Data-Driven Analysis of Cellular Network Resilience in the Netherlands

Dylan D. Janssen
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
d.d.janssen@student.utwente.nl

ABSTRACT

The importance of analysing the resilience of a mobile cellular network has increased, since almost everyone in the world uses the mobile cellular network. This paper evaluates the resilience of cellular networks in the Netherlands using a crowd-sourced data set, i.e. OpenCellId. We perform a literature survey to determine which resilience metrics can be used for mobile cellular network and also the potential risks for a mobile cellular network. A simulator created by us uses an OpenCellId data set of base stations to simulate the potential risks and evaluate the resilience of the mobile cellular network in cities of the Netherlands. The analysis shows that Amsterdam is the most resilient city in the Netherlands against natural disasters. On the other hand, Middelburg is the least resilient against natural disasters, since its number of base stations in Middelburg is significantly lower than in Amsterdam. Moreover the area of Amsterdam is significantly larger than Middelburg, so the simulated natural disaster would not cover Amsterdam completely while Middelburg is completely covered. Malicious attacks do not have a large impact on the cities of the Netherlands. All cities have an acceptable level of resilience for the network during a malicious attack. When increasing the requested data rate, Middelburg performed the best of all the cities and Rotterdam the worst. Since there are significantly more users connected to the base stations in Rotterdam than in Middelburg, the increasing requested data rate has more effect on the resilience of the network. This can also conclude that there is a relation between connected users to base stations and the satisfaction level.

Keywords

Mobile network, Cellular network, Resilience

1. INTRODUCTION

Almost everyone in the world uses mobile cellular networks for everyday activities, e.g. phone call and web browsing. However, it is possible for a base station (BS) to partially drop out of the network. A possible reason for this is that the BS is damaged due to a disaster, malicious attack or deprecated parts. This could result in a less functional network and users would receive a lower quality of service than normally. Therefore, it is important to understand the resilience of mobile networks because almost everyone is depending on a functioning network even in hard times. But how can the resiliency of a network be determined? Previous studies provide multiple definitions of resilience. For instance, Alliance et al. [3] define resilience as "the capability of the network to recover from failures", while Liu et al. [7] defined it as "the percentage of lost traffic upon failures" and Sternbenz et al. [17] defined it as "the ability of the network to provide and maintain an acceptable level of service". According to [16] and [17] the goal of resilience is that the system continues to work according to the user's expectations regardless of changes that may themselves be hidden away. The resilience of mobile cellular networks must be acceptable to provide service to users. Since emergency services also use mobile networks, public safety will decrease when the resilience of mobile networks is not acceptable.

The goal of this research is to evaluate how resilient the mobile cellular network is in the Netherlands. If certain cities in the Netherlands do not have an acceptable level of resilience, then a more in-depth analysis of the networks in these cities should be performed.

RQ1. What metrics are used in the literature to measure the resilience of a cellular network?

RQ2. What are the potential risks for the resilience of cellular networks?

RQ3. Are all cities in the Netherlands equally resilient or are there differences in the resiliency of certain cities in the Netherlands?

To address the above-listed questions, we first conduct a literature survey on the resilience metrics and potential risks. As we do not have access to the information of cellular operators' infrastructure, we will use a OpenCellId [18] data set which records the location of cell towers across the world. Then we will consider major cities in the Netherlands and evaluate the resilience of the cellular networks in each city under increasing level of risks such as disaster radius.

The rest of the paper is organized as follows. Section 2 discusses the related works on this topic. Section 3 overviews the literature survey of the resilience metrics. Section 4 determines the literature survey of the potential risks. Section 5 will provide the methodology. Section 6 analyses the performance of the considered system. Section discusses the shortcoming of this research. Finally, Section 8 concludes the results of the performance analysis.

35^{th} Twente Student Conference on IT July 2^{nd}, 2021, Enschede, The Netherlands.

2. RELATED WORK

This section will discuss the related works on this topic.

