RAMS

Reliability, Availability,
Maintainability, and Safety

This is the Title of my Thesis

Your Name

August 2014

PROJECT / MASTER THESIS

Department of Production and Quality Engineering

Norwegian University of Science and Technology

Supervisor 1: Professor Ask Burlefot

Supervisor 2: Professor Fingal Olsson

Preface

Here, you give a brief introduction to your work. What it is (e.g., a Master's thesis in RAMS at NTNU as part of the study program xxx and...), when it was carried out (e.g., during the autumn semester of 2021). If the project has been carried out for a company, you should mention this and also describe the cooperation with the company. You may also describe how the idea to the project was brought up.

You should also specify the assumed background of the readers of this report (who are you writing for).

Trondheim, 2012-12-16

(Your signature)

Ola Nordmann

Acknowledgment

I would like to thank the following persons for their great help during ...

If the project has been carried out in cooperation with an external partner (e.g., a company), you should acknowledge the contribution and give thanks to the involved persons.

You should also acknowledge the contributions made by your supervisor(s).

O.N.

(Your initials)

Summary and Conclusions

Here you give a summary of your your work and your results. This is like a management summary and should be written in a clear and easy language, without many difficult terms and without abbreviations. Everything you present here must be treated in more detail in the main report. You should not give any references to the report in the summary – just explain what you have done and what you have found out. The Summary and Conclusions should be no more than two pages.

You may assume that you have got three minutes to present to the Rector of NTNU what you have done and what you have found out as part of your thesis. (He is an intelligent person, but does not know much about your field of expertise.)

Contents

Preface i

Acknowledgment ii

Summary and Conclusions iii

1 Approaches for Detecting Robots in Social Media **2**

1.1 Introduction 3

1.2 Definition and History of Social Bots 4

1.3 Important Social Media Platforms 5

1.4 Why is Bot Detection in Social Media Important? 6

1.5 Social Bot Detection Approaches 8

1.5.1 Based on Social Network Information 8

1.5.2 Based on Crowd-Sourcing 10

1.5.3 Based on Features 12

1.6 Summary and Outlook 14

2 Equations, etc **16**

2.1 Simple Equations 16

2.2 Including Figures 18

2.3 Including Tables 19

2.4 Copying Figures and Tables 19

2.5 References to Figures and Tables 21

2.6 A Word About Font-encoding 21

2.7 Plagiarism 21

3 Summary **23**

3.1 Summary and Conclusions 23

3.2 Discussion 23

3.3 Recommendations for Further Work 24

A Acronyms **25**

B Additional Information **26**

B.1 Introduction 26

B.1.1 More Details 26

Bibliography **27**

Curriculum Vitae **30**

Chapter 1

Approaches for Detecting Robots in Social Media

Management Summary

This is the management summary blablabla mhmhm...

1.1 Introduction

Social media is an important part of todays Internet. Of the approximately 3.4 billion internet users, about 2.3 billion use social media actively what means that almost 70 percent of all internet users use social media on a regular basis [2]. Especially in order to obtain information about events and the like, social media is often irreplaceable. For some people social media platforms even substitute real life personal contact to a large degree.

With this importance of social media platforms in the lives of so many people, these platforms get more and more interesting for people that want to benefit economically from them. These are for example companies that want to promote their products and services via those social channels. However, the problem here is that, due to their size, it is hard to disseminate a certain message on social media platforms. Like in many other areas of today's information technology, big data is a huge topic in social media.

This is one of the reasons, why social robots, in the form as we know them today, have been developed. As software robots are often simply called bot, we will use the term social bot or simply bot in the following synonymously for social robot. The propagation of such bots has reached a remarkable high level. In 2014, the social media platform Twitter, about we will hear more later on, stated in a report to the United States Securities and Exchange Commission, that up to 8.5% of their active user base may be social bots[1]. We will see in the upcoming chapters, that they are used to spread certain messages, hide others or simply to give the impression of a much bigger support for a person, thing or belief than there actually is. As we will see as well, though, social bots are also used to directly attack other, actual users directly, for example to steal their personal data.

First of all, we will take a look at the definition and history of social bots, in order to clearly define what we are talking about and where it originates from. We will then take a look at the online social media platforms that are important for this chapter, namely Twitter, Facebook and Renren, and give a short overview about their characteristics relevant here. Afterwards, we will motivate why social bot detection is actually important. In the main part of this chapter, we will introduce several social bot detection approaches and give examples for them. In the last section we will finally summarize our findings and give an outlook about the further challenges

in this area.

1.2 Definition and History of Social Bots

This section will introduce the term social bot formally and give a short overview about the beginning and the development of this topic.

