

# Security and Privacy for NextG Networks

Jennifer Rexford



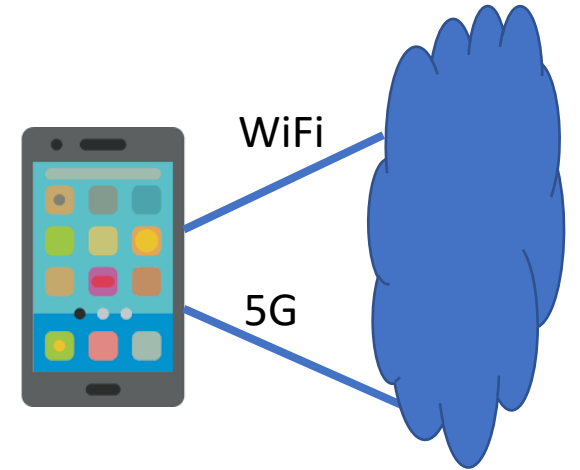
# NextG Networks: Extreme Conditions

- Privacy risks (e.g., user location)
- Low-end hosts (Internet of Insecure Things)
- Tremendous scale (# devices, churn)
- Tight latency and reliability requirements
- Complex protocols, software, equipment
- Variable wireless network properties
- Variable CPU/storage (host, edge, cloud)



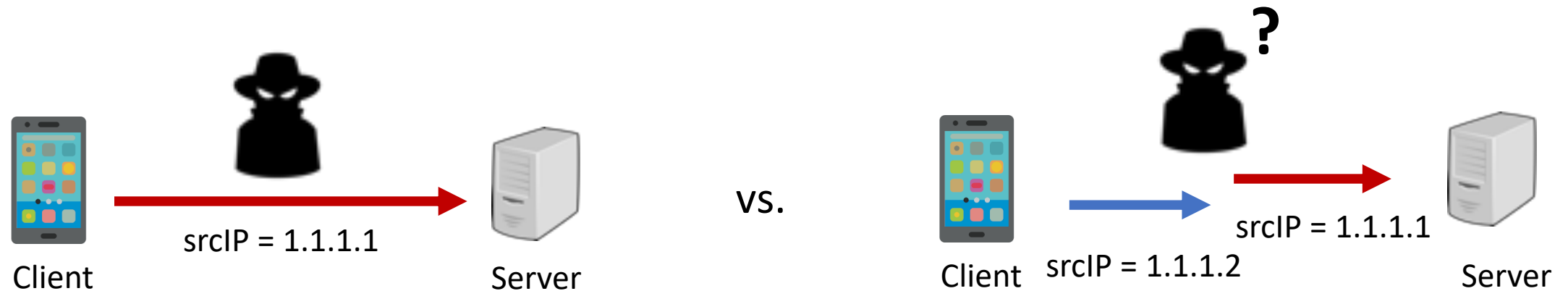
# End-Host Session Protocols

- Internet protocols were not designed for
  - Mobility: changing of network attachments
  - Multihoming: using multiple interfaces
  - Middleboxes: steering traffic through functions
- Where should we solve these problems?
  - Network: routing
  - End-host: session protocols
- Session protocols are more flexible and scalable
  - E.g., multipath TCP, connection migration in QUIC, etc.



# Session Protocols to Protect User Privacy

- Protecting privacy
  - IP addresses reveal user identity (and location)
  - Size of data transfers can reveal the content (e.g., fingerprinting)
- Change IP addresses within a data transfer

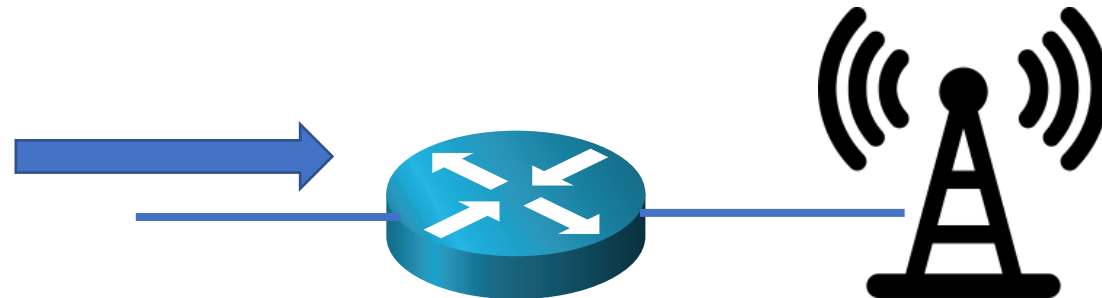


# Programmable Network Defenses

- NextG networks are attractive targets
  - Cyber-physical systems affecting the Real World
  - Even short service disruptions are a problem
  - End hosts are insecure and have limited resources
- Deep network programmability
  - Customize to handle ever-evolving attacks
  - React quickly, directly in the data plane

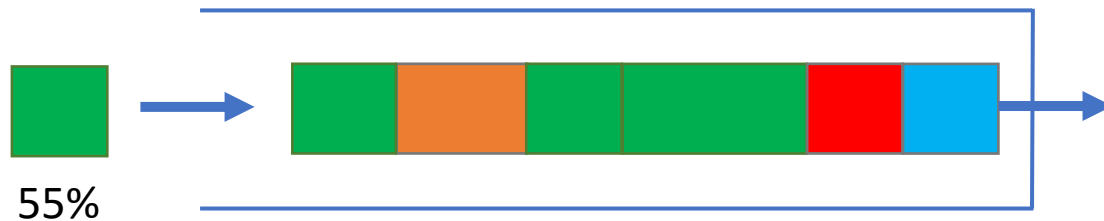


IOT



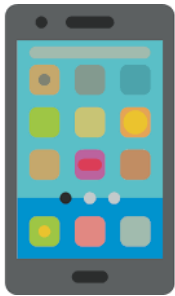
# Programmable Network Defense

- Higher-level query languages
  - E.g., destination receiving traffic from many sources
  - E.g., flow responsible for a large fraction of backlog in queue



- Closed-loop control of the network
  - Integrate measurement, analysis, and control
  - E.g., probabilistically drop packets responsible for queue backlog
  - (Verified) compiler synthesizing the control and data plane code

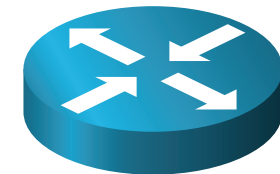
# Rethinking the Division of Labor: From Top-to-Bottom and End-to-End



Session protocols



Radio access network



Programmable defenses