UNDERSTANDING CONTAGION SPREADING PROCESSES OF CYBER SECURITY THREATS THROUGH SOCIAL NETWORKS

TERRY BRETT

A thesis submitted in fulfilment of the requirements of the University of Greenwich for the degree of Doctor of Philosophy

This research programme was carried out in collaboration with the University of Zaragoza

March, 2021

Declaration

"*I certify that the work contained in this thesis, or any part of it, has not been accepted in substance for any previous degree awarded to me, and is not concurrently being submitted for any degree other than that of Doctor of Philosophy being studied at the University of Greenwich. I also declare that this work is the result of my own investigations, except where otherwise identified by references and that the contents are not the outcome of any form of research misconduct*"

Student Name: Terry Brett

Student Signature:
Date: 17/02/2021

First Supervisor's Name: Nicola Perra

First Supervisor's Signature:
Date: 17/02/2021

Second Supervisor's Name: George Loukas

Second Supervisor's Signature:
Date: 17/02/2021

Third Supervisor's Name: Yamir Moreno

Third Supervisor's Signature:
Date: 17/02/2021

Acknowledgements

Throughout the writing of this dissertation I have received a great deal of support and assistance. I would like to recognize all that help and endorse many people who have been part of this research.

I would firstly like to thank my supervisory team, Dr. Nicola Perra, Dr. George Loukas and Prof. Yamir Moreno for their expertise, feedback, advice, resources and all their contributions put into this project.

Also I would like to extend this to Carlos Gracia and Felipe Cardoso from the University of Zaragoza, for helping with translations, recruitment of the participants and running the experiments.

Special thanks to Nicolò Gozzi for his time and resources provided during the data analysis stage in order to speed up the process.

My sincere thanks go to all participants that took part in the study and enabled this research to be possible.

My deepest thanks and appreciation go to my extraordinary friend Emilie. You are always there for me, your support and encouragement was worth more than I can express on paper. Your motivation made all the difference in the world, and I'll always be grateful. Could not have done it without you.

Finally, there are my friends, Oliver, Josh and Xu, who were of great support in deliberating over my research problems and findings, as well as providing happy distraction to rest my mind outside of my research.

UNIVERSITY OF GREENWICH

Abstract

Faculty of Business
Business School

Doctor of Philosophy

Understanding contagion spreading processes of cyber security threats through social networks

by Terry BRETT

The spreading of ideas, memes, norms, products, and diseases are few examples of phenomena that can be studied and modelled as contagion processes on networks. Over the last decade, the unprecedented access to high resolution data about on/offline human interactions has shifted such studies from theoretical scholarly exercises to data-driven realistic models now used in a range of applications in different industries and domains.

Surprisingly, the dynamics of contagion in terms of semantic social engineering threats, such as phishing, scams, drive-by-malware etc. have received so far little attention. Indeed, although their spreading is conducted primarily in online social networks, studies in cyber security have been focused mainly on defining the characteristics of threats and users that are more likely to result in successful attacks. In other words, the complexity emerging from the unsupervised interactions and actions of a large number of users as well as threats strategies have been largely neglected.

The project has tackled this limitation head-on. By leveraging expertise on modelling contagion processes in networks, cyber security, and data science we first introduced a theoretical modeling framework that captures temporal nature of social interactions and the heterogeneity of users' susceptibility. We study two realistic types of viruses propagating on temporal networks featuring different categories of susceptibility and derive analytically the invasion threshold. We then developed and deployed an experimental online platform to observe, empirically, the spreading of simulated cyber threats in a population of connected users. The platform allows users to interact passing and receiving content (potentially compromised) to/from others. By considering different threats, network configurations and different levels of information provided to users about their contacts, the dynamics of threats diffusion has been observed in 8 experiments involving 109 participants. The aim is to isolate the social mechanisms responsible for the spreading of cyber threats in online networks and devise new efficient ways for cyber protection at societal level.

Contents

List of Figures

List of Tables

List of Abbreviations

OSN	**O**nline **S**ocial **N**etwork
UI	**U**ser **I**nterface
UML	**U**nified **M**odelling **L**anguage
ERD	**E**ntity **R**elationship **D**iagram
XML	E**X**tensible **M**arkup **L**anguage
BA	**B**arabási-**A**lbert
WS	**W**atts-**S**trogatz
ER	**E**rdős-**R**ényi
NUTMEG	**N**etwork eval**U**a**T**ion **M**ultiplay**E**r **G**ame

List of Symbols

G	graph
S	susceptible population
I	infected population
k	degree of a node
$P(k)$	degree distribution
$\langle k \rangle$	average degree
$\langle a \rangle$	average activity of a node
μ	recovery rate
β, λ	infection rate
m	number of edges connected to a node
R_0	basic reproductive number
τ	timesteps

Chapter 1

Introduction

Online Social Networks (OSNs) have gradually turned into prime means for the spreading of computer viruses, leading to being one of the most targeted computer-mediated technologies. Unlike hardware or software vulnerabilities, which are harder to breach, cyber threats present on social media tend to target their weakest point, the user [Heartfield and Loukas, 2018; Heartfield, Loukas, and Gan, 2016; Heartfield and Loukas, 2016c].

Indeed an average user creates their online presence on multiple platforms with around 23 accounts on different sites [Davis, 2018; Benevenuto et al., 2009]. The significant proportion of these accounts is found on social media sites, which also carry a large number of overall internet traffic [SimilarWeb, 2020]. Given their significance, social media users have became a major target for many cyber attacks [Bilge et al., 2009; Chandramouli, 2011]. Hence the large number of users and ease of sharing information on Online Social Networks (OSNs), means that the attackers can find their victims easily.

Over 22% of social media users have fallen a target of a cyber attack [Wilbanks, 2020], with 55% of them being successful globally [Proofpoint, 2020]. It is estimated that due to user related security breaches, the cost of cyber-crimes in 2018 was $600 billion [McAfee, 2018]. These high numbers have driven cyber security experts to study the impact of cyber threats on platforms and their users. Cyber criminals use number of different techniques to obtain their goal, which usually involves obtaining personal information or access to users credentials. Brute-force, code injection, and social engineering attacks are amongst the most popular cyber threats [Krombholz et al., 2015; Enterprise, 2019].

Brute-force attack is a trial and error process, of different variation of passphrases, which an attacker submits to the target software, in order to attempt to guess the u ser's password. Often this kind of attack will make a use of either a dictionary of common words, or attempt a exhaustive approach, in which the attackers software will attempt to iterate through every single possibility, creating the following pattern: "a", "aa", "ab", "ac" and so on, then gradually add more and more characters (numbers and special characters) in order to find the password [Owens and J. Matthews, 2008]. Brute-force attacks however have become obsolete over the years, as introduction of security measures such as CAPTCHA tests or 2-factor authentications have made it a lot harder to automatically submit large number of trial and error phrases to a website.

The code injection techniques are based on flaws in written software, in which

an attacker will submit an untrusted input into the program, such that the program will interpret it as a command to execute, usually resulting in revealing the database entries. This happens if a badly written software encounters special characters, such as quotations, ampersand, front and back slashes, which in computer software will be treated different to a usual text, and will indicate to perform an action depending on the software [Halfond, Viegas, Orso, et al., 2006]. To mitigate code injections, a software engineering feature called a *prepared statement* has been introduced. This feature allows to treat any input as plain text, instead of interpreting special characters that might be included in it. The success of the attack is therefore dependant on the design of the system, and whether or not it uses prepared statements, or if the software treats any input as a commands.

In the dissertation we focus on the last of the mentioned attacks, social engineering, which is the most popular method of targeting the vulnerable users, with with 98% of cyber attacks relying on it [PurpleSec, 2019], and they account for 30% of global security breaches [Enterprise, 2019]. Social engineering is an attack method that relies heavily on interactions with humans instead of computers [Wiley, 2008]. A popular example of this type of cyber threats, is phishing, which usually occurs when a malicious email is sent to a victim disguised as something legitimate [S. Gupta, Singhal, and Kapoor, 2016; Heartfield and Loukas, 2018; Huber et al., 2009; Mouton, Leenen, and Venter, 2016].

Studies show that users often fall for these type of attacks, unable to identify that they are malicious, and a successful cyber attack can lead to business loosing money, government not being able to provide essential services, sensitive data being stolen, causing equipment damage [Knapp and Langill, 2014] among many other consequences.

A recent report by Verizon indicates that phishing accounts for 90% of data breaches [Enterprise, 2019], this has resulted in companies and private users loosing millions of pounds of financial income and compromising their personal identity and reputation they have. Attackers will often use the compromised accounts to further propagate the malicious content to friends of a users, in order to take full advantage of trust and reputation the victim had.

1.1.1 Cyber Threats in Online Social Networks

OSNs are exposed to a variety of cyber attacks, which will often adapt to the type of the service being used [Bendovschi, 2015]. The malicious actors will use number of features and functionalities available on the given platform, to increase the chances of success of the breach. The information available on most social networks (name, date of birth, workplace etc.) is exploited as a part of a social media attack, to increase the chances of its success. Using this information, more customised attacks can be created. They will appear as services the target is familiar with, and pray on the reputation of that service and the gullibility of the user. With that information, social engineering attacks such as phishing, fake profiles or malicious content, or some combination of all are widely used by malicious agents to gain access to others profile.

Defense mechanisms against these threats of course exist, tools such as phishing detection [B. B. Gupta et al., 2017] aim to automate the discovery of some

of these attacks. Antiviral software always scans for malicious links and content users might be exposed to online. These tools however often rely on frequent updates and libraries to detect this content [Sukwong, Hyong Kim, and James Hoe, 2010].

Studies show that users' characteristics have an impact on the susceptibility of the cyber threat [Heartfield and Loukas, 2016c]. In a business setting, to improve the awareness and address some of these characteristics such as attitude, trust, conscientiousness, familiarity with the system, frequency of usage, users will go through a training process in order to improve their cyber security awareness, or company will introduce policies, which restrict the access to some links or files that might be shared via email.

1.1.2 Network Thinking

Networks can be conveniently used to describe systems in which nodes (computers, people, etc..) interact and exchange information via edges (wires, social interactions) [Albert-László Barabási, 2013].

Networks hold different topological properties, which will affect how they work and how information is carried across them [Ganesh, Massoulié, and Towsley, 2005; Alain Barrat, Marc Barthelemy, and Alessandro Vespignani, 2008; Mark Newman, 2018]. These include heterogeneity in different statistical indicators such as number of connections of nodes and intensity of interactions, organization of connections in communities (groups), small word phenomena, and complex temporal dynamics [Petter Holme, 2015; Petter Holme and Saramäki, 2012; Nicola Perra, Gonçalves, et al., 2012; S. Liu et al., 2014]. These properties yield non-trivial effects on spreading processes, such as diseases and information, unfolding on their structures. In particular, heterogeneity in the number of connections (i.e. the presence of hubs) facilitate the spreading process and make systems fragile to target attacks that try to influence their functionality". The presence of communities (groups) might slow down the spreading of some dynamical processes while accelerating others [Nadini et al., 2018]. Complex temporal dynamics such as the sequence, order, co-currency, burstiness, and different types of correlations give raise to a rich and case dependent phenomenology [K. Sun, Andrea Baronchelli, and Nicola Perra, 2015].

It is important to stress how, since computer virus is akin to its biological counterpart (to which a large fraction of the literature is devoted) [Jagdev Singh et al., 2018; L.-X. Yang and X. Yang, 2014a; S. Xu et al., 2014; Kephart and S. R. White, 1992], we can apply these studies to the field of cyber security.

In fact computers are part of a network, whether it's a local network at home or a global network like the internet. Computer viruses and cyber threats in general spread over computer networks, often via virtual social interactions [Soumya and Revathy, 2018]. As computer viruses are created for a range of purposes [Levin, 1990], they will have different impact on the system they infect. They could either aim to infect a network and stay there e.g. a keylogger, which can be used to record all the keys struck and send the information to the attacker, or they could spread to other computers before being removed by an antivirus e.g. trojan.

Clearly the study of networks helps to understand and map how cyber threats spread [Guo, Cheng, and Kelley, 2016; Lan Liu et al., 2017; Ikhalia, 2017]. This can support the creation of network topologies which are robust and versatile, reduce the damage caused by attacks and safely manage the network to minimise the spread, as well as recover operations if a cyber attack occurs. To understand how network effects modulate the spreading of cyber threats on online social networks, we built a platform designed for the study of propagation of phenomena on different types on networks.

1.1.3 Related work

The extant research on the subject focuses on three main categories. First, the development of automated tools for preventing cyber threats such as phishing and similar content. Second the understanding of users' characteristics and their susceptibility to attacks. Third the affect of network properties on the propagation of malicious content.

Assessing user cyber security awareness as a weakness has lead to the development of various automated detection and prevention tools. Phishing detection, spam filtering, antivirus software, and popup blockers are just a few available resources to tackle the issue. These work to some degree of success, by using different approaches, such as black listing, database of viruses or machine learning [B. B. Gupta et al., 2017; Sukwong, Hyong Kim, and James Hoe, 2010; Cormack, 2008; Miyamoto, Hazeyama, and Kadobayashi, 2008]. While these are useful and can help to prevent an ample of compromised content, they might fail at detecting similar threats spreading in different context or on different platform [Heartfield and Loukas, 2018]. Once the threat incorporates a legitimate and intended behaviour into its functionality, the likelihood of detection drops [Heartfield and Loukas, 2018].

User awareness however can be trained, and the second area of research focuses on understanding how idiosyncrasies impact the vulnerability to cyber attacks. The behaviours which has been found across the population of users, mainly includes openness, trust, gullibility, computer literacy and compliance [Workman, 2008; Alseadoon, 2014; Mohebzada et al., 2012; Halevi, Memon, and Nov, 2015; Halevi, Lewis, and Memon, 2013]. Computer related security training as well as frequency of use has been shown to improve the robustness of computer system, by users being able to detect the threat themselves and cease to open it [Sheng et al., 2007; Heartfield and Loukas, 2016c; D. C. Rowe, Lunt, and Ekstrom, 2011]. The limitation of this however arises, as the classic setup of this methodology considers users in isolation, neglecting the fact that users are connected with others. This constitutes one of the key research gaps the dissertation aims to tackle.

As users are a part of a connected social network, they are subject and give rise to structural properties of the graph, which impact the spreading of cyber threats. Network properties such as the complex temporal dynamics, degree and weights distributions have on one hand found that heterogeneity makes the system resilient to random attacks [A. L. Lloyd and R. M. May, 2001b; Justin Balthrop et al., 2004; Romualdo Pastor-Satorras and Alessandro Vespignani, 2001], but on the

other hand it makes the system vulnerable to targeted attacks, as targeting central nodes by either infection or complete removal of these nodes leads to changes in the spread of the virus, increasing their impact [Justin Balthrop et al., 2004; C.-Y. Huang et al., 2013]. However, the large majority of studies ignore the fact that users have different levels of susceptibility to cyber threats and that networks are not static, but change over time. These limitations constitute other two research gaps that the dissertation aims to tackle.

1.1.4 Hypotheses

As mentioned above, the studies in the cyber security community have been focused on measuring the susceptibility and risk perception of the users [Adali et al., 2010; Heartfield and Loukas, 2018; Heartfield and Loukas, 2016b], but neglect the fact that they are part of a network. In fact, the classic approach considers users in isolation and focuses on their abilities to identify cues of a threat. On the other hand, the literature from the network science community focuses on understanding how the topological features of networks affect the spreading of cyber-threats [Petter Holme, 2015; Petter Holme and Saramäki, 2012; Carrington, Scott, and Stanley Wasserman, 2005; K. S. Cook et al., 2013; S. Dong, Deng, and Y.-C. Huang, 2017; Barrat and Cattuto, 2015; S. Liu et al., 2014; M. J. Williams and Musolesi, 2016]. However, it largely neglects that users' susceptibility is heterogeneous and that their interactions are not static but subject to complex temporal dynamics [Sloot, Kampis, and Gulyás, 2013; Petter Holme and Fredrik Liljeros, 2014; Takaguchi, Sato, et al., 2012; K. Sun, Andrea Baronchelli, and Nicola Perra, 2015; Scholtes et al., 2014; Starnini, Machens, et al., 2013].

Bridging the gap between cyber security and network science, we combine the two approaches to characterize how users' susceptibility to social engineering attacks is affected by network effects, and how this drives the spreading of cyber threats in OSNs.

We have defined the following hypotheses to test

- H_0 - Networks effects, emerging from the temporal interactions of users and their features and trust, do impact the spread of malicious content on OSNs
- H_1 - The limited user trust in a new social group, evolves over time, as people create connections between each other, and remove them if they have been compromised
- H_2 - Awareness of virus presence increases user suspicion towards social media content and potential indicators of a malicious attack, heavily throttling the spread of a virus

1.2 Aims & Research Questions

The combination of cyber security and network science is essential to capture the interplay between the nature of human interactions and its link to the spread of computer viruses.

Very broadly defined, the aim of the research can be summarised as the following question:

- What are the network effects, emerging from the unsupervised interaction of many individuals, affecting the spreading of cyber threats on OSNs?

Building trust in their new network the users will gain an idea who are the neighbours, who have been the most "trustworthy". Given that trust results in likely communication behaviors which are statistically different from random communications [Adali et al., 2010], we can investigate how the exchange of information between users has changed. We ask the question to test H_1:

- Can we characterize empirically the spreading of cyber threats on online social networks and what are the effects of trust, socio-demographic, and gullibility?

Social media users tend to share information in strongly tied and temporal networks [Friedkin, 1982; Y. Kim and Choi, 2018], as the users already have a prior knowledge of who their neighbours are. This information, whether formal or informal, has been mentally verified by the user to be safe, since there is a history of past information exchange and trust between the known individuals.

However without any knowledge about their friends, users are more likely to be more cautious and prejudice. New information from unknown source could contain misleading information or fake/malicious content. Testing H_2, we form the following question:

- Can we model the spreading of such phenomena accounting for heterogeneous susceptibility of users and their temporal interaction dynamics?

1.3 Research Methods

In order to validate the research questions and attest our hypotheses, we first created a novel theoretical time-varying network model to characterize the spreading of different types of cyber threats on temporal networks considering the presence of different gullibility classes. We then develop the platform to observe empirically such phenomena. Our platform has the basic functionality of a prototypical online social network thus allowing users to send/receive, view the timeline and content. To empirically characterize users interactions we have implemented a tracking engine, which allows us to monitor and collect user actions.

We have preset three different experimental scenarios, each of which exposes users to different levels of information about their network, such as whom they are interacting with, and information about the infection. We set a baseline scenario, in which the user has no knowledge about the infection, they do not know if they get infected at all, nor they know whom they are receiving the messages from, as they interact with others.

Having control over parameters, we are able to engineer connections between users considering different topologies (Barabasi-Albert, Watts-Strogatz, Erdős–Rényi, Complete Graph), controlling parameters, which will affect the node connectivity,

and we can change what information the users have about the infection dynamically.

Considering a standard scenario in a Online Social Network, if an individual is a target of a successful cyber attack, their computer becomes compromised, which puts his/her data and contacts at risk. Following the same principle, the infection that exists on our platform is a representation of a compromised machine.

Each user on our network has a binary flag of infected or susceptible. In the beginning all users are susceptible, with a small number of initially infected seeds. If an infected user sends a message to his/her friend, and they open it, they too become infected. The status of the compromised node will change to infected, and its messages will carry the same flag.

With the scenarios that we have, we gradually introduce more information about the infection. In first scenario user has no information about the infection, in second scenario they know whom they've got infected by after opening a message, and in the third scenario they have the ability to remove an infection by the use of antivirus and block a friend if they choose to.

With these different levels and different network configurations, we aim to isolate the social factor responsible for the spread of malicious content, and understand the impact of the network effect on the spread.

The behaviour that we track from the user is what they decide to do with a message they receive, that is they are only able to open, reply and delete a message. We link the interactions and choices to trust and gullibility, as trust affects social interactions, which in turn affect users actions and thus the propagation of cyber threats [Brett et al., 2019]. Given the credibility of a source and perception users have towards it, this will impact the spread phenomena [C. Shao et al., 2018].

Using machine learning we aim to predict the possibility of infection, given the past actions taken leading up to the contagion. We also introduce metrics of trust and gullibility, based on the survey incorporated into our platform, and the tracked actions, we link these metrics to the probability of user getting infected.

We carried out 8 experiments with 109 participants in total between the UK and Spain, and analyse the data gathered from the experiments.

1.4 Research Outline

The thesis composes of the following seven chapters.

Chapter 1: **Introduction**. This chapter gives an introduction to the thesis, providing the background, hypotheses and research questions.

Chapter 2: **Literature Review**. Here we show research that has already been conducted in various areas, which is either of interest of similarity to our project. We show how cyber threats and networks are being studied, and talk about tools available to help with their studies, highlighting the gap in the research for a tool and study that we have developed for the purpose of this project. The amount of publications in the two areas is vast, thus the review is concentrated on the

research contributions which are related. The main limitations of the existing research however are that the research in cyber security focuses on studies in which the participants are in isolation, the cyber threats they are introduced to don't come from a friend or a malicious actor, as they do in a real social network, but from a preset protocol. Network scientists on the other hand study the topologies of networks and the propagation of the virus, neglecting the fact the users susceptibility to cyber threats is not homogeneous, and can change over time.

Chapter 3: **The spreading of computer viruses on time-varying networks**. In this chapter we present our theoretical model. The model show that our hypotheses work in theory, and it shapes the development path for the platform and the experiments.

Chapter 4: **Experimental Platform**. This chapter focuses on the experimental platform, which was the tool we have used to collect our data. The platform has been built from scratch for the purpose of this research, and we show the software development methodology and the process of developing our own social network.

Chapter 5: **Experiments**. Experiments performed and their design are described here.

Chapter 6: **Towards an empirical characterisation of threats on social networks**. We discuss the empirical results of the experiments, talk about the type of analysis done, what we have found from it, test our hypotheses and answer our researcher questions.

Chapter 7: **Conclusion**. This chapter concludes the thesis by outlining the main contributions of the research and discusses how the work could evolve in the future.

1.4.1 Publications

- Terry Brett, George Loukas, Yamir Moreno, and Nicola Perra, Spreading of computer viruses on time-varying networks, Phys. Rev. E 99, 050303(R)
- Terry Brett, George Loukas, Yamir Moreno, and Nicola Perra, SoftwareX, NUTMEG: Network Evaluation Multiplayer Game for studying contagion processes on networks - Under revision/submitted

Chapter 2

Literature Review

The literature review covers the work done in the areas of cyber security and network science to characterise, model and predict the spread of cyber threats via computer networks.

In the first section we cover the introduction to cyber security. In doing so we introduce the idea of cyber security, and mention common ways in which cyber criminals choose to conduct an attack. These include software attacks i.e. programs which users would download from the web, typically by following a malicious link. Such viruses can cause damage to the system, and and be self-replicative, meaning it can infect users close network of computers/friends. The other types of attacks are called deceptive attacks, which partition into cosmetic and behavioural deceptions. These are attacks such as phishing and scamming, which trick users to believe that the website or software they are using is legitimate.

In the second, instead we provide a summary of graph theory, the key results in the study of real networks and of contagion processes unfolding on their structure. In revising the research in this area, we include a number of studies on social networks, on the spread of biological viruses as well as on the spread of ideas, beliefs and emotions (i.e. complex contagion). We summarize the main network models (both static and time-varying) and discuss how the topological/temporal features of such networks affect the propagation of contagion processes.

In the third section, we mention the work that has been done in modelling the spread of cyber threats. The work includes the spread and prevention of the virus, its impact on the network, self-replicative bots, and the spread of behaviour. This is important, since the behaviour has an impact on the decisions users will make online. Users can be influenced by each other, and thus adopt a certain behaviour, which then might be compromised by a cyber criminal.

In the final section, we summarise the research gaps in the extant literature.

2.1 Cyber Security

The word "cyber" is relatively new, and has been introduced for a specific purpose of computing, machines and robotics by Norbert Wiener in his 1948 book [Wiener, 1948]. It relates to the world of computers and everything that is digital around us. Cyberspace has become popular now-days more then ever, and as our

physical security, it too needs to be protected, since we share so much of information via the world wide web. Even since its early days, technology has been target to attempted security breaches, which over the years got more sophisticated with creations of different kind of cyber threats, among which we can highlight computer viruses.

Computer viruses have been around since as early as 1970's [T. M. Chen and Robert, 2004]. However some earlier work dating back to 1949, has given birth to self-replicating software [Von Neumann, Burks, et al., 1966], which on a very basic level can be compared to modern computer virus, which will copy itself onto all possible hosts. This work was only very early, and at that time, there was no consideration of computers being connected with each other, especially on a global scale as they are today.

Modern technology goes beyond just desktop computing. In recent years the boom of smartphone market has brought a world of whole new possibilities, not only for the users and smartphone developers, but also for data scientists and cyber criminals. With everyone now having access to the internet, and mobile devices being able to keep track of everything from location to fingerprints, the amount of data generated allows for modelling of human behaviour worldwide, but it also makes users more vulnerable to cyber threats, as the exposure to them is ubiquitous [Yu et al., 2005, Yu, 2004].

Over the years, different techniques of cyber attacks have adapted with the ever changing technology [Hemsley and Fisher, 2018]. We therefore have to go beyond the traditional approaches to virus spread, such as USB devices [Zhu, X. Yang, and J. Ren, 2012, Serazzi and Zanero, 2004], which are now slowly becoming obsolete in favour of cloud based systems, which are now increasingly becoming a new target for cyber criminals [Hamad and Al-Hoby, 2012]. Such attacks are highlighted in [Chou, 2013], in which number of different breach attempts are described on cloud systems. The attacks include a Malware Injection Attack, which allows hackers to exploit vulnerabilities in software, in which flaws in design of a language let attackers change the normal execution of code.

Some of the most popular code based injection attacks are SQL injections and XSS (Cross-site scripting) attacks, aimed at targeting web applications most used technologies, that is SQL databases and JavaScript. A more comprehensive attack, which is known as the Wrapping Attack, targets a vulnerability on HTTP header side. When a client requests a service, the service is interacted with using SOAP (Simple Object Access Protocol), which is transmitted in XML (Extended Markup Language). In order to securely pass the message between client and server, the SOAP packet uses a digital signature to encrypt the message. However when the XML packet is being transmitted it can be overridden by a hacker. Extra code can be injected into the packet, and then sent to the server for validation, since the original body of the message sent to the sever is still valid, the request is authorised and the hacker is able to gain access to the cloud account.

2.1.1 Social Engineering

The attacks in the previous sections are not only comprehensive, but also require an extensive knowledge of technology and programming. The advances made in

software engineering, have made it harder to exploit software vulnerabilities, thus more popular type of attacks are not focused on software or hardware weaknesses, but instead they focus on humans as a weak point. Despite using technology on day to day basis, humans still fail to spot unsafe cyberspace environment[D. C. Rowe, Lunt, and Ekstrom, 2011]. This is a big issue since humans are the first layer of protection against cyber threats, as it is indeed a human factor that initiates the virus, by allowing it into the system, and executing it. Social engineering are deceptive attacks, aimed at human users specifically. They imitate a real person or a business, and they aim to manipulate the the user's perception, in order to gain users trust, who in turn, will enter sensitive information, into a form shown by the cyber criminal.

Deceptive attacks

We can identify three types of deceptive attacks: cosmetic, behavioural, hybrid [Heartfield and Loukas, 2016a].

- Cosmetic type of attacks focus on the user interface. For example a file can have a right icon association with user expectation, such as adobe reader for pdf files, yet be a .pdf.exe file, which is an executable.
- Behavioural attacks mimic the behaviour of a system. Following certain standards and conventions users are tricked to believe that what they are using is indeed legitimate, such as seeing an open WiFi connection in the list of available networks.
- Finally hybrid deception combines the two. Not only the application in use looks legitimate, but it also behaves in the same way the original would. This is because some attackers copy the code from the original [Dhamija, Tygar, and Hearst, 2006]. The combination of two therefore creates a convincing attack, which is more likely to be successful.

A new concept has been introduced to tackle this issue head on, in which it is the human that is to detect a potential threat c. The user reports the threats they can detect, as this will yield a stronger indications to a potential cyber threat compared to something detected by software, which may be a mistake, or it might not detect as a threat at all [Sukwong, Kim, and Hoe, 2010]. To evaluate the awareness of an average computer user, a study was carried out [Heartfield and Loukas, 2016c] in which participants were asked to identify potential cyber attacks based on a series of images. These were cosmetic behavioural attacks, shown on some of more popular websites such as Twitter, Facebook, Starbucks and Gmail. With the data collated, the researchers the created a machine learning model, which was assessing users' cyber security awareness [Heartfield and Loukas, 2016b]. The model has proven to have around 60% accuracy, taking into consideration features which included age, gender, computer security training, familiarity with the social networking platform etc.

Despite the fact that users can indeed identify more cues indicating a potential cyber attack, the average user cannot identify all security indicators [Heartfield,

Loukas, and Gan, 2017]. Considering browsing the web as a day-to-day activity; the experience is completely different on a desktop computer and a mobile device. For example the HTTPS security indicator visible in the URL address bar disappears on a mobile device. There is also a lack of additional extensions on mobile devices, which for example might protect privacy such as "HTTPS everywhere" extension, which will block all non encrypted connections.

The variation of information on different devices, means that the security indicators are therefore harder to identify, in addition to which, helpful extensions, which exist on a desktop computer, are not available. Indeed numerous applications exist for portable devices, which aim to increase the security, but they are found to be very unreliable. For example anti-phishing tools, which aimed to protect users from phishing attacks, have been found to have a very poor performance [Benenson, Gassmann, and Landwirth, 2017]. Although many websites were correctly identified as fraudulent, the tools also incorrectly identified legitimate websites as being a fraud.

The unreliable nature of these tools therefore still requires users to be aware to some degree of the content they are viewing through the web, and security indicators are important signs of evidence, that a website is legitimate. Although important, some of the more common security indicators (e.g. SSL lock), are still hard to identify for some users, even on a computer [Stojmenoviæ and Biddle, 2018; Felt et al., 2016; Schecter et al., 2007]. In [Schecter et al., 2007] the researchers gradually removed security indicators, first they removed the HTTPS indicator, then the site-authentication image and finally presented a warning page to them. Even when the warning page was displayed 53% of participants still ignored it and entered their bank login details. [Alsharnouby, Alaca, and Chiasson, 2015] used eye tracking to measure what draws user attention, and has shown that 53% of users although successfully identified an attack, did not pay attention to simple security indicators such as the HTTPS lock. This gullibility, makes social engineering attacks easier [Hinson, 2008], and making the indicators difficult to locate, can increase the success of an attack [Heartfield and Loukas, 2015].

Since cosmetic attacks are hard to spot, whether it's a website that looks very similar to the original, or a shortened URL, the indicators aren't as obvious. Using this knowledge the their advantage, cyber criminals create phishing attacks, which are emails disguised as a legitimate activity [S. Gupta, Singhal, and Kapoor, 2016; Heartfield and Loukas, 2018; Huber et al., 2009; Mouton, Leenen, and Venter, 2016]. Some of the earlier studies in this area, have claimed that users cannot be trained in cyber security awareness [Evers, 2006], due to poor performance of the participants. Some phishing attempts, such as asking users to open a URL can however be improved by visual training [Sheng et al., 2007]. Some users will find that numbers or hyphen in the URL can indicate that it's a phishing attempt, however inexperienced users would also identify some of legitimate websites as scam if they contained those, for example if a subdomain ww2 was used.

The reason phishing is particularly popular via email, is that email allow to obfuscate some information, such as a URL or images[Bouguettaya and Eltoweissy, 2003]. This can allow for propagation of malware, which could also lead to reinfection and self-execution of a virus, once a certain script is ran via the opened link [Bincy, Liji, and Dhanya, 2015, Zou, Gong, and Towsley, 2002]. Usual phishing

attacks will be personalised to a victim, this is a variation of the phishing attack known as spear phishing attack. This kind of attack is usually sent to a group of people and appears to be from a trusted source e.g. Facebook. Even if the message is not personal, the risk of falling for an attack is still high. There is also a significant difference between being targeted via email and via an OSNs direct message, which contains a link asking to be opened [Benenson, Gassmann, and Landwirth, 2017]. In [Benenson, Gassmann, and Landwirth, 2017] the study click rates for email attacks were 20% compared to 42.5% on Facebook. The main reason for opening the message and clicking on the link, was reported to be curiosity (34%), followed by the message fitting the recipients expectations (27%). These kind of attacks still are quite popular, since the users pay little attention to security indicators on a site.

Automated attacks

SNS (Social Networking Sites) have been categorised into privacy related threats and traditional network threats [Gharibi and Shaabi, 2012]. Privacy related threats consider the setup of the social network account i.e. what information we share with the public, our friends, groups etc. and traditional threats are the ones related to people and computers, that is users who are targeted by spammers, phishing and malicious attacks.

Users tend to have accounts on multiple social network sites such as Facebook & Twitter, where they share information with their friends/followers. This phenomenon is exploited in semantic social engineering attacks.

In the previous section we looked at social engineering attacks in general, and users perception towards them. The attacks that are created are rarely carried out manually, and are launched to multiple users using scripts. Using information from at least two platforms, an attacker can launch an automated crawler. Such crawler would gather information about users whom have multiple accounts. If a user had an account on Facebook, but not Twitter, and was mutual friends with someone who has account on both, the crawler would create Twitter account and befriend the known acquaintance [Bilge et al., 2009]. From previous chapter we know that spear phishing attacks are quite successful, but now the attackers exploit trust between two friends. Since two users know each other it is easier to manipulate them to open content of a message [Jagatic et al., 2007]. The more we trust another person, the more likely we are to open the message received from them, ignoring security indicators. This can also be considered when an individual has an expertise in certain areas, such as cyber security, in which case we would outsource our trust to them, thus becoming more vulnerable [Colwill, 2009].

One of the more popular ways to launch an automated attack is to use self-replicating bots, that is bots which can by themselves crawl user profiles and create new social media accounts, befriending their victims. A number of studies have been carried out on the problem of self-replicating bots. This is but growing issue, as some more sophisticated software is able to automatically solve CAPTCHA tests, and register on a social network with minimal human input [Adewole et al., 2017]. Bot spammers will then use social networks to post malicious links, misuse

the following/followee and reply functions, as well as hijack trending topics [A. H. Wang, 2010].

Using social media bots can manipulate opinions, and even impact the decisions of voters, and can popularise low-credibility sources [C. Shao et al., 2018], such as the 2017 Catalan independence [Stella, Ferrara, and De Domenico, 2018], which has been shown to have been influenced by social bots, that would hijack the trending topic at the time in Spain. Similarly the bots had an impact on the 2016 UK-EU membership referendum [Howard and Kollanyi, 2016]. By collecting tweets with the hashtags related to the referendum, the researchers aim to determine if the tweet was posted by a bot or not. Users who posted often (more than 50 times a day) were mostly identified to be bots in this case.

Although countermeasures such as already mentioned CAPTCHA have been created to prevent the creation of accounts using automated scripts, they have been proven to be breakable since they follow a symmetrical pattern [C. Funk and Y. Liu, 2016], or machine learning has been applied [Chellapilla and Simard, 2005, Stark et al., 2015], which with partial human interaction can also break the protection of these challenge-responses [Van Tilborg and Jajodia, 2014].

The impact of self-replicating bots, and the difficulty to identify them by a normal users shows the importance of the spread of malicious content on social media, which can not only affect individuals, but also groups and masses, which will have an impact on democracy. Combining social engineering with automation has a big impact on the trust and gullibility of the people, it is therefore important to address these issues.

Combating automated attacks

Automated attacks are deployed on a large scale, and usually follow a certain pattern which can be observed, in the behaviour of the bots [Stieglitz et al., 2017; Stringhini, Kruegel, and G. Vigna, 2010]. Since the gullibility and targeted attacks of this nature can be inherently difficult for users to detect these kind of attacks, a large number of automated attacks can be identified with number of different methods.

As mentioned, researchers have noticed that spam bots tend to follow a certain behaviour, and classified it. **Displayer**, who is a bots that does not post spam messages, but only displays some spam content on their profile. **Braggers**, post messages to their own feed. **Posters**, send messages directly to each victim. **Whisperer**, send private message to each victim [Stringhini, Kruegel, and G. Vigna, 2010]. Using this approach and some machine learning classification, the researchers have managed to successfully identify and delete nearly 16,000 spam profiles on Twitter. Another novel approach by [K. Lee, Caverlee, and Webb, 2010] used social honeypots in order to detect spam accounts. Once enough profiles were identified, the researchers used machine learning algorithm, and were able to find spammers with about 80% accuracy. This was done on a set of 210,000 people [K. Lee, Caverlee, and Webb, 2010].

A novel approach proposed in [Martinez-Romo and Araujo, 2013] uses natural language processing techniques, to capture the bots present online. Their approach focuses on how the messages from the spammer are worded. These

kind of messages would usually try to divert a user to another site, and also contain a link to it. These kind of diversions would usually lead to a site that has no semantic relation with the message.

Another approach has been introduced in [Morstatter et al., 2016], in which different measurements are taken into account to measure bots more effectively. Most studies will have very accurate bot detection mechanisms, however they focus on precision, which indeed makes them identify bots very well, however it is a small fraction of bots. Here the researchers proposed measures which they claim can target larger numbers of content polluters. These heuristics include the fraction of re-tweets, since [Ratkiewicz et al., 2011] claimed that bots are not competent enough to create original content. The length of tweet for bots tends to be shorter, since they will usually try to encourage user to visit a particular URL [S. Lee and J. Kim, 2014], as well as the number of URLs the account has posted. They also consider how often an account would post on their timeline, since in [Y. Xie et al., 2008], bots have been characterised to have a tendency to post more content than a typical user.

The combination of different approaches, whether it is to use human-as-security-sensors, and creating tools to tackle human limitations based on the observations, or the subduing of automated attacks, can lower the infection rates. It is still the user who initiates the nevertheless, and the spread of that infection is driven by the connections that he/she has as a list of contacts. The user network is important, since the connection of an individual, will lead how the infection propagates through social media.

2.1.2 Summary

Despite the advances in technology and tools which help to tackle cyber threats, malicious content is still a big issue. With new technology being developed with security in mind [Mehrabi, Doche, and Jolfaei, 2020; Šišejković et al., 2019; Mohammed et al., 2017; Jeetendra Singh, 2021], attackers target the weakest link in the system, the user.

Social Engineering has become the most popular form of cyber attacks, with 98% of cyber attacks relying on it [PurpleSec, 2019]. Malicious users use a number of different techniques, to disguise themselves as legitimate. For example they will attempt to copy social media accounts onto multiple platforms, to befriend their victim, or copy source code of a web page to make it indistinguishable from the original source. Although methods to detect some of these attempts are automatic, the attackers efforts still succeed, with 55% of social engineering attacks being successful [Proofpoint, 2020].

A new approach has been proposed to tackle this issue head on, in which the user is playing a role of a security sensor [Heartfield, Loukas, and Gan, 2016]. This research focuses on idiosyncrasies of the users such as gullibility, security training, trust and other characteristics which impact the perception towards malicious content [Heartfield and Loukas, 2016b; Heartfield and Loukas, 2015]. As users gain more experience, they are better at identifying malicious cues, making the system more robust. This approach, as well as others in cyber security research however have users in isolation, where they are asked to identify series

of links, images, video etc. to study their awareness. This overlooks the fact that under normal circumstances users are connected with others in a network.

2.2 Network Science

A network is a set of interconnected units, i.e. people or things. Computers are part of the biggest technological network ever created, the World Wide Web [National Research Council, 2005], and with ever-growing popularity of portable devices and PCs, in 2010 the number of electronic devices overtook the number of human population (12.5 billion), giving 1.84 personal device for each person on the planet [Dave et al., 2011]. In 2017 the number of devices stood at 20.35 billion, with the number predicted to grow to 51.11 billion in 2023 [Rathod, Pandya, and Doshi, 2020]. This is indeed an enormous socio-technical system, with every single device producing some kind of data, which brought into the market new possibilities, such as Online Social Networks (OSNs) and the Internet of Things (IoT). These networks allow researchers to study new social phenomena, such as the location tracking, spread of fake news and cyber threats.

In other to understand how these devices are connected, we apply the study of Graph Theory, which we describe in detail in A.1.

2.3 Centrality measures

A topological structure of any graph can be entirely defined by the adjacency matrix. A variety of measures have been introduced to capture and describe its features. The most essential measures of a node in a network are concerned with the *importance* and *centrality* of the vertex. These measures are called centrality measures. The most widely used metrics of centrality are the degree, closeness and betweenness centrality. We describe those in depth in A.2, showing the numerical analysis of measures of network centrality, and the statistical metrics characterization in A.3.

2.4 Networks Models

The study of real networks has highlighted how they are typically characterised by a set of non-trivial features/properties. First, most nodes aren't neighbours of each other (i.e. connections are sparse), but nevertheless most nodes can be contacted via a small number of steps [Duncan J Watts and Steven H Strogatz, 1998]. Furthermore, several metrics such as degree, weights, strengths follow heterogeneous distributions, which are often modelled as power laws, meaning, for example, that while the majority of nodes have a low degree, and a small number of nodes have a large degree (i.e. hubs) [Albert-László Barabási and Réka Albert, 1999]. More precisely, key properties of real networks follow distributions that are heavy-tailed. Thus, they are far from *bell-shaped* distributions and averages are poor descriptors of the population.

In order to understand the mechanisms behind the formations of the real networks, several models have been proposed. Random graphs [ERDdS and R&WI, 1959, Erdos and Rényi, 1960], small world networks [Duncan J Watts and Steven H Strogatz, 1998] and preferential attachment models [Albert-László Barabási and Réka Albert, 1999] are prototypical examples.

Erdös-Rényi (ER) model

Random Graph model developed by Paul Erdös and Alfréd Rényi [Erdös and Rényi, 1959; Erdös and Rényi, 1960; Erdös and Rényi, 1961] is a network generator model, which takes a graph of N vertices, and connects each node with m random links among $N(N-1)/2$ of all nodes. The equivalent of this is a binomial model, where we start with N vertices, and for each pair of nodes (i,j) a link is formed with a probability p. The number of links is then a random variable with average value of $m = pN(N-1)/2$. To compute the average degree of these graphs, we can get the average number of edges generated in the construction which is $\langle E \rangle = \frac{1}{2}N(N-1)p$, and since every edge contributes to the degree, we get

$$\langle k \rangle = \frac{2\langle E \rangle}{N} = (N-1)p \simeq Np$$

By construction, ER models creates networks which feature homogeneous degree distributions and clustering coefficients, which are far from reality, but are characterised by small-world phenomena

Watts-Strogatz (WS) model

The Watts and Strogatz model mark an important milestone in our understanding of the mechanisms responsible for the emergence of real networks properties [D. J. Watts and S. H. Strogatz, 1998]. In this graph, N nodes are initially set in a ring topology. Each node is connected with $k/2$ nodes to its left and $k/2$ nodes to its right. Then each connection in the starting network is randomly re-assigned (i.e. rewired) with probability p. In the limit $p = 0$ the network is characterized by high clustering, but since the graph is a regular ring, the average distance between nodes is high. Interestingly, by increasing p there is a regime in which the network features high clustering but small world phenomena due to the *short-cuts* introduced by the rewiring. Increasing the value of p will decrease the clustering as the graph will become progressively closer to an ER network. Historically, this network model is the first to provide a mechanism able to create graphs with two key properties of real systems: small-world phenomena and high clustering. However, the emerging degree distribution from the model is still far from those observed in real networks [Alizadeh, Cioffi-Revilla, and Crooks, 2017].

Barabási-Albert (BA) model

The final model described in here is the Barabási-Albert model, is the first able to reproduce the heterogenities in the degree distributions observed in real networks [A.-L. Barabási, R. Albert, and Jeong, 1999]. The graph is generated in the following way:

1. the graph begins with small number of disconnected nodes n_0, with each new timestep $t = \Delta t + 1$ a new vertex is added to the graph and is connected with $m < n_0$ other nodes, which already exist in the graph

2. the probability π that the new node will be connected to the node i is function of the degree k_i: *preferential attachment* $\pi(k_i) = \frac{k_i}{\sum_j k_j}$.

Interestingly, it is easy to prove how this model generates systems characterised by power-law degree distributions of exponent of -3 and small-world phenomena. Although, the resulting clustering is far from those of real social networks, the model is a land-mark showing how preferential attachment mechanisms might be, at least in part, responsible for the heterogenities observed in real systems [Alizadeh, Cioffi-Revilla, and Crooks, 2017; Chattopadhyay and Murthy, 2017].

2.5 Epidemic models

Generally speaking the study of networks can be divided in two interconnected areas [Newman, M.E.J., 2010]. The first, deals with the definition and modeling of the topological features of networks. The networks models described above are a small sample of such studies. The second instead, deals with the function of networks studying among other things, the role that networks in driving dynamical processes unfolding on their fabric [Barrat, A. and Barthèlemy, M. and Vespignani, A., 2008]. A prominent example of this, which is key for the research presented here, is the study of contagion processes such as the propagation of viruses. Here, the study of networks intersect the field of epidemiology. In fact, epidemic models can be used to represent the spread of infections. Each agent/individual can be described as a node, and edges are connections between those agents. If one agent is infected, and an edge exists between them, the disease will be able to spread. The population is divided into compartments, which include susceptible, infected and recovered in its simplest forms. These are known as compartmental spreading models, and include SI, SIS, and SIR models[1], for which derivations of exist, for example the SEIR or SIRQ models, which include exposed and quarantine states respectively. [W. O. Kermack and A. G. McKendrick, 1932]. These models have applications outside of simply studying biological viruses. Number of studies have used these techniques to model the spread of infection on social, sexual and digital networks, such as the mobile phone network [Pu Wang et al., 2009] or Facebook [Kramer, Guillory, and Hancock, 2014].

[1] S - Susceptible, I - Infected, R - Recovered

2.5.1 SI model

The very basic model consists of two compartments, the Susceptible and Infected. Here a susceptible agent can only be infected with probability β, and they remain in the infected state, thus making the entire network eventually becoming totally infected, giving $S + I \rightarrow 2I$. This spread can be modelled with a set of simple differential equations

$$d_t S = -\frac{\beta SI}{N}$$
$$d_t I = \frac{\beta SI}{N}$$

yielding the number of susceptible and infected individuals at each time-step respectively. The numerator represents the rate of infection, where the denominator the total population, with each equation giving a ratio of population in given compartment [Brauer, 2008; Martcheva, 2015].

2.5.2 SIS model

Building up on the SI model, return to the susceptible compartment, meaning that already infected agents can recover with probability μ, and become susceptible again. This happens for example with sexually transmitted diseases. This is not a permanent immunity, and the agent has a chance of becoming infected again with probability β. We can find the number of infected and susceptible agents by working out the differential equations

$$d_t S = -\frac{\beta SI}{N} + \mu I$$
$$d_t I = \frac{\beta SI}{N} - \mu I$$

which similarly to SI gives us the ratio of infected and susceptible agents at each time-step, however in this case we also consider the recovered population μI. In the first equation we add number of recovered to the number of susceptible, changing the infected compartment back to susceptible, thus $S + \mu I \rightarrow 2S$, and in the second part we remove number of recovered population. It is to show how in this model the disease will be able to spread and affect a finite fraction of the population only if the basic reproductive number $R_0 = \frac{\beta}{\mu}$ is larger than one. The quantify describes the average number of secondary infections, from a single infection (a seed), in a fully susceptible population. If $R_0 < 1$ the infection will die out, however if $R_0 > 1$ the infection will become persistent. In fact, in this case the two compartments will transition into a stable sate, leaving the population fluctuating between the two [Brauer, 2008; Martcheva, 2015].

2.5.3 SIR model

The SIR model is similar to the SIS model, where an agent can recover from the infection, however in this case once an agent is recovered, they stay recovered (or die). The system is expected to get fully recovered with this model, meaning that the infection will eventually die out, and the agents become immune to it.

$$\begin{aligned} d_t S &= -\frac{\beta S I}{N} + \mu I \\ d_t I &= \frac{\beta S I}{N} - \mu I \\ d_t R &= \mu I \end{aligned}$$

in this model we do not consider births and deaths of an agent, and the population is constant in a way that $S(t) + I(t) + R(t) = N$. In this case the disease will eventually die out, meaning that all of the population will eventually recover (or die). Interestingly, the SIR model features the same R_0 of the SIS model [Brauer, 2008; Martcheva, 2015; Prakash, Chakrabarti, et al., 2012].

2.5.4 Epidemic models on networks

The equations described above are valid in a particular limit, the so-called homogeneous mixing, in which all individuals are in possible contact. However, as mentioned above, many real socio- technical networks are far from homogeneous. The fluctuations, and the absence of a characteristic scale (i.e. averages are not a good representation of the system's properties) play a main role in determining the propagation of contagion processes [Anderson, R.M. and May, R.M., 1992; R. Pastor-Satorras and A. Vespignani, 2001; R. Pastor-Satorras and A. Vespignani, 2004; Balcan, V. Colizza, et al., 2009].
In order to relax the well-mixed approximation, we can use a mean-field approach which assumes that all nodes with the same degree are statistically equivalent. Thus, we move from the number of infected and susceptible nodes in the system, to variables describing the number of ratio of infected and susceptible nodes in a each degree class k:

$$i_k = \frac{I_k}{N_k}, \quad s_k \frac{S_k}{N_k}. \tag{2.1}$$

The SI model

The variation of the fraction of infected nodes in each degree class in the SI model can be written as:

$$d_t i_k(t) = \beta[1 - i_k(t)]k\theta_k(t). \tag{2.2}$$

where we have defined $\theta_k(t)$ as the density of infected neighbors of vertices of degree k. It is important to recall how in the homogeneous assumption described above the last term was equal to the density of infected nodes. In a heterogeneous network it is in general a very complicated term that takes into into account the

different degree classes and their connections. Just to give an example, let us consider the simplest case where degree classes are not correlated:

$$\theta_k(t) = \theta(t) = \frac{\sum_{k'}(k'-1)P(k')i_{k'}(t)}{< k >}. \tag{2.3}$$

Plugging this in the (2.2) we can write:

$$d_t i_k(t) = \beta k \theta(t). \tag{2.4}$$

By multiplying both sides of this expression for $\sum_k (k-1)P(k)$ and summing over all degree classes we get:

$$d_t \theta(t) = \beta \theta(t) \left(\frac{< k^2 >}{< k >} - 1 \right). \tag{2.5}$$

Imposing, as initial condition $i_k(t=0) = i_0$ we can solve the equation obtaining:

$$i_k(t) = i_0 \left[1 + \frac{k(< k > -1)}{< k^2 > - < k >} (e^{t/\tau} - 1) \right], \tag{2.6}$$

where we defined

$$\tau = \frac{< k >}{\beta(< k^2 > - < k >)}. \tag{2.7}$$

The results control that the fraction of people infected is rising exponentially. Interestingly, this processes is faster for nodes with high degree. In addition to that, the growth timescale is determined by the second and first moment ratio of the degree distribution ($< k^2 > / < k >$). Networks with higher degree distribution, with exponent $2 < \alpha \leq 3$ (in the limit $N \to \infty$), follow a power-law and would have a divering second moment. We will therefore have a nearly immediate increase in the scale of the epidemic size. In fact, it can easily spread through the network as soon as the disease has reached the hubs [Lawyer, 2015; J.-G. Liu et al., 2016].

The SIS and SIR model

A generalization for these two models, accounting for the presence of a network, follows the same steps described above:

$$d_t i_k(t) = \beta k s_k(t) \theta_k(t) - \mu i_k(t), \tag{2.8}$$

where we have $s_k(t) = 1 - i_k(t)$ for the SIS model and $s_k(t) = 1 - r_k(t) - i_k(t)$ for the SIR model. It is easy to show (see Ref. [Barrat, A. and Barthèlemy, M. and Vespignani, A., 2008]) how for the two models, in uncorrelated networks, the disease will be able to spread to a finite fraction of the system only if

$$\frac{\beta}{\mu} \geq \frac{< k >}{< k^2 > - < k >}. \tag{2.9}$$

For SIS models the expression is the same but for the last term in the denominator. In case of networks with a power-law degree distributions with exponent $2 < \alpha \leq 3$ (in limit of infinite size) the second moment diverges, so we have a null epidemic threshold. Real networks are not finite, thus the threshold is not zero, but really small. This is key result in Network Science. It highlights how heterogeneous networks behave in a completely different way from homogeneous networks and show the effects of heterogenous degree distributions.

2.5.5 Beyond SI, SIS and SIR models

Changing the properties of the compartmental epidemic models, allows for creation of different variations, which can capture additional phenomena even beyond biological contagion. This could be length of exposure to infected node, quarantine of them, adding categories of susceptibility/recovery, time-aspect of the network. Introducing a required contact between infected and recovered nodes, in order for an agent to recover, has been found to reduce the error of predicting the contagion of a virus on an online social platform [Cannarella and Spechler, 2014]. Changing the parameters of a model can also have an impact on the contagion, for example considering quarantined files, or the ones which are exposed, but the virus is removed before causing damage [Guillén, Rey, and Encinas, 2017]. The methodologies used to study infection spread, often use theoretical data or partial data sets. If the data is incomplete, it can however be reconstructed with fair level of accuracy [Génois et al., 2015]. The idea of reconstructing the data can lead to limitations, especially if the fraction of nodes excluded becomes too large, this would lead the properties of the data to start differ very quickly. Another limitation of the reconstruction method lies in the need to know the number of individuals missing in each department or class. If these numbers are completely unknown, giving an estimation of outbreak sizes is impossible, as adding arbitrary number of nodes and links to the re-sampled data can lead to arbitrarily large epidemics.

Social Contagion

Networks can yield a spread of beliefs, emotions, behaviour etc. These collective processes diffuse through social contacts and can be modelled as complex (social) contagions on networks [Guilbeault, Becker, and Centola, 2018]. The word complex is used to distinguish them from simple, biological, contagions. Indeed, while we have a fixed probability of being biologically infected given a contact with an infectious person, we might or might not spread an information item according to its origin, what our friends think about, or its originality. Complex contagions have a social and psychological origin [Guilbeault, Becker, and Centola, 2018; Centola and Macy, 2007]. They are active rather than passive acts (such as getting infected), might be advantageous, require multiple exposures, and are linked to social legitimation, credibility, uncertainty, as well as various externalities. In the context of opinions or innovations dynamics, complex contagions are often modelled as threshold processes [Centola and Macy, 2007]. In these, a node might adopt an innovation if a fraction (or number) of its connections are adopters. Consequently, they require a critical mass to spread. The adoption

threshold might depend on the characteristics of individuals and their connections; we might be more inclined to adopt an innovation if one of our strong ties (i.e., best friend) or prominent person (i.e., celebrity) is an adopter. In the context of social norms or conventions dynamics, complex contagions are often modelled within the Naming Game framework [Andrea Baronchelli, 2018]. Here, individuals are characterized by an inventory of alternatives (e.g., possible conventions), which is empty at the beginning of the process. In each time step a pair of neighboring nodes is chosen randomly, one to play as hearer and the other a speaker. The speaker randomly selects one of its alternatives or invents a new one if its inventory is empty. If the hearer's inventory contains such alternative, the two individuals update their inventories so as to keep only the one involved in the interaction, otherwise the hearer adds it to those already stored in its inventory. Thus, at least two interactions are needed for an individual to go from state A to state B, a characteristic feature of complex contagion.

Thus, in social contagion processes, agents would be influenced by their local neighbourhood, estimating the global behaviour based on their local observations [Lerman, Yan, and X.-Z. Wu, 2016]. Individuals will grossly overestimate the prevalence of some attribute, making it appear more popular what it is. Another effect defined here is the "false consensus" in which an individual overestimates the prevalence of their own features in the population, by believing it is more common. For example the democrats believe most people are also democrats. "Pluralistic ignorance" is another social perception bias. This effect arises in situations when individuals incorrectly believe that a majority has an attribute or accepts a norm that they themselves don't share. Pluralistic ignorance was invoked to explain why bystanders fail to act in emergencies and why collage students tend to overestimate alcohol use among their peers. The behaviour of a minority can also be adopted under certain conditions [Alvarez-Galvez, 2016]. The most important factor of that adoption would be how it is influenced, for example by more important agents or media [N. Chen, 2009]. The success of minority opinions does not only depend on the network structure and composition but also on external factors such as mass media information or average connectivity, that can mediate the strength of these structural determinants.

Adoption of behaviour between individuals can increase the spread of virus, especially when a susceptible and infected agents create a link between each other [Albert-László Barabási, 2013]. The adoption of behaviour is more likely to occur between individuals who know each other [Centola, 2010].

Predicting the future interactions between individuals would allow for a dramatic improvement into minimising the spread of contagion. This however has been proved to be very difficult, and have low accuracy [Liben-Nowell and Jon Kleinberg, 2007]. Using a simple link-prediction problem, the study focused on prediction of links between scientists i.e. if two researchers collaborate, a link is created. The network used here has very similar properties to ones used in [Centola, 2010]. However the co-authorship prediction was fairly low, with the different predictors accuracy scoring between 18% and 54%.

2.6 Time-varying networks

Real networks are not static [Petter Holme and Saramäki, 2012]. They change in time, subject to non-trivial dynamics. In particular, the activity, defined as the propensity per unit time to initiate a social interaction (e.g., send a message), and the attractiveness, defined as the propensity per unit time to be the target of a social act (e.g., receive a message), are heterogeneously distributed and correlated [Nicola Perra, Gonçalves, et al., 2012; Ribeiro, N. Perra, and A. Baronchelli, 2013]. People activate more often in a small set of (strong) ties, which are organised in tight communities that emerge and evolve in time [Onnela et al., 2007]. Furthermore, the inter-event time (i.e., interval between two consecutive social interactions) is also heterogeneous; interactions do not take place at a constant rate [Márton Karsai, Kivelä, et al., 2011].

Any system with coupling connections and information about time can be modeled as a temporal network [Petter Holme and Saramäki, 2012]. For example, humans tend to create these kind of patterns in proximity networks. Simply putting, the individuals meet each other in time and space, allowing for creation of time-varying network [Alain Barrat and Ciro Cattuto, 2013, Ciro Cattuto et al., 2013, Kibanov et al., 2014]. Temporal data can be obtained from variety of sources, such as mobile phone operators [M.-X. Li et al., 2014, Kovanen et al., 2013, Miritello, Moro, and Lara, 2011], network of emails [Holger Ebel, L.-I. Mielsch, and Stefan Bornholdt, 2002, Eckmann, Moses, and Sergi, 2004], or social media platforms [Romero, Meeder, and Jon Kleinberg, 2011].