In order to be able to discuss social media bot detection, we need a clear understanding of what social bots actually are. For that, we use the definition given by Ferrara et al. in their article The Rise of Social Bots:

> "A social bot is a computer algorithm that automatically produces content and interacts with humans on social media, trying to emulate and possibly alter their behavior." [12]

The root of of social bots, or just bots how we will sometimes call them here as well, can probably be found in the Turing test, developed by Alan Turing in 1950 [19]. It involves three parties, two of which are human and one is a computer program. While one human is having a conversation with the software, it is the task of the other human to identify the program. If he is not able to do so, the software is passing the Turing test. This led to the development of a lot of so called chatbots, which just aimed to appear as human as possible in a conversation.

A rather famous and often cited example for such a chatbot is ELIZA, introduced by Joseph Weizenbaum 1966 in [23]. It mimicked a psychotherapist and showed that – at least some kind of – communication between a human and a computer is possible.

Since then, a lot of things have changed. Today, bots are a lot more than bare entertainment or proof of concept. With the triumph of the Internet and especially social networks like Facebook and Twitter, the possible use cases for social bots have increased dramatically. While they were initially mostly used to simply post content, today they are able to credibly interact with each other and even humans [6, 14]. As we will see in the next section, nowadays bots are used to spread messages, for marketing and a lot more.

1.3 Important Social Media Platforms

In this section we want to give an short overview about the social media platforms, or online social networks (OSNs), that are relevant for this chapter. This is necessary in order to better understand the problems and attacks that will be presented later on. However, we will describe those networks only as detailed as necessary in this context, since a comprehensive explanation would go beyond the scope of this chapter.

The first and probably most important OSN that needs to be mentioned here is Twitter[1]. Twitter is a microblogging network which allows its users to broadcast short messages, so called tweets. Tweets can be seen by anyone that follows the tweeting account. Following is hereby a one-way process, that does not need any confirmation by the followed account. Thus, tweets can be seen as public. Furthermore, tweets can be retweeted. Retweets can be seen as a forwarding of a tweet in order to disseminate it: all followers of the retweeting account get the retweeted message. Tweets can be tagged with hashtags, that associate them with a certain topic or an ongoing discussion.

Another OSN that is important for this chapter is Facebook[2]. As on Twitter, it is possible to publish messages on Facebook. However, the visibility of those messages, or posts, can be adjusted. Usually, posts are only visible to users that are friends with the posting account. A friendship is here, in contrast to follow-relationship on twitter, bilateral: a user can send a friendship request to another account which has to accept it in order for the relationship to be built. A difference to Twitter that is important is well is, that Facebook accounts respectively profiles usually contain a lot more personal information than Twitter accounts do. Like it was the case with posts, the visibility of Facebook profile pages can be adjusted and usually they are only visible to accounts that are friends.

The last platform we want to mention shortly is Renren[3], which is a chinese OSN directed mainly at college students. Like Facebook it uses the concept of friendships and highly personalized profiles. It also allows to post messages that can be seen by friends.

[1] https://twitter.com/
[2] https://www.facebook.com/
[3] http://renren.com

1.4 Why is Bot Detection in Social Media Important?

Another point that is important to be looked at before we go into detail about the actual detection methods is, why social media bot detection is important at all. In this section we will argue, why this is a – especially today – important topic.

As already said above, social media platforms are nowadays an important component in the life of many people. For some, they even substitute real personal contact sometimes. Thus, it is important to ensure, that humans are still able to estimate what is happening in their social media surrounding and what can be seen as trustworthy – and what can not. While the challenge of verifying facts or news from the Internet is not new, social bots add a new factor to this challenge. They can make a non-trustworthy source look trustworthy by simulating that it is highly popular.

An example for this, is the so called astroturfing. In an astroturfing campaign, an attacker tries to give the impression of a broad grassroot support for a certain person, belief or political position. A known political astroturfing case are for example the 2010 Massachusetts senate elections in the US. During these, a small number of Twitter social bot accounts produced a large amount of tweets that contained a link to a website that smeared one of the candidates. The tweets also mentioned users that had shown the same political position in beforehand and thus were likely to retweet. In a few hours the smearing website link spread rapidly what was even noticed by the Google search engine. That way, the website got promoted to the top search results for the name of the smeared candidate [15].

A similar approach can also be used to distract from potentially inconvenient or just unwanted facts or opinions and is then called smoke screening. By just flooding the platform with information it aims to draw attention away from the unwanted topic to a topic that suits the attacker more. The flooding information can hereby even be related to the topic that is to be screened. It just focuses on a component that is more pleasant to the attacker and withholds the inconvenient part. An example for this is given by Abokhodair et al. in [3] in the context of the syrian civial war. They analyze a social botnet on Twitter from April until December 2012. It made heavy use of this technique in order to cover up news about the civil war in Syria.

Another, more direct, example for an attack scenario is described by Boshmaf et al. They

operated a network of social bots on the social media platform Facebook and successfully tried to build as many relationships as possible with real users. After this was done, they were able to extract data from the profiles of those real users that were not publicly available, like for example mail addresses or phone numbers. While they show that operating such a botnet for the sole purpose of data extraction might not be efficient for an attacker, they argue that this data can be used for more advanced attacks afterwards [6].

