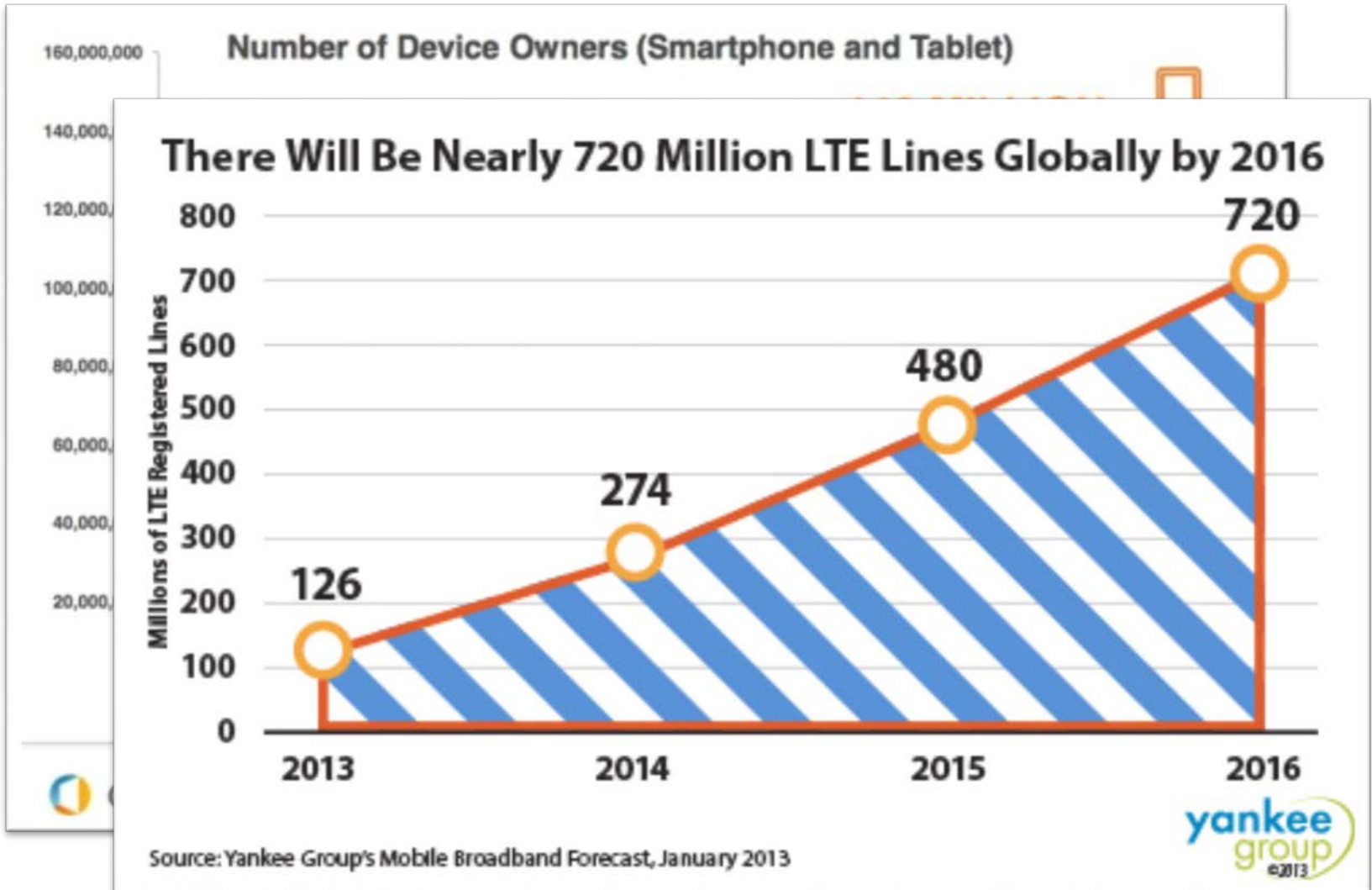




# Unveiling the Hidden Dangers of Public IP in 4G/LTE Networks

**Wai Kay Leong**, Aditya Kulkarni, Yin Xu, Ben Leong

# Mobile Internet is *Hot*



# Public IP - What's the deal?

» [Forums Archive](#) » [Wireless ISPs](#) » [Telstra](#) » Which 4G modem to get bridged public IP?

[Archive version](#)

[Return to standard view](#)

User #5897 56 posts

**Dr Vik**

Forum Regular

We desperately need to get a 4G backup in our office as we are having significant congestion issues at times bringing our VOIP system to the ground (15mbit shared connection between 90 offices!!).

O.P.

After some reading on here I have ascertained that the cleanest way to give our router internet access is to use a Dovado Tiny in bridged mode with a 4G modem using either Bigpond or Telstra Business with a public IP.

Subscribers want Public IP

- 1) Is it correct that none of the Bigpond supplied devices are bridgeable?
- 2) Can I purchase some other (older?) bridgeable Bigpond branded device off ebay and use our current SIM inside that?
- 3) If I have to go down the path of Telstra branded 4G modem, WHICH ONE is bridgeable and which plan do I sign up for to be able to access a public IP with the correct code and telstra.extranet APN?

Many thanks for all your contributions.

drvik

reference: whrl.pl/RdKF  
posted 2013-Oct-24, 9:52

User #40602 9088 posts

**zaxa**

Whirlpool Forums Addict

If you have a telstra service you can use a different modem (like a telstra prepaid, or a telstra business postpaid), its the Bigpond branded consumer plans that won't allow a different modem.

# M2M - Machine to Machine



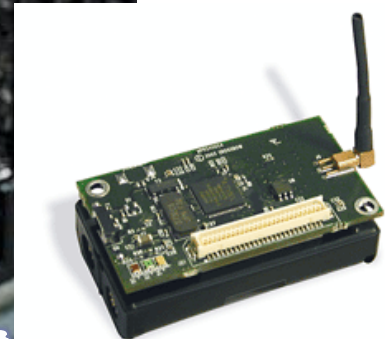
Delivery Vans



Security Cameras



Traffic Control



Sensor Nodes

*pit & Marion*



# Our Local Situation

---

- ▶ **ISP A**    Public IP by default<sup>†</sup>
- ▶ **ISP B**    Change APN
- ▶ **ISP C**    Change APN



