

Towards Trustworthy Telemetry and QoE Measurements

Zaoxing “Alan” Liu

<https://www.cs.umd.edu/~zaoxing>



Collect and analyze measurements to understand what is happening in the network for operation and management.

Examples:

- What are the largest flows in the current network?
- Are there any flows with high packet loss?
- Is there an ongoing SYN flood attack?
- What is the network latency of my application?

A Typical Network Operator

Network Operators



Network Traffic

- Heavy hitter detection
- Performance estimation
- Security analysis

Network Devices

Telemetry algorithms

Example Scenario: Performance Analysis

Troubleshooting and fixes

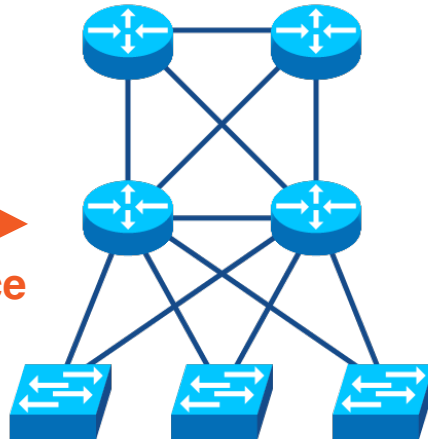


What's happening?

- ↑ Packet drop
- ↑ Latency
- ↓ Bandwidth



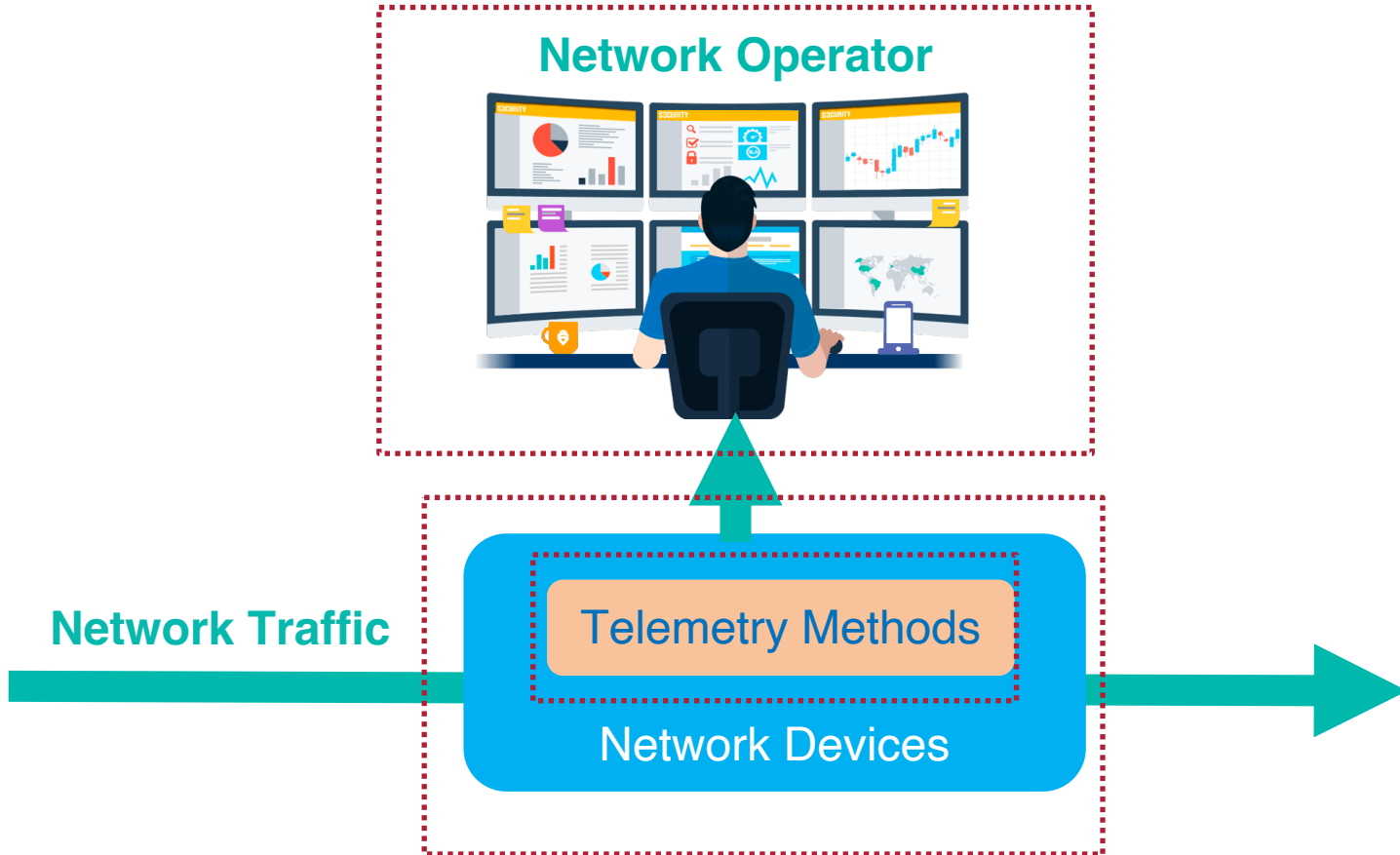
Poor
Performance



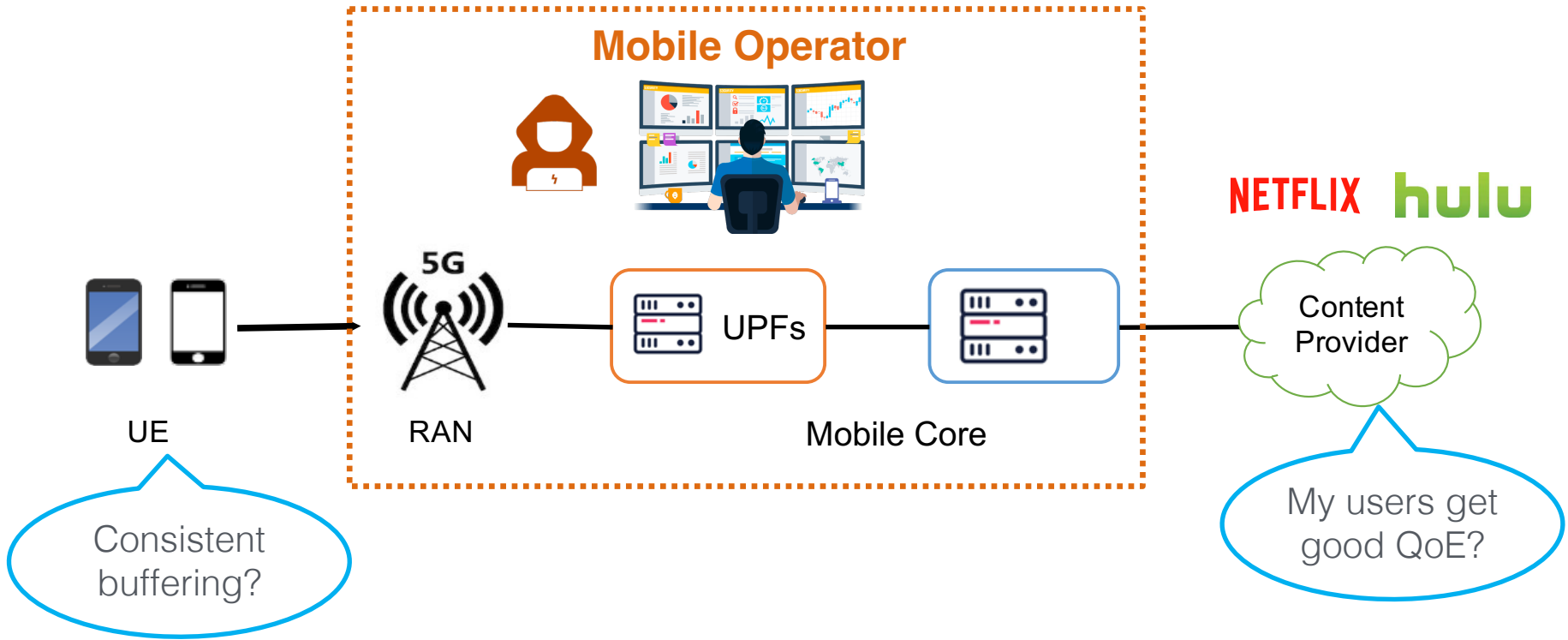
Poor
Performance



“The Problem of Trust”

