APPLICATIONS OF ATTENTION ECONOMICS IN STUDYING EQUILIBRIA IN SOCIAL NETWORKING

By

SHENG YU

Bachelor of Science in Information Security
University of Electronic science and Technology of China
Chengdu, China
2007

Master of Science in Information and Communication Engineering
University of Electronic science and Technology of China
Chengdu, China
2010

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
DOCTOR OF PHILOSOPHY
December, 2014

APPLICATIONS OF ATTENTION ECONOMICS IN

STUDYING EQUILIBRIA IN SOCIAL NETWORKING

Dissertation Approved:

Dr. Subhash Kak

Dissertation Adviser

Dr. Christopher Crick

Dr. Eric Chan-Tin

Dr. Weihua Sheng

ACKNOWLEDGEMENTS

During my study, there are many people who helped me a lot to whom I wish to show my sincere gratitude. First of all, I want to thank my advisor Dr. Subhash Kak for his encouragement, guidance, and help throughout all my graduate study and research at Oklahoma State University. I would like to thank my committee members, Dr. Christopher Crick, Dr. Eric Chan-Tin, Dr. Weihua Sheng and Dr. Tingting Cheng who offered many valuable suggestions. I am also thankful to the members in the computer science department at Oklahoma State University for their support.

I want to thank my parents for their unconditional love and support during my whole life. Additionally, I want to thank my wife for supporting my in everything. I would never be able to live a complete life, let alone be able to complete the doctoral degree study, without them.

I would also like to thank my friends for their encouragement. In particular I would like to thank Dr. Rui Yang and Mr. Yang Jin for several insightful discussions.

Finally, I appreciate Tencent Inc, the organizers of KDD Cup 2012, for sharing the datasets of microblogging service with the public.

Name: SHENG YU

Date of Degree: DECEMBER, 2014

Title of Study: APPLICATIONS OF ATTENTION ECONOMICS IN STUDYING EQUILIBRIA IN SOCIAL NETWORKING

Major Field: COMPUTER SCIENCE

Abstract: Within social networking services, users construct their personal social networks by creating asymmetric or symmetric social links. They usually follow friends and selected professional users, such as celebrities and news agencies. On such platforms, attentions are used as currency to consume the information. The economic theory that deals with this situation of excessive information and scarce attention is called attention economics and it parallels standard economic theory although there are some interesting points of difference. In this dissertation, we use attention economic method to analyze interactions on social media. We statically and dynamically analyze a huge social graph with a manually classified set of professional users. The results show that the in-degree of professional users does not fit to power-law distribution. Conversely, the maximum number of professional users in one category for each user shows power-law property. We analyze the reasons of these phenomena wherein we consider questions of supply and demand, the game among professional users, the game among common and professional users, and the marginal utility of common users. The result of supply and demand determines the proportion of professional users in different subjects and the games strongly influence the profession users' interaction patterns. The marginal utility is the direct reason for users to follow and unfollow others. Finally, game theory from economics is applied to analyze the malicious URL attack on social media. Unlike other cyberspace, it is hard to directly publish malware or phishing page on social media. The attackers publish some bad-content URLs on social media, and lure users to click them with the URLs leading the users to the malicious page. These malicious URLs become the major gateway to further cyber-attacks on these platforms. We have shown that even with perfect and real-time detection algorithms, malicious URLs can easily snag many visitors, if they are checked by the system only once. We propose some countermeasures. Our research on the use of attention economics has demonstrated its significance for the study of social networks.

TABLE OF CONTENTS

Chapter Page

I. INTRODUCTION 1

II. TECHNICAL BACKGROUND AND RELATED WORKS 5

2.1. Social Network 5
2.2. Social Networking Service 7
2.3. Attention Economics 11
2.4. Uniform Resource Locator (URL) 12
2.5. Detecting Malicious URLs 15

III. DATASETS AND THEIR BASIC ANALYSIS 18

3.1. Social Graph Dataset 19
3.2. Professional Entities Dataset 21
3.3. The Uneven Distribution of Categories 25

IV. ANALYSIS ON HOW USERS ADOPT THE PROFESSIONAL ENTITIES 37

V. FOLLOWEE ADOPTION FROM AN ATTENTION ECONOMICS PERSPECTIVE 46

5.1. Game among Followees 46
5.2. Game among Followers and Followees 51
5.3. Marginal Utility 55

VI. MALICIOUS URLS ON SOCIAL MEDIA 60

6.1. Why Malicious URLs Are Widely Used on Social Media 60
6.2. The Simplest Model of One-Time Check Scheme 63

Chapter Page

6.3. The Model of One-Time Check Scheme with Constant-Rate Partial Attack 65
6.4. The Simplest Model of One-Time Check Scheme with Hibernation 70

VII. DISCUSSION, FURTHER WORK AND CONCLUSION 81

7.1. Discussion 81
7.2. Future Work 83
7.3. Conclusion 85

REFERENCES 87

LIST OF TABLES

Table Page

Table 3-1.The Brief Distribution of Top 100 Twitter Followees in Categories 35
Table 5-1. The Game between One Followee and One Follower 51

LIST OF FIGURES

Figure Page

Figure 2-1. Two Major Social Network Models 6
Figure 2-2. A Snapshot of Coca-Cola on Twitter 9
Figure 2-3. A Social Network Example and Corresponding Bipartite Graph 10
Figure 2-4. A General Process to Access a Webpage 13
Figure 3-1. The Out-Degree Distribution of Followers 19
Figure 3-2. The In-Degree Distribution of Followee 20
Figure 3-3. The In-Degree Distribution of Professional Entities 21
Figure 3-4. The log-log Plot of In-Degree Distribution of Professional Entities 22
Figure 3-5. The Distribution of Professional Entities in Each Category 25
Figure 3-6. The Demand Curve of Single User for Tweets and Followees in One Topic 26
Figure 3-7. The Aggregate Demand-Aggregate Supply Curves for Followees in One Topic 30
Figure 4-1. The Distribution of Maximum Number of Professional Followees in One Category (MPFC) 38
Figure 4-2. The Distribution of MPFC with Part of the Users 39
Figure 4-3. Percentage Cumulative Distribution of MPFC 40
Figure 4-4. The Distribution of Adoption Rate 41
Figure 4-5. The Adoption Simulation 43
Figure 5-1. The Hotelling's Model 48
Figure 5-2. An Example of Law of Diminishing Marginal Utility 56
Figure 6-1. The Payoff of Attackers and Defender I - Always Malicious 64

Figure Page

Figure 6-2. The Payoff of Attackers and Defender II – Partial Malicious 67
Figure 6-3. The Relation between Detection Rate and Maximal Attacker Payoff 69
Figure 6-4. The Attacker's Payoff under Best Security 70
Figure 6-5. The Extended Form of the Game 71
Figure 6-6. The Payoff of Attackers and Defender III – With Hibernation 72
Figure 6-7. The Mixed Strategy at the Nash Equilibrium 76

CHAPTER I

INTRODUCTION

A Social Networking Service (SNS) consists of online sites and applications that have three components: users, social links, and interactive communications. During recent years this kind of service has advanced greatly and changed our lives undoubtedly.

Within the social networking services, users mirror social relations in real life, build new social connections based upon interests and activities, or both. When building new social links, users typically adopt different kinds of professional entities. For example, on Twitter, a user might follow BBC Breaking News (@BBCBreaking) for news and Johnny Depp (@J0HNNYDepp) for personal preference.

Three worldwide popular SNS providers, Twitter, Facebook, and Tencent (qq.com), demonstrate the explosive growth and profound effect of this service. According to Alexa ranking, these three providers are in the top 10 most-visited websites in the world. The least known of these three services, Tencent Inc., is the biggest social networking platform in China. Tencent Weibo, which has 425 million registered users and 67 million daily users, is a major production of Tencent Inc. Actually, to serve specific social needs of different groups, we have different types of social media. For instance, for friendship maintenance, we have Facebook and Twitter. For fashion things, Pinterest is a leading platform. And for professional networking, LinkedIn does a good job. Apparently, they have become an integral part of our daily life.

The popularity of these platforms even leads to the creation of new jobs such as Director of Social Media in Coach and Social Media Marketing Manager in Fandango, just to name two well-known companies. From this perspective, social media platforms seem to create a new world. Both the general public and businessmen get uncountable benefits from social media.

Although social media sites have created the new ways to communicate, the question may be asked, if foundational interaction patterns have changed? We say hello to someone on Facebook, as same as we do that in real world, because we are friends. In reality, we might get bored with some ads, and wish them to stop. Similarly, on Twitter, if we do not want any more messages from some organization, we will unfollow it. Social media just reallocates our time and attention from physical world to the cyberspace. But the entities and the interactions stay essentially the same.

The claim can be made that there is no social media science, and it is just a special case of well understood social interaction on brand new platforms. On one hand, psychology and economics explain the users' motivations and interactions and maybe predict them. On the other hand, computer science, such as big data and machine learning, serves as a powerful tool to investigate and confirm the result.

Academic research work has been done to analyze social networks and social media with computer science and other human sciences. In particular, attention economics tries to combine computer science and economics for social media.

In the usage of social media, the common user, as information seeker, uses attention as currency. Information and interaction among the users determine the messages' utility. Professional users and friends, as information providers, receive the attention to increase their influence. In such a system, information always tends to be excessive and attention is in scarcity.

Economic theory that deals with this situation of excessive information and scarce attention is attention economics. Attention economics is essentially different from the traditional material economics, which is based upon excessive consumption demand and scare resources supply. At the same time, they have much in common, because both of them study production, distribution and consumption of some material and/or information. As a result, when we do research on social media and social networking, we have to keep both the difference and the consistency into consideration.

One significant barrier in this research is the difficulty in measuring the users' attention on social media. Even though qualitative analysis is part of economics, quantitative methods are more significant. Without numerical measurements, the application of economic theories and methods in social media research is not always feasible.

We used qualitative economic method to analyze interactions on social media and social networking. Supply and demand models help in analyzing the volume of professional users in each realm. Game theory and utility theory explain how users follow others in different fields. Furthermore we used game theory to investigate the threat of malicious URLs on social media, and argued for the need of multi-check schemas.

We statically and dynamically analyze a huge social graph with a manually classified set of professional users. The results show that the in-degree of professional users does not fit to power-law distribution. Conversely, the maximum number of professional users in one category for each user shows power-law property. After that, from an attention economics perspective, we discuss the reasons of these phenomena with the supply and demand, the game among professional users, the game among common and professional users, and the marginal utility of common users. The result of supply and demand determines the proportion of professional users in different subjects.

These games strongly influence the profession users' interaction patterns and the marginal utility is the direct reason for users to follow and unfollow the others.

Finally, game theory from the perspective of economics is applied to analyze the malicious URL attack on social media. Unlike other varieties of cyberspace, it is hard to directly publish malware or a phishing page on social media. The attackers typically publish some bad-content URLs on social media and lure users to click them, which will lead the users to the malicious page. Such malicious URLs become the major gateway to further cyber-attacks on these platforms. We use game theory to analyze the threat of the malicious URLs on social media. We have shown that even with perfect and real-time detection algorithms, malicious URLs can easily snag many visitors, if they are checked by the system only once.

The rest of the dissertation is organized as follows: in chapter 2, some technical background and related research works are introduced. Chapter 3 describes the dataset and discusses why the distribution of professional entities is not similar among different categories. Static and dynamic analyses of the dataset are discussed in chapter 4, and further discussion is provided in chapter 5. The discussion about malicious URLs on social media is provided in chapter 6. Chapter 7 talks about the work that remains to be done in the future. Conclusions are presented in chapter 8.

CHAPTER II

TECHNICAL BACKGROUND AND RELATED WORKS

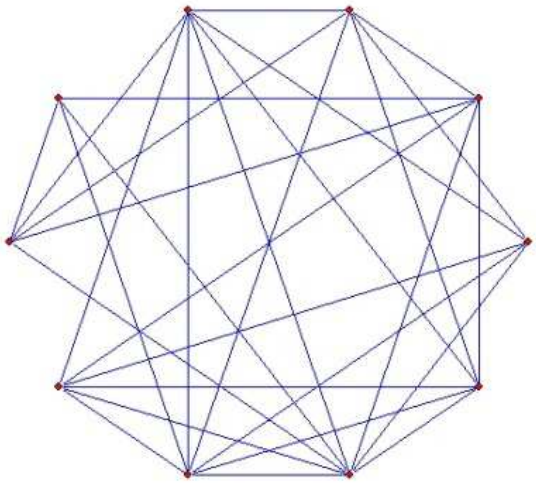
In this section, technical background and related research works are discussed. Firstly, we introduce the concept of social network and describe main features of social networking service. Then we discuss attention economics, which has the potential of explaining several phenomena related to social networking service. Finally, we provide the background and characteristics of URL and DNS system.