Free Public IP for LTE networks

<sup>†</sup>Does not work for certain devices

# The Dangers of Public IP



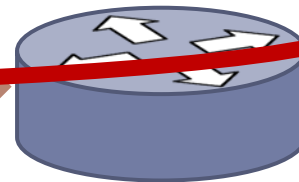
Susceptible to **simple IP** attacks

1. DoS Flooding
2. Quota Drain
3. Battery Drain



Attacker

10.42.0.1  
No route  
to host



NAT

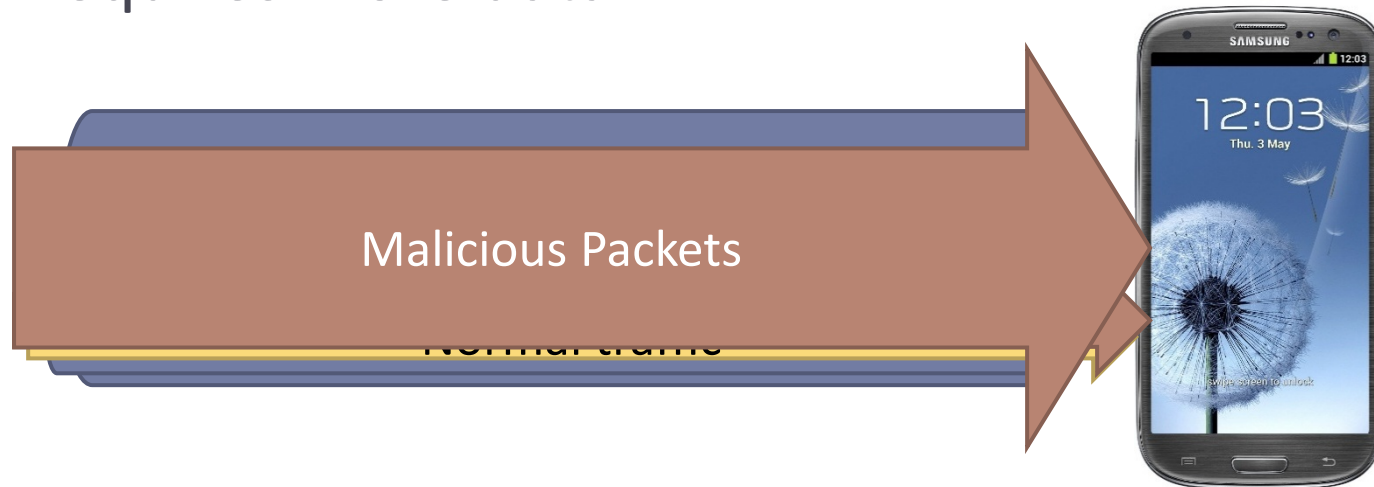


Private IP  
105.42.0.1

# Attack 1: DoS Flooding

---

- ▶ Overwhelm the link/resources
- ▶ Conventionally
  - ▶ Higher bandwidth (30 Mb/s)
  - ▶ Requires more data



# Buffer Sizing Matters

ISP	Buffer
ISP A	2,000 pkts
ISP B	600 pkts
ISP C	800 ms

Xu et al. PAM 2014

## ▶ ISP C

### ▶ Drop

Low traffic is sufficient to DoS

## ▶ Sized in packets

- ▶ 1,500-byte packet  $\equiv$  1-byte packet



# Experiment Set-up

---



Send rate (Mb/s)  
Packet Size (bytes)