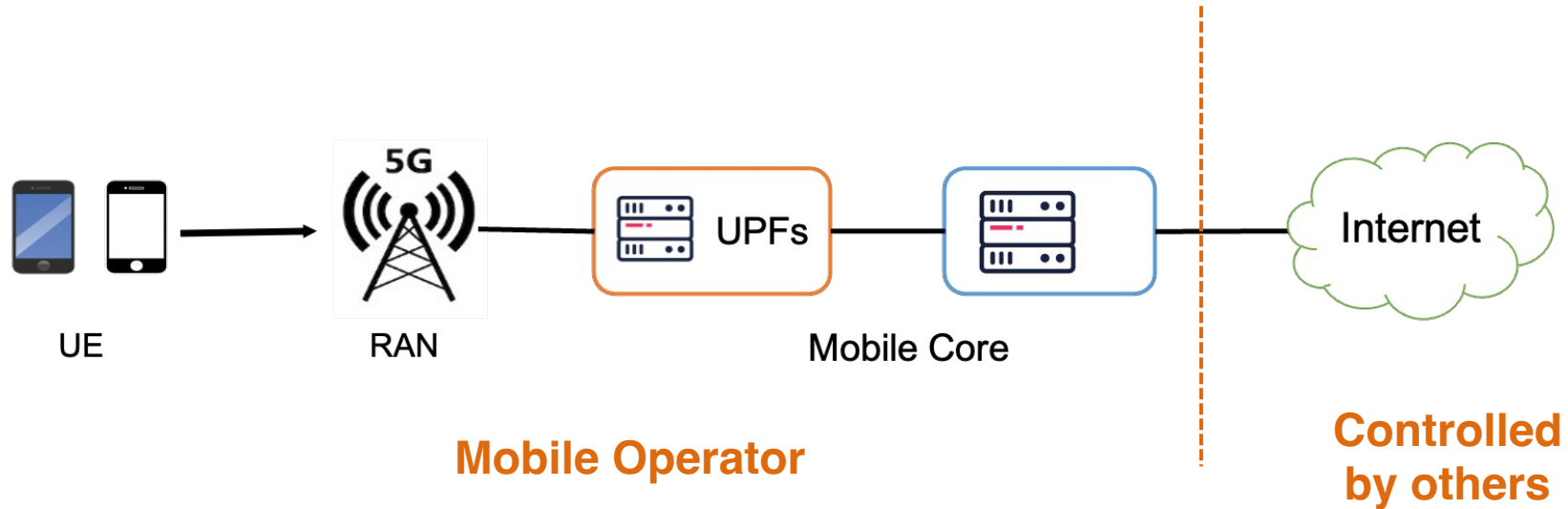


Threat Model 1: Untrusted Operators



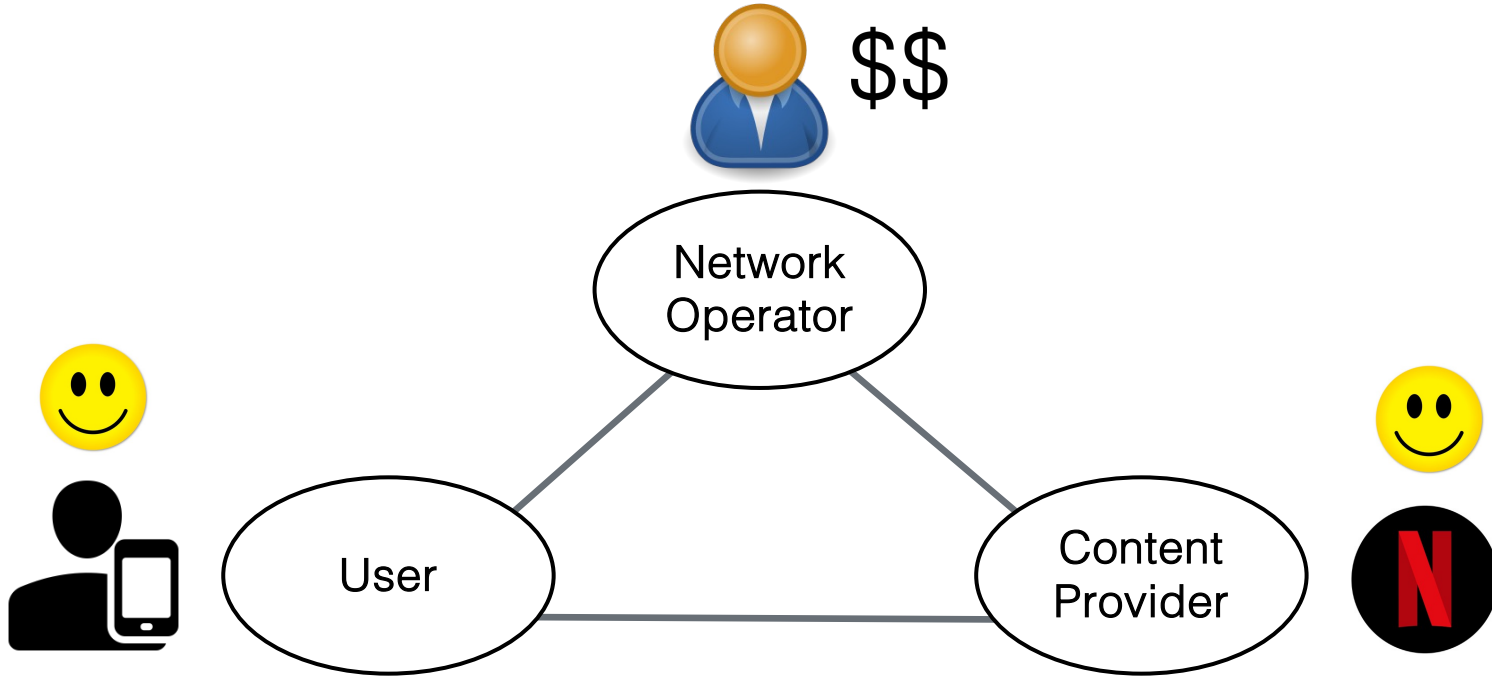
If operators can prove their network QoS,