Sterbenz et al. [17] introduced a resilience strategy called D^2R^2+DR, in which D^2R^2 stands for Defend, Detect, Remediate and Recover while DR stands for Diagnose and Refine. Additionally, they also introduce a Resilience state space diagram. Lummen et al. [8] research the resilience between nodes and edges of a network using the definition of resilient and state-space diagram of Sterbenz et al. [17]. Lummen et al. [8] defined resilience metrics such as clustering coefficient and number of connected components. By performing multiple simulations the conclusion is that the link placements between nodes are very important for having an acceptable level of service. However, the research did not include the resilience of wireless networks, this research will on the other hand include the resilience of wireless networks. Labib et al. [10] analysed and enhanced the resilience of LTE and LTE-A System to RF Spoofing. They proposed multiple changes to the LTE system to make it more resilient. This research will not consider RF Spoofing in particular on the LTE system but will consider malicious attacks in general that can damage the cellular network. Kamola et al. [6] analysed network resilience on a country-level. The authors determine the term resilience as the vulnerability of a network of autonomous systems located in a single country to link or node failures. They conclude that there are noticeable effects on the resilience only when large areas are affected (800 meters or more). Kamola et al. [6] research is different from this study, since they analyse the resilience on a link and node level while this research focuses on the resilience of wireless cellular networks.

Dobson et al. [4] focus on the self-organization and resilience for networked systems. The self-organized system can optimize or manage itself and does not need any human interaction. The resilience of the self-organized systems will increase because the system will optimize itself even in challenging situations. The authors did not determine resilience metrics, but proposed multiple ways that could improve the resilience of the system. The authors concluded that the self-organization properties can help with the level of service, but human behaviour should be taken into account when designing a resilient system. In this work, we will also consider self-organization by allocating bandwidths to the user in case of failures. Ahmadi et al. [2] researched the resilience of airborne networks. They use the definition of [17] as the resilience metric. The authors concluded that machine learning and blockchain techniques might be able to improve the resilience of airborne networks. The work in [2] is different from this research because they investigate the resilience of airborne networks while this research will focus on a terrestrial cellular network.

3. RESILIENCE METRICS

After a survey of the literature, we identified the following metrics used in the literature to assess the resilience of a cellular network: Quality of Service, fraction of isolated users, and signal-to-noise ratio.

- **Quality of Service**:

  The Quality of Service (QoS) is arguably the most important resilience metric in mobile networks. One of the widely-used QoS metrics is the data rate (in Mbps) experienced by a user. This metric gives insights on how much the network can satisfy the users and if the network is still functioning or not. According to Kamola et al. [6] QoS is part of the trustworthiness of the resilience of a network.

- **Isolated Users**:

  The number of isolated users is used as a resilience metric in Malandrino et al. [9]. The isolated users are the number of users that do not have any connection to a BS at all. This metric could give insights on how many users will not have any service in the area where a potential risk occurred.

  Also, the average number of users connected to a base station can be used as a resilience metric. This will provide similar results as the number of isolated users since the number of isolated users increases when the average number of users connected to a base station will decrease. But this metric will give insights on how dense the number of BS are in a city.

- **SNR**:

  The Signal-to-Noise ratio (SNR) can be used as a resilience metric. The SNR is a ratio for the signal strength to signal noise [19]. The SNR shows how far users are located and how well the signal reaches the user. Together with the assigned bandwidth, the data rate can be calculated. The SNR can on the other hand show different results since SNR will give information on how close the user is to the BS and the data rate only shows how much the data can be sent to the user.

4. POTENTIAL RISKS

It is important that potential risks are determined to evaluate the resilience of a mobile cellular network. When a potential risk occurs this can lead to errors which can extend to multiple failures of the complete system. Çetinkaya et al. [20] divide potential risks in seven categories: large-scale disasters, socio-political and economic risks, dependent failures, human errors, malicious attacks, unusual but legitimate traffic and environmental risks. Using the potential risks, we determined different potential risks for a mobile cellular network, natural disaster, natural disasters with a power outage, malicious attacks and socio-political risks and other risks.

- **Natural disaster**:

  A natural disaster such as earthquakes, floods and wildfires are a potential risk for a mobile cellular network. A natural disaster can also occur when there are dependent failures, which can cascade through the network and affect multiple BSs. The natural disaster has a big impact on the base stations around the epicentre of the disaster. The BS closest to the epicentre will be more damaged than the BS further away from the epicentre.

  A natural disaster would have a large impact on the resilience of a mobile cellular network. It is expected that there would be a large number of users which are disconnected from all nearby BSs. This would imply that these users will not get any service and that the resilience of the network will be decreased significantly.