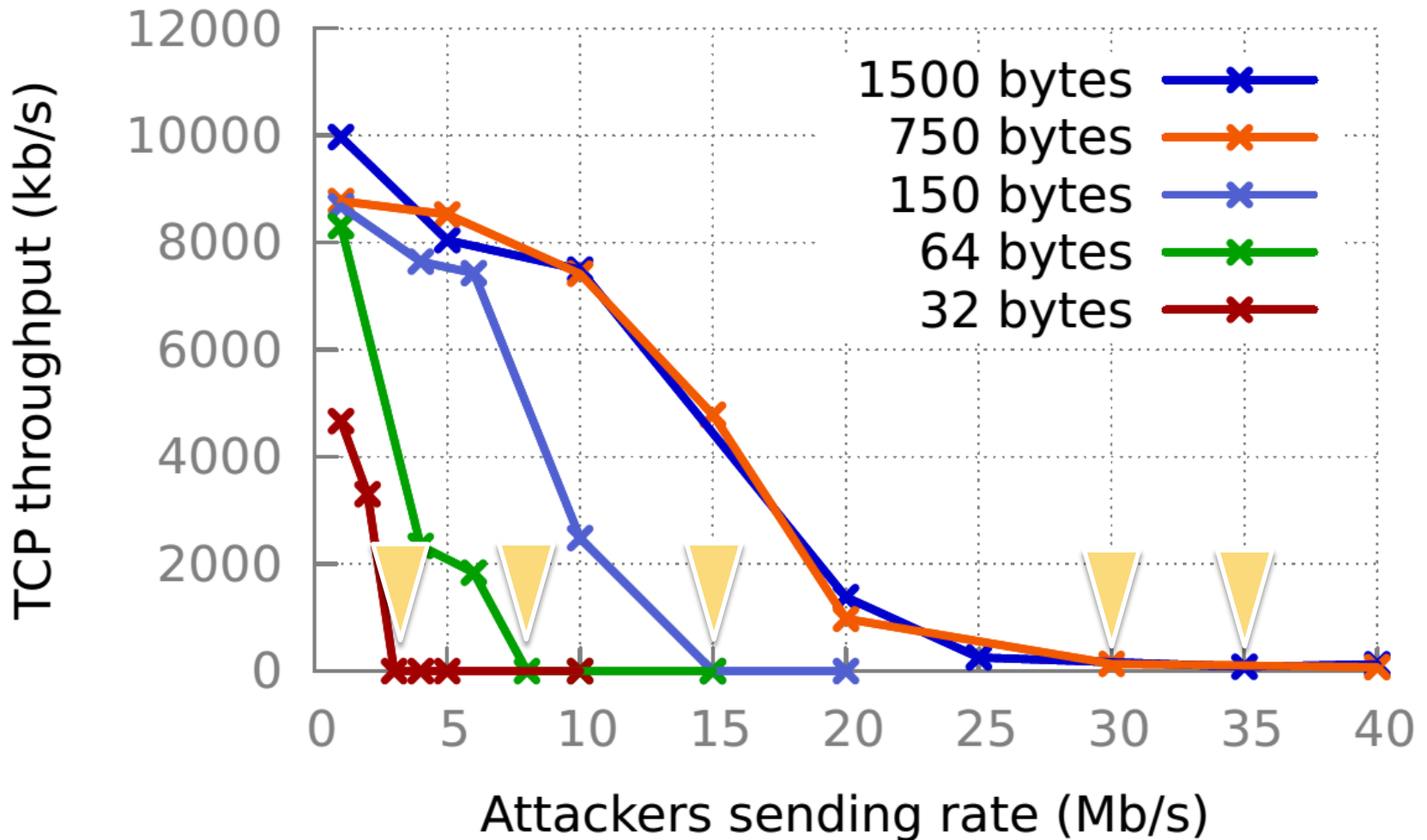
UDP DoS



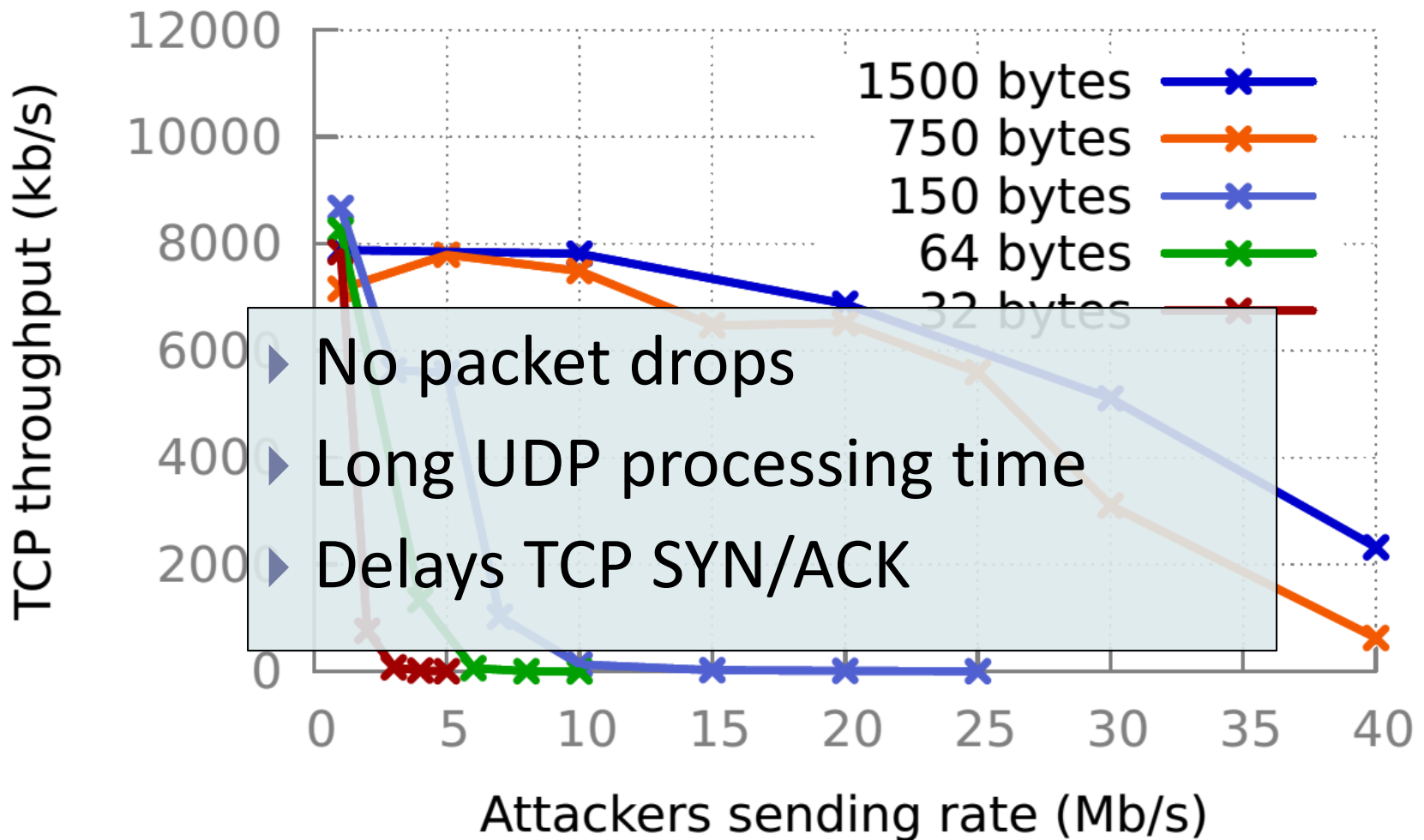
TCP traffic

Measure TCP  
throughput (kb/s)