Besides all these specific attacks, which are carried out by bots built for this purpose, there are also simple negative effects from social bots that have not necessarily been built for an attacking purpose. The information in social media is often used by various entities. An example for this is the area of emergency response. By analyzing the information streams of social media platforms it is possible to estimate emergency situations and to take proper actions for decision makers. Cassa et al. for example, show in [8] that information about the Boston Marathon attacks in 2013 were available on the social media platform Twitter more than five minutes earlier than the public health alerts, even though on this event there were already many first responders present. Another area where information from social media platforms is leveraged is the stock market. By monitoring the general mood on Twitter for example, it is possible to predict the market trend to a certain degree [4]. A case can be made that this is also already done by traders. When in 2013 for example the Twitter account of the Associate Press was hacked and it posted rumors about a terrorist attack, the stock market crashed significantly [12]. It is therefor not hard to see that bot-caused information distortion on social media platforms – that does not even necessarily needs to be intended malicious – can have severe impact. Some social bots are built just to retweet and if they retweet false information or rumors they help to make this information popular. This happened for example also after the former mentioned Boston Marathon attacks, where false accusations were spread by such social bots [13].

Furthermore, social bots are often used by public persons in order to appear more popular and thus to gain influence or by companies in order to promote their products on social media platforms [17]. Here, social bot detection is necessary as well for ordinary users to be able to distinguish between real and bought support.

1.5 Social Bot Detection Approaches

In this chapter we want to introduce several techniques for detecting social bots. Based on Ferrara et al. [12] we distinguish three detection approach classes.

The first category of detection approaches is based on social network information. They are also called graph-based, since they map users and their relations into a graph and then try to identify bots in the hereby obtained social network by means of graph theory.

Afterwards we will discuss crowd-sourcing based social bot detection approaches. They use actual humans to detect bots, assuming that the human ability to notice details in communication will make this an easy task.

The last category we want to elaborate on are detection approaches based on behavioral features. Mechanisms that make use of this approach try to observe behavioral patterns that are typical for social bots. By doing so they aim to distinguish bots from human users. [12].

In the following sub sections, we will go into detail about each of these three approaches and illustrate them using real detection systems. It has to be noted though, that the borders between the individual approaches is not always very clear, so that some examples could also be mentioned in a different category. Many schemes for example, use some kind of graph theory. However, we try to categorize them by their core traits.

1.5.1 Based on Social Network Information

A term that is often used in combination with detection of bots by using social networks is sybil or the sybil attack. It was presented as a thread to distributed systems by John R. Douceur in [11]. In the specific context of social media platforms when conducting a sybil attack, an attacker creates a large amount of fake identities in a system to the point where these identities make up a considerable fraction of the system's whole user base. When this is achieved, the attacker can influence the whole system and control its contents to a certain degree. A sybil, sybil node or sybil account is therefor simply one of the fake entities, or, depending on the attack architecture, just a social bot. It is not hard to see that social bot detection can, more specifically, be viewed as a defense against the sybil attack.

The general proceeding of social network based bot detection approaches is rather simple.

They map the users base of the social platform they aim to defend into a social graph, where a node is corresponding to a user and an edge between two nodes exists if there is a specific kind of relationships between the two respective users on the platform. The nodes can be hereby be distinguished in sybil nodes, respectively bots, and non-sybil nodes, respectively legitimate users. The goal of the detection approach is now, to identify whether a given node is a sybil or not [20].

There are a number of proposed social network based sybil detection schemes like for example SybilGuard [25], SybilInfer [9] or SumUp [18]. While they all have different assumptions and use varying algorithms to achiever their goal, Viswanath et al. show in [20], that, at a high level, all of them work by them same principles.

Basically they can be viewed as graph partitioning algorithms, which partition a given graph into multiple disjoint subgraphs. As already mentioned above, ideally two subgraphs are assembled, one that contains only sybil nodes and one that contains only non-sybil nodes. Since a clear distinction is often hard to make, the approaches basically assign a rank to each node and decide afterwards, depending on several parameters, which ranks are classified as sybil and which as non-sybil. It is thereby obvious, that the ranking algorithm is crucial for the whole scheme. Though, of course, the ranking algorithms for the different detection schemes are differing, they generally have in common, that they base their rating on how tightly connected the respective node is to a known trusted node. Thus, they work by detecting local communities of nodes. In other words closely connected groups of nodes [20].

It is not hard to see, that these algorithms are therefor easy to deceive. If an attacker is able to establish so called attack edges, connections between his sybil nodes and non-sybil nodes which are connected to a trusted community, it gets significantly harder to identify the bots. A common assumption is that these attack edges are hard to create [25], which means, that legitimate users tend not to establish social network connections to social bots. However, Boshmaf et al. show in [5] that this assumption is to be questioned. They tried to infiltrate the social media platform Facebook with a large number of sybil accounts and tried to establish connections to real users. The average acceptance rate of their relationship requests came to about 20% and could be increased to 80% depending on how many indirect relationships between the sybil and the user already existed [5].

