Son Doan Trung

On Trustworthiness Recommendation

Mathematik und Informatik

Dissertation

FernUniversität in Hagen

On Trustworthiness Recommendation

Son Doan Trung

On Trustworthiness Recommendation

Dissertation

zur Erlangung des akademischen Grades

DOKTOR-INGENIEUR

der Fakultät für

Mathematik und Informatik

der FernUniversität

in Hagen von

Son Doan Trung

Hanoi, Vietnam

Hagen 2017

On Trustworthiness Recommendation

Betreuer :
Prof. Dr.-Ing. habil. Herwig Unger
Gutachter :
1. Prof. Dr.-Ing. habil. Herwig Unger
2. Prof. Dr. Phayung Meesad, KMUTNB Bangkok
Tag der Prűfung:
23rd June 2017

ISBN-nummer: xx-xxx-xxxx-x

Contents

Acknowledgements

The thesis has not been accomplished without undivided supports of a lot of people. First and foremost, I would like to express my gratitude to my 'Doktorvater' (supervisor) Prof. Dr. Herwig Unger, for his guidance, inexhaustible assistance and help to overcomes many hard challenges for myself. Prof. Unger always showed me a way out of puzzling situations, inspire me and gave me hope to reach my goal.

I also have to thank Dr. Mario Kubek for the long discussions with him, his kindness and patience as well as proofreading the thesis. Many thanks Dr. Hauke Coltzau for providing a lot of knowledge on content models as seen in chapter 3 of the thesis as well as fruitful comments and critical questions on presentations. Dr. Panchalee Sukjit always encouraged me in difficult hours and kind-hearted commented my activities. Without the administrative help and support of Werner Schubert, Barbara Kleine and Jutta Düring it would have been much more difficult to work in the unknown, German environment.

In general, it has been a great time to work together with everybody during my time in Hagen. The chair of Communication Networks offers a real inspiring research atmosphere, thanks to its amazing members. I found a lot of friends not only from Germany, but also Thailand, Vietnam and Colombia, who share personal and professional time at University of Hagen with me.

A special thank you is given to the internship student Khuong Ngoc Nguyen, who has been financially supported by a scholarship of the DAAD-IAESTE program. He could effectively programming some major parts for the simulations in this thesis.

Furthermore, I wish to express my profound acknowledge to Ministry of Public Security, People's Security University, Faculty of Security Science and Technology and the financial support from the Commission for Mass Organization, 165 Project of Vietnamese government for four years (2012-2015) in Germany. In addition, I would like to thank University of Hagen for the final support of my Ph.D. thesis for a duration of three months.

Last but not least, without the endless love of my wife Hoa Le Thai and my little son Binh Doan Hoa I could not do my Ph.D. research work. I have to thank them to be my source of strength for a tough period in Germany.

Their spirits will stay with me forever.

Son Doan Trung
Hagen, June 28, 2017

Abstract

Nowadays, people use more and more the Internet and On-line Social Networks as their preferred media for communication as well as business and financial transactions. In particular, the technological progress significantly increases possibilities to interact with people over big distances.

However, any first contacts come along with incalculable risks. Without the physical presence of a partner, the usual six human senses cannot give people a feeling of trust, safety and security. Even over longer periods, on-line partners are hard to evaluate. Therefore, many users look for any non-subjective possibility to get recommendations on trustworthiness of Internet partners for private communication and/or business.

In this thesis, a new model for trustworthiness estimation is introduced. It calculates the trustworthiness of a user by an evaluation of his/her activities with all partners over a longer time. This practice directly corresponds to the human behaviour and psychology and may, therefore, insure a high acceptance among the user community.

Basing on random walks, a decentralised method is derived to combine pairwise, locally kept trustworthiness evaluations into a global trustworthiness value or recommendation on trustworthiness for any participating user. A set of simulations shows the evidence and practicability of the introduced approach.

Furthermore, a decentralised, P2P-based approach for its implementation is suggested, which may be employed in parallel to existing on-line social network platforms like Facebook or Google+. It allows to obtain the wanted trustworthiness recommendation for each participant. Differing from existing implementations, it safely keeps sensitive (since private) data, since they are stored in a distributed, local manner including a fraud as well as a privacy protection and (limited) owner control.

Zusammenfassung

Heutzutage werden das Internet und Online-Soziale-Netze als bevorzugtes Medium für Kommunikation, Geschäftsbeziehungen und finanzielle Transaktionen verwendet. Der technologische Fortschritt erweitert insbesondere die Möglichkeiten zur Interaktion über große Distanzen.

Ein gewisses Risiko stellen jedoch Erstkontakte dar. Durch die fehlende physikalische Präsenz des Gegenübers können die dem Menschen zur Verfügung stehenden sechs Sinne kein Gefühl von Vertrauen und Sicherheit geben. Auch über länger andauernde Kontakte hinweg sind Online-Gesprächspartner schwer einzuschätzen. Aus diesem Grund suchen viele Nutzer nach objektivierbaren Hinweisen und Empfehlungen in Bezug auf Vertrauenswürdigkeit von Online-Gesprächspartnern sowohl im privaten als auch im geschäftlichen Umfeld.

In dieser Arbeit wird ein Modell zur Bewertung der Vertrauenswürdigkeit von Gesprächspartnern in diesem Kontext vorgestellt. Es ermittelt die Vertrauenswürdigkeit eines Nutzers auf Basis seiner Aktivitäten in Bezug auf andere Nutzer über einen längeren Zeitraum. Dieser Ansatz orientiert sich stark am menschlichen Verhalten in der Realwelt und hat dadurch ein hohes Akzeptanzniveau bei den Nutzern.

Durch den Einsatz von Random-Walkern werden vollständig dezentral auf dem Nutzergraphen paarweise Vertrauensbeziehungen evaluiert und in einen globalen Vertrauenswert für jeden einzelnen Nutzer überführt. Die praktische Durchführbarkeit wird an Hand von Simulationen demonstriert.

Weiterhin wird auf Basis dessen ein dezentraler Ansatz zur Implementierung dieses Mechanismus in Form eines Aufsatzes auf bereits bestehende Online-Soziale-Netzwerke wie Facebook oder Google+ vorgeschlagen. Dieser ermöglicht es, die gewünschten Empfehlungen bzw. Vertrauenswerte für jeden Teilnehmer zu ermitteln. Im Gegensatz zu bestehenden Implementierungen werden sensible (private) Daten auf verteilte und damit lokale Art und Weise verwaltet, sodass den Nutzern weiterhin Sicherung der Privatsphäre und (begrenzte) Eignerschaft an diesen Daten garantiert ist.

Chapter 1

Introduction

1.1 Motivation

On-line social networks like Facebook (*facebook.com*), Google Plus (*plus.google.com*) or Twitter (*twitter.com*) rapidly increase the possibilities of people to communicate with each other and exchange information in different forms. They are quite convenient since –compared to the real-world– the user's personal availability (i.e. the need to be at a given time at a well-specified location) becomes less and less important. However, a user is usually overwhelmed with a plenty of information, which need to be filtered following a set of criteria depending on the user's context [1]. Meanwhile, on-line commerce recognises the value of social networks for advertisement and to bring customers and merchants together to find, negotiate and agree on selling contracts.

Since only a few contacts in a social network are people, organisations or companies known from real-world contacts, new problems arise in the area of safety and security (i.e. the degree of resistance to, or protection from, harm). This applies to any vulnerable and valuable asset, such as a home, private items, persons, communities, organisations or even whole nation (cyber-war) [2, 3, 4].

Consequently, an increasing need arises to protect people's health and well-being as well as their goods, money and transactions from any unwanted loss or manipulation, today.

According to [5], progress in computer science mostly secures the technical infrastructure (i.e. computer, networks, data storages from any unwanted activities). The growing effort in research and commercial endeavours for doing so is an evident proof of that.

Nevertheless, the biggest risks to an individual do not arise from the technical infrastructure, but from interferences with the real-world and people in it. Information becoming available in the network may leak sensitive private details (although the user may even not be directly aware of it) and expose his health and property to unpredictable influences.

In most cases, the unpredictability of the real background of activities as well as the goals

of the on-line network users is the reason for that. Also, first alarming signals and behaviours may be easily neglected by the affected users.

In real life, people can process a plenty of information from their environment and their experiences, feelings and care can additionally protect them, in most cases, from any danger. Individuals develop trust for each other (i.e. 'a feeling how high the danger is that the *activities and contents distributed* of the partner may harm its health and well-being' [6, 7, 8]) as a deep in the brain-installed natural, very individual process. Therefore, it is also immediately clear that trust is a very subjective parameter and feeling with personal dynamics in its progress of development [9, 10].

Recently, there is an increasing number of persons on the Internet that –despite the lack of environmental signals and information– make private and business contacts in a fast manner. The high speed of Internet communications puts a high pressure on people to promptly react on incoming messages and makes it impossible to develop the needed confidence and awareness. Consequently, the trustworthiness of a partner (especially of a newly-found one) in an on-line social network is not based on natural trust feelings and may be often and easier than usually manipulated. In addition, quickly established (and manipulable) guest books, customer reviews and evaluations as well as *LIKE* or *+1* buttons are additional means to suggest any (detailed) judgements to the user to change, replace and cheat his (emotional) trust feelings [11, 12].

Despite the existence of those technical endeavours to convince users of the well-behaviour of partners, the common user prefers to rely on the feelings arising from (the usually unconscious interpretation of) all of his 6 human senses. In such a manner, the *word of mouth* [13] and the *wisdom (knowledge) of the (local) crowd* [14] are –so far– still the strongest-influencing factors affecting the human's evaluation of Internet and social network users. More general, reputation concepts (i.e. a public opinion about any entity –e.g. user, company, community, etc.) are typically built as a result of a social evaluation of a set of criteria [15, 16]. In contrast, the concept of trustworthiness accentuates a personal and subjective opinion.

In the case of the web and on-line social networks, reputation (i.e. any opinion regarding a few criteria spread among several members of a community) is the only way to obtain information about the so far unknown character of a partner. Therefore, reputation has often replaced the lack of private knowledge about an intended partner in public and may be also used to be a measure for its trustworthiness [17].

Although innovative results of science and engineering to obtain an objective user evaluation might be a significant marketing factor, there is neither a big support from content providers nor from the user community to develop respective solutions for this purpose.

The author of the thesis argues that users interact via computers and social network application with unknown partners. But no trust feeling exists due to missing presence. Besides, a lot of freely-available information in on-line social networks is not collected and processed in the right manner so far by computer. Since any progress in the described area may boost

the success of on-line businesses and networks in a tremendous manner by supporting decision-making based on trustworthiness recommendation, new approaches in this regards have been developed and will be described in this thesis, which use computers in order to calculate recommendation information from social networks. Hereby, the author is aware that establishing any new, automated trustworthiness estimation needs a long time for general acceptance and wide usage.

1.2 Challenges of Online Social Networks

The characteristics and opportunities of on-line social networks have been recently addressed in a plenty of publications, for some surveys see [4, 11, 18, 19]. Most of those systems are centralised services running on a server or a farm of servers, offering users clients to access information but perform a quite limited set of services [4, 20]. While user interfaces can be different and adapted to the services (like matchmaking, topic-oriented information or interest areas) most of those systems offer as basic operations:

- a target-selective possibility to post information;
- receive information from other users including a few unwanted information upon decision of the system;
- forward this information;
- publish and review profile information of users;
- review the history of posted messages in a kind of 'timeline';
- characterise a set of users as friends and remove them from this list again (and sometimes distinguish good friends from people in different interest circles);
- like or comment content (most systems do not have an unlike possibility yet);
- broadcast, mail or post personal messages including chats in some systems.

Usually, the built friendship network (i.e. the reflection of the real-world social relations of the user outside the computer system) is not to be seen by the single user and obviously a well-protected –since valuable– secret of the on-line social network provider.

Scientists in the area of social network mining have been dealing for a couple of years with the investigation of the information distribution as well as the influence of the underlying friendship network to the dynamics of on-line social networks [18]. Those considerations, which are mostly of theoretic [21] or simulative nature, figured out that:

- the friendship graph has small-world properties [22] showing a high clustering coefficient as well as short average distances between any two nodes;
- the power law is not only a description of the on-line social network structure (Flickr, LiveJournal, Orkut, Youtube) [18] but can also be used to model the intensity of most user activities such as [23, 24, 25, 26, 27]. A rare kind of activities follow a Zipf-distribution [28];
- information distribution can be modelled using physical analogous like diffusion [21] and is strongly influenced by the topological properties of the underlying friendship graph;
- there is a particular dynamic in the evolution of networks.

In on-line social networks, the balance between security and privacy depends on the purpose of that network. Challenges in this case mostly make an effort to impair conflicts in the design of these systems [29, 30].

Guaranteeing privacy in the context of on-line social networks relates to the following different aspects:

- prohibiting the discovery of information identifying user's private data;
- ensuring confidence and anonymity of data. In this case, access control is used to realise a solution;
- prohibiting the linkage of multiple private data of the owner. Therefore, storage and transmission operations of private data must be controllable to avoid both leakages of useful information as well as undesired manipulation on data transmission line.

As a consequence, the following goals can be defined, like protecting:

- identities across multi-systems using an anonymous access;
- personal privacy space;
- communication privacy by hiding location, time and length of connections, messages, physiological parameters, mobile communication information and so on.

Often, users of on-line social networks easily share private (even intimate data) and a large amount of personal and sensitive information with strangers and activities take place with a much lower level of caution and prudence than in reality. In fact, it seems that there is no balance between this open nature of the on-line social network behaviour and the concerns about an increasing privacy and a requirement for special security mechanisms.

Appropriate mechanisms of security and safety are needed to defeat possible vulnerabilities to ensure the security goal (i.e. confidentiality, integrity and availability) of information and resources (CIA Triad) such as:

- authentication and authenticity (i.e. avoiding communication with unauthorised entities in order to protect private and secure sensitive information);
- data integrity (i.e. avoiding manipulation –modification, deletion, addition– of data);
- availability (i.e. ensuring a proper and prompt operation of services);
- accountability (i.e. ensuring the traceability in particular of bad, suspicious, fraud or offending user activities).

In particular, three main security principles can and must be provided in on-line social networks as stated in [31]:

- emphasising and developing the awareness of risk-free activities and relevant content protection based on trust management;
- utilising an efficient access control of the users-generated information flow;
- managing a secure identity control to avoid identity theft attacks from malicious users.

Most systems are designed to keep personal information confidential. As such, interesting information is often not accessible by an automated systems, since the providers protect their systems against an (automated) access of agents, crawling robots or bots [32, 33, 34] and enforce privacy policies accordingly. This makes an estimation of global trustworthiness more difficult.

Nevertheless, there is –for sure– a trade-off between the use of results of data mining on the one hand and keeping the privacy of on-line users on the other hand today. Less privacy results from the wish, more exact conclusions obtain from data mining processes. Obviously, the realisation of both goals is a contradictory wish.

Admittedly, the design of an underlying system as a fully decentralised (i.e. Peer-to-Peer) system may be an approach to get closer to realise the privacy-related goal. The local storage and management grant the possibility of self-protection, complete control of privacy but also a trust-based access control, in case the respective methods are developed. Thereof, the service provider's control of private and sensitive information may be avoided however the user exploration by data mining will be significantly more difficult. Last but not least, confidentiality and integrity of stored data are naturally obtained.

So far, research failed to establish such a fully decentralised approach. The author of the thesis claims that any serious evaluation of users and their activities and contents distributed

must and can be carried out in a peer-to-peer fashion by an independent user-owned entity, which is not involved in the collection and presentation of information by the centralised service providers and cannot be influenced by the participating parties, although it will be transparent to them.

The fundamentals of such a system shall be introduced in the thesis presented.

1.3 Contribution of Thesis

The author argues for the development of his solution that a separate system outside the typically centralised, on-line social network(s) needs to be built to evaluate different user's activities coupled with contents distributed. To acquire a robust and flexible system which is impossible to manipulate, a decentralised solution basing on a peer-to-peer network will be suggested. As already said, such a system will also contribute –due to its decentralised character– to the user data protection and might later replace even the centralised on-line social network systems.

The proposed method offers a newly-developed mechanism for the calculation of a global trustworthiness parameter for every participant of a social network as the result of processing all mutual partner-to-partner activities. In a second step, another approach allows a combination of the network-wide, pairwise trustworthiness parameters by another local, random walker-based method. It evaluates trust depending on the position of the partners in the social network and combines those values accordingly into a single trustworthiness recommendation for each user.

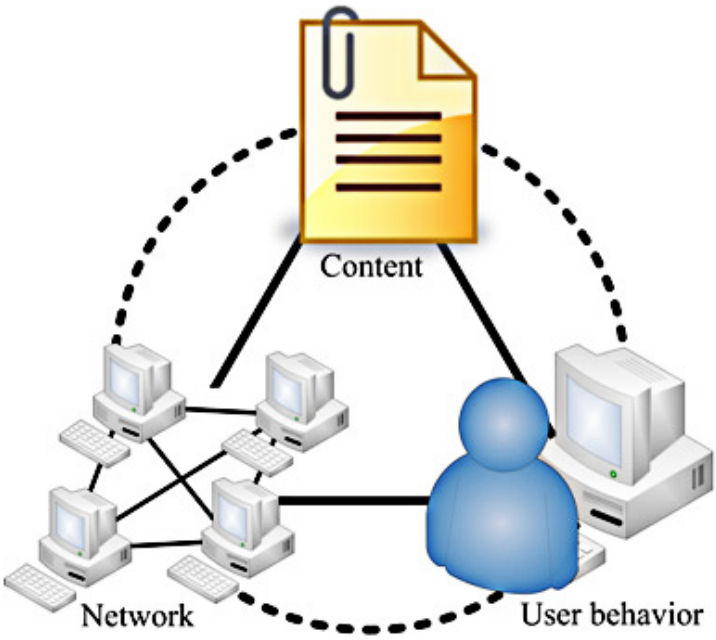

Figure 1.1: Mutual Influences in Service Networks

The intended trustworthiness to a direct user is based on the understanding and modelling of the trust feeling in the human brain, which is usually established between two human parties only by:

- knowing each other for a long time;
- being able to predict the other person's activities together with its-related contents;
- confirming that those activities and contents distributed do not harm the partner.

It is known (see also Figure 1.1) that besides network properties also the contents of any information distributed shall be processed. It will be shown that quantitative evaluations of user activities, content distributed, distribution times, frequencies, receivers, etc. are all together significant sources for the intended evaluation of trustworthiness of a user.

A method will be introduced, which can recognise data in a local manner and on a longer time frame but also shows an 'oblivion' character to adapt to new developments as well as the configuration of trust dependence. Therefore, the author will contribute to the state of the art with the following methods, results and solutions:

- It will be shown that an evaluation of trust towards a partner basing on interactive activities of users in an on-line social network is possible. Besides activities, also contents distributed as well as social interactions are considered. The awareness of how human beings psychologically develop trust is used by including an 'oblivion' process, introducing initial trust, customising trust development and endurance processes following human character traits.
- A fully, decentralised random walker-based method *TrustScore* for a peer-to-peer network will be derived, which can combine trust of all local users to a recommendation on trustworthiness for every participant depending on their activities and contents distributed as well as position in the full, complex connection structure of the network.
- Simulations will demonstrate that the consideration of trust in a social network can have stabilising effects on the topology of the network structure itself.
- A trustworthiness recommendation framework is introduced, which is also protected against fraud and includes a full privacy preservation.

In the suggested implementation, a system architecture will be developed running a separated peer software on every client node of the on-line social network. This software is able to record and control local data and activities and communicate independently with other instances. It will be shown that the bootstrap problem to set up this decentralised system can

be solved by copying and updating the existing friendship relations of the participating nodes from the on-line social network. Of course, the presented approach will work even if not all on-line social network members participate.

1.4 Outline of Thesis

Following the above-described progress to be achieved, the thesis will have the following outline:

Chapter 2: The following chapter will discuss the current state of the art.

Since effects investigated in psychology and sociology have influenced the research in a significant manner, an interdisciplinary review about this topic shall be given first. It is followed by some computer-science related considerations on the evaluation of trust or trustworthiness of direct users, trust propagation and global trustworthiness as well as the needed, fundamentals of complex networks, peer-to-peer and on-line social network systems. Since also content aspects shall be considered, a short review on the needed methods of natural language processing will conclude this chapter.

Due to the interdisciplinary character of the thesis, this literature review allocates a bigger space than usual to explain sociological and psychological backgrounds in a clearer manner.

Chapters 3 and 4: These chapters contain the main, scientific part of the thesis. In particular, the formal background of the new methodology is presented. At first, the human process of gaining trust will be modelled. Cumulated activity factors are introduced among two partners and these increasing and decreasing factors are analysed in a qualitative and quantitative manner. By doing so, different parameters of activities coupled with contents are made combinable on a single scale. In the sequel, exponential 'oblivion' process of human thinking is solved through utilising time window techniques. It makes possibility of dismissing the influence of obsolete, historical activities to cumulated activity factor. Later, it will be shown how this cumulated activity factors can be transferred into a pairwise trust in a real-valued spectrum of $[0, 1]$ via normalisation functions. As a closure part of the chapter, negative activities and their impact on pairwise trust are taken into account.

Subsequently, in chapter 4, a method is presented, to calculate a global trustworthiness value for the participants in a decentralised manner. Therefore, pairwise trust of any two users in the network, originating from their activities and contents distributed, will be processed. For this purpose, the well-known PageRank algorithm [94] is modified into a $TrustScore$ method. It will be shown that this $TrustScore$ calculation can be executed in fully distributed, decentralised P2P system, if a respective interface is implemented. Subsequently, some needed side algorithms and methods like a network-sized estimation are discussed to complete the description of the approach.

Particular specification details and demands will also be derived and discussed here.

Chapter 5: After its introduction, the *TrustScore* method shall be evaluated. Since a mathematical proof is impossible, some simulations with the respective results shall be discussed in this chapter. Furthermore, the author comes up with the hypothesis that trust has manifold influences on the social network, what shall be also considered, simulated and discussed here using the application and effects of the developed trustworthiness evaluations.

Chapter 6: This chapter shall present a possible implementation of the new *TrustScore* approach in the context of (existing) on-line social networks. Several aspects of a possible implementation are discussed. Consequently, the integration of all the described mosaic stones in a single, trustworthiness recommendation framework for existing on-line social networks will be presented, which also supports both fraud-protecting and privacy-preserving criteria.

Chapter 7: At this point, in the final chapter, all relevant results achieved shall be summarised and an outlook on future, possible research works and application perspectives will be given.

It shall be mentioned that most of the presented results have already been published by the author by talks and in the proceedings of international, peer-reviewed scientific conferences (e.g. in [35, 36, 37]). The main contributions of these articles have been investigated and worked out by the author of this thesis.

Chapter 2

State of the Art

2.1 Aspects of Human Interactions

Understanding the basics of human interactions is indeed very helpful for the ability to evaluate other people's intentions, choose a possible answer action and assess their relative pro's and con's for an accurate decision-making. Differing from animals, the human being is –beside its underlying limbic (or animal) character– able to think, plan and make decisions, which results in social behaviour, control and interactions.

Social interactions (Definition 1.) *are dynamic sequences of social actions between two or more people within the human society.*

According to [38], a social action is not only psychological behaviour based on internal physical movements inside an individual but also includes a meaning and a purpose of the action towards the partners and especially expects a respective reactive action. Depending on the replies of an interaction of partners, people can adjust actions in the course and react accordingly. Both, understanding and evaluating actions help people in suitably determining reactions. Consequently, there is diversity in patterns of social interactions. The intertwined patterns of actions and social interactions establish the concept of social relations.

Social relations (Definition 2.) *(also called social ties) are relationships between two individuals in group, organisation, society.*

A complex series of social relations build the social structures, in which the networking possibility is enabled by connecting each unit of groups, organisations or societies to others. More precisely, social relationships are the fundamental elements of the social structure. Social relationships reflect the role of all units in the society as well as maintain it. Friendships, business and financial exchanges are just several examples of social relations.

Social structure (Definition 3.) *consists of individuals and a set of connections among them, which are derived from their social relations.*

There are some primary characteristics, which may be observed in existing social struc-

tures. The activities of their individuals usually ensure that:

- the stability of the structure despite changes in the population is preserved;
- a context in which human interactions occur effectively is constructed;
- the privileges in which each participant is involved are restricted and protected.

One important question related to the properties of social structures of the large off-line social network is: how the structures can be characterised and how an appropriate model can be found? The psychologist Stanley Milgram conducted one of his famous experiments in 1967 [22]. His observation was that there usually exist small average shortest path length as well as clusters in such structures. He attempts to find the average distance between any people in the network and obtained the well-known presence of so-called small-world phenomenon, and later known as the "six degrees of separation" in the human society. The result indicates that any two individuals in the social structure are likely to be connected through short chains of intermediate acquaintances (i.e. chains containing in average six people in-between).

Later on, Watts and Strogatz [39, 40] –inspired from Milgram's ideas– proposed a particular category of small-world networks.

Their model, which is also used in the simulations of this thesis, starts from a construction of a ring lattice with n vertices and k edges per vertex connecting it to its nearest neighbours. Then, the model mechanism allows a re-adjustment of the edges. Therefore, the end point of each edge is randomly rewired with a probability p.

In fact, small-world properties are observed in many real-world phenomena including food chains, electric power grids, networks of brain neural, and last but not least also in on-line, social network friendship graphs. Finding these properties in structures of real systems supports the possibility of modelling real-world processes and computing them within this model.

The knowledge of interactions between individuals and the respective social structure (i.e. context of interaction) shape different patterns of human behaviour. Human behaviour is considered as action and reaction in response to influences of the environment. In a distinctive context, a sequence of behaviours is grouped into different social interaction types, for example in the context of on-line social networks, in term of on-line cooperation, information sharing, revelations of personal information and so on. In this context, behaviours are classified by both the different forms of activities and their related contents, which can be observed, recorded and measured.

The assessment of social interactions and behaviours composes a (mostly hierarchical) structure constraint within the society. The structure is determined by the trust connection and determines how a party can interact with its partners which also affects the question of how

global trustworthiness of individuals in an entire community can be calculated by a method concerning analysis of that complex structure?

The observed structures of human social relationships were assumed from effects of:

- cooperative and non-cooperation (competitive) behaviour in Ostrom [41] and
- trust from human behaviour in Sutcliffe et al. [42]

The computational trust model introduced by Sutcliffe involves:

- Dunbar's distribution of different social relationship layers (viz. strong ties, medium ties, weak ties) in relation to trust;
- social interaction strategy and behaviour processes following Dunbar's 'Social Brain Hypothesis (SBH)'.

The 'Social Brain Hypothesis' is an evolutionary social psychological theory explaining the evolution of human social structure. Different intensity levels of social interaction determine the structures of relationships. Trust –derived from interactions– is considered as a major factor influencing the strength of relationship layers.

- *Strong tie layer:* results in a trust value which is higher than a threshold (i.e. stable point).
- *Medium tie layer:* is a sensitive case with a trust value oscillates between two values. This tie can reduce to a weak tie if –for instance– too many lies are detected. Medium tie may only develop to a higher layer, if a significant, additional social effort is invested in trust gain.
- *Weak tie layer:* is determined, if trust between two individuals is lower than a threshold. Normally, such a trust value is significantly small due to the restriction of social relationship between the individuals.

As an extension of the research in the context of social networks, the influence between social structure characteristics (measured by the two metrics average shortest path length and average clustering coefficient) and social trust will be later investigated in a simulative manner in subsection 5.4.

The above discussed thoughts are the psychological and sociological foundations not only for the terms of trust and trustworthiness, but also for their application in on-line social networks. Consequently, trust and recommendation on trustworthiness as basics for a trust-aware decision-making are briefly discussed in the next subsections of this chapter.

2.2 Psychological and Sociological Aspects of Trust

2.2.1 Fundamentals of Understanding of Trust

In interpersonal communication, humans frequently must intuitively make a decision with who to communicate, interact, cooperate, compete, and for what purpose. From this decision depends on which resources may be used along with which conditions and how long. All these decisions are made in the sense of reliability depending on what humans call *trust*:

Trust (Definition 4.) *is a feeling of how high the danger or risk is that the activities and contents distributed of the partner may harm its health and well-being.*

Note that trust is a feeling generated inside each human in a very individual manner. This process is hard to understand and its modelling seems to be even more difficult. In the human brain, a set of different areas is activated in charge of making a model of mental states of others in terms of trust determination without being consciously aware of it [43].

The trust mechanism in the human brain assists in decision making in uncertainty situations containing some inherent risk in cooperating in organizational relationships with other individuals. However, in a dynamic and complex environment, trust matters exist not only on the individual level [8, 44, 45] but also at team level between different groups (friends, communities, organizations, companies, nations, etc. ...) [46, 47, 48].

In a computer environment these so far not fully understood processes cannot be implemented or used. Instead, a justification or a simple quantitative hint shall be given to a human user, whether a user should trust another individual or not (this will later be called trustworthiness). Remarkably, almost all researchers concentrate on 'trust' itself, but recently, the notion of 'distrust' is a hotly discussed research topic, too. [49, 50, 51, 52, 53].

Since trust is a feeling deep inside each human personality/brain it can be identified only through measurement processes of so-called trust signals.

Trust signals (Definition 5.) *are sets of activities and contents distributed which may be the reason for any concerns of harm or non-harm.*

In general, trust signals can be regarded as information that affect the building, change or destruction of the feeling of trust. The sequence of these signals over time can be helpful to analyse and determine the degree of trust among any two individuals.

2.2.2 Measuring Trust Signals

Two major strategies exist for the determination of trust signals from an individual:

- Exploring rational-choice behaviours [54, 55]. This approach bases on the fact that individuals try to maximise positive feelings and results while undesirable, adverse ones shall be minimised.

That means that positive, friendly or supportive behaviour from a partner is rated as a maximum of positive trust signal of that person and vice versa. One example is behaviour exhibited in behavioural games (e.g. the Prisoner's the organizational Dilemma Game).

- Quantitative physiological measurements. Today's technical progress allows with both hardware and software technology to measure body signals and behaviours which are used in the area of affective computing to detect trust signals.
  Therefore, it is assumed that affective states and physiological conditions not only influence human behaviours but directly correlate to an expression of trust in activities. As a result, measuring differentiated signals of affective states by different technologies enables a determination of current trust signals. Potential sources of such information can typically be:

  - brain activities;
  - psychological response patterns;
  - cognitive and emotional processes;
  - neurochemical processes;
  - social and emotional factors.

  Commonly, the following technologies can be, therefore, applied in affective computing exploitations:

  - electroencephalography (EEG): recording and evaluating the electrical activity in the brain over a period of time;
  - functional near infrared spectroscopy (fNIR or fNIRS): measuring brain activity through thermodynamic responses associated with neuron behaviour;
  - functional magnetic resonance imaging (fMRT): measuring brain activity by detecting changes in blood flow;
  - questionnaire: collecting information from respondents by using a series of questions and other prompts.

  There are a lot of empiric attempts to find a connection between several physiological, physical measurements and trust. In the literature, a plenty of partial results are published.

  - Following neuroscience and neuropsychology of social behaviour, brain activities and psychological response patterns of observed behaviours are measured to find a correlation with trust relationships, for results see [56];

- It was shown that cognitive and emotional states (i.e. frustration, surprise and workload) indicated are correlated to the existence of trust in typical interactions between humans and their computer systems, according to [57]. Thereof, these states were measured by experiments using EEG and fNIRS;
- Several significant results of the research direction give important information on the Limbic System consisting of many cognitive processes involving the amygdala. According to [58] and measurements with fMRT, the amygdala plays a key role in the general evaluation of trust feelings of an individual;
- There is some significance for a relationships between neurochemicals and trust (e.g. the role of oxytocin as "trust hormone" in interpersonal trust and relationship behaviour [59, 60]);
- Following social/emotional approach, [8, 44, 61, 62] identify particularly psychological influences to trust, trust-influencing sociological factors and behaviours predictable by character properties of the individual, and deeply programmed in the limbic system of amygdala;
- Researchers rely on social and emotional signals in order to find correlations between trust feelings and their dynamics through an assessments of answers in a questionnaire. The Big-Five personality traits (i.e. Five Factor Model abbreviated by FFM) is the most famous approach for doing so. It evaluates five dimensions, describing the human personality and psyche (i.e. its openness, conscientiousness, extroversion, agreeableness –including good-natured, cooperative, trustful– and neuroticism). According to [63], basing on values determined for those 5 dimensions, mostly agreeableness positively correlates with the quality of trust relationships;
- It is known that the antecedents of trust to relations are very diverse, hardly identifiable, difficult to quantify but can not be ignored. According to [64], recent research also pays attention to the perception of social and emotional-relevant factors such as stereotypes (gender, prejudices, occupational group, voice, physical appearance ...), rapid judgements or responses to facial features, even smell processes [65];
- Additionally, some research discovered a strong relationship between trust and culture as well as a pattern of socialisation [66, 67].

Unlike living system, biological factors do not exist for explaining trust in technical systems. As a result, be confined in social network systems, the quantitative physiological measurements based on characteristics and interests of the user in the network

–reflecting via indicators of social and emotional information– is dedicated for the main contribution throughout this thesis.

A plenty of further psychological and sociological publications deal with the complex problem of understanding trust [7, 8, 9, 15, 55, 62, 64]. Most papers extend the above given definition of trust in a diverse, broad and complicated manner depending on the concrete researcher, applications or purpose. A few aspects of those trust definitions are given as an overview below. Trust is defined as:

- "... the willingness (or acceptance) of a party to be vulnerable by an actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party ..." by Mayer et al. 1995 [8];
- "... a subjective expectation an agent has about another agents future behaviour based on the history of their encounter ..." in multi-agent systems by Mui [15];
- "... (or –symmetrically– distrust) a particular level of a subjective probability with which an agent will perform a particular action ..." by Gambetta [55];
- "... a willingness to accept vulnerability or risk based on expectations regarding to another person's behaviour ..." by Borum [64];
- "... a commitment to an action based on belief that the future actions of that person will lead to a good outcome and trust ..." in the Semantics Web by Golbeck [68].

