Table of contents

- Introduction
  - 4G
  - (D)DoS attacks
- Motivation
- Approach
- Results
- Conclusion
- Questions

Fourth Generation (4G)

- Live implementations; Wimax and LTE
- LTE is commonly used in the Netherlands

(D)DoS

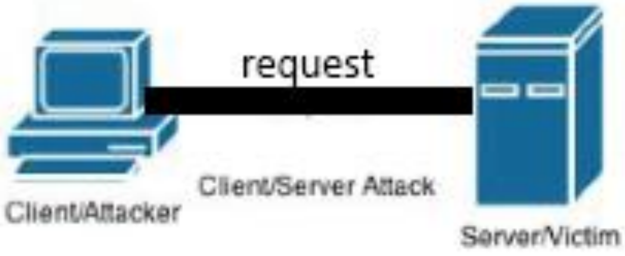
- Denial Of Service: An attack designed to render a computer or network incapable of providing normal services*.

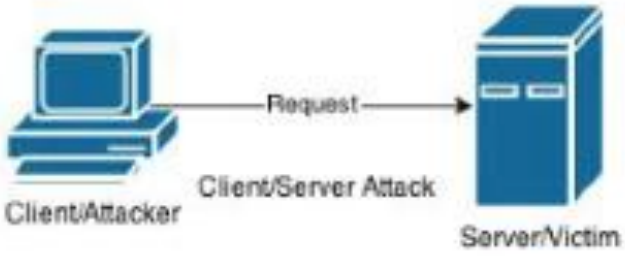
* Described by the Internet Engineering Task Force (IETF)

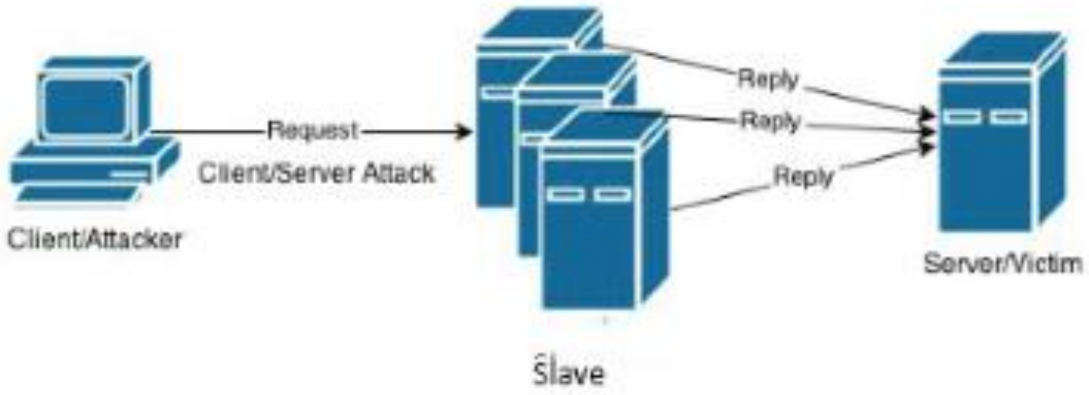
(D)DoS Categorization

Attack Type	Attack name
Bandwidth attack	ICMP, UDP Fragment, UDP Flood
Resource attack	HTTP Get, POST, Fin, Push, Head, Syn, Ack, Push, Rst
Distributed amplification attack	Chargen, DNS, NTP