- **Natural disasters with a power outage**:

  A natural disaster with a power outage is similar to a normal natural disaster. However in this case, the electricity grid might also be affected by the disaster resulting in total power outage at a certain region. But the area affected by the natural disaster will have no power, which implies that every BS in that area will not have power and will not function completely (it is assumed that backup power is not available for the BSs).

It is expected that a natural disaster with a power outage has more impact on the resilience of a mobile cellular network than a normal natural disaster. It is also expected that this type of disaster has the most impact on the resilience of a mobile cellular network because it would create a lot of isolated users in an area and also users that are connected to BS that are far away. This would imply that many users would not get a satisfactory service.

- **Malicious attacks and socio-political risk**:

  Malicious attacks like a DDoS attack or a targeted attack on a BS could have an impact on the resilience of a mobile cellular network. A DDoS attack could be able to take up parts of the maximum data rate of the BS. Unusual but legitimate traffic occurs when a large number of people try to access the same service at the same time. This will result in the same effects on the network as a DDoS attack. These risks prevent users to get a acceptable level of service.

  It is expected that the resilience of a mobile cellular network will be affected by the malicious attack. But it will only affect a few BS and would not have a big impact on the rest of the network. So it is expected that it will affect the resilience marginally.

- **Increase of requested data rate**:

  A potential risk for a mobile cellular network is that the users request more data rate than the network can actually deliver. This means that the users are less satisfied with the service that they receive. It is expected that the satisfaction level of the users will decrease when more users increase their requested data rate.

- **Other risks**:

  Human errors can fail a BS, but this would not have a very big impact on the resilience of a mobile cellular network, since the human error only affects a limited number of BSs. So this risk will not be taken into account in this research.

5. METHODOLOGY

This section will address the methodology that is being used to answer RQ3. Now that the resilience metrics and potential risks are defined, we will assess the resilience of the cellular networks in the Netherlands via simulations using a data set from OpenCellId [18].

5.1 Cities of the Netherlands

It is not possible to calculate the complete resilience of the complete network in the Netherlands, since the algorithm is too complex and this would require a long simulation time. So we will divide the network into different cities. For this, the 12 provincial cities of the Netherlands will be used. The provincial cities of the Netherlands are Groningen, Leeuwarden, Assen, Zwolle, Lelystad, Arnhem, Utrecht, Haarlem, Den Haag, Middelburg, Den Bosch and Maastricht. Additionally, important cities of the Netherlands are used, such as Amsterdam and Rotterdam. Moreover since this research is performed at the University of Twente, Enschede will also be used in this research. Information of each city is presented in Table 1. We use the population of each city to generate the number of users of a cellular network. Since not all users will be active simultaneously, we assume that only 0.7% of the population is active at the same time.

Table 1: City information

City	Abbreviation	#BSs	#Active users
Amsterdam	Ams	334	5752
Arnhem	Arn	88	1066
Assen	Ass	36	475
Den Bosch	Bos	61	1056
Den Haag	Haa	154	3604
Enschede	Ens	40	1109
Groningen	Gro	74	1402
Haarlem	Hrm	79	1645
Leeuwarden	Lee	38	753
Lelystad	Lel	36	545
Maastricht	Maa	66	856
Middelburg	Mid	24	339
Rotterdam	Rot	178	4386
Utrecht	Utr	236	2515
Zwolle	Zwo	59	867

Since mobile networks do not reveal their infrastructures with the public, we leverage a crowd-sources data set. This is a crowd-source database listing information about the cell towers worldwide. The data set contains information about the location in terms of longitude and latitude, radio type (e.g., 3G or 4G), range and local area code of the BS. Using the longitude and latitude of each city, it is possible to determine which BS is within that city. The range is used to determine if users are close enough to the BS to connect to it. Since the data set contained a large number of entries, some BSs are very close to each other, so we first group them using the local area code to reduce the number of BSs in that area. Due to the time constraints of this research, the difference in delivering service to the users of the different radio types are not taken into account. It is assumed that every BS is an LTE eNodeB and has bandwidth according to that radio type. This will have an impact on the results since LTE has faster performance than a GSM or UMTS network. Moreover, the connectivity between BS and the way data travels between the BSs is also not simulated, for the sake of simplicity.

