ICMP Blind Connection-Reset + Blind throughput reduction attack against TCP

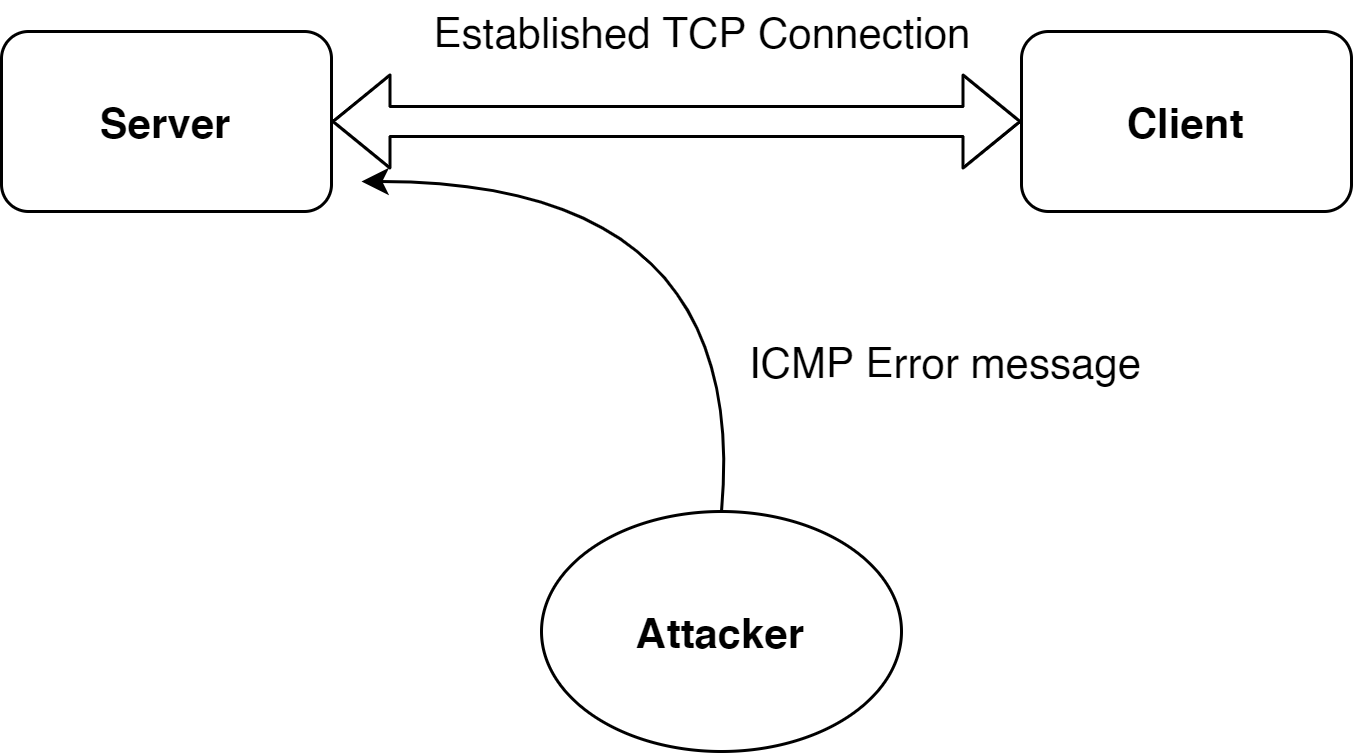
Md. Tahmidur Rafid

Student ID : 1605046

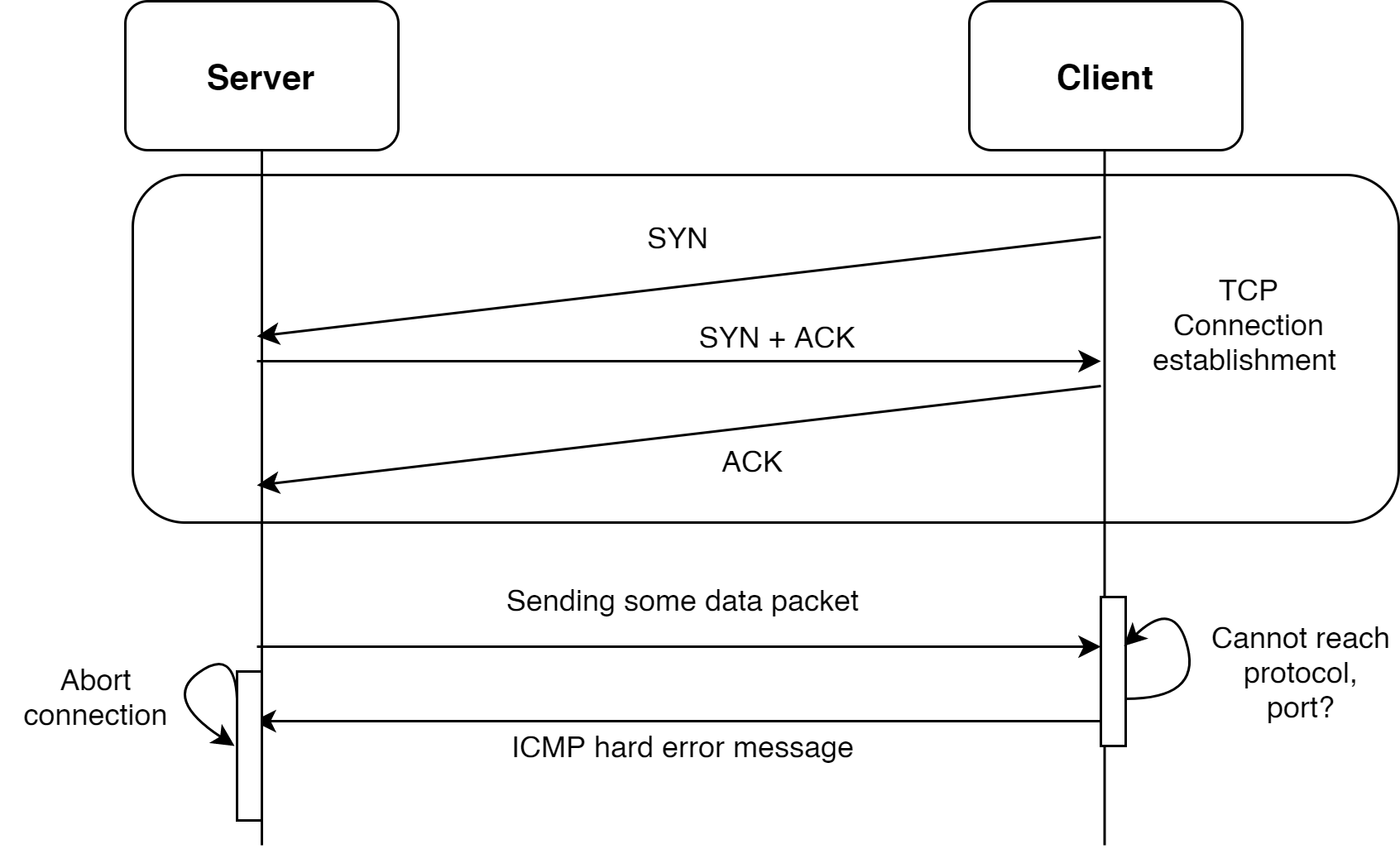
**Definition :**

ICMP Blind connection-reset attack is an attack against TCP. Using ICMP (Internet Control Messaging Protocol), communication between two hosts are performed regarding queries or informing about errors. ICMP error messages are of two types: one is hard error and another is soft error. Hard error should abort a connection. So, in this ICMP Blind connection-reset attack, an attacker will send fake ICMP hard error message to close a connection. ICMP error type 3 (Destination unreachable) with code 2 (Protocol Unreachable), 3 (Port Unreachable), 4 (Fragmentation needed) are considered as hard reset. ICMP error type 4 (Source Quench) is used for congestion control mechanism. So when a sender receives a Source quench message, it will reduce the packet transmission rate, thus the throughput will be reduced.