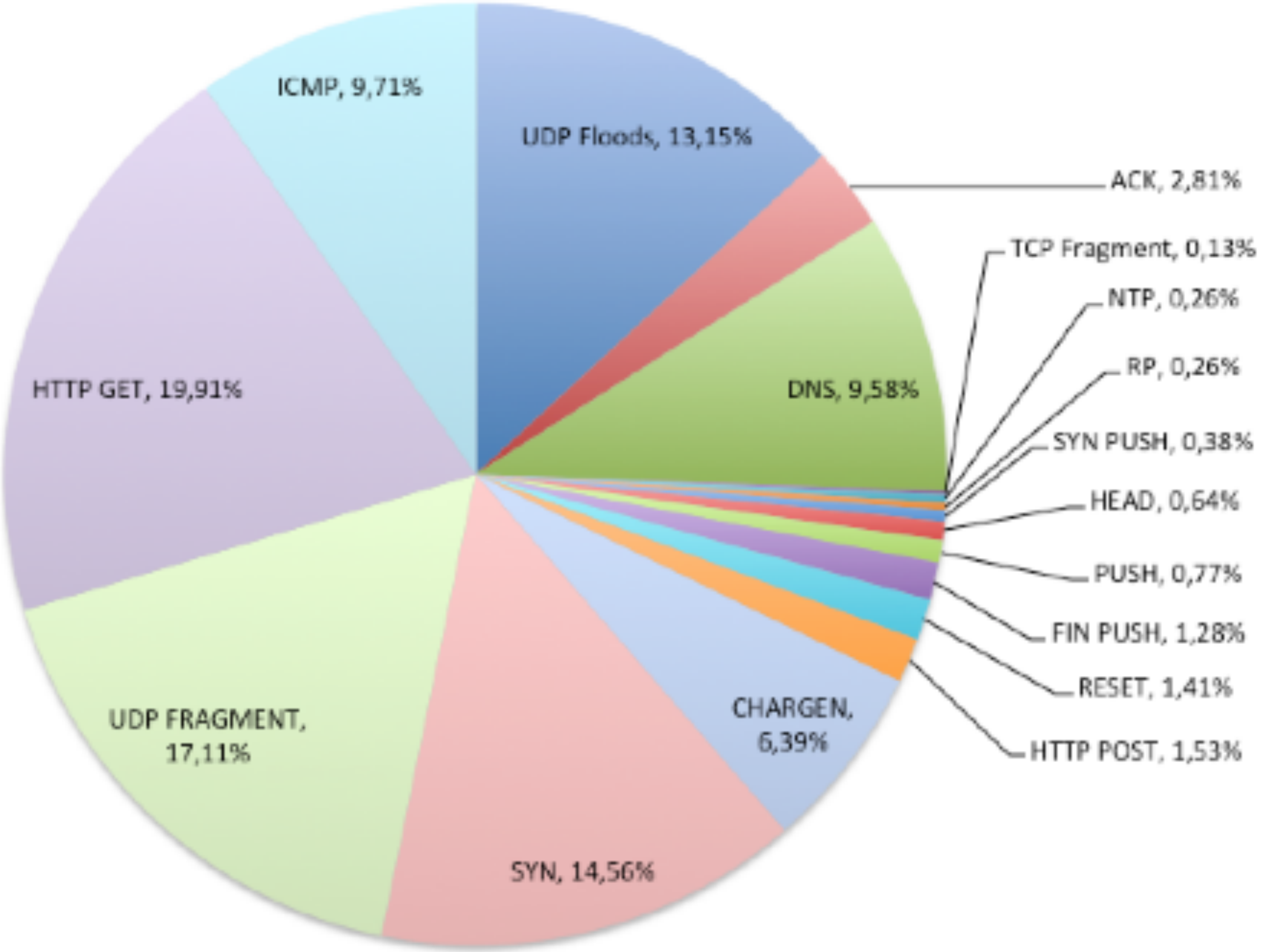
(D)DoS


request
Client/Attacker
Client/Server Attack
Server/Victim


Request
Client/Attacker
Client/Server Attack
Server/Victim


Request
Client/Server Attack
Client/Attacker
Reply
Reply
Reply
Slave
Server/Victim

(D)DoS


ICMP, 9,71%
UDP Floods, 13,15%
ACK, 2,81%
TCP Fragment, 0,13%
NTP, 0,26%
RP, 0,26%
DNS, 9,58%
SYN PUSH, 0,38%
HEAD, 0,64%
PUSH, 0,77%
FIN PUSH, 1,28%
RESET, 1,41%
HTTP POST, 1,53%
CHARGEN, 6,39%
SYN, 14,56%
UDP FRAGMENT, 17,11%
HTTP GET, 19,91%

Motivation

- Amount of recent (D)DoS attacks
- Uprising of 4G speed and useage
- Anonymity can be bought

  Mobile Prepaid Cards in shops

Research Question

- What are the possibilities for (D)DoS attacks and mitigation techniques on LTE networks, and how do they differ from wired connections?

