Enhancing Ethereum P2P Network Security through Fuzzing

Tim Fan

AgnopraxLab

Section 1

Intro fuzzing test

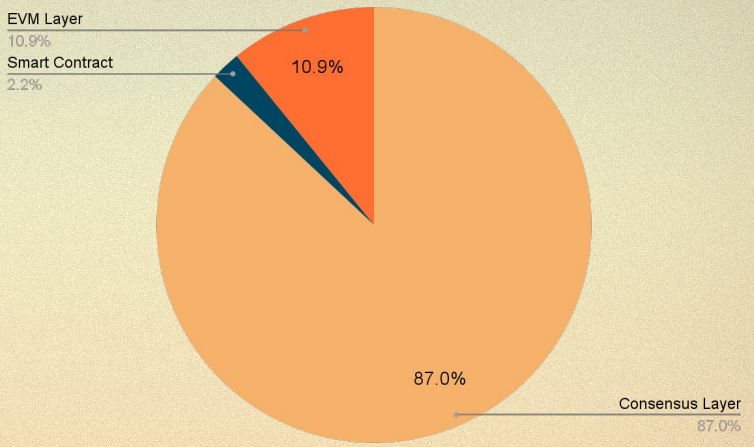
Fuzzing is popular

- Fuzzing is a software testing method with high efficiency , widely used for software vulnerability
- Fuzz tools like oss-fuzz , find 25000 cve-confirmed vulnerability in last one year.
- Kinds of fuzz tool design for Ethereum: EVMFuzzer, goevmlab , tx-fuzz

Vulnerabilities discovered By fuzzing

Consensus Layer	Memory Access & Free Runtime Crashes
	Safety Issues Liveness Issues
Smart Contract Layer	Authentication Authorization
	Integer Related Resource Management
	External Dependencies Exception & Reentrance
EVM Layer	System Stability Execution Issues Undisclosed Security Issues
P2P Network Layer	Needs further development

*fuzzing research in 2023-2024



Need a specialized fuzzing tool for the P2P network layer of blockchain systems!

Section 2

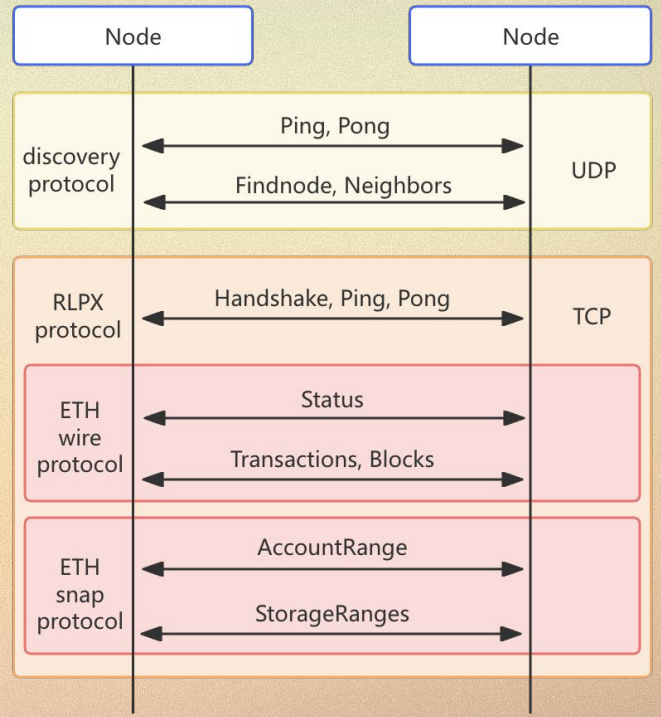
Fuzz in devp2p

Recap Ethereum devp2p protocol

- **Ethereum Execution Layer (EL) use devp2p protocol , Consensus Layer use libp2p . We mainly focus on devp2p now**

- Devp2p is a modular, layered network protocol for Node discovery, session management, data transfer.

- We focus on sub protocol : discv4, discv5, rlpx and wire and snap .

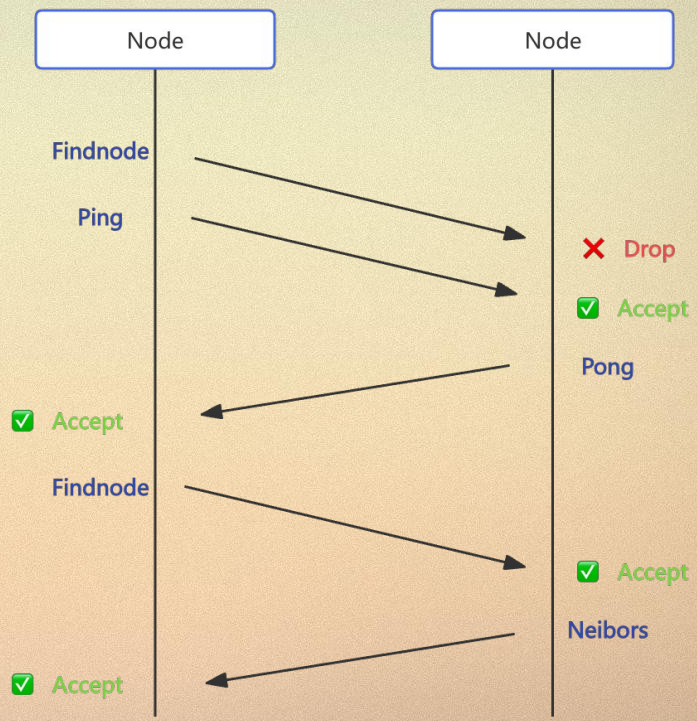


Why we fuzz on devp2p

Directly send a findnode packet directly to the target node as a peer, it will be dropped

