Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations

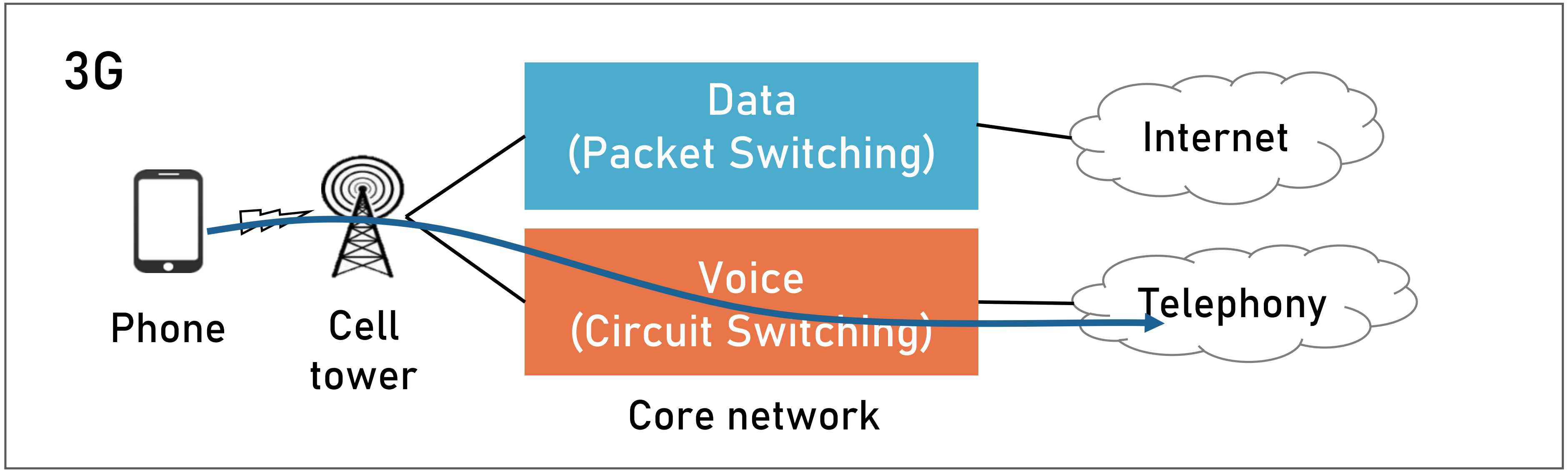
Presenter : Gyuhwan Park
Slides from SysSec Lab

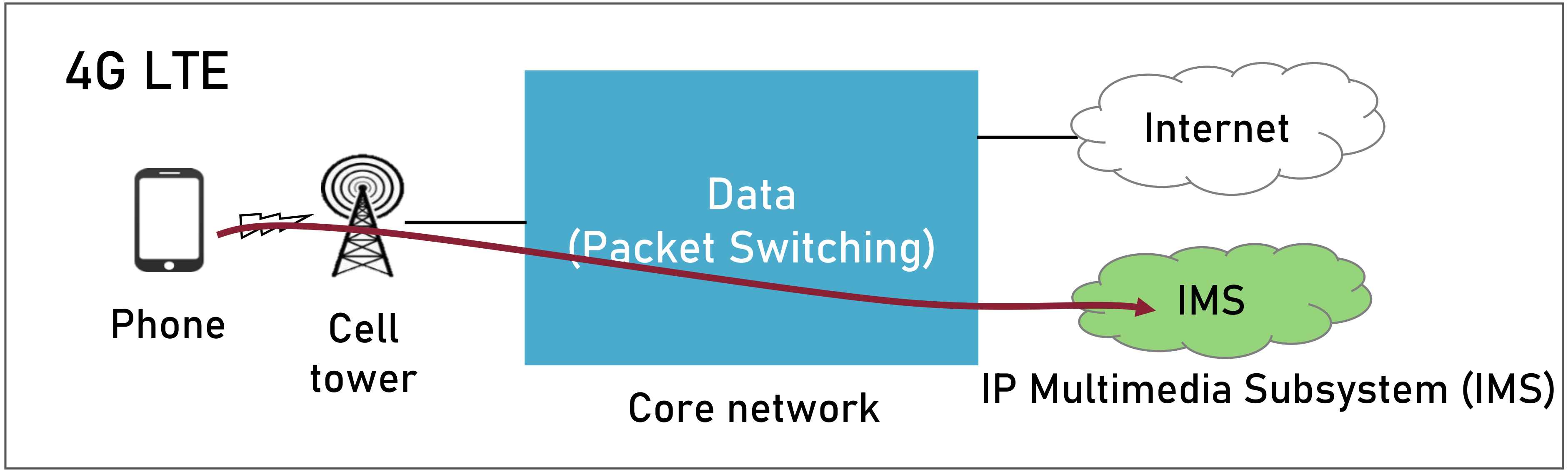
VoLTE = Voice over LTE

- Implementation of VoIP on LTE

- 3G network
  - Data and voice are separated
- 4G LTE network : All-IP based Network
  - Both data and voice are delivered as data-flow

