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

Hongil Kim*, **Dongkwan Kim***, Minhee Kwon, Hyeongseok Han,
Yeongjin Jang, Taesoo Kim, Dongsu Han, Yongdae Kim

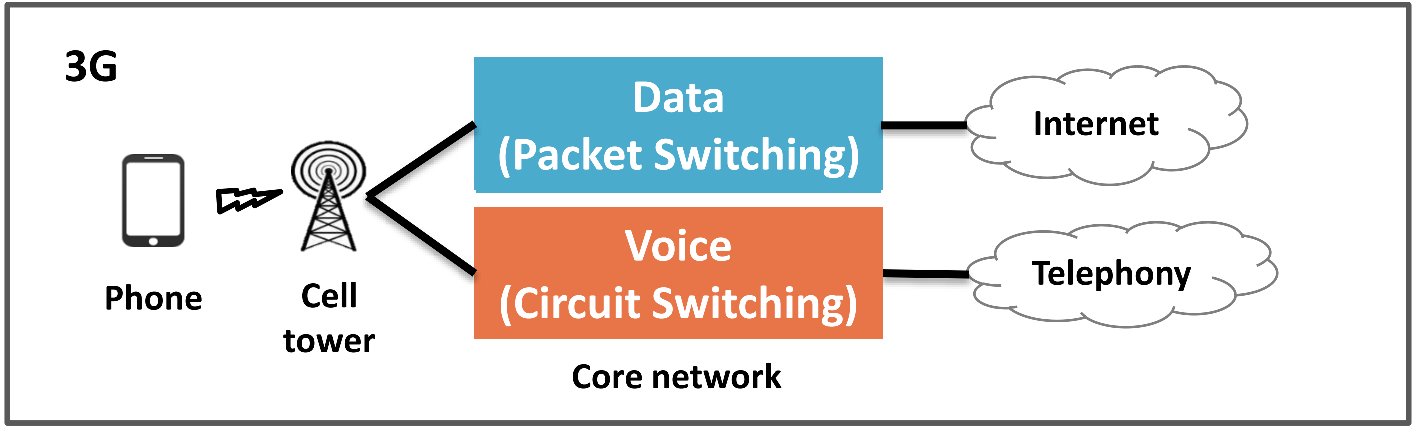
KAIST Georgia Tech

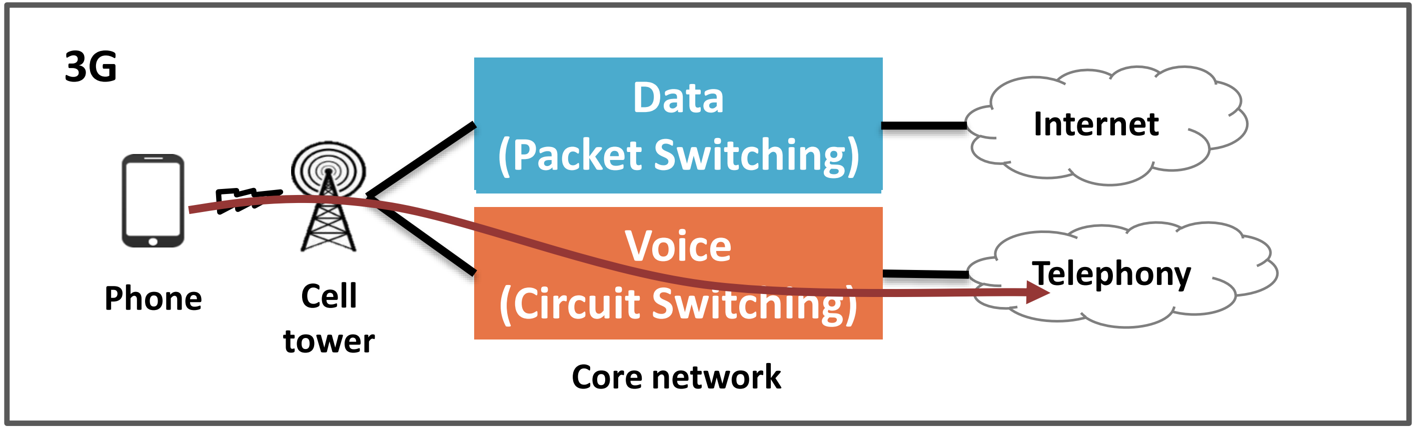
VoLTE = Voice over LTE

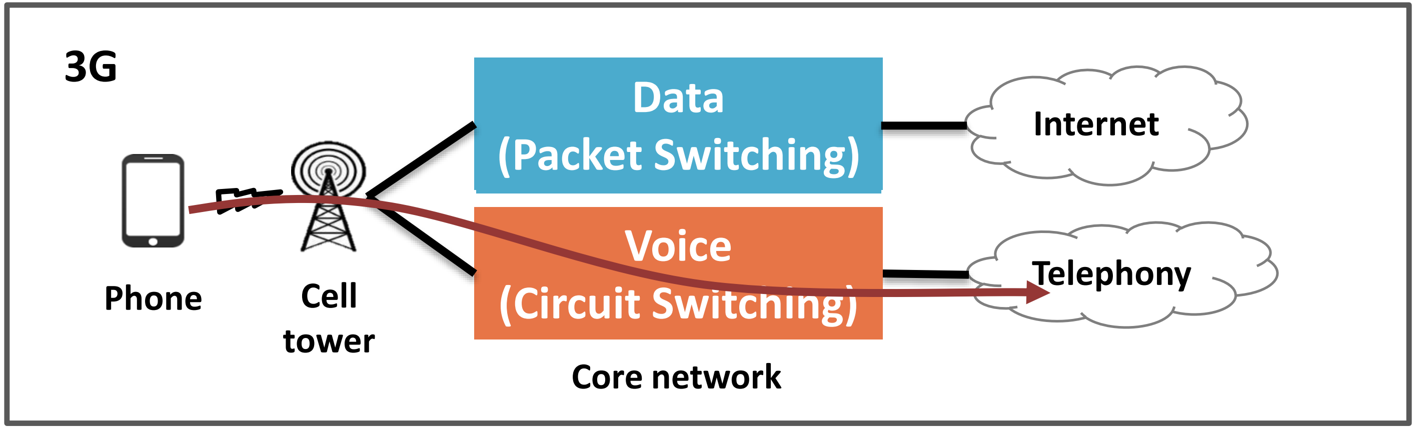
- 4G LTE: All-IP based Network
- Voice call: Implementation of VoIP on LTE

- 3G network
  - Data and voice is separated

- 4G LTE network
  - Both data and voice are delivered as data-flow


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


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



3G

Phone

Cell tower

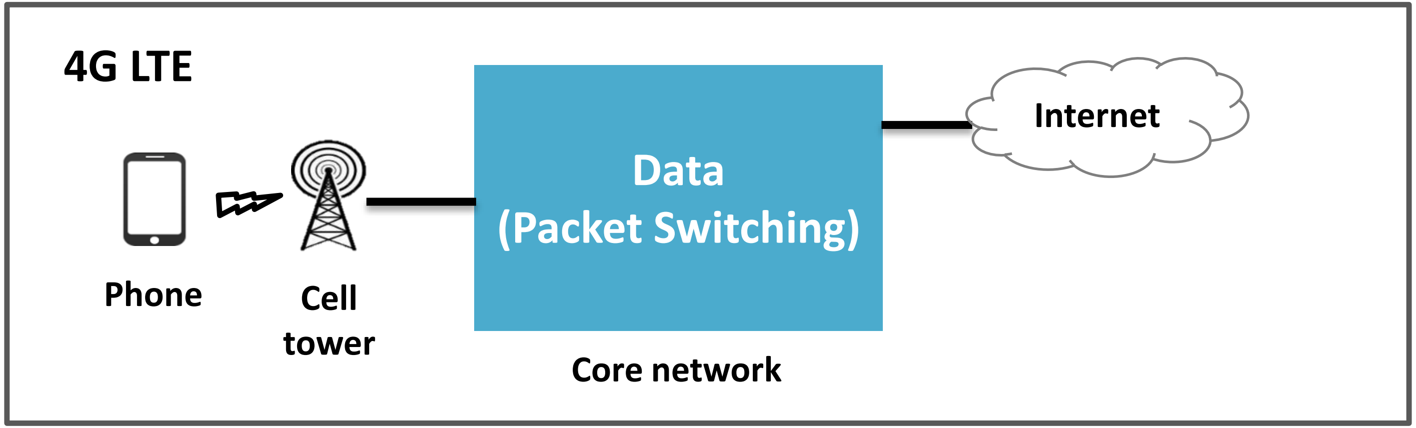
Data (Packet Switching)

Voice (Circuit Switching)

Core network

Internet

Telephony



4G LTE

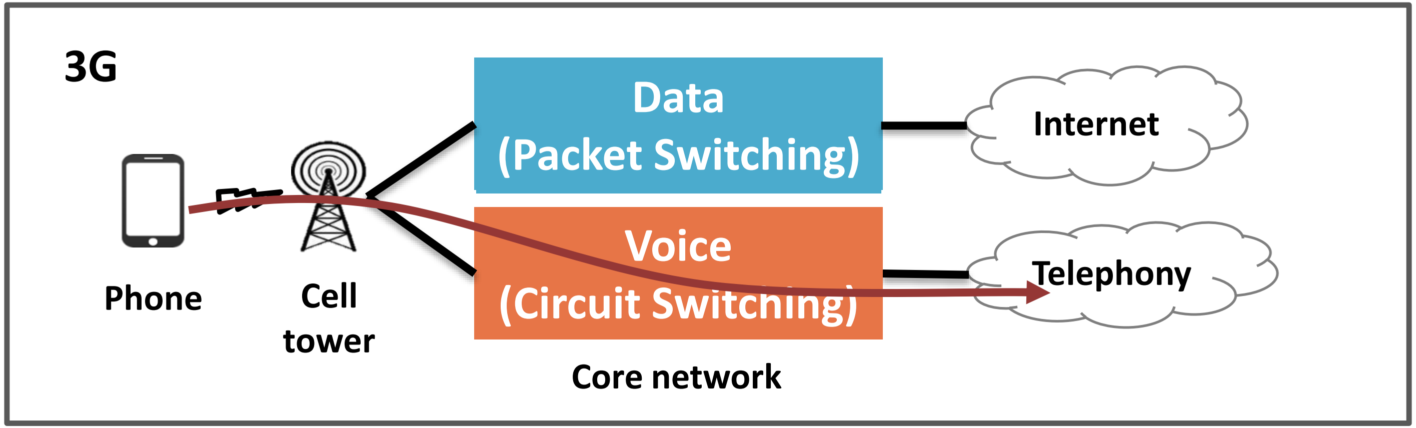
Phone

Cell tower

Data (Packet Switching)

Core network

Internet



3G

Phone

Cell tower

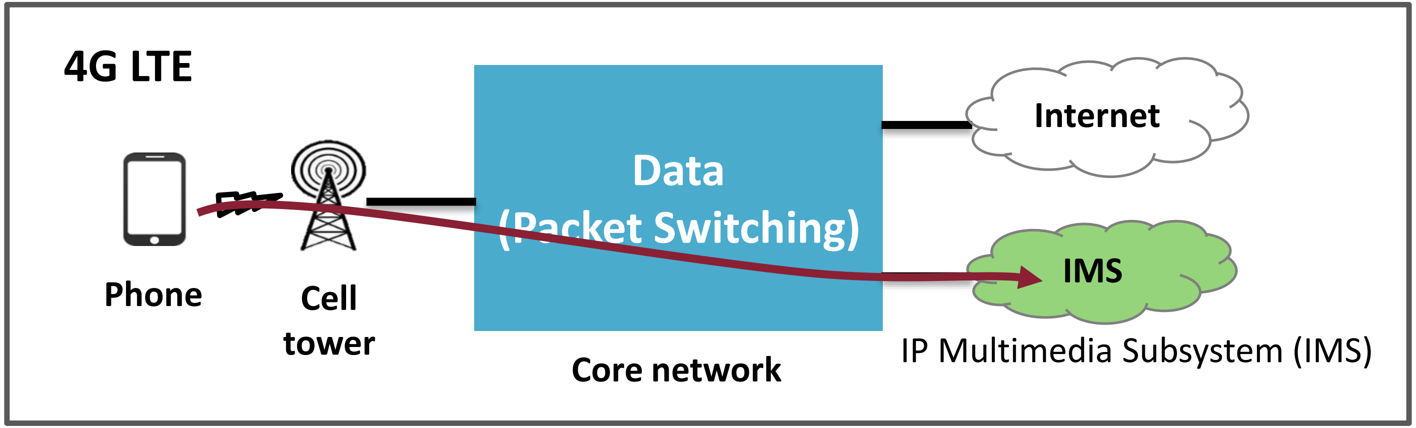
Data (Packet Switching)

Voice (Circuit Switching)

Core network

Internet

Telephony



4G LTE

Phone

Cell tower

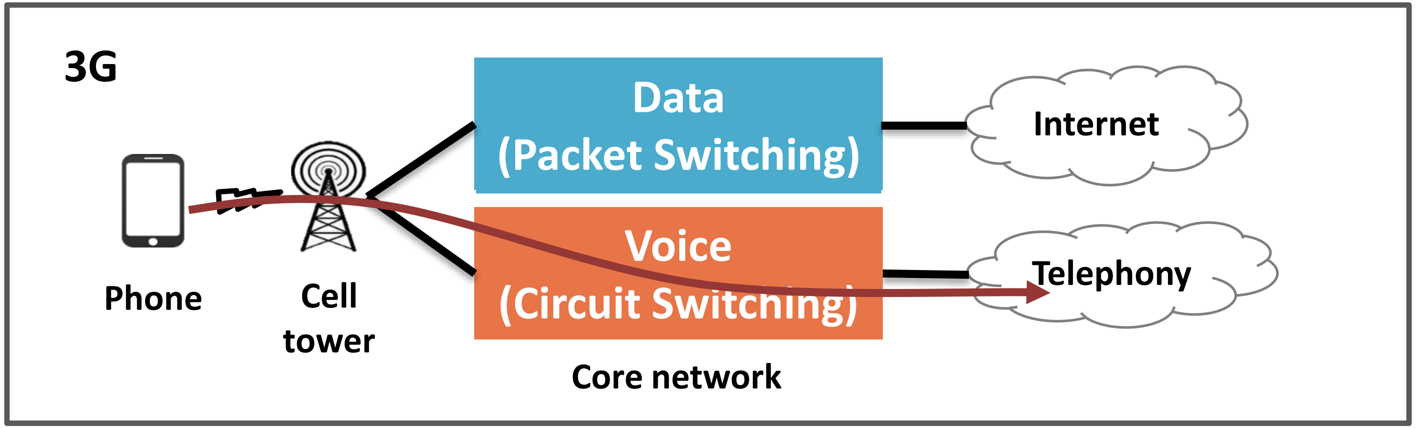
Data (Packet Switching)

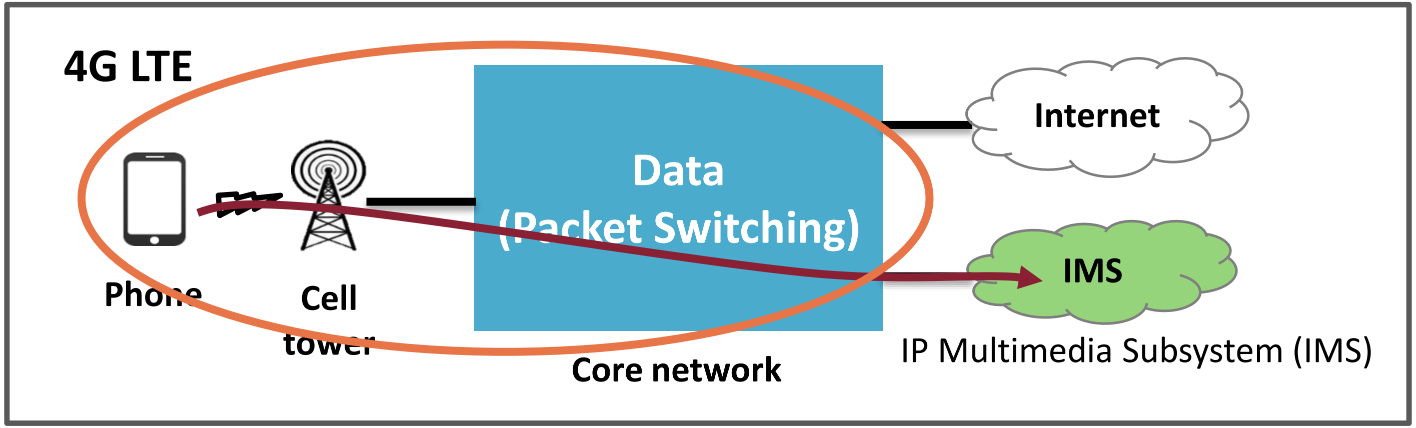
Core network

Internet

IMS

IP Multimedia Subsystem (IMS)


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)

Voice delivery in LTE

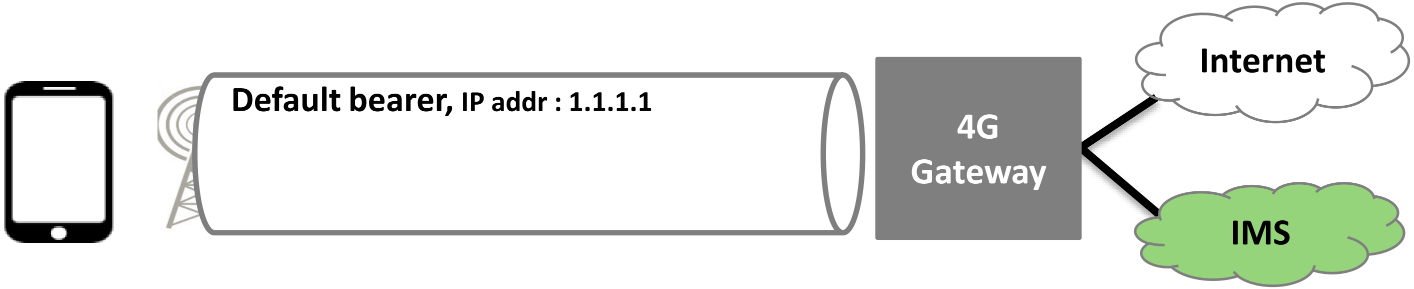
- Voice is delivered through two data channels, called “bearer”
  - Bearer: a virtual channel with below properties
  - Bandwidth, loss rate, latency (QoS)
- For VoLTE service,
  1. Control plane (default bearer): call signaling, *SIP
  2. Data plane (dedicated bearer): voice data, *RTP

4G Gateway
Internet
IMS

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

Voice delivery in LTE

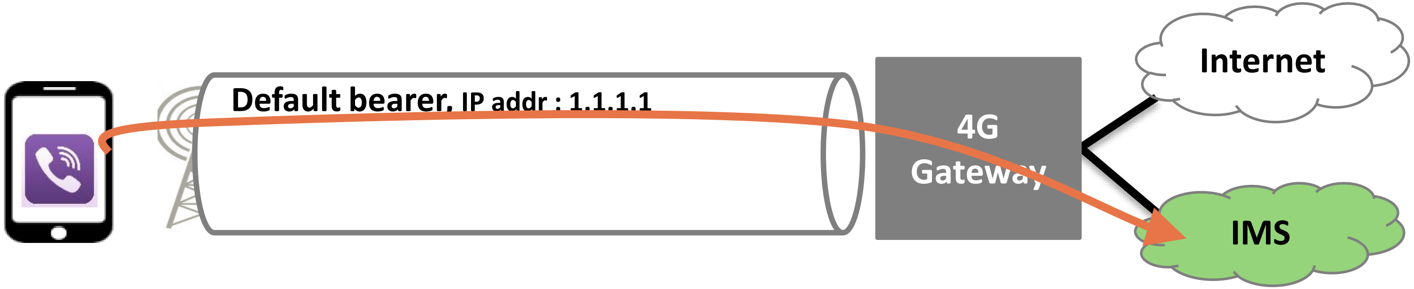
- Voice is delivered through two data channels, called “bearer”
  - Bearer: a virtual channel with below properties
  - Bandwidth, loss rate, latency (QoS)
- For VoLTE service,
  1. Control plane (default bearer): call signaling, *SIP
  2. Data plane (dedicated bearer): voice data, *RTP



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

Voice delivery in LTE

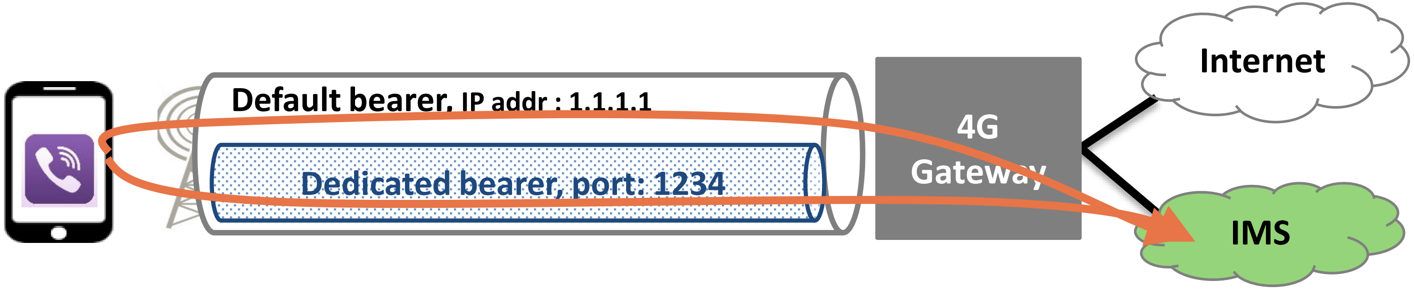
- Voice is delivered through two data channels, called “bearer”
  - Bearer: a virtual channel with below properties
  - Bandwidth, loss rate, latency (QoS)
- For VoLTE service,
  1. Control plane (default bearer): call signaling, *SIP
  2. Data plane (dedicated bearer): voice data, *RTP



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

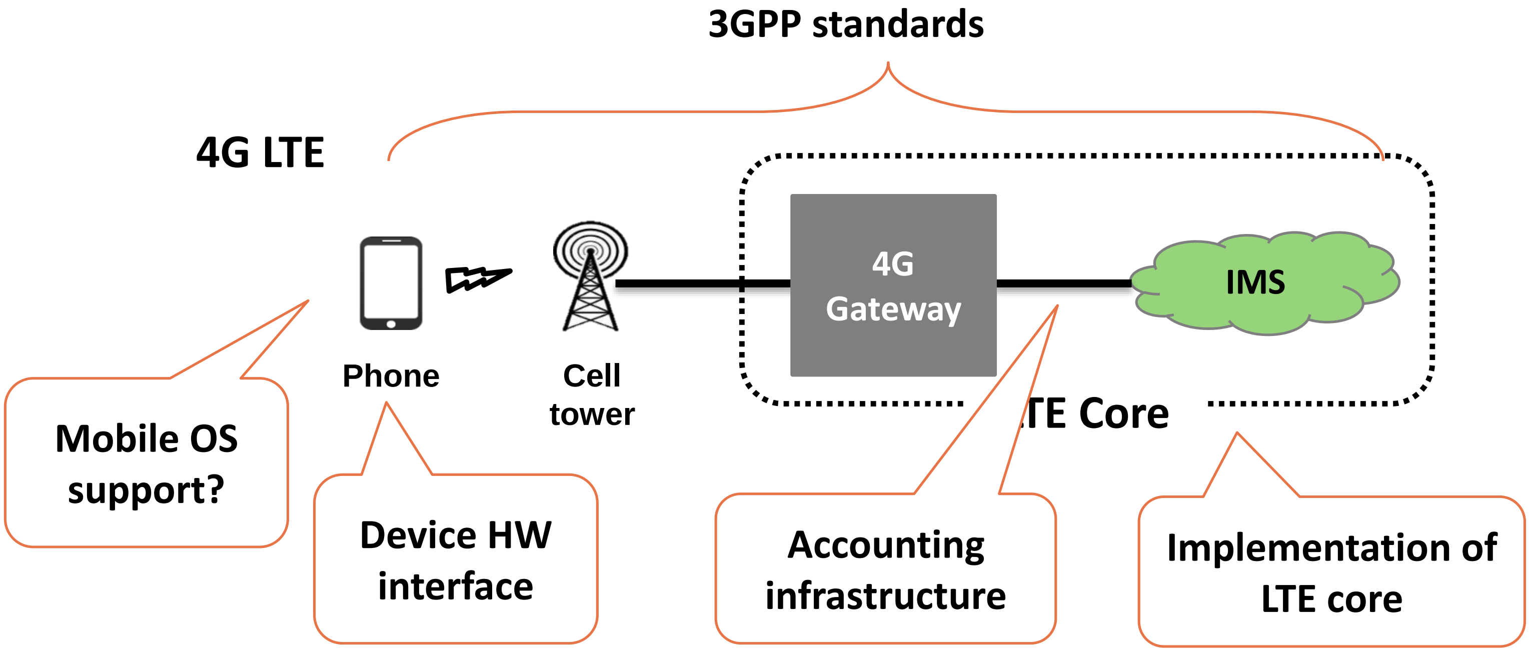
Voice delivery in LTE

- Voice is delivered through two data channels, called “bearer”
  - Bearer: a virtual channel with below properties
  - Bandwidth, loss rate, latency (QoS)
- For VoLTE service,
  1. Control plane (default bearer): call signaling, *SIP
  2. Data plane (dedicated bearer): voice data, *RTP


Default bearer, IP addr : 1.1.1.1
Dedicated bearer, port: 1234
4G Gateway
Internet
IMS

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

VoLTE makes cellular network more complex



3GPP standards

4G LTE

Phone

Cell tower

4G Gateway

IMS

LTE Core

Mobile OS support?

