University of Amsterdam

System and Network Engineering

(Distributed) Denial of Service attacks via 4G/LTE network

Authors:
Wouter van Dullink
Rawi Ramdhan

Abstract

Long-Term Evolution (LTE) is the fourth generation of mobile telecommunications technology. (Ab)using the anonymity that prepaid cards provide and the high speed of 4G networks, (D)DoS attacks via 4G networks could be just as harmful as wired connections, but with the added risk that anonymity can be bought.
Common (D)DoS attacks are divided in three categories; Bandwidth, Resource and Distributed Amplification -Attacks. Via LTE network measurements, the most promising attack for each category is chosen. For each attack a practical implementation on the Android operating system is provided. Tests with these applications show that Vodafone mitigates two out of three attacks, were other providers mitigate less. LTE network measurements indicate that T-Mobile provides the best network characteristics for a (D)DoS attack over LTE. Furthermore they provide information on the necessary phones needed for a 100 Mb/s bandwidth attack per provider, for which T-mobile needs the least amount.
This research also discusses LTE specific mitigation techniques which might result in a safer network infrastructure.

1 Introduction

4G, short for fourth generation, is the fourth generation of mobile telecommunications technology. The requirements for 4G are specified in the International Mobile Telecommunications Advanced (IMT-Advanced) [5]. Specific requirements include; based on Internet Protocol (IP), packet switched, 100 Mb/s download speed for moving clients and 1Gb/s download speed for stationary clients. Current implementations do not always adhere to the standard, specifically not to the download speeds. Currently there are two 4G capable technologies; Worldwide Interoperability for Microwave Access (Wimax) and Long-Term Evolution (LTE) Advanced. The latter one is used in the Netherlands and therefore in this research. There have been many Distributed Denial of Service ((D)DoS) attacks in the last few years [32], mainly via botnets. Botnets provide both the necessary speed and power, but also make it hard to identify the attacker. Due to this the attacks are sometimes difficult to mitigate and the attackers hard to find.
(Ab)using the anonymity that prepaid cards provide and the high speed of 4G networks, (D)DoS attacks via 4G networks could be just as harmful as via wired connections, but with the added risk that anonymity can easily be bought. Computers need to be hacked to form a botnet, but prepaid cards can be purchased in stores. Wireless networks do differ from wired networks; speed, latency, reliability and bandwidth [27] make them possibly less suited for a (D)DoS attack.

1.1 Research question

The goal of this research is to answer the following questions:

What are the possibilities for (D)DoS attacks and mitigation techniques on LTE networks, and how do they differ from wired connections?
To answer this question several sub questions need to be answered, this is done in the following structure:

Based on literature studies, (D)DoS attacks will be explain in chapter 2 and the LTE techniques in chapter 4. In chapter 6 the networks characteristics results are described. These three chapters combined provide an answer to the following questions:

- What type of (D)DoS attacks and prevention methods are there?
- What are the characteristics of the LTE networks from KPN, Vodafone and T-Mobile?

With the answers to these questions the most feasible (D)DoS attack on the LTE networks of the dutch providers will be chosen. In chapter 7 a (D)DoS proof of concept setup is explained. The results of this are discussed in chapter 8. In chapter 9 the conclusion is written and the final question is answered:

- How do these kind of attacks and mitigation techniques differ from a wired connections?

2 (D)DoS

A Denial Of Service is described by the Internet Engineering Task Force (IETF) as an attack designed to render a computer or network incapable of providing normal services [16].

2.1 (D)DoS Summary

This section briefly describes the most common (D)DoS attacks as shown in figure 1. With this overview the network requirements for a successful (D)DoS attack can be determined. Further research on LTE characteristics can provide detailed information on these attacks in regards to the Dutch LTE providers (KPN,

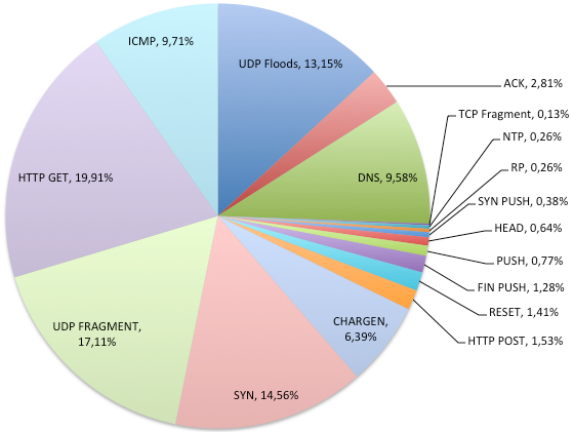

Figure 1: Most used (D)DoS attacks [32]

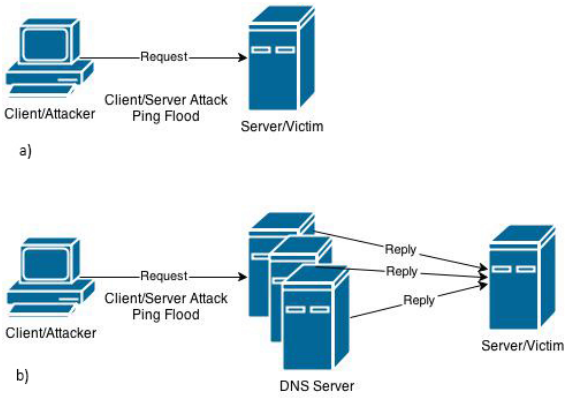

Figure 2: Two (D)DoS scenarios:
a) Direct attack
b) Attack where a slave is used.

Vodafone and T-Mobile). A more detailed description of these (D)DoS attacks can be found in appendix A .
There is a lot of research done on (D)DoS attacks [17],[48],[25]. Papers regarding this subject describe the participants with different names. In this paper the following terms will be used:
Attacker: The initiator of the (D)DoS attack.
Slave: An entity that partakes in the attack, most of the time unknowingly (e.g. bots in a botnet).
Victim: An entity that experiences negative consequence of the attack. This can be a slow/unresponsive server or service. Figure 2a shows a client/attacker setup used for a Ping Flood attack. Figure 2b shows a setup where a server is abused as a slave. To process a domain name service (DNS) request, the response is sent to the victim and not to the attacker.

2.2 Resources

(D)DoS attacks aim to consume resources to take down a server/service. These resources can be; network bandwidth, Central Processing Unit (CPU) cycles, memory and file allocation. How much there should be consumed to take down a server/service is explained in the following paragrahps.

2.2.1 Network bandwidth

If there is too much network traffic the network buffers will fill up. These buffers are located in network devices (e.g. routers and network interface cards). Packets will spend more time in buffers and the network throughput will go down. When these buffers are full, the routers or receiver will start to drop packets. Depending on the protocol this could mean that packets are retransmitted, causing extra network traffic. In order to saturate network links, large packets have to be generated. The payload is the information that needs to be transferred, extra information (e.g. headers) is not part of the payload but is part of the packet. The exact payload size differs per protocol, Transmission Control Protocol (TCP) has a larger overhead than User Datagram Protocol (UDP) [8]. The maximum payload size for Internet protocol (IP) is 65.536 bytes (2 bytes in the total length header) the maximum packet size is further restricted by the maximum transmission unit (MTU). The MTU varies per vendor and

network but is usually around 1420 and 1500 bytes. Therefore to fill a 1Gb/s line $\frac{10^9}{1500+38}$ packets per second have to be generated.

2.2.2 CPU cycles

When a server receives network packets they have to be processed. To what extent these packets are processed by the Network Interface Card (NIC) or the CPU depends on the configuration. Some NICs support offload features which offload the CPU by calculating check sums or aggregate packets. Once it is clear that the packets have to be handled by the CPU an interrupt is generated, which notifies the CPU that data is ready for processing. There are optimisations to reduce the amount of interrupts or ensure better distribution for multicore processors [24]. Estimating the CPU load according to the amount of packets is difficult, there are a lot of local variables (e.g. NIC offload features and processor cores). However, for the slower CPUs the following rule of thumb can be used; 1 byte is 1 hz.[12].

2.2.3 Memory and file allocation

The amount of TCP sessions a server can handle is limited. The session has to be unique and consists of four variables; source port/IP and destination port/IP. In theory one client could generate 65.536 sessions to one server. Only the source port number changes, this is a 2 byte field in the TCP header. Multiple systems can generate more sessions. Every session gets a file descriptor, the maximum amount of file descriptor under Linux is defined in sysctl fs.file-max, default set to 300.000. This defines the maximum amount of active TCP sessions. However, before they become active they enter different stages [23]. The maximum amount of sessions in syn received state is defined in tcp_max_syn_backlog, default set to 256.
In order to calculate the amount of packets necessary to fill the backlog, the timeout time is required. This is defined in tcp_synack_retries and depends on the number of retransmissions. Its default value is set to 5 for most Linux operating systems, which causes the half-open connection to be removed after 3 minutes [13]. In order to crash a TCP service via a syn attack $\frac{256}{180}$ packets per second are needed.