5.2 Simulation Model

The simulation will load in all the BS of a city using the OpenCellId [18] data set. In the same area users will be randomly distributed in the cities. Each user will have a longitude, latitude, link object to a BS and a requested data rate. The requested data rate is a randomized integer between 10 and 100 Mbps to simulate different traffic profiles, e.g., users with a video streaming application or web browsing.

A link can be created between a user and a BS when the user is within the range of the BS, which is retrieved from the OpenCellId data set [18]. The simulator will determine which BS is the closest to the user. It will try to connect the user to the BS, if that is not possible, because for instance there is no available bandwidth left for the user then it will try to connect the user to the second closest BS. If the user is not able to connect to a BS, this user will be considered as an isolated user. When the link object is created, multiple properties will be defined. First, it will save the distance between the user and the BS. Given the requested rate of the user, it is possible to calculate how much bandwidth the users needs using the Shannon Capacity formula [14].

The number of channels that each BS has in the simulation is 5. Each channel has a maximum bandwidth of 20 MHz. Each channel can provide different bandwidths to the user. This bandwidth will be allocated to the users considering the following concrete bandwidths, [20, 15, 10, 5, 4, 1.4] MHz. These bandwidths are from LTE channels and are also applied to BS with another radio type for the sake of simplicity. For instance if a user requests 7 MHz then 10 MHz will be allocated to the user. When assigning bandwidths to the users, the users will be sorted in decreasing order according to the amount of requested bandwidth. When a channel does not have enough bandwidth to serve another user, the user with the most bandwidth will receive a lower bandwidth so that another user can be served. For instance if there are 2 users where 1 user is using 10 MHz and the other 15 MHz of bandwidth, then the total bandwidth is 25 MHz. This is too much for the channel, so the bandwidth of the user that receives 15 MHz will reduce the bandwidth to 10 MHz. This will ensure that less users are isolated, but it will less satisfy some users. Since it is arguably more important to serve more users than to give a higher satisfaction level to some users.

5.3 Simulation Environment

We develop a system-level simulator in Python [13] to simulate the potential risks on the cities and retrieve the resilience metrics.

Frameworks

It will load in the BSs for the city, create a baseline, fail some of the BSs according to the model of the potential risk and retrieve resilience metrics. After that, it saves all the retrieved data in a CSV file. NumPy [11] is used to have some helper functions for randomization of the distribution of the users and for failing of the BSs. The SciPy [15] and NumPy [11] libraries are used to determine the 95% confidence interval of the data. Plotly [12] is used to plot all the retrieved metrics into charts. Since it is an easy-to-use library to plot charts with a large amount of data.

LTE framework

The larger the distance between the user and BS the lower the receiving power will be. The received power can be calculated as follows:

$$P_{rx} = P_{tx} - Max(PL - G_{tx} - G_{rx}, MCL) \tag{1}$$

where P_{rx} is the received signal power, P_{tx} the transmitted signal power, G_{tx} the transmitter antenna gain, G_{rx} the receiver antenna gain and MCL the minimum coupling loss, which is the minimum signal loss between BS and user. Also, the path loss needs to be calculated to complete this formula. We assume a Macro cell propagation model for an Urban Area [1]. The propagation model can be calculated as follows:

$$\begin{aligned} L = 40 \cdot (1 - 4 \cdot 10^{-3} \cdot Dhb) + \log_{10}(R) \\ -18 \cdot \log_{10}(Dhb) + 21 \cdot \log_{10}(f) + 80 \end{aligned} \tag{2}$$

where R is the distance between the user and the BS, f the carrier frequency and Dhb the base station antenna height in meters, measured from the average rooftop level. Finally, the path loss formula can be calculated as follows [1]:

$$PL = L + \sqrt{10} * randn(1). \tag{3}$$

The signal bandwidths are carried over a 2000 MHz frequency. The base stations have a P_{tx} of 43 dB [1], the antenna height is 15 meters, the MCL is 70 dB, the G_{tx} is 15 dBi, G_{rx} is 0 dBi.

After calculating the receiving power using (1), the SNR can be calculated using (6). The SNR can then be used to calculate the data rate that the user receives. The data rate can be calculated using the Shannon Capacity (4), where B the bandwidth in MHz and C is the data rate (capacity) in Mbps:

$$C = B * \log_2(1 + SNR). \tag{4}$$

5.4 Calculating Resilience Metrics

The simulator needs to calculate the resilience metrics for a certain scenario. This subsection will discuss how the resilience metrics are calculated for a certain scenario.