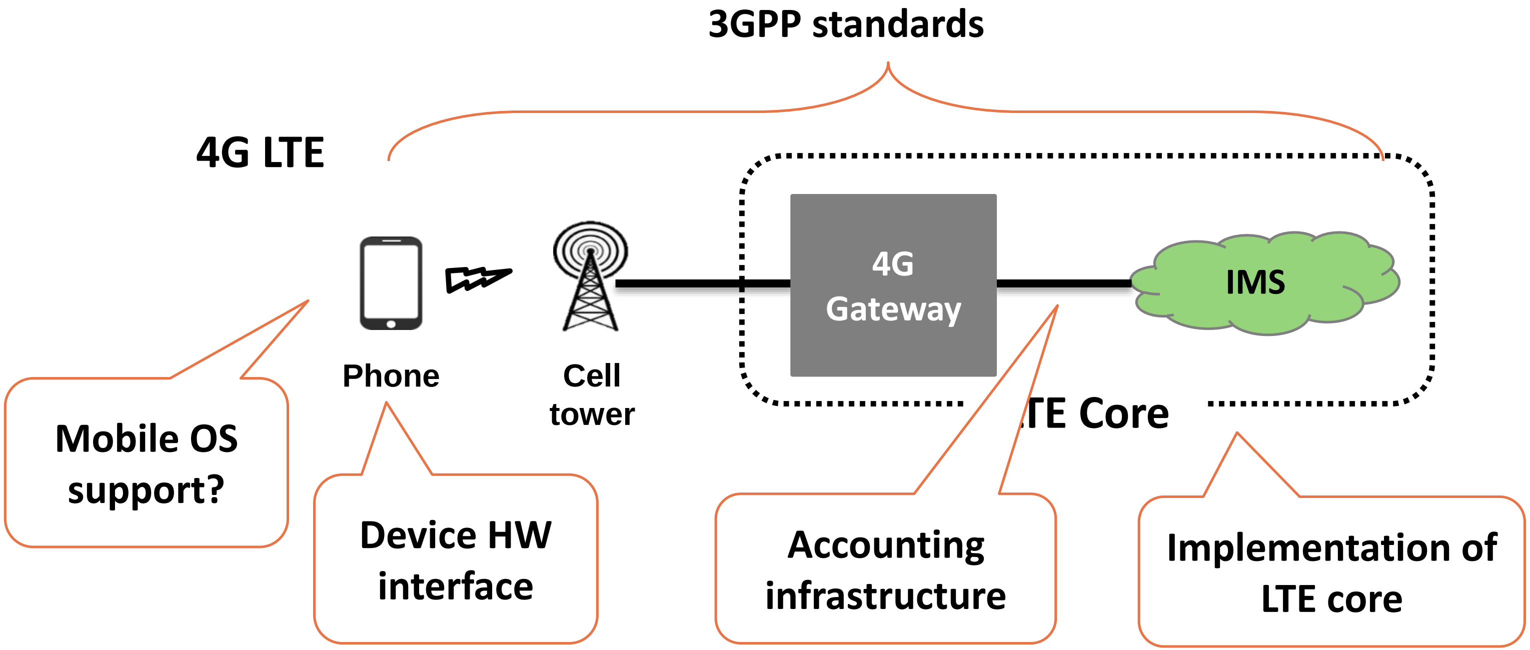
Device HW interface

Accounting infrastructure

Implementation of LTE core

VoLTE makes cellular network more complex

- Let’s check potential attack vectors newly introduced in VoLTE



3GPP standards

4G LTE

Phone

Cell tower

4G Gateway

IMS

TE Core

Mobile OS support?

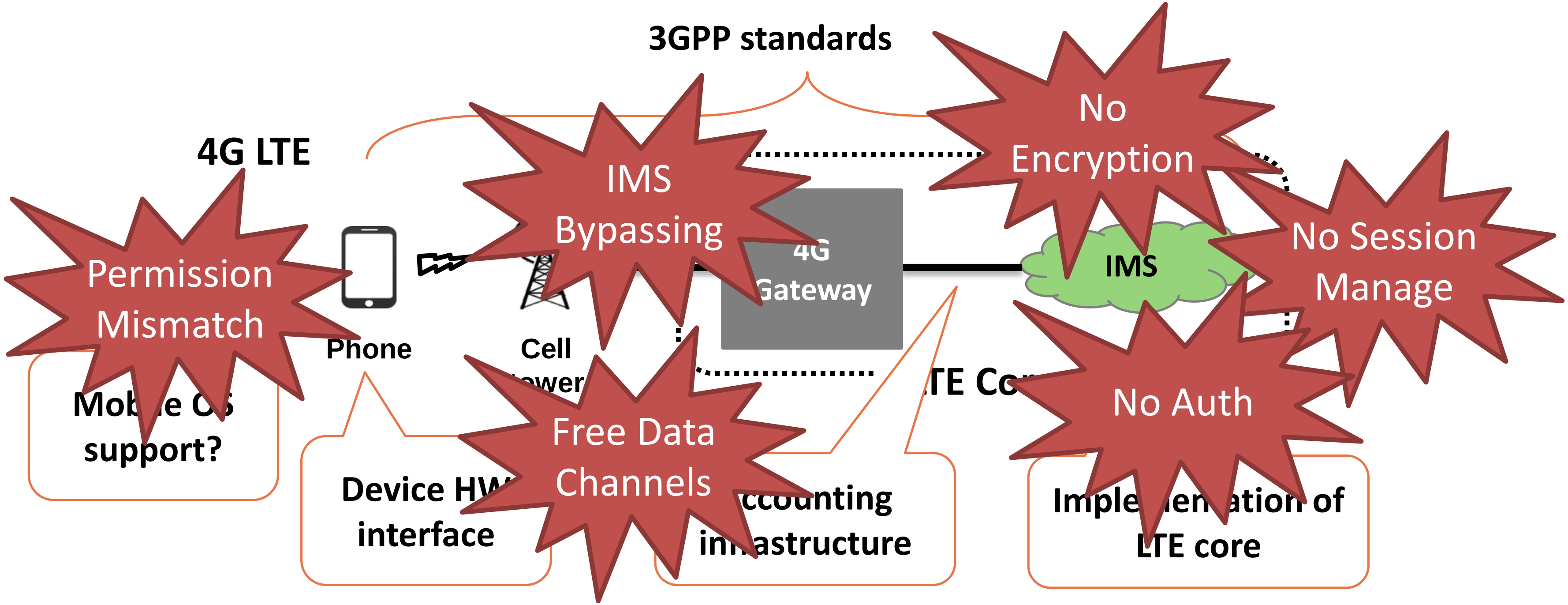
Device HW interface

Accounting infrastructure

Implementation of LTE core

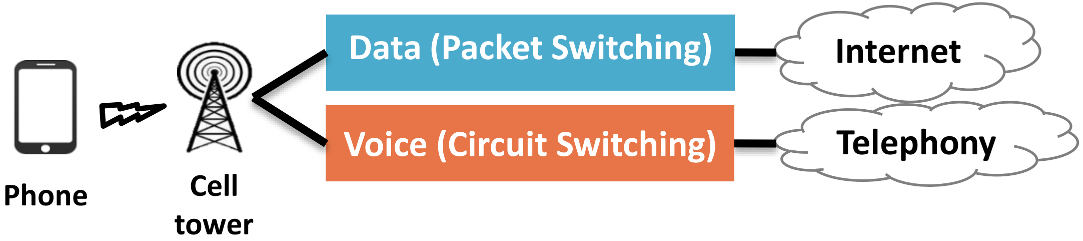
VoLTE makes cellular network more complex

- Let's check potential attack vectors newly introduced in VoLTE



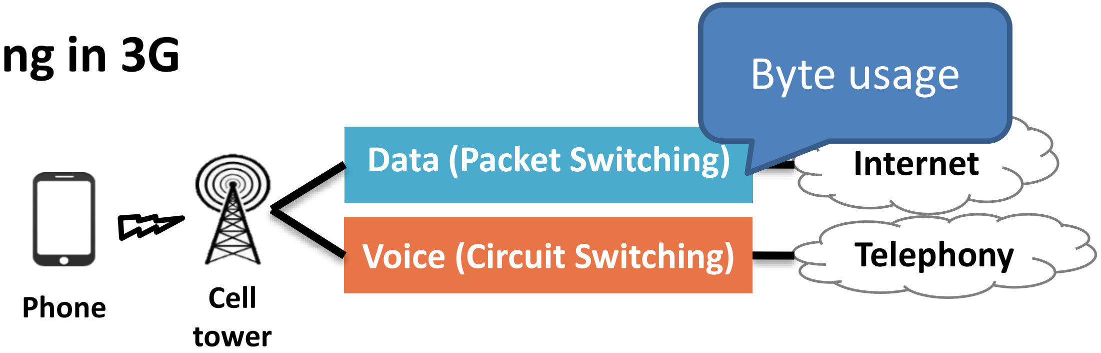
#1: VoLTE Accounting

- Accounting in 3G



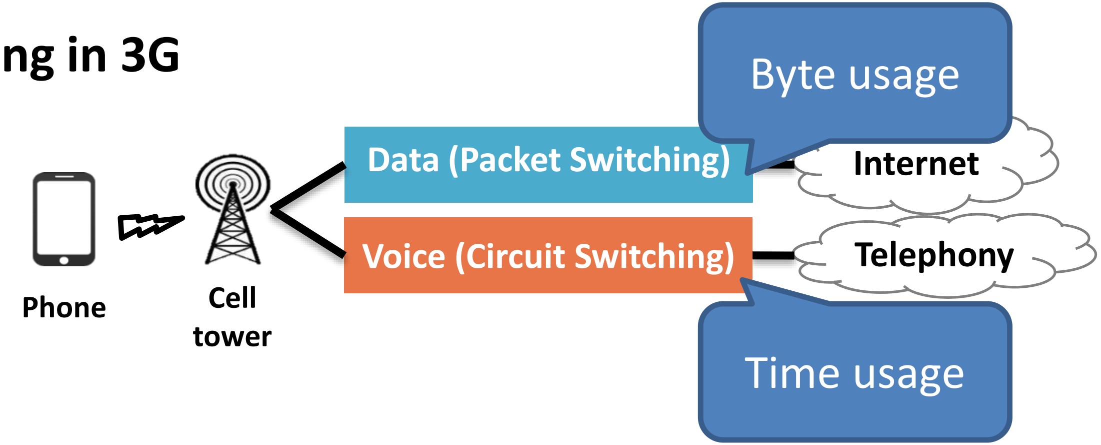
#1: VoLTE Accounting

- Accounting in 3G



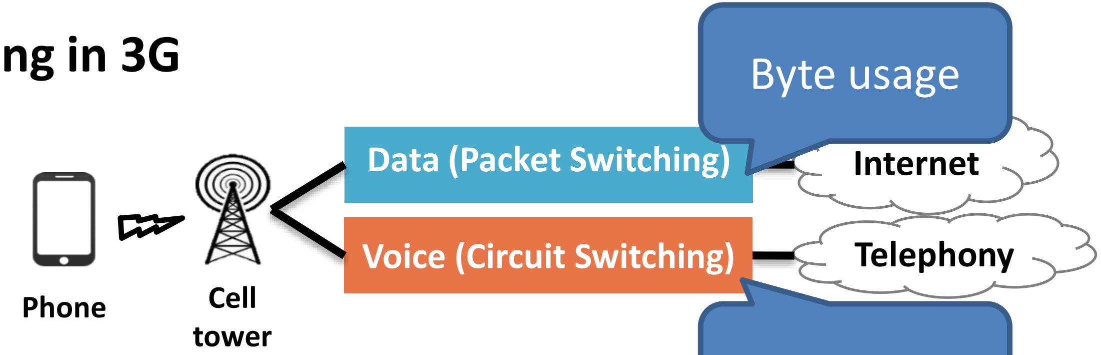
#1: VoLTE Accounting

- Accounting in 3G

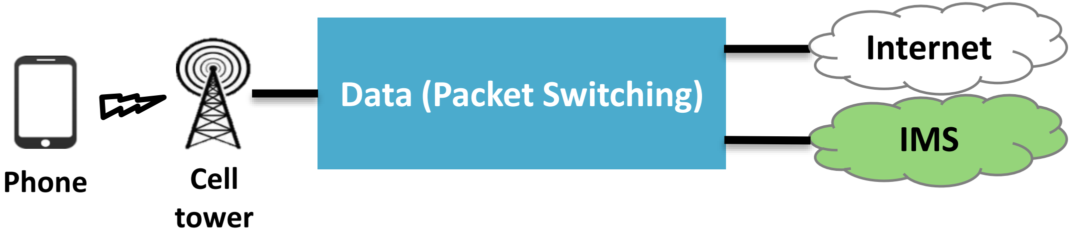


#1: VoLTE Accounting

- Accounting in 3G

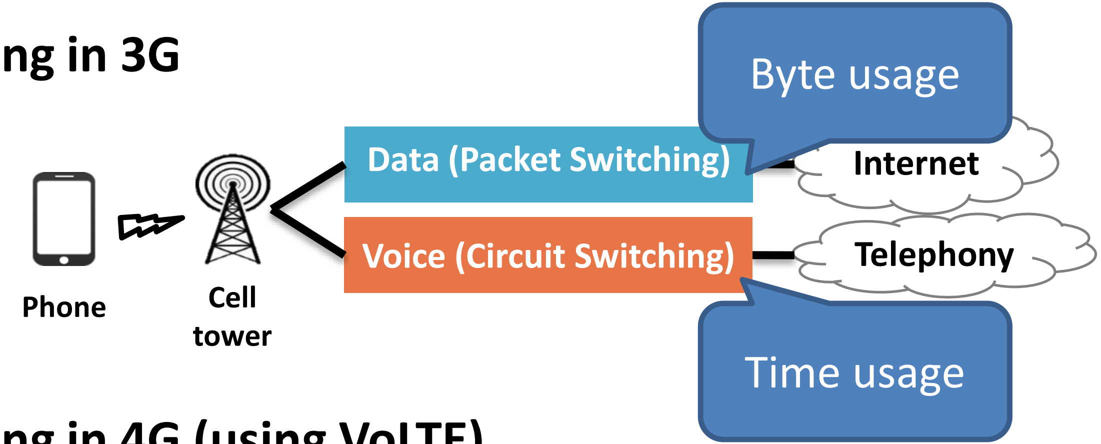


- Accounting in 4G (using VoLTE)



#1: VoLTE Accounting

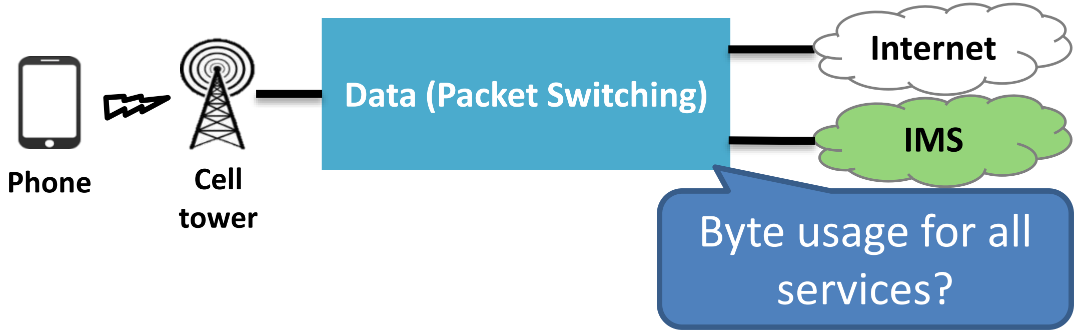
- Accounting in 3G



Byte usage

Time usage

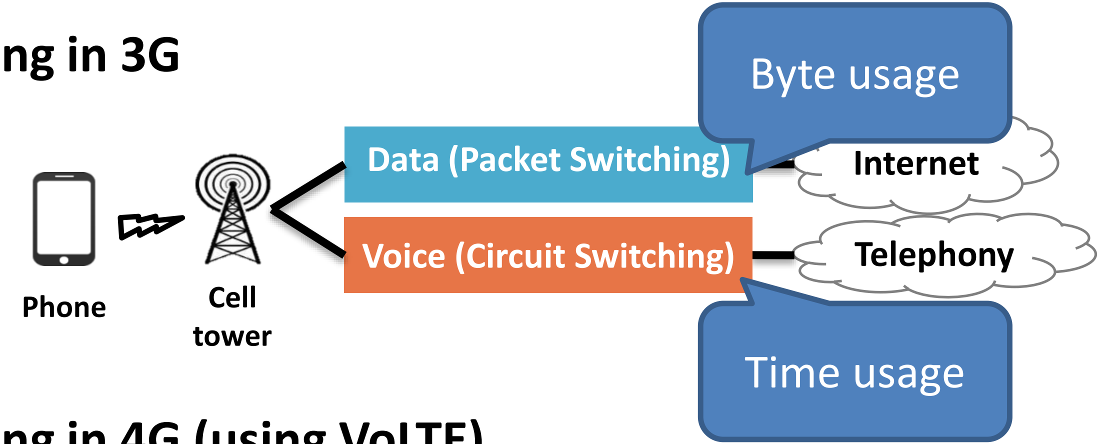
- Accounting in 4G (using VoLTE)



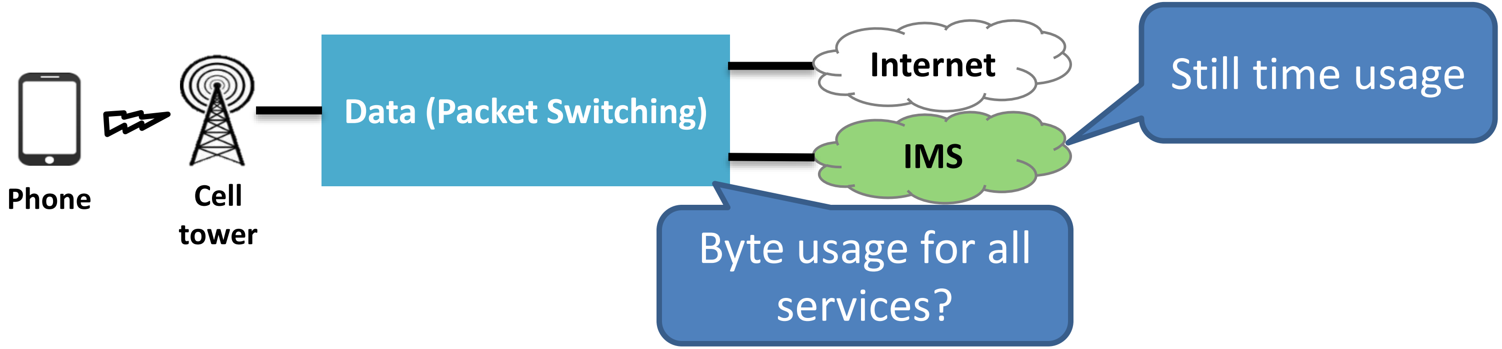
Byte usage for all services?

