Real Threats to Your Data Bills:

Security Loopholes and Defenses in Mobile Data Charging

Chunyi Peng

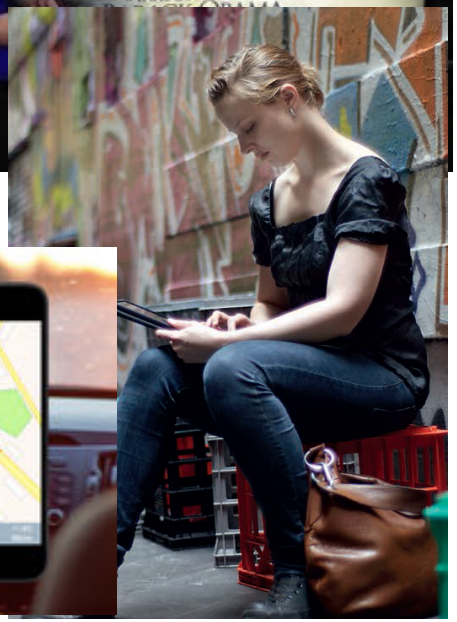
Chi-Yu Li, Hongyi Wang, Guan-Hua Tu, Songwu Lu

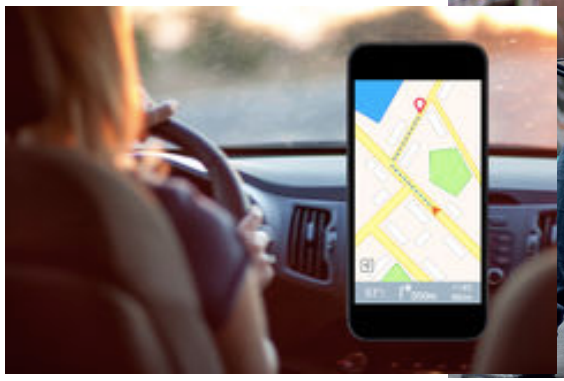
THE OHIO STATE UNIVERSITY

UCLA

Mobile Data Services, Everywhere

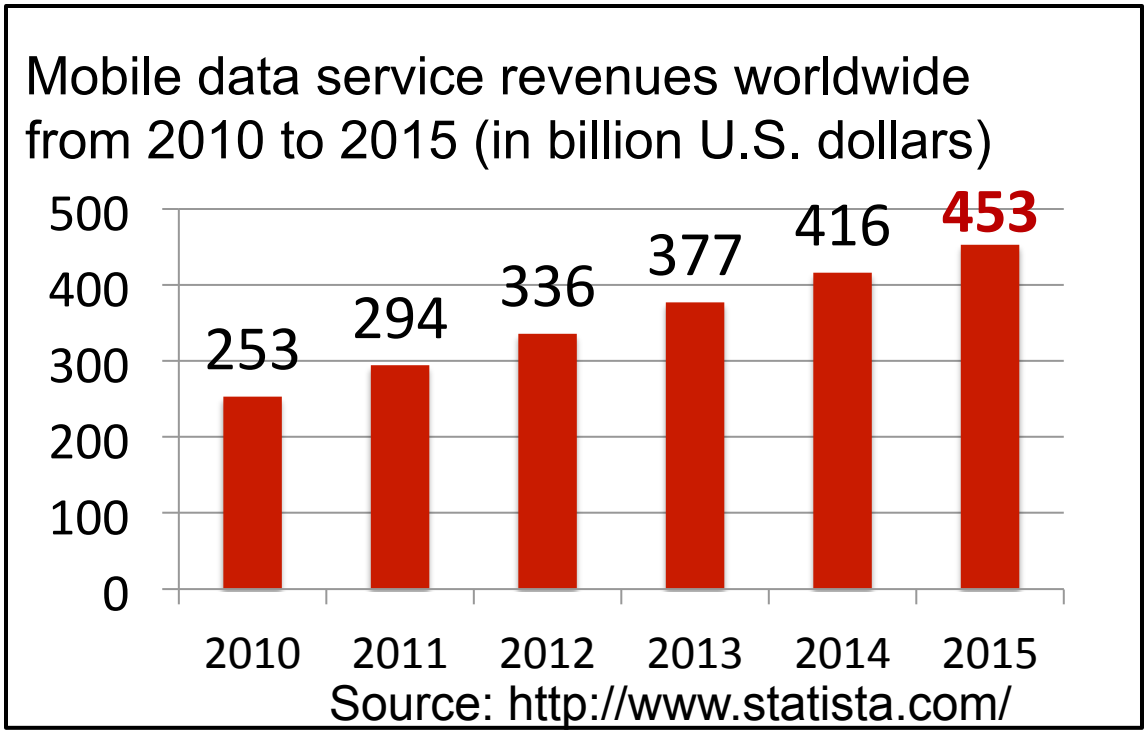
Images from Google search (online)





Certainly, No Free Lunch

- Mobile data bills: pay for usage
- Essential to carriers and users
  - $400-500B revenue
  - Monetary rights of billions of users



6.8+ billion subscribers

Volume-based Mobile Data Charging

- Various data plans
  - Volume-capped, e.g., $20/300MB
  - Per-use, e.g., $0.0195/KB for roaming
  - …
  - Single line or shared plans
  - Prepaid or postpaid
  - …
- The core: charged by **usage volume**

Are our data bills CORRECT?

We pay for what we use;

We do not pay for what we do not use.

Overcharges and Undercharges [CCS'12]

*Flaws in Mobile Networks Allow Users to **Surf the Internet for Free** (via DNS tunneling)*

(Fixed)

technology review

Published by MIT

English | en Español | auf Deutsch | in Italiano | 中文 | in In

HOME COMPUTING WEB COMMUNICATIONS

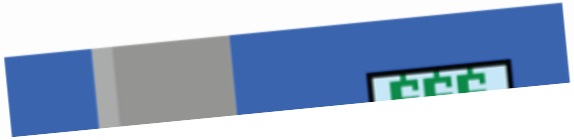
NEWS // COMMUNICATIONS

How Your Wireless (
You

Bad coverage and streaming video c
for data you never receive.