2.1. Social Network

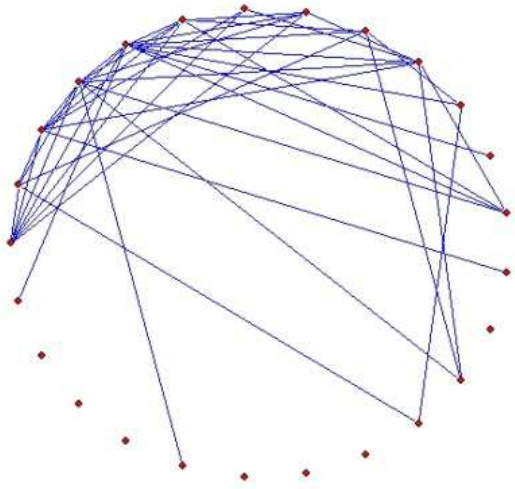
A social network represents varieties of social structure. Persons and/or organizations are usually represented as nodes in the network and social relations correspond to the connections among nodes (Borgatti, Mehra, Brass, & Labianca, 2009). The social relation could be both explicit, such as kinship and classmates (Acock & Hurlbert, 1990), and implicit, as in friendship and common interest (Guo & Chen, 2010)(Cha, Mislove, & Gummadi, 2009). As shown in Fig. 2-1.1, the small world and the scale free are two significant properties of social networks.

When a social network is viewed as a small world network, most nodes can reach every other node through a small number of links (D J Watts & Strogatz, 1998)(Kleinberg, 2000). In the real world, the famous theory of "six degree of separation" suggests that, on average, any two persons could be linked within six hops.

The situation in online SNS is somewhat different. The average distance on Facebook in 2008 was 5.28 hops, while in November 2011 it became 4.74 (Facebook Data Team, 2012). In MSN messenger network that contains 180 million users, the median and the 90th percent degree of separation are 6 and 7.8, respectively (Leskovec & Horvitz, 2008). On Twitter, the median, average, and 90th percent distance between any two users are 4, 4.12 and 4.8, respectively (Kwak, Lee, Park, & Moon, 2010). In other words, the degree of separation varies on different SNS platforms and it changes with time.



(a) Small World Network



(b) Scale Free Network

Figure 2-1. Two Major Social Network Models

At the same time, other researchers argue that social networks are not connected as strongly as indicated by a straightforward analysis (Huberman, Romero, & Wu, 2008). In the measurement of users' distance, it is customary to include all connections. But if we only consider connections with some communications, the number of friends is approximately half of the total number of followees on Twitter. Thus in the friends' network, the degree of separation should be greater than that in the original network.

Many properties of social networks show scale free property (Ebel, Mielsch, & Bornholdt, 2002)(Duncan J. Watts, 2004), that is, the degree distribution asymptotically follows a power law. For example, on Twitter, the number of followees/followers fits the power-law distribution with the exponent of about 2.276 (Kwak et al., 2010). In addition, the number of tweets being retweeted and mentioned on Twitter also follows a power law (Cha, Haddadi, Benevenuto, & Gummadi, 2010). If we take the number of followers as the sole indicator of influence, as power law implies, the information propagation and trend promotion are strongly influenced by a set of information "oligarchs".

2.2. Social Networking Service

The social networking service embraces collections of online websites, applications, and platforms, which allow users to build social network and provide additional services (Ahn, Han, Kwak, Moon, & Jeong, 2007)(Wilson & Nicholas, 2008). A social network could be symmetric or asymmetric. In symmetric SNS such as Facebook, undirected social relations must be confirmed by both peers. Conversely, in an asymmetric SNS like Twitter, the directed social link could be made without the explicit permission from the destination user.

Different users publish their opinions and experiences via SNS. Therefore, SNS aggregates crowd wisdom and different standpoints. If extracted and analyzed properly, the data on SNS can lead to successful predictions of some human related events in a near-time horizon (Asur & Huberman,

2010)(Tumasjan, Sprenger, Sandner, & Welpe, 2010)(Yu & Kak, 2012). Even though currently most predictions using social media can be done better by human agents who are experts, automatic prediction with data on social media still has great potential.

Firstly, compared with human labor, automatic prediction with machines has much lower costs (Bothos, Apostolou, & Mentzas, 2010). Secondly, persons tend to overvalue low probabilities and undervalue high probabilities. Consequently events with low and high probabilities are poorly predicted by people (Wolfers & Zitzewitz, 2004). Thirdly, intentionally or unintentionally, a person may make decision influenced by their desire, interests and benefit, not purely based upon objective probability (Wolfers & Zitzewitz, 2004)(Hanson & Hanson, 2006). Lastly, automatic prediction methods could process greater amount of data and provide response quickly.

In this dissertation, we focus on microblogging service, one kind of asymmetric social networking services. First of all, we present some definitions.

Follow: user *a* follows user *b* means that there is *a* directed social link from *a* to *b*.

Follower/*Followee*: if user *a* follows user *b*, *b* is *a* followee of *a*, and *a* is a follower to *b*.

Professional entity: professional entities are influencers on social networking service. They are typically celebrities, famous organizations, and some well-known groups. In this chapter, we focus on the followees being professional entities, which are named as *professional followees*.

Tweet: the form of message. In our discussion, tweets are not specific to the messages on Twitter, but to all kinds of information pieces on microblogging services.

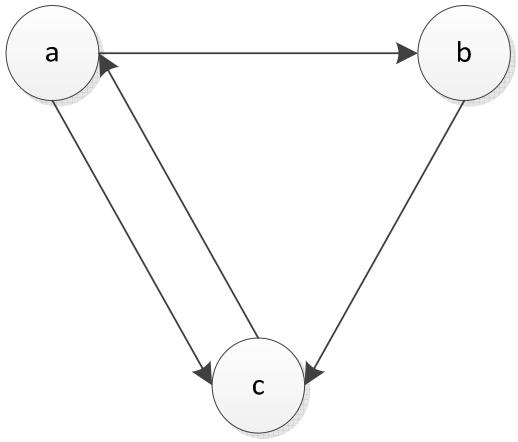
The user intention on social media could be roughly classified into three categories: information sharing, information seeking, and friendship maintenance (Java, Song, Finin, & Tseng, 2007). For common users, their activity is motivated by a mix of these three inspirations. But for professional users, the overwhelming purpose of their existence and operation is providing

information to the public. As shown in Fig 2-2, the Coca-Cola Company treat Twitter platform as a promotion and customer service channel.

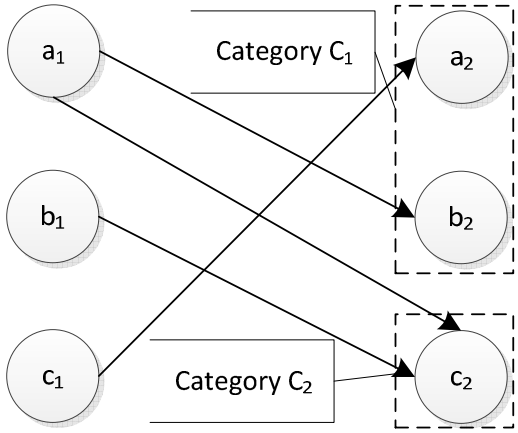
Figure 2-2. A Snapshot of Coca-Cola on Twitter

Focusing on directed relationships, we could convert the original social network $G = (V, E)$ into a bipartite graph $G' = (U', V', E')$. For a user u, who is a follower to others and followee of someone else, we "divide" user u into two nodes as u_1 and u_2 in G'. The u_1 represents the follower role of U, while u_2 denotes the followee role. As a result, the U' in G' includes all followers nodes, and V' contains all followees nodes. For each edge $\{a, b\}$ in G, we could construct an equivalent edge $\{a_1, b_2\}$ in G'. Figure 2-3 demonstrates the equivalent bipartite graph for a social network example.

Within a real social networking service, an overwhelming proportion of users are followers and followees at the same time. Thus the bipartite graph is nearly a balanced bipartite graph.



(a) Social Network Example



(b) Corresponding Bipartite Graph

Figure 2-3. A Social Network Example and Corresponding Bipartite Graph

In this dissertation, we discuss how common users adopt professional users. As a result, we exclude some nodes in V', which represent the non-professional entities. For example, in Fig. 2-3(b), if user *b* was not in our professional users' dataset, the node b_2 and all directed edges that end with b_2 would be removed.

Furthermore, we group the remaining nodes in V' into categories according to a human-labeling dataset. For instance, users *a* and *b* are in the same category C_1, while *c* is in the different group C_2.

2.3. Attention Economics

Attention economics is a new branch of economics, which treats the individual's attention as a resource (Michael H Goldhaber, 1997)(Pope, 2007). The development of attention economics stems from the rise of information industry (Essig & Arnold, 2001)(Evans & Wurster, 1997).

In the pre-information age, most items of exchange in the economic system were physical. In the information era, we also exchange items of information. These items of information can lead to wealth that is beyond our expectation (Erik & Joo, 2013). The production and consumption of information have some significant differences from the material world.

In the economy of material things, most of wanted products are scarce, such as computers, food, and land. These economic goods form the basis of exchange in society and determine the fabric of our daily life. In the economy of information, goods and information items are not scarce, but rather excessive in most cases. For example, according the statistics of YouTube[1], there are about 74 hours of video, newly uploaded every minute. No one could watch all the videos in just YouTube, let alone the whole Internet. In one word, this is an extreme buyer's market.

Within traditional economics, when we produce goods, we have to consider both the fixed cost and variable cost. The production of an additional piece involves additional cost, which is the marginal cost. In information economy, research and development of new products cost a lot, while reproducing an item of information costs very little. For example, Microsoft spent millions of dollars to finish Windows 8. However once you get a copy of it, the cost to make an additional copy is less than ten dollars. Compared with the fixed cost, the marginal cost is next to zero.

The circulating currency is also different. In the material world, currency is a kind of generally accepted medium for exchange of goods and services. No matter what is the specific form of currency, it reflects one's ability to get the items and this ability varies greatly among people. In

[1] http://www.youtube.com/yt/press/statistics.html

the information economy, the currency is changed to users' attention, of which everyone holds nearly the same amount. For instance, we could access the website of U.S. News for its news and reports without even a penny. However we do pay our attention to U.S. News which adds to its reputation.

In spite of being different in some ways from traditional economics, attention economics must also deal with three basic questions: What to produce? How to produce? And for whom we produce? Individual preferences and technology are the keys to answer these questions.

2.4. Uniform Resource Locator (URL)

URL is a character string to indicate some resource globally. In the simplest case, URL contains a schema name, a host name, and a full path for the resource. The schema name specifies the protocol to handle the URL. Some common schemas include http(s) for web pages, ftp for transferring files, and mailto for emails. Considering the URLs with http(s) protocol are the major part of malicious URLs, we only consider the http(s) URLs in the following discussion. In the host name section after schema name, there is a string as domain name such as "example.org" or an IP address like 93.184.216.119. After that, the remaining part of the URL is the full path of one resource in the host.

URL acts as a name tag. It helps persons to recognize and remember the resources. However, it does not mean, one URL is strictly associated with one physical resource. This feature could be used to enhance the servers' reliability. For example, when you type "google.com" in your web browser, the DNS system will translate the domain name into an IP address, whose corresponding host is estimated to have a good performance for you. In addition, this feature could customize the webpage for different users. A website's homepage typically shows different content to different login users.

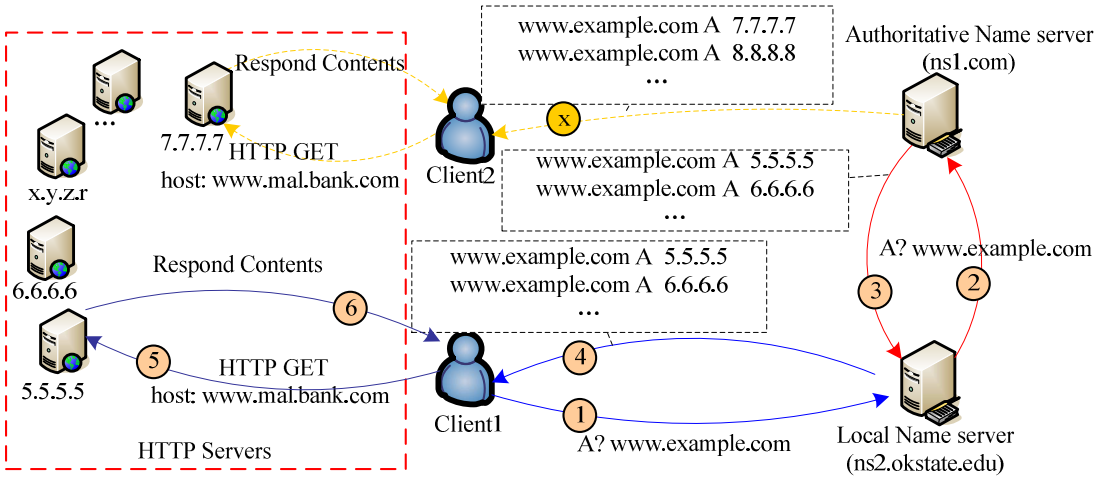


Figure 2-4. A General Process to Access a Webpage

To achieve the dynamic of URL, there are generally three methods. Firstly, if the host name section is a string as domain name rather than an IP address, which is the most common case, some DNS techniques could be applied (Mockapetris, 1987)(Yu, Zhou, & Wang, 2010). DNS is a global database system, which maps domain names to IP addresses. When a user (client) wants to access the website, it firstly looks up the IP address of the domain before it downloads the web page from the host. The client queries its local name server. After recursive queries and/or iterative queries, the name server sends back zero or one or more records for the domain name. Finally the client could communicate with the specified server to fetch the webpage content. Essentially the mapping between domain names and IP addresses is managed by a single or a set of name server(s). For the query about one domain name with multiple servers, the name server might return a random server's IP, or the physical-closest server's IP, or the best-performance server's IP. Under such circumstance, two clients may access different resources on different servers, even though they are using one completely same URL. In the Fig. 2-4, when two different users try to access the website www.example.com, both clients need to translate the domain name www.example.com to an IP address. The DNS servers return different IP sets to

these two clients. Consecutively, after the DNS query stage, the two clients will contact two different hosts.