#1: VoLTE Accounting

- Accounting in 3G

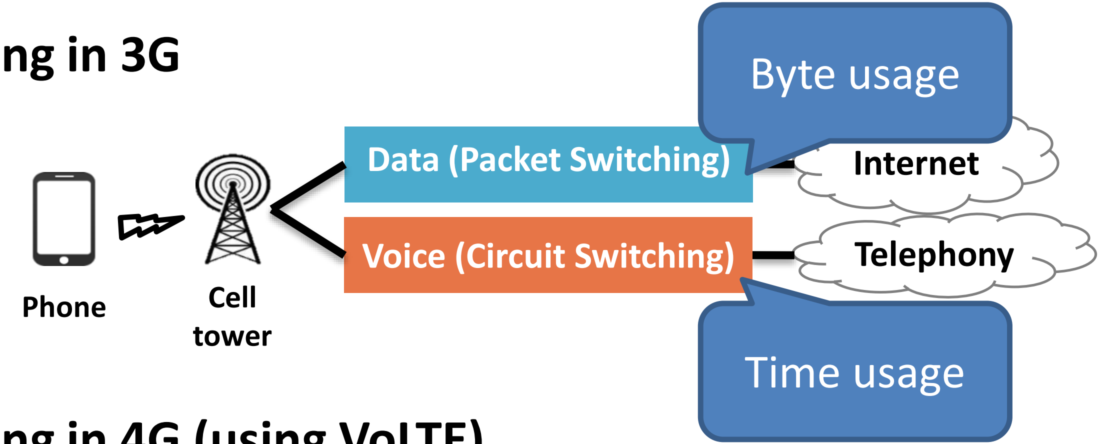


- Accounting in 4G (using VoLTE)

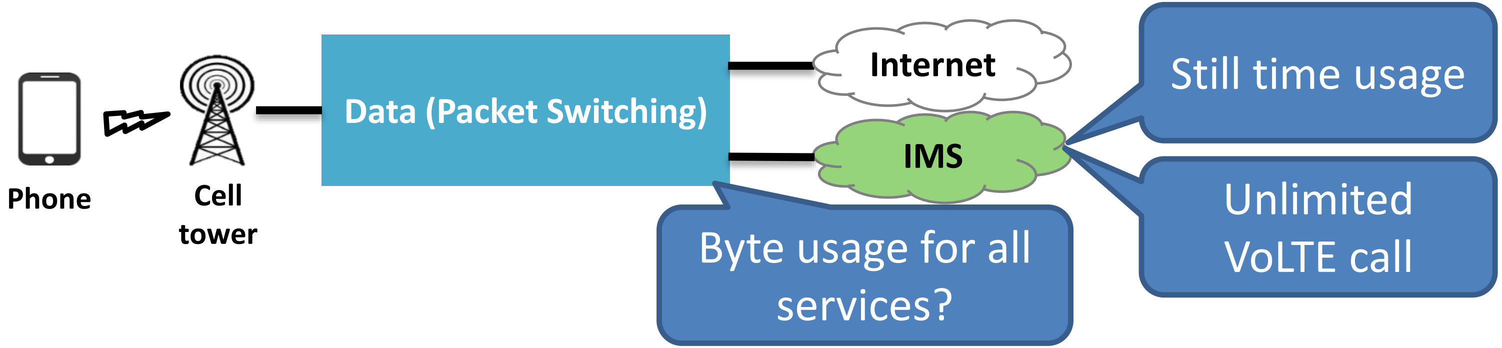


#1: VoLTE Accounting

- Accounting in 3G



- Accounting in 4G (using VoLTE)



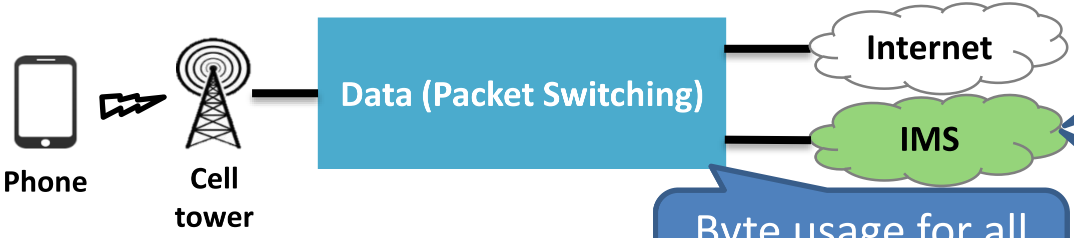
#1: VoLTE Accounting

- ❖ Accounting in 3G

Byte usage

Do operators implement this complicated accounting correctly?

- ❖ Accounting in 4G (using VoLTE)



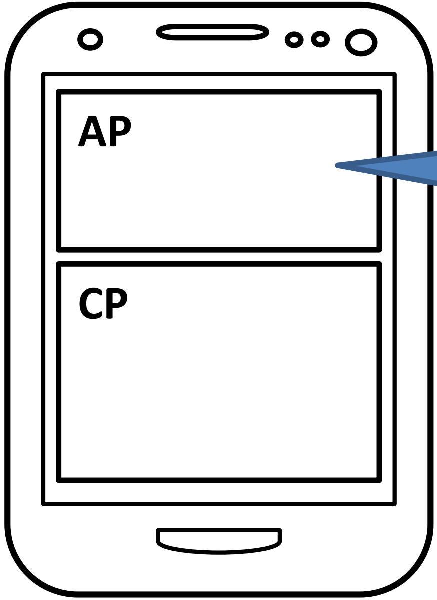
Still time usage

Unlimited VoLTE call

Byte usage for all services?

Anatomy of smartphone

- Smartphone has two processors

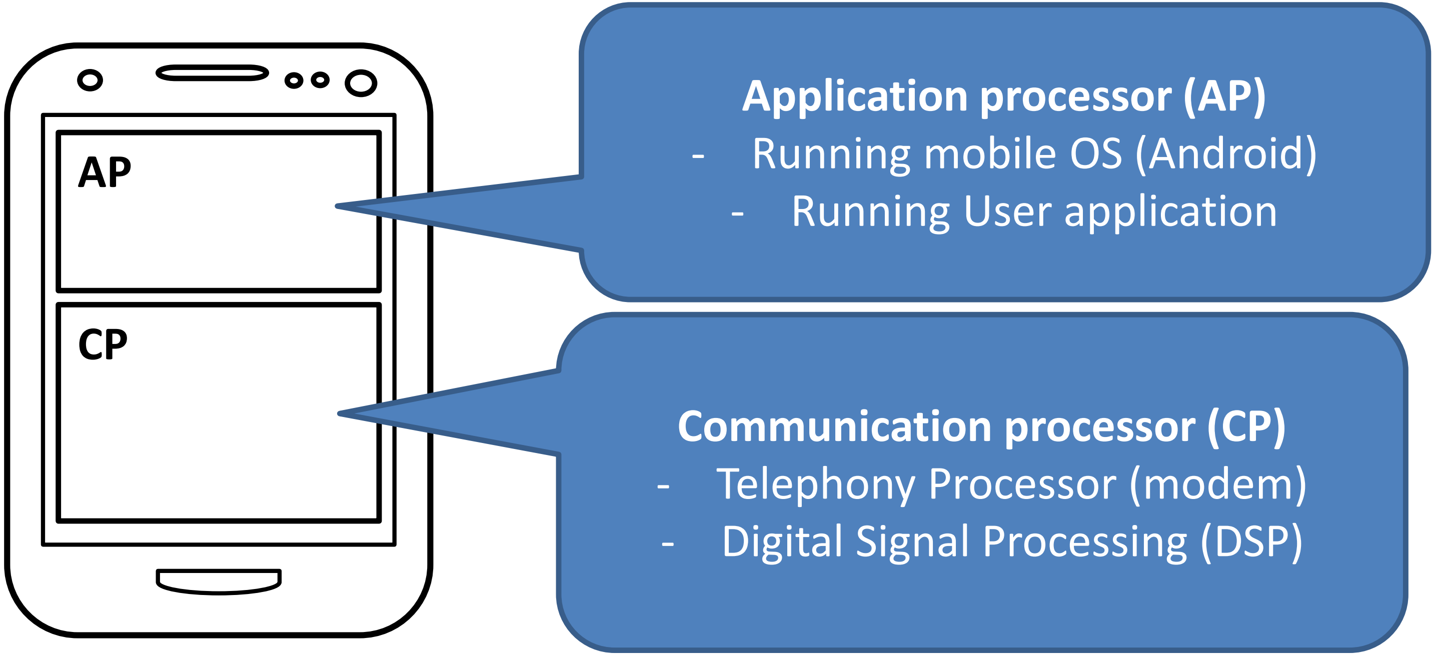


Application processor (AP)

- Running mobile OS (Android)
- Running User application

Anatomy of smartphone

- Smartphone has two processors



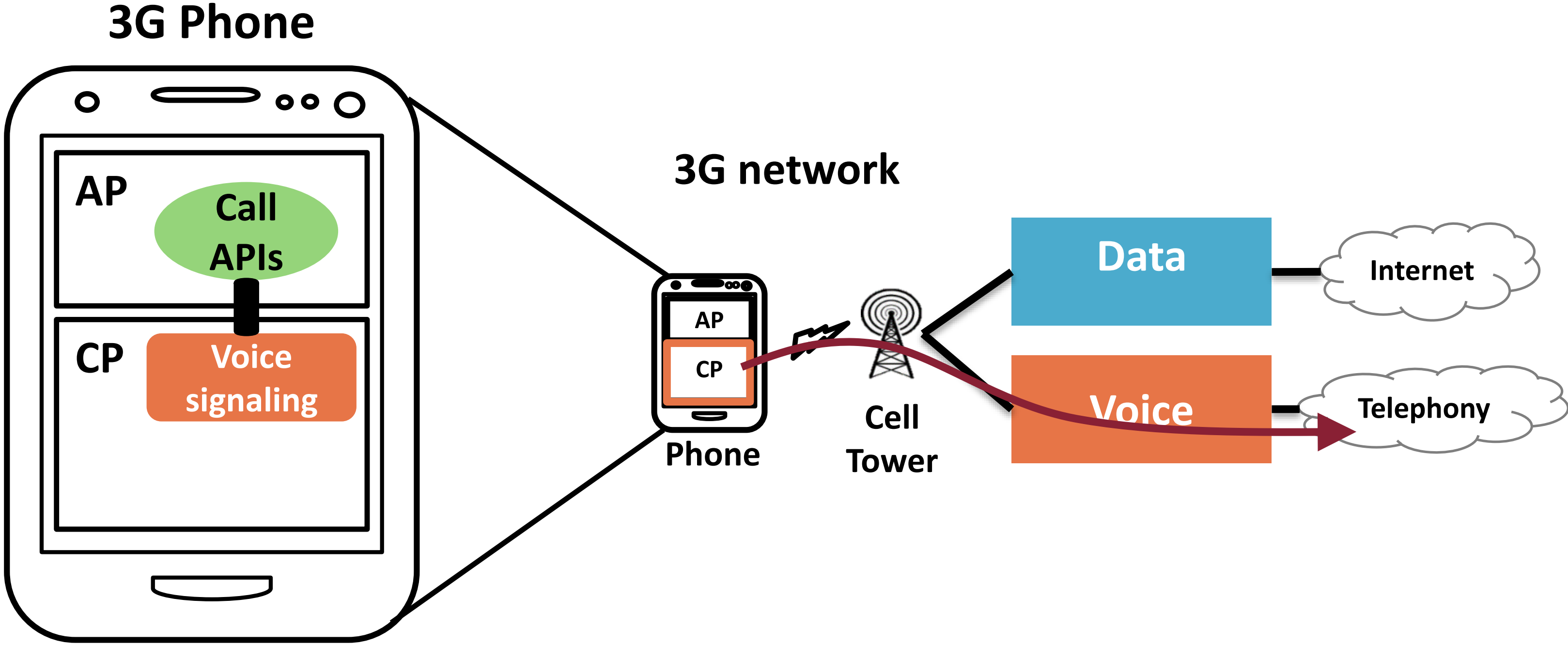
Application processor (AP)

- Running mobile OS (Android)
- Running User application

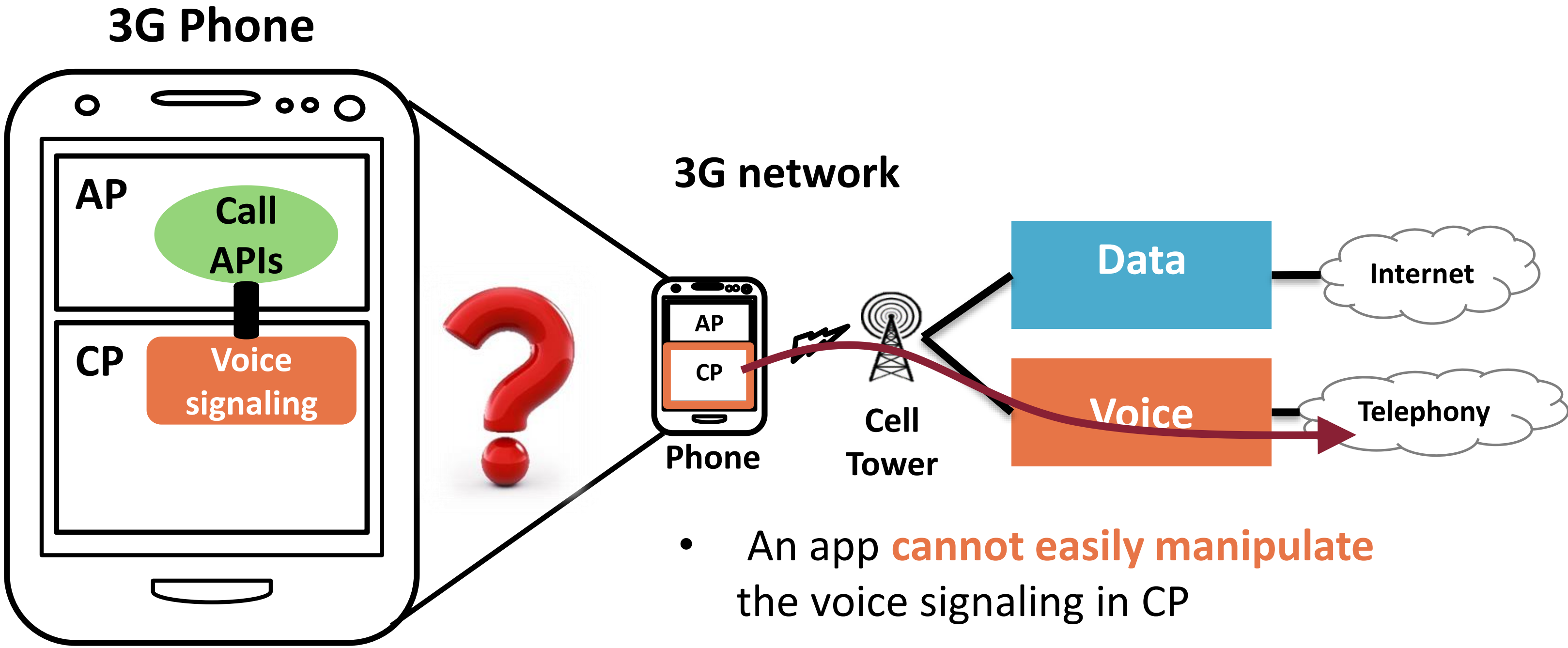
Communication processor (CP)

- Telephony Processor (modem)
- Digital Signal Processing (DSP)

#2 Voice solution in device, 3G case

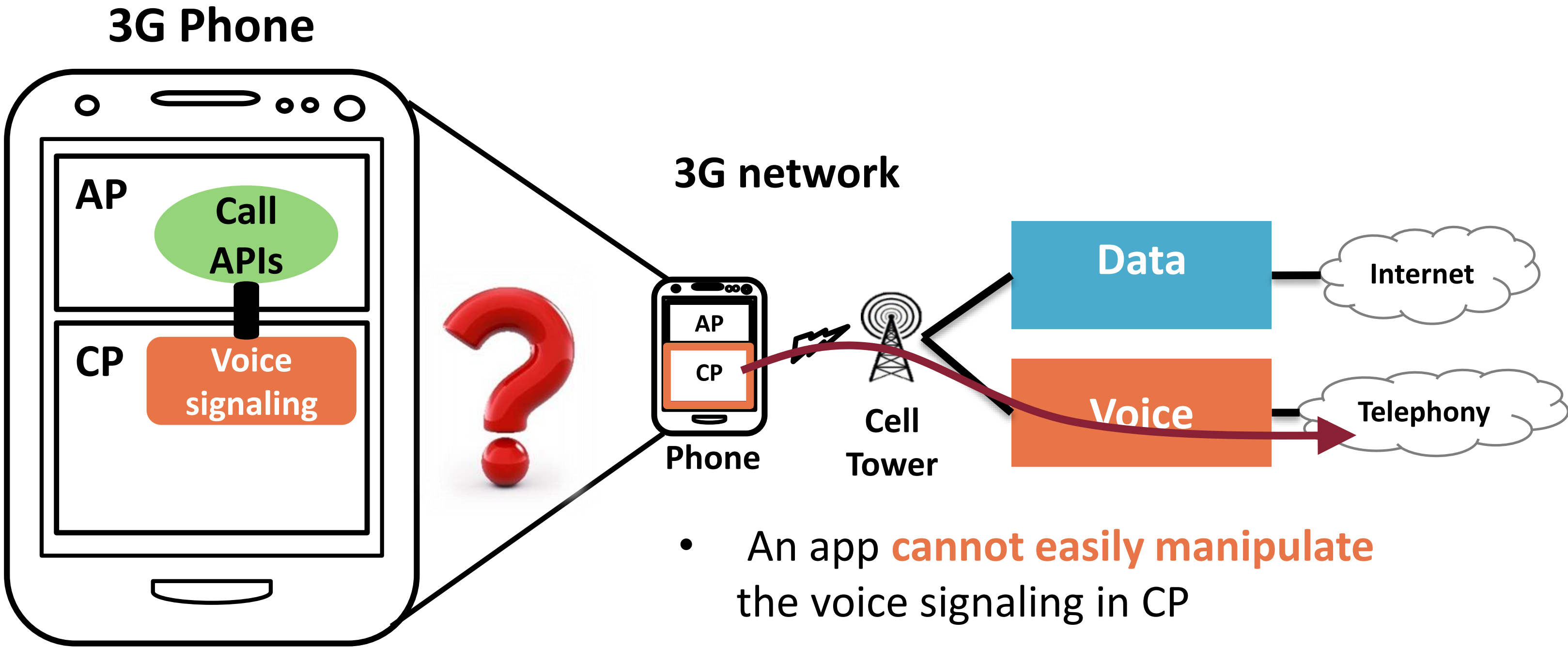


#2 Voice solution in device, 3G case



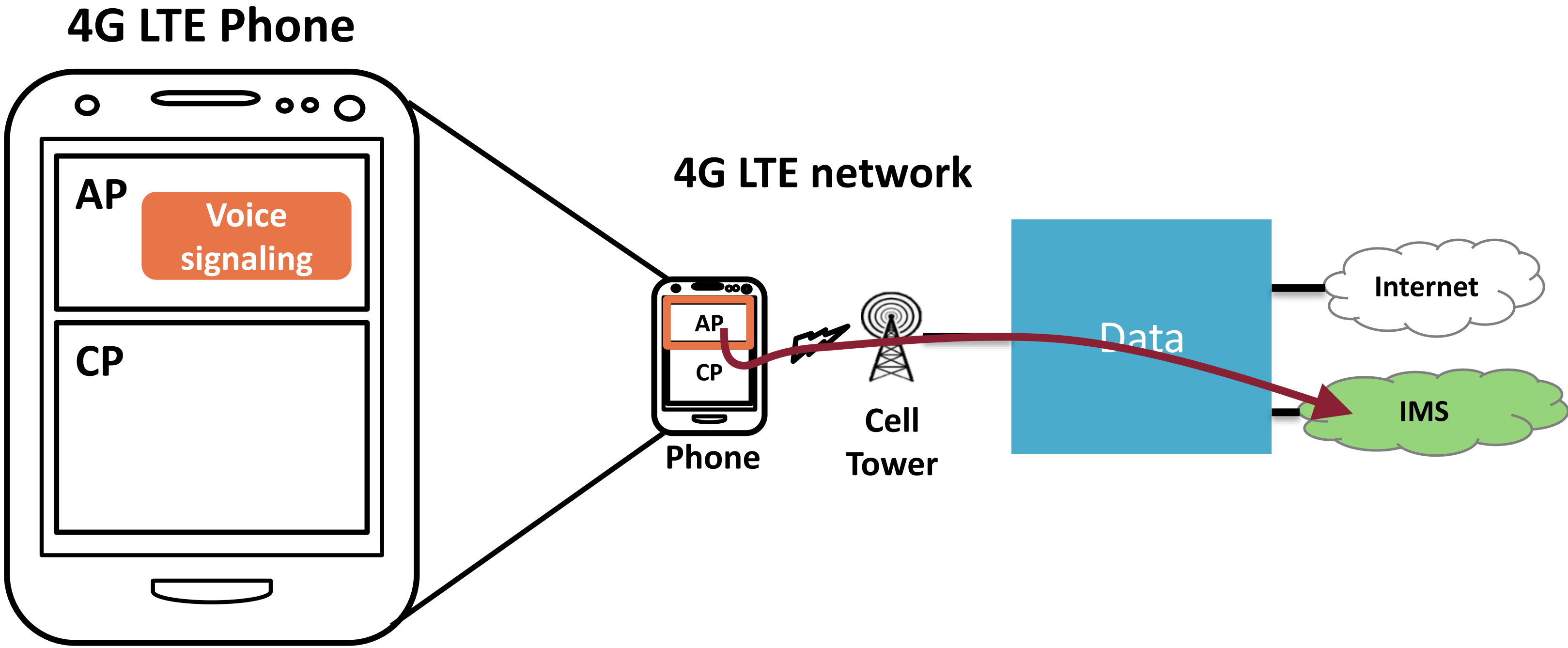
- An app **cannot easily manipulate** the voice signaling in CP

#2 Voice solution in device, 3G case

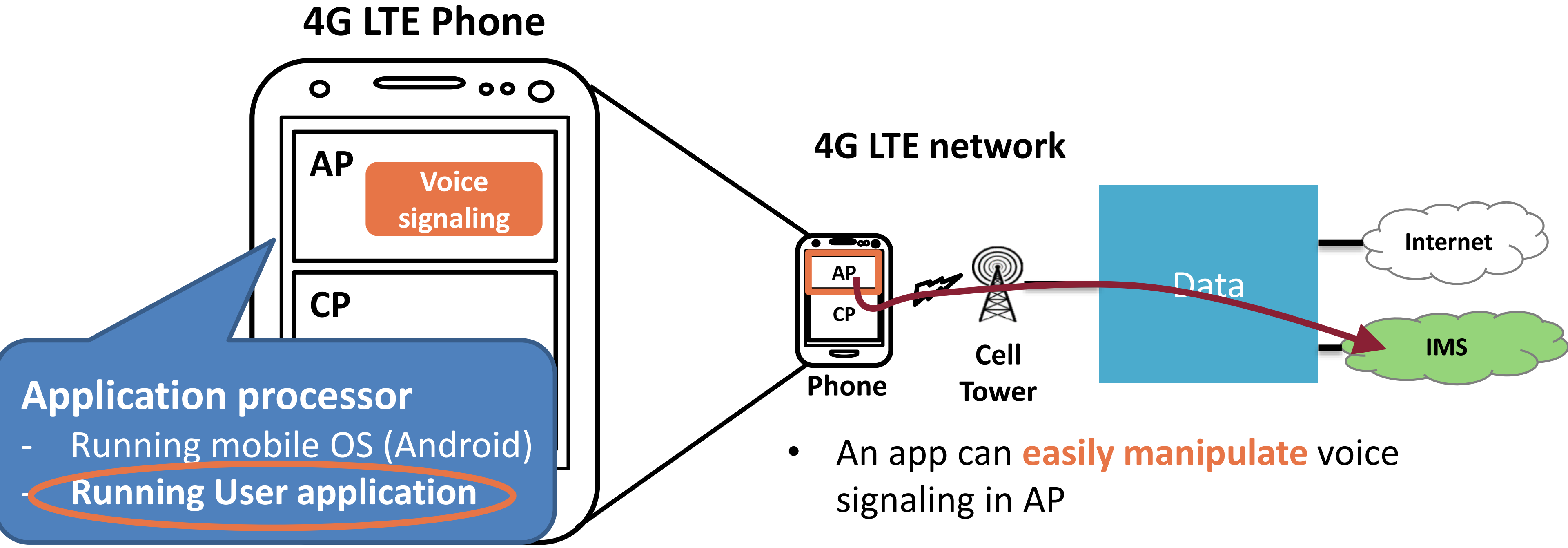


- An app **cannot easily manipulate** the voice signaling in CP
- An app needs **“CALL_PHONE” permission** for calling