2.2.4 Used attacks

Table 1 shows the different (D)DoS attack forms and types, and how important the bandwidth, availability and latency is in relation to LTE.
To test if a (D)DoS attack can be performed on a LTE network the following attacks are chosen based on the characteristics; UDP Floods, SYN attack and DNS Reflection attack.
The selection is based on the most used (D)DoS attacks listed in Figure 1 and the characteristics: bandwidth, availability and latency. There are attacks which are slightly more common (Hyper Text Transfer protocol (HTTP) Get, UDP Fragment) but cannot be performed without causing disturbance on the providers network. Therefore no proof of concept is created for these attacks.

1. Bandwidth Attacks - UDP Floods: Bandwidth and availability are important for this attack. Without a continuous stream of packets the server has time to process the data. The amount of delay is not important as long as this is constant. However, jitter (variance in delay) is important. Therefore low jitter is necessary for a successful attack.
2. Resource Attacks - SYN: The upload speed is crucial for this attack, therefore the bandwidth is important. If there are not enough packets generated, the server has time to process the requests. This also holds for the availability. If the connection drops the packets can be processed

Attack Type	Attack name	Bandwidth	Availability	Jitter
Bandwidth Attacks	ICMP, UDP Fragment, UDP Flood	++	++	+
Resource Attacks	HTTP GET, POST, FIN PUSH, HEAD,SYN,ACK,SYN PUSH, RST	++	++	+
Distributed Amplification Attacks	Chargen, DNS, NTP	+	+	-

Table 1: Relative weight of network metrics in relation to (D)DoS attack types

and the attack looses its strength. Latency is less important, the packets must arrive but delay is not an issue. Just like the Bandwidth attacks jitter is important.

3. Distributed Reflector Attacks - DNS: With a DNS attack a small request is sent but the reply is bigger [21]. Due to the amplification factor bandwidth is less important than with bandwidth attacks. Availability is not a problem for the attacker, as long as the slaves are available.

2.3 List of (D)DoS Attacks

The attacks can be categorised in three types; Bandwidth , IP spoofed, protocol and distributed Amplification -attacks. Some attacks can be categorised into more types but their classification is based on the most important characteristic.

- With Bandwidth Attacks the goal is to send excessive volume of useless traffic to consume network resources, eventually resulting in a non-responsive server/service.
- In IP Spoofed Attacks the attacker modifies the source address to hide his identity [42], making it hard to distinguish packets sent by a legitimate user [22]. It is also a method to force the response of the attack to a different IP address.
- With a protocol attack resources like CPU and memory are consumed to take down a service/server.
- In Distributed Amplification Attacks the attacker does not flood the victim, but uses other servers (slaves) as reflectors to do this. For example; NTP (Network Time Protocol) and DNS -servers can be used as reflectors. The attacker uses the challenge-response method [38] during this attack but with a subtle change. The attacker changes the source address of the request packets (spoofs) with that of the victim, and sends them to the slaves. Because the IP address is changed the slaves reply (reflect) to the victim instead of the attacker.

3 (D)DoS Mitigation techniques

There is not only a large variety in (D)DoS attacks, also the prevention mechanisms are widely spread. The mitigation techniques can be broadly divided into two categories [15], general solutions and filtering.
General solutions are common prevention measures that individual servers and ISPs should follow [14] (e.g. patch security holes, update your application to the latest version). Filtering techniques include; ingress filtering, egress filtering, router based packet filtering.
The International Telecommunications Union-

Radio communications sector (ITU-R) specified a set of requirements for 4G standards. These include that all implementations should be IP based and packet switched. All mitigation techniques (General solutions and Filtering) are developed to work on packet switched and IP based networks. Therefore, there is no difference in mitigation techniques on wired and 4G networks at first sight. However, the content that can be expected over 4G differs from wired networks, especially for prepaid cards. For example it is highly unlikely that DNS slave servers are connected via private subscriptions. In general it is therefore possible to filter DNS AXFR requests from the cellular networks.

4 LTE

LTE is developed by the third Generation Partnership Project (3GPP) and is the newly evolved technology for mobile devices. This new technology is developed with the following motivations [18]:

- Need to ensure the continuity of competitiveness of the 3G system for the future.
- User demand for higher data rates and quality of service.
- Packet Switch optimised system.
- Continued demand for cost reduction (CAPEX and OPEX).
- Low complexity.
- Avoid unnecessary fragmentation of technologies for paired and unpaired band operation.

To get higher down/up-load speeds for LTE (compared to 3G) there are some technical solutions implemented [39]:

1. Orthogonal Frequency Division Multiple Access (OFDMA) for downlink data transmissions.
2. Single Carrier Frequency Division Multiple Access (SC-FDMA) for up-link data transmissions.
3. Multiple Input Multiple Output (MIMO)

A brief explanation of the inner workings of these techniques can be found in the appendix C. In general the assumption is that the average user will download more information than they are uploading. For this research the upload speed is very important because most (D)DoS attack require a lot of data transmission.

4.1 SC-FDMA

LTE up-link requirements differ from those of down-link due to low power consumption requirement at User Equipment (UE). SC-FDMA [10] is chosen for up-link because it combines the low peak-to-average ratio techniques of single-carrier transmission systems, such as Code division multiple access with the multi-path resistance and flexible frequency allocation of OFDMA.
To fulfil the requirement such as coverage, robustness, capacity and high data rates, LTE uses different multiple antennas with the MIMO technique. More information about this technique can be found in appendix C.

4.2 Peak Data Rates

In the Netherlands only Frequency Division Duplex (FDD) is used. A full comparison between the two techniques (FDD and TDD) can be found online [20].
national coverage is achieved by mixing different frequencies [40]. Lower frequencies have a longer range but lower speed. The opposite is true for higher frequencies. Therefore distance to the antenna is not the only limiting factor in the bandwidth speeds. The peak upload rates for various channel bandwidths and antenna options for FDD-LTE are shown in table 2. Peak download rates can be found in appendix, table (13). Even though the theo-

Channel Bandwidth Mhz		1,4	3	5	10	15	20
Number of Resource Blocks		6	15	25	50	75	100
Modulation	MIMO	Data Rates, Mb/s					
QPSK	Not used	1,8	4.5	7.5	15	22.5	30
16 QAM	Not used	3,45	8,64	14.4	28,8	43,2	57,6
64 QAM	Not used	5,184	12,96	21,6	43,2	64,8	86,4

Table 2: Peak Upload Data Rates for FDD-LTE

retical maximum upload speed is given by the protocol, ISPs have further limited this. No information regarding the upload speed is advertised by the providers.

5 LTE Test

The previous chapters describe the necessary bandwidth characteristics for a successful (D)DoS attack. This chapter explains the method that will be used to test the bandwidth characteristics of LTE. With this data the most feasible (D)DoS attack can be chosen.

5.1 Application

An Android application is developed for this project, that measures various network characteristics; download and upload -speed, jitter, delay, round-trip time (RTT) and loss. Extra information as GPS coordinates, LTE signal strength and service provider is gathered in order to determine the best provider for executing (D)DoS attacks.
The application will gather information on; download and upload -speed, Jitter from a content delivery network (CDN) server in Amsterdam. The RTT and packet-loss are determined via the Google DNS servers. Finally all data is uploaded to a database and in real time available online (see figure 3).

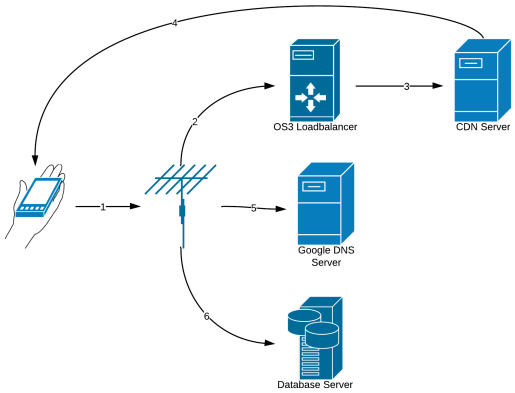

Figure 3: LTE test method

5.1.1 Download

Bandwidth measurements can be done via several protocols. In this research the packets have to traverse the Internet, therefor Ethernet and IP encapsulation are mandatory. Any other encapsulation (e.g. TCP or UDP) is optional. Raw data transfer would provide the most accurate bandwidth measurement but features like payload size and retransmissions have to be programmed manually. TCP may not provide the most accurate data regarding troughput, due to the retransmit features and the different types of TCP implementations. However it will provide real-life results, as most of the Internet traffic is TCP [49]. Therefore TCP is chosen.
Determining the download speed begins with downloading the smallest sample file (128 KB).

If it takes less than eight seconds, the next sample will be tried. The sample file sizes are: 128 KB, 256 KB, 512 KB, 1, 2, 4, 8, 16, 32, 64 and 128 MB. Among all downloaded samples only the last one, which took more than eight seconds, will be accepted. The download speed is based on the last sample file. After this, the upload speed is tested.

5.1.2 Upload

Half of the last downloaded sample file will be sent back to the server and the upload speed will be calculated.

