DNS based DDoS mitigation solution

Schematic Diagram

Sukhun Yang

Seoul National University

August 14, 2023

Contents

Table of Contents

Architecture

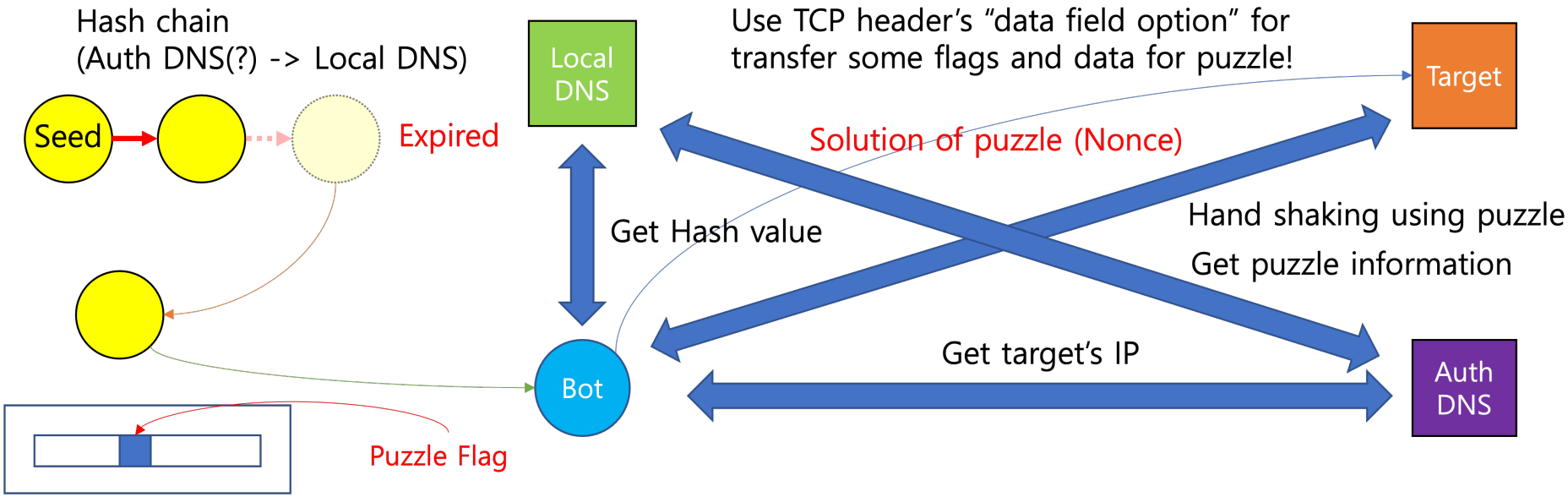