# Results

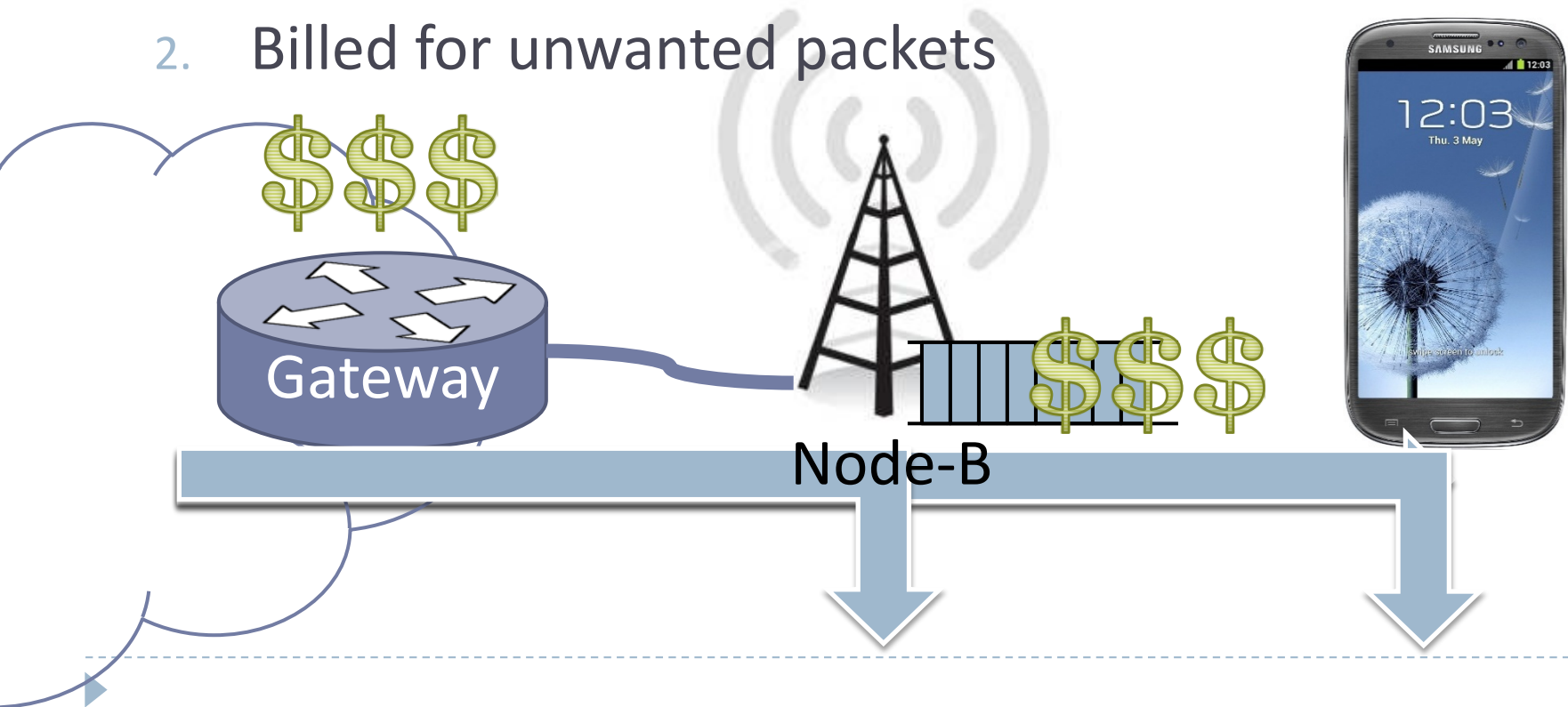


# ISP C - AQM

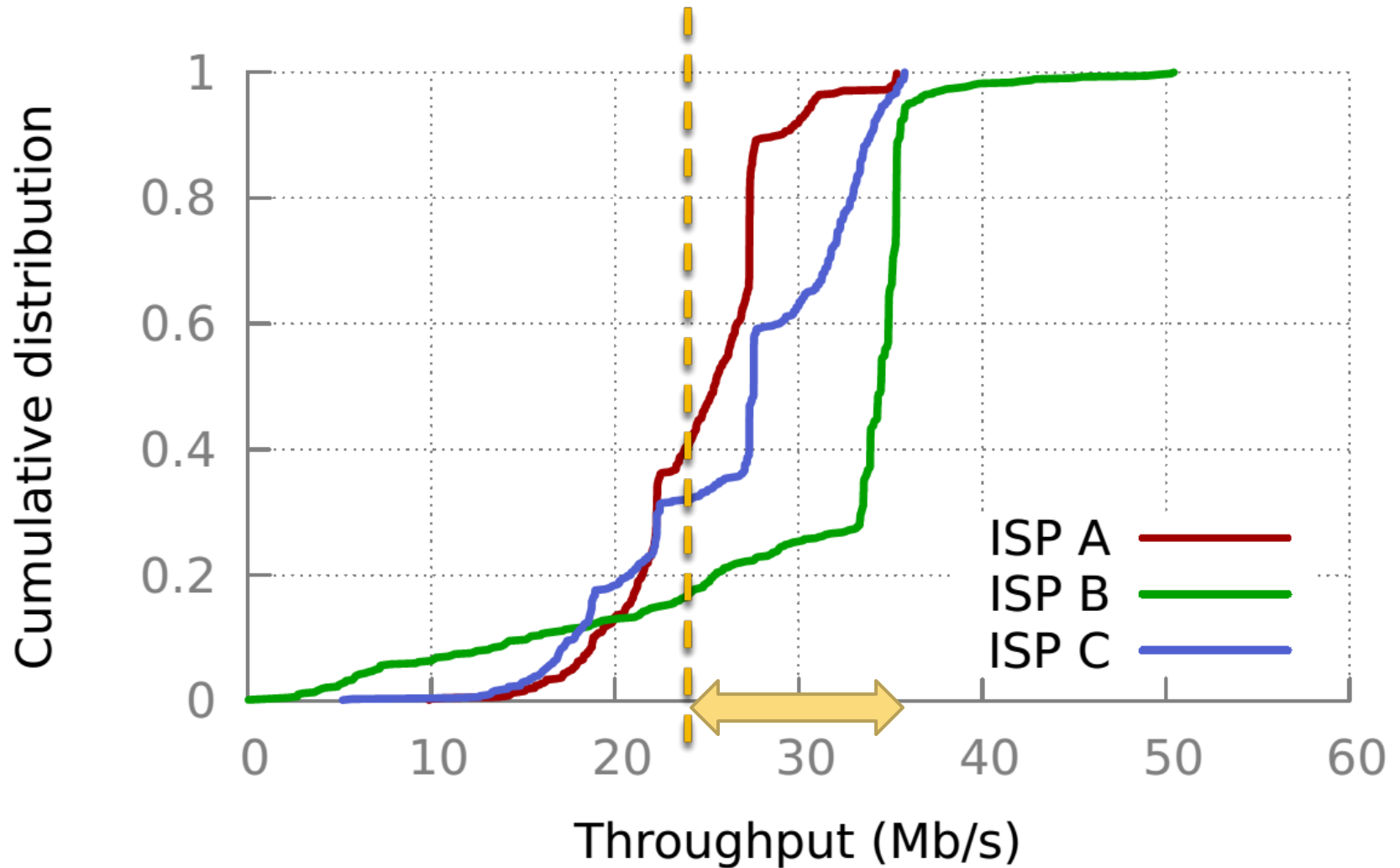


# Attack 2: Quota Drain

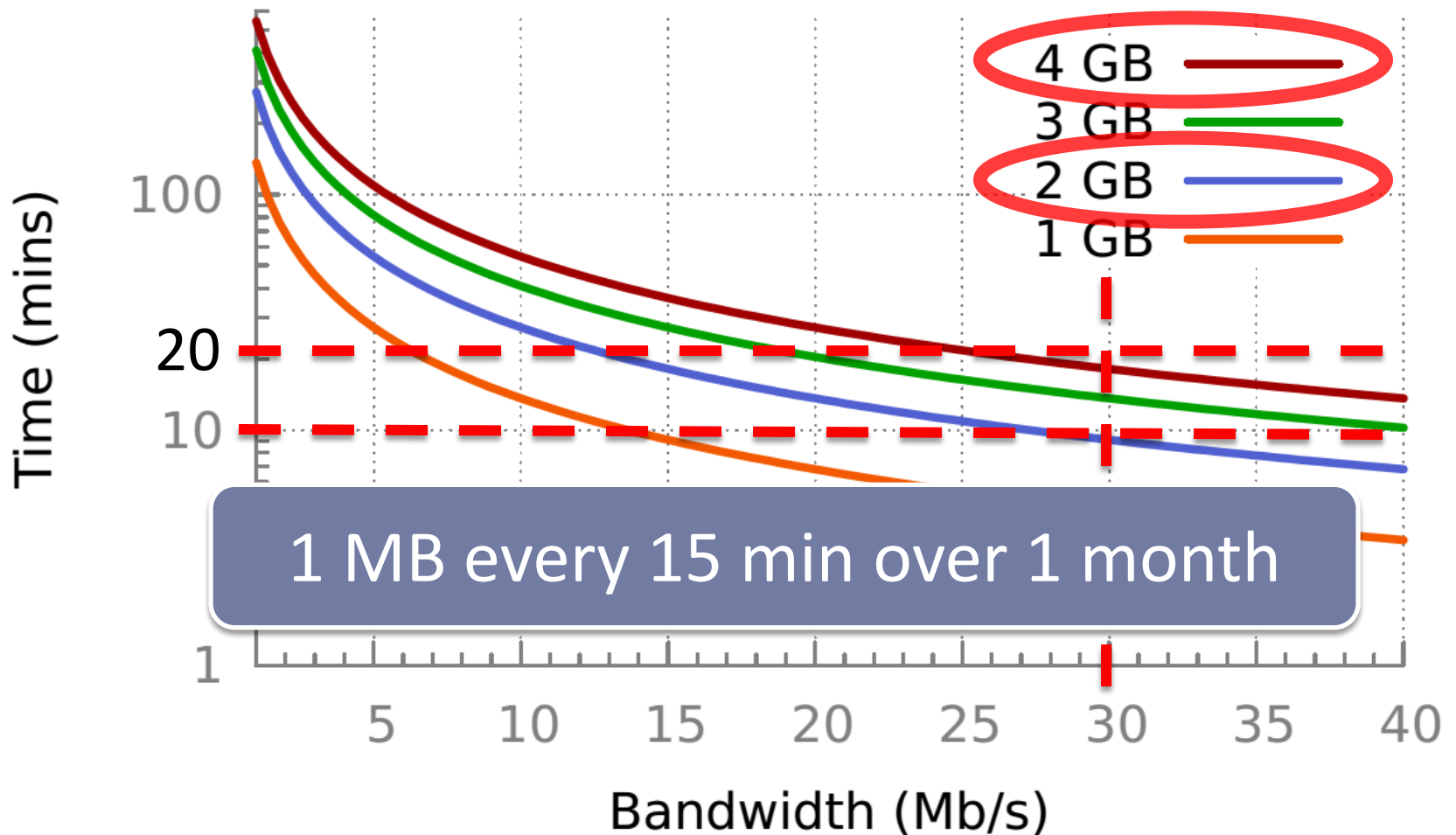
- ▶ Data cost \$\$\$
- ▶ Limited free quota.
  1. Billed for dropped packets (Peng et al.)
  2. Billed for unwanted packets