Interestingly, the mechanisms driving the formation of contacts depend on the time-scale and time horizon considered. In fact, those describing interactions at the time-scale of minutes are very different than those at the time scale of months or years Sekara, Stopczynski, and Lehmann, 2016. This observation is of key importance when studying the spreading of contagion processes Morris and Mirjam Kretzschmar, 1995; Nicola Perra, Gonçalves, et al., 2012; Rocha, Fredrik Liljeros, and Petter Holme, 2011; Stehlé et al., 2011; Masuda and Petter Holme, 2013; Moody, 2002; S.-Y. Liu, Andrea Baronchelli, and Nicola Perra, 2013; Fefferman and Ng, 2007; Machens et al., 2013; S. Liu et al., 2014; Starnini and Romualdo Pastor-Satorras, 2014; K. Sun, Andrea Baronchelli, and Nicola Perra, 2015; D. Han, M. Sun, and D. Li, 2015; Sunny, Kotnis, and Kuri, 2015; Petter Holme and Masuda, 2015; Fredrik Liljeros, Giesecke, and Petter Holme, 2007; Petter Holme and Fredrik Liljeros, 2014; Toth et al., 2015; Romualdo Pastor-Satorras, Claudio Castellano, et al., 2015; Bruno Ribeiro, Nicola Perra, and Andrea Baronchelli, 2013. The order, co-occurrence, correlations and more in general the temporal dynamics of contacts patterns have a drastic effects on dynamical processes [Petter Holme, 2015].

2.6.1 Activity-Driven Networks

A popular modeling framework of time-varying networks is that of activity-driven networks [Nicola Perra, Gonçalves, et al., 2012]. This modeling approach is based on the empirical observation that the propensity of individuals of being engaged in social acts, *activity*, is heterogeneously distributed [Nicola Perra, Gonçalves, et

al., 2012]. Remarkably, such observations have been reported in a wide range of real systems capturing different types of human interactions or human dynamics ranging from R&D alliances between firms to conversations on Twitter [Nicola Perra, Gonçalves, et al., 2012; Tomasello et al., 2014]. For a given time interval the activity of each node i can be measured as the fraction between the number of interactions made by i, n_i, divided by the total number of interactions made by all the nodes:

$$a_i = \frac{n_i}{\sum_l n_l} \tag{2.10}$$

While the value of the activity of each node might change in time [Moinet, Starnini, and Romualdo Pastor-Satorras, 2015] observation in real data have shown how the distribution of activity is virtually independent of the choice of time window size [Nicola Perra, Gonçalves, et al., 2012; Bruno Ribeiro, Nicola Perra, and Andrea Baronchelli, 2013; Tomasello et al., 2014]. This candidates the activity as good variable to describe some important aspects of time-varying networks. Starting from this intuition and empirical findings, in activity-driven networks each node is assigned to an activity a extracted from a distribution $F(a)$. At any time step t the network G_t is build starting from N disconnected vertices. In their simplest form, the generative process of the network is as follows:

- At each discrete time step t the network G_t starts with N disconnected vertices;
- With probability $a_i \Delta t$ each vertex i becomes active and generates m links that are connected to m other randomly selected vertices. Non-active nodes can still receive connections from other active vertices;
- At the next time step $t + \Delta t$, all the edges in the network G_t are deleted. From this definition it follows that all interactions have a constant duration $\tau_i = \Delta t$.

Once the model is generated we can consider $\langle k \rangle_t = \frac{2E_t}{N} = 2m\eta\langle x \rangle$ as the average degree at each time step. Where E_t is the total number of edges per unit time and $\eta\langle x \rangle$ is the average number of active nodes. The instantaneous snapshot of the network will have a star-like topology, where the $k \geq m$. In fact, in case of heterogeneous activity distributions at each time step, the large number of nodes will be not active and the topology of each G_t will be based on set of mostly disconnected stars centred around active nodes. However, it is possible to show how integrating links over sufficient T time-steps such that $k/N \ll 1$ and $T/N \ll 1$ the resulting network will have a degree distribution that follows the activity distribution [Nicola Perra, Gonçalves, et al., 2012; Starnini and Romualdo Pastor-Satorras, 2014]. Thus, the heterogeneity in the number of contacts integrated over time is driven by the heterogeneity in the propensity of nodes to be engaged in social acts. Interestingly, *hubs* emerge in time due to their constant engagement rather than due to some first mover (rich-get-richer) advantages as in classic preferential attachment models. Furthermore, the complex dynamics of the network and its ensuing structure is completely encoded in the activity distribution.

The simplicity of the model makes it possible to derive and study the dynamical properties of contagion processes unfolding on its fabric. Consider a SIS model. At a mean-field level, the epidemic process will be characterized by the number of infected individuals in the class of activity rate a, at time t, namely I_a^t. It is interesting to note how in time-varying network the degree k we used above to describe epidemic models unfolding on static graphs is not a key variable any longer. In fact, the degree is function of the time-window used to observe the system. The activity distribution instead has been shown to be independent of such choice. The number of infected individuals of class a at time $t + \Delta t$ given by:

$$I_a^{t+\Delta t} = -\mu \Delta t I_a^t + I_a^t + \lambda m (N_a^t - I_a^t) a \Delta t \int da' \frac{I_{a'}^t}{N} + \lambda m (N_a^t - I_a^t) \int da' \frac{I_{a'}^t a' \Delta t}{N}, \tag{2.11}$$

where N_a is the total number of individuals with activity a.

The above equation can be solved, yielding the following epidemic threshold for the activity driven model:

$$\frac{\beta}{\mu} > \frac{2\langle a \rangle}{\langle a \rangle + \sqrt{\langle a^2 \rangle}}. \tag{2.12}$$

Thus threshold is function of the first and second moments of the activity distribution thus it takes into account the dynamics of interactions. Importantly, the epidemic threshold is not function of the time-aggregated network presentation. It depends just on the interaction rate of nodes. This results show the importance of time-scales. Indeed the spreading condition is dependent on the interplay between the time-scales of the network and spreading process.

The activity-driven framework has been expanded [K. Sun, Enrico Ubaldi, et al., 2019], respect to the simplest form described here, considering more realistic links' creation mechanisms to account for the presence/emergence of weak and strong ties [M. Karsai, N. Perra, and A. Vespignani, 2014], communities [Nadini et al., 2018], burstiness [Enrico Ubaldi et al., 2017], and popularity effects [Alessandretti et al., 2017]. As described in Chapter 3, we have extended the literature proposing another extension necessary to model the spreading of cyber threats in online social networks.

2.7 Modelling the contagion of cyber security threats

Computer and biological processes are clearly different but, for some aspects similar to each other [Kephart and S. R. White, 1992]. For example, the propagation of a virus from host to host, whether biological or digital follows the same general principles of contagion [F. Cohen, 1987]. There are however differences. Biological viruses' range is bounded by physical or proximity contacts. Computer viruses instead can infect and spread through the Internet, meaning they potentially have a world wide (almost instantaneous) range.

Since cyber threats are similar to their biological counterparts, we can use the compartmental spreading models to study the behaviour of a virus on a social

network. Such studies have been carried out number of times, and have came to confirm this intuition. Using compartmental modelling Zhang, X et al. [X. Zhang and Tadi, 2007] modelled a virus spread on a small world networks, to characterize how it would impact a hybrid wireless and wired networks. The research offers a guideline at which optimal time to introduce an anti-virus, in order to reduce both cost of developing it, and the damage caused by the virus.

The propagation of viruses via emails has been successfully modeled adapting classic epidemic models on directed networks [M. E. Newman, Stephanie Forrest, and Justin Balthrop, 2002].

Restraining the virus as early as possible will reduce the number of infected users [Zhu and Cen, 2017, Zhu, X. Yang, and J. Ren, 2012]. Because of the heterogeneity of the degree distribution, smaller percentage of nodes can compromise the network. This would lead to a less infectious virus lasting longer and infect substantial part of the network [Yasir et al., 2017]. Depending on the environment in which virus exist it would have a different contagion speed [Barrett et al., 2008].

Contagion of information is growing on social networks, thanks to their ease of use, accessibility and impact factor that this form of media has. Creating a larger social network would indicate individuals' influence, and popularity. Larger social networks would mean a larger audience i.e. a larger degree of a node. If a user with high degree was compromised, or was a spammer themselves, they would infect a large number of susceptible agents.

Bots can indeed be used for spread of information, and be an effective in influencing trending topics. On social platforms such as Twitter, using a hashtag would mark a message related to a specific topic. Using popular hashtags in San Francisco Area Mønsted, B. et al. conducted research, showing how the information can spread using popular hashtags [Mønsted et al., 2017]. The bots appeared as human like, which was achieved by using simple language processing rules, and recycling popular Twitter content. Whenever a user would follow a bot, the ID of that user was automatically 'given' to other bots, so that they would also attempt to follow that user. The researchers managed to gain around 25,000 followers at the time.

We can also model the contagion of emotions via social networks. A large scale study involving over 689,000 Facebook users carried out by Kramer et al. modelled how users would respond to positive and negative reactions on the platform [Kramer, Guillory, and Hancock, 2014]. Looking at greater number of positively or negatively written posts at any one time, the research looked into how friends would react to the post, if it was with the same reaction as the original post or not, in other words, if friends would respond with positive messages to a positive post and vice versa. Posts would fall under one of the two categories, if they contained at least one positive or negative word. The research has indeed found that there is an emotional contagion, with people responding negatively when positivity was reduced, and positively when negativity was reduced.

Further studies into emotional contagion also focus on the two aforementioned categories [Bliss et al., 2012, Bollen et al., 2011, Ferrara, Varol, et al., 2016]. Since the two categories can break down into a number of sub-categorical human behaviours, it can be divided further down, for better understanding of which

emotion has more impact on the contagion. Using data from Chinese equivalent of Twitter, from over 11 million tweets, an attempt to bridge this emotional gap identified four different categories, joy, anger, disgust and sadness. In their longitudinal study, researchers find that joy and anger are the most spread emotions, with anger being more contagious than joy, indicating that it can spark more angry follow-up tweets [Fan, K. Xu, and J. Zhao, 2016].

The spread of emotion can have an impact on real world actions. Messages that have published in during the 2010 US congressional elections, had an impact on how voters party affiliations [Bond et al., 2012]. Studying methods used computational social sciences, we can find how people think/behave/feel in different situations. Since in some social media human users tend to follow a certain pattern, that is similar to a physical trace, finding that pattern would allow for data collection. Such methods would involve finding popular content, in a museum this could be indicated by worn out tiles near more famed attractions. On the World Wide Web, this data would include likes, number of posts (accretion traces), or the removal of content, articles, unfollowing/unfriending users(erosion traces) [Strohmaier and C. Wagner, 2014].

Responding to a certain message is also impacted by its content [C. Wagner, M. Rowe, et al., 2012]. Catching attention of users in study by Wagner et al. depended on numerous things, such as the topic, title, age and popularity of the account. These features applied to an Irish community message board, where the community driven content was categorised by a subject. Content driven communities, such as tech based or motor based, have more supportive communities compared to the more general ones, indicating the willingness of people with similar interests to create a connection with each other. In the communities which lack specificity, the post seem to require to be short and contain distinct term in order to get a response.

This social paradigm allows to measure the susceptibility of users in online social networks. Using social bots and defining an infection as a interaction with the bot, and and susceptibility as being within the bots secondary connection, Wagner et al. modelled the behaviour of susceptible users who interacted with the social bot [C. Wagner, Mitter, et al., 2012].Susceptible users tend to have a higher conversational balance, which shows they communicate with high variety of users, and they don't focus on communicating with their circle of friends, rather they spend an equal amount of time communicating with large variety of users. Interestingly the negative emotions tend to spark more interactions with the bots, which correlates with other study on emotional contagion [Fan, K. Xu, and J. Zhao, 2016]. Negative words and words related to the topic of death were found to interact more with the bots than other susceptible users. [Guha and Daswani, 2005, A. Khan and Heckel, 2011] [Meloni et al., 2011] .

Considering different network configurations can help us study the behaviour of the contagion [Dadlani et al., 2016]. For example considering limiting the number of new connections made by a node at time t, would change the behaviour of the disease by causing it to spread slower [Alain Barrat, Marc Barthelemy, Romualdo Pastor-Satorras, et al., 2004], or that scale free networks are more prone to

persistence to the spreading [Romualdo Pastor-Satorras and Alessandro Vespignani, 2001]. Studying localised attacks on such networks, leads to findings described by Shao et al. They find that the effect of a localised attack on an ER network is identical to a random attack. For random network, the threshold of localized attack is always smaller (network is more robust) compared to a random attack, and for scale free network, localized attack is found to be critically dependant upon the power law exponent. [S. Shao et al., 2015]

2.8 Research Gaps

Despite the restless research activity, we can identify three key research gaps that may be impeding significant progresses in the area.

First, susceptibility to cyber threats is typically measured and studied considering users in isolation thus neglecting that they are instead connected via networks. In other words, gullibility is typically considered as an individual property. This approach ignores that it might be modulated by networks' effects emerging from users' interactions. For example, independently of its content, we might be more prone to open a message sent by a close friend than a random person.

Second, beside some early work on the spreading of viruses via Bluetooth among mobile phones [Pu Wang et al., 2009], the study of the propagation of cyber threats considering the temporal nature of social interactions is still missing. Furthermore, with few exceptions [Peng et al., 2017], the literature devoted to the study of computer viruses unfolding on networks typically neglects that the susceptibility of online users is not homogenous.

Third, there is a lack of real data describing the real spreading of such phenomena. This is stark contrast respect to the case of spam for which public large-scale datasets have been collected [B. B. Gupta et al., 2017]. It is important to notice how the data does exist, but it is in the hands of for-profit corporations that have little interest in publicizing the risks and threats their users might be exposed to.

Chapter 3

The spreading of computer viruses on time-varying networks

The chapter has been published as a work of multiple authors in Physical Review E. [Brett et al., 2019]

As mentioned in the first two chapters, alongside clear societal and economic benefits, modern technology exposes us to serious challenges. In particular, the spreading of malicious content online, often based on ingenious deception strategies, is one of the most pressing because it poses serious threats to our privacy, finances, and safety [Kayes and Iamnitchi, 2017]. Victims of a typical social engineering attack [Heartfield and Loukas, 2016a] may receive a message containing a malicious link or file, appearing to originate from a friend or other trusted entity. If opened, it may compromise the computer, access personal information, and spread the virus further unbeknownst to the victim. Recent research has shown how the susceptibility of individuals to such attacks is not homogenous and depends on several features such as age, prior training, computer proficiency, familiarity with social network platforms, among others [Heartfield and Loukas, 2018, Heartfield, Loukas, and Gan, 2016, Heartfield and Loukas, 2018]. Furthermore, the properties of real networks are known to facilitate the propagation of such processes [A. L. Lloyd and R. M. May, 2001b; Justin Balthrop et al., 2004; Romualdo Pastor-Satorras, Alexei Vázquez, and Alessandro Vespignani, 2001; Yamir Moreno and Vazquez, 2003; M. E. Newman, 2002; Newman, 2010; Romualdo Pastor-Satorras, Claudio Castellano, et al., 2015; Alain Barrat, Marc Barthelemy, and Alessandro Vespignani, 2008; L.-X. Yang, X. Yang, et al., 2013; L.-X. Yang and X. Yang, 2014b]. In particular,the heterogeneity in contact patterns makes socio-technical systems quite fragile to biological and digital threats.

3.1 The challenge and research gap

The study of these phenomena has largely neglected the complex temporal nature of online contact patterns in favor of static and time-aggregated approaches. These approximations might be fitting. Indeed, in the past, computer viruses would spread mainly via email networks, targeting the address books of victims, which contain contacts lists. However, not many people create such lists any more and

access to them is restricted. In the context of social or biological contagions, neglecting the temporal nature of the networks where the processes unfold has been shown to induce misrepresentations of their spreading potential. In fact, the order and concurrency of connections is key to capture the dynamics of face-to-face interactions [Alain Barrat and Ciro Cattuto, 2015], to correctly characterize diffusion processes such as random walks [N. Perra, A. Baronchelli, et al., 2012; Ribeiro, N. Perra, and A. Baronchelli, 2013; Starnini, Andrea Baronchelli, et al., 2012; Scholtes et al., 2014; Pfitzner et al., 2013], to define more accurate centrality metrics [M. J. Williams and Musolesi, 2016; Rocha and Masuda, 2014], to describe contagion processes such as epidemic spreading [N. Perra, Gonçalves, et al., 2012; Starnini, Machens, et al., 2013; Valdano, Ferreri, et al., 2015; K. Sun, Andrea Baronchelli, and Nicola Perra, 2015; Takaguchi, Masuda, and Petter Holme, 2013; Petter Holme and Fredrik Liljeros, 2014; Petter Holme and Masuda, 2015; Z. Wang et al., 2016; Gonçalves and Nicola Perra, 2015] and social contagion [Mistry et al., 2015].

To the best of our knowledge, beside some early work on the spreading of viruses via Bluetooth among mobile phones [Wang, 2009], the study of the propagation of cyber threats considering the temporal nature of social interactions is still missing. Further-more, with few exceptions [Peng et al., 2017], the literature devoted to the study of computer viruses unfolding on networks typically neglects that the susceptibility of online users is not homogenous. Conversely, the literature that studies the susceptibility of users to cyber threats traditionally focuses on single users neglecting their connections.

To tackle these limitations, here we introduce a theoretical framework to study the spreading of computer viruses, based on social engineering deception strategies, on time-varying networks. We model users' interactions using a time-varying network model and consider two types of viruses. The first mimics threats that can propagate only via connections activated at each time step. The second, on the contrary, considers viruses able to access also information about past connections. We investigate the impact of different classes of susceptibility considering that they might also influence the link formation process. In all cases, we analytically derive the conditions regulating the spreading of the virus. Interestingly, these are defined by the interplay between the features of the cyber threats, the categories of susceptibility and their time-varying connectivity. Furthermore, in some scenarios, the temporal coupling between categories creates a complex phenomenology that favors the spreading of the virus. These results have the potential to initiate future efforts aimed at describing more realistically the spreading of computer viruses on online social networks.

3.2 Proposed model

We consider a population of N online users which exchange messages in a time-varying network. Nodes are assigned to one of Q categories describing their susceptibility to cyber threats measured in terms of their *gullibility* and time needed to recover from successful attacks. Since susceptibility is linked to demographic features, we consider that the membership to a category might influence the link

creation process. In fact, homophily is a strong social mechanism known to affect the structure and organization of ties [McPherson, Smith-Lovin, and J. M. Cook, 2001]. We model the contact patterns between users with a generalization of the activity-driven framework [N. Perra, Gonçalves, et al., 2012; M. Karsai, N. Perra, and A. Vespignani, 2014; E. Ubaldi et al., 2016; Tizzani et al., 2018]. Here, nodes feature an activity a describing their propensity to initiate communications. Activities are extracted from a distribution $F(a)$ which, as observations in real systems have shown, is typically heterogenous [N. Perra, Gonçalves, et al., 2012; Ribeiro, N. Perra, and A. Baronchelli, 2013; E. Ubaldi et al., 2016; Tomasello et al., 2014]. We select power-law distributions $F(a) \sim a^{-\alpha}$ with $a \in [\epsilon, 1]$ to avoid divergences. At each time step nodes are active with probability $a\Delta t$. Active nodes select m others and create directed (out-going) links which mimic messages.

In the simplest version of activity-driven networks the selection is random and memoryless [N. Perra, Gonçalves, et al., 2012]. Here, we propose a variation: with probability p each target is selected, at random, among the group of nodes in the same category, and with probability $1 - p$ among the nodes in any other category. In other words, p tunes the homophily level in the network with respect to susceptibility to cyber threats. At time $t + \Delta t$ all edges are deleted and the process starts from the beginning. Unless specified otherwise, links have a duration Δt. Without loss of generality we set $\Delta t = 1$. The model is clearly a simplification of real interactions. However, it offers simple, yet non trivial, settings to study the effects of temporal connectivity patterns on contagion processes unfolding at a comparable time-scale with respect to the evolution of connections [N. Perra, Gonçalves, et al., 2012; N. Perra, A. Baronchelli, et al., 2012; M. Karsai, N. Perra, and A. Vespignani, 2014; S. Liu et al., 2014].

We describe the propagation of a computer virus adopting the prototypical SIS model [M. Keeling and P. Rohani, 2008; A. Barrat, Barthélemy, and A. Vespignani, 2008]. At each time step t the virus, unbeknownst to the victims, sends a message, with malicious content, to all the nodes genuinely contacted at t (virus type 1) or within $t - \tau$ time-steps (virus type 2). The focus is not defining the optimal set of nodes to maximize/minimize the damage. Thus, we select randomly a small percentage (0.5%) of nodes as initial seeds. In these settings, susceptible nodes of class $x \in [1, \ldots, Q]$, that receive a malicious message, become infectious with probability λ_x which defines their gullibility. They recover and become susceptible again with rate μ_x. In the literature of epidemic spreading on static networks we find few studies that consider different classes of infectiousness and/or recovery rates [Smilkov, Hidalgo, and Kocarev, 2014; Miller, 2009; Gou and Jin, 2017]. Interestingly, this body of research highlights how heterogeneities in such quantities, especially in case of correlations with topological features such as the degree or in presence of large values of clustering, induce no trivial phenomena that might speed up or slow down the spreading. As shown below, our results confirm this picture.

3.3 Analytical derivations

We assume that nodes with the same value of activity and in the same category are statistically equivalent, we group them according to the two features. At each time step, we call S_a^x and I_a^x the number of nodes susceptible and infected in activity class a and category x. Clearly $\int da S_a^x = S^x$, $\int da I_a^x = I^x$, $\sum_x S^x = S$, and $\sum_x I^x = I$. Furthermore, N_a^x describes the number of nodes of activity a in category x, thus $\int da N_a^x = N^x$ and $\sum_x N^x = N$. In these settings, we can represent the variation of the number of infected nodes of activity a in category x as:

$$d_t I_a^x = -\mu_x I_a^x + \lambda_x m S_a^x \left[p \int da' a' \frac{I_{a'}^x}{N^x} + (1-p) \sum_{y \neq x} \int da' a' \frac{I_{a'}^y}{N - N^y} \right]. \tag{3.1}$$

The first term on the right hand side, describes the recovery process. The second term instead describes susceptible nodes that are connected by active nodes in the same category that are infected. These nodes get infected with probability λ_x and selected with probability $p\frac{m}{N^x}$ (where N^x is the total number of nodes in the category x). The third term, accounts for the same process but in which the susceptible node in activity class a receives a message from active and infected nodes in other categories. Each node is selected with probability $(1-p)\frac{m}{N-N^y}$ by active vertices in class y. At early stages of the spreading we can assume that the number of infected to be very small respect to the susceptible thus we can approximate $S_a^x \sim N_a^x$. This is equivalent to neglect terms of the order of $(I_a^x)^2$. We can also define $\int da' a' I_{a'}^x = \Theta^x$, thus summing over all activity classes we get:

$$d_t I^x = -\mu_x I^x + \lambda_x m \left[p\Theta^x + (1-p) \sum_{y \neq x} \frac{N^x}{N - N^y} \Theta^y \right]. \tag{3.2}$$

In order to characterize the behavior of the number of infected at such early times, we can write, starting from Eq. 3.1 the equation for each auxiliary function Θ^x. In particular, we can multiply both sides of Eq. 3.1 for a and integrate over all classes of activity. Doing so, we obtain:

$$d_t \Theta^x = -\mu_x \Theta^x + \lambda_x m \left[p\Theta^x \int da \frac{a N_a^x}{N^x} + (1-p) \sum_{y \neq x} \frac{N^x}{N - N^y} \Theta^y \int da \frac{a N_a^x}{N^x} \right]. \tag{3.3}$$

where we have multiply and divided the third term for N^x. We can now define $F_x(a) = \frac{N_a^x}{N^x}$ as the distribution of activities in the category x, and thus $\int da \frac{a N_a^x}{N^x} = \int da a F_x(a) = \langle a \rangle_x$ is the average activity in the category. Finally, we let's define $c_{x,y} = \frac{N^x}{N - N^y}$ which is acts as the mixing probability between categorie. In these settings we get:

$$d_t \Theta^x = -\mu_x \Theta^x + \lambda_x m \langle a \rangle_x \left[p\Theta^x + (1-p) \sum_{y \neq x} c_{x,y} \Theta^y \right]. \tag{3.4}$$

Thus we have a system of differential equations made of $2Q$ equations. In particular, we have two equations for each x in the form:

$$\begin{aligned} d_t I^x &= -\mu_x I^x + \lambda_x m \left[p\Theta^x + (1-p) \sum_{y \neq x} c_{x,y} \Theta^y \right] = g^x. \\ d_t \Theta^x &= -\mu_x \Theta^x + \lambda_x m \langle a \rangle_x \left[p\Theta^x + (1-p) \sum_{y \neq x} c_{x,y} \Theta^y \right] = h^x. \end{aligned} \quad (3.5)$$

The conditions for the spreading can be identified by studying the eigenvalues of the Jacobian matrix of such system. The Jacobian can be written as follows:

$$J = \begin{bmatrix} \frac{\partial g^1}{\partial I^1} & \frac{\partial g^1}{\partial I^2} & \cdots & \frac{\partial g^1}{\partial I^Q} & \frac{\partial g^1}{\partial \Theta^1} & \frac{\partial g^1}{\partial \Theta^2} & \cdots & \frac{\partial g^1}{\partial \Theta^Q} \\ \frac{\partial g^2}{\partial I^1} & \frac{\partial g^2}{\partial I^2} & \cdots & \frac{\partial g^2}{\partial I^Q} & \frac{\partial g^2}{\partial \Theta^1} & \frac{\partial g^2}{\partial \Theta^2} & \cdots & \frac{\partial g^2}{\partial \Theta^Q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial g^Q}{\partial I^1} & \frac{\partial g^Q}{\partial I^2} & \cdots & \frac{\partial g^Q}{\partial I^Q} & \frac{\partial g^Q}{\partial \Theta^1} & \frac{\partial g^Q}{\partial \Theta^2} & \cdots & \frac{\partial g^Q}{\partial \Theta^Q} \\ \frac{\partial h^1}{\partial I^1} & \frac{\partial h^1}{\partial I^2} & \cdots & \frac{\partial h^1}{\partial I^Q} & \frac{\partial h^1}{\partial \Theta^1} & \frac{\partial h^1}{\partial \Theta^2} & \cdots & \frac{\partial h^1}{\partial \Theta^Q} \\ \frac{\partial h^2}{\partial I^1} & \frac{\partial h^2}{\partial I^2} & \cdots & \frac{\partial h^2}{\partial I^Q} & \frac{\partial h^2}{\partial \Theta^1} & \frac{\partial h^2}{\partial \Theta^2} & \cdots & \frac{\partial h^2}{\partial \Theta^Q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial h^Q}{\partial I^1} & \frac{\partial h^Q}{\partial I^2} & \cdots & \frac{\partial h^Q}{\partial I^Q} & \frac{\partial h^Q}{\partial \Theta^1} & \frac{\partial h^Q}{\partial \Theta^2} & \cdots & \frac{\partial h^Q}{\partial \Theta^Q} \end{bmatrix} \quad (3.6)$$

Substituting the general terms with the actual partial derivatives we get:

$$J = \begin{bmatrix} -\mu_1 & 0 & \dots & 0 & p\lambda_1 m & (1-p)\lambda_1 m c_{1,2} & \dots & (1-p)\lambda_1 m c_{1,Q} \\ 0 & -\mu_2 & \dots & 0 & (1-p)\lambda_2 m c_{2,1} & p\lambda_2 m & \dots & (1-p)\lambda_2 m c_{2,Q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & -\mu_Q & (1-p)\lambda_2 m c_{Q,1} & (1-p)\lambda_2 m c_{Q,2} & \dots & p\lambda_Q m \\ 0 & 0 & \dots & 0 & -\mu_1 + p\beta_1 & (1-p)\beta_1 c_{1,2} & \dots & (1-p)\beta_1 c_{1,Q} \\ 0 & 0 & \dots & 0 & (1-p)\beta_2 c_{2,1} & -\mu_2 + p\beta_2 & \dots & (1-p)\beta_2 c_{2,Q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & (1-p)\beta_Q c_{Q,1} & (1-p)\beta_2 c_{Q,2} & \dots & -\mu_Q + p\beta_Q \end{bmatrix} \quad (3.7)$$

where we defined $\beta_x = m\langle a \rangle_x \lambda_x$. It is important to notice the peculiarities of the Jacobian. The first $Q \times Q$ block made of the partial derivatives of the g^x functions in the various I^x is a diagonal block that features the recovery rates of each category. The second block on the bottom left side is a $Q \times Q$ block of all zeros. Indeed the variables I^x do not appear in the h^x equations. The adjacent block on the right, features in the diagonal the same function $-\mu_x + p\beta_x$. Due these properties, Q eigenvalues are negative and equal to the negative of each recovery rate. The largest eigenvalue instead can be written as

$$\Lambda_{max} = -\sum_x \mu_x + p \sum_x \beta_x + \Xi \quad (3.8)$$

where Ξ is an algebraic term function of all the β_x, μ_x and $c_{x,y}$. We focus on Λ_{max} because the virus will be able to spread if and only if the largest eigenvalue is larger than zero. From this observation we obtain the conditions spreading:

$$R_0 = \frac{p\sum_x \beta_x + \Xi}{\sum_x \mu_x} > 1 \tag{3.9}$$

where R_0 is the reproductive number defined as the number of infected nodes generated by an initial seed in a fully susceptible population. It is important to mention that for any number of categories Ξ has an analytical expression. However, since it derives from the characteristic equation of the Jacobian matrix, Ξ gets more and more complicated as the dimensionality of the matrix increases. Generally speaking for Q categories Ξ is a polynomial of order Q in all variables.

3.3.1 Q=1

In case of single category the expression of R_0 becomes:

$$R_0 = \frac{\beta}{\mu} \tag{3.10}$$

In fact, in this limit $p = 1$ and the Jacobian matrix reduces to

$$J = \begin{bmatrix} -\mu & 0 \\ 0 & -\mu + \beta \end{bmatrix} \tag{3.11}$$

The two eigenvalues are $-\mu$ and $-\mu + \beta$. Thus the disease will be able to spread only if $\beta > \mu$.

3.3.2 Q=2

In the case of two categories, $Q = 2$, the Jacobian becomes:

$$J = \begin{bmatrix} -\mu_1 & 0 & p\lambda_1 m & (1-p)\lambda_1 m c_{1,2} \\ 0 & -\mu_2 & (1-p)\lambda_2 m c_{2,1} & p\lambda_2 m \\ 0 & 0 & -\mu_1 + p\beta_1 & (1-p)\beta_1 c_{1,2} \\ 0 & 0 & (1-p)\beta_2 c_{2,1} & -\mu_2 + p\beta_2 \end{bmatrix} \tag{3.12}$$

In these settings we have:

$$\Xi^2 = (\mu_1 - \mu_2)^2 + p^2(\beta_1 - \beta_2)^2 + 2p(\mu_2 - \mu_1)(\beta_1 - \beta_2) + 4\beta_1\beta_2 c_{1,2} c_{2,1}(p-1)^2 \tag{3.13}$$

It is important to notice how with two categories, independently of their sizes $c_{1,2} = c_{2,1} = 1$. In fact, the two sizes are constrained by $N = N^1 + N^2$. Thus

we have:

$$c_{1,2} = \frac{N^1}{N - N^2} = \frac{N^1}{N - N + N^1} = c_{2,1} = \frac{N^2}{N - N^1} = \frac{N^2}{N - N + N^2} = 1 \tag{3.14}$$

The expression of Ξ reduces to:

$$\Xi^2 = (\mu_1 - \mu_2)^2 + p^2(\beta_1 + \beta_2)^2 + 2p(\mu_2 - \mu_1)(\beta_1 - \beta_2) + 4\beta_1\beta_2(1 - 2p) \tag{3.15}$$

In order to develop a better understanding of the results, let's first consider the case in which $\mu_1 = \mu_2 = \mu$. The expression of R_0 becomes:

$$R_0 = \frac{p(\beta_1 + \beta_2) + \sqrt{p^2(\beta_1 + \beta_2)^2 + 4\beta_1\beta_2(1 - 2p)}}{2\mu} \tag{3.16}$$

In the limit $p = 0$, nodes in each category will connect just with nodes in the other. The expression of R_0 becomes: $R_0 = \sqrt{\beta_1\beta_2}/\mu$. In the opposite limit, $p = 1$, nodes in the two categories are separated. Thus we have two independent conditions that have the same mathematical form we encountered for $Q = 1$. In fact, we have $R_0^1 = \beta_1/\mu$ and $R_0^2 = \beta_2/\mu$. The virus will be able to spread in the system in case either of the R_0^x are larger than one. Of course, in case both are larger than one each group will experience the virus. What happens in case $0 < p < 1$? It is interesting to notice how the value of R_0 for a general p is bounded by the R_0^x of the two categories taken in isolation: $\min_x R_0^x \leq R_0(p) \leq \max_x R_0^x$. Before the mathematical proof, let us try to develop the intuition behind. Suppose that $\beta_1 > \beta_2$. Any value of $p < 1$, will reduce the spreading power of nodes in the first category. In fact, nodes in category one will be connected to some nodes in category two that are less gullible, or less active, or create a smaller number of connection (remember that $\beta_x = m\langle a\rangle_x\lambda_x$). Conversely, nodes in category two, will get in contact with nodes that increase the spreading potential of the virus. In order to prove this, let us consider the case $\beta_1 > \beta_2$. We have to show how $R_0^1 > R_0(p)$ and $R_0^2 < R_0(p)$. Let us consider the first condition:

$$\frac{\beta_1}{\mu} > \frac{p(\beta_1 + \beta_2) + \sqrt{p^2(\beta_1 + \beta_2)^2 + 4\beta_1\beta_2(1 - 2p)}}{2\mu}, \tag{3.17}$$

which is equivalent to:

$$\beta_1(2 - p) - p\beta_2 > \sqrt{p^2(\beta_1 + \beta_2)^2 + 4\beta_1\beta_2(1 - 2p)} \tag{3.18}$$

This condition is respected in case $\beta_1(2 - p) - p\beta_2 > 0$, $p^2(\beta_1 + \beta_2)^2 + 4\beta_1\beta_2(1 - 2p) > 0$ and $(\beta_1(2 - p) - p\beta_2)^2 > p^2(\beta_1 + \beta_2)^2 + 4\beta_1\beta_2(1 - 2p)$. The first condition implies $\beta_1 > \frac{p\beta_2}{2-p}$, which is always true since $\beta_1 > \beta_2$ was the initial assumption. Furthermore, it is easy to show that equation $p^2(\beta_1 + \beta_2)^2 + 4\beta_1\beta_2(1 - 2p) = 0$ as no solution in p, thus the condition is always respected.

Finally, the third condition implies

$$4\beta_1^2+p^2\beta_1^2-4\beta_1^2p+p^2\beta_2^2-2p(2-p)\beta_1\beta_2>p^2\beta_1^2+p^2\beta_2+2p^2\beta_1\beta_2+4\beta_1\beta_2-8p\beta_1\beta_2 \tag{3.19}$$

that reduces to $\beta_1 > \beta_2$. The three conditions prove Eq. 3.17 for all p. We have now to prove

$$\frac{\beta_2}{\mu}<\frac{p(\beta_1+\beta_2)+\sqrt{p^2(\beta_1+\beta_2)^2+4\beta_1\beta_2(1-2p)}}{2\mu}, \tag{3.20}$$

which is equivalent to:

$$\beta_2(2-p)-p\beta_1<\sqrt{p^2(\beta_1+\beta_2)^2+4\beta_1\beta_2(1-2p)} \tag{3.21}$$

This condition is respected in region in which $\beta_2(2-p)-p\beta_1 \geq 0$, $(\beta_2(2-p)-p\beta_1)^2 < p^2(\beta_1+\beta_2)^2+4\beta_1\beta_2(1-2p)$ and $p^2(\beta_1+\beta_2)^2+4\beta_1\beta_2(1-2p) \geq 0$, $\beta_2(2-p)-p\beta_1 < 0$. The first two conditions are respected when in the region $\frac{p\beta_1}{2-p} \leq \beta_2 < \beta_1$. The other two instead in the region $\beta_2 < \frac{p\beta_1}{2-p}$. Overall, Eq. 3.20 is valid in the union of these two that implies $\beta_2 < \beta_1$ which is exactly the initial assumption.

Let's consider now the general case in which also the two recovery rates are different. In the limit $p = 0$, we have $R_0 = \frac{\sqrt{(\mu_1-\mu_2)^2-4\beta_1\beta_2}}{\mu_1+\mu_2}$. In the opposite limit instead, $p = 1$, the two categories are independent thus we have two conditions as before: $R_0^1 = \beta_1/\mu_1$ and $R_0^2 = \beta_2/\mu_2$. It is interesting to notice how in case the two recovery rates are not the same, the phase space of the process becomes significantly more complex. In fact, differences in the rate at which nodes recovers might create interesting non-linear behaviors. In particular, consider a scenario in which the first category features a larger β_1 and μ_1 respect to the second. Thus, such nodes are more prone to infection but recover faster. In case $p < 1$, the coupling between the two categories might boost the spreading of the virus, since the node in category one are able to infect those in two which, although less prone to the disease stay infected for longer. For a given configuration of parameters (i.e. setting βs and μs) we can analytically determine the value of p above which this phenomenon is observed. In particular, let's assume that $\beta_1/\mu_1 < \beta_2/\mu_2$. Next, we need to compute the value of p (if any), for which $\beta_2/\mu_2 < R_0(p)$. This implies:

$$\frac{\beta_2}{\mu_2}<\frac{p(\beta_1+\beta_2)+\Xi}{\mu_1+\mu_2} \tag{3.22}$$

that can be written as:

$$\beta_2(\mu_1+\mu_2)-\mu_2p(\beta_1+\beta_2)<\mu_2\sqrt{(\mu_1-\mu_2)^2+p^2(\beta_1+\beta_2)^2+2p(\mu_2+\mu_1)(\beta_1-\beta_2)+4\beta_1\beta_2(1-2p)} \tag{3.23}$$

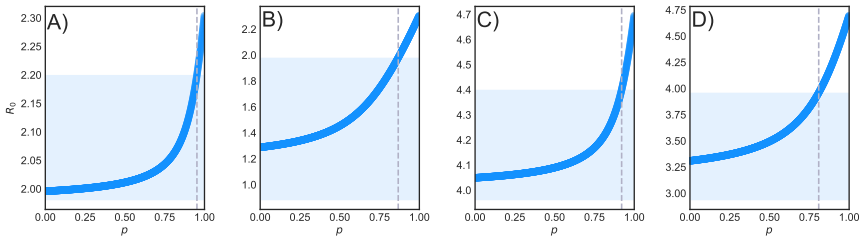


FIGURE 3.1: R_0 as function of p. The shaded area describe the region in which $\min_x \beta_x/\mu_x \leq R_0 \leq \max_x \beta_x/\mu_x$. The vertical line describe the value of p^* from conditions Eq. 3.24 and Eq. 3.25. In panels A-B we set $\mu_1 = 10^{-2}$, $\mu_2 = 5 \times 10^{-3}$, $m = 4$, $\lambda_1 = 0.9$,$\lambda_2 = 0.5$ (A) and $\lambda_2 = 0.2$ (B). In panels C-D we set $\mu_1 = 5 \times 10^{-3}$, $\mu_2 = 3 \times 10^{-3}$, $m = 4$, $\lambda_1 = 0.9$,$\lambda_2 = 0.6$ (C) and $\lambda_2 = 0.4$ (D).

It is important to notice how this inequality is at the first order in p. Indeed, all second order terms cancel out. The value of p that verifies the above inequality lays in the union of two systems of inequalities: i)$\beta_2(\mu_1+\mu_2) - \mu_2 p(\beta_1+\beta_2) < 0$ and the quantity inside the square root is larger equal than zero, ii) $\beta_2(\mu_1+\mu_2) - \mu_2 p(\beta_1+\beta_2) > 0$, and $(\beta_2(\mu_1+\mu_2) - \mu_2 p(\beta_1+\beta_2))^2 < \mu_2^2\Xi^2$. Extensive numerical computations show that the values inside the square roots are always positive. Furthermore, the first condition in the first system result in values of p always larger than one. Thus, the first system does not provide any physical ($p < 1$) condition. Conversely, the first condition in the second system implies $p < 1$ while the second:

$$p > p^* = \frac{\beta_2^2(\mu_2+\mu_1)^2 - \mu_2^2(\mu_1-\mu_2)^2 - 4\beta_1\beta_2\mu_2^2}{2\mu_2\beta_2(\mu_2+\mu_1)(\beta_1+\beta_2) + 2\mu_2^2(\mu_2-\mu_1)(\beta_1-\beta_2) - 8\beta_1\beta_2\mu_2^2}. \tag{3.24}$$

Thus, this is the only physical condition necessary to observe a reproductive number larger than in each category in isolation. Clearly, in the case $\beta_2/\mu_2 < \beta_1/\mu_1$ the condition above becomes:

$$p > p^* = \frac{\beta_1^2(\mu_2+\mu_1)^2 - \mu_1^2(\mu_1-\mu_2)^2 - 4\beta_1\beta_2\mu_1^2}{2\mu_1\beta_1(\mu_2+\mu_1)(\beta_1+\beta_2) + 2\mu_1^2(\mu_2-\mu_1)(\beta_1-\beta_2) - 8\beta_1\beta_2\mu_1^2}. \tag{3.25}$$

In Figure 3.1 we verify the above condition. In particular, we set the values of β_x and μ_x and plot R_0 from Eq. 3.9 as function of p. In particular, we consider that nodes are assigned to the categories randomly. The shaded area is the region where $\min_x \beta_x/\mu_x \leq R_0 \leq \max_x \beta_x/\mu_x$. The vertical line show the value of p^* determined from the condition derived above. It is clear how for a given setting, there might be a value of p above which the reproductive number gets indeed larger than the the R_0^x of each category in isolation.

It is important to stress how the region of the phase space in which we observe this phenomenon is generally speaking quite limited. In fact, it might happen only in case the category with the larger recovery rates has also the larger gullibility.

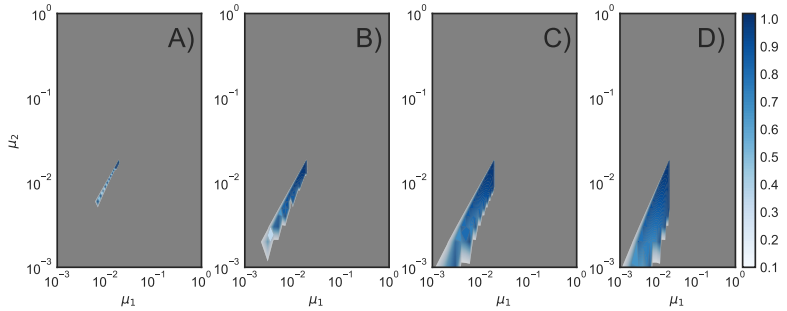


FIGURE 3.2: We show as function of μ_1 and μ_2 the region of parameters in which the reproductive number of system is larger than the correspondent values computed in each category in isolation. The colors refer to the value of p (calculated from Eq. 3.24 and Eq. 3.25) above which this phenomenon is observed. We set $\lambda_1 = 0.9$, $\lambda_2 = 0.8$ (A), $\lambda_2 = 0.6$ (B), $\lambda_2 = 0.4$ (C), $\lambda_2 = 0.2$ (D)

In Figure 3.2 we show as contour plots the region of parameters where the reproductive number of the system is larger than that correspondent value in the two categories in isolation. In particular, we set $\lambda_1 = 0.9$, $\lambda_2 = 0.8$ (A), $\lambda_2 = 0.6$ (B), $\lambda_2 = 0.4$ (C), $\lambda_2 = 0.2$ (D) and show as function of μ_1 and μ_2 the value of p^*. It is clear this region increases as the difference between the two gullibilities increases. It is important to notice how the expression for p^* is perfectly in line with the case in which $\mu_1 = \mu_2$. Indeed, in this limit we get $p^* > 1$ which implies, as expected, that the necessary condition to have a reproductive number larger than in each category in isolation is to have different recovery rates.

3.3.3 Q>2

As mentioned above, in the most general case of Q categories, the expression of Ξ, becomes quite complex. However, its expression is set unequivocally by the characteristic equation of the Jacobian matrix and can be easily obtained with any programming language that allows symbolic computations such as Mathematica. The problem can be significantly simplified in case some of the variables describing the system are set. For example in the case of $Q = 3$ one might wonder what is the critical value of λ_1 in a system in which β_y (with $y = [2,3]$) and μ_y with ($y = [1,2,3]$) are set. In these settings, as shown later on, it is extremely easy to compute the largest eigenvalue of the Jacobian for the particular system under consideration as function of λ_1.

3.3.4 $\tau > 1$

We now turn the attention to the second type of virus that is able to access not only the connections establish at time t but also those in previous τ time steps. In order to characterize the conditions for the spreading in this case, let us first understand how many people del virus will be able to reach from each node of

activity a. This number is equal to the out-degree of those nodes. In the case considered in the previous sections $\tau = 1$, thus the virus was able to reach only the nodes contacted by each active and infected node within the time-step t. By construction, the out-degree of such nodes is $k^{out}(a) = ma$, since their are active with probability a and when active they create m random connections. What about for $\tau = 2$?Active nodes at time t might either have m connections or $2m$. The first group describes nodes that were not active at time $t-1$ but they were active at time t. The second group instead describe nodes that were active in both time steps. Thus:

$$k^{out}(a) = (1-a)am + 2ma^2 = m(a+a^2). \tag{3.26}$$

In fact, nodes of activity a are not active with probability $1-a$ and are active two times in a row with probability a^2 (since the events are independent). The same reasoning applies for $\tau = 3$. Here we could have three groups having either degree m, $2m$, and $3m$. As before, the first group describes nodes that were not active at time $t-2$ and $t-1$ but they were active at time t. The second group instead accounts for all the nodes that were active two times. Finally the third those that were active three times. Thus we get:

$$k^{out}(a) = ma(1-a)^2 + 4ma^2(1-a) + 3ma^3 = m(a+2a^2) \tag{3.27}$$

In the case $\tau = 4$ instead we have:

$$k^{out}(a) = ma(1-a)^3 + 6ma^2(1-a)^2 + 9ma^3(1-a) + 4ma^4 = m(a+3a^2) \tag{3.28}$$

It is clear that the structure of the out-degree for a general τ can be written as:

$$k^{out}(a) = m\left[a + (\tau-1)a^2\right]. \tag{3.29}$$

Within a mean-field approximation, we can approximate the process assuming that the virus will try to infected $k^{out}(a)$ other nodes as for the case $\tau = 1$. This is an approximation because each active node, at time t, as a quenched list of contacts, those established in the time-steps before. The node will not re-draw them ex novo as in the case $\tau = 1$. Thus, we can expect the approximation to be closer to the actual process for small values of τ. Within such approach, the structure of the equation is the same as those above, the only different is in the βs since we will have $m\langle a\rangle_x \to m\left[\langle a\rangle_x + (\tau-1)\langle a\rangle_x^2\right]$.

3.4 Numerical simulations

In this section, we will test the analytical treatment discussed above and characterise in more details the phase space of the model and its dynamics. For simplicity, let's first tackle the case of two categories ($Q = 2$). Furthermore, let's consider two main approaches to assign nodes to categories. The first is at random, the second is instead in decreasing order to activity. In particular, we order activity in decreasing order and then assign the first gN nodes to the first category and

the remaining to the second. Thus $\langle a \rangle_1 = \int_{a_c}^{1} daaF(a)$ and $\langle a \rangle_2 = \int_{\epsilon}^{a_c} daaF(a)$ and a_c is determined in such a way that the fraction of nodes in the first class is g. This can be easily done imposing:

$$\int_{a_c}^{1} F(a)da = g. \tag{3.30}$$

Since $F(a) = \frac{1-\alpha}{1-\epsilon^{1-\alpha}} a^{-\alpha}$ we get:

$$a_c = \left[1 - g(1-\epsilon^{1-\alpha})\right]^{\frac{1}{1-\alpha}} \tag{3.31}$$

It is important to notice that in Eq. 3.9 the expression of $\langle a \rangle_x$ in the two assignment scenarios is slightly different. In particular we defined $\langle a \rangle_x = \int daF_x(a)a = \int da \frac{N_a^x}{N^x} a$. In case nodes are assigned randomly to the two categories we have that $F_x(a) \sim F(a)$ since $N_a^x = N_a/g$ and $N^x = N/g$ (where g is the fraction of node in the general category x in this case). Thus, $\langle a \rangle_x = \langle a \rangle$ for the two categories. In case instead nodes are assigned in decreasing order of activity $\langle a \rangle_x = \langle a \rangle / g$. In fact, in this limit $N_a^x = N_a$ (since nodes are assigned to categories as function of their activity) but $N^x = gN$.

In Fig. 3.3-A-C, we compare analytical predictions with numerical simulations in the case in which the recovery rates of the two categories are the same. We set $\lambda_2 = 0.3$ and use Eq. 3.16 to estimate the critical value of λ_1 for which $R_0 \equiv 1$. On the y-axis we plot the lifetime of the process defined as the time that the virus needs either to die out or to reach a fraction Υ of the population [Boguña, Castellano, and Pastor-Satorras, 2013]. The lifetime acts as the susceptibility of a second order phase transition and allows a precise numerical estimation of the threshold of SIS processes [Boguña, Castellano, and Pastor-Satorras, 2013]. In panels A-B we consider a scenario in which nodes are assigned randomly to one of the two categories. Thus the average activity in the two is the same and set $p = 0.9$ and $p = 0.4$ respectively. The analytical value of the threshold (vertical solid line) perfectly matches the numerical estimation. For $p = 0.9$ the threshold is smaller than for $p = 0.4$ and closer to the threshold of a system with a single category (dashed lines). For smaller values of homophily, instead, the critical conditions are driven by the interplay between the activation rates and gullibility of the two categories. Panels D-E show the analytical value of R_0 as a function of λ_1 and λ_2 for the two values of p. The grey regions are sub-critical, i.e., the virus is not able to spread. Since the average activity in the two categories is the same, the two plots are symmetric. Interestingly, the region where the virus is able to spread is larger for large values of p. This is due to the fact that in these settings the virus will spread if above the threshold in at least one category independently of the other. In the opposite limit, on the contrary, the two categories get intertwined and a small value of the infection probability in one category should be associated to a progressively large value in the other.

In panels C-F we consider that the first category contains a fraction g of nodes selected in decreasing order of activity. Thus, this category contains the gN most

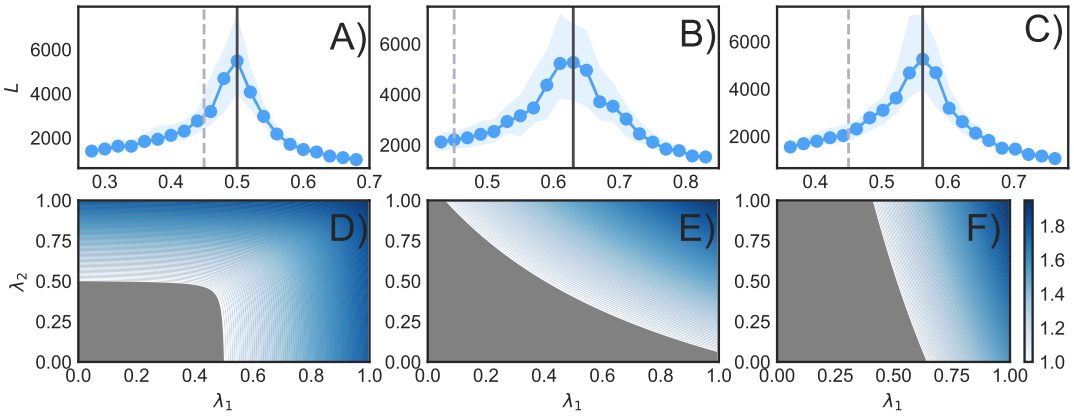


FIGURE 3.3: Lifetime of the SIS process (A-C) and contour plot of R_0 (D-F). In A-B-D-E nodes are randomly assigned to two categories, in C-F instead in decreasing order of activity. We set $p = 0.9$ (A-D), $p = 0.4$ (B-C-E-F). In A-C we fix $N = 2 \times 10^5$, $m = 4$, $\alpha = -2.1$, $\mu_1 = \mu_2 = 10^{-2}$, $\lambda_2 = 0.3$, $Y = 0.3$, and 0.5% of random initial seeds. We plot the median and 50% confidence intervals in 10^2 simulations per point. The solid lines come from Eq. 3.9, and the dashed lines are the analytical threshold in case of a single category. In the contour plot we set $\mu_1 = \mu_2 = 10^{-1}$.

active nodes, while the other the $(1-g)N$ least active. To compare with panel B, we set $g = 0.5$ and $p = 0.4$. First, the analytical threshold nicely matches the numerical simulations. Second, although the other parameters are the same used in panel B, the critical value of the gullibility of the first class is smaller. Thus, correlations between activity and gullibility facilitate the spreading. This is confirmed in panel F where the active phase space features a region in which the spreading is completely dominated by the category of most active nodes. Overall, all the plots show the importance of distinguishing nodes according to their gullibility. Indeed, neglecting the presence of different classes of users might induce a strong misrepresentation of the virus propagation (dashed lines).

In Figure 3.4 we consider the general case of different recovery rates. In particular, we set $\mu_1 = 10^{-2}$, $\mu_2 = 10^{-1}$, $\lambda_2 = 0.3$ and $m = 4$. In panels A-B-D-E we consider random assignment of nodes to categories. In C-F we consider the correlation between activity and category. We assign to category one to most active nodes. Also, in panels B-C-E-F we considered $p = 0.6$ while in panel A-D we set $p = 0.9$. Overall, the figure confirms the validity of the theoretical approach and highlights one more time the effects of correlations between category assignment and activity that reduce the non-active phase space (see panel F). Furthermore, it is important to notice how the critical value in case of a single category with a recovery rate average of the two here would be $\lambda_1^c = 2.5$ (not shown in the figure) which implies that the virus would not be able to spread since all the gullibilities should be smaller or equal to 1. This confirms the importance of accounting for the presence of different categories of users in order to correctly capture the spreading power of the virus.

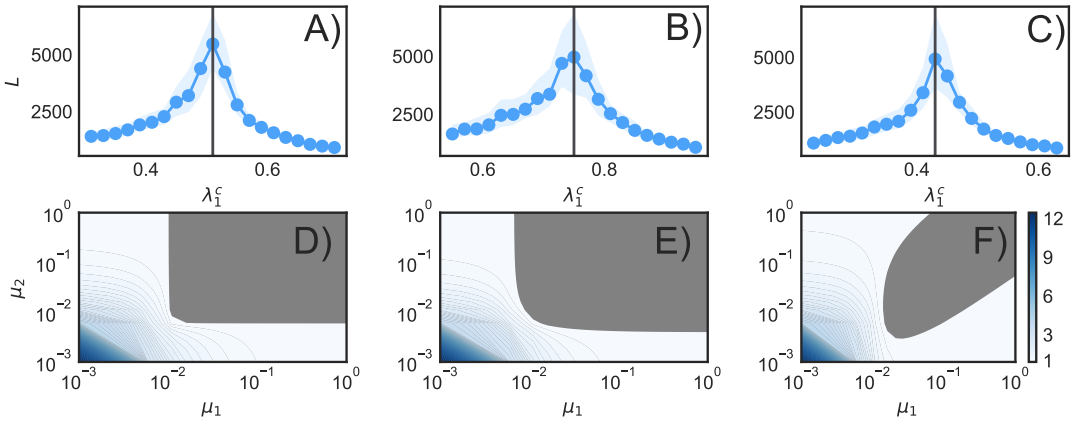


FIGURE 3.4: Lifetime of the SIS process (A-C) and contour plot of R_0 (D-F). In A-B-D-E nodes are randomly assigned to two categories, in C-F instead in decreasing order of activity. We set $p = 0.9$ (A-D), $p = 0.6$ (B-C-E-F). In A-C we fix $N = 2 \times 10^5$, $m = 4$, $\alpha = -2.1$, $\mu_1 = 10^{-2}$, $\mu_2 = 10^{-1}$, $\lambda_2 = 0.3$, $Y = 0.3$, and 0.5% of random initial seeds. We plot the median and 50% confidence intervals in 10^2 simulations per point. The solid lines come from Eq. 3.9, and the dashed lines are the analytical threshold in case of a single category. In the contour plot we set $\lambda_1 = 0.51$ and $\lambda_2 = 0.3$.

In Figure 3.5 we test the sensitivity to the parameter m. Respect to the previous plots, here, we fix $m = 6$ keeping all the other parameters the same as in the Figure 3.4. The analytical solutions one more time match the numerical simulations and the contour plots confirm the picture discussed in the main text and all the other similar plots.

In Figure 3.6 we test the sensitivity to the exponent of the activity distribution. In all the other plots we set $\alpha = -2.1$, here instead we consider $\alpha = -2.5$. We considered a scenario in which the recovery rates of the two categories is the same, set $\lambda_2 = 0.4$, $m = 6$ and consider two different values of p. As clear from the figure, also in this case the analytical estimation matches the numerical simulations. Furthermore, it is interesting to notice how, in case of faster decay of the activity distribution (i.e. smaller value of the exponent α), the threshold of the correlated case (panel C-F) is closer to the scenario of a single category (dashed line). Indeed, the average activity of the more active category gets closer to the average activity of the whole network.

$Q = 3$

Here we consider the case of three categories. For simplicity let's consider nodes are assigned to the categories at random and that categories have the same size $N^x = N/3$. Also, let's us set the values of β_x with $x = [2,3]$, μ_x with $x = [1,2,3]$, $m = 4$, and assume that links are created randomly between categories thus $p = 1/3$. In particular, if we set $\beta_2 = \beta_3 = 0.3$, $\mu_1 = \mu_2 = \mu_3 = 0.01$,

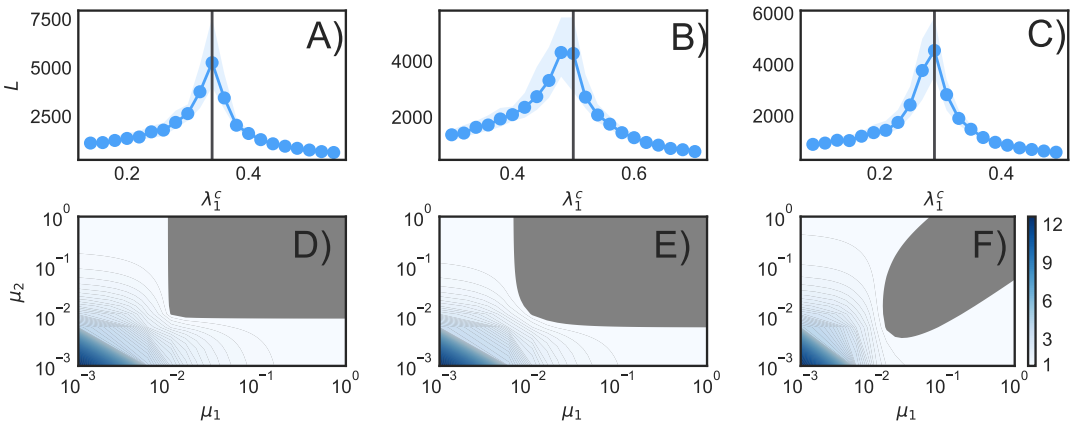


FIGURE 3.5: Lifetime of the SIS process (A-C) and contour plot of R_0 (D-F). In A-B-D-E nodes are randomly assigned to two categories, in C-F instead in decreasing order of activity. We set $p = 0.9$ (A-D), $p = 0.6$ (B-C-E-F). In A-C we fix $N = 2 \times 10^5$, $m = 6$, $\alpha = -2.1$, $\mu_1 = 10^{-2}$, $\mu_2 = 10^{-1}$, $\lambda_2 = 0.3$, $Y = 0.3$, and 0.5% of random initial seeds. We plot the median and 50% confidence intervals in 10^2 simulations per point. The solid lines come from Eq. 3.9, and the dashed lines are the analytical threshold in case of a single category. In the contour plot we set $\lambda_1 = 0.34$ and $\lambda_2 = 0.3$.

