For TLS1.3

T-statistic: 1.8600

P-value: 0.0646

Result: Accept the null hypothesis (no significant difference between means)

For Kyber512

T-statistic: 0.9811

P-value: 0.3273

Result: Accept the null hypothesis (no significant difference between means)

For Kyber768

T-statistic: 2.9047

P-value: 0.0041

Result: Reject the null hypothesis (means are significantly different)

For Kyber1024

T-statistic: 1.8600

P-value: 0.0646

Result: Accept the null hypothesis (no significant difference between means)

Regarding the RTT measurements used to evaluate the latency in client and server response times, as well as to detect any additional delays introduced by the network, it is important to account for the fact that the local network used during the experiments may have been simultaneously accessed for other ongoing lab activities. RTTs are commonly treated as waiting times between independent events in this case, the time between sending a message and receiving its acknowledgment.

Since the RTTs are commonly treated as waiting times between independent events in this case, the time between sending a message and receiving its acknowledgment, the exponential distribution is a natural fit for modeling such waiting times, as it characterizes the time between events in a Poisson process. Specifically, it captures the stochastic nature of asynchronous and variable packet transmissions and acknowledgments in networked systems \cite{exponential\_rtt}.

To compare the RTT distributions of the client and server, two-sample t-tests were conducted to determine whether the means of the two distributions differ significantly at a 5% significance level. This test is appropriate because the exponential distribution is governed by a single parameter, $\lambda$, which is directly related to the mean. Thus, comparing means through a t-test provides a valid approach to assess whether the client and server RTTs stem from statistically similar distributions.

Discussion

Based on the results of the t-tests presented in Table \ref{t\_test\_table} and the raw RTT values illustrated in Figure \ref{raw\_RTT\_kyber768}, it is evident that Kyber768 introduced latency spikes in the client’s RTT during the video transmission phase. Increased client RTT typically indicates either that the server was slow to respond or that the client experienced CPU bottlenecks, or there is high network traffic.

However, examining the tegrastats data for Kyber768 reveals that toward the end of the mission, during the video transmission period, the client’s CPU usage actually drops suggesting the system was no longer under heavy load. These timestamps align with the latency spikes observed in the RTT graph, indicating that the delays were not caused by CPU limitations on the client side.

Therefore, the increased RTT is likely attributed to delays at the server side, either due to slower response times or the impact of uncontrolled network traffic. In either case, the latency cannot be linked to client-side resource constraints.

We can further conclude that this latency might explain why the overall send and receive time for Kyber768 is slightly lower than that of Kyber512, as shown in Figure \ref{fig:sending\_and\_receiving\_speed}. This is consistent with the fact that Kyber768 has the highest encryption speed among the Kyber variants, and its signing speed is nearly equivalent to that of Kyber512.

@techreport{exponential\_rtt, title={Generating a function for network delay}, author={RIPE NCC}, year={2016}, institution={RIPE Network Coordination Centre}, note={Analysis of network delay distributions including fitting exponential distribution functions}, url={https://www.ripe.net/ripe/mail/archives/mat-wg/attachments/20161129/9dcb6b34/attachment.pdf} }