# High Speed LTE



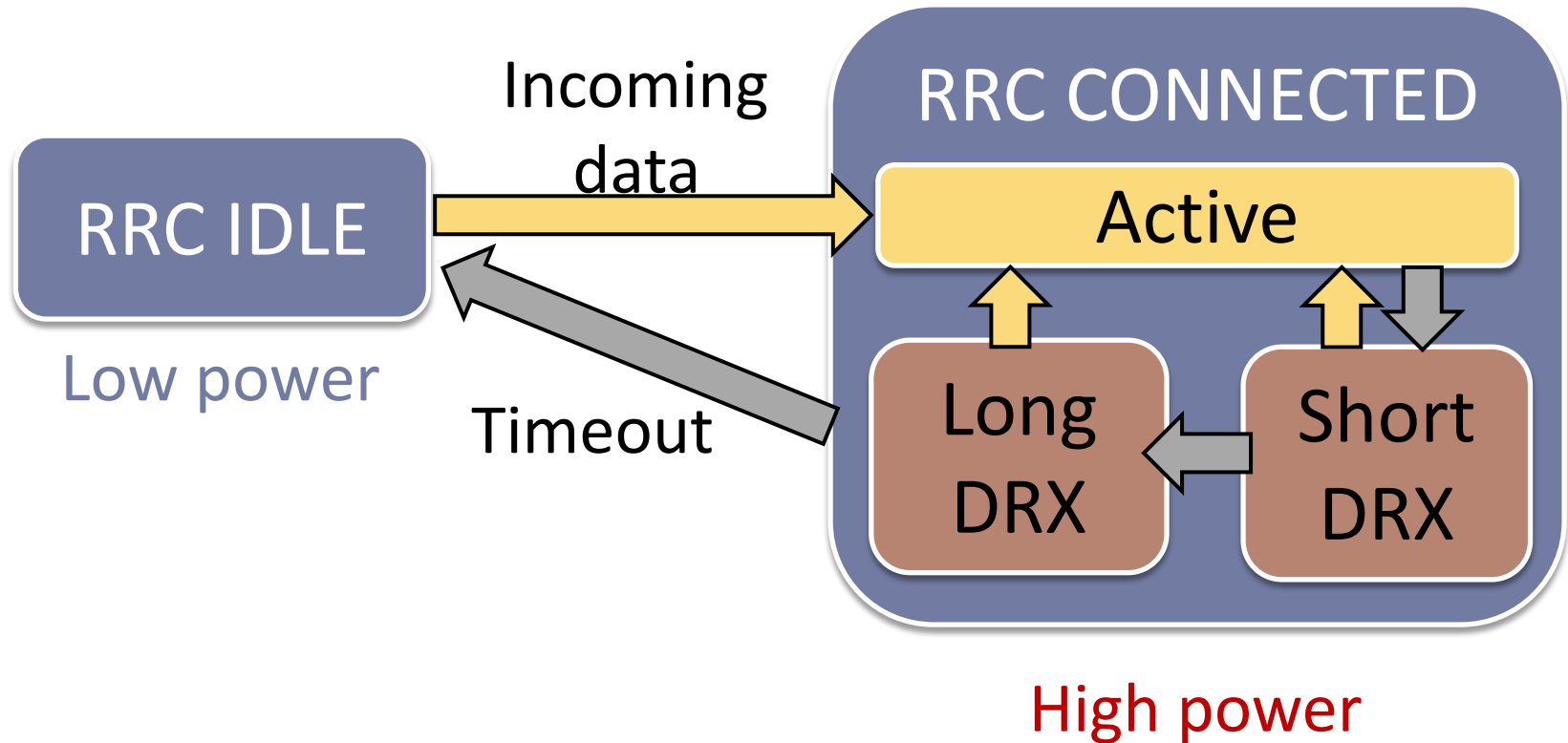
# Time to Drain Quota





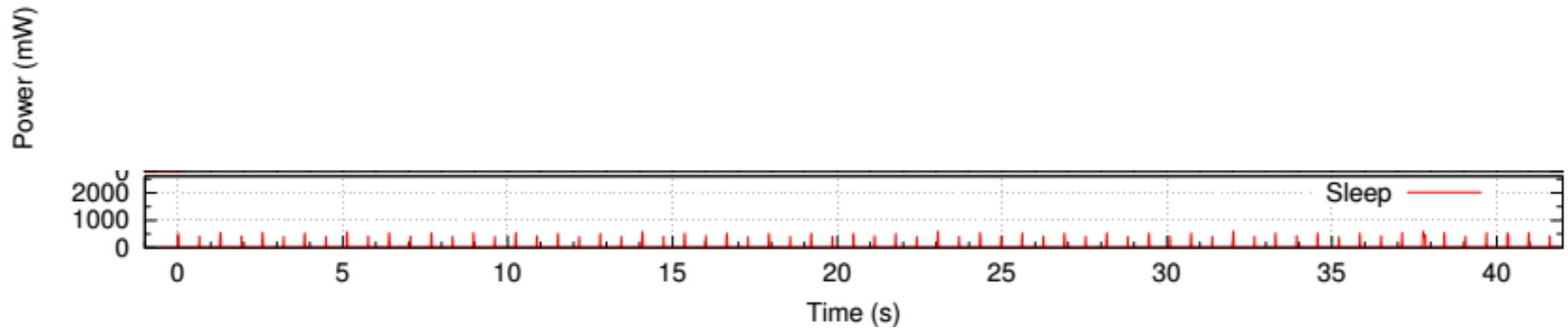
# Attack 3: Battery Drain

- ▶ Network communication consumes power
- ▶ LTE protocol states



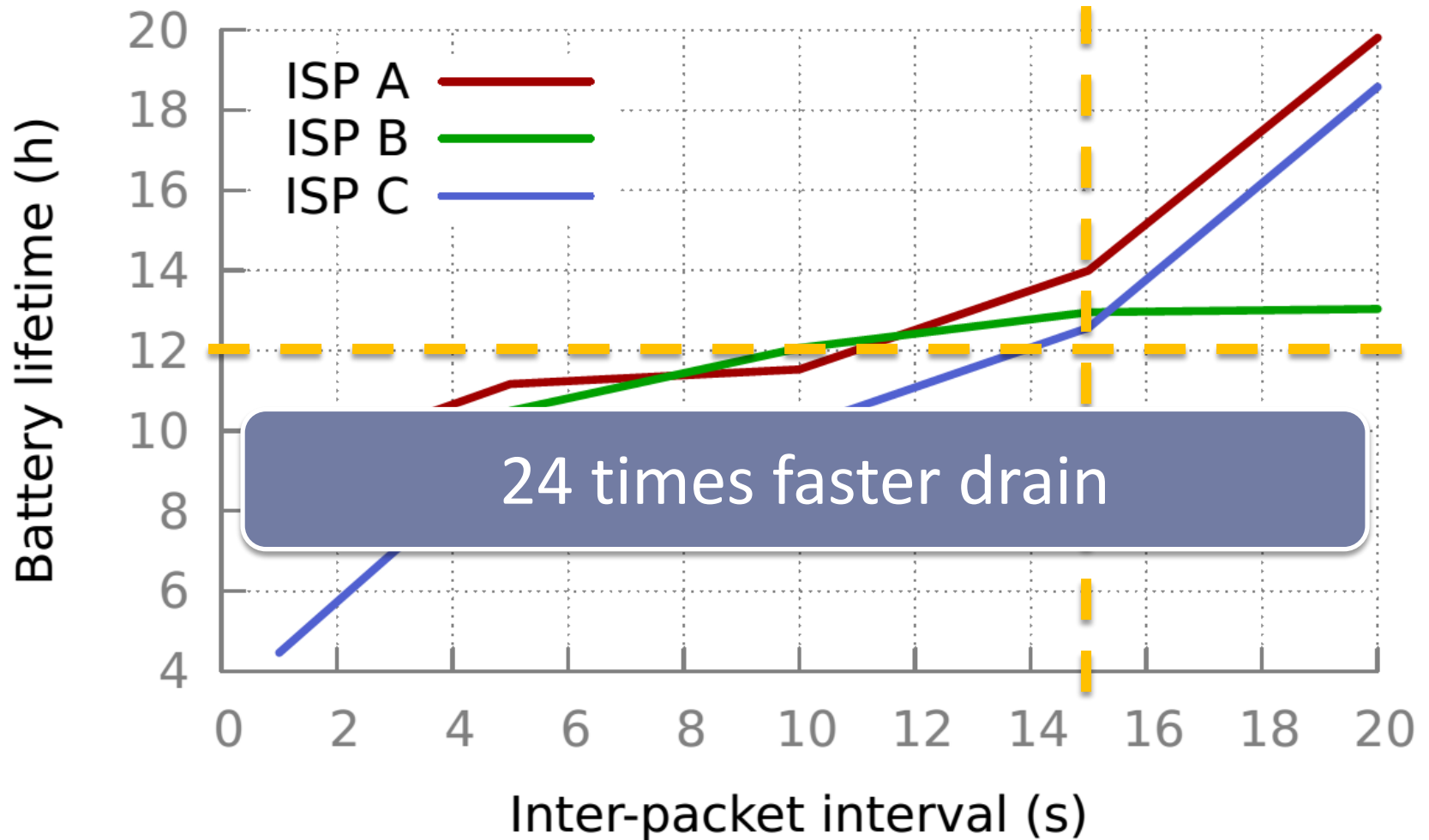
# Power Monitor

---



- ▶ Different ISPs → Different patterns
  - ▶ Same device