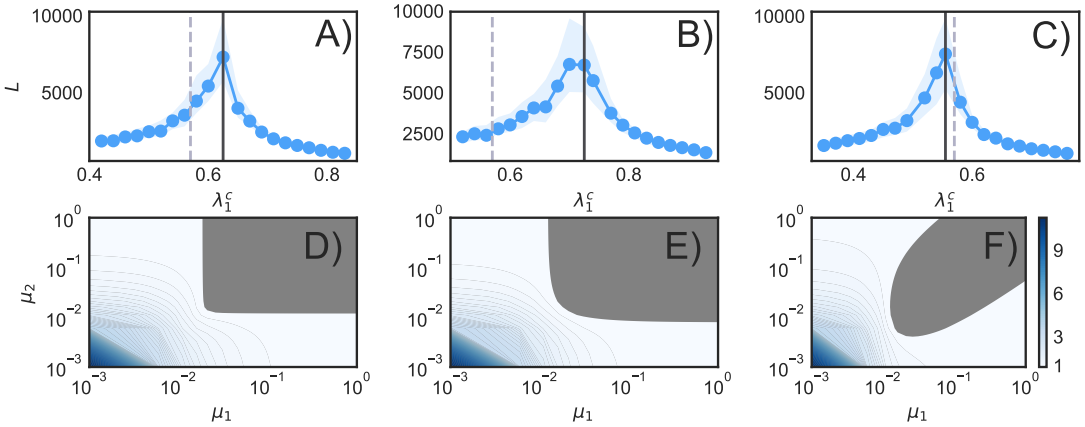


FIGURE 3.6: Lifetime of the SIS process (A-C) and contour plot of R_0 (D-F). In A-B-D-E nodes are randomly assigned to two categories, in C-F instead in decreasing order of activity. We set $p = 0.9$ (A-D), $p = 0.6$ (B-C-E-F). In A-C we fix $N = 2 \times 10^5$, $m = 6$, $\alpha = -2.5$, $\mu_1 = 10^{-2}$, $\mu_2 = 10^{-2}$, $\lambda_2 = 0.4$, $Y = 0.3$, and 0.5% of random initial seeds. We plot the median and 50% confidence intervals in 10^2 simulations per point. The solid lines come from Eq. 3.9, and the dashed lines are the analytical threshold in case of a single category. In the contour plot we set $\lambda_1 = 0.625$ and $\lambda_2 = 0.5$.

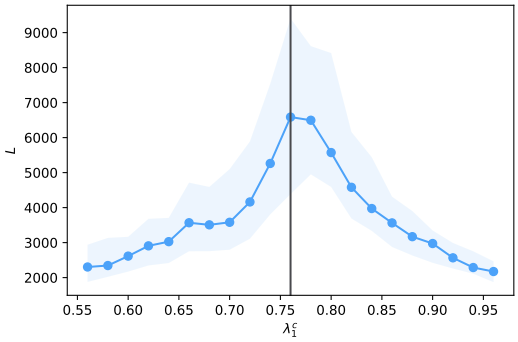


FIGURE 3.7: We show the lifetime of the SIS process in case of $Q = 3$ as function of λ_1. The vertical line describes the analytical estimation of its critical value. In the simulation we set $\beta_2 = \beta_3 = 0.3$, $\mu_1 = \mu_2 = \mu_3 = 0.01$, $N = 3 \times 10^5$, $m = 4$, $\alpha = -2.1$, $\epsilon = 10^{-3}$ and run 10^2 simulations for each data point. We show the 50% confidence intervals in the shaded area and the median with the dots.

we can use Eq. 3.7 to obtain the critical value of λ_1. In particular, the general expression of the Jacobian is:

$$J = \begin{bmatrix} -\mu_1 & 0 & 0 & p\lambda_1 m & (1-p)\lambda_1 m c_{1,2} & (1-p)\lambda_1 m c_{1,3} \\ 0 & -\mu_2 & 0 & (1-p)\lambda_2 m c_{2,1} & p\lambda_2 m & (1-p)\lambda_2 m c_{2,3} \\ 0 & 0 & -\mu_3 & (1-p)\lambda_3 m c_{3,1} & (1-p)\lambda_3 m c_{3,2} & p\lambda_3 m \\ 0 & 0 & 0 & -\mu_1 + p\beta_1 & (1-p)\beta_1 c_{1,2} & (1-p)\beta_1 c_{1,3} \\ 0 & 0 & 0 & (1-p)\beta_2 c_{2,1} & -\mu_2 + p\beta_2 & (1-p)\beta_2 c_{3,1} \\ 0 & 0 & 0 & (1-p)\beta_3 c_{3,1} & (1-p)\beta_2 c_{3,2} & -\mu_3 + p\beta_3 \end{bmatrix} \tag{3.32}$$

Since the categories have the same size:

$$c_{x,y} = \frac{N^x}{N - N^y} = \frac{N}{3}\frac{1}{N - \frac{N}{3}} = \frac{1}{2} \tag{3.33}$$

Plugging all the values and solving for λ_1 we obtain:

$$\lambda_1^c = \frac{42}{55} \tag{3.34}$$

In Figure 3.7 we show the comparison between the analytical prediction and the numerical simulations which perfectly matches.

Let's turn our attention to a second type of virus able to access also past contacts of infected users within a time window τ. As before, the virus propagates via active infected nodes, but at each time t active users might infect their contacts in a time-window $(t - \tau, t]$. Within a mean-field approximation, we can adopt the same equations described above and change the probability that a node in each activity class receives a message by active and infected nodes. As mentioned above, the out-degree of each active node is not m, but a function of τ:

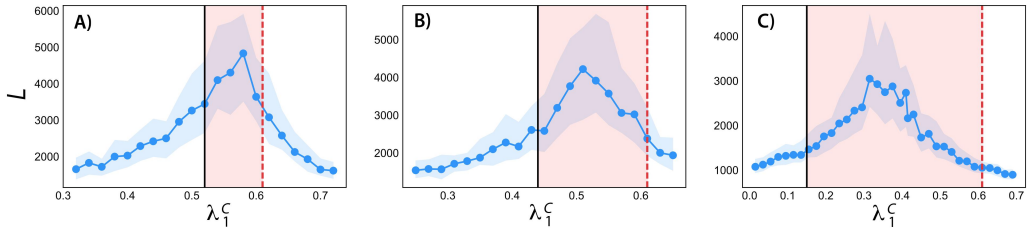


FIGURE 3.8: Lifetime of the SIS process for $\tau = 2, 3, 10$ (A,B,C) for two categories to which nodes are assigned randomly. Simulations are done setting $N = 2 \times 10^5$, $m = 4$, $\alpha = -2.1$, $Y = 0.3$, $\mu = 10^{-2}$, $\lambda_2 = 0.3$, $p = 0.5$, and 0.5% random initial seeds. We plot the median and 50% confidence intervals in 10^2 simulations per point.

$k^{out}(a) = m\left[a + (\tau - 1)a^2\right]$. To grasp the derivation, consider the simplest scenario in which $\tau = 2$. In this case, active nodes might have either m or $2m$ contacts in two time steps. The first class describes nodes that are active at time t but were not active at time $t-1$; whereas the second, nodes that were active in both time steps. Thus the out-degree of these nodes, on average, is $k^{out}(a) = ma(1-a) + 2ma^2$. The condition for the spreading has the same structure of Eq. 3.9 where, however, the value of βs are changed with the following transformation $m \to m\left[\langle a\rangle + (\tau - 1)\langle a^2\rangle\right]$. Thus, the larger the visibility of past connections, from the virus point of view, the larger R_0. Intuitively this is due to the fact that the virus, for large values of τ, is able to access more contacts, which results in a larger spreading potential. This observation nicely shows how neglecting the temporal nature of connectivity patterns in favor of static (or time integrated) approximations might lead to a poor description of the propagation of viruses that do not have access to contacts lists or past connections. In Fig. 3.8 we show the comparison between analytical (solid lines) and numerical values of the threshold for different values of τ. To isolate the effect of τ we considered two categories, a single recovery rate, and set $p = 0.5$. The analytical value is a good approximation only for small values of τ. The mean-field approximation becomes less accurate as more connections from past time-steps are kept in memory. Thus, the analytical estimation provides only a lower bound, which together with the solution for $\tau = 1$ (dashed lines) −that constitutes an upper bound−, marks the region containing the epidemic threshold (red regions). In other words, for a general value of τ, the threshold will be lower than the analytical value computed for $\tau = 1$, and larger than the corresponding value computed at τ

3.5 Summary

Overall our results highlight how the spreading of computer viruses based on social engineering is critically affected by the temporal nature of our interactions and different susceptibilities to cyber threats. Our findings show that networks' dynamics and their interplay with the characteristics of users have to be considered in order to avoid misrepresentation of the spreading power of computer viruses in

social networks. We have also quantified the extent to which the previous mismatch is important for three plausible scenarios. We, however, note that we have studied a simple network model that neglects a range of properties of real social networks such as the presence of weak and strong ties, high order correlations, and community structures. The study of the impact of these features on the unfolding of computer viruses calls for additional research.

Chapter 4

Experimental Platform

This chapter covers the new experimental platform we have developed to facilitate studying the propagation of threats, such as semantic social engineering, in social networks. The platform has been developed largely from scratch, as it is the first of its kind. An exception is the network generation, which is based on NetworkX. Here we introduce the software design, the development process, the functionality and the platform's components.

4.1 Software Methodology

In approaching the problem of designing this new platform from scratch, we have considered several software engineering methodologies, including Agile development, waterfall model, rapid prototyping and spiral development among many others and permutations thereof [Collier, 2012; Awad, 2005; Vijayasarathy and Butler, 2015; Despa, 2014; Al Ahmar, 2010; Connors, 1992; Hijazi, Khdour, and Alarabeyyat, 2012; Boehm, 1988; Devadiga, 2017]. Each methodology has a different life cycle, but the most common phases are planning, analysis, design, development, testing and integration and maintenance of the software product [Ali, 2017; Faizi and S. Rahman, 2019; Tiky, 2016].

Online Social Networks are web based applications, which given their ubiquitous nature of being accessible via any internet enabled device have to be robust and adaptive to needs of the users. Since these can change quite rapidly, Agile software development is common practice for web development [Sarkar, 2018; Ruby, Copeland, and Thomas, 2020; Cortiñas et al., 2017]. It focuses on an iterative process during its development stage, meaning that the developers often review what they have built in incremental stages, and validate their work with the client [Beck et al., 2016; Alliance, 2017]. This methodology is popular when clear requirements are not defined, as it focuses more on the development rather than the needs, which might not be known at the start of the project.

A slightly different approach is Rapid Prototyping, which also aims to produce number of software iterations quickly, but instead of focusing on the development stage [Conway, M. Koch, and Salinas, 2019; Devadiga, 2017; Baydogan, 2008; Kelly and Neetz, 1988], it focuses on the design and planning stages. Unlike Agile methodology, which has a baseline idea of what software product has to be built, in Rapid Prototyping we can blend Agile into enterprise software development. The Rapid Prototyping methodology allows for a quick creation of prototypes,

which are built with a small set of working features, and can be demonstrated regularly to the stakeholders for feedback. Prototypes can be easily discarded, and rebuilt into a new version, as there is no specific requirements set for the software [Suranto, 2015]. The development focus is set on the user evaluation and refining the prototype recurrently, until the acceptance of the prototype, which is then moved forward to build a full version of the software.

Due to the nature of our research, we deemed the prototyping approach to be the most suitable. It allows to recurrently come up with a new design which would then be reviewed and revised, as in the phases of the Rapid Prototyping model seen in Fig 4.1. Specifically, aiming to separate the network effect and the bias of the content present on OSNs, we have proposed two separate versions of the platform.

The first version of our platform has featureless messages, i.e. messages which do not have any content or information beside username. This is because we want to remove bias linked with personalising a message, as content which can appear from a trustworthy source, or what platform is being targeted e.g. the phishing attack is carried out via email or Facebook has an impact on the likelihood of a successful attack [Alsharnouby, Alaca, and Chiasson, 2015; Benenson, Gassmann, and Landwirth, 2017; Colwill, 2009]. The second version of the platform would allow to share common content, such as text, images, videos from a library that we have built.

4.1.1 Software Requirements

Having a web based online social networking platform as a baseline, we have established some of the requirements and functionality that is common in the most popular social networks. For that we have created a specifications requirement documentation below, this is a planned blueprint for a software project, prior to its commencement.

Scope

The application is a custom built social network with an emphasis on studying the sharing of malicious content in a controlled research environment. The main feature of the tool is the ability to track users' behaviour and customise the depth of content and functionality available to the user.

The web app allows the users to communicate with their connected friends and send messages (or tokens) to each other. The platform has a user-friendly interface, following the standards used by OSNs, that will allow for a familiar design.

Environments

Operating Environments for the web application:

- AMPP (Apache, MySQL, PHP, Python) Server
- Client/server system

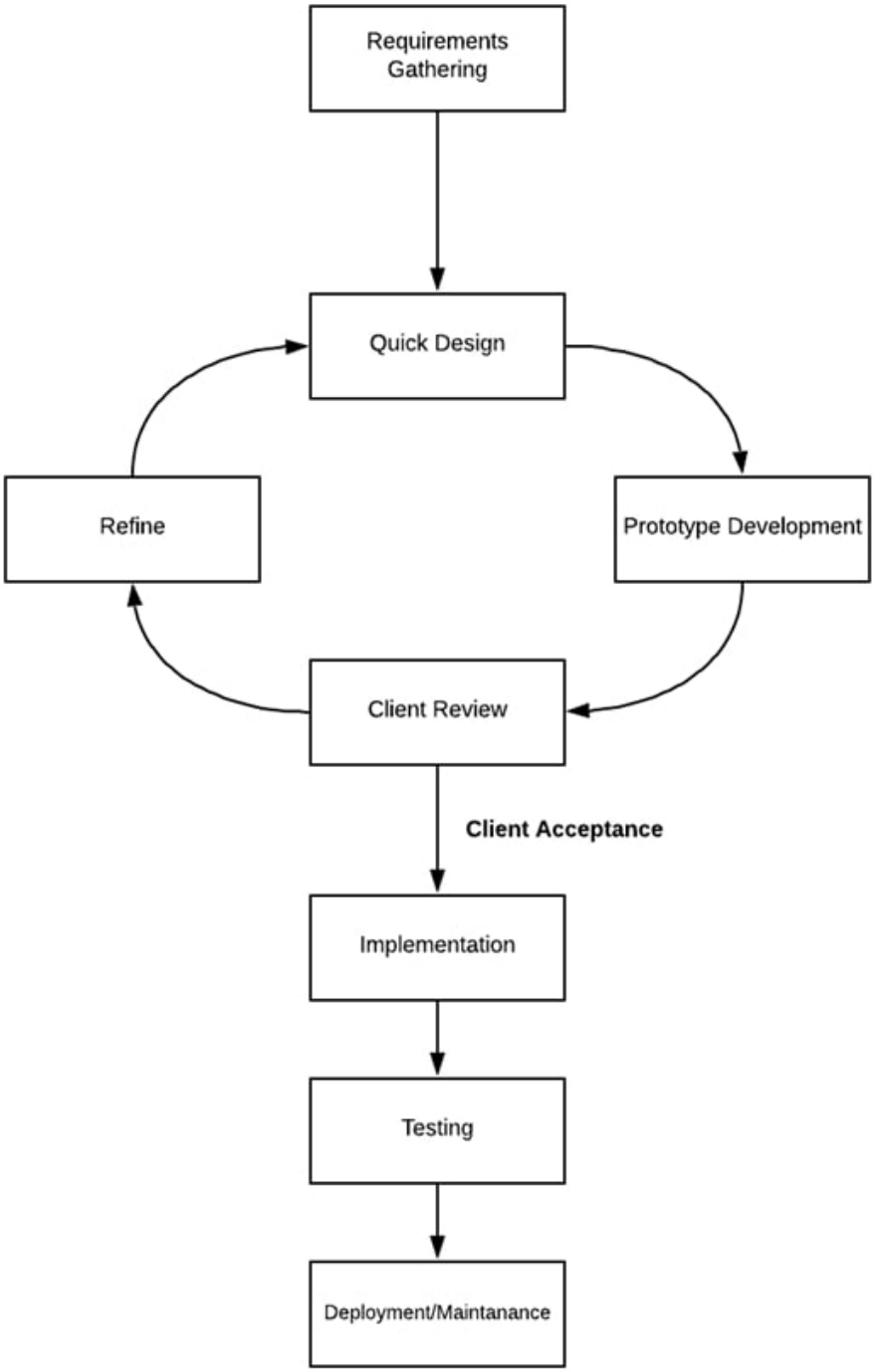


FIGURE 4.1: The Rapid Prototyping Model shows the iterative process focused on design and implementation of new prototypes iteratively

- Operating System: Linux Server, Windows Server
- Browser Support: Google Chrome, Mozilla Firefox, Microsoft Edge

Functional Requirements

1. Send & Receive messages

   The users should be able to share the messages with each other, via their list of friends or their timeline. Some of the shared messages could be 'compromised', which will infect the user profile after opening.

2. Tracking the spread of content

   Each message sent and received should be tracked. This includes what happens with the message i.e. if it has been opened or deleted, who it came from, is it infected, what type of content it carried.

3. List of friends connected to user

   The users should see the list of friends they are connected with, and be able to interact with them.

4. Show list of messages

   The messages that have been received, should show in a timeline format, similar to Facebook or Twitter.

5. Allow to control information given to the user

   In order to remove any factors that might impact user perception towards messages or their friends, the users will be given different level of information, depending on the setting given by the administrator or the researcher. The level of information is the experimental treatment to validate our hypotheses.

6. Allow to set up and customise the platform

   The platform should allow to see the network of connected users, generate a new network, customise what the participants will see, the score of the sent tokens, the content they will be given.

7. Run bots alongside human users

   The platform should allow to run non-human users alongside the participants. The AI bots will have the same functionality as a human user, and will appear on the scoreboards.

Non-functional Requirements

1. Security

   The data collected should be encrypted and have limited access to only researchers.

2. Show number of friends and messages sent/received

   To give a user an idea who they have been interacting with in their new network of friends, whom they will not be familiar with, the number of messages will act as a indication to who they have been interacting with the most.

3. Allow to customise profile

   For the platform to feel like a personal social space, the user should see their avatar, and some personal information about themselves such as their username and join date.

4. Automate the process of running the experiment

   The automation of the protocol will allow for easy collection of experiments, secure data download and automatic network generation to avoid any distraction for the researcher. This allows to make sure all the experiments are repeated in the same ways.

5. Easy to analyse data

   The data collected through the platform should easily incorporate with Python's pandas software library, for easy data analysis.

4.1.2 Software Modelling

As Rapid Application methodology lacks a defined and scalable architecture by omitting a traidtional design stage [Coleman and Verbruggen, 1998; Nasution and Weistroffer, 2009; Dahiya, 2010], it can result in software that is undocumented and lacks proper relationships between classes in code. We address this limitation by visualising its functionality in the Unified Modelling Language (UML) [Weilkiens, 2011; Chaudron, Heijstek, and Nugroho, 2012]. This helps in maintenance and adoption by other developers.

Use Case Diagram

Having defined the functionality of the system in the requirement stages, we can assign that functionality to the different actors. UML is used to depict the functionality and how it relates to the users of the system in the use case diagram [Weilkiens, 2011; Gemino and D. Parker, 2009], which shows the interactions of users with different parts of the system. An actor can either be a user or hardware/software actor, such as an API. Each use case can be enhanced by extra functionality, using the «extends» and «includes» clauses. The first of these clauses means that a functionality would have an additional step, which is an *extension* of the original functionality. For example when building the platform, instead of implementing our own network generation algorithms, we used NetworkX. We can see that in Fig 4.2, where our network generator includes the functionality of Python's library.

The «includes» clause means that we are using a functionality of another use case. Unlike the extension, this is not an extra step, but instead something that

can happen either in parallel or in the background i.e. the functionality of another use case is *included*. Opening a message from another user for example in our platform, in addition to its primary function, will calculate the score in addition to performing its intended functionality.

FIGURE 4.2: Use Case diagram

Modelling the basic functionality identified in the requirements specification, we can see in Fig. 4.2 how the users will interact with the system.

We have identified four actors, two of which are non-human actors - the database and the bots. The bots inherit the behaviour from the user actor, since the bots will be able to perform the same actions on the platform, yet they are not human users. Both the user and the bots will be able to interact with their friends, which then will be tracked to see the behaviours users exhibit towards each other. The administrator actor is mainly responsible for setting the scenarios and supervising the platform. This actor can set which scenario should be ran, see the network and the status of the nodes in real-time, control the database and generate the networks, which will connect users with each other.

Entity-Relationship Diagram

Establishing the user needs and the functionality, now gives us a better overview of what the system will do. Since we have that information, we can now consider what the users will see and what they will input into the system themselves. All this data needs to be stored in one way or another, and in order to plan for the most optimal way of storing information about the user, and their data on our platform, we can create an ERD (Entity-Relationship Diagram), which is a model of the database [Dick, Hull, and Jackson, 2017; Date, 2004].

This diagram helps to visualise the SQL database, and the relationships between the tables. In ERDs, we use tables, which will hold data with types reflecting the chosen DBMS (Database Management System).

The tables have relationships with other tables, where we store more data. Storing all the data in one table would be inefficient, hard to manage, duplicating data, and insecure if compromised. Therefore each table has its own taxonomy and is linked with another table by using a Primary Key - Foreign Key (PK-FK) relationship. These keys are simply unique IDs, which then allow to query the tables, where the keys overlap in a Venn diagram fashion [Date, 2004; Data and User, 2015; Bagui and Earp, 2011].

Some of the basic relationships between the tables are one-one, one-many, many-many. These specify how many instances of an entity can relate to another entity e.g. one user can have many friends, as seen in Fig. 4.3.

For the data to be accessed quickly and to reduce any duplicates, thus saving space, the ERDs and the databases have to normalised. This reduces data redundancy and improves data integrity. The basic process of normalisation involves removing repeating groups of columns, make proper use of relationships and keys.

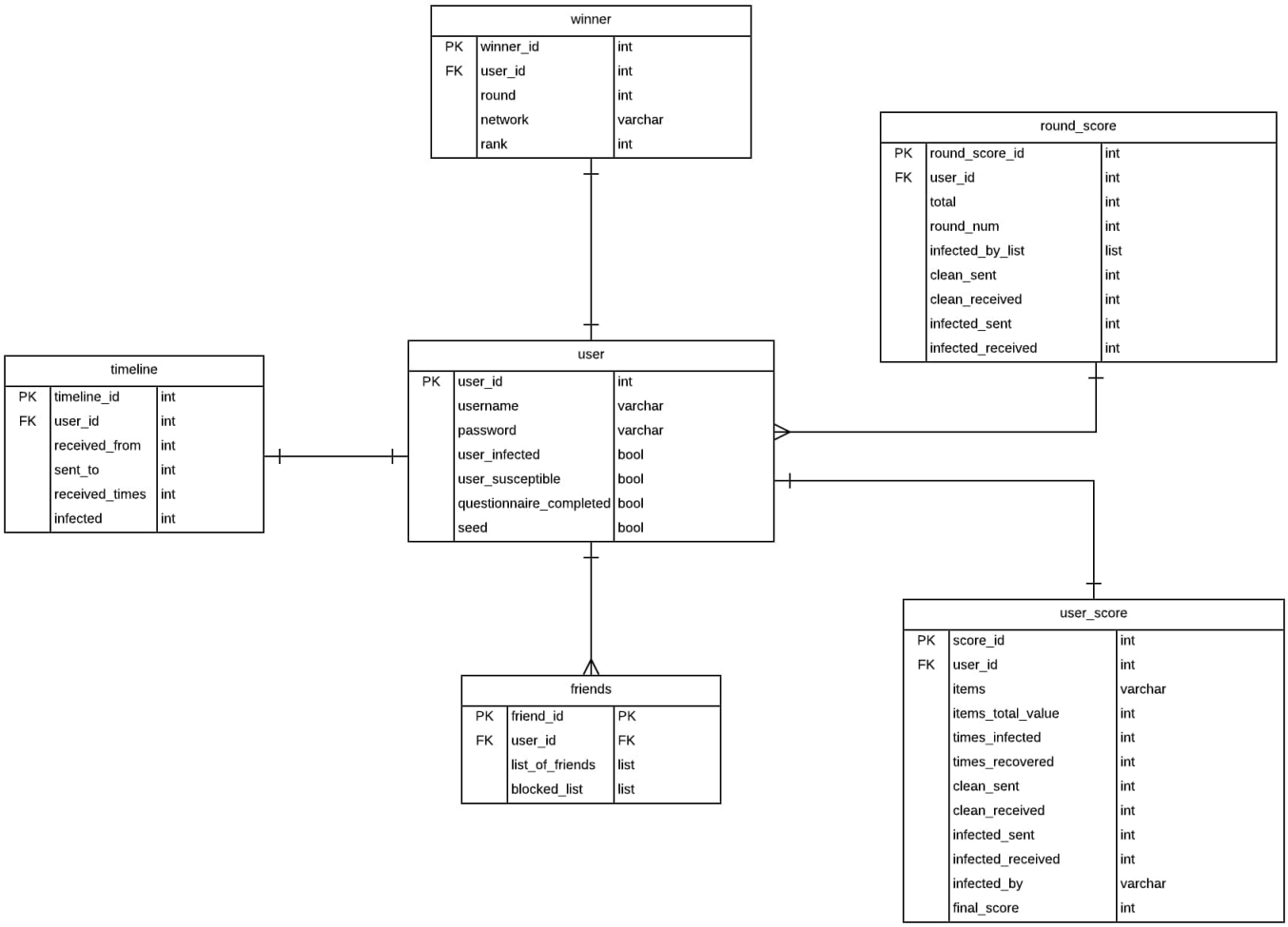


FIGURE 4.3: Use Entity-Relationship diagram

Identifying what actors we have and how they will interact with the system has helped us to identify what data should be stored for the system to function.

As seen in Fig 4.3 we have defined six tables, each connected to the user table. As the user is the central table of the design, they will be linked to all the other information stored about them.

The user has different information linked to them, which is stored across different tables. Most of the information in the user table is constant throughout all the scenarios in the experiment, aside from the 'seed' row, which changes with each new scenario. The 'timeline', 'friends' and 'user score' store temporal data, it changes as users interact and as the network is rewired by the administrator. The timeline stores interactions during each scenario, and gets reset afterwards, where user score table is responsible for the statistics per each round. Once the statistics have been calculated in the background, at the end of the round, the players' ranks are inserted into the 'winner' table, which will store this information until the end of the experiment, where the administrator can find the top player, based on the rank across all scenarios, with a simple executable script.

The user can view their timeline in each round, know their list of friends, see their score after each round, and at the end of each experimental run the winner is

decided. All this is stored in the database.

Class Diagram

A modular and abstract software allows for high re-usability and adaptability of the software for other purposes. This kind of approach can often be seen in APIs, which usually aim to make it easy to use code someone else has created, by providing algorithms that are written in a general way or in other words, code that isn't fit to work only for one purpose, and can be adapted to developers needs.

Having to visualise code can be difficult, especially working on large projects, and trying to plan for modularity and abstraction may cause some issues further down the line, as the software will be expanded.

To map out the structure of our code, we can use a Class Diagram, which shows structures, properties, classes, attributes, operations, and relationships between objects. These would then translate into data types, functions, variables that are used in the code.

Each of the variables and functions will have a data type and access type. As we know which variables we might want to expose to other classes, for example if we are using same database connection information for the whole system, we might want to allow classes to have access to that, by giving our database details a public access, meaning it can be accessible from anywhere and is represented as '+' symbol in the Class Diagram. Variables can also be private ('-') and therefore only accessible within the class they were declared in, and protected ('#'), which allow for access from the class they were declared in and classes which are (child) of the latter.

Class diagram also helps to show the integrity of the code, aiding to help design modular software. The relationships between classes can use aggregation and composition.

Aggregation, represented by a white diamond implies that child can exist independently of the parent, that is if we remove one class, it won't affect the functionality of the other. Composition on the other hand (black diamond), implies that a child cannot exist without the parent.

Depending on the language that is being used to develop the software, we can include some more specific details in the class diagram, for examples making some of the classes *abstract* as languages such as Java or C++ allow to do so.

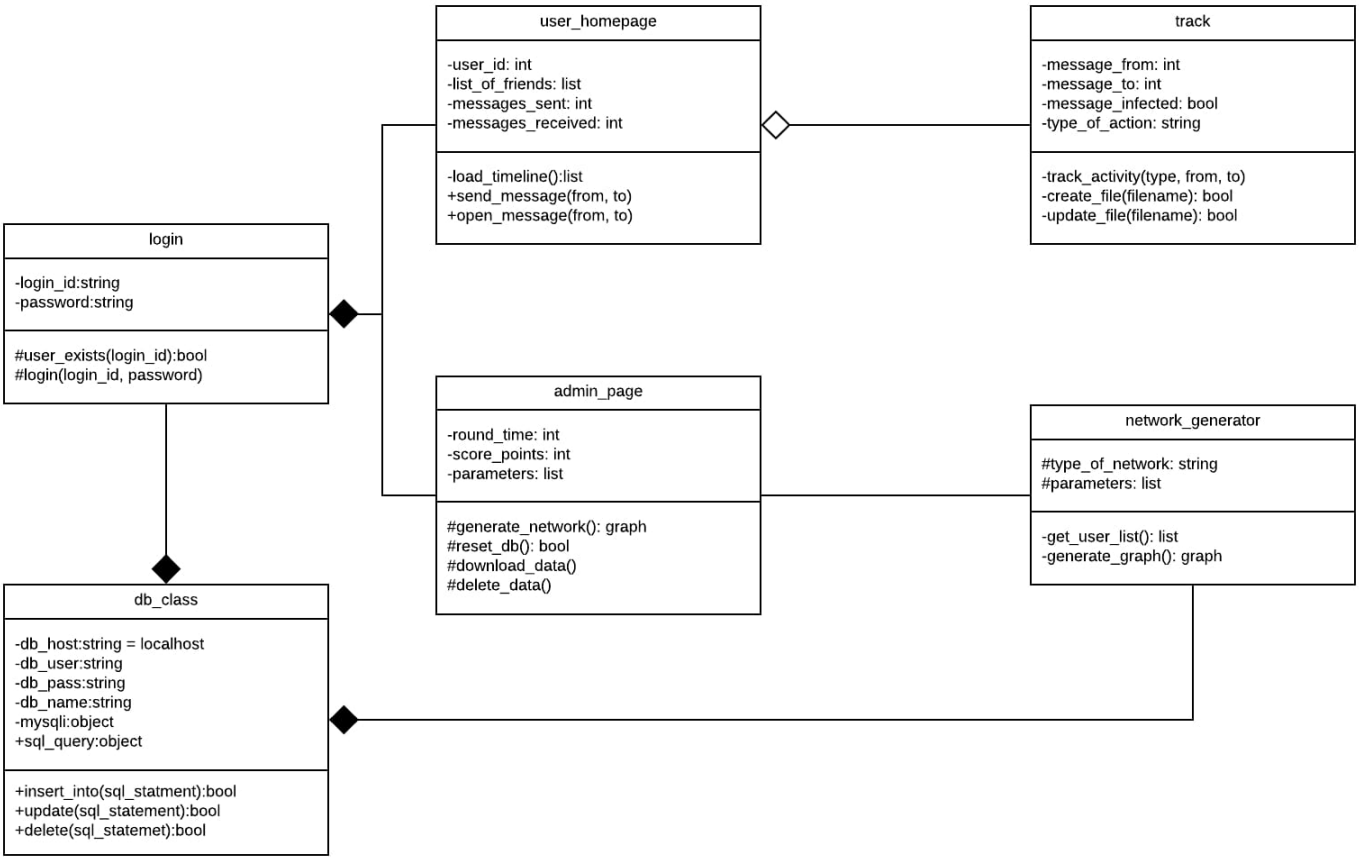


FIGURE 4.4: Class diagram

Designing our platform to be modular, we have defined integrity between the classes. This helped with platforms modularity, knowing which parts could work individually and which ones could not. Following this principle, we have created the platform in such a way that in can be used as a standalone social network, without having to use the functionality of tracking, as seen in 4.4. The standard code functionality still allows to log in, either as a regular user or an administrator. Compared to a regular user, the administrator does not participate in the experiment, therefore their functionality does not include any of the social interactions methods, as defined in *user_homepage* class. The admin however is responsible for generating the graph, which is connected to Python's NetworkX API, and depending on the purpose of the study, the network generator could be used to connect users with each other, or this could be done in other ways, such as setting the list of friends in the database (in a CSV format), under the *list_of_friend* row in 'friends' table as seen in 4.3. Because of this flexibility, the network generator class is neither connected with the *admin_page* using aggregation nor composition, as this would be project dependant.

Aside from the standard functionality found in a typical social network, storing data was one of the more important features of the platform. The tracking comes directly from user interactions, as every interaction performed is stored in an XML file, and also temporarily in the database, to tracking the score and infection.

4.2 Development

Our platform named NUTMEG (Network evalUaTion Multi playEr Game) was created using modular approach with main use of PHP scripting language. PHP is a general purpose language created for web development, and unlike HTML and JavaScript it allows to enhance sites functions, by executing on the web server rather than users browser. This means we could create more functionality served to the user, rather than relying on the availability of functions built into the web browser.

Dependencies and Operating Environments

NUTMEG as all other online platforms is accessible via the web, thus it resides on a web server. For the platform to run as we intended, we have used the following dependencies and Operating Environments:

- Ubuntu Server 16.04.6 LTS
- Apache 2
- MySQL 5.6
- PHP 5.6.40
- Python 3.5.2
- JQuery 3.4.0
- Bootstrap 3.4.0
- NetworkX
- JSNetworkX
- PEAR (PHP Extension and Application Repository)
- Probability Distributions Library (https://github.com/php-math/PDL)
- DiceBear Avatars: Avatar Placeholder Library

Implementation

Firstly before starting to write code, we have set up our environment and dependencies. To help with visualising the database we have used phpMyAdmin (Fig. 4.5), which is administration tool for MySQL database. In order to keep track of software changes and for code backup we have used GitHub.

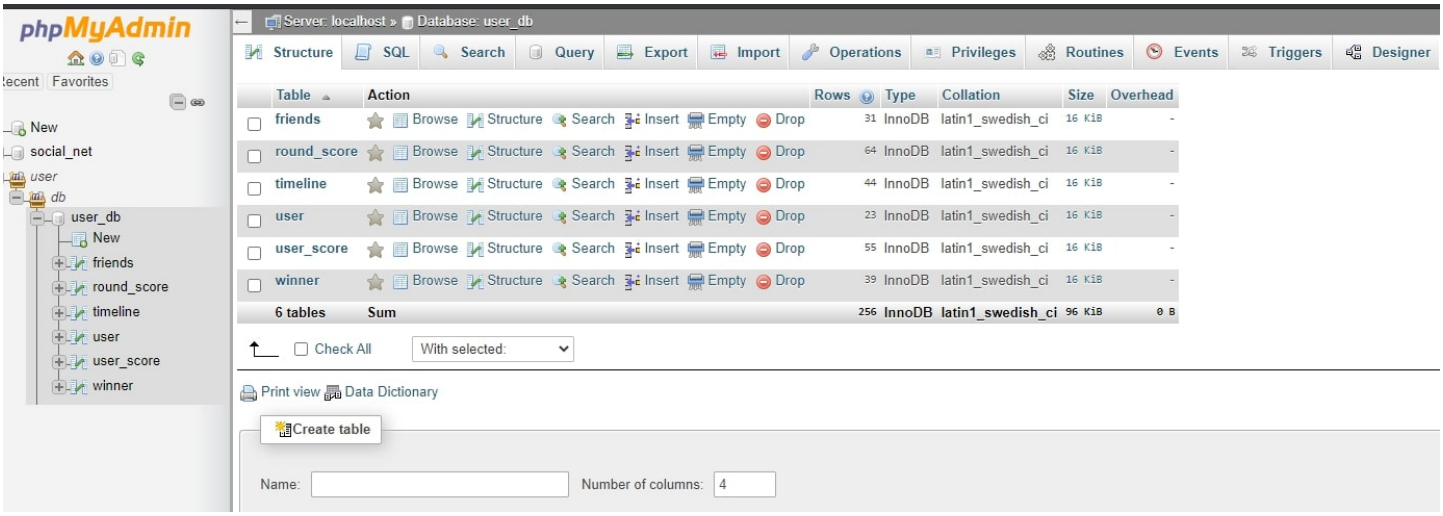


FIGURE 4.5: View of the Database Structure in phpMyAdmin

As NUTMEG was mainly written in PHP, it can easily connect with SQL and exchange information with other scripts/programs, thus the use of Python and its APIs allowed to further enhance the functions of our web application.

These scripts make the platform more dynamic, as they allow to add information during runtime. Parts of the platform can therefore be updated live, as real-time view will reflect the changes instantly.

This was an important element of choosing PHP to be the main language, as during the design stages, we had to consider features that would allow to automate the run of our experiments, and easily adapt each scenario, without affect the functionality, or having the users refresh their browser each time we make a change.

Following the rules of Software Prototyping methodology, we have been able to create new revisions of our platform, which included new features and changes in short amount of time.

Knowing standards that apply on social networks, that is having a network of friends a user is connected with, seeing his/hers friends posts and being able to interact with those, we have started off with a simple prototype of a social networks, on top of which we have built up all of the other functionality, needed to built our research tool. This prototype has also had the ability for administrator to connect the network of users into friends, using NetworkX generating algorithms.

Each future iterations of the build, was based on that initial prototype. On top of this prototype, we have developed the following functionality to achieve the final product.

- The ability to update experimental scenarios in real time - as we are running several different scenarios set for the experiments, the ability to change what information we give to user on their homepage has been added, so that this can be done in between scenarios, without the user noticing or having to refresh their page.

- Timeline - the timeline shows the messages received from friends. Here the user can see how many interactions they had with their friend, and decide

what to do with the message they have received (open, delete). The timeline is updated in real-time and can be customised.

- Blocking - as in many other social networks, we have added the ability to block users. This is useful to see what kind of behaviour the user will exhibit after getting infected by malicious content, as we expect one would block a friend whom they got infected by.

- Tracking - the main feature of our platform is the ability to track user behaviour. The behaviour of the users includes: send, open, delete, recover and block. We track all the information about those interactions in an XML file (Fig. 4.6).

  The XML file is made up of elements. An XML element is everything from the element's start tag to the element's end tag. Tags can contain text, attributes, other elements or mixture of those. Our tracking file is built up of XML tags, such that the action taken by the user is the root element, and every child of that element is the metadata about the action. The metadata here is the timestamp of the action, user infection status (infected/not infected), who the message was sent by and if the message sent was infected.

  As seen in Fig. 4.6, the XML root tags correspond to the action taken by the user, and contain an ID, which is unique to the action, for example a *sent* tag with the *messge_id* means that the message has been sent from i to j at time t, where t is a UNIX timestamp for when the action took place.

  Each child nested within the root tag contains specific details about the action, such as whom the message has been sent to or who it has been received from, at which point in time, if it was infected, or if the sender/receiver of the message was infected at that time, and the type of message sent (if there was content avaliable).

- Antivirus - one of the scenarios allows users to remove malicious content by making use of antivirus. The antivirus will remove the infected status from the user profile, and it will also clear the timeline from any infected items that the user has received.

- Real-time network view - the administrator user is able to see the network in real time. This is done by making use of NetworkX and JSNetworkX. The view of the network will show all the nodes, who they are connected with and their status. The status of the node can be healthy, susceptible and infected. As nodes change the status, the colour of each node will update corresponding to that status.

- The ability to add content - using MIME (Multipurpose Internet Mail Extensions), it is also easy to add common content to our platform. By creating a folder corresponding to the type of content we wish to add e.g. 'video' or 'images' folder, we can then populate it with various types of files. The platform will take that file and using its extension it will render the file appropriately, depending on what type of the file it was, and it will fit it to the screen size.

```
<sent message_id="41_42_1590409647">
  <to>42</to>
  <time>1590409647</time>
  <user_infected>0</user_infected>
  <message_infected>0</message_infected>
  <file_type>emails</file_type>
</sent>
<received message_id="42_41_1590409676">
  <from>42</from>
  <time>1590409676</time>
  <user_infected>0</user_infected>
  <message_infected>0</message_infected>
  <file_type>images</file_type>
</received>
```

FIGURE 4.6: The XML data generated by tracking user behaviour

Testing

To ensure that our platform is working as intended, we have carried out number of test on both user and software sides.

From the user perspective, we have ran 3 pilot studies with 43 participants, in which we have tested the beta version of the platform from the user point of view. We observed what behaviour user exhibited and carried out a simple survey asking about the user interface (UI), the length of the experiment and how intuitive the UI was, as well as general comments on the platform. Based on the feedback and our observation we have made changes, which reflected for better experimental treatment.

Testing the software we carried out number of software testing methodologies, which have helped us to ensure that the platform was functional as intended as all the modules worked as planned.

Smoke testing is a type of test that ascertains that critical parts of the program that were planned are working properly. This test is quick and gives assurance that the major functionalities of the system work as expected [Chauhan, 2014]. In other words, smoke testing is running the software as if it was already released, and making sure everything works.

We have carried out a number of smoke tests with NUTMEG after each prototype iteration was ready before moving on to the next functionality. Once each part worked, we have tested another from the perspective of the user.

Integration testing verifies that different modules work with each other as a group [IEEE, 2017].

NUTMEG is a modular platform, thus during this phase we examined whether the interactions between our platform and database as well as interactions between PHP and Python worked together as expected.

End-to-end (E2E) testing refers to testing an application from start to finish, to check its workflow. The purpose of this is to simulate real user scenario [Tsai et al., 2001].

Once the platform was complete, we have carried out a number of E2E tests with colleagues, as well as ran several pilot studies to validate for component integration and data integrity.

4.3 Software Architecture

The platform has been developed using Service-oriented architecture (SOA) design and the Modular programming paradigm. We keep different components of the platform separate, so that if one component fails it won't affect the rest of the functionality of the platform, but also it allows for removal or customisation of different components. In Fig. 4.7 we show different components of the platform.

The front-end of the application layer is the user interface. The user and the admin have their own separate views. The admin is responsible for configuring the round set up, which will then be displayed to the user. This can be done in real-time, so the changes the admin makes to the network, the score system or the round description will be reflected instantly. The user will see the preset rounds, which have been prepared and loaded by the admin. For instance in our case, we have preset three different experimental scenarios, where in each one the participants are exposed to different levels of information regarding the messages they exchange.

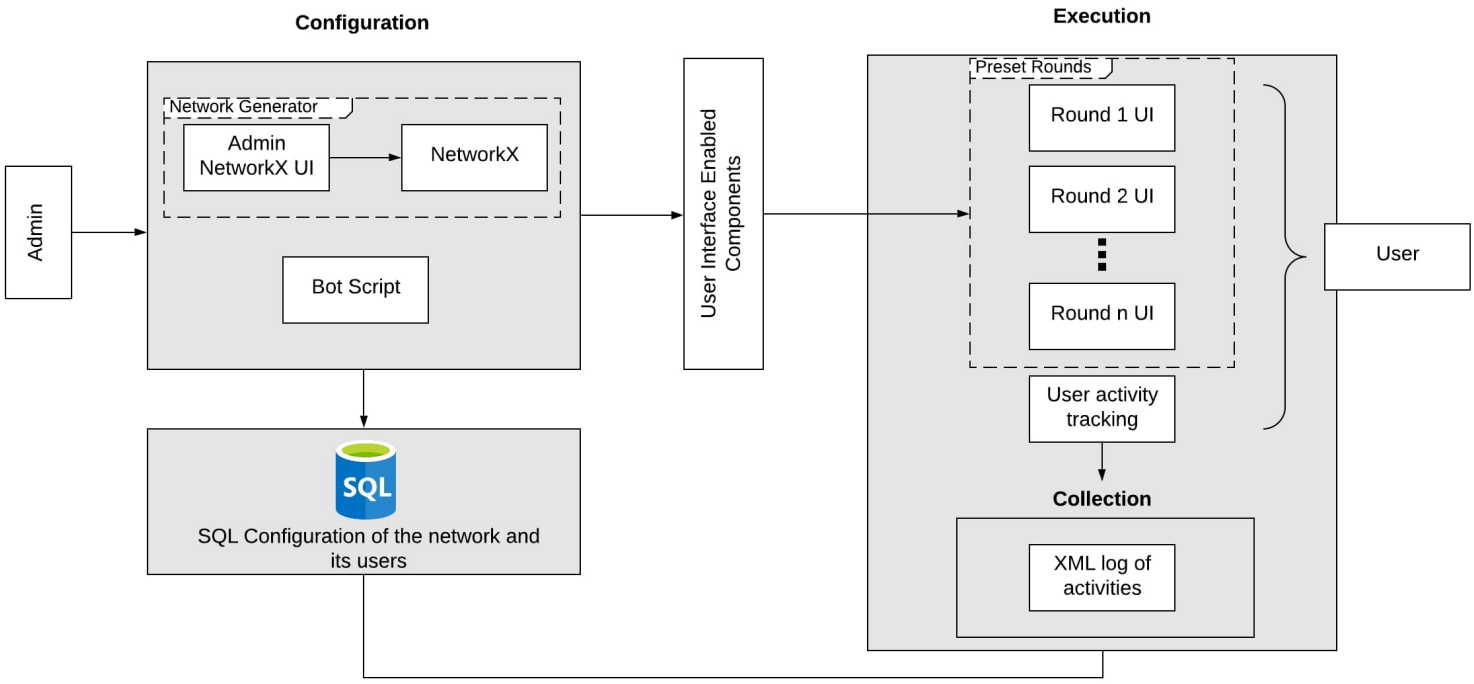


FIGURE 4.7: Simplified illustration of the software architecture

The back-end is responsible for providing most of the functionality, including the tracking of the user and network generation. Each action of the user is linked to a different PHP script, which has a function that tracks that activity. The actions correspond to different scripts e.g. *send_item.php* or *remove_item.php*. This is to

make it easier to find and change how the functionality of those actions works and to allow execution of other code in parallel if necessary. In scenario 3, which allows for the use of antivirus, we make use of this modular approach, as the antivirus is its own module, which makes use of the *remove_item* functionality. The actions scripts are linked to the tracking library, which will recording the specific action, and write the data into an XML file corresponding to the username. (See figure 4.8 for an example of activity the tracking function).

```
function track_activity(){
    global $send_to;
    $sender_username = get_username($_SESSION["user_id"]);
    $receiver_username = get_username($send_to);

    $sender_filename = "data/tracking/$sender_username.xml";
    $receiver_filename = "data/tracking/$receiver_username.xml";

    $message_id = $_SESSION["user_id"] . "_" . $send_to . "_" . time();

    update_tracking($sender_filename, "sent", $message_id, $send_to, NULL, time(), true, true); // sender tag
    update_tracking($receiver_filename, "received", $message_id, NULL, $_SESSION["user_id"], time(), false, true); // reciever tag

}
```

FIGURE 4.8: Sample code that tracks user sending a message to a friend

XML has been used to track user data. Every action performed by the user is stored in an XML file that corresponds to the username e.g. user1.xml would contain activity data of user1. The main tracked activities are: send, open, block and remove item.

Network Generator is provided to the Admin View. The administrator is able to generate a network with NetworkX as API, given different parameters depending on the type of network being used. The default network that is being generated is Watts–Strogatz, which generates a scale-free network [Duncan J Watts and Steven H Strogatz, 1998] with seed (number of initially infected nodes) set to 10%.

The information about the network, friendship, timeline etc. is stored in the database. The database is used to store the generated data but not for data analysis. The database provides the information to the live view of the network on admin side, most of information on the user side and the information to bots about the status of the users and messages.

The messages themselves are stored as JSON files. The JSON contains the information where the file came from, who it is sent to, at which time it was sent, if the file was opened and if it was "infected". These are only temporary files and are only used to pass the interactions and the "infection" between the users, they do not contain information about tracking.

4.3.1 Bot Agents

Aside from the platform having real players, it is also possible to have the users interact with bots. The bots aim to mimic the behaviour as a normal user would. They are also able to send, receive and open messages as well as get infected. The bots will appear on the score board alongside real players. The interactions of the bots are timer based, such that during $1 \leq \Delta t \leq 10$ seconds the bot will perform

each of the mentioned actions with a certain probability p, given that the action is possible, for example the action of opening the message will only be possible if a message is received. It is possible for bots to interact with each other.

4.4 Illustrative Examples

The illustrative examples demonstrate the interfaces available for the admin (Fig. 4.9) and the participants (Fig. 4.10). Once the user sends a message in the first version of the platform, it does not contain any content, however they do get a confirmation of the message being sent as seen in Fig. 4.13. In the second version, where we add content from our library, the user will see either images, videos or text as seen in Fig. 4.11. The admin who is responsible for setting up the network can choose to create smaller individual groups to separate the participants. This is beneficial in an experimental scenario, where we want to test multiple networks on small parts of the cohort at the same time as you can see in figure 4.12.

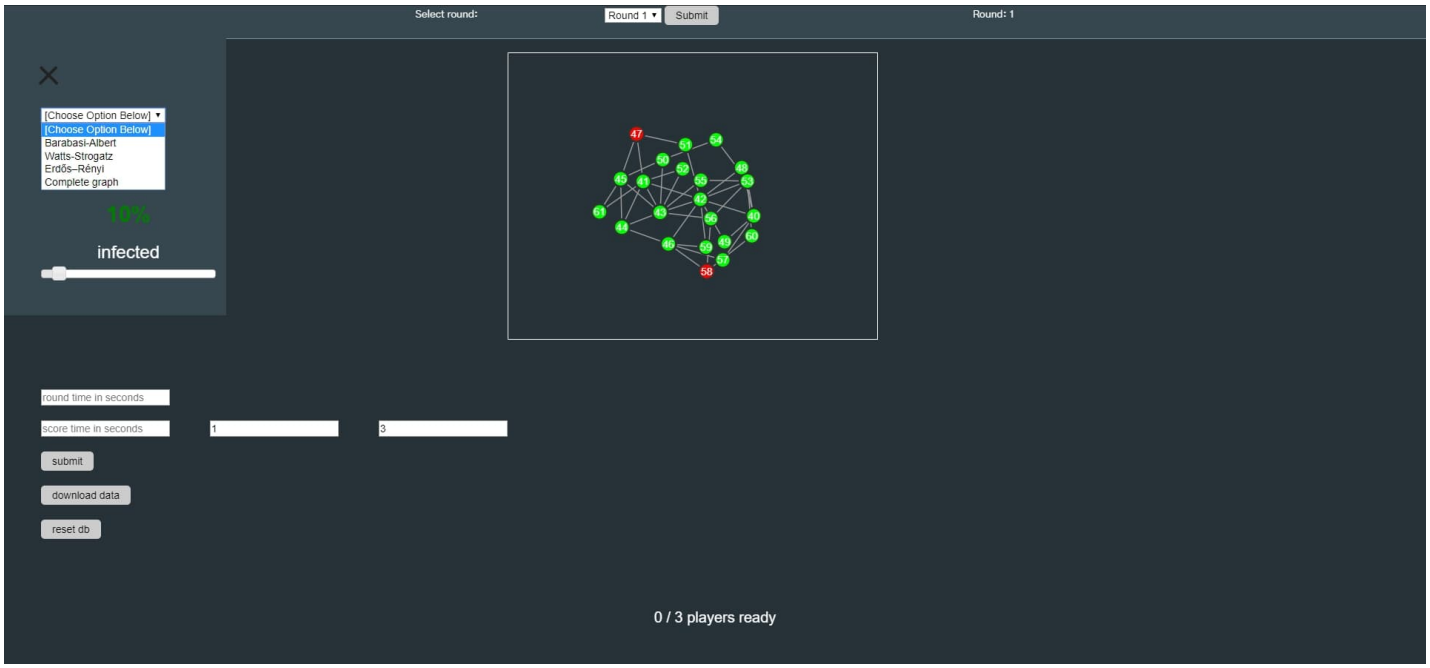


FIGURE 4.9: The administrator UI. In the centre, the admin is shown the current status of each node. Green refers to uncompromised accounts. Red refers to node that have been infected. On the left hand side, the admin can set up the network topology, change the number of initial infected nodes, fix the duration of the experimental run, as well as submit the changes, downloading the data, or clear the database.

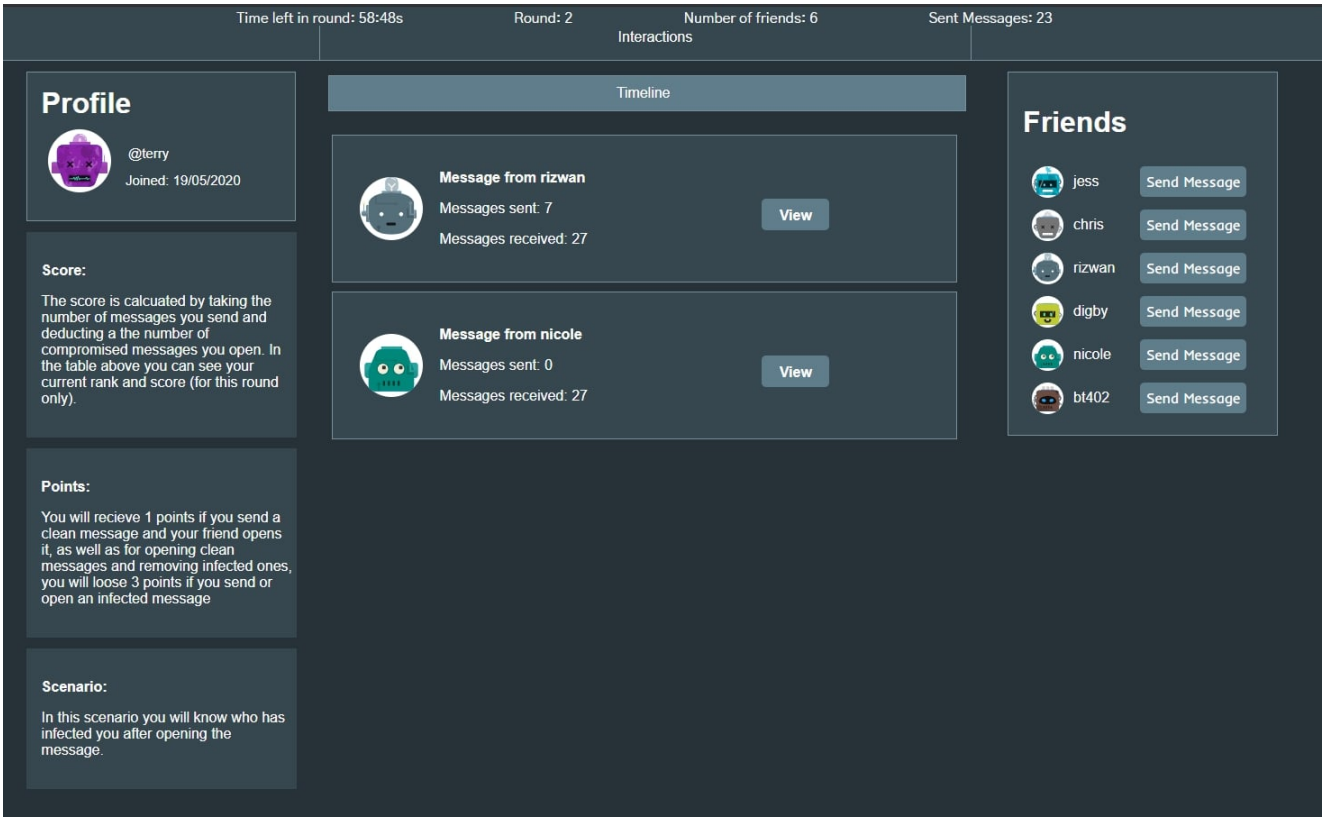


FIGURE 4.10: Participant UI. On the left hand panel, users can see their avatar as well as general information about the scenario they are playing, their score, and the point system. For example, in this case, users will receive one point for any message sent that has been opened, and for opening a clean (not compromised) message or removing an infected one. Furthermore, users will lose three points for each infected message they send. The point system/scheme can be easily adapted/customized and it is added to introduce an element of gamification thus incentivising users to take actions. On the right hand side, users can see the list of friends to whom they can send a direct message. On the top bar, users can see a summary of relevant information such as the time left in the experimental run, the number of friends and the number of messages they sent. Finally, in the centre of the UI, users can see their timeline. In this case, the user has received two messages. She can view such messages and decide whether to opening or deleting them.

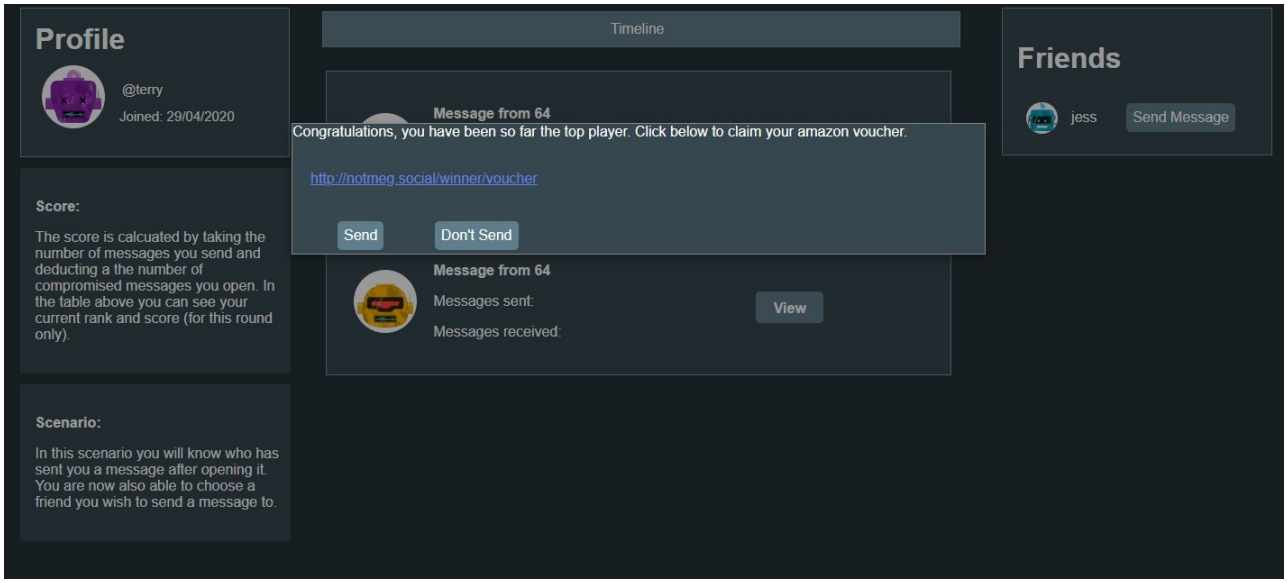


FIGURE 4.11: Example of compromised message in the second version of the platform. In this case, the user is compromised. Thus, when she decide to send a message, the platform picks at random in the list of malicious message in the library. The user has then the possibility of inspecting the message and decide whether to sent it or not.

