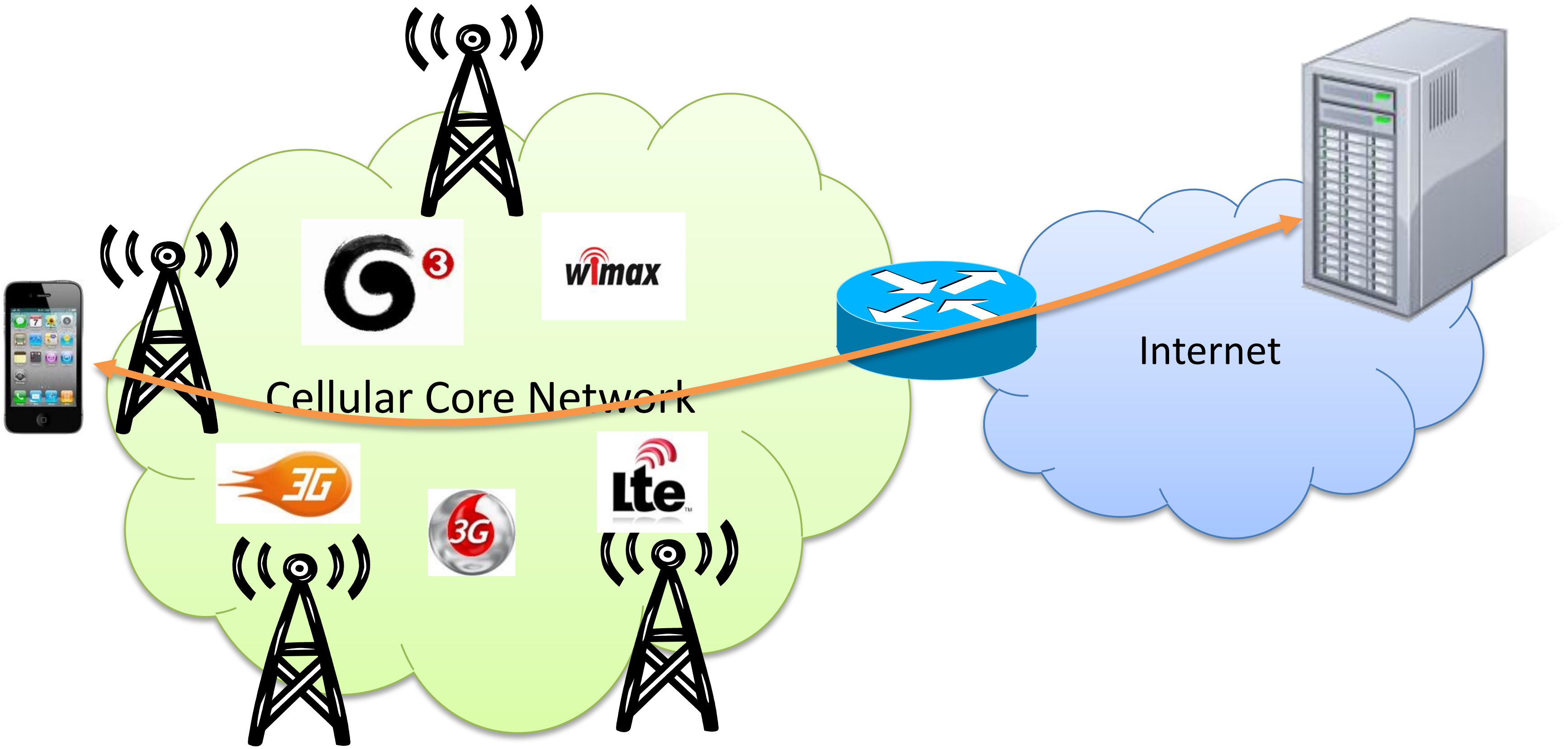
An Untold Story of Middleboxes in Cellular Networks

Zhaoguang Wang[1]

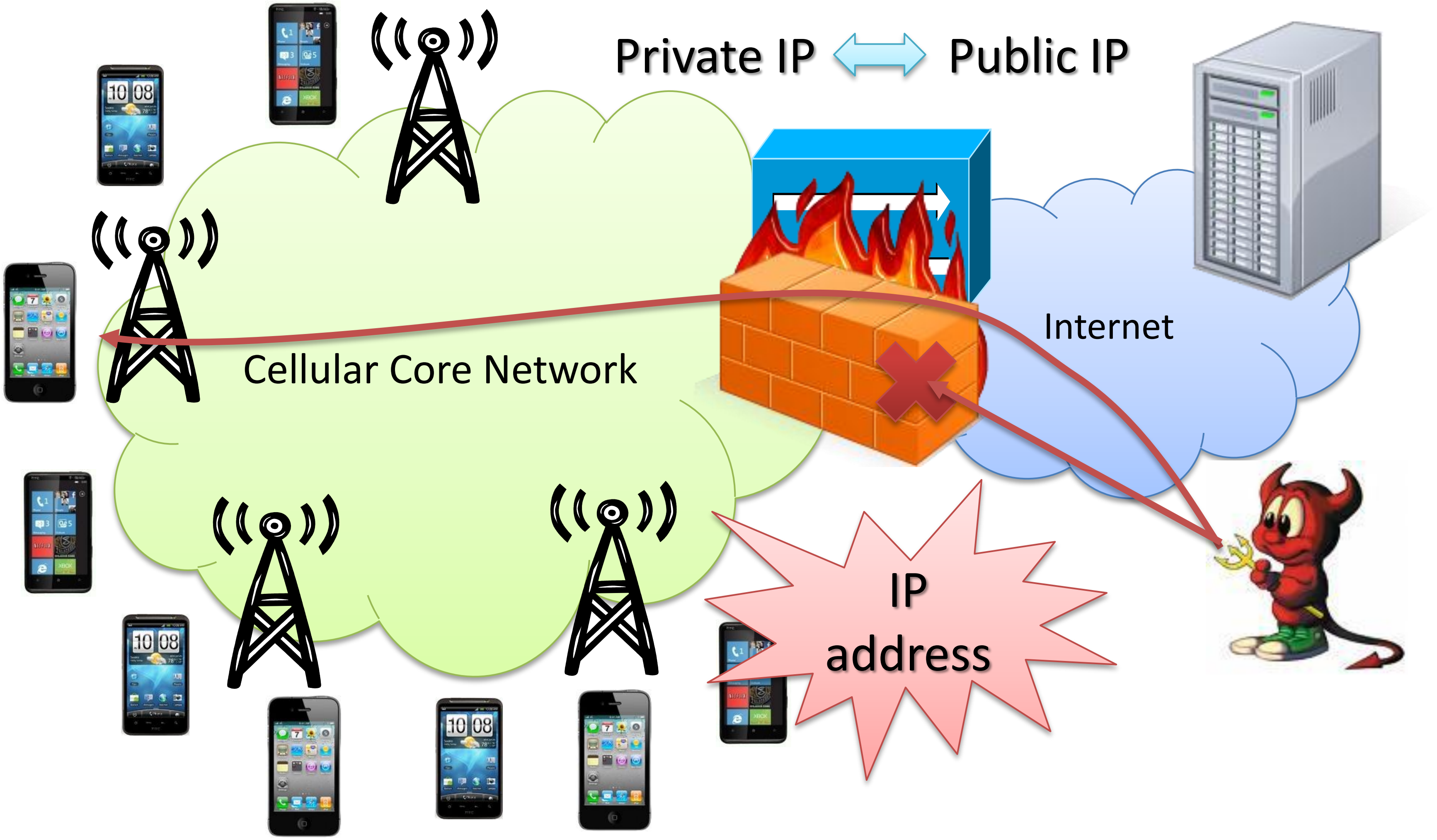
Zhiyun Qian[1], Qiang Xu[1], Z. Morley Mao[1], Ming Zhang[2]