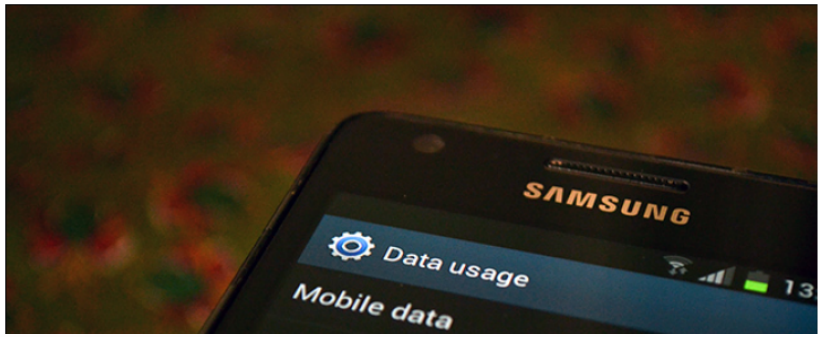
1 comment

TOM SIMONITE
Thursday, September 13, 2012



Your carrier may be charging you for data you didn't receive

By Aaron Souppouris (http://www.theverge.com/users/AaronSoup) on September 20, 2012 08:15 am Email (mailto:aaron@theverge.com) @AaronIsSocial (https://twitter.com/intent/user?screen_name=AaronIsSocial)



When your wireless carrier charges you for the amount of data you used on your cell

Now, are they CORRECT?

This Talk

- Real threats to mobile data bills
  - Free uplink data access at other's cost
  - Overcharges while victims do nothing
    - In a much more covet way
  - No sophisticated attacks needed: readily launched
- Security breach against Authentication, Authorization and Accounting (AAA)
  - How they work?
  - How they fail?
- Defense solutions

Three Requirements

- Mobile data charging: collect how much data is actually used by whom at his/her consent

Authentication	Authorization	Accounting
The user being billed = Who transfers data.	The user agrees to use data and pay it.	Volume should be accurate.