So far, in most cases trust problems have been discussed only in the context of the human society. Things may change significantly, if technical systems are used for communication or replace partially human activities. To understand those issues, things must be understood in a deeper manner and formal models must be derived, which can be processed in a computer environment.

2.2.3 User Trust and Technical Systems

The definitions in the previous sections are very diverse, however some common characteristics of trust can be derived from them:

- there is a high ambiguity in the fundamental understanding of trust concepts, and consequently there are multiple definitions of trust;
- distinctions between trust feelings, concepts of trust determination and the perception of trust and trustworthiness are unclear and often not mentioned;

- it is difficult to find consensus in definition of trust and related terms due to different points of view of the researchers and the different affected fields of science (e.g. psychology, sociology, medicine, economy);
- none of the definitions is adequately capable of satisfying all different meanings and context-specific properties of trust for a commonly accepted trust definition;
- the derivation of trust between any two users is a very subjective process of each party which might be represented as quality of relationship with someone else so-called a pairwise trust (PT) value on a given scale. Pairwise trusts each another between two users are called mutual trust (MT). The pairwise trust values are not identical (not symmetric) for any pair of users.

Depending on the application, purpose or personal background of the researcher, different models of trust and its dynamic may be established to describe the process of trust building, change and possibly destruction of trust.

A Trust model (Definition 6.) *is a set of rules aiming at describing the influence of trust signals for evaluation and maintaining trust in relationships among parties as well as methods or algorithms to calculate a quantitative, maybe multi-dimensional, measure for its intensity.*

It is clear that trust depends on the history of the trust feeling for another individual, as well as the history of signals received, which are influenced by the mutual activities and the information exchanged.

Trust evaluation (Definition 7.) *comprises all processes by which a quantitative determination of trust between a pair of parties is derived from their history and trust signals with their history.*

Note again that there is a subjective perception of trust, risk and vulnerability from possible negative consequences of harming behaviours and the decision, whether they are willing to depend on or intend to depend on it. This feeing may be even different in two similar situations (e.g. if only the expected benefit from the cooperation with the partner is changed).

Besides the history of trust and trust signals also the arrival of predicted situations, events or activities may play a role [69]. In this case, even a harming event may be positively evaluated, if it occurs as predicted.

In general, any model must be able to process positive and negative trust signals which may cause an increased or reduced trust feeling. Furthermore, in a particular context, a plethora of trust signals might be available, even within a wide spectrum from negative to positive meanings. In this case, positive and negative trust signals may intertwine and interfere with each other (abnormal case of detection of inconsistency), it is said that the consistency for trust signals is not given or probably ignored. Instead of considering consistency, these contradictory

trust signals result in most cases in a negative evaluation, since the behaviour of the other party is not clear, well-defined or predictable.

It is also important to mention that trust does not depend only on the history and character of the persons participating in any mutual activities. Further influencing factors are:

- ...social and contextual elements of the relationships. The interpretation of the context of the relationship affects trust evaluation. When the context varies, trust needs to be re-evaluated;
- ...the social acceptance of behaviour [70] in the whole (group, community, organisation) (i.e. *contextual norms*). These norms satisfy the expectation of the whole particular system. Contextual norms are comparable to law or ethic discipline in a real society and may differ with country or region on earth;
- ...public opinions (preference and interestingness) vary constantly due to dynamic group building processes in bigger communities. An automated-detection might be required over time but is hard to automatise.

As several times mentioned, trust has dynamic components and depends on history. Figure 2.1 shows the development of an assumed, quantitative and one-dimensional trust representation among any, in the beginning unknown persons over time and definitely demonstrates the cumulative property of that process.

The choice of a S-like shape of the trust curve was motivated by Straker [71]. His works also include the concept of a hysteresis between the curves of gaining and destructing trust, where increasing trust and betrayal or lies, deception follow the different directions in the curves (see also [72, 73]).

It can be seen that the trust value is initialised with a certain value, the so-called initial trust which depends on the subjective properties of a person and its character traits. Trust develops over time in a non-linear manner. Only after some time of positive experiences the given trust to a person is increased until it reaches a stable point (i.e. saturation phase) when the person are fully trusted. In the same manner, betrayal may result in an opposite development as shown by the red curve. Usually, there is a hysteresis between the curves of gaining and destructing trust, caused by the characteristics of human brain to remain in a given status. Note that rough life situations (e.g. significant, hard lies or life-saving activities) may result in an immediate jump of the trust evaluation. In the first time in this thesis, even a lower final level (0) of trust reduction than the given initial trust may be reached.

Basing on trust evaluations in the human brain, decisions about the interaction and cooperation with partners are made.

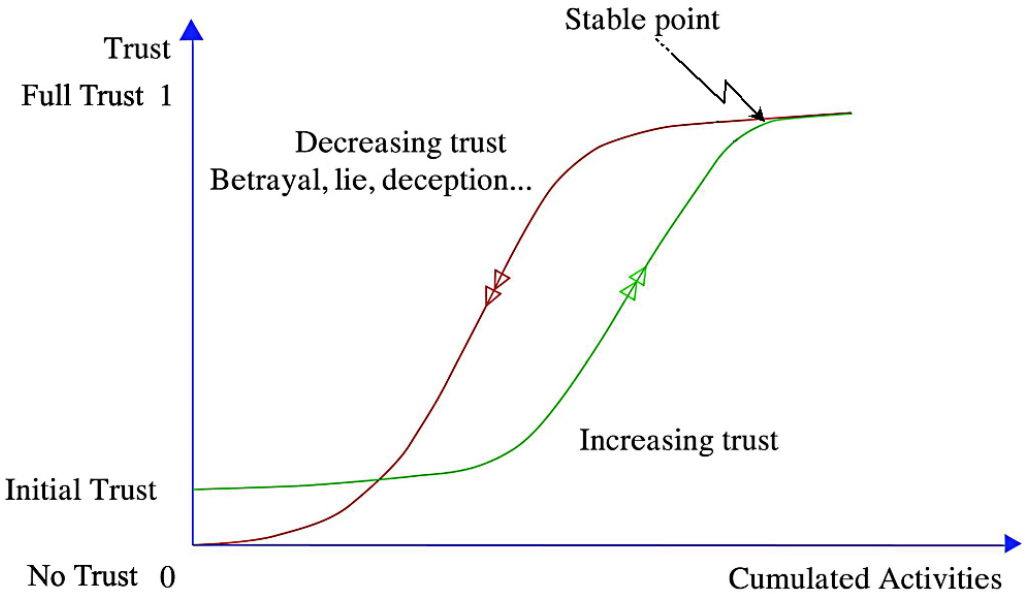

Figure 2.1: Activities-based Utilisation of Trust

A Trust decision (Definition 8.) *expresses the willingness to depend or intend to depend on someone with a feeling of freedom from danger in a specific context even with the possibility of a risk-taking assessment.*

Consequently, trust is important for supporting social control [74] as well as decision making [75], social networking [76, 77], commerce [78] and especially in e-commerce [79, 80, 81, 82].

As above mentioned, trust is a subjective feeling inside the human brain and depends on human behaviour, individual psychological characteristics and the environment. All participating processes are very complex, hard to understand and so far never fully modelled or even projected in an expressible value or string.

As a consequence, it must be understood that trust cannot be given to another human by any rational activity or communication process. All what can be done is the determination and exchange of any experience or recommendation concerning a partner expressed in numbers or vectors. Trustworthiness is considered to represent such characteristic by unique representative value [62]. Basing on Borum definition in [64], trustworthiness definition is derived as following:

Trustworthiness (Definition 9.) *is the degree or quantitative calculation which reflexes the characteristics of the user being trusted. It is derived from the environment in which trust may occur or not.*

Different publications in the literature can be distinguished by the components (i.e. dimensions) used to compose trustworthiness. Appearance of trustworthiness is only when a user willing to trust its partner and confidently believe that partner is reliable and has high dimensions of trustworthiness. In that case, partner has trustworthiness and obtained

value is considered as level of trustworthiness of partner. Level of trustworthiness is not only '... measure of belief in the honesty, fairness and benevolence ...' but may contain more facets. In fact, due to the use of slightly different language by various researchers to describe the components of a perceived trustworthiness, a classification and comparison may be difficult. Several examples are:

- Solomon 1960 [83] -benevolence;
- Larzelere et al. 1980 [84] -benevolence, honesty;
- Kee and Knox 1970 [85] -competence, benevolence;
- Lieberman 1981 [86] -competence, integrity;
- Kasperson et al. 1992 [87] -competence, benevolence, predictability;
- Gabarro 1978 [69] -competence, goodwill, integrity, predictability, openness, carefulness;
- Anderson and Narus 1990 [88] -competence, predictability;
- MacKnight & Chervany [49, 81] has identified four categories of components in trusting belief instead of only three collections –ability, benevolence, integrity– in Mayer et al. 1995 [8]. In the work of MacKnight & Chervany, analysing 65 published definitions of trust indicates that they are categorised within four groups:
    - competence (*competence*[including ability, capability, good judgement], expertness, dynamism),
    - benevolence (*benevolence*, goodwill, responsiveness),
    - integrity (*integrity*[including honesty, sincerity], morality [including goodness], credibility, reliability, dependability)
    - predictability(*predictability*[including consistency], openness, carefulness [including confidences safe], personal attraction)

  Based on highest number of appearance of trustworthiness components in each group as *1)* competence (13%), *2)* benevolence(19%), *3)* integrity (8%) and *4)* predictability (7%) (value-less), a label of each group is selected as a representative component of group. Predictability is less important and can be excluded from these groups. The reason is that the investigation bases on the survey and on the initial trust model, which attempt to examine characteristics of people to be trusted.
  However, in ongoing trust model, actions become the most important factors for the

development of trust. In this respect, predictability along with consistency becomes the most key factors. In a nutshell, MacKnight & Chervany describe a set of major components of trustworthiness (competence, benevolence, integrity, predictability).

Recently, nearly all research works have chosen 3 big predictors of trustworthiness at the broadest level of abstraction [8, 89] as well as [64]:

- *ability,*
  which refers to the perceptions of a partners capability or to accomplish an activity or work and

- *benevolence,*
  which refers to perception and demonstration of altruistic, kind, caring, goodwill, empathic, agreeable, desiring, motivating and operating non-profit work to aid others and

- *integrity*
  which refers to perceptions of honesty, good faith, agreement, not lying, moral and ethical principle, keeping promises.

Trust decisions are thus, not surprisingly, rather trustworthiness decisions. They are basing on maybe fuzzy functions of the perceived fundamental data of the partner, which expresses the characteristics of a person to be trusted in terms of ability, benevolence and integrity. In consequence, psychological, sociological aspects and technological functions, as well as utilities in the context of a social network must be smoothly mingled into trustworthiness parameters (or trust estimations via trustworthiness calculations).

Trustworthiness calculation (Definition 10.) *(analogously: estimation) are calculative processes by which the trustworthiness of users is determined.*

An example for such trustworthiness calculations –i.e. calculating global trust values– is given in *EigenTrust* [90], which only considers either successful or unsuccessful file download information. In general, collecting data for evaluating trust is not easy but the more difficulty to apply any trust-related information in computer systems is that instrumental measurements and additional sensors might not be applied to a common system user. In addition, in the data protection laws of some countries, the collection of sensitive personal information is forbidden or strongly limited. Thus, new innovative methods must be found to collect the needed information from other channels or in an indirect manner (as it has been done for instance via mouse movements for intrusion detection and user identification [91]).

2.2.4 Sources of Trust-related Content

Evaluating trust between a pair of users often relies on different either explicit or implicit signals from social relations. As soon as technical systems are involved, data sources must be established, which may give hints or reasons to a user, why to trust an entity (or not). There are three main sources from interactions in social media to obtain trust:

- Explicit source
  Trust is derived from explicit data –emphasising on feedback as a source of trust– which are provided intentionally rather than analysed or interpreted for further meaning.
  Feedbacks from commercial transactions in the past about the different qualities of the seller are available on-line on Ebay, Amazon are examples. Furthermore, in Web of Trust in [92] a third party relies on explicit rating-based trust information. On *Advogato*, judgements on other users basing on a three-level certification may be made (i.e. master, journeyer and apprentice). The scale of 10 distinct levels is used in a website offering an evaluation of the hospitality of homestay (*couchsurfing.com*). The taxi-system Uber (*uber.com*) allows taking rider feedback very seriously from 1 to 5 stars. Grab (*grab.com*) identifies low or 5 star performing drivers by evaluating feedback about drivers and service on different aspects such as punctuality, smile, attitude of driver (polite, cautious and courteous), state of car (clean, comfortable and pleasant) and reminding to rate for service. Last but not least, guestbooks on most commercial webpages give the possibility to express feedback opinions by text contributions.
  However, the approach based on feedback incurs a lot of deficiency as descriptive seven reasons below:

  - losing multi-facets of trust. In the feedback approach, both histories of interactions and the context are not considered. Feedback-based trust only reflexes a snapshot of mind at the time when users giving feedbacks. With this respect, the generation of feedback-based trust is not reasonable and similar to the construction of interpersonal trust;
  - being inconvenient for providing ratings after having experience (e.g. only 60.7% of the buyers and only 51.7% sellers on eBay rating about each other [17]);
  - lacking considerations on feedback credibility. For instance, the Pollyanna effect (i.e. a bias toward positive rating (see [15])) indicates that almost all feedbacks refer to a positive outcome and rarely to a negative one. According to statistics from [17], empirical buyer-giving ratings on eBay's reputation

system indicates that 0.6% is negative; less than 0.5% is neutral, but approximately 99% is positive. Also the eBay's sellers gave only 1.6% negative rating to the buyers;

- being unsuitable for support of constructing automated trust systems since the supply of feedbacks is mandatory;
- supporting various potential attacks such as Sybil attack, on-off attack, independent bad-mouthing attack, collaborative bad-mouthing attacks, and conflict behaviour attack [93];
- also having the possibility that complex, differentiated feedback cannot be given like in Facebook, Google Plus or Twitter. In fact, reactions exist here only in textual replies or reviews, comments and a simple form of 'like' button. It has been proved that such 'simple' activities with advantage of enormous volume of it within an entire on-line community will contribute more meaning than explicit feedbacks, but normally only positive and not differentiated feedback is provided;
- a lower amount of feedback is collected in comparison with a direct interaction and behaviour approach. For instant, following source of Facebook as of 10th Feb 2014, the like and share buttons are viewed and used across almost 10 million websites per day, while up to 4.75 billion pieces of content shared daily as investigation statistics in May of 2013. The drawback of a limited data volume is that it is the main reason leading to scarcity problem. As a result, computational trust methods based on propagation obtains a deterioration in the accuracy.

- Implicit source

  In this case, trust is derived from behaviour and personal experience analysis of users. Relevant features are established to determine how much trust is expressed by inference of user's activities and textual contents concern.

  There are several typical examples from different contexts which are of relevance. On Peer-to-Peer systems, trust evaluations also may considered provided poisoned or faked files as well as the availability of peers or the number of files for download. As an example, successful downloads in a P2P network are analysed in [90]. PageRank [94] relies on the vast of links as an indicator of trust. The endorsements and connections in LinkedIn (*linkedIn.com*) for discovering potentially interesting business partners and a number of re-tweets in Twitter could are considered in other works.

  In addition, the users could be evaluated by bookmarking interesting URLs (*del.icio.us*), posts and comments on new stories on science and technology (*slashdot.org*), visible

songs to listen (*last.fm*), sharing videos, photos, messages and comments via profiles and networks (*friendster.com*), comments on uploaded photos by other users (*flickr.com*), adding other users as friends for viewing public events (*rsscalendar.com*) as stated in [11]. Trust-related activities in (*instagram.com*) are likes and comments on posts in form of photos or videos that is posted by user or friends are liking and commenting on it. Some researchers, for instants, [95, 96], utilise human perceptions such as stereotypes for the potential of assessing trust.

- Hybrid source
  Trust can be also derived from combining both explicit and implicit source of data (i.e. combine several information sources using intelligent algorithms).
  Amazon.com uses an explicit rating whenever possible and user's historical activities of purchase in the case of unavailable explicit ratings. In *youtube.com*, not only explicit ratings for partner's videos posted but also information about subscribers, uploads, comments, adding to favourites are treated [97]. *Epinion.com* possibly supports not only interesting product reviews, the number of reading reviews, inserting users into block list but also a numeric review ratings from 1 to 5. In *airbnb.com*, along with textual reviews, an overall star rating and a set of star rating following different categories (i.e. overall experience, cleanliness, accuracy, value, communication, arrival, location) could be submitted by guests.

Finally, it must be concluded that there are a lot of reasons for supporting the use of implicit sources and a lot of models of trust are based on different kind of trust signals derived from this approach (i.e. derive trust implicitly from interactions and behaviour [98]). There are several supportive arguments:

1. In reference to *Theory of Reasoned Action* (TRA) in [99], behavioural beliefs and intentions lead to related behaviours. Therefore, actual behaviours are required to be understood and exploited for evaluating trust.

2. The derivation of trust from behaviours is affirmed by various application contexts presented in prior researches, for instances, work collaboration and social communications [7, 8], e-banking and e-commerce [100], automation and intelligent machine [101], mobile application [102, 103] as mentioned in [102].

3. Most researchers in the social network context have criticised the direct feedback approach, see above.

4. Textual contents, referring to the trust definition of Rotter [62]: "... a long time ago an expectancy held by an individual or a group that word, promise, verbal or written

statement of another individual or group can be relied upon ..." would give a great value to trust evaluation.
These contents make one vulnerable from harm with the utilisation of this information. Thus, textual contents and its characteristics assist in deciding if relying on another one or not. For example, Touhid et al. [104] mentioned that text written in natural language as comments could be used to determine trust-relating human opinions. In a nutshell, the precision of an evaluation of user's activities can be increased by evaluating also texts/contents distributed, which are made publicly available.

5. The importance of activities to trust development in the context of on-line social networks is confirmed by Grabner-Kräuter et al. [76, 77].
Trust is established stably primarily based on interactions upon interpersonal trust communication. Trusted relationships are mostly based on the indicator of the observed communication behaviours, the prediction of processes from historic experiences and the interaction frequency with other community members in the past.

6. Research works related to behaviour in social networks have recently obtained several exciting results, but are still limited regarding the kind of interactions and social relations. Examples are YouToBe [97], the exchange of personal messages in Facebook [105], quantifiable measures of observed communication behaviour using Twitter data [106] or the use of the Boltzmann-like mathematical model in [107] and game theoretic models in [108].
Several articles showed a positive correlation between trust and interactive activities on an on-line system based on presented classifications and prototypical examples [11] or only suggested a model to characterise user behaviour (publicly visible activities and around 90% in hardly identifiable or unmeasurable form of silent activities) and differentiated activities in different classes (search, scrapbook, message, testimonial, videos, photos, profiles and friends, communities and others) across multiple on-line social networks sites in [109].
It could be declared that there is absolutely no trust models based on activities and content distributed in the on-line social networks Google Plus and Facebook.

Considering the above cited and classified works, it becomes clear that a recommendation on trustworthiness is needed in the near future, which evaluates trust while considering both activities and contents of interactions in on-line social networks. For doing so, it must be investigated, how trust signals can be derived from these sources? Respective models must be developed.

2.3 Modelling Interaction Processes

2.3.1 Graph Models

The most helpful models to understand the described trust problems within the context of computer science and systems are basing on graphs. Such a network representation of real-world as well as computer systems and relations is useful to understand basic principles and functions as well as to do analyses.

In graph theory, a network is as graph $G = (V, E, W)$, which is defined by a set of nodes (i.e. actor, agent) $V = u_1, u_2...u_n$ where n is the number of nodes in the network and $E \subseteq V \times V$ a set of edges (i.e. arcs, links) $\{u_x, u_y\}$ and $x \neq y$ with a corresponding weight $w(u_x, u_y) \in W$. The weight of an edge usually represents the importance of that edge or describes the intensity of any mutual property. Edges might be directed or undirected according to the uni- or bidirectional character of the underlying relation. Additionally, the neighbourhood of node u_x in a directed network is defined by two types:

- Predecessors (In-nodes): i.e. all nodes at the end of incoming edges or the set of nodes pointing to node u_x: $N^{-}_{(u_x)} = \{u_y \in V | \{u_y, u_x\} \in E\}$.
- Successors (Out-nodes): i.e. nodes which can be reached by outgoing egdes or the set of nodes that node u_x points to: $N^{+}_{(u_x)} = \{u_y \in V | \{u_x, u_y\} \in E\}$.

With these few and simple settings, trust-related problems can be modelled. This will be discussed in the following subsection.

2.3.2 Trust Propagation

Internet and On-line social networks work only because trust implicitly exists between users involved each other. When users are networked, an initial problem of trust in networks is the question of trust propagation. Assume a user A knows another user B and evaluates trustworthiness of direct user B. User B may know another user C and have another trustworthiness evaluation for direct user C. Is it possible to calculate a (indirect) trustworthiness or a recommendation on trustworthiness that user A shall accept about C?

From the complex nature of trust becomes clear that any of such evaluation can only be a very rough approximation. To answer the question and to handle trust topics in the network context, two main principles in computational trust are needed:

- propagation
- aggregation (being similar the concept of an open composition function in [110] and also mentioned in [92])

Trust propagation is originated from several prior works. AbdulRahman et al. [111] proposed a trust model based on Web of Trust [112] and under the assumption that trust can be transitive among inter-connected users. The trust propagation mechanism is inspired from a transition of trust along observed friendship chains in the sociological context of the human society.

In the 'Balance Theory of Heider' [113], transitivity characteristics in a social network are explained based on the tendency that 'a friend wants to interact (rather) with a friend than unknown people'. Propagation of trust is similar to processes of passing information between intermediary users in 'word-of-mouth' [13].

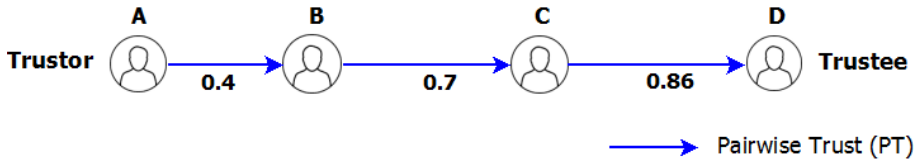

Figure 2.2: Sample Single Trust Chain

In Figure 2.2, the A has its local neighbour B (direct trust relation) but has no adequate information to make any decision about its relation to D, who is unknown (i.e. indirect trust relation) to A. However, trustor A can collect not only direct trust to neighbour B but also B's recommendations on trustworthiness about the intermediate partner C. C itself has an evaluation about the trustworthiness of direct partner D. In such manner, A may find a decision how trustworthy D might be for him above the initial trust A may give in every case to D. This decision sequence –presented by (ABCD)– is a so-called trust chain. As a result, trust propagates from A to D following chain (ABCD). The concept of trust propagation appears to help A in calculating how much trust A imposes on D.

A Trust chain (Definition 11.) *is a path connecting the neighbours of neighbours from trustor to trustee in trust network, whereby each have an evaluation about the trustworthiness of its direct neighbour.*

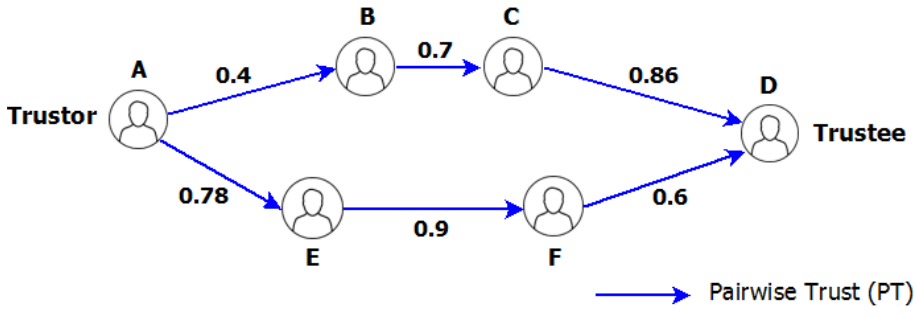

Figure 2.3: Sample Multiple Trust Chains

In fact, usually there is not only one single trust chain from trustor A to trustee D as in Figure 2.3. Trustworthiness of D is calculated concurrently from two or more independent

chains (ABCD) and (AEFD).

Usually, trust calculation on a simple trust chain could use elementary functions such as Min or Multiplication:

- Min strategy: trust following a chain is defined as minimal trust value among set of edges on that chain
- Multiplication strategy: trust following a chain is defined by multiplying trust values of all edges on that chain

In the case of multi-chains, another important concept of trust, namely the aggregation, needs to be defined. The process of estimating trustee's trust consists of:

- handling each separated single trust chain in order to calculate trust following each separated chain in the first phase and
- merging the results of all possible trust chains calculation for an unique personalised trust value by an aggregation function in the second phase.

The use of a (weighted) average- or max function of values calculated following each chain are examples for usable aggregating functions:

- Average function: calculate the average value of all trust from multi-chains
- Max function: calculate maximal value of all trust from multi-chains

Below, some examples to count the aggregating trust from a multi-chain system are given in Figure 2.3:

- *Min Calculation Strategy:*
  - *Chain (ABCD):* $t_{(ABCD)} = min(t_{A,B}, t_{B,C}, t_{C,D}) = 0.4$
  - *Chain (AEFD):* $t_{(AEFD)} = min(t_{A,E}, t_{E,F}, t_{F,D}) = 0.6$
  - *Aggregating trust by Average function:* $t_{A,D} = \frac{1}{2}(t_{(ABCD)} + t_{(AEFD)}) = 0.5$
  - *Aggregating trust by Max function:* $t_{A,D} = max(t_{(ABCD)};\ t_{(AEFD)}) = 0.6$
- *Multiplication Calculation Strategy:*
  - *Chain (ABCD):* $t_{(ABCD)} = t_{A,B} \times t_{B,C} \times t_{C,D} = 0.24$
  - *Chain (AEFD):* $t_{(AEFD)} = t_{A,E} \times t_{E,F} \times t_{F,D} = 0.234$
  - *Aggregating trust by Average function:* $t_{A,D} = \frac{1}{2}(t_{(ABCD)} + t_{(AEFD)}) = 0.237$
  - *Aggregating trust by Max function:* $t_{A,D} = max(t_{(ABCD)};\ t_{(AEFD)}) = 0.24$

More complex strategies improving trust propagation in a path are presented in [114], including a weight of a path (calculation of trust following chains is influenced by the length of the path and therefore number of partners on that path) and a decay rate (the trust value of any edge in a path is reduced depending on how far that edge is away from trustor).

TidalTrust algorithm [92] is processed in two computational stages:

- Paths Search Stage: searching all paths from the trustor to the trustee, simultaneously labelling the nodes on these paths and finally, determining a threshold MAX, if needed. A threshold MAX may assist in filtering out redundant nodes with a low labelling in calculation of the next stage.

    - Labelling for nodes, forward from the trustor to the trustee:
      (a) labelling of one predecessor y to node x is minimum between y's labelling and trust of y towards to node x. Note that trustor is labelled with positive infinity.
      (b) labelling of node x which has more than one predecessor. That is the maximum of the labellings these predecessors gave to x.
    - Determining MAX:
      (c) eventually, MAX is the maximum of labelling of predecessors of trustee. From the Figure 2.4, MAX is $max(0.4, 0.5) = 0.5$.

- Trust Aggregation Stage: aggregating trust, backwards towards the trustor in order to return the final value to trustee. This process calculates trust from u to v, follows recursive processes by the expression as below:

$$t_{u,v} = \frac{\sum\limits_{x \in N^+_{(u)} | t_{u,x} \geq MAX} t_{u,x} t_{x,v}}{\sum\limits_{x \in N^+_{(u)} | t_{u,x} \geq MAX} t_{u,x}}, \tag{2.1}$$

  where $N^+_{(u)}$ is set of successors of node u. The threshold MAX indicates that node x is trustable only in case if $t_{u,x} \geq MAX$. The following sequential equations illustrate this process for calculating t_{AD} in Figure 2.4:

    - *Step 1:* $t_{B,D} = \frac{t_{B,C} \times t_{C,D}}{t_{B,C}} = 0.86$
    - *Step 2:* $t_{E,D} = \frac{t_{E,F} \times t_{F,D}}{t_{E,F}} = 0.6$
    - *Step 3:* $t_{A,D} = \frac{t_{A,E} \times t_{E,D}}{t_{A,E}} = 0.6$. Notably, trust chain $(ABCD)$ does not involve to calculate t_{AD} because of $t_{AB} < MAX$. In this case, nodes B, C are filtered out.

In the result, of the above described method, an trust value aggregated from various trust chains will be obtained.

There are two overall types of distinguishable computational trust models, which base on different ways to aggregate trust from various trust chains. They consist of the following types of trust metrics:

- local trust metrics
- global trust metrics

Local trust metrics are the above cited examples like Min, Multiplication strategy and TidalTrust algorithm as well as MoleTrust [115], AppleSeed [116] which defining trust along chains of personalised trust, one user has imposed on another user in its indirect neighbourhood.

These metrics allow the aggregation of trust considering all single trust chains from trustor and trustee. The implication of local trust is reasonable to assume that different users are expected to have a different estimation about the target trustee.

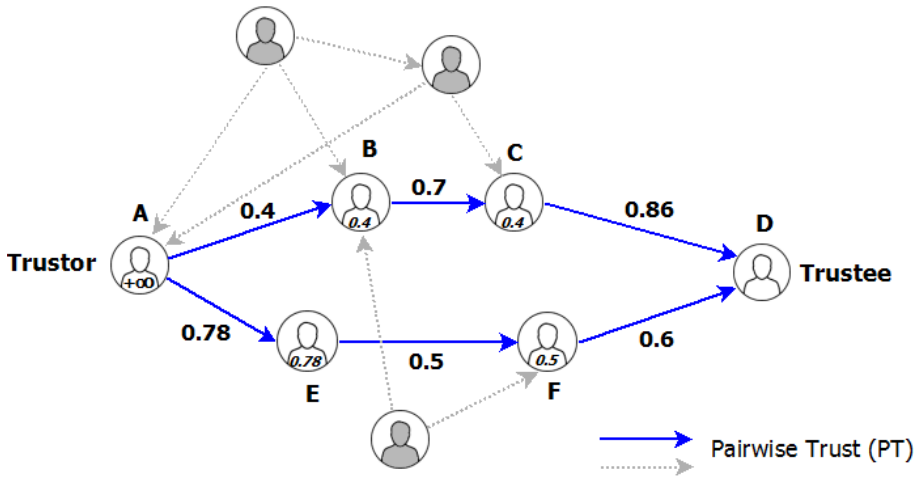

Figure 2.4: Calculation of t_{AD} in TidalTrust

Local trust metrics are diverse but have the following typical characteristics:

- chains in a network are usually short, because networks exhibit the small-world property;
- in order to apply those metrics, trust data must be available within the network at least to nodes along trust chains;
- according to [16], networks may be created from recommendation processes of nodes via communication protocols;

- only a small subset of nodes is utilised for particular calculation processes. With respect to this, the complexity of network-building problem is tackled. That is why local trust scales well to a big-sized systems because only a relatively small subset of the network is considered.
  As an illustrative example in Figure 2.4, all grey-coloured users are not involved in t_{AD}-calculating processes of the TidalTrust algorithm.

- regarding good and bad behaviours (i.e. positive or negative trust signals from interactions) which are *universally* accepted by all nodes, global trust metrics are usually utilised in order to calculate global trust value for each user as mentioned in [117]. Local trust metrics are only appropriate when emphasising personalised trust of user.

In contrast to local methods, global trust metrics define trust knowing the whole network (viz. considering all relationships in complex structures) instead of small parts of the whole structure, only.

Trust chains in global scale (Definition 12.) *contain all possible paths between all arbitrary pairs of users in trust network.*

One typical global trust metric utilises PageRank [94]. In this metric, implication of trust propagation or mutually trust influence in its entirety is necessary for calculating global trust value as Figure 2.5. In reference to [16], global trust values could be synthesised from all possible trust chains in a (complex) whole. In the case of utilising PageRank, a central authority is needed (i.e. server) for being able to manage the whole immense trust relationships and their computation.

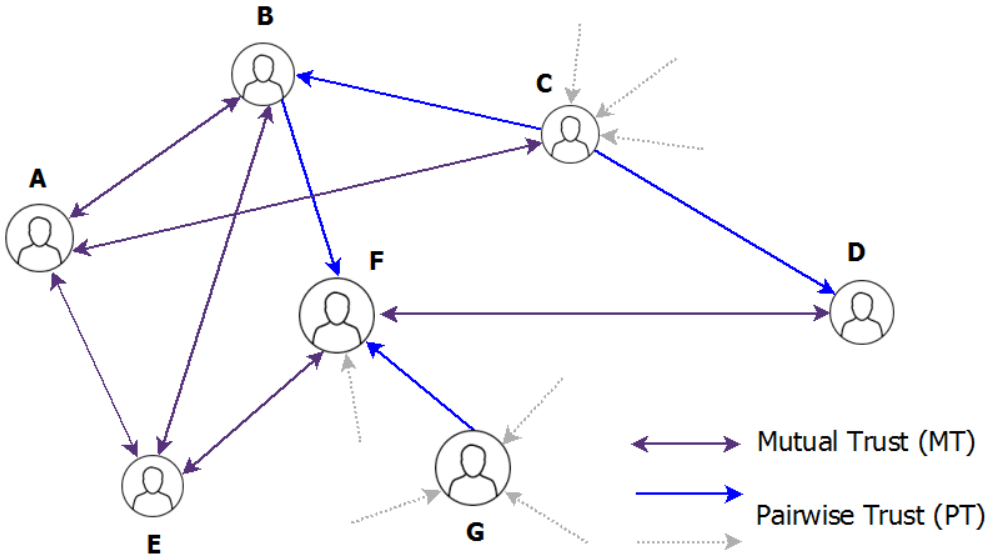

Figure 2.5: Sample Partial Trust Network

Centralised global trust computation on central authority is not feasible in several distributed systems because of the need of servers. It is synonymous with the mission of a single

trusted server that computes global values for all individuals. Furthermore, global trust values are disseminated to all requesting entities. Therefore, the existence of global/centralised servers decrease the privacy of each entity and the autonomy of the system in case of failures.

