# MOBILE DATA CHARGING:

# NEW ATTACKS AND COUNTERMEASURES

Chunyi Peng,

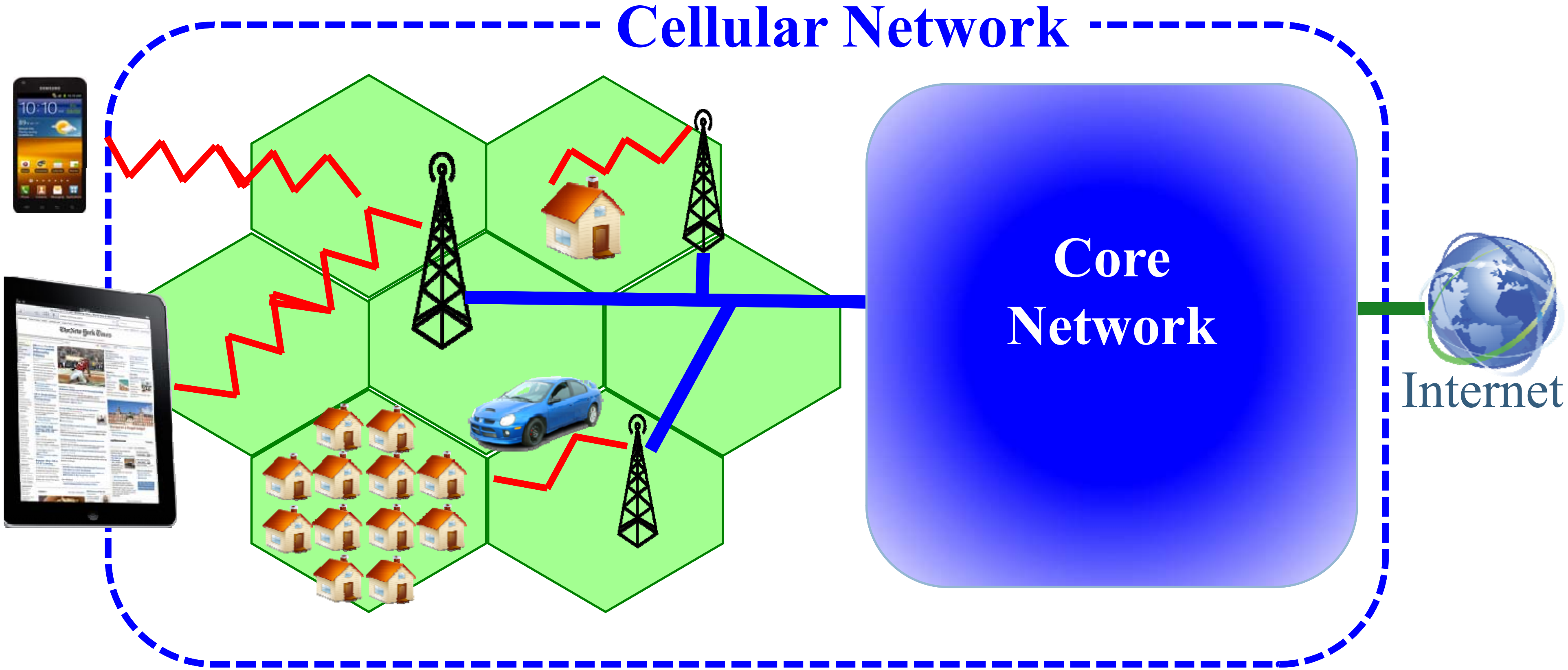
Chi-Yu Li, Guan-Hua Tu, Songwu Lu, Lixia Zhang