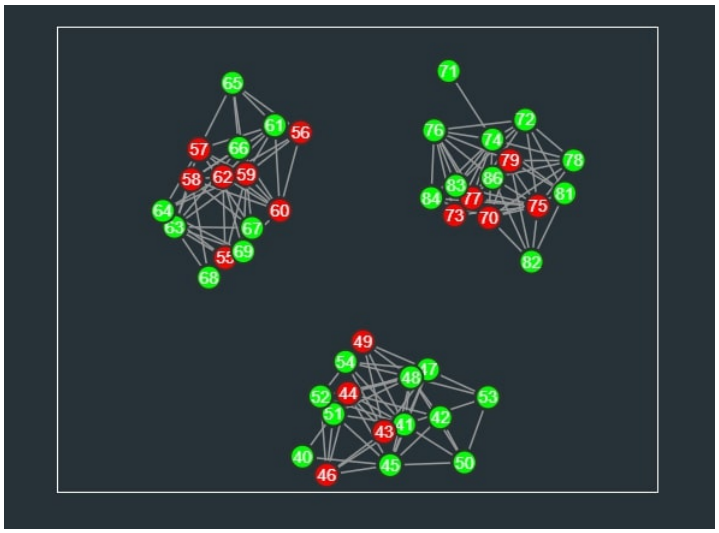


FIGURE 4.12: The network has been split into 3 separate groups

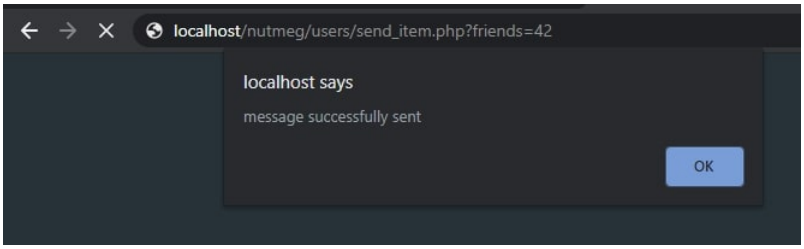


FIGURE 4.13: After user has sent a message to one of their friend, they get a confirmation popup

4.5 Summary

We developed a new experimental platform called NUTMEG, which is aimed at observing and characterizing the spreading of cyber threats on online social networks. The platform exposes users to different levels of information, by introducing them to a range of different experimental scenarios. In each subsequent scenario more elements of the user interface are being enabled, giving the participants different level of details about their network and the threat level they might be exposed to.

The features of the platform allow for setting up a network with % of infected seeds, and thanks to back-end created in Python, it is easy to use various different network generators available in NetworkX library [Developers, 2010]. As a result of modular approach design, the separate components of the platform can be easily customised without affecting the overall functionality of the platform. For example this can be achieved by changing the code responsible for displaying the timeline, where any kind of content can be added/displayed. The ability to track every action is particularly suited to isolate the effects and drivers of particular behaviors. Furthermore, the web based nature of the platform, makes it easy to set up online experiments, which can be accessed from anywhere. Although the original idea to build NUTMEG was to study the behaviour of users on online social networks, its features and modularity allow to enhance its functionality for other purposes.

We bear in mind the fact that the quality of software is correlated with the amount of time spent testing and debugging it. In that regard making our platform open-source will help to find and fix bugs, and improve the overall quality of our software through the work of the community. Through this, the code will become more robust and optimised for number of different scenarios it could be used in.

Chapter 5

Experiments

Using the platform described in the previous chapter, here we present the experimental settings, the design and purpose of different experimental scenarios, demographics of the participants, and metrics that we define to study the underlying behaviour of users and its impact on networks.

5.1 Experiments Description

The experiments aim is to study the propagation of malicious content on social network by using different configurations of the graph, and finding how different information impacts the behaviour of people and its correlation with the network properties.

Using our platform, we have preset three experimental settings (treatments). Each scenario gives the user different levels of information, about their network and it is used to isolate/test specific hypothesis about the main drivers of cyber threats. Here utilising these scenarios we collect data from 109 participants (26 in UK and 83 in Spain).

We obtained the authorization from the University Research Ethics Committee to carry out our experiments online and to recruit the participants online, via advertisements on different social platforms such as Twitter and Reddit, as well as internal messaging system at the University of Greenwich, and a specialised recruitment system at the University of Zaragoza, used and developed for other experiments [Cuesta et al., 2015; Gracia-Lázaro et al., 2012].

In order to take part in the experiment, the recruited participants have to create an account and sign a digital consent form followed by a questionnaire, which aims to investigate computer literacy levels and gullibility towards malicious content, by asking cyber security related questions e.g. Do you know how to tell if your computer is hacked or infected?

Participants numbers per each experiment

Date	Number of participants
15/04/2020	10
22/04/2020	11
18/06/2020	5
16/06/2020	17
17/06/2020	16
23/06/2020	20
23/06/2020	16
24/06/2020	14
Total	109

5.1.1 Experimental Settings

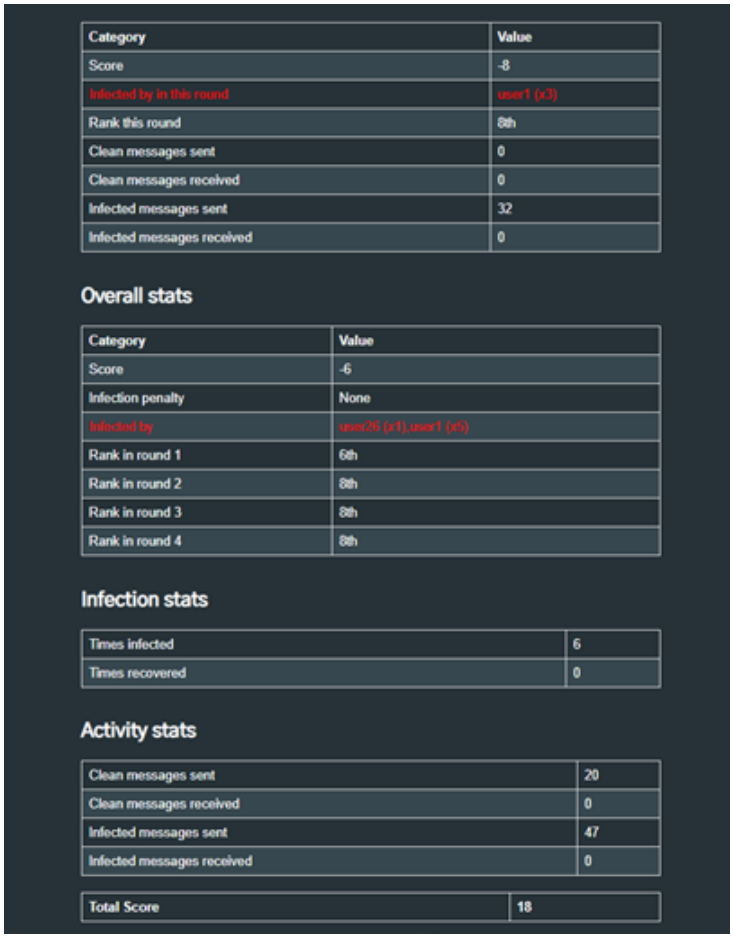
Before each experiment began, and after the questionnaires were complete, the users have been given instructions on how to use the platform, via a lobby page, which was presented before the start of the experiment. They were informed on the purpose of the experiments, how to exchange messages between each other and the scoring system.

When interacting between each other, the users see different information on their timeline about whom they are interacting with, and they are gradually given more information about the infection as scenarios progress. These interactions and user status are scored, based on the following formula:

points = + 1 (if your message was opened by your friend) + 1 (if opened a “clean” message) + 1 (if removed an infected message) – 2 (if send infected message) – 1 (if infected opened)

The points are incentive to users interacting together, and correctly identifying a malicious partner. They provide extrinsic feedback to the users’ actions, and point are considered to be the most basic concept found in almost all gamified applications [Dichev and Dicheva, 2017]. Our scoring system has been created to incentivise cooperation and reciprocity. The point is only awarded if node j opens a message from node i, and no points are gained if a message is ignored and depending on the status of the opened message, the points can either increase or decrease. We use this approach to penalize spamming behaviour, as if a user is either a spammer or subject to large volume of messages, the spammer will not gain points for sending a number of messages, and the receiver can potentially be penalised for opening a message with infected status.

After each scenario is complete, the user is provided with statistical information about their performance, among the stats they can find information if they have got infected during their scenario, their score, how many safe/infected messages they opened, whom they got infected by etc. This information provided there is meant to provide users with feedback about their performance, and they can devise a new strategy based on this information, for example stop interacting with a particular node, if they got infected by them.



Category	Value
Score	-8
Infected by in this round	user1 (x3)
Rank this round	8th
Clean messages sent	0
Clean messages received	0
Infected messages sent	32
Infected messages received	0

Overall stats

Category	Value
Score	-6
Infection penalty	None
Infected by	user26 (x1),user1 (x5)
Rank in round 1	6th
Rank in round 2	8th
Rank in round 3	8th
Rank in round 4	8th

Infection stats

Times infected	6
Times recovered	0

Activity stats

Clean messages sent	20
Clean messages received	0
Infected messages sent	47
Infected messages received	0

Total Score	18

FIGURE 5.1: User is shown a statistics page, outlining their general performance in the round and information about the infection. The rows highlighted in red show who the user has been infected by in a particular round in the top table, and throughout the game in 'overall stats' table.

After a completed scenario run, we move to the next scenario. And after we run all three scenarios, we modify the network parameters, and reconnect the participants. This is done by changing the parameters of the network, and then rewiring the edges (list of friends), with this all the actions taken on the same network are also reset, and the memory of past interactions is lost and started again with each new network introduced.

5.2 Experimental Scenarios

We have created three different experimental scenarios to study three different cases. Each scenario incrementally builds up upon the previous.

5.2.1 Scenario 1

The first scenario is a 'baseline', which we use to define the behavior and tendencies of users when they did not have any information to make educated guesses

about the risk linked to opening a particular message.

In the first scenario, the elements that are enabled only allow for users to see his/her friends list with full name, and their timeline. However in the timeline, the users do not see the identity of the sender, and they do not receive information if they have been infected after opening the message.

The purpose of this is to see how baseline interactions between users impact trust behaviour, as here the participants will build up trust with their neighbours, by interacting between each other. We assume that if two users interact a lot , they will have the memory of this interaction in next scenarios, and will be more likely to open the messages from his/her friend.

The only actions in this scenario is for the user to open, reply and delete a message.

5.2.2 Scenario 2

In the second scenario in addition to the features from the first, users will know if they have been infected after they open a message and the identity of the sender of each message. As this builds up on the previous scenario, the participants now have more information about the network and the infection. Given previous interactions, which will now be visible in the user timeline, we can now observe how trust is evolving and how network effects impact the spread of virus, and how gullibility impacts the likelihood of opening messages.

5.2.3 Scenario 3

The final scenario, which also builds up on its predecessor gives the user ability to block his/her friends as well as use an 'antivirus' if the user has been infected. The ability to block others will prevent the user from receiving and sending any more messages to/from the blocked friend. The antivirus will remove the infection from the profile, setting it to be susceptible again, and it will remove any message that user had in the timeline.

Blocking their friends, means that the users are effectively changing their network, removing nodes which are connected with them. This behaviour will have an impact on trust, as blocking is a high indication of lack of trust, and it will change how the virus can spread, since it won't be reaching as many nodes. This feature will allow to observe the resilience that is created towards the virus, and should change how the virus spreads.

Experiments runs and configurations

We set three different network configurations, each of which is ran for all three scenarios. We run scenarios 1, 2 and 3, before we change the network configuration. The following parameters have been tested across different experimental runs, where as described above we reconfigured the network after running all three scenarios, using these parameters, each network was tested per each experiment:

Network	p	m	$\langle k \rangle$	$\langle C \rangle$	$\langle d_{uv} \rangle$
Watts–Strogatz	0	4	4	0.5	3.14
	0.4	4	4	0.14	2.2
	1	4	4	0.18	2.22

p - The probability of rewiring each edge,
m - Each node is joined with its m nearest neighbors in a ring topology,
$\langle k \rangle$ *- Average degree,*
$\langle C \rangle$ *- Average clustering,*
$\langle d_{uv} \rangle$ *- Average shortest path between two vertices* u, v

Network	p	m	$\langle k \rangle$	$\langle C \rangle$	$\langle d_{uv} \rangle$
Watts–Strogatz	0	8	8	0.64	1.33
	0.2	8	8	0.58	1.43
	1	8	8	0.52	1.47

Network	m	$\langle k \rangle$	$\langle C \rangle$	$\langle d_{uv} \rangle$
Barabási–Albert	2	1.8	0.33	2.18
	3	2.55	0.38	1.87
	4	3.2	0.6	1.68

m - Number of edges to attach from a new node to existing nodes

5.2.4 Questionnaire

In order to be able to use the platform, the participants first have to create an account. The registration process which asks for the username and password, in order to be completed, requires a key, which can be set by the developer. They key restricts access to who can register and use the platform, as only invited participants should be able to register. After this process is complete, all the participants are required to complete a survey. The survey is adapted from Ref. Heartfield and Loukas, 2016b and is aimed at gathering an independent estimation of the gullibility (i.e. susceptibility), but it can also be adapted to needs of other studies, hidden or disabled.

We have divided the survey answers into statistics for both countries, to see the difference between the two, as well collated the UK and Spanish data to get overall statistics for the whole population.

The recruitment in the UK has mostly been successful amongst the students on computer science courses, where as in Spain the cohort was more random. This

can be seen in the answers to some more cyber-security related questions, where proficiency in the area will have an impact on the response.

The survey questions, in the order they appeared to the participants, and answers to them are in tables 5.1 - 5.9;

TABLE 5.1: Primary Web Browser

	Chrome	Safari	Firefox	Edge	Other
Spain	82%	10%	5%	1%	2%
United Kingdom	81%	15%	4%	0%	0%
Total	82%	11%	5%	1%	2%

TABLE 5.2: Primary Operating System

	Windows	MacOS	Android	iOS	Linux	I don't know
Spain	77%	13%	10%	0%	0%	0%
United Kingdom	69%	27%	4%	0%	0%	0%
Total	75%	17%	8%	0%	0%	0%

TABLE 5.3: How often do you use a computer

	Every day	Several times per week	Once or more per week	Once or less per week
Spain	84%	11%	2%	2%
United Kingdom	92%	4%	4%	0%
Total	86%	9%	3%	2%

The large majority of our participants are using their computer every day. Given the observed demographics this makes sense, as most young adults rely on their devices for a lot of daily tasks and work.

TABLE 5.4: How often do you use social media

	Every day	Several times per week	Once or more per week	Once or less per week
Spain	87%	8%	4%	1%
United Kingdom	73%	8%	0%	19%
Total	83%	8%	3%	6%

This is one of the more important questions we could ask. As we see a large number of our participants use some form of social media on daily basis. The research focuses on the study of OSNs, so the experience with other social media platforms could produce some interesting results.

TABLE 5.5: Do you know how to tell if your computer is hacked or infected?

	Yes	No
Spain	35%	65%
United Kingdom	65%	35%
Total	42%	58%

The participants who were successfully recruited in the UK have largely had either a degree in computer science or exposure to experience in the technology industry. In this questions we can see this clearly with the UK population being more knowledgeable in the area of cyber security.

TABLE 5.6: Is your computer configured to be automatically updated?

	Yes	No	I don't know
Spain	72%	23%	5%
United Kingdom	77%	15%	8%
Total	73%	21%	6%

Computer updates bring not only new features, but also security patches and fixes to potential exploits [Vaniea and Rashidi, 2016]. On modern devices updates are usually set to automatically download, so as reported by majority of participants their computer is set to automatically update.

TABLE 5.7: How careful are you when you open an attachment in email?

	Very*	Cautious*	Not at all*
Spain	55%	45%	0%
United Kingdom	69%	31%	0%
Total	59%	41%	0%

Here we've shortened the answer to the questions. Each column corresponds to the following answer:

- Very* - I always make sure it is from a person I know and I am expecting the email
- Cautious* - As long as I know the person or company that sent me the attachment I open it
- Not at all* - There is nothing wrong with opening attachments

As we see, the whole population is somewhat cautious when opening the attachment, checking at least if its from a company or a person they know.

TABLE 5.8: Do you know what a phishing attack is?

	Yes	No
Spain	63%	37%
United Kingdom	77%	23%
Total	66%	34%

TABLE 5.9: Do you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?

	Yes	No
Spain	17%	83%
United Kingdom	27%	73%
Total	19%	81%

Phishing attacks will often ask users for their passwords, as they pretend to be a legitimate service, they will present login box where the user is expected to enter their credentials. Our participants however reported quite high familiarity with this, and they show resilience to this, as most of them do not re-use the same password on multiple sites.

5.3 Demographics

The recruited participants came from different backgrounds across two different countries. Majority of UK participants are computer science students, and the Spanish participant population were recruited amongst a wider audience.

The 26 UK participants make 24% of the total and the 83 Spanish participants make 75% of all participants combined.

Majority of participants were young people, aged under 30, who account for total of 63% of participants, and people over the age account for 37% of the total.

Females were the majority, with 57% of all participants declaring as female and 43% as male. This is different for each country, as in UK 81% of people were male, compared to only 19% female. The Spanish population was more female dominant, with 69% of total participants being female and 31% being male. Below we show the population pyramids, by binning each participants into age and gender, we show the division of males (in green) and females (in orange).

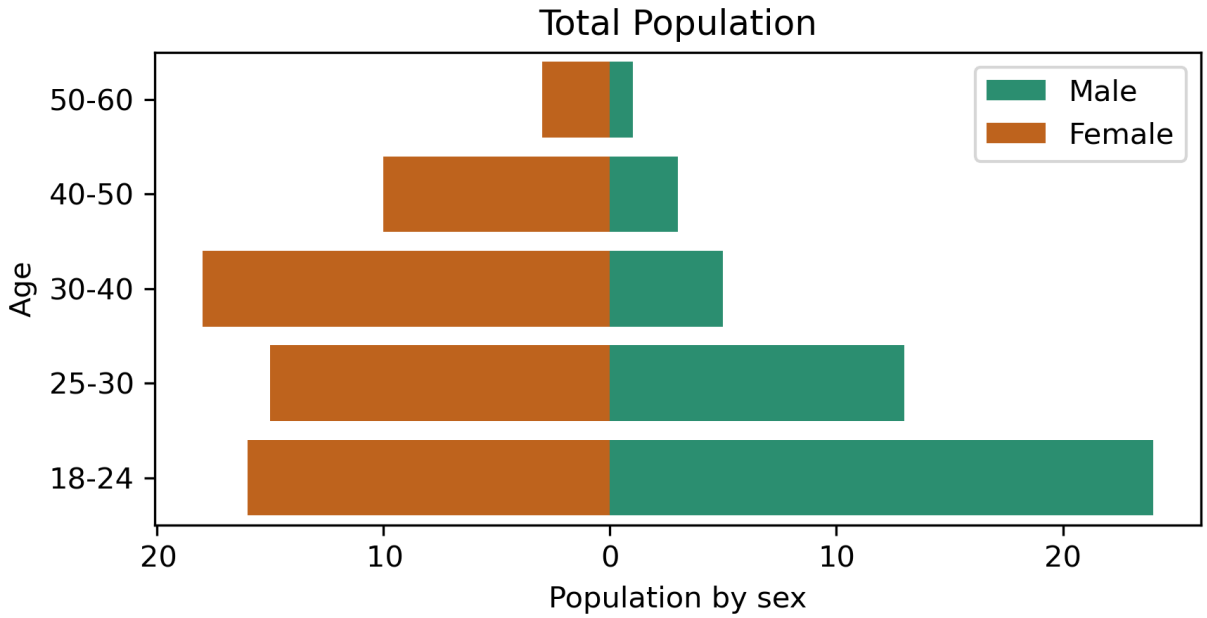


FIGURE 5.2: Total combined population between Spain and the UK

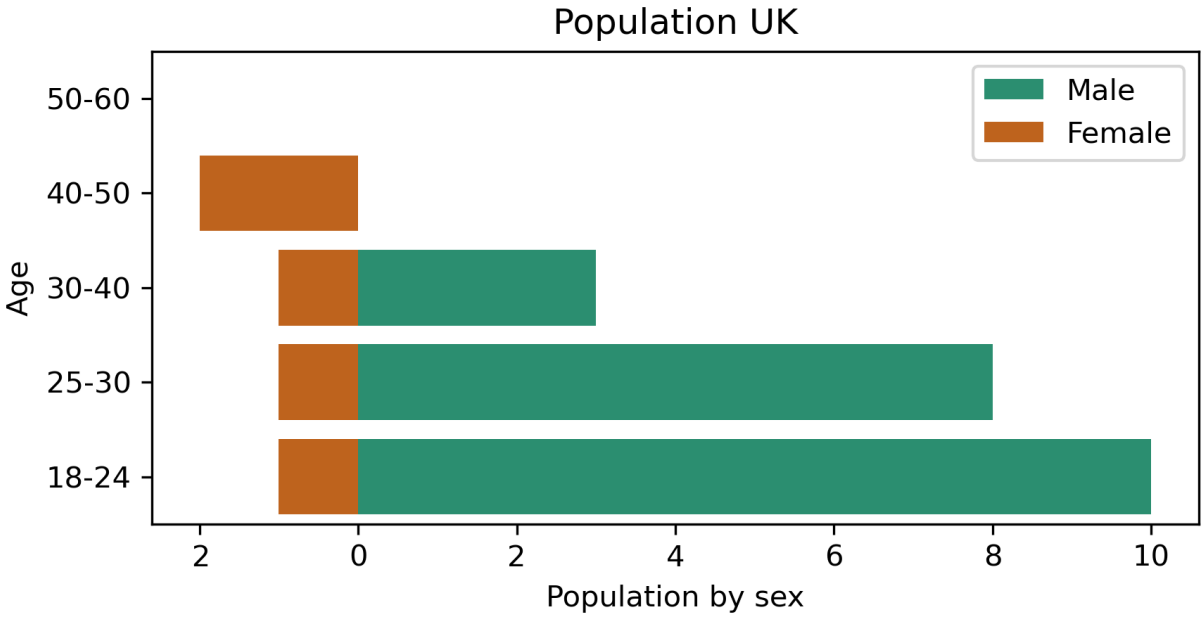


FIGURE 5.3: UK population pyramid

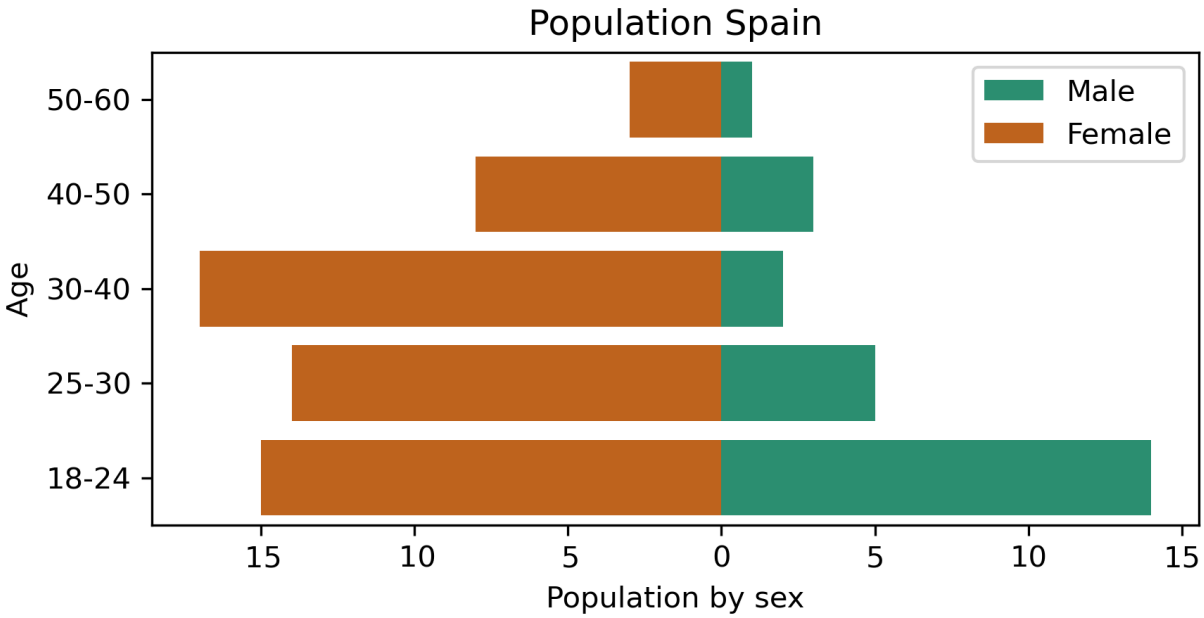


FIGURE 5.4: Spain population pyramid

5.4 Trust and Gullibility Metric

Trust and gullibility are one of the key user characteristics taken in into consideration when studying cyber security awareness [Jagatic et al., 2007; Heartfield and Loukas, 2016b; Heartfield, Loukas, and Gan, 2016; Qureshi et al., 2018].

These characteristics however consider the fact the users see content, and they are able to identify malicious cues. The knowledge, skills and situational characteristics are part of a trust framework in holistic cyber security studies [Henshel et al., 2015; Oltramari et al., 2015], and the situational setting of the studies also depends on ones ability to sift through vast amount of data, and their ability to understand and interpret signals of potentially infected messages [D'Amico and Whitley, 2008].

5.4.1 Trust

In order to define trust in the context of our platform, we consider the user interactions, mainly the messages received and opened between nodes i and j. The actions the user can take change during each scenario, as given more functionality to the user interface, they can start blocking and deleting messages. The actions that do stay consistent across all the scenarios are sending, receiving and opening.

Considering the ratio of messages opened to message received, we normalise this value, using the Softmax Function [Goodfellow, Bengio, and Courville, 2016; Bishop, 2006], and get a "Trust ratio", which is equivalent to a similarity index, between how many messages the two nodes opened between each other.

The Softmax Function allows us to normalise the ratios, between the values 0 and 1, considering the weights of the messages. The Softmax Function is a function that turns a list of floating point numbers into a probability distribution of these numbers, proportional to their weight [Goodfellow, Bengio, and Courville, 2016; Bishop, 2006].

The input of this function, as a list of real numbers, might contains values which are negative or positive and do not sum up to 1. Once the function applied, each element of the list will be in the interval $(0,1)$ and the sum of all elements will be 1. As the value are weighted, the larger input will correspond to a larger probability in the output.

The standard version of the function is defined as:

$$\text{Softmax}(x_i) = \frac{\exp(x_i)}{\sum_j \exp(x_j)}$$

Applying the function to the measure of trust, we test it against different values. We input different values as a list of the ratio $\frac{\text{messages opened}}{\text{messages received}}$ by both nodes i and j. If normalised value is 1.0 this means that node i and j have opened all of the messages received between themselves.

For the individual trust ratio, we only apply the Softmax function, which gives the normalised value of messages opened. For example if node i opened 85% of messages, and node j opened 82% of messages, the normalised list is [0.51, 0.49], meaning node i opened more messages, and has slightly higher trust towards its neighbour, however since the two numbers are not far apart, the two nodes interacted in a similar fashion.

Computing the trust ratio for the pair of nodes, aside from considering the normalised fractions, we also consider the total number of $\frac{\text{messages opened}}{\text{messages received}}$, between i, j. This gives an overall trust value between two nodes, indicating how many

messages either node has opened approximately, considering the weight of the total interactions, and depending how many messages the two exchanged between each other, this impacts the overall trust ratio.
Firstly we calculate the Softmax function of the list for the pair of nodes, with node i opening 85% of messages and node j 82% we get our output vector:

$$softmax(x_i, x_j) \equiv softmax([0.85, 0.82]) = [0.51, 0.49]$$

We then calculate how far apart the two normalised values are, as 0.51 and 0.49 are 0.02 away from each other, the two trust ratios are 98% similar (both nodes opened comparable amount of messages). We find this by the equation $1 - |x_i - x_j|$ where x is the normalised element of the output vector.

$$1 - |x_i - x_j| \equiv 1 - |0.51 - 0.49| = 0.98$$

We then multiply these by $\frac{\text{total opened}}{\text{total received}} \equiv \frac{\sum messages\ opened_{ij}}{\sum messages\ received_{ij}}$, and obtain the trust ratio, which defines how similar are the two nodes in terms of their $\frac{opened}{received}$ weighted by total interactions.

$$0.98 * \frac{24}{26} = 0.91$$

The overall trust between nodes i and j is 91%, meaning that between each other the pair of nodes opened most of the messages they exchanged, showing high number of interactions i.e. high trust.

In order to describe the trust metric and its different components, let's consider 4 different cases. The first in which two nodes opened a high number of messages, the high number of interactions would indicate high levels of trust. The second where trust was one sided, one of he nodes opened most of the messages, while the other only a small fraction (or none). This could mean that one node trusts its neighbour, or that could also indicate spam, since one person is opening most of the messages while the other is passive. The third case where the trust is similar, but also low, that is two nodes only had briefly interacted with each other, for example node i send message to j only once, and j has reciprocated only once as well. And finally we consider no trust, where both nodes opened no messages, this case is interesting, as lack of trust is also equal trust. This is since both node equally don't trust each other, thus the softmax function returns the output vector of [0.5, 0.5]. Once we multiply this however by $\frac{0}{\text{total received}}$, the overall trust is 0.

Examples:
We find the ratio of opened to received between pair of nodes:

- high trust = [0.85, 0.82] - node i opened 85% of messages, node j 82%
- asymmetric trust = [0.8, 0.1] - node i opened 80% of messages, node j 10%
- low similar trust = [0.13, 0.1] - node i opened 13% of messages, node j 10%
- no trust = [0.0, 0.0] - both nodes opened no messages

We then apply the Softmax function to the vector:

- Normalised high trust: [0.51 0.49]
- Normalised asymmetric trust: [0.67 0.33]
- Normalised low similar trust: [0.51 0.49]
- Normalised no trust: [0.5 0.5]

We calculate the "closeness" measure i.e. how similarly did the two nodes behave. The greater the number, the further apart the defined actions were.

- High trust closeness: $1 - |0.51 - 0.49| = 0.98$
- Asymmetric trust closeness: $1 - |0.67 - 0.33| = 0.66$
- Low Similar trust closeness: $1 - |0.51 - 0.49| = 0.98$
- No trust closeness: $1 - |0.5 - 0.5| = 1.0$

We can see that two values here are the same, since the two ratios are very similar. The high trust and low similar trust are the same, as in the original input (before applying softmax), the difference between the values was 0.3 in both cases, yielding the same number. This indicates that nodes behave in similar fashion, which is true, however we now take into consideration the fact that one of these pairs has opened a larger number of messages between each other, compared to the second pair.

Multiplying the closeness measure by the $\frac{\text{total opened}}{\text{total received}}$:

- High trust ratio: $0.98 * \frac{24}{26} = 0.91$
- Asymmetric trust ratio: $0.66 * \frac{13}{26} = 0.33$
- Low Similar trust ratio: $0.98 * \frac{3}{26} = 0.11$
- No trust ratio: $1.0 * \frac{0}{26} = 0.0$

The $\frac{\text{total opened}}{\text{total received}}$ fraction changes the trust ratio output, allowing to see how many messages were opened between both nodes. In the high trust, the two nodes opened around 91% of messages between each other, indicating high trust, where if we consider the similar trust, which had the exact same closeness between the two ratios previously, the trust ratio is small here, since between each other both nodes opened around 11% of messages in total. In the low trust example, since the trust was one sided (one node opened 80% of messages), which could indicate a node being spammed, however since the node still chose to open the message, some underlying trust exists between i, j.

5.4.2 Gullibility

The other metric we use is the user gullibility. Since user gullibility has been found to be correlated with the content and cyber security training, we aim to use the technical knowledge of the user, obtained from the survey, as a measure of how likely they are to open a message, and become resilient or passive towards their neighbours once infected.

To calculate the gullibility, we use the sum of the answers to the survey above, based on the "positive" and "negative" answers, such that each positive answer would be for example "No I do not reuse my passwords on multiple websites" or "I am very cautions when opening email attachment", and negative is the opposite. The positive answers are worth -1 points and negative +1 points.

Using the last five questions, which are related to cyber security awareness, we sum the gullibility points (1 point per question) of a user, with -5 being least gullible and +5 very gullible. We extend this with the usage of the computer/social media, ranging from 0 points, if they are used every day to 3 points if used one or less per week. The sum of the points indicates the gullibility, the lower the number the less gullible the user is.

5.5 Machine Learning Prediction Algorithms

The ability to predict a likelihood of an event, gives way for preparation and mitigation of the occurrence. Since we are tracking the actions of users on our platform, we explore the possibility of predicting infection of a node, based on past actions. For that purpose we use different machine learning algorithms in Chapter 6, which the basic concept of is described here.

5.5.1 Decision Tree

Decision Tree is a supervised algorithm, which aims to classify (or predict) a certain outcome, based on specific interactions, in which branches of the tree will lead to [Breiman et al., 1984; Salzberg, 1994; Hastie, Tibshirani, and Friedman, 2009]. The tree is built of branches and leafs. Each leaf in the tree represents a class, which classifier would use to make a prediction based on it's path to that leaf. Each leaf contains a True or False conditions, which will apply for most of the samples in the set. Based on whether or not this argument passes, the branch to a class will take a different direction. At each "step" the feature class will be removed from samples that do not apply to the conditions, and the tree will display that. The value list shows count of records of each feature that have reached the leaf.

5.5.2 K-Means

K-means is a unsupervised learning algorithm, which finds groups in the data [Sculley, 2010; Hartigan and Wong, 1979], with the number of groups (clusters) is represented by the "K". The algorithm picks k random data points, and works

iteratively to assign the closest data point to the each cluster, one another point is added to the cluster, the algorithm takes the mean value, and picks another point closest to the cluster (using Euclidean distance). It will assign each data point to one of the "K" groups based on the features that are provided, those are clustered based on similarity. Each centroid of a cluster is a collection of feature values which define the resulting groups.

5.5.3 Principal Component Analysis

Principal component analysis (PCA) is a dimensionality reduction technique [Tipping and Bishop, 1999; Halko, Martinsson, and Tropp, 2011; Martinsson, Rokhlin, and Tygert, 2011]. PCA converts the complexity that exists in multidimensional data, and converts that into a 2D/3D scatter plot, while preserving the trends and patterns of the original dataset.

Data that is clustered is highly correlated. A principal component is the normalised sum of original variables in the dataset. PCA looks for the properties that show as much variation as possible. Instead of looking for properties that are same for most cases, PCA would create a new property, and although each variable is different PCA would make them all look the same. PCA also looks for the properties that would allow to predict or reconstruct the original characteristics. So again if we come up with a new property, that has no relationship to original characteristics, if we use our new property, we cannot reconstruct original ones. So PCA looks for properties that allow to reconstruct the original characteristics as well as possible. First principal component (PCA1) is the linear combination of original predictor variables, which captures the maximum variance in the dataset. It determines the direction of highest variability in the data. Larger the variability captured in first component, larger the information captured by component. No other component can have variability higher than first principal component. Second principal component (PCA2) is also a linear combination of original predictors, it captures the remaining variance, and it's not correlated with PCA1. So the correlation between PCA1 and PCA2 is zero. The axis are ranked in order of importance. Difference along the first principal component axis PC1 (the x-axis) is more important that the second principal component axis PC2 (the y-axis). On an 2D plot, the clusters would show how different the clusters are from each other. For example, if the distance from the red cluster to yellow, and blue cluster were the same. The clusters marked in orange are more different from each other, than the ones marked in blue.

5.6 Summary

Our experiments were based in Spain and the UK, having participants from different nations and background. The experimental setting allowed us to gather demographic data and computer literacy skills of our participants, which lead to development of new metrics. A total of 109 (26 from the UK and 83 from Spain) people have participated, each had to complete a questionnaire prior to the experiment [Heartfield and Loukas, 2016b].

The experiments consisted of 3 scenarios, each building on the previous one. The first scenario was the baseline, in which users had limited UI elements enabled. The purpose of the baseline was to investigate how users behave in a new environment without any knowledge about their network or infection. Preliminary random interactions should then start to phase out as we introduced scenario 2, in which the user was informed that they got infected after opening a message. New information in amalgamation with past interaction should now start showing creation of a new network of friends. In the final scenario users know at all time if they are infected or not, they have the ability to block their network of friends, and can additionally use an antivirus which will remove infection from their profile. Having interacted with others for two scenarios, the past interactions could indicate creation of trust between agents, or loss of trust if two agents block each other.

The two metrics developed as a result of the questionnaire and the exchange of messages are gullibility and trust. The former is a measure of users experience with cyber threats, and their counteraction to those. The latter is a new measure we created based on the exchange of messages between two users. It is a normalised value which takes into consideration the fraction of messages opened and sent between two nodes. The higher this value is the more messages the two nodes have sent and opened between each other.

Chapter 6

Towards an empirical characterisation of threats on social networks

Gathering data from 109 participants in two different countries, below we perform analysis to address the remaining research questions using machine learning, network analytics, and other statistical techniques. We introduce metrics of trust and gullibility to study the behaviour of our users. Furthermore, we attempt to predict the propagation of infection, based on the the empirical observations.

6.1 Analysis of user behaviour

To understand the prevalence of infection and its impact, we firstly turn our attention to the behaviour of our users, that is the recorded actions in each of the experimental scenarios. Given that each scenario reveals different information to the participants, their perception towards the messages and their friends will be different, which in turn will impact the spread of the malicious content and its prevalence. The behaviour is especially important in the third experimental scenario, as users are allowed to block each other, which changes the network structure. The empirical findings of the behaviour are therefore important, as they are the driving factor for the spread of cyber threats. We first average the data across the whole data collected to gather an initial understanding of users' behavior before moving towards more detailed analyses.

Time-integrated interactions

The exchange of messages between two nodes (i, j) on a OSN typically is function of time. Depending on the characteristics, this exchange can either grow or decline. As we measure this exchange in each scenario, we carry over some past message to future scenarios. After all three runs are complete, the network gets re-wired, and everything gets reset. Prior to that however, the connections and the possibility of exchanging messages between two nodes remain unchanged for all three runs.

6.1.1 Behaviour leading to infection

The actions that users can perform on our platform are send (which is correlated with receiving), open and delete messages in their timeline. These are constant across all scenarios, and in the final scenario the users can also block each other.

Each scenario was designed for different purpose. As described in chapter 5, first scenario is used to define a baseline and meant to introduce the user to the platform. During the first play-through, the participants should get to know their friends, and start building up trust. The following scenarios are meant to then measure that trust and observe how it changes, given that users will know more information about the infection.

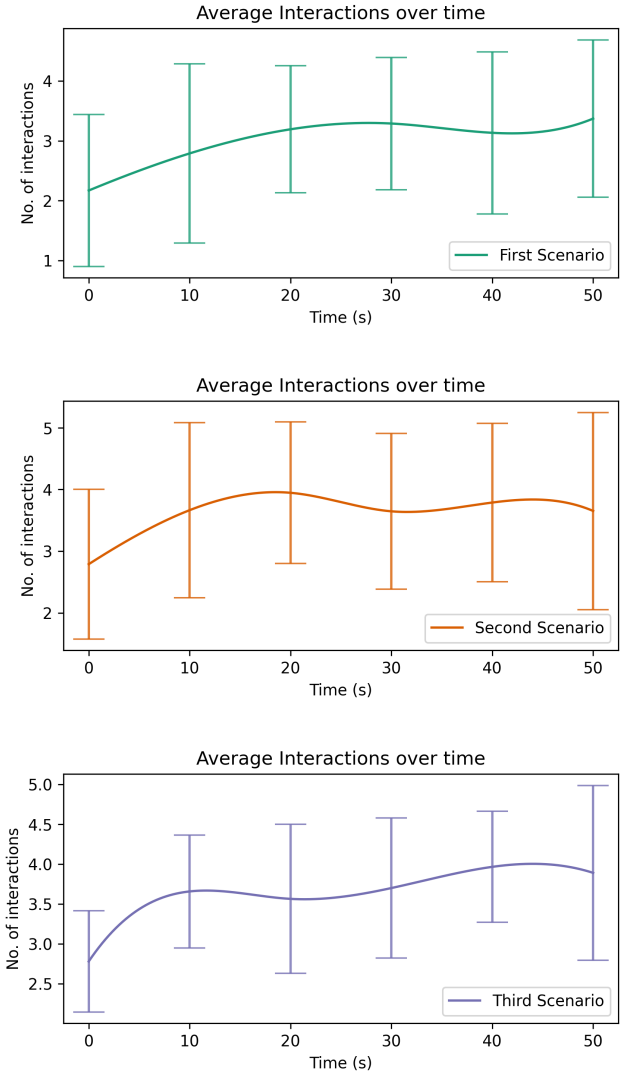
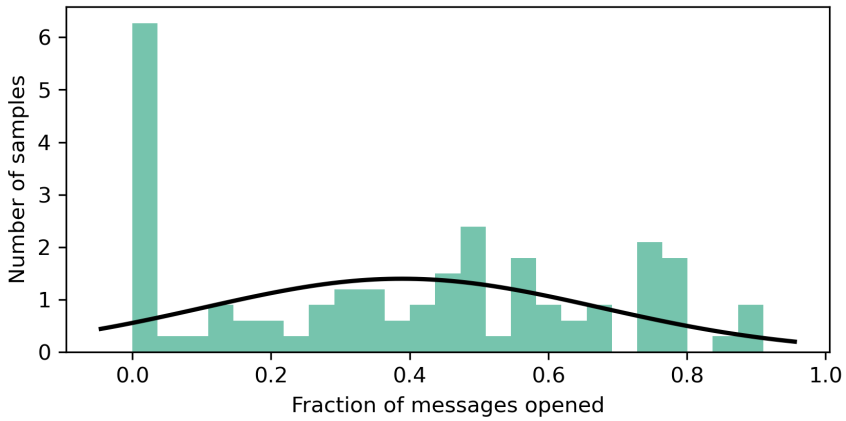


FIGURE 6.1: The average number of interactions over time during each scenario. The interactions are binned in 10 second time intervals.

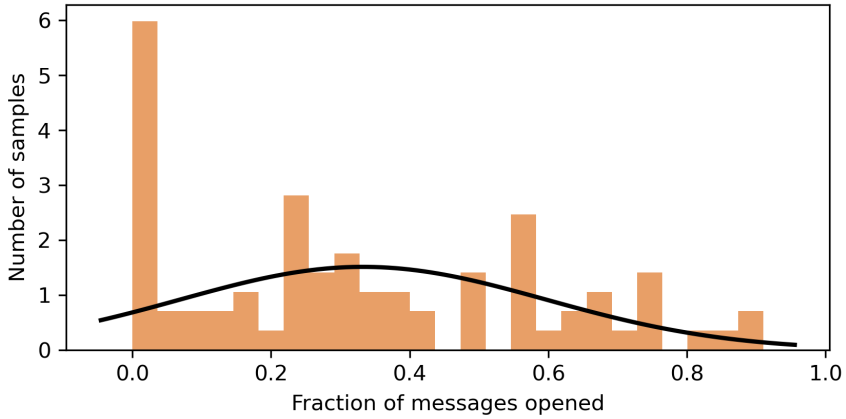
Considering that the scenarios had different levels of information about the infection and the messages received, we look at the average number of interactions in each of the experimental scenarios. As seen in Fig 6.1 there is an initial

growth in all three lines, as at the very beginning the users initiate interactions, this is mostly by sending messages to each other, as at that point no other action is possible, until a message is received. This of course is different in the third scenario, which allows to block from the start.

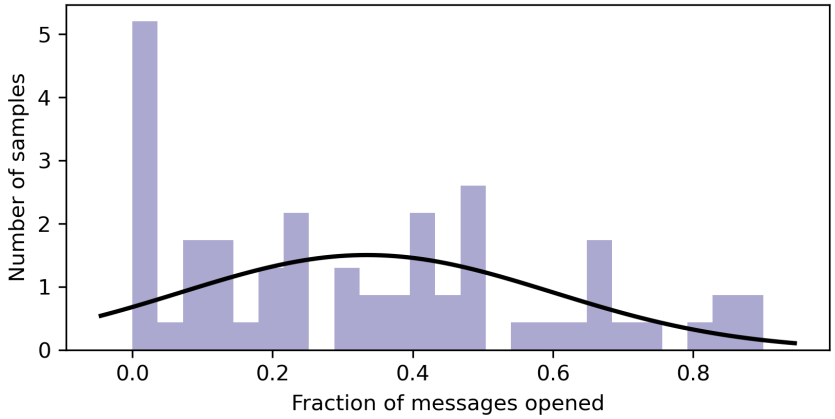
As we can see scenario two and three have more average interactions per second then the first. This could indicate the trust factor, which will change over time, and once users get acquainted, they will interact more but also, the lack of trust induced by the lack on information about the sender of each message in the first scenario.



(A)



(B)



(C)

FIGURE 6.2: The number of people infected given the fraction of messages opened. This is the measure of all messaged opened from the whole population, and not for individual nodes.

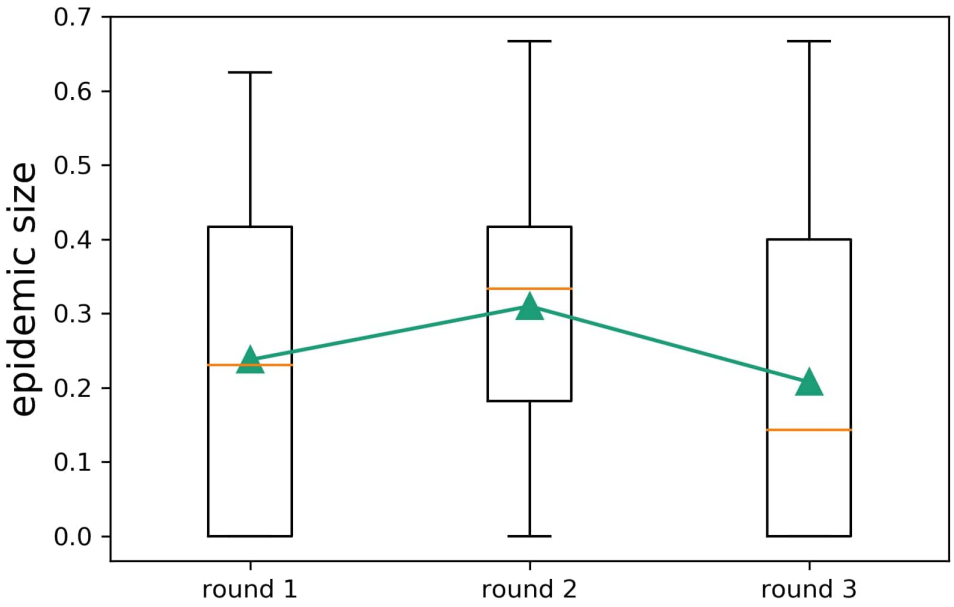


FIGURE 6.3: The size of the epidemic in each experimental scenario, which we also refer to as rounds.

The exchange of message is what lays the base for the infection. As users interact, they build trust and share more messages. This experience builds robustness, the more the users learn, and more they interact with each other, the less likely they seem to become infected. This can be observed in Fig. 6.2, where more people get infected with a smaller number of opened messages, get infected early, and thus becoming passive. Looking at the epidemic size in Fig. 6.3, we see that the fraction of infected varies across scenarios, with most infected individuals being in round 2. We find the median and confidence interval for each round:

- Round 1: 0.23 (CI 0.95 [0.0, 0.62])
- Round 2: 0.33 (CI 0.95 [0.0, 1.0])
- Round 3: 0.14 (CI 0.95 [0.0, 0.67])

Though the intervals are big, the median of round 2 is indeed larger than in the other rounds. The number of messages open would be one of the main causes for that. The change of the opening behaviour, could be either due to trust of nodes or change of their strategy. We also bare in mine the difference between the scenarios, in which during the first scenario users have very few features enabled, and we gradually add this. From second scenario the users gain the knowledge of whom they interacted with, which seems to change the epidemic size. We use Kolmogorov–Smirnov test [Hodges, 1958] to compare the distributions. The null hypothesis of the test is that the two distributions are the same. To reject the null hypothesis we should expect a small p-value respect to a significance level. D (i.e., KS statistic) is the maximum distance between two distributions, the smaller

that distance is the more similar the two distributions are, and p-values higher than the significance level of 0.05 mean that we cannot reject the hypothesis

- rounds 1 and 2 KS statistic: 0.14, p-value: 0.99
- rounds 1 and 3 KS statistic: 0.19, p-value: 0.85
- rounds 2 and 3 KS statistic: 0.33, p-value: 0.2

As clear from the p-values we cannot reject the null hypothesis for any of the pairs of distributions.

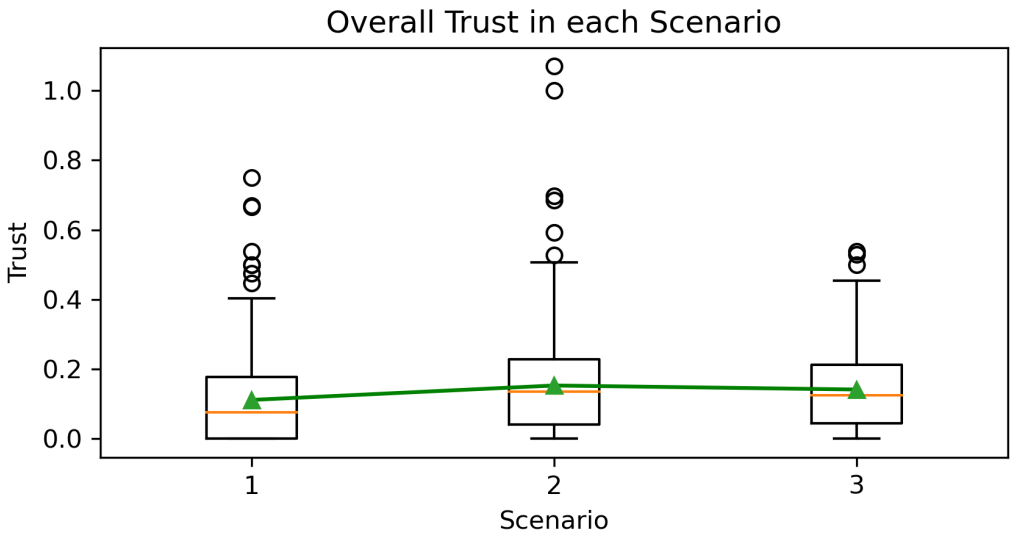


FIGURE 6.4: The average trust towards other nodes in each scenario. Using our trust metric, we find the average trust between node i and his/her neighbours

The general overview of the interactions (Fig. 6.1) and the probability of infection (6.2) indicate a rate of learning over time, and in line with the literature we find that the information exposed about the infection impacts user perception [Adali et al., 2010; Heartfield and Loukas, 2018; Heartfield and Loukas, 2016b; C. Shao et al., 2018; Bilge et al., 2009].

Using our metrics of trust and gullibility introduced in Chapter 5, we measure how this varies among the population. The overall trust we measure, is the trust that node i exhibits on average towards all of her neighbours, and as we can see from Fig 6.4 although overall trust is very similar across the board, it is higher in scenario 2 and 3 in respect to the baseline. Using KS-test we compare if the distributions are the same.

- rounds 1 and 2 KS statistic: 0.17, p-value < 0.001
- rounds 1 and 3 KS statistic: 0.17, p-value < 0.001
- rounds 2 and 3 KS statistic: 0.06, p-value: 0.67

The null hypothesis of the KS-test cannot indeed be ruled out in case of rounds 2 and 3. The first round instead is the most different respect to the others. In the first scenario the users had no information about the infection, from Fig. 6.1 we see that they also were the least active in that scenario. Once the users were informed about their state in scenario 2 and 3, their behaviour would then be different. In fact in respect to scenario 1, trust increased once the participants were given more information about each other.

The gullibility of the users follows a bell shape distribution mostly, as majority of population have 'neutral' level of gullibility seen in Fig. 6.5. This means that most of the users take some precautions and have some knowledge of cyber threats, with a few of them having little security awareness and a few having a high awareness. We plot the gullibility distribution in Fig 6.6 separating those who get and do not get infected. We do not observe significant changes (i.e. those who get infected are not more gullible on average). We test our observations with KS test:

- rounds 1 and 2 KS statistic: 0.68, p-value: 0.5
- rounds 1 and 3 KS statistic: -1.17, p-value: 0.24
- rounds 2 and 3 KS statistic: -1.72, p-value: 0.09

Across the board the test confirms the similarity of the distributions (i.e., the null hypothesis cannot be rejected). In Fig 6.7 we look at the distribution of trust. We observe that most participants exhibit little trust towards each other with only a few nodes opening over half the messages. Interestingly, this trend is not observed in the first scenario where we see the trust ratio being the lowest. This is line with the fact that it is the baseline and no information about senders if provided.

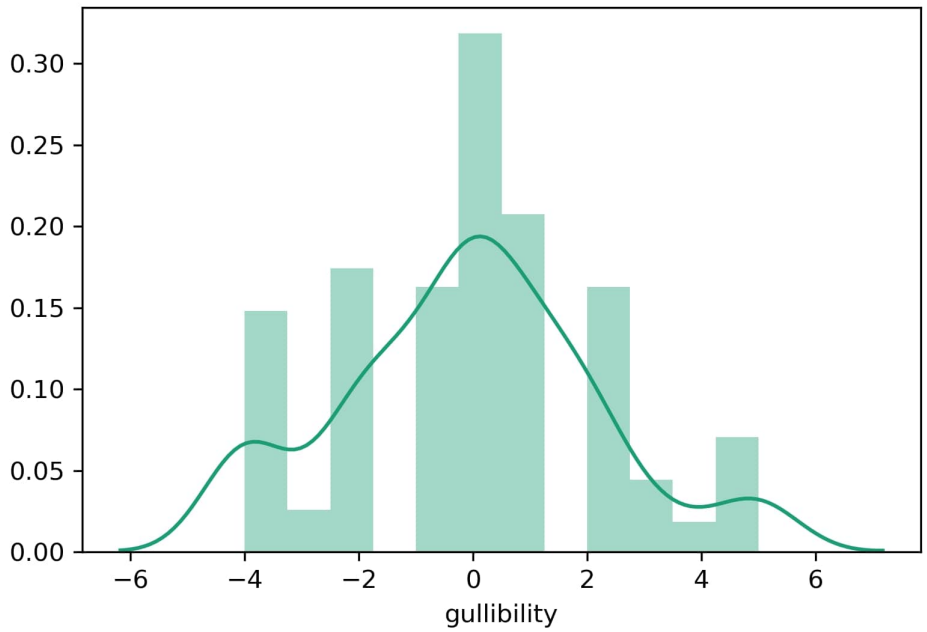


FIGURE 6.5: The distribution of user gullibility. Using the questions from the survey we defined a metric in chapter 5 to measure how gullible the user is. The lower the number the less gullible a person is.