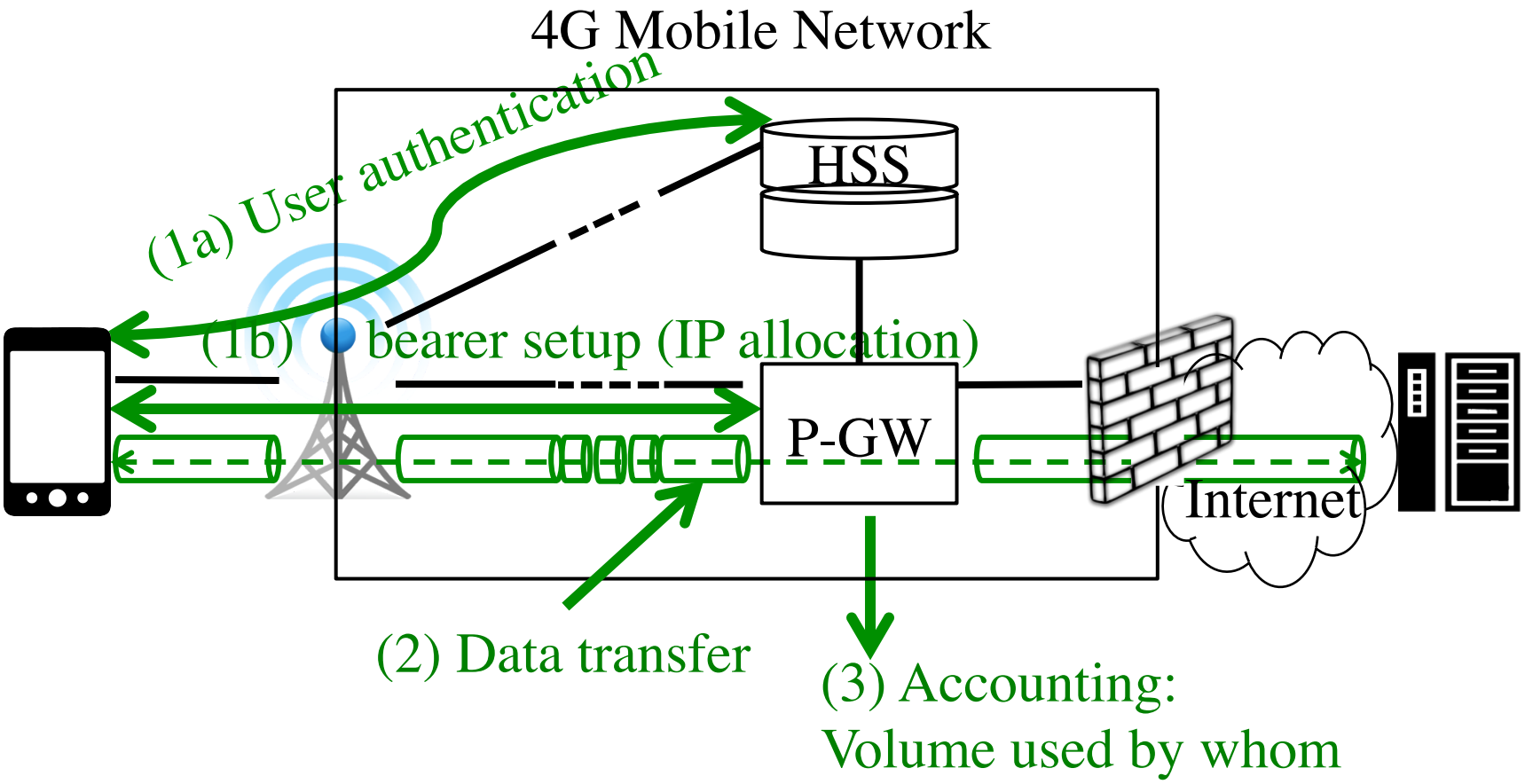


Attack Model

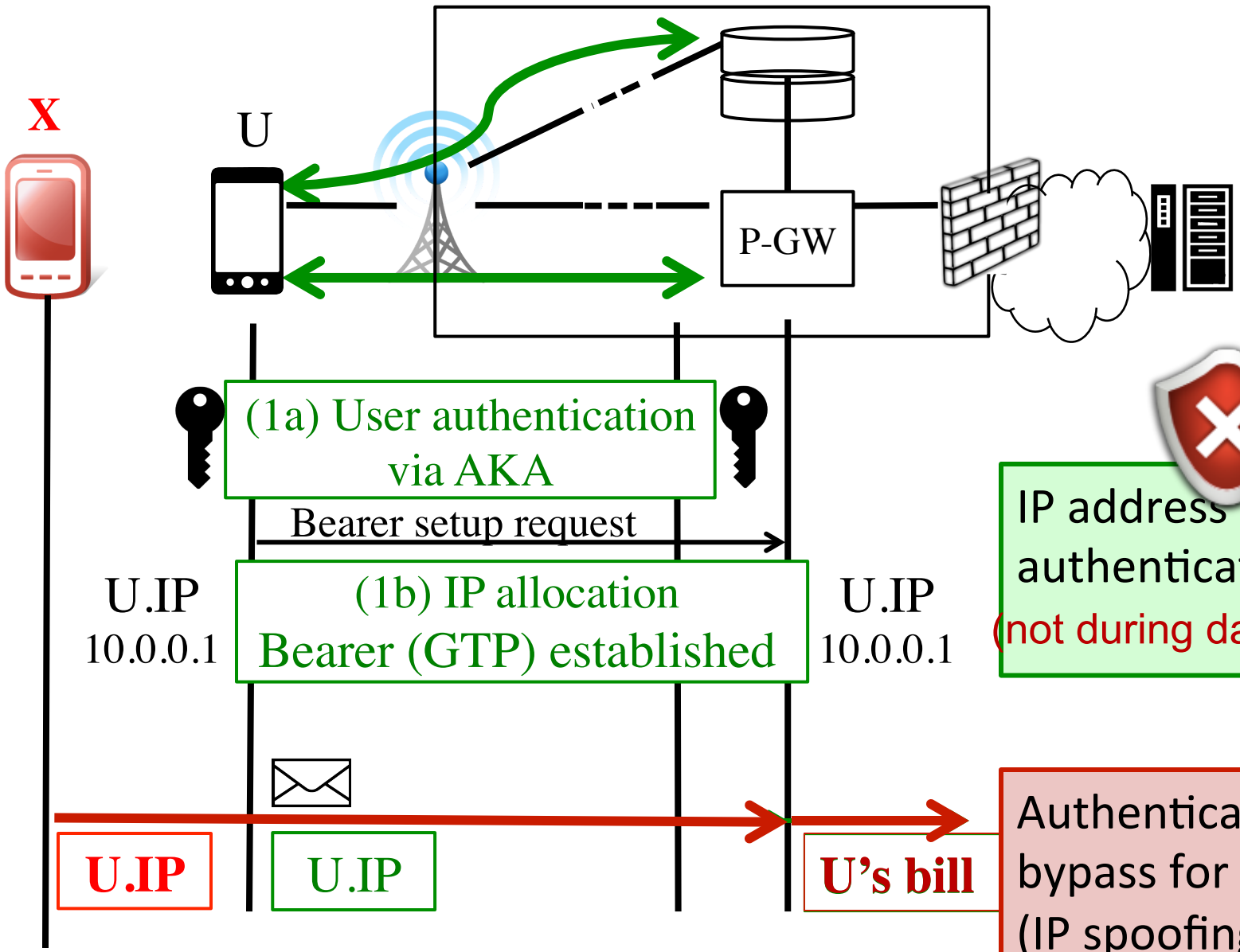
- No extra capability needed at the attacker
  - No comprise or access to operator networks
  - No malware or remote access to victim phones
  - Commodity phone and server (optional)
    - E.g, an rooted Android phone

- All proof-of-concept attacks ready to launch NOW
  - Responsible: victims = our own phones