Originally conceived to solve these problems, in a variant of the PageRank method by Sodsee [118], a distributed metric using random walkers is applied. Propagation mechanism of trust is considered as that it resembles a random walk over the trust network [119]. That metric has distributed computation of trust aggregation function, which operates across the whole networks and considers mutual influence in global scale contrast to most previous works that concentrate on centralised propagation and must depend on trust chains. In other words, the global algorithm running on a single trusted server could be transformed into a decentralised, locally working algorithm as already indicated in the original publication of Page and Brin [94]. The author intends to use this idea as a part of its new method to calculate global trustworthiness or –namely– recommendation on trustworthiness in a decentralised network. That value is influenced by weights of all connections in complex network structure. It is expected to be used to give a human-like prediction of what might to be from characteristic of a user.

2.3.3 Quantitative Modelling of Processes

Since the suggested methodology may only be evaluated by simulations, some more useful laws shall be discussed in the modelling section in order to understand and realise proper simulation and experimental settings.

The existence of those laws is a natural phenomenon of various social systems that reflect the core characteristics of the society in general and also ensure the stability of social systems.

Laws in social systems provide a measure for global characterisation of different kinds of data and activities. The quantitative-qualitative strategies in real-world social systems were confirmed by power-law, *Richardson* law and the concept of strong and weak ties.

a. Power Law

The original observation in many social networks points out a typical degree distributions of nodes following the *power-law degree distribution*. The definition of a power law will be:

$$P(k) \approx Ck^{-\gamma}, \tag{2.2}$$

where $C = e^c$ is a constant and $\gamma > 0$ is called the power-law coefficient. $P(k)$ is the *degree distribution* (i.e. probability that a number of nodes having a degree of k in the network). Later it has been observed, that the distribution of user activities and contents also follows a power law distribution.

Empirical studies have shown that $2 < \gamma < 3$ as mentioned in [120]. For an exam-

ple, user behaviour in simulations of social network systems is modelled through the validity of power law distribution of user activities derived from collective questionnaires. According to [23], the questionnaires were given out to college students of Bangkok. The survey aims at determining user behaviour in on-line social networks, particularly Facebook. 1,200 questionnaire were issued, while only 1,173 valid questionnaires were obtained. The final purpose of this work defines behavioural rules, which influence the evolution of on-line social networks. The primary results of empirical measurements showed that activities data about playing on-line games, profile updates, posting/tagging/browsing, visiting link/pages, buy/sell/merchandise adhere to the power-law distribution. Partial results are revealed in log-log plots as in Figure 2.6. More power-law applications can be found in a number of daily user activities (e.g. in Facebook and its connected applications [24] or in the consideration of times and numbers of re-tweets in the Twitter network [25]).
Topologies and the dynamics of the processes of an artificial social network in simulations can now be generated automatically using this law, since –due to technical restrictions– real data cannot be obtained from social network sites such as Google Plus and Facebook.

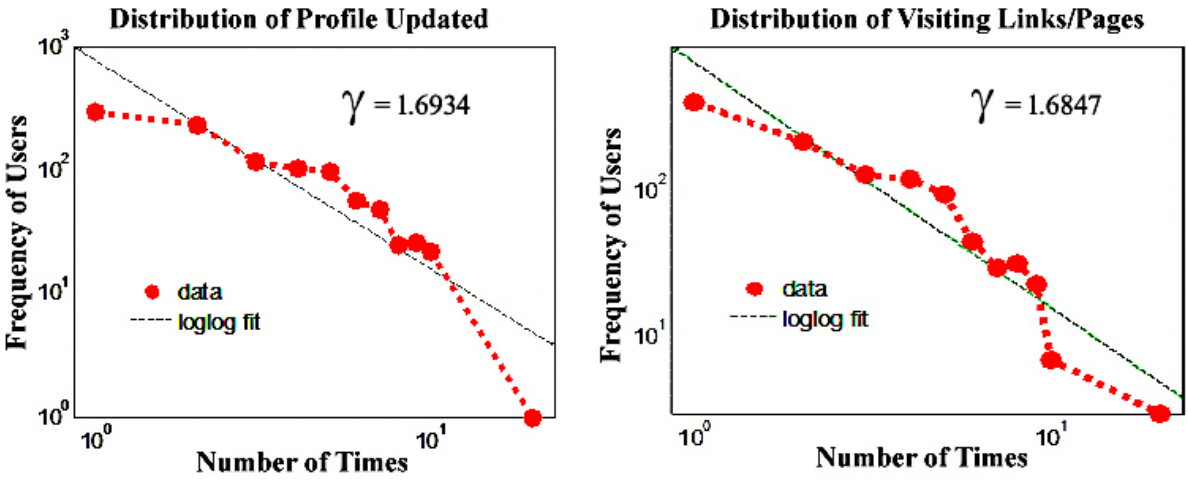

Figure 2.6: Power Law-Exhibiting Results (Profile Update and Visiting Links/Pages)

b. Richardson Law

It was mentioned before that trust is hard to analyse as well as to measure. However, *Richardson* law [110] explores typical distributions of trust values and could therefore be used to generate the respective information in a network in order to have initial simulation data.
In other words, *Richardson et al.* uses law in order to assign trust between two users u_x and u_y. Thereof, the assignment of trust u_x imposed on u_y concerns two parameters:

the quality of the user α_{u_x} and a noise $\beta_{u_x u_y}$. The parameter α_{u_x} is the quality of user u_x and ranges from 0 to 1, determining the probability for the trustworthiness to direct user u_y. The parameter follows a Gaussian distribution with the mean value $\mu = 0.5$ and a standard deviation with $\delta = 0.25$ as selected in [110]. The parameter $\beta_{u_x u_y}$ determines the accuracy of the user u_x in estimating the quality of the user u_y, who is trusted. The assignment of trust was chosen randomly in an interval of $[max((\alpha_{u_x} - \beta_{u_x u_y}), 0);\ min((\alpha_{u_x} + \beta_{u_x u_y}), 1)]$ in the simulation setting of this thesis.

c. Strong and Weak Ties

Strong and weak ties have already been introduced in the section on interactions and has been studied in works of Granovetter in psychology [121] for the first time.
Afterwards, the principle was applied to social networks in the studies of Kleinberg's work [21]. Kleinberg declares in his works that *"... If two people in a social network have a friend in common, then there is an increased likelihood that they will become friends themselves at some point in the future..."*. Additionally, depending on the strength of ties, social relationships (i.e. weak tie and strong tie) can be characterised in a quantitative manner.
The strength of ties is a critical property for the topological evolution of networks as it will be discussed in the next section. At this point, it shall be figured out –for the first time– that the network evolution is connected with trust aspects, since friendship and trust are connected.

Not only quantitative-qualitative strategies characterise social systems, but also the underlying structure, exhibiting the so-called small-world property. Aspects of this property will be discussed in the subsequent subsection.

2.4 Analysing Networks

2.4.1 The Small-World Effect

Many networks –built and used in the context of this work– are so-called small-world networks. Networks with this property exhibit a significant low shortest path length as well as a high clustering coefficient.

a. Shortest Path Length

The length of a path connecting u_x and u_y $d(u_x, u_y)$ is defined as the number of traversed edges on this path. Usually, there are a lot of paths between u_x and u_y in a network but merely one path has the minimal length of all paths, that is the *shortest path* $d_{min}(u_x, u_y)$.

Moreover, the *diameter* of a graph is the longest shortest path between all pairs of nodes connected. A small-world network exhibits a low diameter [22].
In social network analysis, the shortest path length is used in some algorithms for computing betweenness and closeness centrality [122], for further discussion see subsection 2.4.2. There are many algorithms computing shortest path length such as Dijkstra's algorithm -$O(m + nlogn)$, Bellman-Ford algorithm -$O(mn)$, Coppersmith-Winograd algorithm -$O(n^{2.376})$. These algorithms only compute shortest path from a single source to others. In this thesis, Floyd Warshall algorithm [123] is used to calculate all pairs shortest paths in the network for a convenience of calculation purpose.

b. Clustering Coefficient

Another basic characterization of a node in a network can be obtained by describing the structure of its local neighbourhood to capture the inherent tendency to have a cluster, represented by an almost complete sub-graph. Observation in the context of social network shows due to the use of ties and Kleinberg's triadic closure relation a tendency to build such clusters. The *local clustering coefficient* for node u_x $c(u_x)$ is a

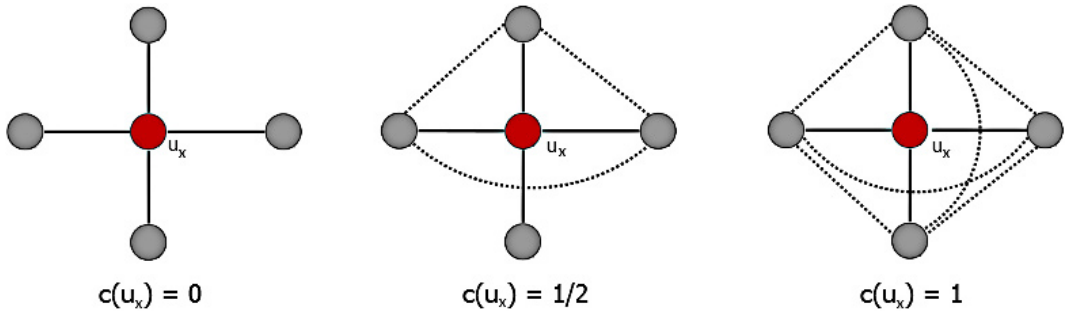

Figure 2.7: Examples of Clustering Coefficient

measure of how strong the clustering property is developed and defined in [21]:

$$c(u_x) = \frac{number\ of\ actual\ edges\ between\ u'_x s\ neighbors}{number\ of\ possible\ edges\ between\ u'_x s\ neighbors}. \tag{2.3}$$

A generalisation of the local cluster coefficient for the whole network can be obtained by building the mean value of all local clustering coefficients of all nodes, namely *average clustering coefficient*:

$$C = \frac{\sum_{i=1}^{n} c(u_x)}{n}, \tag{2.4}$$

where $\forall u_x \in V$.
Clustering coefficients reflect group cohesion around an important member and are extremely valuable for trust-building strategies. It helps to measure trust of a user at a local scale and level of trust in the whole network. In small-world networks, the clustering coefficient is typically higher than in common graphs.

c. Applied Small-World Phenomenon
Complex systems usually unveil valuable information via their underlying structural principles.
According to the article of Capkun et al. [124], small-world properties are built in the result of mutual trust relationships between people in a self-organised system. The implication of self-organization in the article is that the system operates solely by participating end-users.
The publication of Gray et al. in [125] showed that a small-world tendency is exhibited in self-organising networks of users (PGP system or mobile Ad-hoc networks).
Justified by those findings, topologies can be yielded via Watts and Strogatz small-world model [39]. This has been done in the herein conducted experiments in order to reflect real-world structures for testing hypothesis, since topologies of existing on-line social networks cannot be obtained, neither by external crawls nor from providers directly.

In this subsection, two fundamental properties of the small-world effect were elucidated. It was worked out that small-world networks appear as results of many interaction processes in the society. Important knowledge can be obtained, if the properties of those are examined. An overview of important aspects of investigated social network structures will be given in next part.

2.4.2 Social Network Analysis

Social Network Analysis involves the structure of social networks. Therefore, the characteristics of the underlying social network graphs, their properties and especially their connectivity are investigated. While studying social network graphs, major attention is given to:

- node-based analysis,
  which utilises centrality measures, basing for instance on PageRank [94] and HITS [126] in order to study the position and the role of the node in the social network.

- structure-based analysis,
  which employs link prediction algorithms [127] and studies the network evolution [128, 129]. The goal is to explore communication possibilities offered through the connection between nodes as well as to derive rules for structural developments of a network (i.e. its dynamic) over the time.

- community detection-based analysis,
  using clustering algorithms [130, 133] in order to identify groups of users/nodes, with a high connectivity and therefore usually strong interactions. Therefore, usually cluster or community identification algorithms are used.

In this subsection, some literature on the most common centrality measures and an overview of clustering and community identification algorithm is given and discussed. Later, content related aspects will be presented which also have some significant effects on trustworthiness and user activities. A few aspects of structure evolutions will be presented, too.

a. Centrality measures

User centrality determines the role and position of the user in the network. There are three different basic centrality measures: degree centrality, closeness centrality and betweenness centrality, which were introduced by Freeman [131].

- degree centrality: counts the number of adjacent edges. It is used to measure the immediate risk or influence of a user in social network and its capacity for information broadcasting.
- closeness centrality: counts the sum of the length of the shortest paths connecting a given user with all other users in the network. It is useful for information diffusion and reception.
- betweenness centrality: indicates the frequency of shortest paths passing via a given user in the network.

In contrast to degree and closeness centralities, betweenness metric refers to the user ability and importance to facilitate information flow in the network. A node with high betweenness centrality exhibits a high ability to connect different communities within the network. Trustworthiness of a user may vary and depend on centrality parameters at different levels.

The positive influence of betweenness centrality to enhance a user's trustworthiness is validated in the Twitter network, while the influence of connectivity (i.e. degree centrality) is shown to be value-less [132].

b. Clustering

The reduction of network complexity and understanding their intrinsic structure is based on the observation that most elements of the systems are naturally grouped into categories and many of its nodes may be represented by a single 'super'-node. Clustering is the respective process of finding such groups of nodes, usually based on some data/content similarity measures between the elements.

A typical literature, which identifies clusters of Facebook users basing on their activities, is [133]. It is shown that users located in the same cluster and therefore having a close connection often trust each other in comparison with users from different clusters.

Again, users in the same cluster with particularly the same attributes will have a

higher trust to each other than users in other clusters. A representative example is given in [134], where a cluster identification of users having a higher *agreeableness* (including the following attributes: friendliness, empathy, kindness) is carried out and a higher mutual trust in those clusters have been identified.

Summarising, it may be figured out that the structure of social networks can and need to be analysed in order to find out important properties about the static and dynamic behaviours of communities which are also related with respect to explore trust and trustworthiness. A big advantage of the presented analysing mechanisms is their formal character.

2.4.3 Explorations by PageRank

The PageRank [94] algorithm invented by Larry Page and Sergey Brin in 1998 and used by Google to rank websites in their search engine results has been several times cited already as an useful tool to consider the topological properties of a node in a graph, in particular centrality aspects. Hereby, the so-called web graph is obtained by modelling each webpage as a node and establishing a link between two nodes, in case the two webpages are connected by a hyperlink. It is important to mention that PageRank, therefore, surpasses the simple in-degree calculation but calculates the rank of the respective predecessor node on the other end of the edge, too.

Therefore, the PageRank of node/page i is represented in the generalised equation by:

$$PR_i = (1 - \eta) + \eta \sum_{j \in N^-_{(i)}} \frac{PR_j}{|N^+_{(j)}|}, \tag{2.5}$$

where the damping factor shall be $\eta \in [0, 1]$. From the formulae, links from important predecessor nodes are more significant than links from average predecessor nodes. According to Page and Brin [94, 135], the damping factor η is usually set to 0.85.

Approximation of the real PageRank values can be obtained by an iterative computation of these equations with an initial value of 1 for each node. The algorithm of formula Eq. (2.5) must be iterated over whole structure until the score for all nodes stabilizes. Therefore, the number of iterations following Page and Brin is about 100.

So far, due to the global availability of the web graph in the search engines database, almost all researchers focus on centralised global metrics. However, advantage of distributed models is that it could assist in eliminating the need for global knowledge. One of these distributed models (computing "personalized PageRank"), which has eigenvector approach based on PageRank with extension supporting more general metadata as well as attack-resistance is presented by Levien [136] following formulations below:

$$PR_i[j] = \frac{1-p}{|N^-_{(i)}|} \sum_{k \in N^-_{(i)}} PR_k[j] + A, \tag{2.6}$$

where A is p if i is equal to j and zero in either case, while p represent the probability that the walk ends at each step. Each element $PR_i[j]$ of the vector maintains a real value standing for trust that node i assigns to nodes j.

In operation of this distributed model, node i only requests the current value of PR_k from the immediate predecessor node $k \in N^-_{(i)}$ to update asynchronously periodically.

At convergent state, the final values of $PR_i[j]$ is determined as same as the random walk. In particular, $PR_i[j]$ is calculated as the probability that a random walk starting at i will end at j.

Basing on the PageRank-inspired approach, [90] introduces a global trust metric so-called EigenTrust in order to determine global trust values for nodes in peer-to-peer networks.

It has both centralised and distributed versions of the algorithm. Unlike PageRank, the metric needs to have local trust values (i.e. weights) between any pair of users. A value between two nodes i and j is defined by $s_{i,j} = sat(i,j) - unsat(i,j)$, where:

- $sat(i,j)$ is the number of successful downloads;
- $unsat(i,j)$ is the number of unsuccessful downloads.

After that, $s_{i,j}$ is normalised into local trust value $c_{i,j}$ from node i to node j, which is restricted in the domain of $[0,1]$ by formula:

$$c_{i,j} = \frac{max(s_{i,j}, 0)}{\sum\limits_{j \in N^+_{(i)}} max(s_{i,j}, 0)} \tag{2.7}$$

There is a fact that a network exists peers that they do not trust any peer (i.e. inactive peer problem). In that case, a set of pre-trusted peers P are introduced. Considering a distribution over P, each element p_i with $i = 1 \ldots n$ of that distribution is calculated as below:

$$p_i = \begin{cases} \frac{1}{|P|} \text{ if } i \in P \\ 0 \text{ otherwise} \end{cases} \tag{2.8}$$

Local trust value $c_{i,j}$ needs to be refined. The main idea is that if a peer does not trust any peer, it chooses to trust the pre-trusted peers. In that case, $c_{i,j}$ is re-defined as:

$$c_{ij} = \begin{cases} \frac{max(s_{i,j},0)}{\sum\limits_{j \in N^+_{(i)}} max(s_{i,j},0)} \text{ if } \sum\limits_{j \in N^+_{(i)}} max(s_{i,j}, 0) \neq 0 \\ p_j \text{ otherwise} \end{cases} \tag{2.9}$$

The provided, distributed algorithm has the following, remarkable characteristics:

- local trust values of node i giving to set of its successors $k \in N^+_{(i)}$ hold in node i;
- each peer computes and stores its own global trust value.

For that, a fully distributed algorithm runs on every peer. Current peer i implements the following two steps:

Step 0: Query all predecessors $j \in N^-_{(i)}$ for their local trust values giving to node i –represented by $c_{j,i}$– with its initial pre-defined global trust value $t^0_j = p_j$.

Step 1: Repeat until $(\sigma < \epsilon)$ \\pre-defined threshold ϵ determines halting condition

1.a Update current global trust value of node i at iteration q:
$t^{(q+1)}_i = (1-a)\sum_{j=1}^{n} c_{j,i} \times t^{(q)}_j + a \times p_i$. \\a fixed parameter a is less than 1

1.b Send $c_{i,k} \times t^{(q+1)}_i$ to all successors $k \in N^+_{(i)}$.

1.c Compute $\sigma = \mid (t^{(q+1)}_i - t^{(q)}_i) \mid$

1.d Wait for all predecessors $j \in N^-_{(i)}$ to return $c_{j,i} \times t^{(q+1)}_j$.

It can be seen that the distributed algorithm has a lot of advantages. Computation load is distributed and sensitive private data does not need to be collected in a centralised database. The complexity of the algorithm in simulation is relative fast. It converges after only 100 query cycle for a network of 1000 peers.

However, the transmission of local trust values to neighbour peers may reduce privacy and may cause violations of confidence. Moreover, the assumption that every node is honest, is required for a proper work of EigenTrust algorithm.

Recently, the study of random walks [137, 138] has been playing an important role in the field of analysis of complex structures and to avoid the above problems.

Random walks (Definition 13.): *are sequences of forwarding steps (of a message or agent, called a 'random walker') starting from a selected initial node, whereby every intermediate node determines the next target node randomly out of the set of its neighbours.*

Inspired by the remark of Page and Brin themselves that the PageRank-value [94] is equivalent to the visiting probability of a random walker, in [118] the concept is used to find suitable nodes for a file placement in P2P systems. In this case, the transition probability of the random walker was influenced by a set of system parameters, which let the random walker preferably visit nodes with high hard- and software capacities.

The important characteristic of the random walks-based method is the capability of coordination of random walkers and the management of populations of random walkers in a fully distributed manner via a local algorithm.

In [139], more important random walks-based algorithms may be found. The self-stabilisation of a random walker based population by the following, fully decentralised working algorithm:

Step 0: *Initialize* variable $\tau_{avg} = \infty$ and constants τ_{max}, τ_{min}.
Step 1: If $\tau_{avg} > \tau_{max}$ then ***Generate*** a new random walker into population.
Step 2: If $\tau_{avg} \geq \tau_{min}$ then
2.a *Select* a neighbour u_y with non-uniform chosen probability of current node u_x.
2.b ***Move*** all random walkers to neighbour node u_y.
2.c *Mark* identification of loop τ_1.
Step 3: If $\tau_{avg} < \tau_{min}$ then ***Remove*** a random walker from population at current node u_x.
Step 4: *Wait* until a new random walker arrives and mark identification of loop τ_2.
Step 5: *Update* τ_{avg}: $\tau_{avg} = \tau_2 - \tau_1$.
Step 6: *Wait* until any random walker arrives and *Goto* Step 1.

Hereby, each node defines τ_{min}, τ_{max} describing the length of the shortest and of the longest period in which the node (in average) shall be visited by any two subsequent random walkers of the population. τ_{avg} controls the average visiting time from a fixed number of last visits.

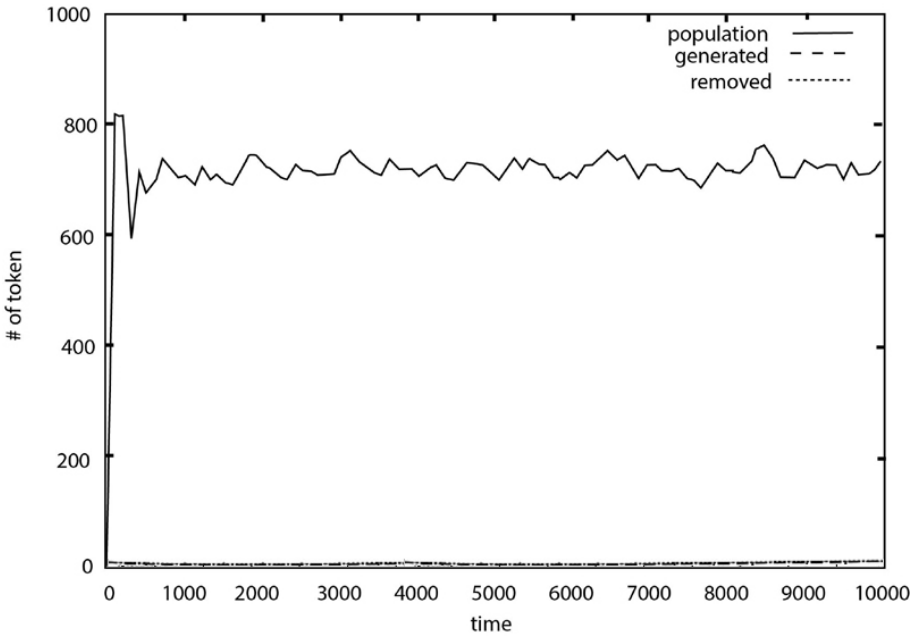

Figure 2.8: Population Size of Random Walks Controlled in [139]

At each node, a local algorithm may perform three operations: *generate*, *remove* and *move* random walkers based on the comparison of the $\tau_{min}, \tau_{max}, \tau_{avg}$ variables.

From Figure 2.8, it can be seen that the obtained population size is almost constant. It will also adapt itself to a changing network size. The generated random walker population may now be used to fulfill management tasks (e.g. in the context of the intended trust management). Note that the concept of random walks fully protects privacy of local trust values in calculations on each node. In contrast to other existing works, random walkers process only local data in a private way without sharing sensitive information such as local trust giving to neighbour nodes

and pattern of interactions. In the case of expecting increase of trust relationships against sink nodes, idea of predefined trusted peer from EigenTrust algorithm could be used. Possibilities to trace random walkers in a decentralised manner may avoid unwanted fraud in such a system as mentioned in [139].

2.5 Content Analysis

2.5.1 Content Similarities

As mentioned before, most information in on-line social network is presented in textual form. Therefore, text mining becomes an important tool to derive implicit trust signals of content posted from different users. There are several text mining-related methods, which are useful for the purpose of this thesis: (simple) *similarity*-based comparisons, the (more complicated) opinion mining and finally the *volatility analysis*, to detect rough changes in a user's textual expression. Also, as mentioned in subsection 2.2, text-mining may give precious hints on the context, in which the users are acting as well as it –continuous– changes.

Different similarity (distances) measures can be applied to decide correlation between similarity and trust, whether contexts are similar, messages fit to a given context or whether users matching well by having similar personal preference and interests. Measuring similarities is basing on different distance measures, like the Minkowsky distance between two term frequency vectors of texts x and y by:

$$sim(x, y) = \sum_{k=1}^{n} (\mid x_k - y_k \mid^r)^{1/r} \tag{2.10}$$

In Eq. (2.10), n denotes the number of attributes, x and y are texts with two respective term frequency vectors $(x_1, x_2 \dots x_n)$ and $(y_1, y_2 \dots y_n)$.

The usually preferred Euclidean similarity between x, y (viz. $L2 - norm$) is obtained, if $r = 2$ by:

$$sim(x, y) = \sum_{k=1}^{n} \sqrt{(x_k - y_k)^2} \tag{2.11}$$

For an overview of further approaches to measure text similarities, the best general reference is the survey [140].

2.5.2 Opinion Mining

Opinion mining (also called sentiment analysis) is the approach of extracting users' opinions and moods expressed by the use of special word sets within textual contents.

The main subtasks are the detection of emotions (happy, sad, anger, surprise) [141] as well as an automatic identification of their polarity (positive, neutral, negative) in subjective text documents.

Polarity analysis is the most widely studied field in opinion mining. Texts expressing opinions can be addressed by distinct levels of words, sentences or generally documents, from a data source. In this section, a short overview is given how to accomplish these tasks.

Several automatic working methods have been developed to extract knowledge in opinion mining for many real-world practical applications. In [142], an overview of graph-based approaches is presented. These solutions rely on the analysis of graphs of semantically related/associated terms and words constructed from texts. Several examples are:

- Min-Cut algorithm [143] performed to determine effectively sentiment polarity;
- random walk-based algorithm [144] to solve the problem of ranking synsets according to positivity and negativity.

These graph-based algorithms showed a significantly better performance than other machine learning and classification methods. A machine learning approach uses supervised learning method for building a trained model. After the training, a process can predict to which category a new textual input pertains.

Several popular classifiers are Naive Bayes and Support Vector Machines. An advantage of these methods is that only minimal training data sets are needed to achieve reliable results. It is probable in [145] that machine learning is well suitable to indicate opinions in particular domains such as hotel, product, travel, restaurant...

There are comparatively less research works applying the sentiment analysis concept to social network data and analysis, like for Facebook in [146] or Twitter in [147, 148].

Dealing with all problems of sentiment analysis is still an ongoing research problem due to the complex character of natural language processing. The problem becomes in on-line social networks even more complex, since:

- usually, there is a huge, heterogeneous volume of different on-line documents and user-generated content on the Web;
- the structure of texts is often not clear, noise texts exist due to unwanted, topically unrelated postings;
- not all posts are accessible due to privacy restrictions;
- posts and comments are short;
- posts and comments contain slang, phrase of idioms, emojis, links, colloquial language with ironic or even sarcastic content;

- topical cohesion between and even in posts is less likely than in examples in a textbook or scientific article on a particular problem.

These problems might lead to unsatisfying results, especially, if adverse features are contained in short texts of unknown users. So far, the polarity approach to detect emotions within documents using pre-built dictionaries or lexical resources (like WordNet [149]) seems to fit mostly to the intention to generate usable trust signals. Several created examples of such systems are:

- SentiWordNet [150];
- SentiWS [151]:
- WordNet-Affect [152];
- Network Overlap Technique [153] containing a contextual-aware polarity strategy;
- Emoji Sentiment Ranking [154] for the consideration of symbol sets like emoji.

Usually, in those approaches, terms/words/symbols are mapped to dictionaries to fetch sentiment scores for them as well as to synonyms or antonyms. Each document is classified by calculating a sentiment score for each element of it and then simply summarising the polarity score of all elements of that document. In fact, this approach may have two major drawbacks by:

- taking into account several issues related to word position, word relationships, unjust or negation handling;
- requiring a high quality of polarity dictionaries. There are three main approaches for generating dictionaries: manual, dictionary-based and corpus-based [155].

However, recent examples even in industrial applications have shown the advantage of of sentiment and especially polarity analysis. In particular, changes giving a reason for trust re-evaluations may be well detected. The detection of changes is also the reason, why text volatility may play an important role in trust signal considerations.

2.5.3 Volatility of Content

While it might be hard to determine and classify the exact topic of a text, it is often easier to detect changes in a topic or recognise an upcoming new content element. Often, such changes cannot be detected in overall frequency measures but in changes in its dispersion (i.e. in changes in the rank) of:

- plain term frequencies;
- signal phrases;
- co-occurrences of terms.

Among them, the approach to determine the volatility of term co-occurrences seems to be the most promising one. Measuring volatility variance is used to facilitate detecting or tracking of topic changes and change of meaning. Maxima in the variance of volatility over time may be automatically found and indicate interesting changes. The following volatility algorithm presented in Holz et al. [156] can be used for the needed calculations:
Step 0: Construct a corpus including all corpora of n time slices
Step 1: Compute for the overall corpus all significant co-occurrences $C(t)$ for specific term t. Set m is total number of significant co-occurrences of term t, $m = |C(t)|$
Step 2: Compute all significant co-occurrences $C_i(t)$ of term t for every time slice i , $i = 1 \dots n$
Step 3: For every co-occurrence term $c_{t,j} \in C(t)$, $j = 1 \dots m$, compute all series of rank, denoted by $rank_{c_{t,j}}(i)$ with $i = 1 \dots n$ over all time slices i. Analogously to that a rank series consists of n ranks of $c_{t,j}$. Rank of a term in a time slices i is position of that term in sorted list of $C_i(t)$ based on significant values. For example, significant values could be measured by log-likelihood and afterwards normalised.
Step 4: Compute the coefficient of variation (abbr. CV) of the series of rank $\mathrm{CV}_i^n(rank_{c_{t,j}}(i))$ for every significant co-occurrence $c_{t,j} \in C(t)$. CV measures the relative variability of rank series on a ratio scale following the formulae $CV = (standard\ deviation(\sigma)/mean(\lambda))$
Step 5: Compute the average of all these coefficients of variation for every significant co-occurrence $c_{t,j} \in C(t)$

$$Vol(t) = \mathrm{avg}_j^m \, \mathrm{CV}_i^n(rank_{c_{t,j}}(i)) \tag{2.12}$$

Equally

$$Vol(t) = \frac{1}{m} \sum_j^m \sum_i^n CV(rank_{c_{t,j}}(i)) \tag{2.13}$$

The presented approach exhibits several advantages to derive trust signals:

- high-volatile topics immediately indicates opinion changes and may cause the generation of alerting trust signals;
- for that purpose, even new topics (carefully brought to a community) with a low frequency ("weak signal") can be detected, a trend of those topics will be identified and might be used to identify and alert a user on upcoming adverse activities;
- hidden lies in text messages may be indicated via topic changes;

- it is also possible to combine this approach with the detection of the (average) polarity of the terms using lexical resources. If there exist terms, which have not been classified yet, techniques for label propagation [157] in co-occurrence graphs can be used to assign a polarity score to it.

Differing from the polarity detection, the volatility analysis works without well-trained data bases and does not depend on subjective changes in case of multiple users. It might therefore immediately be applied without too much preparations or learning phases.

In general, it is expected that processing textual content submitted from users in on-line social network systems may increase the accuracy of trustworthiness recommendations once more.

2.6 Summary

Human interactions take place in today's society in a manifold manner, in complex environments and with mutual dependencies, which are hard to understand and to analyse by formal methods, so far. The feeling of trust, usually generated by human intuition in the unconsciously working limbic system is giving people a good guidance in reality. It does not work, in case computer systems and in particular on-line social networks are involved in communication, business or financial processes. To avoid a loss of money, property or reputation, reliable recommendations on trustworthiness must be given to the users.

Until today, there is no tool or any other kind of support, allowing humans to evaluate the trustworthiness of a (so far unknown) communication or business partner and protect them from any harm or loss in a similar manner as human feelings can do in the reality.

Existing solutions cannot conquer the complexity of the problem or convey the human trust feeling in a reasonable as well as persuading way. Mostly, explicit trust signal sources offer manifold opportunities to detect lies, fraud and manipulations.

People are overwhelmed severely by the sheer amount and the complexity of data available, which –however– may contain a plenty of implicit trust signal sources. Nevertheless, processing all this information exceeds the limited capacity of the human for perception and optimising his interactions. Additionally, a high amount of irrelevant information may irritate even the most caring users. Although the demand is clearly motivated, there is still no tool available, making information from several sources compatible and use them to generate a recommendation on trustworthiness, which can be accepted by a big amount of users.

Chapter 3

Trustworthiness Recommendation

3.1 Overview

The following two chapters constitute the main part of this work. In the previous chapters, the fundamentals of trust and trustworthiness have been reviewed and presented. It became increasingly clear that the human feeling of trust (i.e. the feeling inside the brain of any user in front of a computer system/on-line social network is hard to model and even harder to influence).

That is why it can only be tried to give reliable recommendations on trustworthiness to the users of the system, which might be derived from their behaviour over a long time. Such a recommendation system must be able to filter the plenty of available information, recognise the relevant data and compute a decision proposal for the applicant using a suitable algorithm.

The Chinese social credit system is an example for such a recommendation system. It was developed in order to recommend 'social credit' of every citizen [158]. Trustworthiness of each citizen is built up from commercial activities, social behaviour and criminal records and so on.