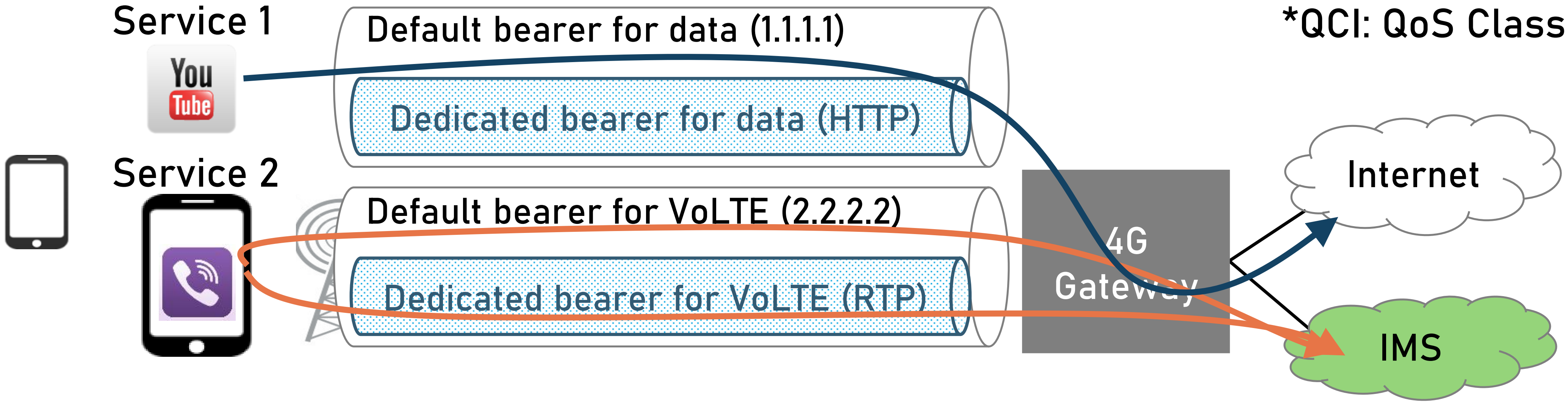
- Advantages on VoLTE
  - For users: high voice quality, faster call setup, better battery life.
  - For operators: increase usability, reduce cost, rich multimedia services


3G
Phone
Cell tower
Data
(Packet Switching)
Voice
(Circuit Switching)
Core network
Internet
Telephony


4G LTE
Phone
Cell tower
Data
(Packet Switching)
Core network
Internet
IMS
IP Multimedia Subsystem (IMS)

Bearer

- In LTE, all services are delivered with data channels, called “bearers”
  - Data, Voice, Video, …
- Bearer: a virtual channel with below properties
  - Based on QCI* value, it determines bandwidth, loss rate, latency (QoS)
  - Default bearer: Non Guaranteed Bit rate
  - Dedicated bearer: Guaranteed Bit rate



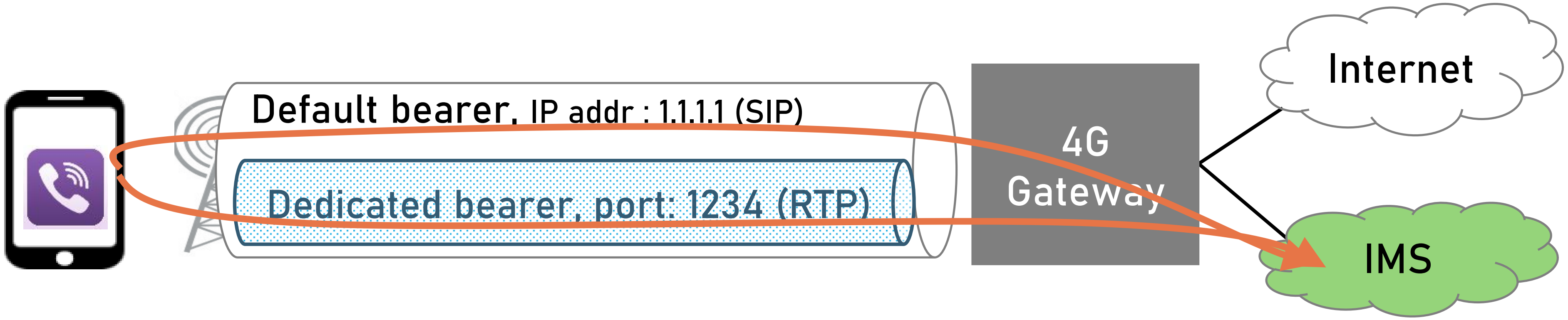
Service 1
Service 2
Default bearer for data (1.1.1.1)
Dedicated bearer for data (HTTP)
Default bearer for VoLTE (2.2.2.2)
Dedicated bearer for VoLTE (RTP)
4G Gateway
Internet
IMS