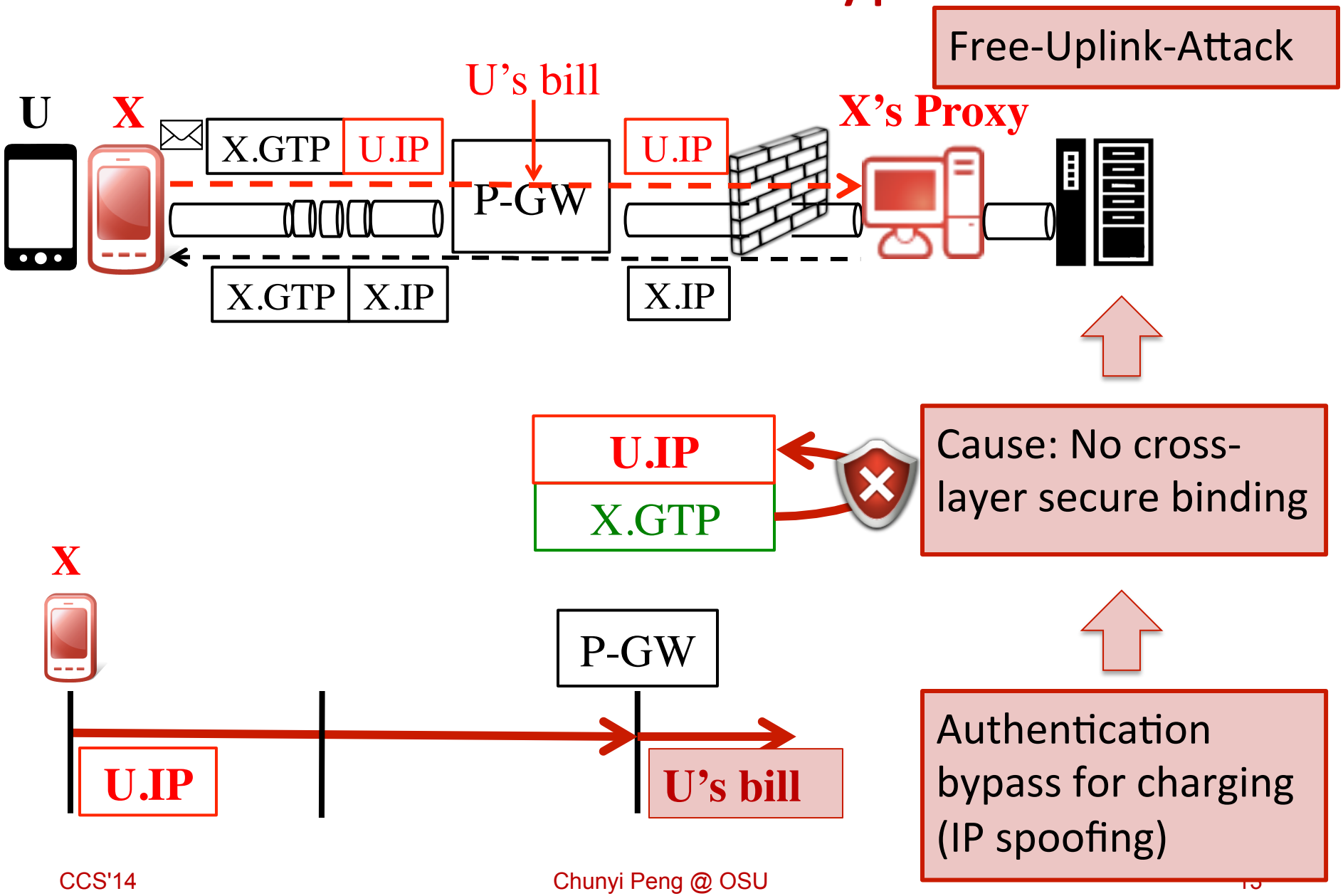
Current Mobile Data Charging



Authentication



Authentication Bypass



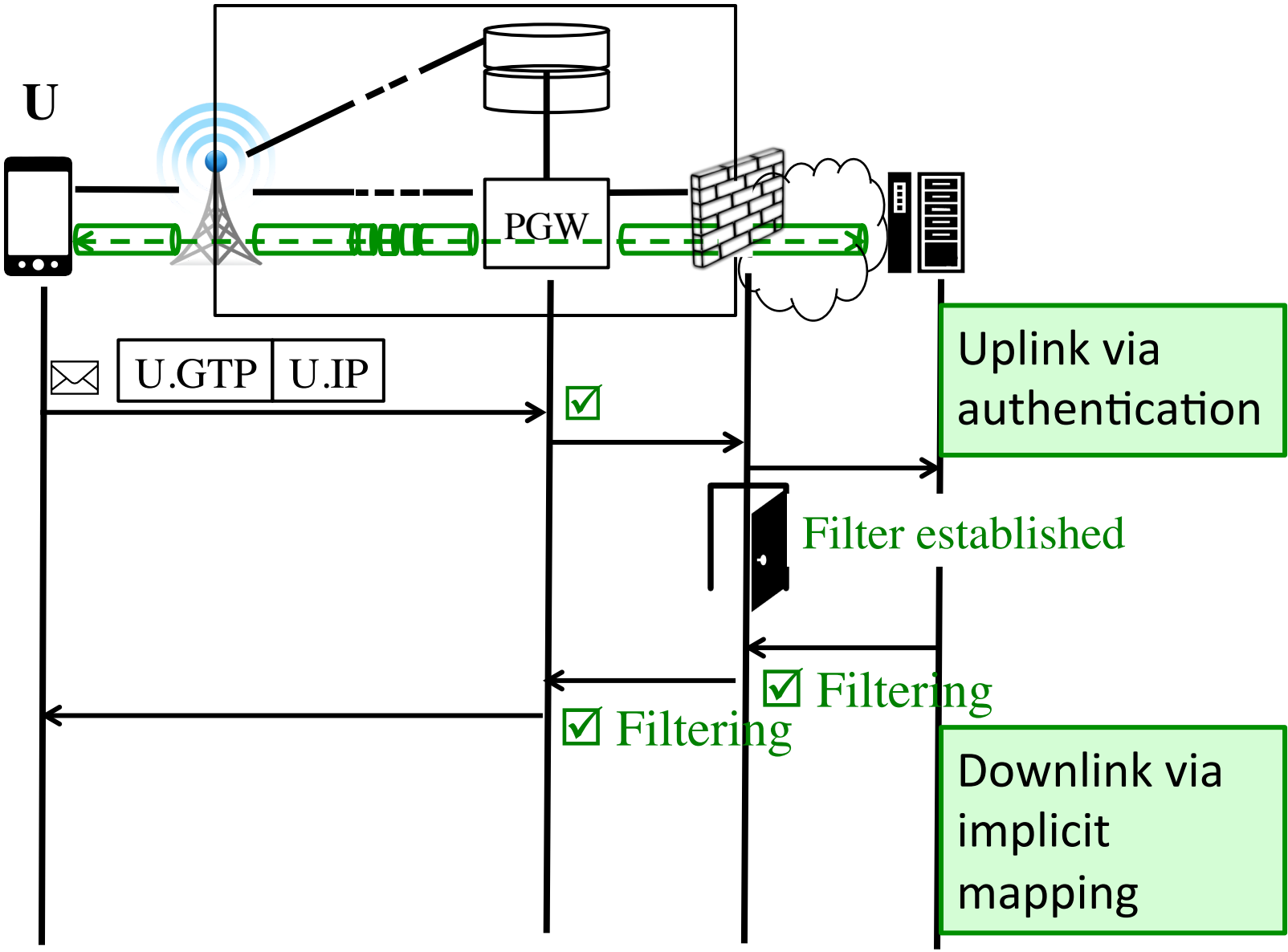
In Real Networks

- Two US carriers: OP-1 and OP-2

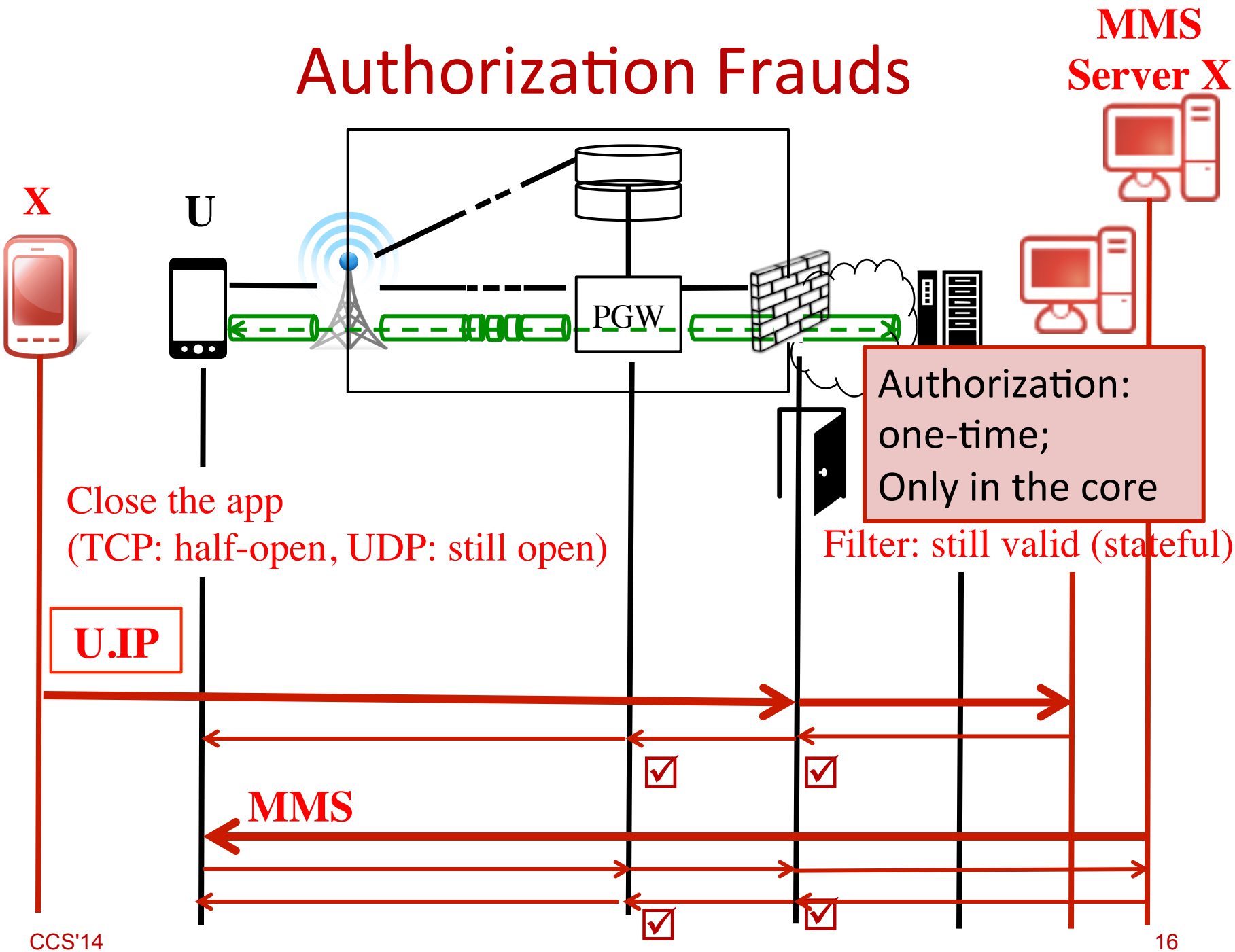
	OP-1	OP-2
IP spoofing is feasible	**Yes**	**Yes**
Free-uplink-attack is viable	**Yes**	**No**