Figure 1: Architecture

Testbed

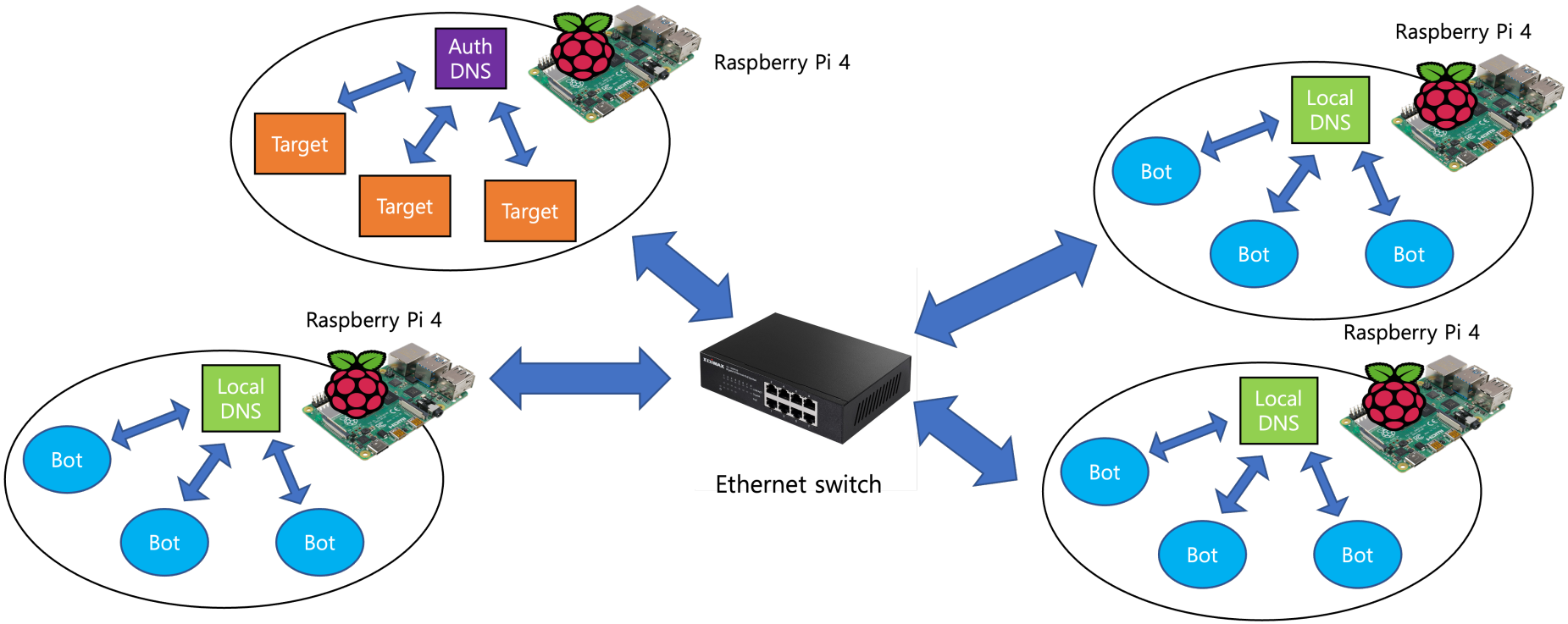
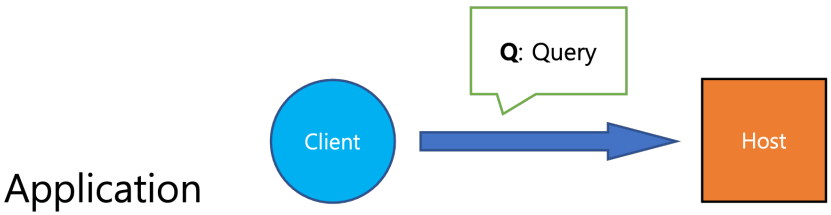
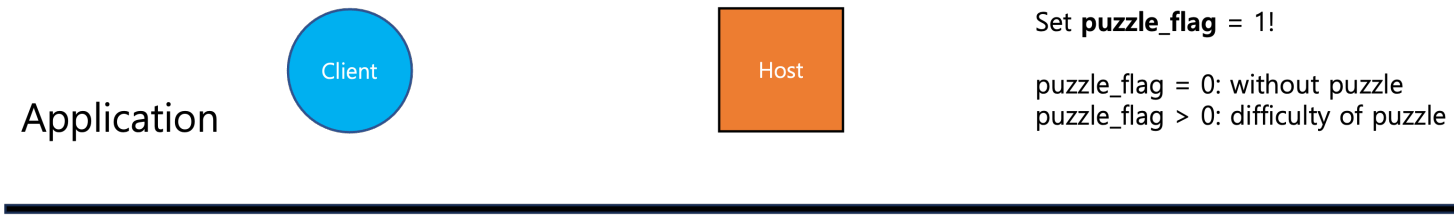