University of California, Los Angeles

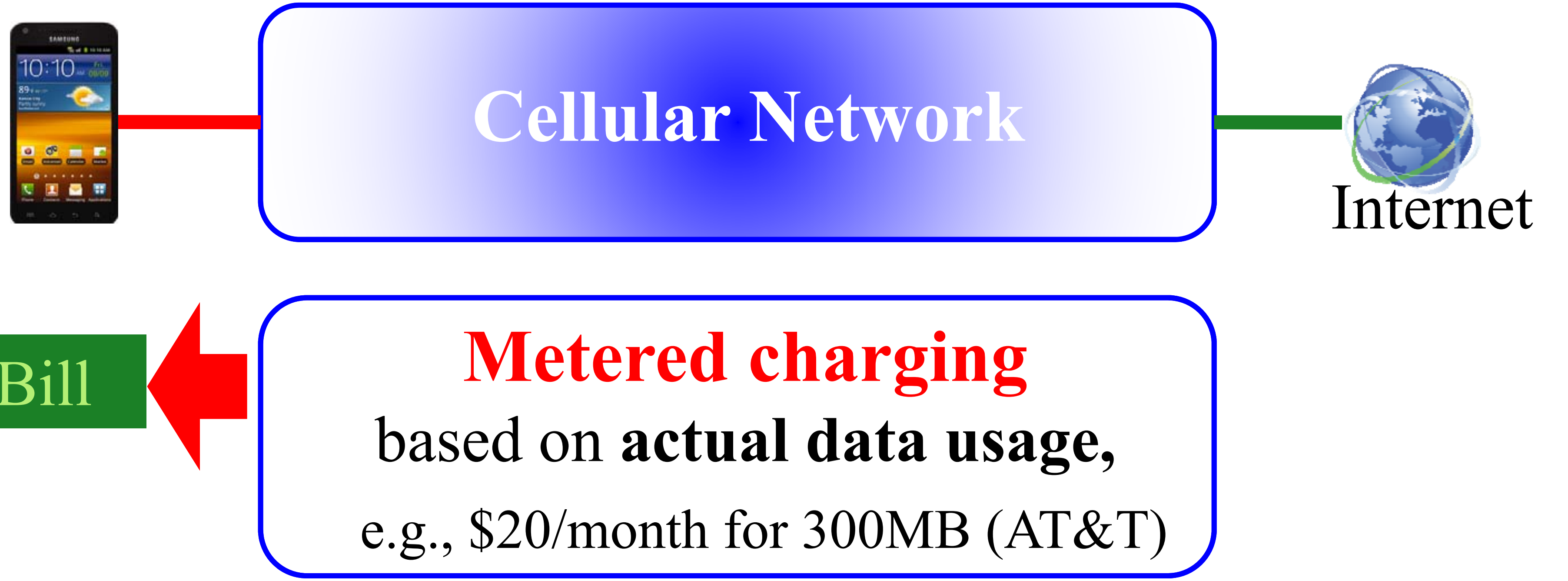
ACM CCS'12

# Mobile Data Access

- **1.2 billion** global users



# Mobile Data Charging



Cellular Network

Internet

Bill

**Metered charging**

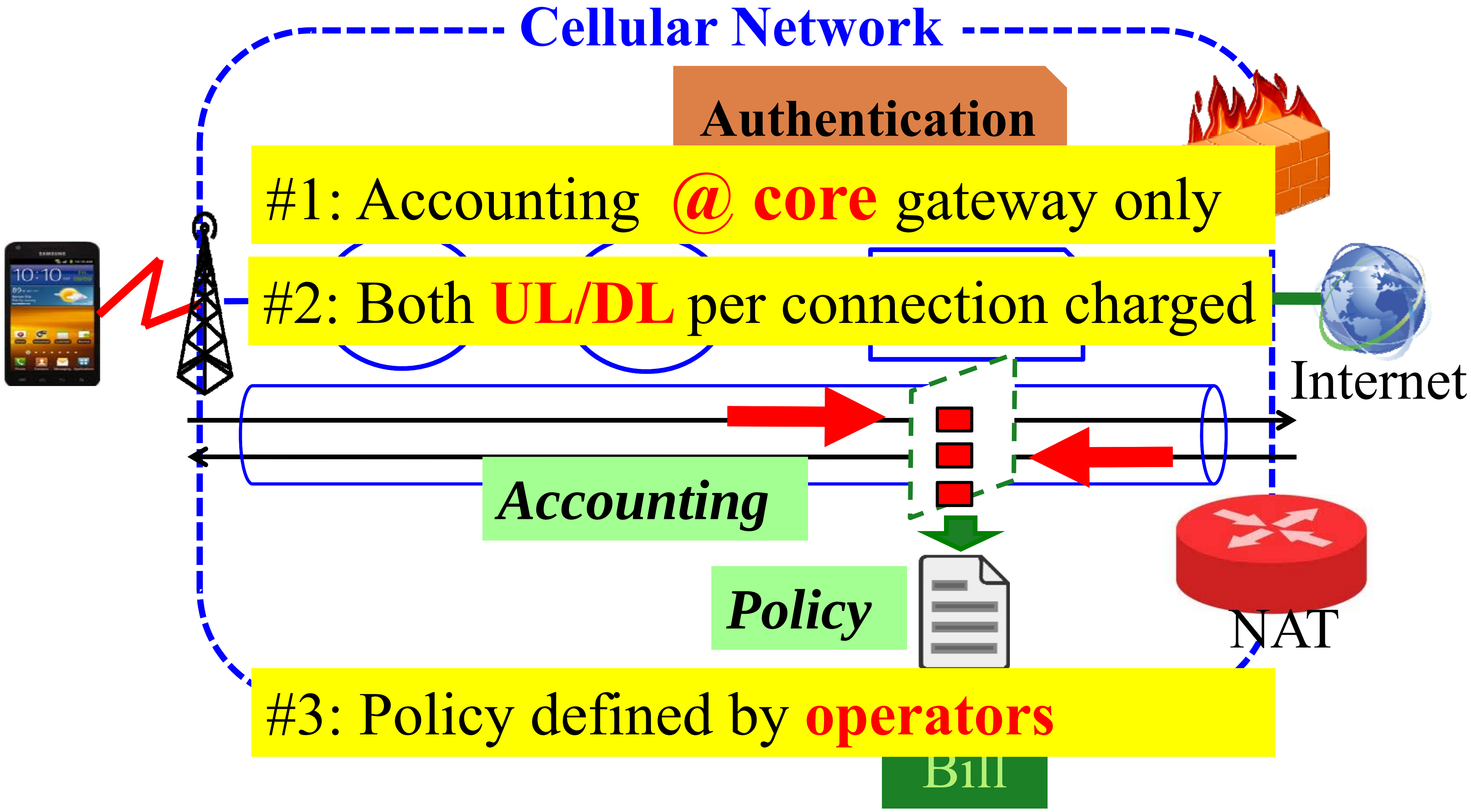
based on **actual data usage,**

e.g., $20/month for 300MB (AT&T)

**Security:**

Can any attack make the users pay **MORE/LESS**?