Maximum spoofing MSB	24 (all)	32 (all)
Fully spoofable?	No OP-1: fewer spoofable addresses	

- More findings: 4G/3G/2G, geo locations

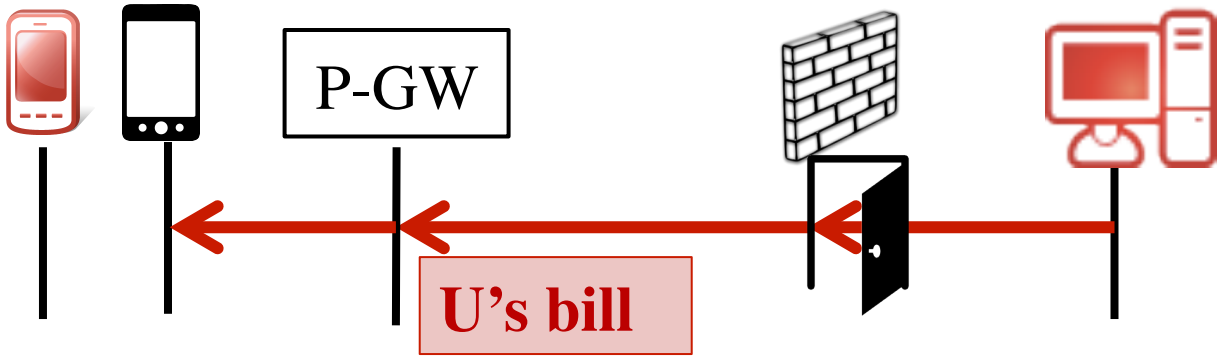
Authorization



Authorization Frauds



Authorization Frauds



No proper authorization for downlink traffic

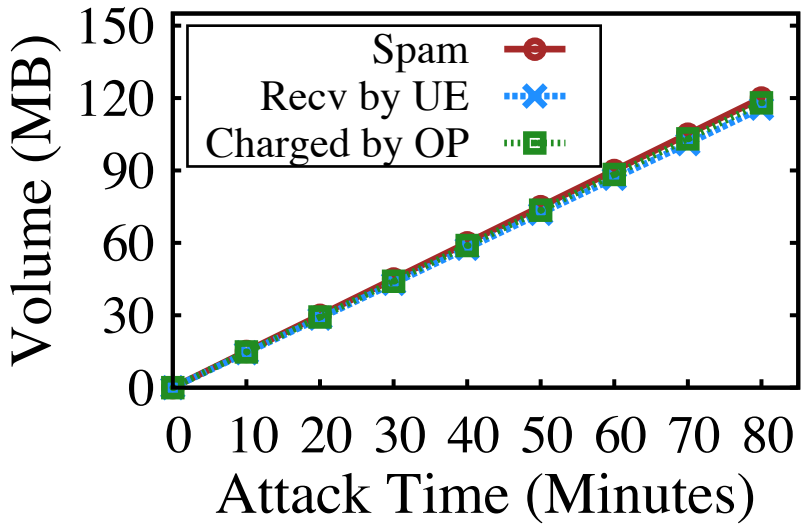
Causes:
Network-based authorization;
IP-push model