- **Quality of Service**

  To determine the QoS resilience metic, the satisfaction level will be calculated. The formula to calculate the satisfaction level is as follows:

  $$S = \frac{\sum_{i=0}^{\#users} \frac{C_i}{R_i}}{\#users} \tag{5}$$

  where S is the satisfaction level, C_i the received data rate and R_i the requested data rate of a user. This formula creates an average of the satisfaction level of the users.

- **Isolated users**

  The number of isolated users is the number of all the users that are not connected to a BS. We also report the average number of users per BS.

- **SNR**

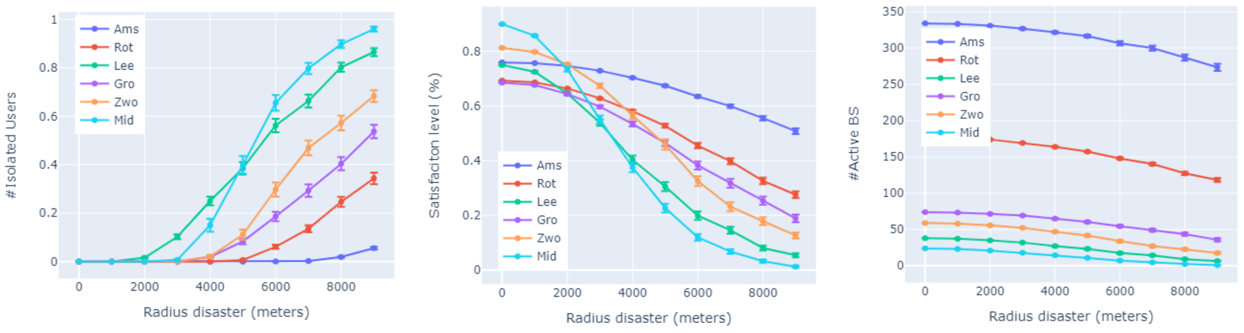
  SNR is calculated as follows:

  $$SNR = \frac{P_{signal}}{P_{noise}}. \tag{6}$$

  The signal strength will be determined using a path loss model [1]. The signal noise will be set as a constant in the simulation.

5.5 Test Scenarios

To determine how much effect each potential risk has on the resilience of mobile networks, test scenarios are performed in the simulation. Each scenario will run 200 times to ensure that the randomizations performed are unified and a normal distribution can be used to determine a 95% confidence level. When running a scenario each round the user will be placed randomly in the city. The following scenarios will be performed:



(a) Isolated Users.

(b) Satisfaction level.

(c) Number of active BSs.

Figure 1: The impacts of increasing radius of a natural disaster on the resilience

- **Natural disaster**:

  This scenario will simulate how a natural disaster would impact the resilience of a mobile cellular network. The position of the natural disaster will change at each round of the simulation. This will evaluate how resilient the network is in different parts of the city. This simulation will alter the radius of the disaster. The simulation starts with a radius of 0 meters to create a baseline and will be increased by 1000 meter up until 9000 meters. To represent the fact the the failure probability of a BS depends on its distance from the epicentre of the disaster, we define the probability of failure of a BS as follows:

$$\left(\frac{Distance\_to\_BS}{Radius\_of\_disaster}\right)^2. \tag{7}$$

- **Natural disaster with a power outage**:

  This scenario works the same as a standard natural disaster, but in this scenario all BSs in the area of the disaster will completely fail. The same range for the radius for the disaster will be used as the standard natural disaster.

- **Malicious attack**:

  This scenario will simulate a malicious attack on a network. The simulation will randomly choose 50% of the base stations. This will be randomized each simulation round. Each severity level the amount of available functionality of the BS will be decreased by 0.1, starting with 1 and ending with 0.

- **Increase of requested data rate**:

  To simulate the increase of requested capacities of the users, the simulation will start with a low requested data rate for the users and increases the request. The requested capacities for each severity level is shown in Table 2.

6. PERFORMANCE ANALYSIS

This section will discuss the results obtained from the simulated scenarios discussed in Section 5. Each value point in the charts has an error bar which shows the 95% confidence interval. The potential risks are simulated on every city, but to decrease the amount of information in the figures a set of cities will be removed from the figures, since they show similar results to other cities. The simulator can be found on the git repository [5].