The study of this and other system showed set of lacks and disadvantages, which shall be overcome by the new suggested approach in the following two chapters. This means to design a methodology and afterwards a working system, which

- is able to generate a recommendation on trustworthiness to all users;
- derive trustworthiness from processing a manifold of user activities not only limited to financial and business activities;
- does not distribute sensitive information of the user but builds the possibility to process sensitive data locally on the users's host, only;
- supports the possibility of an observation of the own recommendation on trustworthiness and –at least– a possibility to restart the trust-gaining process at well determined times to all users;

- strictly avoids the possibility of governmental influence and unwanted use of the collected data;
- runs autonomously besides an (already existing) on-line social network systems (i.e. is not owned, influenced or manipulable by the respective service provider).

To obtain recommendations on trustworthiness of users in a decentralised manner, the new methodological approach is proposed in the two consecutive chapters which relies on evaluations of activities and contents distributed. That methodology can be strategically separated into the following two steps:

- *Step 1:* recognising trust between every pair of users expressed by their activities coupled with content distributed;
- *Step 2:* calculating the system's recommendation on trustworthiness of any user by processing all pairwise user relations depending on the users' embedding in the social network expressed by their connections to communication partners, friendship relations and business partners.

To obtain and understand the way to reach the indicated goal, the following, more detailed major five steps must be carried out:

1. In order to understand the operation of systems and figure out possible input parameters and activities to be considered, a simple model of an on-line social network (i.e. a user-content-network) is designed. The reason for this step is that, so far, existing network models are dealing with structural aspects only and are incapable to handle user behaviours and the variety of contents existing in real networks.
   This model and the understanding of real social network functionality might be later also used as the basis for the intended simulation experiments, since many considerations are impossible to do in the real environments.
2. In a next step, it must be understood, how characteristics and interests of the users are manifested in real networks and how those characteristics may be included in the model. Special attention must be given to an evaluation of textual contents and to understanding, how contents may influence a user.
3. After the deep understanding of the functionality of on-line social networks and their modelling, an evaluation of the obtainable information must be carried out. This mostly means to evaluate, which data might be used as trust signals and might be relevant for further processing. This process shall also include a weighting of the different measurable signals for further processing.

4. Starting from trust signals (i.e. both activities and contents distributed) conclusions related to the trust of two involved users in the real-world shall be derived by cumulating the scores calculated from all obtained trust signals (Note that –of course– both estimations made for every user may be different).

5. Finally, a fully decentralised working algorithm will be introduced, which takes the different cumulated user activities and the partial structure of a social network system into account and computes depending on this information a global trustworthiness for every user in the system.

All the described design steps will be made, such that later a decentralised implementation of a respective system will be possible, which can obey the requirements on privacy and data protection.

3.2 Model of User-Content-Network

In this section, a simple usable model of a typical on-line social network shall be presented.

It is obvious to use a graph-based model for doing so, where the set of users build the set of nodes and connections among them represent communication links and exchanges of contents along so far established friendship relations.

Recently, the works of Coltzau et al. [159, 160] have presented an advanced mathematical model based on the origin of the preferential attachment model by Yule [161]. The model attempts to explain network structure evolution over time along with various social processes including user's behaviours and contents and can be used to obtain the initial network structure.

In a second step, contents and content transport in such a network must be investigated and –with the respective simplifications and generalisation– be modelled. Therefore, the following settings can be specified.

In the model, let $U = \{u_x, u_y \dots\}$ be the set of all users, $A = \{a_1, a_2 \dots\}$ a set of activities and $C = \{c_1, c_2 \dots\}$ a set of contents. It might be assumed that C is a integer or arbitrary type of data and $sim(c_i, c_j)$ measures how similar the content of any two elements c_i and c_j is. In order to evaluate this similarity, sim simply determines the Euclidean distance between the textual parts of a post distributed.

Now the processing and distribution of contents by each of the users must be considered. There are three major steps for doing so:

- content is received, organised in the users account content area, typically timeline, and presented to the user, when the user is on-line. Since there exists a plenty of contents, the newest content is presented first.

- if the user is on-line, he/she might review, evaluate and process content.
- the interesting part of content is that one, which is either from the user generated or liked by the user. Those elements are usually re-distributed (i.e. shared) with other subgroups of users (usually friends or parts thereof) and therefore put on another, output data storage.

Consequently, stacks have been used in the model for the content management. These stacks may host any information element and support two principal operations: push and pop. They also satisfy the condition of a last in, first out (LIFO) operating principle (i.e. that any new data elements are presented at first to the user).

As mentioned above, content processing by the user is executed when the user is on-line. In the literature mostly an on-line and an off-line state of a user is considered, although [134] –in addition– distinguish between active and passive on-line status, depending on the intensity a user is dealing with his on-line social network due to other (minor or major) works processing. In the suggested model, the simple two status model is used, having the following property:

- **On-line:** In this mode, a user shows up, takes content elements from his input stack, evaluates them and decides which elements shall be re-distributed to which target group of users known to him. He may also add up some new elements to the output stack. Note that in this simple model, any kind of content like mails, chats, posts are processed in the same manner.
- **Off-line:** No interactions are possible to be executed in this mode. An off-line node is in a fully inactive status, although it will be possible to store contents received from other users. This content elements are saved and are ready for processing, when the node is on-line again.

These states are concretely possessed in a probabilistic model of on-line social network user's lifetime in [134] for a better design of the content network model in terms of activity prediction and information distribution. The model defines the conditional probability of the transition between on-line and off-line states based on distinguishable on-line activities and group characteristics. There is an interesting result in [21] indicating that dependency between lifetime and number of users exhibits power-law distribution.

At this point, more details and working mechanisms of the model can be more formally described. An arbitrary user $u \in U$ has an input or recommendation stack $R(u)$ and a stack of liked or newly added content $L(u)$ and set of neighbours $N^+_{(u)}$.

In Figure 3.1, neighbours of the user u are illustrated by the set $N^+_{(u)} = \{u_u, u_p, u_q, u_k\}$. The stack $R(u)$ receives content elements $c \in C$ from other neighbours knowing him (e.g. on-line users u_1, u_2 and an off-line user u_3) and randomly from on-line social systems. If the user is on-line, the element c is transferred to the stack $L(u)$ if :

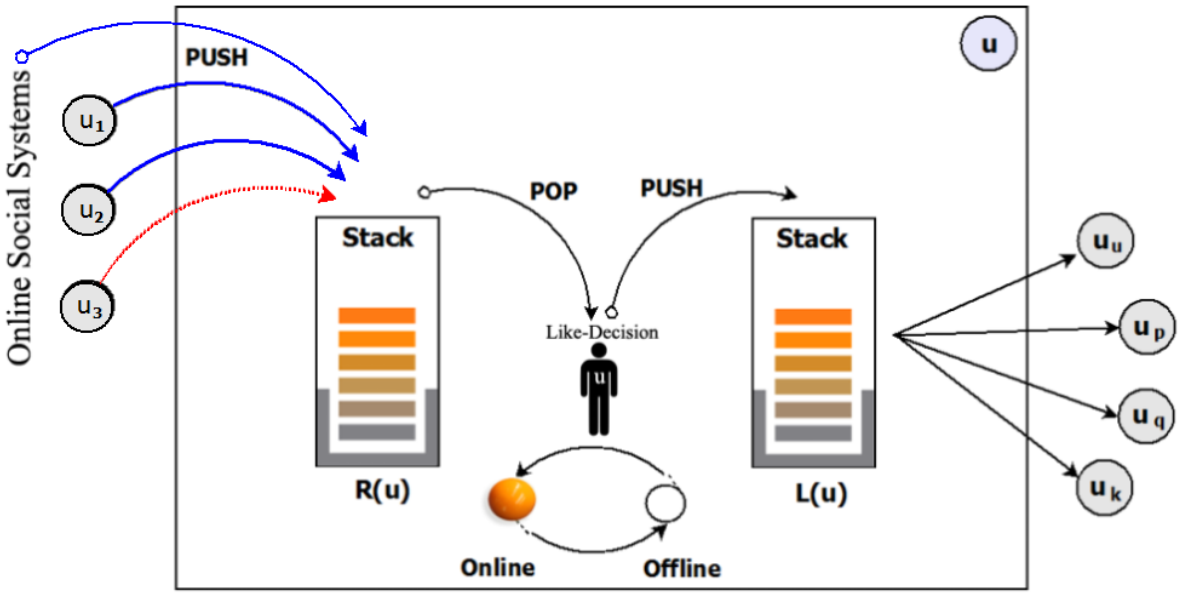

Figure 3.1: Simplified User Content Network Model

- $c \in R(u)$
- the user u makes a like-decision to put c into $L(u)$

Each element in $L(u)$ will be re-distributed to a partial –for simplicity– randomly chosen set of u's neighbours viz. $D(u) \subseteq N^{+}_{(u)}$. Redistribution means to put the element to recommendation stack of these users accordingly to its time of arrival.

In order to evaluate content recommendations received from other users, each user defines a set of interests as a subset of all possible contents $I(u) \subseteq C$.

An element $c \in R(u)$ is evaluated using a decision function: $f : c \to \mathbb{R}$.

Experimental works (e.g. by [159, 134]) confirm the practicability of the introduced simple modelling approach. [159] considers the occurrence of super-popular contents in two scenarios and investigates the proposed content propagation mechanisms. Meanwhile, another work of [160] even adds and investigates the effect of changes in the link structure in this model (in two scenarios) and its effects to an average like rate of special content.

With the flow of information, useful hints for the wanted recommendation on trustworthiness can be derived (either in the considerations of this work from the described model or from real content flow). The following aspects might be considered in doing so:

Similarity

Discovering content similarity is of importance because user tend to trust each other, if they have similar interest as indicated in from empiric studies using taxonomy-driven similarity computation technique in [116]. In such a manner, a user u shall check for every element $c_i \in R(u)$, whether the similarity of those elements $sim(c_i, I(u))$ is

higher than a given threshold μ. In this case, not only the fact that the respective communication among two users has been made shall be taken into account to determine their trustful relation but a given, additional positive quantum shall be added to the respective trustworthiness relation. Of course, also the probability to resubmit these contents is taken into account.

Opinion mining
The similarity analysis is superposed and/or is affected by the opinion or polarity analysis. Positive results (e.g. friendly, supporting opinion) will increase trustworthiness by a given quantum, while negative (e.g. angry, rude, opposing) may reduce or –from a given intensity– even destroy trust in the sending user.

Volatility
High volatility values indicates a change in topics by first, weak signals and signalise usually that something in the person, context or intentions of that person have been changed. Consequently, high volatility values shall in general increase attention and are being evaluated as negative influences to trustworthiness.

The contents of any communication, for examples, posting, publishing, sharing, notifying, answering, messaging, profile contents, comments, articles, photo, emoticons, emoji, hashtag, link and its-relevant contents... may also be analysed and used to derive valuable trust information.

3.3 Cumulated Trust

Following the characterisation of trust in chapter 2 and applying the results to on-line social network systems, it must be figured out that a feeling of trust may develop in users depending on:

- the time that two users know each other;
- the similarity of their interests and personal preference;
- a mutual predictability of their activities and contents distributed;
- and last but not least, often initially given trust.

Differing from the human approach of building trust, a technical system must be based on exact measurements of suitable parameters and algorithms as well as on how to combine them to a reliable trust value. In this case, trust is cumulated from trust signals from communication behaviours as activities and contents distributed between pairs of users.

The different activities related to a user u may be evaluated in an on-line social network system. Evaluation may be carried out in general for all users or separately for each user depending on her/his personal feelings. Questionnaires as in [134] have been proven to be a sufficient tool for doing so.

In such a manner, trust signal elements $k \in K$ with $K \in A \cap C$ may be identified. These elements have the property to be able to increase, support or reduce trust in a person or shall correspondingly influence the trustworthiness. Also weights regarding the intensity of their trust-influencing properties may be obtained. For formalisation, the function $E(k)$ is defined $\forall k \in K$, determining to each trust element (i.e. activity or content) the intensity if the effect to the trust of the affected user u. Negative values of E(k) describe trust or trustworthiness reducing, negatively affecting but its positive values express trust increasing. The value of zero denotes a neutral influence.

A user built is overall trust feeling not from several single activities or contents received. Trust must be built in a cumulative process over a given time or the whole history of a relation between any two users u_x and u_y.

Therefore, it was decided to setup $T(u_x, u_y)$ to evaluate the effect of the communication between two users u_x and u_y over a given time horizon. $T(u_x, u_y)$ is called '*Cumulated Activity Factor (CAF)*' (i.e. describes the effect of user u_x on user u_y). All trust signals are derived from the pairwise communication and must be considered for each pair of users. For each user u_x, a vector of *trust-effect-sum* $T(u_x, u_y)$ for evaluating its neighbours is introduced. The $T(u_x, u_y)$ value should initially be set to $T_0(u_x, u_y) = 0$.

In the described approach, (both) the activities as well as the evaluation of contents regarding their similarity, polarity and volatility will be used to initiate a periodical update of the cumulated activity factor between any pair of users. Series of trust signals over time update the value of the cumulated activity factor by summarising scores of each single activity and contents distributed in a time sequence.

$$T(u_x, u_y) = T_0(u_x, u_y) + \sum_{\forall k \in K} E(k). \tag{3.1}$$

Note at this point that the cumulated activity factor is not symmetric (i.e. $T(u_x, u_y) \neq T(u_y, u_x)$). Also, in case of too many negative influences, $T(u_x, u_y)$ might become negative and shall be adjusted in such a case to zero. The reason is, that zero corresponds to an absolutely adverse feeling which cannot become worse.

In detail, in an on-line social network, on-line behaviour covers a limited set of social activities that users can perform on-line such as like, comment, tag, being follower, hide-post, turn-on-notification-for-a-post, hide-ad, confirming-useful-ad, browse-profile, add-friend, receive-email, un-friend, un-follow, report-post, block-friend. All these activities and fore-mentioned contents are trust signal-building elements and can be used to define applicable

rules for an update of the cumulated activity factor $T(u_x, u_y)$ through those elements between u_x and u_y by an intensity E(k):

- Being liked from a user u_x will contribute a positive $E(k)$.
- Consecutive like activities may increase the cumulated activity factor to an extent. The consistency –as a signal of reinforcing trustworthiness– of positive like activities is considered as an indicator of intimate friendship. As a result, the cumulated activity factor could be increased by a significantly high $E(k)$.
- Tagging a user and reviewing post friends tags also results in a positive value for $E(k)$.
- Being added as a friend or receiving email from another user is also a quite positive signal, which results in a positive $E(k)$, the same for receiving email respectively. Changing status of a friend (close friends, acquaintances or pre-defined friend list) or suggesting friends also significantly impact to trust.
- Being a follower –not count the case of making friend since friends automatically follow posts by default– to see posts in public timeline or turning-on-notification-for-a-post may result in a positive $E(k)$. In contrast, un-follow triggers result in a negative $E(k)$ value.
- The content analysis or analysing contents surrounding a link will compute $E(k)$ as described in the previous section depending on the strength of the found similarity, polarity or volatility.
- Hide-ad, confirming-useful-ad could respectively decrease or increase a negligible portion of trustworthiness.
- Reaching a given cumulated activity factor will result in adding u_y as a friend by u_x. As a result, cumulated activity factor $T(u_x, u_y)$ increases by a positive $E(k)$ by this making-friend activity.
- In the same manner, a much lower value of $T(u_x, u_y)$ may result in an un-friend activity. As a result, also the cumulated activity factor $T(u_x, u_y)$ decreases by this un-friend activity.
- Finding a triadic closure (i.e. u_x and u_z are friends and recognize that u_y and u_z are friends as well) may increase $T(u_x, u_z)$ like add-friend activity. A differentiation using strong and weak ties may also be useful for determining how much cumulated activity factor increases.

- Also, a new friend may be randomly added with a small probability, representing a new friend from the real-world. For those people, a initial cumulated activity factor must be interactively determined but later adapted following the given rules here.

- Recognised lies will result in $T(u_x, u_y)$ being set to zero. Consecutive un-friend activities as an example, may depend on the user's character. Conscious lies are a proven possibility in social life to reach a goal. Therefore, later more complex handling rules for lies must be derived.

- Hide-posts activity is synonymous that posts are not interesting or even (potentially) harmful. A higher level of reaction to a post is to report that post. The report-post activity clearly confirms that the post is serious harms to someone or something. Thus, the cumulated activity factor $T(u_x, u_y)$ must be reduced significantly by a respective $E(k)$. In another case, block-activity may result in reducing the cumulated activity factor to zero.

Some of the last examples already demonstrate that the cumulated activity factor $T(u_x, u_y)$ may have direct influences to the friendship relation. Friends are not added only as a result of a certain, single activity or request, but as soon as a user feels comfortable with another one. Hereby, for the first time, a direct influence of trust to network topologies is given. Therefore, from the consideration of $T(u_x, u_y)$, the following two rules may derived:

- *Rule 1:* If $T(u_x, u_y) \geq \phi$ then u_y is automatically added as friend of u_x, where ϕ is a upper-bound determining friendship generation.

- *Rule 2:* If $T(u_x, u_y) < \eta$ then u_y is removed from u_x friends list, where ϕ is a lower-bound determining to eliminate the considered friendship(s).

The constants ϕ, η must satisfy the condition $\phi \geq \eta$ and depend on the established model and circumstances as a function of the affected person. The application of these rules automatically results in a social network structure changing dynamically over time[1].

The modelling described above is just a first approach. It may not contain all possible trust signal elements, due to the complexity of the systems. Also, for simulation purposes, general assumptions must be made to initialise all parameters as well as to describe the update properties of different events, which must be –for a practical use significantly– refined. However, the described settings are sufficient to demonstrate the success, capabilities as well as the practicability of the presented approach.

[1] As aforementioned, the respective changes satisfy the power law for the in- and out-degree of the nodes in the network.

3.4 Oblivion

So far, any accumulated trust signals are kept forever in cumulated activity factor $T(u_x, u_y)$ and influence its value and therefore the subsequent trust evaluation of u_y by u_x. This does not reflect the usual behaviour known from people, which tend to forget positive as well as negative experiences over time. Therefore, some oblivion should be added to the presented model at this point.

Although this has not been addressed –so far– the local cumulated activity factor $T(u_x, u_y)$ depends on the time (i.e. becomes $T(u_x, u_y, \tau)$) where τ stands for discrete time steps.

If ${}_{\Delta}T(u_x, u_y, n+1)$ denotes the cumulated activity factor changes obtained in the last time interval from n until $(n+1)$, $T(u_x, u_y, (n+1))$ can be calculated in a recursive manner without keeping all history values of $T(u_x, u_y, \tau)$ in the memory by:

$$T(u_x, u_y, (n+1)) = T(u_x, u_y, n)e^{-\lambda} + \frac{{}_{\Delta}T(u_x, u_y, n)}{S}, \tag{3.2}$$

wherein λ is a fixed parameter to describe the strength of oblivion. While $T(u_x, u_y, n)$ is multiplied at every time step by $e^{-\lambda}$, successively the impact of trust signals considered in the last time step are weighted with $e^{-\lambda}$, those from the step before is multiplied by $e^{-2\lambda}$ and so on. Since $e^{-\lambda} \geq 1$ for any positive selection of λ, the influence of older trust signals become smaller and smaller in every time step.

S can be understood as the number of considered (weighted) values and therefore also as the influencing part of the last determined ${}_{\Delta}T(u_x, u_y, n)$. As it is easy to be seen, it can be counted by:

$$S = \sum_{k=0}^{\infty} e^{-\lambda k} = \frac{1}{1 - e^{-\lambda}}.$$

The value of the parameter λ needs to be investigated and depends on the obliviousness and the limbic personal character traits of the respective person.

Replacing S in the previous formula by the calculation for S generates the final formula to count $T(u_x, u_y, (n+1))$ by:

$$T(u_x, u_y, (n+1)) = T(u_x, u_y, n)e^{-\lambda} + (1 - e^{-\lambda})_{\Delta}T(u_x, u_y, n). \tag{3.3}$$

Figure 3.2 illustrates the impact of the included oblivion factor in a graphical manner and clearly shows the obtained time window for considering $T(u_x, u_y, (n+1))$.

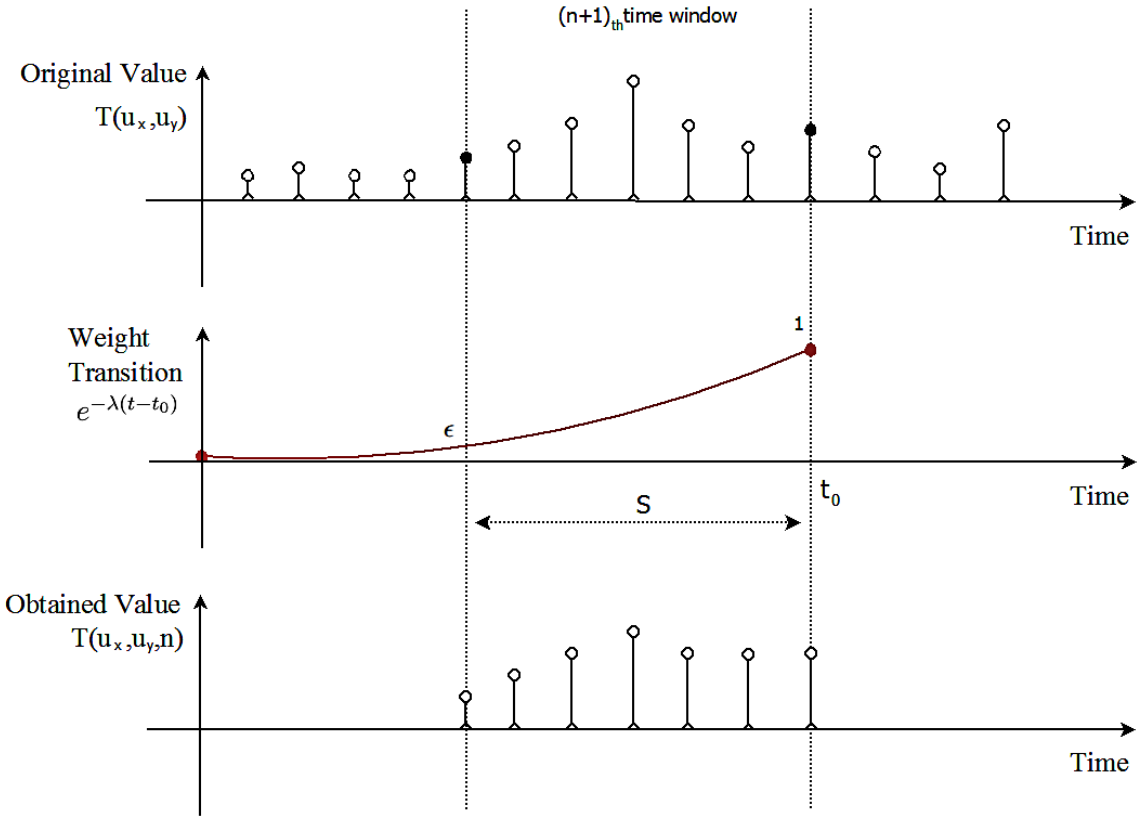

Figure 3.2: Illustrative Example of the Considered Time Window through Oblivion

3.5 Normalisation

3.5.1 Need and Requirements

The aforementioned trust signal elements determine the cumulated activity factor $T(u_x, u_y)$ of an user u_x for another user u_y with or without oblivion. It is clear that $T(u_x, u_y)$ can vary in a large range from 0 to ∞. That is why a normalization process is needed, to adjust the modelled trust values as well as trustworthiness in a fixed interval, typically between $[0, 1]$. Hereby the value of 0 denotes no (or zero) trust and 1 full trust as suggested by Gambetta [55] and formalised by Marsh [9].

The output values of the normalization process is the estimation for the level of trust a user u_x may have in another user u_y or the trustworthiness which may be recommended to u_x about u_y denoted by $t(u_x, u_y)$.

In the following, the question shall be discussed, which normalisation function shall be used to obtain a suitably, uniformed $t(u_x, u_y)$ in the interval of $[0, 1]$ from $T(u_x, u_y)$ and which parameters must be, therefore, defined or calculated? The author refers for this propose to the research results introduced in chapter 2 and specially to the observations expressed in

Figure 2.1. The respective curves can be divided into several elementary parts and fixed by their parameters by knowing the following information about a user:

- *Initial trust:* Is initial trust given and how strong it will be?
  According to [162] and [163, 9] initial or basic trust is given as a credit to ever user. This basic trust is required and useful, because it helps each user to actively establish contacts and interactions with others.
  The specification of initial trust could be carried out by measuring personality characteristics of users by questionnaires, as suggested in [63].

- *Inception phase:* How long does the inception phase take?
  There is an inception phase, in which newly met partners are carefully observed only. In this time, any given and initial trust is usually not or insignificantly increased. This time may depend on the user –of course– but may also be influenced by the frequency of activities of the other users observed (i.e. if frequent messages, prompt replies with positive content are received) the inception phase might be shorter.

- *Trust development rate:* How fast the trust level is increased?
  A user is normally very careful in the beginning and gains remarkable trust only after the described inception time. How fast the saturation (i.e. fully trust) is reached takes some times, the duration of this time depend on the slope of the trust function.

- *Restitution of trust:* How to deal with negative trust signal elements?
  In fact, personal relations do not only develop in a positive, progressive manner. Manifold reasons in life let users also observe negative trust signals from their partners. While it is normal to receive in larger time intervals a few negative signals, a burst of negative signals may destroy any so far successful, intimate relation. While occurrences of negative trust signals will reduce the trust development in the inception and development phase immediately, there will be some endurance times once full trust is given to a partner. If after this endurance time still negative or a majority of negative signals is received, trust is reduced with a given slope (which may differ from the slope value for gaining trust). Note that rough disturbances of a trust relation (e.g. lies, cheating, deception or fraud) may immediately set the trust of a partner to zero (i.e. without any delay or slow trust reduction).

- *Grade of trust:* How to distinguish different partners?
  So far it has been assumed that in case of receiving permanently positive trust signals, full trust (i.e. stable point) can be reached after some time. However, the human brain is much more accurate and fine grained in its estimations and may distinguish different saturation levels in the interval between 0 and 1. This grade of trust depends on very

subjective feelings (e.g. sympathy, love, physical attraction) a person may have for another one but maybe even have a measurable component given by the relation of the amount of positive received trust signals (or signals above a expected, given and positive threshold) in relation to the overall number of trust signals received.

Different trust normalisation functions may be suggested but must meet more or less all the above characteristics. In the sequel, two possible functions are presented in order to model user characteristics with different pro's and con's.

3.5.2 Normalisation Functions

A first possibility for a normalisation function results directly from the works of [164] discussed in chapter 2 that the dynamic of trust is definitely more or less approximation of S-curve. The suggested S-curve directly has its mathematical correspondence in sigmoid functions. A set of different sigmoid functions –which are introduced in [165]– guarantees the needed characteristics to model trust as mentioned in [73].

For the purpose of this work

$$t(u_x, u_y) = \frac{1}{2} + \frac{T(u_x, u_y) - CAF_{init}}{2\sqrt{1 + (T(u_x, u_y) - CAF_{init})^2}}, \tag{3.4}$$

is the most suitable sigmoid function, since it contains only polynomial and no trigonometric components. Figure 3.3 shows to different parameterised sigmoid functions of that type, whereby CAF_{init} determines initial trust $t_0(u_x, u_y)$. The function is derived from the original sigmoid function $g(u_x, u_y) = \frac{1}{2} + \frac{x}{2\sqrt{1+x^2}}$ with $-\infty \leq x \leq +\infty$ by shifting a specific distance CAF_{init} following X-axis. Via that, several wanted different parameters of inception times and initial trust are obtained. A saturation at a stable point level –approximately 1– is assumed.

Although the sigmoid function seems to fit well for the intended modelling purpose, it also exhibits some problems and difficulties:

- sigmoid functions needs to be derived from a few constants (i.e. inception time, slope of trust, expected trust saturation level) which need to be assigned to points of the sigmoid functions. This may be a non-trivial task, especially since more parameters might be used and determined (e.g. where is the end point of the inception time? how much trust increase in the inception time is acceptable? how to determine the point of the curve? where the slope may be represented?) since the available sigmoid functions are not ideal ones;
- curly figure of sigmoid curve is relatively rigid to adapt to expected parameters;
- depending on the needed shift as above-mentioned for the parameter adaptation, the characteristics of the dependence function may be violated;

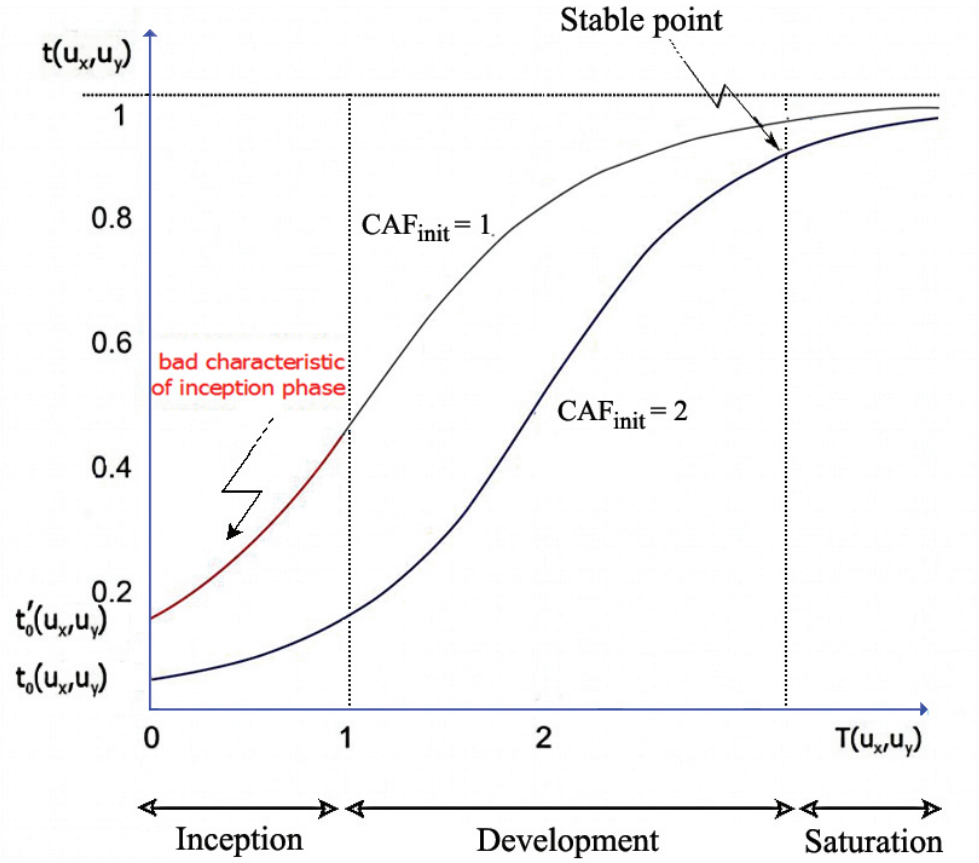

Figure 3.3: The Sigmoid Dependence Functions with Different CAF_{init} Values from Matlab Plotting Tools

- the overall calculation requires some effort (i.e. increasing overhead of the proposed method) because the calculations need to be executed quite often.

Dealing with these drawbacks –especially considering the needed computational effort on mobile devices–, more simple solutions shall be preferred. Linear functions are much more easy to handle and may adapt on long ranges to the sigmoid curves well.

The set of linear curves also show the three separated phases of trust gaining: inception, development and saturation –see [76, 77] for further discussions about these phases– as plotted in Figure 3.4. Several labels are annotated in the figure as described below:

- a: initial trust, which is determined for inception phase;
- c: stable point of trust when saturation phase is reached;
- b: trust-effect-sum of u_x on u_y at the end of inception phase;
- d: trust-effect-sum of u_x on u_y at the beginning of saturation phase.

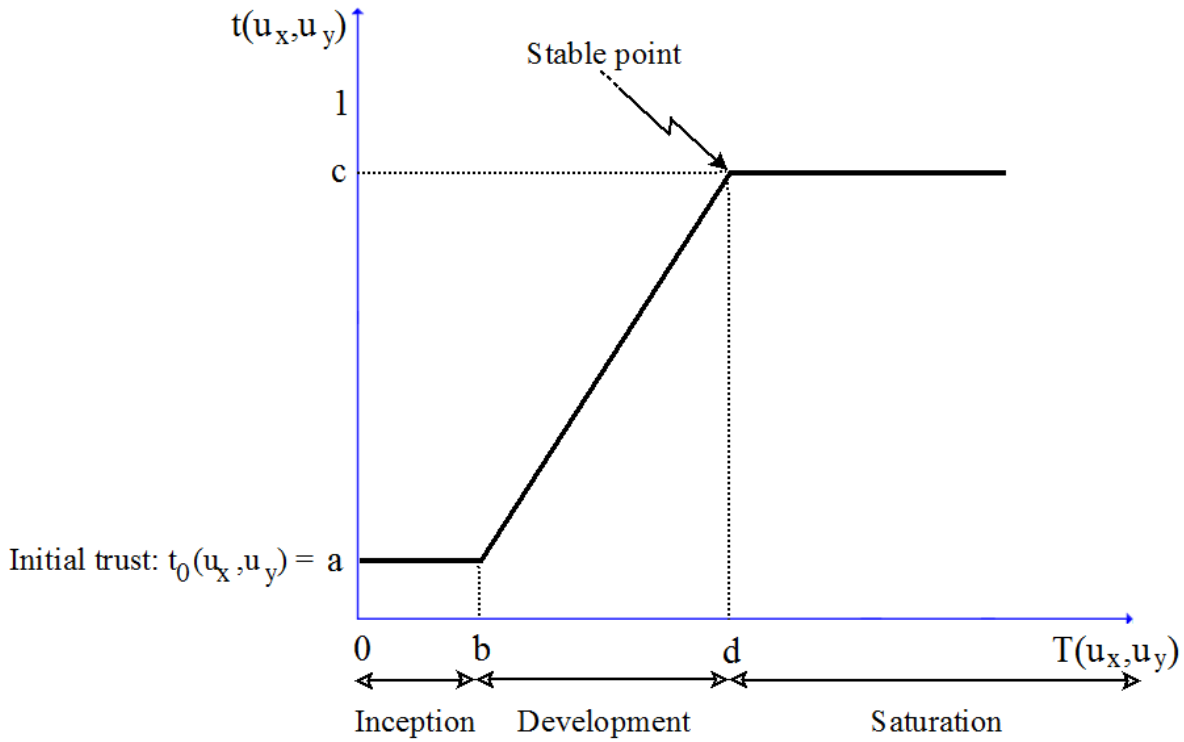

Figure 3.4: Linear-phasing Normalisation Functions

Mathematical, the tripartite shown function might be described by:

$$t(u_x, u_y) = \begin{cases} a, & \text{if } 0 \leq T(u_x, u_y) < b \\ (T(u_x, u_y) - b)\frac{c-a}{d-b} + a, & \text{if } b \leq T(u_x, u_y) < d \\ c, & \text{otherwise} \end{cases} \tag{3.5}$$

The set of linear curves also show the three phases of trust gaining: inception, development and saturation. Finally, it could be stated that the use of linear-phasing functions becomes easier and more flexible in comparison with sigmoid functions.