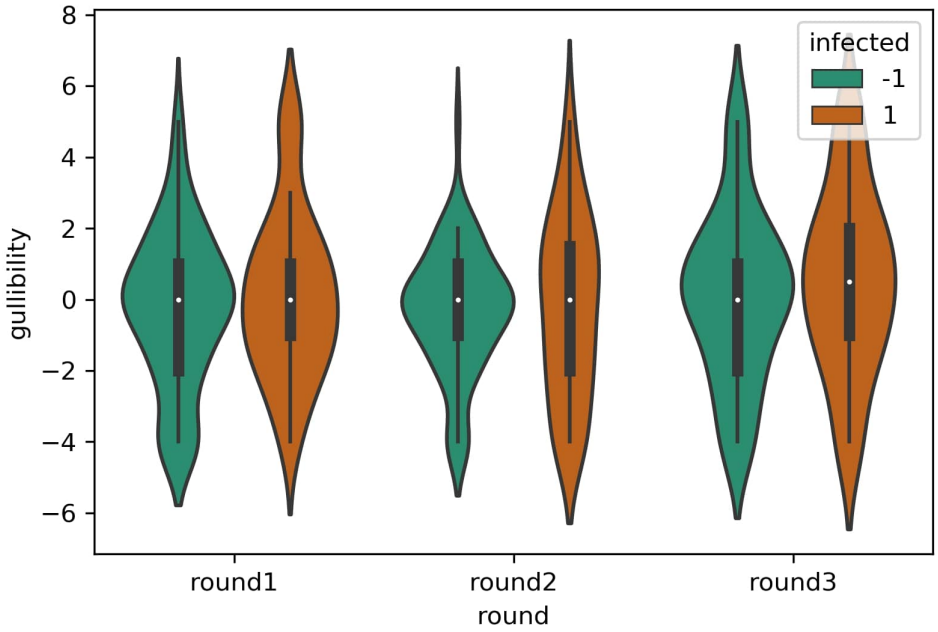
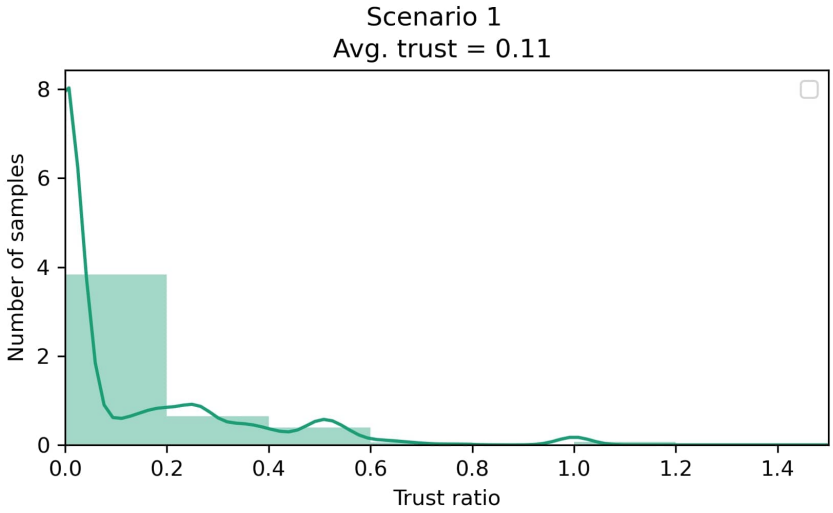
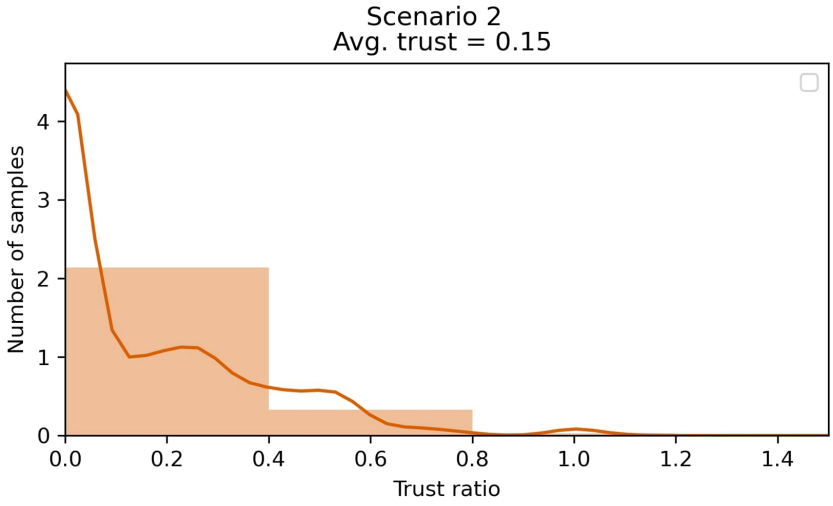


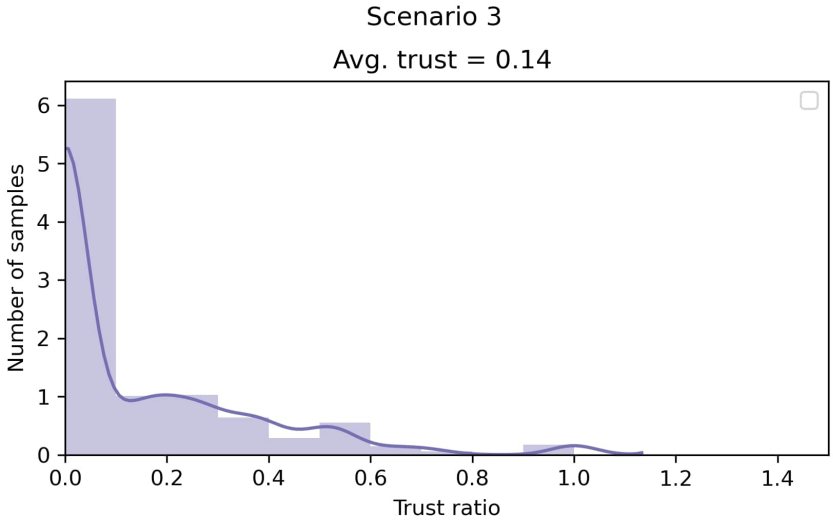
FIGURE 6.6: Distribution of gullibility for users that got infected (orange) and those that did not (green) across scenarios. The distribution of data in the violin plot shows the density of users infected depending on their gullibility level.



(A)



(B)



(C)

FIGURE 6.7: The distribution of average overall trust in a given scenario. Each panel correspond to each scenario in a numerical ascending order. We use the same value of bins for all plots, in 6.7a and 6.7b we can see multiple bins of same height next to each other.

Using the trust and gullibility metrics, we investigate if the gullibility has an impact on trust. Considering different network configuration of the Watts-Strogatz model, which changes after all three experimental runs have been finished, we look at how the correlation changes, after the network has been re-connected. This is across all of the experimental scenarios, per each network. This means that each scenario (1, 2 3) have been completed, and then the parameters of the network have changed.

There is a growth in trust, after a new set of neighbours have been connected, as we see in Fig. 6.8, in networks 2 and 3, there is an upwards trend of that. The third network, is a random graph with low clustering, the first instead it is ordered ring with high clustering. So beside time, also the type of the network might impact trust since it constraint differently the spreading of the cyber threats.

From that we can say that that less gullible population has lower trust overall. Because we know that our trust metric considers number of opened messages, the higher the trust ratio, the more messages are opened. In other words more gullible people are more trusting and they open more messages.

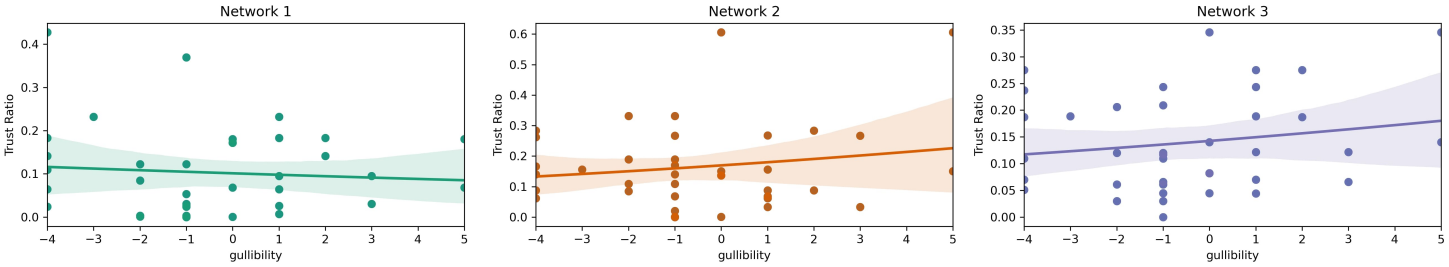


FIGURE 6.8: Correlation between trust and gullibility. The network used was Watts-Strogatz with $m = 4$ and different parameteres of p. In Network 1: $p = 0$; Network 2: $p = 0.2$; Network 3: $p = 1$.

6.1.2 Prevalence of Spammers

Social networks are subject to a variety of behaviour and intentions of use. As a lot of other OSN, our platform too had a number of spammers, that is people who chose to send a high volume of messages in a short amount of time or focus on sending only, with a very small fraction (or even none) messages opened.

We investigate the widespread of this behaviour, finding that there is only a small fraction of people in the general population, who focus on spam only on few occasions. We do not remove this behaviour from our data, since these users decided to interact in such as way, and this kind of behaviour exists on standard OSNs.

The most messages sent by a spammer was 107 per 60 seconds (length of the experimental run), which is 1.7 messages sent per second on average.

Here we investigate further on the presence of spammers. In Fig. 6.9 we plot boxplot of the inter-event time for each round. The bullets are the "outliers", hence those below the box are the potential spammers. This again shows that the

prevalence of spam is relatively small, and that most people take approx. 4.5 seconds to exchange a message. This suggests that during that time, they would take other actions, such as open or delete. In round 3, as seen in Fig. 6.9, the range of time between two events is greater, as here there is the most functionality and also users have learned the most about their friends by this experimental scenario. The longer times here could suggest a more thorough review, before the user makes a decision to open a message. We test the findings with KS test. The large KS statistics and small p-values across the board clearly show that the distributions are different.

- rounds 1 and 2 KS statistic: 0.52, p-value < 0.001
- rounds 1 and 3 KS statistic: 0.51, p-value < 0.001
- rounds 2 and 3 KS statistic: 0.64, p-value < 0.001

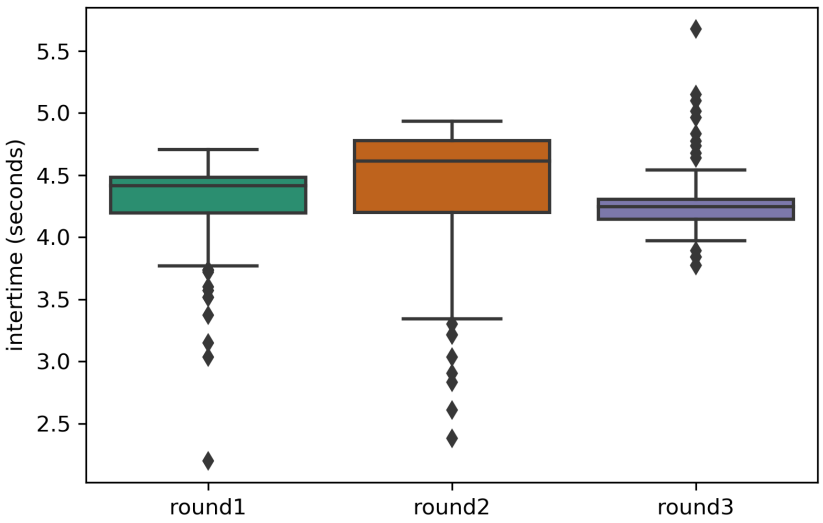


FIGURE 6.9: The range of inter-event time in seconds, per each experimental round.

6.1.3 User approach to non-human players

A large majority of actions took place between human players, with only 11% of total interactions taking place between a participants and an AI bot. The overall trust towards bots is also lower as seen in Fig. 6.10, with an average of around 10%, which compared to the rest of the agents is around 20% in Fig. 6.11. Gullibility does not seem to influence the attachments to bots. Here we do not observe any obvious patterns.

FIGURE 6.10: User gullibility and trust behaviour towards bots agents

FIGURE 6.11: User gullibility and trust behaviour towards human agents

6.2 The impact of trust and gullibility

As we see from the previous section trust and gullibility play an important role in the behaviour of the users. The number of opened messages is correlated with user gullibility, and this can change over time, as indicated by the trust ratio. Depending on the information we give to the participants, the trust ratio varies and seems to range across different scenarios, with some pairs of nodes showing higher levels of trust than others. Because of this, we investigate what drives the high levels of trust, and if gullibility and past actions play a role in this.

Firstly in Fig. 6.12 we observe the fraction of neighbours each node has interacted with. The baseline scenario 1 as expected has a wide range of data, as the users are likely to trial their friends, due to the fact they do not know whom they are interacting with in their timeline. Over time however we don't see a clear

trend, but at the end of each scenario interestingly most users had at least one interaction with one of their friends.

However, the Kolmogorov-Smirnov test:

- rounds 1 and 2 KS statistic: 0.14, p-value < 0.001
- rounds 1 and 3 KS statistic: 0.04, p-value: 0.91
- rounds 2 and 3 KS statistic: 0.15, p-value < 0.001

suggests a difference between scenario 2 and the others. In scenario 1, users did not have information about the identity of their neighbors. In scenario 3 they could block some of them. Scenario 2 is the one where users interacted with a largest fraction of their connected friends.

We know that trust changes over time (Fig. 6.13), and that gullibility has an impact on trust. We analyse the impact of infection on trust, and if becoming a compromised node, will change the user behaviour to being more passive. We look at past interactions with nodes who are connected across all scenarios, to understand if they form clusters. These clusters might affect trust and infection, and for the purpose of analysis we are testing if time-integrated interactions will have higher levels of trust and exchanged messages, due to the amount of time two nodes have been connected together.

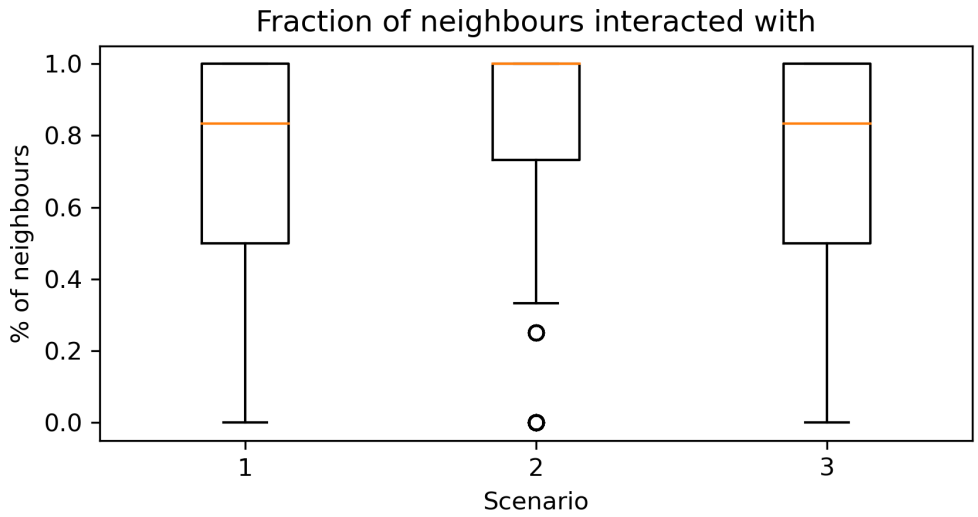


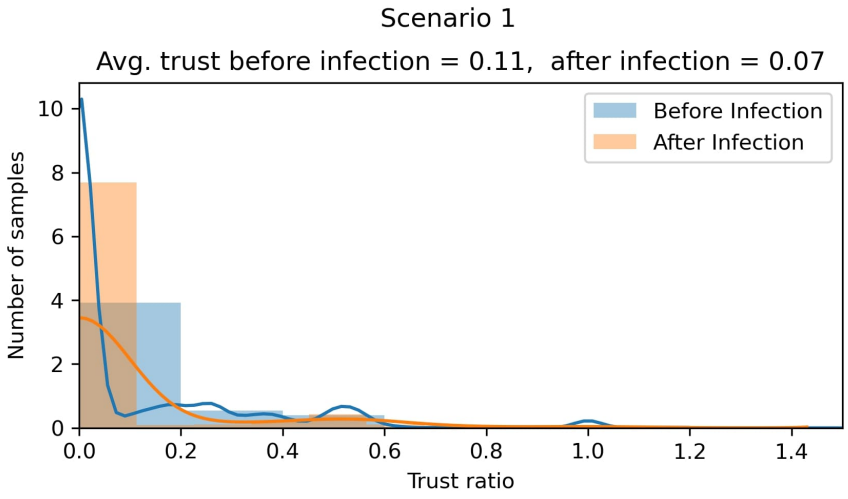
FIGURE 6.12: Fraction of neighbours interacted with across the whole population.

6.2.1 The effect of infection on trust

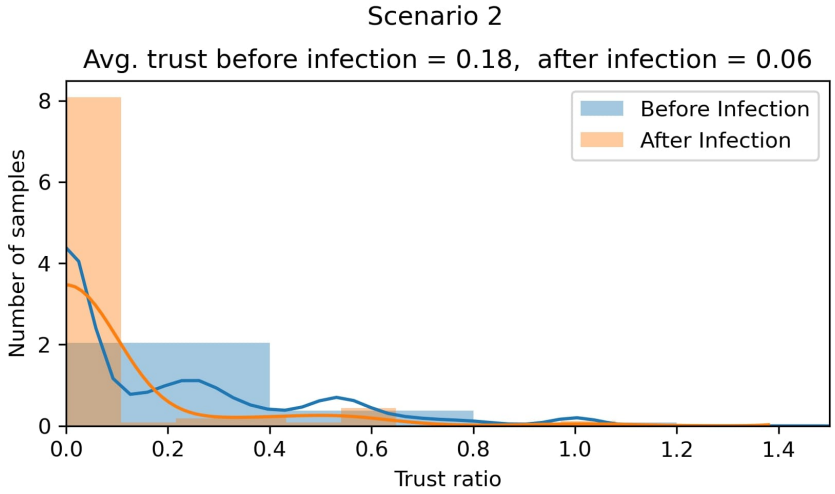
As we saw above, most users have at least one interaction with one of their neighbours (6.12) and most users don't trust each other (Fig. 6.7). This kind of behaviour leads us to study users who form clusters of trust, in which they interact with each other a lot, and how getting infected impacts the trust. Exposure to information is non-trivial, we thus separate this data for each scenario. In Fig. 6.13

we observe how infection changes the trust ratio. Looking at the average overall trust ratio before the user gets infected, and after they get infected, we can see that infection has a significant impact on the change of behaviour. The smallest change in trust is observed in scenario 1 (Fig. 6.13a), as there is no information given to user regarding the infection, thus this is based on random interactions. Once we however provide this information, we can see a much considerable change in Scenario 2 and 3 (Fig. 6.13b, Fig. 6.13c), with average trust ratio drop of 12%.

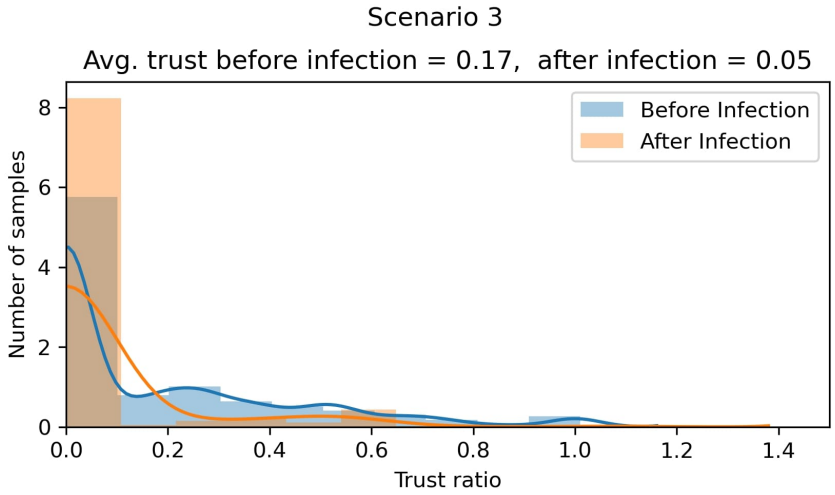
We compare overall interactions with the baseline observing that the behaviour changes, and is driven by the infection, we turn our attention to past interactions, and the impact of user characteristics on infection. The temporal connections between nodes change as well, with on average users dropping about 40% of the number of people they interact with in their neighborhood as seen in Fig. 6.14. Here we consider the baseline, as the initial fraction of connections created by each node, in other words how many users did node i interact with, and how many of them did she keep in touch with during all three scenarios. The links which remain throughout all three rounds, are the ones we look at next.



(A)



(B)



(C)

FIGURE 6.13: The distribution of trust in a given scenario. Each panel correspond to each scenario in a numerical ascending order. Using the same bins for all three plots, we can see that in 6.13a and 6.13b there are bins with the same height.

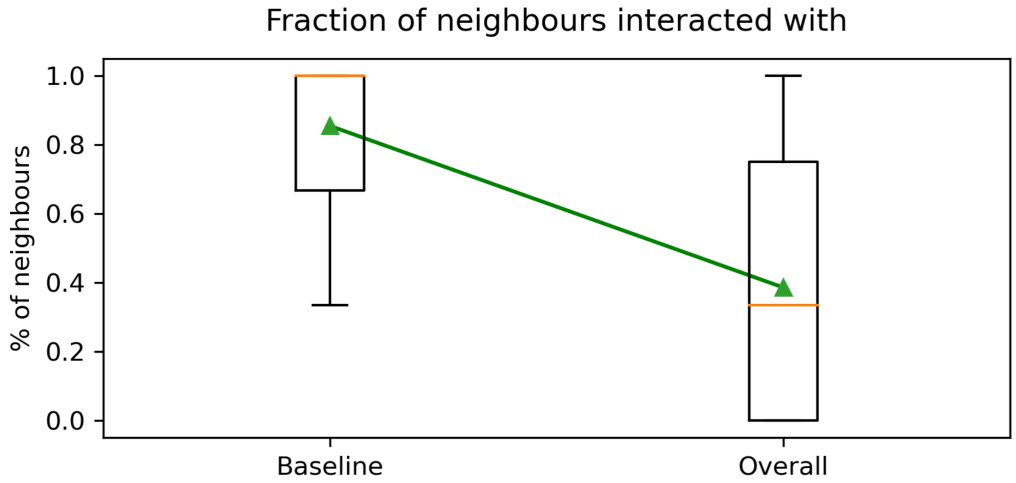


FIGURE 6.14: The fraction of population with constant interactions. Baseline is the first scenario, and we combine the nodes, which have interacted across all three scenario.

6.2.2 The effect of trust and gullibility on infection

Presence of trust and gullibility as well as the actions taken by users which are driven by those characteristics have an impact on the size of the epidemic (Fig. 6.3). The epidemic grows as users learn about infection in scenario 2, but drops as they gain experience and trust towards each other, this with combined gullibility factor (the more gullible the more messages you open) indicates that with time, the participants become less gullible and learn how to avoid infection, as the epidemic size drops.

The changes of trust (Fig. 6.13) and the variation of epidemic size (Fig. 6.3) are correlated. The only way to get infected is by opening a message, and over time users change their behaviour, and open less messages (Fig. 6.2). Trust and gullibility are correlated with how many messages a node will open, and thus impacting the infection. Here we explore the impact of these characteristics on infection, as we look at clusters with higher trust levels.

In Fig. 6.15 we plot the change of trust, as a function of time and the fraction of nodes infected. We explore how trust shifts, once the epidemic size has grown. As we observe in Fig. 6.15 we see that in each scenario, as the infection grows, the trust ratio changes, in the beginning the trust levels rise, indicated by brighter areas, before dropping towards the end. We also notice that in the final scenario in Fig. 6.15c, the epidemic size is the lowest.

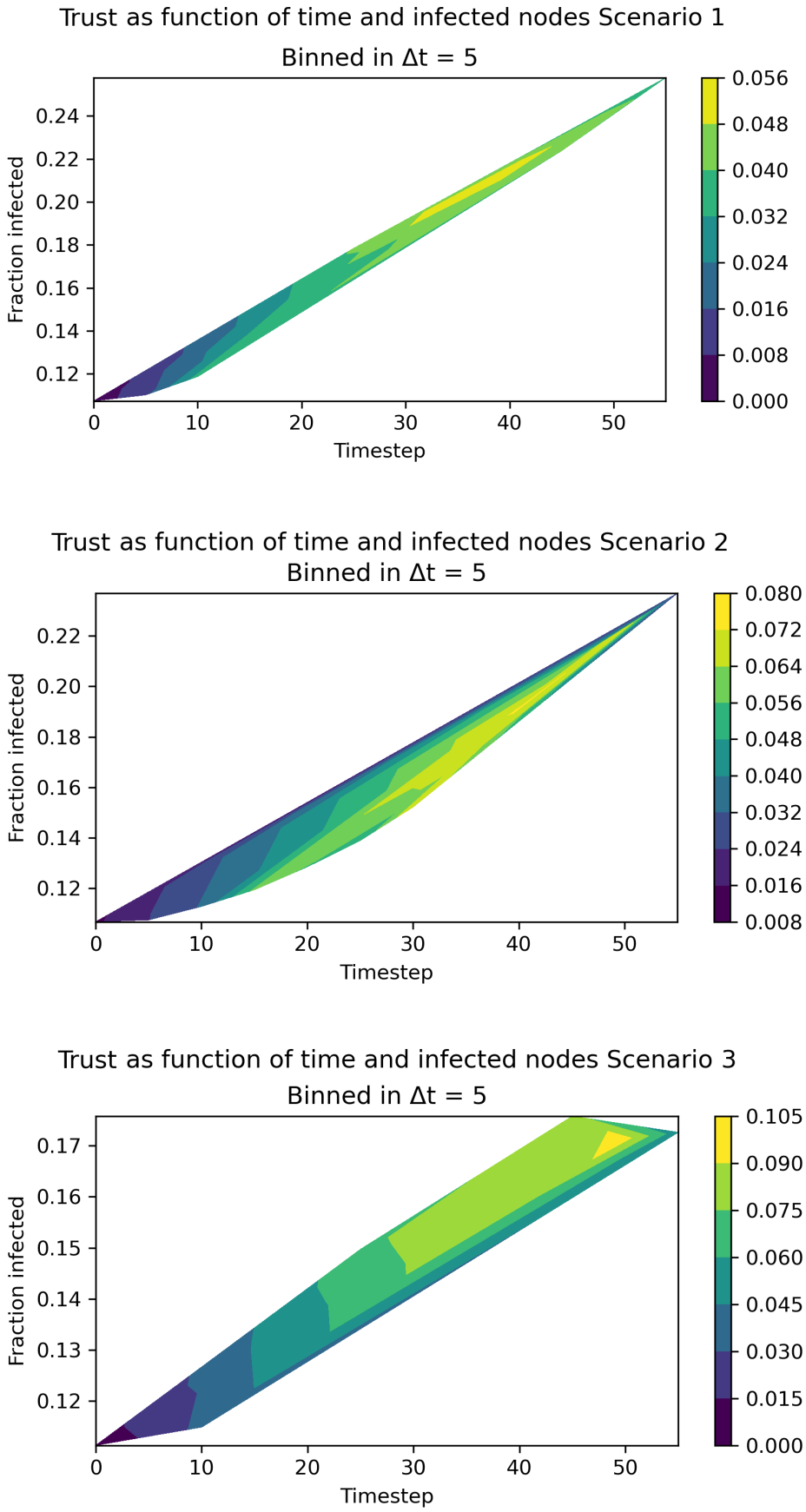


FIGURE 6.15: Over time (x-axis) the fraction of nodes infected (y-axis) increases. At each time-step $\Delta t = 5$ we measure the levels of trust across the whole population, to see how infection changes that metric.

Time-aggregated trust and community clustering

During each run, that is three experimental scenarios with same network parameters, the neighbours of each node i remain the same. To focus on the historical data, we take the nodes who have interacted across all three scenarios, these pairs here have to had interactions in all three of the scenarios to be taken into account.

Exploring the interactions on each network, as in Fig. 6.8, we look at nodes who were connected across all three networks, after the parameters have changed. In H_1 we state that trust evolves over time. This is based on the assumption that the longer you are connected, the higher your trust would be, as you have built up a history with your neighbours. We compute trust ratios between pairs who are connected across all three networks, and in Fig. 6.16 we observe that there is an increasing trend across scenarios, and across network, with regular high clustered network having lowest trust, to random graph having highest. The median and error ranges we find show that overall the trust indeed grows in different network:

- Network 1: 0.03 (CI 0.95 [0.0, 0.63])
- Network 2: 0.1 (CI 0.95 [0.0, 0.61])
- Network 3: 0.14 (CI 0.95 [0.0, 0.54])

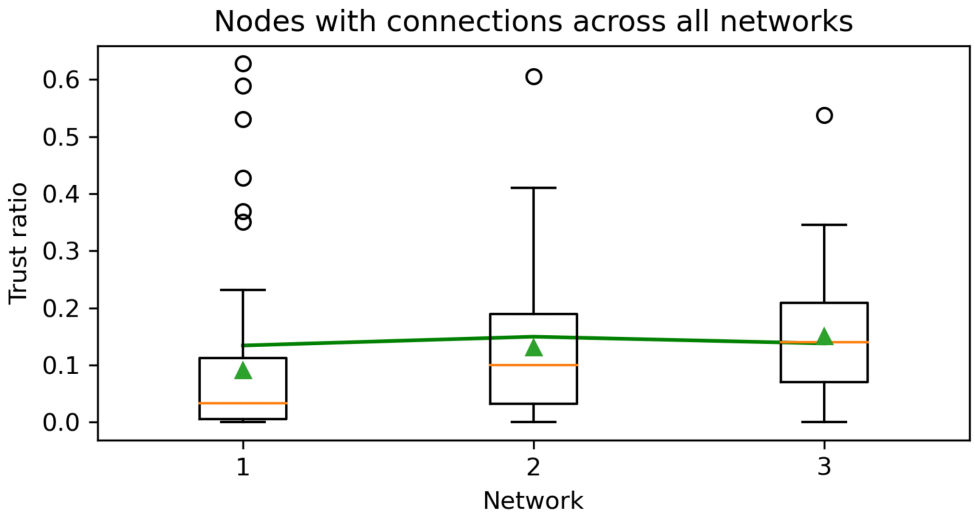


FIGURE 6.16: Overall average trust ratio computed for pairs of nodes, who are connected across all three networks with different parameters. The network used was Watts-Strogatz with $m = 4$ and different parameteres of p. In Network 1: $p = 0$; Network 2: $p = 0.2$; Network 3: $p = 1$.

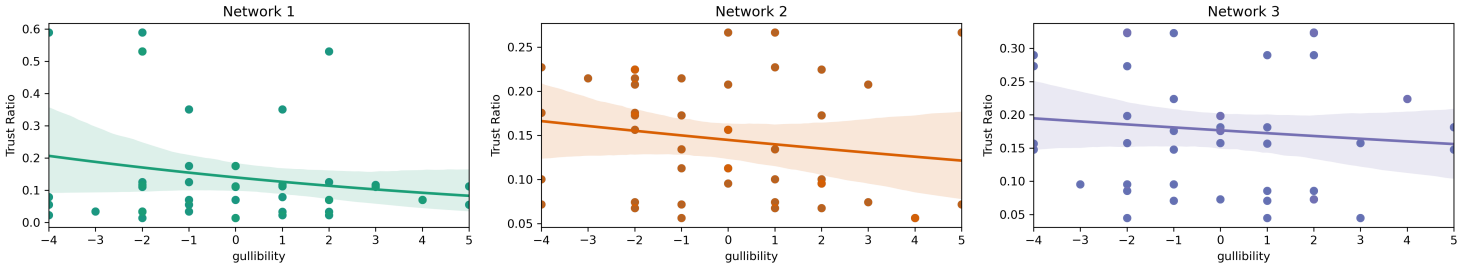


FIGURE 6.17: Correlation between trust and gullibility across nodes with past connections in all three scenarios.

Looking at how the gullibility correlates with trust in the communities that are forming, interestingly we notice that the less gullible you are the more likely you will form a connection with someone else, and the more you will trust that person as seen in Fig. 6.17.

6.3 Network Effects

So far, we have observed how trust and gullibility impact the spread of malicious content, as after infection the trust and the number of messages between pairs of nodes decreases (Fig. 6.2), and less gullible nodes interact with less people, leading to higher likelihood of forming a cluster. Clustering becomes apparent when we look at neighbours who are connected with each other even after we change the network parameters. The 'friendship' remains, and we looked at how time-aggregated interactions impact trust in those groups.

The propagation of infection reduces the trust ratio over time (Fig. 6.15), meaning once a node gets infected, it reduces its interactions. The lower the trust (Fig. 6.7), the lower the epidemic size (Fig. 6.3). With this, we aim to isolate the networks effects behind the spreading of cyber threats, and examine if the position of a node in the network has an impact on its interactions and the possibility of getting infected. In other words, we are testing H_0, which is also associated with one of our key research questions, mainly the question tackling networking effects.

6.3.1 Impact of network connectivity on infection

Betweenness centrality of a node is the fraction of the shortest paths passing between every pairs of nodes passing through i respect to the total . This measure indicates how central a node is, based on number of shortest paths it has with all other nodes in the network. With betweenness indicating how central a node is, we look if nodes with higher values of betweenness are more or less likely to get infected. More generally we study the correlation between centrality and risk of infection.

The clustering coefficient for the graph is the measure of how connected the neighbors of each node are. Its the fraction of all possible triangles among all nodes that are connected together.

In Fig. 6.18 nodes that get infected have, on average, have lower betweeness centrality this might be due to the fact that on average only 20% of the nodes get infected and since the initial seeds are selected at random, the virus might not diffuse enough to see the most central, especially in case of high clustered networks like WS with p=0.

The clustering coefficient in Fig. 6.19 seems to have no clear trend. In some cases we do observe that the more clustered a node is, the more likely it will be infected (in the BA models), but in general there is no obvious patterns emerging. We however don't observe any strong correlation between infection and clustering as seen in Fig. 6.21.

The degree of a node is simply the number of connections it has. The effects of the degree do not seem to have a pattern, with various levels of infections, depending on the graph type (See Fig. 6.20).

From the three figures we can conclude that the propagation propagation of the threat is not just function of the position of the node, but it is driven by a complex interactions of factors among which the centrality of the nodes.

We compare the distributions (6.18 - 6.20). The Kolmogorov-Smirnov test in general across all the graphs, does not reject that the two distributions are the same.

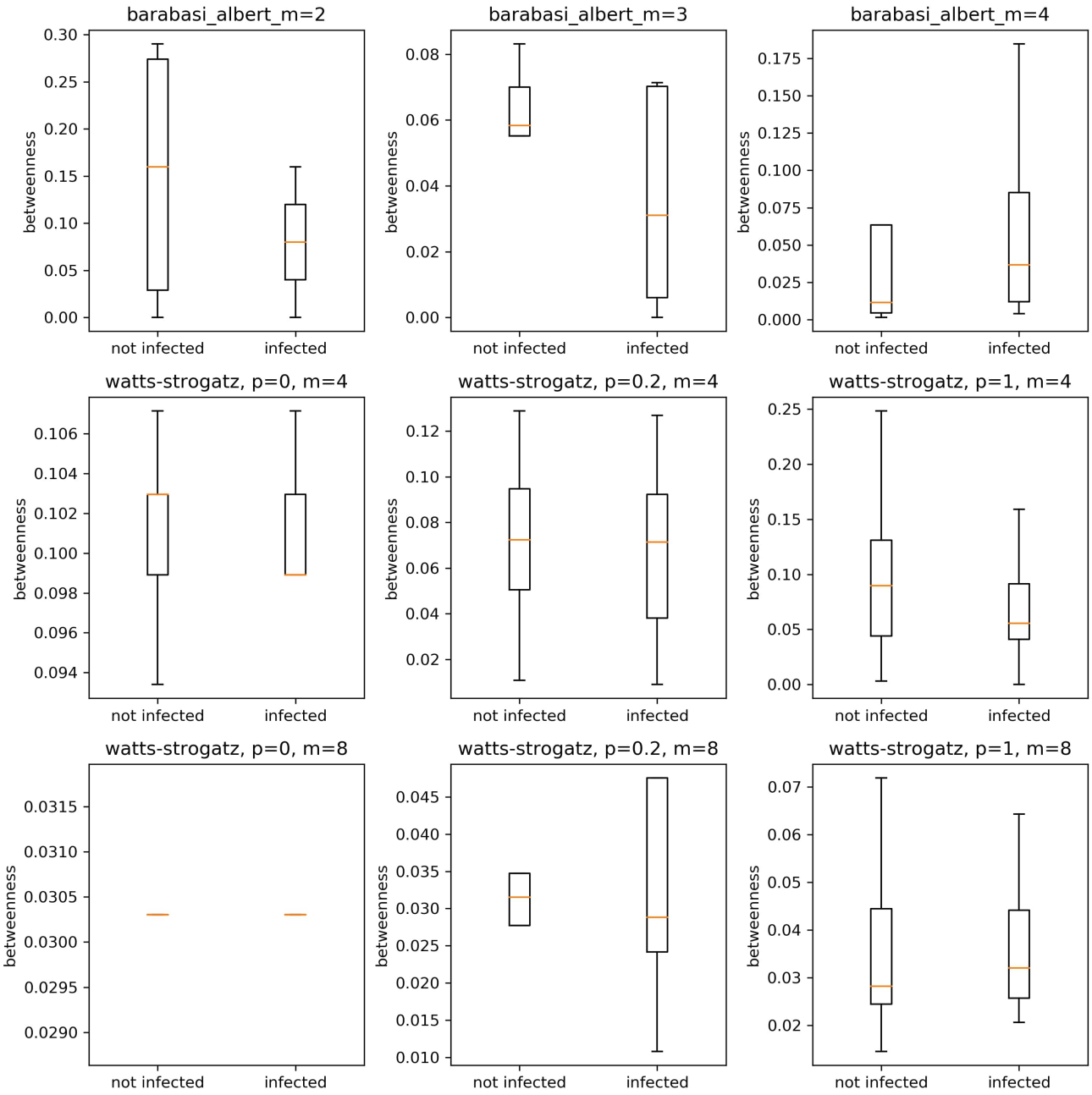


FIGURE 6.18: The measure of betweenness amongst the infected and non-infected population across different network parameters.

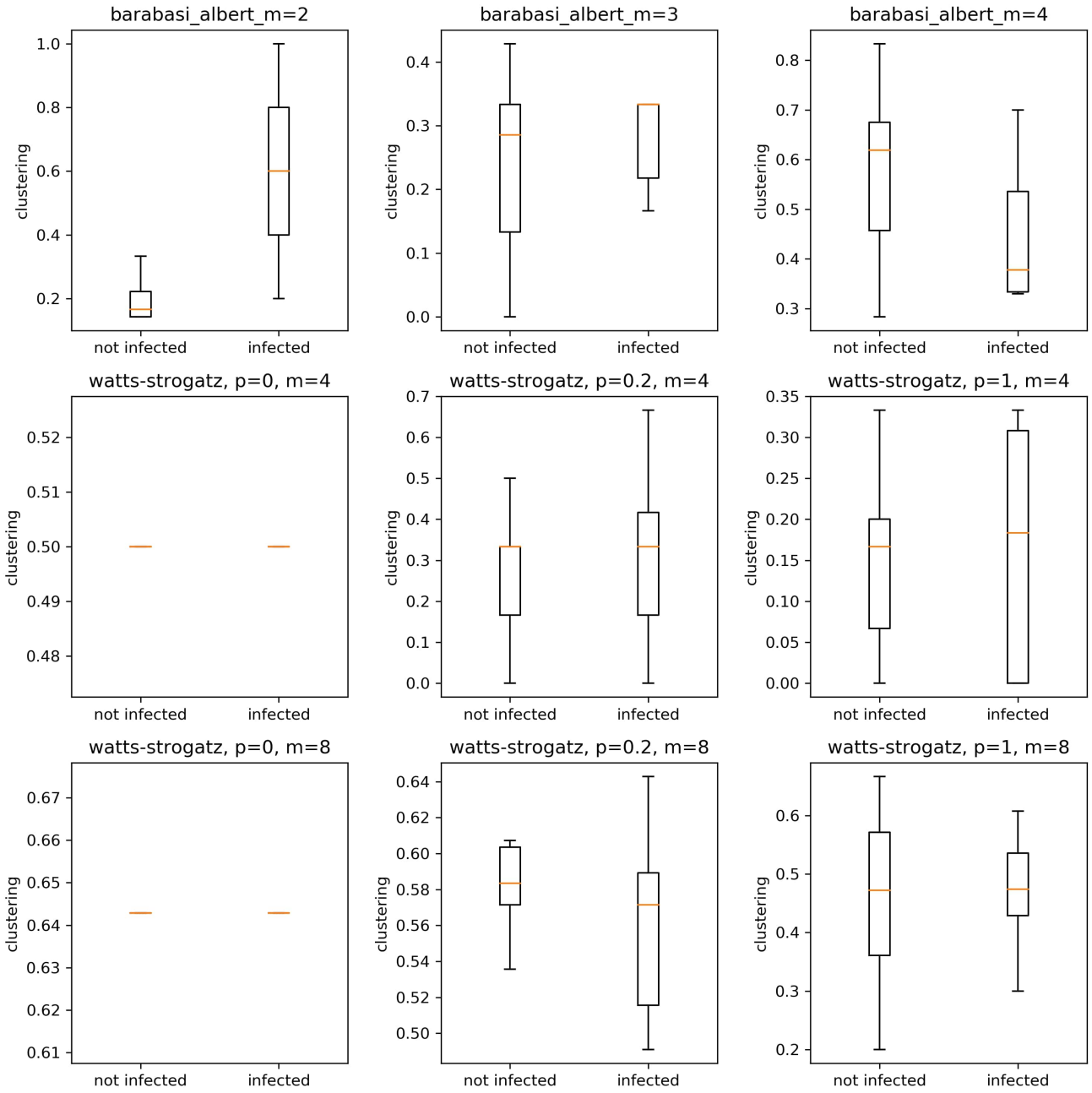


FIGURE 6.19: The measure of clustering amongst the infected and non-infected population across different network parameters

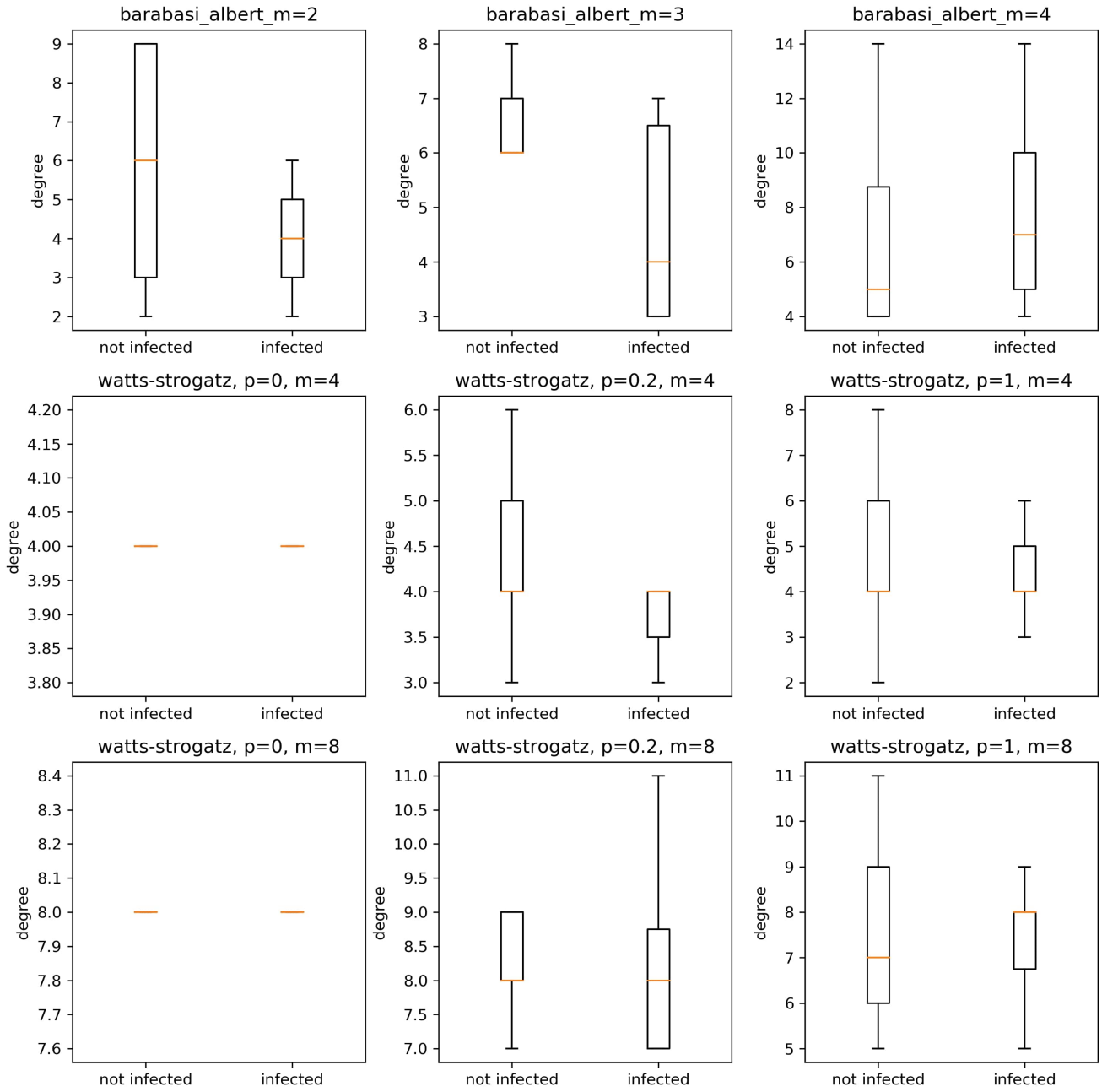


FIGURE 6.20: The measure of degree amongst the infected and non-infected population across different network parameters

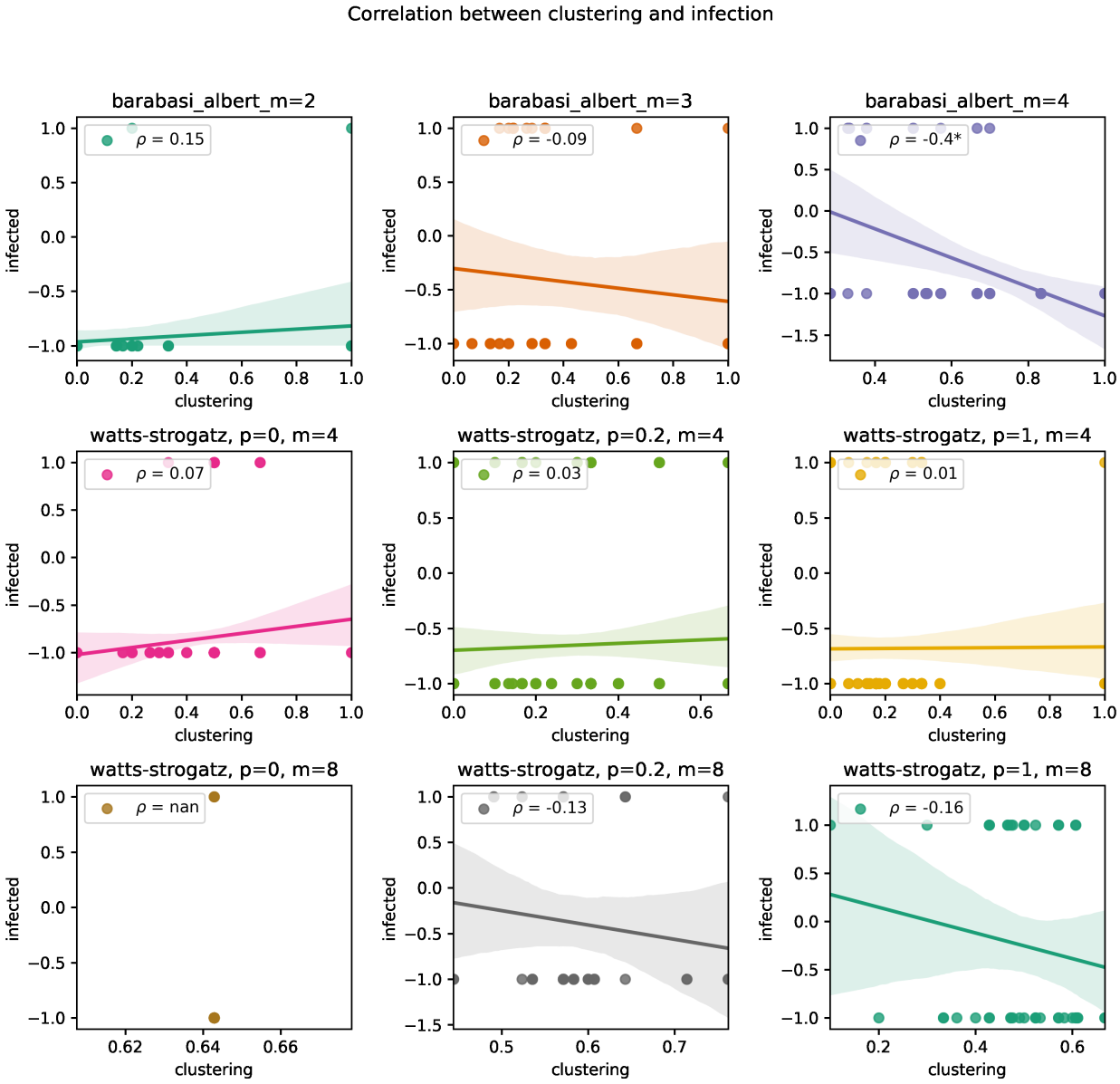


FIGURE 6.21: Pearson Correlation between nodes that have been infected in each network and clustering coefficient. 1 represents infected nodes and -1 are the nodes which have not been infected.

Blocking

In the third experimental scenario we have introduced the ability to block friends, which will not allow to send or receive any messages from that person. We investigate how much this functionality was used, by simply looking at how many users use blocking, and how many people have they blocked. From Fig. 6.22 we see that up to 40% of nodes have used this feature at some point. At most 15% of population has blocked 6 of their friends.

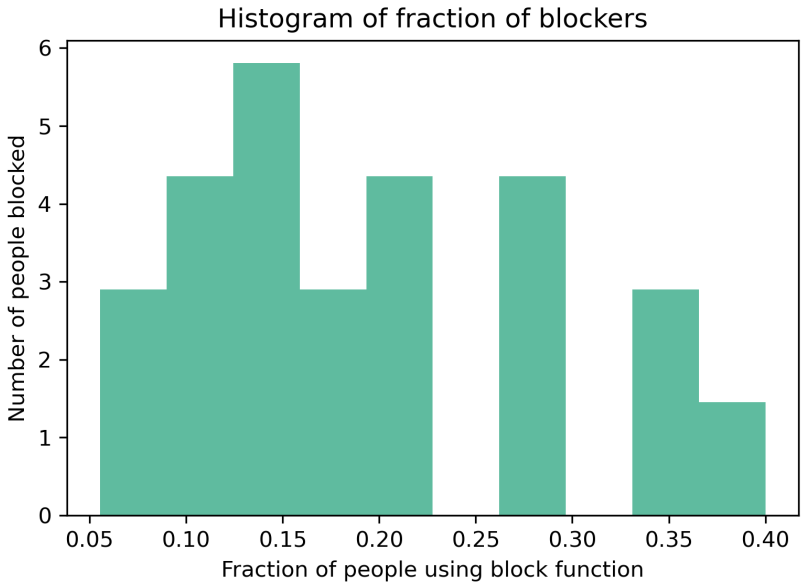


FIGURE 6.22: The fraction of users using the 'block' function in scenario 3

Out of the total population that have used the blocking functionality, we then see if this blocking action was repeated again towards the same user. We see in Fig. 6.23, that 20% of people did not block the same person more than once, with 50% of people have blocked 1 of their friends at least twice, and less than 1% of people have blocked 4 or more of their friends at least twice.

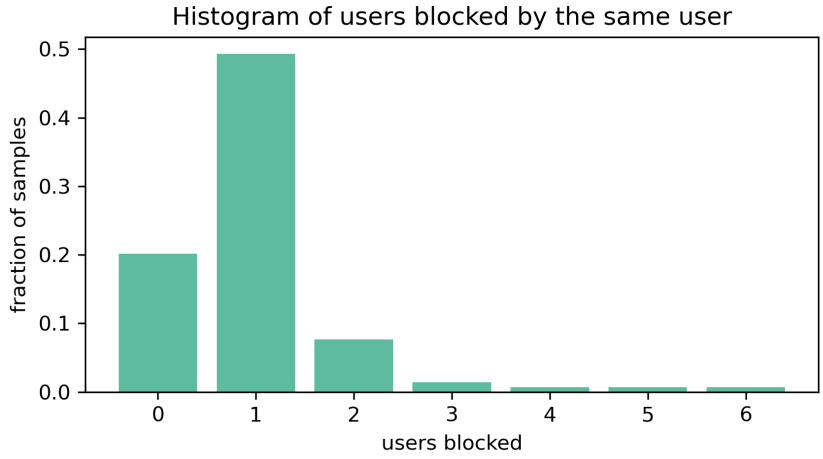


FIGURE 6.23: The number of people blocked by the same user, that is the number of friends node i has blocked

The effects of blocking on network Topology

Second, we see how blocking affects network topology. We use two metrics, node connectivity [Esfahanian, 2013] and the effective size [Burt, 2009; S. P. Borgatti, 1997]. Note that, the node connectivity is defined for a pair of nodes. Hence, for

each node we compute the connectivity between her and all her neighbours. Then we compute the average over all her neighbours to obtain the average connectivity of a node.
In both cases we do the same procedure. We describe it for the node connectivity:

- consider the initial topology, call it *G_noblock*
- consider the network with blocking (i.e. the modified network), call it *G_block*
- for each blocker, we compute the connectivity in *G_block* and *G_noblock* and take the percentage difference, in other words, we observe how much the connectivity decreased, in percentage, in the network with blocking

We also consider a random blocking model, which we refer to as the null model:

- for each blocker, we take the number of people blocked and we block random neighbours. Doing this we obtain a null graph *G_null* where have been removed the same number. of edges as in *G_block* (but these edges have been removed randomly)
- we repeat the procedure just described above to get the decrease in connectivity considering *G_null* instead of *G_block*

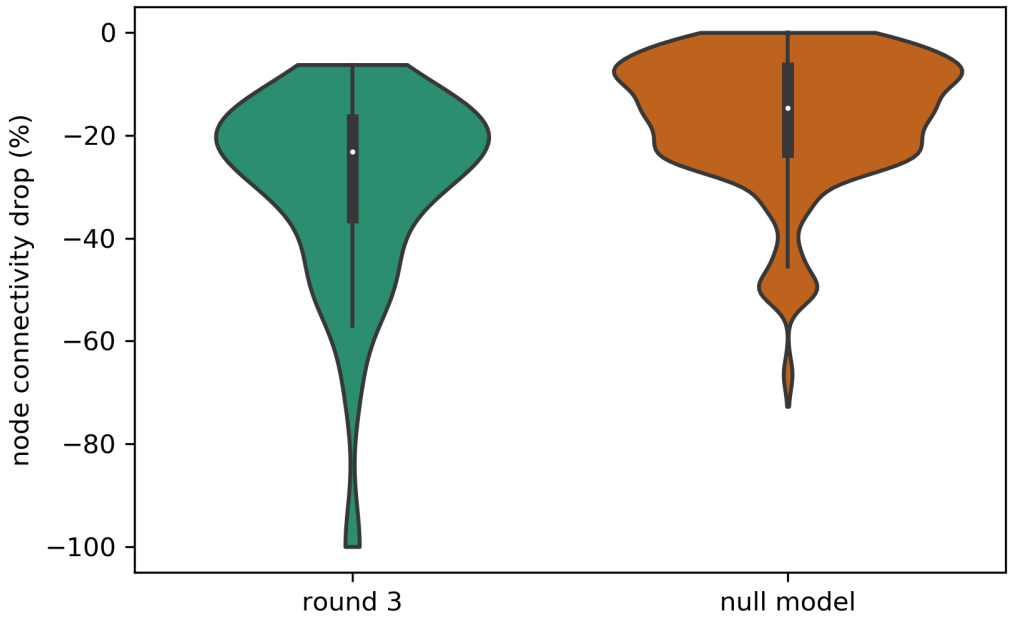


FIGURE 6.24: Comparison of the distribution of node connectivity in final scenario and null model, observing number of edges that are removed using the blocking functionality.

Using KS-test we see that the distributions are really different. The non-random blocking imply in general a much greater decrease in the node connectivity. in Fig. 6.24 is $D = 0.41$ (i.e., KS statistic), with the $p - value < 0.001$. The low value of p is below the significance level, so the large deviations between the two means we reject the null model for the node connectivity.

We repeat the same test for the decrease of the effective size (Fig. 6.25), obtaining analogous results of $D = 0.29$ and $p - value < 0.001$, so the two distributions are very different again.

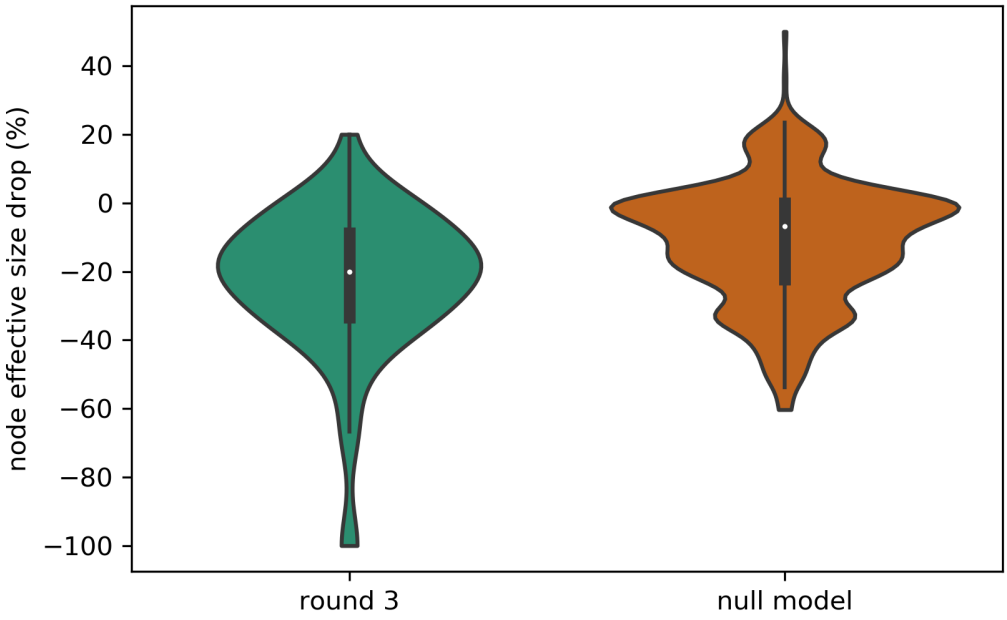


FIGURE 6.25: Change of effective size considering the blocking behaviour in final scenario and the null model.

6.3.2 Network properties driving user behaviour

We turn our attention to network properties and their correlation with user behaviour. Using clustering, degree and betweenness, we find the magnitude of impact on the number of items received, opened and sent.

In Fig. 6.26 we observe some emergent correlation between certain network properties with higher degree and betweenness in the BA model. This indicates that the network properties are correlated with the number of items received and opened. In other words, the more connections you have and the more in between of nodes you are the higher the exchange of messages is.