*QCI: QoS Class Identifier

Voice delivery in LTE

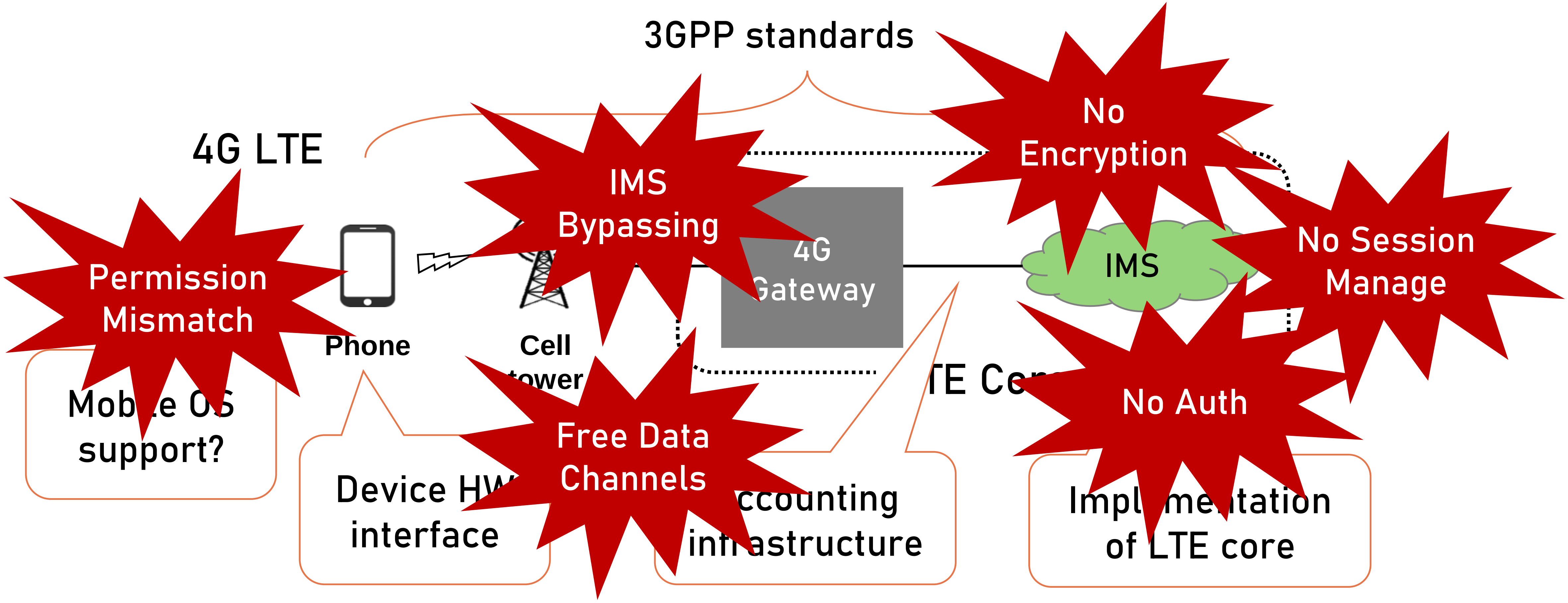
- Voice is delivered through two bearers
- For VoLTE service,
  1. Default bearer: call signaling (control-plane), *SIP
  2. Dedicated bearer: voice data (data-plane), *RTP

*SIP: Session Initiation Protocol
*RTP: Real-time Transport Protocol


Default bearer, IP addr : 1.1.1.1 (SIP)
Dedicated bearer, port: 1234 (RTP)
4G Gateway
Internet
IMS