Secondly, the web server could redirect the users from the initial URL to some other ones. URL redirection is also referred as URL forwarding. It leads the client to move from the original URL to the destination URL without client's operation. For example, if the client accesses the webpage http://www.wikipedia.com/wiki/URL_redirection, they are firstly redirected to http://www.wikipedia.org/wiki/URL_redirection. Then they are forwarded to the final destination http://en.wikipedia.org/wiki/URL_redirection. The URL redirection could be done with HTTP status codes, HTTP response header, and JavaScript redirection. Sometimes, a single HTML frame, that contains the target page, is also considered as URL redirection. In the Fig. 2-4, in the sixth step, the web server could redirect the clients to any other URL, instead of returning the actual content.

Finally, the web server could return different content to the end users under different rules. These rules are completely managed by the web application and administrator. The techniques to generate customized content can be either server-side or client-side dynamic web pages. With server-side dynamic web page, the customized content is generated by server-side scripts such as PHP or Python. In contract, the client-side dynamic happens at the clients, usually in the Internet browsers. The most widely used client side dynamic script is JavaScript. For example, in the Fig. 2-4, the web server 5.5.5.5 could act as a reverse proxy for multiple hosts, rather than the actual content host. It might take the requests from all clients in Asia, forward them to the host 7.7.7.7, and finally return the response content from 7.7.7.7 to the original clients. Differently for all the requests from Europe, it services as the proxy between clients and host 6.6.6.6. All the clients are completely unaware of the host 7.7.7.7 and 6.6.6.6. However, the clients are actually communicating with different hosts for different content.

2.5. Detecting Malicious URLs

With the development of the Internet, the cyber-attack is much more serious than before. Nowadays, the malicious URLs have become one of the major threats on Internet. They are related with the phishing site, malicious software distribution, and spam.

On social media, the providers are always running some security protections. It is next to impossible to use these platforms to host the malicious software directly. Spam and phishing page are possible in some sites, like Facebook. However, the users' report and platform's direct blocking make this choice less economic for attackers and the malicious content will become unavailable in a short time. Additionally limited by the content length in some media like Twitter, it is hard to post information with full phishing/spam content.

To handle with the new circumstance, the cyber-attackers deploy the URLs on social media for their attack purpose. On one hand, the URLs could be used to lead social media users to external attack sites (Chu, Gianvecchio, Wang, & Jajodia, 2010) (Grier, Thomas, Paxson, & Zhang, 2010)(McGrath & Gupta, 2008). As a result, their attacks are no longer restrained by the original content type and length limitations.

On the other hand, publishing the URLs instead of the malicious content enhances the attack's robustness. If the attackers post the malicious content directly on social media platforms, it is hard to update these posts automatically. Therefore, we could treat the contents as static, and the attack detection system could easily recognize them. With posted URLs, the attackers have complete control over the final content for the given URLs. They could modify the contents as quick as they want (Yu et al., 2010). What is worse, the URL could show different contents to security agencies and common users, which makes the detection much harder.

As a result of constraints of social media platforms and advantages of URLs, the malicious URLs become the major gateway to further attacks on social media. To cope with them, many malicious

URLs detection schemes are proposed (Zhao & Hoi, 2013)(Canali, Cova, Vigna, & Kruegel, 2011)(Obied & Alhajj, 2009). Some of them are specially designed or optimized for the ones on social media (S. Lee & Kim, 2013)(Thomas, Grier, Ma, Paxson, & Song, 2011). All these detection schemes can be categorized as account feature based detection, relation feature based detection, and content feature based detection. Some of these systems are original designed for spam detection on social media. They also work well for finding out malicious URLs, because the URLs in spam posts are typically malicious.

Account feature based detection check the features of the accounts (Benevenuto, Magno, Rodrigues, & Almeida, 2010) (K. Lee, Caverlee, & Webb, 2010) (Stringhini, Kruegel, & Vigna, 2010). These methods focus on the signatures of the spam senders such as the account creation date, the number/ratio of followers and followees, and the proportion of the tweets with and without URLs. These features are easy to extract and use. At the same time, the attackers can easily bypass these detection systems, by adding some fake "friends" and publishing more normal tweets. These detection systems cannot identify all the suspicious accounts, but do increase the operating cost of the attackers.

Relation feature based detection investigates a bigger social graph, rather than only the individual users (Song, Lee, & Kim, 2011) (Yang, Harkreader, & Gu, 2011). Social graph is the individual users, as the nodes, and their social connections, as direct links among nodes. These methods are based upon more robust features including the distance and shared friends. For example, even though the attackers could add many fake accounts as their friends, it is unlike that the attackers and common users share a noticeable number of common friends. Unfortunately these schemes have a significant shortage: they need lots of time and resources to extract and compute these metrics, because of the huge size of the social graph.

Content feature based detection focuses on the URLs and corresponding webpages (Canali et al., 2011) (Thomas, Grier, Ma, et al., 2011) (Thomas, Grier, Song, & Paxson, 2011) (S. Lee & Kim, 2013). These schemes statically or dynamically fetch the webpages and inspect the whole life cycle of fetching, including the lexical feature of URLs, the DNS responses, the redirection of URLs, and the contents of the final webpages. These operations need less time than analyzing the social graph, and have a quite good accuracy. However, malicious servers may block these crawlers according to their signatures such as IP addresses and browser fingerprinting (Eckersley, 2010). These hosts also may provide different contents at different time to bypass the detection systems (Thomas, Grier, Ma, et al., 2011).

CHAPTER III

DATASETS AND THEIR BASIC ANALYSIS

In this section, we introduce our dataset, and give some basic characteristics of it. Then we consider the reason for the uneven distribution of professional followees in different categories.

Our dataset was published by Tencent Weibo for KDD Cup 2012[2]. Tencent Weibo was launched in April 2010, and is currently one of the largest microblogging providers in China. As a major platform of SNS, it has 425 million registered users, 67 million daily users, and 40 million new messages each day. The dataset is a sampled snapshot of Tencent Weibo, including user profiles, social graph, professional entities, professional followee adoption history, and so on. Here we only use these three datasets, including social graph, professional entities, and adoption history, for our analysis.

Social graph: contains all the following information at the sample time of the selected users, who were the most "active" ones during the sampling period.

Professional entities: includes all the information of professional users. A professional entity is a special user in Tencent Weibo to be recommended to other users. Typically, well-known celebrities, organizations and groups are selected to be the professional entities. The professional entities and their categories were chosen and assigned by Tencent Inc.

[2] http://www.kddcup2012.org/c/kddcup2012-track1/data

Adoption history: indicates that records of users' new adoption of professional entities in the sampling period. This dataset contains both rejections and acceptances records.

In the remaining part of this section, we will introduce and analyze the first two datasets. The adoption history dataset will be discussed when it is used in section 4.

3.1. Social Graph Dataset

Firstly, we give a brief description of the social graph dataset. There are 1,944,589 users, including 1,892,059 followers, 920,110 followees in the dataset. Because this is a sampled snapshot, the dataset is asymmetrical. With 50,655,143 social link records, the average out-degree for followers is 26.77, and the average in-degree for followees is 55.05. The distributions are partly shown in Fig. 3-1 and Fig. 3-2. Similar to the results in previous research (Kwak et al., 2010)(Mislove, Marcon, Gummadi, Druschel, & Bhattacharjee, 2007), we find that both the out-degree and in-degree distributions fit to power-law.

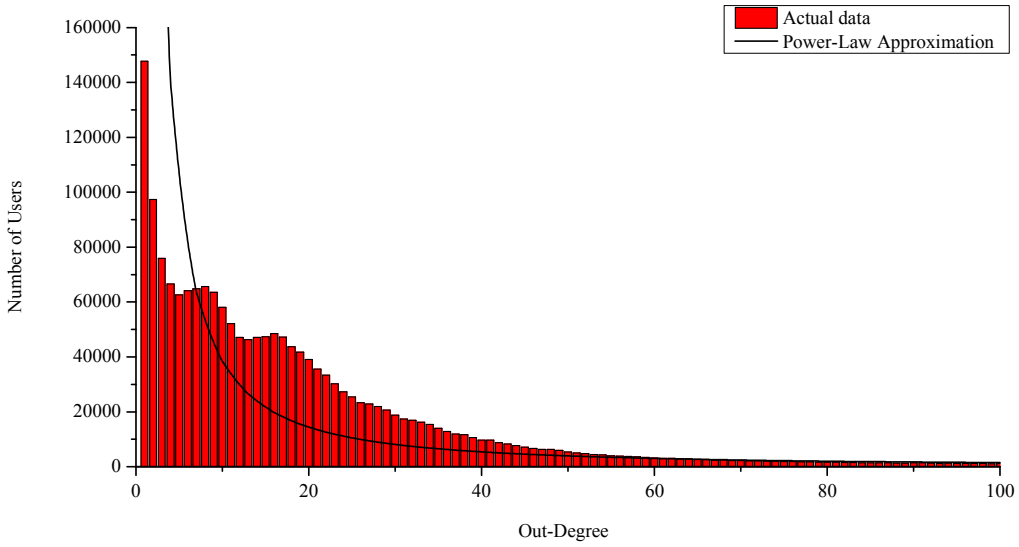


Figure 3-1. The Out-Degree Distribution of Followers

Among 1,892,059 followers, there are 83,474 users following more than 100 followees. They account for only 4.41% of the population and are not included in Fig. 3-1. In total, the minimum, median, 90th percent, and maximum out-degree are 1, 14, 52, and 5188, respectively. Considering only the data in Fig. 3-1, the out-degree distribution approximately fits the following power-law distribution with R^2 of 0.858:

$$Number\_of\_Users = 10^6 \times Out\_Degree^{-1.415} \tag{3-1}$$

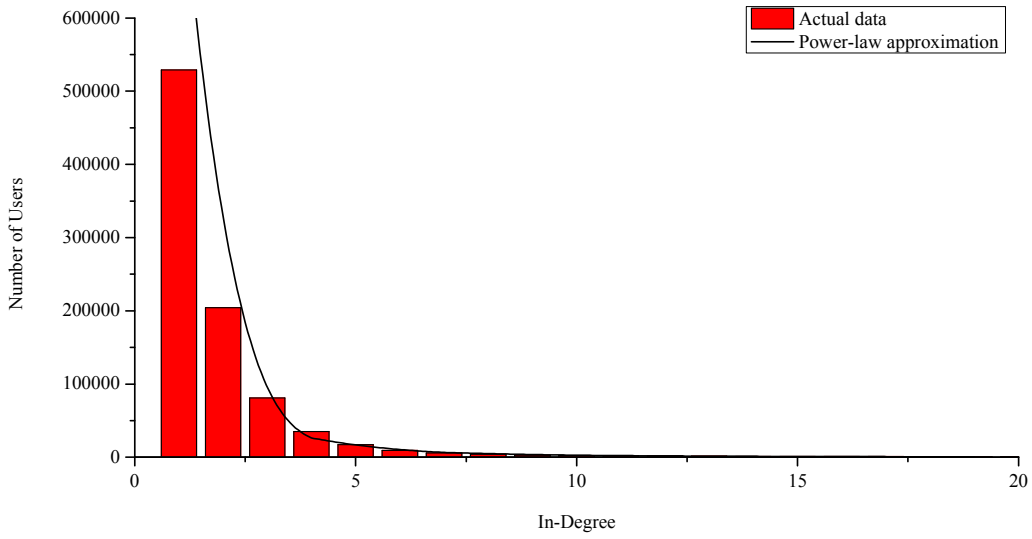


Figure 3-2. The In-Degree Distribution of Followees

Out of these 920,110 followees, 19,538 users, about 2.12% in proportion, are followed by more than 20 other users. These 19,538 followees are not shown in Fig. 3-2. Overall, the minimum, median, 90th percent, and maximum in-degree are 1, 1, 4, and 456,827, respectively. Additionally, only taking the in-degree being equal to or less than 20 into consideration, the in-degree distribution can be approximately represented as the following power-law equation with R^2 being 0.9899:

$$Number\_of\_Users = 840935 \times In\_Degree^{-2.501} \tag{3-2}$$

3.2. Professional Entities Dataset

The professional entities dataset includes all professional users, which are chosen for the followee recommendation system. There are 6,095 professional entities in the dataset. The professional entities and their categories were chosen manually by Tencent Inc. Only 5,796 of them, about 95.09%, are involved in the social graph dataset. The distribution of these professional entities' in-degree is shown in Fig. 3-3, including 4,930 professional entities with 10,000 or less followers.