5.1.3 Jitter and delay

Jitter is the variation in latency. A network with constant latency has no variation and therefore no jitter. Zero jitter means the results were exactly the same every time, and anything above zero is the amount by which they varied. The latency is measured ten times. The jitter is the variance of these ten latency values in milliseconds.

5.1.4 Loss and Round Trip Time

It is difficult to determine packet loss via TCP, as the protocol itself takes care of retransmits. Internet Control Message Protocol (ICMP) on the other hand is made for network tests. Therefor Loss and RTT are measured by sending ten ICMP echo request messages and measuring their response time. The absence of an acknowledge will be administrated as packet-loss.

5.2 Phones and locations

LTE phones from different vendors (Samsung, Sony, Archos) and sim-cards from different providers (T-Mobile, KPN, Vodafone) will be used. The application will be installed on these phones and put in different locations. In order to gather more results the app will be published in the software repository of Android.

6 LTE test results

As explained in the previous chapter an Android application is written to test the characteristics of the LTE network. More network variables were gathered than necessary, this is due to the parallel approach in researching (D)DoS attacks and gathering data. First the overall results are discussed. Then the results necessary for this research are deeper explored. After this a possible use for the other metrics is given, ending with a conclusion.

6.1 Results

In 11 days a total of 2940 test results were collected. These results include tests that were performed during development and finalising of the application. The following results were therefore removed; duplicate uploads (374), missing IP (5), Vodafone provided sim-cards (890 test results)[1], speed measurements via wifi (247) and via 3G (507). When filtered out, 916 test results were left. From now on referred to as results. Because the data was not normally distributed we used the median and the interquartile ranges (IQR) for the descriptive of the raw data. 4.

(D)DoS analysis described in table 1 show that upload, jitter and loss have the most influence on a successful (D)DoS. For these variables the median and the interquartile ranges (IQR) were also calculated per provider (see table 8). In order to take the variation

[1] Uncapped sim cards provided by Vodafone

[a] Speed in Mb/s

[b] Variance in ms of 10 measurements

[c] delay in ms

[d] Loss of 10 packets in percentage

[e] interquartile range

	Upload in Mb/s Median (IQR)[e]	Jitter in ms Median (IQR)	Loss in percentage Median (IQR)
KPN	4.96 (2.81-7.57)	407 (171-1378)	0 (0-10)
Vodafone	5.15 (3.15-7.28)	762 (103-13317)	0 (0-20)
T-mobile	8.13 (6.57-8.53)	271 (124-937)	0 (0-40)

Table 3: (D)DoS relevant results per provider

	Median (IQR)[e]
Total Test Results	916
Download Speed	17,17 (9,81 - 34,19)[a]
Upload Speed	5,41 (3,31 - 8,18)[a]
Jitter	413 (131,5 - 1862)[b]
Latency	47 (40 - 79)[c]
RTT	86,63 (47038 - 120)[c]
Loss	0 (0 - 0)[d]

Table 4: Overall median and IQR of relevant variables

into account, an one sample t-test was conducted. This test also provides a confidence interval that can help estimate the significance of these findings. The assumptions under which this test can be performed are, a normal distribution of the variable and random sampling, of which the latter is met. If a variable was not normally distributed in the data set (see appendix figure **??**), which is the case for jitter and upload, it was log-transformed to approximate the Gaussian distribution (see appendix figure **??**). The log-transformed variables were used in order to perform the statistics of the t-test and the ANOVA. For further references we used the un-logged form of the variables. The 95% confidence interval includes a lower and upper bound. Using this, we can estimate, with 95% certainty, the upload speed (Table 9 in the appendix). From this upload speed the amount of phones necessary for a 100Mb (D)DoS, is calculated (Table 5). These values are only applicable when there is no influence on the location (e.g. Viruses). It is possible to get higher upload speeds by moving closer to the antenna. The jitter is just as important as the upload speed (Table 1). The mean of jitter from each provider was also calculated with a 95% confidence interval (Table 11). The null hypotheses is tested that the upload and jitter mean were the same for all providers. In order to test this hypothesis, an ANOVA (Analysis of Variance) test is applied. The results for upload show that at least two of the means of the three providers are statistically significant different from each other. Looking at the confidence intervals it can be concluded that this probably is T-Mobile. For jitter the ANOVA-test was also statistically significant (Table 7), where Vodafone had significantly higher jitter than the other two providers (see appendix for Vodafone figure 13, KPN figure 11 and T-Mobile figure 12). Figure 13 shows that this is due to more dispersion. The cause of more dispersion is out of the scope for this research.

These results show that T-mobile is the best provider for executing (D)DoS attacks when there is no influence on the location. T-Mobile's coverage is limited to the agglomeration of cities in Netherlands.
Data gathered regarding RTT might be interesting for (D)DoS attacks that require acknowledgement. Information about the download speed could be used to research a (D)DoS

attack on mobile phones. Both these tests are out of the scope of this research.

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

Table 5: Necessary phones for 100Mb (D)DoS attack with a 95% confidence interval

7 Proof of concept

In this chapter a proof of concept of various types of (D)DOS attacks will be discussed. The proof of concept network setup is shown in figure 4. The design consists of the following actors; attacker, provider A (Vodafone), provider B (University ISP) and the Webserver.

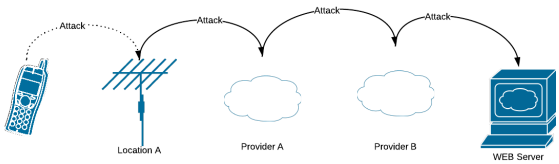

Figure 4: Proof of concept setup

7.1 Attacks

Explained in chapter 2.2.4 the following attacks will be used in the proof of concept; SYN, DNS amplification and UDP floods. All these attacks are carried out via an Android phone. The source code for the developed applications during this research (SYN and UDP attack) can be found online [46].

7.1.1 DNS amplification

To perform a DNS amplification attack with Android, source spoofing is necessary. Java (Android's main programming language) does not support this, in contradiction to C++. For this research an existing application [29] is cross compiled to Android. The application sends out a recursive name query to a name server of your choice with a spoofed source IP address selected at runtime. Spoofing the source address requires unrooted Android phones.

7.1.2 UDP flooding

There are no tools available in the market which allow you to specify the payload size of UDP packets. An Android application is created which sends UDP packets on an configurable interval, the payload is the maximum MTU size (determined via ping sweep) filled with random data.

7.1.3 TCP SYN attack

The SYN attack is created by opening normal TCP sockets, this sends packets with the SYN-flag set. The SYN, ACK response is blocked by a firewall, keeping the session on the server in established state.

The results of these test; Memory usage, CPU load, received and transmitted packets/bytes, and sessions in SYN received state, are logged every minute in a database. This will provide an overview of the impact of the (D)DoS attacks.

8 Proof of concept results

8.1 DNS amplification

Tests showed that the ISP (Vodafone) does not only block spoofed packets but also uses NAT. This means that even if it would be possible to send packets with a spoofed source address they will be rewritten to an address in the ISP's IP space. This in turn means that it would be still impossible to attack someone via DNS amplification. All replies will be send back to the ISP's network.
A similar test (single packet) on a different ISP's network showed that spoofed packets (listing 1) are excepted (listing 2). With a business subscription the DNS amplification attack can be performed, given that all providers provide an Internet subscription without NAT for their business users. This does not hold for the Vodafone/T-Mobile network, as they block spoofed packets.

Listing 1: Sending spoofed DNS request

```
Spoof Source ip: [Spoofed SRC. IP]
Dest ip: [DST. IP]
FQDSN: rp2.prague.studlab.os3.nl
--------------------------------------
Query 1  len 31
Query 2  len 0
Overal DNS len 48
Sending is OK.............root
```

Listing 2: Receiving spoofed data

```
23:07:28.505608 IP [Spoofed SRC.IP] >
[DST.IP]: 7196+ A?
rp2.prague.studlab.os3.nl.(48)
23:07:28.506066 IP [DST.IP] >
[SRC.IP]: 7196* 0/1/0 (95)
```

8.2 SYN

The SYN attack was unsuccessful via the Vodafone network. Vodafone seems to use sophisticated (D)DoS prevention mechanisms to mitigate this attack. This has been tested by capturing all data via Tcpdump on the server, no packets were received. Single packet tests were conducted via the networks from other providers and were successful. Listing 3 shows the receiving of packets with the SYN flag set [S] and the response (SYN/ACK, [S.]) to the spoofed address.

Listing 3: TCP SYN and SYN/ACK

```
T23:14:03.269735 IP [SRC.IP].43926 >
[DST.IP].80:Flags [S], seq 3734739501,
win 14600,options [mss 1460,sackOK,
TS val 46126 ecr 0,nop,wscale 6],
length 0
23:14:03.269775 IP [DST.IP].80 >
[SRC.IP].43926:Flags [S.],seq 369042338,
ack 3734739502, win 28960, options [mss
1460, sack OK,TS val 76700401
ecr 46126,nop, wscale 7],
length 0
```

8.3 UDP Flood

Listing 4 shows that UDP packets are received by the server. The UDP flood resulted in 21 Mb/s of traffic on the server, results are shown in Figure 10. This is more than our LTE test results indicate (see table 8 in the appendix). This test is conducted with an uncapped Vodafone provided Sim-Card which might be a possible explanation (other than location, time and signal-strength).