Figure 2: Testbed

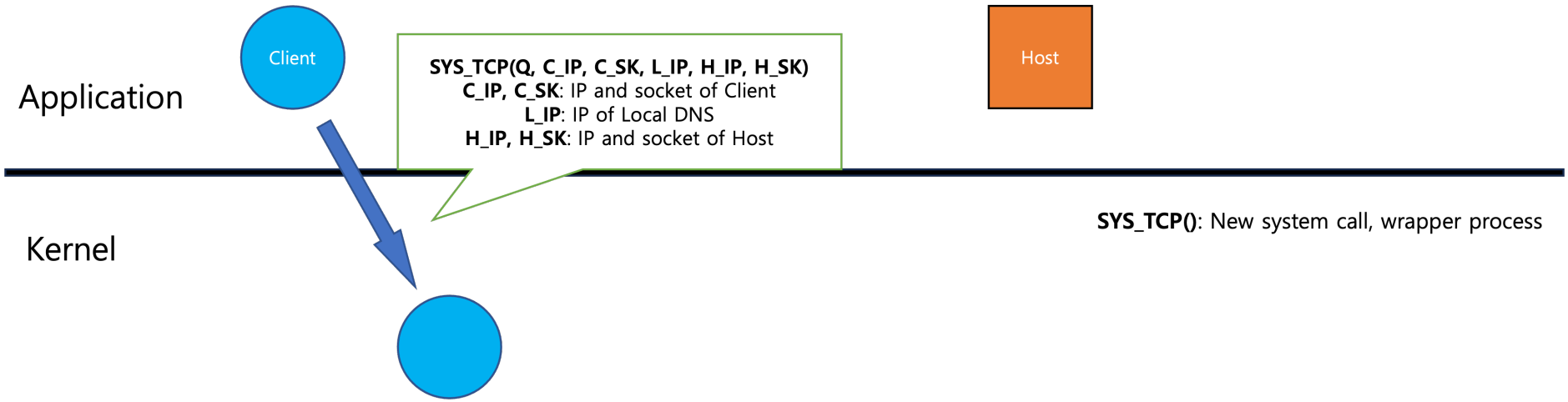
Schematic Diagram



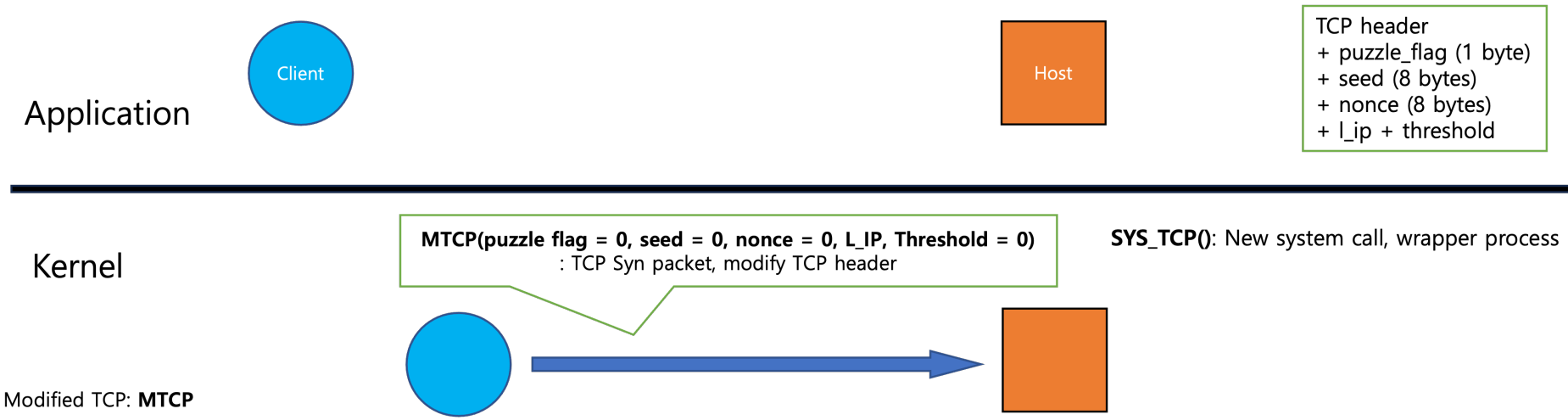
Schematic Diagram



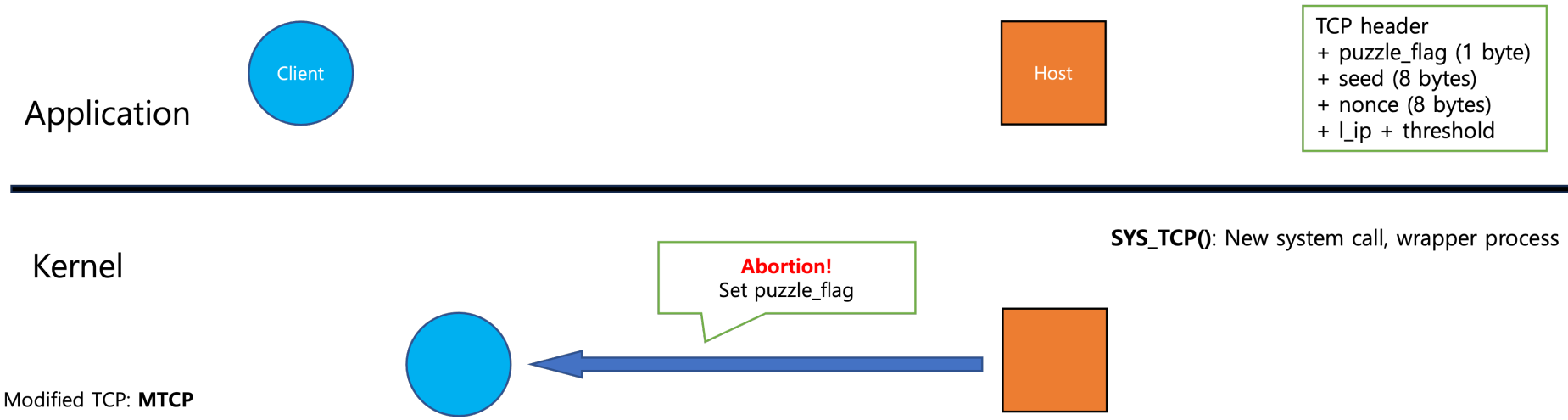
Schematic Diagram



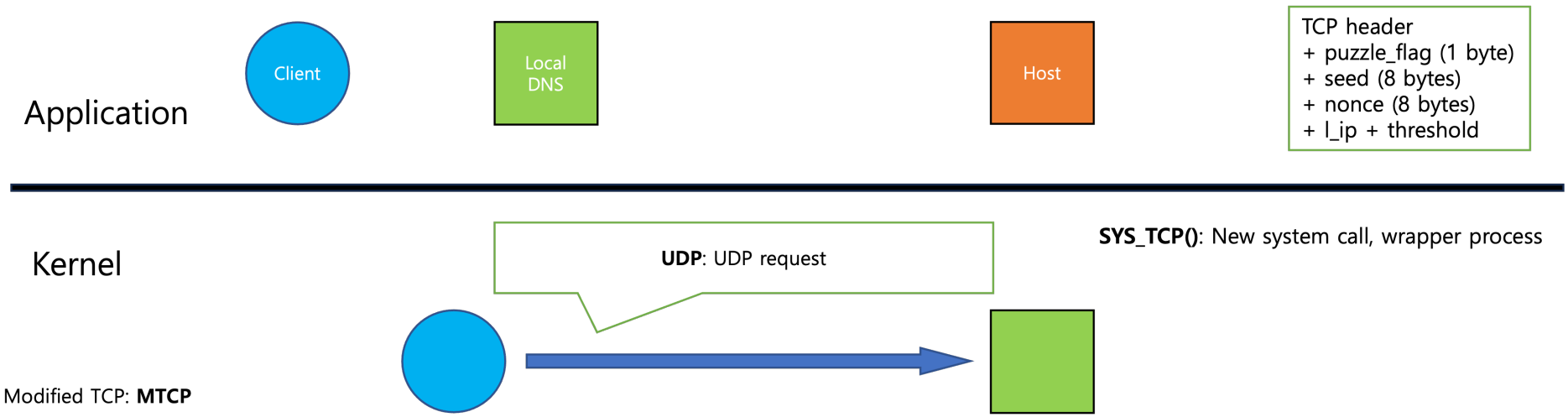
Schematic Diagram



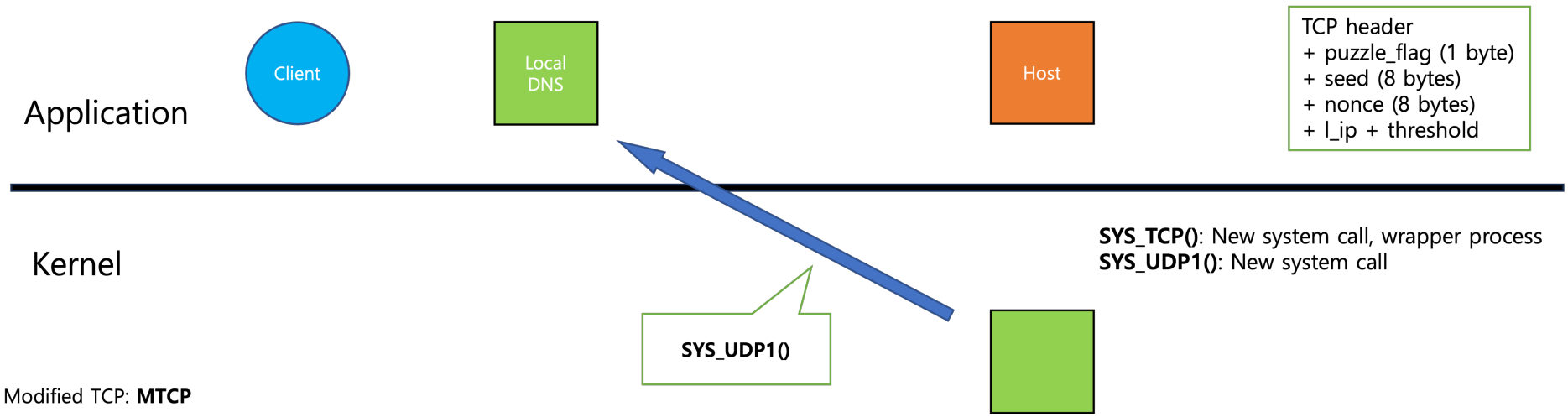