A well known example for a bot detection approach that is based on social network information is the Facebook Immune System (IMS) [16]. This system aims to defend the social media platform Facebook and its users not only against sybil attacks but also to prevent spam, malware distribution, phishing and so on. To achieve this goal, it takes a lot more actions than the above described general approach for social network based detection schemes. The IMS runs checks on every action performed on Facebook in realtime in order to give attackers as less time as possible to accomplish there goals and to react. It classifies these actions according to predefined policies and makes it thereby possible to judge them and the corresponding users.

An example for this could be a newly created Facebook account, that sends a lot of friendship requests. These are used in Facebook to establish relationships between users. A legitimate user starts sending friendship requests usually mainly to people he knows and vice versa, that is, people that are likely to accept his friendship request. If a lot of these requests are now declined, this could be a indication for the system that the sending user might not be legitimate. The IMS also makes heavy use of machine learning, to which we will come back in later on, and generates training data automatically in order to adapt to the fast changing attacks and user behavior [16].

1.5.2 Based on Crowd-Sourcing

A rather straight forward approach for social bot detection is based on crowd-sourcing. In contrast to the above described social network information based approaches, a connection between bots and legitimate users is not a problem for schemes based on this approach – at least not a direct one. The basic idea of crowd-sourcing based social bot detection is, to engage actual human workers to study user profiles and subsequently to decide whether it belongs to an actual user or a sybil.

In [22], Wang et al. presented a study on the effectiveness of this approach and introduce a sample for a crowd-sourcing based social bot detection system. For their tests they use sample data from Renren, China's most popular social media platform, Facebook US and Facebook India. They subdivide their human investigators, or simply testers, in expert workers, and crowd-sourced workers. Each of the testers is presented a number of social media profiles and has to decide, whether it is a real one, or a sybil. While the experts achieve a detection rate at about 90%, the crowd-sourced workers perform not as good individually. If their single votes are ag-

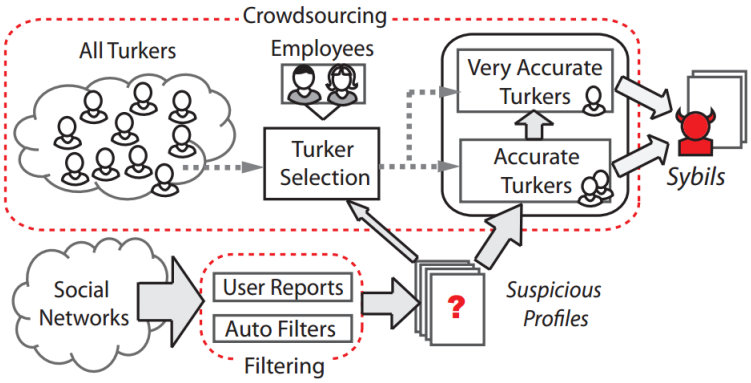


Figure 1.1: A crowd-sourced sybil detection system introduced by Wang et al. [22].

gregated and used for a majority decision though, the results can significantly increased. If this is done for the expert workers, their results can be increased even more, too. A very desirable result of their studies is also that the false positive rate, that is the amount of profiles that are falsely classified as sybils, is in all groups very close to zero. This ensures, that the probability that legitimate users are accused to be social bots, what will probably offend them, is very low.

Wang et al. conclude, that it is very hard for sybil creators, to assemble social bots respectively profiles that are able to pass a "social turing test" and that crowd-sourcing based approaches can perform very well. They proceed with introducing a general practical system that is illustrated in figure 1.1 [4].

The system is working like this: The social network respectively social media platform that is to be defended generates suspicious profiles. This can either happen through explicit reports from users or through automatically applied filters that detect abnormal behavior. The so obtained profiles are then checked by crowd-sourced workers, which are subdivided in accurate and very accurate. To establish this differentiation, some of the suspicious profiles are mixed with some profiles that are known to be sybils. They are presented to all workers and their results allow a classification and to filter out unreliable workers. In the actual checking process, the profiles are first presented to the accurate workers which make a majority vote. If their decision is not clear, the profiles are presented to the very accurate workers which once again make a majority vote. The authors claim, that a system like this is very reliable and cost effective.

[4] Turkers are in this case the former mentioned crowd-sourced workers.

Though such a social bot detection approach based on crowd-sourcing seems very promising at first sight, several problems become obvious on closer examination. First of all, this approach works optimal if every newly created profile can be reviewed in the above described way. However, young social media platforms will probably not be able or willing to pay for this bot detection scheme. A factor that may influence this could be also, that those platforms probably do not have huge issues with the social bot problem in their early stages. Once the platform has grown an the issue arises though, their is usually already a huge user base that has to be reviewed retrospectively. This is not optimal and may take a considerable amount of time.