Listing 4: UDP Flood

```
23:18:16.269363 IP [SRC.IP].38903 >
[DST.IP].80: UDP, length 1473
```

This research shows that from the three above mentioned attacks, Vodafone is capable of detecting and mitigating two (SYN and

DNS amplification). Other 4G providers fail to mitigate specific attacks. However, T-Mobile does block spoofed packets, which in turn prevents any amplification attack. This research was done in collaboration with Vodafone, tests on other networks were conducted with only one packet. It might be possible that other providers need more packets before they start to mitigate attacks.

9 Conclusion

Due to the limited upload speed LTE does not offer the best medium to perform (D)DoS attacks, but there are attacks that could succeed. For this research (D)DoS attacks were categorised in three types; Bandwidth, resource and Distributed amplification -attacks. Bandwidth attacks aim to consume bandwidth resources (e.g UDP Flood) where resource attacks aim to consume other resources like CPU Cycles. The distributed amplification attacks can do both but the main difference is that the attack is amplified by other servers (slaves).

The success of a Distributed Amplification attack is dependent on the provider and subscription type. Vodafone and T-mobile have ingress filtering which blocks packets with a spoofed source address. However, not all LTE providers block these kind of packets. All providers perform (carrier-grade) NAT for prepaid subscriptions, which is a second barrier for these type of attacks. There are subscriptions that do not use NAT but they require a business contract. The lack of anonymity makes these contracts less desirable to perform a (D)DoS attack.

The same mitigation technique used by Vodafone and T-mobile (ingress filtering of packets with a spoofed source address) is used by some wired ISPs. However the amount of successful attacks indicate that not all providers use this. A LTE specific countermeasure for this specific attack is to block AXFR requests from the cellular networks. It is highly unlikely that DNS slave servers are connected via private subscriptions.

The efficiency of bandwidth attacks depend on the provider. LTE characteristics tests shows that T-mobile is best suited with a maximum of 15 phones necessary for a 100Mb/s attack. Least suitable is KPN which requires a maximum of 29 phones. A UDP flood application was developed and was able to generate 20Mb/s via the Vodafone network. A LTE specific countermeasure to discourage this type of attack is limiting the upload speed. Although this might be an undesirable as users will take longer to upload movies or other large files. Wired mitigation techniques like payload length limitation are still applicable.

Resource attacks are the most suited for LTE networks. They require not as much bandwidth as bandwidth attacks and they do not rely on spoofing as Distributed Amplification attacks. This research focused on a SYN-attack, and showed that this attack is mitigated by Vodafone. Although Vodafone was capable of detecting and mitigating the attack, this is not the case for the other 4G providers.

Resource attacks via TCP are not only harmful for the victim but also for the ISP. The amount of sessions can fill the NAT-translation table, resulting in a DOS for other mobile users. This type of attack can be mitigated by monitoring session states and packet payloads.

Due to possible implications on the providers network not all common attacks were tested. This should be researched in dialogue with the providers. Subscription types without NAT

have not been researched. These subscriptions in combination with providers that do not use ingress filtering allow for Distributed Amplification attacks. Tests with these applications show that Vodafone mitigates two out of three attacks, were other providers mitigate none. LTE network measurements indicate that T-Mobile provides the best network characteristics for a (D)DoS attack over LTE. Furthermore they provide information on the necessary phones needed for a 100 Mb/s bandwidth attack per provider, for which T-mobile need the least amount (14).
This research also discusses LTE specific mitigation techniques which might result in a safer network infrastructure.

10 Acknowledgements

We would like to express our special appreciation and thanks to our advisor, Jeroen van der Ham of the University of Amsterdam. Your expertise, understanding, and patience added considerably to our graduate experience.

A special thanks goes out to Vodafone and Hans Nelissen who helped us with the necessary hardware and guidance for this project.

Last but not least we want to thank all the reviewers and those who gave us the possibility to complete this project.

Appendices

A Attacks in detail

This section explains in more detail; how the (D)DoS attacks described in chapter 2 work, the already known mitigation techniques and the impact this has on a server/service. The assumptions of a 4G/LTE network, like higher latency, less availability and lower bandwidth speed is also looked at to find the best suited (D)DoS attack on a 4G/LTE network.

A.1 SYN

A denial-of-service method called SYN flooding works by not responding to the server with the expected ACK response (in a normal TCP 3-WAY Handshake).

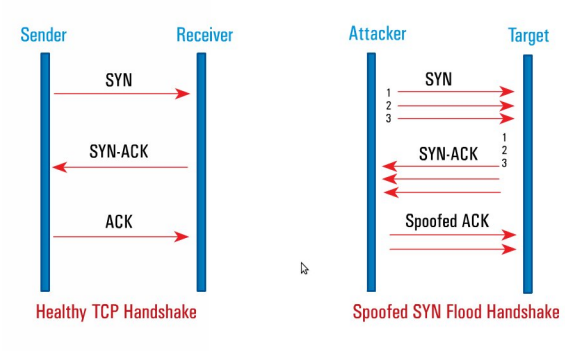

Figure 5: The left figure shows a normal 3-Way TCP Handshake. On the right side you see a SYN Flood attack where the attacker send SYN requests.

The client will simply not send the acknowledgement (ACK), causing the server to send the SYN-ACK to a spoofed IP address, which will not respond to an ACK because it never sent a SYN. The server is then stuck waiting for the acknowledgement, because congestion could also be caused by a delayed or missing ACK. The problem is the amount of bindings of half-open connections during this attack. After a period, depending on the server there are so many that no new connections can be made. This will result in a badly behaving system or even worse a denial of service[9].

Although there are many effective SYN flood mitigation techniques (RFC4987 is covering some common mitigation techniques), there is no single defence mechanism [47].
The SYN Flood attack requires a stable connection and high bandwidth. If the connection between the client and the server drops, the entries in the backlog time out. Because there is no reason for a client (attacker) to receive a response, the latency is irrelevant. Mitigation techniques for this attack are discussed in a RFC[9].

different position

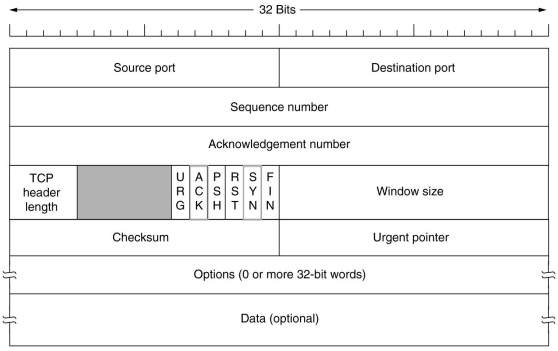

Figure 6: The "SYN" in "SYN flood attack" represents the synchronise flag in the TCP header. The SYN flag gets set when a system first sends a packet in a TCP connection, and indicates that the receiving system should store the sequence number included in this packet.

A.2 ACK

An acknowledgement (ACK) Flood attack uses a large number of ACK packets to attack the victim. All TCP messages that are sent have

the ACK Flag set. Meaning that the host needs to check if the state represented by the packet is legal, after this the packet can be passed to the application layer. If the check states that the packet is illegal then the host's operating system network protocol stack will respond with a Reset (RST) packet.

To summarise, the server has to process two actions: Doing a table look up and responding to a ACK/RST. With an overload of ACK Flood messages, the server will stop processing the requests. Not only servers can be effected also routers and other network devices can be damaged [28].

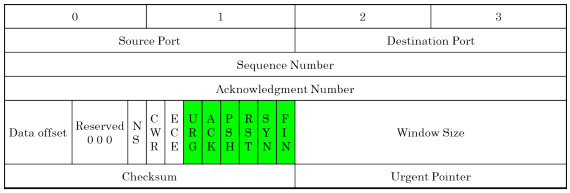

Figure 7: With the ACK flag bit turned on the server has to do some checks. This will cost computing power.

For ACK Flood attacks the availability and bandwidth are important. If the connection drops the server or network device has time to process the requests. Latency for this attack is less important. The goal is to stress the server or network device with computational calculation and if they arrive a bit later that is not a problem.

A.3 NTP

Network Time Protocol (NTP) is an UDP based protocol, used to synchronise clocks between computers. Where a request made by the client (attacker) can result in a big response.