Table 2: Minimum and maximum requested capacities per severity level

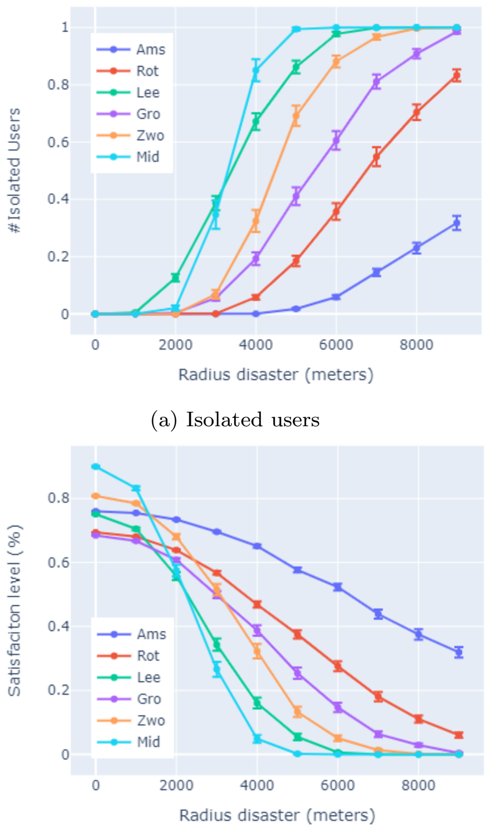
Severity level	Min. Mbps	Max. Mbps
0	10	20
1	20	30
2	30	40
3	40	50
4	50	60
5	60	70
6	70	80
7	80	90
8	90	100
9	100	110

6.1 Natural Disaster

The results of the simulation for a large disaster can be seen in Figures 1a, 1b and 1c. Figure 1a shows the percentage of isolated users in each city. It was expected that the percentage of isolated users would rise when the radius of the disaster increases. According to Figure 1a this is also the case. For instance, the number of isolated users of Middelburg increases rapidly when the radius of the disaster is 3000 meters. The city that has the least number of isolated users is Amsterdam. Even when the radius of the disaster is 9000 meters, the number isolated is still around 5%. A reason why Middelburg is more affected by a natural disaster than Amsterdam is that Amsterdam is larger than Middelburg. Hence, the natural disaster takes up less space in the whole city and the rest of the city will just function normally. In the case of Middelburg, the natural disaster will affect most of the space of the city which results in almost none of the BSs remaining active. The number of active base stations can be found in Figure 1c. When the disaster has a radius of 9000 meters Amsterdam still has around 272 BSs that are still active. Middelburg on the other hand has only 1 BS left that is still active. Consequently, in Middelburg the satisfaction level will also be low, since many more users are connected to that single BS or not even connected at all. The single BS can then only provide the minimum level of service to these users. In Figure 1b it is visible that the satisfaction level of the users is very low in Middelburg. For Amsterdam, the satisfaction level is still at an acceptable level with disaster with a radius of 9000 meters.

6.2 Natural disaster with a power outage

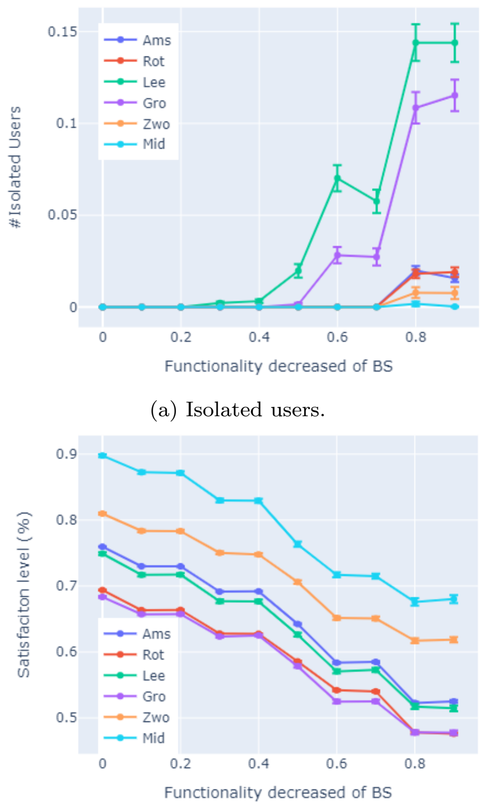
It was expected that a natural disaster with a power outage would have a larger impact on the resilience level of the mobile cellular network. It was also expected that



(a) Isolated users

(b) Satisfaction level

Figure 2: Natural disaster with a power outage



(a) Isolated users.