Another point that mus be taken into consideration is that this approach might not be suitable for all types of social media platforms. While it might be well suited for platforms like Facebook or Renren, where profile pages can be customized a lot and contain usually plenty of information, other networks, like for example Twitter could be less appropriate. Generally it can be said that this detection approach is highly based on the information given in the users' profiles. If the information contained in the profiles is low, human investigators will probably not be able to distinguish as precisely as in the tests of Wang et al.

The last and probably most difficult issue that has to be mentioned is connected to this. Human investigators that are charged with distinguishing between bots and legitimate users have to have access to the profiles of the users. While those profiles are sometimes publicly available anyways, detailed profiles, which are more interesting for this approach, are, as discussed above, usually only visible for certain users. It is not hard to see the privacy issue that arises here, especially when keeping in mind, that the investigators are – at least to a great extent – only crowd-sourced workers, that can not be supervised as easily as ordinary employees [12].

1.5.3 Based on Features

The last detection approach for social bots is based on features. Features hereby means observable characteristics of posted information, profiles and possibly everything else that can be associated to the account in question. Schemes that make use of this approach often also use machine learning algorithms. That are algorithms that are able to make decisions based on learned patterns. They basically consist of two phases. In the first phase, the so called training phase, the algorithm processes training data which is labeled with the decision that should be

made on this piece of data. By processing a lot of training data, the algorithm learns the features that are indicators for a certain decision. In the second phase, real data is processed and the algorithm is able to make decisions based on the learned data. Thus, schemes that make use of this detection approach can be compared to anomaly based intrusion detection systems. In the social bot detection topic, the decision being made is usually whether a specific account is controlled by a bot or a human. Since it is not easy to make a clear decision in many cases, there are often multiple decision options that each express a degree of certainty.

A well known example for this kind of social bot detection is the Bot or Not? system, presented by Davis et al. in [10]. It is a publicly available[5] system that allows a feature based social bot detection for accounts on the social media platform Twitter. Bot or Not? was trained with about 31.000 account samples of both, human and social bot accounts. For classification makes use of more than 1.000 features that can be assigned to six feature-classes. In the following we want to mention these classes shortly:

- **Network** features reflect on the spreading of information, for example citations of different users or the like.
- **User** features take the information given in the actual account into consideration. Metadata, that is basically data about data, is especially relevant in this feature.
- **Friends** features are about the social relationships the account in question has.
- **Temporal** features analyze issues like the rate in which content is produced and the like.
- **Content** features are about wording characteristics in the texts produced by the relevant account.
- **Sentiment** features reflect on emotional aspects and are obtained by using specific algorithms [10].

If a Twitter account name is entered in the Bot or Not? system, it checks all of those features and afterwards decides, based on the former mentioned training data, whether this account is a human or bot account.

[5] http://truthy.indiana.edu/botornot

Another social bot detection approach that can be classified as, kind of, feature based relies on detecting the coordinated behavior between social bots. Schemes that make use of this approach focus generally on the above described network, content and temporal features and often incorporate some graph theory as well. They usually aim at detecting attacks which try to distract from unpleasant facts or to distribute fake facts, like in the above described astroturf attack. An example for such a scheme is SynchroTrap, presented by Cao et al. in [7]. Again, comparable to anomaly based intrusion detection systems, SynchroTrap makes use of clustering algorithms. These algorithms try to group values, that are similar in some aspects into distinct sets.

The system monitors all user activity on a social media platform over an extended time period and monitors aggregated user actions. Then, the pairwise similarity between actions is determined and a hierarchical clustering algorithm is used to group users that show similar behavior at approximately the same time. If a cluster is growing too big, it can be assumed as malicious, since legitimate users tend to behave diverse [7].

An issue with this detection method is though, that it is for example not able to detect bot accounts that show a mixture of bot and human behavior. Thus, the detection systems have to be developed further in order to keep up with the fast evolving social bots and their evermore sophisticated behavior [12].

1.6 Summary and Outlook

In the last chapter, we firstly introduced the term social bot, defined it and looked at the history of robots in social media. Afterwards we gave a really short overview about Twitter, Facebook and Renren and motivated why social bot detection is important after all. In the main part of this chapter we discussed social bot detection approaches. We distinguished hereby social network information based, crowd-sourcing based and feature based approaches.

Social network based approaches model the analyzed OSN into a graph where users correspond to the vertices and relationships between the users correspond to the edges of the graph. Afterwards, an algorithm tries to make a decision whether a given node is a social bot or an actual user. The decision is hereby usually based on the connections the node and his sur-

roundings have. As examples for this kind of detection approach, we mentioned SybilGuard[25], SbilyInfer[9], SumUp[18] and the Facebook Immune System[16]. A problem these systems have to cope with is, that they tend to assume, that bots can't establish relationships to actual, what emerged to be not true.