Why Need Operators to Prove?



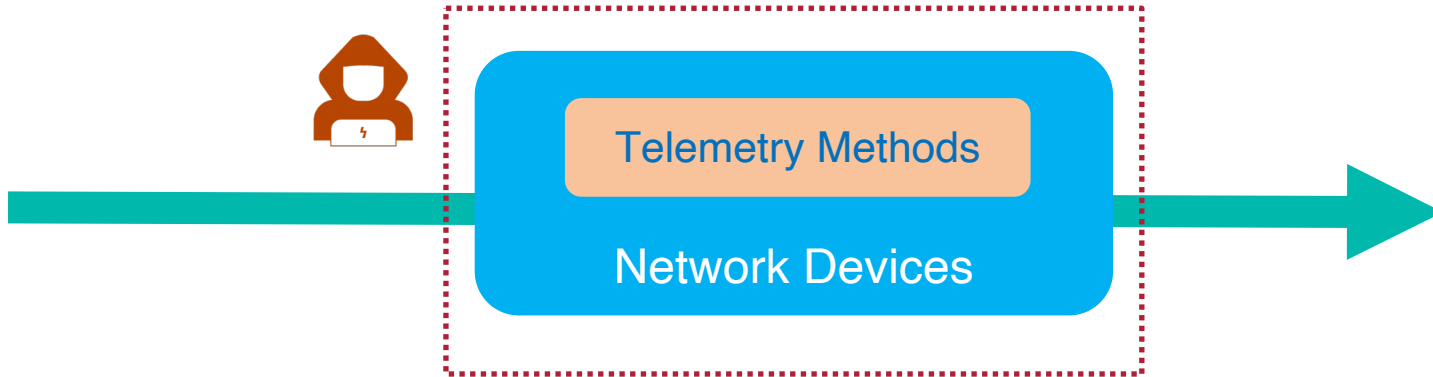
End-to-end QoE measurements can be dominated by wide-area Internet performance variations.

Trustworthy measurement enables new opportunities



Promoted services, split billing, etc.

Threat Model 2: Untrusted Network Devices




[Home](#) > [News](#) > [Security](#) > Cisco warns of critical switch bugs with public exploit code

Cisco warns of critical switch bugs with public exploit code

By [Sergiu Gatlan](#)

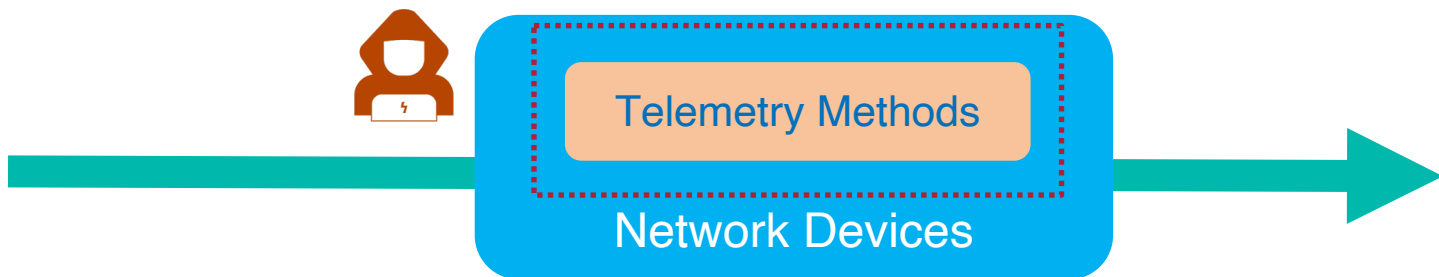
 May 17, 2023

 02:50 PM

 0

Gain unfair performance advantages, billing benefits, etc.