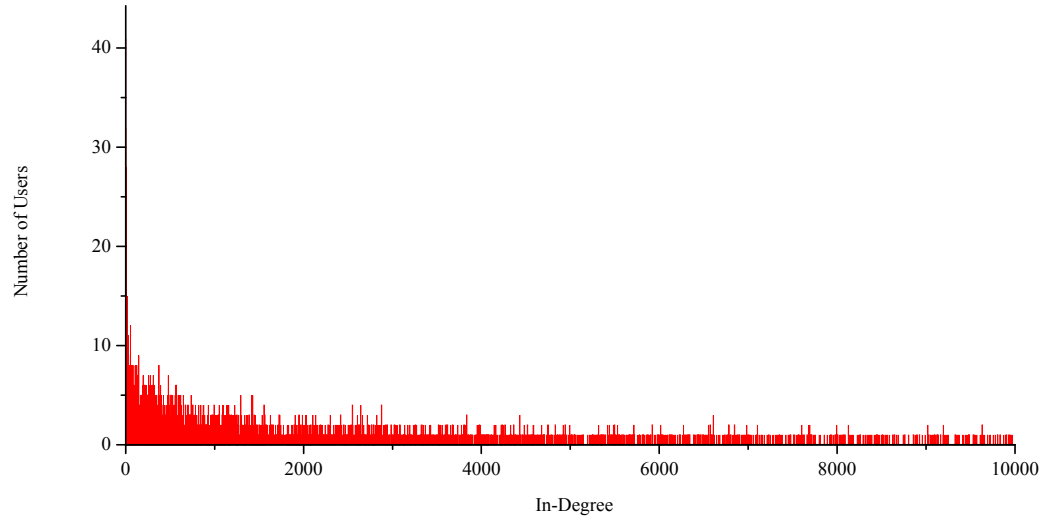
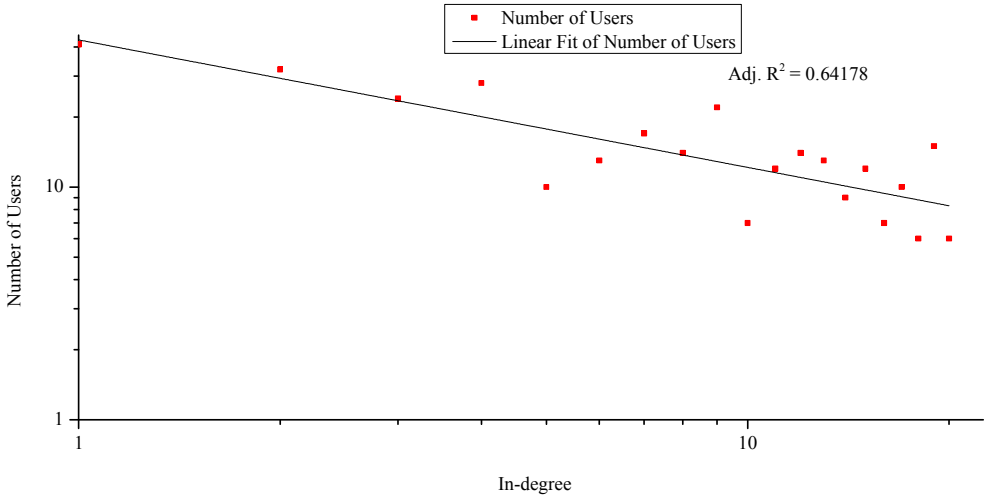


Figure 3-3. The In-Degree Distribution of Professional Entities

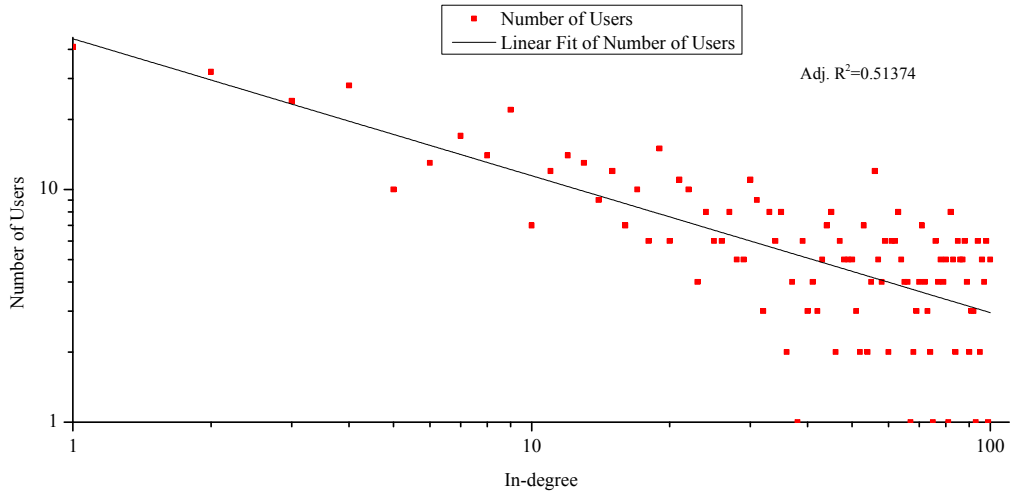
There are 866 professional entities with more than 10,000 followers. These entities account for about 14.94% of the population and are not shown in Fig. 3-3. Totally, there are 44,427,963 social links to these professional entities. Additionally, the minimum, median, average, 90th percent, and maximum in-degree are 1, 1,288, 7,665, 16,509, and 456,827, respectively.

Compared with the in-degree of overall users, which is shown in Fig. 3-2, the professional entities set has much more followers. Subjectively, these professional entities are well known. Their influence and reputations make them likely to be identified among millions of users. Additionally,

and objectively on the Internet, the professional entities are more likely to be reliable and stable information sources. Consequently, the masses need to follow them to get needed information.

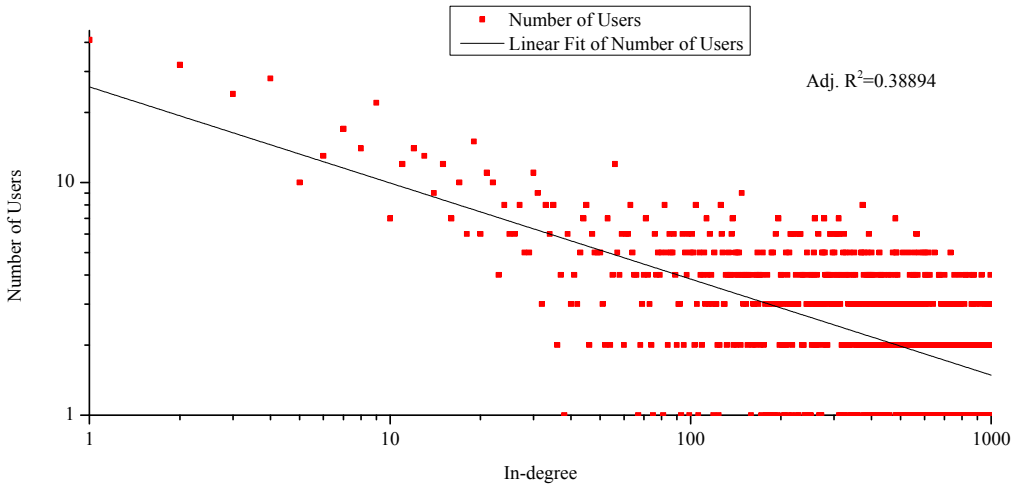


(a) With In-degree≤20 (5.38% of all)

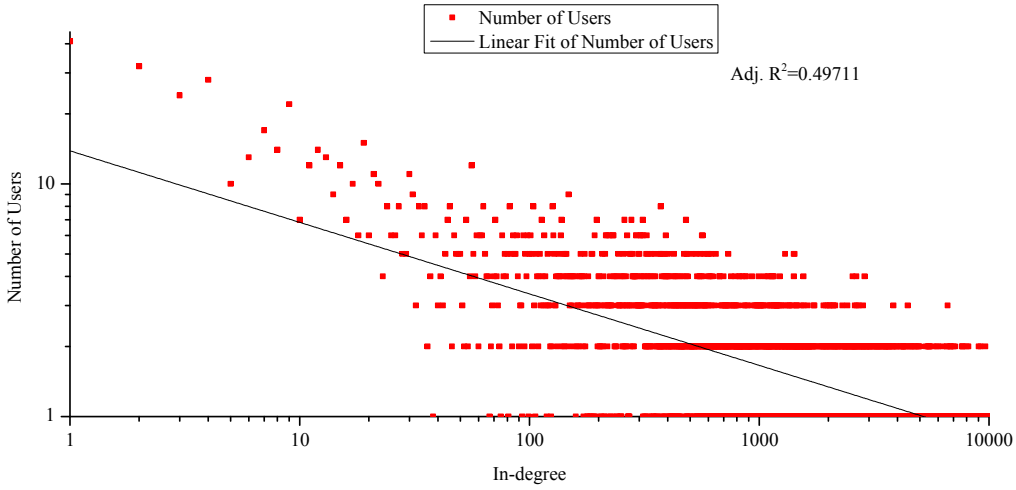


(b) With In-degree≤100 (12.03% of all)

Figure 3-4. The log-log Plot of In-Degree Distribution of Professional Entities



(c) With In-degree≤10^3 (44.74% of all)



(d) With In-degree≤10^4 (85.06% of all)

Figure 3-4. The log-log Plot of In-Degree Distribution of Professional Entities (Cont.)

In Fig. 3-1 and 3-2, the out-degree of followers somewhat roughly and the in-degree of followees rather well fit power-law distributions. Quite differently in Fig. 3-3, as a whole, the in-degree of professional entities is much more evenly distributed than the preceding two. The log-log plot of

their in-degree is shown in Fig. 3-4, and there is no clear and strong linear correlation found in these figures. It does not fit to power-law in any range.

Even though professional entities generally have many followers, the number of followers of each one varies significantly. The mean value and standard deviation of in-degree for all professional entities are as high as 7,665 and 23,703 respectively. For these with in-degree being equal to or less than 10,000, the mean value and standard deviation are 1,846 and 2,241, respectively. In other words, some professional entities may not get the same attentions on social media as in reality. This also implies the importance of microblogging marketing. Without proper dissemination of information and marketing (that is, advertising), it's hard to be a well-known user on social media, even for a famous entity in real life.

Each professional entity has a hierarchical category label, in form of "a.b.c.d". For example, for Yelp, one popular free application on mobile phones, the category label could be: "science-and-technology.internet.mobile.location-based". These labels are made and assigned to each entity by the staff of Tencent Inc.

In our following analysis, we do not care about the hierarchical structure of the categories, and use the full four-level label as a unique category identifier. Two labels, which are not in the strict form of "a.b.c.d", are excluded in Fig. 3-5. As a result, there are 375 categories for these professional entities. In the dataset, professional entities are not evenly distributed in each category, which is shown in Fig. 3-5.

There are eight categories with more than 100 professional entities in them. They have not been counted in Fig. 3-5. At the same time, 298 categories hold no more than 20 entities each. The mean and standard deviation of the number of professional entities in each category is about 16.2 and 28.5, respectively. The volume of each category shows significant difference.

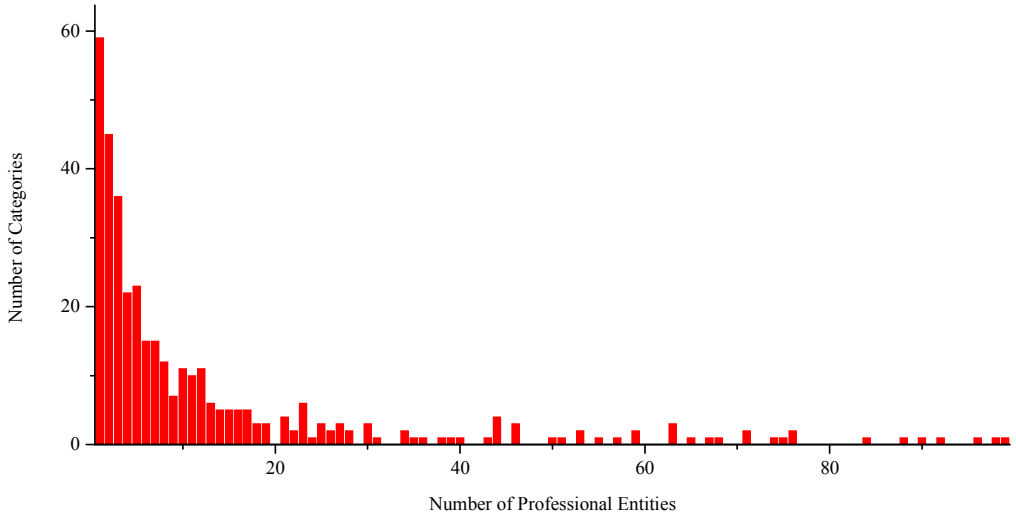


Figure 3-5. The Distribution of Professional Entities in Each Category

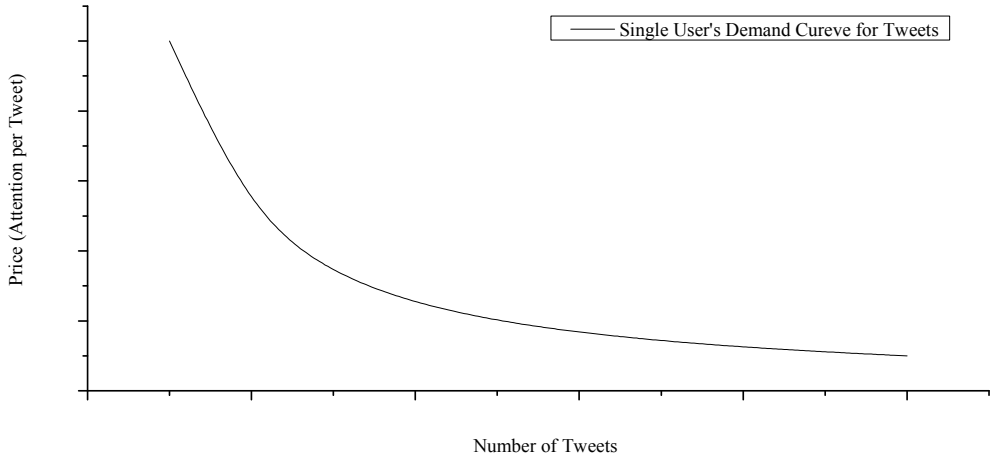
3.3. The Uneven Distribution of Categories

The uneven distribution of professional entities in different categories reflects the uneven distribution of public's attention on corresponding topics. With attention and information pieces being the exchange currency and goods, we can use the demand-supply model to analyze it (Dutt, 2002).