Next we elaborated on crow-sourcing based approaches. The basic underlying idea of these approaches is to engage actual humans to analyze given user profiles and to decide whether those belong to an actual user or a social bot. We discussed the paper "Social turing tests: Crowdsourcing sybil detection" by Wang et al. [22] which analyzes this approach thoroughly and introduces a general practical system. One of the issues this approach has to handle is that some social networks users don't have very detailed profiles what makes crowd-sourced bot detection very hard.

At last, we discussed feature based social bot detection approaches. They observe characteristics of OSN users and information published by them in order to decide – or give a tendency – whether a given account is a bot, or not. Often, they make use of machine learning algorithms. This means that, in a first step, they are trained with datasets in which it is known whether a profile is bot- or human-owned. Afterwards they are used to make decisions about real data. As an example we introduced the Bot or Not? system by Davis et al. [10].

After analyzing the different detection approaches, it becomes apparent that a combination of different approaches yield good results. Observing the social graph and behavioral features of accounts together is for example a promising strategy. Ferrara et al. bring in the Renren sybil detector [21, 24] as a good example for these combined approaches [12].

However, it has to be noted that not all robots in social media have to be necessarily evil. Some social bots provide useful services that many users don't want to miss. It is just important, that users are able to distinguish between other humans and bots for example in order to differentiate whether content they see is actually as popular as it seems.

It is safe to assume that the number of social bots will increase even more and that their methods and behaviors will get even more sophisticated. We expect an arms race between bot herders and bot detection mechanisms, like it was – and still is – the case with malware and malware detection software.

Chapter 2

Equations, Figures, and Tables

The content of Chapter 2 will vary with the topic of your thesis. This chapter only gives guidance to some technical aspects of LaTeX.

Remark: If you want a shorter chapter or section title to appear in the Table of Contents and in the headings of the chapter, you just include the short title in square brackets before the title of the chapter/section. Example:

```
\section[Short Title]{Long Title}
```

.

2.1 Simple Equations

Mathematical symbols and equations can written in the text as λ, $F(t)$, or even $F(t) = \int_0^t \exp(-\lambda x)\,dx$, or as displayed equations

$$F(t) = \int_0^t \exp(-\lambda x)\,dx \tag{2.1}$$

The displayed equations are automatically given equation numbers – here (2.1) since this is the first equation in Chapter 2. Note that you can refer to the equation by referring to the "label" you specified as part of the equation environment.

You can also include equations without numbers:

$$F(t) = \sum_{i=1}^{n} \binom{n}{i} \sin(i \cdot t)$$

More Advanced Formulas

Long formulas that cannot fit into a single line can be written by using the environment `align` as

$$F(t) = \sum_{i=1}^{n} \sin(t^{n-1}) - \sum_{i=1}^{n} \binom{n}{i} \sin(i \cdot t) \tag{2.2}$$

$$+ \int_0^{\infty} n^{-x} e^{-\lambda x^t} \, dt \tag{2.3}$$

In some cases, you need to write ordinary letters inside the equations. You should then use the commands

```
\textrm  and/or \mathrm
```

The first command returns the normal text font and will be scaled automatically, while the second command will be scaled according to the use.

$$\mathrm{MTTF} = \int_0^{\infty} R_{\mathrm{avg}}(t) \, dt$$

Please consult the LaTeX documentation for further details about mathematics in LaTeX.

Definitions

If you want to include a definition of a term/concept in the text, I have made the following macro (see in `ramsstyle.sty`):

☞ **Reliability**: The ability of an item to perform a required function under stated environmental and operational conditions and for a stated period of time.

Figure 2.1: This is the logo of NTNU (rotated 15 degrees).

When text is following directly after the definition, it may sometimes be necessary to end the definition text by the command

`\newline`

I have not included this in the definition of the `defin` environment to avoid too much space when there is not a text-block following the definition.

2.2 Including Figures

If you use pdfLaTeX (as recommended), all the figures must be in pdf, png, or jpg format. We recommend you to use the pdf format. Please place the figure files in the directory **fig**. Figures are included by the command shown for Figure 2.1. Please notice the "path" to the figure file written by a *forward* slash (/). You should not include the format of the figure file (pdg, png, or jpg) – just write the "name" of the figure.

Each figure should include a unique *label* as shown in the command for Figure 2.1. You can then refer to the figure by the *ref* command. Notice that you can scale the size of the figure by the option `scale=k`. You may also define a specific width or height of the figure by replacing the `scale` options by `width=k` or `height=k`. The factor `k` can here be specified in mm, cm, pc, and many other length measures. You may also give `k` as a fraction of the width of the text or of the height of the text, for example, `width=0.45\textwidth`. If you later change the margins of the text, the figure width will change accordingly. As illustrated in Figure 2.1, you may also rotate the figure – and also do many other things (please check the documentation of the package `graphicx` – it is available on your computer, or you may find it on the Internet).