This is one of the reflection attacks to preform a Denial of service. The request sent is a so called NTP mode 7 monlist command,

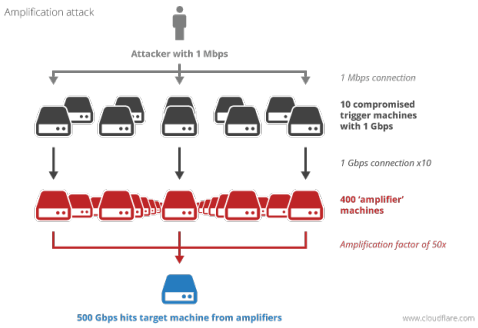

Figure 8: Amplification attack: The initiator sends a small request but the response is big.

where servers are forced to respond with the IP address to a maximum of 600 servers [33].

```
ntpdc -c monlist [server ip]
```

Every server prior to NTP version 4.2.7 is vulnerable for this attack. To protect a server from this attack, upgrading the OS to at least 4.2.7 is an option or if upgrading is not an option the monlist command should be disabled [44]. For the NTP attack to work, less bandwidth is needed compared to a SYN attack. This is due the small request compared to the large response. Exact numbers of multiplication are not found in research papers, but a company named Prologic did a test where a 60 bytes request resulted in a 2604 bytes response. This is a multiplication of more then 43 times [33].

A.4 DNS

With a DNS amplification the attacker first needs to spoof the victims address (reflection part). All reply's from the DNS server will be directed to the victim's server. The attacker also need to find responses that are bigger than the request to preform amplification.

The victim will then get overloaded with a huge amount of traffic and when most or all connections are used new "legitimate" connec-

tions can't be made anymore. An other Denial of Service that can be achieved is that the clients machine is exhausted instead of the bandwidth.

Just as in NTP, with this attack the answer of a request is bigger. Meaning that bandwidth is not a concern if you want to perform this attack [34].

Researcher at the University of the Aegean, Greece found amplification factors of +40. [1].If a connection drops the all ready sent packets can be processed by the servers so availability is crucial. Latency in this attack is less important. The replies are send to the victim not to the initiator.

A.5 Fragment TCP/UDP

This attack sends a high volume of TCP or UDP fragments to a victim host. Designed to overwhelm the hosts ability to re-assemble the packets and degrade its performance. Fragments can often be malformed to cause additional processing.

To transfer large packets the IP Protocol fragments them each having a sequence number and a common identification number. The recipient reasembles the packets due to the fact there is a offset value.

The most famous fragment attack is the Teardrop attack. The principle of the Teardrop attack involves inserting false offset information into fragmented packets. As a result, during reassembly, there are empty or overlapping fragments that can cause the system to be unstable.

In RFC 1858 the other fragmentation versions are explained together with a solution to prevents this attacks. In this RFC they discuss the Tiny Fragment attack and the Overlapping Fragment Attack where I. Miller recommends corrective action for the Indirect Method [26].

A.6 CHARGEN

CHARGEN is defined in RFC0864 [31] and can be used for debugging network connections, network payload generation and bandwidth testing. It listens on port 19 TCP or with UDP. If TCP is used, it continues to stream random characters until the connection is closed. With UDP, it responds with an up to 512 byte response. Because of this behaviour this attack also falls under the (D)DoS amplification category.

Prologic also did a test with Chargen and a 60 bytes request, resulted in a 1066 bytes response. This is a multiplication of more then 17 times [33]. The U.S.-based cybersecurity organization CERT issued an advisory on this attack. Where they advise to disable and filter the Chargen function [43].

This attack compared to DNS and NTP has a amplification factor the answer of a request is bigger. Meaning that bandwidth is not the biggest concern if you want to perform this attack [34].

A.7 ICMP

The Internet Control Message Protocol (ICMP) messages are sent in several situations: for example, when a packet cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram or when the gateway can direct the host to send traffic on a shorter route. The full list of available messages can be found online [19].

The attack using the ping command is known as "ICMP Ping Flood Attack", also known as a "Ping Flood Attack". This attack is a simple Denial of Service where the malicious initiator sends a large amount of ICMP echo Requests (Ping) to the victim machine and with this saturates the network with traffic.

For each request the server sends a response, this limits the available system resources for other processes. The continuing requests and replies are slowing down the network and will cause legitimate traffic to continue at a significantly reduced speed and in some cases to be disconnected [4].

An other DoS ICMP attack is the Smurf Attack where sending an ICMP Echo Requests destined for an IP broadcast address is used. The source IP is spoofed and is the one of the victim. All machines from the destination network respond back with an Echo Reply to the victim and are generating a "Smurf" denial of service attack. Or the term that is used in DNS a reflection.

For the ICMP Flood attack to work, bandwidth and availability are important. If the connection drops or not enough packets are sent the server has time to process the requests. The latency of the network, for this attack is not important because the request arrive at the victim not to the attacker.

Mitigation techniques for this attack are documented in the draft Preventing DDoS Smurf Attacks draft-vshah-ddos-smurf-00:

1. Each Router MUST disable forwarding and receiving of directed broadcasts by default.

2. Each Host MAY silently discard an ICMP Echo Request destined for an IP broadcast

3. Each ISP router SHOULD implement network ingress filtering to prevent forged packets leaving your network boundary

A.8 RIP

Routing Information Protocol (RIP) is a old routing protocol to route packets based on hop count. RIP counts the number of hops on every path available before it makes a routing decision. Where the maximum hop count can be 15 hops where a value higher is infinite or unreachable to prevent loops. In the first version no authentication is used so an attacker can forge RIP routing updates to advertise he least cost path to the target node. This will cause RIP to route all packets to the target node trough attacker as he is the nearest to target node [2]. Due to this he can launch any attack on the target node.

As mentioned there is no authentication so to mitigate this attack authentication is needed. In version 2 and 3 (IPv6) authentication is enabled. Other countermeasures are[3]:

- Filtering packets based on source and destination.
- Frequent log analysis aimed at anomaly detection.
- Check routes before acceptance

A.9 HTTP GET/POST/HEAD

In this attack, an initiator will abuse the HTTP-GET/POST request by sending a large number of malicious requests to a target victim [11]. Because the packets have legitimate HTTP payloads the victims server cannot distinguish normal and malicious requests. To process all these requests, normal and the illegal ones, a server can exhaust their resources.

The HEAD method is identical to GET except that the server MUST NOT return a message-body in the response. The metainformation contained in the HTTP headers in response to a HEAD request SHOULD be identical to the information sent in response to a GET request. This method can be used for obtaining metainformation about the entity implied by the request without transferring the entity-body itself. This method is often used for testing hypertext links for validity, accessibility, and recent modification.

The response to a HEAD request MAY be cacheable in the sense that the information contained in the response MAY be used to up-

date a previously cached entity from that resource. If the new field values indicate that the cached entity differs from the current entity (as would be indicated by a change in Content-Length, Content-MD5, ETag or Last-Modified), then the cache MUST treat the cache entry as stale.

For this attack to be success full the availability is important, if the requests stops the server has the time to process the all ready send requests. Bandwidth is a crucial aspect to. The requests need to be send but if this is done in a low rate the server has time to process the requests. Latancy of the network, for this attack is not crucial. The request must arrive but how fast is not important. Because the connection is TCP based a normal round trip time is needed.

A.10 SSL Get & SSL Post

Secure Sockets Layer (SSL) is a security protocol for network communication and data integrity. SSL encrypts the network connection at the transport layer. This is done to avoid that transmitted plain data is being listened or intercepted.

This security comes with a price because, encryption, decryption, and key negotiation consume huge amounts of system resources, that causes degrading of the performance of a machine. Because of this SSL protocol is only applied to the transmission of classified information, like passwords [7].

Before a client and a server exchange data they need to perform a SSL handshake. This is done to exchange an encryption algorithm and the keys for identity authentication. Normally this is done once but the renegotiation option in the SSL protocol enables it to renew the negotiation to establish new keys.

In 2011 a security researcher proposed the THC SSL DoS attack. It uses the Renegotiation vulnerability to exhaust resources of the victim. After the normal SSL connection and handshake, the malicious initiator repeatedly renegotiates the keys. This process requires the server to invest 15 times more resources than the client. He claims that with a less power full client it could take down a high-performance server [41].

For this attack to be successful availability and bandwidth is important. When connectivity drops the server has time to process the requests. As stated in how this SSL attacks work the more requests the more computation resources are needed. If there is not enough requests a server, with good processing power has time to process requests. Latency is also crucial because it is build on a normal TCP connection. When the latency is to high the connection can be killed [45].

A.11 UDP Floods

With an UDP Flood attack the malicious initiator launches a master control program which serve as a attack handler. This program forwards the attack instructions to their agents. This agents are either demons or zombies (compromised systems) to flood the victim [6].

Demons will be used in a direct attack. With a reflector attack zombie machines are used. Once a zombie receives an attack instruction from the master, they start sending UDP packets to the victim with a spoofed IP address. The victim receiving these packets, send an ACK to the source IP address, but doesn't get any response and will keep waiting . Finally when the victim gives up communication, and all resources have been consumed leading to crash of the system. The master that control the zombies can be multiplied aswell which leads to a large number of UDP packets to the victims system. This consumes the entire bandwidth and other resources by flooding the system[35]. With direct UDP Flooding

bandwidth and availability are very important because also in this case. if the line drops the server has time to process the UDP packets. With the reflector technique bandwidth and availability is less important because the zombie systems preform the attack.