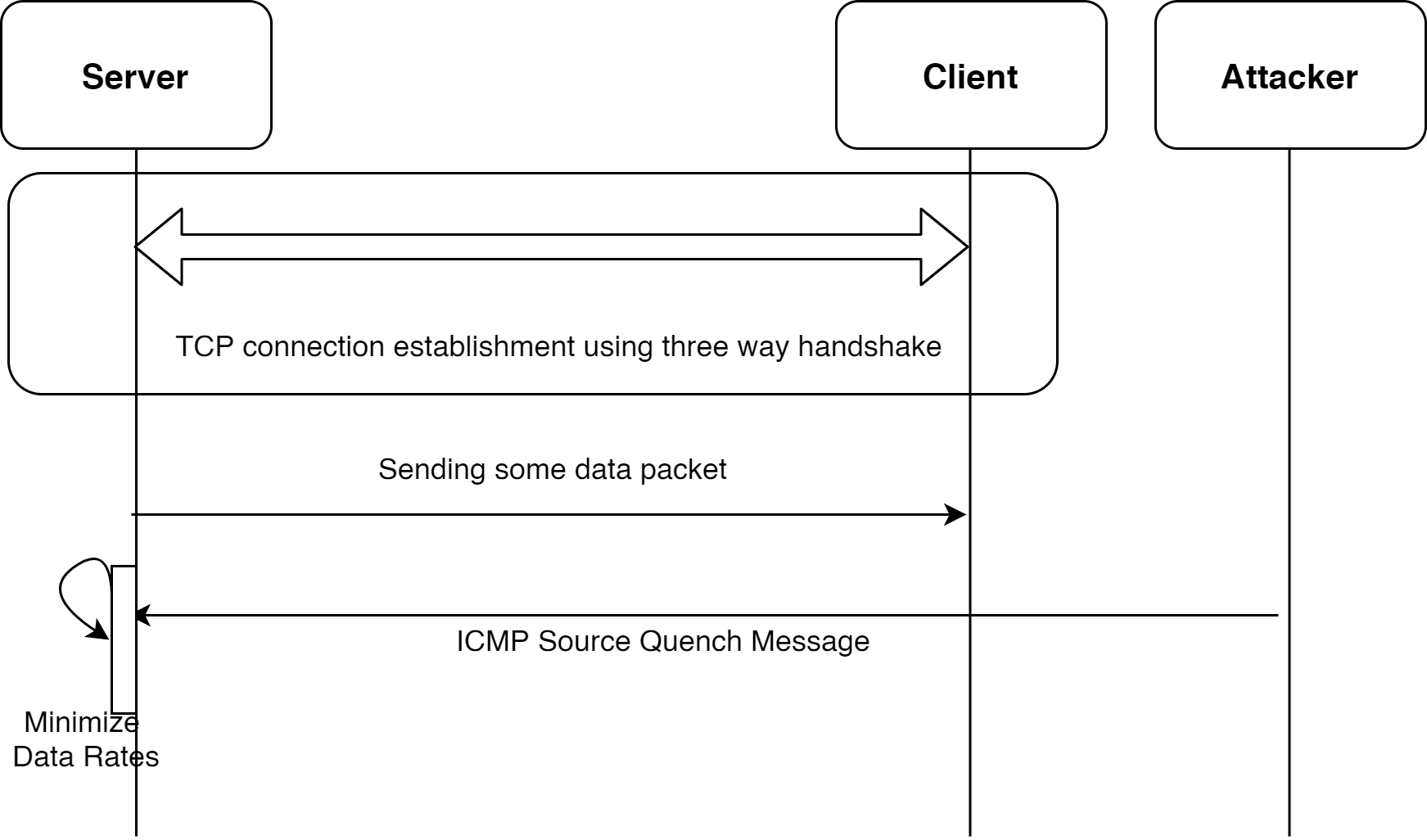
**Topology Diagram:**



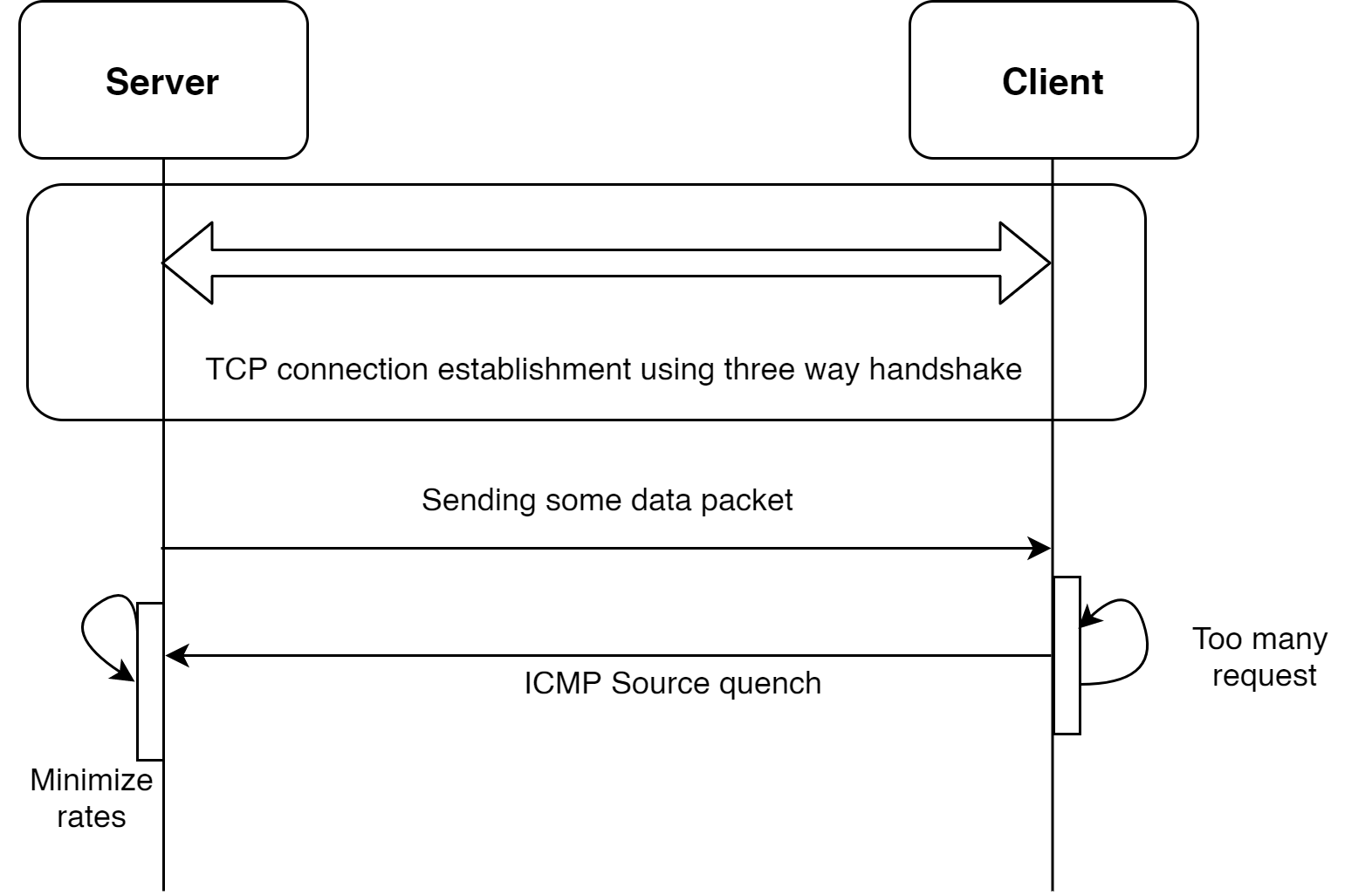
**Timing Diagram:**



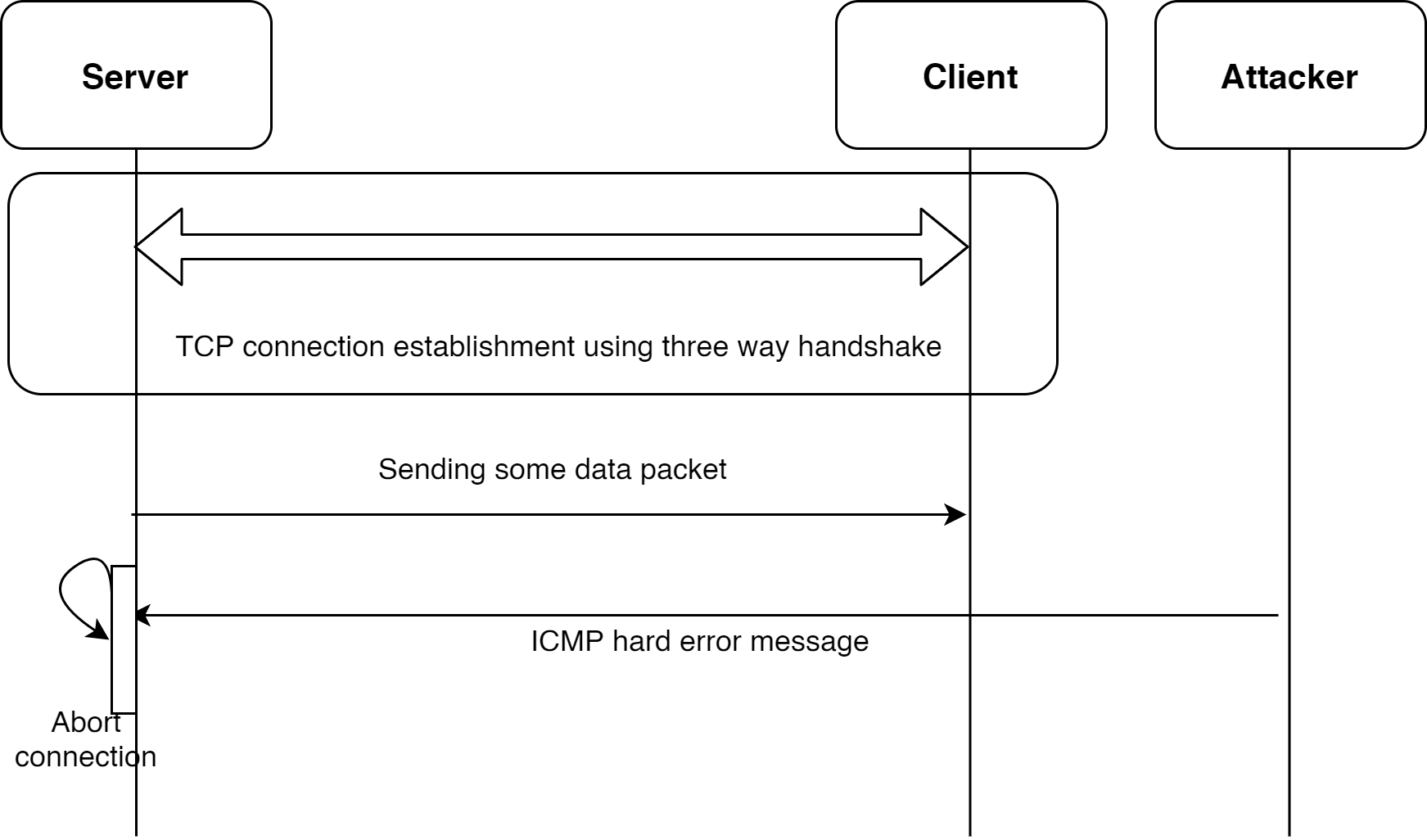
**ICMP Original Connection-reset**



**ICMP Blind Connection reset attack**



**ICMP Original Source Quench Message**



**ICMP Source Quench Attack**

**ICMP Protocol:**

A Dynamic Host Configuration Protocol (DHCP) server is responsible for