3.5.3 Negative Trust Signals

So far, only initial trust and a development phase of trust based on positive trust signals have been considered in detail. However, also negative events may affect a user and their impacts are represented by negative trust signals. The handling of negative trust signals needs to be investigated at this point, too.

Therefore, the concept of having an endurance process (hysteresis) could be applied. The introduced endurance process helps the user to ignore several misbehaviours detected. Support of this process is including capabilities of accepting not only reparation of harmful trust signals but also punishment-enabled possibility. In order to model this process, an endurance

parameter with length of ϵ is introduced, describing the range of activities after which a person may consider significant activities to avoid harm to trust. At this point, many subjective ϵ-influencing factors have to be considered like:

- the acceptable number of negative influences and therefore negative trust signal elements as well as the possible importance of their strength;
- the subjective judgement of harm (i.e. amount of danger);
- the history –so far– containing the recent state or phase in the trust development including the recently gained, quantifiable trust;
- the feeling of empathy with the respective partner.

For the sake of simplicity, the first three factors could be adequate for determining the value of ϵ. It is difficult to model the fourth factor.

The impact of negative trust signals significantly depends on the phase in which T_{break} occurs (i.e. the time of the recognition of negative trust signals appears). The phase mostly influences the character of the endurance process, which has the following different mechanisms of coping with punishment and forgiveness:

- **In inception phase:**

  In this phase, only observation, suspicion and discretion among the partners exist and only seldom initial trust overrides this feelings (e.g. in case of love at first sight). Consequently, the occurrences of negative signal elements will cause a catastrophic impact towards the attitude of user to his partner. Obviously, under this abnormal circumstance, most rough reactions occur and usually the entire trust to the partner is destroyed, even initial trust $t_0(u_x, u_y)$ entirely vanishes (i.e. the harshest punishment) and usually there is no chance for any forgiveness even in future.

- **In development phase:**

  In this phase (and saturation phase), an evaluation of the attitude to the partner is already possible by some gained trust due to mutual activities and therefore a measurable cumulated activity factor $T(u_x, u_y)$ above its initial value exists.

  - $T(u_x, u_y)$ is updated as above described and could oscillate by increasing or decreasing its value;
  - but the level of trust is frozen (i.e. remaining its value for a period of time ϵ). After a clear decision on the evaluation of opposite trust signals is made, the trust value is levelled to the value corresponding to the reached cumulated activity factor $T(u_x, u_y)$.

By doing so, punishment and forgiveness are handled in flexible and rational manner following the usual human behaviour as presented in [166].

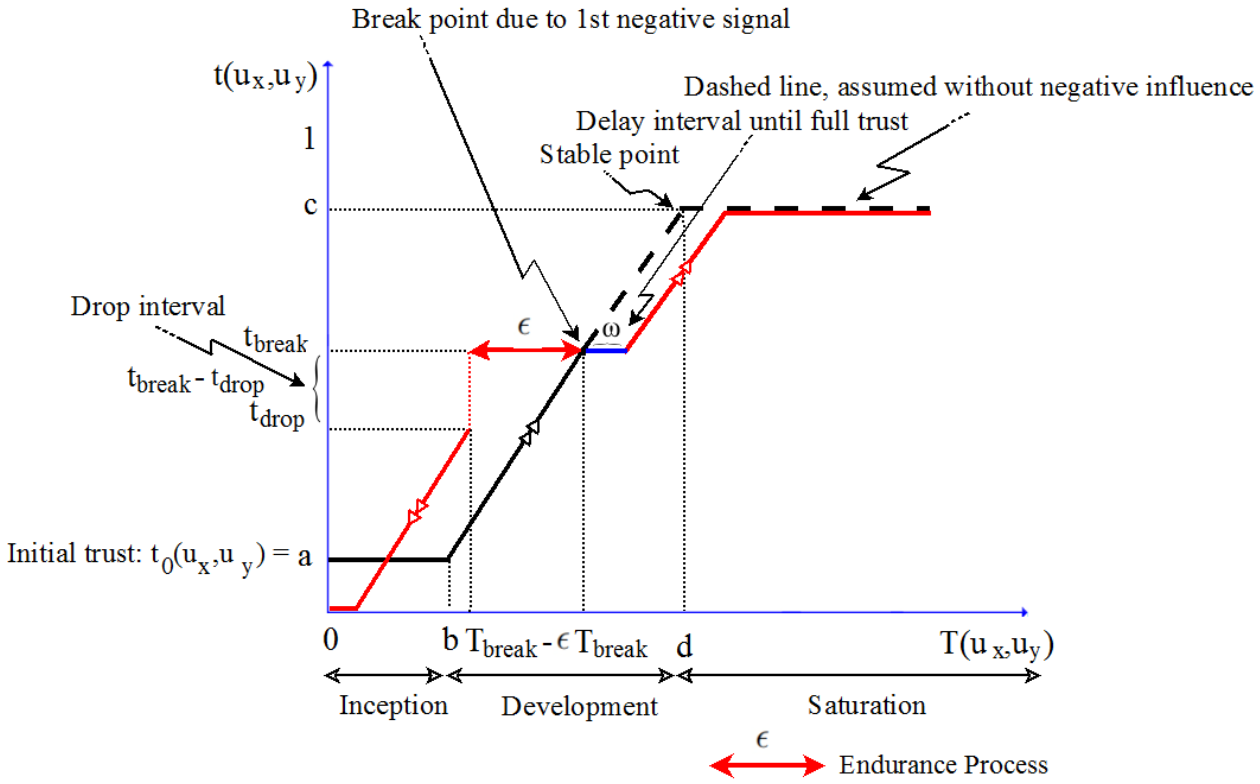

Figure 3.5: Endurance Process of Development Phase

Figure 3.5 shows the above explained process, which can be formally separated into the following four, specific rules after a first negative signal appears at break point:

- *Rule 1:* If $T(u_x, u_y)$ decreases but $T_{break} - \epsilon < T(u_x, u_y) \leq T_{break}$ then $t(u_x, u_y)$ retains its value t_{break}. As described in this model, the robustness of the endurance mechanism alleviates or resists negative trust signals. However, it must be comprehended that trust would not be damaged by only several isolated negative trust signal elements.
  In more complex models, ϵ might be adapted relatively to the already gained level of trust (i.e. the higher the reached trust level with a partner is, the higher the patience with negative influences might be).
- *Rule 2:* If $T(u_x, u_y)$ decreases and $T(u_x, u_y) \leq T_{break} - \epsilon$ –less than utmost of endurance– then the endurance process expires and $t(u_x, u_y)$ immediately drops by $t_{break} - t_{drop}$ like a punishment.
  The effect of punishment is a deterrent against series of undesirable, intentional harming trust signal elements emitted from a partner. A partner must accept to lose significant trust as a consequence of these offences. As an

expectation of punishment, the partner will carry on activities and provide contents with prudence in the future.
Further, the drop interval may be adapted to the moment, when the break happens as well as it depends on the kind of suspicious or harmful activities detected. Since then, the development phase continues starting from the now lower level.

- *Rule 3:* If $T(u_x, u_y)$ increases but $T(u_x, u_y) < T_{break}$ then $t(u_x, u_y)$ maintains its value t_{break}. Partner needs to contribute substantially further positive trust signal elements in order to get through break point.
- *Rule 4:* If $T(u_x, u_y)$ increases and $T(u_x, u_y) \geq T_{break}$ then the current endurance process is interrupted, the negative events are considered to be forgiven after a series of positive activities of repair. Calculation of $t(u_x, u_y)$ starts returning to the normal gaining process when reached higher level of $T(u_x, u_y)$ is obtained. It may delay achieving the saturation phase by an ω interval. Thereof, a little doubt –occurring in period of time ω– remains existing after incurring endurance process.
  The purpose of forgiveness behaviour encourages to maintain positive attitude towards partners after they compensate enough trust-constructive signals.
  The restoration of the development process (i.e. a recovery of trust) again is rewarded to the partner. Differing from the second rule, no positive –however– jump is usually necessary and included in the conceptual design.

At this point, it shall also be mentioned that there are several possibilities for an outlier detection and exception handling, especially in on-line social networks. It is important to recognise and to handle these situations in the right manner:

- Several real situations (also in interdependency with the real-world and its laws, ethics and moral) as lies, cheating and offending posts, causing report-posts and blocking of a user should be appropriately treated. Manifold extremely negative events may even cause the elimination of a partner from the whole system;
- Forgiving behaviours is not synonymous to forgetting. In this sense, a number of subsequent endurance processes need to be recognised and treated in a special manner, because it might help to detect repeated, negative intentions planned on a long term. And it could suggest a respective punishment. Adaptations to T_{break} may be a first, soft consequence;

- Security issues and frauds, like identity theft or multiple identities, shall be considered, detected and handled.

The above-mentioned exceptional cases must be handled following the intentions of the respective users and system policies by special rules. The partners should face with severity of punishment by sustaining ruin of trust. For that, the cumulated activity factor is adjusted to zero (i.e. $T(u_x, u_y) = 0$).

- **In saturation phase:**

If negative signal elements occur when full trust (i.e. stable point) has been already reached, forgiveness undoubtedly becomes easier as well as punishment may be not enforced and further caution might be indicated. In Figure 3.6, the handling of negative activities is similar in development phase with several remarks:

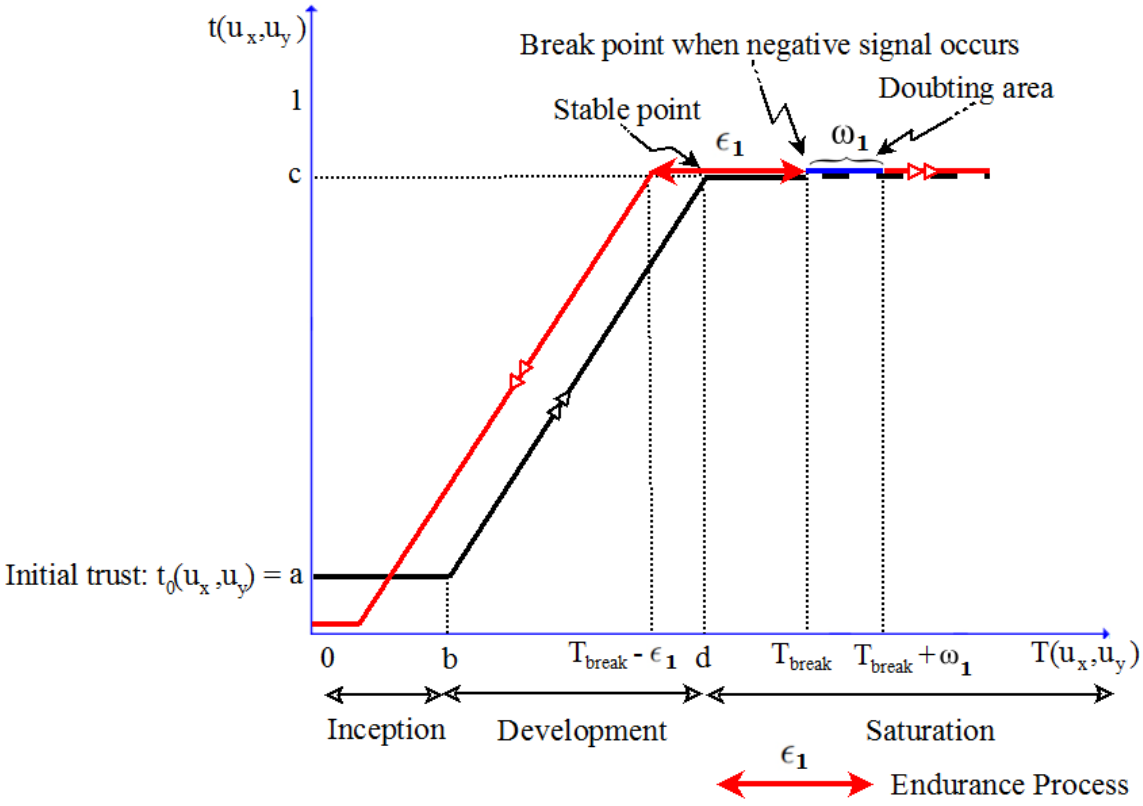

Figure 3.6: Endurance Process of Saturation Phase

- If a negative trust signal emerges, the endurance times starts. The endurance threshold parameter ϵ_1 has a usually higher value than that one in the development phase (i.e. $\epsilon_1 > \epsilon$) as tacit consideration to allow an easier forgiveness to well-trusted people and/or good friends.

- Differing from the development phase, the trust devolution is more likely an erosion process instead of an drastic drop as a punishment (except for heavy harm or dangerous cases). In such a manner, trust is kept on the full level at a stable point for the interval given by ϵ_1. If the cumulated activity factor continues reducing and its value is less than $T(u_x, u_y) \leq T_{break} - \epsilon_1$, a trust reducing-process starts and Figure 3.6 shows this process. In this case, trust may reduce until the level of 0, also the trust reduction follows a stronger decreasing slope than the trust development as described above.
- Leaving the 'doubting blue-coloured area' with length of ω_1, it indicates that when $T(u_x, u_y)$ is greater than $T_{break} + \omega_1$, a complete forgiveness is given. Once full trust have been achieved, the suspicion may take longer time (i.e. $\omega_1 \geq \omega$).
- A user –of course– prioritises a partner, who has been obtained full trust. It is not modelled that the time, two users know each other. It may play an important role, especially if both partners are fully trusted each other.
- Especially if high values of the cumulated activity factor $T(u_x, u_y)$ are reached, it is clear that the user knows the partner well. $T(u_x, u_y)$ might be so high that no endurance needs to be given to the partner.

Hence, for the reason of simplicity and uniform handling, the endurance process is established for the case negative signal occurring in saturation phase.

The foregoing considerations refine the modelling of trust and allow a more fine-grained prediction of trustworthiness in a recommendation system.

3.6 Summary

In this chapter, the connections between user activities with special respect to activities and contents in on-line social networks and trust have been described. Positive as well as negative influences have been considered in detail. Also, it was worked out that a lot of subjective parameters (like given initial trust) must be considered and derived for each user. The consideration of trust-supporting as well as trust-destroying activities have resulted in their modelling within a cumulated activity factor, which is built optionally during a time window with a determinable length.

Later on, it was explained that the real trust feeling and therefore also the intended pairwise trust can be derived from the cumulated activity factor following an S-shape like/or

sigmoid function. It was worked out that there are three phases of trust building, namely the inception, development and saturation phase. In order to make the model clearly and easily understandable, a linear approximation of the S-shape like/or sigmoid functional dependency has been suggested and described, which avoids an explosion of the system's complexity.

For the first time, the effect of received negative trust signals has been investigated, formalised and included in that –simplified, linear– model.

The presented modelling decisions and settings give an extended possibility for a more fined-grained characterisation and parameterisation of the model and make it more similar to the human behaviour.

Chapter 4

Decentralised Trustworthiness Calculation

4.1 Overview and Main Ideas

In the previous chapter, the first step of a new methodological approach to calculate recommendation on trustworthiness in a decentralised system was presented by deriving a pairwise trust depending on user activities and content distributed in an on-line social network.

In a second step, those pairwise trust evaluations must be considered in the context of the (on-line social) network of communications as well as business and financial activities. As a result, a global trustworthiness value of the user shall be calculated, which is called the user's $TrustScore$. A special difficulty in doing so is the requirement to do those calculations in a fully decentralised manner, what also supports an implementation of the method in an autonomously working P2P-system while not relying on any centralised content/on-line network system provider.

The author will show that random walks carried out by random walkers can be utilised to solve this task. Indeed, the results of [118] can be directly modified and applied for this work.

As a first step, a network is considered, in which the user builds the set of nodes and edges induced by any communications, business or financial relations according to the possibilities provided by an on-line or real social network. In this case, it is expected (following the state of the art on social network) that (without the need of any additional functionalities) a connected network is constructed, which exhibits all discussed small-world properties. In order to handle trust and trustworthiness topics, edge weights shall be set corresponding to the determined pairwise trust values, derived using the methodology of the previous chapter 3. Consequently, a structure constrains are defined for the possible calculations concerning analysis of that complex structure.

In a seamless way, for each node, a global trustworthiness calculation shall be determined. At this point, the terms trust and trustworthiness must be strictly separated. In a model or a computer system, all activities included may be observed and evaluated and respective trust signals might be derived from it. Following the investigated knowledge about trust building and destroying processes, a rough estimation can be computed for what a user of the system might feel (note that this estimation may be valid even for one user only, since another one may assess one and the same situation due to his personal background in a completely different manner). In such a manner, any numeric value calculated, may only be a general mean experience of the trust feeling of an average system user. Therefore, the global trustworthiness value counted in a system may be only an approximate estimation or hint relatively to other hints, whether a user might be trustworthy or not. The feeling of trust –again– may only be built in the brain of the user after experiences from a long lasting cooperation with the respective partner have been made.

In order to avoid any misunderstanding or mismatching of terms, it has been decided to introduce the term $TrustScore$ for the calculated recommendation on trustworthiness for the system's users.

TrustScore value (Definition 14.) *(shortly TS) is a recommendation on trustworthiness achieved by implementing the $TrustScore$ method. It shall be a value not solely depending on a special, partial set of trust relations but an overall value derived from the (complex) network structure of interpersonal relations with an extendible set of various, influencing factors.*

The operational mechanism of the $TrustScore$-distributed calculation by random walks will be elaborated in sequential sections.

4.2 Methodology for Calculating TrustScore

In the previous chapter, a network of users (nodes) and weights of edges derived from activities and contents evaluations has been described. In an uninterrupted manner, the calculation of a $TrustScore$ of a node u_x is now a calculation of the overall trust evaluation, all predecessor nodes of u_x may have. Hereby, it shall play –of course– a role, how much those predecessor nodes are trusted in the whole system (e.g. a high trustworthiness for a node from a user which is known as liar or cheating person is –of course– not as valuable as the same evaluation from a well situated other person).

By considering this description, the similarity to the calculation of PageRank [94] or NodeRank in [118] is directly apparent. Consequently, the question of an adaptation of this well-known and established method is coming up, especially since another advantage of it is given by its fully decentralised-working calculation by a random walk approach.

While PageRank reflects –as intended for the search engines purpose– only topological

aspects of nodes embedded into (web-) graphs, [118] includes other factors in the NodeRank generation derived –as in case of $TrustScore$– from graphs with weighted edges, influencing the role of a node in the system.

Originally, in [94], the transition probability of a random walker from a node u_x to one of its neighbour nodes u_y is given by:

$$p(u_x, u_y) = \frac{1}{|N_{(u_x)}|}, \tag{4.1}$$

where $N_{(u_x)}$ represents the set of neighbour nodes of u_x. It shall be repeatedly mentioned that only topological properties of the underlying graph influences the PageRank. Therefore, a neighbouring node u_y of node u_x can be chosen randomly in a uniform manner. The respective transition probability metric for all entries $p(u_x, u_y)$ has some standard key properties:

- *Property (a):* $p(u_x, u_y) \geq 0$
- *Property (b):* $\sum_{u_y \in N_{(u_x)}} p(u_x, u_y) = 1$

In order to obtain a recommendation on trustworthiness for each node in a (complex) network structure, all pairwise trust connections $t(u_x, u_y)$ must be computed in the $TrustScore$ calculation.

The transition probability of a random walker to move from u_x to u_y must be therefore adapted to the respective intensity of trust given by the pairwise trust $t(u_x, u_y)$ assigned to each edge. Consequently, the calculation of the transition probability of a random walker from node u_x to u_y (i.e. $p(u_x, u_y)$) must be changed depending on $t(u_x, u_y)$ for all leaving edges from u_x. Hence, the transition probability can be straightforwardly defined by:

$$p(u_x, u_y) = \frac{t(u_x, u_y)}{\sum_{\forall u_z \in N^+_{(u_x)}} t(u_x, u_z)}, \tag{4.2}$$

where $N^+_{(u_x)}$ is set of out-going neighbour nodes of node u_x and $\sum_{\forall u_z \in N^+_{(u_x)}} p(u_x, u_z) = 1$.

An example for this calculation is given in Figure 4.1. It illustrates an example of a structure with 5 nodes and trust annotations associated to each edge by $(u_x, u_1) = 0.8$; $(u_x, u_2) = 0.95$; $(u_x, u_3) = 0.4$ and $(u_x, u_4) = 0.6$. The transition probabilities from node u_x to its neighbours nodes are calculated and applying the previous formula. As a result, transition probabilities from u_x to its neighbours are obtained by $p(u_x, u_1) = 0.290$; $p(u_x, u_2) = 0.345$; $p(u_x, u_3) = 0.145$ and $p(u_x, u_4) = 0.218$.

Consequently, among the $N^+_{(u_x)}$ neighbouring nodes of u_x, node u_y is chosen non-uniformly but still at random as a target to move to from node u_x. It is easy to be seen that nodes, which are evaluated by its predecessors with a high trust estimation, are now preferred targets for

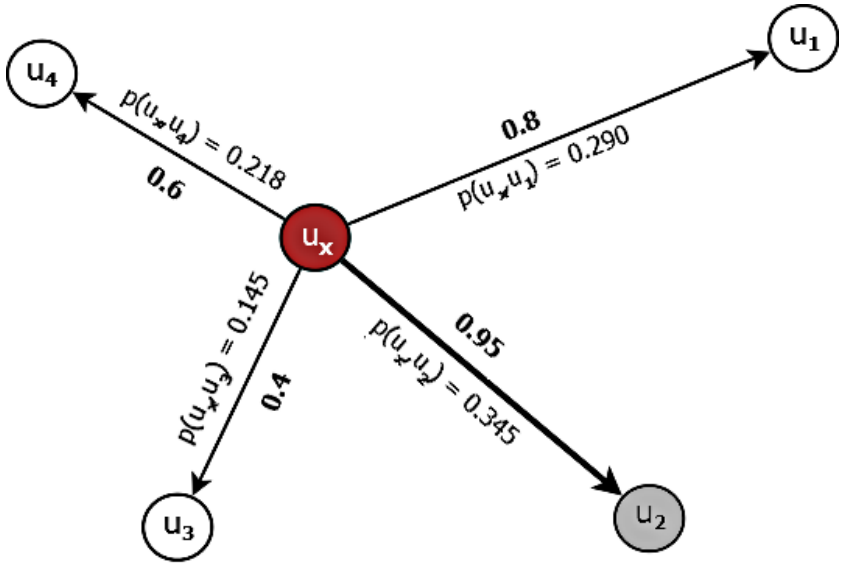

Figure 4.1: Artificial Example Calculating Transition Probabilities

the random walker. In the example, a random walker staying at node u_x is likely to prefer the grey colour-coded node u_2, which exhibits the maximal transition probability of 0.345 among all others.

The global trustworthiness value is now easy to calculate and can be obtained faster by using k random walkers. If $k \in \mathbf{N}$ random walkers are used, then the TS of user u_x at a specific time τ can be calculated by combining all arbitrary walks under the assumption of the superposition of all calculations and decision processes. It is expected that hereby a faster calculation (convergence) may be reached.

The respective calculation formula adapted from [118] is given by:

$$TS_{u_x}(\tau) = \frac{\sum_{\forall k} f_{u_{x_k}}(\tau)}{\sum\limits_{\forall k} step_k(\tau)} = \frac{f_{u_x}(\tau)}{\sum\limits_{\forall k} step_k(\tau)}, \tag{4.3}$$

where $f_{u_{x_k}}(\tau)$ is the number of all visits of the k-th random walker on u_x in all its $step_k(\tau)$ –steps until time τ– and $f_{u_x}(\tau)$ is the number of all visits of all random walkers on u_x.

According to E.q 4.3, the $TrustScore$ value of node u_x changes over time τ by every further visit of a random walker. The stability of that value over all nodes needs a criterion that not only controls the convergence condition (i.e. determining the time τ to terminate the process) but which assures that the TSs of all nodes are reliably calculated such that an acceptable output of global trustworthiness for all nodes can be achieved.

In fact, the proposed method $TrustScore$ including its later discussed implementation are showing crucial differences compared to the approach presented by PageRank and NodeRank as [94, 118]:

- the links are weighted by trust relations;
- differing to PageRank, a fully decentralised processing on the basis of random walkers is carried out;
- differing to the NodeRank calculation, a few nodes will be elected in a decentralised manner (using classical algorithms) to set up and control the population of random walkers. Its size must depend on the size of the community as well as the dynamics of the weight values via trust evaluations, which are not present in [118];
- due to its importance and sensitivity, a special protocol for the random walks must be implemented to protect the obtained values against frauds and manipulations, there was no need for doing so in [94, 118].

To complete the presented approach, some remarks on the convergence and normalisation of the obtained TS-values are needed. This will be discussed in the subsequent two sections.

4.3 Convergence of TrustScore

Due to the permanent movements of random walkers around the network, the $TrustScore$ values are continuously calculated. At any time, new nodes may change the network structure or existing ones may leave it. Also, the estimated pairwise trust value and therefore the transition probabilities for the random walkers may be changed at any time and without any prior notice. This is –of course– no real problem for a fully decentralised random walker based calculation.

Nevertheless, convergence conditions are needed to be defined and subsequent experiments must clarify at least for the statical case:

- does a convergent behaviour exist?
- how long does it take after the start of the calculation, until reliable TS-values are calculated (compared to approx. 100 iterations in the centralised case)?
- how long does it take to re-calculate TS in case a small set of nodes is added to the network or removed?
- how long does it take to adapt to changes which are made on the network weights (pairwise trust values)?

First of all, to consider convergence and to evaluate the above listed topics, a convergence criterion must be defined.

Therefore, a sequence of calculated values $x(\tau) = \{x_1, x_2, ...\}$ obtained at time $= \tau_1, \tau_2, ...$ is considered under the assumption that the system does not change its state for a longer time.

Usually it is said that the value of $x(\tau)$ converges, if there is a fixed, small constant χ and a time τ_i, after which

$$|x_{i+1} - x_i| < \chi,$$

whereby τ_i is called the convergence time. Reaching this state may terminate the $TrustScore$ calculation process. However, the determination of this point may be difficult, since the process may diverge from the convergence condition after reaching it for one time or a short time period. Therefore, it is useful to state convergence after the convergence criterion is kept for a given period, only.

However, concrete experiments must justify the convergence of the $TrustScore$ calculation, its correctness as well as deliver hints for a suitable determination of χ; this will be a subject to a detailed consideration in chapter 5.

4.4 Estimating the Network Size

Calculating $TrustScore$ as described in section 4.2 may result in an incomparable range of TS-values obtained from different networks. The reason is quite simple, since the obtained number of visiting a node by random walkers also –if not mostly– depends on the size of the graph (i.e. its number of nodes). In such a manner, the obtained TS-values could be compared only in a relative manner (i.e. with nodes of the same graph at the same time).

As a substitution, a mean value $\overline{TS}$ could be derived from a subset of nodes in the network. It is known from statistics that a relatively low number of randomly chosen nodes is needed only to obtain a more or less stable mean value. After that, a given node can be roughly classified and recommended as (very) trustworthy, normal (confused) or less trustworthy by the following rules:

- *Normal zone*:
  If TS of X is equal $\overline{TS}$ then X is a normal, average node.
- *Trustworthy zone*:
  If TS of X is greater than $\overline{TS}$ then X is a trustworthy node.
- *Untrusted zone*:
  X is a untrustworthy (or less trustworthy) node.

However, this approach would not be sufficient and would not allow for a comparison of trust from different networks.

In the already cited, centralised PageRank model [94], a simple logarithmic function could assist in easily normalising the obtained value of PageRank $pr(u)$ as proposed in [16]:

$$PR(u) = v + log_{10}pr(u), \tag{4.4}$$

where $pr(u)$ is a value calculated by the PageRank algorithm for page u and a constant v (a typical value of v is 11) defines a cut-off value.

Based on the results obtained from this equation, Google could suggest those pages u which have $pr(u) > 10^{-v}$ or which constitute the top results, like the 10% top-level pages for each search. The normalised value $PR(u)$ gives a global scale evaluating the quality of page u in comparison with the whole set of pages in the WWW network.

Inversely, assessing a node's quality is very difficult in the decentralised scenario of PageRank. This applies to the described $TrustScore$ estimation as well, since so far the $TrustScore$ values are not specified on a fixed, concrete scale. Therefore, as a big challenge, a decentralised normalisation must be defined, which removes the dependency of TS-values from the network size.

As it is easy to be seen that the most wanted parameter for doing so is the network size itself. It may vary over time, but usually do not show big, sudden jumps. However, it may be hard to calculate it by any algorithm and especially any locally working algorithm, which can never oversee or control the whole network or even bigger parts.

Nevertheless, with this knowledge on $\overline{TS}$ and [118], another approach may be suggested. As it was shown, $\overline{TS}$ can be approximated from a random walk by building the mean value of a set of TS values randomly collected in the network and a sufficiently high value of k by:

$$\overline{TS}_{sample} = \frac{\sum_{i=1}^{k} TS(i)}{k} \tag{4.5}$$

where $\overline{TS}_{sample}$ is average $TrustScore$ value of all nodes in sample group.

Since it is known that $\overline{TS}$ is also the average visiting probability of all nodes $\overline{TS}$ can be also approximated by:

$$\overline{TS} \approx \overline{TS}_{sample} = \frac{1}{n}, \tag{4.6}$$

where n is the wanted network size. It can, therefore, easily be calculated:

$$n \approx \frac{1}{\overline{TS}_{sample}}. \tag{4.7}$$

As a condition for the selection of k, the convergence of the possible derivation of $\overline{TS}_{sample}$ shall be used (i.e. k shall have sufficiently high value such that a larger k does not generate significantly different values for $\overline{TS}_{sample}$).

If the obtained network size n is multiplied with the concrete $TS(i)$ value of any node i, nodes with a trustworthiness of normal node will exhibit obtained TS-values around 1, while higher and lower trustworthiness of correspondingly trustworthy and untrustworthy nodes is expressed by obtained TS-values significantly higher or lower than 1, respectively. Mistakes made in the network size calculation may not significantly falsify this calculation too much, especially if the network is big.

Using this normalisation, $TrustScore$ values become not only comparable globally in a single network by their absolute values but also among different networks. Detailed, empiric simulations using the above derived theory are presented in the following experimental sections 5.3.2.

4.5 Summary

The consecutive chapters 3 and 4 presented a complete methodology to evaluate the pairwise trust obtained from any interactions of the users in a network and to calculate global trustworthiness values, so-called $TrustScore$, for each user.

This calculation is carried out in a fully decentralised manner by a population of random walkers, which uses the connected, small-world network built by users and their communications, business as well as financial activities.

It was justified that the respective calculation process will converge. Also, a simply applicable normalisation has been presented, which bases on a statistic estimation of the network size, again performed by the random walks approach.

While –so far– mostly the theory of the $TrustScore$ approach has been worked out, the following chapter is devoted to its empiric investigation by a set of simulations.

Chapter 5

Empiric, Experimental Results

5.1 Introduction

In previous chapters, the theoretical foundation and methodology of the *TrustScore* method was described. However, this method still needs to be justified by experimental results.

The *TrustScore* method bases on the utilisation of random walkers and is a fully decentralised method working without any central control or the possibility to control the entire system. Therefore, experiments must reveal its ability to perform well in networks with a high dynamic character and a changing number of participant. It is the ultimate goal of these experiments to test and validate the correctness of the proposed *TrustScore* method regarding its different aspects.

For this purpose, a detailed study was conducted on different datasets obtained from both real networks and automatically-generated test data. Real network scenarios are extracted from two studies: *Advogato* [1] and *Epinions* [2]. Details of these networks will be presented in the respective subsection 5.2.1. In addition, stochastic structural and topological models of the underlying networks known from the cited literature in subsection 2.4.1 and trust-generating techniques by Richardson in subsection 2.3.3 will support the automatical generation of the simulation environment.

To obtain this goal, the experiments have to deal with the following tasks:

1. validating that random walks are a suitable tool to calculate a converging value of *TrustScore* of the nodes in complex networks;

2. confirming a possible estimation of the size of a network by random walks in order to be able to normalise the *TrustScore* value into a standardised range $[0, 1]$;

[1] *www.advogato.org*
[2] *www.epinions.com*

3. considering the distribution of $TrustScore$ value. Results of this task contribute more knowledge about the characteristics of obtained $TrustScore$ values;

4. observing the convergence time in a scalable network. Since the sizes of the network influences the convergence time of the method, the dependency of the convergence time depending on the network size is an important parameter to estimate the practicability of the developed method;

5. finding a correlation between the number of random walkers and the convergence time. Since the convergence time of the method is a crucial value, any methods to shorten it may significantly increase performance and acceptance;

6. investigating the determination of the $TrustScore$ values regarding their stability in a automatically-generated network with a fixed size. As a result, the method's practicability shall be demonstrated once more;

7. observing the re-convergence behaviour if the size of networks changes;

8. exploring the changes in the $TrustScore$ value of a given node, if both the number of neighbours and the weight of their connections to that node is changed. Besides the re-convergence, also the influence of neighbours and their trust evaluation shall be investigated;

9. studying the effect of the consideration of trust on the properties of the whole social network structure. This additional work is presented in the separated section 5.4 due to its importance. It shall be shown that the consideration of the trust supports the building of small-worlds structures, namely supports the formation of clusters and an average short path length (instead a sometimes assumed about network connectivity).