We also notice similar findings in the WS model. After clustering the correlation data in Fig. 6.27, there exist a cluster, in which number of items sent tie in with the number of connections.

n.b. Detailed correlation plots available in Appendix B

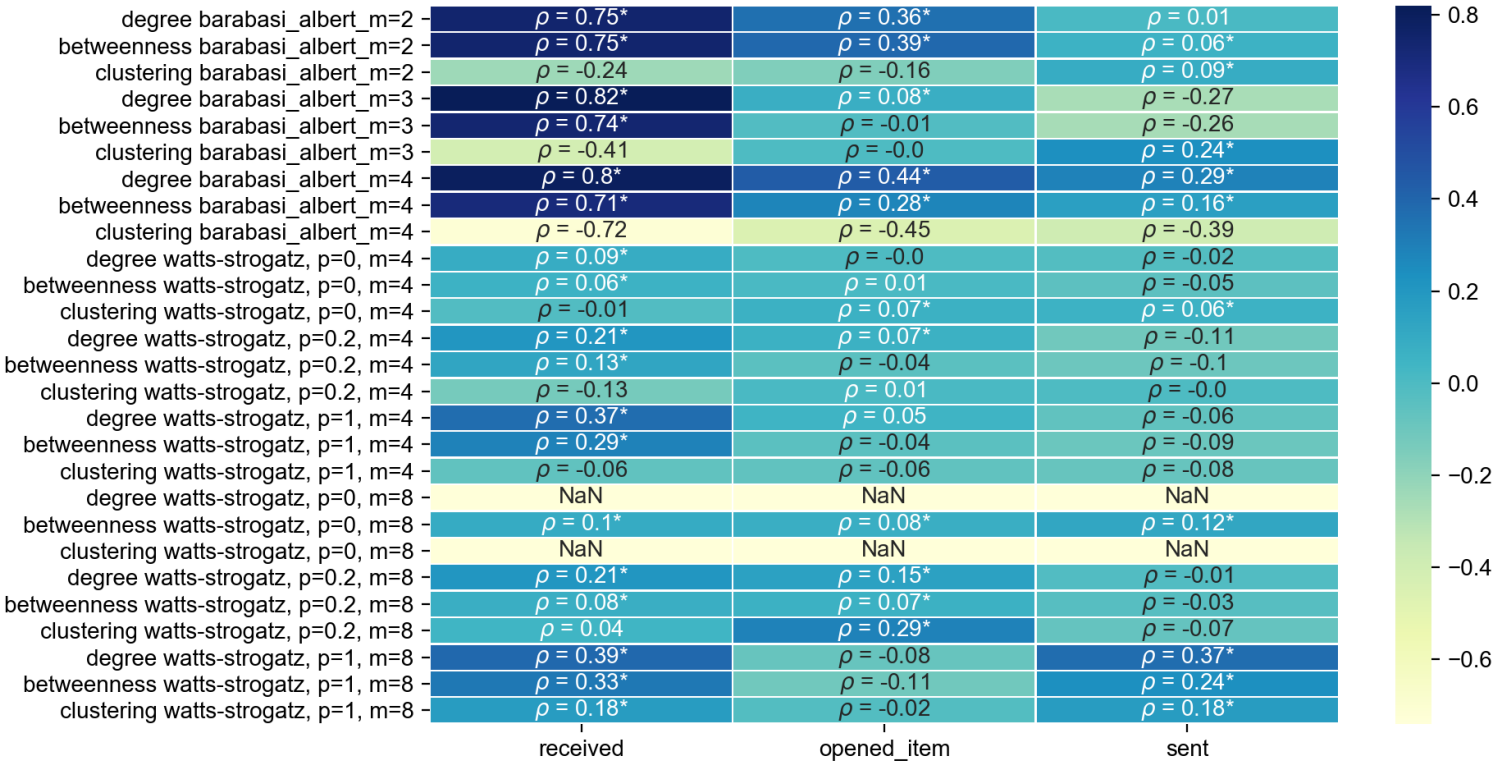


FIGURE 6.26: Heatmap displaying the correlation significance (* indicates that a correlation is significant) between user actions and network properties

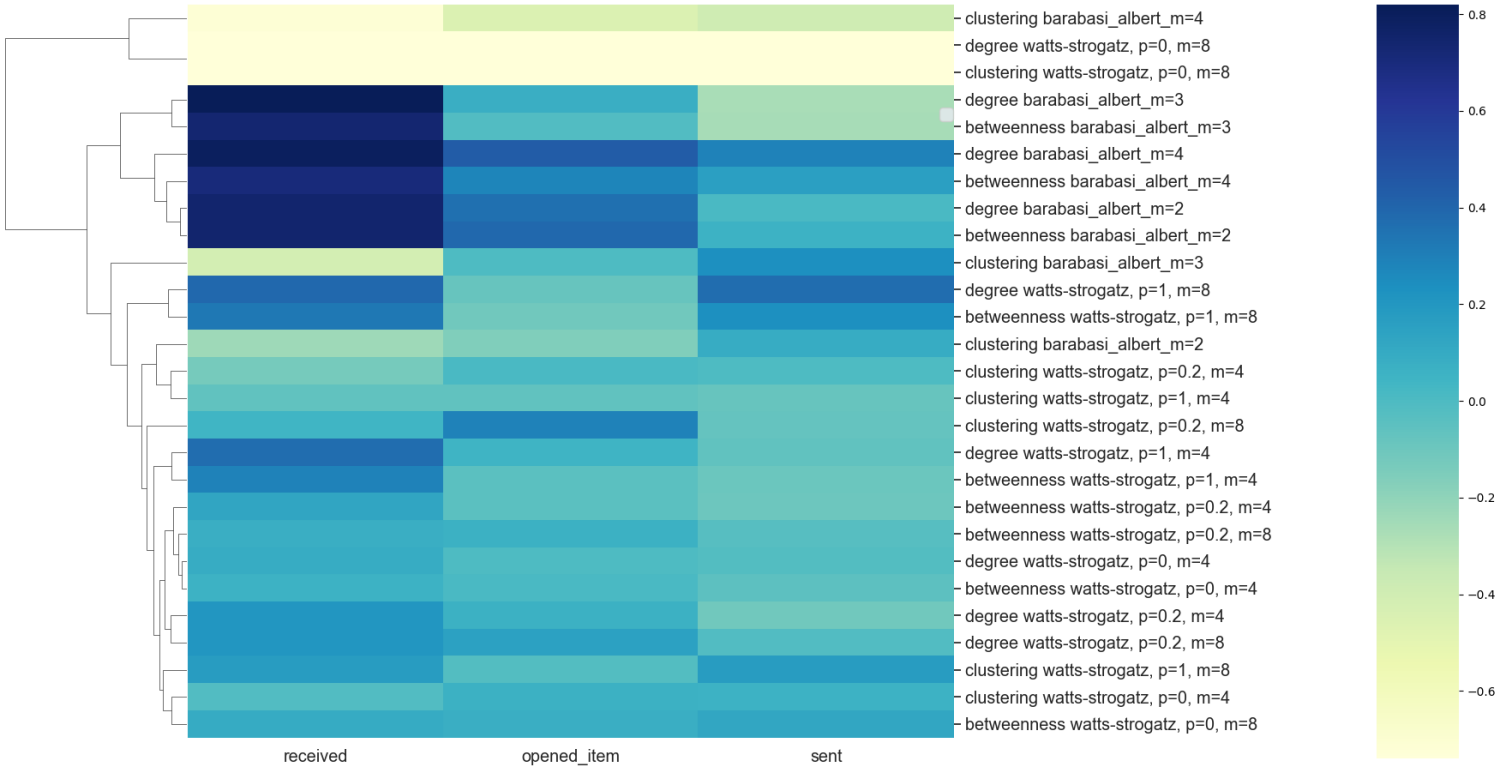


FIGURE 6.27: Clustered heatmap representing reordered data based on significance levels

6.3.3 Reactive Behaviour

The reactive behaviour of the participant, is the response (reaction) to the messages received i.e. individuals who receive more messages are also prompted to send more messages. We calculate the correlation between number of messages received and sent, so if you receive more messages, are you likely to reply.

Here we investigate the presence of a reactive behaviour on different network topologies. Overall in some cases we observe a positive (and significant) correlation between sent and received messages. This is mainly for the nodes with higher degree, as we see in most cases in Fig. 6.28. The more populated and more connected the network is, the more activity it displays, with higher response rate after receiving a message. Simply put more connections and more messages received, mean that you will send more. In a couple of cases we see a negative correlations, that is to say the higher connectivity of a node in BA model where $m = 3$ and random graph in which $p = 1, m = 4$ might impact this behaviour, however we do not have sufficient data to confirm this.

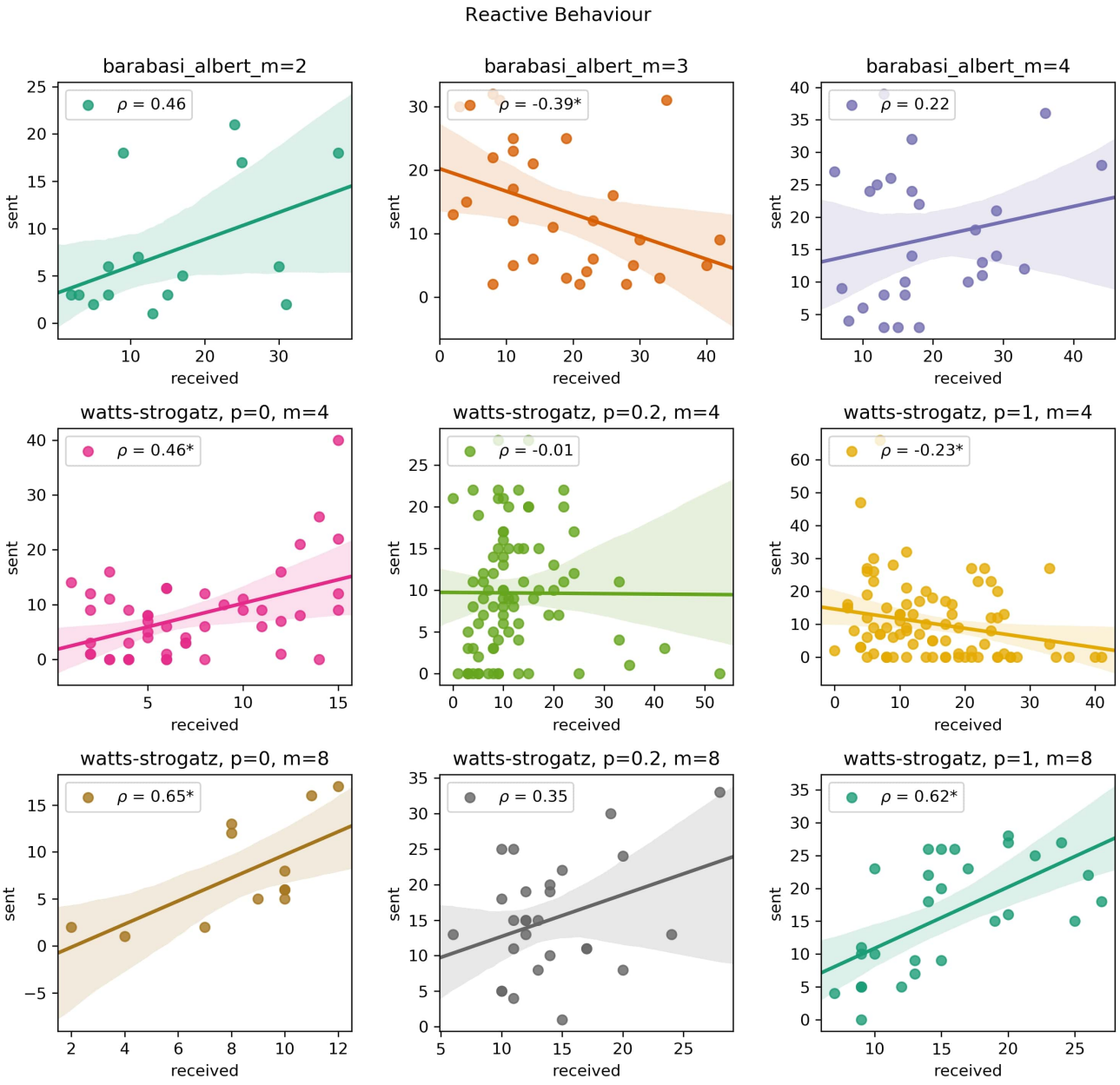


FIGURE 6.28: Reactive Behaviour for networks with different parameters. Each row shows different network connectivity (degree).

6.4 Towards infection prediction based on user behaviour

The benefit of tracking user interactions, is the ability to use the data for the purpose of predicting the infection based on those. After showing how networks feature affect the spreading of cyber threats and users behavior we use some machine learning techniques, as we aim to explore the possibility of predicting use

behaviour and the state of infection. Such a forecast would allow to throttle the spread of malicious content, just based on user interactions.

Decision Tree

Using the decision tree model we try to identify which behavior leads to infection. With three different actions the users took, that is sent, received and opened, we firstly analyse the behaviour with a decision tree.

Each leaf contains the condition, the number of samples, number of observations and classification. If there is no stopping conditions, i.e. how deep the tree should be, the algorithm will continue until each group is pure. A node is pure when all the training samples belong to the same class. That means that the tree will be split into as many classes as possible. To reach a pure node each sample would have to meet strict conditions to reach a certain class, essentially overfitting our model. To avoid this we limit the the depth of the tree. We find an optimal depth but looping through a range of different values from *minimum tree depth* to *max tree depth*, at each point calculating the accuracy score.

From our tree in Fig. 6.29, we see that it is necessary to open messages in order to get into the infected state, indicated by blue colour. The most samples are interestingly classified when the users only opened messages. The required conditions leading to that state are to open at least 2 messages, and sent 0.

We included seeds in our analysis, as the infection starts spreading from them and we measure their interactions too. Therefore the left branch, with the blue leaf is a seed, as in that case there was no messages opened to get infected.

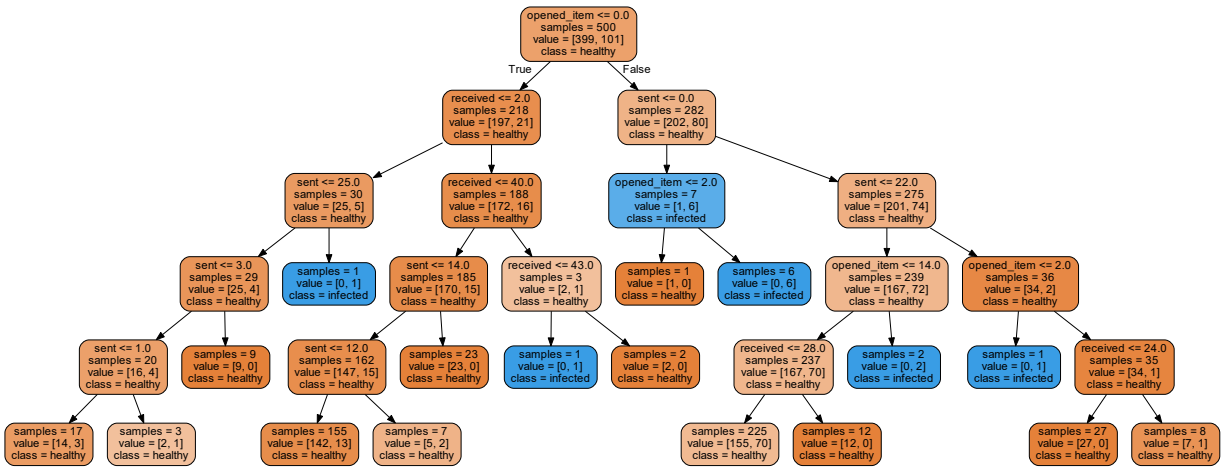


FIGURE 6.29: Decision Tree

K-Means

Passing in three actions into K-Means we attempt to predict the possibility of a node in either infected or healthy state based on those actions. As the data is in 3-dimensions, the K-Means algorithm reduces the dimensionality, by taking the Euclidean distance to the cluster center.

From the output of the model in Fig. 6.30, we can see how the two states cluster. The 2 centroids represent healthy and infected classes, and around them we can see dots, which represent each individual user. The axes we have the amalgamated actions, and since sent/received represent the same class (as these two numbers are equal for all e.g. i sent 5 messages, j receives 5), we can only consider two classes. X-axis is the opened action, and y-axis is the sent/received. We can observe clustering of the healthy and infected nodes, indicating that the actions taken by users have a pattern leading to infection. This goes in line with the decision tree, as the specific actions user takes lead to infection, so the aggregate of the actions, and what they are produces clustering. Another point we note with previous results is that the nodes that have the tendency to open more messages, which could be a result to high value of the degree or centrality, are more prone to infection.

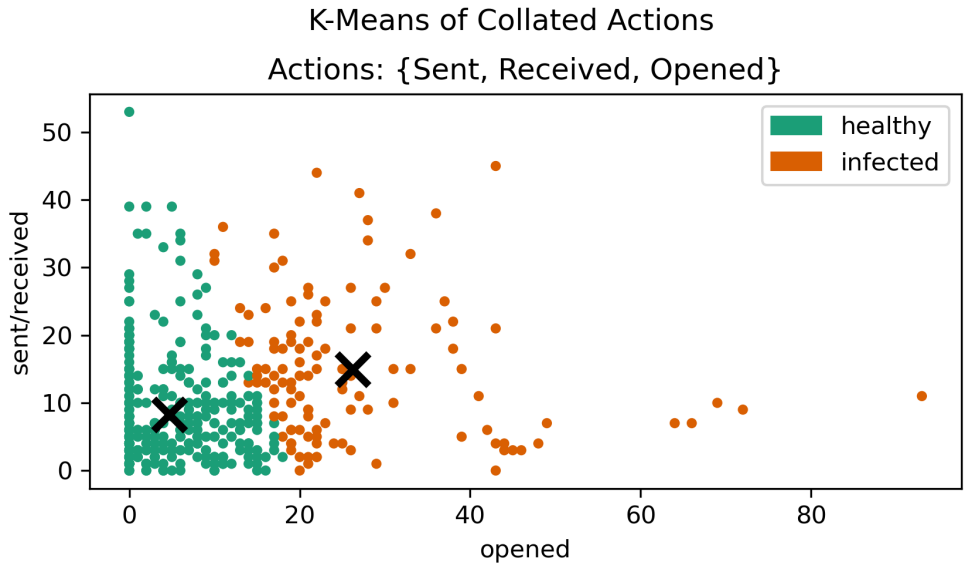


FIGURE 6.30: K-means prediction

Cluster Analysis

Using the PCA dimenstionality reduction technique, which captures the variance across the actions, and considers correlation amongst variables, we review the performance of the predictions. From 6.31 we do not observe any obvious clustering. So although the number of actions taken may impact the likelihood of getting infected, as predicted by the two previous models, the type of the action doesn't seem to explain the reason for that. We can observe the correlation between the types of actions in Fig. 6.32. Interesting correlation in that plot is the more you sent the more you receive. Which is something we've observed that is true in the network effect section.

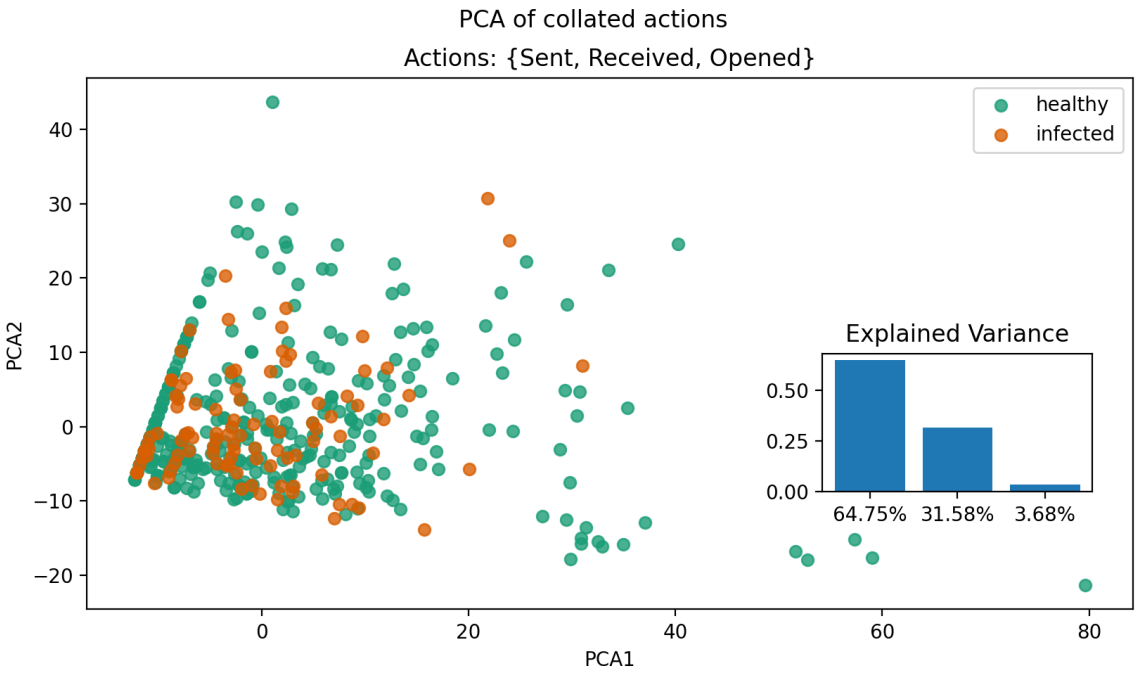


FIGURE 6.31: Principal Component Analysis

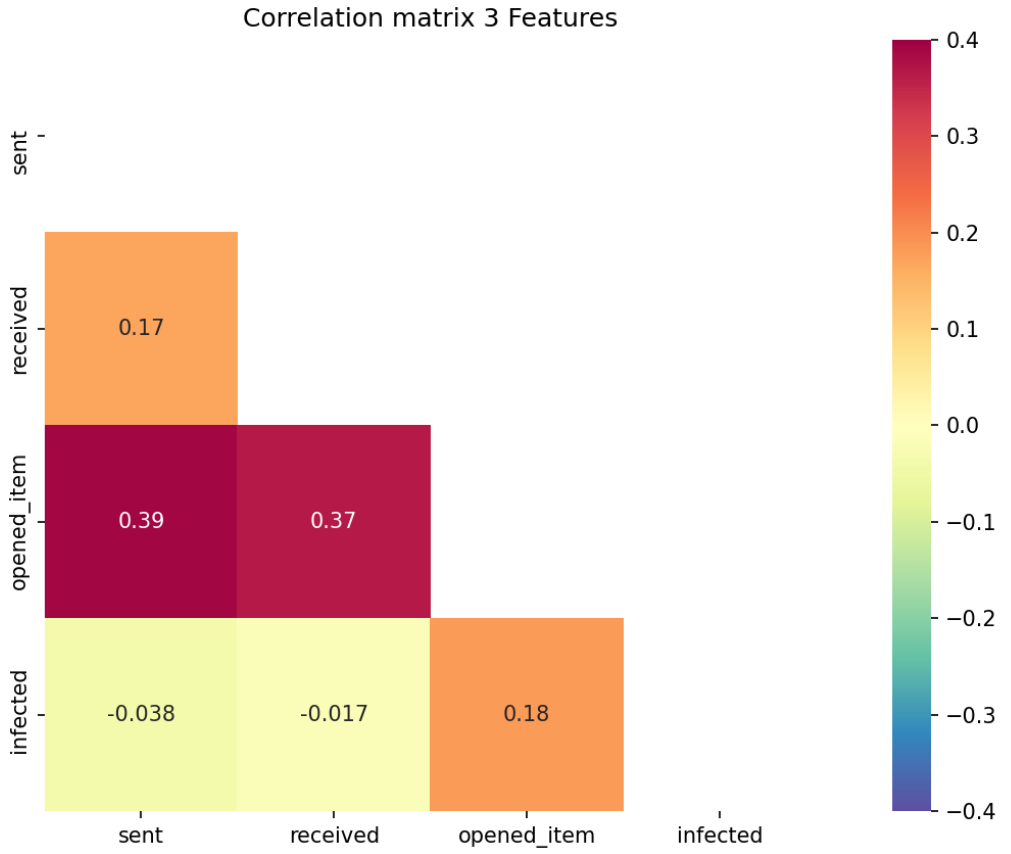


FIGURE 6.32: Correlation between types of actions

6.5 Summary

Aligned with our research questions and experimental settings, we analyse the data collected during 8 separate experiments that took place online. Our results show how under different scenarios and user groups (based on computer literacy) a computer virus is able to spread. A computer virus that exist in our platform is a simple binary flag, which indicates if a user and the message they have sent is infected or not. We present our results showing how the spread of computer viruses is affected by inherent user characteristics such as trust and gullibility, and how the network effects impact the spread of the virus, interplaying with those characteristics. We also use some machine learning techniques to find underlying patterns between user behaviour and infection.

Our findings show that the spreading processes of cyber threats is indeed impacted by the presence of user characteristics. The temporal nature of the interactions and the level of information regarding threat level, changes user trust and perception as the infection spreads. We find that connectivity and position of users in the network introduced non-trivial effects, affecting both the user behaviour and the spreading of cyber threats. From the position of a node in network we find that well connected nodes are easier to infect, and that centrality and betweenness affect the number of messages received and opened.

Chapter 7

Conclusion

7.1 Contributions

The PhD thesis aims at characterising the networks' effects behind the spreading of cyber threats on online social networks. The current state of knowledge in the field of network science and cyber security research consists of a rich body of work, mostly focussing either on the propagation of viruses on static networks [Jagdev Singh et al., 2018; L.-X. Yang and X. Yang, 2014a; S. Xu et al., 2014; Kephart and S. R. White, 1992; Soumya and Revathy, 2018; Guo, Cheng, and Kelley, 2016; Lan Liu et al., 2017; Ikhalia, 2017], or on users' ability to identify malicious content [Heartfield and Loukas, 2018; Heartfield, Loukas, and Gan, 2016; B. B. Gupta et al., 2017; Sukwong, Hyong Kim, and James Hoe, 2010; Cormack, 2008; Miyamoto, Hazeyama, and Kadobayashi, 2008]. Only a handful of studies cover both areas, in which the spread of cyber security threats is explored, but in the context of perception (e.g. emotions towards a message) [Kramer, Guillory, and Hancock, 2014; Bliss et al., 2012; Bollen et al., 2011; Ferrara, Varol, et al., 2016; Bond et al., 2012] or the effect of the computer virus on a network [X. Zhang and Tadi, 2007; M. E. Newman, Stephanie Forrest, and Justin Balthrop, 2002; Zhu, X. Yang, and J. Ren, 2012; Zhu and Cen, 2017; Mønsted et al., 2017].

The continuous efforts of research activity in the area has indeed addressed a lot of issues, however we can still identify three key research gaps that are impeding significant progresses, first of which is the user susceptibility. The susceptibility of an individual is typically measured and studied with separation of users. The user is detached from a network, and as an individual, so in other words the gullibility is typically considered as an individual property. This method doesn't take into consideration the properties of individual, which might be modulated by networks' effects emerging from users' interactions. For example, independently of its content, we might be more prone to open a message sent by a close friend than a random person.

The temporal dynamics of social interactions are the second overlooked phenomena. Some early work on the spreading of viruses via Bluetooth among mobile phones [Pu Wang et al., 2009] addresses the nature of propagation of cyber threats, considering temporal interactions on social network, but aside from the early study and a few exceptions [Peng et al., 2017], the literature largely overlooks that social interactions are subject to complex time-varying dynamics and that susceptibility of online users is not homogenous.

The third gap is the lack of empirical data, which describes the real spreading of such phenomena. Large data-sets exist for studies of spam [B. B. Gupta et al., 2017], but the data which tracks user interactions is available only in for-profit corporations that have little interest in publicizing the risks and threats their users might be exposed to.

We address these gaps in research, by studying, both theoretically and empirically via experiments, at users' behaviour, their connections, how they impact the spreading of cyber threats.

We first proposed and analytically solved a new theoretical model to study and characterise the spreading of cyber threats on time-varying networks. The model considers two types of computer viruses. The first mimics threats that can propagate only via connections activated during the infection period. The second considers viruses able to also access information about past contacts. We add memory to the virus, that is we consider a virus which spreads to a list of friends we contacted previously, so past contacts can get infected. In the model we consider different levels of user gullibility to deception-based threats and different levels of homophily across gullibility classes.

In order to develop an empirical understanding about the spreading of social engineering attacks on online social networks we then developed a new experimental platform called NUTMEG, which follows standards of an online social network. The main objective of the experimental platform was to track the propagation of the infection, as well as the actions users perform, to establish how they got infected, and who by.

Our experimental platform has been developed largely with custom code, without much use of any external APIs. This approach allowed us to highly customise its functionality and software design, leading to a modular experimental platform, which is open-source and adaptable to different experiments. The novel approach the platform takes allows to customise the setup of User Interface (UI) served to users, and parameters for the generation of the network from a web interface.

By carrying out 8 experiments, with 109 total participants (26 from the UK and 83 from Spain), we use preset experimental scenarios, each one serving a different purpose, to measure different user characteristics, based on what features each scenario is revealing to the user.

The first experimental scenario was the 'baseline' scenario, in which the elements of the UI that we enabled to the user, only included for the user to see his/her friend list with usernames and the timeline. In the timeline users see past interactions, in the first scenario users did not see the identity of the sender. The purpose of this is to observe how the interactions between users impact trust. The second and third scenarios build up on the first, where in the second the users can now see the name of their friend in the timeline and how many interactions they had with them, and they will be notified if they got infected once they open a message. Final experimental scenario builds up on that, additionally allowing to block friends, preventing from any further interactions between the two nodes, and also use the 'antivirus' feature, which removes the infected state of the profile, and all of the infected messages from the timeline.

After each scenario we show user their performance in form of some simple statistics. The statistics page shows each user the information if they have got

infected during the experimental scenario, their score, how many safe/infected messages they opened, whom they got infected by etc. This information is meant to provide users with feedback about their actions, and based on this, they can develop a different approach to their interactions in future scenarios. Their new approach might change, as if they find someone they trusted has infected them, they might choose not to interact with the same person again, or even block them (in scenario 3).

Using the data gathered from these experiments and experimental scenarios, we seek to understand the presence and impact of the infection, and the effect of user characteristics and network properties on the spread of the virus. We have defined two main characteristics, the trust ratio and gullibility, and we investigate their change over time and change of trust, based on the fact if the user got infected or not.

To the best of our knowledge, NUTMEG is the only platform which allows to study social networks from the combined perspective of network science and cyber security. The platform can aid researchers to understand the spreading of cyber threats. The modular structure and its open source nature allow for further extensions aimed at developing a better understanding of these critical phenomena. Its modular approach allows to change the network to fit research in different areas, and it has the potential of future applications of machine learning and self-adaptivity of social networks. The data that is generated by interacting via NUTMEG has the potential of training machine learning algorithms for social networks which could adapt their content, based on social interactions and help block malicious software before it widely spreads. The platform will allow researchers to study not only the spread of cyber security threats, but also other kinds of network-propagated threats such as fake news, and how the behaviour of the people impacts the propagation of such content.

Research Questions

Using both our theoretical framework and the experimental platform we investigated the following research questions:

1. Can we characterize empirically the spreading of cyber threats on online social networks and what are the effects of trust, socio-demographics and gullibility?

2. What are the network effects, emerging from the unsupervised interaction of many individuals, affecting the spreading of cyber threats on OSN?

3. Can we model the spreading of such phenomena accounting for heterogeneous susceptibility of users and their temporal interaction dynamics?

The first objective is attained by analysing the user behaviour which leads to infection via the experimental platform.

We define two metrics which we measured during the experiments, gullibility and trust. The former is a score calculated based on the survey, which all users are required to complete prior to the start of the experiments. The lower the gullibility

score, the more capable users are in recognising a social engineering attack against them. The trust score is a normalised ratio between the numbers of messages opened to received between two nodes (i, j). The more messages you open, the more you trust someone. Using these two metrics, we observe how these user characteristics change over time and how that affects the spread of the virus and vice-versa.

While an average user on an OSN can have hundreds of friends, they typically interact with a small proportion of those people [S. Zhao, 2006; J. Han and H. Lee, 2012; D. Lu et al., 2016]. Because of this, we expect that the pairs of people who do interact with each other, will have a higher trust compared to the rest of the network. We take that observation as we look at the second objective.

From our analysis we learn that most users exhibit little trust towards each other, and that infection reduces that trust. We also see that the more gullible people are more likely to open messages, and they display higher levels of trust. This goes in line with previous research, as it has been found that two users who known each other are more likely open messages mutually [Jagatic et al., 2007; Colwill, 2009]. However despite the gullibility (the higher this is the more interactions there are), interestingly most users have at least one interaction with one of their friends.

The experimental scenarios, and the features we enabled in each one, also have played a role in the size of the epidemic. Depending on the enabled features that we present in the UI, the trust ratio changes across different scenarios, with some pairs of nodes showing higher levels of trust than others. Once the infection starts growing however, the trust and tendency towards opening messages are reduced, thus reducing the final reach of the cyber threat (i.e. epidemic size).

Although indeed trust grows over time, it is impacted by other factors, such hompohily, infection and gullibility. Users with higher levels of gullibility open more messages, and thus their trust ratio is high. We explore different network topologies, to find if the position of the node in the graph, will impact the user actions, and in therefore the trust ratio and epidemic size.

As we look at the second objective, running the experiments connecting users according to different topologies, we test a range of parameters on two networks. We studied different regimes (p=0, 0.2, 1; and m=4, 8) of the Watts-Strogatz model thus connecting users in networks of varying clustering, average path length, and degree. We also run some experiments on the Barabasi-Albert Model where $m = 2, m = 3$ and $m = 4$. We investigate the correlation between the spreading patterns and several centrality measures such as betweenness, clustering and degree. We did not find any clear correlation patterns between centrality measures and the spreading of the virus, but rather a case dependent phenomenology. This could be due to the size of the networks, as the limitations induced by small sample sizes of the experiments, produce networks, which are too small to see clear effects. Furthermore, the position, thus centrality, of each user in the network is only one variables behind the spreading processes.

The network properties do however yield correlations between them and some of the actions. We observe that, in general, higher degree implies a larger number

of messages received / opened. The BA model shows that degree and betweenness are correlated with the number of items received and opened. The better connected you are, the more messages you receive and open. In case where $m = 4$ in the BA model and $p = 1, m = 8$ in the WS model, we also observe that higher degree implies more messages sent. This leads us to explore reactive behaviour of the participants. The reactive behaviour is the reaction to the messages received, which in the case of our platform is the "reply" response. In other words, this means that individuals who receive more messages, are driven to send more messages.

The final objective is to model the spreading phenomena for the heterogeneous susceptibility. In doing so, we have proposed and analytically solved a novel theoretical time-varying network model which features different classes of gullibility and different levels of homophily between them. Interestingly, we saw that the networks dynamics and their interplay with the characteristics of users have to be considered in order to avoid misrepresentation of the spreading power of computer viruses in social networks. Remarkably, in some scenarios, which we characterized analytically, the temporal coupling between gullibility classes creates a non-trivial phenomenology that might favors the spreading of the cyber threats. Furthermore, we used machine learning approach to find patterns and correlations between the variables in the experimental data collected via the platform. Our samples show promising results, meaning that the patterns emerging from the user actions have potential to be predicted. The significance of this, is the prospect of future work, for a model which will be able to predict the spreading of cyber threat, based only on the interactions of the user. This could allow to further train machine learning algorithms, to help reduce the number of infections if user interactions were tracked.

7.2 Limitations

As any research, this study comes with limitations. Although our mathematical model presented in Chapter 3 highlights that the spreading of cyber threats is critically affected by different levels of susceptibility and temporal change of the network, we note some limitations. These limitations are the fact that we used a simple network model, which overlooks some of the properties of a real social network. The presence of weak and strong ties, high order correlations, and community structures are not studied, and thus additional research in this would be required.

Our experimental platform has proven to be a valuable and beneficial tool, which firstly was tested during the pilots, and then during the experiments. As we collected feedback from the pilots, where we trialed different setup of the platform (length of time, features enabled, number of scenarios etc.), we found that users tend to have a limited attention span. We have set the length of the rounds at 60 seconds, as longer periods have proven for users the simply get bored. This was because we do not present content in the experiments. As we already explained, we remove bias of the content, to isolate the social effects, which in turn makes the platform less interesting for the end-user. The experiments and the platform

emulate a real social network, unlike a most social networks, the connections do not last for long periods of time, but only for duration of the experiment. This could potentially have an effect on building trust, but we believe this would also be correlated with content, as on a standard social network content has shown to be one of the key influences on trust.

Unlike a real social network, our experiments include a gamification factor. We reproduce an experiment which simulates a real social network, but unlike those, the participants are being scored on their behaviour. The point system has been developed to hone the engagement, but we are aware that in a real social network there is no such method.

We also note the limitation with the sample size. Although we do find some patterns and observe some findings, a real social network would have millions of users. The recruitment of the participants was also a limitation, as primarily the recruitees from the UK were mostly from computer science background. Of course as expected, the results show they have higher resilience to cyber threats and lower gullibility, but a mixed population, as recruited in Spain would have been more realistic as well.

In this research we have focused on two main characteristics of the user, their trust and their gullibility. On a real social network, there would be more characteristics than that. As described in Chapter 1 characteristics such as attitude, familiarity with the system, frequency of usage, training also have an impact on the perception towards malicious content. This goes back to the previous paragraphs, where the attention span and lack of content have limited us in what characteristics we could measure.

7.3 Impact and Future work

Our research sets the stage for studies, which consider both the network effects and user characteristics. As only a small number of these exist, there is no extensive knowledge or tools which we are aware of, that could be used to capture user characteristics on a social network, considering different graphs. Of course, we bare in mind the limitations of our study, but we do find some patterns of characteristics and their impact on behavior and infection.

The limitations pointed out in the previous section point towards some of the future work that can be addressed. The model can be extended by considering more network properties which we highlight in the previous section, and by using a more complex network.

The promising results from our machine learning model could lead to a development of a new type of social network, which would be able to predict the status of the user (infected or healthy), just based on the interactions, and ignoring the content, as including all that data is computationally expensive, especially for a large amount of users that social networks have.

Expanding our platform to a larger sample or including some content and customising it for different kind of metrics could yield interesting results, further investigating the impact of other characteristics, and perhaps revealing network effects, which impact the spreading. This would be especially interesting, if our

platform was adapted to a longitudinal study, where the customised and design of the user interface would further reflect a real social network, and as on a real OSN, the interactions would last over time, where more accurate trust and other metrics which we mention, could yield further information about the impact of user susceptibility.

To conclude our understanding of the contagion spreading processes of cyber security threats through social networks is that this process is indeed impacted by the presence of user characteristics such as gullibility, that the users trust and perception changes with the spread of the infection, finally and that the connectivity and position of users in the network introduces non-trivial effects affecting on one side the behaviors of users and on the other the spreading of the cyber threat.

Appendix A

Network Science Supplementary Material

A.1 Graph Theory

Mathematically, networks can be represented as graphs. A graph is a collection of vertices connected to each other by edges. Any undirected graph G consists of a set of vertices and edges, thus giving us $G = (N, E)$. The size of the graph N is the number of vertices E present.

A graph can be represented in a form of an adjacency matrix. Where each element that has a 1 in it, would represent the connection between corresponding vertices represented by the two corresponding rows for which the NxN matrix can be written as

$$a_{ij} = \begin{cases} 1 \text{ if } (i,j) \in E \\ 0 \text{ if } (i,j) \ni E \end{cases}$$

where E is a set of pairs of different ordered vertices. This can be applied for two types of graphs. An undirected graph; that is one in which an edge does not have direction i.e. the process (or exchange) flow between both nodes, and a directed graph, in which the process will flow in the direction from node i to node j only.

Undirected Graph

N and E are nonempty sets representing N vertices (also known as nodes) and E edges of an undirected graph $G(N, E)$. When an edge is created between two nodes such that $i \to j$ and $j \to i$, this is known as *adjacency* or *neighbour*.

Directed Graph

Directed graph $D(N, E)$ similarly consists of vertices and edges, but the set of E is ordered, and the edge between (i, j) only exists such that $i \to j$, but the reverse connection might not exist.

A.1.1 Weighted graphs

The edges between the vertices can be weighted, meaning that they will have a certain level of importance attached to them. The weighted value usually represents a physical property such as capacity, bandwidth, traffic. The strength of a vertex s_i represents the sum of the weights of its links, and can be considered as a generalization of the degree.

$$s_i = \sum_{j \in V(i)} w_{ij}$$

A.1.2 Clustering coefficient

Clustering in a network is the tendency of neighbouring nodes to form connections (or cliques). In other words if vertex i is connected with vertex j, and vertex j is connected with vertex k there is a high probability, in some types of networks such as social networks, that i and k are connected together. The fraction of pairs connected in this fashion is known as the *clustering coefficient*, and the general version of it in an undirected graph can be defined as $C_i = \frac{2}{k_i(k_i-1)} \sum_{j,k} a_{ij} a_{ik} a_{jk}$ [Saramäki et al., 2007].

A.2 Centrality measures

A.2.1 Degree

The degree of a node is the number of links that a vertex has with its neighbours. It is the simplest measure of centrality, and its most commonly depicted as k. Using an adjacency matrix to represent this variable, it is easy to understand:

$$k_i = \sum_{j=1,n} a_{ij}. \tag{A.1}$$

For directed graphs instead, we have to split this quantity to *in-degree* (incoming links) and *out-degree* (outgoing links)

$$k_i^{in} = \sum_{j=1,n} a_{ij}^T, \tag{A.2}$$

$$k_i^{out} = \sum_{j=1,n} a_{ij}. \tag{A.3}$$

For a weighted graph the *weighted degree* can be defined as:

$$k_i^w = \sum_{j=1,n} a_{ij}^{w_{ij}}. \tag{A.4}$$

As mentioned above this quantity is call *strength*. It has be proven that for different real networks, strength and degree are related [Garlaschelli et al., 2005]:

$$k_i^w \propto k_i^\eta. \tag{A.5}$$

A.2.2 Closeness centrality

Closeness centrality is defined as the average distance of a vertex to all the others:

$$g_i = \frac{1}{\sum_{j \neq i} l_{ij}}. \tag{A.6}$$

Where l_{ij} is the number of edges in a shortest path between i and j, or in other words the distance between i and j. Of course, the nodes with a small shortest path distance to the other nodes have a large closeness centrality.

A.2.3 Betweenness centrality

Betweenness of a node is the measure of how in-between other nodes a vertex is [L. Freeman, 1977]. It is the sum of all shortest paths between ij. It can be defined as:

$$B(i) = \sum_{i \neq j \neq k} \frac{\mathcal{D}_{jl}(i)}{\mathcal{D}_{jl}} \tag{A.7}$$

where $\mathcal{D}_{jl}$ is the number of shortest paths between jl and $\mathcal{D}_{jl}(i)$ is also the number of shortest paths between jl, but those that pass through a node i.

A.3 Statistical properties

A statistical characterization is needed to study the properties of graphs as a whole.

A.3.1 Degree distribution

Degree distribution $P(k)$ defines the probability that any chosen vertex in the graph has degree k. The degree defines the number of connections a node has.The average degree $\langle k \rangle$ is defined as:

$$\langle k \rangle = \sum_k kP(k) \equiv \frac{2E}{N}. \tag{A.8}$$

If the average degree is very small compared to the number of nodes, i.e. $\langle k \rangle \ll N$, a graph is known as *sparse*. For directed graphs we of course have two

distributions $P(k_{in})$ for the in-degree and $P(k_{out})$ for the out-degree. Therefore we can see that:

$$\langle k_{in} \rangle = \sum_{k_{in}} k_{in} P(k_{in}) = \langle k_{out} \rangle = \sum_{k_{out}} k_{out} P(k_{out}) \equiv \frac{\langle k \rangle}{2}. \tag{A.9}$$

Appendix B

Network Properties driving user behaviour Supplementary Material

B.1 Overview

Here we display a scatter plot of a certain network metric vs a certain action. On the network side we consider:

- degree
- betweenness
- clustering

On the actions side we consider:

- number of messages received
- number of messages opened
- number of messages sent

Each scatter plot has a regression line and the value of the Pearson correlation coefficients (the * indicates that the coefficient is significant with $\alpha = 0.05$). We separate the different types of networks used in the experiments. Overall, we observe that, in general, higher degree implies a larger number of messages received / opened.

The Barabasi-Albert Model, with different parameters of m in Figs. B.1, B.2, B.3 indicate that degree and betweenness are correlated with the number of items received and opened. The more central you are in term of global connectivity or the more in between of nodes you are the more messages you receive and open.

We note a similar observation in Watts-Strogatz topology, in Figs. B.7 and B.8, the probability of rewiring each edge $p = 1$. For the values of $p = 0$ and $m = 8$, we do not observe any correlation.

In some cases for the BA model $m = 4$ (Fig. B.3) and in WS model $p = 1$, $m = 8$ we also observe that higher degree implies more messages sent. This suggest the existence of a "reactive" behaviour which we explore next.

B.2 Plots

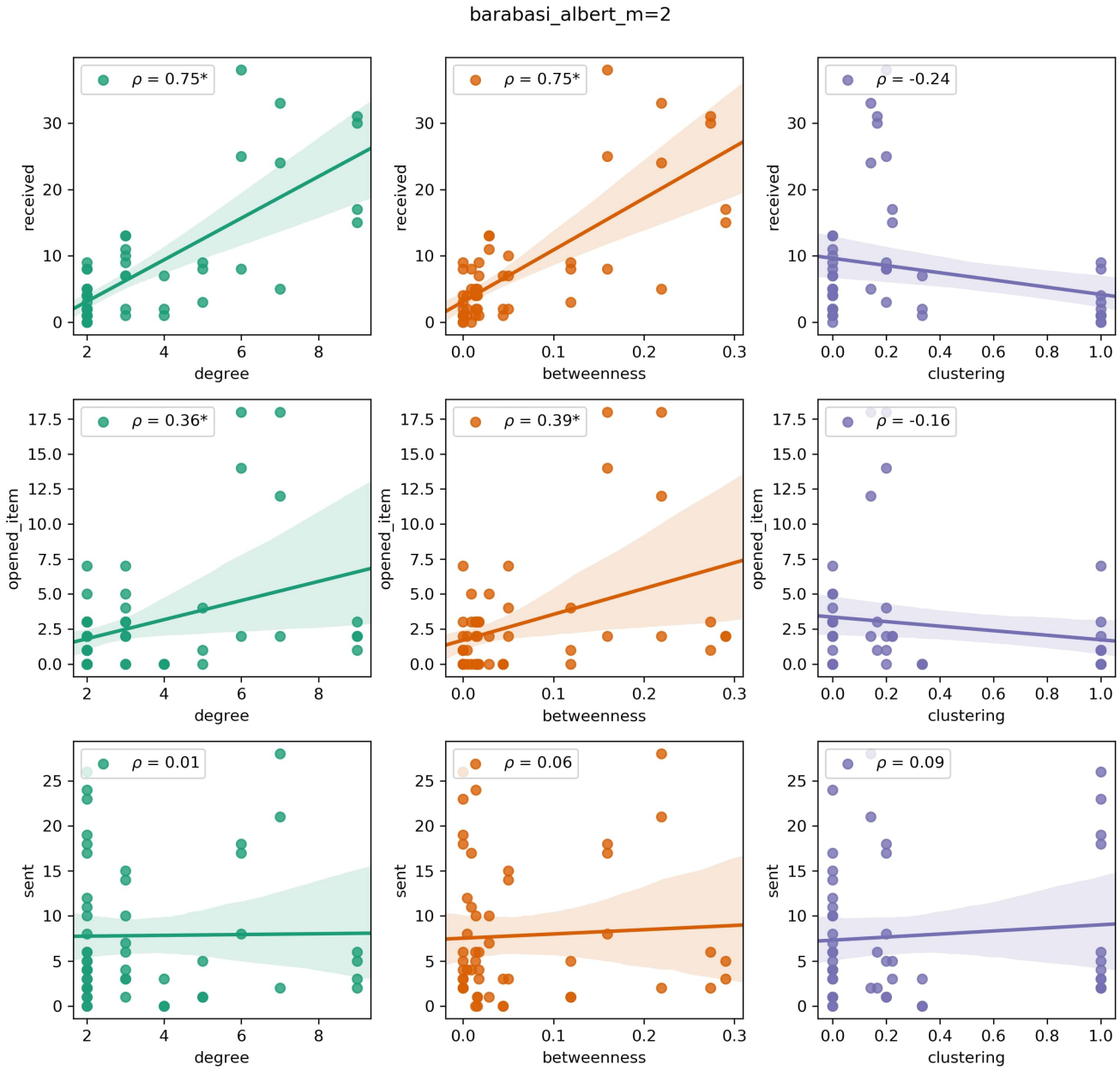


FIGURE B.1: The correlation between actions taken by user and Barabási-Albert network topology, with number of edges to attach from a new node to existing nodes $m = 2$.

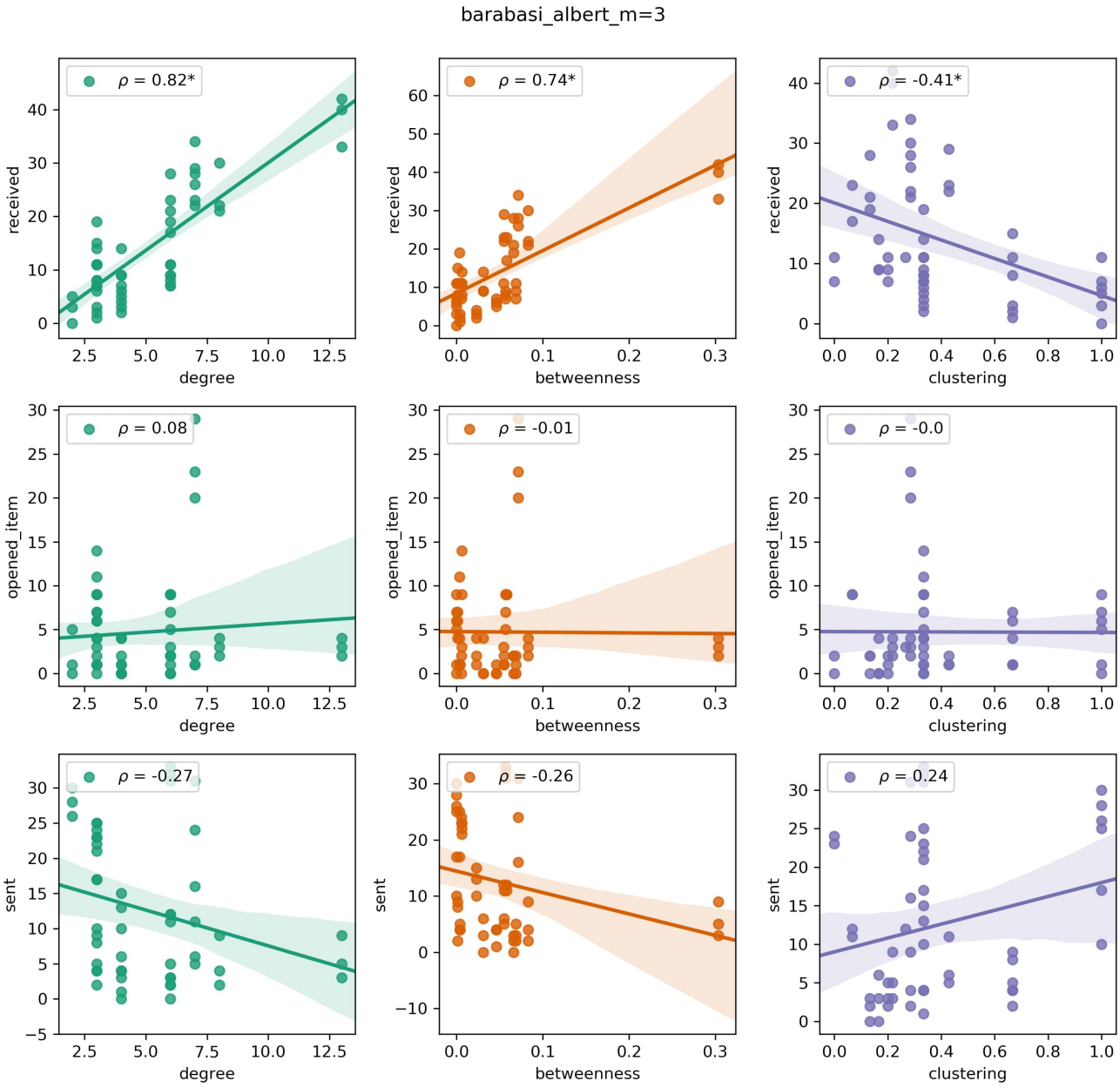


FIGURE B.2: The correlation between actions taken by user and Barabási-Albert network topology, with number of edges to attach from a new node to existing nodes $m = 3$.

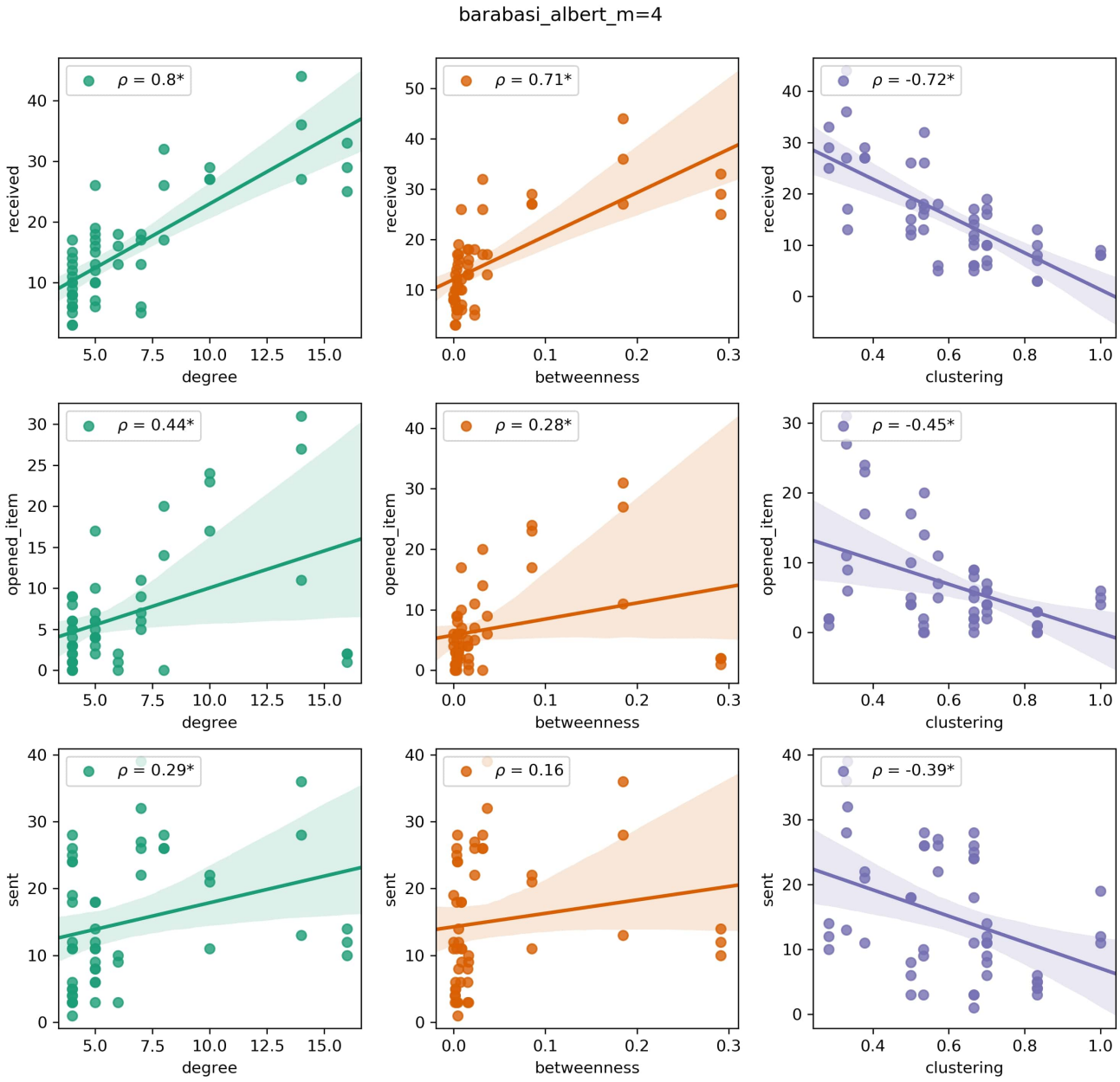


FIGURE B.3: The correlation between actions taken by user and Barabási-Albert network topology, with number of edges to attach from a new node to existing nodes $m = 4$.

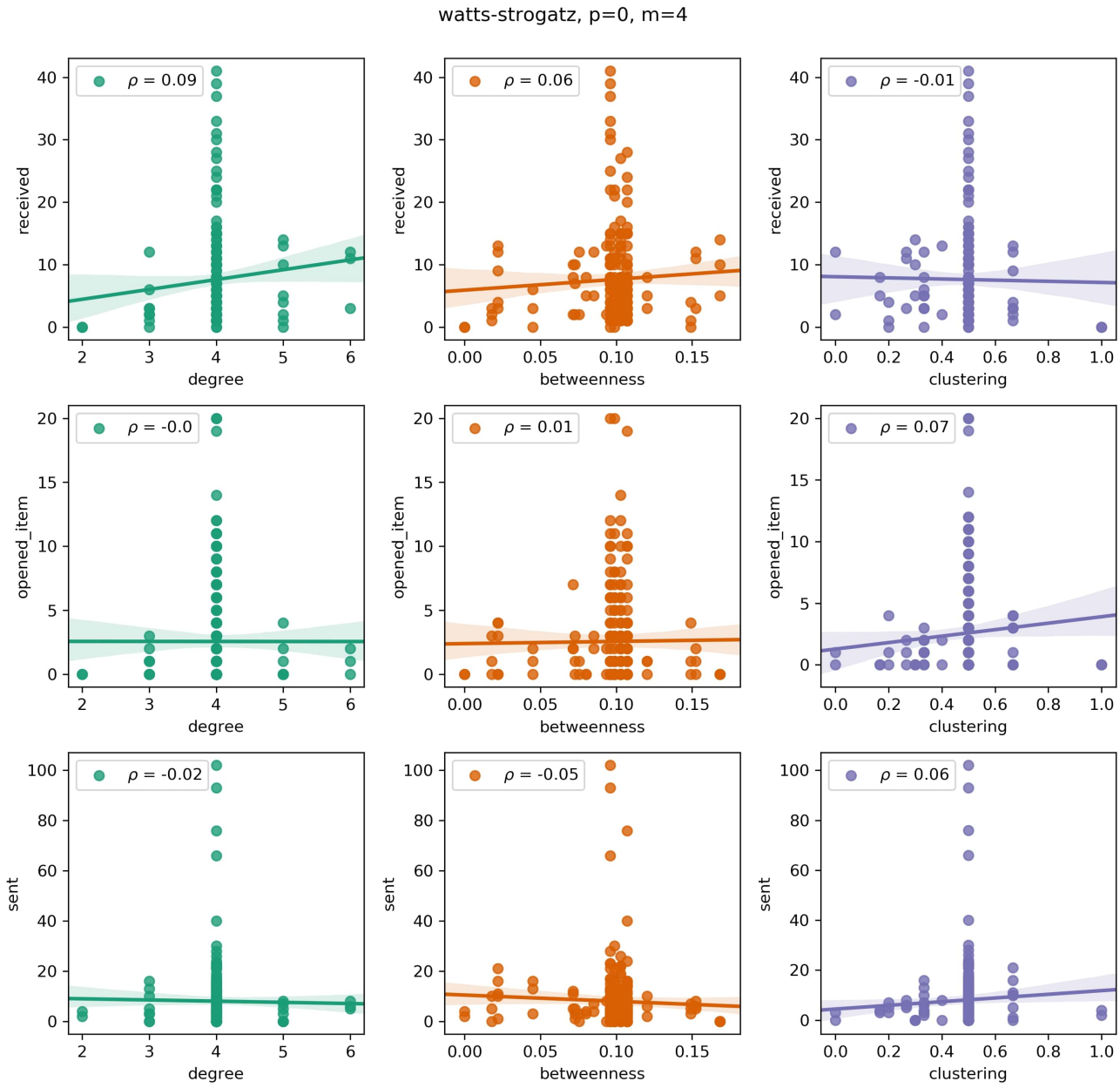


FIGURE B.4: The correlation between actions taken by user and Watts-Strogatz network topology, with the probability of rewiring each edge $p = 0$ and with $m = 4$ nearest neighbours to join in a ring topology.