issuing IP addresses to devices on its network. This is done through a series of packet exchanges between individual DHCP clients and DHCP servers.

A DHCP IP address allocation transaction depends on four types of packets: DISCOVER, OFFER, REQUEST, and ACKNOWLEDGEMENT.

The details about each packet are discussed below :

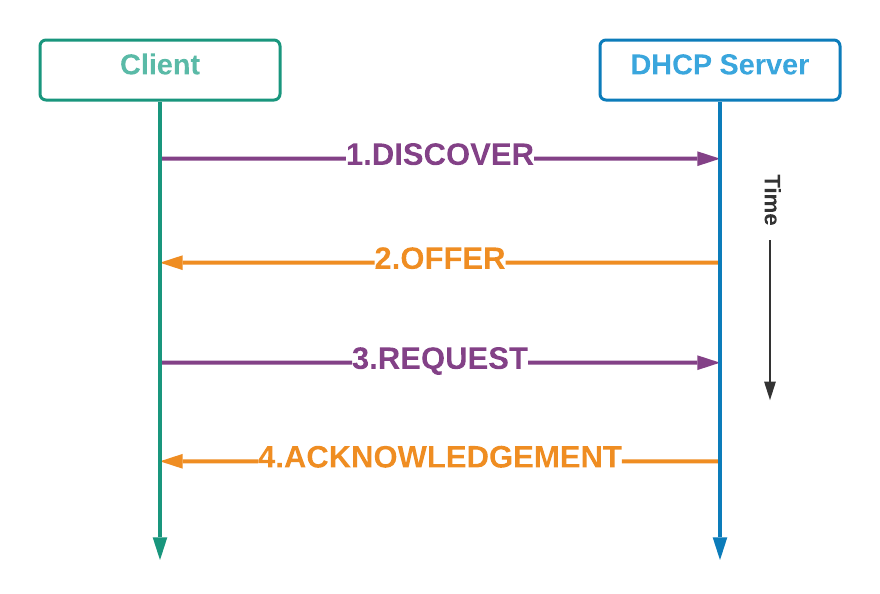
**DISCOVER :** When a host boots up on the network, if it's a DHCP client, it's going to broadcast a DHCP DISCOVER packet to all hosts in Layer 2 segment (destination address is FF:FF:FF:FF:FF:FF). Frame with this DISCOVER message hits the DHCP Server.

**OFFER :** The DHCP server has a pool of addresses it can select from. When it receives a DISCOVER packet, the DHCP server chooses one of its remaining IP addresses from its pool, reserves it for the new client and offers it to the new client by unicast via OFFER message.

**REQUEST :** After the client receives the OFFER message, it requests the exclusive rights on that offered IP by sending a REQUEST message to the server by unicast.

**ACKNOWLEDGEMENT :** Server sends ACKNOWLEDGE message to the client and anyone else listening confirming the DHCP lease to client. Now the client is allowed to use new IP settings.