Schematic Diagram



Schematic Diagram

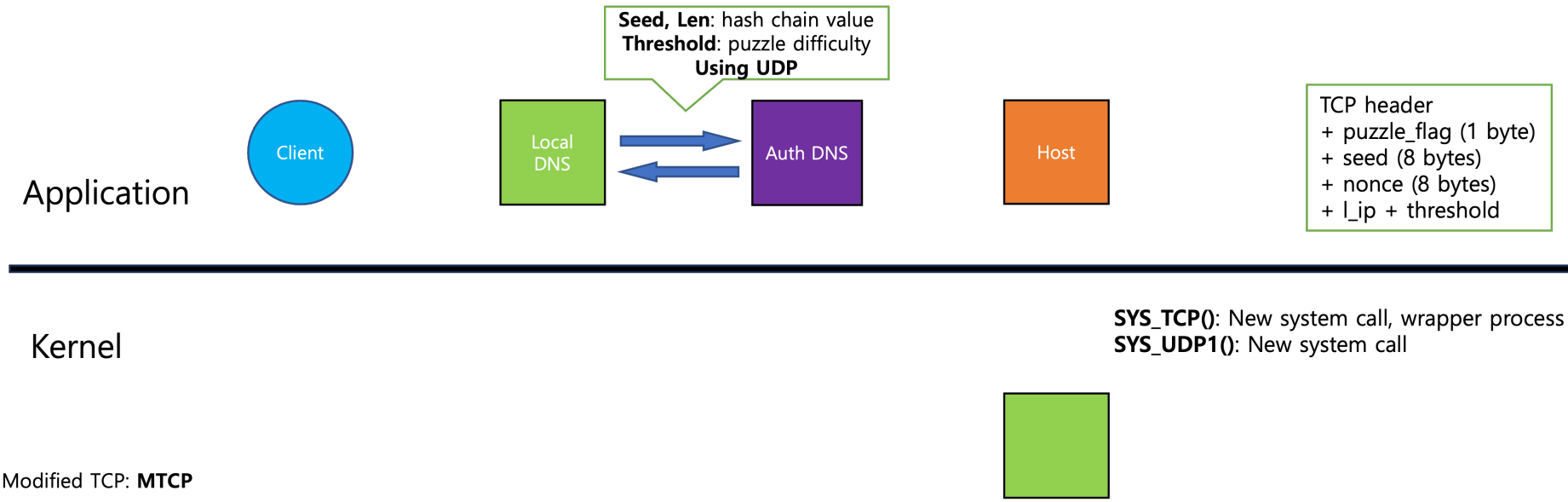


Schematic Diagram

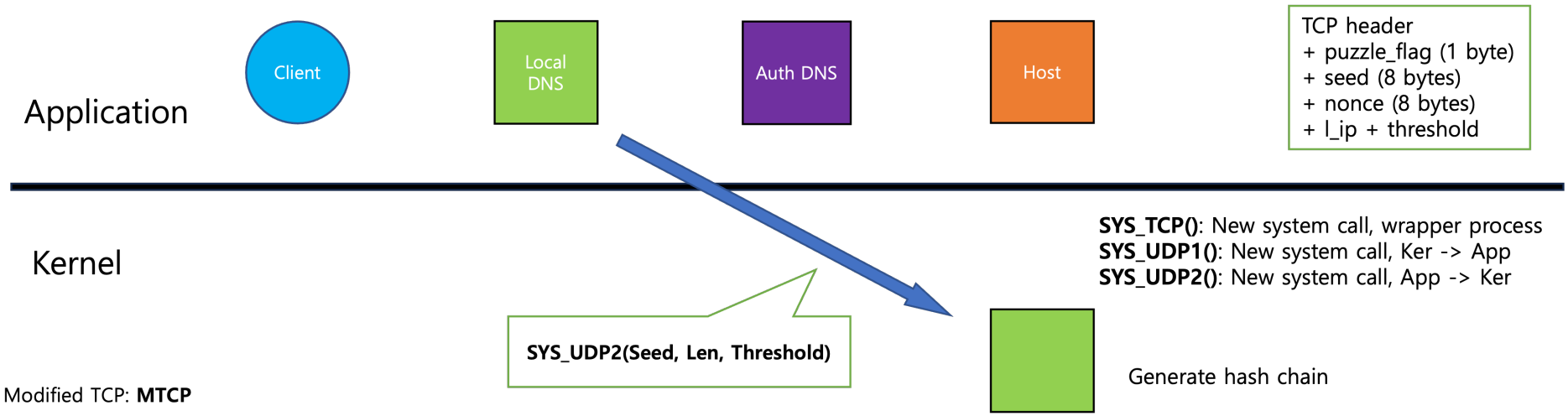


Modified TCP: **MTCP**

Schematic Diagram

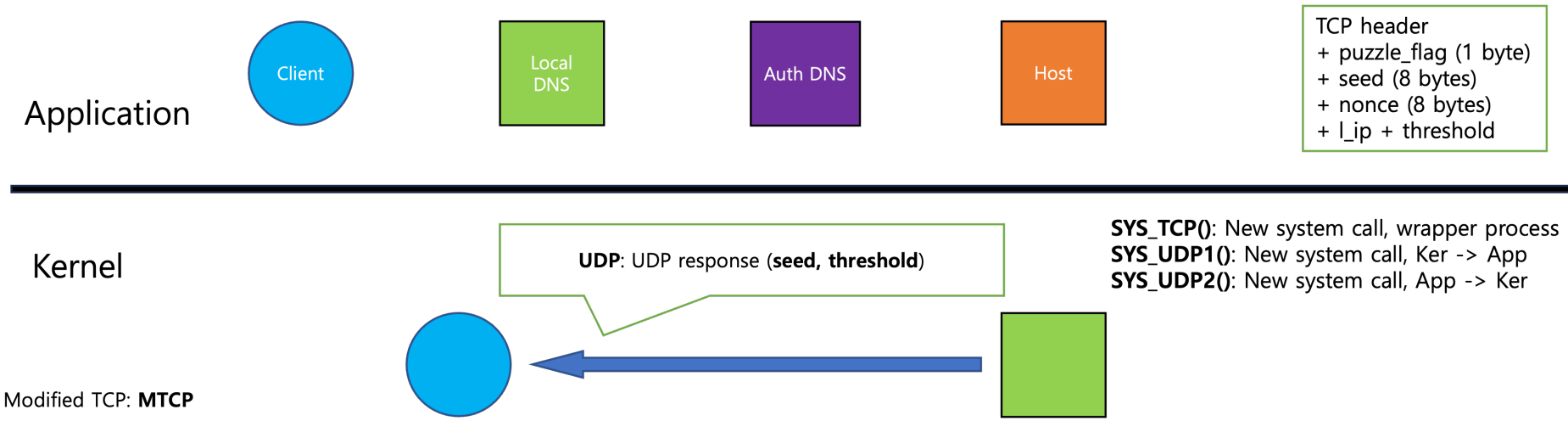


Schematic Diagram

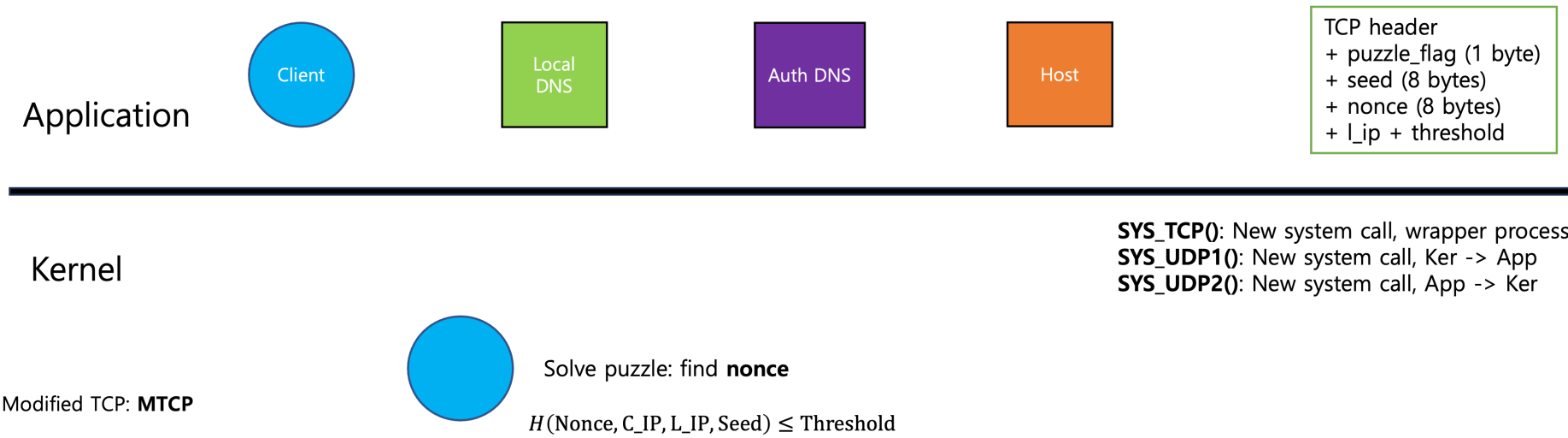


Modified TCP: **MTCP**