Ping-Pong is performed, and a reply is received if findnode is sent again

Devp2p protocols are <u>correlated in time order and has huge state space</u>



Our Fuzz tool works on devp2p

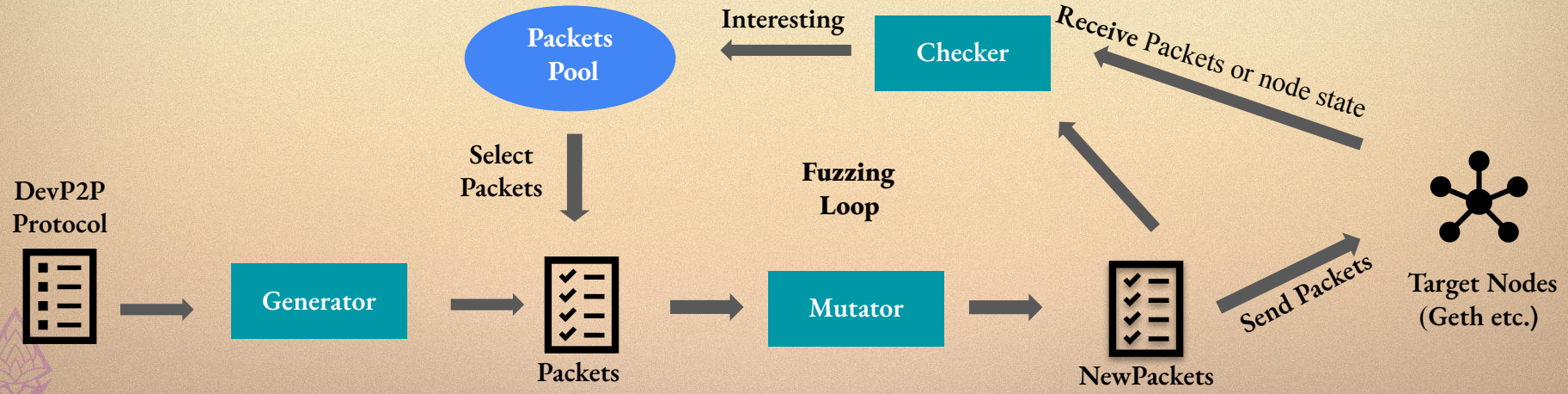
1 Generate packets according to devp2p spec

2 Mutate packets

4 Compare received packets and collect interesting Packet

5 Select packets to next Loop

3 Send NewPackets to target node (Node we want to test) and collect response packet

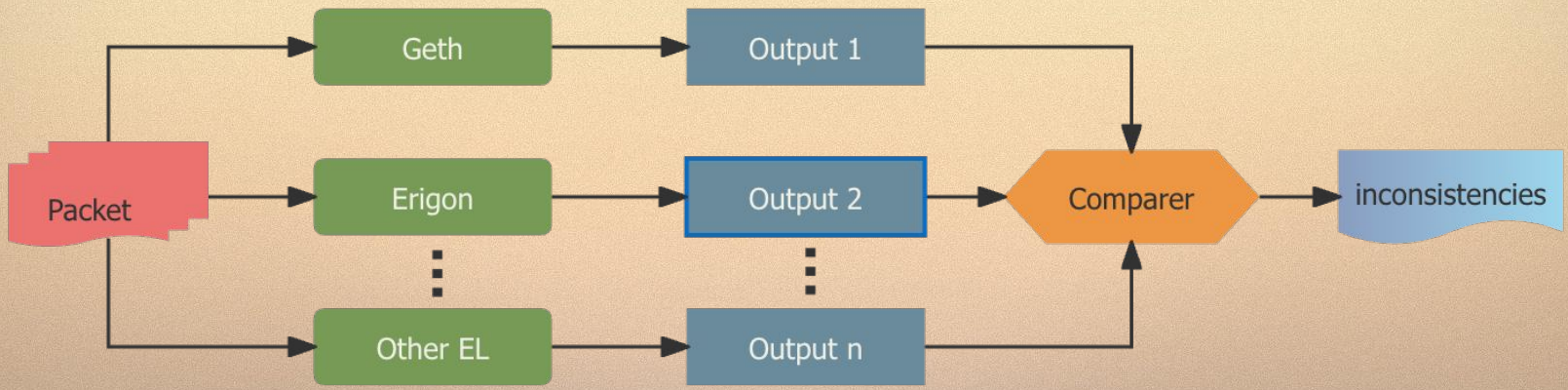


Fuzz on different client

Different CL's devp2p implementation should follow same input and output rules

Inconsistencies caused by cross-client logic flaws, different program language features

Our way can expand to any EL client seamlessly



About us

Tim Fan
TG: @tkattk

Fudong Wu
TG: @fudongwu

Haochen Sun
S230130@e.ntu.edu.sg

Scan to follow our research