#2: Voice solution in device, LTE



#2: Voice solution in device, LTE

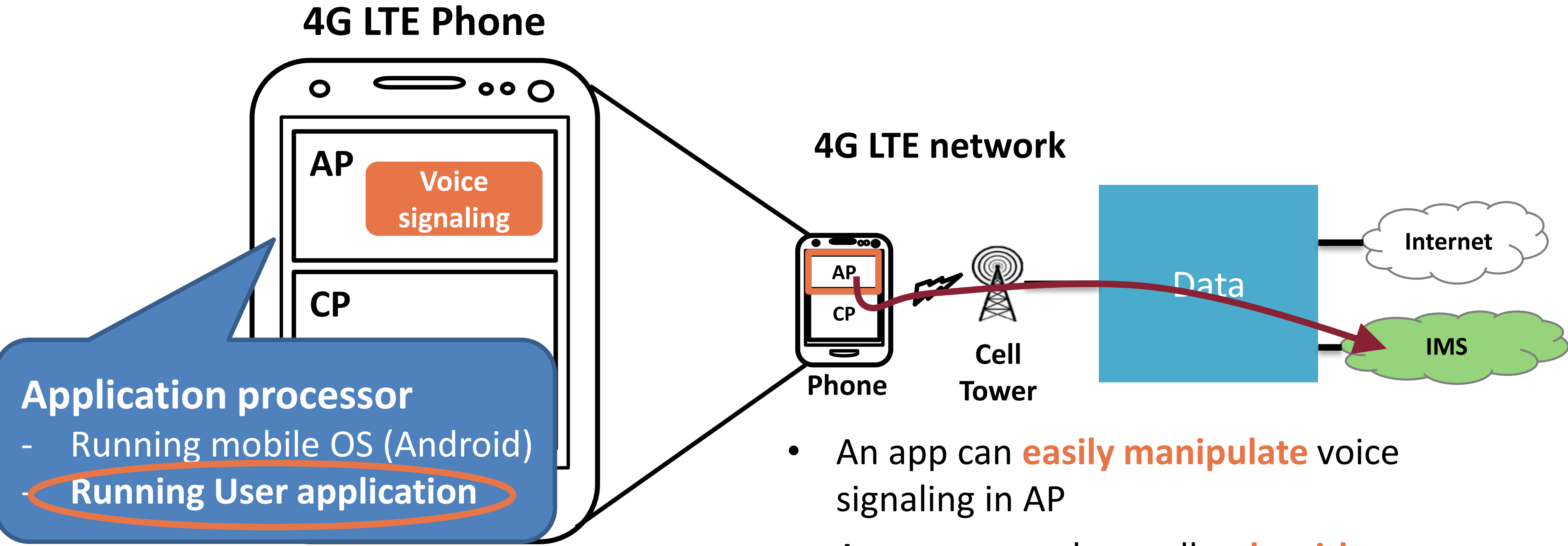


Application processor

- Running mobile OS (Android)
- **Running User application**

- An app can **easily manipulate** voice signaling in AP

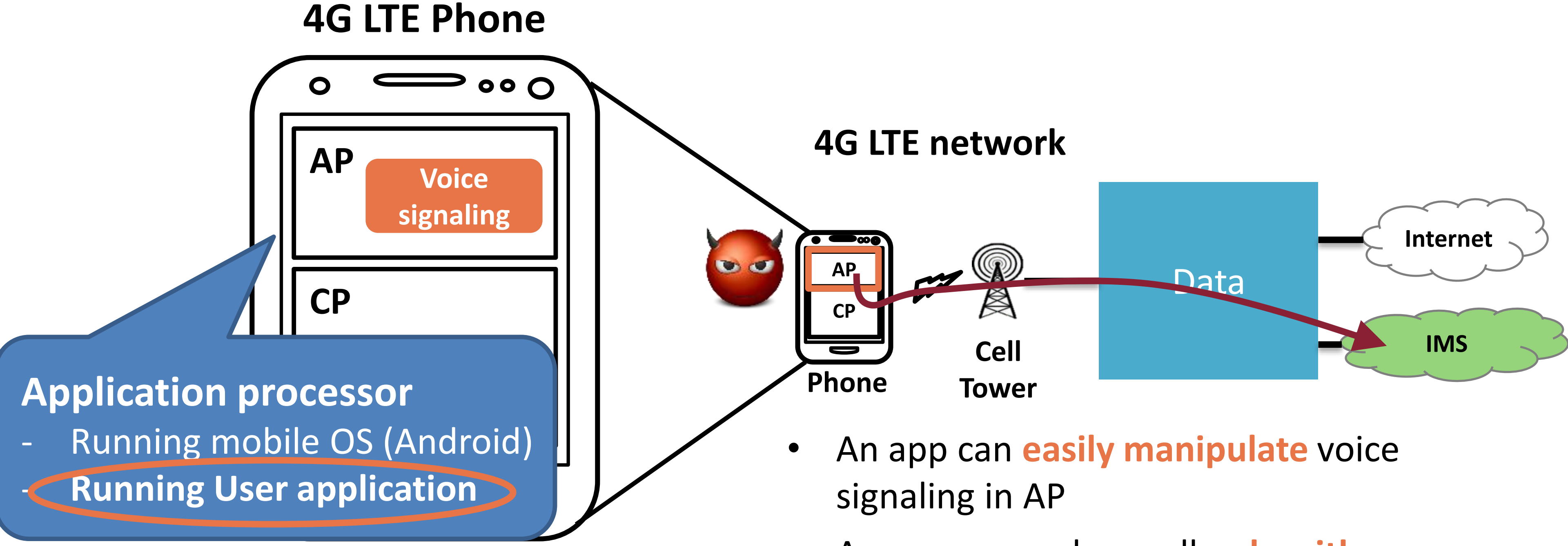
#2: Voice solution in device, LTE



Application processor
- Running mobile OS (Android)
- **Running User application**

- An app can **easily manipulate** voice signaling in AP
- An app can make a call **only with "INTERNET" permission**.

#2: Voice solution in device, LTE



Application processor

- Running mobile OS (Android)
- **Running User application**

- An app can **easily manipulate** voice signaling in AP
- An app can make a call **only with "INTERNET" permission**.

Two problems in VoLTE

1. A complex accounting infrastructure

2. Delegating voice signaling (previously done by CP) to AP

Our approach to attack two problems

Our approach to attack two problems

- Analyze 3GPP standards related with VoLTE service
  - Leave detail implementation to operators, chipset vendors, …

Our approach to attack two problems

- ❖ Analyze 3GPP standards related with VoLTE service
  - – Leave detail implementation to operators, chipset vendors, …
- ❖ Make a checklist of potential vulnerable points in the VoLTE feature
  - – About 60 items for both control and data plane

Our approach to attack two problems

- ❖ Analyze 3GPP standards related with VoLTE service
  - – Leave detail implementation to operators, chipset vendors, …
- ❖ Make a checklist of potential vulnerable points in the VoLTE feature
  - – About 60 items for both control and data plane
- ❖ Perform an analysis in 5 major operational networks
  - – 2 U.S. operators and 3 South Korea operators

Quick Summary of Our Finding

Quick Summary of Our Finding

- **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

Quick Summary of Our Finding

- **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

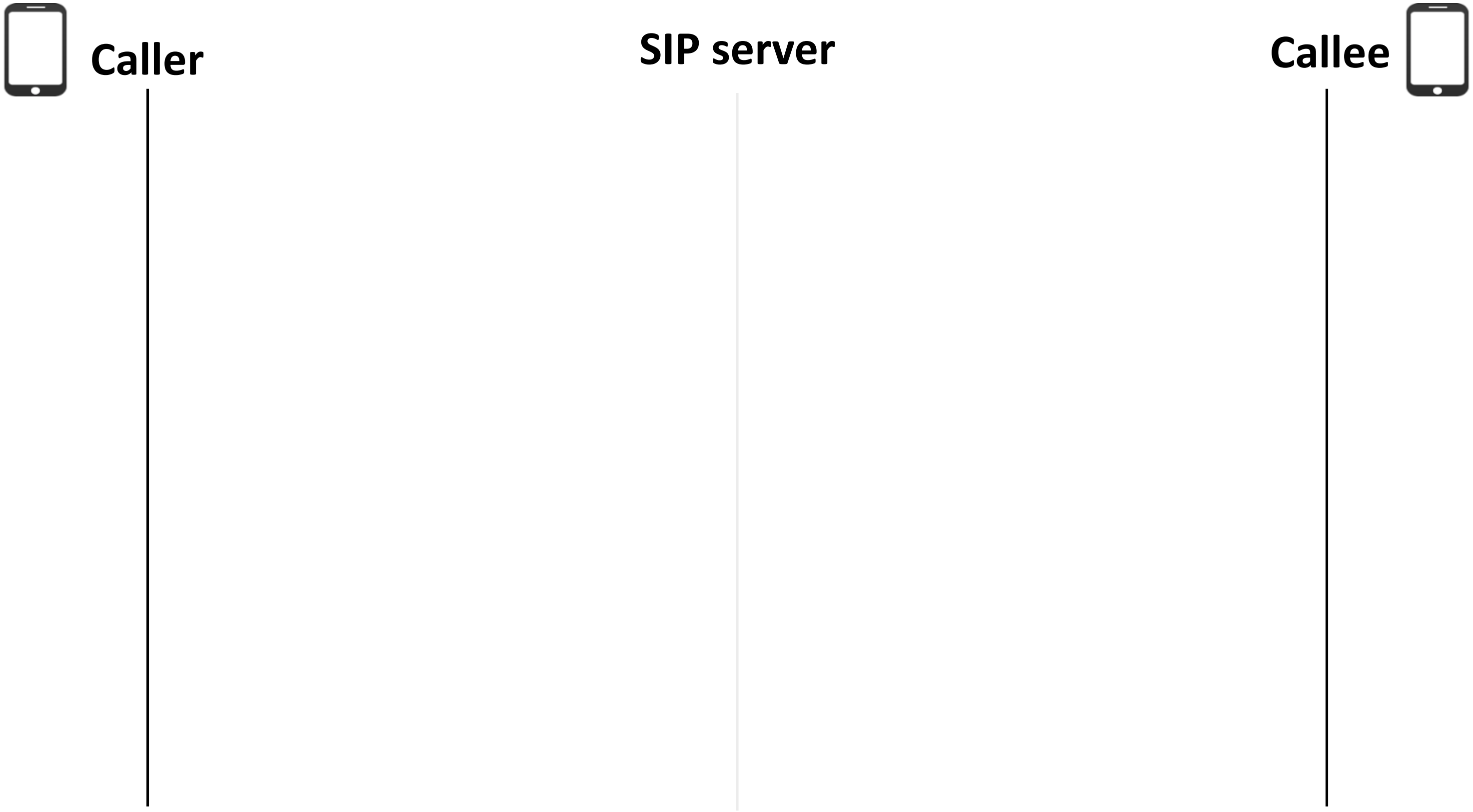
- **Five security issues**
  - **No encryption** of voice packets
  - **No authentication** of signaling
  - **No call session management** (DoS on the cellular infrastructure)
  - **IMS bypassing**
  - **Permission model mismatch** (VoLTE call without “CALL_PHONE” permission)

Quick Summary of Our Finding

- **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)