(b) Satisfaction level.

Figure 3: The impact of increasing severity of malicious attacks

there would be more isolated users than in a natural disaster without a power outage. When comparing Figure 1a to Figure 2a it is visible that a natural disaster with a power outage has significantly more impact on the number of isolated users. Middelburg will be completely isolated when there is a natural disaster with a power outage with a radius of 5000 meters, while in a natural disaster without a power outage there never was a situation where the whole city was isolated. Even for Amsterdam, the natural disaster with a power outage had more impact than the natural disaster without a power outage. A disaster with a power outage with a radius of 9000 meters would isolate around 35% of the users in Amsterdam. Compared to the 6% of natural disaster without a power outage, this is a large increase of isolated users. Due to a large number of isolated users, the received data rate is also low for most of the cities, see Figure 2b. The same reason as for disaster without power outage can be used. Since there are only a couple of BSs left, the number of connected users to each BS will increase and the data rate available for each user will also decrease.

6.3 Malicious attacks

In Figure 3a the number of isolated users is presented. According to the Figure 3a Leeuwarden has the most isolated users. However this is only 14%. Moreover, Figure 3b shows that the satisfaction level in the cities are decreasing equally. The satisfaction level of each city decreases around 0.2 than the starting satisfaction level. So Figure 3a and 3b conclude that a malicious attack does not have a large impact on the resilience of the network. Additionally, all cities are resilient at an acceptable level against malicious attacks. Users are still connected but they will have a lower satisfaction due to the malicious attacks.

6.4 Increase of requested data rate

In Figure 4 the satisfaction level of the users is provided. In comparison to a natural disaster Middelburg is performing relatively the best. The satisfaction level of the users remains high compared to the other cities, while Rotterdam gets affected more by the increase of requested data rate. We notice that Rotterdam has 25 users per BS. This is significantly larger than Middelburg, since Middelburg only has 14 users per BS. So there is a relation between the number users connected to the BS and the satisfaction level of the users when there are no failures on the BS.

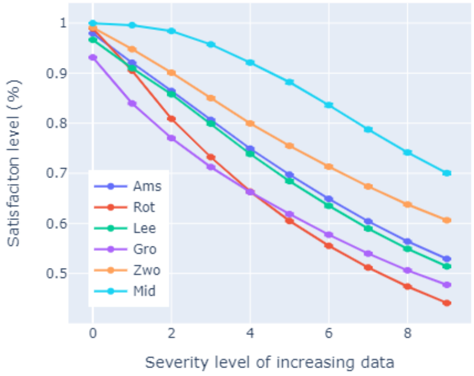


Figure 4: The satisfaction level when increasing requested data rate

7. DISCUSSION

In this seciton, we discuss the shortcomings of our research.

First a key shortcoming of our research is that our analysis depends on the data retrieved from OpenCellId. Since the data is crowd-sourced, the data is not verified by the network operators. This can affect the data on the location and range of the data set. Additionally, the people collecting the data for OpenCellId can be not equally distributed over the Netherlands. This means that there are location with more BS and other location with less BS. Hence, the results of this paper are in favor for the cities where more BS are recorded.

Secondly for the simulations, we have made some assumptions which results in less realistic setting. For example, the LTE model used in the simulator is less realistic than a normal LTE network. It is possible to model the LTE network so that the requested bandwidth is provided to the user. When there is not enough bandwidth, users will receive less bandwidth, resulting in a lower satisfaction level. Moreover this simulation assumes that every BS is an eNodeB BS and does not consider GSM or UMTS. This should be taken into account in future studies.

Finally, the simulator normally distributes the users over the city. Most of the time this is not the case and the users are more close to the center of the city. This should be taken account in future research.

