Insecurity of Voice Solution VoLTE in LTE Mobile Networks

Chi-Yu Li[1], Guan-Hua Tu[1], Chunyi Peng [2],
Zengwen Yuan[1], Yuanjie Li[1], Songwu Lu[1], Xinbing Wang[3]

1: University of California, Los Angeles;
2: The Ohio State University;
3: Shanghai Jiao Tong University

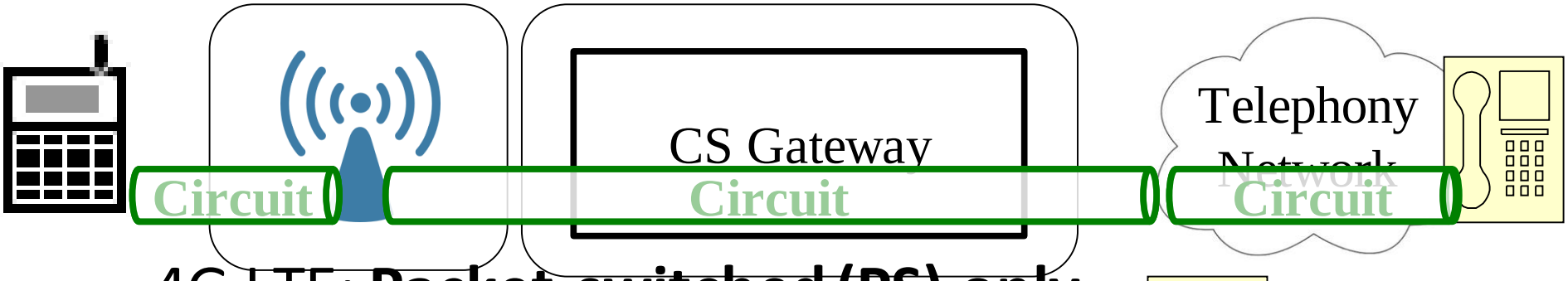
The first two authors equally contribute to this work.

Voice: Vital Carrier Service All Along

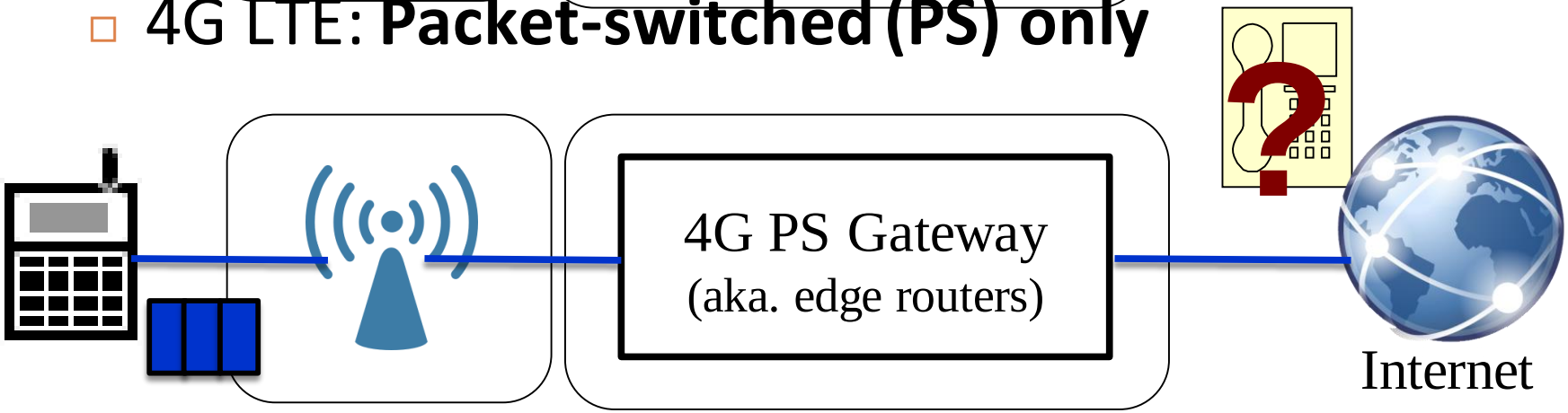
30+ years support in cellular networks

Voice Evolved in 4G LTE

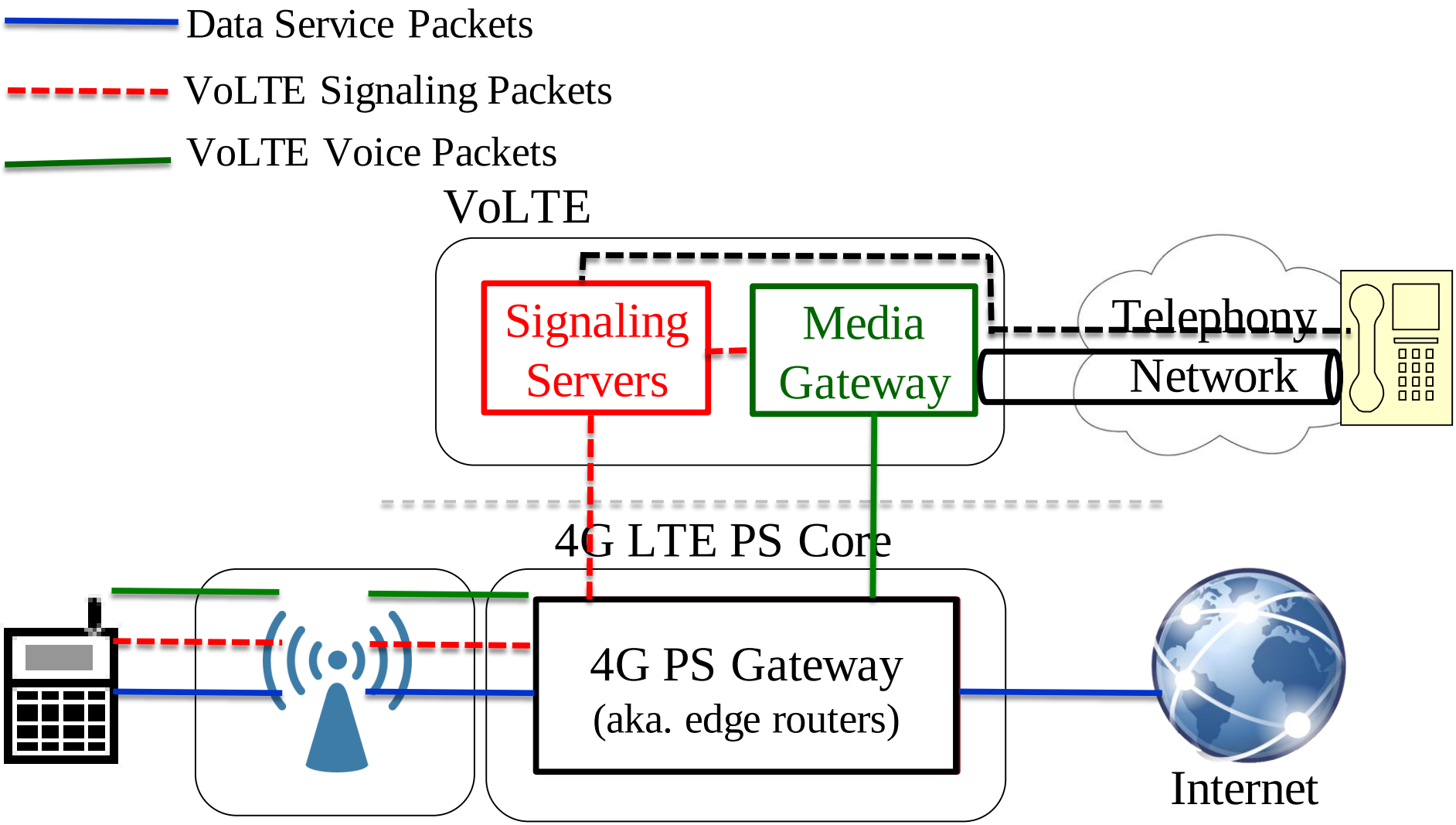
- Legacy voice solution: Circuit-Switched (CS)
  - **Carrier-grade quality**