VoLTE Call Procedure



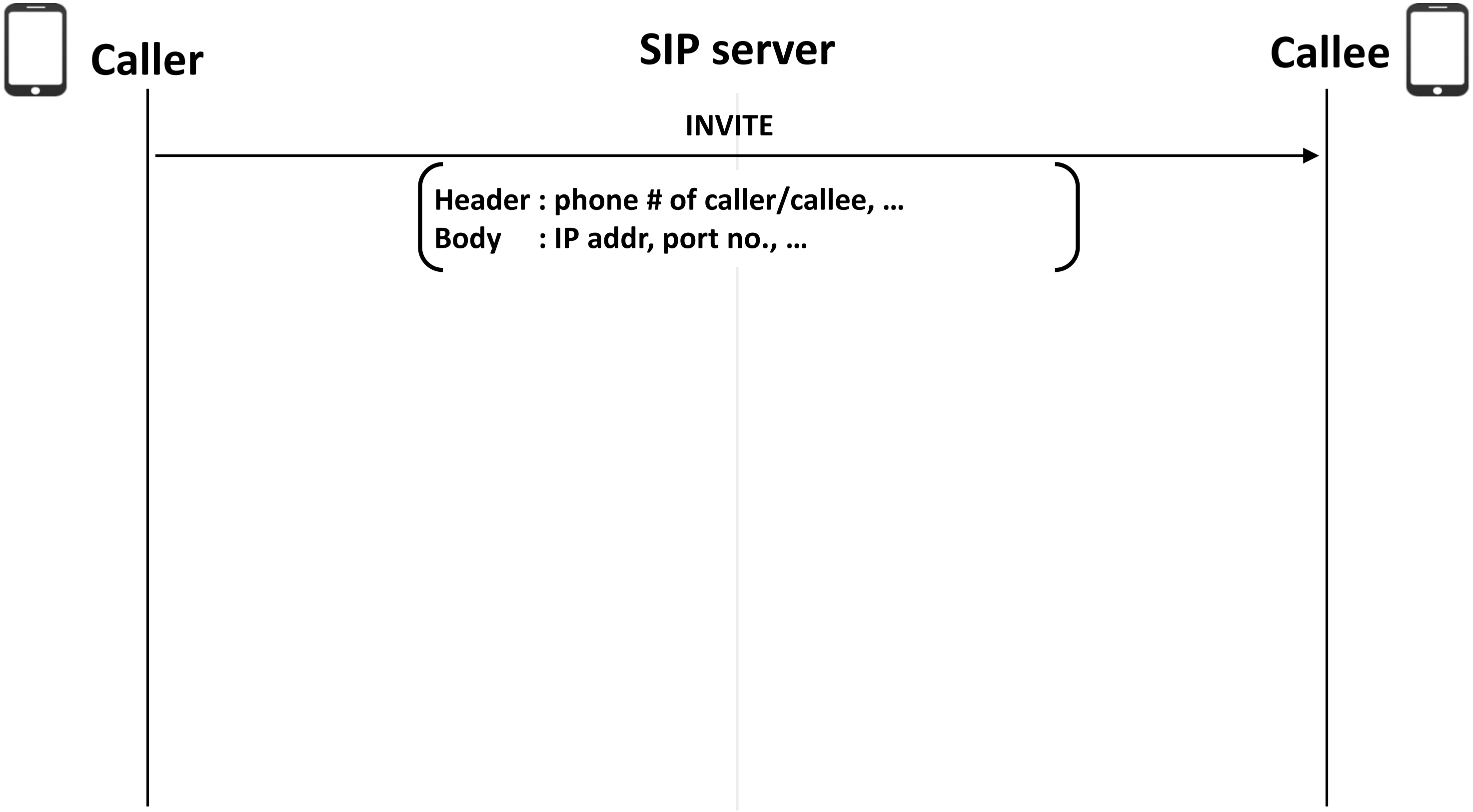
Caller

SIP server

Callee

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

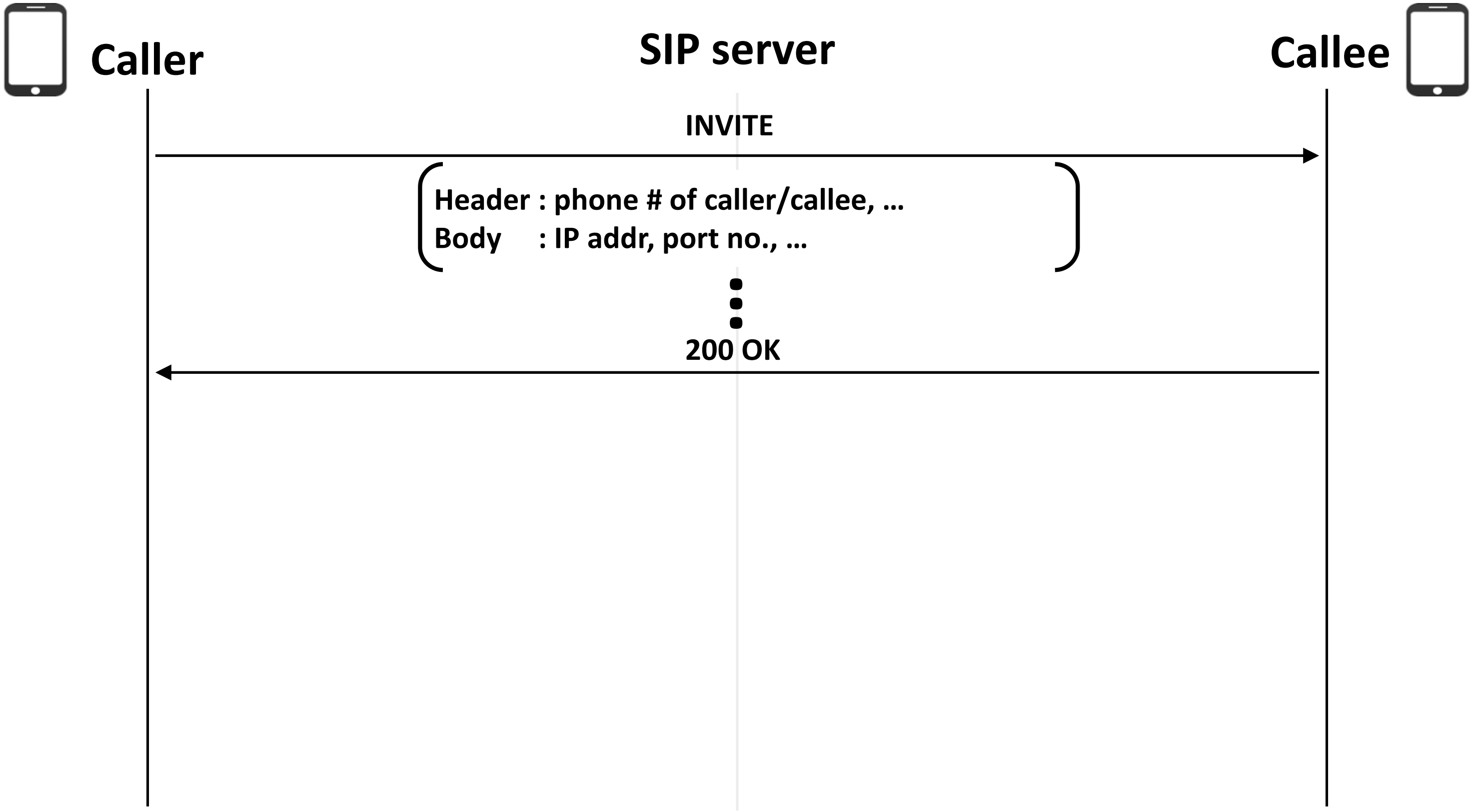
VoLTE Call Procedure



Header : phone # of caller/callee, …
Body : IP addr, port no., …

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

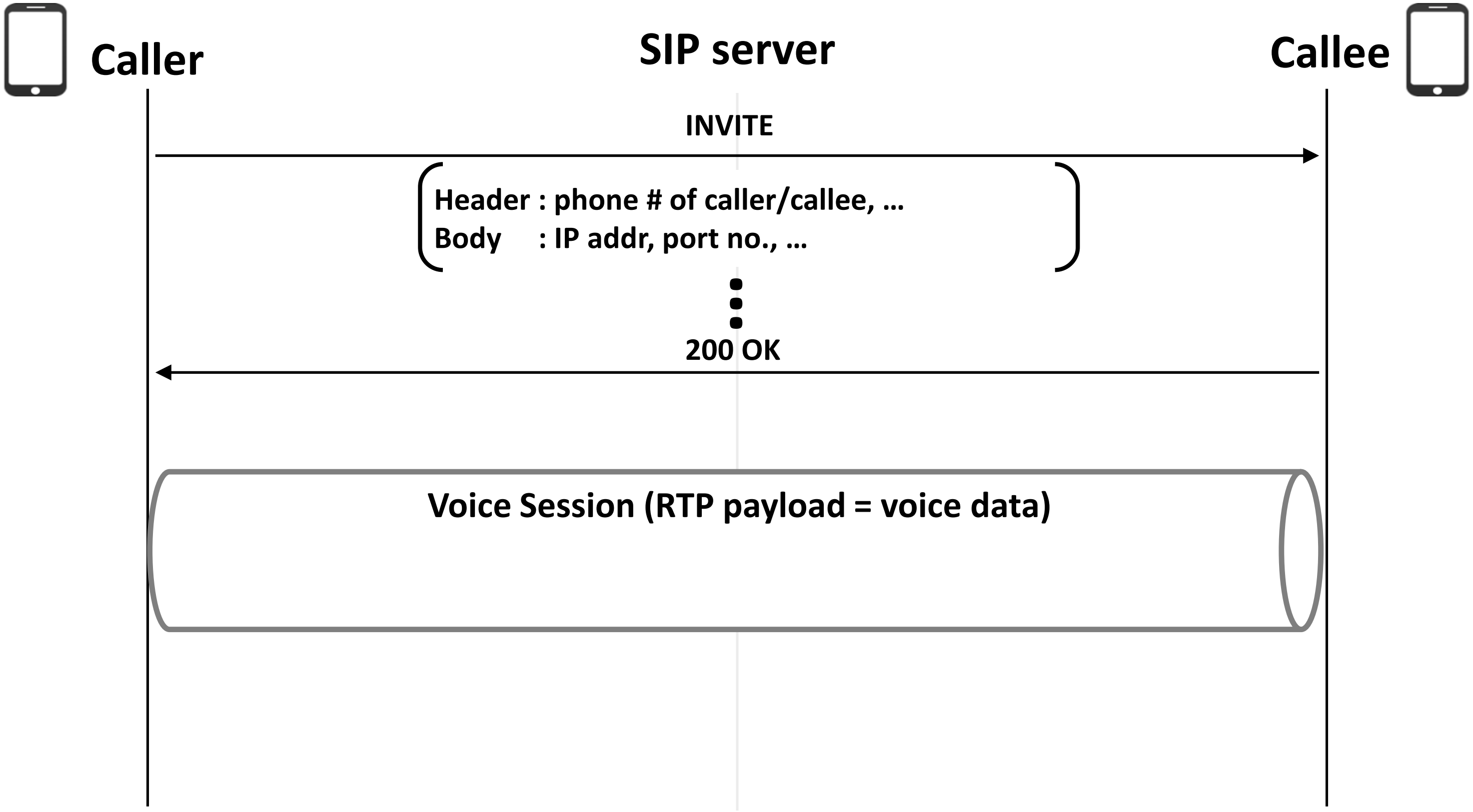
VoLTE Call Procedure



Header : phone # of caller/callee, …
Body : IP addr, port no., …

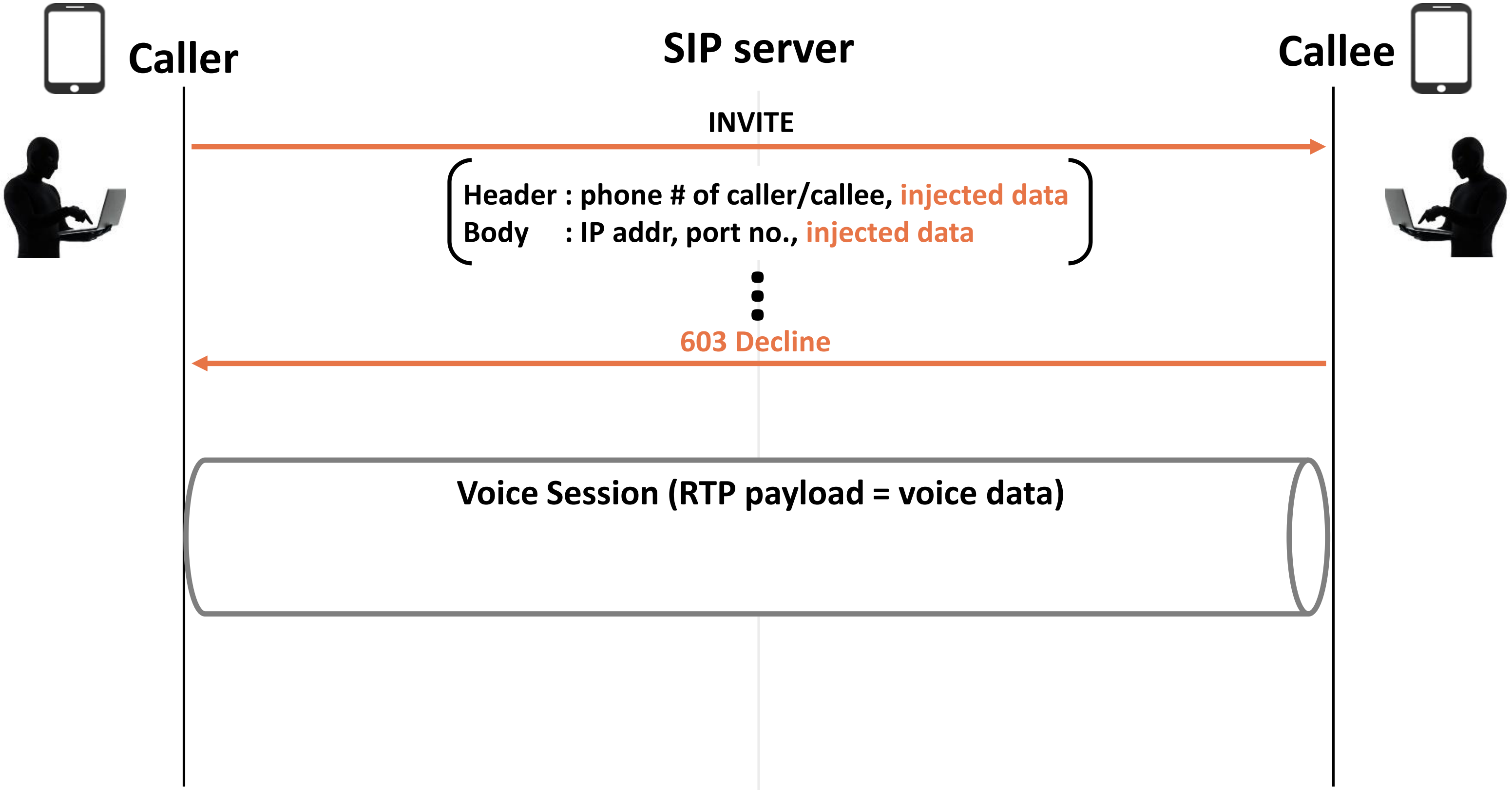
*SIP: Session Initiation Protocol, *RTP: Real-time Transport Protocol

VoLTE Call Procedure


Caller
SIP server
Callee
INVITE
Header : phone # of caller/callee, …
Body : IP addr, port no., …
200 OK
Voice Session (RTP payload = voice data)

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

Free Channel: SIP Tunneling



Caller

SIP server

Callee

INVITE

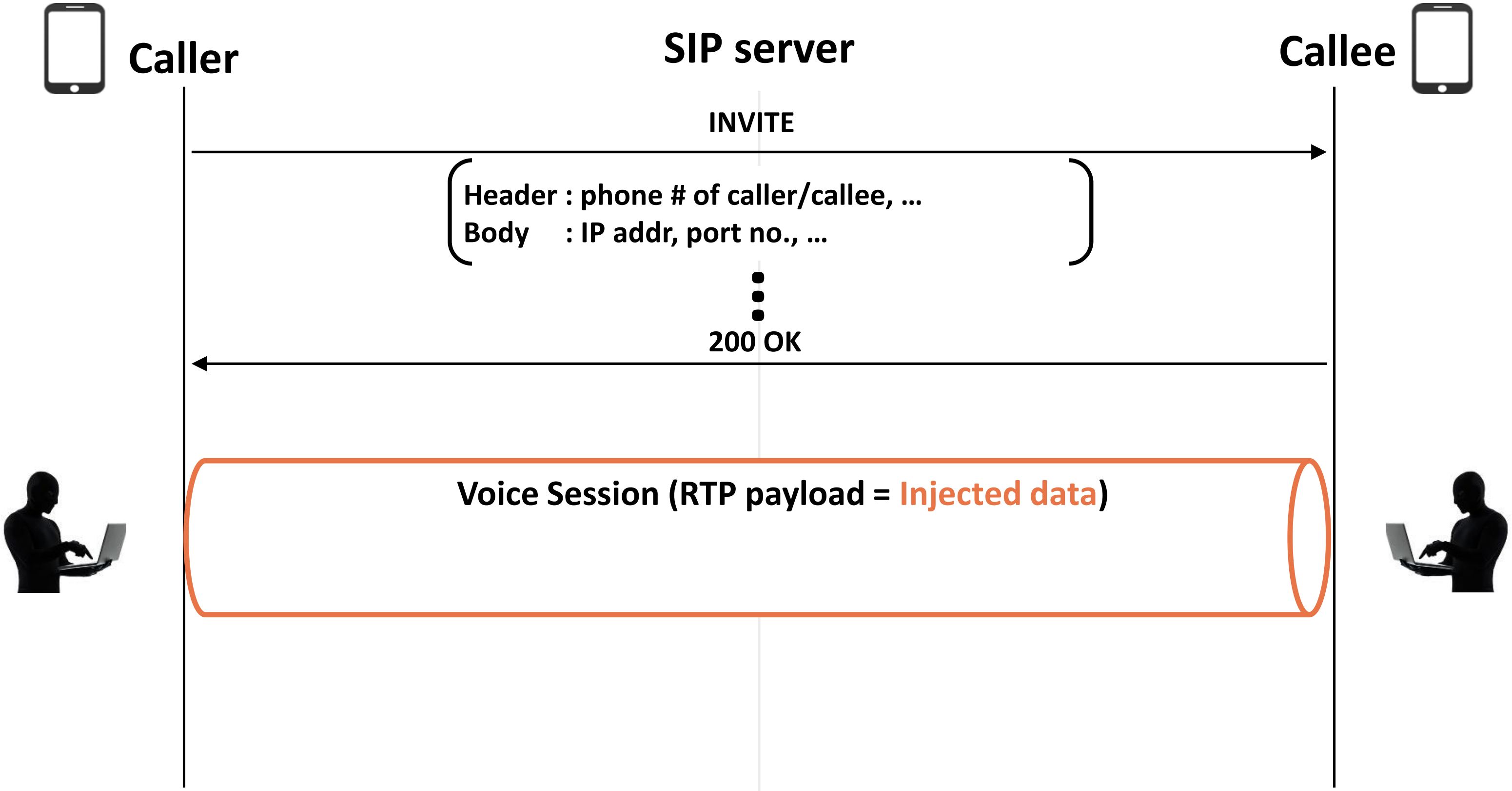
Header : phone # of caller/callee, injected data
Body : IP addr, port no., injected data

603 Decline

Voice Session (RTP payload = voice data)

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

Free Channel: Media Tunneling



Caller

SIP server

Callee

INVITE

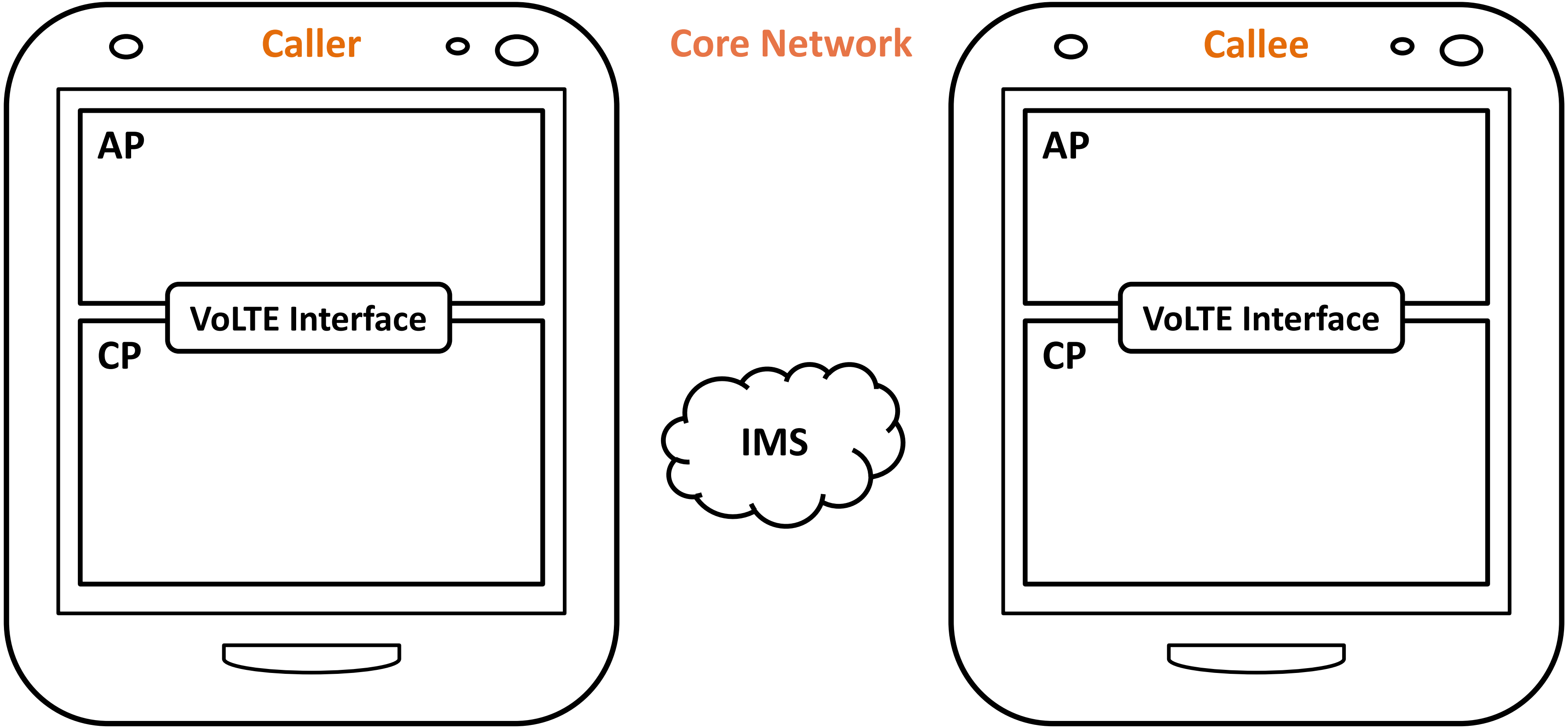
Header : phone # of caller/callee, …
Body : IP addr, port no., …

200 OK

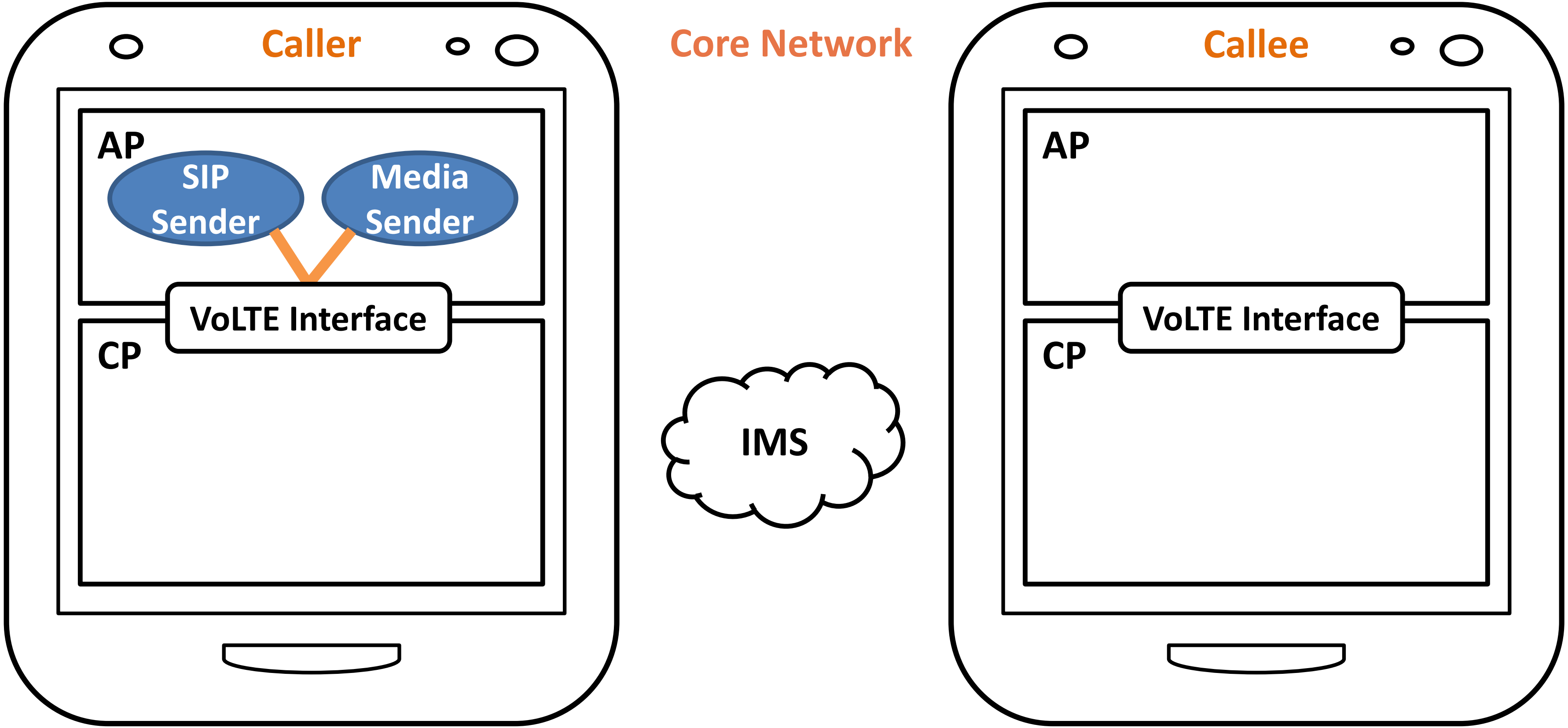
Voice Session (RTP payload = Injected data)