[1]University of Michigan [2]Microsoft Research

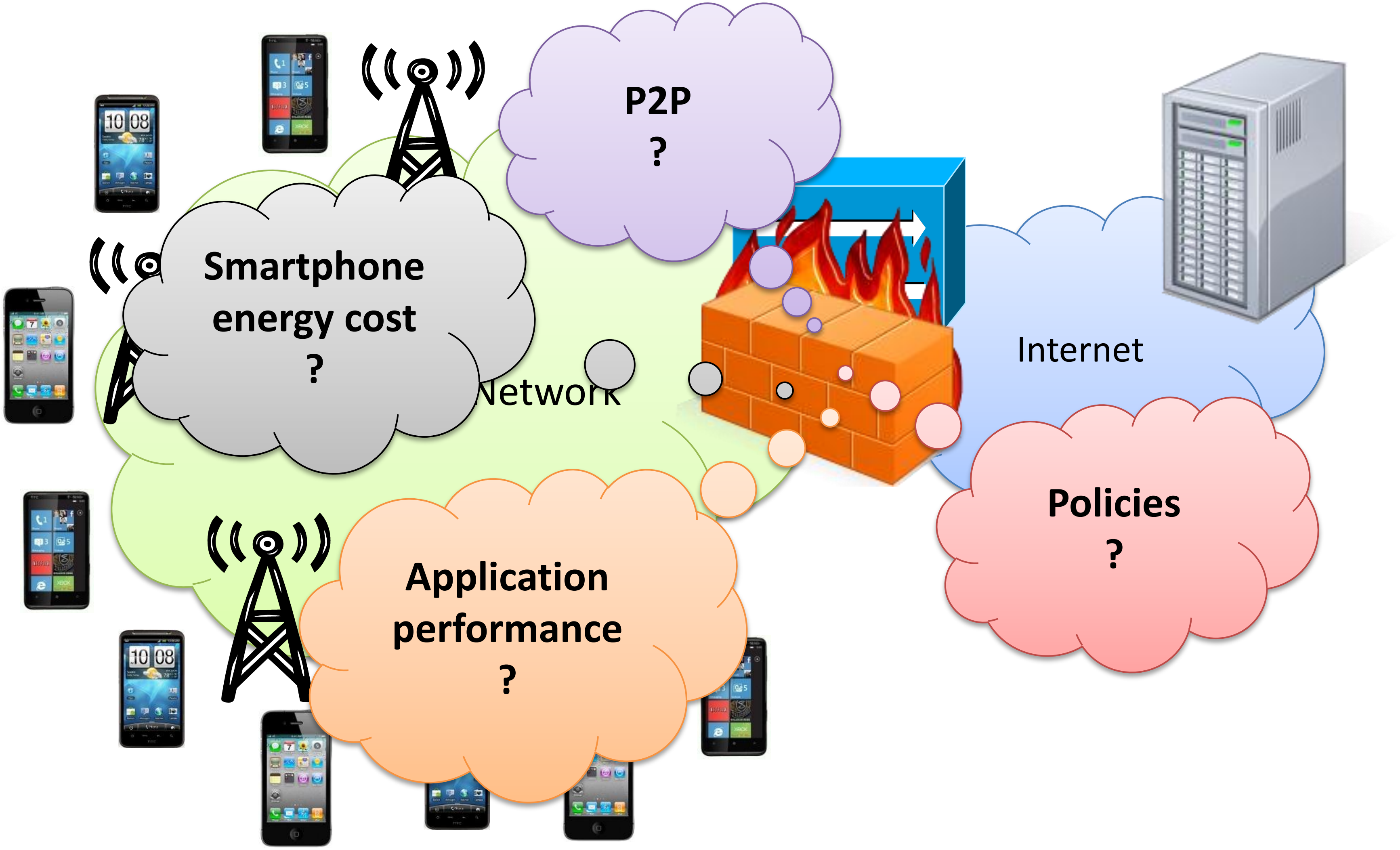
Background on cellular network



Why carriers deploy middleboxes?



Problems with middleboxes



Challenges and solutions

- Policies can be complex and proprietary

  √ Design a suite of end-to-end probes

- Cellular carriers are diverse

  √ Publicly available client Android app

- Implications of policies are not obvious

  √ Conduct controlled experiments

Related work

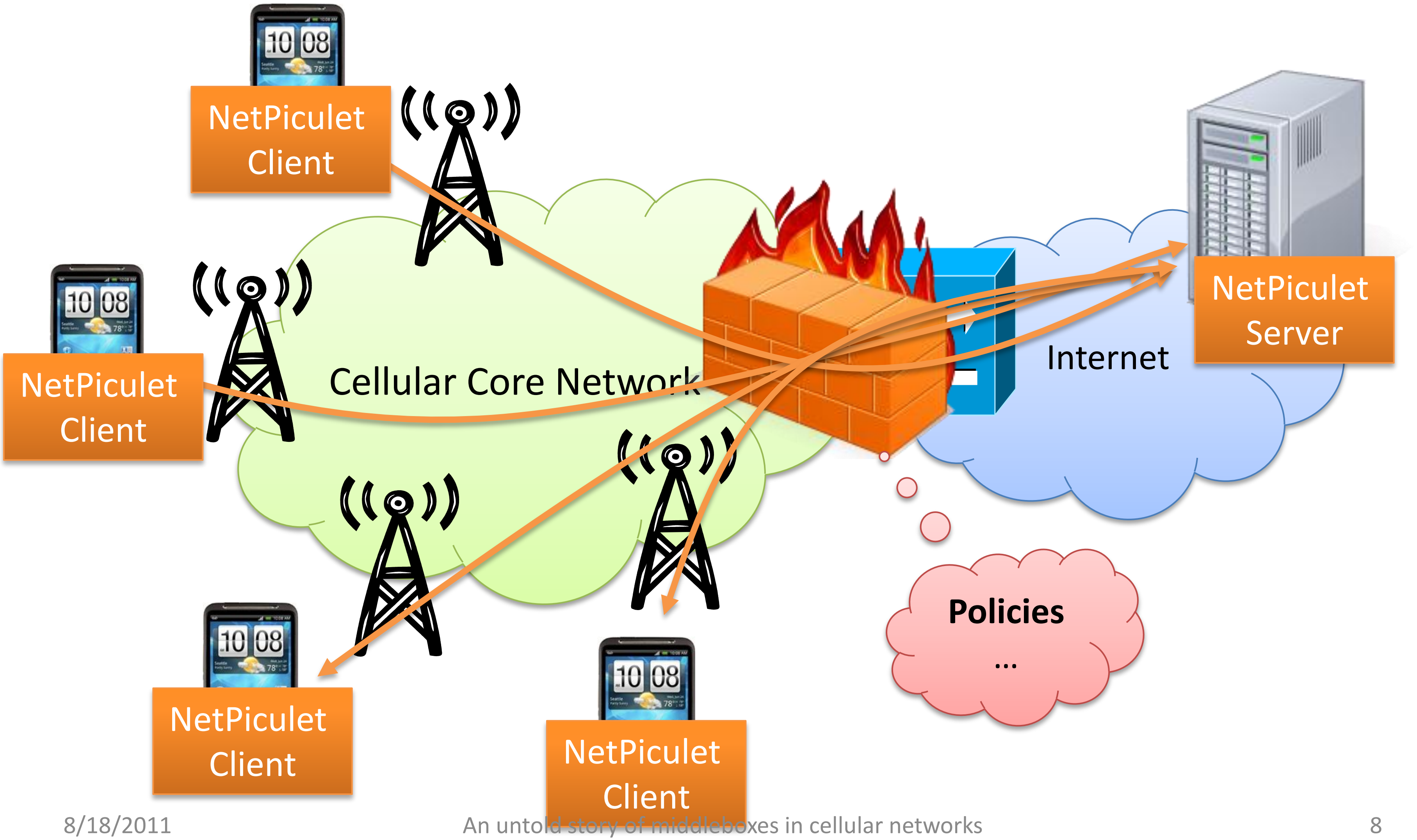
- Internet middleboxes study
  - [Allman, IMC 03], [Medina, IMC 04]
- NAT characterization and traversal
  - STUN[MacDonald et al.], [Guha and Francis, IMC 05]
- Cellular network security
  - [Serror et al., WiSe 06], [Traynor et al., Usenix Security 07]
- Cellular data network measurement
  - WindRider, [Huang et al., MobiSys 10]

Goals

- Develop a tool that accurately infers the NAT and firewall policies in cellular networks

- Understand the impact and implications
  - Application performance
  - Energy consumption
  - Network security

The NetPiculet measurement system



Target policies in NetPiculet

Firewall	IP spoofing
	TCP connection timeout
	Out-of-order packet buffering
NAT	NAT mapping type
	Endpoint filtering
	TCP state tracking
	Filtering response
	Packet mangling

Target policies in NetPiculet

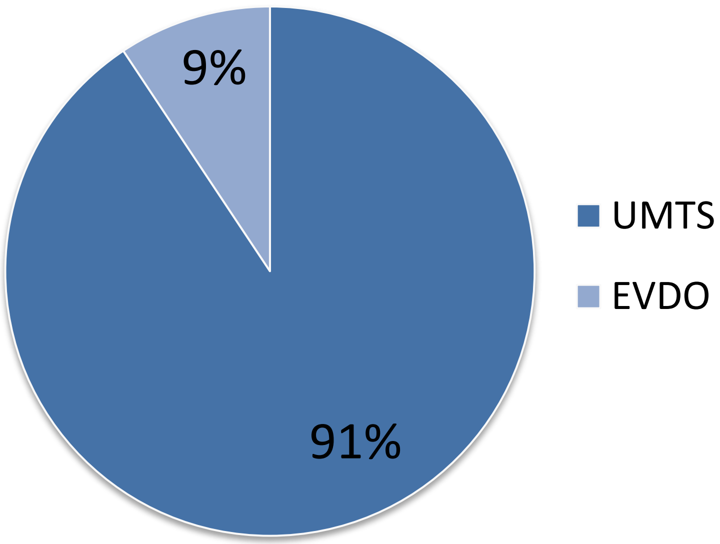
Firewall	IP spoofing
	TCP connection timeout
	Out-of-order packet buffering
NAT	NAT mapping type
	Endpoint filtering
	TCP state tracking
	Filtering response
	Packet mangling

Key findings

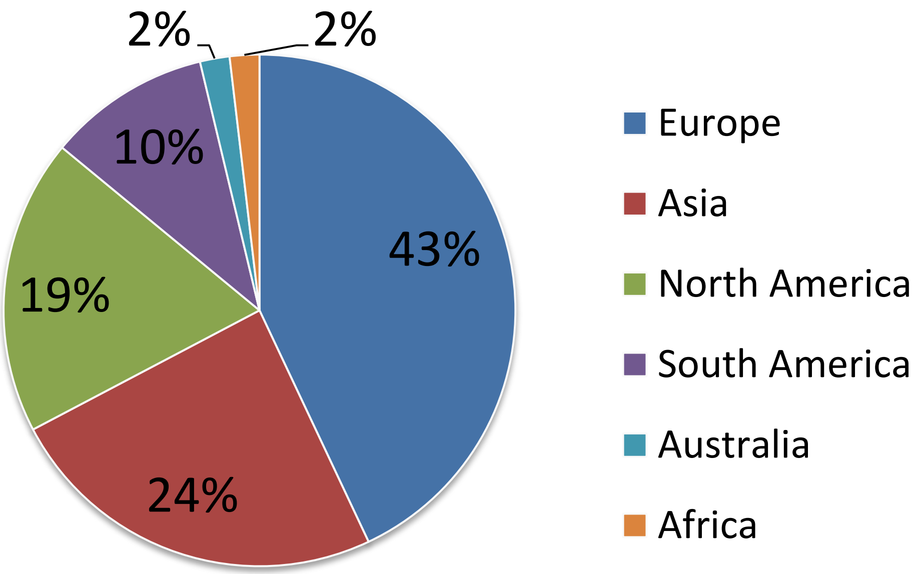
Firewall	Some carriers allow IP spoofing **Create network vulnerability**
	Some carriers time out idle connections aggressively **Drain batteries of smartphones**
	Some firewalls buffer out-of-order packet **Degrade TCP performance**
NAT	One NAT mapping linearly increases port # with time **Classified as random in previous work**