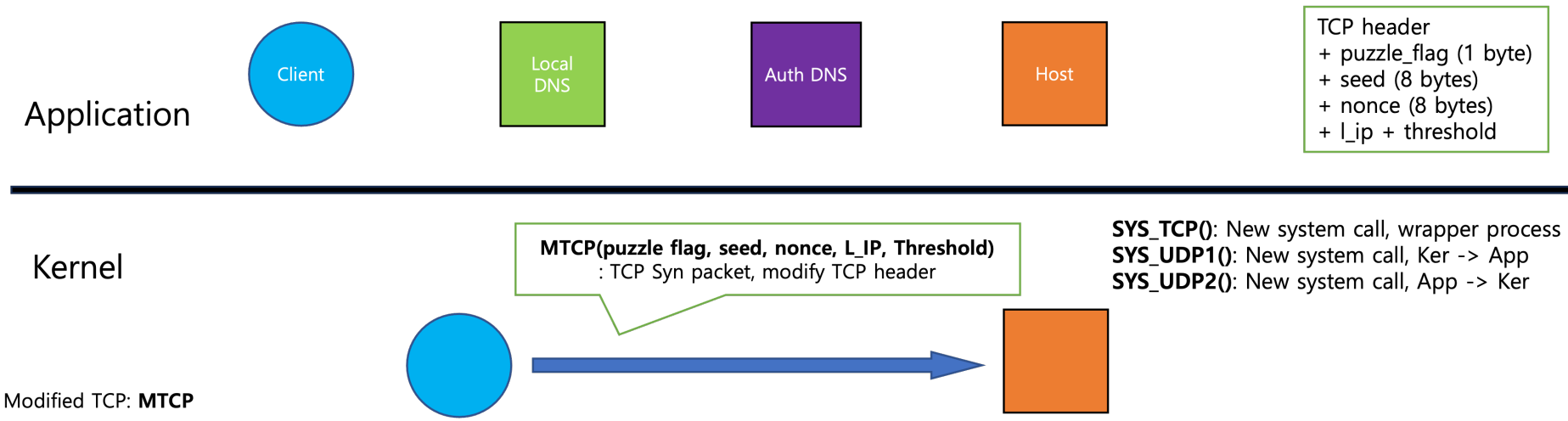
Schematic Diagram



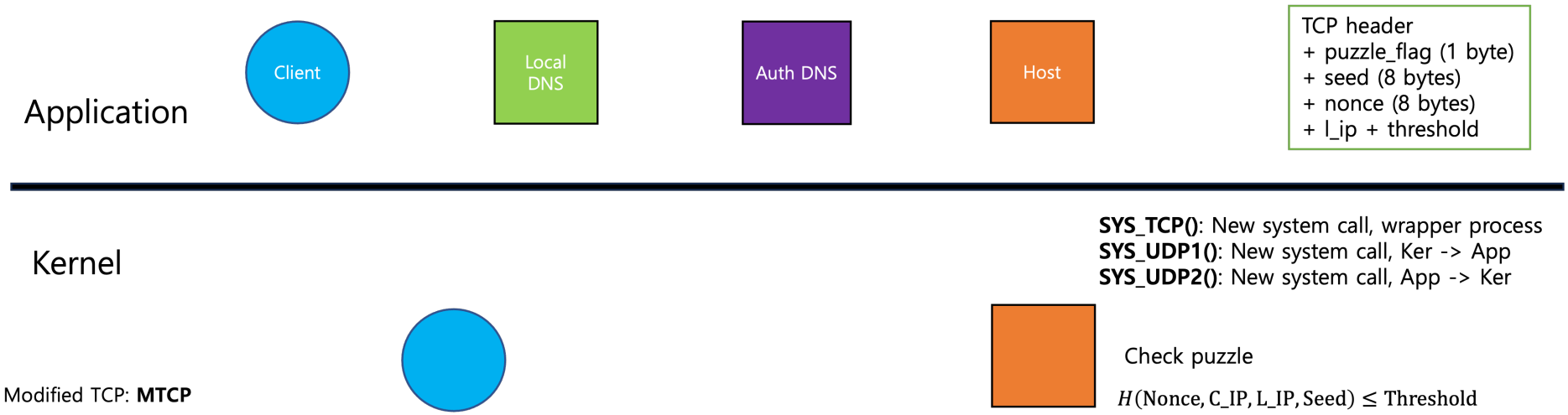
Schematic Diagram



Schematic Diagram



Schematic Diagram



Schematic Diagram

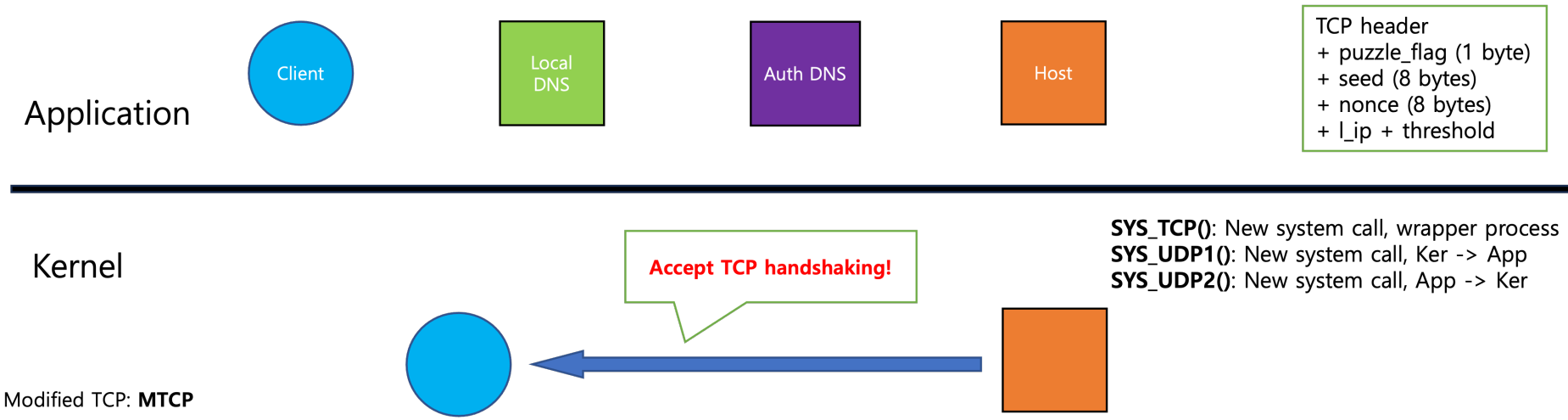


Table of Contents

Specification

Detailed parameters and values are appeared in above diagram.
The following is a brief summary of what needs to be done.

To-do list

Plan to make wrapper process as syscall at linux kernel

Client

1. New syscall **SYS_TCP()** as wrapper process
2. Modify TCP handshaking process in linux kernel
3. Modify UDP process in linux kernel
4. Application level: running **SYS_TCP()**

To-do list

DNS

1. UDP socket programming between local DNS and auth. DNS
2. New syscall **SYS_UDP1()** as signal for get hash value in application level
3. New syscall **SYS_UDP2()** to drop off hash values to kernel level
4. Application level: open UDP socket and running both syscalls

To-do list

Host

1. Make 3 or 5 difficulties of puzzle (control threshold)
2. Generate random seed values for each local DNS
3. Autonomous system for control difficulties automatically

Table of Contents

Source code

Currently Working

https://github.com/Sagit25/DNS-based-DDoS-mitigation