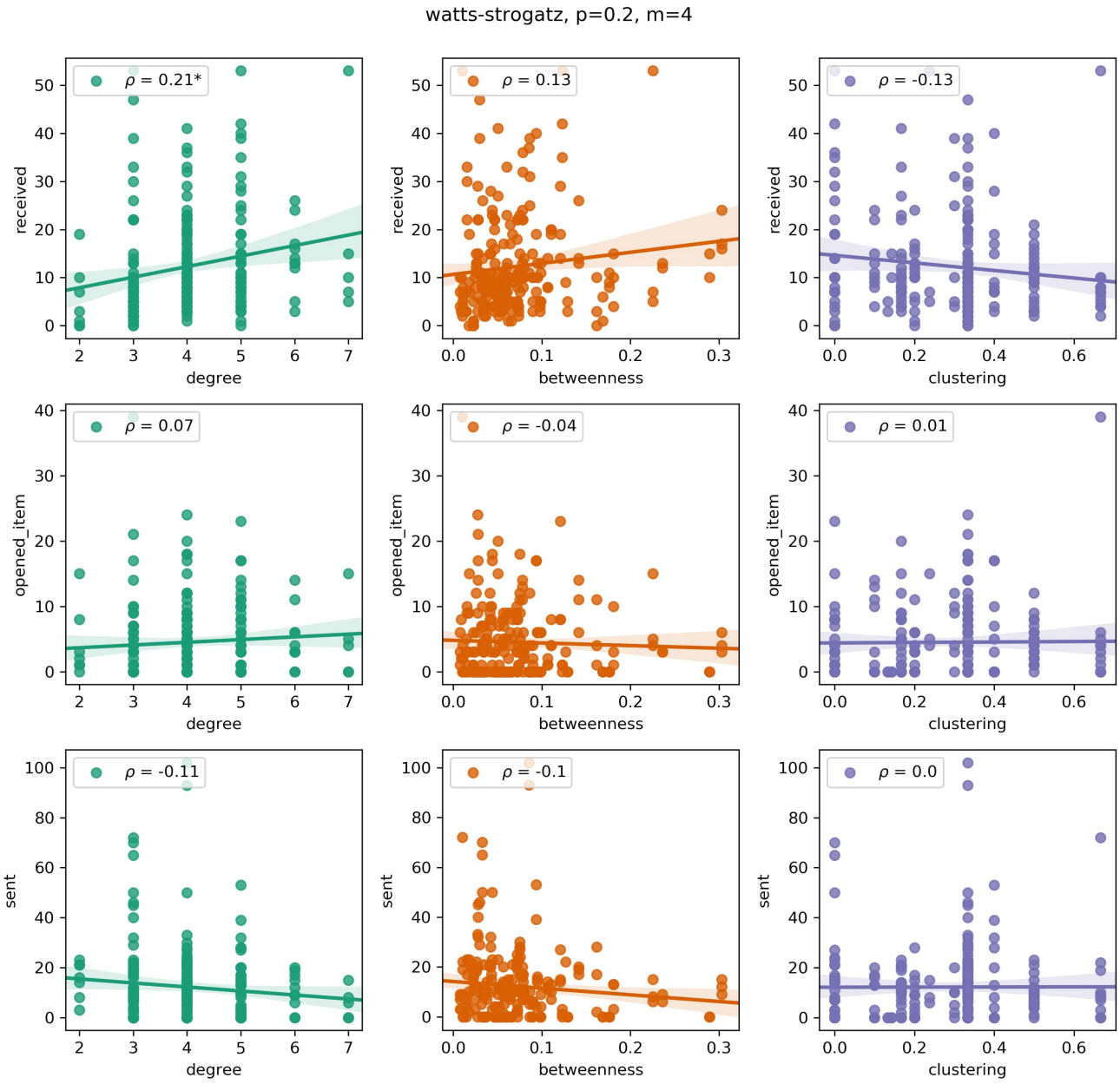


FIGURE B.5: The correlation between actions taken by user and Watts-Strogatz network topology, with the probability of rewiring each edge $p = 0.2$ and with $m = 4$ nearest neighbours to join in a ring topology.

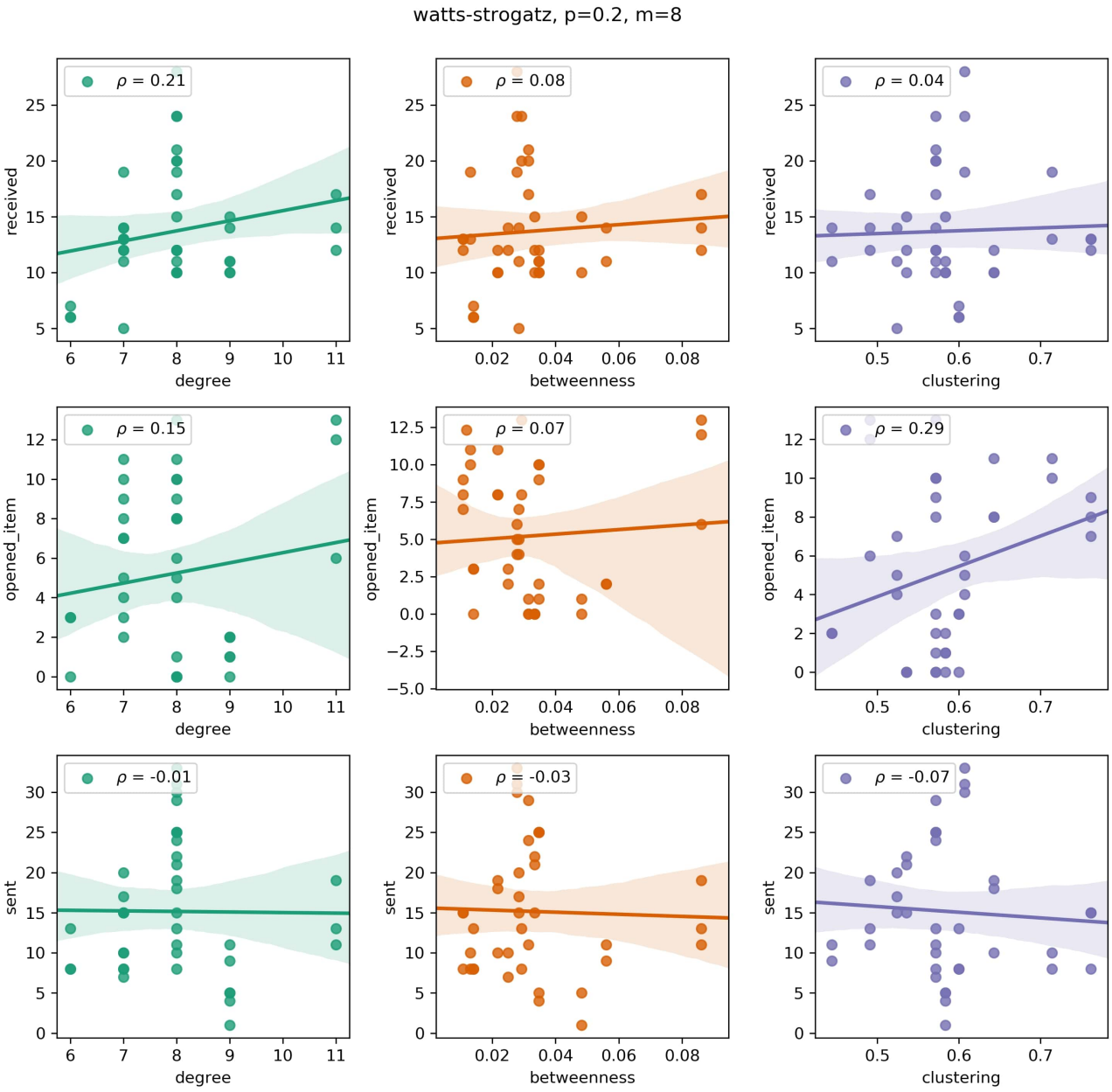


FIGURE B.6: The correlation between actions taken by user and Watts-Strogatz network topology, with the probability of rewiring each edge $p = 0.2$ and with $m = 8$ nearest neighbours to join in a ring topology.

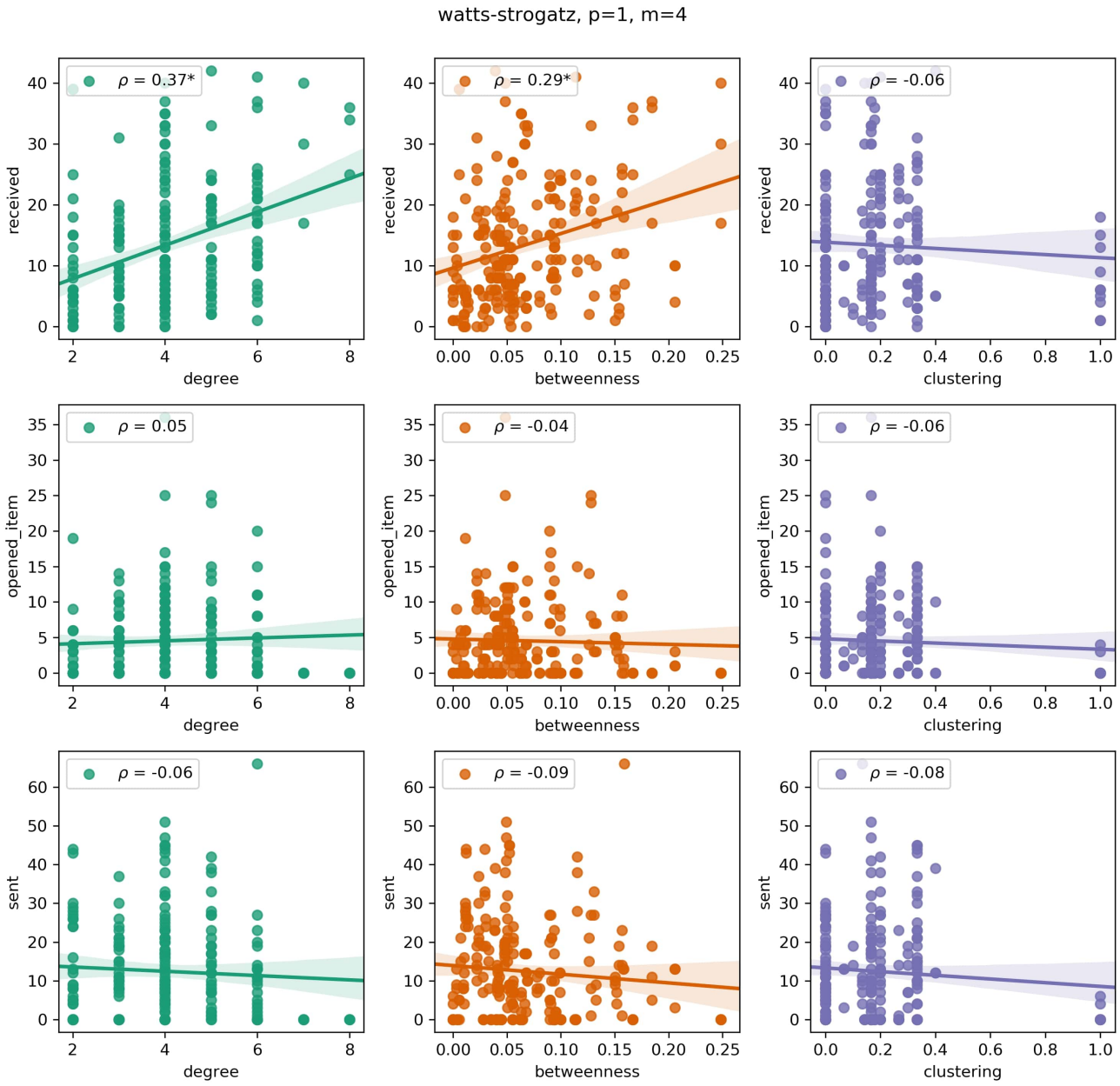


FIGURE B.7: The correlation between actions taken by user and Watts-Strogatz network topology, with the probability of rewiring each edge $p = 1$ and with $m = 4$ nearest neighbours to join in a ring topology.

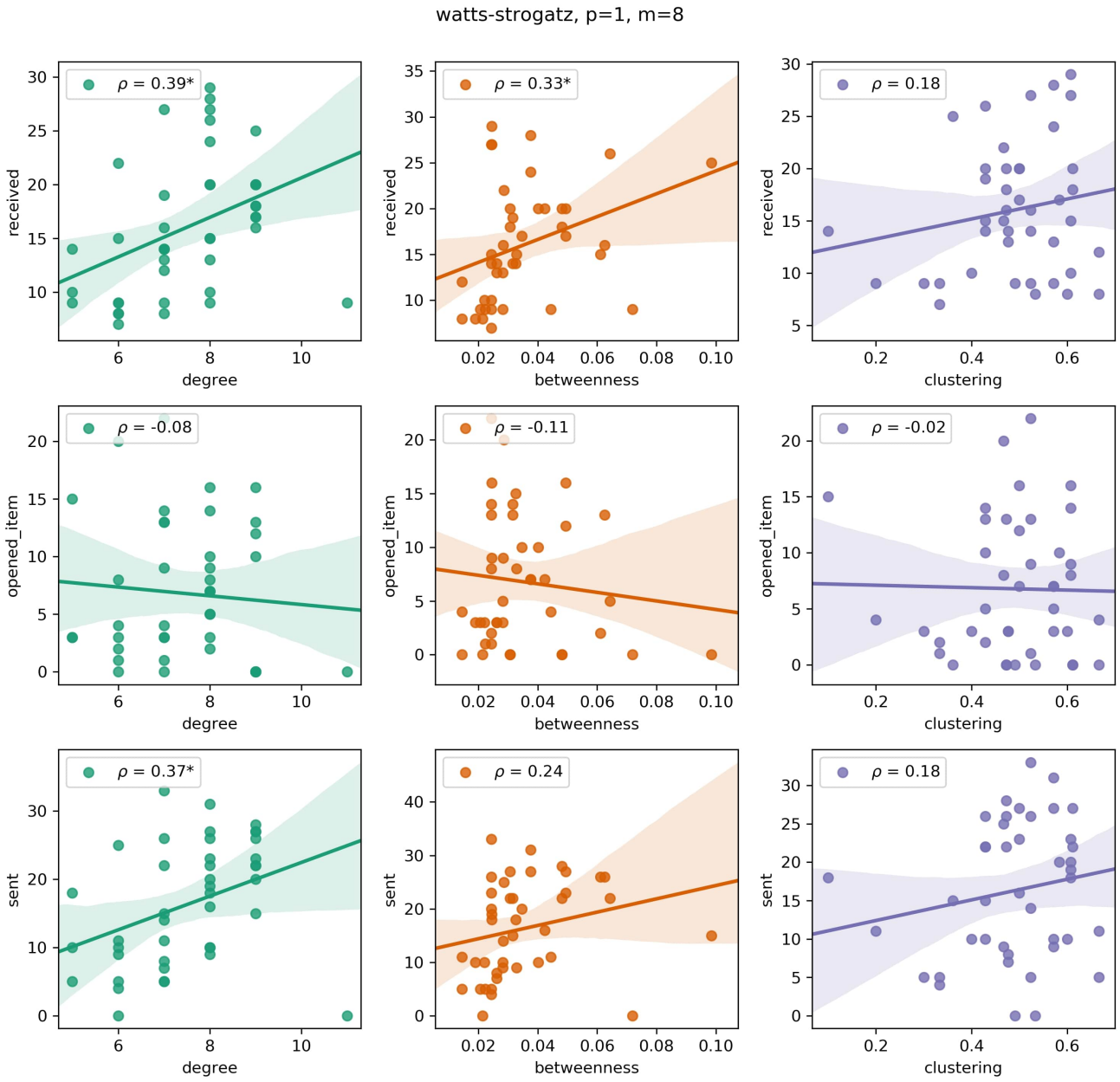


FIGURE B.8: The correlation between actions taken by user and Watts-Strogatz network topology, with the probability of rewiring each edge $p = 1$ and with $m = 8$ nearest neighbours to join in a ring topology.

Bibliography

A, Ercole et al. (2009). “Modelling the impact of an influenza A/H1N1 pandemic on critical care demand from early pathogenicity data: the case for sentinel reporting”. In: *Anaesthesia* 64, pp. 937–941.

A., Lynch (1991). “Thought Contagion as Asbract Evolution”. In: *J Ideas* **2**, pp. 3–10.

ABC news, Swine flu cases confirmed in Scotland, April 28 (n.d.). URL: http://www.abc.net.au/news/stories/2009/04/28/2554208.htm.

Adali, Sibel et al. (2010). “Measuring behavioral trust in social networks”. In: *2010 IEEE International Conference on Intelligence and Security Informatics*. IEEE, pp. 150–152.

Adamic, L.A. and N. Glance (2005). “The political blogosphere and the 2004 US Election”. In: *Proceedings of the WWW-2005 Workshop on the Weblogging Ecosystem*.

Adamic, Lada A and Eytan Adar (2003). “Friends and neighbors on the web”. In: *Social networks* 25.3, pp. 211–230.

Adewole, Kayode Sakariyah et al. (2017). “Malicious accounts: Dark of the social networks”. In: *Journal of Network and Computer Applications* 79, pp. 41–67.

Aiello, W., F. Chung, and L. Lu (2000). “A random graph model for massive graphs, (2000)”. In: *in Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, p. 171180.

Al Ahmar, M Ayman (2010). “Rule based expert system for selecting software development methodology”. In: *Journal of Theoretical and Applied Information Technology* 19.2, pp. 143–148.

al, Graske et (2009). “Assessing the severity of the novel A/H1N1 pandemic”. In: *BMJ* 339, b2840.

al, Singer et (2008). “Meeting Report: Risk Assessment of Tamiflu Use Under Pandemic Conditions”. In: *Environ Health Perspect* 116, pp. 1563–1567.

Albert, R., H. Jeong, and A.-L. Barabási (1999). “Internet: Diameter of the World Wide Web”. In: *Nature* **401**, pp. 130–131.

— (2000). In: *Nature* **406**, p. 378.

Alessandretti, Laura et al. (2017). "Random walks on activity-driven networks with attractiveness". In: *Physical Review E* 95.5, p. 052318.

Ali, Kazim (2017). "A Study of Software Development Life Cycle Process Models." In: *International Journal of Advanced Research in Computer Science* 8.1.

Alizadeh, Meysam, Claudio Cioffi-Revilla, and Andrew Crooks (2017). "Generating and analyzing spatial social networks". In: *Computational and Mathematical Organization Theory* 23.3, pp. 362–390.

Alliance, AGILE (2017). "Agile Practice Guide This book". In: Project Management Institute.

Alon, U. (2003). "Biological networks: the tinkerer as an engineer". In: *Science* **301**, pp. 1866–1867.

Alseadoon, Ibrahim Mohammed A (2014). "The impact of users' characteristics on their ability to detect phishing emails". PhD thesis. Queensland University of Technology.

Alsharnouby, Mohamed, Furkan Alaca, and Sonia Chiasson (2015). "Why phishing still works: User strategies for combating phishing attacks". In: *International Journal of Human-Computer Studies* 82, pp. 69–82.

Alvarez-Galvez, Javier (2016). "Network models of minority opinion spreading: using agent-based modeling to study possible scenarios of social contagion". In: *Social Science Computer Review* 34.5, pp. 567–581.

Amaral, L. A. N. et al. (2000). " Classes of small-world networks". In: *Proceeding of the National Academy of Science (USA)* **97**, pp. 11149–11152.

and (1927). "A contribution to the mathematical theory of epidemics". In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 115.772, pp. 700–721. ISSN: 0950-1207. DOI: 10.1098/rspa.1927.0118. eprint: http://rspa.royalsocietypublishing.org/content/115/772/700.full.pdf. URL: http://rspa.royalsocietypublishing.org/content/115/772/700.

Anderson, R.M. and May, R.M. (1992). *Infectious Diseases in Humans*. Oxford Univ. Press.

Anderson, P.W. (1972). "More is different. Broken symmetry and the nature of the hierarchical structure of science". In: *Science* 177.

Anderson, R.M. and R.M. May (1984). "Spatial, temporal and genetic heterogeneity in hosts populations and the design of immunization programs". In: *IMA J. Math. Appl. Med. Biol.* 1, pp. 233–266.

Arinaminpathy, N. and A.R. McLean (2008). "Antiviral treatment for the control of pandemic influenza: some logistical constraints". In: *J. R. Soc. Interface* 5, pp. 5945–553.

Atti, M.L. Ciofi degli et al. (2008). "Mitigation measures for pandemic influenza in Italy: An individual based model considering different scenarios". In: *PLoS ONE* 3, e1790.

Avrachenkov, K. (1999). "Analytic Perturbation Theory and its Applications". In: *PhD thesis university of South Australia*.

Avrachenkov, K., N. Litvak, and Kim Son Pham (n.d.). " A Singular Perturbation Approach for Choosing PageRank Damping Factor". In: *arXiv:math/0612079v1* ().

Awad, MA (2005). "A comparison between agile and traditional software development methodologies". In: *University of Western Australia* 30.

Bagui, Sikha and Richard Earp (2011). *Database design using entity-relationship diagrams*. Crc Press.

Bailey, N.T. (1975). *The mathematical theory of infectious diseases*. Griffin.

Bajardi, P. et al. (2009). "Modeling vaccination campaigns and the fall/winter 2009 activity of the new a(h1n1) influenza in the northern hemisphere". In: *Emerging Health Threats* **2:e11**.

Balcan, D., V. Colizza, et al. (2009). "Multiscale mobility networks and the large scale spreading of infectious diseases". In: *Proc. Natl Acad. Sci.*, 106:21484.

Balcan, D., B. Goncalves, et al. (2010). "Modeling the spatial spread of infectious diseases: The GLobal Epidemic and Mobility computational model". In: *Journal of Computational Science* 1, 3:132–145.

Balcan, D., H. Hu, et al. (2009). "Seasonal transmission potential and activity peaks of the new influenza a(h1n1): a monte carlo likelihood analysis based on human mobility". In: *BMC Medicine* **439**, 7:45.

Balescu, R. (1997). *Statistical Dynamics: Matter Out of Equilibrium*. Wiley.

Ball, F., D. Mollison, and G. Scalia-Tomba (1997). "Epidemics with two levels of mixing". In: *Ann. Appl. Probab.* 7, pp. 46–89.

Balthrop, J (2004). "J. Balthrop, S. Forrest, MEJ Newman, and MM Williamson, Science 304, 527 (2004)." In: *Science* 304, p. 527.

Balthrop, Justin et al. (2004). "Technological networks and the spread of computer viruses". In: *Science* 304.5670, pp. 527–529.

Barabási, A.-L. and R. Albert (1999a). In: *Science* **286**, p. 509.

— (1999b). In: *Nature* **286**, p. 509.

Barabási, A.-L., R. Albert, and H. Jeong (1999). In: *Physica A* **272**, p. 173.

Barabási, A.-L. and Z.N. Oltvai (2004). "Network biology: understading the cell's functional organization". In: *Nat. Rev. Gen.* **5**, pp. 101–113.

Barabási, A.L. (2002). *Liked*. Perseus.

Barabási, Albert-László (2013). "Network science". In: *Phil. Trans. R. Soc. A* 371.1987, p. 20120375.

Barabási, Albert-László and Réka Albert (1999). "Emergence of scaling in random networks". In: *science* 286.5439, pp. 509–512.

Baronchelli, Andrea (2018). "The emergence of consensus: a primer". In: *Royal Society open science* 5.2, p. 172189.

Baroyan, O.V. et al. (1969). "An attempt at large-scale influenza epidemic modelling by means of a computer". In: *Bull. Int. Epidemiol. Assoc.* 18, pp. 22–31.

Barrat, A. and Barthèlemy, M. and Vespignani, A. (2008). *Dynamical Processes on Complex Networks*. Cambridge University Press.

Barrat, A., M. Barthélemy, and A. Vespignani (2008). *Dynamical Processes on Complex Networks*. Cambridge Univesity Press.

Barrat, A., M. Barthélémy, et al. (2004a). "The architeture of complex weighted networks". In: *Proceedings of the National Academy of Sciences of the United States of America* **101**, pp. 3747–3752.

Barrat, A. and M. Weigt (2000). In: *Eur. Phys. J. B* **13**, p. 547.

Barrat, A and C Cattuto (2015). "Social Phenomena". In:

Barrat, Alain, Marc Barthelemy, Romualdo Pastor-Satorras, et al. (2004). "The architecture of complex weighted networks". In: *Proceedings of the national academy of sciences* 101.11, pp. 3747–3752.

Barrat, Alain, Marc Barthelemy, and Alessandro Vespignani (2008). *Dynamical processes on complex networks*. Cambridge university press.

Barrat, Alain and Ciro Cattuto (2013). "Temporal networks of face-to-face human interactions". In: *Temporal Networks*. Springer, pp. 191–216.

— (2015). "Face-to-face interactions". In: *Social Phenomena*. Springer International Publishing, pp. 37–57.

Barrat, Alain, Ciro Cattuto, et al. (2014). "Measuring contact patterns with wearable sensors: methods, data characteristics and applications to data-driven simulations of infectious diseases". In: *Clinical Microbiology and Infection* 20.1, pp. 10–16.

Barrett, Christopher L et al. (2008). "EpiSimdemics: an efficient algorithm for simulating the spread of infectious disease over large realistic social networks". In: *High Performance Computing, Networking, Storage and Analysis, 2008. SC 2008. International Conference for*. IEEE, pp. 1–12.

Baydogan, Emre (2008). “Rapid prototyping for virtual environments”. In:

Beck, K et al. (2016). “The Agile Manifesto. Manifesto for Agile Software Development”. In: *Retrieved November* 15.

Bendovschi, Andreea (2015). “Cyber-attacks–trends, patterns and security countermeasures”. In: *Procedia Economics and Finance* 28, pp. 24–31.

Benenson, Zinaida, Freya Gassmann, and Robert Landwirth (2017). “Unpacking spear phishing susceptibility”. In: *International Conference on Financial Cryptography and Data Security*. Springer, pp. 610–627.

Benevenuto, Fabrıcio et al. (2009). “Characterizing user behavior in online social networks”. In: *Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement*, pp. 49–62.

Beretta, Edoardo et al. (2001). “Global asymptotic stability of an SIR epidemic model with distributed time delay”. In: *Nonlinear analysis, theory, methods & applications* 47.6, pp. 4107–4115.

Bergé, C. (1976). *Graphs and Hypergraphs*. North-Holland.

Bilge, Leyla et al. (2009). “All your contacts are belong to us: automated identity theft attacks on social networks”. In: *Proceedings of the 18th international conference on World wide web*. ACM, pp. 551–560.

Bincy, George, Jacob Liji, and P J Dhanya (2015). “An SII Model for Tracking the Propagation of Modern Email Malware”. In:

Binney, J.J. and Dowrick, N.J. and Fisher, A.J. and Newman, M.E.J. (1992). *The Theory of Critical Phenomena*. Oxford Science Pubblications.

Bishop, Christopher M (2006). *Pattern recognition and machine learning*. springer.

Bliss, Catherine A et al. (2012). “Twitter reciprocal reply networks exhibit assortativity with respect to happiness”. In: *Journal of Computational Science* 3.5, pp. 388–397.

Boehm, Barry W (1988). “A spiral model of software development and enhancement”. In: *Computer* 21.5, pp. 61–72.

Boelle, P.Y., P. Bernillon, and J.C. Desenclos (2009). “A preliminary estimation of the reproduction ratio for new influenza A(H1N1) from the outbreak in Mexico, March-April 2009”. In: *EuroSurveilliance* 14.

Boguña, M., C Castellano, and R Pastor-Satorras (2013). “Nature of the Epidemic Threshold for the Susceptible-Infected-Susceptible Dynamics in Networks”. In: *Physical Review Letter* 111, p. 068701.

Boguña, M. and R. Pastor-Satorras (2002). “Epidemic spreading in correlated complex networks”. In: *Physical Review E* **66**, p. 047104.

Boguñá, M. and R. Pastor-Satorras (2003). “Class of correlated random networks with hidden variables”. In: *Phys. Rev. E* 68, p. 036112.

Boguñá, M., R. Pastor-Satorras, and A. Vespignani (2004). "Epidemic spreading in complex networks with degree correlations". In: *Lect. Notes Phys.* 625, pp. 127–147.

Boguná, Marian, Claudio Castellano, and Romualdo Pastor-Satorras (2013). "Nature of the epidemic threshold for the susceptible-infected-susceptible dynamics in networks". In: *Physical review letters* 111.6, p. 068701.

Boguná, Marián, Romualdo Pastor-Satorras, and Alessandro Vespignani (2003). "Epidemic spreading in complex networks with degree correlations". In: *arXiv preprint cond-mat/0301149*.

Boldi, P., M. Santini, and S. Vigna (2005). "PageRank as a Function of the Damping Factor". In: *WWW2005*, pp. 557–566.

Boldi, P. and S. Vigna (2004). "The Web Graph framework I: Compression Techniques". In: *WWW2004*, pp. 595–601.

Bolker, B.M. and Grenfell. B.T. (1995). "Space persistence and dynamics of measles epidemics". In: *Phil. Trans. Biol. Sci.* 348, pp. 309–320.

Bollen, Johan et al. (2011). "Happiness is assortative in online social networks". In: *Artificial life* 17.3, pp. 237–251.

Bollobás, B. (1985). *Random Graphs*. Cambridge studies in advanced mathematics.

— (1998). *Modern Graph Theory*. Springer-Verlag.

Bollobás, B. and O. Riordan (2002). "The diameter of scale-free random graphs". In:

Bonacich, P. and P. Lloyd (2001). In: *Soc. Netw.* 23, p. 191.

Bond, Robert M et al. (2012). "A 61-million-person experiment in social influence and political mobilization". In: *Nature* 489.7415, p. 295.

Bonyah, Ebenezer, Abdon Atangana, and Muhammad Altaf Khan (2017). "Modeling the spread of computer virus via Caputo fractional derivative and the beta-derivative". In: *Asia Pacific Journal on Computational Engineering* 4.1, p. 1.

Bootsma, M.C.J. and N.M. Ferguson (2007). "Public Health Interventions and Epidemic Intensity During the 1918 Influenza Pandemic". In: *Proc. Natl Acad. Sci.* **104**, pp. 7588–7593.

Borgatti, Stephen P (1997). "Structural holes: Unpacking Burt's redundancy measures". In: *Connections* 20.1, pp. 35–38.

Böttcher, Lucas, Jan Nagler, and Hans J Herrmann (2017). "Critical behaviors in contagion dynamics". In: *Physical review letters* 118.8, p. 088301.

Bouguettaya, ARA and MY Eltoweissy (2003). "Privacy on the Web: facts, challenges, and solutions". In: *IEEE Security & Privacy* 1.6, pp. 40–49.

Brandes, U. (2001). “A faster algorithm for betweenness centrality”. In: *J. Math. Sociol.* 25, pp. 163–177.

Bransford, JD, AL Brown, and R Cocking (2016). “How People Learn: Brain, Mind, Experience and School. Nationale Academy Press, Washington.” In:

Brauer, Fred (2008). “Compartmental models in epidemiology”. In: *Mathematical epidemiology*. Springer, pp. 19–79.

Breiman, Leo et al. (1984). “Classification and regression trees. Belmont, CA: Wadsworth”. In: *International Group* 432, pp. 151–166.

Brett, Terry et al. (2019). “The spreading of computer viruses on time-varying networks”. In: *arXiv preprint arXiv:1901.02801*.

Brin, S. and L. Page (1998). “ The anatomy of a large-scale hypertextual Web search engine”. In: *Computer Networks* **30**, pp. 107–117.

British Thoracic Society (n.d.).

Brockmann, D., L. Hufnagel, and L. Geisel (2006). “The scaling laws of human travel”. In: *Nature* **439**, pp. 462–465.

Broder, A. et al. (2000). “ Graph Structure in the Web”. In: *Computer Networks* **33**, pp. 309–320.

Brote de infeccion respiratoria aguda en La Gloria, Municipio de Perote, Mexico Secretaria de Salud, Mexico (n.d.). URL: http://portal.salud.gob.mx/contenidos/noticias/influenza/estadisticas.html.

Buchanan, M. (2002). *Small World: Uncovering Nature’s Hidden Network*. London: Weidenfeld and Nicolson.

BUCKINGHAM, D (n.d.). “Defining digital literacy–what do young people need to know about digital learning”. In: *Digital Kompetanse-Nordic Journal of Digital Literacy* 4 ().

Burt, Ronald S (2009). *Structural holes: The social structure of competition*. Harvard university press.

Butt, C.T. (2009). “Revisiting the foundations of networks analysis”. In: *Science* 325, pp. 414–416.

C, Reed et al. (2009). *Estimates of the prevalence of pandemic (H1N1) 2009, United States, April–July 2009*.

Caldarelli, G. (2007). *Scale-Free Networks Complex Webs in Nature and Technology*. Oxford Finance Series.

Caldarelli, G., R. Marchetti, and L. Pietronero (2000). In: *Europhys. Lett.* 52, p. 386.

Callaway, D.S. et al. (2001). “Are randomly grown graphs really random?” In: *Physical Review E* **64**, p. 026118.

Cannarella, John and Joshua A Spechler (2014). "Epidemiological modeling of online social network dynamics". In: *arXiv preprint arXiv:1401.4208*.

Carrat, F. et al. (2008). "Time lines of infection and disease in human influenza: a review of volunteer challenge studies". In: *Am J Epidemiol* **167**, pp. 775–785.

Carrington, Peter J, John Scott, and Stanley Wasserman (2005). *Models and methods in social network analysis*. Vol. 28. Cambridge university press.

Cattuto, Ciro et al. (2013). "Time-varying social networks in a graph database: a Neo4j use case". In: *First international workshop on graph data management experiences and systems*. ACM, p. 11.

CDC (2009a). "Bacterial Coinfections in Lung Tissue Specimens from Fatal Cases of 2009 Pandemic Influenza A (H1N1) - United States, May-August 2009". In: *MMWR* 58, pp. 1–4.

— (2009b). "Hospitalized patients with novel influenza A (H1N1) virus infection - California, April-May, 2009". In: *MMWR* 58, pp. 536–541.

— (2009c). "Intensive-care patients with severe novel influenza A (H1N1) virus infection - Michigan, June 2009". In: *MMWR* 58, pp. 749–752.

CDC Interim guidance for clinicians on identifying and caring for patients with swine-origin influenza A (H1N1) virus infection (2009). URL: http://www.cdc.gov/h1n1flu/identifyingpatients.htm.

CDC: Briefing on Public Health Investigation of Human Cases of Swine Influenza, April 23, 2009, 3:30 p.m. ES. (N.d.). URL: http://www.cdc.gov/media/transcripts/2009/t090423.htm.

CDC: Novel H1N1 influenza vaccine (n.d.). URL: http://www.cdc.gov/h1n1flu/vaccination/public/vaccination_qa_pub.htm.

Center for International Earth Science Information Network (CIESIN), Columbia University; and Centro Internacional de Agricultura Tropical (CIAT). The Gridded Population of the World Version 3 (GPWv3): Population Grids. Palisades, NY: Socioeconomic Data and Applications Center (SEDAC), Columbia University (n.d.). URL: http://sedac.ciesin.columbia.edu/gpw.

Center for International Earth Science Information Network (CIESIN), Columbia University; International Food Policy Research Institute (IFPRI); The World Bank; and Centro Internacional de Agricultura Tropical (CIAT). Global Rural-Urban Mapping Project (GRUMP), Alpha Version: Population Grids. Palisades, NY: Socioeconomic Data and Applications Center (SEDAC), Columbia University. (N.d.). URL: http://sedac.ciesin.columbia.edu/gpw.

Centola, Damon (2010). “The spread of behavior in an online social network experiment”. In: *science* 329.5996, pp. 1194–1197.

Centola, Damon and Michael Macy (2007). “Complex contagions and the weakness of long ties”. In: *American journal of Sociology* 113.3, pp. 702–734.

Chachra, Neha, Stefan Savage, and Geoffrey M Voelker (2015). “Affiliate crookies: Characterizing affiliate marketing abuse”. In: *Proceedings of the 2015 Internet Measurement Conference*. ACM, pp. 41–47.

Chai, Wei Koong (2017). “Modelling Spreading Process Induced by Agent Mobility in Complex Networks”. In: *IEEE Transactions on Network Science and Engineering*.

Chandler, D. (1987). *Introduction to Modern Statistical Mechanics*. Oxford University Press, London (UK).

Chandramouli, R (2011). “Emerging social media threats: Technology and policy perspectives”. In: *2011 Second Worldwide Cybersecurity Summit (WCS)*. IEEE, pp. 1–4.

Chartrand, G. and Lesniak, L. (1986). *Graphs and Digraphs*. Wadsworth and Brooks/Cole.

Chattopadhyay, Swarup and CA Murthy (2017). “Generation of power-law networks by employing various attachment schemes: Structural properties emulating real world networks”. In: *Information Sciences* 397, pp. 219–242.

Chaudron, Michel RV, Werner Heijstek, and Ariadi Nugroho (2012). “How effective is UML modeling?” In: *Software & Systems Modeling* 11.4, pp. 571–580.

Chauhan, Vinod Kumar (2014). “Smoke Testing”. In: *Int. J. Sci. Res. Publ* 4.1, pp. 2250–3153.

Chellapilla, Kumar and Patrice Y Simard (2005). “Using machine learning to break visual human interaction proofs (HIPs)”. In: *Advances in neural information processing systems*, pp. 265–272.

Chen, Jilin et al. (2009). “Make new friends, but keep the old: recommending people on social networking sites”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, pp. 201–210.

Chen, Ning (2009). “On the approximability of influence in social networks”. In: *SIAM Journal on Discrete Mathematics* 23.3, pp. 1400–1415.

Chen, P. et al. (2007). In: *J. Informet.* 1, p. 8.

Chen, Q. et al. (2002). “ The origin of power laws in Internet topologies revisited”. In: *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies*.

Chen, Thomas M and Jean-Marc Robert (2004). "The evolution of viruses and worms". In: *Statistical methods in computer security* 1.

Chick, S et al. (n.d.). "SIMULATION OF LARGE-SCALE NETWORKS USING SSF". In: ().

Chou, Te-Shun (2013). "Security threats on cloud computing vulnerabilities". In: *International Journal of Computer Science & Information Technology* 5.3, p. 79.

Chung, F. and .H Lu (2001). In: *Advances Applied Mathematics* **26**, p. 257.

Clark, J. and Holton, D.A. (1991). *A First Look at Graph Theory*. World Scientific.

Cockcroft, Adrian (2006). "Simulation of Skype Peer-to-peer Web Services Choreography Using Occam-Pi". In: *E-Commerce Technology, 2006. The 8th IEEE International Conference on and Enterprise Computing, E-Commerce, and E-Services, The 3rd IEEE International Conference on*. IEEE, pp. 88–88.

Cohen, Fred (1987). "Computer viruses". In: *Computers & security* 6.1, pp. 22–35.

Cohen, R. et al. (2000). In: *Phys. Rev. Lett.* 85, p. 4646.

Coleman, Gerry and Renaat Verbruggen (1998). "A quality software process for rapid application development". In: *Software Quality Journal* 7.2, pp. 107–122.

Colizza, V., A. Barrat, M. Barthelemy, A.J. Valleron, et al. (2007). "Modeling the Worldwide Spread of Pandemic Influenza: Baseline Case and Containment Interventions". In: *PLoS Med* **4**. DOI: doi:10.1371/journal.pmed.0040013.

Colizza, V., A. Barrat, M. Barthelemy, and A. Vespignani (2006a). "The modeling of global epidemics: Stochastic dynamics and predictability". In: *Bull Math Biol* **68**, pp. 1893–1921.

— (2006b). "The role of the airline transportation network in the prediction and predictability of global epidemics". In: *PNAS* 103, p. 2015.

— (2006c). "The role of the airline transportation network in the prediction and predictability of global epidemics". In: *Proc. Natl. Acad. Sci.* **103**, pp. 2015–2020.

Colizza, V. and A. Vespignani (2007). "Invasion threshold in heterogeneous metapopulation networks". In: *Phys. Rev. Lett.* 99, p. 148701.

— (2008). "Epidemic modeling in metapopulation systems with heterogeneous coupling pattern: Theory and simulations". In: *Journal of Theoretical Biology* 251, pp. 450–467.

Colizza, Vittoria et al. (2006). "Detecting rich-club ordering in complex networks". In: *Nature physics* 2.2, p. 110.

Collier, Ken (2012). *Agile analytics: A value-driven approach to business intelligence and data warehousing*. Addison-Wesley.

Colwill, Carl (2009). "Human factors in information security: The insider threat–Who can you trust these days?" In: *Information security technical report* 14.4, pp. 186–196.

Connors, Danny T (1992). "Software development methodologies and traditional and modern information systems". In: *ACM SIGSOFT Software Engineering Notes* 17.2, pp. 43–49.

Conway, Ryan, Meghan Koch, and Lisa Salinas (2019). "Prototyping Software Development Cycle". In: *Software engineering and CS Journal* 4.1.

Cook, Karen S et al. (2013). "Social exchange theory". In: *Handbook of social psychology*. Springer, pp. 61–88.

Cooper, B.S. et al. (2006). "Delaying the International Spread of Pandemic Influenza". In: *PLoS Medicine* 3, e212.

Coppersmith, D., P. Tetali, and P. Winkler (1993). "Collision among random walks on a graph". In: *SIAM J. Discr. Math* **6**, pp. 363–374.

Cormack, Gordon V (2008). *Email spam filtering: A systematic review*. Now Publishers Inc.

Correa, Teresa, Amber Willard Hinsley, and Homero Gil De Zuniga (2010). "Who interacts on the Web?: The intersection of users' personality and social media use". In: *Computers in Human Behavior* 26.2, pp. 247–253.

Cortiñas, Alejandro et al. (2017). "Enabling Agile Web Development Through In-Browser Code Generation and Evaluation". In: *International Conference on Model and Data Engineering*. Springer, pp. 311–323.

Cross, P. et al. (2005). "Duelling timescales of host movement and disease recovery determine invasion of disease in structured populations". In: *Ecol. Lett.* 8, pp. 587–595.

Cruz-Pacheco, G. et al. (2009). "Modelling of the influenza A(H1N1)v outbreak in Mexico City, April-May 2009, with control sanitary". In: *EuroSurveillance* 14, p. 19254.

Cuesta, Jose A et al. (2015). "Reputation drives cooperative behaviour and network formation in human groups". In: *Scientific reports* 5.1, pp. 1–6.

D'Amico, Anita and Kirsten Whitley (2008). "The real work of computer network defense analysts". In: *VizSEC 2007*. Springer, pp. 19–37.

Dadlani, Aresh et al. (2016). "System dynamics of a refined epidemic model for infection propagation over complex networks". In: *IEEE Systems Journal* 10.4, pp. 1316–1325.

Dahiya, Deepak (2010). "Enterprise systems development: Impact of various software development methodologies". In: *The 2nd International Conference on Software Engineering and Data Mining*. IEEE, pp. 117–122.

Danon, Leon et al. (2013). "Social encounter networks: characterizing Great Britain". In: *Proc. R. Soc. B* 280.1765, p. 20131037.

Data, Modeling Historical and Guide User (2015). *Database Design*. Perancangan Basis Data) merupakan salah satu.

Date, Christopher John (2004). *An introduction to database systems*. Pearson Education India.

Dave, E et al. (2011). "How the next evolution of the Internet is changing everything". In: *The Internet of Things*.

Davis, Gary (May 2018). *The Past, Present, and Future of Password Security*. URL: https://www.mcafee.com/blogs/consumer/consumer-threat-notices/security-world-password-day/.

Dawood, F.S. et al. (2009). "Novel Swine-Origin Influenza A (H1N1) Virus Investigation: Emergence of a Novel Swine-origin Influenza A (H1N1) Virus in Humans". In: *N Engl J Med* 360, pp. 2605–2615.

De Los Rios, P. (2001). In: *Europhys. Lett.* 56, p. 898.

De Montis, A. et al. (2006). "The structure of Inter-Urban traffic: A weighted network analysis". In: *Env. Planning Journal B*.

DeFleur, M.L. and Ball-Rokeach, S. (1989). *Theories of Mass Communication*. Longman, NY.

Despa, Mihai Liviu (2014). "Comparative study on software development methodologies". In: *Database systems journal* 5.3, pp. 37–56.

Devadiga, Nitish M (2017). "Tailoring architecture centric design method with rapid prototyping". In: *2017 2nd International Conference on Communication and Electronics Systems (ICCES)*. IEEE, pp. 924–930.

Developers, NetworkX (2010). "NetworkX". In: *networkx. lanl. gov*.

Dhamija, Rachna, J Doug Tygar, and Marti Hearst (2006). "Why phishing works". In: *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, pp. 581–590.

Dichev, Christo and Darina Dicheva (2017). "Gamifying education: what is known, what is believed and what remains uncertain: a critical review". In: *International journal of educational technology in higher education* 14.1, p. 9.

Dick, Jeremy, Elizabeth Hull, and Ken Jackson (2017). *Requirements engineering*. Springer.

Diekmann, O., A.J.P. Heesterbeek, and J.A.J. Metz (1990). "On the definition and the computation of the basic reproduction ratio R0 in models for infectious diseases in heterogeneous populations". In: *J. Math. Bio.* 28, p. 1432.

DM, Morens, Taubenberger, and Fauci AS (2008). "Predominant role of bacterial pneumonia as a cause of death in pandemic influenza: implications for pandemic influenza preparedness". In: *J Infect Dis* 198, pp. 962–970.

Dodds, P.S., R. Muhamad, and D.J. Watts (2003). "An experimental study of search in global social networks". In: *Science* **301**, pp. 827–829.

Dodds, Peter Sheridan (2018). "A simple person's approach to understanding the contagion condition for spreading processes on generalized random networks". In: *Complex Spreading Phenomena in Social Systems*. Springer, pp. 27–45.

Donato, D. et al. (2008). "Mining the inner structure of the Web graph". In: *Journal of Physics A* **41**, p. 224017.

Dong, Suyalatu, Yan-Bin Deng, and Yong-Chang Huang (2017). "SEIR model of rumor spreading in online social network with varying total population size". In: *Communications in Theoretical Physics* 68.4, p. 545.

Dong, Tao, Xiaofeng Liao, and Huaqing Li (2012). "Stability and Hopf bifurcation in a computer virus model with multistate antivirus". In: *Abstract and Applied Analysis*. Vol. 2012. Hindawi.

Dorogovtsev, S.N. and J.F.F. Mendes (2002). "Evolution of Networks". In: *Advances in Physics* **51**, pp. 1079–1187.

— (2003). *Evolution of Networks From Biological Nets to the Internet and the WWW.* Oxford University Press.

Dorogovtsev, S.N., J.F.F Mendes, and A.N. Samukhin (2000). "Structure of growing networks with preferential linking". In: *Physical Review Letter* **85**, pp. 4633–4636.

Dunbar, Robin IM (1998). "The social brain hypothesis". In: *Evolutionary Anthropology: Issues, News, and Reviews: Issues, News, and Reviews* 6.5, pp. 178–190.

Dunne, J.A., R.J. Williams, and N.D. Martinez (2002). "Food-web structure and network theory: the role of connectance and size". In: *Proc. Natl Acad. Sci.* **99**, pp. 12917–12922.

Earn, D.J.D., P. Rohani, and B.T. Grenfell (1998). "Persistence, chaos and synchrony in ecology and epidemiology". In: *Proc. Roy. Soc. Lond. B* 265, pp. 7–10.

Ebel, H., L.I. Mielsch, and S. Bornholdt (2002). "Scale-free topology of e-mail networks". In: *Physical Review E* **66**, p. 035103.

Ebel, Holger, Lutz-Ingo Mielsch, and Stefan Bornholdt (2002). "Scale-free topology of e-mail networks". In: *Physical review E* 66.3, p. 035103.

Eckmann, Jean-Pierre, Elisha Moses, and Danilo Sergi (2004). "Entropy of dialogues creates coherent structures in e-mail traffic". In: *Proceedings of the National Academy of Sciences* 101.40, pp. 14333–14337.

Economou, E.N. (2006). *Green's functions in quantum physics*. Springer.

Ekekwe, Ndubuisi and Aham Maduka (2007). "Security and risk challenges of voice over IP telephony". In: *Technology and Society, 2007. ISTAS 2007. IEEE International Symposium on*. IEEE, pp. 1–3.

El Periodico Guatemala, Ministro de Salud confirma primer caso de AH1N1 en Guatemala, May 5 2009 (n.d.). URL: http://www.elperiodico.com.gt/es/20090505/pais/99779/.

El Salvador Journal,Primeros casos de gripe porcina El Salvador, May 4 2009 (n.d.). URL: http://www.contrapunto.com.sv/index.php?option=com_content&view=article&id=496:primeros-casos-de-gripe-porcina-el-salvador&catid=55:categoria-ambiente&Itemid=60.

Elveback, L.R. et al. (1976). "An influenza simulation model for immunization studies". In: *Am J Epidemiol* 103, pp. 152–165.

Enterprise, Verizon (2019). "Data breach investigations report". In: *2019 Data Breach Investigations Report*. URL: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

Epstein, J.M., D.M. Goedecke, et al. (2007). "Controlling Pandemic Flu: The Value of International Air Travel Restrictions". In: *PLoS ONE* 2, e401.

Epstein, J.M., J. Parker, et al. (2008). "Coupled Contagion Dynamics of Fear and Disease Mathematical and Computational Explorations". In: *PloS ONE* **3**, E3955.

ERDdS, P and A R&WI (1959). "On random graphs I". In: *Publ. Math. Debrecen* 6, pp. 290–297.

Erdös, P. and A Rényi (1959). In: *Publ. Math.* **6**, p. 290.

— (1960). In: *Publ. Math. Inst. Hung. Acad. Sci.* **5**, p. 17.

— (1961). In: *Bull. Inst. Int. Stat.* **38**, p. 343.

Erdos, Paul and Alfréd Rényi (1960). "On the evolution of random graphs". In: *Publ. Math. Inst. Hung. Acad. Sci* 5.1, pp. 17–60.

Esfahanian, Abdol–Hossein (2013). "Connectivity algorithms". In: *Topics in structural graph theory*. Cambridge University Press, pp. 268–281.

Eubank, S. et al. (2004). "Modelling disease outbreaks in realistic urban social networks". In: *Nature* 429, pp. 180–184.

Eubank, Stephen et al. (2004). "Modelling disease outbreaks in realistic urban social networks". In: *Nature* 429.6988, p. 180.

European Centre for Disease Control and Prevention, Pandemic (H1N1) 2009 Daily Update (November 23, 2009) (n.d.). URL: http://European%20Centre%20for%20Disease%20Control%20and%20Prevention,%20Pandemic%20(H1N1)%202009%20Daily%20Update%20(November%2023,%202009).

EuroSurveilliance (n.d.).

EuroSurveilliance (n.d.).

Evers, J (2006). *User education is pointless*.

Faizi, Salman and Shawon Rahman (2019). "Choosing the Best-fit Lifecycle Framework while Addressing Functionality and Security Issues." In: *CATA*, pp. 107–116.

Faloutsos, M., P. Faloutsos, and C. Faloutsos (1999). " On power-law relationships of the internet topology". In: *Computer Communications Review* **29**, pp. 251–262.

Fan, Rui, Ke Xu, and Jichang Zhao (2016). "Higher contagion and weaker ties mean anger spreads faster than joy in social media". In: *arXiv preprint arXiv:1608.03656*.

Fefferman, NH and KL Ng (2007). "How disease models in static networks can fail to approximate disease in dynamic networks". In: *Physical Review E* 76.3, p. 031919.

Fell, D.A. and A. Wagner (2000). "The small world of metabolism". In: *Nature Biotechnology* **18**, pp. 1121–1122.

Felt, Adrienne Porter et al. (2016). "Rethinking connection security indicators". In: *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, pp. 1–14.

Ferguson, N. M. et al. (2005). "Strategies for containing an emerging influenza pandemic in Southeast Asia". In: *Nature* 437, p. 209.

Ferguson, N.M. (2007). "Capturing Human Behaviour". In: *Nature*, 466:733.

Ferguson, N.M., D.A.T. Cummings, et al. (2006). "Strategies for mitigating an influenza pandemic". In: *Nature* 442, pp. 448–452.

Ferguson, N.M., M.J. Keeling, and W.J. et al Edmunds (2003). "Planning for smallpox outbreaks". In: *Nature* 425, pp. 681–685.

Ferrara, Emilio, Onur Varol, et al. (2016). "The rise of social bots". In: *Communications of the ACM* 59.7, pp. 96–104.

Ferrara, Emilio and Zeyao Yang (2015). “Measuring emotional contagion in social media”. In: *PloS one* 10.11, e0142390.

Flahault, A. and A.J. Valleron (1991). “A method for assessing the global spread of HIV-1 infection based on air-travel”. In: *Math. Popul. Stud.* 3, pp. 1–11.

Flahault, A., E. Vergu, et al. (2006). “Strategies for containing a global influenza pandemic”. In: *Vaccine* 24, pp. 6751–6755.

Fortunato, S. and A. Flammini (2007). “ Random Walks on Direct Networks: the Case of PageRank”. In: *Int, J. Bif. Ch.* 17.

Fortunato, S., A. Flammini, et al. (2005). “ How to make the top ten: Approximating PageRank from in-degree”. In: *arXiv.org,physics,physics/0511103*.

Fraser, C. et al (2009). “Pandemic potential of a strain of influenza A(H1N1): early findings”. In: *Science* 324, pp. 1557–1561.

Freeman, L.C. (1977). “A set of measures of centrality based upon betweenness”. In: *Sociometry* **13**, pp. 141–154.

— (1979). “Centrality in social networks: conceptual clarification”. In: *Social Networks*.

Freeman, L.C., S.P. Borgatti, and D.R. White (1991). “Centrality in valued graphs: A measure of betweenness based on network flow”. In: *Social Networks*.

Freeman, Linton C (1977). “A set of measures of centrality based on betweenness”. In: *Sociometry*, pp. 35–41.

Friberg, Elle (Sept. 2018). *Supercookies: how dangerous are they?* URL: https://nordvpn.com/blog/super-cookies-going-global/.

Friedkin, Noah E (1982). “Information flow through strong and weak ties in intraorganizational social networks”. In: *Social networks* 3.4, pp. 273–285.

Funk, Chris and Yanxi Liu (2016). “Symmetry recaptcha”. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 5165–5174.

Funk, S. et al. (2009). “The Spread of Awareness and its Impact on Epidemic Outbreaks”. In: *Proc. Natl Acad. Sci.*

Ganesh, Ayalvadi, Laurent Massoulié, and Don Towsley (2005). “The effect of network topology on the spread of epidemics”. In: *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.* Vol. 2. IEEE, pp. 1455–1466.

Gani, R. et al. (2005). “Potential Impact of Antiviral Drug Use during Influenza Pandemic”. In: *Emer. Inf. Dis.* 11, p. 1355.

Gardiner, C.W. (1990). *Handbook of Stochastic Methods for Physics, Chemistry and Natural Sciences*. Springer-Verlag.

Gardner, D. (2009). *The Science of Fear: How the Culture of Fear Manipulates Your Brain*. Plume.

Garlaschelli, D. and M.I Loffredo (2004). "Patterns of link reciprocity in directed networks". In: *Phys. Rev. L* **93**, p. 188701.

Garlaschelli, D et al. (2005). "The scale free topology of market investments". In: *Physica A.* **350**, pp. 491–499.

Garton, Laura, Caroline Haythornthwaite, and Barry Wellman (1997). "Studying online social networks". In: *Journal of computer-mediated communication* 3.1, JCMC313.

Gemino, Andrew and Drew Parker (2009). "Use case diagrams in support of use case modeling: Deriving understanding from the picture". In: *Journal of Database Management (JDM)* 20.1, pp. 1–24.

Génois, Mathieu et al. (2015). "Compensating for population sampling in simulations of epidemic spread on temporal contact networks". In: *Nature communications* 6, p. 8860.

Germann, C. et al. (2006). "Mitigation strategies for for pandemic influenza in the United States". In: *Proc. Nat. Acad. Sci.* 103, pp. 5935–5940.

Germann, T.C. et al. (2006). "Mitigation strategies for pandemic influenza in the United States". In: *Proc. Natl. Acad. Sci.* 103, pp. 5935–5940.

Gharibi, Wajeb and Maha Shaabi (2012). "Cyber threats in social networking websites". In: *arXiv preprint arXiv:1202.2420*.

Ghoshal, G. and P. Holme (2006). "Attractiveness and activity in Internet communities". In: *Physica A: Statistical Mechanics and its Applications* 364, pp. 603–609.

Ginelli, F. et al. (2006). "Contact processes with long-range interactions". In: *J. Stat. Mech.*

Global Post, Costa Rica reports first swine flu case, April 28 2009 (n.d.). URL: http://www.globalpost.com/notebook/costa-rica/090428/costa-rica-reports-first-swine-flu-case.

Goffman, W. and V.A. Newill (1964). "Generalization of Epidemic Theory an Application to the Transmission of Ideas". In: *Nature* **4955**, pp. 225–228.

Gonçalves, Bruno and Nicola Perra (2015). *Social phenomena: From data analysis to models*. Springer.

Goodfellow, Ian, Yoshua Bengio, and Aaron Courville (2016). "6.2. 2.3 softmax units for multinoulli output distributions". In: *Deep Learning*. MIT Press, pp. 180–184.

Gott, Sherrie P et al. (1996). "A naturalistic study of transfer: Adaptive expertise in technical domains". In: *Transfer on trial: intelligence, cognition and instruction.–*. Ablex, pp. 258–288.

Gou, Wei and Zhen Jin (2017). "How heterogeneous susceptibility and recovery rates affect the spread of epidemics on networks". In: *Infectious Disease Modelling* 2.3, pp. 353–367.

Grace, Michael C et al. (2012). "Unsafe exposure analysis of mobile in-app advertisements". In: *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*. ACM, pp. 101–112.

Gracia-Lázaro, Carlos et al. (2012). "Human behavior in Prisoner's Dilemma experiments suppresses network reciprocity". In: *Scientific reports* 2.1, pp. 1–4.

Grais, R.F., H.J. Ellis, and G.E. Glass (2003). "Assessing the impact of airline travel on the geographic spread of pandemic influenza". In: *Eur. J. Epidemiol.* 18, pp. 1065–1072.

Grais, R.F., J.H. Ellis, et al. (2004). "Modeling the Spread of Annual Influenza Epidemics in the U.S.: The Potential Role of Air Travel". In: *Health Care Manag Sci* 7, p. 127.

Granovetter, M. (1973). "Strength of weak ties". In: *American Journal of Sociology* **78**, pp. 1360–1380.

Greene, Derek, Donal Doyle, and Padraig Cunningham (2010). "Tracking the evolution of communities in dynamic social networks". In: *Advances in social networks analysis and mining (ASONAM), 2010 international conference on*. IEEE, pp. 176–183.

Guha, Saikat and Neil Daswani (2005). *An experimental study of the skype peer-to-peer voip system*. Tech. rep. Cornell University.

Guilbeault, Douglas, Joshua Becker, and Damon Centola (2018). "Complex contagions: A decade in review". In: *Complex spreading phenomena in social systems*. Springer, pp. 3–25.