- ▶ Packet size does **not** matter
- ▶ More details in the paper

# Battery Consumption



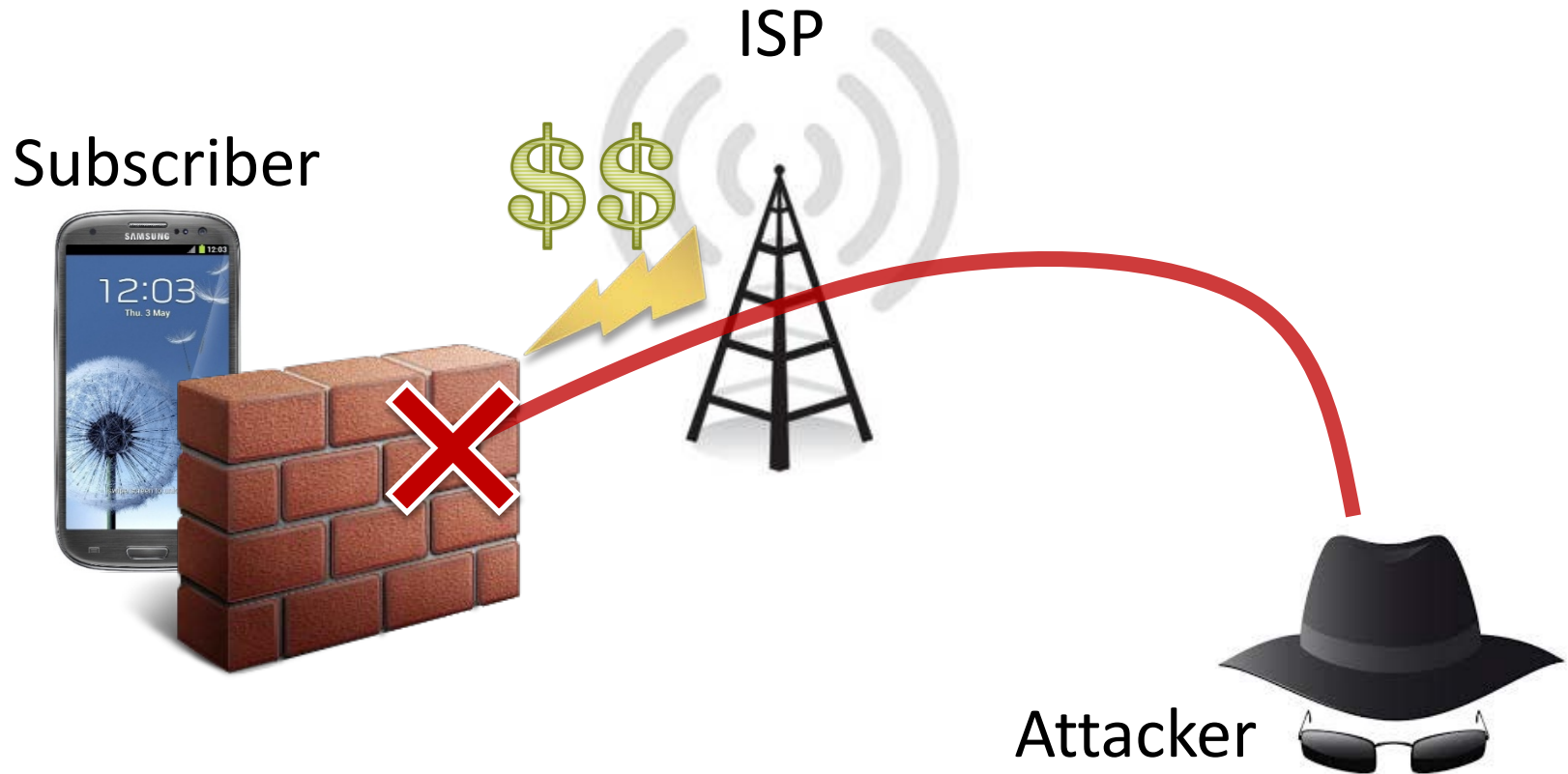
# Defense Against Attacks

---

- ▶ **Avoid Public IP**
  - ▶ Use Network Address Translation (NAT)
- ▶ **NAT traversal**
  - ▶ can be slow
  - ▶ not 100% successful
  - ▶ requires NAT servers
- ▶ **Firewalls?**