In LaTeX all figures are floating objects and will normally be placed at the top of a page. This is the standard option in all scientific reports. If you insist on placing the figure exactly where you

Table 2.1: The degree of newness of technology.

Experience with the operating condition	Level of technology maturity		
	Proven	Limited field history or not used by company/user	New or unproven
Previous experience	1	2	3
No experience by company/user	2	3	4
No industry experience	3	4	4

declare the figure, you may include the command `[h]` (here) immediately after `\begin{figure}`. If you will force the figure to be located either at the top or bottom of the page, you may alternatively use `[t]` or `[b]`. For more options, check the documentation.

Large figures may be included as a *sidewaysfigure* as shown in Figure 2.2:[1]

2.3 Including Tables

LaTeX has a lot of different options to include tables. Only one of them is illustrated here.

Remark: Notice that figure captions (Figure text) shall be located *below* the figure – and that the caption of tables shall be *above* the table. This is done by placing the `\caption` command beneath the command `\includegraphics` for figures, and above the command `\begin{tabular*}` for tables.

2.4 Copying Figures and Tables

In some cases, it may be relevant to include figures and tables from from other publications in your report. This can be a direct copy or that you retype the table or redraw the figure. In both cases, you should include a reference to the source in the figure or table caption. The caption might then be written as: *Figure/Table xx: The caption text is coming here [**?**].*

In other cases, you get the idea from a figure or table in a publication, but modify the figure/table to fit your purpose. If the change is significant, your caption should have the following format: *Figure/Table xx: The caption text is coming here [adapted from **?**].*

[1] You can use a similar command for large tables.

Figure 2.2: This is the logo of NTNU.

2.5 References to Figures and Tables

Remember that all figures and tables shall be referred to and explained/discussed in the text. If a figure/table is not referred to in the text, it shall be deleted from the report.

2.6 A Word About Font-encoding

When you press a button (or a combination of buttons) on your keyboard, this is represented in your computer according to the *font-encoding* that has been set up. A wide range of font-encodings are available and it may be difficult to choose the "best" one. In the template, I have set up a font-encoding called UTF-8 which is a modern and very comprehensive encoding and is expected to be the standard encoding in the future. Before you start using this template, you should open the Preferences ->Editor dialogue in TeXworks (or TeXShop if you use a Mac) and check that encoding UTF-8 has been specified.

If you use only numbers and letters used in standard English text, it is not very important which encoding you are using, but if you write the Norwegian letters æ, ø, å and accented letters, such as é and ä, you may run into problems if you use different encodings. Please be careful if you cut and paste text from other word-processors or editors into your LaTeX file!

Warning

If you (accidentally) open your file in another editor and this editor is set up with another font-encoding, your non-standard letters will likely come out wrong. If you do this, and detect the error, be sure *not* to save your file in this editor!!

This is not a specific LaTeX problem. You will run into the same problem with all editors and word-processors – and it is of special importance if you use computers with different platforms (Windows, OSX, Linux).

2.7 Plagiarism

Plagiarism is defined as "use, without giving reasonable and appropriate credit to or acknowledging the author or source, of another person's original work, whether such work is made up of

code, formulas, ideas, language, research, strategies, writing or other form", and is a very serious issue in all academic work. You should adhere to the following rules:

- Give proper references to all the sources you are using as a basis for your work. The references should be give to the original work and not to newer sources that mention the original sources.
- You may copy paragraphs up to 50 words when you include a proper reference. In doing so, you should place the copied text in inverted commas (i.e., "Copied text follows ..."). Another option is to write the copied text as a quotation, for example:

  > Birnbaum's measure of reliability importance of component i at time t is equal to the probability that the system is in such a state at time t that component i is critical for the system.
  >
  > **?**]

Chapter 3

Summary and Recommendations for Further Work

In this final chapter you should sum up what you have done and which results you have got. You should also discuss your findings, and give recommendations for further work.

3.1 Summary and Conclusions

Here, you present a brief summary of your work and list the main results you have got. You should give comments to each of the objectives in Chapter 1 and state whether or not you have met the objective. If you have not met the objective, you should explain why (e.g., data not available, too difficult).

This section is similar to the Summary and Conclusions in the beginning of your report, but more detailed—referring to the the various sections in the report.

3.2 Discussion

Here, you may discuss your findings, their strengths and limitations.

3.3 Recommendations for Further Work

You should give recommendations to possible extensions to your work. The recommendations should be as specific as possible, preferably with an objective and an indication of a possible approach.

The recommendations may be classified as:

- Short-term
- Medium-term
- Long-term

Appendix A

Acronyms

FTA Fault tree analysis

MTTF Mean time to failure

RAMS Reliability, availability, maintainability, and safety

Appendix B

Additional Information

This is an example of an Appendix. You can write an Appendix in the same way as a chapter, with sections, subsections, and so on.

