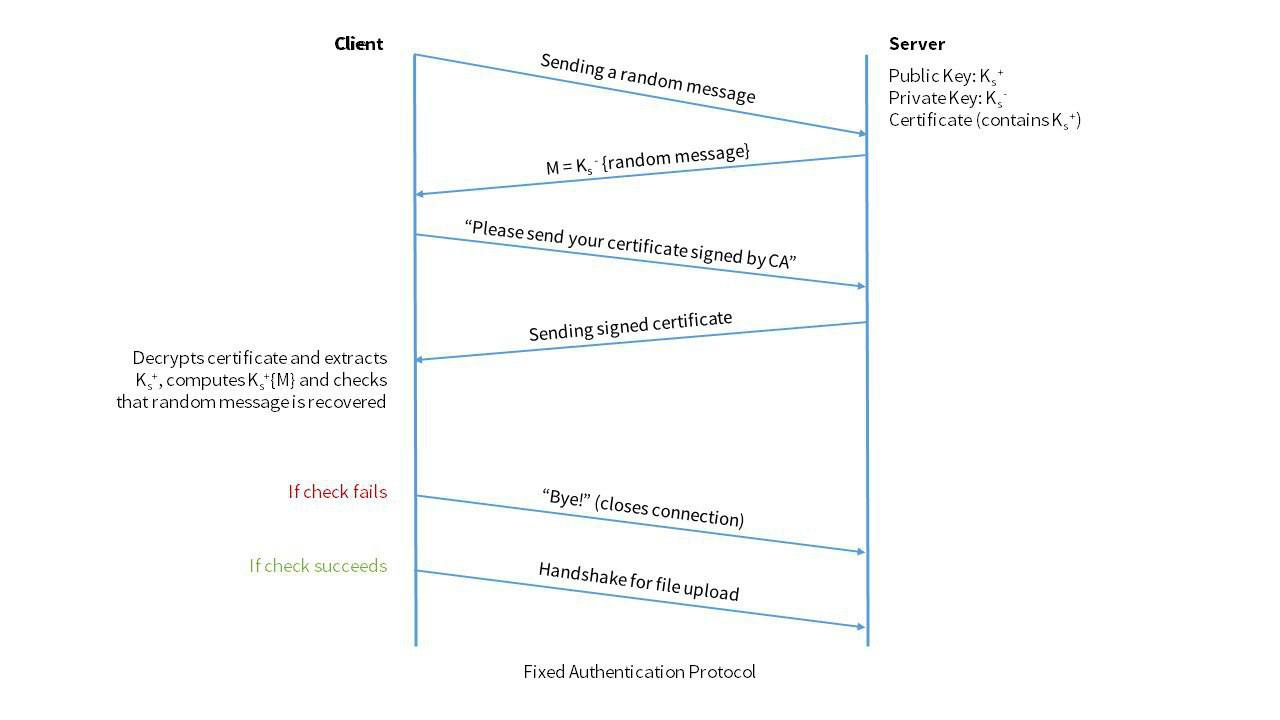
Report

1. Fixed AP Protocol

The problem with the suggested protocol is that with a known message and the server’s public key extracted from the signed certificate, any client can masquerade as server to other clients. The problem was fixed by having the client a random message for the server to encrypt, having the client decrypt that message with the server’s public key extracted from the signed certificate, and then checking if the random message is recovered.

The proposed new protocol is as follows:



1. Throughputs