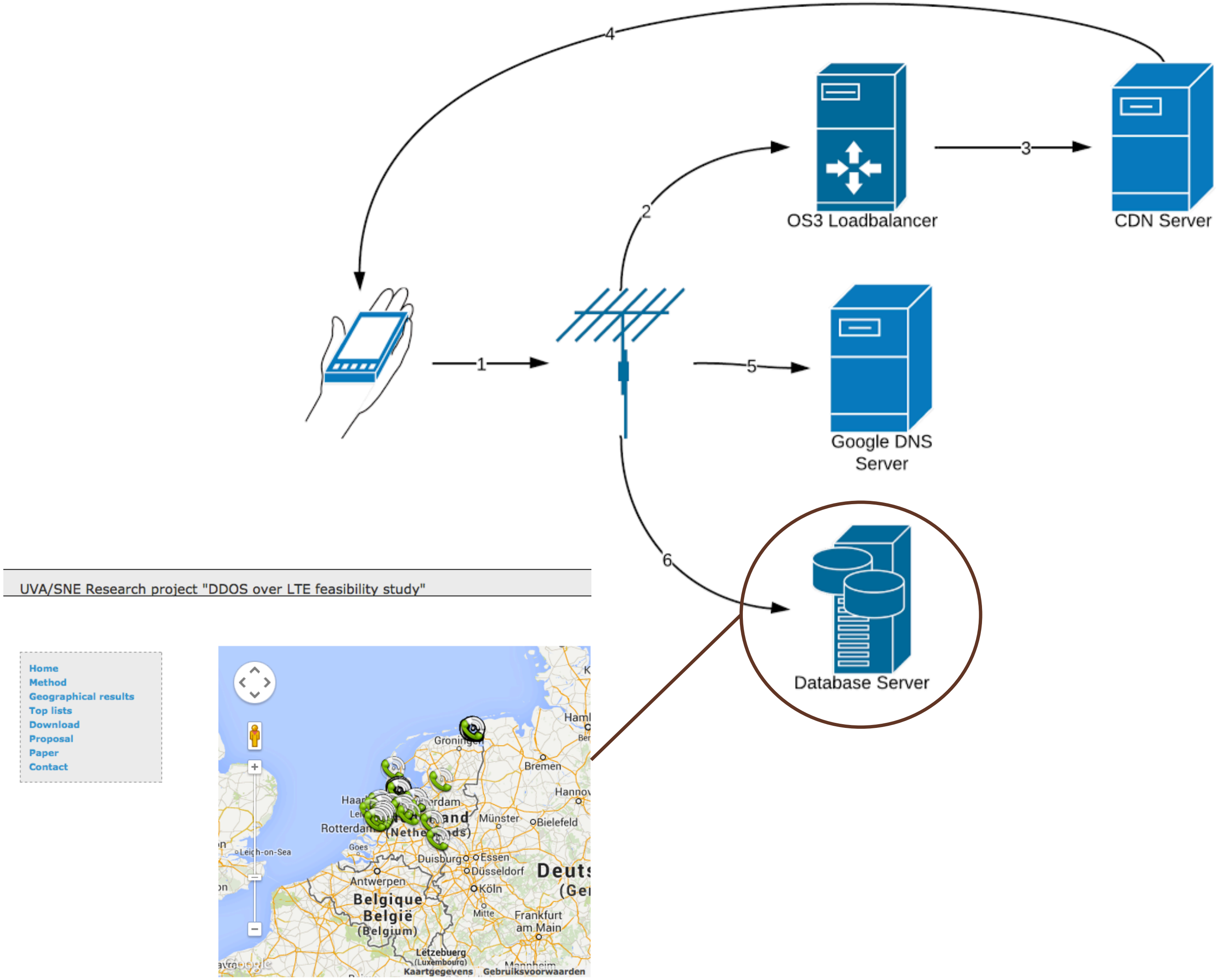
Approach 4G measurements

- Measurements of the different 4G networks

- The app measures* :
  - Upload
  - Download
  - Jitter
  - Delay
  - and more

*Due to time restrictions more data is gathered than nescesary.

Approach 4G measurements



UVA/SNE Research project "DDOS over LTE feasibility study"

- Home
- Method
- Geographical results
- Top lists
- Download
- Proposal
- Paper
- Contact

Results

Total Test results	916
Download speed	24,95 Mb/s
Upload speed	6,04 Mb/s
Jitter	7345,56 ms
Latency	139,74 ms
Loss	0,16 %

	Upload in Mb/s	Jitter in ms	Loss in %
KPN	5,3	2259	0,02
T-Mobile	7,4	271	0,24
Vodafone	6,50	20136	0,37

Results

	Lower Bound	Upper Bound
KPN	24	29
T-Mobile	14	15
Vodafone	21	27

Phones needed for 100Mb/s data with 95% confidence interval

Approach

- Bandwidth Attack: UDP Flooding
- Resource: TCP SYN Attack
- Amplification: DNS Amplification

Results

- Bandwidth Attack: UDP Flooding

  21 Mb/s

- Resource: TCP SYN Attack

  SYN attack mitigation

- Amplification: DNS Amplification

  Network Ingress Filtering

Conclusion

The possibilities differ per provider, Vodafone has the best security.

Bandwidth attack	☑
Resource attack	☒
Distributed amplification attack	☒

Conclusion

Other providers do not filter this much, this is limitedly tested.

	Vodafone	T-mobile	KPN
Bandwidth attack	☑	?	?
Resource attack	☒	?	?
Distributed amplification attack	☒	?	?

Questions?

What about mitigation techniques?

Because 4G is IP based, all IP mitigation techniques are useable.

However, some data can be mitigated because it is unlikely to appear in 4G networks (e.q DNS AXFR)