Diverse carriers studied

- NetPiculet released in Jan. 2011
  - 393 users from 107 cellular carriers in two weeks



Technology



Continent

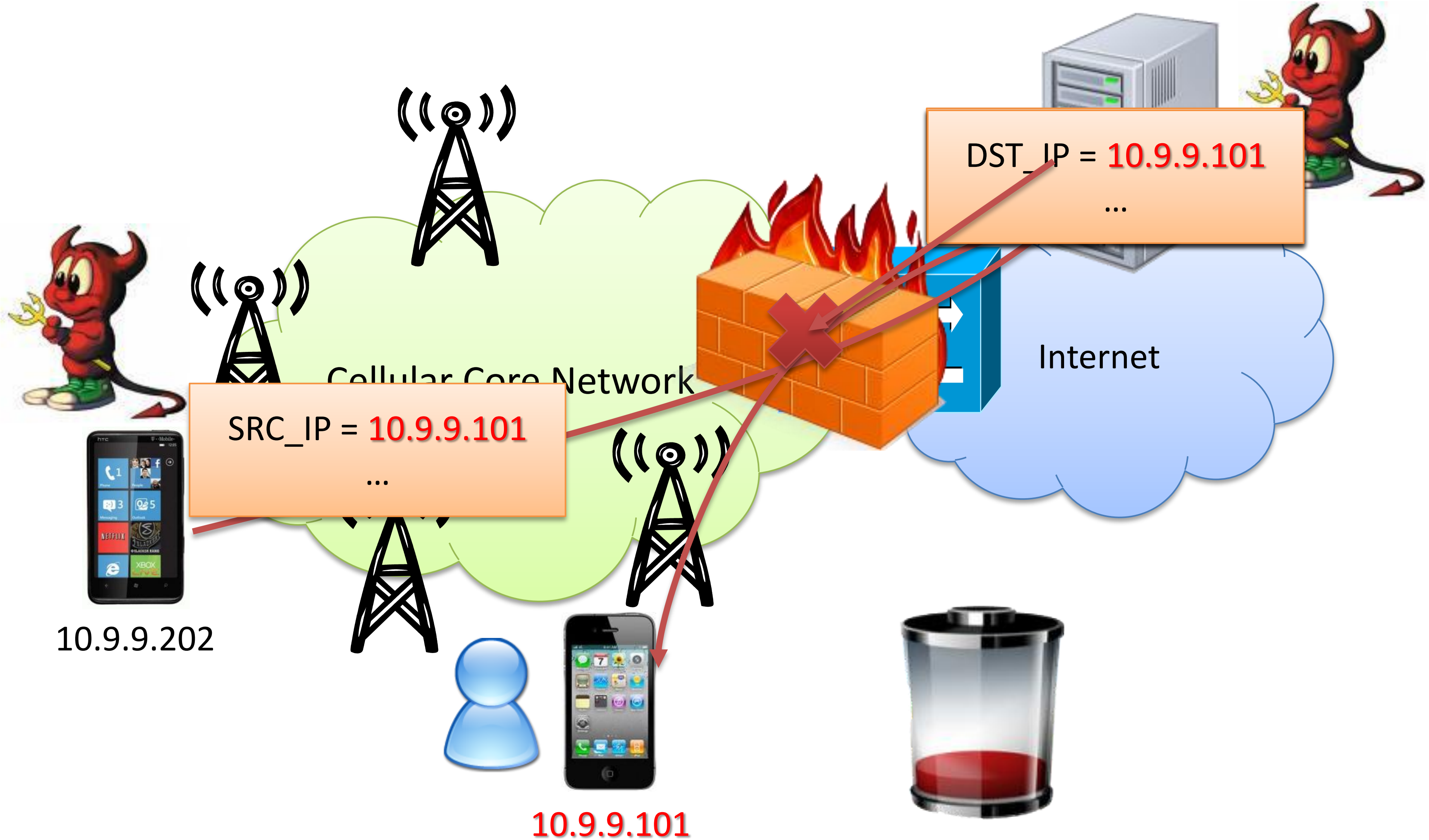
Outline

1. IP spoofing
2. TCP connection timeout
3. TCP out-of-order buffering
4. NAT mapping

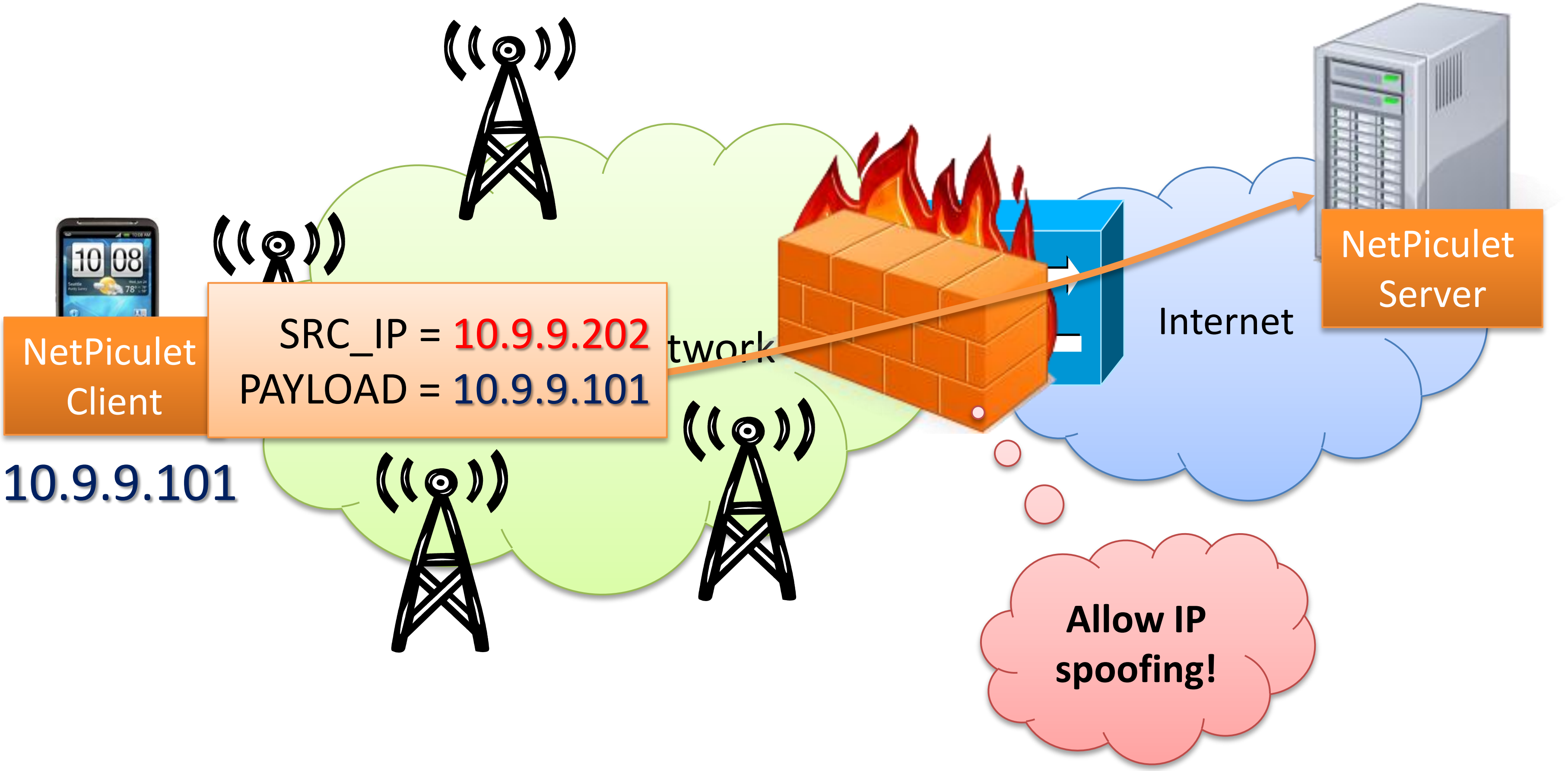
Outline

1. IP spoofing
2. TCP connection timeout
3. TCP out-of-order buffering
4. NAT mapping

Why allowing IP spoofing is bad?