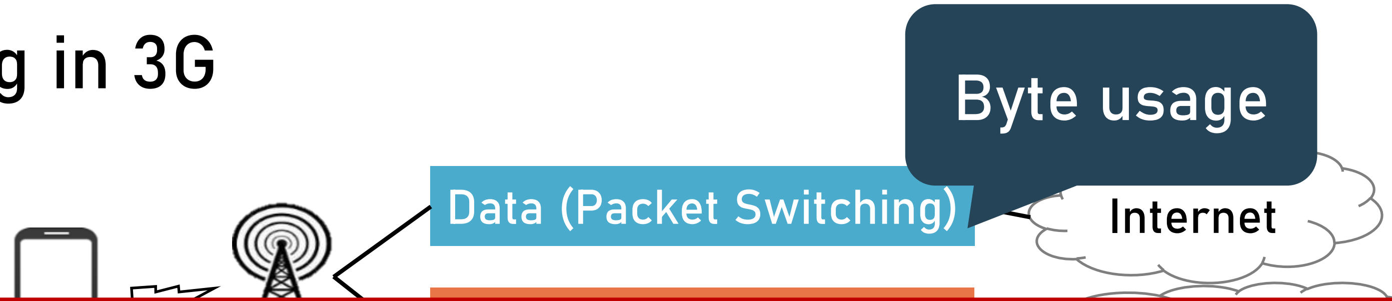
Implementation Problems of VoLTE

- VoLTE makes cellular network more complex



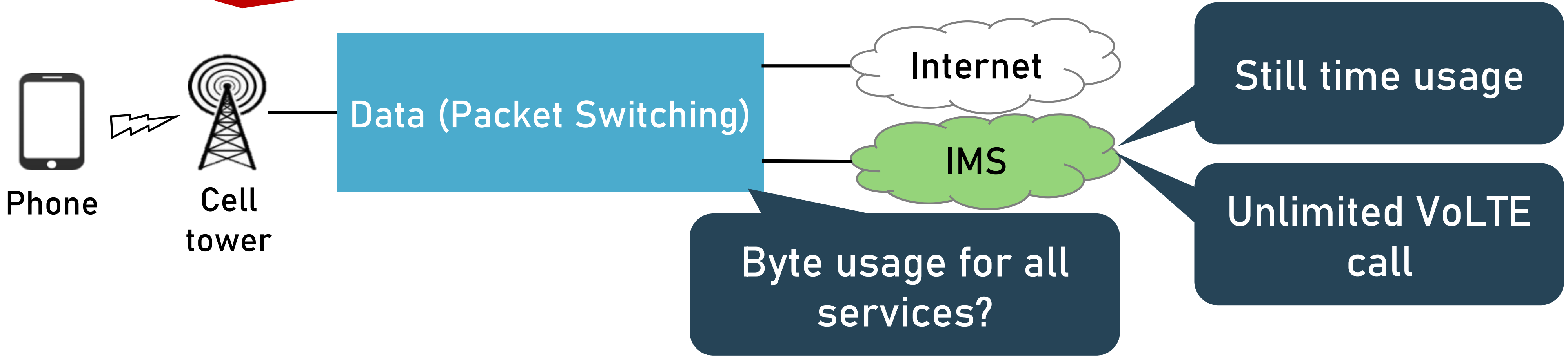
#1: VoLTE Accounting

- Accounting in 3G

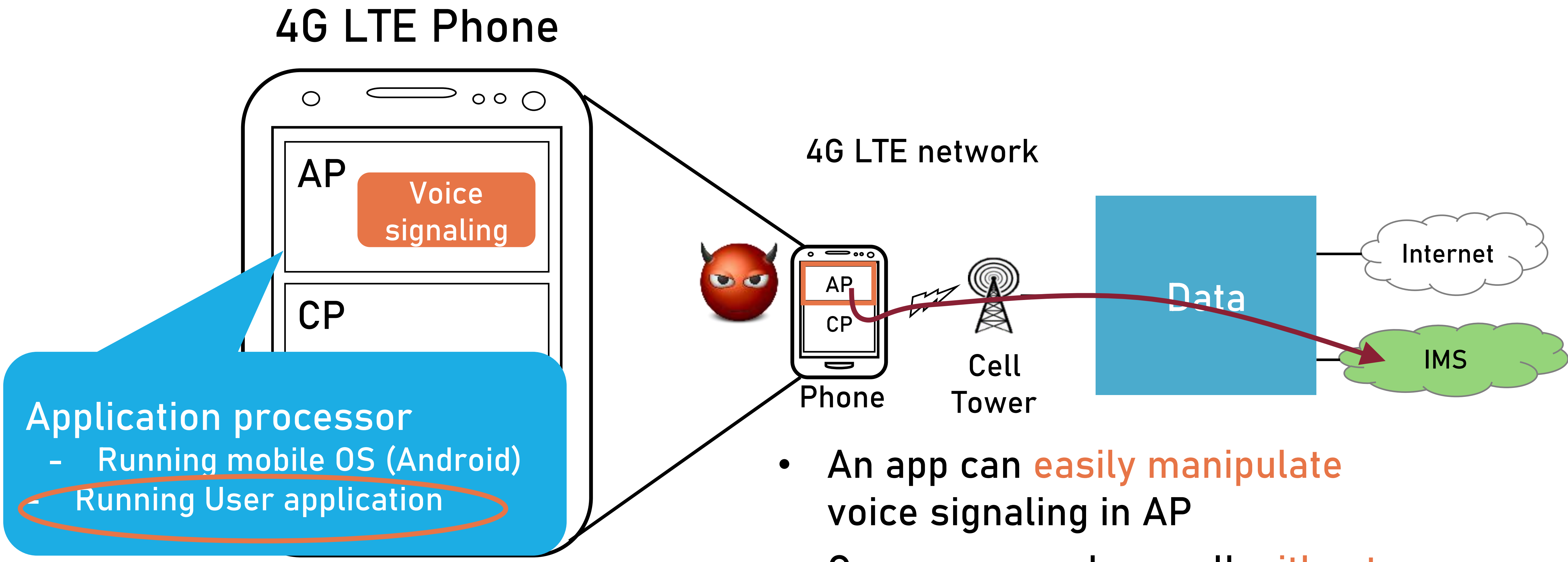


Do operators implement this complicated accounting correctly?