Guillén, JD Hernández, A Martın del Rey, and L Hernández Encinas (2017). "Study of the stability of a SEIRS model for computer worm propagation". In: *Physica A: Statistical Mechanics and its Applications* 479, pp. 411–421.

Guimerá, R. and L.A.N. Amaral (2004). "Modeling the world-wide airport network". In: *Eur. Phys. J.B.* **38**, pp. 381–385.

Guo, Hong, Hsing Kenneth Cheng, and Ken Kelley (2016). "Impact of network structure on malware propagation: A growth curve perspective". In: *Journal of Management Information Systems* 33.1, pp. 296–325.

Gupta, Brij B et al. (2017). "Fighting against phishing attacks: state of the art and future challenges". In: *Neural Computing and Applications* 28.12, pp. 3629–3654.

Gupta, Surbhi, Abhishek Singhal, and Akanksha Kapoor (2016). "A literature survey on social engineering attacks: Phishing attack". In: *2016 international conference on computing, communication and automation (ICCCA)*. IEEE, pp. 537–540.

H, Wunsch et al. (2008). "Variation in critical care services across North America and Western Europe". In: *Crit Care Med* 36.10, p. 2787.

Halevi, Tzipora, James Lewis, and Nasir Memon (2013). "A pilot study of cyber security and privacy related behavior and personality traits". In: *Proceedings of the 22nd international conference on world wide web*, pp. 737–744.

Halevi, Tzipora, Nasir Memon, and Oded Nov (2015). "Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks". In: *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)*.

Halfond, William G, Jeremy Viegas, Alessandro Orso, et al. (2006). "A classification of SQL-injection attacks and countermeasures". In: *Proceedings of the IEEE international symposium on secure software engineering*. Vol. 1. IEEE, pp. 13–15.

Halko, Nathan, Per-Gunnar Martinsson, and Joel A Tropp (2011). "Finding structure with randomness: Probabilistic algorithms for constructing approximate matrix decompositions". In: *SIAM review* 53.2, pp. 217–288.

Halloran, M.E. et al. (2008). "Modeling targeted layered containment of an influenza pandemic". In: *Proc. Natl. Acad. Sci* 105, pp. 4639–4644.

Hamad, Hatem M and Mahmoud Al-Hoby (2012). "Managing intrusion detection as a service in cloud networks". In: *Managing intrusion detection as a service in cloud networks* 41.1.

Han, Dun, Mei Sun, and Dandan Li (2015). "Epidemic process on activity-driven modular networks". In: *Physica A: Statistical Mechanics and its Applications* 432, pp. 354–362.

Han, Jonghyun and Hyunju Lee (2012). "Analyzing social media friendship for personalization". In: *Proceedings of the 2012 workshop on Data-driven user behavioral modelling and mining from social media*, pp. 1–2.

Harary, F. (1995). *Graph Theory*. Perseus.

Harris, T.E (1989). *The theory of branching processes*. Dover Publications.

Hartigan, John A and Manchek A Wong (1979). "Algorithm AS 136: A k-means clustering algorithm". In: *Journal of the royal statistical society. series c (applied statistics)* 28.1, pp. 100–108.

Hastie, Trevor, Robert Tibshirani, and Jerome Friedman (2009). *The elements of statistical learning: data mining, inference, and prediction*. Springer Science & Business Media.

Hatchett, R.J., C.E. Mecher, and Lipsitch M (2007). "Public Health Interventions and Epidemic Intensity During the 1918 Influenza Pandemic". In: *Proc. Natl Acad. Sci.* **104**, pp. 7582–7587.

Heartfield, Ryan and George Loukas (2015). "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks". In: *ACM Computing Surveys (CSUR)* 48.3, pp. 1–39.

— (2016a). "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks". In: *ACM Computing Surveys (CSUR)* 48.3, p. 37.

— (2016b). "Evaluating the reliability of users as human sensors of social media security threats". In: *Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), 2016 International Conference On*. IEEE, pp. 1–7.

— (2016c). "Predicting the performance of users as human sensors of security threats in social media". In: *International Journal on Cyber Situational Awareness (IJCSA)* 1.1.

— (2018). "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework". In: *Computers & Security* 76, pp. 101–127.

Heartfield, Ryan, George Loukas, and Diane Gan (2016). "You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks". In: *IEEE Access* 4, pp. 6910–6928.

— (2017). "An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks". In: *Software Engineering Research, Management and Applications (SERA), 2017 IEEE 15th International Conference on*. IEEE, pp. 371–378.

Heffernan, J.M., R.J. Smith, and L.M. Wahl (2005). "Perspectives on the basic reproductive ratio". In: *J. R. Soc. Interface* 2, p. 281.

Hemsley, Kevin and Ronald Fisher (2018). "A history of cyber incidents and threats involving industrial control systems". In: *International Conference on Critical Infrastructure Protection*. Springer, pp. 215–242.

Henshel, D et al. (2015). "Trust as a human factor in holistic cyber security risk assessment". In: *Procedia Manufacturing* 3, pp. 1117–1124.

Hethecote, H.W. and J.A. Yorke (1984). "Gonorrhea: trasmission and control". In: *Lect. Notes Biomath* 56, pp. 1–105.

Hijazi, Haneen, Thair Khdour, and Abdulsalam Alarabeyyat (2012). "A review of risk management in different software development methodologies". In: *International Journal of Computer Applications* 45.7, pp. 8–12.

Hinson, Gary (2008). "Social engineering techniques, risks, and controls". In: *EDPAC: The EDP Audit, Control, and Security Newsletter* 37.4-5, pp. 32–46.

Hodges, JL (1958). "The significance probability of the Smirnov two-sample test". In: *Arkiv för Matematik* 3.5, pp. 469–486.

Holme, Petter (2015). "Modern temporal network theory: a colloquium". In: *The European Physical Journal B* 88.9, p. 234.

Holme, Petter and Fredrik Liljeros (2014). "Birth and death of links control disease spreading in empirical contact networks". In: *Scientific reports* 4.

Holme, Petter and Naoki Masuda (2015). "The basic reproduction number as a predictor for epidemic outbreaks in temporal networks". In: *PloS one* 10.3, e0120567.

Holme, Petter and Jari Saramäki (2012). "Temporal networks". In: *Physics reports* 519.3, pp. 97–125.

Howard, Philip N and Bence Kollanyi (2016). "Bots,# StrongerIn, and# Brexit: computational propaganda during the UK-EU referendum". In:

Huang, K. (1987). *Statistical Mechanics*. Wiley.

Huang, Chung-Yuan et al. (2013). "A computer virus spreading model based on resource limitations and interaction costs". In: *Journal of Systems and Software* 86.3, pp. 801–808.

Huber, Markus et al. (2009). "Towards automating social engineering using social networking sites". In: *2009 International Conference on Computational Science and Engineering*. Vol. 3. IEEE, pp. 117–124.

Hufnagel, L., D. Brockmann, and T. Geisel (2004). "Forecast and control of epidemics in a globalized world". In: *Proc. Natl. Acad. Sci.* 101, p. 15124.

IEEE (2017). "ISO/IEC/IEEE International Standard - Systems and software engineering–Vocabulary". In: *ISO/IEC/IEEE 24765:2017(E)*, pp. 1–541.

Ikhalia, Ehinome (2017). "A malware threat avoidance model for online social network users". PhD thesis. Brunel University London.

International Air Transport Association (n.d.). URL: http://www.iata.org.

International data base (idb) (n.d.). URL: http://www.census.gov/ipc/www/idb/.

Investigators, The ANZIC Influenza (2009). "Critical Care Services and 2009 H1N1 Influenza in Australia and New Zealand". In: *New Engl J Med* 361, pp. 1925–1934.

Jagatic, Tom N et al. (2007). "Social phishing". In: *Communications of the ACM* 50.10, pp. 94–100.

Jakobsson, Markus (2005). "Modeling and preventing phishing attacks". In: *Financial Cryptography*. Vol. 5.

Jakobsson, Markus and Jacob Ratkiewicz (2006). "Designing ethical phishing experiments: a study of (ROT13) rOnl query features". In: *Proceedings of the 15th international conference on World Wide Web*. ACM, pp. 513–522.

Jeong, H., S. Mason, A.-L. Barabási, et al. (2001). "The large-scale organization of a metabolic networks". In: *Nature* **411**, pp. 41–41.

Jeong, H., S. Mason, A.-L. Barábasi, et al. (2001). "Lethality and centrality in protein networks". In: *Nature* **411**, pp. 41–42.

Jokinen, Juha et al. (2018). "Personal Internet Privacy and Surveillance: Implementation and evasion of user tracking". In:

Jordan, Tobias, Philippe De Wilde, and Fernando Buarque de Lima-Neto (2017). "Modeling Contagion of Behavior in Friendship Networks as Coordination Games". In: *Advances in Social Simulation 2015*. Springer, pp. 181–194.

Joseph Garcia, Angelo and Sinem Mollaoglu (2020). "Individuals' Capacities to Apply Transferred Knowledge in AEC Project Teams". In: *Journal of Construction Engineering and Management* 146.4, p. 04020016.

Karimi, Fariba, Verónica C Ramenzoni, and Petter Holme (2014). "Structural differences between open and direct communication in an online community". In: *Physica A: Statistical Mechanics and its Applications* 414, pp. 263–273.

Karsai, M., N. Perra, and A. Vespignani (2014). "Time varying networks and the weakness of strong ties". In: *Scientific Reports* 4, p. 4001.

Karsai, Márton, Mikko Kivelä, et al. (2011). "Small but slow world: How network topology and burstiness slow down spreading". In: *Physical Review E* 83.2, p. 025102.

Karsai, Márton, Nicola Perra, and Alessandro Vespignani (2014). "Time varying networks and the weakness of strong ties". In: *Scientific reports* 4, p. 4001.

Kas, Miray, L Richard Carley, and Kathleen M Carley (2013). "Monitoring social centrality for peer-to-peer network protection". In: *IEEE Communications Magazine* 51.12, pp. 155–161.

Kayes, Imrul and Adriana Iamnitchi (2017). "Online Social Networks and Media". In:

Keeling, M.J. and Rohani, P. (2008). *Modeling infectious diseases in humans and animals*. Pronceton Univeristy Press.

Keeling, M. J. and P. Rohani (2002). "Estimating spatial coupling in epidemiological systems: a mechanistic approach". In: *Ecology Letters* 5, p. 20.

Keeling, M.J. (2000). "Metapopulation moments: coupling, stochasticity and persistence". In: *Journal of Animal Ecology* 69, pp. 725–736.

Keeling, M.J. and P. Rohani (2002). "Estimating spatial coupling in epidemiological systems: a mechanistic approach". In: *Ecology Letters* **5**, pp. 20–29.

— (2008). *Modeling Infectious Disease in Humans and Animals*. Princeton University Press.

Keeling, Matt J and Pejman Rohani (2011). *Modeling infectious diseases in humans and animals*. Princeton University Press.

Kelly, Ronald and Richard Neetz (1988). "Rapid prototyping: the procedure for software". In: *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*. IEEE, pp. 644–652.

Kempe, David, Jon Kleinberg, and Amit Kumar (2002). "Connectivity and inference problems for temporal networks". In: *Journal of Computer and System Sciences* 64.4, pp. 820–842.

Kempe, David, Jon Kleinberg, and Éva Tardos (2003). "Maximizing the spread of influence through a social network". In: *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, pp. 137–146.

Kendall, M. (1938). In: *Biometrika* 30, p. 81.

Kephart, Jeffrey O and Steve R White (1992). "Directed-graph epidemiological models of computer viruses". In: *Computation: the micro and the macro view*. World Scientific, pp. 71–102.

Kermack, W. and A. McKendrick (1927). "A Contribution to the Mathematical Theory of Epidemics". In: *P Roy Soc Long A Mat.* **115**, pp. 700–721.

Kermack, William Ogilvy and Anderson G McKendrick (1932). "Contributions to the mathematical theory of epidemics. II.—The problem of endemicity". In: *Proc. R. Soc. Lond. A* 138.834, pp. 55–83.

Khan, Ajab and Reiko Heckel (2011). "Model-based stochastic simulation of super peer promotion in P2P VoIP using graph transformation". In: *Data Communication Networking (DCNET), 2011 Proceedings of the International Conference on*. IEEE, pp. 1–11.

Khan, K. et al. (2009). "Spread of a novel influenza A(H1N1) virus via global airline transportation". In: *N Engl J Med* 361, pp. 212–214.

Kibanov, Mark et al. (2014). "Temporal evolution of contacts and communities in networks of face-to-face human interactions". In: *Science China Information Sciences* 57.3, pp. 1–17.

Kim, Yusoon and Thomas Y Choi (2018). "Tie strength and value creation in the buyer-supplier context: A U-shaped relation moderated by dependence asymmetry". In: *Journal of Management* 44.3, pp. 1029–1064.

King's-Edgehill School web site, First cases in Canada was related to a school trip in Mexico (n.d.). URL: http://www.kes.ns.ca/flu_chronology.asp.

Kleinberg, J.M (1999). "Authoritative sources in a hyperlinked environment". In: *Journal of the ACM* **46**, pp. 604–632.

— (2001). "Hubs authorities and communities". In: *Computing surveys* **31**, pp. 1–3.

Kleinberg, J. et al. (1999). " The web as a graph: measurements, models and methods". In: *LNCS* **1627**, pp. 1–18.

Knapp, Eric D and Joel Thomas Langill (2014). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress.

Koch, Daniel B (2016). "A multi-agent simulation tool for micro-scale contagion spread studies". In: *Global Humanitarian Technology Conference (GHTC), 2016*. IEEE, pp. 179–182.

Kovanen, Lauri et al. (2013). "Temporal motifs reveal homophily, gender-specific patterns, and group talk in call sequences". In: *Proceedings of the National Academy of Sciences*, p. 201307941.

Kramer, Adam DI, Jamie E Guillory, and Jeffrey T Hancock (2014). "Experimental evidence of massive-scale emotional contagion through social networks". In: *Proceedings of the National Academy of Sciences*, p. 201320040.

Krapivsky, P.L. and S. Redner (2001). "Organization of growing random networks". In: *Physical Review E* **63**, p. 066123.

Krapivsky, P.L., S. Redner, and F. Leyvraz (2000). In: *Physical Review Letter* **85**, p. 4629.

Krombholz, Katharina et al. (2015). "Advanced social engineering attacks". In: *Journal of Information Security and applications* 22, pp. 113–122.

Kuhl, Michael E et al. (2007). "Cyber attack modeling and simulation for network security analysis". In: *Proceedings of the 39th Conference on Winter Simulation: 40 years! The best is yet to come*. IEEE Press, pp. 1180–1188.

Kumar, R. et al. (2000). " The Web as a Graph". In: *PODS'00: Proceeding of nineteenth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database System*, pp. 1–10.

Kuperman, Marcelo and Guillermo Abramson (2001). "Small world effect in an epidemiological model". In: *Physical Review Letters* 86.13, p. 2909.

Langville, A.N. and Meyer, C.D. (2006). *Google's PageRank and Beyond: The Science of Search Engine Rankings*. Princeton University Press.

Lastname (2007). "Title". In: *Journal of Sth*.

Lawyer, Glenn (2015). "Understanding the influence of all nodes in a network". In: *Scientific reports* 5.1, pp. 1–9.

Lee, Kyumin, James Caverlee, and Steve Webb (2010). "Uncovering social spammers: social honeypots+ machine learning". In: *Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval*. ACM, pp. 435–442.

Lee, Sangho and Jong Kim (2014). "Early filtering of ephemeral malicious accounts on Twitter". In: *Computer Communications* 54, pp. 48–57.

Lerman, Kristina, Xiaoran Yan, and Xin-Zeng Wu (2016). "The" majority illusion" in social networks". In: *PloS one* 11.2, e0147617.

Lessler, J. et al. (2009). "Incubation periods of acute respiratory viral infections: a systematic review". In: *Lancet Infect DisA* 9, pp. 291–300.

Levin, Richard B (1990). *The computer virus handbook*. Osborne McGraw-Hill.

Li, Ming-Xia et al. (2014). "Statistically validated mobile communication networks: the evolution of motifs in European and Chinese data". In: *New Journal of Physics* 16.8, p. 083038.

Liben-Nowell, David and Jon Kleinberg (2007). "The link-prediction problem for social networks". In: *Journal of the American society for information science and technology* 58.7, pp. 1019–1031.

Liljeros, F. et al. (2001). "The web of human sexual contacts". In: *Nature* **411**, pp. 907–908.

Liljeros, Fredrik, Johan Giesecke, and Petter Holme (2007). "The contact network of inpatients in a regional healthcare system. A longitudinal case study". In: *Mathematical Population Studies* 14.4, pp. 269–284.

Lim, W.S. (2007). "Pandemic flu: clinical management of patients with an influenza-like illness during an influenza pandemic". In: *Thorax* 62, pp. 1–46.

Lipsitch, M. et al. (2009). In: *PLoS ONE* 4, e6895.

Liu, Chang et al. (2005). "Beyond concern—a privacy-trust-behavioral intention model of electronic commerce". In: *Information & Management* 42.2, pp. 289–304.

Liu, Jian-Guo et al. (2016). "Locating influential nodes via dynamics-sensitive centrality". In: *Scientific reports* 6.1, pp. 1–8.

Liu, Lan et al. (2017). "Malware propagation and prevention model for time-varying community networks within software defined networks". In: *Security and Communication Networks* 2017.

Liu, Lijun, Xiaodan Wei, and Naimin Zhang (2019). "Global stability of a network-based SIRS epidemic model with nonmonotone incidence rate". In: *Physica A: Statistical Mechanics and its Applications* 515, pp. 587–599.

Liu, Suyu et al. (2014). "Controlling contagion processes in activity driven networks". In: *Physical review letters* 112.11, p. 118702.

Liu, Su-Yu, Andrea Baronchelli, and Nicola Perra (2013). "Contagion dynamics in time-varying metapopulation networks". In: *Physical Review E* 87.3, p. 032805.

Lloyd, A.L. and R.M. May (1996). "Spatial heterogeneity in epidemic models". In: *J. Theor. Biol.* 179, pp. 1–11.

Lloyd, Alun L and Robert M May (2001a). "AL Lloyd and RM May, Science 292, 1316 (2001)." In: *Science* 292, p. 1316.

— (2001b). "How viruses spread among computers and people". In: *Science* 292.5520, pp. 1316–1317.

Longini, I.M. (1988). "A mathematical model for predicting the geographic spread of new infectious agents". In: *Math. Biosci* 90, pp. 367–383.

Longini, I.M., M.E. Halloran, et al. (2004). "Containing Pandemic Influenza with Antiviral Agents". In: *Am J Epidemiol* 159, p. 623.

Longini, I.M., A. Nizam, et al. (2005). "Containing pandemic influenza at the source". In: *Science* 309, pp. 1083–1087.

López-Pintado, Dunia (2006). "Contagion and coordination in random networks". In: *International Journal of Game Theory* 34.3, pp. 371–381.

— (2008). "Diffusion in complex social networks". In: *Games and Economic Behavior* 62.2, pp. 573–590.

Lovász, L. (1993). "Random walks on graphs: a survey". In: *Mathematical studies* **2**, pp. 1–46.

Lu, Dongyuan et al. (2016). "Who are your "real" friends: analyzing and distinguishing between offline and online friendships from social multimedia data". In: *IEEE Transactions on Multimedia* 19.6, pp. 1299–1313.

Ma, S.K. (1985). *Statistical Mechanics*. World Scientific.

Machens, Anna et al. (2013). "An infectious disease model on empirical networks of human contact: bridging the gap between dynamic network data and contact matrices". In: *BMC infectious diseases* 13.1, p. 1.

Mandelbrot, B.B. (1982). *The Fractal Geometry of Nature*. Freeman.

Mangan, S. and U. Alon (2003). "Structure and function of the feed-forward loop network motif". In: *Proceeding of the National Academy of Science (USA)* **100**, pp. 11980–11985.

Markel, H. et al. (2007). "Nonpharmaceutical Interventions Implemented by US Cities During the 1918-1919 Influenza Pandemic". In: *JAMA* **298**, p. 6.

Martcheva, Maia (2015). *An introduction to mathematical epidemiology*. Vol. 61. Springer.

Martinez-Romo, Juan and Lourdes Araujo (2013). "Detecting malicious tweets in trending topics using a statistical analysis of language". In: *Expert Systems with Applications* 40.8, pp. 2992–3000.

Martinsson, Per-Gunnar, Vladimir Rokhlin, and Mark Tygert (2011). "A randomized algorithm for the decomposition of matrices". In: *Applied and Computational Harmonic Analysis* 30.1, pp. 47–68.

Masuda, Naoki and Petter Holme (2013). "Predicting and controlling infectious disease epidemics using temporal networks". In: *F1000 prime reports* 5, p. 6.

— (2017). "Introduction to temporal network epidemiology". In: *Temporal Network Epidemiology*. Springer, pp. 1–16.

Matthews, P. (1988). "Covering problems for Brownian motion on spheres". In: *Ann. Prob.*, pp. 189–199.

May, R.M. and A.L. Lloyd (2001). "Infectious dynamics on scale-free networks". In: *Phys. Rev. E* 64, p. 066112.

McAfee (2018). "Economic Impact of Cybercrime—No Slowing Down". In: *McAfee and Center for Strategic International Studies*. URL: https://www.csis.org/analysis/economic-impact-cybercrime.

McPherson, Miller, Lynn Smith-Lovin, and James M Cook (2001). "Birds of a feather: Homophily in social networks". In: *Annual review of sociology* 27.1, pp. 415–444.

Mehrabi, Mohamad Ali, Christophe Doche, and Alireza Jolfaei (2020). "Elliptic curve cryptography point multiplication core for hardware security module". In: *IEEE Transactions on Computers* 69.11, pp. 1707–1718.

Meloni, Sandro et al. (2011). "Modeling human mobility responses to the large-scale spreading of infectious diseases". In: *Scientific reports* 1, p. 62.

Merler, S. and M. Ajelli (2010). "The role of population heterogeneity and human mobility in the spread of pandemic influenza". In: *Proc. Royal Soc. B: Biological Sciences* 277, pp. 557–565.

Milgram, S. (1967). "The small world problem". In: *Psychoology Today* **2**, pp. 60–67.

Miller, Joel C (2009). "Spread of infectious disease through clustered populations". In: *Journal of the Royal Society Interface* 6.41, pp. 1121–1134.

Mills, C.E., J.M. Robins, and M. Lipsitch (2004). "Transmissibility of 1918 pandemic influenza". In: *Nature* 432, pp. 904–906.

Milo, R. et al. (2002). "Network motifs: simple building blocks of complex networks". In: *Science* **298**, pp. 824–827.

Min, Byungjoon, K-I Goh, and Alexei Vazquez (2011). "Spreading dynamics following bursty human activity patterns". In: *Physical Review E* 83.3, p. 036102.

Ministère de la Santé et des Sports, Official Update, May 1 (n.d.). URL: http://www.sante-sports.gouv.fr/actualite-presse/presse-sante/communiques/bulletin-quotidien-nouvelle-grippe-h1n1-dite-porcine.html.

Ministerio de la Protecciìon Social República de Colombia, Official Update, May 3 2009 (n.d.). URL: http://www.minproteccionsocial.gov.co/VBeContent/NewsDetail.asp?ID=18582&IDCompany=3.

Ministerio de Salud Pública de Guatemala, Official Update, May 5 2009 (n.d.). URL: http://portal.mspas.gob.gt/index.php?ID=6128&action=display&ID_BOLETIN=61.

Ministerio de Salud Pública y Asistencia Social, 8th official update, May 3, 2009 (n.d.). URL: http://www.mspas.gob.sv/virus_gripeA_H1N1/boletines.htm.

Ministerio De Sanidad y Political Social, Official Update, April 27 2009 (n.d.). URL: http://www.msc.es/servCiudadanos/alertas/comunicadosNuevaGripe jsp?time=1238536800000.

Ministry of Health Welfare and Sport (Netherlands), First victim Mexican flu, April 30 2009 (n.d.). URL: http://www.minvws.nl/en/nieuwsberichten/pg/2009/first-victim-mexican-flu.asp.

Miritello, Giovanna, Esteban Moro, and Rubén Lara (2011). "Dynamical strength of social ties in information spreading". In: *Physical Review E* 83.4, p. 045102.

Mistry, Dina et al. (2015). "Committed activists and the reshaping of status-quo social consensus". In: *Physical Review E* 92.4, p. 042805.

Miyamoto, Daisuke, Hiroaki Hazeyama, and Youki Kadobayashi (2008). "An evaluation of machine learning-based methods for detection of phishing sites". In: *International Conference on Neural Information Processing*. Springer, pp. 539–546.

Mohammed, Nabil M et al. (2017). "Exploring software security approaches in software development lifecycle: A systematic mapping study". In: *Computer Standards & Interfaces* 50, pp. 107–115.

Mohebzada, Jamshaid G et al. (2012). "Phishing in a university community: Two large scale phishing experiments". In: *2012 international conference on innovations in information technology (IIT)*. IEEE, pp. 249–254.

Moinet, Antoine, Michele Starnini, and Romualdo Pastor-Satorras (2015). "Burstiness and aging in social temporal networks". In: *Physical review letters* 114.10, p. 108701.

Moler, C.D. and K.A. Moler (2003). " Numerical Computing with Matlab". In:

Monasson, R. (1999). "Diffusion, localization and dispersion relations on small-world". In: *Eur. Phys. J. B* 12, pp. 555–567.

Mønsted, Bjarke et al. (2017). "Evidence of complex contagion of information in social media: An experiment using Twitter bots". In: *PloS one* 12.9, e0184148.

Moody, James (2002). "The importance of relationship timing for diffusion". In: *Social Forces* 81.1, pp. 25–56.

Moreno, J.L. (1934). *Who Shall Survive? Foundations of Sociometry, Group Psychotherapy and Sociodram*. Beacon House.

Moreno, Y., R. Pastor-Satorras, and A. Vespignani (2004). "Epidemic outbreaks in complex heterogeneous networks". In: *Eur. Phys. J. B* 26, pp. 521–529.

Moreno, Yamir and Alexei Vazquez (2003). "Disease spreading in structured scale-free networks". In: *The European Physical Journal B-Condensed Matter and Complex Systems* 31.2, pp. 265–271.

Morris, Martina and Mirjam Kretzschmar (1995). "Concurrent partnerships and transmission dynamics in networks". In: *Social Networks* 17.3, pp. 299–318.

Morstatter, Fred et al. (2016). "A New Approach to Bot Detection: Striking the Balance Between Precision and Recall". In: *Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. ASONAM '16. Davis, California: IEEE Press, pp. 533–540. ISBN: 978-1-5090-2846-7. URL: http://dl.acm.org/citation.cfm?id=3192424.3192525.

Mouton, Francois, Louise Leenen, and Hein S Venter (2016). "Social engineering attack examples, templates and scenarios". In: *Computers & Security* 59, pp. 186–209.

Murray, J.D. (2005). *Mathematical Biology.* 3rd edition Berlin: Springer Verla.

Nadini, Matthieu et al. (2018). "Epidemic spreading in modular time-varying networks". In: *Scientific reports* 8.1, pp. 1–11.

Name (2006). "Title". In: *Journal of Sth*.

Narayanan, Arvind and Vitaly Shmatikov (2009). "De-anonymizing social networks". In: *Security and Privacy, 2009 30th IEEE Symposium on*. IEEE, pp. 173–187.

Nasution, MFF and Heinz Roland Weistroffer (2009). "Documentation in systems development: A significant criterion for project success". In: *2009 42nd Hawaii International Conference on System Sciences*. IEEE, pp. 1–9.

(2005). In: *Network Science*. Ed. by Committee on Network Science for Future Army Applications National Research Council. Washington DC: The National Academies Press.

Newman, M.E.J. (2010). *Networks, an Introduction*. Oxford University Press.

Newman, M. E. J., S. Forrest, and J. Balthrop (2002c). " Email networks and the spread of computer viruses". In: *Physical Review E* **66**, p. 035101.

Newman, M.E.J. (2002a). "Assortative mixing in networks". In: *Physical Review Letters* **89**, p. 208701.

— (2002b). "Community structure in social and biological networks". In: *Proceeding of the National Academy of Science (USA)* **99**, p. 78217826.

— (2001a). "Scientific collaboration networks. I. Network contruction and fundamental results". In: *Phys. Rev. E* **64**, p. 016131.

— (2001b). "Scientific collaboration networks. II. Shortest paths, weighted networks and centrality". In: *Phys. Rev. E* **64**, p. 016132.

— (2001c). "The structure of scientific collaboration networks". In: *Proc. Natl Acad. Sci.* **98**, pp. 404–409.

Newman, M.E.J., S.H. Strogatz, and D.J. Watts (2001). In: *Physical Review E* **64**, p. 026118.

Newman, Mark (2018). *Networks*. Oxford university press.

Newman, Mark EJ (2002). "Spread of epidemic disease on networks". In: *Physical review E* 66.1, p. 016128.

Newman, Mark EJ, Stephanie Forrest, and Justin Balthrop (2002). "Email networks and the spread of computer viruses". In: *Physical Review E* 66.3, p. 035101.

Newman, MEJ (2010). *Networks: An Introduction Oxford Univ*.

Nishiura, H., C. Castillo-Chavez, et al. (2009). "Transmission potential of the new influenza A(H1N1) virus and its age-specificity in Japan". In: *EuroSurveilliance* 14.

Nishiura, H., N.M. Wilson, and M.G. Baker (2009). "Estimating the reproduction number of the novel influenza A virus (H1N1) in a Southern Hemisphere setting: preliminary estimate in New Zealand". In: *NZ Med J* 122, pp. 1–5.

Noh, J.D. and H. Rieger (2004). "Random walks on complex networks". In: *Phys. Rev. Lett.* 92, p. 118701.

Novartis successfully demonstrates capabilities of cell-based technology for production of A(H1N1) vaccine (n.d.). URL: http://www.novartis.com/newsroom/media-releases/en/2009/1322241.shtml.

Official Airline Guide (n.d.). URL: http://www.oag.com/.

Okabe, A. and Boots, B. and Sugihara, K. and Chiu, S.N. (2000). *Spatial Tessellations - Concepts and Applications of Voronoi Diagrams*. John Wiley.

Oltramari, Alessandro et al. (2015). "Towards a Human Factors Ontology for Cyber Security." In: *Stids*, pp. 26–33.

Onnela, J-P et al. (2007). "Structure and tie strengths in mobile communication networks". In: *Proceedings of the national academy of sciences* 104.18, pp. 7332–7336.

Oreizy, Peyman et al. (1999). "An architecture-based approach to self-adaptive software". In: *IEEE Intelligent Systems and Their Applications* 14.3, pp. 54–62.

Owens, Jim and Jeanna Matthews (2008). "A study of passwords and methods used in brute-force SSH attacks". In: *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*.

Park, A.W., S. Gubbins, and C.A. Gilligan (2002). "Extinction times for closed epidemics: the effects of host spatial structure". In: *Ecology Letters* 5, pp. 747–755.

Pastor-Satorras, R. and A. Vespignani (2001). "Epidemic spreading in scale-free networks". In: *Phys. Rev. Lett.* 86, pp. 3200–3203.

— (2002). "Immunization of complex networks". In: *Phys. Rev. E* 65, p. 035108.

— (2004). *Evolution and Structure of Internet: A Statistical Physics Approach*. Cambridge University Press.

Pastor-Satorras, Romualdo, Claudio Castellano, et al. (2015). "Epidemic processes in complex networks". In: *Reviews of modern physics* 87.3, p. 925.

Pastor-Satorras, Romualdo, Alexei Vázquez, and Alessandro Vespignani (2001). "Dynamical and correlation properties of the Internet". In: *Physical review letters* 87.25, p. 258701.

Pastor-Satorras, Romualdo and Alessandro Vespignani (2001). "Epidemic spreading in scale-free networks". In: *Physical review letters* 86.14, p. 3200.

— (2007). *Evolution and structure of the Internet: A statistical physics approach*. Cambridge University Press.

Peiris, J.S.M., K.Y. Yuen, and K. Stohr (2003). In: *N. Engl. J. Med.* 349, p. 2431.

Peixoto, Tiago P and Martin Rosvall (2017). "Modelling sequences and temporal networks with dynamic community structures". In: *Nature communications* 8.1, p. 582.

Peng, Sancheng et al. (2017). "An immunization framework for social networks through big data based influence modeling". In: *IEEE Transactions on Dependable and Secure Computing*.

Perra, N., A. Baronchelli, et al. (2012). “Random walks and search in time varying networks”. In: *Physical Review Letter* 109, p. 238701.

Perra, N. and S. Fortunato (2008). “Spectral centrality measures in complex networks”. In: *Phys. Rev. E* 78, p. 036107.

Perra, N., B. Gonçalves, et al. (2012). “Activity driven modeling of time-varying networks”. In: *Scientific Reports* 2, p. 469.

Perra, N., V. Zlatić, et al. (2009). “PageRank equation and localization in the WWW”. In: *EPL* 88, p. 48002.

Perra, Nicola, Andrea Baronchelli, et al. (2012). “Random walks and search in time-varying networks”. In: *Physical review letters* 109.23, p. 238701.

Perra, Nicola, Bruno Gonçalves, et al. (2012). “Activity driven modeling of time varying networks”. In: *Scientific reports* 2, p. 469.

Pfitzner, René et al. (2013). “Betweenness preference: Quantifying correlations in the topological dynamics of temporal networks”. In: *Physical review letters* 110.19, p. 198701.

Pinheiro, Flavio L et al. (2014). “Origin of peer influence in social networks”. In: *Physical review letters* 112.9, p. 098702.

Poletti, P. et al. (2009). “Spontaneous Behavioural Changes in Response to Epidemics”. In: *J. Theor. Biol.*, pp. 225–228.

Prakash, B Aditya, Deepayan Chakrabarti, et al. (2012). “Threshold conditions for arbitrary cascade models on arbitrary networks”. In: *Knowledge and information systems* 33.3, pp. 549–575.

Prakash, B Aditya, Hanghang Tong, et al. (2010). “Virus propagation on time-varying networks: Theory and immunization algorithms”. In: *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*. Springer, pp. 99–114.

Proofpoint (2020). “State of the Phish”. In: *2020 ’State of the Phish’ Report*. URL: https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/proofpoint/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf.

Public Health Agency of Canada, Cases of H1N1 Flu Virus in Canada, June 10 2009 (n.d.). URL: http://www.phac-aspc.gc.ca/alert-alerte/swine-porcine/surveillance-archive/20090610-eng.php.

PurpleSec (2019). “The Ultimate List Of Cyber Security Statistics For 2019”. In: *Cyber Security Statistics*. URL: https://purplesec.us/resources/cyber-security-statistics/.

Qureshi, Israr et al. (2018). "IT-mediated social interactions and knowledge sharing: Role of competence-based trust and background heterogeneity". In: *Information Systems Journal* 28.5, pp. 929–955.

R, Perez-Padilla et al. (2009). "Pneumonia and Respiratory Failure from Swine-Origin Influenza A (H1N1) in Mexico". In: *New Engl J Med* 361, pp. 680–689.

Rahman, Syed Sadiqur et al. (2017). "Assessing the cyber-trustworthiness of human-as-a-sensor reports from mobile devices". In: *Software Engineering Research, Management and Applications (SERA), 2017 IEEE 15th International Conference on*. IEEE, pp. 387–394.

Ramasco, J.J., S.N. Dorogovtsev, and R. Pastor-Satorras (2004). "Self-Organization of collaboration networks". In: *Phys. Rev. E* **70**, p. 036106.

Rathod, Anooksha Yogesh, Shubham Pandya, and Nishant Doshi (2020). "IoT and modern marketing: Its social implications". In: *2020 22nd International Conference on Advanced Communication Technology (ICACT)*. IEEE, pp. 407–413.

Ratkiewicz, Jacob et al. (2011). "Detecting and tracking political abuse in social media." In: *ICWSM* 11, pp. 297–304.

Rello, J. et al. (2009). *Intensive care adult patients with severe respiratory failure caused by Influenza A (H1N1)v in Spain*.

Ren, Guangming and Xingyuan Wang (2014). "Epidemic spreading in time-varying community networks". In: *Chaos: An Interdisciplinary Journal of Nonlinear Science* 24.2, p. 023116.

Reports of the Brazilian Health Department (Ministerio da Saude) (n.d.). URL: http://portal.saude.gov.br/portal/saude.

Ribeiro, B, N. Perra, and A. Baronchelli (2013). "Quantifying the effect of temporal resolution on time-varying networks". In: *Scientific Reports* 3, p. 3006.

Ribeiro, Bruno, Nicola Perra, and Andrea Baronchelli (2013). "Quantifying the effect of temporal resolution on time-varying networks". In: *Scientific reports* 3, p. 3006.

Robert Koch Institut, Neue Influenza A/H1N1 in Deutschland Bewertung des bisherigen Geschehens (n.d.). URL: http://www.rki.de/cln_091/nn_200120/DE/Content/Infekt/EpidBull/Archiv/2009/25/Art__01.html.

Roberts, M.J. and J.A.P. Heesterbeek (2007). "Model-consistent estimation of the basic reproduction number from the incidence of an emerging infection". In: *J. Math. Bio.* 55, pp. 803–816.

Rocha, Luis EC and Vincent D Blondel (2013). "Bursts of vertex activation and epidemics in evolving networks". In: *PLoS computational biology* 9.3, e1002974.

Rocha, Luis EC, Fredrik Liljeros, and Petter Holme (2011). "Simulated epidemics in an empirical spatiotemporal network of 50,185 sexual contacts". In: *PLoS Comput Biol* 7.3, e1001109.

Rocha, Luis EC and Naoki Masuda (2014). "Random walk centrality for temporal networks". In: *New Journal of Physics* 16.6, p. 063023.

Roche H-L: Update on current developments around Tamiflu (2007) (n.d.). URL: http://www.roche.com/med_events_mb0407.

Rodgers, G.J. and A.J. Bray (1988). "Density of states of a sparse random matrix". In: *Phys. Rev. B.* 37, pp. 3557–3562.

Rohani, P., D.J.D. Earn, and B.T. Grenfell (1999). "Opposite patterns of synchrony in sympatric disease metapopulations". In: *Science* 286, pp. 968–971.

Romero, Daniel M, Brendan Meeder, and Jon Kleinberg (2011). "Differences in the mechanics of information diffusion across topics: idioms, political hashtags, and complex contagion on twitter". In: *Proceedings of the 20th international conference on World wide web*. ACM, pp. 695–704.

Romero, Daniel M, Brian Uzzi, and Jon Kleinberg (2016). "Social networks under stress". In: *Proceedings of the 25th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, pp. 9–20.

Rowe, Dale C., Barry M. Lunt, and Joseph J. Ekstrom (2011). "The Role of Cybersecurity in Information Technology Education". In: *Proceedings of the 2011 Conference on Information Technology Education*. SIGITE '11. West Point, New York, USA: ACM, pp. 113–122. ISBN: 978-1-4503-1017-8. DOI: 10.1145/2047594.2047628. URL: http://doi.acm.org/10.1145/2047594.2047628.

Ruby, Sam, David B Copeland, and Dave Thomas (2020). *Agile Web Development with Rails 6*. Pragmatic bookshelf.

Rvachev, L.A. and I.M. Longini (1985). "A mathematical model for the global spread of influenza". In: *Mathematical Biosciences* 75, pp. 3–22.

Saeedian, M et al. (2017). "Epidemic spreading on evolving signed networks". In: *Physical Review E* 95.2, p. 022314.

Sailer, Kerstin and Ian McCulloh (2012). "Social networks and spatial configuration—How office layouts drive social interaction". In: *Social networks* 34.1, pp. 47–58.

Salzberg, Steven L (1994). *C4. 5: Programs for machine learning by j. ross quinlan. morgan kaufmann publishers, inc., 1993*.

Samukhin, A., S. Dorogovtsev, and J. Mendes (2008). "Laplacian spectra and random walks on complex networks: are scale-free architectures really important?" In: *Phys. Rev. E* 77, p. 036115.

Sänger, Johannes et al. (2016). "Look before you leap: improving the users' ability to detect fraud in electronic marketplaces". In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, pp. 3870–3882.

Saramäki, Jari et al. (2007). "Generalizations of the clustering coefficient to weighted complex networks". In: *Physical Review E* 75.2, p. 027105.

Sarkar, Ashim (2018). "Overview of web development life cycle in software engineering". In: *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 3.6, pp. 2456–3307.

Sattenspiel, L. and K. Dietz (1995a). "A Structured Epidemic Model Incorporating Geographic Mobility Among Regions". In: *Mathematical Biosciences* **128**, pp. 71–91.

— (1995b). "A structured epidemic model incorporating geographic mobility among regions". In: *Math. Biosci.* 128, p. 71.

Schecter, Stuart et al. (2007). "The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies". In: *Proc. IEEE Symposium on Security and Privacy (S&P)*, pp. 51–65.

Scholtes, Ingo et al. (2014). "Causality-driven slow-down and speed-up of diffusion in non-Markovian temporal networks". In: *Nature communications* 5, p. 5024.

Scott, J. (2000). *Social Networks Analysis: a Handbook*. Sage Publications, London.

Sculley, D (2010). "Proceedings of the 19th International Conference on World Wide Web". In:

Secretaria de Salud, Mexico. Situation actual de la epidemia, Oct 12, 2009 (n.d.). URL: http://portal.salud.gob.mx/sites/salud/descargas/pdf/influenza/situacion_actual_epidemia_121009.pdf.

Sekara, Vedran, Arkadiusz Stopczynski, and Sune Lehmann (2016). "Fundamental structures of dynamic social networks". In: *Proceedings of the national academy of sciences* 113.36, pp. 9977–9982.

Serazzi, Giuseppe and Stefano Zanero (2004). "Computer virus propagation models". In: *Performance Tools and Applications to Networked Systems*. Springer, pp. 26–50.

Shao, Chengcheng et al. (2018). "The spread of low-credibility content by social bots". In: *Nature communications* 9.1, p. 4787.

Shao, Shuai et al. (2015). “Percolation of localized attack on complex networks”. In: *New Journal of Physics* 17.2, p. 023049.

Sheng, Steve et al. (2007). “Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish”. In: *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, pp. 88–99.

Shin, Dong-Hee (2010). “The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption”. In: *Interacting with computers* 22.5, pp. 428–438.

Siatuación actual de la epidemıa [Current situation of the epidemic] (July 16). Department of Health of the Mexican Government available online, in Spanish, at (n.d.). URL: http://portal.salud.gob.mx.

SimilarWeb (2020). *"Compare Websites Traffic with SimilarWeb Analytics Tool"*. URL: https://www.similarweb.com/top-websites/ (visited on 06/01/2020).

Singh, Jagdev et al. (2018). “A fractional epidemiological model for computer viruses pertaining to a new fractional derivative”. In: *Applied Mathematics and Computation* 316, pp. 504–515.

Singh, Jeetendra (2021). “Implementation of Memristor Towards Better Hardware/Software Security Design”. In: *Transactions on Electrical and Electronic Materials*, pp. 1–13.

Šišejković, Dominik et al. (2019). “Inter-lock: Logic encryption for processor cores beyond module boundaries”. In: *2019 IEEE European Test Symposium (ETS)*. IEEE, pp. 1–6.

Sloot, Peter MA, George Kampis, and László Gulyás (2013). *Advances in dynamic temporal networks: Understanding the temporal dynamics of complex adaptive networks*.

Smilkov, Daniel, Cesar A Hidalgo, and Ljupco Kocarev (2014). “Beyond network structure: How heterogeneous susceptibility modulates the spread of epidemics”. In: *Scientific reports* 4, p. 4795.

Smith, Aaron and D Page (2015). “Social media usage: 2005-2015”. In: *The Pew Research Center*.

Society of Critical Care Medicine, Critical Care Statistics in the United States 2006 (n.d.).

Sommerfeld A. (1949). *Partial Differential Equations in Physics*. Academic Press, New York.

Soumya, TR and S Revathy (2018). “Survey on threats in online social media”. In: *2018 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, pp. 0077–0081.

Stark, Fabian et al. (2015). "Captcha recognition with active deep learning". In: *GCPR Workshop on New Challenges in Neural Computation*. Vol. 10.

Starnini, Michele, Andrea Baronchelli, et al. (2012). "Random walks on temporal networks". In: *Physical Review E* 85.5, p. 056115.

Starnini, Michele, Anna Machens, et al. (2013). "Immunization strategies for epidemic processes in time-varying contact networks". In: *Journal of theoretical biology* 337, pp. 89–100.

Starnini, Michele and Romualdo Pastor-Satorras (2014). "Temporal percolation in activity-driven networks". In: *Physical Review E* 89.3, p. 032807.

Stauffer, D. and Aharony, A. (1994). *Introduction to Percolation Theory*. Taylor and Francis.

Stehlé, Juliette et al. (2011). "Simulation of an SEIR infectious disease model on the dynamic contact network of conference attendees". In: *BMC medicine* 9.1, p. 87.

Stella, Massimo, Emilio Ferrara, and Manlio De Domenico (2018). "Bots increase exposure to negative and inflammatory content in online social systems". In: *Proceedings of the National Academy of Sciences* 115.49, pp. 12435–12440.

Stieglitz, Stefan et al. (2017). "Do social bots dream of electric sheep? A categorisation of social media bot accounts". In: *arXiv preprint arXiv:1710.04044*.

Stojmenoviæ, Milica and Robert Biddle (2018). "Hide-and-seek with website identity information". In: *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, pp. 1–6.

Stringhini, Gianluca, Christopher Kruegel, and Giovanni Vigna (2010). "Detecting spammers on social networks". In: *Proceedings of the 26th annual computer security applications conference*. ACM, pp. 1–9.

Strohmaier, Markus and Claudia Wagner (2014). "Computational social science for the world wide web". In: *IEEE Intelligent Systems* 29.5, pp. 84–88.

Sukwong, Orathai, H Kim, and J Hoe (2010). "An empirical study of commercial antivirus software effectiveness". In: *Computer* 44.3, pp. 63–70.

Sukwong, Orathai, Hyong Kim, and James Hoe (2010). "Commercial antivirus software effectiveness: an empirical study". In: *Computer* 3, pp. 63–70.

Sun, Kaiyuan, Andrea Baronchelli, and Nicola Perra (2015). "Contrasting effects of strong ties on SIR and SIS processes in temporal networks". In: *The European Physical Journal B* 88.12, pp. 1–8.

Sun, Kaiyuan, Enrico Ubaldi, et al. (2019). "The effects of local and global link creation mechanisms on contagion processes unfolding on time-varying networks". In: *Temporal Network Theory*. Springer, pp. 305–324.

Sunny, Albert, Bhushan Kotnis, and Joy Kuri (2015). "Dynamics of history-dependent epidemics in temporal networks". In: *Physical Review E* 92.2, p. 022811.

Suranto, Beni (2015). "Software prototypes: Enhancing the quality of requirements engineering process". In: *2015 International Symposium on Technology Management and Emerging Technologies (ISTMET)*. IEEE, pp. 148–153.

Surma, Jerzy (2016). "Social exchange in online social networks. The reciprocity phenomenon on Facebook". In: *Computer Communications* 73, pp. 342–346.

Takaguchi, Taro, Naoki Masuda, and Petter Holme (2013). "Bursty communication patterns facilitate spreading in a threshold-based epidemic dynamics". In: *PloS one* 8.7, e68629.

Takaguchi, Taro, Nobuo Sato, et al. (2012). "Importance of individual events in temporal networks". In: *New Journal of Physics* 14.9, p. 093003.

Takahashi, Takeshi et al. (2013). "Risk visualization and alerting system: Architecture and proof-of-concept implementation". In: *Proceedings of the first international workshop on Security in embedded systems and smartphones*. ACM, pp. 3–10.

The Guardian, Spain confirms first swine flu case in Europe, April 27 2009 (n.d.). URL: http://www.guardian.co.uk/world/2009/apr/27/swine-flu-spain-europe.

The Information System of the Federal Health Monitoring (n.d.).

The Scottish Government, Scottish Government News Release, April 26 (n.d.). URL: http://www.scotland.gov.uk/News/Releases/2009/04/26164218.

Tiky, YT (2016). "Software Development Life Cycle". In: *Hongkong: THe Hongkong University of Science and Technology*.

Tipping, Michael E and Christopher M Bishop (1999). "Probabilistic principal component analysis". In: *Journal of the Royal Statistical Society: Series B (Statistical Methodology)* 61.3, pp. 611–622.

Tizzani, Michele et al. (2018). "Epidemic spreading and aging in temporal networks with memory". In: *Physical Review E* 98.6, p. 062315.

Tomasello, Mario V et al. (2014). "The role of endogenous and exogenous mechanisms in the formation of R&D networks". In: *Scientific reports* 4, p. 5679.

Toth, Damon JA et al. (2015). "The role of heterogeneity in contact timing and duration in network models of influenza spread in schools". In: *Journal of The Royal Society Interface* 12.108, p. 20150279.

Tsai, Wei-Tek et al. (2001). "End-to-end integration testing design". In: *25th Annual International Computer Software and Applications Conference. COMPSAC 2001*. IEEE, pp. 166–171.

Ubaldi, E. et al. (2016). "Asymptotic theory of time-varying social networks with heterogeneous activity and tie allocation". In: *Scientific Reports* 6, p. 35724.

Ubaldi, Enrico et al. (2017). "Burstiness and tie activation strategies in time-varying social networks". In: *Scientific Reports* 7, p. 46225.

UK Department of Health. Swine Flu: UK planning assumptions. Issued 3 September (2009).

Usa Today, Cuba confirms its 1st swine flu case, May 12 2009 (n.d.). URL: http://www.usatoday.com/news/world/2009-05-11-cuba_N.htm.

Valdano, Eugenio, Luca Ferreri, et al. (2015). "Analytical computation of the epidemic threshold on temporal networks". In: *Physical Review X* 5.2, p. 021005.

Valdano, Eugenio, Michele Re Fiorentin, et al. (2018). "Epidemic Threshold in Continuous-Time Evolving Networks". In: *Physical review letters* 120.6, p. 068302.

Van Kampen, N.G. (1992). *Stochastic Processes in Physics and Chemistry*. North-Holland Personal Library.

Van Tilborg, Henk CA and Sushil Jajodia (2014). *Encyclopedia of cryptography and security*. Springer Science & Business Media.

Vaniea, Kami and Yasmeen Rashidi (2016). "Tales of software updates: The process of updating software". In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 3215–3226.

Vázquez, A. (2007). "Epidemic outbreaks on structured populations". In: *J. Theor. Biol.* 245, pp. 125–129.

Ventresca, Mario and Dionne Aleman (2013). "Evaluation of strategies to mitigate contagion spread using social network characteristics". In: *Social Networks* 35.1, pp. 75–88.

Vespignani, A. (2009). "Predicting the behavior of techno-social systems". In: *Science* 325, pp. 425–428.

Viboud, C. et al. (2006). "Synchrony, Waves, and Spatial Hierarchies in the Spread of Influenza". In: *Science* 312, p. 447.

Vijayasarathy, Leo R and Charles W Butler (2015). "Choice of software development methodologies: Do organizational, project, and team characteristics matter?" In: *IEEE software* 33.5, pp. 86–94.

Volz, Erik and Lauren Ancel Meyers (2007). "Susceptible–infected–recovered epidemics in dynamic contact networks". In: *Proceedings of the Royal Society of London B: Biological Sciences* 274.1628, pp. 2925–2934.

Von Neumann, John, Arthur W Burks, et al. (1966). "Theory of self-reproducing automata". In: *IEEE Transactions on Neural Networks* 5.1, pp. 3–14.

Wagner, A. (2001). “The yeast protein interaction network evolves rapidly and contains few redudant duplicate genes”. In: *Mol. Biol. Evol.* **18**, pp. 1283–1292.

Wagner, Claudia, Silvia Mitter, et al. (2012). “When social bots attack: Modeling susceptibility of users in online social networks”. In: *Making Sense of Microposts (# MSM2012)* 2.4, pp. 1951–1959.

Wagner, Claudia, Matthew Rowe, et al. (2012). “What Catches Your Attention? An Empirical Study of Attention Patterns in Community Forums.” In: *ICWSM*.

Wallinga, J. and M. Lipsitch (2007). “How generation intervals shape the relationship between growth rates and reproductive numbers”. In: *Proc R Soc B* **274**, pp. 599–604.

Wallinga, J., P. Teunis, and M. Kretzschmar (2006). “Using data on social contacts to estimate age-specific transmission parameters for respiratory-spread infectious agents”. In: *Am. J. Epi.* **164**.

Wang, Alex Hai (2010). “Detecting spam bots in online social networking sites: a machine learning approach”. In: *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, pp. 335–342.

Wang, P (2009). “P. Wang, MC González, CA Hidalgo, and A.-L. Barabási, Science 324, 1071 (2009).” In: *Science* 324, p. 1071.

Wang, Pu et al. (2009). “Understanding the spreading patterns of mobile phone viruses”. In: *Science* 324.5930, pp. 1071–1076.

Wang, Zhen et al. (2016). “Statistical physics of vaccination”. In: *Physics Reports* 664, pp. 1–113.

Wasserman, S. and K. Faust (1994). “Social Network Analysis”. In: *Cambridge University Press.*

Watts, D. J. and S. H. Strogatz (1998). “ Collective dynamics of ‘small-world’ networks”. In: *Nature* **393**, pp. 440–442.

Watts, D.J. et al. (2005). “Multiscale, resurgent epidemics in a hierarchical metapopulations model”. In: *Proc. Natl. Acad. Sci.* 102, pp. 11157–11162.

Watts, Duncan J and Steven H Strogatz (1998). “Collective dynamics of ‘small-world’networks”. In: *nature* 393.6684, p. 440.

Weilkiens, Tim (2011). *Systems engineering with SysML/UML: modeling, analysis, design*. Elsevier.

Welsch, P. (2005). “Revolutionaty vanguard or echo chamber? Polical blogs and the mainstream media”. In: *Sunbelt 2005 presentation*.

West, G.B. (1996). *Introduction to Graph Theory*. Prentice Hall.

White, J.G. et al. (1986). “The structure of the nervous system of the nematode C. Elegans”. In: *Phil Trans R Soc London* **314**, p. 1340.

WHO official data (n.d.). URL: http://www.who.int/csr/disease/swineflu/en/.

WHO Wkly Epidemiol Rec (2009).

WHO, Chronology of Influenza A(H1N1) (n.d.). URL: http://www.searo.who.int/en/Section10/Section2562_14940.htm.

WHO, Pandemic (H1N1) 2009 briefing note 3 (revised): Changes in reporting requirements for pandemic (H1N1) 2009 virus infection (n.d.). URL: http://www.who.int/csr/disease/swineflu/notes/h1n1_surveillance_20090710/en/index.html.

Wiener, Norbert (1948). "Cybernetics". In: *Scientific American* 179.5, pp. 14–19.

Wilbanks, Linda R (2020). "Cyber Risks in Social Media". In: *International Conference on Human-Computer Interaction*. Springer, pp. 393–406.

Wiley, John (2008). "Security Engineering: A Guide to Building Dependable Distributed Systems". In: *2ed Editio*, pp. 239–274.

Williams, Matthew J and Mirco Musolesi (2016). "Spatio-temporal networks: reachability, centrality and robustness". In: *Royal Society open science* 3.6, p. 160196.

Wilson, Christo et al. (2009). "User interactions in social networks and their implications". In: *Proceedings of the 4th ACM European conference on Computer systems*. Acm, pp. 205–218.

Wilson, N. and M.G. Baker (2009). "The emerging influenza pandemic: estimating the case fatality ratio". In: *Euro Surveilliance* 14, p. 26.

Workman, Michael (2008). "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security". In: *Journal of the American Society for Information Science and Technology* 59.4, pp. 662–674.

World Health Organization. Clinical management of human infection with pandemic (H1N1) 2009: revised guidance, November 2009 (n.d.).

Wu, J.T. et al. (2006). "Reducing the impact of the next influenza pandemic using household-based public health interventions". In: *PLoS Med* 3, e361.

Xie, Peng et al. (2010). "Using Bayesian networks for cyber security analysis". In: *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP international conference on*. IEEE, pp. 211–220.

Xie, Yinglian et al. (2008). "Spamming botnets: signatures and characteristics". In: *ACM SIGCOMM Computer Communication Review* 38.4, pp. 171–182.

Xu, Shouhuai et al. (2014). "Adaptive epidemic dynamics in networks: Thresholds and control". In: *ACM Transactions on Autonomous and Adaptive Systems (TAAS)* 8.4, pp. 1–19.

Yang, Lu-Xing and Xiaofan Yang (2014a). “A new epidemic model of computer viruses”. In: *Communications in Nonlinear Science and Numerical Simulation* 19.6, pp. 1935–1944.

— (2014b). “The spread of computer viruses over a reduced scale-free network”. In: *Physica A: Statistical Mechanics and Its Applications* 396, pp. 173–184.

Yang, Lu-Xing, Xiaofan Yang, et al. (2013). “Epidemics of computer viruses: A complex-network approach”. In: *Applied Mathematics and Computation* 219.16, pp. 8705–8717.

Yasir, Muhammad et al. (2017). “Agent-based Modeling and Simulation of Virus on a Scale-Free Network”. In: *Proceedings of the International Conference on Future Networks and Distributed Systems*. ACM, p. 46.

Yu, Wei (2004). “Analyze the worm-based attack in large scale P2P networks”. In: *High Assurance Systems Engineering, 2004. Proceedings. Eighth IEEE International Symposium on*. IEEE, pp. 308–309.

Yu, Wei et al. (2005). “Peer-to-peer system-based active worm attacks: Modeling and analysis”. In: *Communications, 2005. ICC 2005. 2005 IEEE International Conference on*. Vol. 1. IEEE, pp. 295–300.

Zhang, Xi and Krishna Chaitanya Tadi (2007). “Modeling virus and antivirus spreading over hybrid wireless ad hoc and wired networks”. In: *Global Telecommunications Conference, 2007. GLOBECOM’07. IEEE*. IEEE, pp. 951–955.

Zhang, Yue et al. (2007). “Phinding phish: Evaluating anti-phishing tools”. In: *Proceedings of the 14th annual network and distributed system security symposium (NDSS 2007)*. Vol. 28. Citeseer.

Zhao, Shanyang (2006). “Do Internet users have more social ties? A call for differentiated analyses of Internet use”. In: *Journal of Computer-Mediated Communication* 11.3, pp. 844–862.

Zhu, Qingyi and Chen Cen (2017). “A novel computer virus propagation model under security classification”. In: *Discrete Dynamics in Nature and Society* 2017.

Zhu, Qingyi, Xiaofan Yang, and Jianguo Ren (2012). “Modeling and analysis of the spread of computer virus”. In: *Communications in Nonlinear Science and Numerical Simulation* 17.12, pp. 5117–5124.

Zinn-Justin J. (2002). *Quantum Field Theory and Critical Phenomena*. Oxford University Press, London (UK).

Zou, Cliff Changchun, Weibo Gong, and Don Towsley (2002). “Code red worm propagation modeling and analysis”. In: *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, pp. 138–147.