- 4G LTE: **Packet-switched (PS) only**



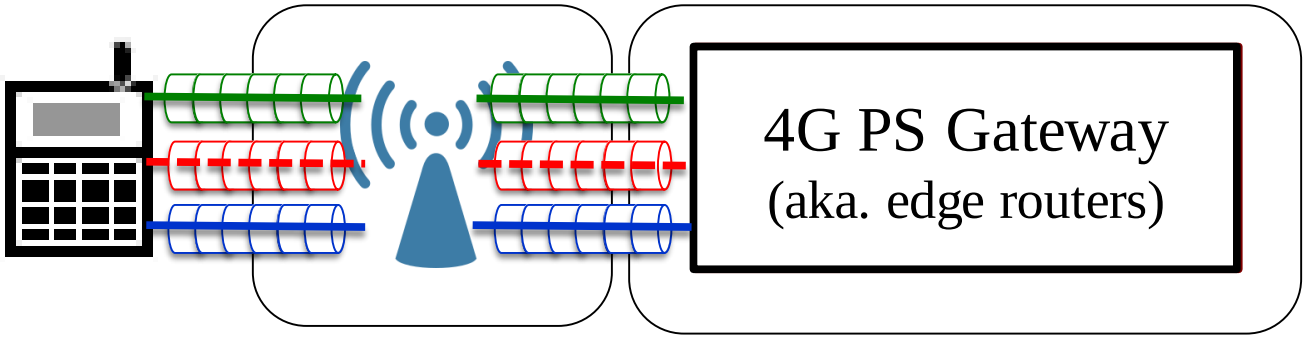
Voice over LTE (VoLTE): Carry Voice in Packets



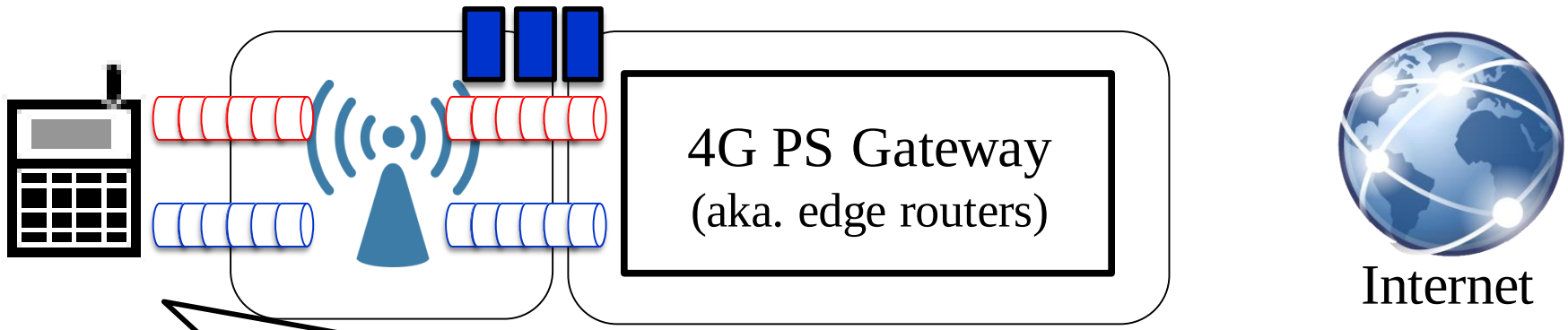
How to provide “Carrier-Grade” Voice in VoLTE?

- Define “Bearer” with distinct QoS profile to deliver packets

	Delivery	Priority
VoLTE Voice Bearer	**Guaranteed-Bit-Rate**	2
VoLTE Signaling Bearer	Best Effort	**1 (highest)**
Data Service Bearer	Best Effort	6-9



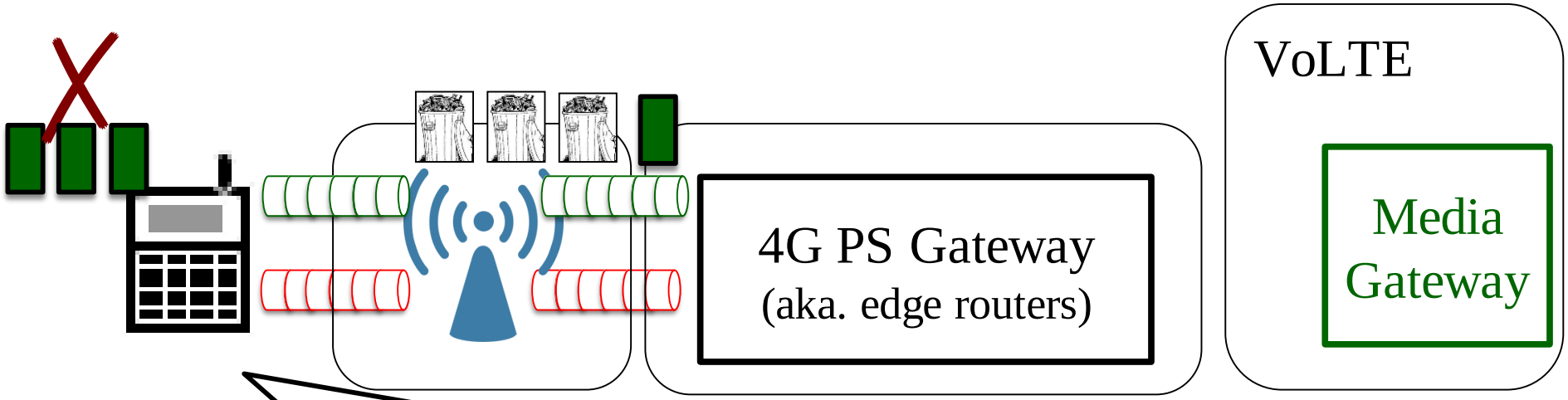
Potential Security Threats in VoLTE



#1: Carry **"data"** over **VoLTE Signaling bearer?**

If yes, abuse its charging scheme (**free**) and higher-priority/QoS scheme for **"data"**?

Potential Security Threats in VoLTE



#2: Inject **(junk) data** into **VoLTE voice bearer?**

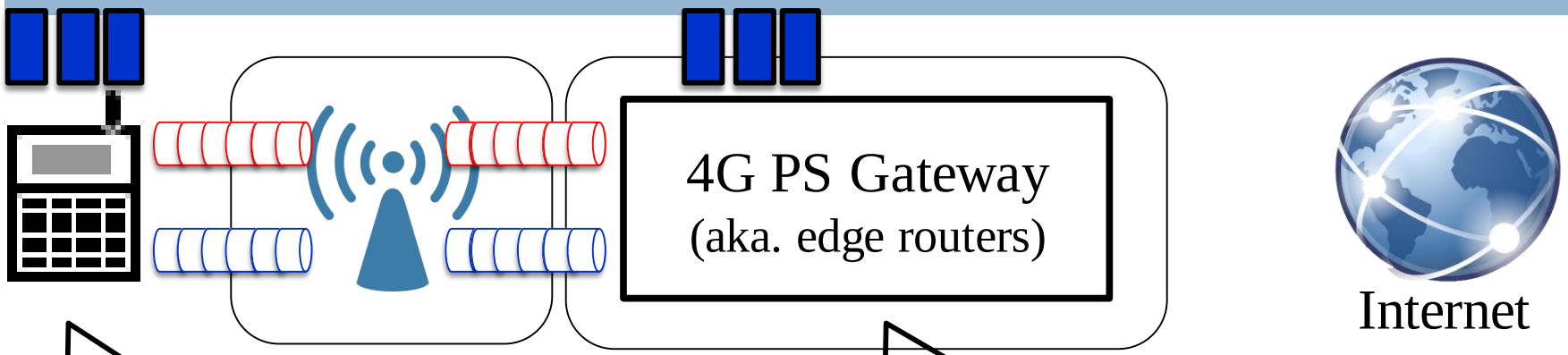
If yes, authentic voice traffic will be blocked.