Before the presentation of the experimental results and their consequences is given, first of all, the simulation environment and the experimental set up is presented in the next section.

5.2 Simulation Environment

5.2.1 Experimental Setup

Due to cost reasons and a missing access to real social network system environments, a simulative justification of correct functionality and practicability of $TrustScore$ method must be given.

Therefore, two bigger datasets could be obtained from real social networking. In this thesis, the following on-line available datasets from the Stanford Large Network Dataset Collection [3] by Jure Leskovec from the University of Stanford have been used:

- *Advogato* with 6,541 nodes and 51,127 edges
  Advogato is a well-known dataset, which has been extracted from an on-line community platform devoted to *developers of free software*. Present trust relations in this network (i.e. so-called "certifications") consist of three different levels of discrete values and labelled corresponding to 0.6 (*apprentice*), 0.8 (*journeyer*) and 1.0 (*master*).

- *Epinions* with 75,879 nodes and 508,837 edges
  Epinions dataset is a who-trust-whom on-line social network belonging to the genres of *general consumer review sites*. All the trust binary relationships are simply assigned either the value 1 corresponding to 'trust' or 0 corresponding to 'no trust' (the trust is not present).

For experiments, either one of the above network data (indicated by their name) or synthetically generated (indicated by the generation information, preferably its size) are used.

The automatically-generated data bases on structural characteristics of real data and data-generating laws described in the subsections 2.3.3 and 2.4.1. Although these networks and data are artificial, a lot of problems can be avoided by using them:

- it is often not easy to collect any kind of datasets, even just small parts, from real-world networks, especially to interaction protocols is really challenging, since special software and permissions of users are needed;

- real-world datasets are noisy and not always reliable and offer properties of a good, representative sample;

- in the majority of cases, the complete analytic dataset is typically not available to researchers, primarily due to privacy concerns. Data retrieval is often controlled (enforced access limitations) by the procedures of service providers ensuring privacy policies;

- it assists in achieving both diverse sources of data and preventing any bias, caused by on-line available datasets;

[3] *snap.stanford.edu/data/*

- in some cases, the collection and processing of a full data sets is too expensive (money and time) simply due to their size.

The approach of using automatically-generated datasets could be a solution for these obstacles and limitations caused by technical circumstances. Usually, a network with distinct parameters using the $Watts - Strogatz - Method$ (generating a ring lattice with n elements, adding chords to the $k = 6$ nearest neighbours as well as having an edge re-assignment probability p of 0.5) is constructed. Then, if needed, trust relationships among users are assigned easily and straightforwardly by the *Richardson* approach.

As a consequence, different and sufficient network environments for the entire set for experiments are provided, which also reflect the situation in real on-line social networks.

5.2.2 Programming of the Simulations

Programming works are accomplished using Java JDK 1.6 with Eclipse IDE 4.6.1 Neon. Experiments were conducted using an unlimited number of possible threads supported by the library in the package *com.isaacdooley.dagexecutor.DAG* [167].

In the simulation, one thread is used to represent each node. Mostly, it is the task of the nodes to simulate a set of interaction activities (if needed in the experiments) and to wait for the arrival of a random walker. When a random walker arrives, the needed data processing is started as described in chapter 3 and 4, the $TrustScore$ values are calculated and for follow-up processing logged in a file protocol. Then, the updated random walker is send to its next destination, determined randomly from the set of neighbours, following the probability distribution of the assigned pairwise trust values. By doing so, the degree of the parallel work mostly depends on the number of random walkers.

The simulation also offers the possibility to oversee and control the whole system, what is difficult or impossible in reality. Therefore, data collection and post-processing of the obtained simulation data from the log-file can be carried out more easily in a centralised manner, what also includes the consideration of convergence criterion as well as time control to reach convergence. Although a decentralisation of data was mostly applied in this programming model, for the sake of simplicity, also the information of the transition probability matrix was organised globally. For the memory handling and control of big real-world datasets from *Advogato* and *Epinions*, a sparse structure was utilised by a storage in centralised matrices.

The experiments were performed on the Lynx CALLEO High-Performance Server 2850 of the Department of Communication Networks of the University of Hagen using an Ubuntu 14.04 operating system. Two servers were involved in the computations:

- *Server 1:* having an 8xAMD@ Opteron^{TM} Processor 16-Core 6272 (2.1 GHz, 80W) with 32x4 GB DDR3 SDRAM, 1600 MHz and 4x500 GB of memory.
- *Server 2:* with a similar configuration as server 1 except for capacity of SDRAM (24x4+8x8) GBDDR3 SDRAM 1600 MHz was used.

Using the above explained settings, experiments were conducted and the delivered results will be described and discussed in the following sections.

5.3 Experimental Results and Discussion

5.3.1 Features of the Used Complex Structures

For an overview, at first, the statistical description of features and topological information of the used complex network structures are given in Table 5.1.

The used networks are divided into automatically-generated and real-world sampled networks. In general, these automatically-generated networks exhibit an average node degree around 12. Further, the average shortest path length and average clustering coefficient are 3.63 and 7.89×10^{-2} respectively. Mutual edges indicate that there is a trust relation between A and B as well as from B to A also having assigned a trust value. The percentage of such mutual edges in the network is around 34.44%.

Besides, the real-world datasets of *Advogato* and *Epinions* datasets have been used. Their edge weight is the respective trust value. The *Advogato* dataset had an average degree of approximately 15.63, the average shortest path length of 3.29 and the average clustering coefficient of 9.22×10^{-2}. The percentage of mutual edges is 38.5%.

The network of *Epinions* is a relatively massive one with its 75,879 nodes and 508,837 edges. It exhibits an average degree of approximately 13.4. The mean shortest path length and average clustering coefficient are correspondingly 4.4 and 6.57×10^{-2}. The percentage of mutual edges is 40.5%.

As a very first result, it may be stated that the different networks all show the small-world property. Also having similar backgrounds and sources (including the automatic generation), the average shortest path length, clustering coefficient and percentage of mutual edges are quite similar. This also proves the quality of the generation of synthetic network structures.

# **Nodes** (users)	# **Edges** (trusts)	**Average Degree** (edges/node)	**Mean Shortest Path Length** (edges)	**Average Cluster Coefficient** ($\times 10^{-2}$)	**Mutual Edges** (%)	**Diameter** (edges)
Automatically-generated Networks						
1,000	5,069	10.14	2.46	8.22	25.28	7
5,000	24,966	11.99	3.54	7.74	40.25	10
10,000	50,049	10.01	4.28	7.75	39.23	9
15,000	90,021	12.00	3.58	7.92	35.29	10
20,000	100,021	10.00	4.02	7.98	38.18	7
25,000	225,097	18.01	3.89	7.67	28.43	12
Average of Above Values (under row)						
		12.02	3.63	7.89	34.44	9.16
Real-world Dataset Networks						
Advogato *advogato.tar.bz2 (195.18 KiB)*						
6,541	51,127	15.63	3.29	9.22	38.5	9
Epinions *soc-Epinions1.tar.bz2 (1.64 MiB)*						
75,879	508,837	13.4	4.4	6.57	40.5	15

Table 5.1: Experimental Network Details and its Features

5.3.2 Results and Discussion

In the following section, the experimental results of the 9 simulations made are described. For a simple reading, the main goal, a short description of the experiment as well as its major outcomes are –uniformly– given for all of them.

Experiment 01

Goal: validating that random walks are a suitable tool to calculate a converging value of $TrustScore$ of the nodes in complex networks.
Description: At the beginning, the classic $PageRank$ (PR) algorithm runs on the network with 200 nodes. After that, the random walks-based method (RW) is executed on the same weighted network. The overall difference between both methods is observed over time (i.e. over the number of iterations).
Results:

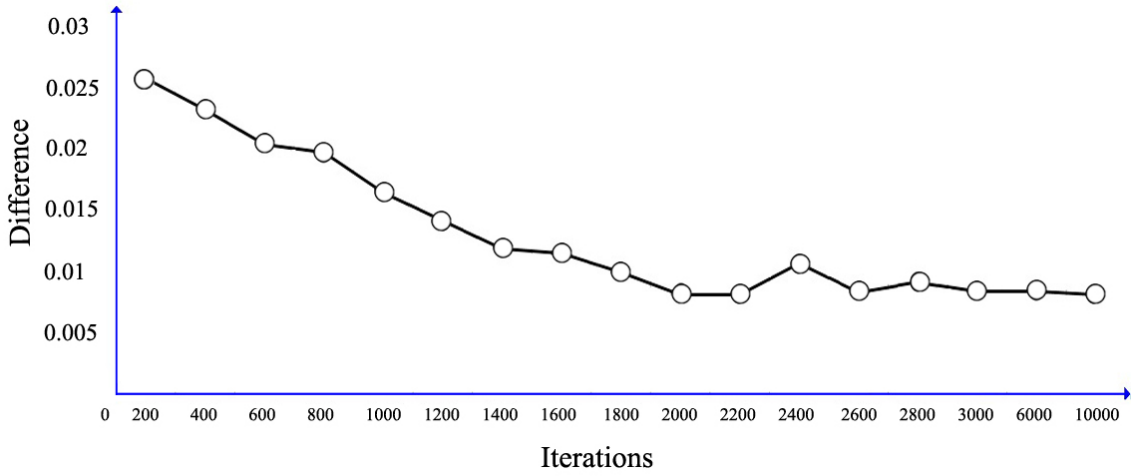

Figure 5.1: Difference following the Time

The difference between the PR and RW values is calculated as a sum of differences from all nodes of the network by the following equation:

$$\text{Difference}(\tau) = \sum_{i=1}^{n} \mid PR_i - RW_i(\tau) \mid, \tag{5.1}$$

where τ indicates the number of iterations, $RW_i(\tau)$ is the RW-based value for node i at the iteration round τ, PR_i is PageRank of node i.

Figure 5.1 shows the obtained difference. As it can be seen, there is a descending difference over time indicating a convergence. After $\tau \geq 2.000$, the difference is negligible and under around 0.008. In other words, the random walks-based method converges after using a

significant number of iterations to the value of the PageRank algorithm. However, the number of needed iterations is quite high such that any mechanisms improving the convergence speed shall be investigated.

Experiment 02

Goal: confirming a possible estimation of size of a network by a random walk. It assists in normalising the $TrustScore$ value into a standardised range $[0, 1]$.
Description: The average $\overline{TS}_{sample}$ shall approximate $\frac{1}{n}$ (see Eq. 4.6). This relation is analysed to determine the estimated size of the network depending on the sample size afterwards.
Results:

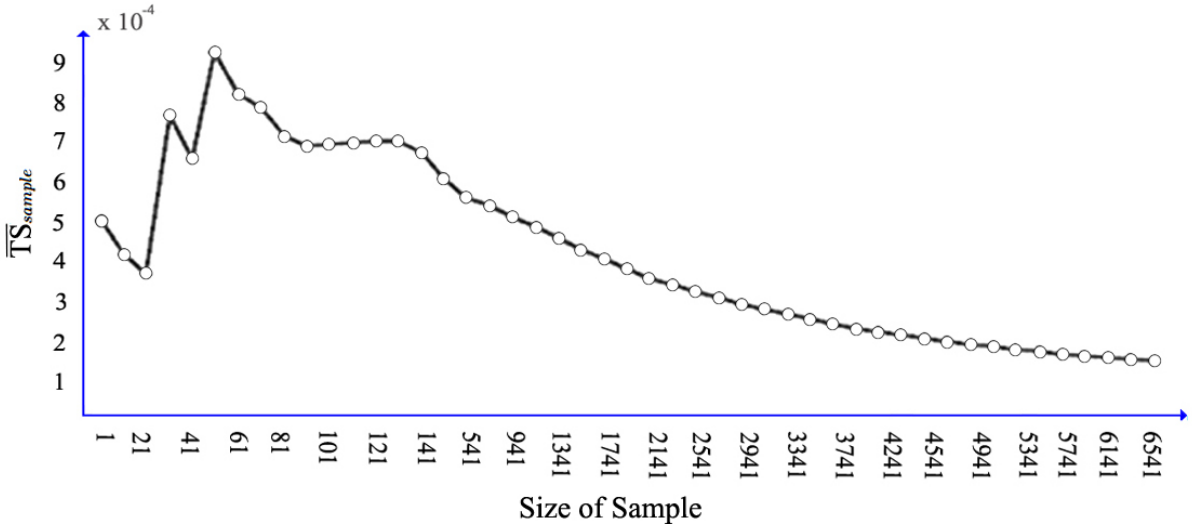

Figure 5.2: Different Sample Sizes for Trust Network *Advogato*

As in Figure 5.2, $\overline{TS}_{sample}$ reduces gradually from sample sizes over approximately 200 nodes. As it is to be seen that it is quite hard to reach a stable, converging value of $\overline{TS}_{sample}$ with a small sample size for the needed, subsequent calculation of the network size by Eq. 4.7. However, since big sample sizes can be collected in a successive manner by a few (additional) random walkers, this might not be a real problem.

Experiment 03

Goal: considering the distribution of $TrustScore$ value.
Description: Implementing the $TrustScore$ method on six different automatically-generated networks with sizes of $\{1000, 5000, 10000, 15000, 20000, 25000\}$ nodes and a real-world network *Advogato* (6541 nodes). Plotting the distribution of $TrustScore$ values in order to observe the characteristics of the distribution.

Results:

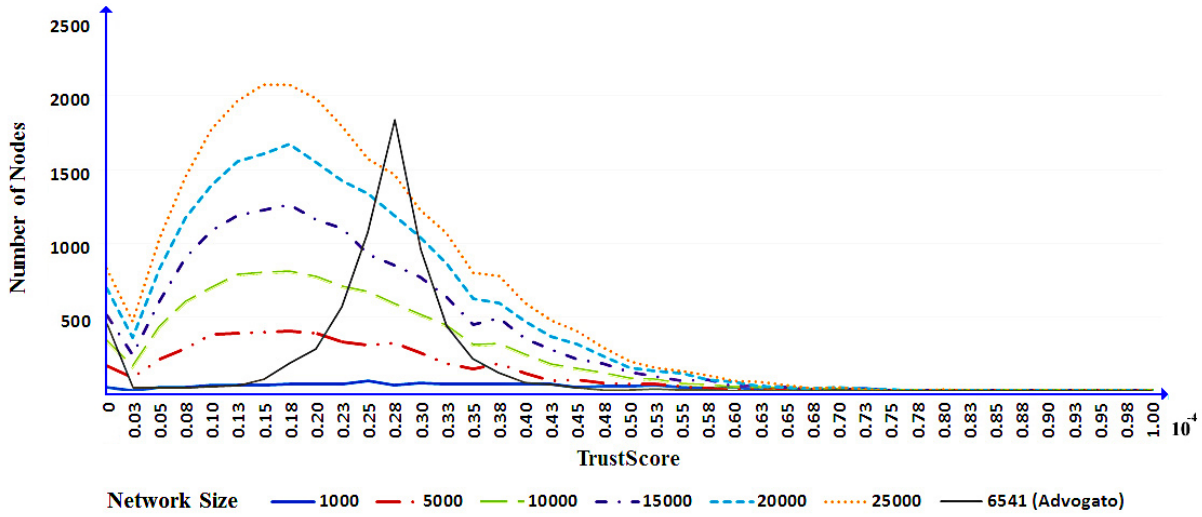

Figure 5.3: TrustScore Distribution in Different Sized Networks

Consequently, fine grained, distinguishable $TrustScore$ are calculated for different nodes in complex network structures. Further, many nodes with an average $TrustScore$ are obtained while higher $TrutScore$ values are really seldom. That corresponds to experience of humans. That is one person maybe have several friends to trust but almost strangers.

Consequently, the results in Figure 5.3 reveal that independent on network size, the distribution of $TrustScore$ values follows a Gaussian distribution. In the case of five automatically-generated networks, it can be seen that the highest density of nodes (mean of Gaussian distribution) was obtained at around 0.20×10^{-4}. There seems to be no influence of network size to the characteristics of the Gaussian distribution.

Judging from statistic data of the *Advogato* network, in Figure 5.3, a Gaussian distribution was preserved, the mean is located at around 0.28×10^{-4}. Comparing the characteristics of the Gaussian distribution of the two kinds of networks, it was recognised that:

- the means of the Gaussian distribution are different. In the case of *Advogato*, the value is significantly greater than for the other cases;
- there is a low standard deviation in case of the *Advogato* network, indicating that the number of nodes tends to have a $TrustScore$ value closer to the mean value.

In the detected Gaussian distribution, most-frequent $TrustScore$ values are clustered around the mean and fall off smoothly on both sides of it. It is assumed that due to the diverse and random assignment of trust values in automatically-generated networks, the standard deviation of the Gaussian distribution on these networks have higher values in comparison with the *Advogato* network. It can be concluded that the distribution is differentiated than in the *Advogato* network mostly because it has discrete trust values at 3 levels (0.6, 0.8 and 1).

Experiment 04

Goal: observing the convergence time depending on the size of the network
Description: In this simulation, the impact of different network sizes on the number of needed iterations to obtain stable values is studied. For that, automatically-generated networks with different sizes are selected (i.e. with {1000, 5000, 10000, 15000, 20000, 25000} nodes).
Results:

As an immediate result, it can be determined that –in accordance with [118]– the performance of the method is heavily influenced by the size of the network. In other words, the experiment indicates that the network size determines the time to reach convergence. Figure 5.4 shows the respective dependencies.

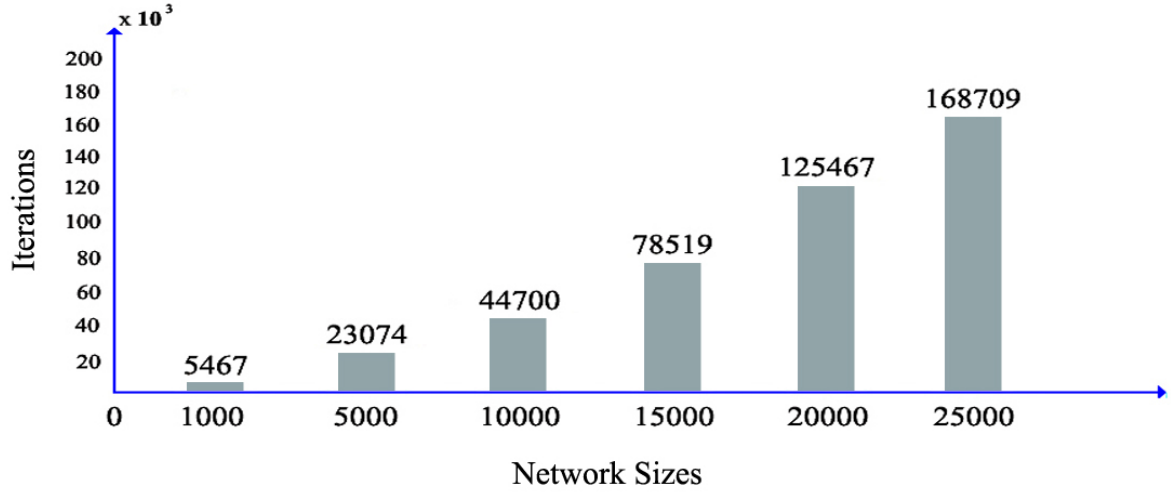

Figure 5.4: Convergence in Networks with Different Sizes

It must be stated that normally only a slow convergence is observed. However, an increased number of random walkers as considered in the next experiments may help to solve this problem.

Experiment 05

Goal: finding a correlation between the number of random walkers and the convergence time.
Description: Eleven tests were conducted using different numbers of random walkers in the population. In a comparative study, the number of iterations –which is needed for convergence– is determined.
Results:

The respective results are given in detail in Figure 5.5 and in Table 5.2. They are obtained from the same 1,000-nodes-network and clearly show that a higher number of random

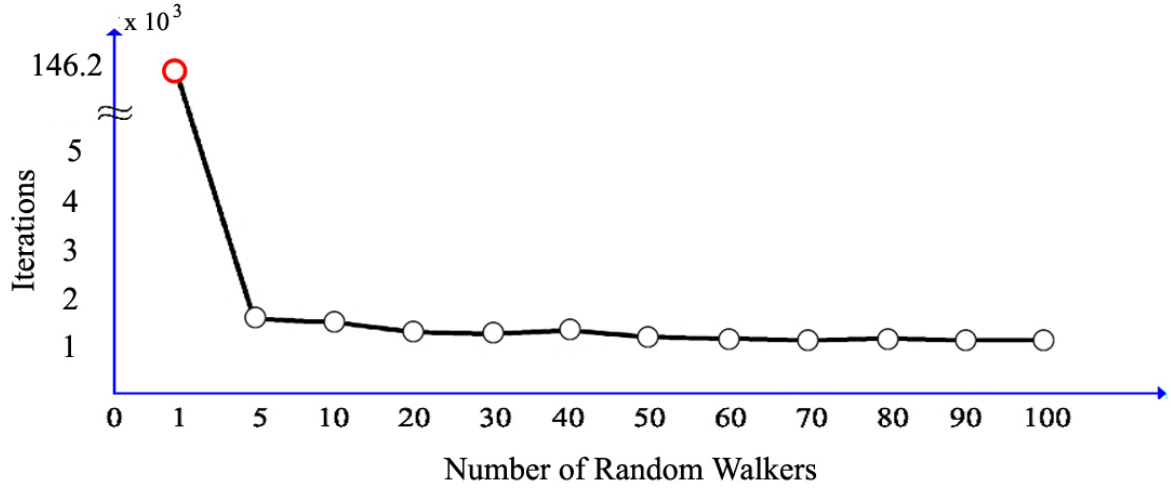

Figure 5.5: Convergence Depending on the Size of the Random Walker Population

walkers (increased from 1 to {10, 20, 30, 40, 50, 60, 70, 80, 90, 100}) accelerates the convergence by parallel processing in the wanted, significant manner. The worst case with a time use of 146, 287 steps is the single random walker case (recognised by a red circle in Figure 5.5). After that, the parallel work reduces the needed time. Already a relatively small number of $5 - 10$ random walker achieves a quite fast convergence behaviour at an almost stable number of time steps (here 1, 444 to 1, 903 steps are needed), only.

Table 5.2: Number of Random Walkers Corresponding to Required Number of Iterations

# **Random Walkers**	# **Iterations**
1	146,287
5	1,903
10	1,853
20	1,649
30	1,605
40	1,677
50	1,525
60	1,510
70	1,444
80	1,480
90	1,453
100	1,455

Experiment 06

Goal: investigating the derivation of $TrustScore$ on a set of fixed nodes within an automatically-generated network having 1000 nodes.
Description: Implementing 20 repeated runs of the $TrustScore$ method using random walkers. Observing the derivation of $TrustScore$ values on selected nodes.
Results:

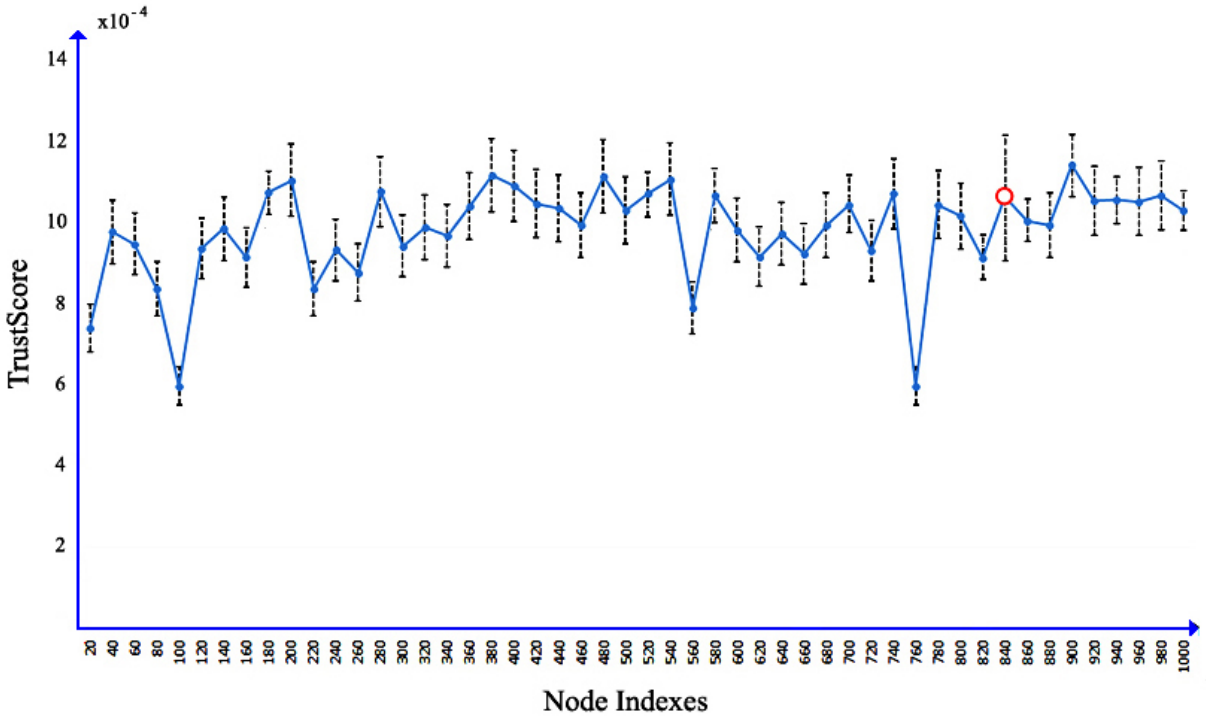

Figure 5.6: Derivation of TrustScore after 20 Repeated Runs

Due to different environments, neighbourhoods and other side conditions, the performance of the TS calculation may behave differently and reaching the convergence might be an intractable process. The $TrustScore$ value of a node can only be determined as a constant one, if the network does not change. However, the randomness in several decisions may cause different and oscillating behaviours in every part of the repeated calculations, especially if only a few random walkers are employed.

Figure 5.6 shows the average results of $TrustScore$ and its deviation from a simulation running 20 times. Exemplary, node 840 (recognised by a red circle in Figure 5.6) is considered, having a maximal deviation of around 3.68×10^{-4}, what is acceptably small. In general, it can be concluded that the outcomes of the simulation under an identical configuration and the same underlying topology are stable and identical for different simulation runs.

Experiment 07

Goal: observing the re-convergence behaviour if the size of networks changes.
Description: The *TrustScore* method is implemented on different automatically-generated networks with the size of {200, 300, 400, 500} nodes. After having received a convergence of the *TrustScore* value calculation, several nodes (1, 5, 10, 15, 20) were added. The number of needed iterations to re-enter the convergence zone is observed.
Results:

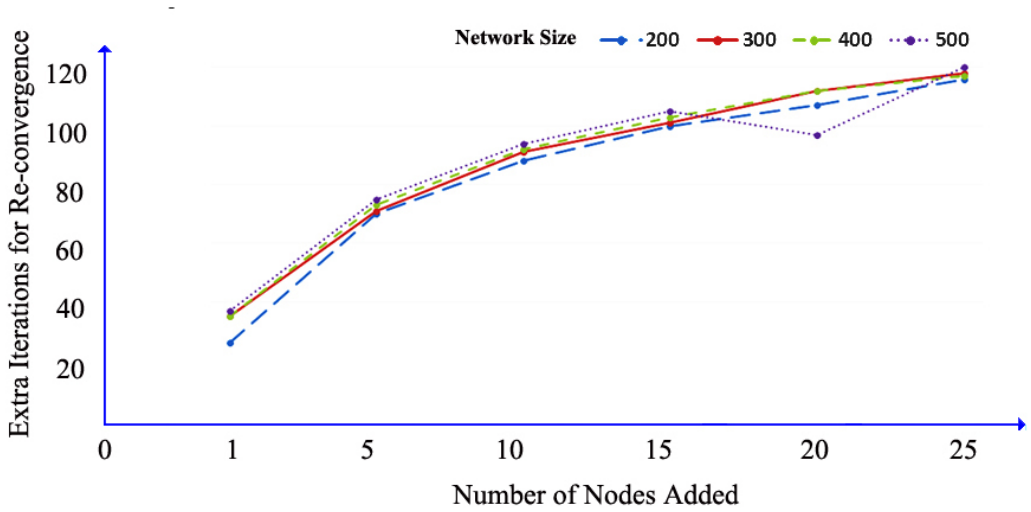

Figure 5.7: Re-Convergence Time with 1, 5, 10, 15, 20, 25 Newly Added Nodes

Normally, nodes come and go in the network which means that the topological structure of network changes, too. Re-convergence of *TrustScore* method is –of course– reached faster than for the whole network in the beginning. Since nodes frequently join and leave the network, the re-convergence time is an important value to evaluate the *TrustScore* methodology.

As shown in Figure 5.7, there is a relatively short re-convergence time, which is increased with the number of nodes joining. However, it increases less than linearly with the number of added nodes, what is a really positive outcome of this experiment. Network shape, network size and –of course– the number of random walkers may influence the absolute needed time for re-convergence.

Experiment 08

Goal: exploring the changes in the *TrustScore* value of a given node, if both the number neighbours and the weight of their connections to that node are changed.
Description: Implementing the *TrustScore* method on *Advogato* with different changes regarding node 429. In particular, simultaneously both the number of neighbours and the weight

of connections were changed.
The number of neighbours of node 429 is reduced by 10%, 20%, 50%,and 70%. Also, a change of the weights by 0%, 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90% and 100% was considered. The $TrustScore$ value's alteration of node 429 is observed and discussed in the result.

Results:

The $TrustScore$ value of a node is not only impacted by structural characteristics of the whole network such as network size but –of course– also by its in-nodes (i.e. in-coming nodes) and the intensity of the trust relation.

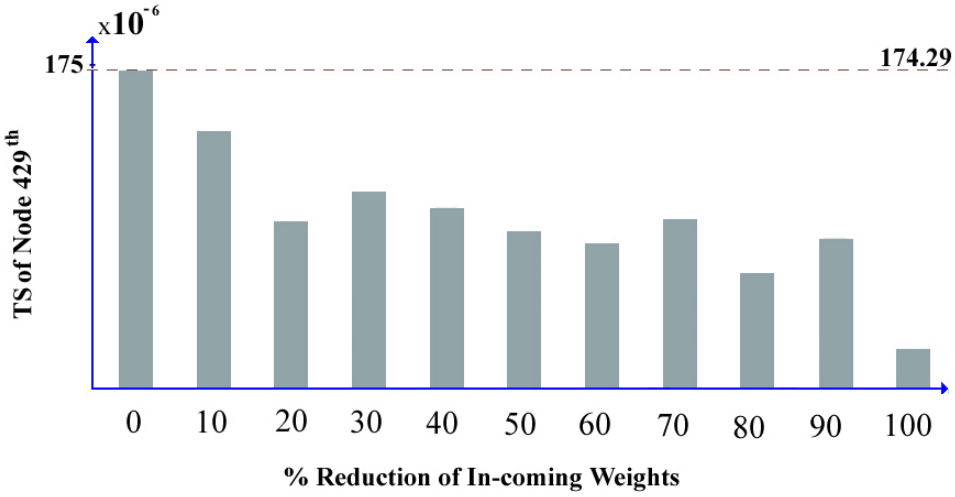

Figure 5.8: 10% of In-Nodes Randomly Leave

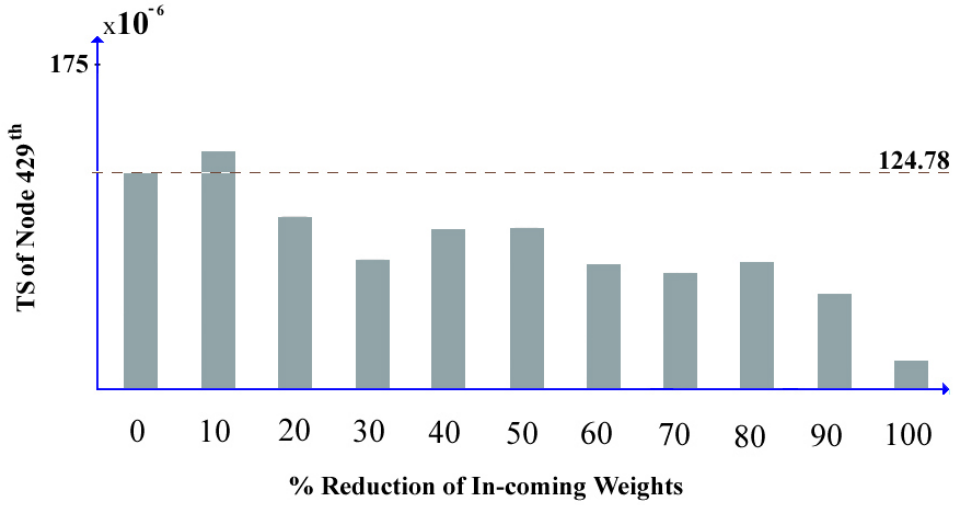

Figure 5.9: 20% of In-Nodes Randomly Leave

To conduct the experiments, a random node was chosen. However, since changes could especially well studied on nodes with a high in-degree, a node with a maximal number of in-nodes should be chosen. In the experiments on *Advogato* network, node 429 satisfies this

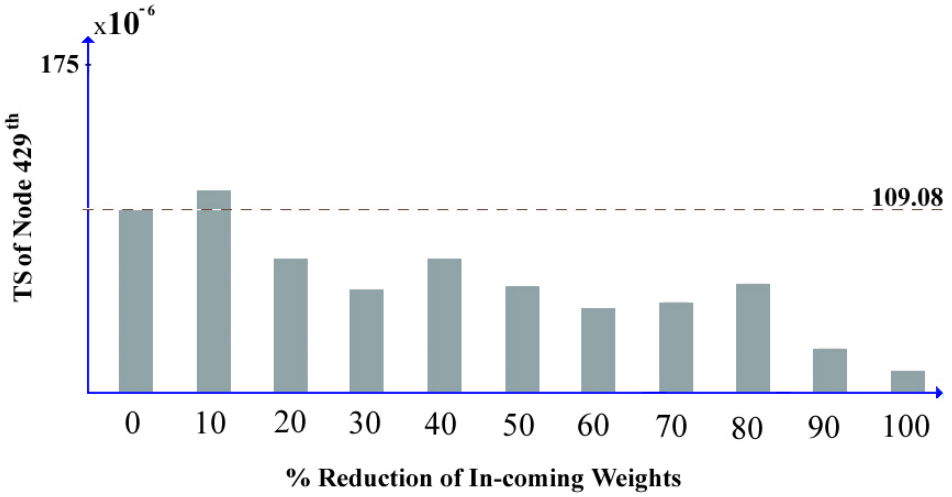

Figure 5.10: 50% of In-Nodes Randomly Leave

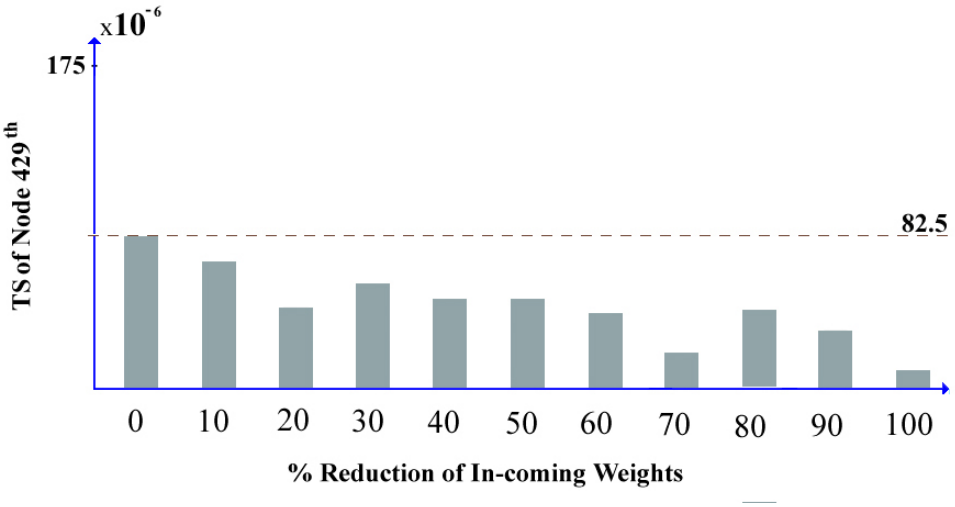

Figure 5.11: 70% of In-Nodes Randomly Leave

condition by having 145 in-nodes. However, the choice does not destroy the general applicability of the simulation results.

