time to implement your own socket layer and reliable transport layer! You'll get to learn how the socket interface is implemented by the kernel and how a reliable transport protocol like TCP runs on top of an unreliable delivery mechanism (which is the real world, since in real world networks nothing is reliable). This lab should be fun since your implementation will differ very little from what would be required in a real-world situation. The network communication in the upper two stages was provided through a reliable transfer protocol (TCP/IP). In this stage, you are required to implement a reliable transfer service on top of the UDP/IP protocol. In other words, you need to implement a service that guarantees the arrival of datagrams in the correct order on top of the UDP/IP protocol.

2 Reliability Specifications

2.1 Introduction and Background

Please refer to the lectures' slides for reliable data transfer techniques: Go-back-N, Stop and Wait and Selective repeat.

2.2 Specifications

Suppose you've a file and you want to send this file from one side to the other (server to client), you will need to split the file into chunks of data of fixed length and add the data of one chunk to a UDP datagram packet in the data field of the packet. Three methods for RDT should be implemented:

2.2.1 Stop-and-Wait

The server sends a single datagram, and blocks until an acknowledgment from the client is received (or until a timeout expires).

2.2.2 Selective repeat

At any given time, the server is allowed to have up to N datagrams that have not yet been acknowledged by the client. The server has to be able to buffer up to N datagrams, since it should be able to retransmit them until they get acknowledged by the client. Moreover, the server has to associate a timer with each datagram transmitted, so that it can retransmit a datagram if it is not acknowledged in time.

2.2.3 GoBackN

In a Go-Back-N (GBN) protocol, the sender is allowed to transmit multiple packets (when available) without waiting for an acknowledgment, but is constrained to have no more than some maximum allowable number, N, of unacknowledged packets in the pipeline.

2.3 Packet types and fields

There are two kinds of packets, Data packets and Ack-only packets. You can tell the type of a packet by its length. Ack packets are 8 bytes, while Data packets vary from 12 to 512 bytes (This is just an example but you're free to choose the header/data size for the packets).

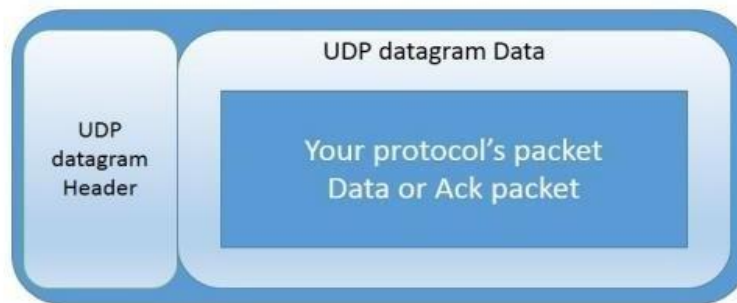


Figure 1: Including your packet inside the UDP packet.

```
1  /* Data-only packets */
2  struct packet {
3      /* Header */
4      uint16_t cksum; /* Optional bonus part */
5      uint16_t len;
6      uint32_t seqno;
7      /* Data */
8      char data[500]; /* Not always 500 bytes, can be less */
9  };

1 /* Ack-only packets are only 8 bytes */
2 struct ack_packet {
3     uint16_t cksum; /* Optional bonus part */
```

3 Lost and Corrupted Packets Simulation

Since we don't have machines with OS that we can modify, your implementation will run in a simulated environment, this means that we will simulate the packet loss probability (PLP) and corrupted packets since packet loss and corruption are infrequent in a localhost or LAN environment.

3.1 Packet Loss Specifications

PLP ranges from 0 to 1. For PLP=0 your implementation should behave with no packet loss. For non-zero values of PLP, you should simulate packet loss (by dropping datagrams given as parameters to the send() method) with the corresponding probability - i.e. a datagram given as a parameter to the send() method is transmitted only $100 \cdot (1 - \text{PLP})\%$ of the time (A value of 0.1 would mean that one in ten packets (on average) are lost.).

3.2 Corrupted Packets Specifications

The same as Packet Loss, it is required to simulate some corruption in the packets. That can be done either before sending or after receiving them (i.e. inside the client program or the server program).

4 Work flow between server and client

4.1 Flow of data

The main steps are:

1. The client sends a datagram to the server giving the filename for the transfer. This send needs to be backed up by a timeout in case the datagram is lost.
2. The server forks off a child process to handle the client.
3. The server (child) creates a UDP socket to handle file transfer to the client.
4. Server sends its first datagram, the server uses some random number generator `random()` function to decide with probability p if the datagram would be passed to the method `send()` or just ignore sending it.
5. Whenever a datagram arrives, an ACK is sent out by the client to the server.
6. If you choose to discard the package and not to send it from the server the timer will end at the server waiting for the ACK that it will never come from the client (since the packet wasn't sent to it) and the packet will be resent again from the server.
7. Update the window, and make sure to order the datagrams at the client side.
8. Repeat those steps till the whole file is sent and no other datagrams remains.
9. Close the connection.

4.2 Handling time-out

You're supposed to use timers (or a timer) at the server side to handle time-out events.

4.3 Arguments for the client

The client is to be provided with an input file `client.in` from which it reads the following information, in the order shown, one item per line :

- IP address of server.
- Well-known port number of server.
- Port number of client.
- Filename to be transferred (should be a large file).
- Initial receiving sliding-window size (in datagram units).

4.4 Arguments for the server

You should provide the server with an input file `server.in` from which it reads the following information, in the order shown, one item per line :

- Well-known port number for server.
- Maximum sending sliding-window size (in datagram units).
- Random generator seed value.
- Probability p of datagram loss (real number in the range $[0.0, 1.0]$).

5 Network system analysis

You should provide a comparison between stop-and-wait, ~~GoBackN~~ and selective repeat strategies in terms of throughput, based on a series of transfers of large files (e.g.: 4 MBytes, or higher). Your test runs should be performed with at least the following PLP values: 1%, 5%, 10% and 30%. For each PLP value, you should report the average of at least 5 (consecutive) runs.

6 Notes

- Your server should handle multiple client connections.
- You must provide a suitable way for observing the loss of packets, time-outs and resending packets.
- START SIMPLE. Set the probabilities of loss and corruption to zero and test out your routines. Better yet, design and implement your procedures for the case of no loss and no corruption, and get them working first. Then handle the case of one of these probabilities being non-zero, and then finally both being non-zero.
- You must understand thoroughly the main difference between UDP and TCP, so you can provide the functionalities of TCP-like protocol using UDP, from the main differences is the ordering of packets, reliability and Congestion control.
- Its required to implement the three techniques (Stop&Wait- Selective Repeat- GoBackN) and comparing the results between these different protocols.
- Error detection and check-summing - You will need some kind of check-summing to detect errors. The Internet checksum is a good candidate here. Remember that no check-summing can detect all errors but your checksum should have sufficient number of bits (e.g. 16 bit in Internet checksum) to make undetected errors very rare. We can not guarantee completely error-free delivery because of check-summing's limitation. But you should be convinced that this should happen very rarely with a good check-summing technique.
- The output of your program must be printed on the screen during the running time illustrating all your steps for both client and server programs.
- A report must be delivered with your implementation and testing .
- Your report must include a detailed comparison between the performance of the three techniques.
- You can work on this project in groups with max 2 students per group.

7 Bonus

- Any additional features will be highly appreciated.
- Capture the traffic between your client and server using the proper packet capture and sniffing tools if possible (highly ranked)

8 Reference

Textbook: computer networking top down approach section

2.7 socket programming

3.4 Principles of Reliable Data Transfer

Good Luck