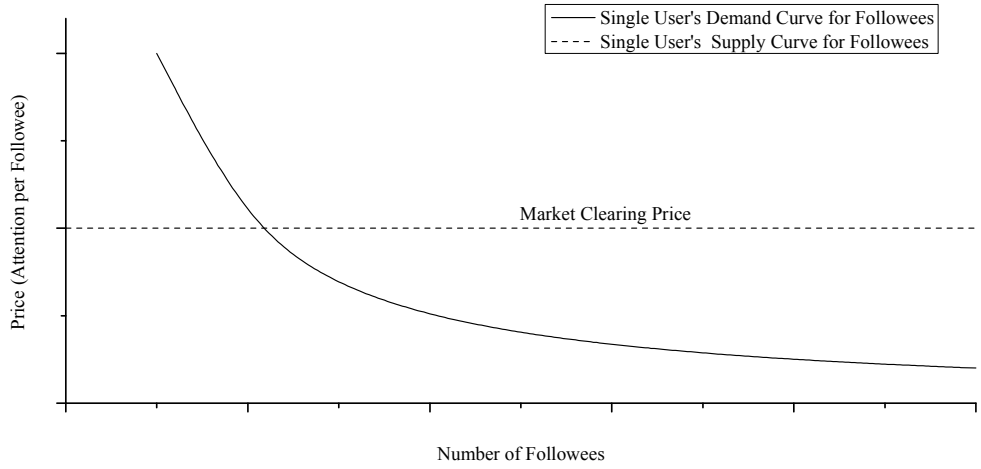
As the carrier and medium of attention, time is an approximate metric of attention (Erik & Joo, 2013). Paying attention implies expenditure of time. For instance, if we follow Justin Bieber on Twitter, we pay attention to consume his tweets and show our interest in him. Simultaneously, we spend time to read the information pieces provided by him. Thus time is an indirect metric of attention. However, sometimes we are absentminded while visiting the social media. Thus time is a biased measure of attention. Overall, it is reasonable to use time as the metric of attention.

Consider now the demand of a single user. For one specific topic, if some users have no interest completely, the demand curve for tweets or followees would be the y-axis in Fig. 3-6. In other

words, no matter how much attention is needed to purchase and consume the information in the topic, the users would not pay it.



(a) Curves for tweets



(b) Curves for followees

Figure 3-6. The Demand Curve of Single User for Tweets and Followees in One Topic

Otherwise, as shown in Fig. 3-5, like many ones for the material goods, the demand curve for tweets in any one topic is downward sloping. The demand is determined by both preference and technology. The technology level stays relatively the same in a short period. So the users' preference plays a more important role in the market. The more one is interested in the topic, the more attention is put into it, and consequently the more time is spent on consuming the related information.

In the short term, the demand curve could be treated as constant, since interests do not change dramatically. However, there are exceptions to this rule. When some breaking and important event happens, the public's attention might be attracted on it in a very short time. In daily life, we do not care about earthquakes, because of its rare possibility. But once an earthquake happens, for the public around its epicenter, the demand for earthquake related information will surpass all other kinds of messages in minutes and hours (Sakaki, Okazaki, & Matsuo, 2010)(Mendoza, Poblete, & Castillo, 2010).

Given a constant demand for information of one topic, the quantity demanded increases with the reduction of unit cost. For example, if the tweets contain less video than before, information amount decreases, and we need less attention to read and think about each message. In this case, the price drops. We would like to consume more tweets, without paying more attention. The curve could be described by equation 3-3, where attention is a constant.

$$\frac{Attention}{Tweet} \times Number\ of\ Tweets = Attention \approx Time \tag{3-3}$$

Theoretically, the equation only holds around the current status. While the price does not change greatly, the substitution effect is so little that we could assume the attention in equation 3-3 approximately remains the same. If it goes too far from current status, the substitution effect would change the total attention paid to this topic. For example, if the tweets for news have a much

higher price than before, the users have to reallocate their attentions among different categories to maximize their utility. The details of utility maximization are discussed later in section 5.2.

In practice, the price varies within a small range, unless some form of technology revolution happens. Considering the habits of customers and price strategies of other competitors, the best response of each provider is to follow the common price strategy of competitors. As a result, information oligarchs like to maintain the price and not to change it dramatically. The competition focuses on the quality of tweets. Otherwise, the provider will face the serious risk of loss of customers: a bad price strategy will be a loser even with good information goods.

The demand curve for professional followees is quite similar to the curve for tweets. If we change the x-axis to the number of followees and the y-axis to a new form of price as attention per followee, the curve would remain the same on the whole. Let the productivity be the same for every followees, we could derive the demand curve for professional followees from equation 3-3.

$$
\begin{aligned}
Attention &= \frac{Attention}{Tweet} \times Number\ of\ Tweets \\
&= \left(\frac{Attention}{Tweet} \times \text{Productivity}\right) \times \frac{Number\ of Tweets}{\text{Productivity}} \\
&= \frac{Attention}{Followee} \times Number\ of\ Followees
\end{aligned}
\tag{3-4}
$$

On social media, the demand curve for information provider could describe the users' behaviors more accurately than the curve for tweets because of the consumption pattern. In our daily life as also in the world of information, the customer needs to find, choose and then consume the goods. For instance, if we want to find an answer to some question on the Internet, we will search the question through search engine, choose some pages in the result set, and finally read them until we find the answer. But after that, we do not care about new information pieces on the viewed

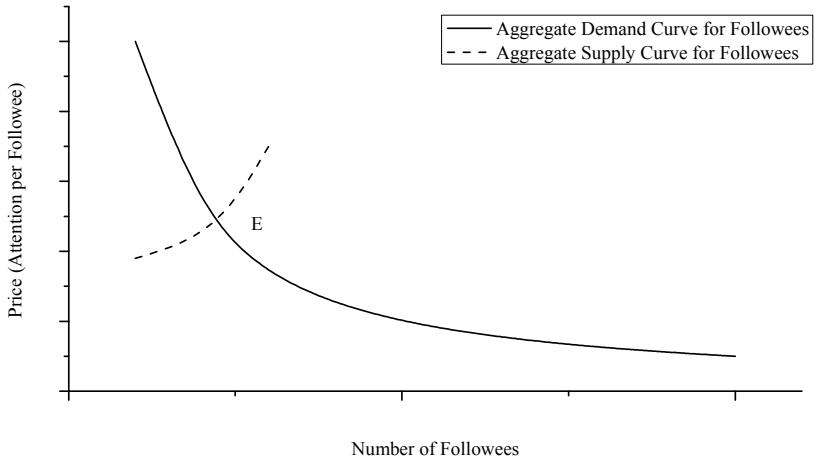
websites. In other words, our attention is paid majorly to the specific goods, rather than to the information providers.

In contrast, on social media, the users show a significantly different consumption pattern: subscription. The users have to find out some providers in one interested topic and subscript their tweets. After that, because of the indivisibility of these information sources, the users will receive all the tweets from these followees and have the potential to consume all of them. The attention is allocated to these followees directly.

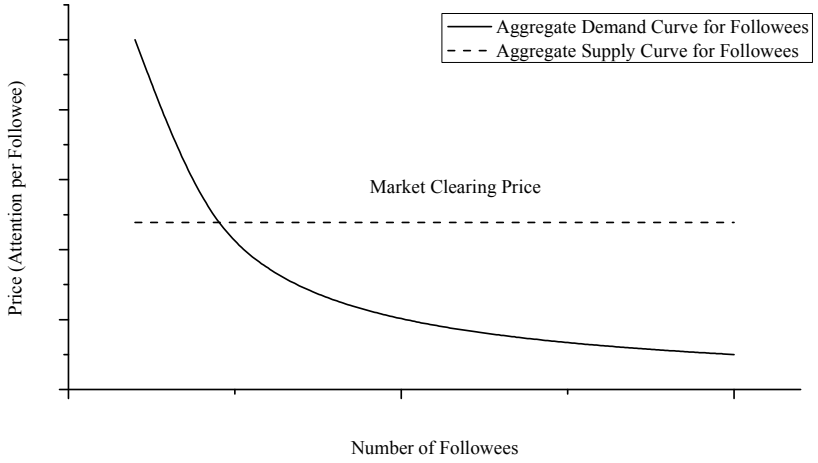
In a nutshell, on social media, we are not paying our attention to individual tweets. One user, rather than one tweet, is the smallest communication unit. So the demand curve for information provider is better at describing the real social networking service.

The supply curve for followees of a single user is a straight line, which is parallel to the x-axis. The preference of a single user is not powerful enough to influent the followees' producing habit, such as the amount of tweets per day and the information density in tweets. Furthermore, the reading skill of users is constant in short term. Therefore, the price in the supply curve for single user and the attention needed to consume the tweets of one followee would not vary greatly. They always stay at the market clearing price. Under such price, as the information always is excessive, there are as many professional followee candidates as the user wants. If some professional user quits this information market, someone else will take its position quickly.

For one specific topic, if we add the demand curves for all users together, we get the aggregate demand curve. Even though the paid attention of users is different and hard to measure, the demand curves are same in shape. As a result, the aggregate demand curve is the same in shape as that in Fig. 3-6. The aggregate demand and supply curves, in short term and long term, are shown in Fig. 3-7.



(a) Short Term Aggregate Demand-Aggregate Supply Curve



(b) Long Term Aggregate Demand-Aggregate Supply Curve

Figure 3-7. The Aggregate Demand-Aggregate Supply Curves for Followees in One Topic

On market clearing status, the users would like to follow these providers in an equilibrium price. The price is accepted by both followers and followees. Without external forces or changed conditions, no one has the motivation to change the price. As an equilibrium point, the demand for followees is always equal to supply, as indicated in the equation 3-5:

$$Aggregate\ Demand = \sum_{u \in users} \#(Followee_u) = \sum_{u \in users} \#(Follower_u) = Aggregate\ Supply$$

(3-5)

where $Followee_u$ means the followees of user u, and $\#(Followee_u)$ means the number of these followees.

In the short term, the aggregate supply curve slopes upward. When the demand of users suddenly increases, the demand curve would move toward the right. The price and supply would both increase. In other words, the users will pay more attention to each followee, and more information providers emerge. For instance, when an earthquake suddenly happens, the nearby users would carefully read all information from government originations and news agents. At the same time, some other users, including some persons in the vicinity, would become temporary information sources. As example, more and more breaking news is broadcasted by common users on social media. Due to the low threshold of being information sources, the response of social media market is quite quick.

If the attention change is temporary, only the short term phenomenon would appear. Then everything would go back to the original status with the restoration of attentions. For example, when the Super Bowl takes place, you can see the reports and news everywhere in USA. However, during the rest of the year, it is discussed much less. If the attention change is persistent, it leads to a long term modification of behavior. For instance, the development of cloud computing has caused it to become the focus of attention of many researchers. Unlike the temporary event, such attraction stays strong for a long time.

In the long term, at the market clearing price, the elasticity of supply is infinite. That is, there are as many professional followees as the market's aggregate demand wants. On one hand, at the end of the short term drift, all these followees would lower the abnormal price, because it probably

would not be accepted by their followers. And some temporary information sources turn into qualified long-term followees. On the other hand, with the increase of the supply, the users have more choices. To enhance the diversity of information, users would like to make the price back to normal and follow more sources. After these adjustments, the number of professional followees increases, while the price approximately remains the same. The situation of decrease in aggregate attention is similar.