The $TrustScore$ value of the given node 429 were observed regarding its the variation for a reduced number of in-nodes leaving randomly from the network and for changed in-coming weights.

The original $TrustScore$ value of node 429 is represented by the first bar in each of the Figures 5.8–5.11. The value decreased gradually from 174.29×10^{-6} in Figure 5.8, over 124.78×10^{-6} in Figure 5.9, 109.08×10^{-6} in Figure 5.10 and to 82.5×10^{-6} in Figure 5.11.

When fixing percentage of reducing in-nodes, each figure among Figures 5.8–5.11 showed how the $TrustScore$ value changes due to decreasing percentage of in-coming weights. It can be seen from these figures that the $TrustScore$ value oscillates in a small margin but a general

trend towards a reduction is visible. To evaluate the trend of the $TrustScore$ variation at node 429, the average $TrustScore$ for all experiments on each figure could help to discover the real trend.

As a results, the average values were calculated at $136,37 \times 10^{-6}$ in Figure 5.8, $108,24 \times 10^{-6}$ in Figure 5.9, $82,02 \times 10^{-6}$ in Figure 5.10 and $56,12 \times 10^{-6}$ in Figure 5.11. Obviously, these statistics intuitively show the descending trend of $TrustScore$ due to the changes caused by the direct neighbours of node 429.

5.4 Effects of Trust on Social Structures

As discussed in the state of the art, the small-world structure of a network is important to keep social relationships intact. The introduction of trustworthiness of users will surely change the topology of the considered network. Consequently, it is interesting and important to discover whether the properties of the small-world effect are strengthened or weakened by doing so. The effect may be evaluated by measuring the two significant small-world properties: the average shortest path length and the average clustering coefficient.

Regarding the characteristics of social relationships assumed in [21], relationships are simply categorised by two types: strong ties (corresponding to friends) and weak ties (corresponding to acquaintances) (instead of the distribution of relationships by Dunbar's Social Brain Hypothesis as assumed by Sutcliffe et al. [42]).

Furthermore, the triadic closure law describes the impact, a trustworthiness of each direct user may have:

- two kinds of relationship are considered, only: strong ties and week ties depending on calculated high and low trustworthiness of a direct user.
  In these experiments, a chosen border point was fixed at 0.7, exemplary;
- if a user A have trusted, strong tie relations to user B and C, it is probable that also B and C will establish such a relation;
- if and only if AB and AC are the strong ties, the added edge BC is annotated as a strong tie. (In another consideration, BC is a weak tie).

The following steps of methodology and implementation were taken in the experiments:

Step 0: An automatically-generated trust network with different sizes of 100, 200, 300, 500, 1000 and 1500 nodes has been constructed.
Step 1: Social ties (strong and weak) have been assigned depending on the strength of the assigned trust relations.

Step 2: The average shortest path length (utilising the Floyd Warshall algorithm) and the average clustering coefficient of the current network have been determined.
Step 3: The triadic closure principle is applied as described above to generate new connections.
Step 4: The algorithm stops if new triadic closures can no longer be found any more in the current network or 3500 cycles have been reached. If stop is indicated, computation terminates at *Step 2*. (Notice that the different size of the networks in the experiment leads to a difference in the number of steps needed, until no new triadic closure is found. However, the algorithm stops at the same point of 3500 cycles in every case.)

Using the this description, the average shortest path length and average clustering coefficient were measured to investigate the development of the structure. In the next subsection, these results are presented and discussed.

Experiment 09

Goal: Studying effect of trust on properties of the social structure and especially its small-world properties.
Description: Experiments of this part were conducted as revealed in the previous section. Two measurements of the average shortest path length and the average clustering coefficient were utilised.
Result:

Measurement of structural properties of social network over time returns several results as described below:

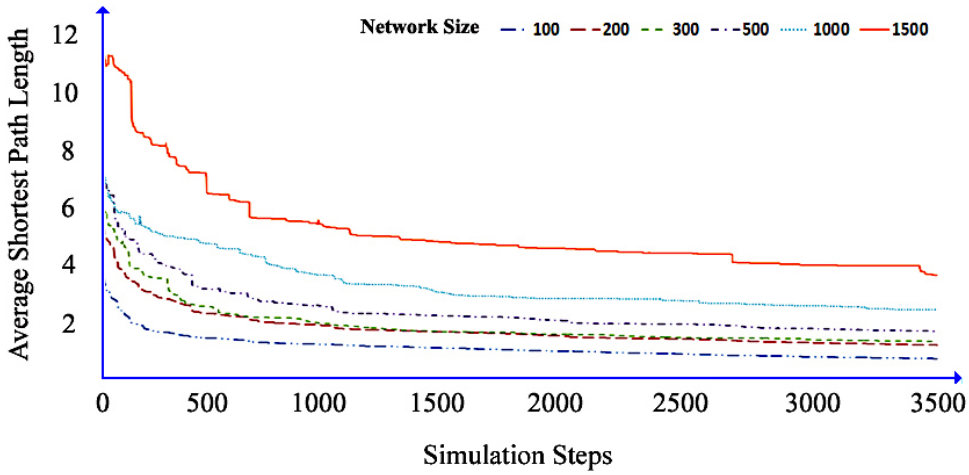

Figure 5.12: Structure Property According to Average Shortest Path Length

The experimental results presented in Figure 5.12 show the results regarding the changes in the average shortest path length. Six different sizes of networks were used. At the beginning, the average shortest path length mostly depended on the network size. During the running

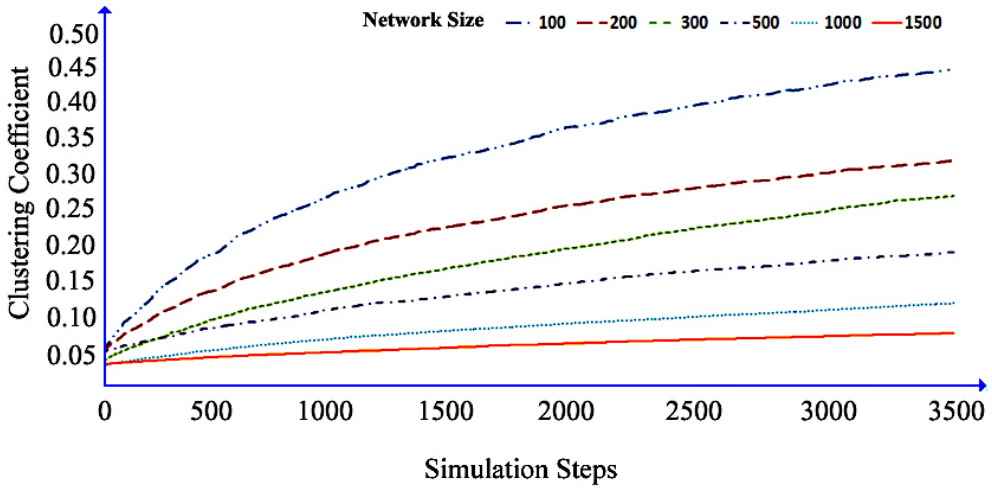

Figure 5.13: Structure Property According to Average Clustering Coefficient

time of the algorithm, the average shortest paths length gradually reduced its value. It can be recognised that at the terminate state, the average shortest path length in all networks has been significantly reduced.

The measured average clustering coefficient is shown in the plots in Figure 5.13. It reveals clearly an increasing tendency to build local clusters expressed by an increased average clustering coefficient.

Summarising, it may be figured out that trust has a positive effect on the structure of the underlying social network. The topology of network structures tends to be stable and is strengthened due to the intensified small-world properties. The evolution of structures ensures both a reduction of the average shortest path length and an increase of the average clustering coefficient over time.

5.5 Summary

The heart of the introduced new methodology calculating recommendation on trustworthiness is the decentralised determination of the $TrustScore$ value for each member of the community.

Since experiments in a real environment of an on-line social network are impossible, the new methodology has been evaluated by simulations. Therefore, artificially-generated networks as well as samples of real-world networks like *Advogato* and *Epinions* have been used.

It could be demonstrated that the $TrustScore$ values of all nodes in a network can be determined by a locally-working algorithm on the basis of random walkers. The obtained values show the expected Gaussian distribution, if calculated using an underlying network with real-world samples for the trust values.

Since the convergence speed of the proposed implementation is not very high, it is useful to employ a population of random walkers. However, a faster re-convergence of the $TrustScore$ values in case of dynamic changes in the network (i.e. joining and leaving of nodes as well as changes in edge weights) could be stated.

Another major result was the confirmation that the two small-world properties (i.e. having average minimal path length as well as a high clustering coefficient) are not weakened but strengthened by considering trustworthiness of direct users during the establishment of new connections in the network. This might be an important argument to justify trust-related considerations in on-line social networks against their critics.

Chapter 6

Perspectives and Applications

6.1 Recent Application Trends

The social commerce (s-commerce) innovation emerges recently as a fusion of two big digital trends –'social media' and 'e-commerce'. Primarily, this technique enables an on-line trade and connects customers to so far unknown merchants via recommendations of friends. The idea behind social commerce comes from simple numerical statistics, which indicates that *"70% of UK Internet users trust recommendations from strangers"* by *Graeme Foux Knexus*. That is why, in general, the recommendation on trustworthiness in the whole network becomes more and more important. There are two possible types of social commerce sites for trade activities:

- *Option (a):* sites with a direct transaction, when purchasing products (Ebay, Amazon). Customers of these systems rely on the reputation of the merchant through the direct on-line shopping experience. A Trust system on these sites often bases on the feedback approach with a lot of deficiencies as indicated in the subsection 2.2.4.

- *Option (b):* Social Commerce (s-commerce) using marketplaces and social systems like Google Plus, Facebook for on-line marketing and promoting purchases.
  Differing from the e-commerce model, members of s-commerce may have both roles as merchant as well as buyer at the same time. The estimation of the trustworthiness of a merchant could be based not only on direct interactions but also on an opinion shared on the whole social platform. A huge community of buyers may, therefore, influence purchasing decisions by buying and selling of products, using service and giving recommendations.

In a reference on *Trust Transference Theory* [168, 169], it is expected that the global trustworthiness of a merchant in the social commerce is transferred to any related resources. In that manner, this value might be a catalyst mitigating risk in interaction-making and therefore also promoting purchase intentions in reality.

Another futuristic approach and trend comes from China. A government-managed Social Credit System assigns a social score to each citizen. The intention of that system is to evaluate the qualification and trustworthiness of each citizen of the 1.3 billion population. The system's goal is to accumulate all collectable data ranging from financial credibility, criminal and medical records from all on-line and off-line behaviours and finances across communities and marketplaces. All information will be distilled into a single social score (i.e. government-managed credit score) from 2020 onwards.

Figure 6.1: An Imagination of Future Social Credit

It is claimed that trustworthiness is a perfect solution for the question about how to receive a social score. That social score could be considered as creditworthiness code in control of the behaviour of citizens, especially in on-line digital communities. Therefore, trustworthiness is becoming a valuable asset like wealth, power, personal identity, currency. It is expected that a new economy of trust appears. In that place, social score will influence our lives in unimaginable ways. Consequently, it will be a prerequisite for carrying out any daily needed activities such as getting a particular job on the labour market or booking a hotel without disclosure of cash deposit. So far, the reached scope of the SeeSame Credit System [170], which accumulates the electronic purchasing behaviour data of 400 million Alibaba's service consumers is the first running example and seed for future social credit systems.

Massive problems may arise from the fact that usually a simple user does not know:

- which data are collected and stored about him;
- how those are evaluated;
- how he may get to know his trust evaluation;
- how he may protest against it or take legal actions against his (maybe unjustified) evaluation.

Moreover, critics are afraid that the use of such systems may be a possibility to control a mass of users and force them to show an intended behaviour in order to gain or keep a respective social score to be able to manage its daily life hassle-free.

6.2 A Concept of Decentralised Trust Frameworks

6.2.1 Related Works

The described problems may be reduced, if the trustworthiness calculation is carried out under the user's control in a decentralised network. [171, 172] mentioned already that this may generate a new class of trust management. Already for some decades, there are a few security frameworks developed based on the decentralisation of a trust calculation, as described in [125] and [163].

The new methodology introduced in chapter 3 and chapter 4 may allow the development of a new kind of trustworthiness recommendation system. This new approach solely bases on the use of decentralised networks and employs a P2P-based system as a parallel working, separate and independent architecture for handling private, trust-based information.

This may also help to avoid to store and frequently updated huge amounts of data in giant storage architectures. An example for such almost un-manageable data amounts might be given by Facebook, again. According to Facebook statistics [1], with its last updated in 04/27/16, there were 1.09 billion active users, the raw topological data of the friendship network alone (without node attributes) counts at least 1.09×155 (approximate number of friends 155 on average) $\times$ 8 bytes (assuming that a user ID needs 8 bytes to be encoded) $\approx$ 1258.8 GB.

However, due to the huge amount of information which is already presented in centralised networks, it cannot be expected that those networks will be re-developed in a fully decentralised manner in the next few years. In order to separate trustworthiness estimations from big companies and the service providers itself, an implementation of a trustworthiness recommendation system within existing centralised service systems is unsuitable.

Consequently, the only solution consists of the establishment of a decentralised, P2P-based side-network system, as it is suggested in [20, 173, 174, 175]. That system and online social network work in parallel, independent manner. It may ensure the needed privacy and user control on its own data and avoid shortcomings of a centralised system like offering a single point of failure, having access limitations, being susceptible for attacks (like denial of service attacks). Thus, the capabilities of peer software meets exactly the needs of the trust management.

However, the development of such a decentralised system still remains a very critical

[1] *expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/*

challenge. Therefore, a new concept shall be introduced in the next subsection.

6.2.2 A Trustworthiness Recommendation Framework

In Figure 6.2, the intended architecture of a new P2P-based trust management system is shown.

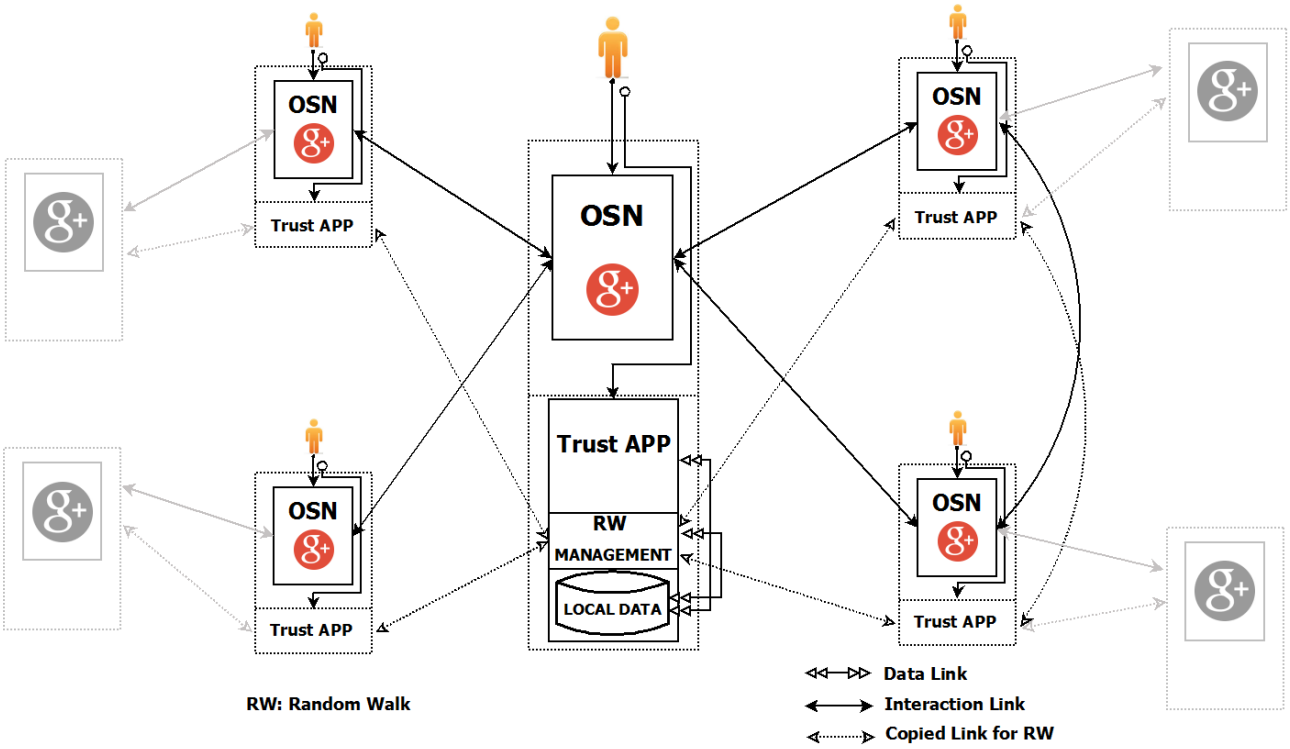

Figure 6.2: Block-scheme of the Intended Trust Management System

Since most on-line social network systems use the WWW and therefore any kind of web-browser as user interface and HTTP for communication purposes, the central, crucial part of trust management system is a plug-in as extension to the web-browser, which may (locally) observe the users activities and the responses of the on-line social network system. The purpose of this browser extension is just carry out a one-way transfer of those data into the local data base of the trustworthiness recommendation system (TrustApp). Therefore, it may ensure a full separation of any sensitive data and their computation from any centralised service provider.

The TrustApp itself will be an autonomously-working peer-to-peer system running in parallel to the on-line social network system.

It establishes a peer for every user, running on his own computer and keeping all sensitive data of that user privately and confidently on the local host. These data contain information about the local user's activities and contents, activities of other users related to him as well as his (pairwise) trust evaluations for his direct neighbours in the social network (i.e. his friends). As a part of his cooperation with other users in the network, the peer –of course– has to handle requests from other users, like answering requests on his own trustworthiness (later, a fraud

protection for this value by the user itself will be introduced) as well as support the processing of random walkers to support the newly developed trustworthiness calculation.

The bootstrap problem (i.e. the initial connection of this peer to other peers of the same peer-to-peer network) is solved by copying the friendship relations of the considered user in the on-line social network system and use this system to exchange the respective contact information via private messages.

The core elements of the TrustApp are shown in Figure 6.3.

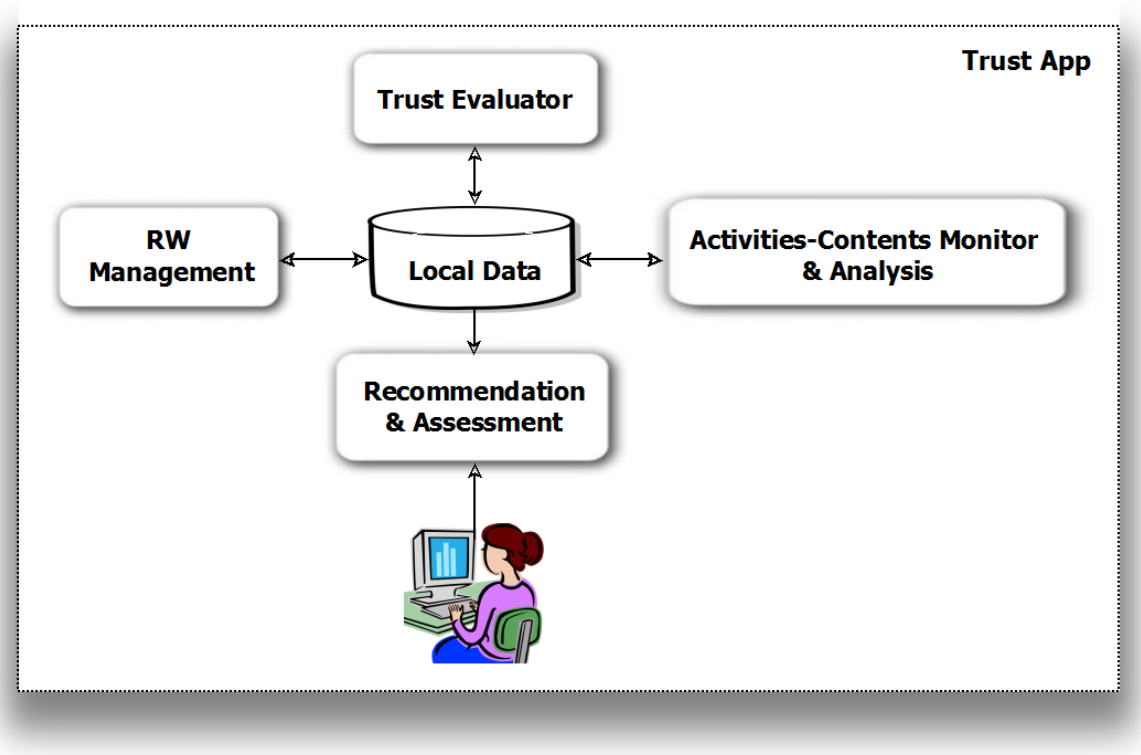

Figure 6.3: Trustworthiness Recommendation Framework

Local Data

This local data is the central part of the locally working peer, which contains all kind of trust-related data of the user, like activities, contents distributed as well as activities of other users observed and all trust-related information including evaluated/calculated recommendations on trustworthiness. All data are confidential and kept solely local (i.e. only the local peer may access those data). However, the user has the possibility to delete the entire peer, what removes all information about him from the system and forces him to fully restart with any trust-gaining activities at initial trust level (possibly set to 0).

Activities-Contents Monitor & Analysis
This component tracks, collects all kind of data related to the interactions made through the respective, one-way data transmission from the on-line social network system to the TrustApp via the respective browser extension. This information will be collected, filtered and transferred to the Local Data for storage and later processing for the purpose of trust evaluation by the Trust Evaluator.

Trust Evaluator
The Trust Evaluator is the heart of the TrustApp. It performs the needed evaluations and information processing to obtain the wanted trustworthiness of neighbour users. Therefore, this component may employ all needed interactions and access the Local Data. Pairwise trust values are processed as described in the main chapter 3. It will be ensured that trust- and recommendation(on trustworthiness)-related information are regularly updated.

RW Management
The Random Walker Management controls the population of random walkers, traces steps of each random walker and controls the data collection for the $TrustScore$-calculation as worked out in chapter 4 of the thesis. In particular, it is the responsibility of this unit to ensure the pairwise trust-depended calculation of the probability distribution for a proper forwarding of the random walkers. The exactness of the intended trustworthiness estimation depends it.
Last but not least, the RW Management is also responsible to ensure the needed classical and basic P2P functionalities. This especially includes to ensure the connectivity of the whole network system by a permanent update of the neighbourhood relations besides any eventually added friendship relations in the on-line social network.

Recommendation & Assessment
The Recommendation and Assessment unit is responsible for all communication with the user and optionally with other (local) applications using the recommendation on trustworthiness for their work.
The major task is –of course– to give context-depending recommendations about the trustworthiness of any, maybe so far unknown, partners in the network. However, as it was mentioned in this work, this estimation may depend on a lot of private, very subjective factors and feelings of the local user. Therefore, especially after the start of the system, the user must get the opportunity to configure the system's decisions depending on his personal attitude and possibly even perform some wanted adaptations and re-configurations. The respective dialogue is also provided by this unit.

The so far specified P2P-System[2] is a fully autonomously-working system, which meets the requirements given at chapter 2.

The still open question of how to protect the local global trustworthiness values (especially against suspicious activities of the local user) from fraud will be answered in the next section.

6.3 Fraud Protection

The locally calculated recommendations on trustworthiness of any node are stored locally on the owners node. On the one hand, this is a big advantage to ensure the user's control of his own, private and maybe sensitive data. On the other hand, it gives manifold possibilities for fraud, cheating and manipulations to him. Since no centralised, trusted third authority, like a Certification Authority, exists in a fully decentralised P2P-system, other possibilities for a fraud protection must be found. These mentioned weakness can be optimized for "diamond in the rough" by using special protocol in fully distributed configurations.

In fact, a very suitable, interesting idea for this purpose and to design a respective protocol can be found in [139]. The original problem discussed therein is the protection of tokens representing coins of a virtual payment system from fraud and copying. In order to do so, the missing third authority is replaced by a randomly chosen group of users. This is a stochastic approach, whereby the size of the group determines security of the system (i.e. bigger groups ensure a higher fraud protection on the costs of the needed overhead).

The presented approach bases on the assumption that :

- nodes will join and leave the established community but this just is a more or less seldom case even when dealing with well-established really working social communities;
- changes of edges will never result in a deletion of all edges of a node or an addition of a huge number of new connections.

In the work of [139], coins or tokens are designed to be random walkers as also used in the *TrustScore* approach presented in this work. These random walkers are entitled to move forward to the next node in a very special way due to additional data and a specially designed protocol (see Figure 6.4). While moving to the next node, the random walker re-visits the node, it has been on k steps before and is again authenticated by that node (i.e. within k steps a group of k former –randomly chosen– visited nodes has to re-confirm the authenticity of the token).

Therefore, the random walkers carry a set of additional information, as shown in the below Table 6.1:

[2]Unfortunately, the full specification and implementation of this new kind of system could *not* be completed due to purely technique issues as well as the support possibility of service providers.

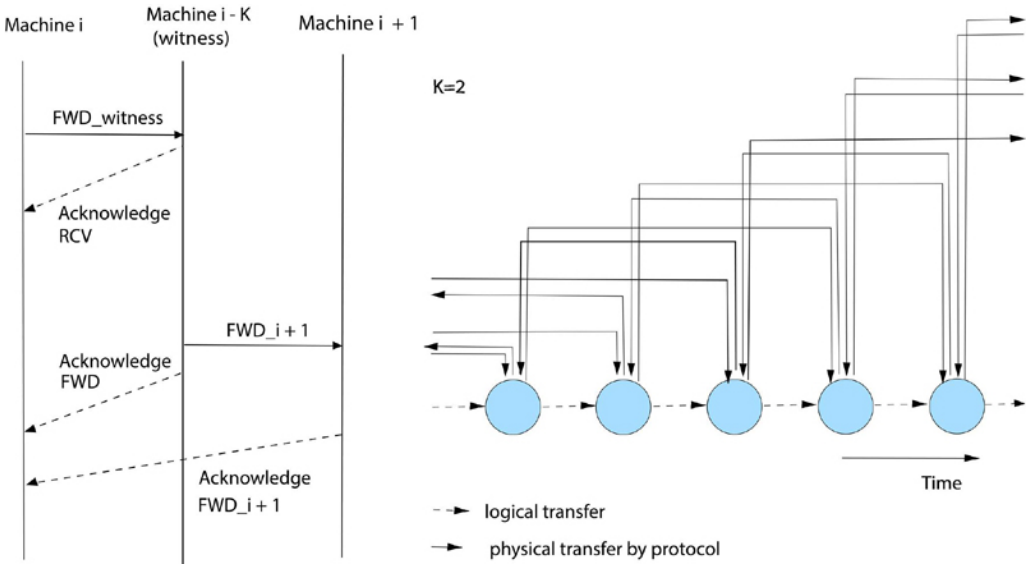

Figure 6.4: Token Forward Protocol from [139]

Field	***Description***
id	identification of random walker
history	list of k witnesses/formerly visited nodes
information-of-owner	recommendation on trustworthiness and address of owners
mode-id	indicates authentication or not (default not)
successor	address of next node, random walker wants to move to

Table 6.1: Description of Fields

In [139], an estimation for the reachable security of authentication as well as detailed considerations to increase the fault tolerance of the method (by applying an m-out-of-k approach) are given.

The cited protocol can be used with a few small changes to solve the manipulation problem of the TS-values by the owners. Therefore, the following changes are needed:

- All nodes in the system are ready to keep temporarily a trace of the visited random walkers and keep for a given time TS-value of any other node.
- The local TS-value of a node u_x are collected and carried by each bypassing random walker for k steps.

- While being randomly forwarded to the $1, 2, ..., k$-th next node, the random walker re-visits (following the protocol from [139]) the $k, k-1, k-2, .., 1$ predecessor of u_x again. Hereby, he may leave the TS_{u_x}-value on all those nodes.
  Since those predecessor nodes are randomly and independently chosen from u_x, it may be assumed that they are un-influenced witnesses.

- The owner u_x of TS_{u_x}-value keeps the information about the k last steps of the last (or to avoid problems with update times the last 2 random walkers, which have visited u_x).

By contacting, the k nodes stored on a $TrustScore$'s owner node, the authenticity of the offered value may be verified at any time by the k witnesses. A critical consideration of the addresses of the k-returned witnesses over time may indicate any violent activities of u_x if there is no periodic change of those nodes (which shall be due to the random walker's characteristic), a fraud is possible. It becomes clear that a user must own at least $2k$ machines in order to mask any manipulations –if k is sufficiently big, this is a rather hard solvable problem.

In order to separate functionality, an only for this purpose generated sub-population of random walkers may care for this authentication process. Adjusting the size of this special random walker population will also allow to control overhead and memory used for authentication and fraud protection on every participating peer (machine).

With the made changes, it becomes difficult for an owner to tamper with its own $TrustScore$ value, what solves a major application and security problem of the given approach.

6.4 Summary

s-Commerce as a new trend in the Internet turns recommendation on trustworthiness for so far unknown merchants into a wanted pre-requisite to establish any commercial or financial transaction.

To obtain the needed global trustworthiness values, a fully decentralised platform on the basis of a peer-to-peer network is introduced, which supports the determination of $TrustScore$ values using an evaluation of different, observed, mutual activities of the users in an independently-working on-line social network. This approach ensures the privacy of any sensitive user information and allows –at least– a limited control of the user of its own information (by a possible system restart). Furthermore, any governmental or organisational control of user activities and influences to his personal life and behaviour are avoided. Last but not least, an effective protocol for an avoidance of fraud/manipulation is given.

Chapter 7

Conclusion and Outlook

A contribution to an automatic global trustworthiness calculation in on-line social networks has been made. The investigated approach is a strong support for the emergence of s-commerce systems. It allows for automated assessments and risk evaluations of unknown business partners, which are –so far– mostly carried out by the *word-of-mouth* method in local groups. By the new methodology, the geographic range of the evaluation is expanded to the world-wide covering range of the on-line social network systems. Thus, also the amount of considerable information for the trustworthiness-estimating procedures has been significantly increased.

In order to develop the new solution, the psychological background of trust-building processes in the human brain has been considered. It has been figured out that trust is built or destroyed by the cumulated impact of activities of two partners over a longer time. Three phases have been identified in the trust-building process and modelled in an efficient manner to give (human-like) trustworthiness of direct users. For the first time, also trust-reducing activities (e.g. lies, deception and betrayal) and their impact have been included adequately into the considerations.

In the next step, activities in on-line-social networks have been analysed and their impact has been described within the model by introducing respective weight factors. As a new feature, also aspects of the submitted content could be included into the set of the trustworthiness-influencing factors. Therefore, similarity and sentiment as well as volatility analysis have been proposed as suitable investigation methods. The outcome of the content analysis could be quantified and be processed together with the impact of other activities in the single, pairwise trust parameter of the model.

A significant progress and contribution to the state of the art could be reached by a method combining all pairwise trust information of the network into a single, global trustworthiness value for every user. Therefore, an adaptation of the well-known PageRank algorithm has been used in the proposed $TrustScore$ methodology. To avoid any manipulable and attackable central instance, a fully decentralised calculation of the TS-values by a random walks approach was suggested, which can be accelerated by the use of a population of random walkers.

To demonstrate the practicability and performance of the developed methodology, simulations have been used. This approach was necessary, since no experiments with real on-line social networks were possible and also no data could be obtained from the providers of such systems. The made simulations are using reproducible initial settings derived from an automated generation of complex network structures as well as from obtained initial settings from the real-world networks *Advogato* and *Epinions*. It could be shown that the needed $TrustScore$ values could be obtained in a reasonable time, that the calculation process converges and that the values will be fast adapted, if changes in the network appear. In addition, quantitative results about the convergence speed and its dependency on the size of the network as well as the population of random walkers were derived.