Test whether IP spoofing is allowed



NetPiculet Client

10.9.9.101

SRC_IP = 10.9.9.202

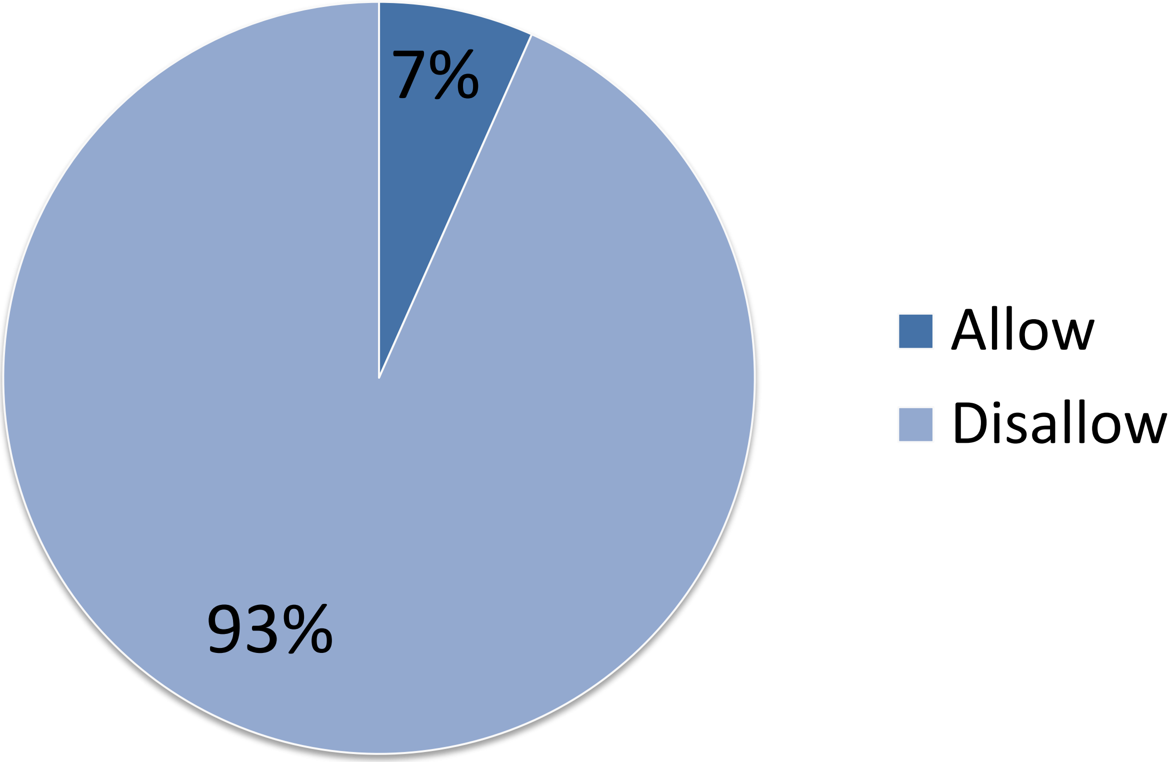
PAYLOAD = 10.9.9.101

NetPiculet Server

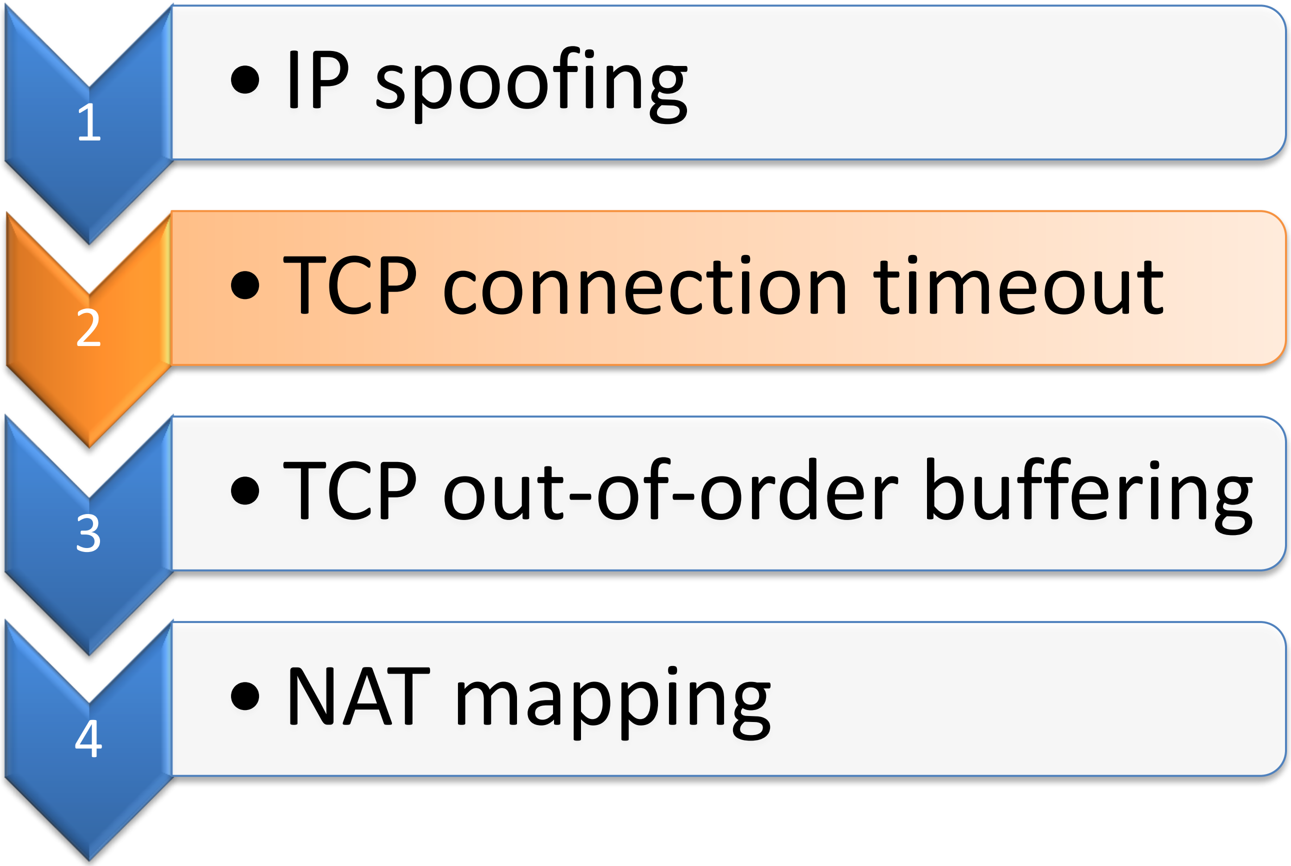
Allow IP spoofing!