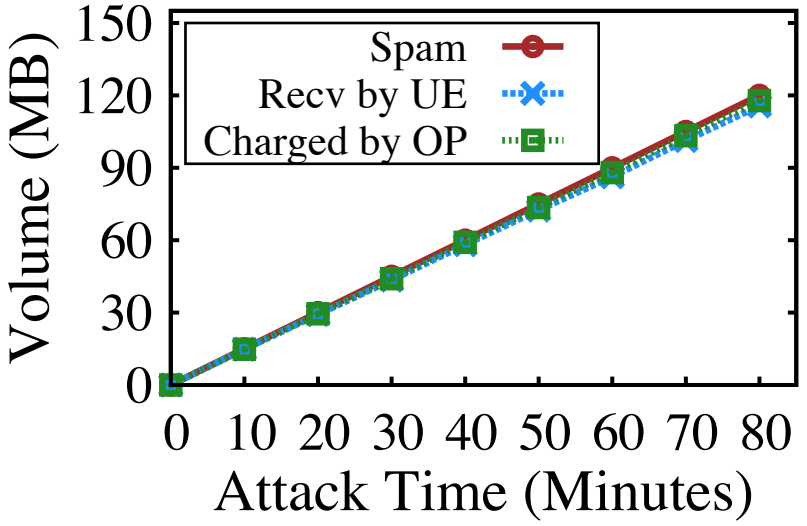
Cloak-and-dagger attacks:
- via MMS
- via IP Spoofing

More covet and threatening:
Nothing done at the victim

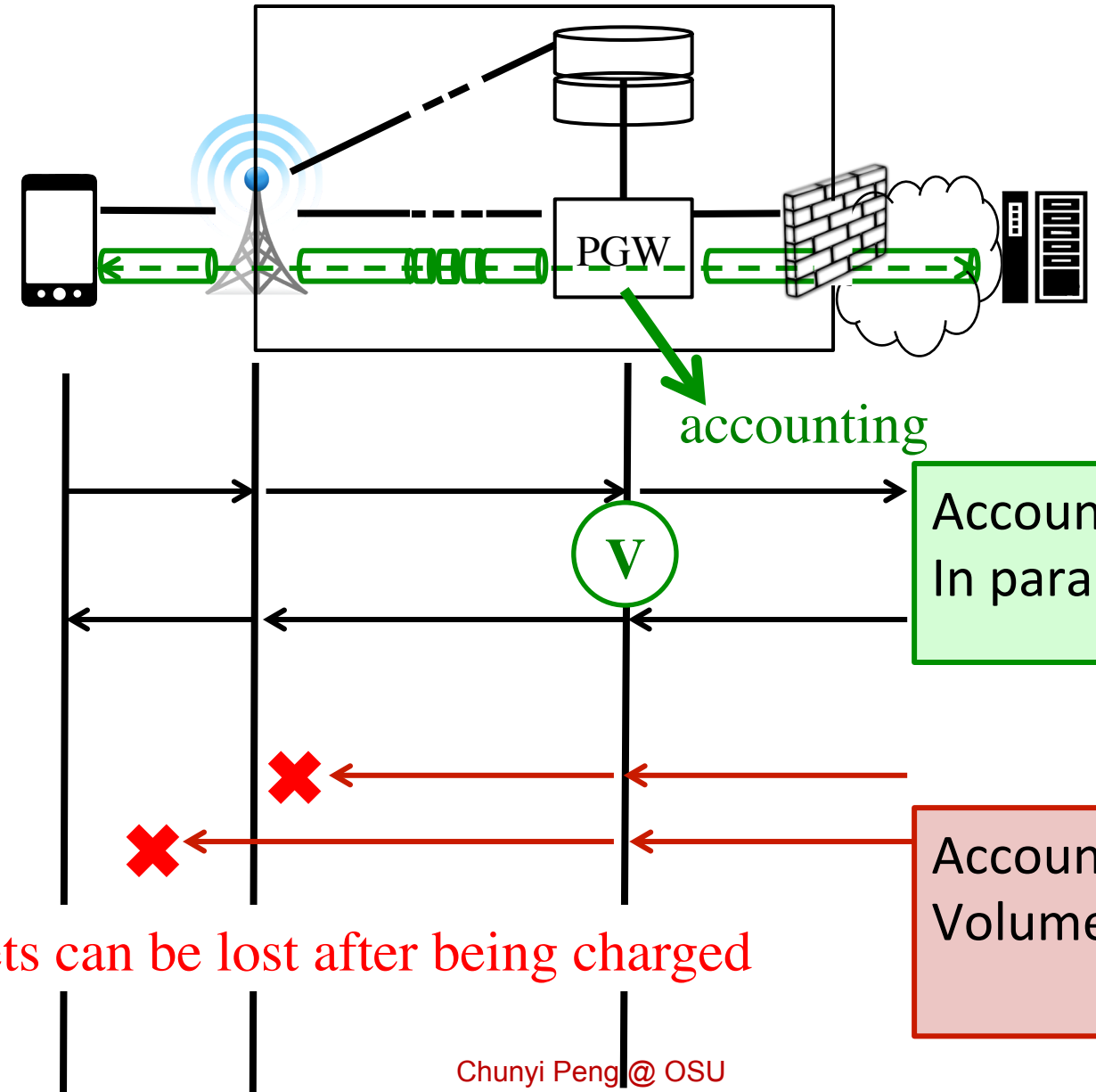
In Real Networks

- US-1: via IP spoofing
- US-2: via MMS
- Attacks (overcharge)
  - Last 80 minutes (no sign of limit)
  - ~ 120MB charged (no sign of limit)