# How Charging Works & Be Secured

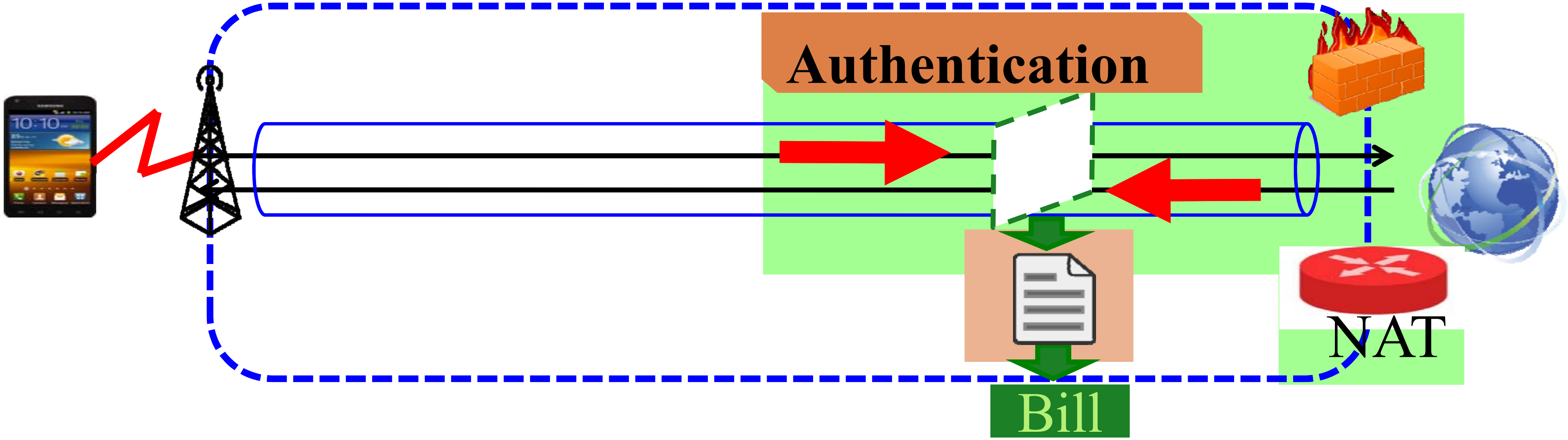


#1: Accounting @ **core** gateway only

#2: Both **UL/DL** per connection charged

#3: Policy defined by **operators**

# Two Security Issues



#1: Can the attacker **bypass the security mechanism** to **exploi**

**Stealth-spam-attack**

the users pay **MORE**?

#2: Can th

**Toll-Free-Data-Access-Attack**

**LESS**?

# Threat Models

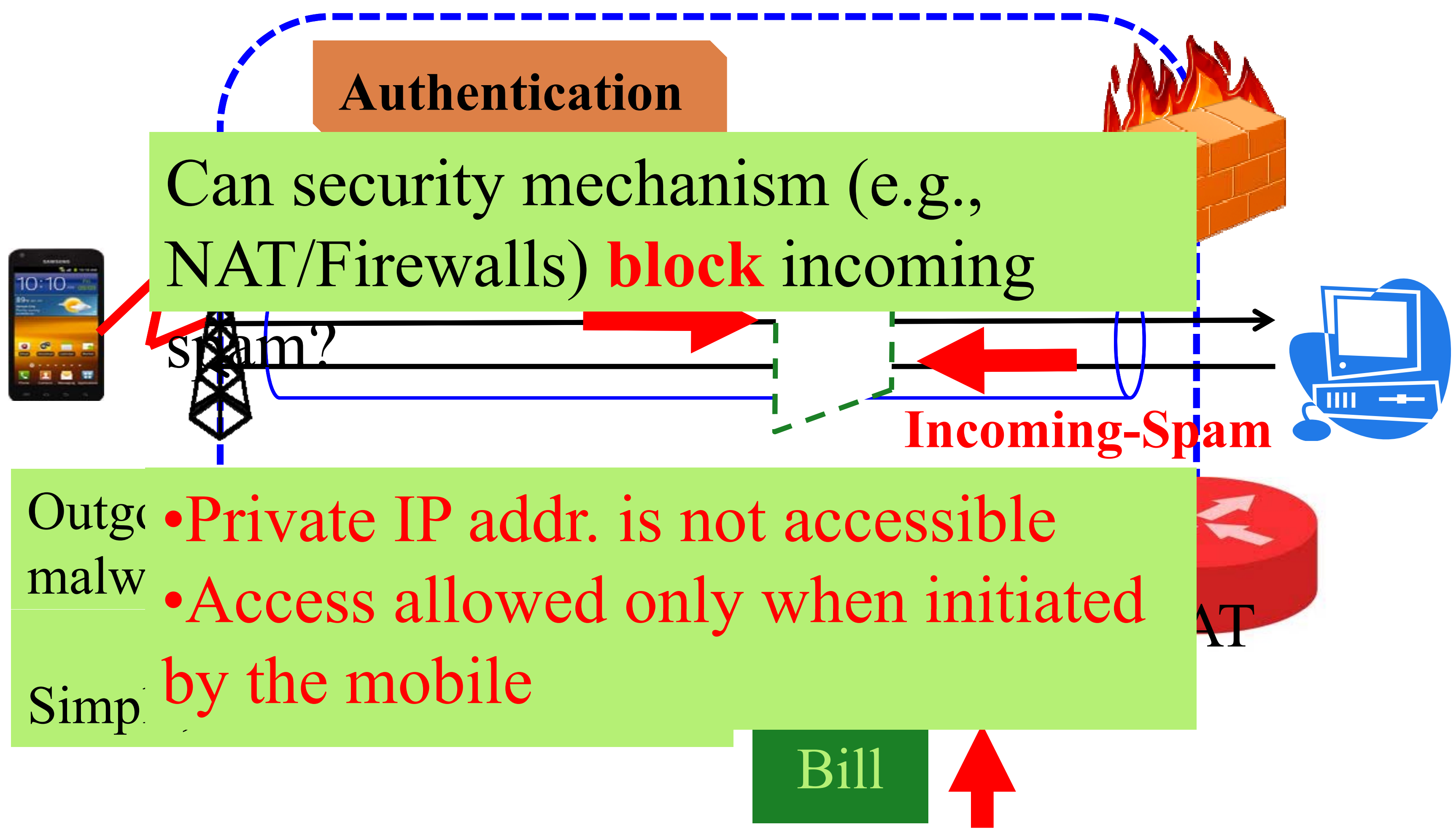
- Cellular network is **not compromised**
  - Charging subsystem works as designed
  - Security mechanism works as designed
- Attacker's capability
  - Only use **installed apps** @ mobile, or
  - Deploy malicious servers **outside cellular networks**