Overview of Our Findings

- **Data:** Carry data over VoLTE signaling bearer
  - Free data service
  - Higher-priority data service
  - Overbilling
  - Data Denial-of-Service
- **Voice:** Inject junk data into VoLTE voice bearer
  - Voice Denial-of-Service (muted voice)
- **Vulnerabilities** from
  - VoLTE standards
  - Carrier networks
  - Mobile devices (software and hardware)

Carry Data in VoLTE Signaling Bearer

Two Access Control at Device & Network

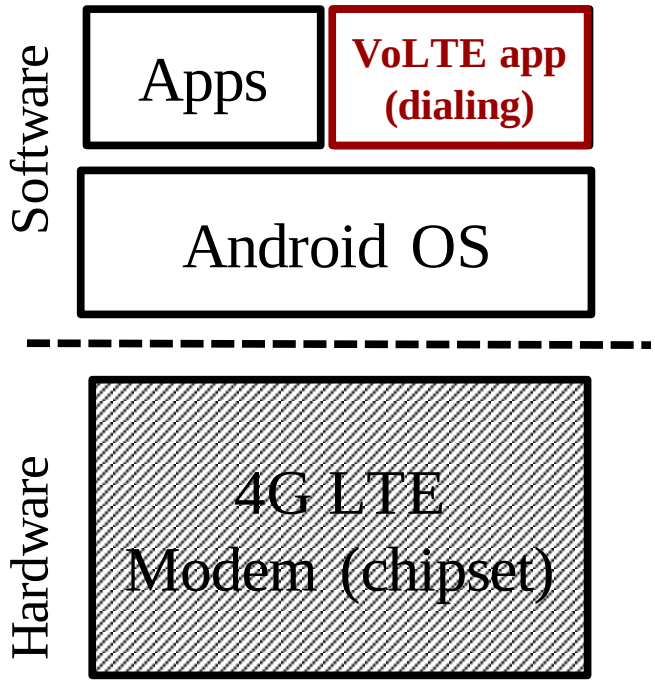


Q1: [Device]
Will the phone allow an app (user-space) to send data packets out into VoLTE signaling bearer?

Q2: [Network]
Will the network allow packets over VoLTE signaling bearer to non-VoLTE destinations (Internet)?

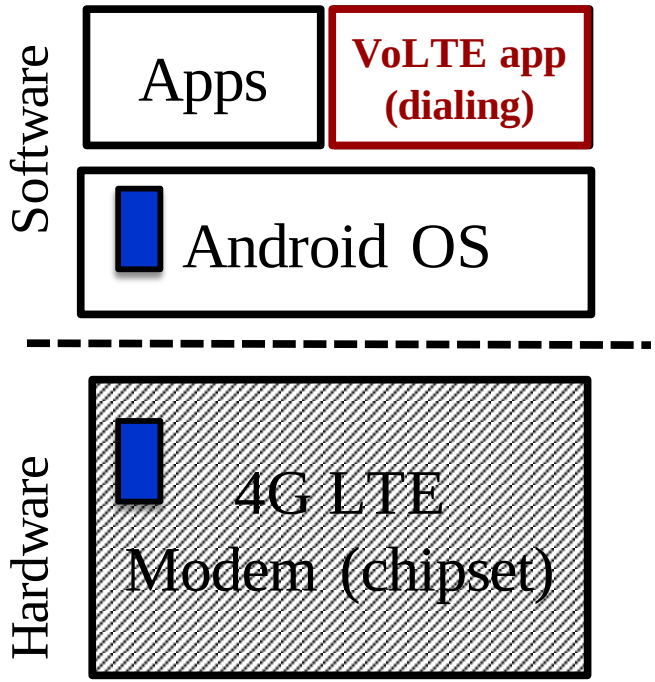
No Access Control on the Phone

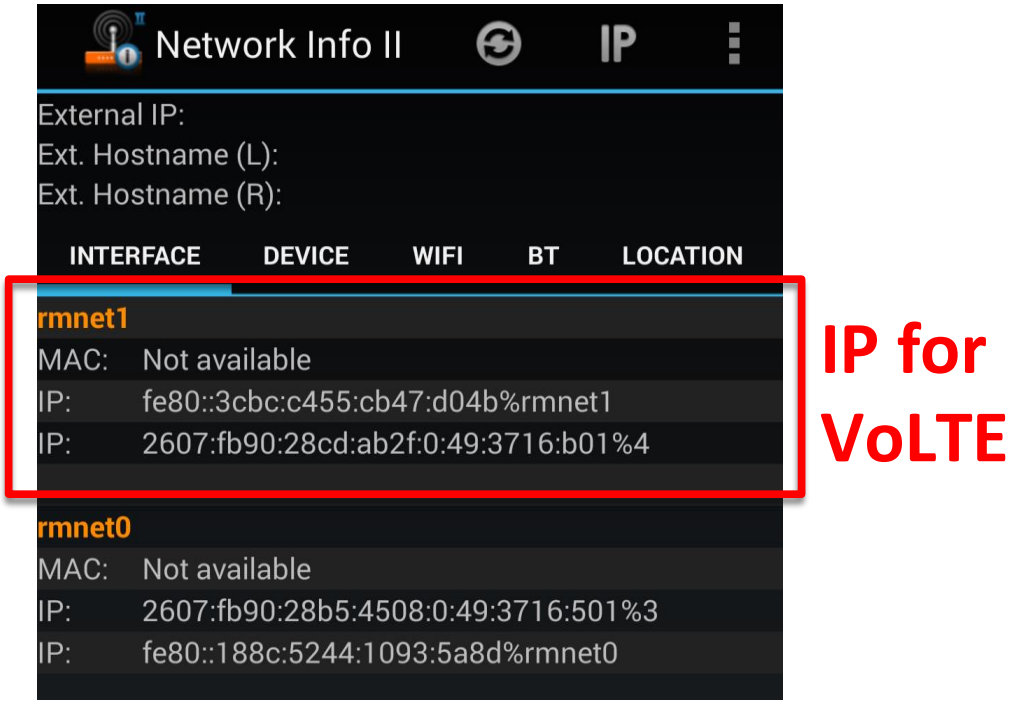
- #1: VoLTE signaling functions are implemented in IP-based software (**Open** to OS and apps)
  - A system app