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

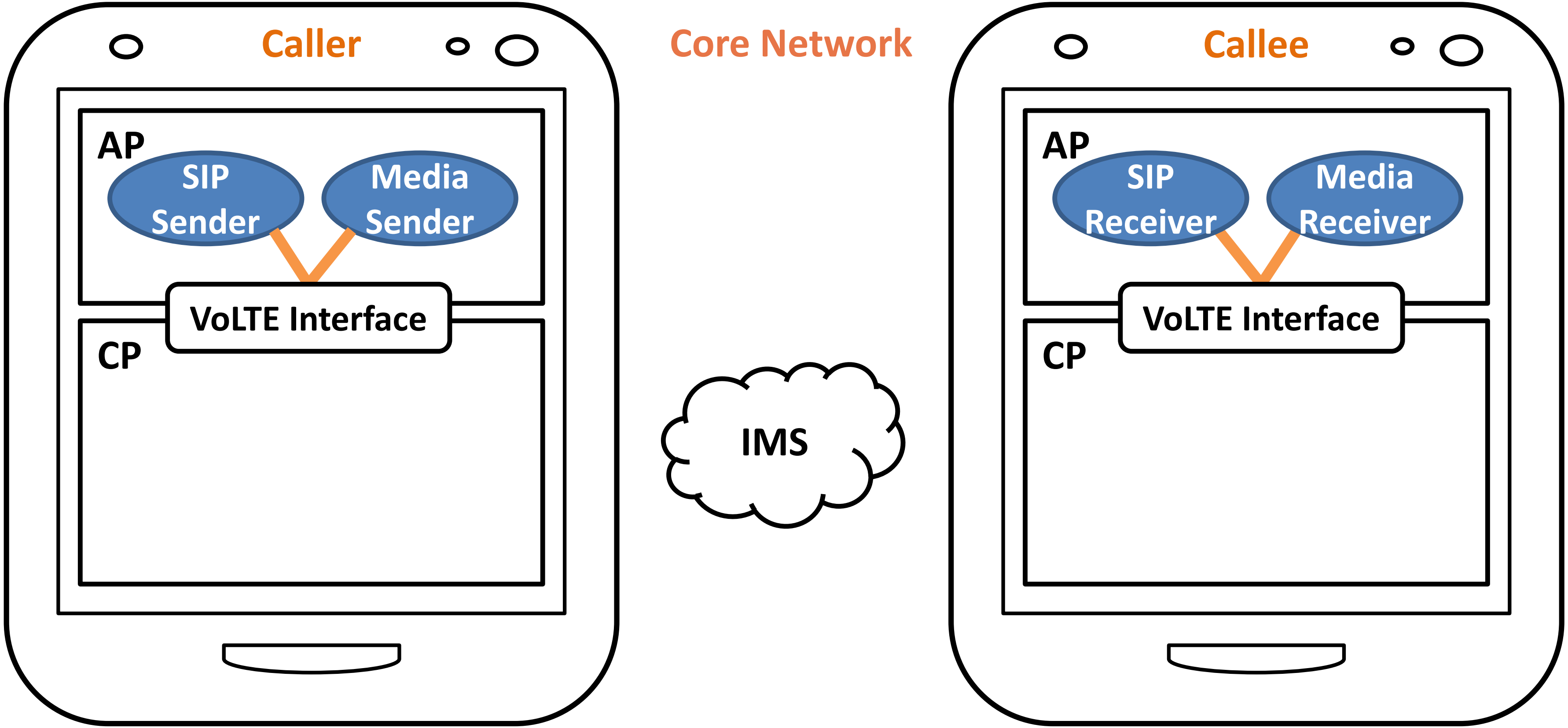
Attack Implementation in Detail



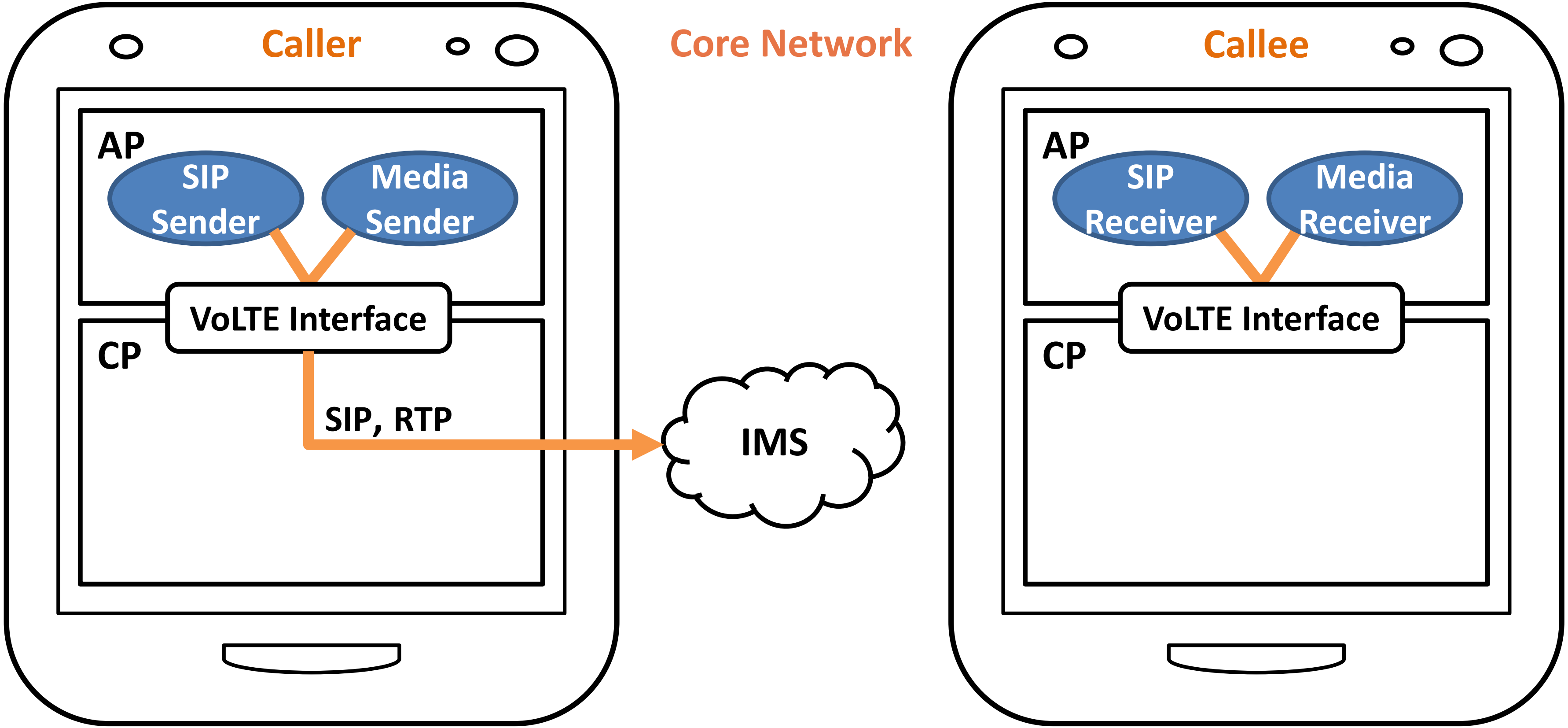
Attack Implementation in Detail



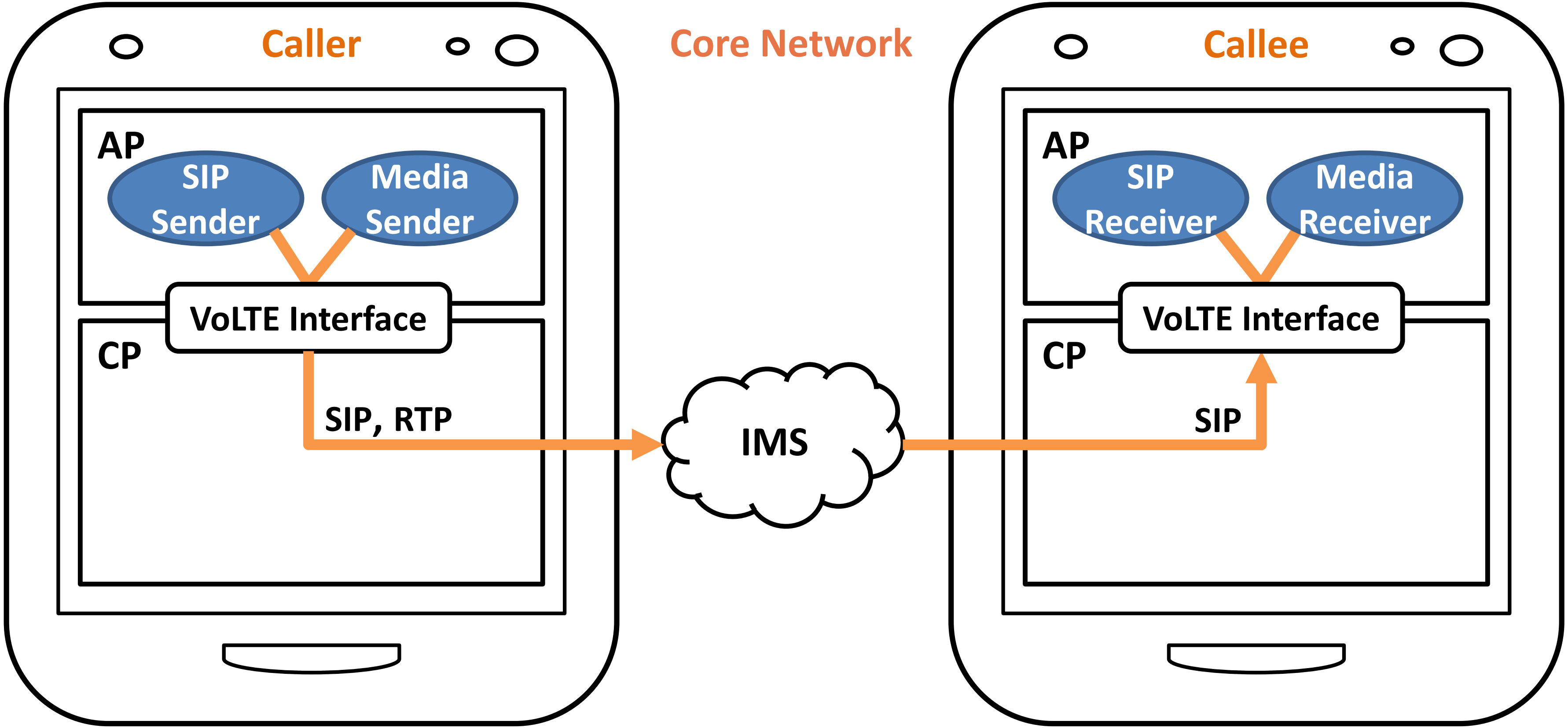
Attack Implementation in Detail



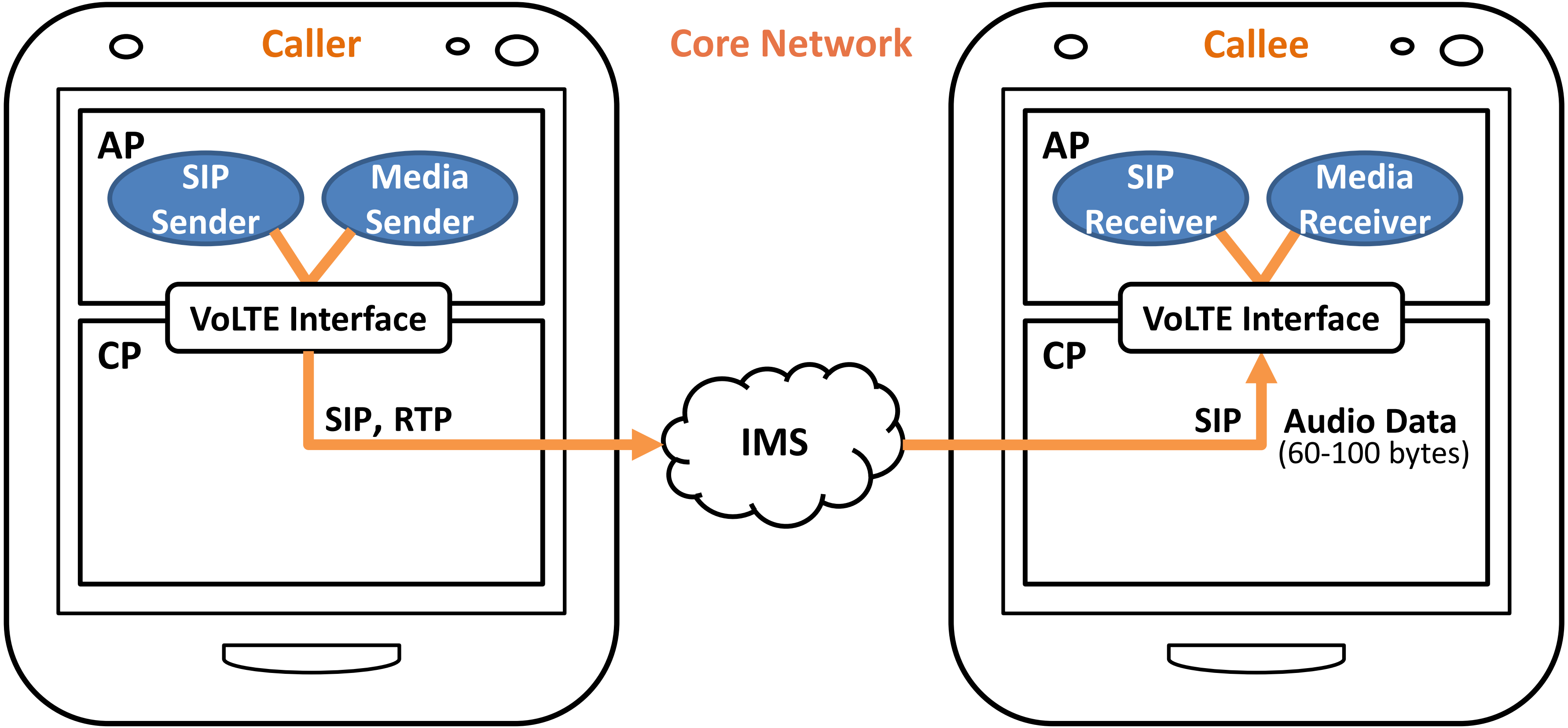
Attack Implementation in Detail



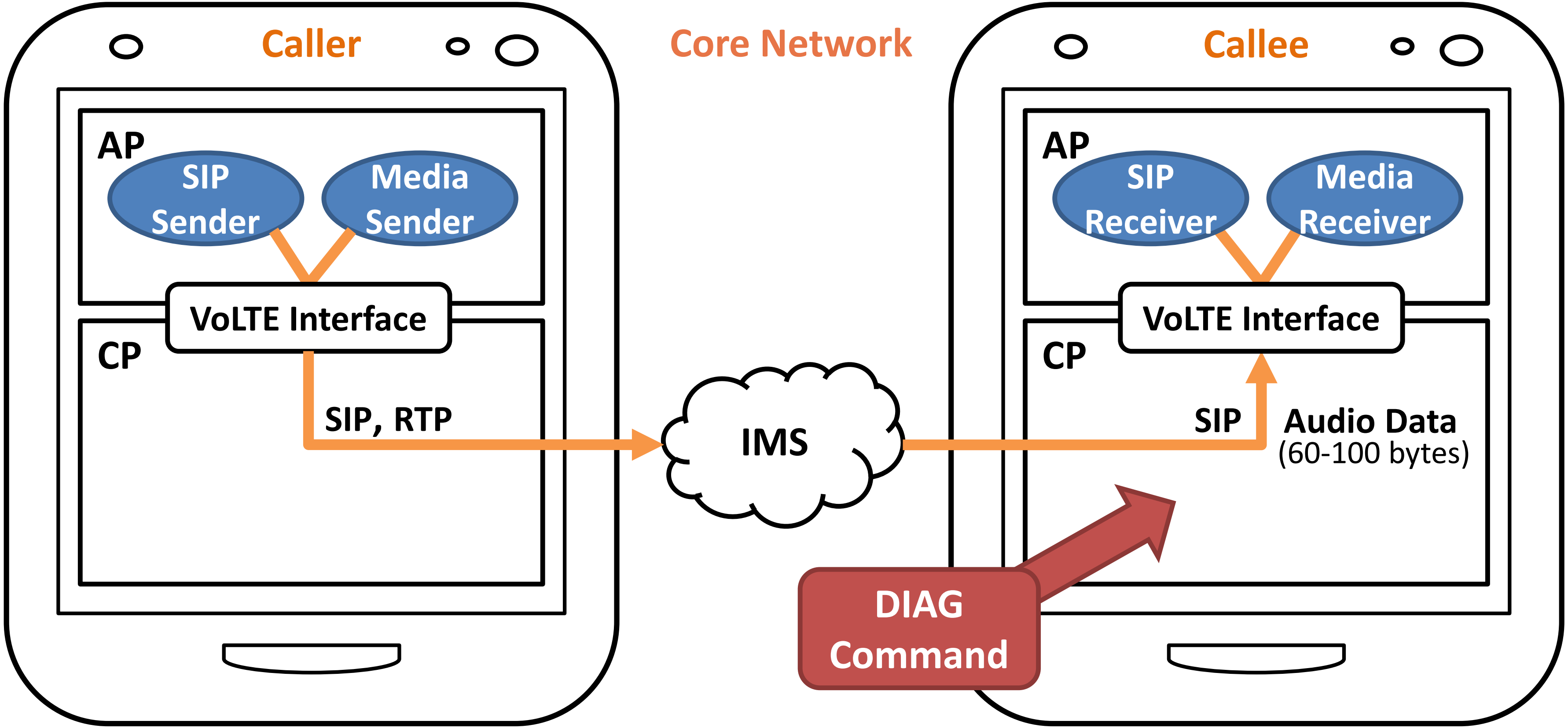
Attack Implementation in Detail



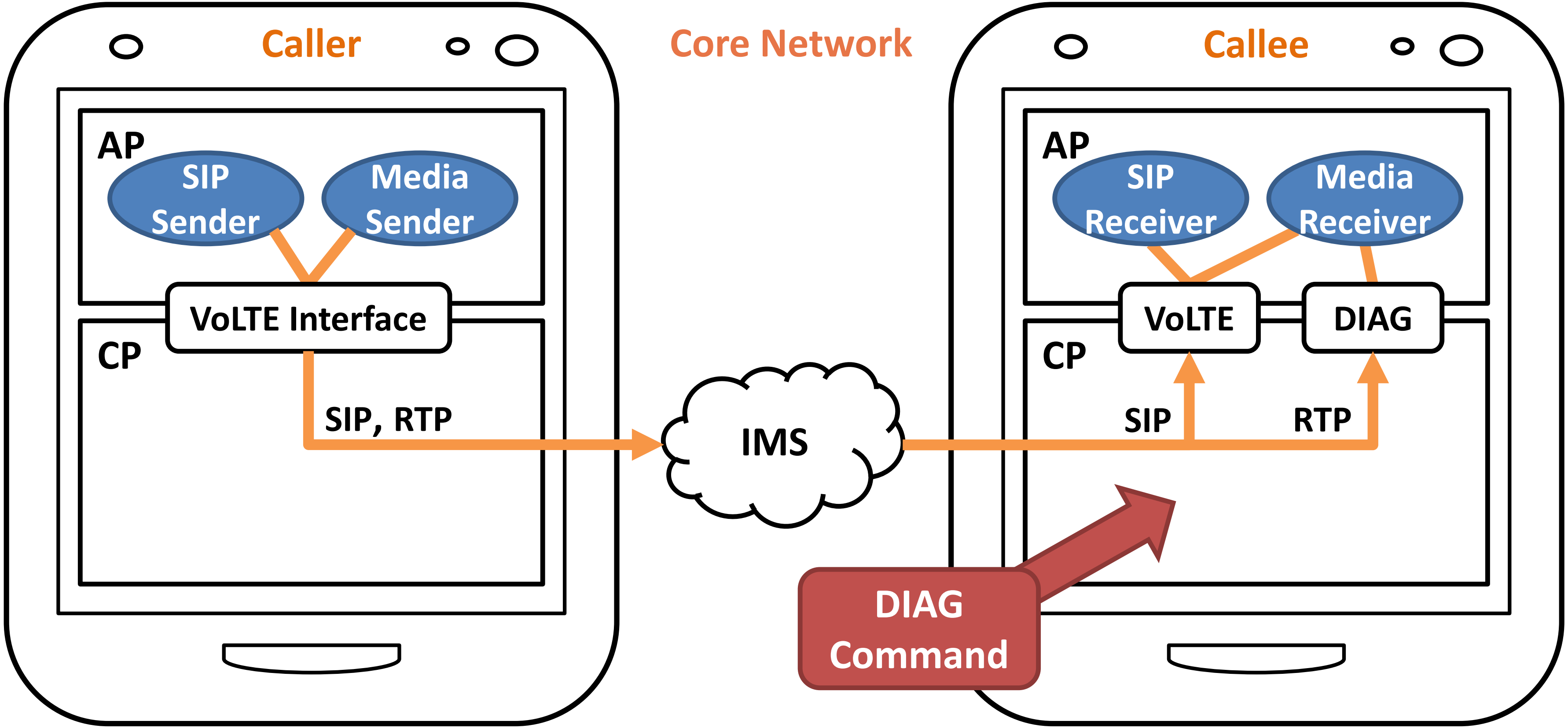
Attack Implementation in Detail



Attack Implementation in Detail



Attack Implementation in Detail



Outline

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

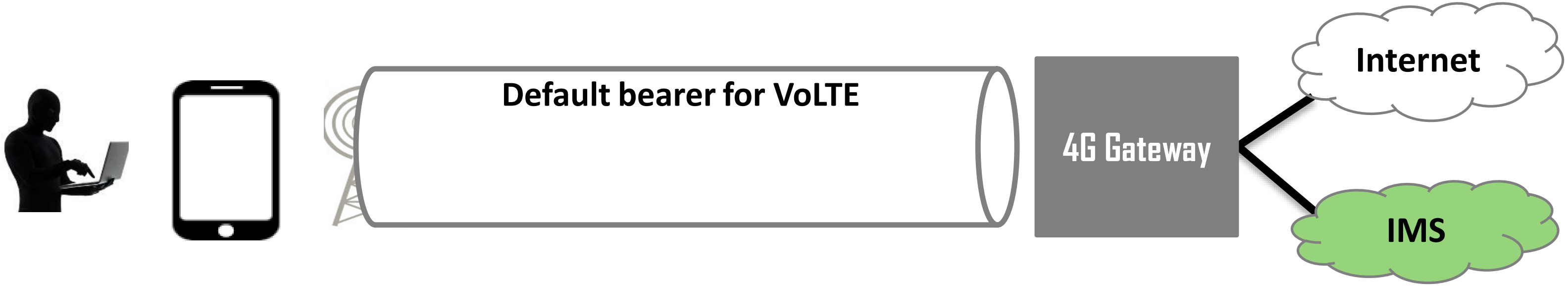
Five security issues

- **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: Direct communication

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

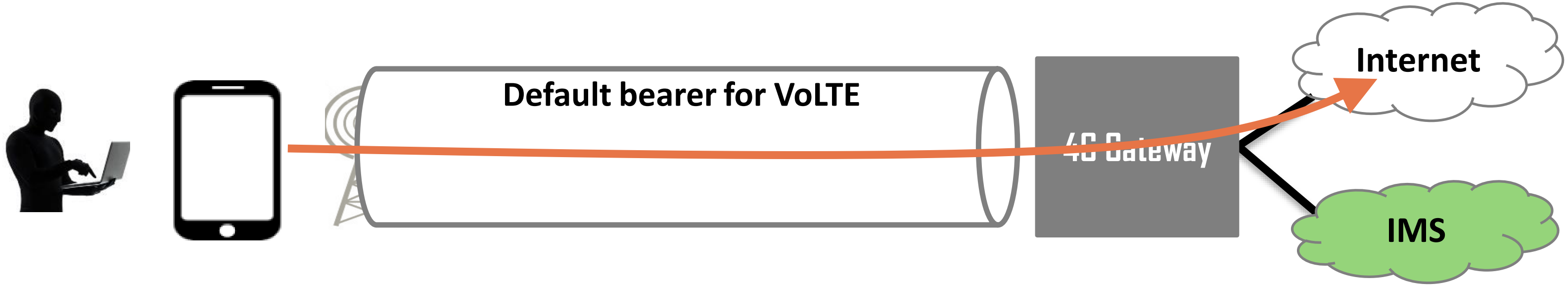
  E.g. TCP/UDP Socket (Src: voice IP/port, Dst: youtube.com/port)



Free Channel: Direct communication

- **Phone-to-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)

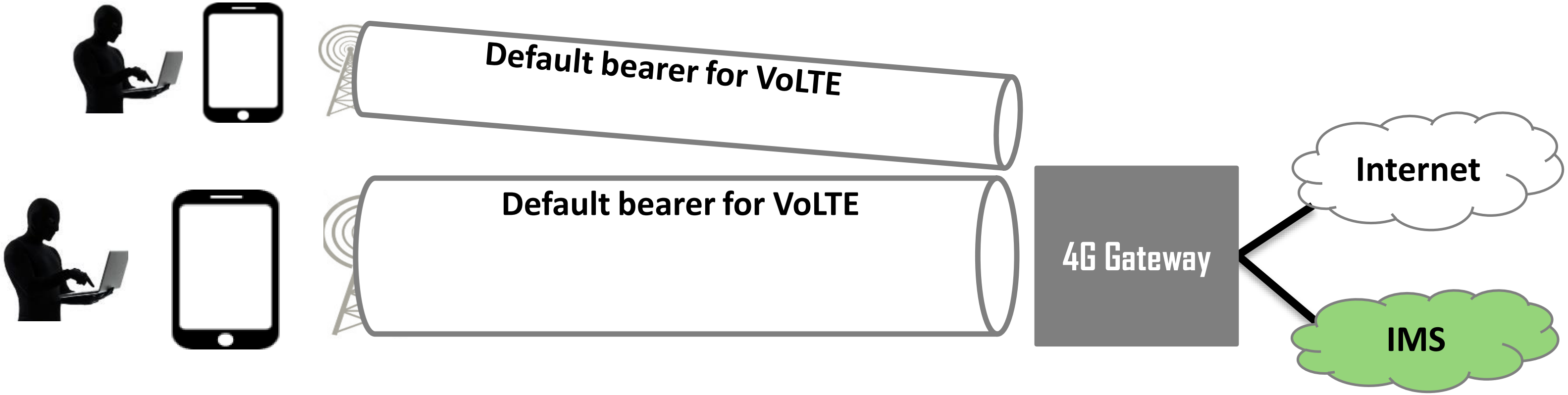


SysSec System Security Lab

Free Channel: Direct communication

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

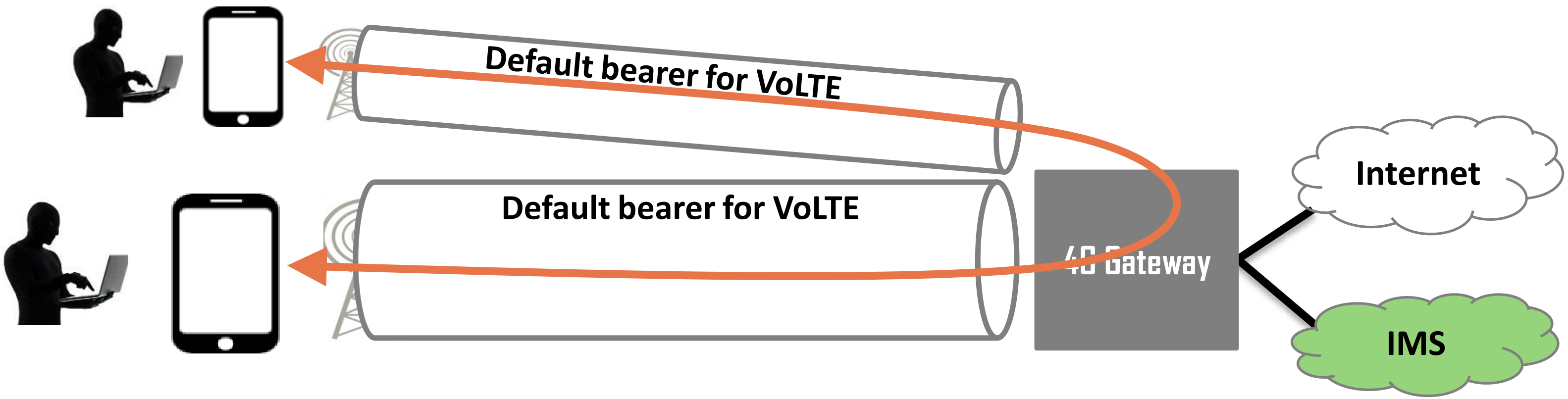
E.g. TCP/UDP Socket (Src: voice IP/port, Dst: callee’s voice IP/port)



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)



Evaluation Result: Accounting Bypass

	Free Channel
Using VoLTE Protocol	SIP Tunneling
	Media Tunneling
Direct Communication	Phone to Phone
	Phone to Internet

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Evaluation Result: Accounting Bypass

	Free Channel	US-1	US-2
Using VoLTE Protocol	SIP Tunneling	✓	✓
	Media Tunneling	✓	✓
Direct Communication	Phone to Phone	✓	✗
	Phone to Internet	✗	✓

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Evaluation Result: Accounting Bypass

	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	✗	✓	✓	✗	IPv4:✓ IPv6:✗

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Evaluation Result: Accounting Bypass

	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	✗	✓	✓	✗	IPv4:✓ IPv6:✗

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Evaluation Result: Accounting Bypass

	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	✗	✓	✓	✗	IPv4:✓ IPv6:✗

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Evaluation Result: Accounting Bypass

	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	✓	✓	✓	✓	✓
	Media Tunneling	✓	✓	✓	✓	✓
Direct Communication	Phone to Phone	16.8 Mbps				
	Phone to Internet	21.5 Mbps				

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Evaluation Result: Accounting Bypass

	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	✓	✓	✓	✓	✓
	Media Tunneling	42 Kbps				
Direct Communication	Phone to Phone	16.8 Mbps				
	Phone to Internet	21.5 Mbps				

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Evaluation Result: Accounting Bypass

	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	X				
	Media Tunneling	42 Kbps				
Direct Communication	Phone to Phone	16.8 Mbps				
	Phone to Internet	21.5 Mbps				

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Evaluation Result: Accounting Bypass

	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	X				
	Media Tunneling	42 Kbps				
Direct Communication	Phone to Phone	16.8 Mbps				
	Phone to Internet	21.5 Mbps				

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Outline

- **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)

No Encryption for Voice Packets

- For voice signaling,
  - only one operator was using IPsec
  - An attacker can easily manipulate VoLTE call flow
- For voice data,
  - no one encrypted voice data
  - An attacker might wiretap the outgoing voice data

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

😈 : Vulnerable 🙂 : Secure

No Authentication/Session Management

- ❖ No authentication
  - – Make a call with a fake number

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No Authentication	🙂	🙂	😈	😈	🙂	Caller Spoofing
	No Session Management	😈	😈	😈	🙂	😈	Denial of Service on Core Network