# Outline

- Stealth-spam-attack (pay MORE)
  - Vulnerability
  - Attack design & implementation & damage
  - Countermeasures & insight
- Toll-free-data-access-attack (pay LESS)
  - Vulnerability
  - Attack design & implementation & damage
  - Countermeasures & insight
- Summary

# Stealth-Spam-Attack

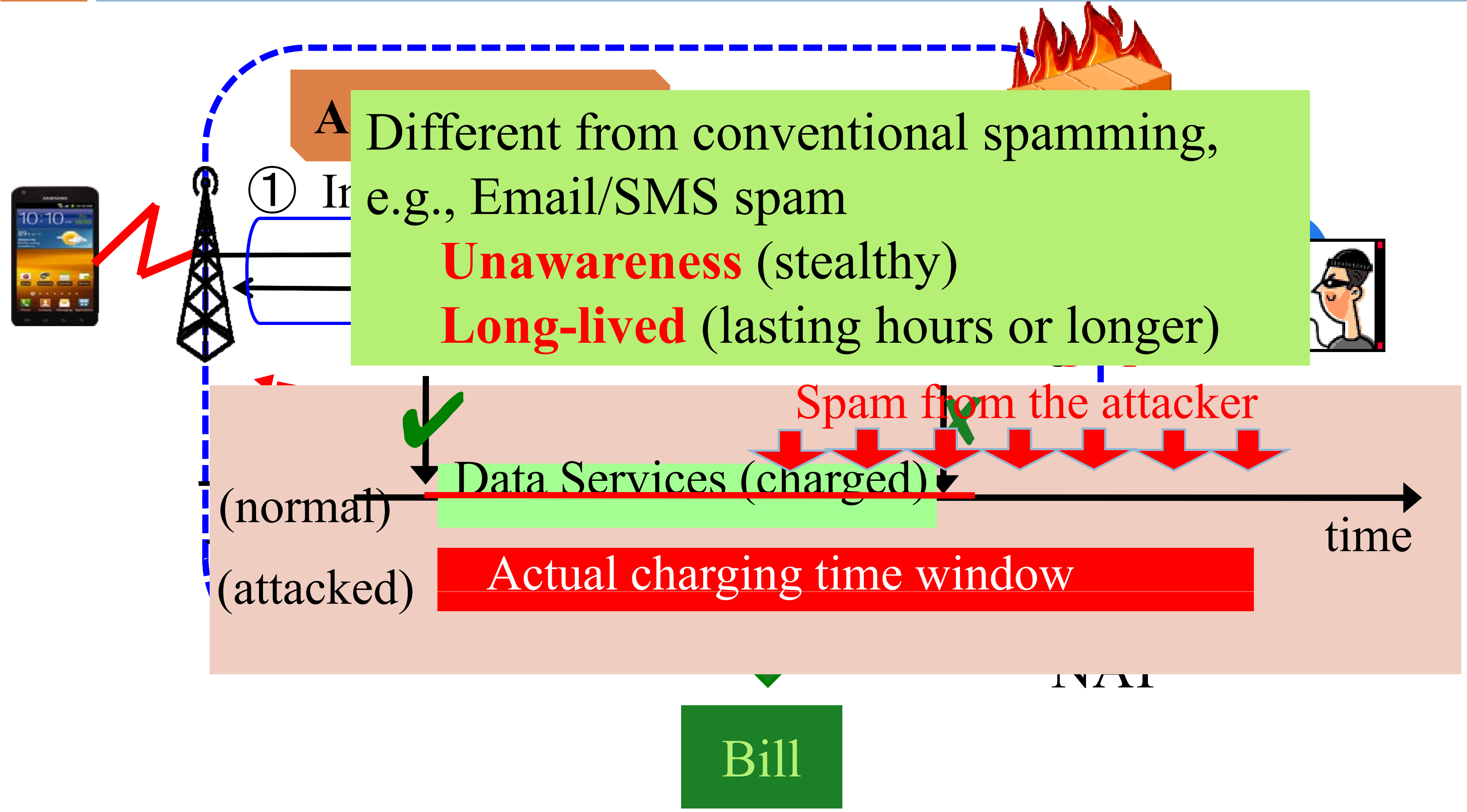
# Security Against Spamming



Can security mechanism (e.g., NAT/Firewalls) **block** incoming spam?