Back to the equilibrium price, we will now analyze how the amount of professional followees in one category is determined. Let the $\#(FR)$ be the number of followers, P be the price, and T stand for the threshold, these long-term qualified information sources are willing to produce and provide tweets if and only if they receive enough attention:

$$\#(FR) \times P \geq T$$

$$In\_dgree = \#(FR) \geq \frac{T}{P}$$

As widely known, the distributions of both in-degree and out-degree are fitting to power law. So we estimate the proportion of professional entities as following:

$$\Pr\left(In\_degree \geq \frac{T}{P}\right) = \left(\frac{T}{P}\right)^{-a} \tag{3-6}$$

For the balance of aggregate supply and demand, it is expressed with the aggregate attention (AA):

$$\frac{AA}{P} = Aggregate\ Suppy = Aggregate\ Demand = \sum_{k=1}^{\infty} \#(\#(FR) = k) \times k \tag{3-7}$$

where $\#(\#(FR) = k)$ means the number of followees, who have k followers. In terms of the total number of entities (C) in one category, we derive the equation as following to get it.

$$\sum_{k=1}^{\infty} \#(\#(FR) = k) \times k = \sum_{k=1}^{\infty} \Pr(\#(FR) = k) \times C \times k$$

$$= \sum_{k=1}^{\infty} \Pr(\#(FR) = k) \times C \times k$$

$$= \sum_{k=1}^{\infty} (\Pr(\#(FR) \geq k + 1) - Pr(\#(FR) \geq k)) \times C \times k$$

$$= C \times \sum_{k=1}^{\infty} (\Pr(\#(FR) \geq k) - Pr(\#(FR) \geq k + 1)) \times k$$

$$= C \times \sum_{k=1}^{\infty} \Pr(\#(FR) \geq k)$$

$$= C \times \sum_{k=1}^{\infty} k^{-a} \qquad (a > 1)$$

(3-8)

For the sum, it is hard to get an exact result. But an approximation can be estimated with integration.

$$1 + \int_{k=1}^{\infty} (k + 1)^{-a} \leq \sum_{k=1}^{\infty} k^{-a} \leq 1 + \int_{k=1}^{\infty} k^{-a}$$

$$1 + \frac{1}{a - 1} \times 2^{-a+1} \leq \sum_{k=1}^{\infty} k^{-a} \leq 1 + \frac{1}{a - 1}$$

So we represent the sum as:

$$\sum_{k=1}^{\infty} k^{-a} = 1 + \frac{1}{a-1} \times \varepsilon^{-a+1}, \qquad where\ \varepsilon \in (1,2)$$

(3-9)

To combine the equations 3-7, 3-8, and 3-9, we get the relation between aggregate attention and total number of professional entities:

$$\frac{AA}{P} = C \times (1 + \frac{1}{a-1} \times \varepsilon^{-a+1})$$

$$C = \frac{AA}{P \times (1 + \frac{1}{a-1} \times \varepsilon^{-a+1})}$$

(3-10)

Then, we estimate the number of professional followees (*PFE*) in each category with equation 3-6 and 3-10.

$$\#(PFE) = C \times \Pr\left(In\_degree \geq \frac{T}{P}\right) = \frac{AA}{P \times \left(1 + \frac{1}{a-1} \times \varepsilon^{-a+1}\right)} \times \left(\frac{T}{P}\right)^{-a}$$

After simplification, the result is:

$$\#(PFE) = \frac{AA \times P^{a-1}}{T^a \times \left(1 + \frac{1}{a-1} \times \varepsilon^{-a+1}\right)}, \qquad where\ a > 1\ and\ \varepsilon \in (1,2)$$

(3-11)

From equation 3-11, the number of professional entities in the topic would change in the same direction of *AA*'s change. If the aggregate attention gets higher, the market needs more information providers. If the situation is converse, less professional entities would survive. And some "*failed*"

providers cannot get enough attention as expected and might switch to other topics or leave the market.

Similarly, the number of professional entities would increase if price rises, and decrease if price drops. When only price increases, and all other parameters stay the same, these followees need fewer followers than before to get enough attention that exceeds the threshold *T*. As a result, the scope of professional entity candidates is extended, and the total amount increases.

Table 3-1. The Brief Distribution of Top 100 Twitter Followees[3] in Categories*

Category	Gross	Proportion	Example
Singer & Actor	61	61%	Justin Bieber (justinbieber); Jim Carrey (JimCarrey)
TV host	10	10%	Oprah Winfrey (Oprah); Conan O'Brien (ConanOBrien)
Sport	8	8%	SHAQ (SHAQ); FC Barcelona (FCBarcelona)
Technique	7	7%	Instagram (instagram); YouTube (YouTube)
Socialite	5	5%	Kim Kardashian (KimKardashian); Bill Gates (BillGates)
News	3	3%	CNN (CNN); The New York Times (nytimes)
Writer	2	2%	Perez Hilton (PerezHilton); Paulo Coelho (paulocoelho)
TV Channel	2	2%	MTV (MTV); ESPN (espn)
Religion	1	1%	Dalai Lama (DalaiLama)
Politics	1	1%	Barack Obama (BarackObama)

*: Some celebrities cover many topics. But we only assort them into one category.

If the threshold for a professional entity to survive changes, the number of professional entities would change toward the opposite direction. For instance, if followees need more attention to act as professional entities, because of the constant amount of aggregate attention, the gross number of professional entities would decrease.

[3] http://twitaholic.com/top100/followers/ (access on March 31, 2013)

Generally, in a stable market, the parameter P, T, and a are approximately constant. So the number of professional entities in different topics is not uniform and strongly determined by the aggregate attention of public. The case of Twitter celebrities, as shown in the table 3-1, confirms this rule.

CHAPTER IV

ANALYSIS ON HOW USERS ADOPT THE PROFESSIONAL ENTITIES

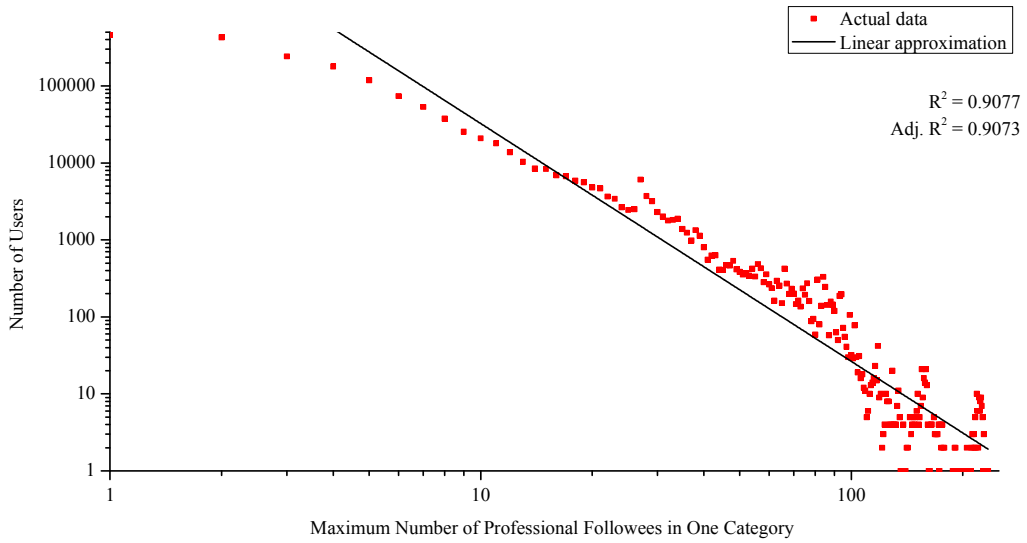
In this section, we analyze how users follow professional entities based upon the static snapshot of users' social graph and the followee adoption history.

We measure the maximum number of professional followees in one category (*MPFC* for short in the following) for each user. Accordingly we could define *MPFC* as:

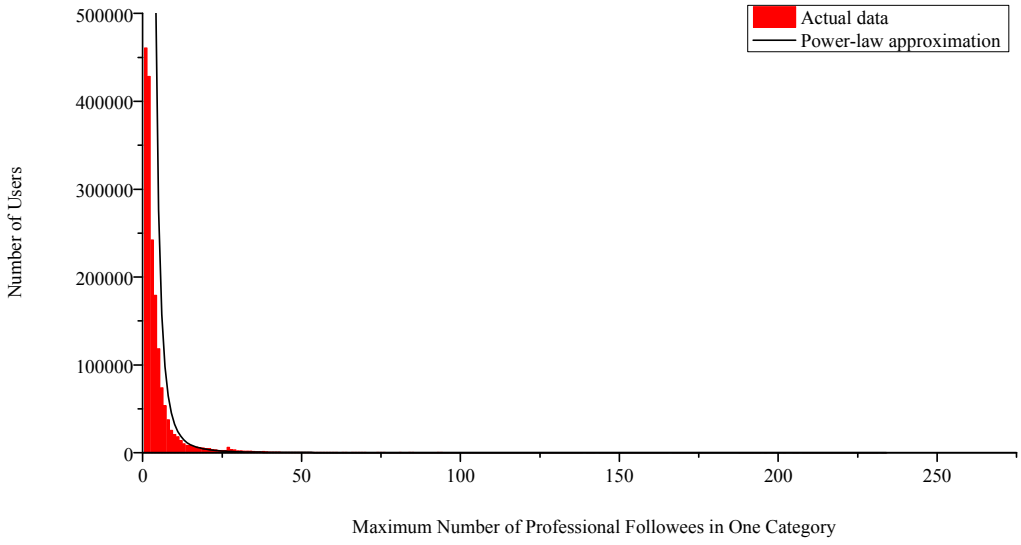
$$MPFC_a = \max_{C_i \in Categories} \#(C_i \cap FE_a)$$

where $MPFC_a$ means the *MPFC* for user a, and FE_a means the set of followees of a. For example, if user a follows three non-professional entities, two movie stars, and one news agency, its *MPFC* should be two. We assume the category with most followees of each user indicate the user's most interesting field. Therefore the *MPFC* measures the users' maximal capacity of followees in one category.

In the dataset of users' social graph, which is descripted in section 3.1, there are 97,655 followers. But about 5.16% of these users do not have any social link to professional entities in the social graph dataset. Therefore they are not involved in the following discussion. Only taking the users with professional followees into account, we obtain the overall distribution of *MPFC* as shown in Fig. 4-1.



(a) In log-log plot in base 10



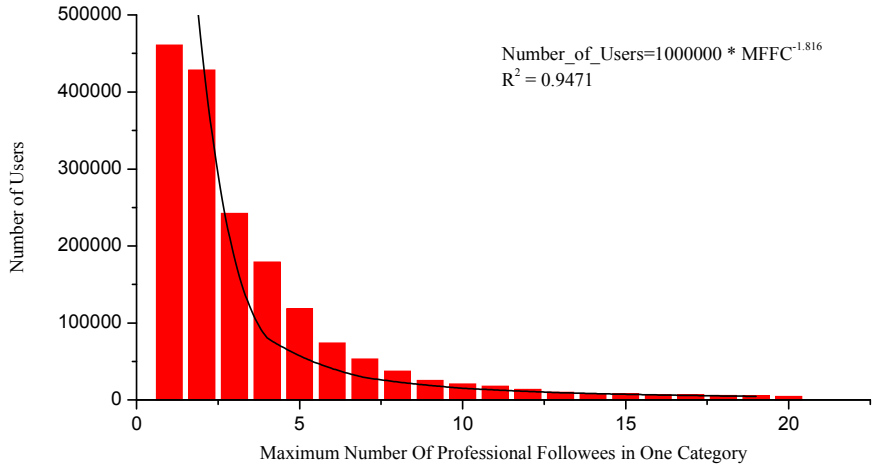
(b) In original coordinate

Figure 4-1. The Distribution of Maximum Number of Professional Followees in One Category (*MPFC*)

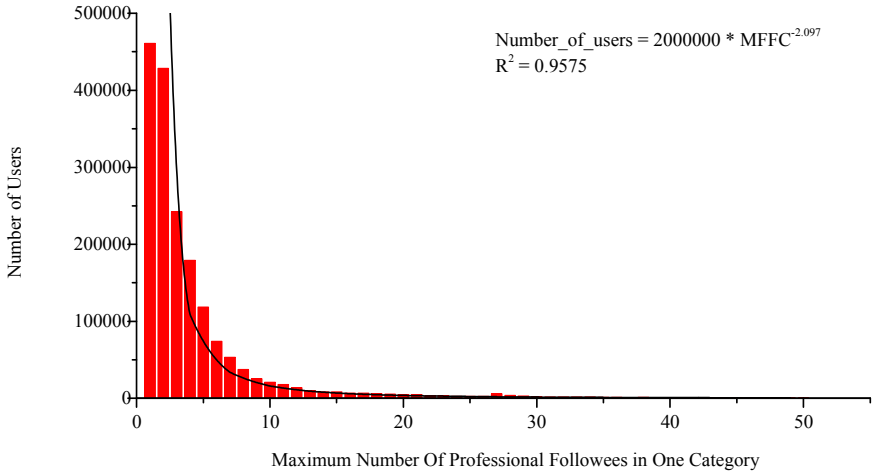
Deriving from the linear regression result in Fig. 4-1(a), we get the power-law approximation as following in Fig. 4-1(b):

$$Numbe\_of\_Users = 10^{7.601223} \times MPFC^{-3.08936}$$

Overall, with users of *MPFC* being 0, the minimum, median, 90th percent, and maximum *MPFC* are 0, 2, 9, and 234, respectively. The average *MPFC* is about 4.55. To make the power-law property clearer, we make the distribution in smaller ranges in Fig. 4-2.



(a) With MPFC≤20 (96.39% of all users)



(b) With MPFC ≤50 (99.37% of all users)

Figure 4-2. The Distribution of MPFC with Part of the Users

Additionally, the percentage cumulative distribution is provided in Fig. 4-3. Generally, most users do not follow lots of professional entities in one category, and this phenomenon may be explained by marginal utility.