No Access Control on the Phone

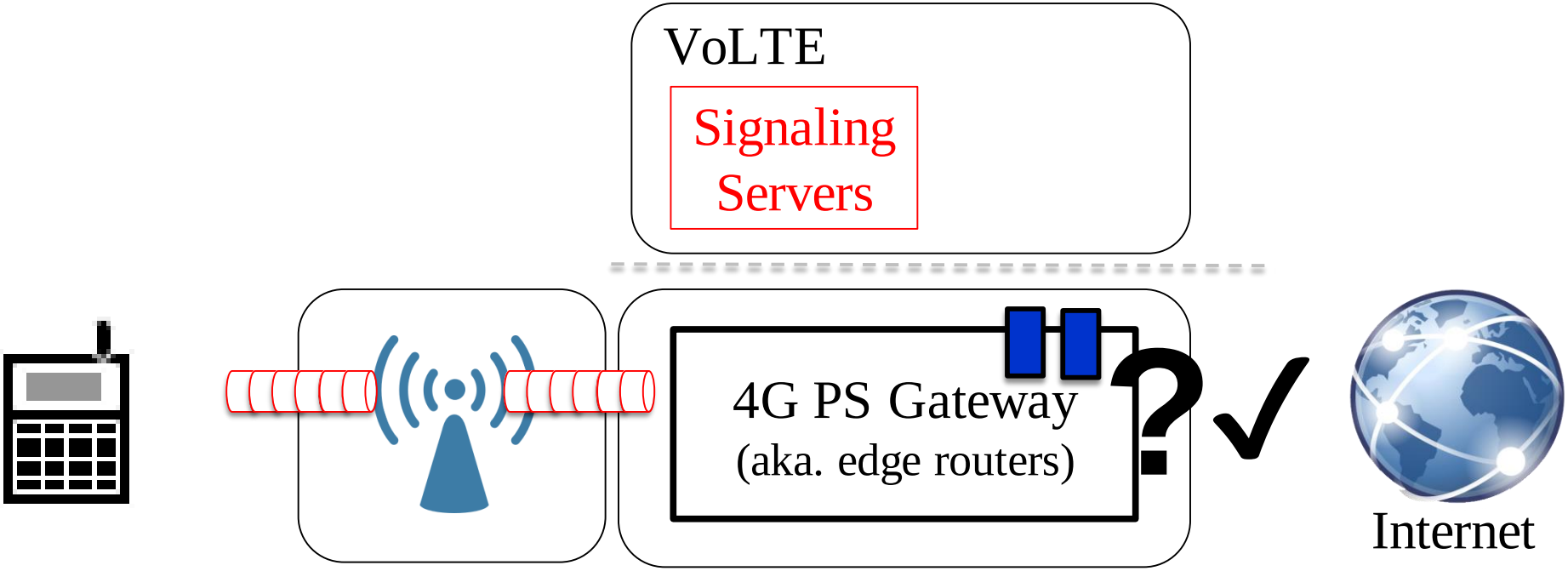
- #2: No proper permission control to VoLTE Signaling network interface in OS (software)
  - Given IP, app (w/Internet permission) send packets
- #3: No access control in chipset (hardware)





No Access Control in Network

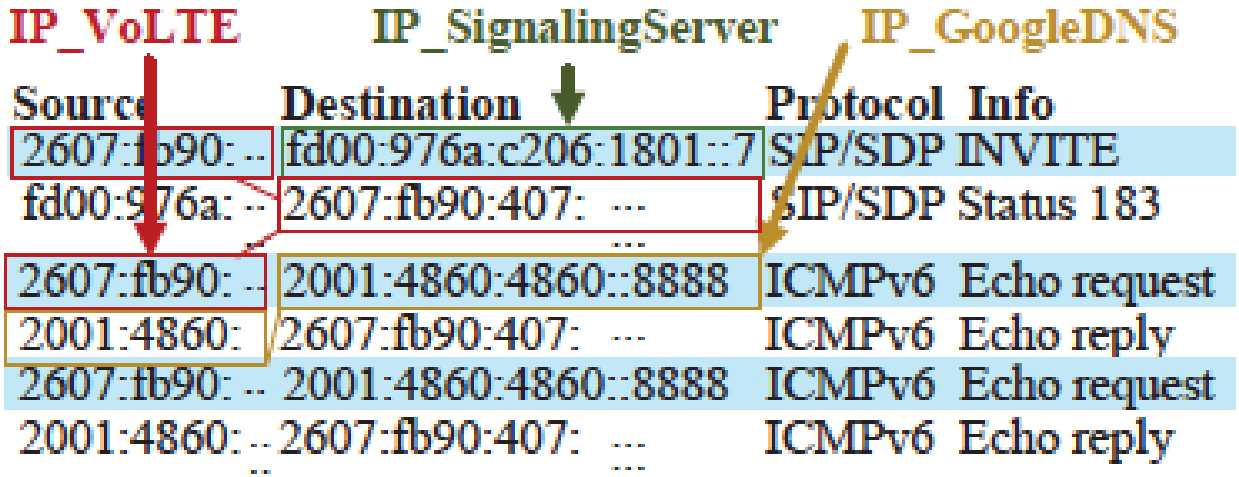
- #4: Imprudent routing in network
  - Simply routing based on destination IP
  - US-I: Internet and Mobile ✓
  - US-II: Mobile ✓



Finally, it works out!

- Mobile-to-Internet
  - Example: ping Google

(a) Two interfaces

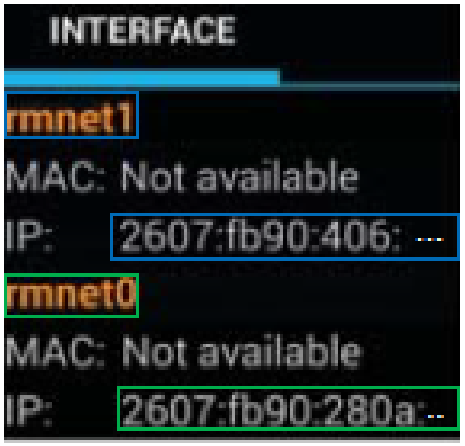


(b) Mobile-to-Internet (Google DNS server)

Finally, it works out!

- Mobile-to-Internet

- Mobile-to-Mobile
  - VoLTE-to-VoLTE
  - VoLTE-to-PS



(a) M2's interfaces

Mobile 1: IP_VoLTE Mobile 2: IP_VoLTE, IP_Data

Source	Destination	Protocol	Info
2607:fb90:407: ...	2607:fb90:406: ...	ICMPv6	Echo request
2607:fb90:406: ...	2607:fb90:407: ...	ICMPv6	Echo reply
2607:fb90:407: ...	2607:fb90:406: ...	ICMPv6	Echo request
...	...		
2607:fb90:407: ...	2607:fb90:280a: ...	ICMPv6	Echo request
2607:fb90:280a: ...	2607:fb90:407: ...	ICMPv6	Echo reply
2607:fb90:407: ...	2607:fb90:280a: ...	ICMPv6	Echo request
...	...		

(b) Mobile-to-Mobile (M1 → M2)

Free for VoLTE Signalings

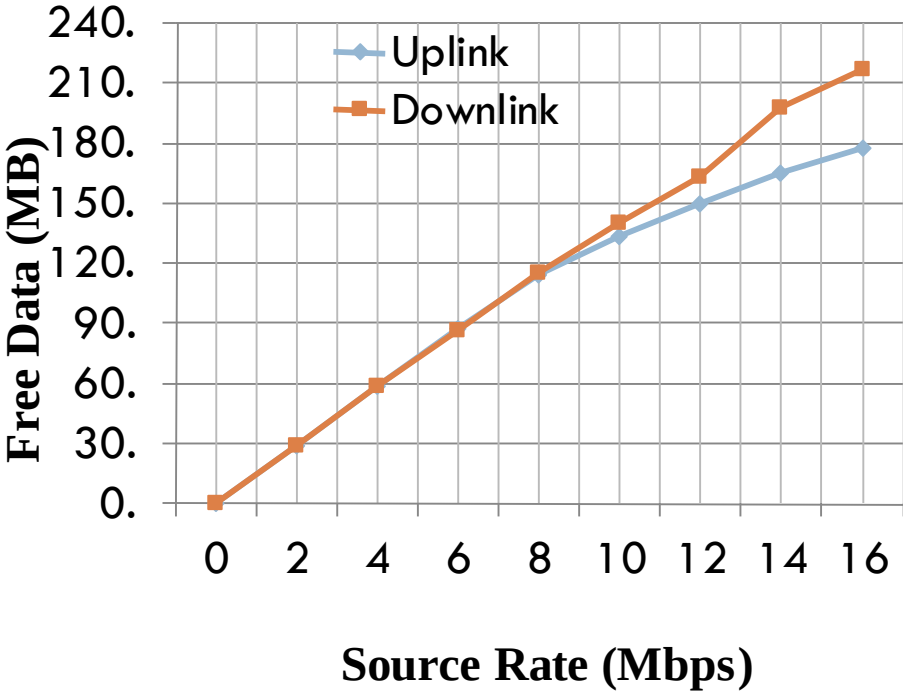
- VoLTE Signaling free of charges
  - Voice calls: charged by minutes
  - Signaling: no charges (usually small volume)
  - Validated in two US major carriers