A.12 PUSH

In a PUSH + ACK attack the malicious initiator sends a TCP packet with PUSH and ACK bits set to one. Because of this trigger, the victim system unloads all data in the TCP buffer (regardless of whether or not the buffer is full). An acknowledgement is send when this is completed. With multiple agents the receiving system cannot process the high volume and the victim system will crash [35].

Latency is for this attack not really important because the replies are not needed. In this case, again bandwidth and availability is of great importance. When the connection drops the server has the change to process the requests.

A.13 FIN Floods & FIN Push

The FIN (Finish) flag is used to negotiate between the peer systems that the communication is over and they can drop the connection. FIN is a 4 way handshake and it tears down the TCP virtual connection [30].

The FIN flag is rarely used as a (D)Dos attack, but they are used as a form of reconnaissance to determine what servers are active on a given IP. In other words the TCP FIN flag is used to scan servers to find listening TCP port numbers on how the victim reacts. With this open ports a specific attack can be preformed for example if you know that port 19 is open you can use the CHARGEN attack.

To mitigate/block this scan an intrusion detection systems (IDS) and intrusion prevention systems (IPS) can be used. To block it the IDS or IPS systems need to discard packets that are not part of an active TCP connection [36].

B Statistics

B.1 Providers

carrier			rttavg	download	upload	latency	jitter	Loss
KPN	N	Valid	478	478	478	478	478	478
	Mean		102,7	15.386	5.305	49.044	2259.031	2.3
	Median		99,3	12.98	4.96	45	407	0
	Std. Deviation		35,62	11.391	3.629	15.675	17037	0.460
	Range		248,56	248,56	36.910	141	364111	10
	Minimum		34,86	0.41	0	31	17	0
	Maximum		283,42	61.01	36.910	172	364128	10
	Percentiles	25	77,58	7.985	2.81	41	171	0
		50	99,25	12.98	4.96	45	407	0
		75	126,72	18.102	7.572	50	1378.5	0
T-Mobile	N	Valid	166	166	166	166	166	166
	Mean		54,38	31.870	7.407	64.139	1006.181	0.240
	Median		41,27	31.190	8.130	32	270.5	0
	Std. Deviation		92,04	14.0470	2.195	358.590	1711.861	3.105
	Range		1155,4	52.70	11.96	4626	12035	40
	Minimum		24.18	0.24	0.75	26	0	0
	Maximum		1179,57	52.94	12.71	4652	12035	40
	Percentiles	25	35,32	20.762	6.567	30	124.25	0
		50	41,26	31.190	8.130	32	270.5	0
		75	49,07	46.5625	8.53	36	936.5	0
Vodafone	N	Valid	273	273	273	273	273	273
	Mean		215,07	37.514	6.505	344.527	20136	0.366
	Median		88,59	26.9	5.15	88	762	0
	Std. Deviation		373,35	30.772	10.433	625.110	68073	2.068
	Range		4051,05	120.49	147.420	2946	783225	20
	Minimum		32,90	0.23	0.22	65	0	0
	Maximum		4083,95	120.72	147.640	3011	783225	20
	Percentiles	25	70,96	13.18	3.145	78	102.5	0
		50	88,59	26.9	5.15	88	762	0
		75	127,86	61.57	7.275	101	13317	0

Table 6: The mean, Median, standard deviation, Range, minumum and maximum per provider for RTT, Up/Down-Load, latency and jitter

B.2 Anova test

		Sum of Squares	df	Mean Square	F	Sig.
lnupload	Between Groups	44.724	2	22.362	25.640	1.465
	Within Groups	796.279	913	0.872		
	Total	841.005	915			
lnjitter	Between Groups	344.995	2	172.498	53.394	1.329
	Within Groups	2820.340	873	3.231		
	Total	3165.335	875			

Table 7: The Analysis Of Variance upload and jitter

B.3 LOG

carriername		N	Mean	Std. Deviation	Std. Error Mean
KPN	upload	477	3.82	2.82	1.05
T-Mobile	upload	166	6.95	1.50	1.03
Vodafone	upload	273	4.21	2.64	1.06

Table 8: Log transformed for upload

carrier		Test Value=0					
		t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
						Lower	Upper
KPN	upload	28.21	476	1.17	3.83	3.48	4.2
T-Mobile	upload	61.78	165	5.59	6.96	6.54	7.4
Vodafone	upload	24.48	272	1.05	4.21	3.75	4.7

Table 9: Confidence Interval of the difference for upload

Carrier		N	Mean	Std. Deviation	Std. Error Mean
KPN	jitter	478	475.02	4.45	1.07
T-Mobile	jitter	165	380.79	380.79	1.11
Vodafone	jitter	233	1834.47	1834.47	1.18

Table 10: Mean and standard deviation for jitter.

carrier		Test Value=0					
		t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
						Lower	Upper
KPN	jitter	90.28	477	4.81	475.025	415.4	543.2
T-Mobile	jitter	56.9	164	5.2	380.78	309.94	467.85
Vodafone	jitter	45.67	232	6.2	1834.45	1326.5	2536.9

Table 11: Confidence Interval of the difference for jitter

B.4 Overall

Statistics								
		loss	rttavg	latitude	download	upload	jitter	latency
N	Valid	917	917	917	917	917	917	917
Mean		0.16	127.40	482718.78	24.96	6.04	7354.56	139.74
Std. Error of Mean		5.85	7.17	4665.50	0.73	0.21	1319.78	13.10
Median		0	86.625	523246	17.17	5.41	413	47
Std. Deviation		1.77	217.14	141280.7	22.09	6.38	39965.67	396.42
Range		40	4059.77	533238	120.49	147.64	783225	4626
Minimum		0	24.18	0	0.23	0	0	26
Maximum		40	4083.95	533238	120.72	147.64	783225	4652
Percentiles	5	0	35.33	0	0.57	0.639	21.70	30
	25	0	47038		9.81	3.31	131.5	40
	50	0	86.625	523246	17.17	5.41	413	47
	75	0	120.024	523246	34.185	8.175	1862.5	79
	90	0	157.68	533238	54.516	9.274	9563	99

Table 12: Mean, median, standard deviation, range, minumum and maximum for the providers together

C LTE

C.1 OFDMA

Orthogonal Frequency Division Multiplex (OFDM) comes in different forms but the basic concept is the same. The available spectrum is split into smaller sub-carries which are orthogonal to each other. To provide a complete signal the data from the sub-carriers is combined during the demodulation phase.

Channel Bandwidth Mhz		1,4	3	5	10	15	20
Number of Resource Blocks		6	15	25	50	75	100
Modulation	MIMO	Data Rates, Mb/s					
QPSK	Not used	1,728	4.32	7.2	14.4	21.6	28.8
16 QAM	Not used	3,456	8,64	14.4	28,8	43,2	57,6
64 QAM	Not used	5,184	12,96	21,6	43,2	64,8	86,4
64 QAM	2x2	10,368	25,92	43,2	86,4	129,6	172,8
64 QAM	4x4	20,736	51,84	86,4	172,8	259,2	345,6

Table 13: Peak Downlink Data Rates for FDD-LTE & TD-LTE

	Channel Bandwidth (Mhz)					
	1,4	3	5	10	15	20
Transmission Bandwidth (Mhz)	1.08	2.7	4.5	9	13.5	18
Transmission Bandwidth (RB)	6	15	25	50	75	100

Table 14: Each channel (in Mhz) indicates the download speed in bandwith

C.2 SC-FDMA

To reduce power consumption the LTE up-link requires a different technique than chosen for the down link. For this reason Single-carrier frequency-division multiple access (SC-FDMA) is chosen.

LTE up-link requirements differ from those of down-link due to low power consumption requirement at User Equipment (UE). SC-FDMA [10] is chosen for up-link because it combines the low peak-to-average ratio techniques of single-carrier transmission systems, such as Code division multiple access with the multi-path resistance and flexible frequency allocation of OFDMA.

To fulfil the requirement such as coverage, robustness, capacity and high data rates. 3G LTE uses different multiple antennas with the MIMO techique. More information about this techique can be found in apendix C

C.3 Peak Data Rates

In the Netherlands only Frequency Division Duplex (FDD) is used. A full comparison between the two techniques can be found online [20].

The peak data rates for various channel bandwidths and antenna options for both FDD-LTE and TD-LTE are shown in table 13 and 2

C.4 Multiple-input and multiple-output

To fulfil the requirement such as coverage, robustness, capacity and high data rates. 3G LTE uses different multiple antennas. In order to increase the coverage and/or capacity the Beamforming technique is used. Multiple-input and multiple-output (MIMO) [37] is used to enhance the data rates by exploiting the spatial diversity in radio channels up to 20 Mbps. For this multiple antennas at the transmitter and receiver side are used.