- Private IP addr. is not accessible
- Access allowed only when initiated by the mobile

# Vulnerability



Different from conventional spamming, e.g., Email/SMS spam

- **Unawareness** (stealthy)
- **Long-lived** (lasting hours or longer)

Actual charging time window

# Stealth-Spam-Attack

- Step1-**Trap:** init data access
  - Example-1: click a malicious web link
  - Example-2: login Skype once / stay online
- Step2-**Spam:** keep spamming
  - No matter what status @mobile

# Web-based Attack

- Implementation
  - Phone: click a malicious web link
  - Attacker (server): send spam data at constant rate (disable TCP congest control and tear-down)

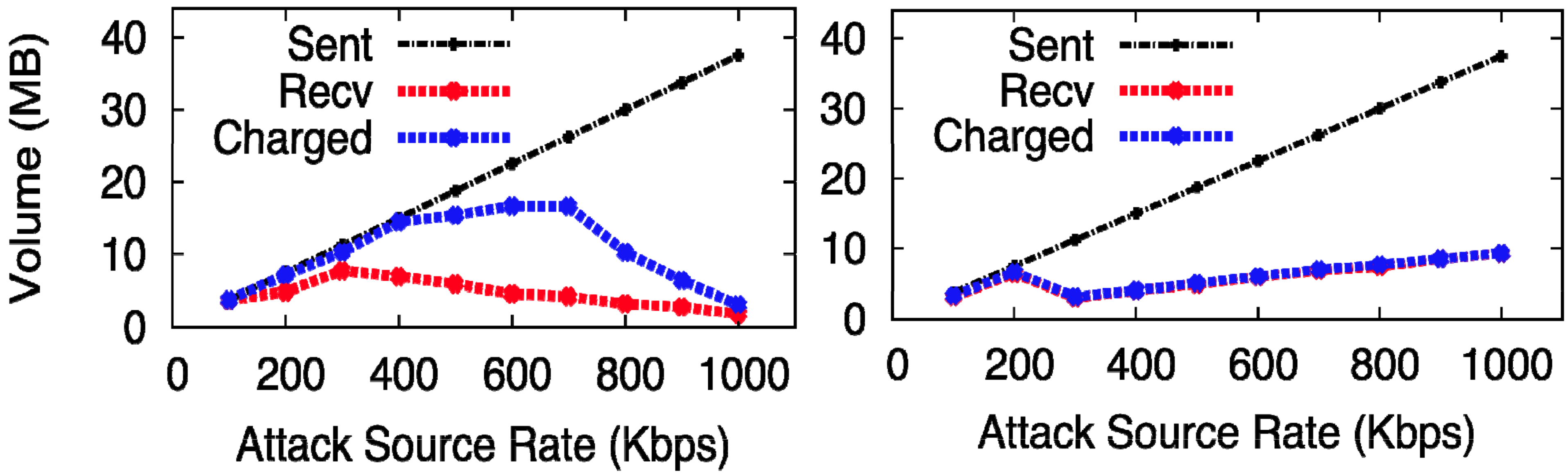
- Result: charging keeps going
  - Even after the phone tears down TCP
    - TCP FIN, timeout
  - Even when many “TCP RESET” sent from the mobile

# Damage vs. Spamming Rate

Charging volume vs. spamming rate

Operator-I

Operator-II



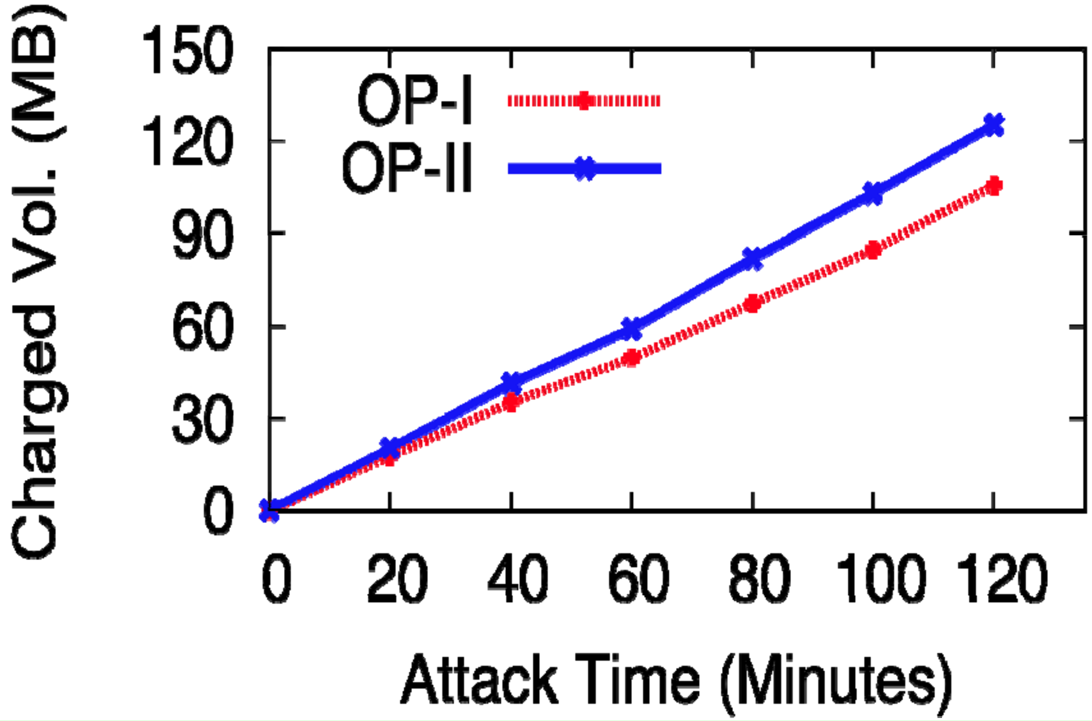
**In proportion to spamming rate** when rate is low