B.1 Introduction

B.1.1 More Details

Bibliography

[1] United states securities and exchange commission - form 10-q - twitter, inc.

[2] Global social media research summary 2016, 2016.

[3] N. Abokhodair, D. Yoo, and D. W. McDonald. Dissecting a social botnet: Growth, content and influence in twitter. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pages 839–851. ACM, 2015.

[4] J. Bollen, H. Mao, and X. Zeng. Twitter mood predicts the stock market. *Journal of Computational Science*, 2(1):1–8, 2011.

[5] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. The socialbot network: when bots socialize for fame and money. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 93–102. ACM, 2011.

[6] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. Design and analysis of a social botnet. *Computer Networks*, 57(2):556–578, 2013.

[7] Q. Cao, X. Yang, J. Yu, and C. Palow. Uncovering large groups of active malicious accounts in online social networks. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 477–488. ACM, 2014.

[8] C. A. Cassa, R. Chunara, K. Mandl, and J. S. Brownstein. Twitter as a sentinel in emergency situations: lessons from the boston marathon explosions. *PLOS Currents Disasters*, 2013.

[9] G. Danezis and P. Mittal. Sybilinfer: Detecting sybil nodes using social networks. In *NDSS*. San Diego, CA, 2009.

[10] C. A. Davis, O. Varol, E. Ferrara, A. Flammini, and F. Menczer. Botornot: A system to evaluate social bots. In *Proceedings of the 25th International Conference Companion on World Wide Web*, pages 273–274. International World Wide Web Conferences Steering Committee, 2016.

[11] J. R. Douceur. The sybil attack. In *International Workshop on Peer-to-Peer Systems*, pages 251–260. Springer, 2002.

[12] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini. The rise of social bots. *arXiv preprint arXiv:1407.5225v3*, 2015.

[13] A. Gupta, H. Lamba, and P. Kumaraguru. $1.00 per rt # bostonmarathon # prayforboston: Analyzing fake content on twitter. In *eCrime Researchers Summit (eCRS), 2013*, pages 1–12. IEEE, 2013.

[14] T. Hwang, I. Pearce, and M. Nanis. Socialbots: Voices from the fronts. *interactions*, 19(2):38–45, 2012.

[15] E. Mustafaraj and P. T. Metaxas. From obscurity to prominence in minutes: Political speech and real-time search. 2010.

[16] T. Stein, E. Chen, and K. Mangla. Facebook immune system. In *Proceedings of the 4th Workshop on Social Network Systems*, page 8. ACM, 2011.

[17] G. Stringhini, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Y. Zhao. Follow the green: Growth and dynamics in twitter follower markets. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 163–176, New York, NY, USA, 2013. ACM.

[18] D. N. Tran, B. Min, J. Li, and L. Subramanian. Sybil-resilient online content voting. In *NSDI*, volume 9, pages 15–28, 2009.

[19] A. M. Turing. Computing machinery and intelligence. *Mind*, 59(236):433–460, 1950.

[20] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove. An analysis of social network-based sybil defenses. *ACM SIGCOMM Computer Communication Review*, 40(4):363–374, 2010.

[21] G. Wang, T. Konolige, C. Wilson, X. Wang, H. Zheng, and B. Y. Zhao. You are how you click: Clickstream analysis for sybil detection. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, pages 241–256, 2013.

[22] G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, and B. Y. Zhao. Social turing tests: Crowdsourcing sybil detection. *arXiv preprint arXiv:1205.3856*, 2012.

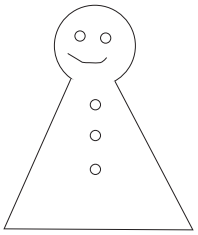
[23] J. Weizenbaum. Eliza—a computer program for the study of natural language communication between man and machine. *Communications of the ACM*, 9(1):36–45, 1966.

[24] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai. Uncovering social network sybils in the wild. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 8(1):2, 2014.

[25] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman. Sybilguard: defending against sybil attacks via social networks. In *ACM SIGCOMM Computer Communication Review*, volume 36, pages 267–278. ACM, 2006.

Curriculum Vitae

Name:	**Your Name**
Gender:	Female
Date of birth:	1. January 1995
Address:	Nordre gate 1, N–7005 Trondheim
Home address:	King's road 1, 4590 Vladivostok, Senegal
Nationality:	English
Email (1):	your.name@stud.ntnu.no
Email (2):	yourname@gmail.com
Telephone:	+47 12345678



Your picture

Language Skills

Describe which languages you speak and/or write. Specify your skills in each language.

Education

- School 1
- School 2
- School 3

Computer Skills

- Program 1

- Program 2
- Program 3

Experience

- Job 1
- Job 2
- Job 3

Hobbies and Other Activities