- Accounting in 4 g oLTE)



#2: Voice solution in device, LTE

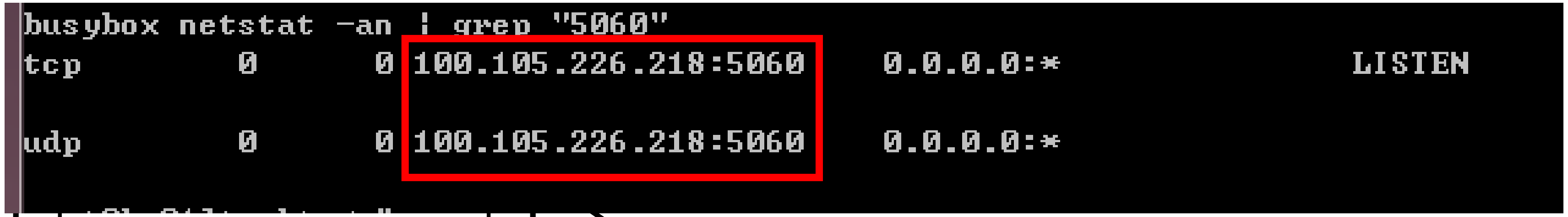


Application processor

- Running mobile OS (Android)
- Running User application

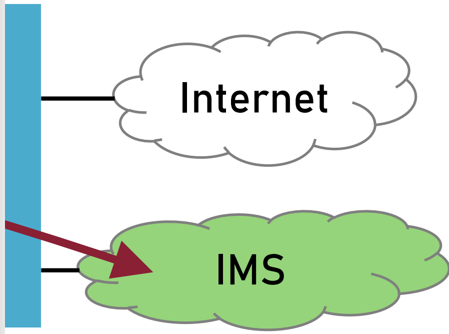
- An app can easily manipulate voice signaling in AP
- Can an app make a call without "CALL_PHONE" permission?

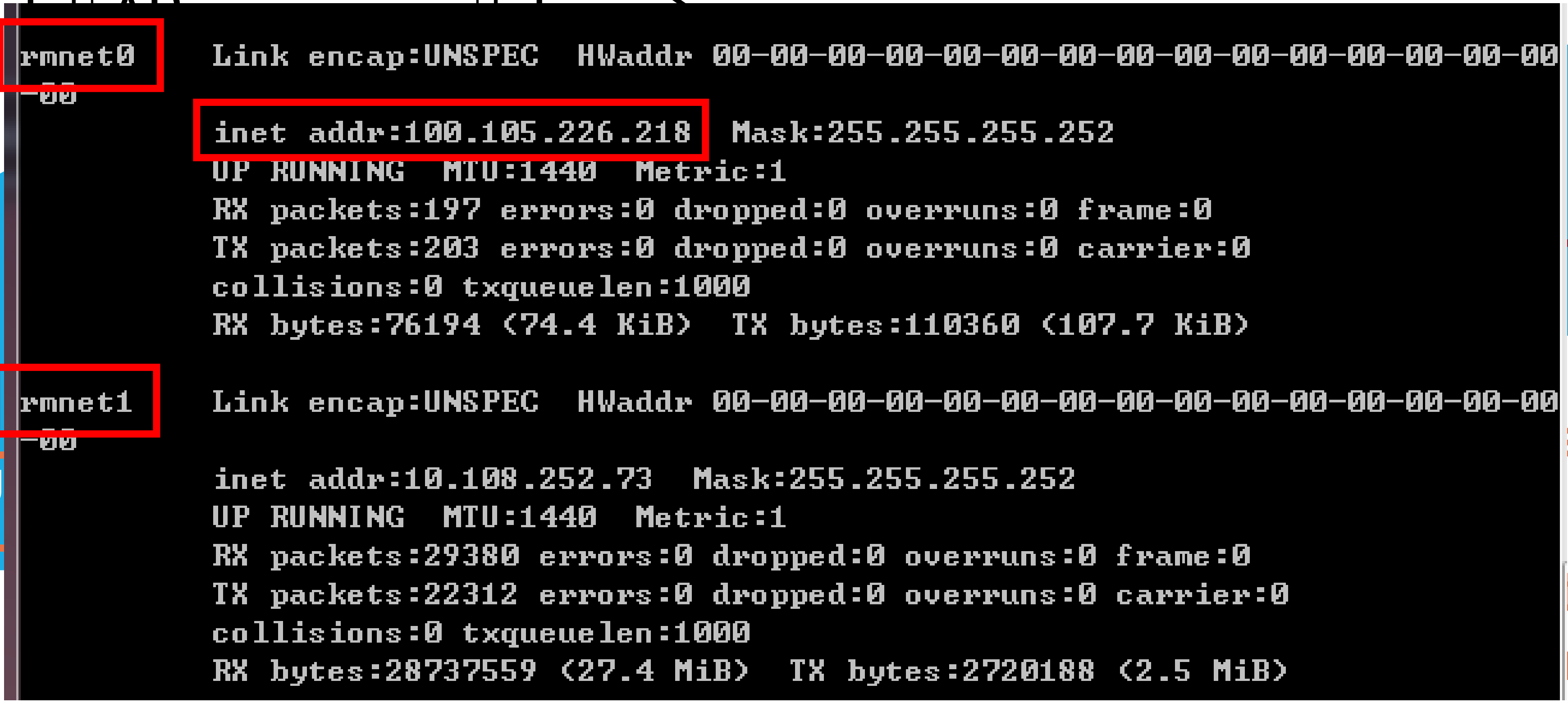
#2: Voice solution in device, LTE



```
busybox netstat -an | grep "5060"
tcp        0      0 100.105.226.218:5060    0.0.0.0:*               LISTEN

udp        0      0 100.105.226.218:5060    0.0.0.0:*
```





```
rmnet0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:100.105.226.218  Mask:255.255.255.252
          UP RUNNING  MTU:1440  Metric:1
          RX packets:197 errors:0 dropped:0 overruns:0 frame:0
          TX packets:203 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76194 (74.4 KiB)  TX bytes:110360 (107.7 KiB)

rmnet1    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:10.108.252.73  Mask:255.255.255.252
          UP RUNNING  MTU:1440  Metric:1
          RX packets:29380 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22312 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28737559 (27.4 MiB)  TX bytes:2720188 (2.5 MiB)
```