8. CONCLUSION

Since the use of mobile cellular networks has increased significantly, it is important to understand the resilience of mobile cellular networks. This paper uses a literature survey to determine resilience metrics and potential risks for a mobile cellular network. Some of the resilience metrics are Quality of Service, isolated users and the Signal-to-Noise ratio. The potential risks for a mobile cellular network are natural disaster, natural disaster with a power outage, malicious attack, socio-political reason and economic risks and environmental risks. This paper analyses the potential risks on cities in the Netherlands using a simulation created in Python [13] using an OpenCellId [18] data set of the base stations. To conclude the results, all cities are resilient against malicious attacks. Amsterdam has the best resilience of the Netherlands when a natural disaster occurs, due to a large number of base stations and the large area of Amsterdam. Middelburg is the least resilient of the Netherlands against natural disasters, since it is significantly smaller and has a smaller number of base station than Amsterdam. However, if there are no failures in the network but the requested data rate of the users increases, then Middelburg is performing the best and Rotterdam is performing poorly. This occurs, because Rotterdam has the highest number of connected users per BS and Middelburg has the lowest. So it can be concluded that there is relation between the number of connected users per BS and the satisfaction.

9. ACKNOWLEDGEMENTS

I would like to thank Suzan Bayhan and Syllas Magalhaes for being supervisors during this research period. All the advice that both of my supervisors provided were taken into account for this research.

10. REFERENCES

[1] 3GPP. Etsi tr 136942 v10.2.0. May 2011.

[2] H. Ahmadi, G. Fontanesi, K. Katzis, M. Z. Shakir, and A. Zhu. Resilience of airborne networks. *Annual International Symposium on Personal, Indoorm and Mobile Radio Communications*, pages 1155–1156, 2018.

[3] N. Alliance. 5g white paper. *Next generation mobile networks, white paper*, 2015.

[4] S. Dobson, D. Hutchison, A. Mauthe, A. Schaeffer-Filho, P. Smith, and J. P. Sterbenz. Self-organization and resilience for networked systems: Design principles and open research issues. *Preceedings of the IEEE*, 107(4):819–834, March 2019.

[5] D. D. Janssen. https://github.com/ddjanssen/resilsimulator. June 2021.

[6] M. Kamola and P. Arabas. Network resilience analysis: Review of concepts and a country-level. case study. *Computer Science*, 15(3), 2014.

[7] G. Lio and C. Ji. Scalability of network-failure resilience: Analysis using multi-layer probabilistic graphical models. *IEEE/ACM TRANSACTIONS ON NETWORKING*, 17(1), February 2009.

[8] D. Lummen. An analysis of link and node level resilience on network resilience. *33rd Twente Student Conference on IT*, July 2020.

[9] F. Malandrino and C. F. Chiasserini. Quantifying and minimizing the impact of disasters on wireless communications. *I-TENDER 2017 - Proceedings of the 2017 1st CoNEXT Workshop on ICT Tools for Emergency Networks and Disaster Relief*, 2017.

[10] V. M. Mina Labib and J. H. Reed. Analyzing and enhancing the resilience of lte/lte-a systems to rf spoofing. *2015 IEEE Conference on Standards for communications and Networking, CSCN 2015*, pages 315–320, 2016.

[11] NumPy. https://numpy.org/. May 2021.

[12] Plotly. https://plotly.com/python/. June 2021.

[13] Python-Software-Foundation. https://www.python.org/. April 2021.

[14] T. J. Rouphael. Rf and digital signal processing for software-defined radio - chapter 3 - common digital modulation methods. pages 25–85, 2009.

[15] SciPy. https://www.scipy.org/. May 2021.

[16] P. Smith, D. Hutchison, J. P. Sterbenz, M. Schöller, A. Fessie, M. Karaliopoulos, C. Lac, and B. Plattner. Network resilience: A systematic approach. *IEEE Communications Magazine*, 49(7):88–97, July 2011.

[17] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. Rohrer, M. Schöller, and P. Smith. Reilience and survivability in communication networks: Strategies principles and survey of disciplines. *Computer networks*, 54(8):1245–1265, March 2010.

[18] Unwired-labs. https://www.opencellid.org/. April 2021.

[19] Wikipedia. https://en.wikipedia.org/wiki/signal-to-noise_ratio. June 2021.

[20] E. K. Çetinkaya and J. P. Sterbenz. a taxonomy of network challenges. *2013 9th International Conference on the Design of Reliable Communication Networks, DRCN 2013*, 2013.