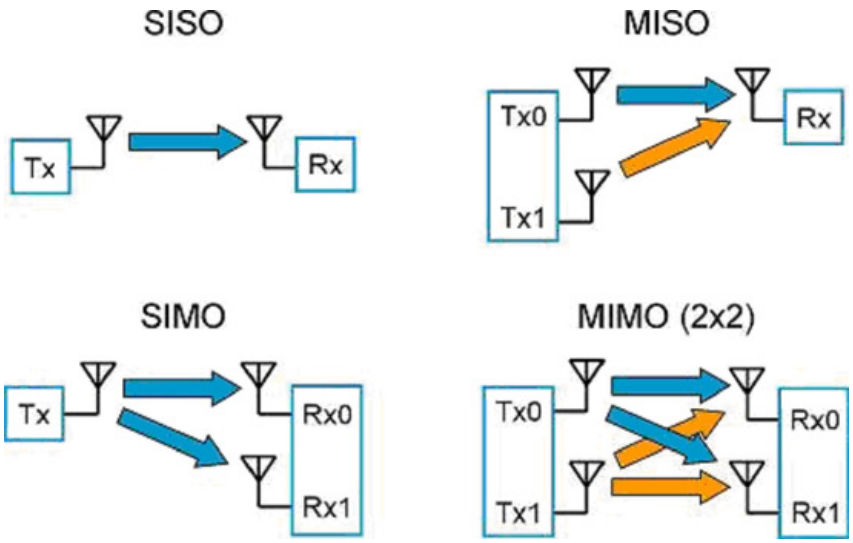

Figure 9: This graphic shows antenna and channel configurations for SISO, SIMO, MISO, and MIMO (2x2) techniques.

As shown in picture 9 there are multiple antenna techniques. For MIMO the transmitter splits the information bits into several streams (S1,S2) and transmitts via the different antennas. The channel mixes the streams so at the receiver each antenna has the combination of the streams in the received signal.

The advanced receiver recovers the transmitted information at multiple antennas which analyses the unique pattern corresponding to each transmitter and then the stream gets recovered [5].

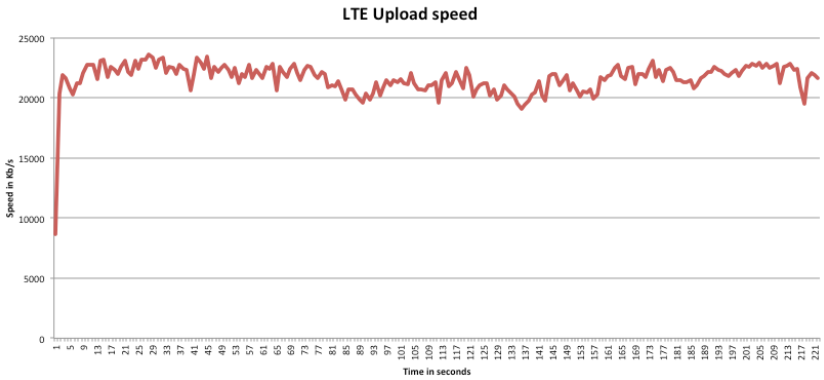

Figure 10:
N = 212
Mean = 21601

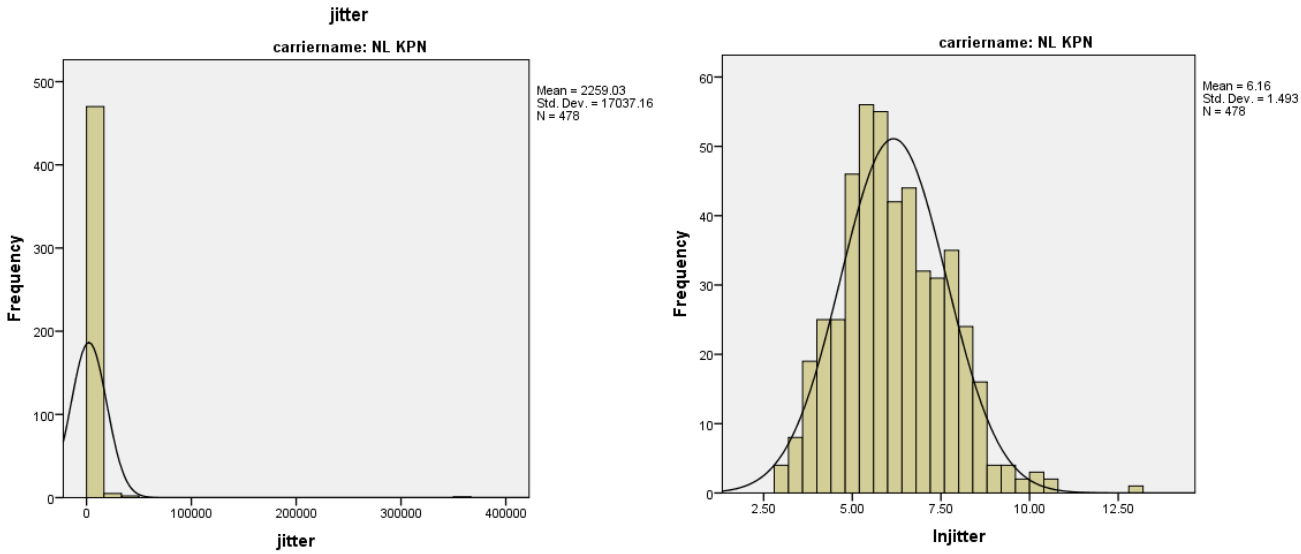

Figure 11: Unlogged and Logged data - Jitter KPN

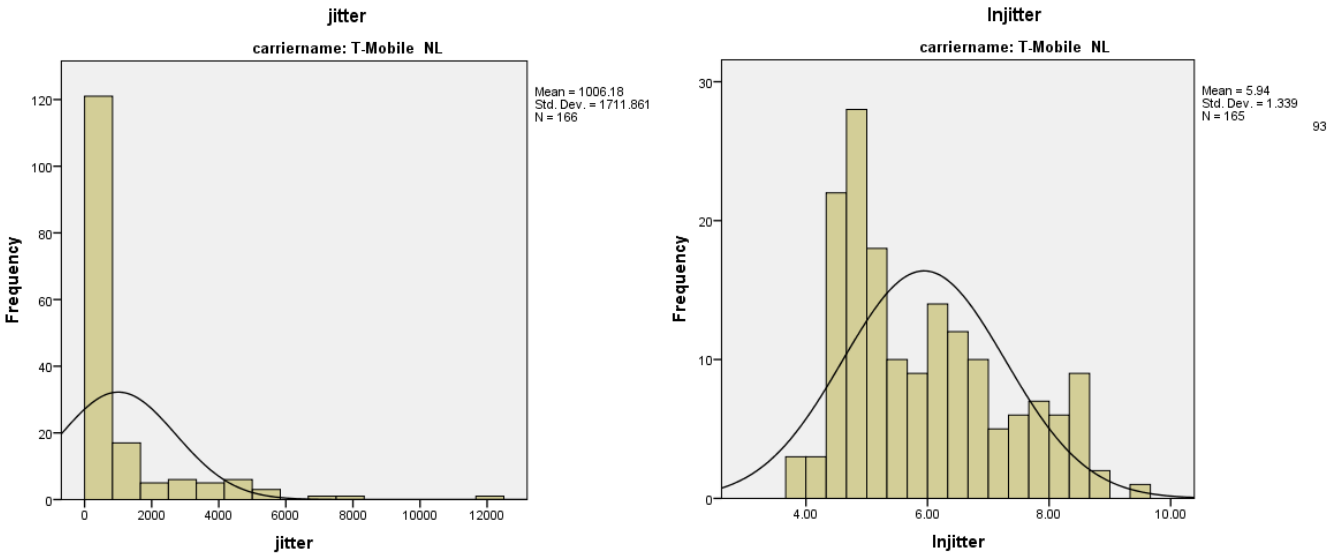

Figure 12: Unlogged and Logged data - Jitter T-Mobile

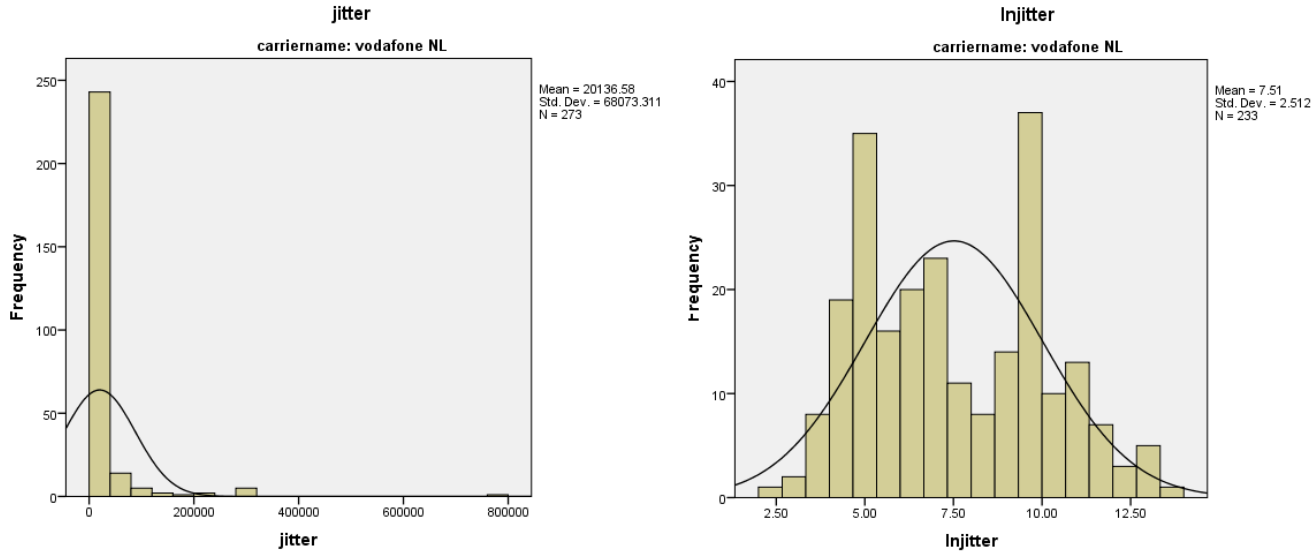

Figure 13: Unlogged and Logged data - Jitter Vodafone

References

[1] Marios Anagnostopoulos, Georgios Kambourakis, Panagiotis Kopanos, Georgios Louloudakis, and Stefanos Gritzalis. Dns amplification attack revisited. *Computers & Security*, 39:475–485, 2013.