Application
- Running
- Running U

ate

thout

n?

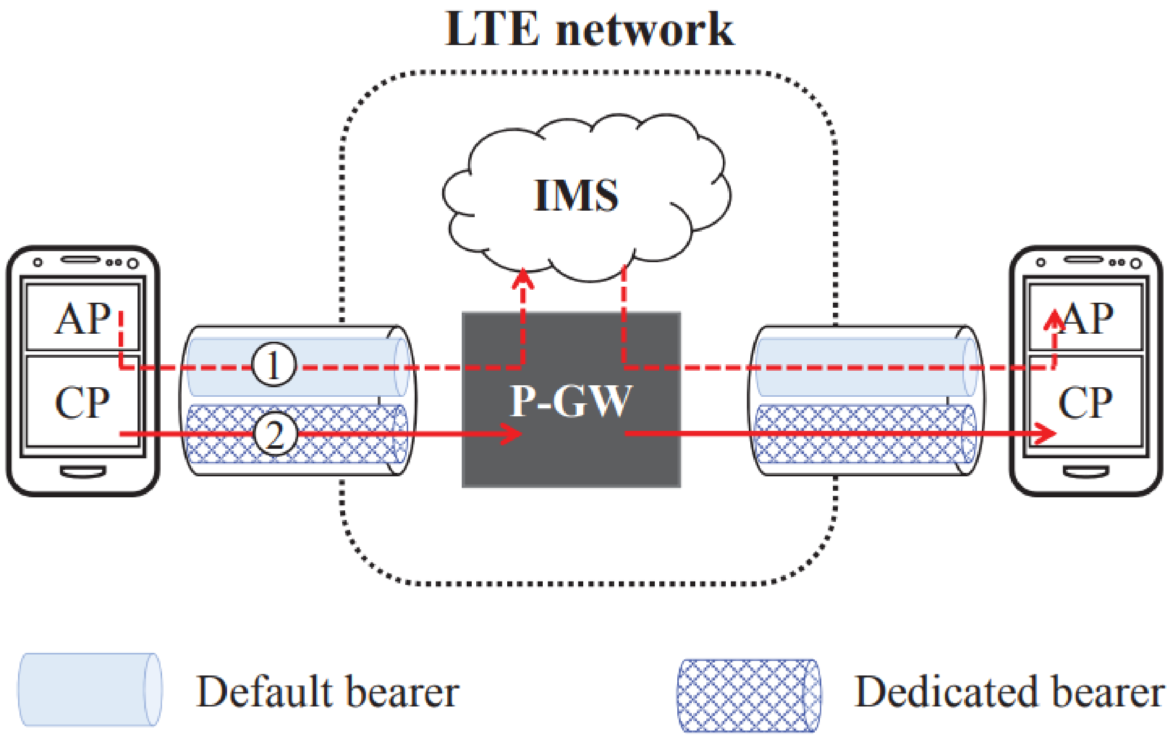
Quick Summary

- Four free data channels
  - Using VoLTE protocol (for all operators)
    - SIP tunneling
    - Media tunneling
  - Direct communication (for some operators)
    - Phone-to-Internet
    - Phone-to-Phone