4 out of 60 carriers allow IP spoofing

IP spoofing should be disabled

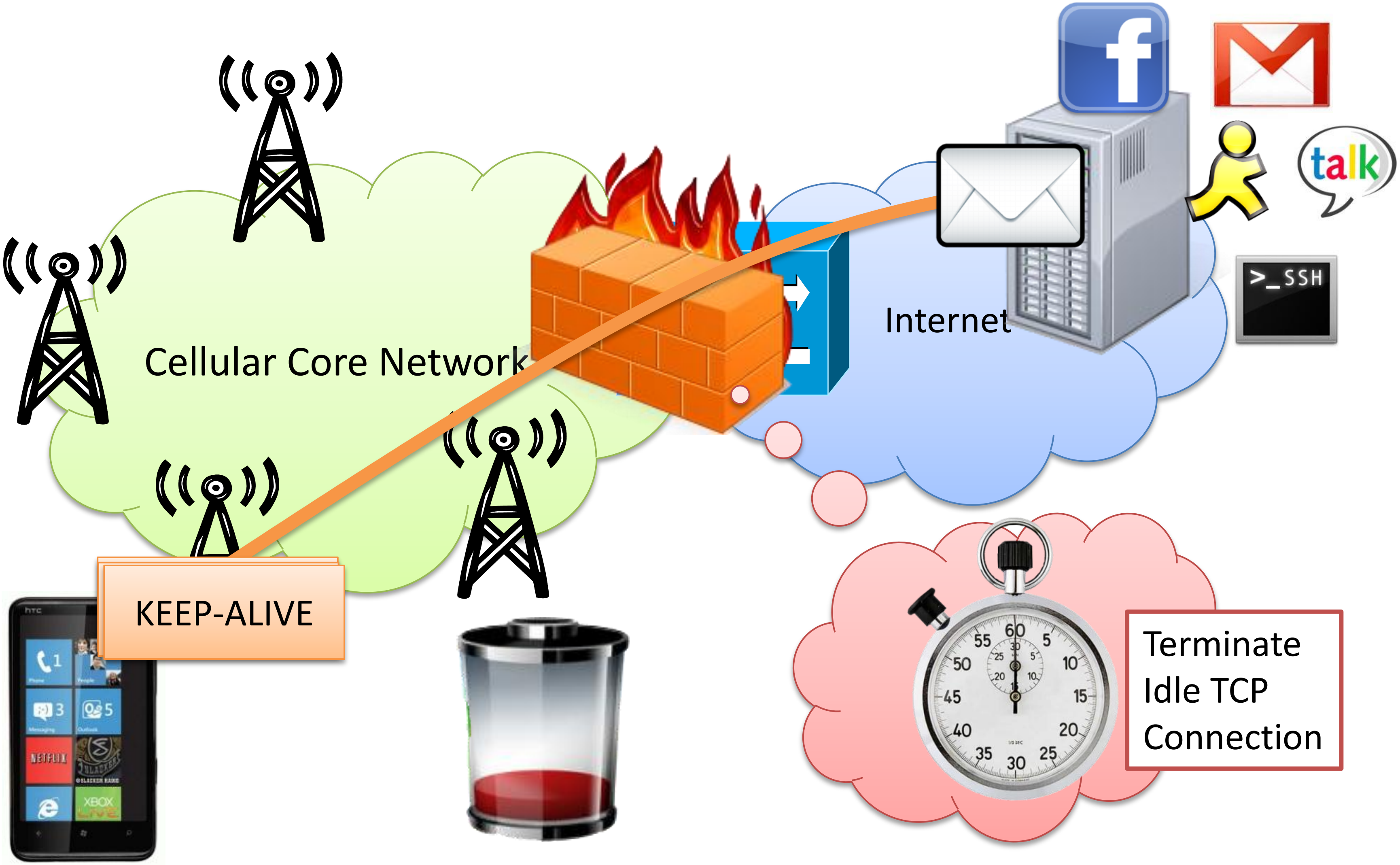


Outline



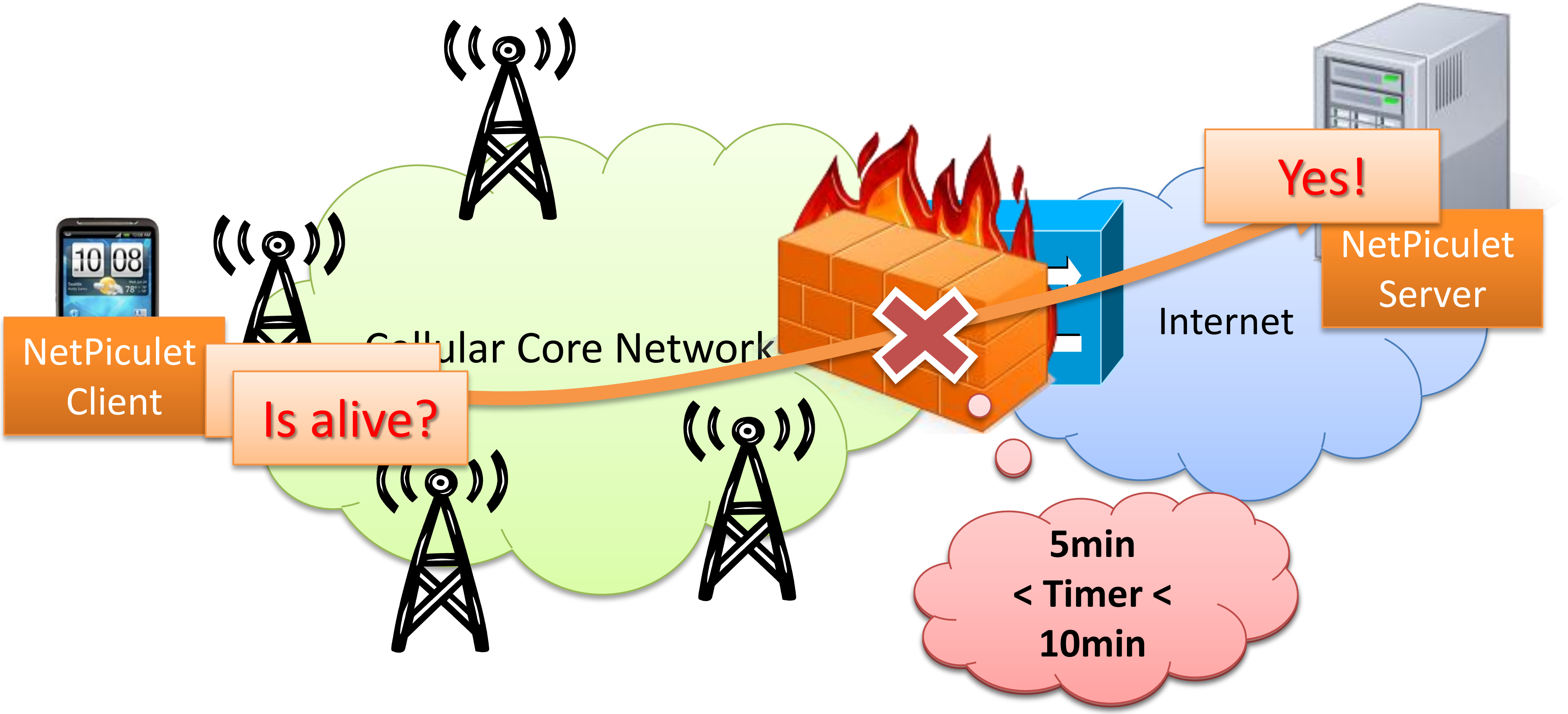
1. IP spoofing
2. TCP connection timeout
3. TCP out-of-order buffering
4. NAT mapping

Why short TCP timeout timers are bad?



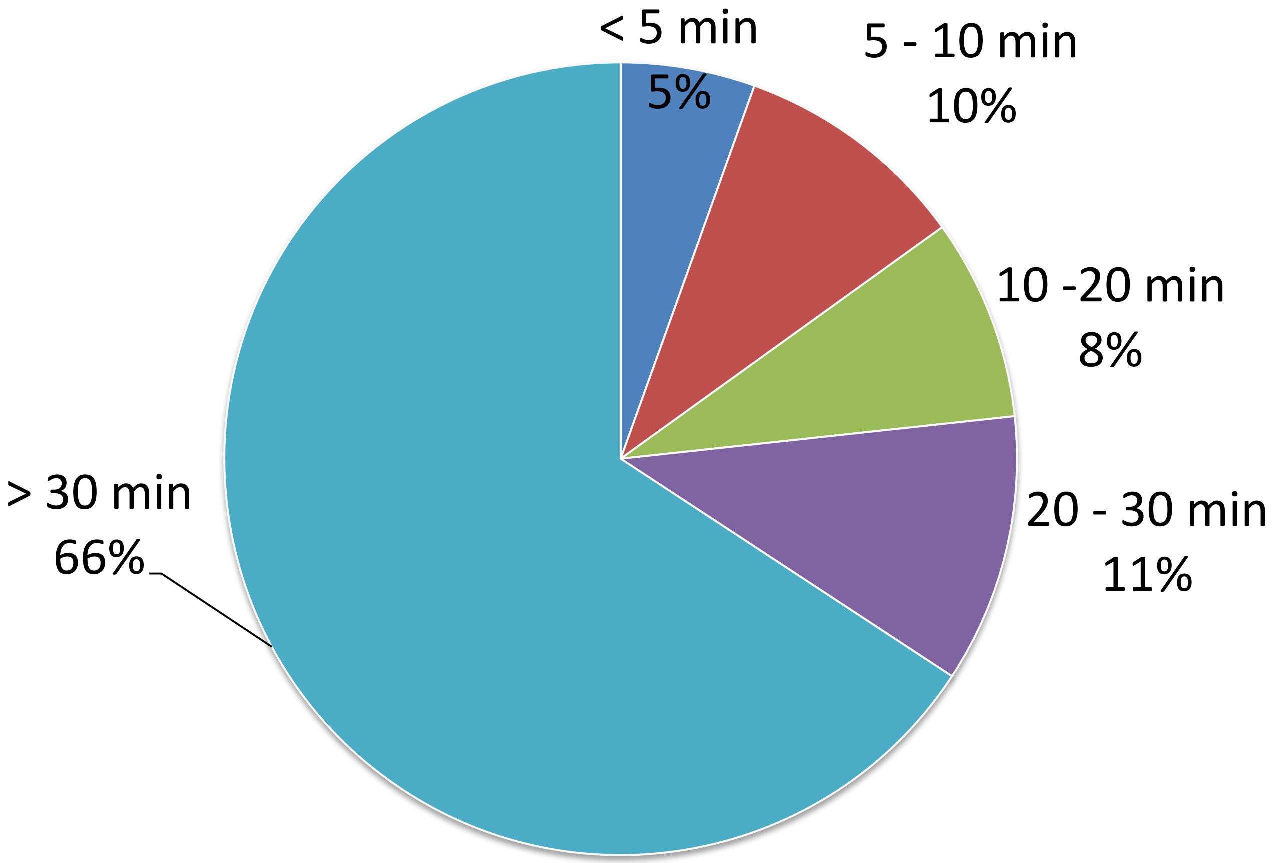
Measure the TCP timeout timer

Time = 10min



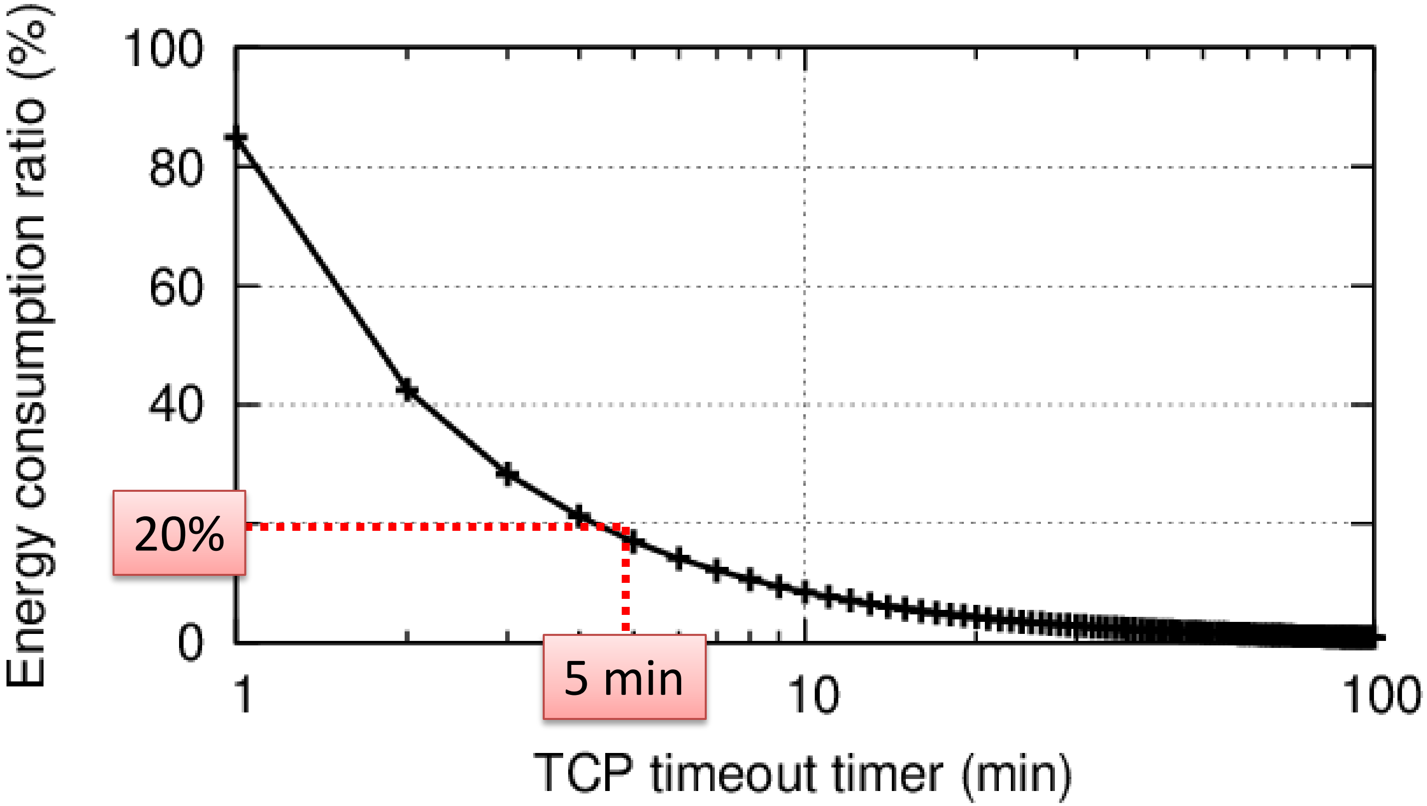
Short timers identified in a few carriers