**Charging blocked** when rate is high (> 1Mbps)

The charged volume could be **>** the received one [Mobicom’12]

# Damage vs. Duration

Spamming rate = 150Kbps

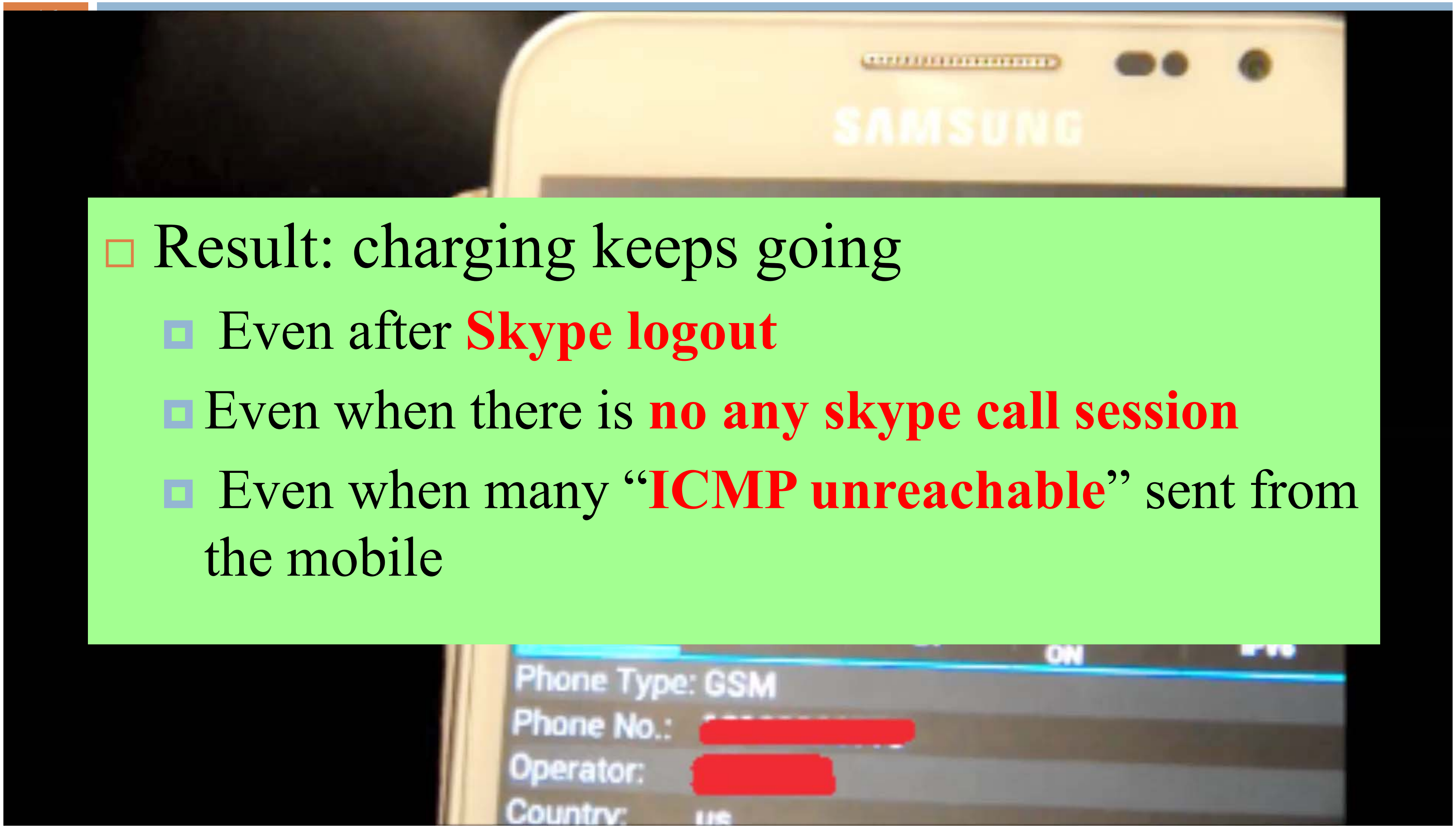


**No observed sign to end** when the attack lasts **2 hours** if the rate is low (**spamming> 120MB**)

# Skype-based Attack

- Implementation
  - **Phone: do nothing (stay online once in Skype)**
  - **Attacker: Skype call the victim and hang up**
  - Attacker (server): send spam data at constant rate
- Exploit Skype "loophole"
  - allows data access from the host who attempts to call the victim before the attempt is accepted
- Demo