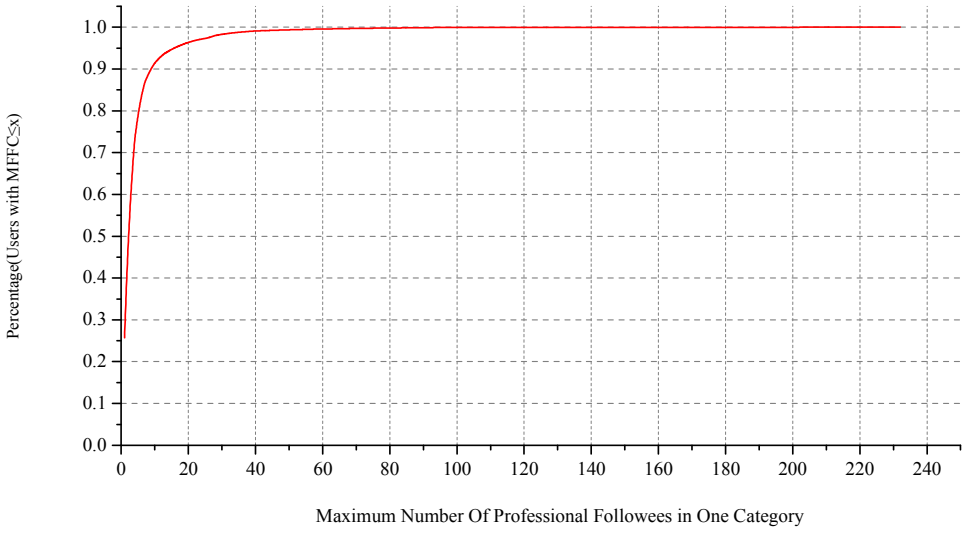


Figure 4-3. Percentage Cumulative Distribution of MPFC

With the long-tail property, a small fraction of users have lots of professional followees --- up to 234, in one category. Because all the information in these datasets is encoded as random strings and numbers to protect personal privacy and keep fairness in KDD Cup 2012, we cannot make a deeper analysis of this matter here. We guess that the unusual and excessive adoption of professional entities in one single category may be related with the users' working and living environments. For example, an IT staff might follow more professional entities, in related categories of computer science, than others.

In addition, we check the users' adoption history for professional followees. The users' adoption history contains the users' choices, both rejections and acceptances, to the recommendations from Oct 11, 2011 to Nov 11, 2011. Totally there are 73,209,277 records in this dataset. The following

two kinds of records are removed and not used: (1) the follower in the record does not have its social links information in the social graph dataset; or (2) the followee in the record is not a professional entity in our dataset.

Consequently, there are 62,169,578 (84.92% of all) valid records in this dataset. A user could accept a recommendation to follow one professional entity, then unfollow it, and accept the same recommendation again later. Therefore, there are some repeated records with different timestamps, and we do not remove them from our discussion. For user u, the adoption rate for a specific category C_i is generally defined as following:

$$Adoption\ Rate\left(AR_{u-C_i}\right) = \frac{\#(Acceptances\ in\ C_i\ for\ u)}{\#(Acceptances\ in\ C_i\ for\ u) + \#(Rejections\ in\ C_i\ for\ u)}$$

The average adoption rates for all users are shown in Fig. 4-4. According to Fig. 4-1, more than 90 percent of users have 9 or less professional followees in their maximum category. As a result, the samples for acceptance rates for the cases, in which the number of professional followees in one category is more than 9, are not sufficient. Thus we combine all these cases into one class as "10+" in Fig. 4-4.

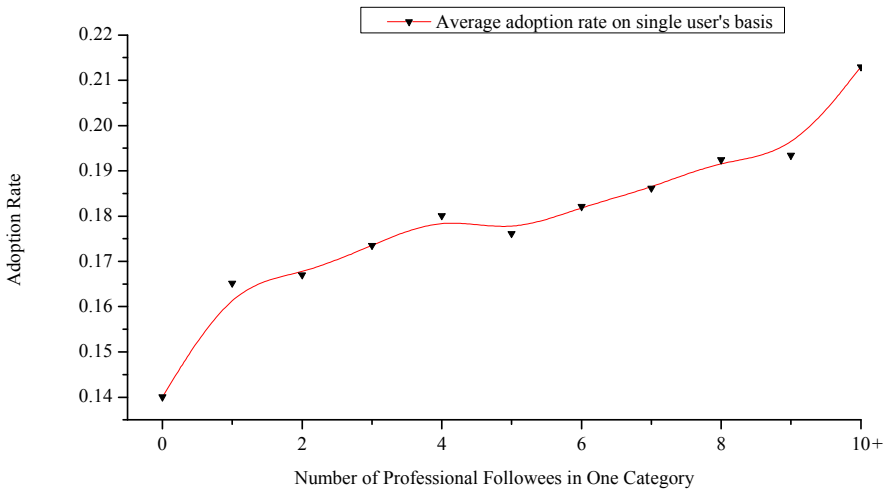


Figure 4-4. The Distribution of Adoption Rate

In particular, the average adoption rate for all cases with *n* number of professional followees in one category is computed as:

$$\overline{AR_{\#(FE\cap C_i)=n}} = \frac{\sum_{u\in U_n} AR_{u-\cup_{\#(FE_u\cap C_j)=n} C_j}}{\#(U_n)}$$

where U_n means the set of users, who have *n* followees in one or more category.

The users might follow some new entities, and unfollow some old followees in this sampling period. However, we only have the adoption history and are lacking of the unfollow history. We could not accurately know the number of professional followees in each category for each user at different time in this adoption period. So we use the data in the social graph dataset to statically estimate the number of professional followees for users.

In the beginning, the adoption rate increases rapidly. But with the increase of professional followees in one category, the adoption rate of that category grows much slower and becomes stable.

Assuming that there is no cost for adopting new followees in the interested fields, the users might like to follow as many professional entities as there are to get the most information. Thus the more professional entities are followed in a specific category, the more interest is developed in that realm, and thus it is more likely to adopt new followees in the same field. However, in real life, adopting new followees needs more energy and time to digest the additional messages. There is cost associated with adoption.

Overall, for more than 90 percent of users, there are 9 or less professional followees in their maximum category. That is, 9 or less information sources in one field are enough to provide sufficient messages with affordable cost. There are also less than 10% of users, who follow more than most of masses. For these users, the value of new messages is much higher than the cost.

Thus even though they could get only a little additional information by recruiting more followees, they continue to adopt new ones. For example, the publicity department of one company is willing to follow and monitor the advertising of all its partners and competitors, no matter how many there are.

In addition, the result in Fig. 4-4 fits with the general conclusions of Fig. 4-1. To confirm this, we make an iterative and slightly non-rigorous simulation. Initially, we set the number of users as 1,892,059, which is the same as the total number of followers in the social graph dataset. And the *MPFC* of all users are set to 0 at the beginning. In each iteration round, each user has one opportunity to increase its *MPFC* by one with the probability in Fig. 4-4. Because we are short of samples to evaluate the adoption rates for $MPFC \geq 10$ well, the maximum *MPFC* of users in this simulation is limited to 10.

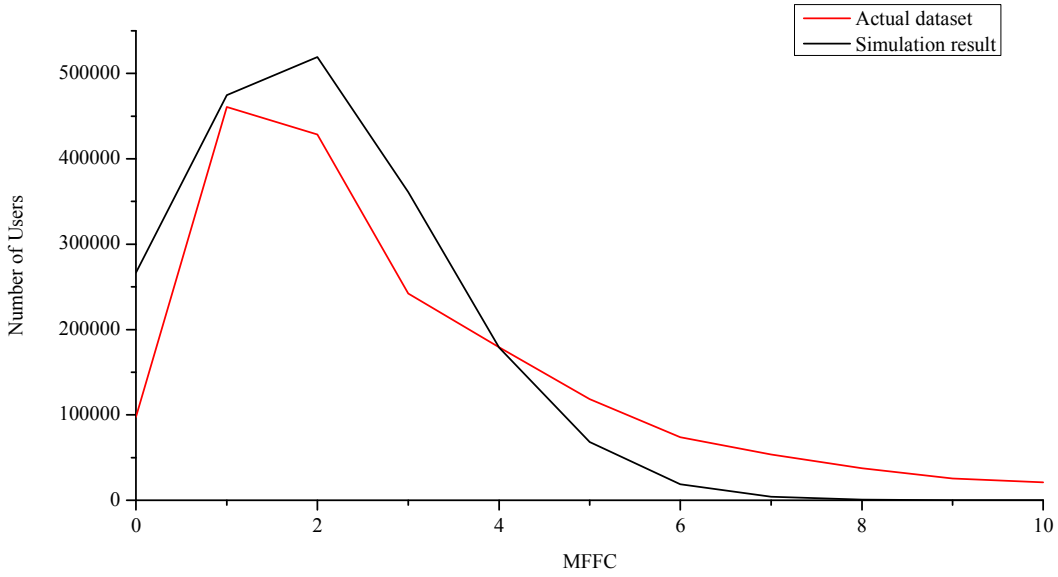


Figure 4-5. The Adoption Simulation

After 13 rounds, we get the result which is similar to the real situation as shown in Fig. 4-5. Taking the simplicity of the simulation into account, the simulation matches the real situation

very well. In other words, the adoption rates pattern could lead to the power law distribution in Fig. 4-1.

For the cases where *MPFC* is zero, the data in both actual dataset and simulation is not accurate. In the simulation, we did not consider new users, who continually join into the system. And the inaccuracy of real dataset could be an artifact of the sampling method. As we discussed in section 3, the sampled users are the most "active" ones, who are less likely not to adopt any professional entity, compared with the non-selected "inactive" ones. In real life, overall, the users with zero *MPFC*, including the zombie accounts and forgotten users, should be represented by a much greater proportion than it is in our samples dataset.

Furthermore, in real life, there are other methods in addition to recommendation system for the users to choose and adopt new followees. For example, the word of mouth and the influence of followees in real life play important and critical roles. With these limitations, our simple simulation is unable to accurately fit the real case. However, it does show the same general shape.

Theoretically, our case is similar with the classic Barabási–Albert model (Barabási & Albert, 1999):

1. Expand continuously: in terms of individuals, when they enter the SNS system, they commonly follow many other users in a short time, and then continue to adopt or abandon selective followees with a relatively slower pace. In terms of whole system, the existing users might quit this social system. At the same time, the new users continue to enter the platform.
2. Rich get richer: on one hand, with more professional followees, users show more interest and are more likely to adopt more. On the other hand, the professional users with more followers have more chance to be exposed and recommended to the other users, and

therefore increase their in-degree easily. But the increase rate in our case appears slightly different from the Barabási–Albert model.

In sum, the above discussion supports that the *MPFC* of users fits the power law distribution.

CHAPTER V

FOLLOWEE ADOPTION FROM AN ATTENTION ECONOMICS PERSPECTIVE

In the previous section, we analyzed how the users adopt professional followees based upon an empirical dataset. In this section, we will analyze and discuss the phenomenon from an attention economics perspective (Yu & Kak, 2014).

5.1. Game among Followees

One can speak of many naturally defined games within social media (Hassan & Rafie, 2010). The interactions among followers and followees have inherent conflict and cooperation. On one hand, the followees always want to have more fans and influence, and user loyalty also means a lot for these information providers. On the other hand, the common users want to get information with least attention from the followees. Among the followers, balance theory plays an important role in their interactions. In the following, we will discuss the game between follower and followee, and among followees.

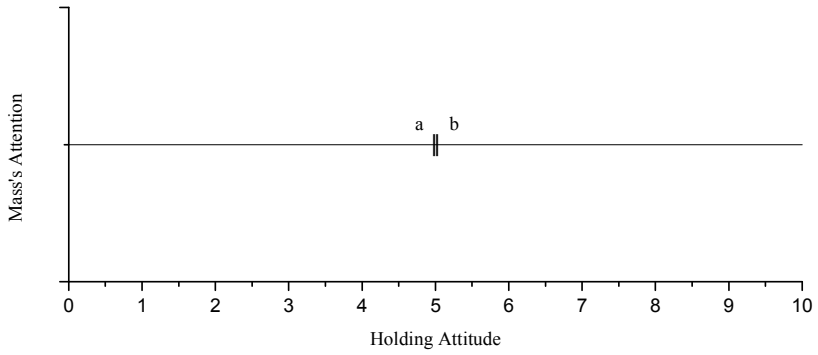
Generally, the game among followees is a classic public choice problem (Congleton RD, 2002; Enelow & Hinich, 1989; Holcombe, 1989). For example, in a political election, which is the case of the traditional public choice, voters hold different political views, and candidates try to articulate a position to maximize the proportion of supporting voters.

In the information network, the public's attention has different focus points, and the followees try to produce the information in an optimized subset of the topics to attract as much attention as possible. For example, when Steven Jobs (co-founder and later CEO of Apple Inc.) and Dennis MacAlistair Ritchie (creator of C programming language and co-creator of UNIX operating system) passed away in October 2011, some information providers within social media had to choose how to allocate their sources to report the events and commemorate these two celebrities. Despite their personal preferences and to maximize the satisfaction of their followers, they had to decide the ratio of the tweets about Jobs to these about Ritchie.