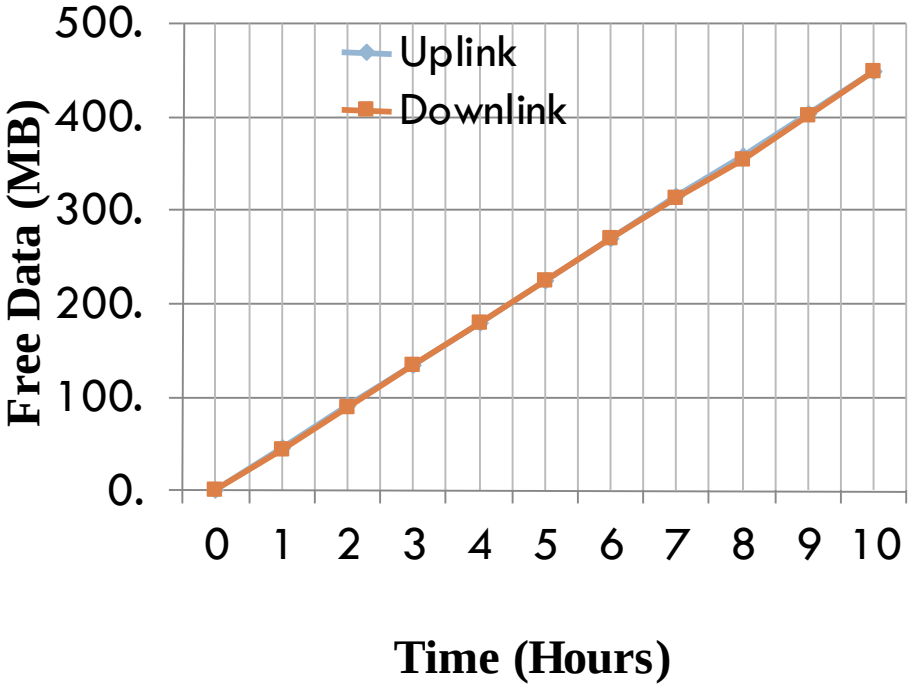
- Rational, but exploited for free data access

Free Data Service: Skype as Demo

http://web.cs.ucla.edu/~ghtu/myfiles/free-data-service.mp4

Free Data Service

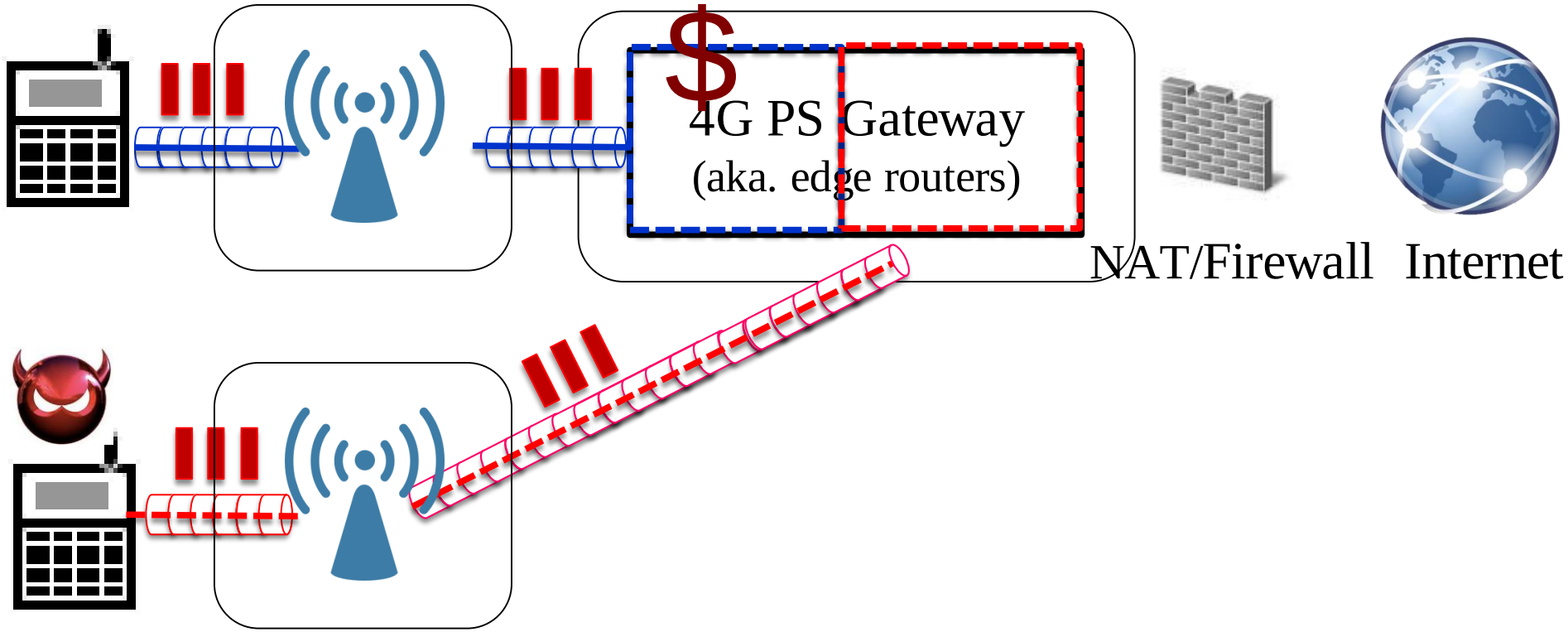




There exists NO signs of limit on the *volume*, *throughput* and *duration* for free data service