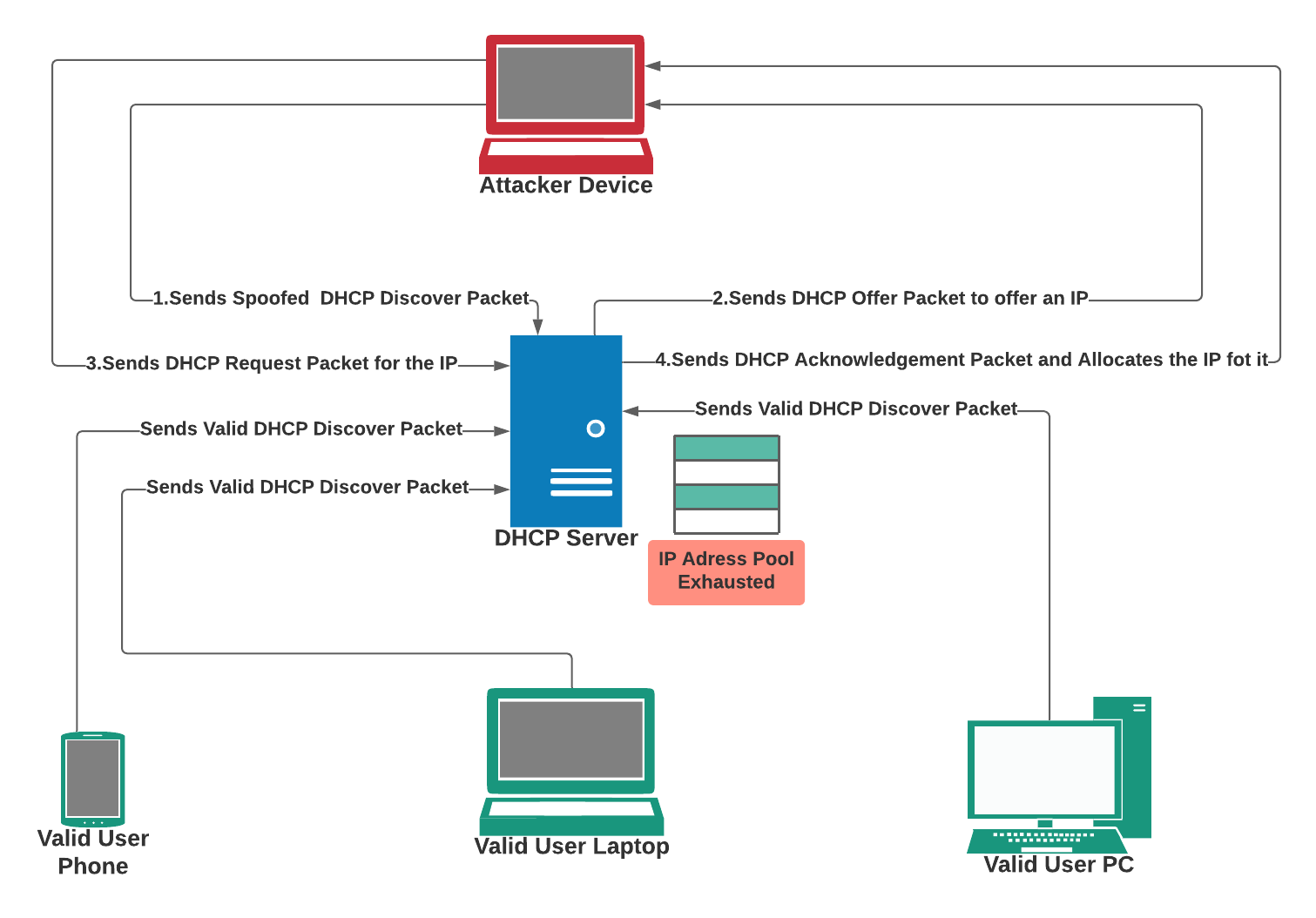
**Timing Diagram of DHCP Protocol :**

****

**Attacking Strategies :**

1. A raw socket will be opened.
2. A random MAC address will be created.
3. DHCP Discover packet will be broadcasted.
4. After receiving the DHCP offer packet, the DHCP request packet will be sent.
5. If the steps from 2-4 are done repeatedly, the IP addresses will get used up in no time.
6. Sending DHCP discover packets will be stopped when no more DHCP offer packets are received in a fixed time interval.

**Timing Diagram of Attack :**

****