- Five security issues
  - No encryption of voice packets
  - No authentication of signaling
  - No call session management (DoS on the cellular infrastructure)
  - IMS bypassing
  - Permission model mismatch (VoLTE call without “CALL_PHONE” permission)

Free Channel: VoLTE protocol

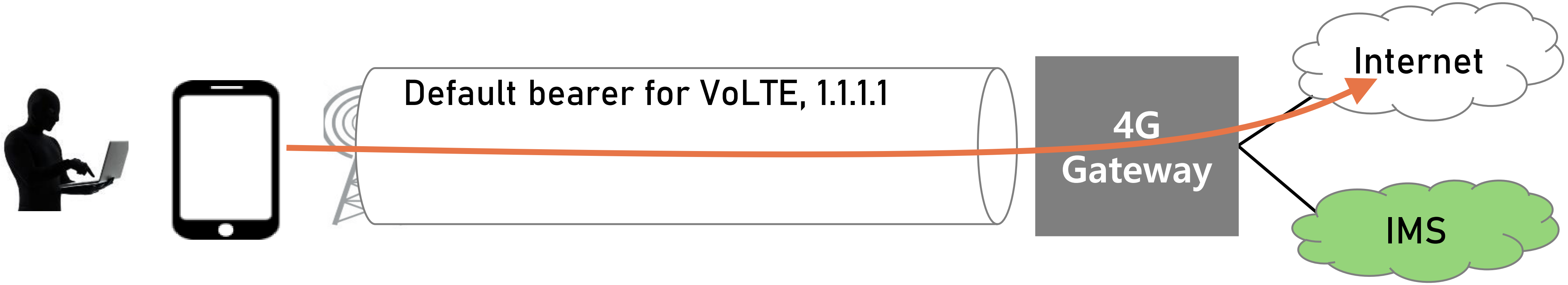
- Free channel using VoLTE protocol
  - 1) SIP tunneling
  - 2) RTP tunneling



Free Channel: Direct communication

- Phone-to-Internet
  - Open a TCP/UDP socket with voice IP
  - Send data to the Internet

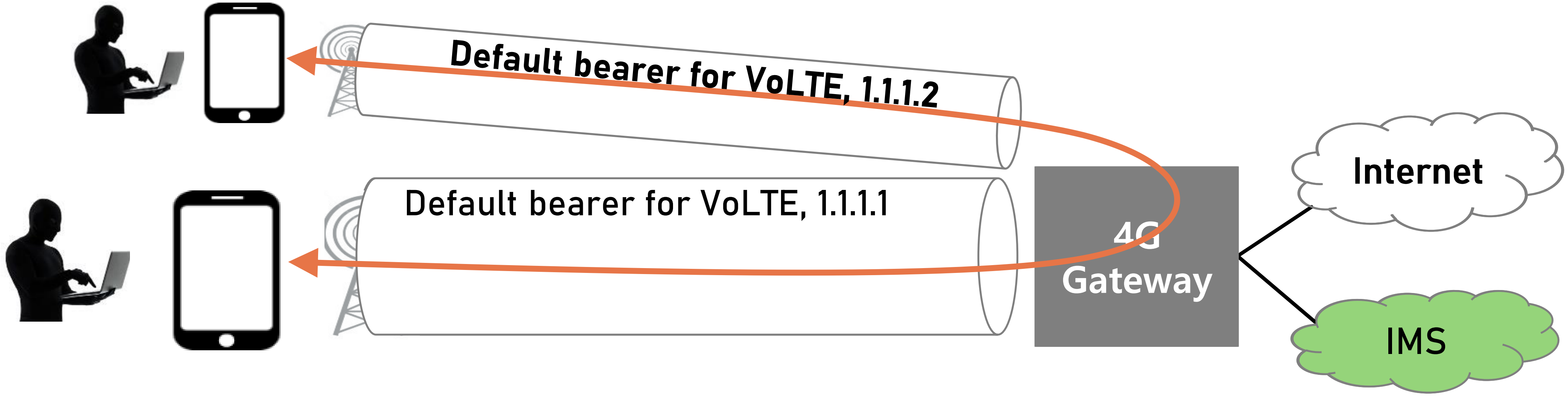
    E.g. TCP/UDP Socket (Src: voice IP/port, Dst: youtube.com/port)