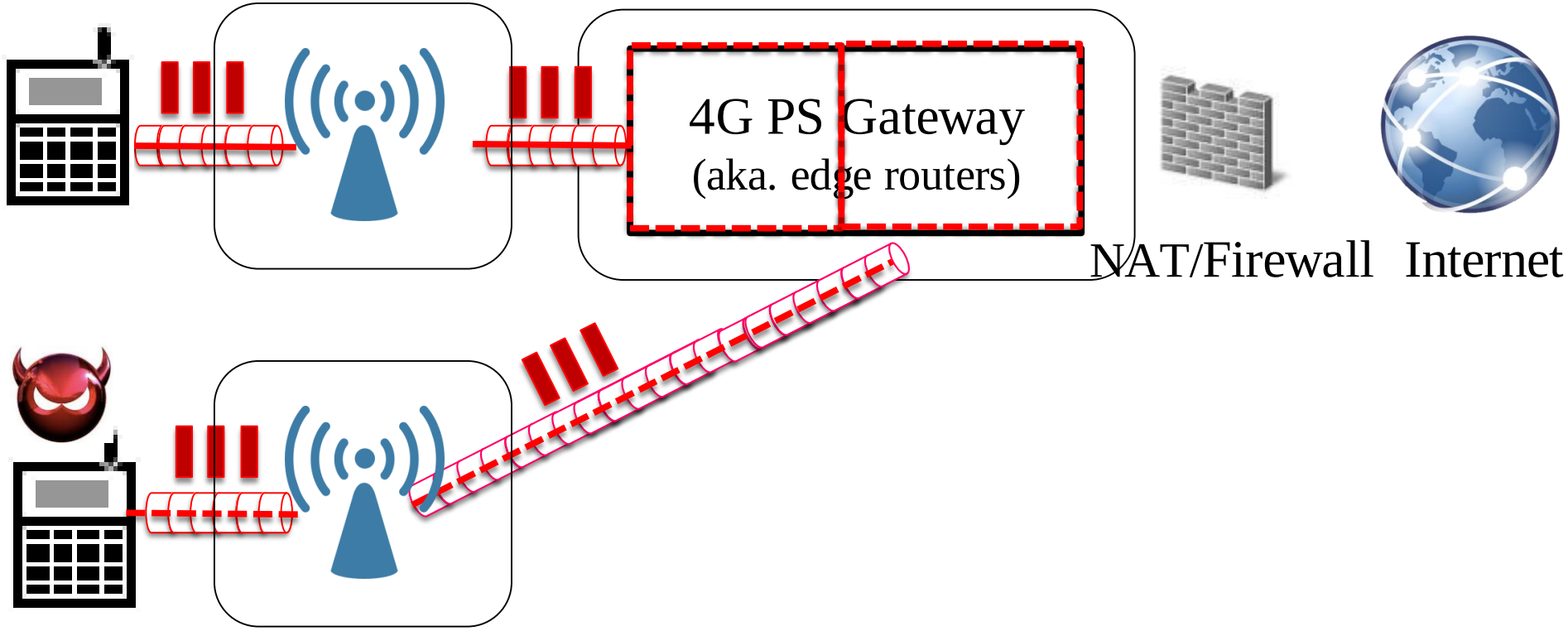
Overbilling Attack

- Spamming via Mobile-to-Mobile (VoLTE-to-PS)
  - Bypass inbound traffic access control at border



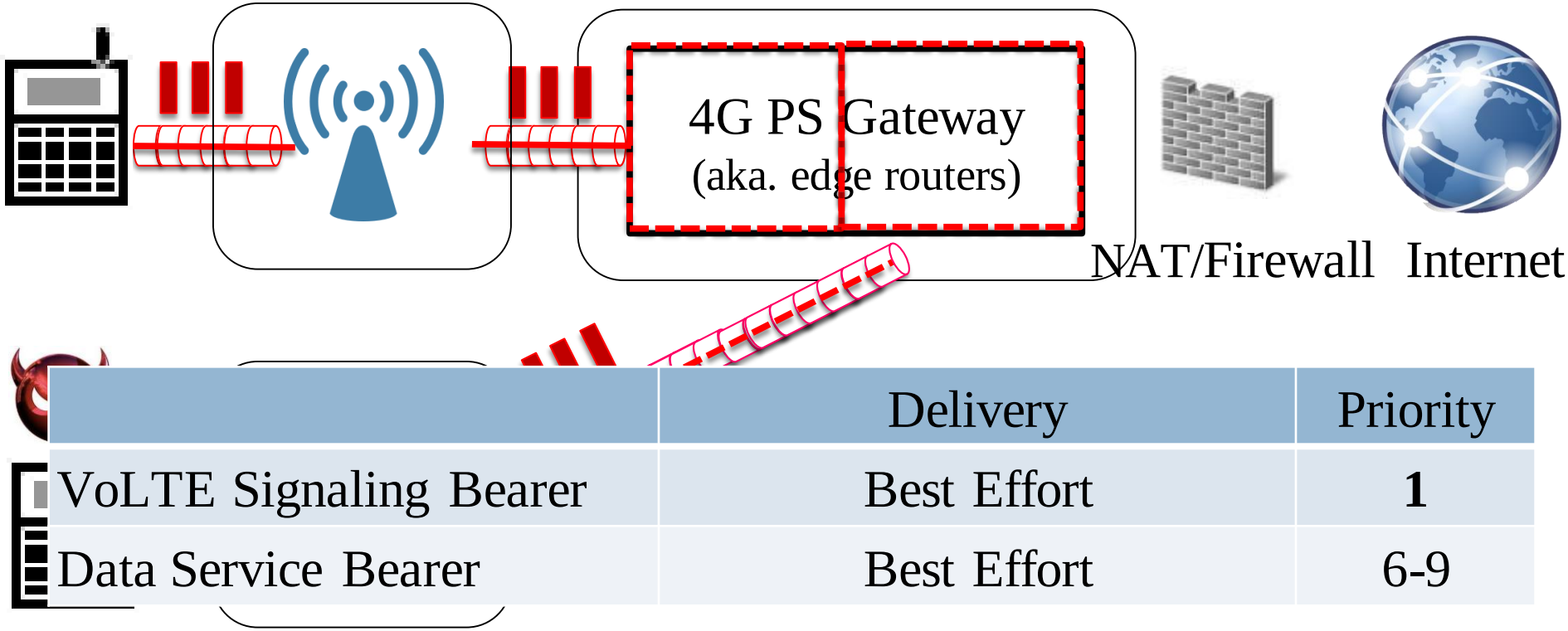
Data Denial-of-Service Attack

- Spamming via Mobile-to-Mobile (VoLTE-to-VoLTE)
  - Exploit higher priority of VoLTE signaling bearer