Last but not least, a system architecture for the calculation of $TrustScore$ values for each user was introduced. A fully decentralised working peer-to-peer approach is used, which works in parallel to an existing browser-based on-line social network. It implements the random walks-based $TrustScore$ method and solves the bootstrap problem by copying the social network friendship relations of a user and obtains all necessary information by a browser plug-in. Also, the privacy of sensitive user data is ensured and a special protocol was developed to avoid fraud and manipulation of the obtained and locally stored $TrustScore$ values. A suitable interface supports the recommendation-making request of the user and may also set the initial parameters and weight factors following the user intentions expressed in the form of questionnaire.

Future Works shall –of course– include a full implementation of the $TrustScore$-methodology within an existing social network environment and refinements of the suggested methodology.

Two major tasks include improvements for the convergence speed of the random walks-based approach as well as parameter tuning by a sufficiently big sample of users. Also, other activities of a user from outside the target on-line social network system may be included, like a user's general communication behaviour and other passive and active sensing methods (e.g. collecting mobile data Call, SMS and Bluetooth logs . . .) as suggested initially in [176]. Further more physiological parameters from fitness bracelets are possible.

Since human decision-making is also affected by emotions (including happiness, disgust, fear, anger and sadness) and its importance in psychological and social risk perception has already been addressed in [177], those factors might be included in the trust model proposed as well.

However, most future works and the continuation of research in the working area of this thesis require a strong support from social network service providers to verify the made assumptions in a real-world user community. Also, possibilities of an interdisciplinary work with colleagues from psychology and sociology are given, since their research results will directly influence the further development and extension of the needed trust models.

Bibliography

[1] K. Nirmala and S. Satheeshkumar. “Filtering the Unwanted Messages from Online Social Networks Using Machine Learning Techniques”. Artificial Intelligent Systems and Machine Learning, 6(5), 189-192, 2014.

[2] G. NaliniPriya and M. Asswini. “A Survey on Vulnerable Attacks in Online Social Networks”. In Innovation Information in Computing Technologies (ICIICT), 2015 International Conference on (1–6), IEEE, Feb. 2015.

[3] H. Gao, J. Hu, T. Huang, J. Wang and Y. Chen. “Security Issues in Online Social Networks”. Internet Computing, IEEE, 15(4), 56–63, 2011.

[4] Z. Chi. et al. “Privacy and Security for Online Social Networks: Challenges and Opportunities”. Network, IEEE 24.4: 13–18, 2010.

[5] G. Sadowsky, J.X. Dempsey, A. Greenberg, B.J. Mack, A. Schwartz. “Information Technology Security Handbook”. World Bank Publications, 2003.

[6] M. Burke, M. Cameron and L. Thomas. “Social Network Activity and Social Well-being”. Proceedings of the SIGCHI conference on human factors in computing systems. ACM, 2010.

[7] M. Deutsch. “The Resolution of Conflict: Constructive and Destructive Processes”. Yale University Press, New Haven, 1973.

[8] R.C. Mayer, J.H. Davis and F.D. Schoorman. “An Integrative Model of Organizational Trust”. Academy of Management Review 20, 709–734, 1995.

[9] S.P. Marsh. “Formalising Trust as a Computational Concept”. PhD dissertation, University of Stirling, 1994.

[10] D. Zejda. “Characteristics of Trust in Online Social Networks and Community of Trust as a Special Case of Online Community”. In WEBIST (pp. 531-534), 2011.

[11] M. Paolo. “A Survey of Trust Use and Modelling in Real Online Systems”. In Trust in E-Services: Technologies, Practices and Challenges, Idea Group Inc, 51–83, 2007.

[12] M. Anderson, J. Sims, J. Price and J. Brusa. “Turning Like to Buy Social Media Emerges as a Commerce Channel”. Booz and Company Inc, 2011.

[13] C. Dellarocas. “The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms”. Management Science 49 (10), 1407–1424, 2003.

[14] J. Surowiecki. “The Wisdom of Crowds”. Anchor Publisher, ISBN: 0385721706, 2005.

[15] L. Mui. “Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks”. Ph.D. thesis.

[16] A. Jøsang. “Trust and Reputation Systems”. In Foundations of security analysis and design IV, 209–245, Springer Berlin Heidelberg, 2007.

[17] A. Jøsang, R. Ismail and C. Boyd. “A Survey of Trust and Reputation Systems for Online Service Provision”. Decision Support Systems, 43(2), 618-644, 2007.

[18] A. Mislove, M. Marcon, K.P. Gummadi, P. Druschel and B. Bhattacharjee. “Measurement and Analysis of Online Social Networks”. In ’IMC ’07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement’, ACM, New York, NY, USA , 29–42, 2007.

[19] J. Long, C. Yang, W. Tianyi, H. Pan and A.V. Vasilakos. “Understanding User Behaviour in Online Social Networks: a Survey”. In Communications Magazine, IEEE , vol.51, no.9, 144–150, September. 2013.

[20] M.N. Huhns. “Software Agents: The Future of Web Services”. In Ryszard Kowalczyk; Jörg P. Müller; Huaglory Tianfield; Rainer Unland, ed., ’Agent Technologies, Infrastructures, Tools, and Applications for E-Services’, Springer, 1–18, 2002.

[21] D. Easley and J. Kleinberg. “Networks, Crowds, and Markets: Reasoning About a Highly Connected World”. Cambridge University Press, 2010.

[22] S. Milgram. “The Small World Problem”. Psychology Today 67 (1), 61–67, 1967.

[23] S. Vongsingthong, S. Boonkrong, M. Kubek and H. Unger. “On the Distributions of User Behaviors in Complex Online Social Networks”. In Recent Advances in Information and Communication Technology 2015, 237–246, Springer International Publishing, 2015.

[24] H. Liu, A. Nazir, J. Joung and C.N. Chuah. “Modeling Predicting the Evolution Trend of OSN-based Applications”. In Proceedings of the 22nd international conference on World Wide Web, 771–780, International World Wide Web Conferences Steering Committee, 2013.

[25] A.J. Morales, J.C. Losada and R.M. Benito. "Users Structure and Behavior on an Online Social Network during a Political Protest". Physica A: Statistical Mechanics and its Applications, 391(21), 5244–5253, 2012.

[26] G. Chen, C.P. Low, and Z. Yang. "Enhancing Search Performance in Unstructured P2P Networks based on Users? common interest". IEEE Trans. Parallel Distrib. Syst., 19:821-836, ISSN, 1045–9219, 2008.

[27] K. Pussep, C. Leng and S. Kaune. "Modeling User Behavior in P2P Systems". In K. Wehrle et al., editors, Modeling and Tools for Network Simulation, 447–461, Springer, July 2010.

[28] E. Veloso, V. Almeida, W. Meira, A. Bestavros, and S. Jin. "A Hierarchical Characterization of a Live Streaming Media Workload". In Proc. of the 2nd ACM SIGCOMM Workshop on Internet Measurment (IMW-02), Marseille, France, 117–130, 2002.

[29] M.A. Devmane and N.K. Rana. "Privacy Issues in Online Social Networks". International Journal of Computer Applications, 41(13), 5–8, 2012.

[30] M.A. Devmane and N.K. Rana. "Security Issues of Online Social Networks". In Advances in Computing Communication and Control, Springer Berlin Heidelberg, 740–746, 2013.

[31] B. Carminati, E. Ferrari and M. Viviani. "Security and Trust in Online Social Networks". in Security and Trust in Online Social Networks, Morgan and Claypool, pp.120, 2013.

[32] S.A. Catanese, P. De Meo, E. Ferrara, G. Fiumara and A. Provetti. "Crawling Facebook for Social Network Analysis Purposes". In Proceedings of the international conference on web intelligence, mining and semantics, p. 52, ACM, 2011

[33] Mondal Mainack. et al. "Defending Against Large-scale Crawls in Online Social Networks". Proceedings of the 8th international conference on Emerging networking experiments and technologies, ACM, 2012.

[34] A.H. Wang. "Detecting Spam Bots in Online Social Networking Sites: a Machine Learning Approach". In Data and Applications Security and Privacy XXIV, 335–342, Springer Berlin Heidelberg, 2010.

[35] T.S. Doan and M. Kubek, "A Concept for Trust Derivation from User Activities". International Conference on Computing and Information Technology, 2015.

[36] T.S. Doan, M. Kubek and H. Unger, "Activity and Content-based Trust Estimation in Online Social Network". International Symposium on Nonlinear Theory and its Application (NOLTA), HongKong, 2015.

[37] T.S Doan, M. Kubek and H. Unger, "Mutual Influences between Trust and Online Social Network Systems". 8th GI Conference on Autonomous Systems, Marlloca, 2015.

[38] P. Sztompka. "Socjologia". Analiza spoleczenstwa. Krakow: Znak, ISBN 83-240-0218-9, 2002.

[39] D. Watts and S. Strogatz. "Collective Dynamics of Small-world Networks". Nature (393), 440–442, 1998.

[40] D.J. Watts. "Small worlds: the Dynamics of Networks between Order and Randomness". Princeton University Press, 1999.

[41] E. Ostrom. "Towards a Behavioural Theory Linking Trust, Reciprocity and Reputation". In E. Ostrom and J. Walker (Eds), Trust and reciprocity: Interdisciplinary lessons from experimental research, 19-79. New York: Russel Sage Foundation, 2002.

[42] A. Sutcliffe and D. Wang. "Computational Modelling of Trust and Social Relationships". Journal of Artificial Societies and Social Simulation, 15(1), 3, 2012.

[43] L. Margalit. "The Physchology behind Social Media Interactions". Psychology Today. Retrieved from `https://www.psychologytoday.com/blog/behind-online-behavior/201408/the-psychology-behind-social-media-interactions`, 2014.

[44] D.J. McAllister. "Affect-and Cognition-based Trust as Foundations for Interpersonal Cooperation in Organizations". Academy of management journal, 38(1), 24–59, 1995.

[45] R. Lewick and B.B. Bunker. "Developing and Maintaining Trust in Work Relationships". Trust in Organizations: Frontiers of Theory and Reach, 114–139, 1996.

[46] A. Fox. "Beyond Contract: Work, Power and Trust Relations". London: Faber and Faber, 1974.

[47] E.H. Lorenz. "Trust, Community and Cooperation: toward a Theory of Industrial Districts". 195–204 in Scott, A. and Storper, M. (eds), Pathways to industrialization and regional development, London, Routledge, 1992.

[48] R.I.M. Dunbar. "Coevolution of Neocortex Size, Group size and Language in Humans". Behavioural Brain Sciences, 16, 681–735, 1993.

[49] D.H. McKnight and N.L. Chervany. "Trust and Distrust Definitions: One Bite at a Time". In Rino Falcone; Munindar P. Singh and Yao-Hua Tan, ed., 'Trust in Cyber-societies', Springer, 27–54, 2000.

[50] S.B. Sitkin and N.L. Roth. “Explaining the Limited Effectiveness of Legalistic Remedies for Trust/Distrust”. Organization Science, 4: 367-392, 1993.

[51] R.J. Bies and T.M. Tripp. “Beyond Distrust: Getting Even and the Need for Revenge”. Trust and organizations. Ed. R.M. Kramer M.A. Neale. Thousand Oaks, CA: Sage, 1996.

[52] S.B. Sitkin, D. Stickel. “The Road to Hell: The Dynamics of Distrust in an Era of Quality”. Trust in organizations: Frontiers of theory and research, 196–215, 1996.

[53] R.M. Kramer. “Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions”. Annual Review of Psychology, 50, 569–598, 1999.

[54] J. Coleman. “Foundations of Social Theory”. Cambridge, Mass: Harvard University Press, 1990.

[55] D. Gambetta. “Can We Trust Trust?”. In Trust, Making and Breaking Cooperative Relations, Electronic Edition, D. Gambetta, Ed. University of Oxford, Chapter 13, 213–237, 1990.

[56] J. Decety and J.P. Keenan. “Social Neuroscience: A New Journal”. Social Neuroscience, 1, 1–4, 2006.

[57] L.M. Hirshfield, S.H. Hirshfield, S. Hincks, M. Russell, R. Ward, T. Williams. “Trust in Human-computer Interactions as Measured by Frustration, Surprise, and Workload”. In International Conference on Foundations of Augmented Cognition, 507–516, Springer Berlin Heidelberg, 2011.

[58] T.R. Koscik and D. Tranel. “The Human Amygdala is Necessary for Developing and Expressing Normal Interpersonal Trust”. Neuropsychologia, 49(4), 602-611, 2011.

[59] E. Fehr, U. Fischbacher and M. Kosfeld. “Neuroeconomic Foundations of Trust and Social Preferences: Initial Evidence”. The American Economic Review, 95, 346-351, 2005.

[60] P.J. Zak. “The Neurobiology of Trust”. Scientific American 298, 88-95, 2008.

[61] M. Deutsch. “Cooperation and Trust: Some Theoretical Notes”. Nebraska Symposium on Motivation. University of Nebraska Press, Lincoln, 1962.

[62] J. Rotter. “A New Scale for the Measurement of Interpersonal Trust”. Journal of Personality, Vol 35(4), 651–665, 1967.

[63] R.T. Sicora. “Personality and Trust: A Qualitative Study on the Personality Styles/Traits of Leaders and Employees and the Impact on Culture of Trust within Organizations”, Dissertation, 2015.

[64] R. Borum. “The Science of Interpersonal Trust”. Mental Health Law and Policy Faculty Publications. Paper 574, 2010.

[65] M. Kosfeld, M. Heinrichs, P.J. Zak, U. Fischbacher and E. Fehr. “Oxytocin Increases Trust in Humans”. In: Nature, Vol. 435, 673–676, 2005.

[66] K.Y. Wang and S. Clegg. “Trust and Decision-making: Are Managers Different in the People’s Republic of China and in Australia?”. Cross Cultural Management, 9(1),30–45, 2002.

[67] E. Hall. “The Silent Language”. Anchor Press, New York, 1959.

[68] J. Golbeck. “Combining Provenance with Trust in Social Networks for Semantic Web Content Filtering”. IPAW 2006: 101–108, 2006.

[69] J.J. Gabarro. “The Development of Trust, Influence, and Expectations”. A. G. Athos and J. J. Gabarro, eds.Interpersonal Behavior:Communication and Understanding in Relationships. Prentice-Hall, Englewood Cliffs, NJ, 1978.

[70] F. Fukuyama. “Trust: The Social Virtues and the Creation of Prosperity”. New York: Free Press, 1995.

[71] D. Straker. “Changing Minds: in Detail”. Syque Press, 2008.

[72] J. Urbano, A.P. Rocha and E. Oliveira. “Computing Confidence Values: Does Trust Dynamics Matter?”. In Portuguese Conference on Artificial Intelligence, 520–531, Springer Berlin Heidelberg, 2009.

[73] J. Urbano, A.P. Rocha and E. Oliveira. “Extracting Trustworthiness Tendencies Using the Frequency Increase Metric”. In International Conference on Enterprise Information Systems, 208–221, Springer Berlin Heidelberg, 2010.

[74] L. Rasmusson. “Socially Controlled Global Agent Systems”. Master’s Thesis, Swedish Institute of Computer Science, 1996.

[75] A. Abdul-Rahman and S. Hailes. “Supporting Trust in Virtual Communities”. Presented at the 33rd Annual Hawaii International Conference on System Sciences, 2000.

[76] S. Grabner-Kräuter. “Web 2.0 Social Network: The Role of Trust”. Journal of Business Ethics, 90, 505–522, 2009.

[77] S. Grabner-Kräuter and B. Sofie. “Trust in Online Social Networks: A Multi-faceted Perspective”. Forum for social economics. Vol. 44. No. 1. Routledge, 2015.

[78] L. Rasmusson and S. Jansson. “Simulated Social Control for Secure Internet Commerce (position paper)”. In Proceedings, New Security Paradigms Workshop, Lake Arrowhead, 1996.

[79] B. Kaur and S. Madan. “Trust Concerns of the Customers in E-Commerce Market Space by Indian Customers”. 2015.

[80] D. Harrison McKnight et al. “What Trust Means in E-commerce Customer Relationships: an Interdisciplinary Conceptual Typology”. International journal of electronic commerce, 6(2), 35–59, 2001.

[81] D.H. McKnight, V. Choudhury and C.J. Kacmar. “Developing and Validating Trust Measures for e-Commerce: An Integrative Typology”. Information Systems Research 13 (3), 334–359, 2002.

[82] P. Palvia. “The Role of Trust in E-commerce Relational Exchange: A Unified Model”. Information and management, 46(4), 213–220, 2009.

[83] L. Solomon. “The Influence of Some Types of Power Relationships and Game Strategies upon the Development of Interpersonal Trust”. J. Abnormal Soc. Psych. 61(2), 223–230, 1960.

[84] R.E. Larzelere and T.L. Huston. “The Dyadic Trust Scale: Toward Understanding Interpersonal Trust in Close Relationships”. Journal of Marriage and the Family, 595-604, 1980.

[85] H.W. Kee and R.E. Knox. “Conceptual and Methodological Considerations in the Study of Trust and Suspicion”. Conflict Resolution, 14(3), 1970.

[86] J.K Lieberman. “The Litigious Society”. 1981.

[87] R.E. Kasperson, D. Golding and S. Tuler. “Social Distrust as a Factorin Siting Hazardous Facilities and Communicating Risks”. J. Soc.Issues48(4), 161–187, 1992.

[88] J.C. Anderson and J.A. Narus. “A Model of Distributor Firm and Manufacturer Firm Working Partnerships”. J. Marketing54(1) 42–58, 1990.

[89] R. Peters, V. Covello and D. MacCallum. “The Determinants of Trust and Credibility in Environmental Risk Communication: An Empirical Study”. Risk Analysis, 17, 43–54, 1997.

[90] S.D. Kamvar, M.T. Schlosser and H. Garcia-Molina. “The EigenTrust Algorithm for Reputation Management in P2P Networks”. In ’Proc. 12th International World Wide Web Conference’, 2003.

[91] A.A. Ahmed and I. Traore. "Intrusion Detector based on Mouse Dynamics Analysis". U.S. Patent Application No. 10/427,810, 2003.

[92] J.A. Golbeck. "Computing and Applying Trust in Web-based Social Networks". PhD dissertation, University of Maryland, 2005.

[93] Y. Sun, Z. Han and K.J.R. Liu. "Defense of Trust Management Vulnerabilities in Distributed Networks". IEEE Commun Mag 46(2):112–119, 2008.

[94] L. Page, S. Brin, R. Motwani and T. Winograd, "The PageRank Citation Ranking: Bringing order to the Web". Technical Report, Stanford Digital Library Technologies Project, 1998.

[95] C. Burnett, T.J. Norman, K. Sycara. "Bootstrapping Trust Evaluations through Stereotypes." In Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: volume 1-Volume 1, 241–248, International Foundation for Autonomous Agents and Multiagent Systems, 2000.

[96] X. Liu, A. Datta, K. Rzadca and E.P. Lim. "Stereotrust: a Group based Personalized Trust Model." In Proceedings of the 18th ACM conference on Information and knowledge management (pp. 7-16). ACM, 2009.

[97] Y.S. Han, L. Kim and J.W. Cha. "Computing User Reputation in a Social Network of Web 2.0". Computing and Informatics 31(2), 447–462, 2012.

[98] D.M. Rousseau, S.B. Sitkin, R.S. Burt, C. Camerer. "Not so Different after All: A Cross-discipline View of Trust". Academy of management review, 23(3), 393-404, 1998.

[99] M. Fishbein and I. Ajzen. "Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research". 1977.

[100] S. Grabner-Kräuter, E.A. Kaluscha, "Empirical Research in Online Trust: a Review and Critical Assessment". In: International Journal of Human-Computer Studies, 58(6), 783–812, 2003.

[101] B.M. Muir. "Trust in Automation Part I: Theoretical Issues in the Study of Trust and Human Intervention in Automated Systems". Ergonomics 37(11):1905–1922, 1994.

[102] Z. Yan and R. Yan. "Formalizing Trust Based on Usage Behaviours for Mobile Applications". In: Gonzalez Nieto, J., Reif, W., Wang, G., Indulska, J. (eds.) ATC 2009. LNCS, vol. 5586, 194–208, Springer, Heidelberg, 2009.

[103] Z. Yan, Y. Dong, V. Niemi and G. Yu. "Exploring Trust of Mobile Applications Based on User Behaviors". Lecture Notes in Computer Science, Springer Berlin Heidelberg, 212–226, 2010.

[104] B. Touhid, J. Audun and X. Yue. "Trust and Reputation Management in Web-based Social Network". Z. Usmani (editor), Web Intelligence and Intelligent Agents. In-Tech, Croatia, ISBN: 978-953-7619-85-5. ISBN 978-953-7619-85-5, 207–232, 2010.

[105] S. Iraklis, B. Filipe and P. Bart. "fRiendTrust: A Privacy Preserving Reputation System for Online Social Networks". In Proceedings of the IFIP Information and Communication Technology, Lecture Notes in Computer Science LNCS, J. Camenisch, and R. Leenes (eds.), Springer-Verlag, 17 pages, 2014.

[106] S. Adali, R. Escriva, M.K. Goldberg, M. Hayvanovych, M. Magdon-Ismail, B.K. Szymanski, W.A. Wallace and G.T. Williams. "Measuring Behavioural Trust in Social Networks". In Christopher C. Yang; Daniel Zeng; Ke Wang; Antonio Sanfilippo; Herbert H. Tsang; Min-Yuh Day; Uwe Glasser; Patricia L. Brantingham and Hsinchun Chen, ed., 'ISI' , IEEE, 150–152, 2000.

[107] D. Helbing. "A Mathematical Model for the Behaviour of Individuals in a Social Field". J. Math. Sociol. 19, 3, 189–219, 1994.

[108] T. Alpcan and C. Örencik and L. Albert and S. Erkay. "A Game Theoretic Model for Digital Identity and Trust in Online Communities". In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 341–344, 2010.

[109] B. Fabrício and R. Tiago and C. Meeyoung and A. Virgílio. "Characterizing User Behavior in Online Social Networks". In Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement Conference, ACM, 49–62, 2009.

[110] M. Richardson, R. Agrawal and P. Domingos. "Trust Management for the Semantic Web". International Semantic Web Conference 2003, Springer-Verlag, 351–368, 2003.

[111] A. Abdul-Rahman and S. Hailes, "A Distributed Trust Model". Proceedings of the 1997 Workshop on New Security Paradigms, ACM, 48–60, 1997.

[112] J. Golbeck, B. Parsia, J. Hendler. "Trust Networks on the Semantic Web". In 'Proceedings of Cooperative Intelligent Agents', 2003.

[113] F. Heider. "The Psychology of Interpersonal Relations". New Orkney, USA, Wiley, 1958.

[114] P.S. Chakraborty, S. Karform. "Designing Trust Propagation Algorithms based on Simple Multiplicative Strategy for Social Networks". Procedia Technology, 6, 534-539, 2012.

[115] P. Massa and P. Avesani. “Trust Metrics on Controversial Users: Balancing between Tyranny of the Majority”. International Journal on Semantic Web and Information Systems (IJSWIS), 3(1), 39-64, 2007.

[116] C.N. Ziegler. “Towards Decentralized Recomrmender Systems”. PhD dissertation, Institute for Informatik, 2005.

[117] J. Golbeck. “Trust on the World Wide Web: a Survey”. Foundations and Trends® in Web Science, 1(2), 131-197, 2008.

[118] S. Sodsee. “Placing Files on the Nodes of Perr-to-Peer Systems”. PhD dissertation, University in Hagen, Published in VDI Fortschrittsberichte Informatik, ISBN: 978-3-18-381610-1, Volume 218, Dusseldorf, 2012.

[119] M. Paolo, et al. “Trustlet, Open Research on Trust Metrics”. Scalable Computing: Practice and Experience 9.4, 2001.

[120] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez and D.U. Hwang. “Complex Networks : Structure and Dynamics”. Phys. Rep. 424 (4-5), 175–308, 2006.

[121] M. Granovetter. “The Strength of Weak Ties”, The American Journal of Sociology 78(6), 1360–1380, 1973.

[122] R. Zafarani, M.A. Abbasi, H. Liu. “Social Media Mining: an Introduction”. Cambridge University Press, 2004.

[123] R.W. Floyd. “Algorithm 97: Shortest Path”. Communications of the ACM, 5(6), 345, 1996.

[124] S. Capkun, L. Butty and J.P. Hubaux. “Small Worlds in Security Systems: An Analysis of the PGP Certificate Graph”. Proceedings of the 2002 Workshop on New Security Paradigms, ACM, 28–35, 2002.

[125] E. Gray, J. Seigneur, Y. Chen and C.D. Jensen. “Trust Propagation in Small Worlds”. The First International Conference on Trust Management, Springer Verlag, LNCS 2692, 2003.

[126] Kleinberg, Jon M. “Authoritative Sources in a Hyperlinked Environment”. J. ACM, 604–632, 1999.

[127] N. Benchettara, R. Kanawati, and C. Rouveirol. “A Supervised Machine Learning Link Prediction Approach for Academic Collaboration Recommendation”. In Proceedings of the fourth ACM conference on Recommender systems, RecSys 10, pages 253–256, New York, NY, USA, ACM, 2010.

[128] J. Leskovec, J. Kleinberg, and C.Faloutsos. “Graphs Over Time: Densification Laws, Shrinking Diameters and Possible Explanations”. In Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining, KDD 05, pages 177–187, New York, NY, USA, ACM, 2005.

[129] R. Kumar, J. Novak, and A. Tomkins. “Structure and Evolution of Online Social Networks”. In KDD 06: Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, pages 611–617, New York, NY, USA, ACM, 2006.

[130] M.E.J. Newman. “Fast Algorithm for Detecting Community Structure in Networks”. Physical Review E, 69(6):066133+, June 2004.

[131] L.C. Freeman. “Centrality in Social Networks: I. Conceptual Clarification”. Soc Netw 1:215–239, 1979.

[132] V. Nikolaos “Trust in Online Social Network”. Master thesis, University of Edinburgh, 2011.

[133] S. Vongsingthong, H. Unger and P. Meesad. “Identifying Clusters within Facebook’s User Behaviour”, Proceeding of the 8th GI Conference, Autonomous Systems 2014.

[134] S. Vongsingthong, S. Boonkrong and H. Unger. “Refining User Lifetime model by Big five Characteristics”, Proceeding of the 8th GI Conference, Autonomous Systems 2015.

[135] A.N. Langville and C.D. Meyer. “Google’s PageRank and Beyond: The Science of Search Engine Rankings”. Princenton University Press, 2006.

[136] R. Levien. “Attack-Resistant Trust Metrics”. In Jennifer Golbeck, ed., ’Computing with Social Trust’, Springer, 121–132, 2009.

[137] P. Erdős and A. Rényi. “On Random Graphs”. I. Publicationes Mathematicae Debrecen 6:290–97, 1959.

[138] M. Bui, T. Bernard, D. Sohier and A. Bui. “Random Walks in Distributed Computing: A Survey”. In Innovative Internet Community Systems, 1–14, Springer Berlin Heidelberg, 2004.

[139] H. Unger and T. Bohme. “A Decentralized, Probabilistic Money System for P2P Network Communities”. In: Proceedings of the Virtual Goods Workshop, Ilmenau, 60–69, 2003.

[140] W.H. Gomaa and A.A. Fahmy. “A Survey of Text Similarity Approaches”. International Journal of Computer Applications, 68(13), 2013.

[141] P.D. Turney. “Thumbs up or Thumbs down?: Semantic Orientation Applied to Unsupervised Classification of Reviews”. In Proceedings of the 40th annual meeting on association for computational linguistics, 417–424, Association for Computational Linguistics, 2002.

[142] R. Mihalcea and D. Radev. “Graph-based Natural Language Processing and Information Retrieval”. Cambridge University Press, 2011.

[143] B. Pang and L. Lee. “A Sentimental Education: Sentiment Analysis using Subjectivity Summarisation based on Minimum Cuts”. In: Proceedings of the 42nd Meeting of the Association for Computational Linguistics, 271–278, Barcelona, Spain, 2004.

[144] A. Esuli and F. Sebastiani. “PageRanking WordNet Synsets: An Application to Opinion Mining”. In: Proceedings of the Annual Meeting of the Association of Computational Linguistics, 424–431, Prague, Czech Republic, 2007.

[145] V.B. Raut and D.D. Londhe. “Survey on Opinion Mining and Summarization of User Reviews on Web”. International Journal of Computer Science and Information Technologies, 5(2), 1026-1030, 2014.

[146] A. Ortigosa, J.M. Martin and R.M. Carro. “Sentiment Analysis in Facebook and its Application to E-learning”. Computers in Human Behavior, 31, 527-541, 2004.

[147] A. Agarwal, B. Xie, I. Vovsha, O. Rambow and R. Passonneau. “Sentiment Analysis of Twitter Data”. In Proceedings of the workshop on languages in social media (pp. 30-38). Association for Computational Linguistics, 2011.

[148] A. Tumasjan, T.O. Sprenger, P.G. Sandner and I.M. Welpe. “Predicting Elections with Twitter: What 140 Characters Reveal about Political Sentiment”. ICWSM, 10, 178-185, 2010.

[149] C. Fellbaum. “WordNet: An Electronic Lexical Database”. Blackwell Publishing Ltd., 1998

[150] S. Baccianella, A. Esuli and F. Sebastiani. “Sentiwordnet 3.0: An Enhanced Lexical Resource for Sentiment Analysis and Opinion Mining”. Proceedings of LREC, 2200–2204, Retrieved 2014-04-05, 2010.

[151] SentiWS: `http://asv.informatik.uni-leipzig.de/download/sentiws.html`

[152] C. Strapparava and A. Valitutti. “WordNet-Affect: An Affective Extension of WordNet”. Proceedings of LREC, 1083–1086, 2004.

[153] A. Das. “Opinion Extraction and Summarization from Text Documents”. In Bengali (Doctoral dissertation, Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., Jadavpur University), 2011.

[154] P. Kralj Novak, J. Smailovic, B. Sluban and I. Mozetic. “Sentiment of Emojis”, 2015.

[155] B. Liu and L. Zhang. “A Survey of Opinion Mining and Sentiment Analysis”. In Mining text data, 415–463, Springer US, 2012.

[156] F. Holz, S. Teresniak. “Towards Automatic Detection and Tracking of Topic Change”. In: Alexander F. Gelbukh, ed., ’CICLing’ , Springer, 327–339, 2010.

[157] C. Biemann. “Chinese Whispers: an Efficient Graph Clustering Algorithm and its Application to Natural Language Processing Problems”. In Proceedings of the first workshop on graph based methods for natural language processing (73–80). Association for Computational Linguistics, 2006.

[158] H. Celia. “China Social Credit: Beijing Sets up Huge System”. BBC News. Retrieved 2015-12-23.

[159] H. Coltzau and H. Unger. “A Model Approach on Superpopular Contents in Online Networks”. 8th GI Conference on Autonomous Systems, Marlloca, 2015.

[160] H. Coltzau and M. Kubek. “User Triggered Structural Changes in OSN-alike Distributed Content Networks”. International Conference on Computing and Information Technology, 2016.

[161] U.G. Yule. “A Mathematical Theory of Evolution”. Based on the Conclusions of Dr. J. C. Willis, F.R.S. Philosophical Transactions of the Royal Society of London. Series B, Containing Papers of a Biological Character: 213, 21–87, 1925.

[162] D.H. McKnight, L.L. Cummings and N.L. Chervany. “Initial Trust Formation in New Organizational Relationships”. Academy of Management review, 23(3), 473-490, 1998.

[163] J.M. Seigneur. “Trust, Security and Privacy in Global Computing”. PhD dissertation, 2005.

[164] J. Tang, H. Gao, H. Liu, and A.D. Sarma. “eTrust: Understanding Trust Evolution in an Online World”. in The 18th ACM Conference on Knowledge Discovery and Data Mining (SIGKDD), 2012.

[165] M.N. Gibbs, D.J.C. MacKay, “Variational Gaussian Process Classifiers”. IEEE Transactions on Neural Networks and Learning Systems, 11 (6), 1458–1464, 2000.

[166] G. Piolle. "Affective Computing, Software Agents and Online Communities". Master's thesis, Imperial College London, Dpt of Computing (supervisors: Jeremy Pitt and Keith Clark), 2005.

[167] DAGExecutor:
http://www.java2s.com/Open-source/Java_Free_CodeDownload/d/DAGExecutor-master.zip

[168] D.J. Kim. "Self-perception-based versus Transference-based Trust Determinants in Computer-mediated Transactions: A Cross-cultural Comparison Study". Journal of Management Information Systems, 24(4), 13–45, 2008.

[169] C.S.P. Nguyen. "Intention to Purchase on Social Commerce Websites across Cultures: A Cross-regional Study. Information and management". 50(8), 609–620, 2013.

[170] S. Catherine. "Data From Alibaba's E-Commerce Sites Is Now Powering A Credit-Scoring Service". TechCrunch. Retrieved 2015-12-22.

[171] M. Blaze, J. Feigenbaum and J. Lacy. "Decentralized Trust Management". Proceedings of the 1996 IEEE Symposium on Security and Privacy, 1996.

[172] M. Blaze, J. Feigenbaum, J. Ioannidis and A.D. Keromytis. "The Role of Trust Management in Distributed Systems Security". In Secure Internet Programming, 185–210, Springer Berlin Heidelberg, 1999.

[173] J. Baumann, F. Hohl, K. Rothermel and M. Strasser. "Mole Concepts of a Mobile Agent System". World Wide Web, 1(3), 123–137, 1998.

[174] D. Kotz and R.S. Gray. "Mobile Agents and the Future of the Internet". Operating systems review, 33(3), 7–13, 1999.

[175] R.J. Thomas and T.D. Mount. "Using Software Agents to Test Electric Markets and Systems". IEEE Power Engineering Society General Meeting, 2808–2812, 2005.

[176] S. Erez, K.S. Vivek, L. Bruno and S.P. Alex. "Sensing, Understanding, and Shaping Social Behavior". Computational Social Systems, IEEE Transactions on 1.1: 22–34, 2014.

[177] Y. Dong, H. Chen, X. Tang, W. Qian, A. Zhou. "Prediction of Social Mood on Chinese Societal Risk Perception". In Behavioral, Economic and Socio-cultural Computing (BESC), International Conference on (102–108), IEEE, 2015.