😈 : Vulnerable 🙂 : Secure

No Authentication/Session Management

- No authentication
  - Make a call with a fake number
- No session management

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No Authentication	🙂	🙂	😈	😈	🙂	Caller Spoofing
	No Session Management	😈	😈	😈	🙂	😈	Denial of Service on Core Network

😈 : Vulnerable 🙂 : Secure

No Authentication/Session Management

- No authentication
  - Make a call with a fake number
- No session management

* In a normal call, one user can call to only one person

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No Authentication	🙂	🙂	😈	😈	🙂	Caller Spoofing
	No Session Management	😈	😈	😈	🙂	😈	Denial of Service on Core Network

😈 : Vulnerable 🙂 : Secure

No Authentication/Session Management

- No authentication
  - Make a call with a fake number
- No session management

  * In a normal call, one user can call to only one person

  - Send multiple INVITE messages
    - Several call sessions are established
    - For each call session, high-cost bearer is established

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No Authentication	🙂	🙂	😈	😈	🙂	Caller Spoofing
	No Session Management	😈	😈	😈	🙂	😈	Denial of Service on Core Network

😈 : Vulnerable 🙂 : Secure

No Authentication/Session Management

- No authentication
  - Make a call with a fake number
- No session management

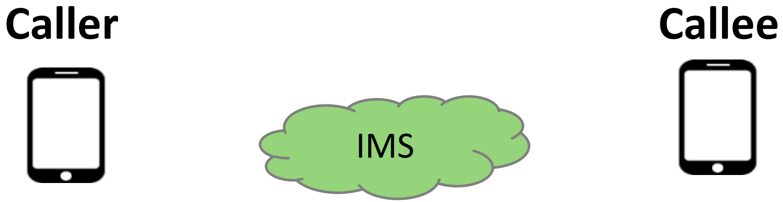
  *** In a normal call, one user can call to only one person**

  - Send multiple INVITE messages
    - Several call sessions are established
    - For each call session, high-cost bearer is established
  - Even one sender can deplete resources of the core network

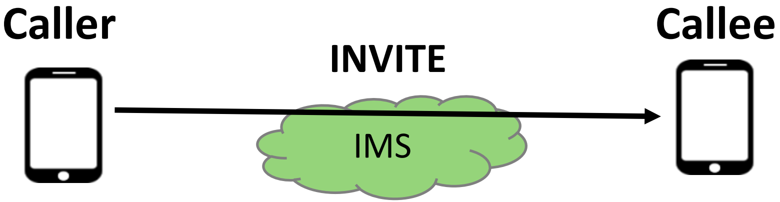
Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No Authentication	🙂	🙂	😈	😈	🙂	Caller Spoofing
	No Session Management	😈	😈	😈	🙂	😈	Denial of Service on Core Network

😈 : Vulnerable 🙂 : Secure

Caller Spoofing Scenario

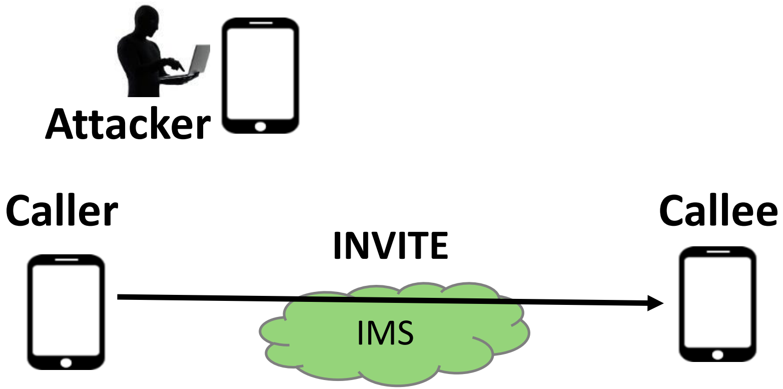


Caller Spoofing Scenario



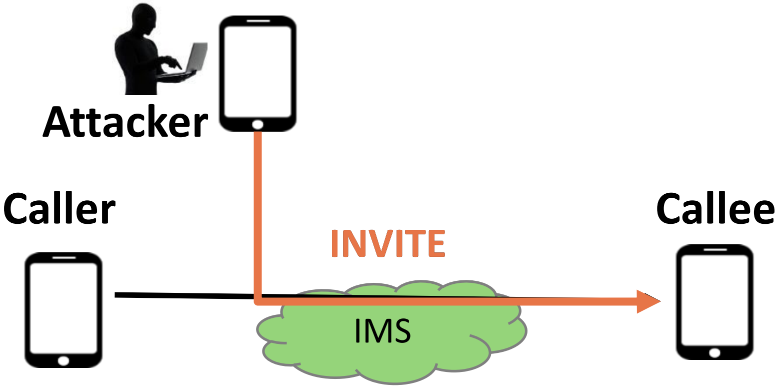
Header : phone # of caller/callee, …
Body : IP addr, port no., …

Caller Spoofing Scenario

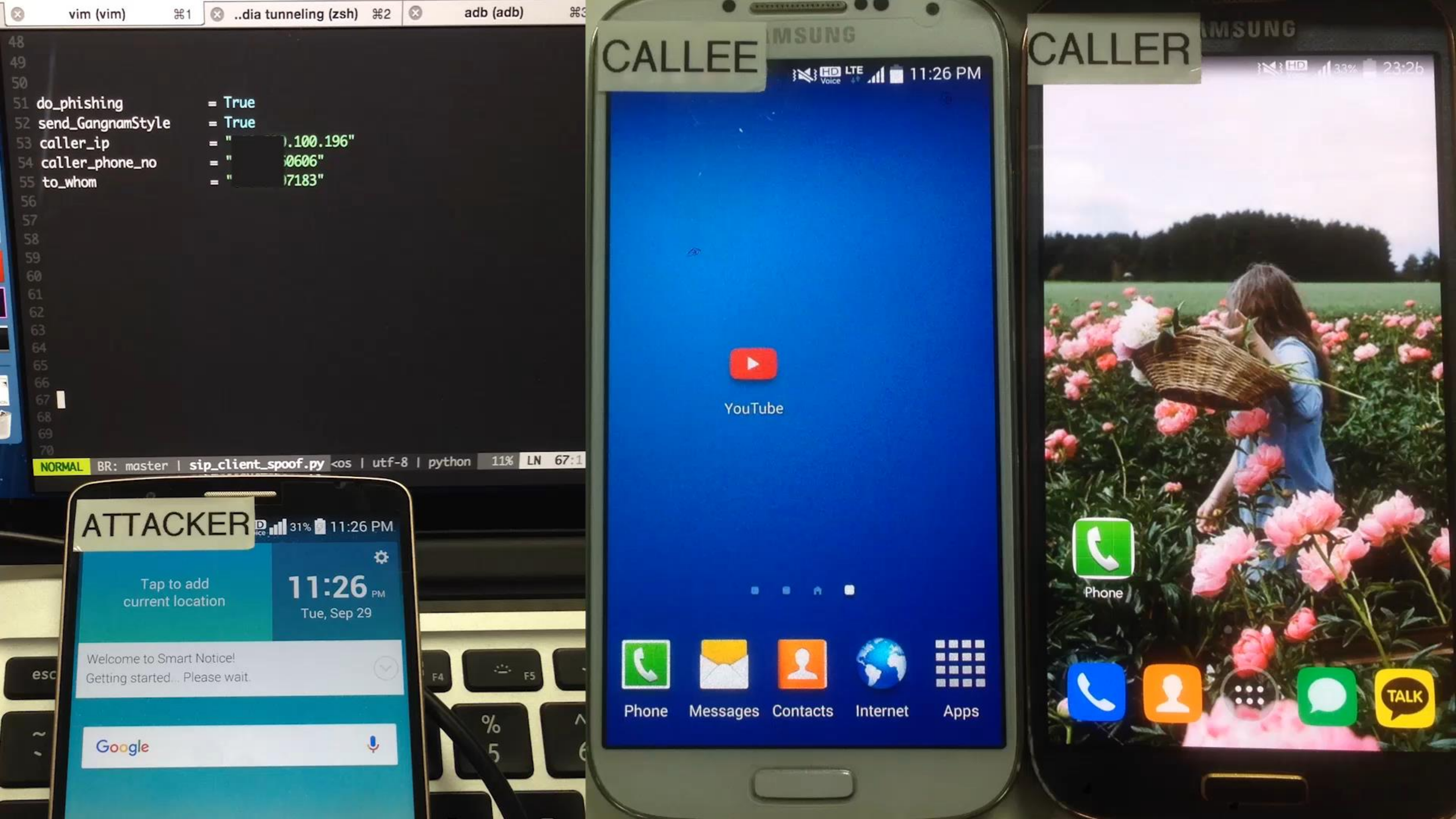


Header : phone # of caller/callee, …
Body : IP addr, port no., …

Caller Spoofing Scenario



Header : phone # of caller/callee, …
Body : IP addr, port no., …



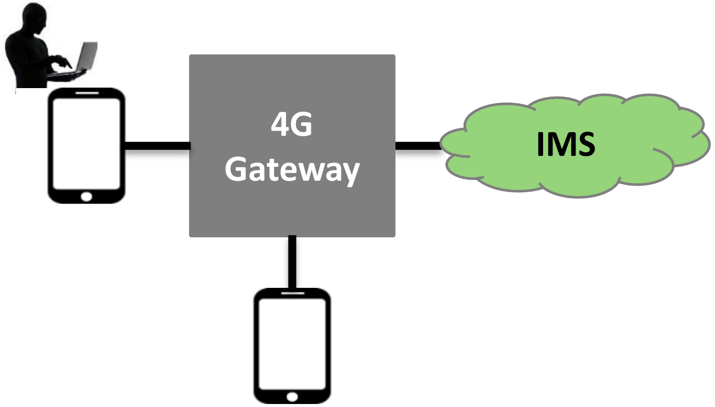
```
do_phishing          = True
send_GangnamStyle    = True
caller_ip            = "[redacted].100.196"
caller_phone_no      = "[redacted]0606"
to_whom              = "[redacted]7183"
```

```
NORMAL  BR: master | sip_client_spoof.py <os | utf-8 | python  11%  LN  67:1
```

Welcome to Smart Notice!
Getting started... Please wait.

IMS Bypassing

- All voice packets should pass IMS, but

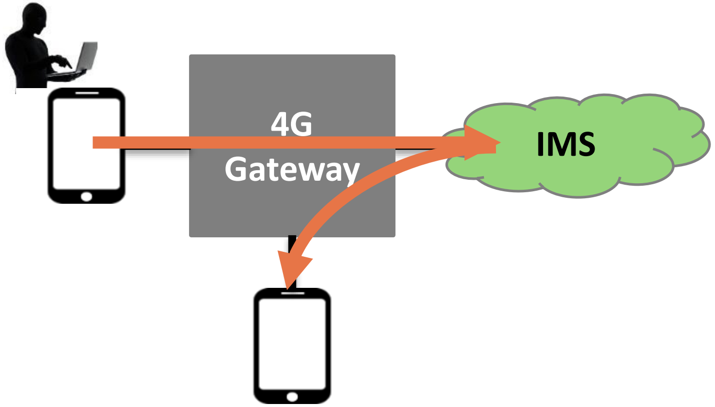


Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
4G-GW	IMS Bypassing	😈	🙂	😈	🙂	🙂	Caller Spoofing

😈 : Vulnerable 🙂 : Secure

IMS Bypassing

- All voice packets should pass IMS, but

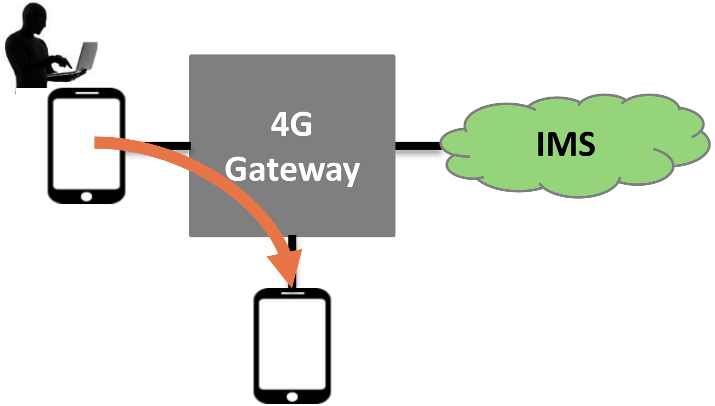


Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
4G-GW	IMS Bypassing	😈	🙂	😈	🙂	🙂	Caller Spoofing

😈 : Vulnerable 🙂 : Secure

IMS Bypassing

- All voice packets should pass IMS, but



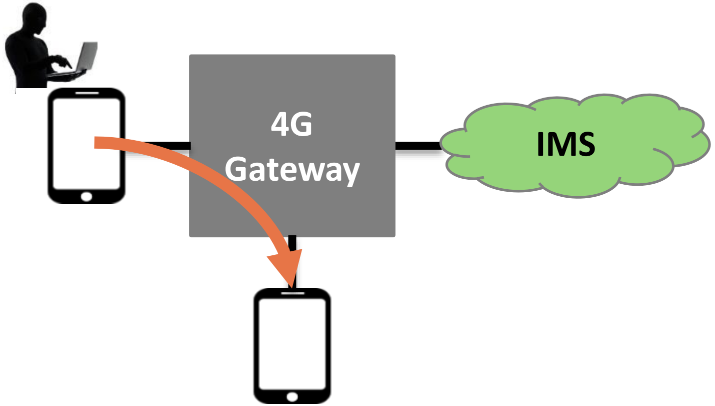
Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
4G-GW	IMS Bypassing	😈	🙂	😈	🙂	🙂	Caller Spoofing

😈 : Vulnerable 🙂 : Secure

IMS Bypassing

- All voice packets should pass IMS, but
- An attacker can bypass SIP servers in IMS
  - IMS vulnerabilities are also possible

    e.g. Make a call with a fake number



Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
4G-GW	IMS Bypassing	😈	🙂	😈	🙂	🙂	Caller Spoofing

😈 : Vulnerable 🙂 : Secure

Android Permission Model Mismatch

- No distinction between a phone call and a normal data socket
  - In 3G, an app needs "*android.permission.CALL_PHONE*"
  - In VoLTE, we found that an app can call with "*android.permission.INTERNET*"

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
Phone	Permission Mismatch	Vulnerable for all Android					Denial of Service on Call, Overbilling

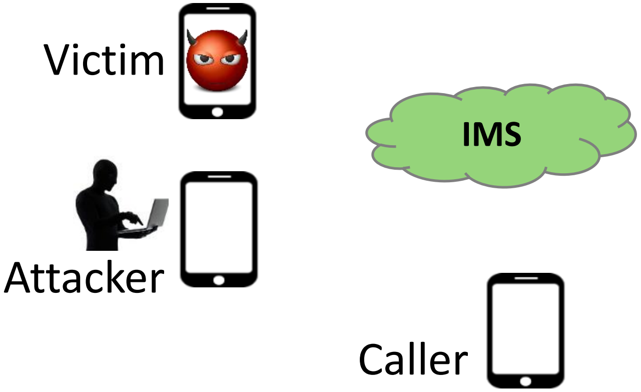
Android Permission Model Mismatch

- No distinction between a phone call and a normal data socket
  - In 3G, an app needs “*android.permission.CALL_PHONE*”
  - In VoLTE, we found that an app can call with “*android.permission.INTERNET*”
- A malicious app **only with Internet permission** can perform
  - Denial of service attack on call
  - Overbilling attack by making an expensive video call

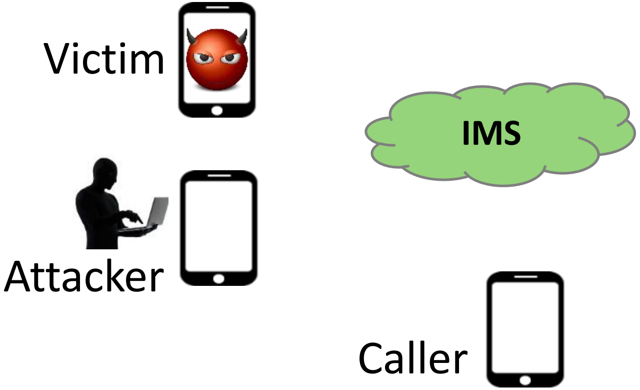
Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
Phone	Permission Mismatch	Vulnerable for all Android					Denial of Service on Call, Overbilling