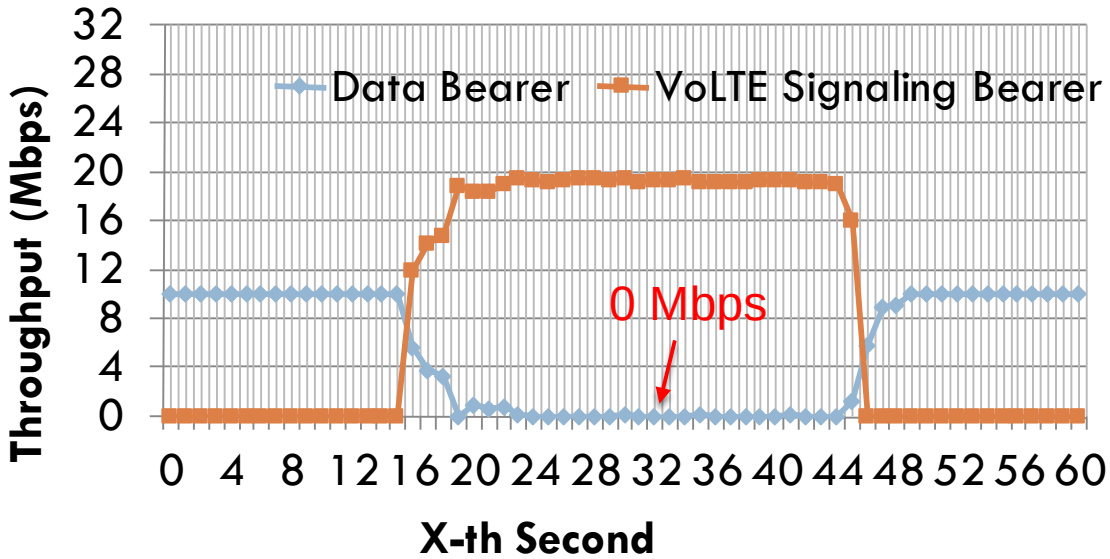
Data Denial-of-Service Attack

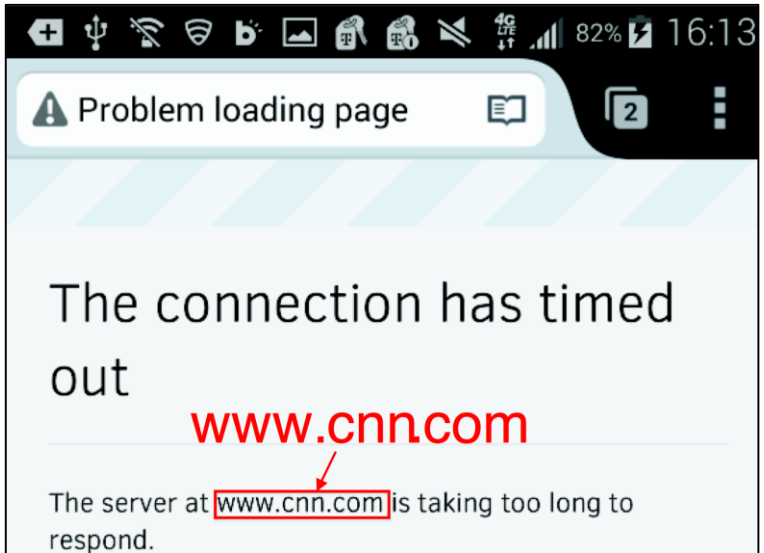
- Spamming via Mobile-to-Mobile (VoLTE-to-VoLTE)
  - Exploit higher priority of VoLTE signaling bearer

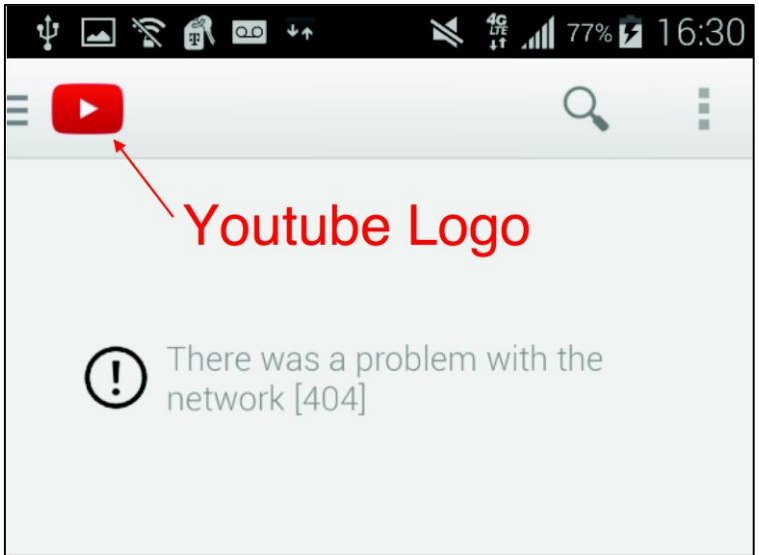


	Delivery	Priority
VoLTE Signaling Bearer	Best Effort	**1**
Data Service Bearer	Best Effort	6-9

Data Denial-of-Service Attack

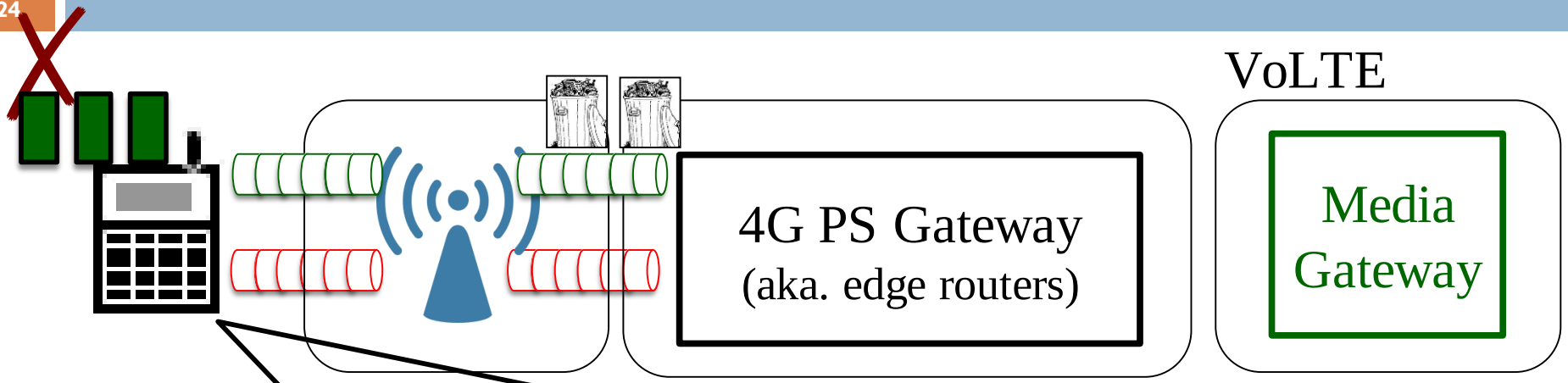






Inject Junk Data into VoLTE Voice Bearer

Similar, but Seemingly More Secure

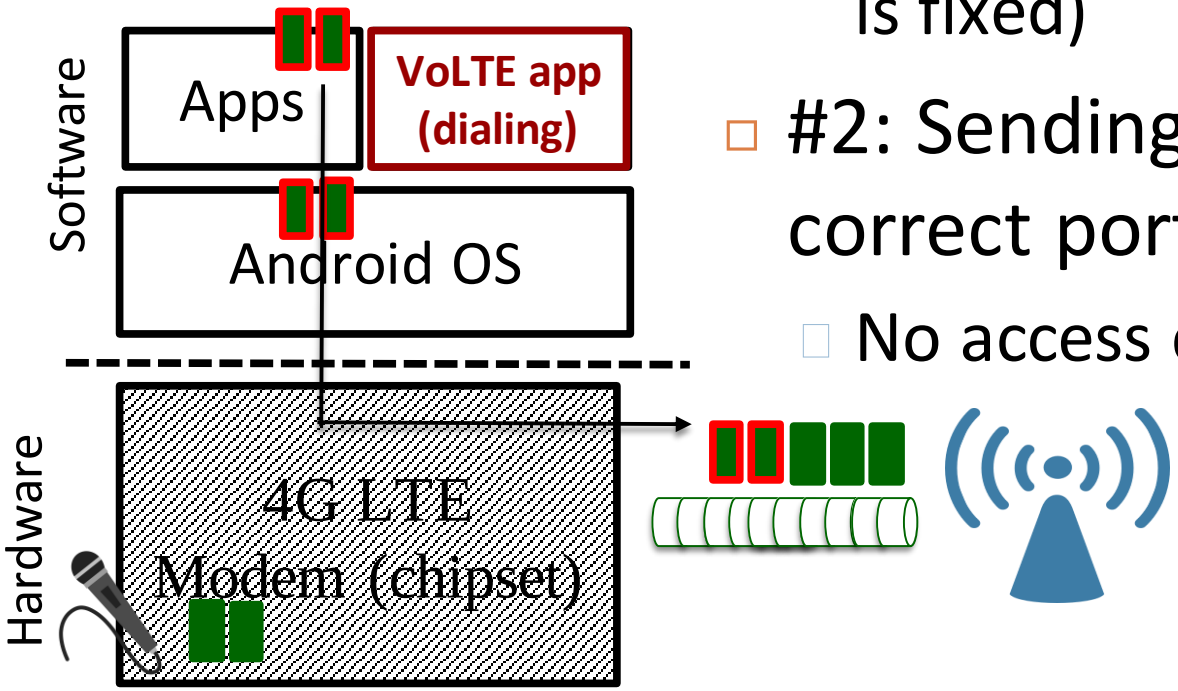


Inject (junk) data packets into **VoLTE voice bearer** as to **VoLTE signaling bearer**