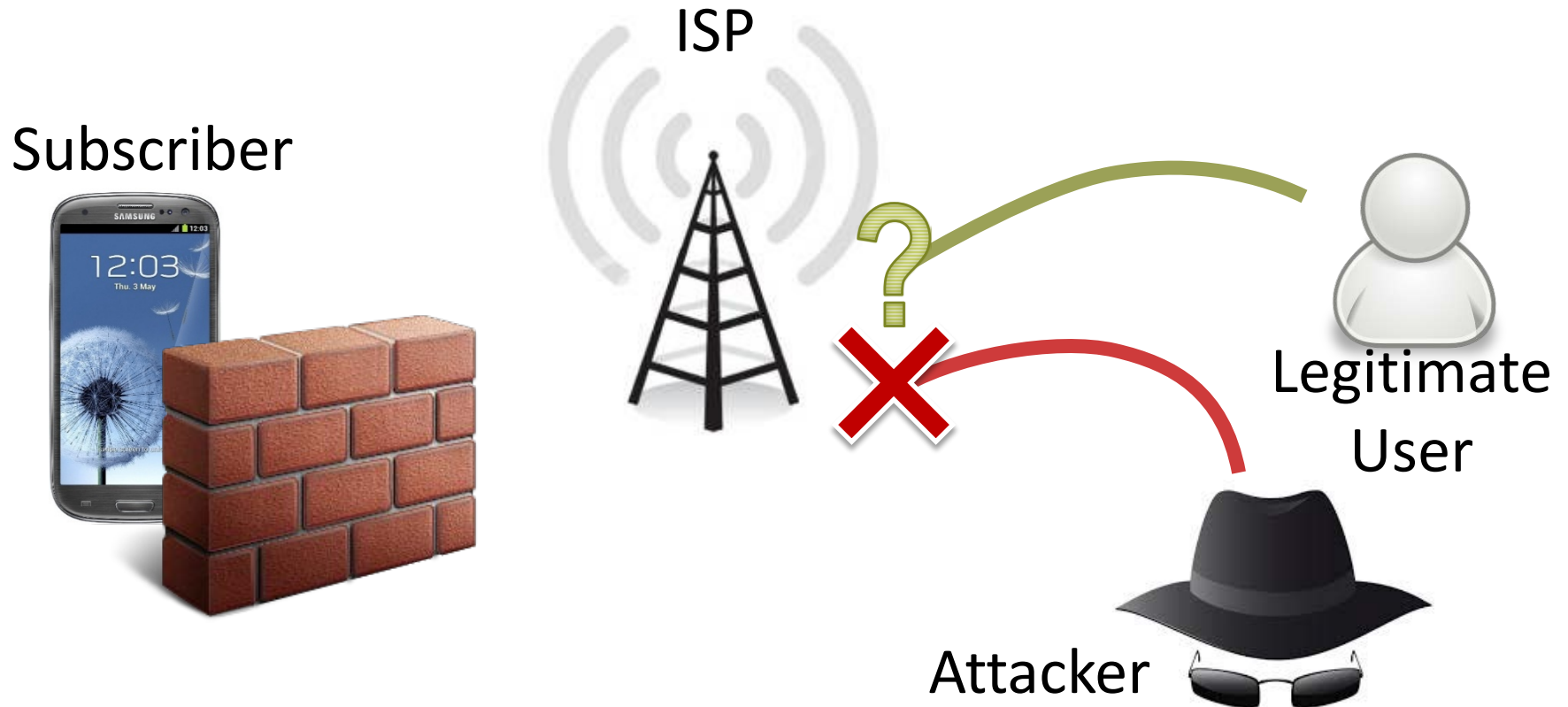
# Firewall on device

Harm is already done



# Firewall on ISP

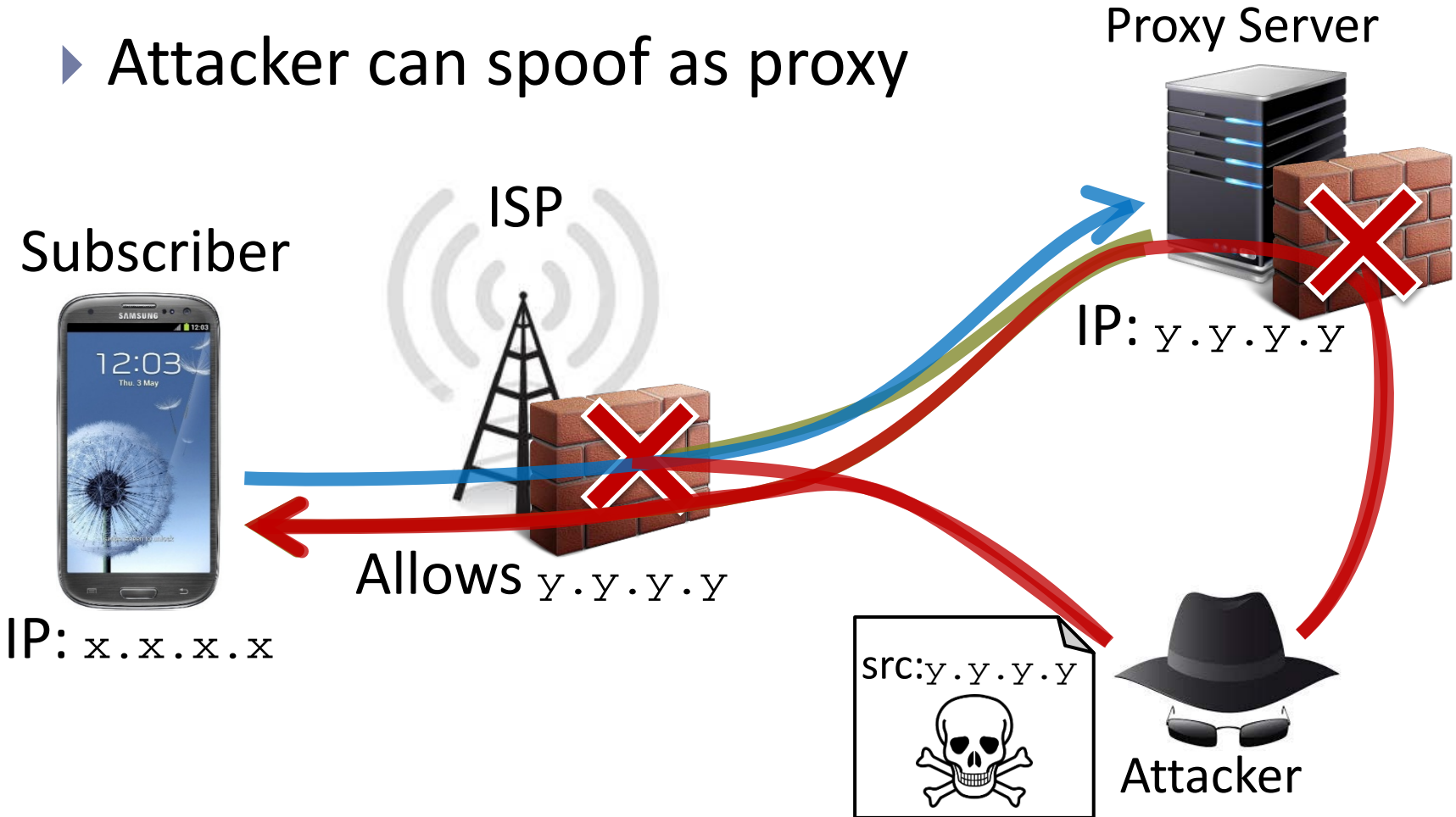
- ▶ Hard to differentiate legitimate traffic
- ▶ Complex firewall hard to deploy