Denial of Service on Call Scenario

- Blocking an incoming call

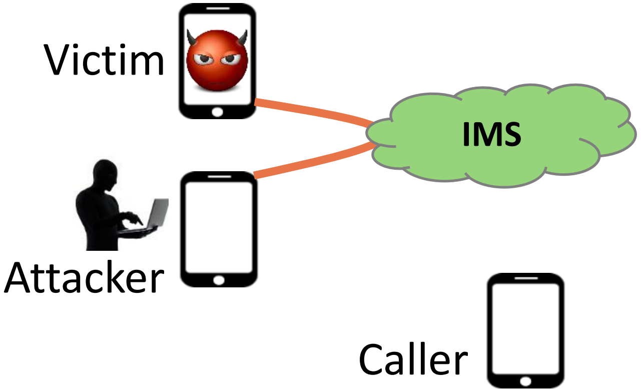


- Cutting off an ongoing call

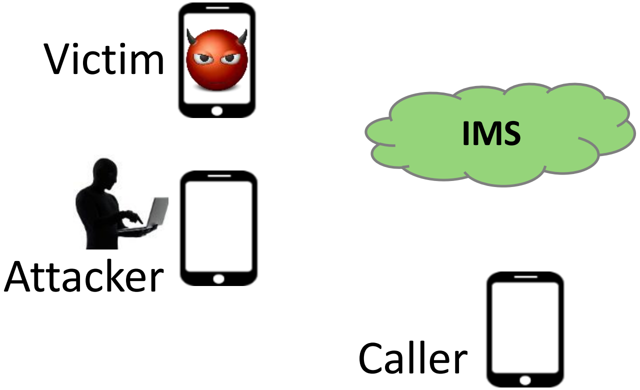


Denial of Service on Call Scenario

- Blocking an incoming call

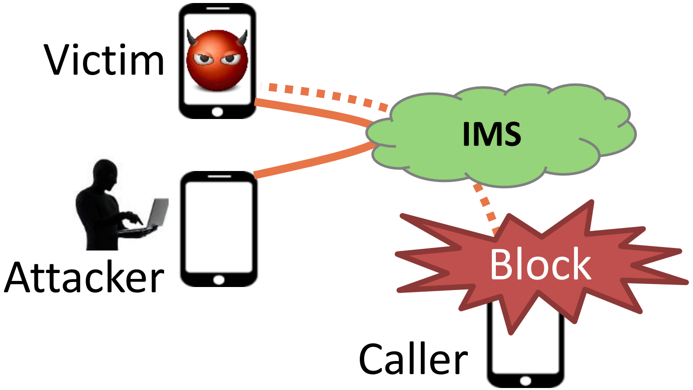


- Cutting off an ongoing call

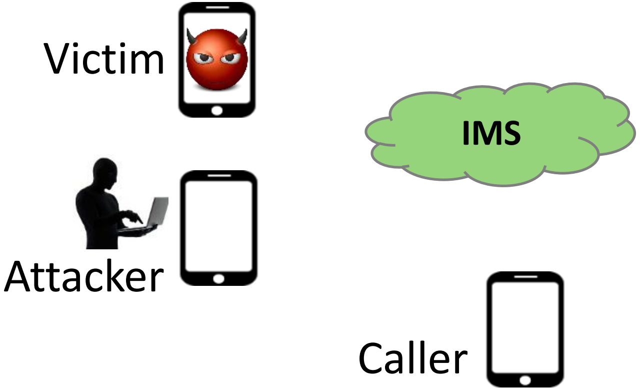


Denial of Service on Call Scenario

- Blocking an incoming call

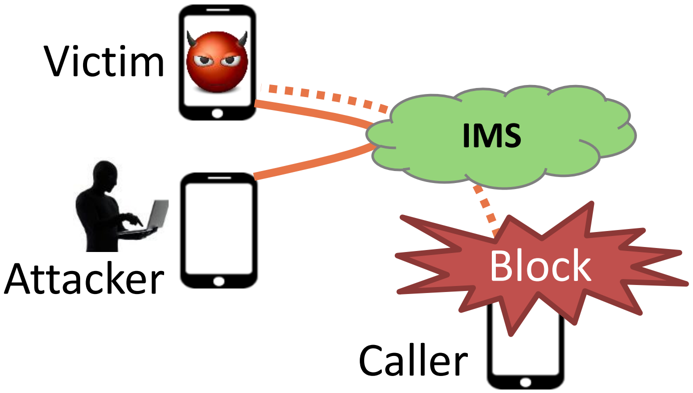


- Cutting off an ongoing call

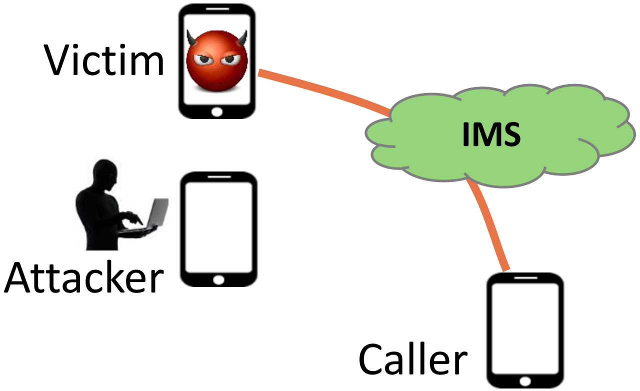


Denial of Service on Call Scenario

- Blocking an incoming call

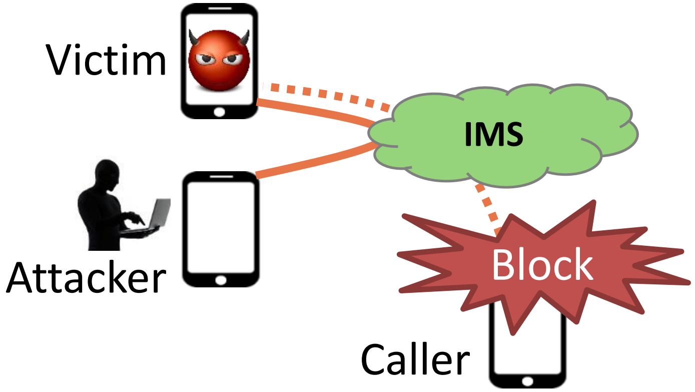


- Cutting off an ongoing call

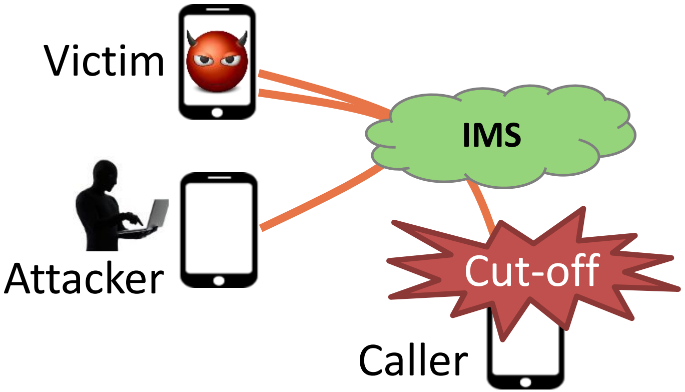


Denial of Service on Call Scenario

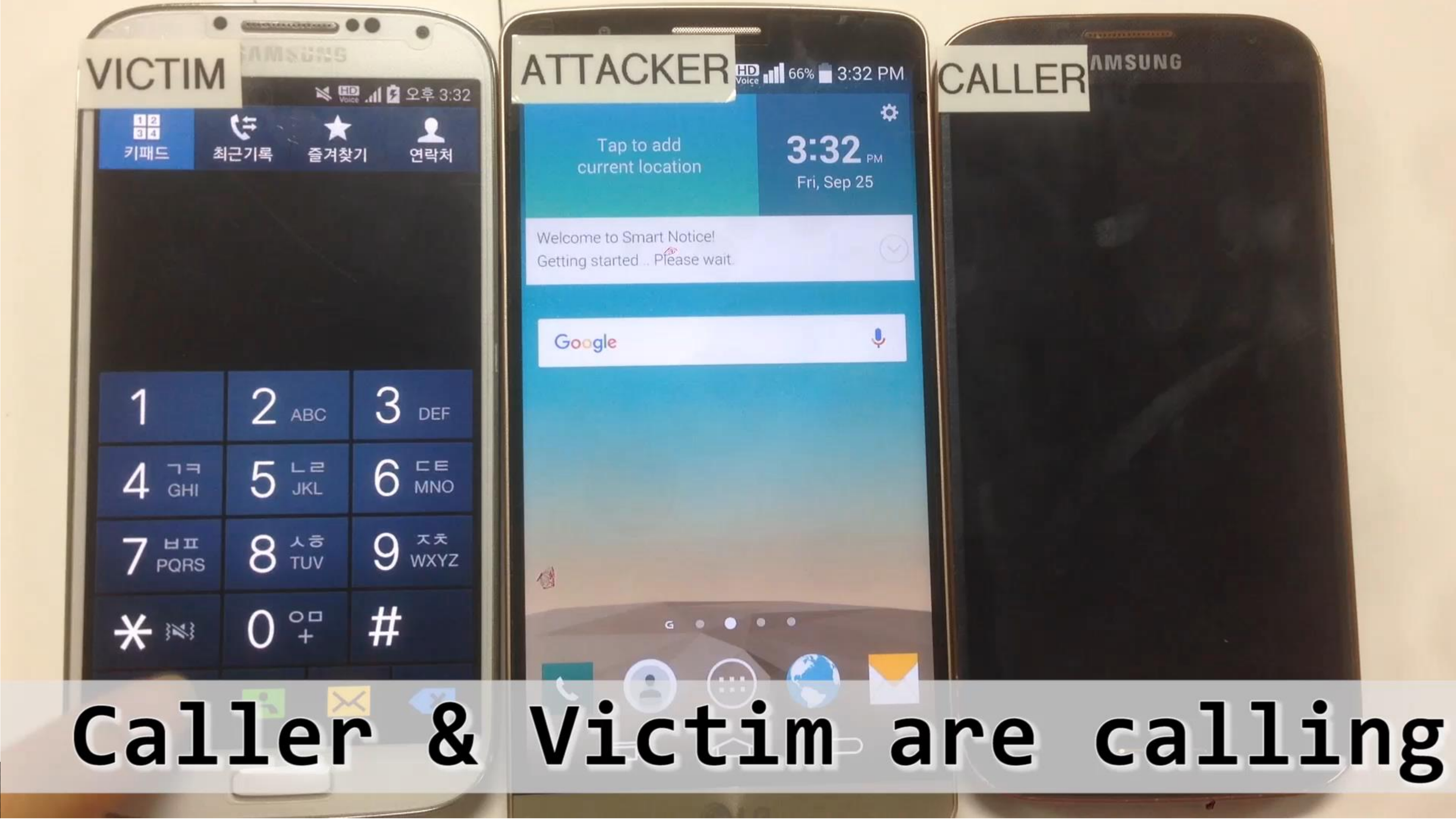
- Blocking an incoming call



- Cutting off an ongoing call



Victim's malicious app calls to attacker



Caller & Victim are calling

Mitigation

Point	Vulnerability	Mitigation	Responsible Entity
IMS	No Security Mechanisms	Encrypt call signaling and voice data	Operators IMS provider
	No Authentication	Place proper authentication on voice packets	
	No Session Management	Allow single call session per device	
4G-GW	Direct Communication	Disallow direct communication	Operators
Phone	Permission Mismatch	Create new permission for VoLTE interface	Mobile OS (Android)
	SIP/Media tunneling	Place proper regulation on packet routing Apply deep packet inspection	Mobile OS (Android) Operators

Mitigation

Point	Vulnerability	Mitigation	Responsible Entity
IMS	No Security Mechanisms	Encrypt call signaling and voice data	Operators IMS provider
	No Authentication	Place proper authentication on voice packets	
	No Session Management	Allow single call session per device	
4G-GW	Direct Communication	Disallow direct communication	Operators
Phone	Permission Mismatch	Create new permission for VoLTE interface	Mobile OS (Android)
	SIP/Media tunneling	Place proper regulation on packet routing Apply deep packet inspection	Mobile OS (Android) Operators

How to resolve media tunneling?

Mitigation

Point	Vulnerability	Mitigation	Responsible Entity
IMS	No Security Mechanisms	Encrypt call signaling and voice data	Operators IMS provider
	No Authentication	Place proper authentication on voice packets	
	No Session Management	Allow single call session per device	
4G-GW	Direct Communication	Disallow direct communication	Operators
Phone	Permission Mismatch	Create new permission for VoLTE interface	Mobile OS (Android)
	SIP/Media tunneling	Place proper regulation on packet routing Apply deep packet inspection	Mobile OS (Android) Operators

How to resolve media tunneling? Not easy! Maybe byte-usage accounting?

Discussion

- Some parts of 3GPP specifications are unclear
  - Several misunderstandings of the operators
  - Different implementations and security problems
  - **Security features are only recommendations, not requirement**

- We reported vulnerabilities to US/KR CERTs, and Google in May
  - Google replied “moderate severity”
  - All two U.S. operators ACK’ed, but no follow-ups
  - Only two among three KR operators have been fixing with us

Conclusion

- Newly adopted VoLTE has
  - A complex (legacy time-based) accounting
  - Delegated voice signal (previously done by CP) to AP

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

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

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, ...

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, ...

Holistic re-evaluation of security for VoLTE?

Thank You!

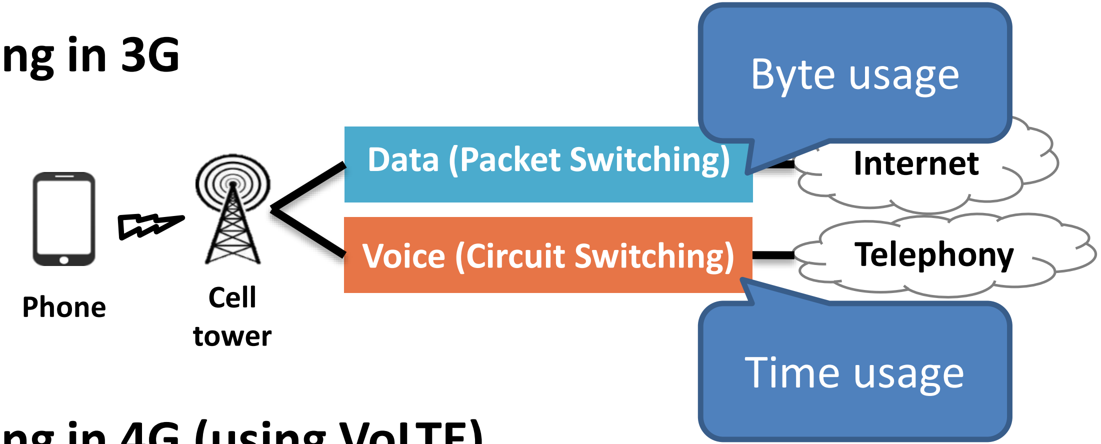
Any questions?

hongilk@kaist.ac.kr
dkay@kaist.ac.kr

APPENDIX

Strange VoLTE Accounting

- Accounting in 3G



Phone

Cell tower

Data (Packet Switching)

Voice (Circuit Switching)

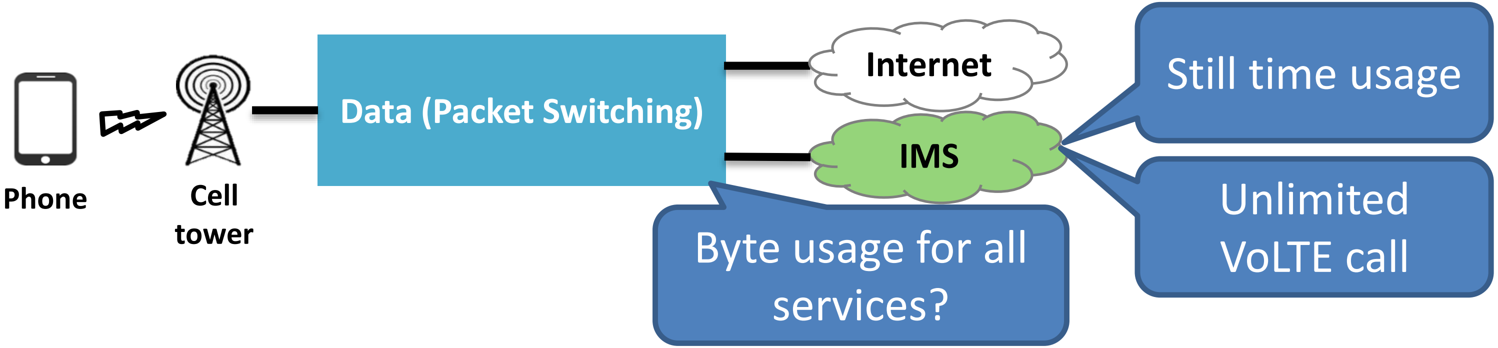
Internet

Telephony

Byte usage

Time usage

- Accounting in 4G (using VoLTE)



Phone

Cell tower

Data (Packet Switching)

Internet

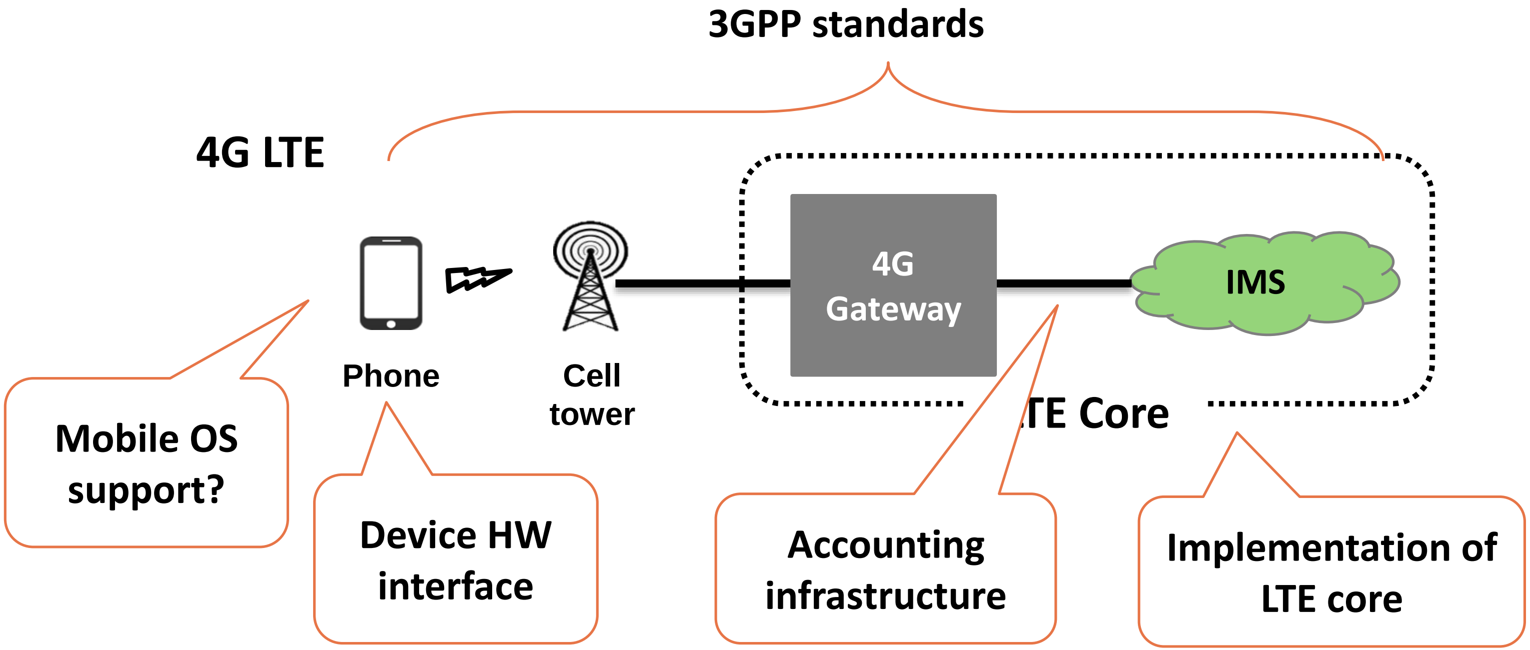
IMS

Byte usage for all services?

Still time usage

Unlimited VoLTE call

Complex Implementation of VoLTE



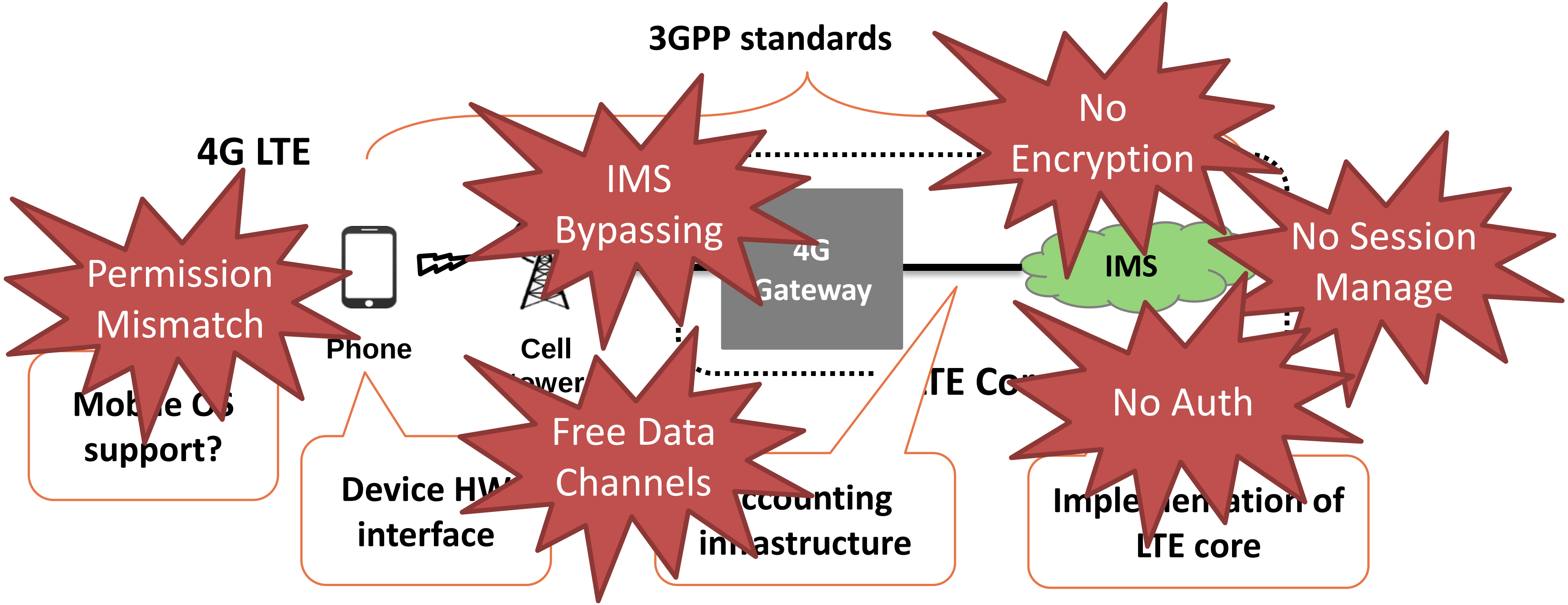
Mobile OS support?

Device HW interface

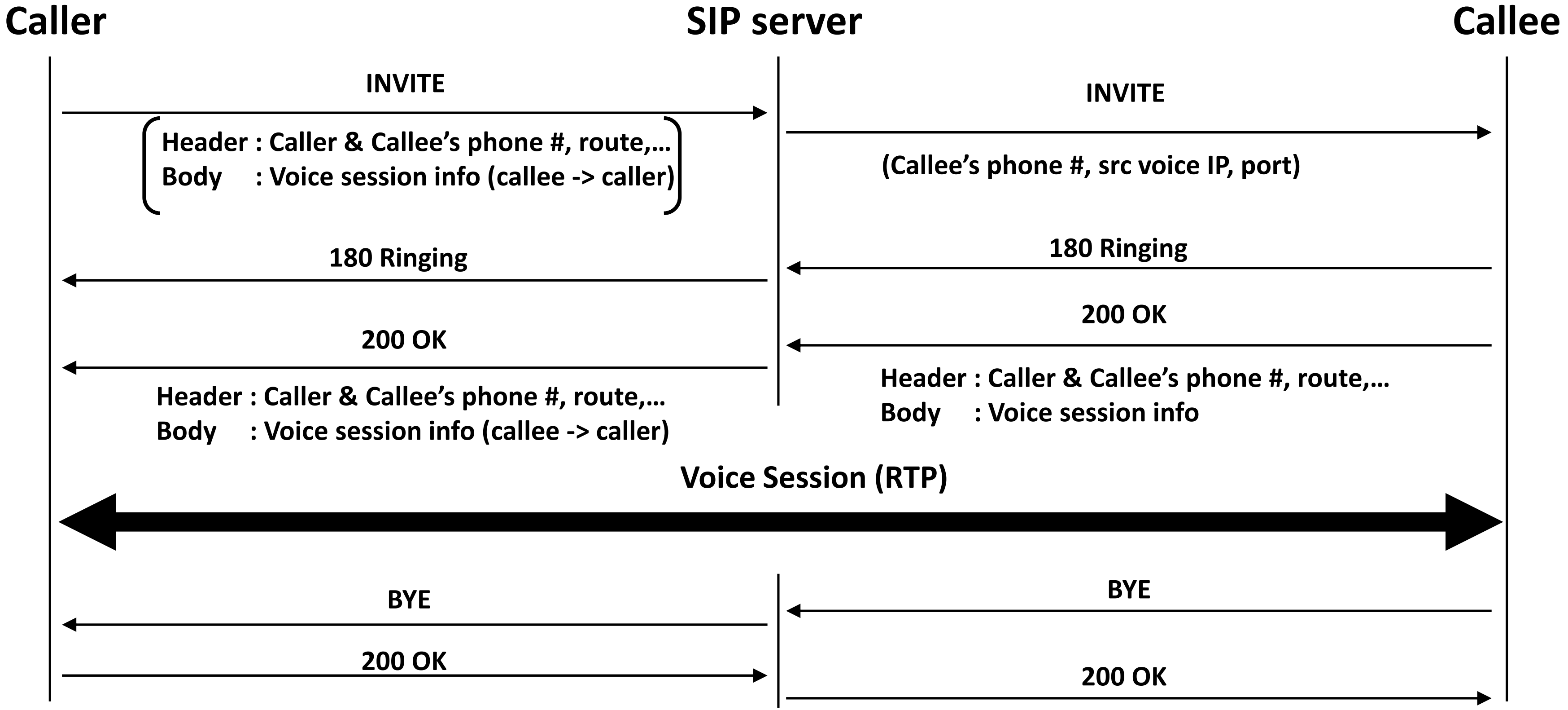
Accounting infrastructure

Implementation of LTE core

Complex Implementation of VoLTE



SIP Signaling Procedure



Caller

SIP server

Callee

INVITE

Header : Caller & Callee’s phone #, route,…
Body : Voice session info (callee -> caller)

INVITE

(Callee’s phone #, src voice IP, port)

180 Ringing

180 Ringing

200 OK

200 OK

Header : Caller & Callee’s phone #, route,…
Body : Voice session info

Header : Caller & Callee’s phone #, route,…
Body : Voice session info (callee -> caller)

Voice Session (RTP)

BYE

BYE

200 OK

200 OK

Results of Media Tunneling

- Media channel characteristics from the control plane messages

	US-1	US-2	KR-1	KR-2	KR-3
QoS Param. (Kbps)	38	49	41	41	49
Bandwidth (Kbps)	38/49	49	65	65	65
Latency (sec)	0.1	0.1	0.1	0.1	0.1
Loss rate (%)	1	1	1	1	1

- Actual measurement results (**trade-offs** between throughput and loss rate)

	US-1	US-2	KR-1	KR-2	KR-3
Throughput (Kbps)	37.90	36.93	45.76	39	50.48
Latency (sec)	0.52	0.02	0.10	0.32	0.30
Loss rate (%)	1.44	1.74	0.77	0.65	0.73

Proposed Attack Comparison

- **This paper**
  - **Free data channels**
    - SIP/Media tunneling
    - Direct communication
  - **Attacks from security problems**
    - Message manipulation
    - Wiretapping
    - Caller spoofing
    - DoS on core network
    - DoS on call
    - Overbilling

- **UCLA paper**
  - **Free data channels**
    - Free external/internal channels
  - **Attacks from security problems**
    - Overcharging attack
    - Data DoS attacks
    - Voice muted attack

Proposed Attack Comparison

- **This paper**
  - **Free data channels**
    - SIP/Media tunneling
    - Direct communication
  - **Attacks from security problems**
    - Message manipulation
    - Wiretapping
    - Caller spoofing
    - DoS on core network
    - DoS on call
    - Overbilling

- **UCLA paper**
  - **Free data channels**
    - Free external/internal channels
  - **Attacks from security problems**
    - Overcharging attack
    - Data DoS attacks
    - Voice muted attack

Proposed Attack Comparison

- **This paper**
  - **Free data channels**
    - SIP/Media tunneling
    - Direct communication
  - **Attacks from security problems**
    - Message manipulation
    - Wiretapping
    - Caller spoofing
    - DoS on core network
    - DoS on call
    - Overbilling

- **UCLA paper**
  - **Free data channels**
    - Free external/internal channels
  - **Attacks from security problems**

Focused on interface corss-over between VoLTE and Data interface

Proposed Attack Comparison

- This paper
  - **Free data channels**
    - SIP/Media tunneling
    - Direct communication
  - **Attacks from security problems**

Focused more on VoLTE and analyzed both protocol and implementation (including mobile OS, 3GPP spec)

- UCLA paper
  - **Free data channels**
    - Free external/internal channels
  - **Attacks from security problems**

Focused on interface corss-over between VoLTE and Data interface