But, voice bearer is designed for specific RTP/RTCP session (e.g., destIP, destPorts) – Such info is **confidential** (It varied with call and only delivered in encrypted VoLTE signaling messages)

Insufficient VoLTE Voice Access Control

- #1: only dest. port# needed
  - Use fixed media gateway (dest. IP is fixed)
- #2: Sending data packets with correct port# is allowed
  - No access control in hardware

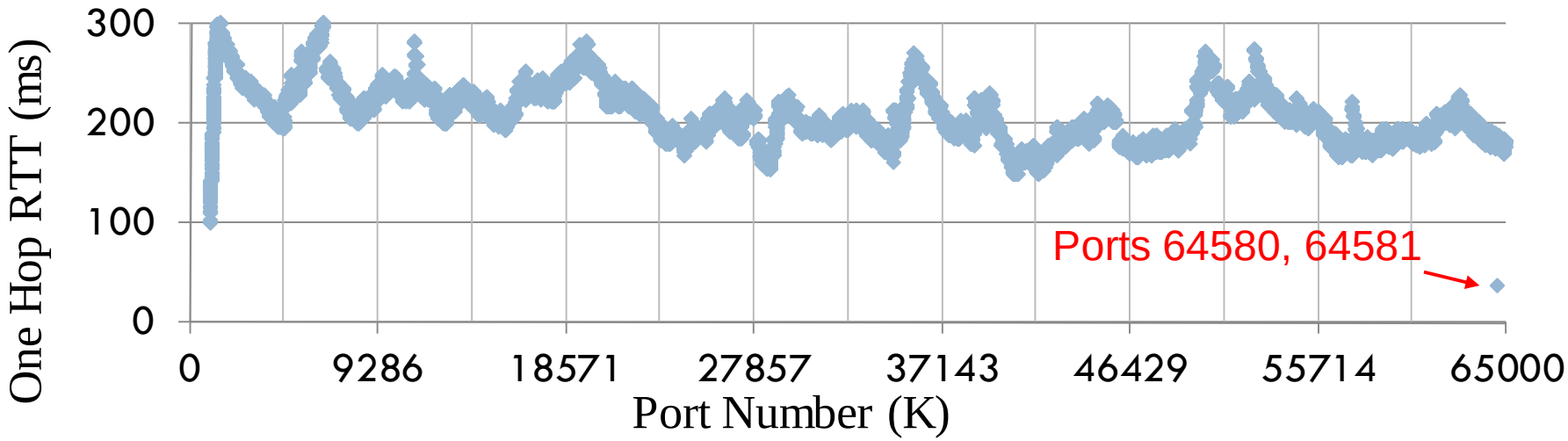


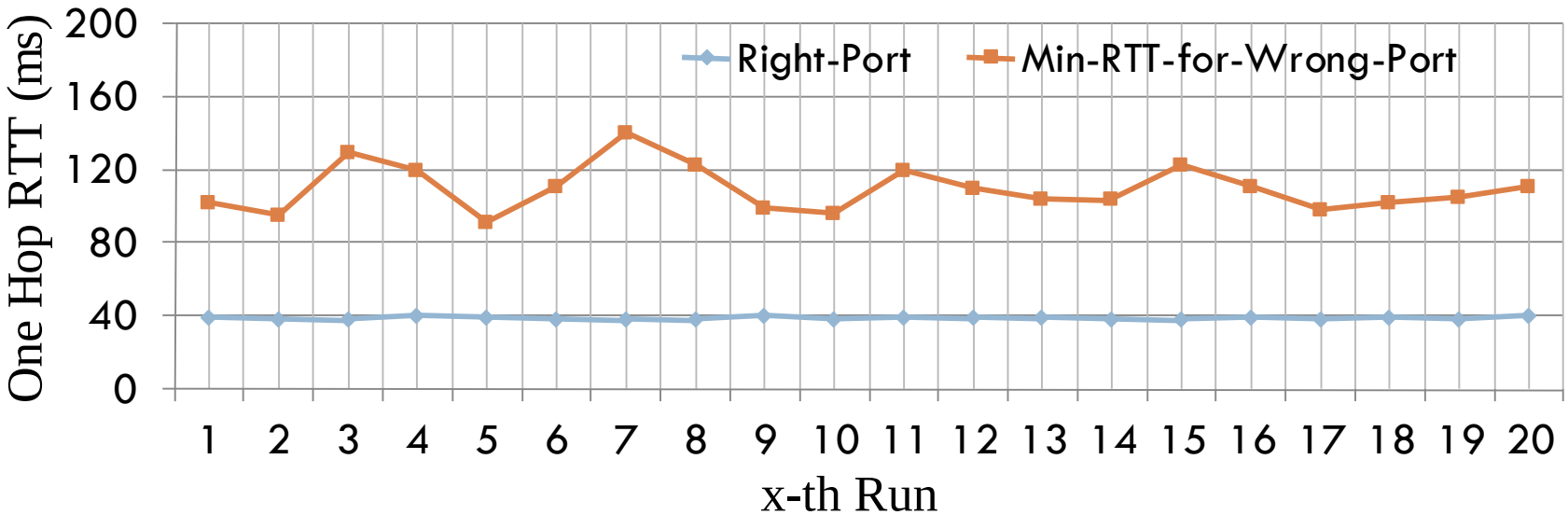
Port# is Secret, but can be Easily Leaked

- Share same IP among voice and signaling bearers
  - Port# matched, →VoLTE voice bearer
  - Port# unmatched, →VoLTE signaling bearer
- Leaked through **distinct** behaviors caused by various QoS profiles
  - Guaranteed-Bit-Rate vs. High-Priority Best Effort
  - Low-rate voice traffic **NOT affected** by heavy VoLTE signaling

	Delivery	Priority
VoLTE Voice Bearer	**Guaranteed-Bit-Rate**	2
VoLTE Signaling Bearer	Best Effort	1

Infer RTP/RTCP Destination Ports





Voice DoS: Muted Call

http://web.cs.ucla.edu/~ghtu/myfiles/mute_voice_attack.mp4

Root Causes & Recommended Solutions

- VoLTE standards
  - Grant the singaling bearer with priority but no speed limit.
- Carrier networks
  - Imprudent routing & charging ploices for VoLTE signaling
  - Fix: disable routing, enable VoLTE volume accounting
- Mobile Devices
  - Lack access control at both software (improper permission) and hardware (missing)
  - Fix: VoLTE-specific permission, anomaly detection

Updates

- Report and work with 2 US carriers to fix problems
- Partial solutions in place (07/2015, 08/2015)
- US-I
  - Disable routing to Non-VoLTE destination
  - Fixed: free data, overbilling, data DoS
  - Not fixed: voice DoS
- US-II
  - Limit the speed of Mobile-to-Mobile to 600 kbps
  - Fixed: data DoS
  - Not fixed: voice DoS, free data, overbilling

Conclusion

- VoLTE **designed to carry voice** can be exploited to **carry data**
  - Real threats: free data, overbilling, data DoS, voice DoS.
- Lessons at its early deployment
  - Carrier network, device OS, chipset vendors and standards have room to improve
- **New opportunity for mobile industry security**
  - Hardware-based Mobile Security
  - Require more close cooperation between various parties…….

Thank you! Questions?

More details or updates about voice security in 4G LTE can be found in our UCLA-OSU cooperation project website