Free Channel: Direct communication

- Phone-to-Phone
  - Open a TCP/UDP socket with voice IP
  - Send data to callee

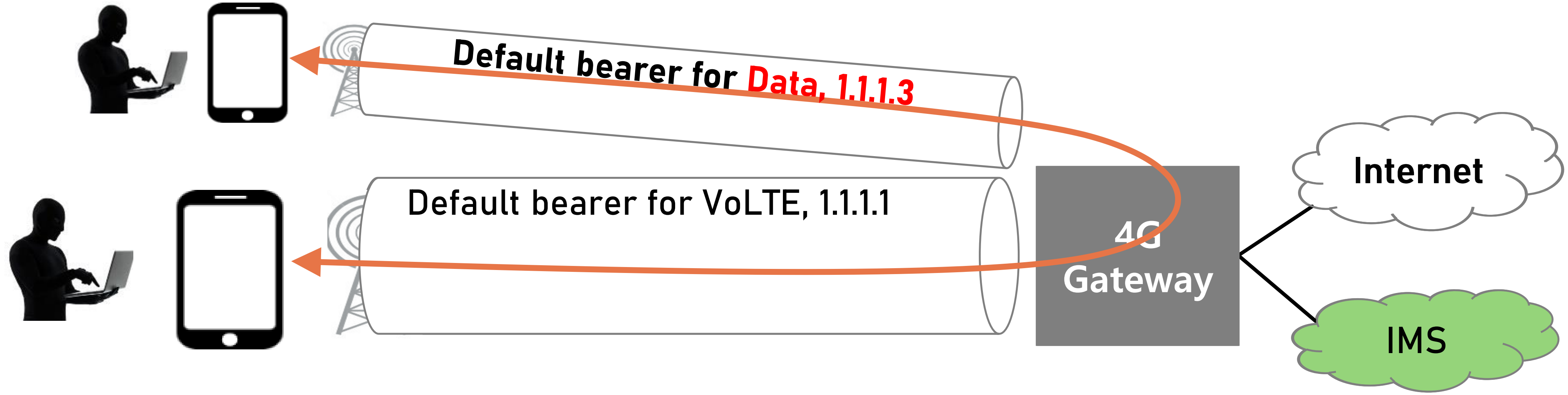
  E.g. TCP/UDP Socket (Src: voice IP/port, Dst: callee's voice IP/port)


Default bearer for VoLTE, 1.1.1.2
Default bearer for VoLTE, 1.1.1.1
4G Gateway
Internet
IMS

Overbilling with Direct Communication?

- Phone-to-Phone
  - Open a TCP/UDP socket with voice IP
  - Send data to callee

  E.g. TCP/UDP Socket (Src: voice IP/port, Dst: callee's data IP/port)


Default bearer for Data, 1.1.1.3
Default bearer for VoLTE, 1.1.1.1
4G Gateway
Internet
IMS

Security issues

- No encryption of voice packets
- No authentication of signaling
- No call session management (DoS on the cellular infrastructure)
- IMS bypassing
- Permission model mismatch (VoLTE call without “CALL_PHONE” permission)

Free Data Channels	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	✓	✓	✓	✓	✓
	Media Tunneling	✓	✓	✓	✓	✓
Direct Communication	Phone to Phone	✓	✘	✓	✘	✘
	Phone to Internet	✘	✓	✓	✘	✘

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No SIP Encryption	😈	🙂	😈	😈	😈	Message manipulation
	No Voice Data Encryption	😈	😈	😈	😈	😈	Wiretapping
	No Authentication	🙂	🙂	😈	😈	🙂	Caller Spoofing
	No Session Management	😈	😈	😈	🙂	😈	Denial of Service on Core Network
4G-GW	IMS Bypassing	😈	🙂	😈	🙂	🙂	Caller Spoofing
Phone	Permission Mismatch	Vulnerable for all Android					Denial of Service on Call, Overbilling

😈: Vulnerable 🙂: Secure

Solutions

- Immediate Solution

- Filtering P-GW
  - P-GW filter out packets other than the SIP message.
- Strict Session Management
  - The SIP server carefully checks the SIP message generated from the UE to prevent SIP tunneling and cellular p2p.
- UE Verification
  - Check the source of the SIP message.
- Deep Packet Inspection
  - recognize whether the user is using a media channel through the DPI.
- Accounting Policy
  - Change the time-based accounting policy.

Solutions

❖ Long term Solution

- Strict binding of sockets to data interfaces in applications is one way to prevent.

- The operator must block packets from the data interface.

Conclusion

- Newly adopted VoLTE has
  - A complex (legacy time-based) accounting
  - Delegated voice signal (previously done by CP) to AP
- We analyzed the security of VoLTE for 5 operators, and found
  - Four free data channels
  - Five security problems
- All related parties have problems
  - 3GPP, telcos, IMS providers, mobile OSes, and device vendors
- More and more reliance on cellular technology
  - Automobiles, power grid, traffic signal, …