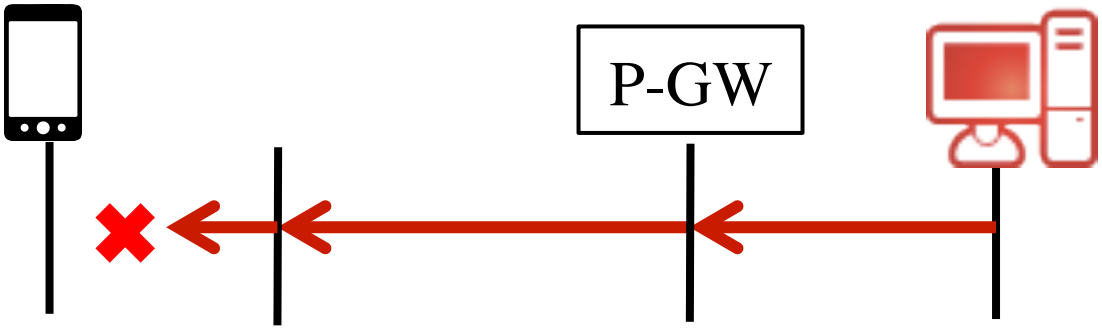




Accounting


PGW
accounting
V
Accounting:
In parallel with data
Accounting:
Volume = local view
@ P-GW
Packets can be lost after being charged