[2] A Barbir, S Murphy, and Y Yang. Generic threats to routing protocols. 2006.

[3] Steven M Bellovin. A look back at" security problems in the tcp/ip protocol suite. In *Computer Security Applications Conference, 2004. 20th Annual*, pages 229–249. IEEE, 2004.

[4] Mitko Bogdanoski and Aleksandar Risteski. Wireless network behavior under icmp ping flood dos attack and mitigation techniques. *International Journal of Communication Networks and Information Security (IJCNIS)*, 3(1), 2011.

[5] SM Chadchan and CB Akki. 3gpp lte/sae: an overview. *International Journal of Computer and Electrical Engineering*, 2(5):806–814, 2010.

[6] Rocky KC Chang. Defending against flooding-based distributed denial-of-service attacks: A tutorial. *Communications Magazine, IEEE*, 40(10):42–51, 2002.

[7] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), August 2008. Updated by RFCs 5746, 5878, 6176.

[8] Phillip Dykstra. Protocol overhead, 2013 (accessed July 7, 2014).

[9] W. Eddy. TCP SYN Flooding Attacks and Common Mitigations. RFC 4987 (Informational), August 2007.

[10] Hannes Ekstrom, Anders Furuskar, Jonas Karlsson, Michael Meyer, Stefan Parkvall, Johan Torsner, and Mattias Wahlqvist. Technical solutions for the 3g long-term evolution. *Communications Magazine, IEEE*, 44(3):38–45, 2006.

[11] Juan M Estevez-Tapiador, Pedro García-Teodoro, and Jesús E Díaz-Verdejo. Detection of web-based attacks through markovian protocol parsing. In *Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE Symposium on*, pages 457–462. IEEE, 2005.

[12] Annie P Foong, Thomas R Huff, Herbert H Hum, Jaidev P Patwardhan, and Greg J Regnier. Tcp performance re-visited. In *Performance Analysis of Systems and Software, 2003. ISPASS. 2003 IEEE International Symposium on*, pages 70–79. IEEE, 2003.

[13] FrozenTux. Tcp connections, 2014 (accessed June 1, 214). `https://www.frozentux.net/ipsysctl-tutorial/ipsysctl-tutorial.html#AEN481"`.

[14] Xianjun Geng and Andrew B Whinston. Defeating distributed denial of service attacks. *IT Professional*, 2(4):36–42, 2000.

[15] BB Gupta, Ramesh Chandra Joshi, and Manoj Misra. Distributed denial of service prevention techniques. *arXiv preprint arXiv:1208.3557*, 2012.

[16] M Handley and Eric Rescorla. Rfc 4732: Internet denial-of-service considerations. 2006.

[17] Salim Hariri, Guangzhi Qu, Tushneem Dharmagadda, Modukuri Ramkishore, and Cauligi S Raghavendra. Impact analysis of faults and attacks in large-scale networks. *IEEE Security & Privacy*, 1(5):49–54, 2003.

[18] Harri Holma and Antti Toskala. *LTE for UMTS-OFDMA and SC-FDMA based radio access*. John Wiley & Sons, 2009.

[19] IANA. Internet control message protocol (icmp) parameters. 2013.

[20] Angel Ivanov. Td-lte and fdd-lte a basic comparison, 2012.

[21] Georgios Kambourakis, Tassos Moschos, Dimitris Geneiatakis, and Stefanos Gritzalis. A fair solution to dns amplification attacks. In *Digital Forensics and Incident Analysis, 2007. WDFIA 2007. Second International Workshop on*, pages 38–47. IEEE, 2007.

[22] Brajesh Kashyap and S Jena. Ddos attack detection and attacker identification. *International Journal of Computer Applications*, 42(1):27–33, 2012.

[23] Charles M. Kozierok. Tcp connection establishment process: The.

[24] Breno Henrique Leitao. Tuning 10gb network cards on linux. In *Proceedings of the 2009 Linux Symposium*, 2009.

[25] Ming Li, Jun Li, and Wei Zhao. Simulation study of flood attacking of ddos. In *Internet Computing in Science and Engineering, 2008. ICICSE'08. International Conference on*, pages 286–293. IEEE, 2008.

[26] I Miller. Rfc: 3128-protection against a variant of the tiny fragment attack, 2001.

[27] Motorola. Long term evolution (lte): A technical overview, 2007 (accessed June 13, 2014). `http://www.motorolasolutions.com/web/Business/Solutions/Industry%20Solutions/Service%20Providers/Wireless%20Operators/LTE/_Document/Static%20Files/6834_MotDoc_New.pdf"`.

[28] NFocus. Common ddos attacks. 2014.

[29] Packetstormsecurity. Amplification attack, 2014 (accessed July 5, 214). `http://packetstormsecurity.com/files/122600/DNS-Reflection-Amplification-Attack-Tool.html`.

[30] J. Postel. Transmission Control Protocol. RFC 793 (Standard), September 1981. Updated by RFCs 1122, 3168.

[31] J. Postel. RFC 864: Character generator protocol, May 1983. See also STD0022 [**?**]. Status: UNKNOWN.

[32] Prolexic. Global ddos attack report. 2014.

[33] Prologic. Snmp-ntp-chargen reflection attack. 2014.

[34] Thijs Rozekrans, Matthijs Mekking, and Javy de Koning. Defending against dns reflection amplification attacks. *University of Amsterdam, Tech. Rep., Feb*, 2013.

[35] Stephen M Specht and Ruby B Lee. Distributed denial of service: Taxonomies of attacks, tools, and countermeasures. In *ISCA PDCS*, pages 543–550, 2004.

[36] Stamius. Types of ddos:fin scan, 2013 (accessed July 7, 2014). "`https://wiki.staminus.net/index.php/Types_of_DDoS:FIN_Scan`".

[37] Gordon L Stuber, John R Barry, Steve W Mclaughlin, Ye Li, Mary Ann Ingram, and Thomas G Pratt. Broadband mimo-ofdm wireless communications. *Proceedings of the IEEE*, 92(2):271–294, 2004.

[38] A.S. Tanenbaum and D.J. Wetherall. *Computer Networks: Pearson New International Edition*. Pearson custom library. Pearson Education, Limited, 2013.

[39] Agilent Technologies. Agilent 3GPP Long Term Evolution: System Overview, Product Development, and Test Challenges. *Application Note, Industry White Papers*, 44(3), June 2009.

[40] Agentschap Telecom. Staat van de ether, 2014 (accessed June 4, 214). "`http://www.agentschaptelecom.nl/sites/default/files/staatvdether_2012_digitaal.pdf`".

[41] THC-SSL-DOS. Thc-ssl-dos tool. 2011.

[42] J. Touch. Defending TCP Against Spoofing Attacks. RFC 4953 (Informational), July 2007.

[43] US-CERT. Udp port denial-of-service attack. 1996.

[44] US-CERT. Ntp amplification attacks using cve-2013-5211. 2014.

[45] David Carrera Jordi Torres Eduard Ayguad e Vicen c Beltran, Jordi Guitart and Jesus Labarta. Performance impact of using ssl on dynamic web applications. 2004.

[46] Wouter and Rawi. Syn attack + udp flood for android, 2014 (accessed July 26, 214). "`http://pastebin.com/h5x2uX9M`".

[47] Zhijun Wu, Guang Li, Meng Yue, and Hualong Zeng. Ddos: Flood vs. shrew. *Journal of Computers*, 9(6):1426–1435, 2014.

[48] Jian Yuan and Kevin Mills. Monitoring the macroscopic effect of ddos flooding attacks. *Dependable and Secure Computing, IEEE Transactions on*, 2(4):324–335, 2005.

[49] Min Zhang, Maurizio Dusi, Wolfgang John, and Changjia Chen. Analysis of udp traffic usage on internet backbone links. In *Applications and the Internet, 2009. SAINT'09. Ninth Annual International Symposium on*, pages 280–281. IEEE, 2009.