

### 4.2.2 Task #2: Attack details

The attack lasts for **0.17s** every **1s**, with a burst rate of **10Mbps**

Reason:

According to section 3.2 in the shrew paper, the attack duration minus the time to fill up the TCP buffer should be greater than the RTT, which is 0.12s. The time to fill up a buffer with size 20 is approximately 0.05s, given a packet rate of approximately 400 per second. In this way, attack duration should be at least  $0.12 + 0.05 = 0.17s$ .

The minRTO should be divisible by the attack period T, with a minRTO of 1s, the maximum value for T is 1s.

The burst rate should be as high as possible, which is 10Mbps.

### 4.3.1 Task #1: Understanding the attack period

Case 1:  $T > \text{minRTO}$ , in this case,  $p(T) = (T - \text{minRTO}) / T$ , which increases with T.

Case 2:  $T \leq \text{minRTO}$ , in this case,  $p(T) = 0$  if and only if minRTO is divisible by T.

To reduce the traffic rate, we should choose the maximum T in case 2, which is minRTO.

### 4.3.2 Task #2: Increase buffer size

The attack is not successful this time.

The packet rate of the TCP connection from hr1 to hl1 is approximately 400 packets per second, according to part3\_task2\_tcpprobe.txt. To fill up the buffer size of 1000, it takes at least 2s, which is much longer than the attack duration. In this way, the condition C1 in section 3.2 is no longer satisfied, making the shrew attack fail.