4 carriers set timers less than 5 minutes



Short timers drain your batteries

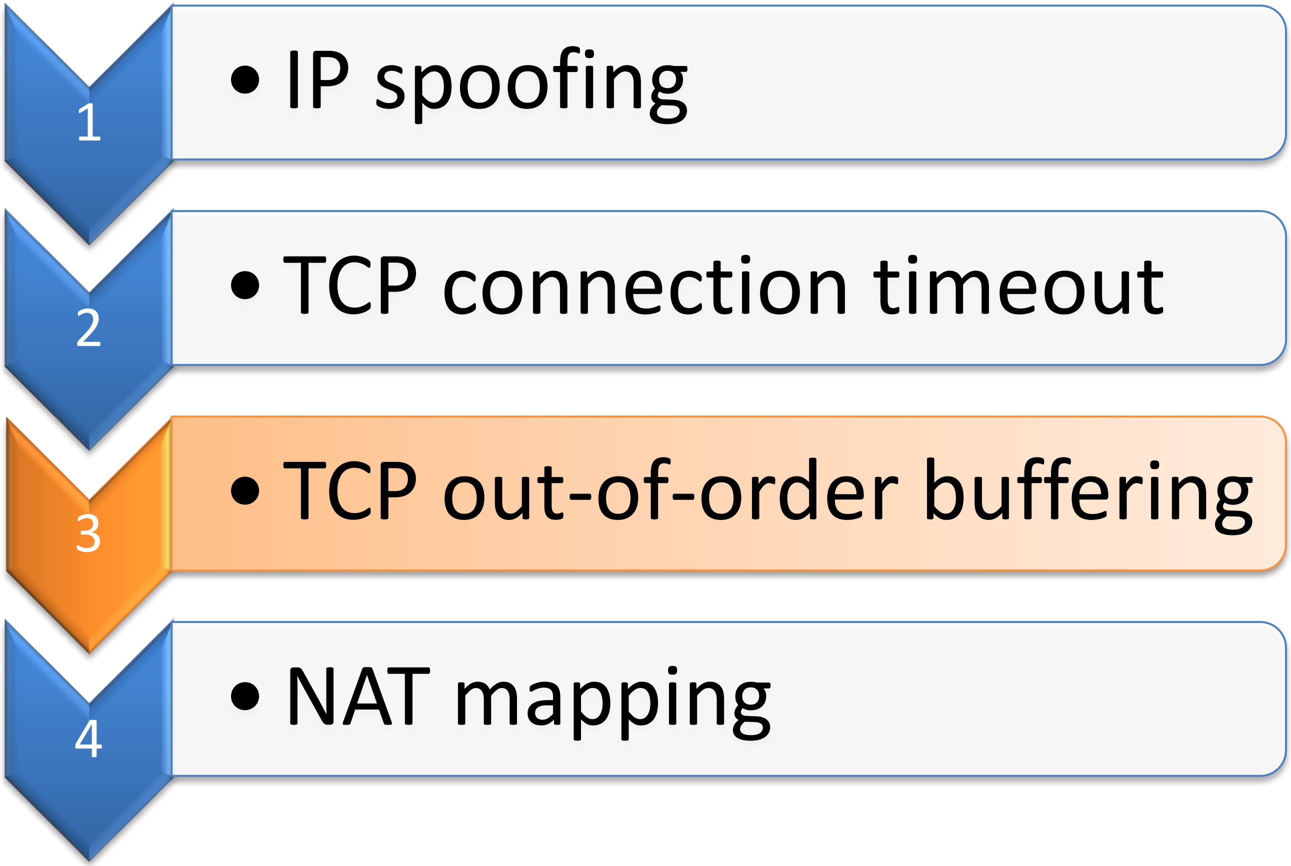
- Assume a long-lived TCP connection, a battery of 1350mAh
- How much battery on keep-alive messages in one day?