# Demo: for a specific victim



- Result: charging keeps going
  - Even after **Skype logout**
  - Even when there is **no any skype call session**
  - Even when many "**ICMP unreachable**" sent from the mobile

Phone Type: GSM

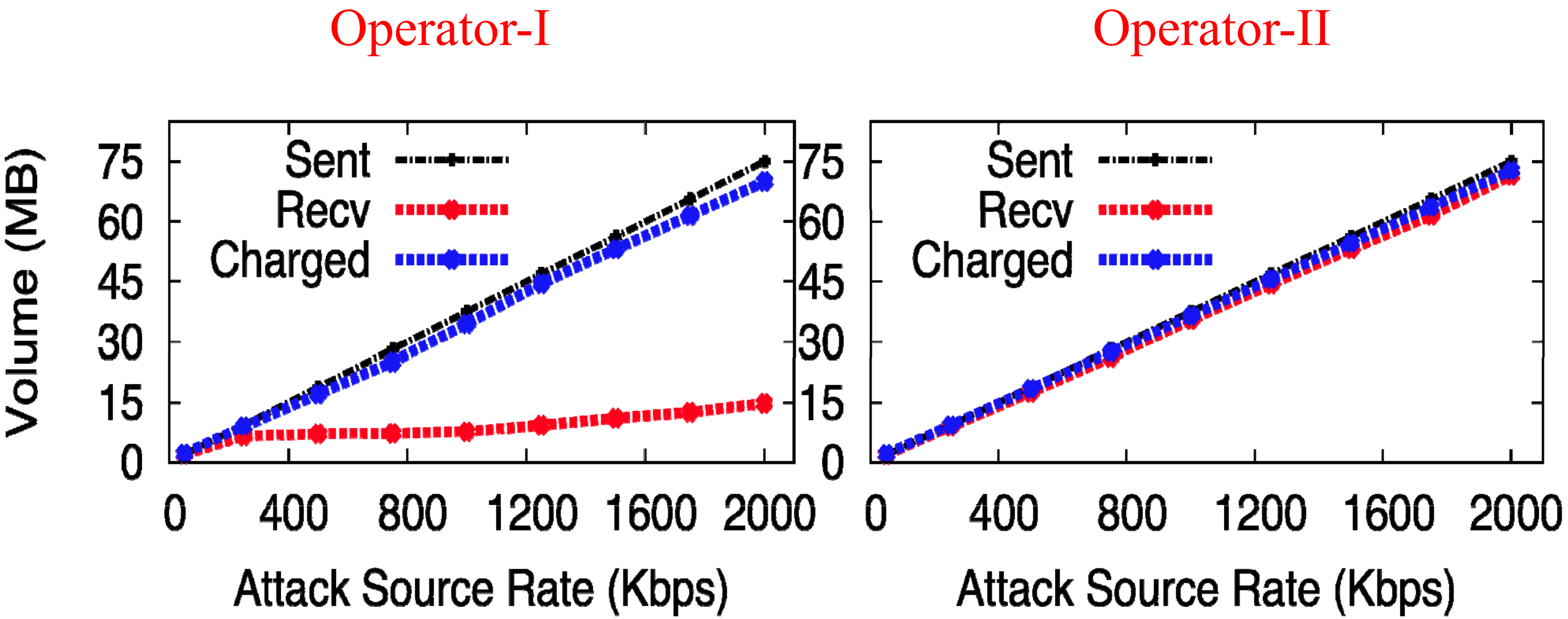
Phone No.: [redacted]

Operator: [redacted]