Threat Model 3: Algorithmic Vulnerabilities



ON THE ROBUSTNESS OF COUNTSKETCH TO ADAPTIVE INPUTS

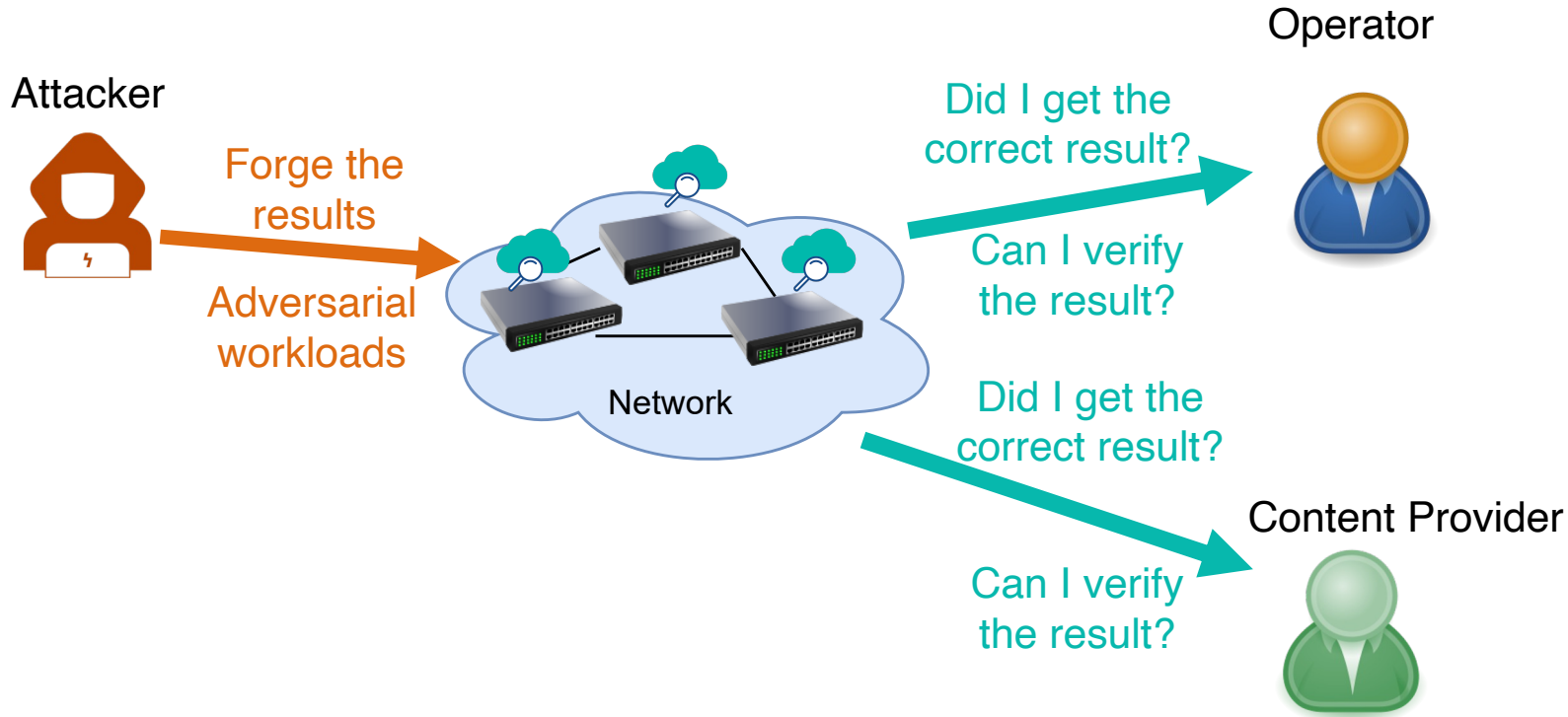
Edith Cohen* Xin Lyu† Jelani Nelson‡ Tamás Sarlós§ Moshe Shechner¶ Uri Stemmer||

How Robust are Linear
Sketches to Adaptive Inputs?

Moritz Hardt, David P. Woodruff

Need algorithmic improvements for network workloads

Vision: Trustworthy telemetry and QoE measurement



What we can do?



Hardware roots of trust

- Trusted Execution Environment (TEE)
- Trusted Platform Module (TPM)



Cryptographic tools

- Interactive proofs and zero-knowledge
- Non-interactive proofs
- Confidential computing



Algorithmic tools

- Robust sketching algorithms
- Verification tools

Contact: Alan Liu
www.cs.umd.edu/~zaoxing