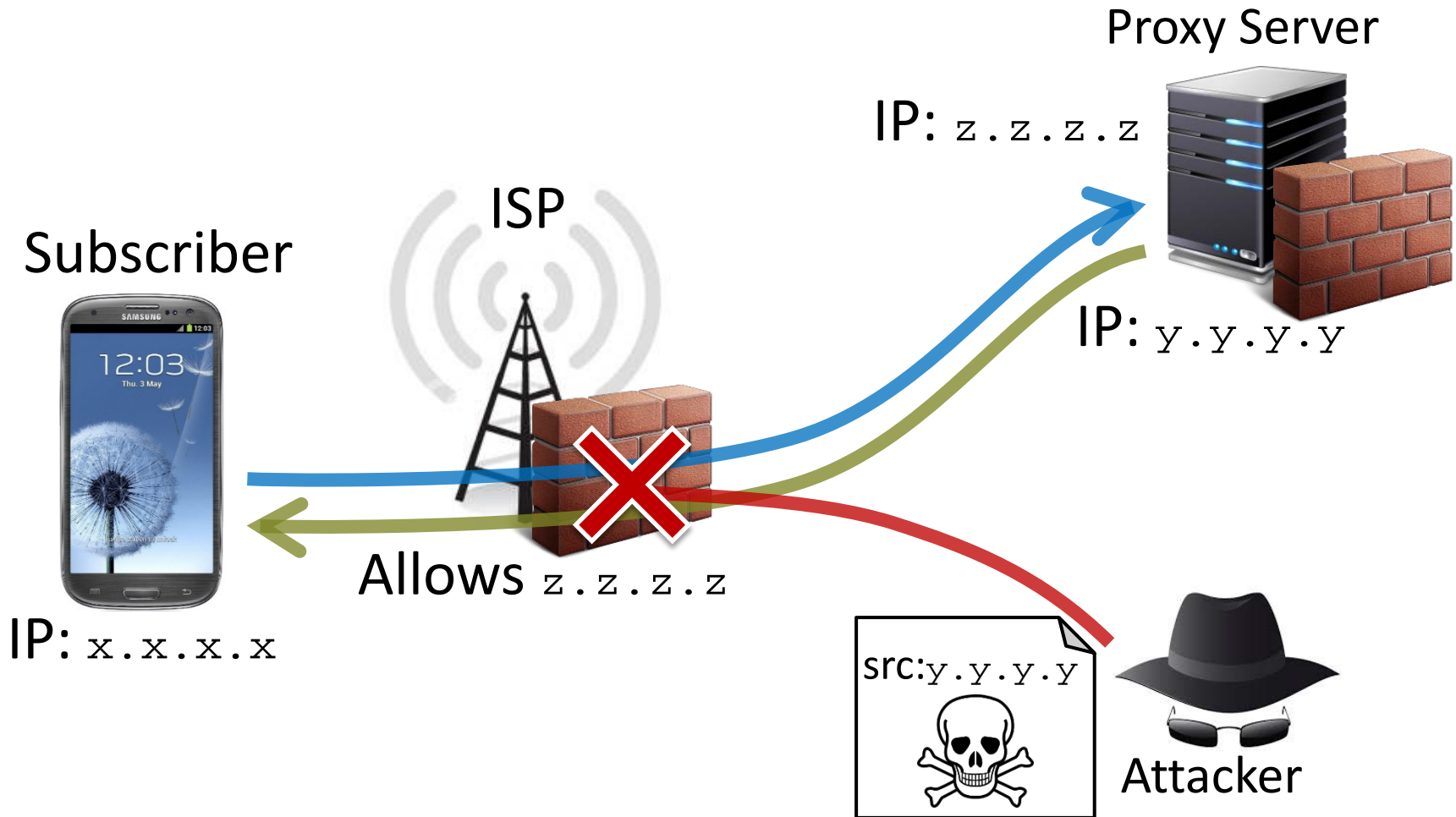
# Proxy + Firewall

- ▶ ISP firewall allows solicited access
- ▶ Attacker can spoof as proxy



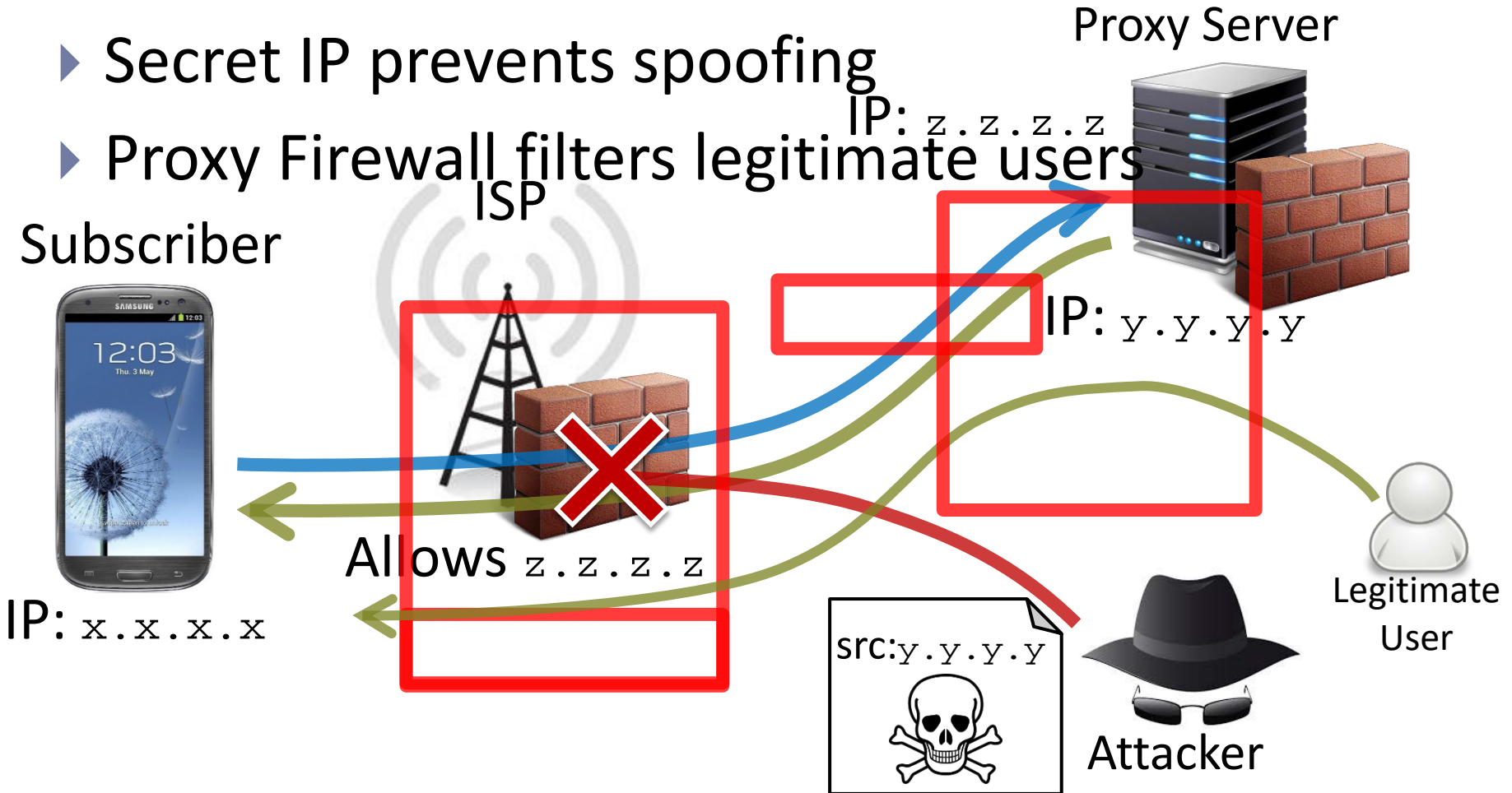
# Double IP address

- ▶ Give proxy a secret IP address



# In Summary

- ▶ Firewall prevents unsolicited access
- ▶ Secret IP prevents spoofing
- ▶ Proxy Firewall filters legitimate users



# Conclusion

---

## ▶ Public IP: Desirable, but Dangerous

- ▶ Best to avoid public IP
- ▶ Sometimes enabled by default!



## ▶ Attacks are

- ▶ Simple
- ▶ Requires little resources
- ▶ Can be hard to detect/differentiate



## ▶ Proxy Solution

- ▶ How effective or reliable?



# Moving Forward...

---

- ▶ Mobile networks will be faster
- ▶ More users
  - ▶ Personal
  - ▶ Commercial
- ▶ Security is a concern
  - ▶ P2P or M2M



Thank You

Questions and Comments