20%

5 min

Outline



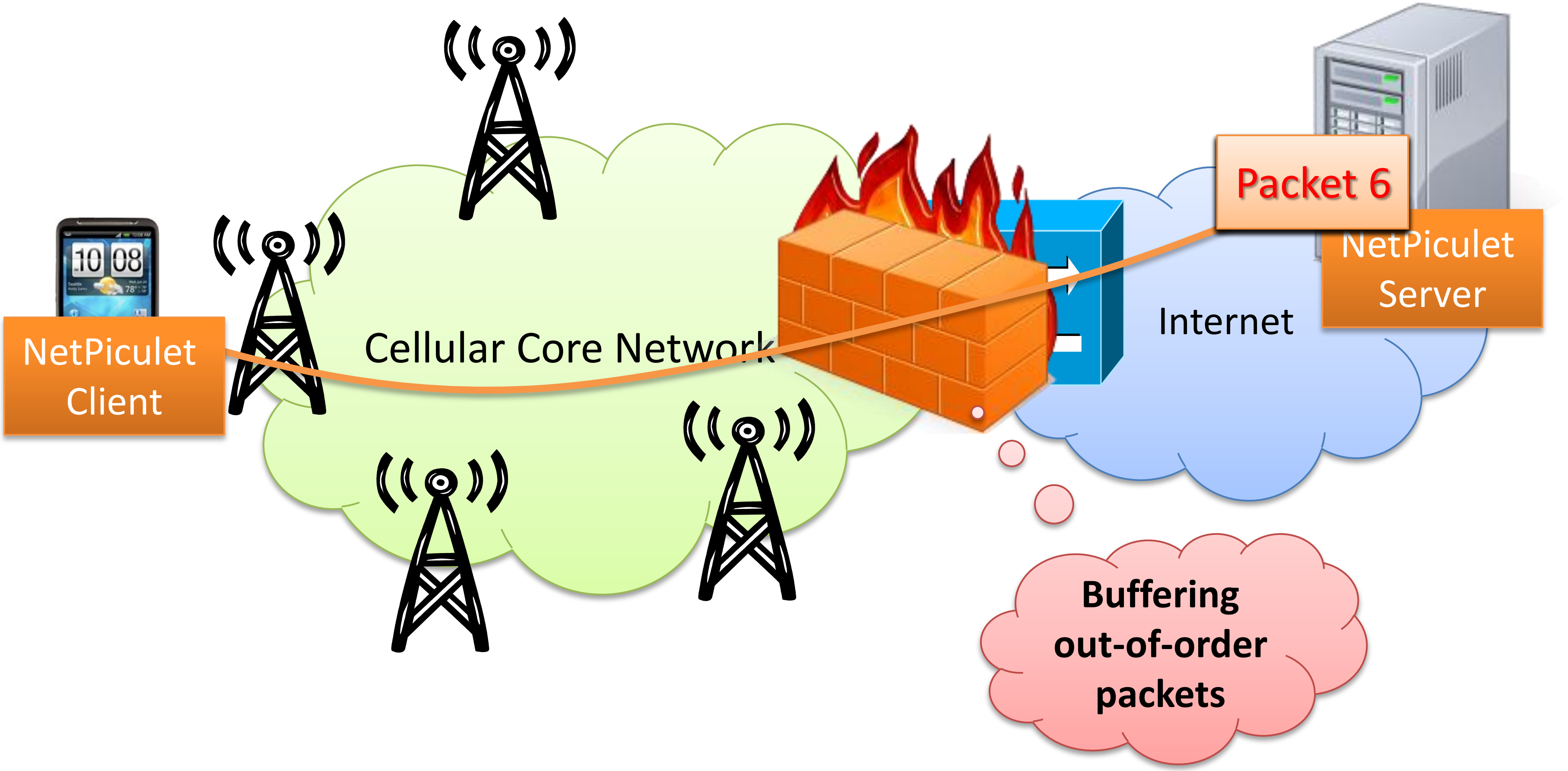
1
- IP spoofing

2
- TCP connection timeout

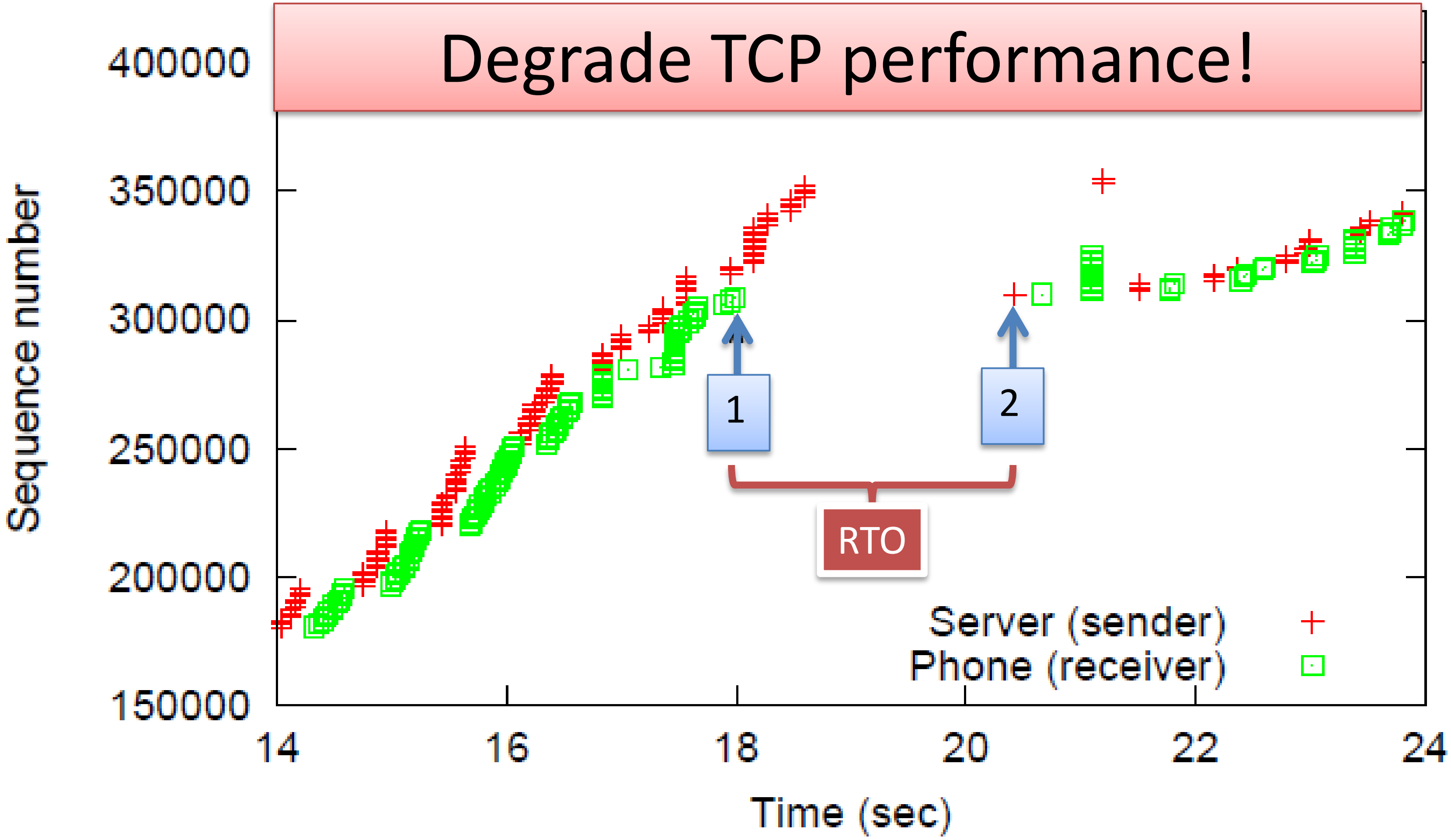
3
- TCP out-of-order buffering

4
- NAT mapping

TCP out-of-order packet buffering



Fast Retransmit cannot be triggered



Degrade TCP performance!

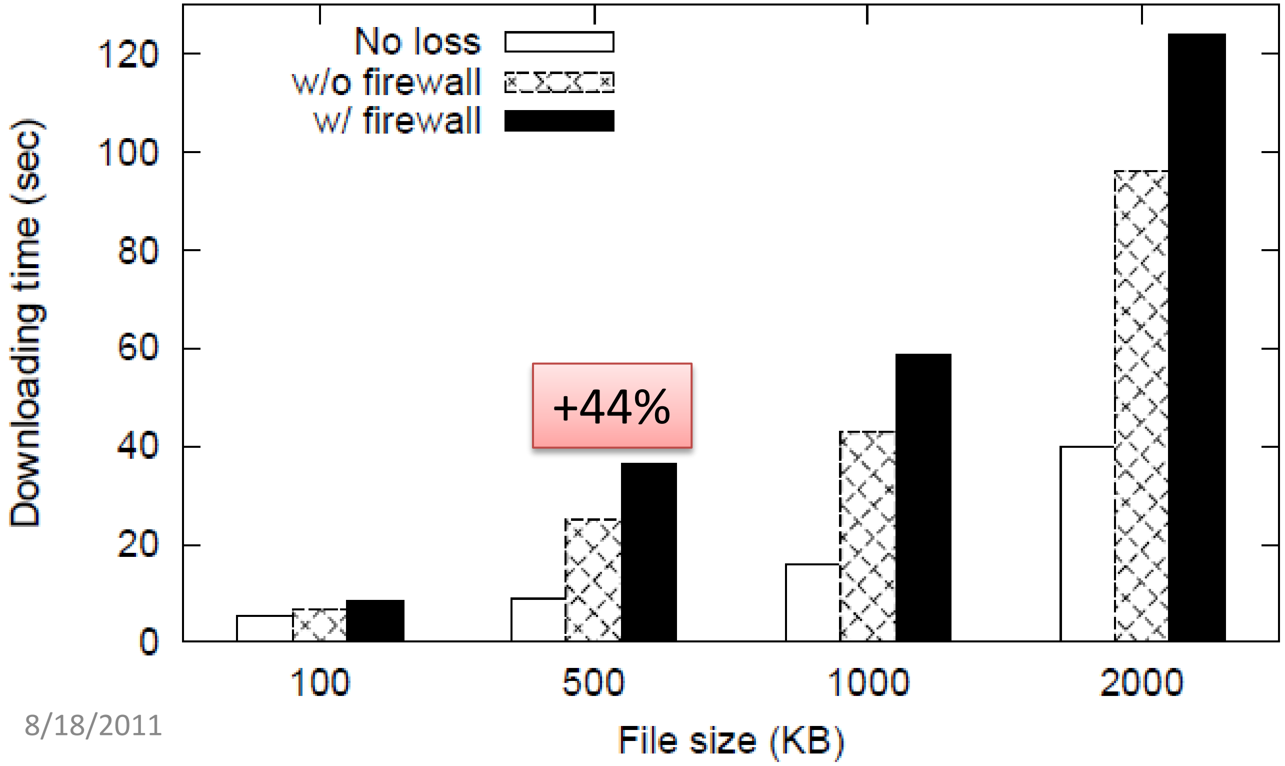
1

2

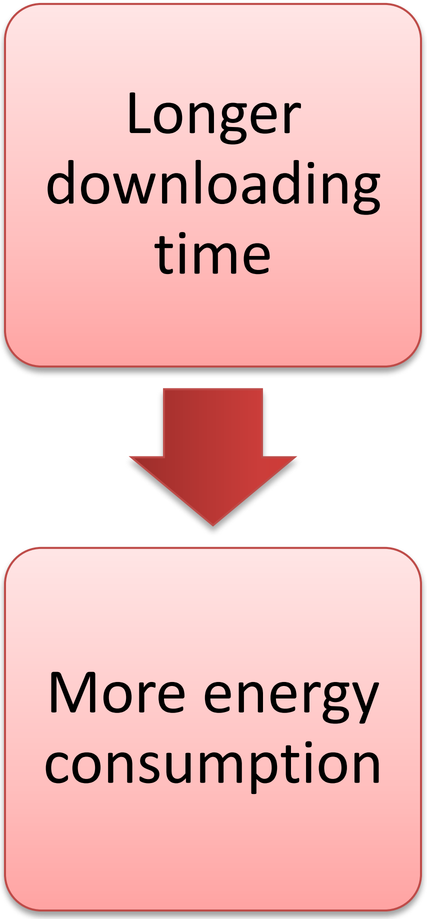
RTO

TCP performance degradation

- Evaluation methodology
  - Emulate 3G environment using WiFi
  - 400 ms RTT, loss rate 1%