Country: us

# Damage vs. Spamming Rate

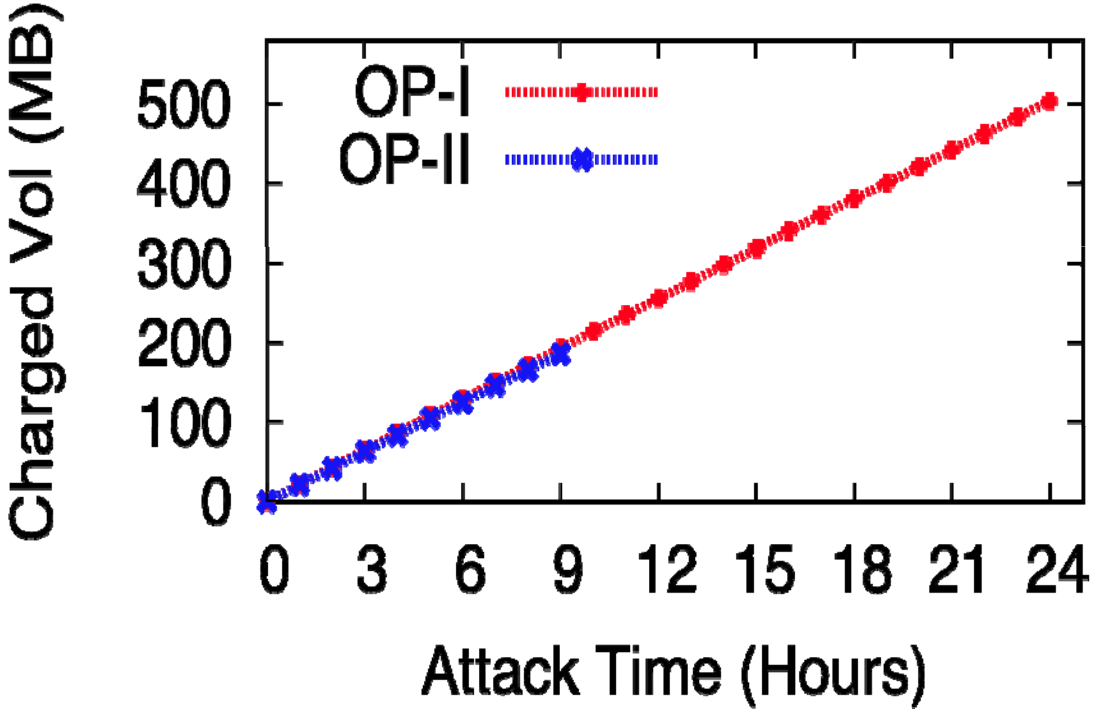
Charging volume vs. spamming rate



**No bounds on spamming rate** compared with TCP-based attack

# Damage vs. Duration

Spamming rate = 50Kbps



**No observed sign to end** when the attack lasts **24 hours** (**spamming > 500MB**)

# Root Cause

**Current system:**
Secure **only the initialization**

IP forwarding can **push packets** to the victim **(not controlled by the victim)**

#1: **Initial authentication** ≠ authentication **all along**

**Current system:**
**Keep charging** if data comes
Local view @ core gateway

Different views @ mobile:
data conn. ends or never starts or exception happens
Lack of feedback/control

#2: Data flow termination @ the phone
≠ **charging termination @** the operator

# Countermeasures

- Spamming inevitable due to IP push model

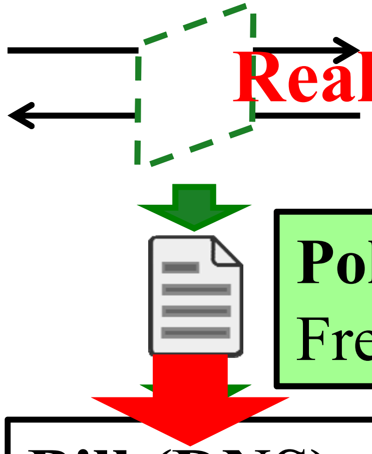
- Remedy: stop early when spamming happens
  - Detection of unwanted traffic @mobile/operator
  - Feedback (esp. from the mobile to the operator)
    - At least allow users to stop data charging (no service)
    - Exploit/design mechanisms in cellular networks: *implicit-block, explicit-allow, explicit-stop*

  - Precaution, e.g., set a volume limit
    - Application: be aware of spamming attack

# Toll-Free-Data-Access-Attack

# Vulnerability

**Both** operators provide **free DNS** service



**Real data over 53**

DNS packets

**Policy:**
Free DNS Service

~~**Bill (DNS) = 0**~~

**Bill (ANY-on-DNS) = 0**

**#1: free fake DNS loophole**

OP-I: Free via **port 53**

OP-II: Free via **UDP+Port 53**

DNS flow ID: (**srcIP, destIP, srcPort, destPort, protocol**)

**#2: no volume-check loophole**

OP-II: Packets via **UDP+Port 53** free

Any enforcement for packets over port 53?

OP-I: **no observed limits**, except 29KB for one request packet

OP-II: **no observed limits**

# Toll-Free-Data-Access-Attack

- Proxy outside cellular network
  - **Tunneling over 53** between the mobile and external network
  - similar to calling 800-hotline
- Implementation
  - HTTP-proxy on port 53 (only for web, OP-I)
  - Sock-proxy on port 53 (for more apps, OP-I)
  - DNS-tunneling on UDP-53 (all apps, OP-I, II)
- Results
  - Free data access > 200MB, no sign of limits
  - Demo if interested

# Countermeasures

- Simplest fix: **stop free DNS service**
  - OP-II stopped it since this July

- Other suggestions
  - Authenticate DNS service
    - Only allow using authenticated DNS resolvers
    - DNS message integrity check
  - Provide free DNS quota

# Beyond DNS

- Existing DNS tunneling tools: iodine etc,
  - Designed for data access when Internet access is blocked

**differentiated-charging policy**

e.g., free access to one website/ via some APN, or cheaper VoIP than Web

**Incentive** to pay less

**(Attackers or even normal users)**

**Gap** btw policy and its enforcement

Bullet-proof design & practice

Wireless Networking Group WiNG

# On Incentive

- Toll-Free-Data-Access-Attack ✔
- Stealth-Spam-Attack
  - **Good news**: no obvious and strong incentive
    - No immediate gain for the attacker unless the ill-intentioned operator does it
  - Monetary loss against the attacker's adversary
  - **Unexpected incentive** in the future?

More information/demo in
http://metro.cs.ucla.edu/projects.html

- □ Assess the **vulnerability** of 3G/4G data charging system
- □ **Two** types of attacks,
  - **Toll-free-data-access-attack** (free > 200MB)
    - Enforcement of **differentiated-charging** policy
  - **Stealth-spam-attack** (overcharging > 500MB)
    - Rooted in charging architecture, security mechanism and IP model
  - **No observed volume limits**
- □ **Insight**
  - IP push model is not ready for metered-charging
  - Feedback or control needed during data charging
  - Differentiated-charging policy has to secure itself