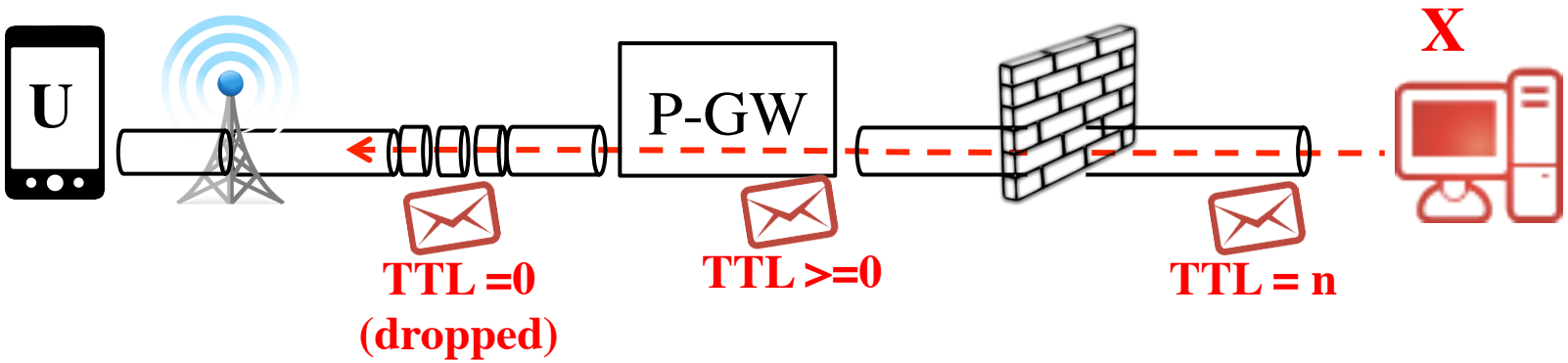
Accounting Inflation



Causes:
(1) Open-loop accounting arch.
(2) Independent packet delivery

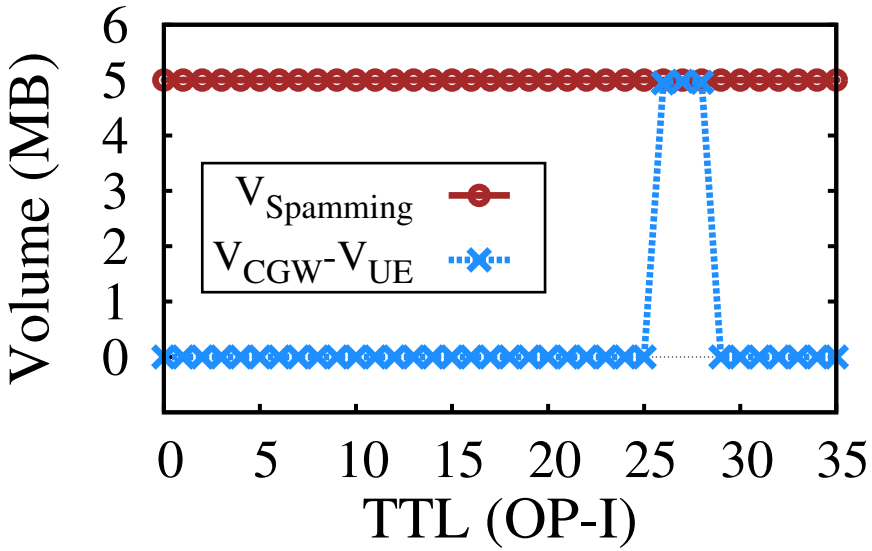
More covet:
no data received at victim

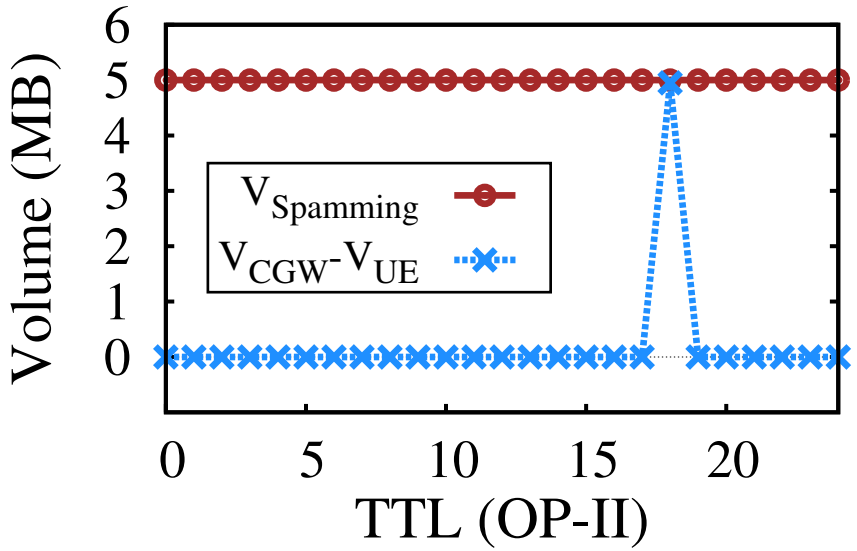
Hit-but-no-touch Attack via TTL



In Real Networks

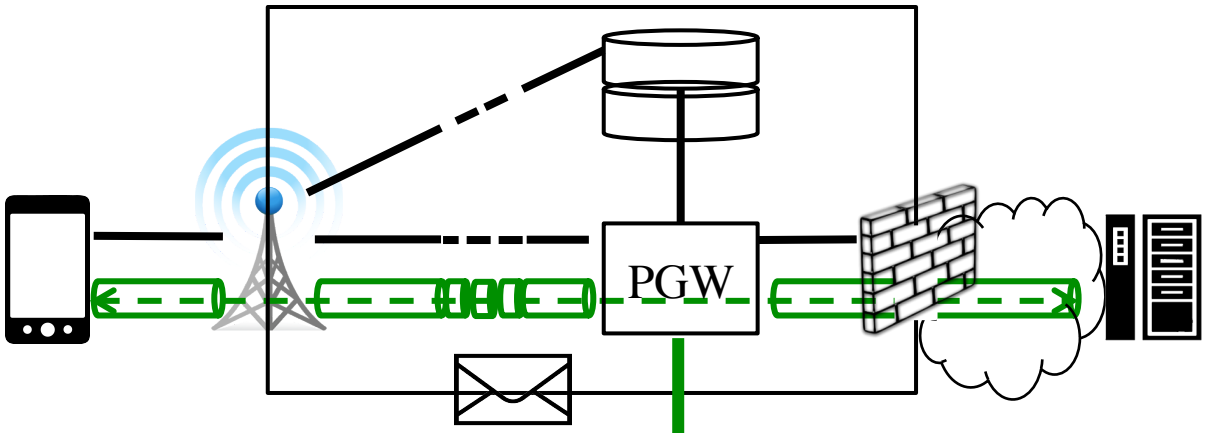
- US-1 and US-2 both suffer
  - US-1: TTL = 26, 27, 28
  - US-2: TTL = 18





How to defend?

Key Issues



Packet: source and destination

Charging: who is authenticated entity? (control plane vs. data plane)

Packet: connectionless, no state

Charging: what is the state of connection packets serves (@phone vs. @network)

Packet: independent over hops

Charging: Is it delivered? (at the end vs. in the middle)

Basic Ideas

Authentication	Authorization	Accounting
The user being billed = Who transfers data.	The user agrees to use data and pay it.	Volume should be accurate.

Loopholes

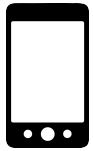
Authen. bypass (No secure binding)	Authorization frauds (No deauthorization)	Account. inaccuracy (Local view @core)

Proposed defense

Cross-layer secure binding in data plane	Explicit de-authorization in the control plane	Feedback from end/ network + de-authorization

Defense Framework

- Standard compatible



P-GW

Authenticated, Verified ID

Secure Binding

Runtime Access Control

Fraud Detector → Always implcit (de) author.

Explicit de-authorization

Accounting Correction

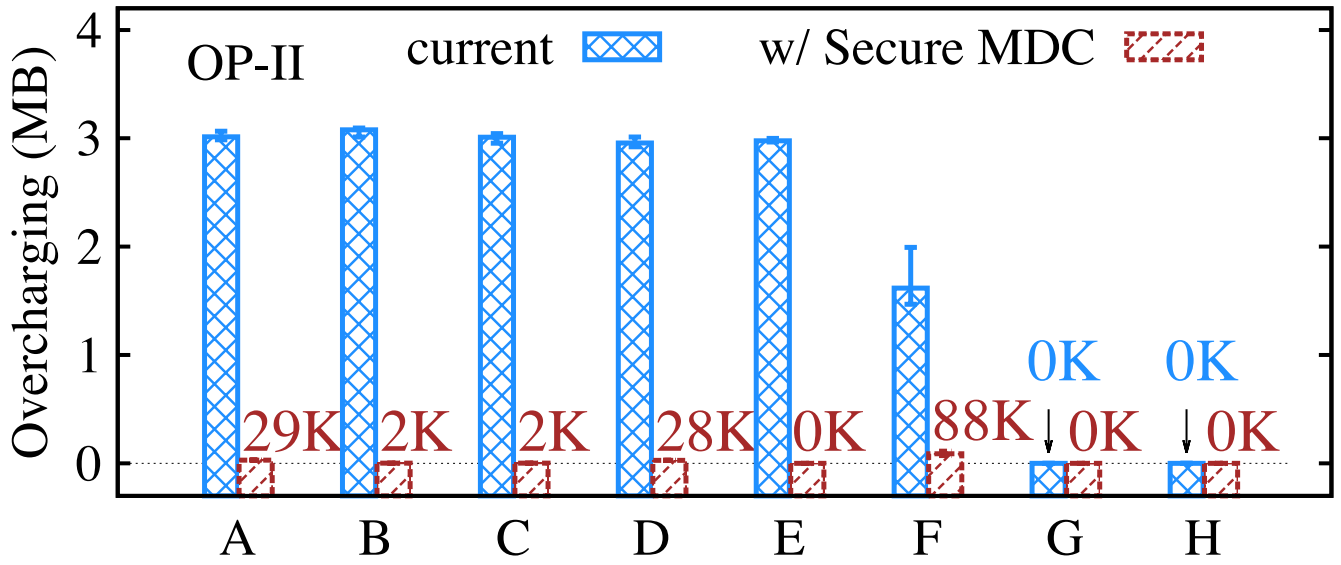
Event Alerter

Event Alerter & Volume Corrector

Mischarging Handler

Prototype and Evaluation

- Gateway = PC (out of carrier network)
- Test: all except secure binding
  - All attacks + other attacks in [CCS'12, NDSS'14]
- Results: effective



Latest Update

- Positive response from US carriers
  - All these vulnerabilities are verified officially
- Work with US carriers to fix the issues
  - Nationwide upgrade (Nov 2014)
  - Initial fix in place

Summary

- Systematic security analysis of AAA for mobile data charging
- Uncover vulnerabilities and real threats
  - No sophisticated attacks needed
- Simple and effective defense proposed
- Immediate upgrade in carrier networks