+44%



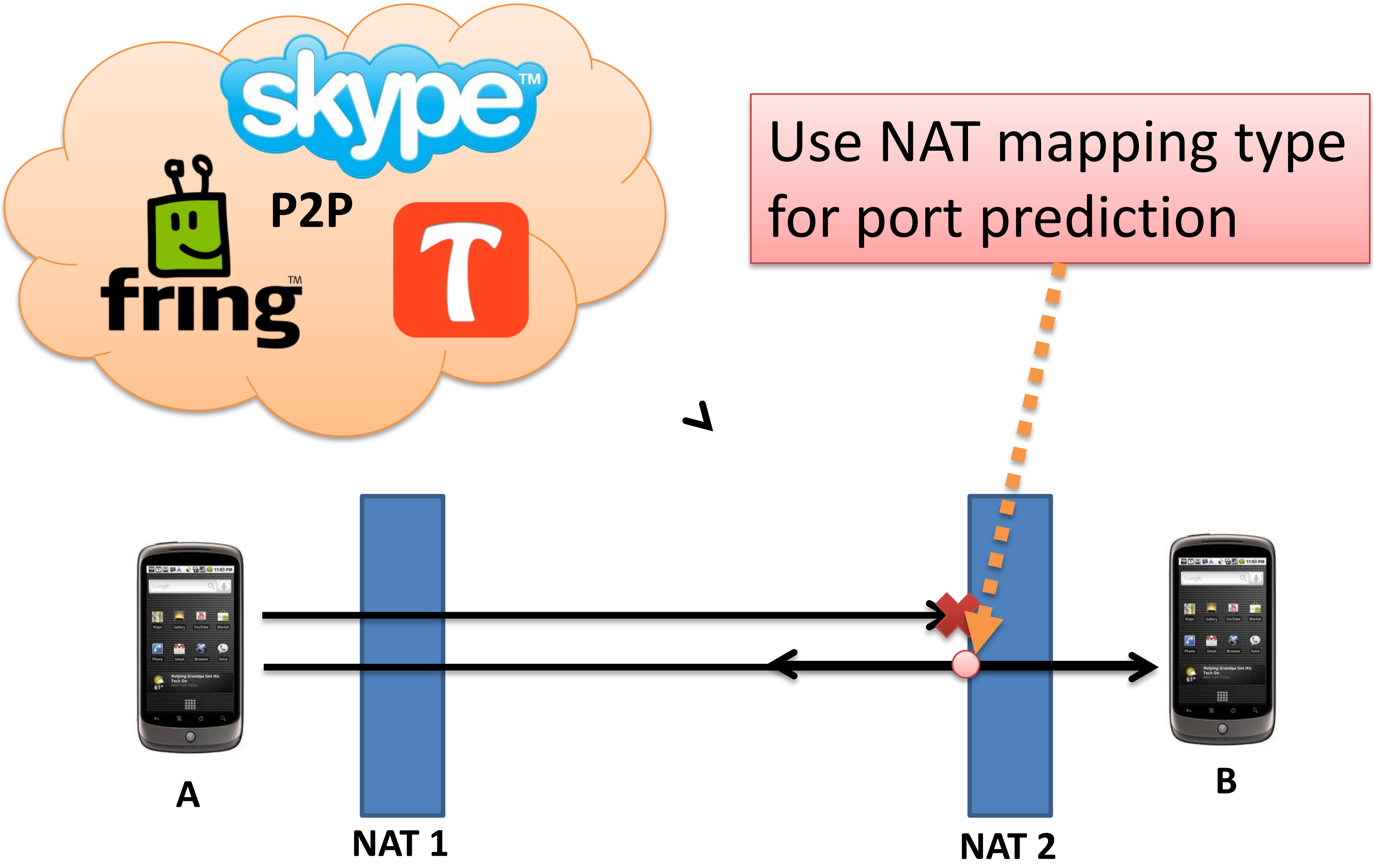
Longer downloading time

More energy consumption

Outline

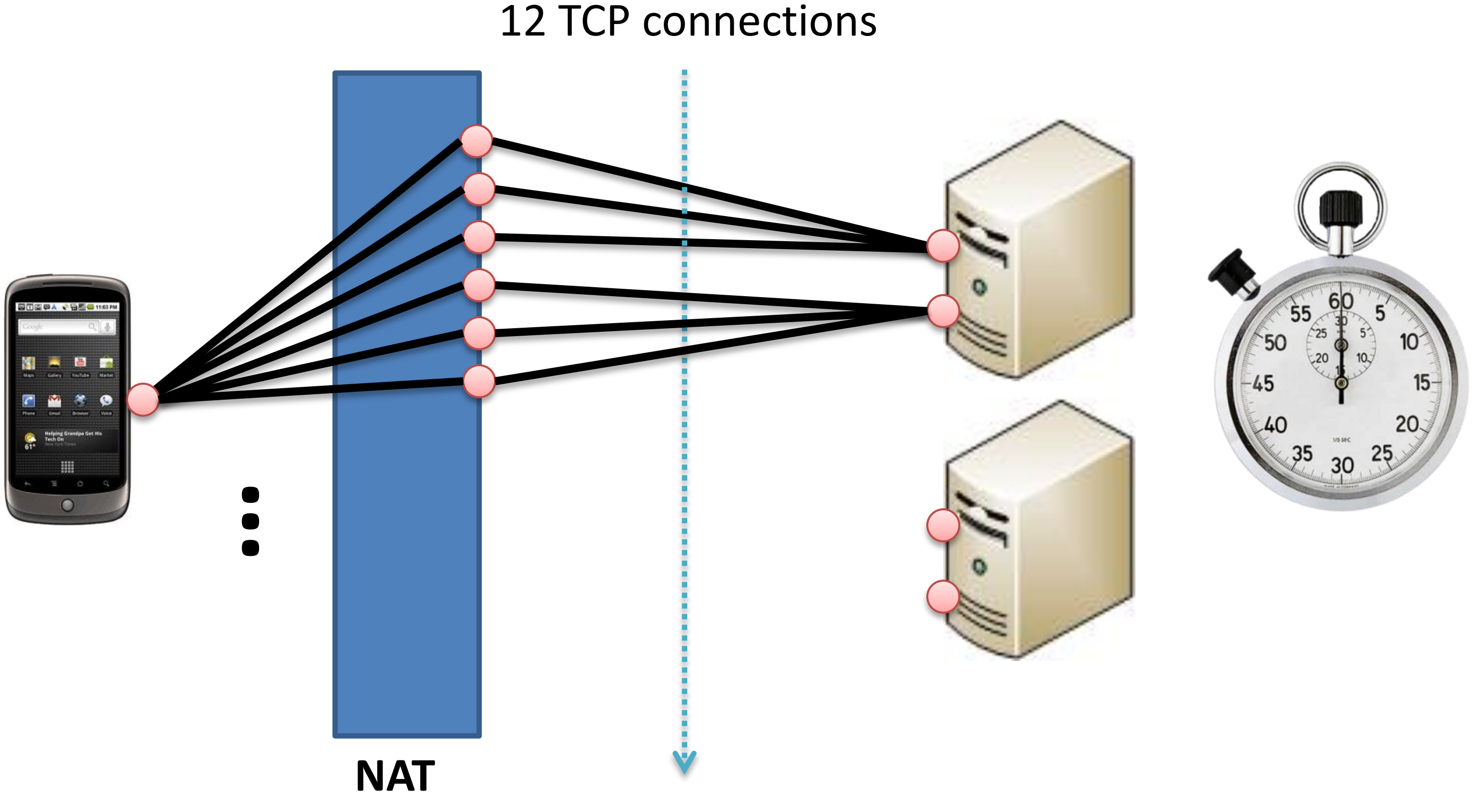
1. IP spoofing
2. TCP connection timeout
3. TCP out-of-order buffering
4. NAT mapping

NAT mapping is critical for NAT traversal



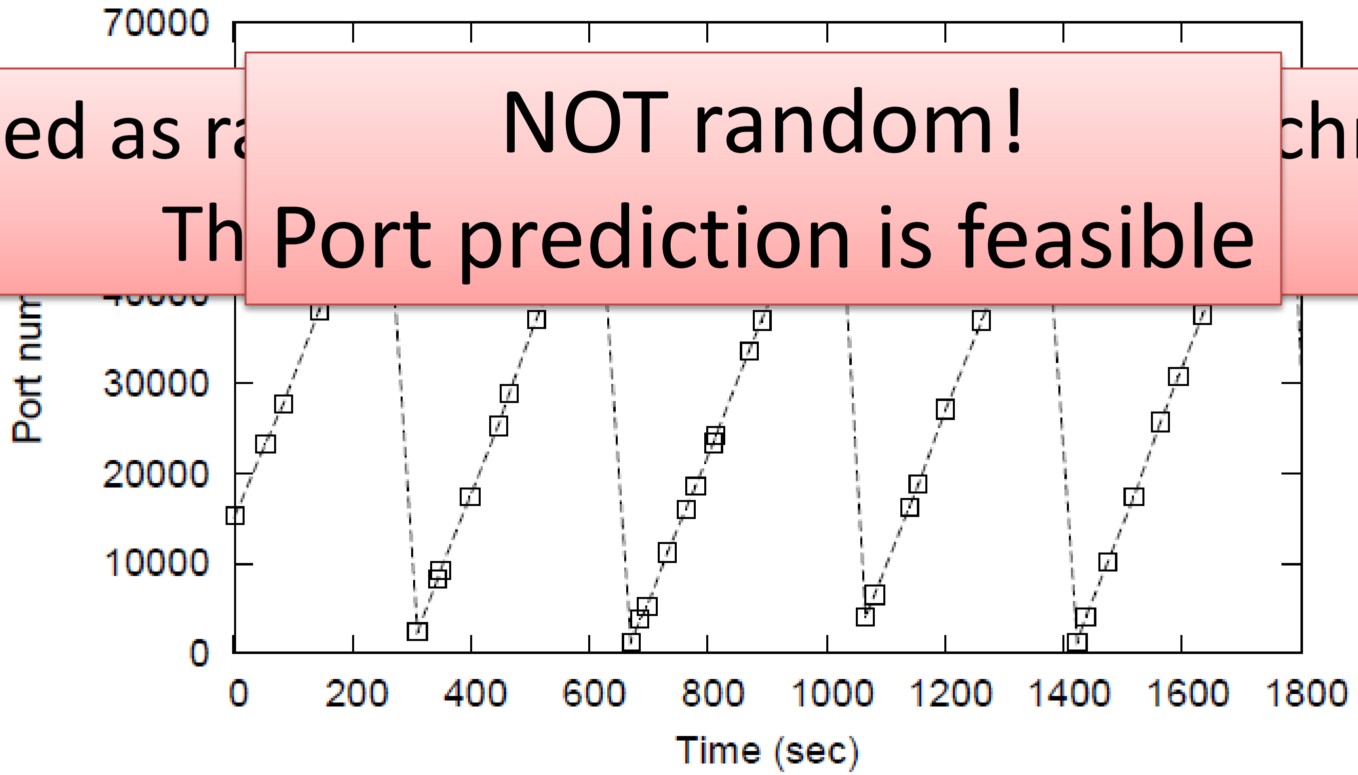
What is NAT mapping type?

- NAT mapping type defines how the NAT assign external port to each connection



Behavior of a new NAT mapping type

- Creates TCP connections to the server with random intervals
- Record the observed source port on server



Treated as ra chniques

Th

NOT random!

Port prediction is feasible

Lessons learned

Firewall	IP spoofing creates security vulnerability **IP spoofing should be disabled**
	Small TCP timeout timers waste user device energy **Timer should be longer than 30 minutes**
	Out-of-order packet buffering hurts TCP performance **Consider interaction with application carefully**
NAT	One NAT mapping linearly increases port # with time **Port prediction is feasible**

Conclusion

- We built NetPiculet, a tool that can accurately infer NAT and firewall policies in the cellular networks
- NetPiculet has been wildly deployed in hundreds of carriers around the world
- We demonstrated the negative impact of the network policies and make improvement suggestions

Thank you!

zgw@umich.edu

http://mobiperf.com