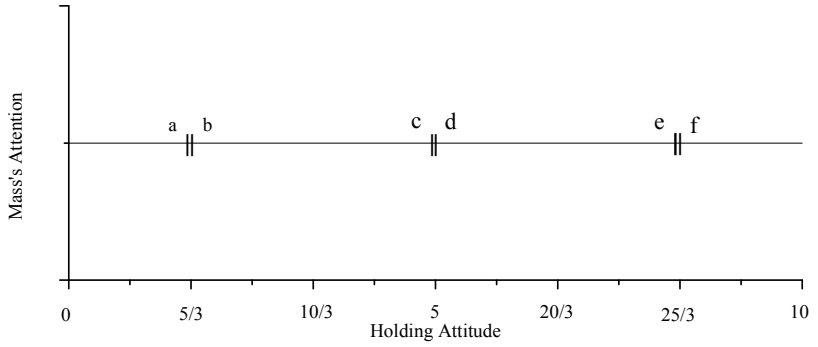
If the public's attention is uniformly distributed, as shown in Fig. 5-1(a), and all customers prefer to choose the provider who holds the most similar ratio as wanted, this game problem is simplified into a Hotelling's model. In Fig. 5-1, the scale of x-axis is from 0 to 10, which represents tweets about only Jobs and only Ritchie respectively. The middle point 5 means that there are equal tweets about them.

With only two information providers, say players *a* and *b*, as an example of median voter model, the Nash equilibrium is in the middle of the market. Position 0 is strictly dominated by position 2, and position 10 is strictly dominated by position 9. With iterative deletion, the final "best" position for *a* and *b* would be the middle of market.

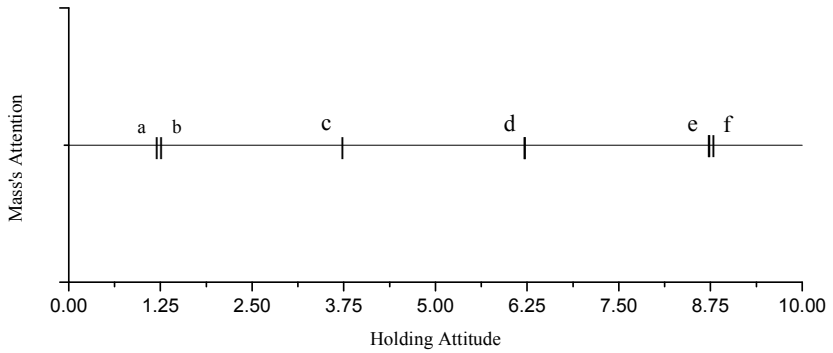
In the middle, they would share the market equally. They cannot get any additional payoff for changing their positions, and even worse they will lose some of the market if they move. In this case, by the strong form of the median voter theorem (Congleton RD, 2002), the customers in the middle of market get the most suitable tweets. The users in the two ends could not get the tweets, which are quite suitable to their demands.



(a) The Nash equilibrium with two players



(b) One Nash equilibrium with six players



(c) The other Nash equilibrium with six players

Figure 5-1. The Hotelling's Model (Example from (Eation & Lipsey, 1975))

In reality, there are numerously more players in the social media game, such that the median voter model could not be applied here. However, Hotelling's model can still be applied to this case (Eation & Lipsey, 1975). For three providers, there is no pure strategy Nash equilibrium (Shaked, 1982). For four or more providers, there are pure strategy Nash equilibriums. For some cases, there are two or more unique Nash equilibrium. For example, with six players, there are two Nash equilibriums as shown in Fig. 5-1(b) and (c). In both situations, no player has motivation to change its attitude.

With more information providers in Hotelling's model, at Nash equilibrium points, the followees are dispersedly distributed in the market rather than stay together in the middle. This distribution increases the diversity of information sources, further segmenting the market, and provides the customers with more targetable and suitable tweets package.

In practice, the public's attention is definitely not uniformly distributed, unlike what was assumed in the previous discussion. Previous studies (Chris, 2007; Erik, Yu, & Michael, 2006) have shown that there is the long-tail phenomenon in the public's demand for products. In other words, there are some products which lots of people like. Other products appear to be attractive to a small fraction of public. However, the tail is so long that these niche products account for a considerable market share. Therefore they could get enough providers.

Furthermore, every customer is a bit eccentric, such that he/she wants both some popular and niche products (Goel, Broder, Gabrilovich, & Pang, 2010). Even though currently there is no direct evidence that the customers for online information pieces show the same behavior pattern as for material products, we reasonably expect they do. As a result, distribution of public's attention among different focus points of one topic would be multi-peak and characterized by asymmetry.

With the uneven distribution of attention, the Nash equilibriums are harder to figure out. But a necessary condition for Nash equilibriums in this case is (Eation & Lipsey, 1975) that no followee's whole market is less than anyone's one-side market. In other words, nobody's market share is greater than twice of any other's and the potential customers are much more concentrated around the peaks. Thus we could expect the density of followees around the peaks to be much greater than that in the long-tails. The public's common demands could be better fulfilled because the followees' strategy is closer to these demands. Our niche preference could not be exactly satisfied sometimes. For example, the public is significantly more familiar with Jobs, so in October 2011, there were many more stories and reports about Jobs, but relatively much less information about Ritchie.

As reality is more complicated than theory, the situation of followees could never be described by a one-dimension model. There are many focus points even in a single topic for public and the followees have to choose positions in each dimension. Consequently, the problem becomes finding equilibrium in an uneven distributed multi-dimensional space with multi-players. The pure strategy Nash equilibrium is hard to find under such circumstances and even does not exist in some cases.

Additionally, the fit between personal preference and followees' attitude is not the only factor to influence the user's choice. For example, if all one's friends show a negative impression of followee *c*, according to the social balance theory (Heider, 1946)(Cartwright & Harary, 1956), the one is less likely to adopt it.

Generally, the game among followees drives the information providers to focus on the public's demand, while not ignoring the niche. As a result, our general interests will be better fulfilled than our niche preferences.

5.2. Game among Followers and Followees

As shown by the previous discussion, the Nash equilibrium in the game among followees determines their market share. However, the social media is not so simple and "peaceful". There is fierce competition among the players not only for the number of followers, but also for the users' stickiness. The competition could be significantly determined by the game among followers and followees.

This is a zero-sum game for followees. Any interaction among single followee and its followers cannot change the total attention from public. And one followee's gain can only come from the loss of others. For example, if one followee increases the quality of its tweets, it attracts more attention from its followers at the cost of attention to other followees.

In practice, the quality of tweets from one followee would not fluctuate greatly in a short time. Thus it could be treated as a constant. This quantity is the core of this game. Generally, the game between a single followee and one of its followers could be simply described by Table 5-1.

Table 5-1. The Game between One Followee and One Follower*

		Followee (Volume of Output)		
		Decrease	Unchanged	Increase
Follower	Follow	±, k	0, 0	±, j
	Unfollow	±, l	±, m	±, n

j>0>k>l>m>n

*: The payoff table is measured by change, not gross.

In this game, the payoff of follower is undetermined, except the point (follow, unchanged). At the point (follow, unchanged), the follower continues to follow, and the followee does not change its productivity. They stay the current status. So there is no change about the gross payoffs of both

players. Otherwise, no matter which strategy is chosen, the total payoff of follower will either increase or decrease. The fluctuation depends on the interactions among the follower and its other followees.

If there are few similar information sources, the substitution effect is weak. Once one unfollows a followee, the follower will not get enough qualified tweets. The payoff of the follower would be decreased. If the follower has many information sources on this topic, the excess of tweets would troublesome. Therefore, unfollowing an unsuitable followee could ease the information flood and promote the payoff.

When the follower keeps a followee, they stay in the current status, and the payoff of both followee and follower doesn't change if the rate of messages doesn't change. When the followee increases the volume of tweets, if the follower already has too many related tweets, the information flood would become worse and the payoff would decrease. In contrast, if currently the follower does not have sufficient information, the increase of supply could ease the information shortage and add its payoff. Similarly, the payoff of follower would increase or decrease depending on different cases.

In terms of the followee, when a follower chooses to continue to adopt it, if it produces more tweets, the follower has to allocate more attention to digest the items of information. This makes the followee become more important, because its tweets account for greater proportion. As a result, the followee gets more attention and improves its stickiness for users. Conversely, a decrease in productivity would lower the payoff of followee.

When the follower chooses to unfollow, no matter which strategy is selected, the followee will lose one follower completely. If the productivity is lower, the total cost to make tweets would decrease, and the total lost would be less than the other two cases.

Overall, in this game, there is no strictly dominating strategy for followee. When follower chooses to unfollow, the best response for followee would be to lower the productivity. Otherwise, the best response is to increase the volume of tweets. And because of the uncertainty of the follower's payoff, it is impossible to find any Nash equilibrium.

Within real social media, there are lots of followers and followees. The actual game would be multi-players with infinite strategy space. There is a range of continue strategies, instead of a few discrete strategies for followees. The strategy space for the followee is infinite. In addition, each individual follower might choose to follow or unfollow according to its specific situation. Therefore the total number of followers might either increase or decrease depends on different reasons, other than the followee's choice.

Generally, when a followee plans to adjust its productivity, it has to analyze market demand and users' stickiness to maximize its payoff as:

$$\max_{PR \in R}(payoff_{PR}) = \max_{PR \in R}(\#(followers_{PR}) * f(price, stickiness) - cost_{PR}) \quad (5\text{-}1)$$

where the subscript PR means the productivity level, and the $f(price, stickiness)$ is a function of price and users' stickiness to represent the total payoff from one individual follower.

For followees, the marginal cost of servicing an additional follower is nearly zero. In contrast, in this multi-players game, the production cost is related with the number of tweets. The more tweets are posted, the higher cost is needed. In other words, the marginal cost of producing an additional unit of tweet is not zero.

The equation 5-1 could be used to explain two important phenomena in social media: why there is no followee, who provides everything in the topic; and why it is not monopoly in social media, even with the marginal cost being zero.

The customer's behavior in social media is different from that in most material transactions. In our daily life, we usually choose the item from a host of candidates and then consume it. Some merchants provide as many kinds of goods as possible. Nearly every customer could get all wanted items in one stop. This kind of shop, which includes everything (such as Amazon), gives the customers more choices and enhances their shopping experience (Chris, 2007)(Erik et al., 2006).

But in social media, like Facebook and Twitter, we subscribe from followees and consume all tweets from them as long as we follow them. If there is one follower, who provide tweets about all information in one topic, few persons could afford to consume all its information pieces. Even though the payoff $f(price, stickiness)$ from one individual follower would be very high, the disadvantage in quantity of followers would lower the total payoff.

As a result, the followees would not produce too many or too few tweets daily. To maximize the number of followers and the total payoff, they would analyze the market demand and the followers' preference to produce the most suitable count of tweets for public. Generally, when the users' stickiness and demand are strong, the elasticity of demand is low, and the followees would like to increase their tweets producing rate. Otherwise, the best response is to keep or lower current productivity.

Furthermore, this statement could explain why there is oligopoly or monopolistic competition on social media, rather than monopoly. Each followee is only willing to produce a limited number of tweets daily. So no followee is able to satisfy all followers' demand. As a result, there are many followees with different focuses in the topic to fulfill the public's demand. If the audiences of the topic are only a few, or the topic is very professional and concentrated on few focuses, there would be a few followees to share the market within social media, as oligopoly. More commonly, it is monopolistic competition. Lots of information providers produce tweets on the topic, while

each of them has different focus. This scheme guarantees, the followers get suitable service, and the followees have enough segments of the market to survive.

5.3. Marginal Utility

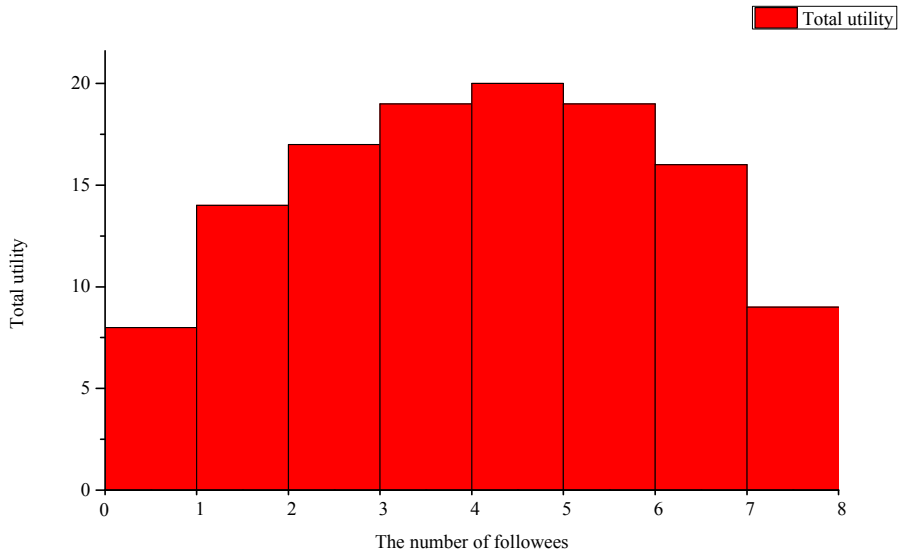
Everyone has the same time and nearly the same attention. We could use it to work, to rest, or to enjoy the Internet, depends on one's own interest and demand. We assume the persons prefer the most valuable goods and services to them. When we use the social media to seek information, we would like to allocate our attention on different topic in general and different categories of followees in particular, so that we can get the maximum satisfaction like we do in material world. The utility is a representation of preferences over different categories of followees and a measurement of satisfaction of topics (Quiggin, 1982)(Starmer, 2000).

When one user adopts a followee on an interesting topic, he/she consumes wanted information, is satisfied by the service to some extent, and gets some utility. The Fig. 5-2 demonstrates an example utility of one user on an individual topic.

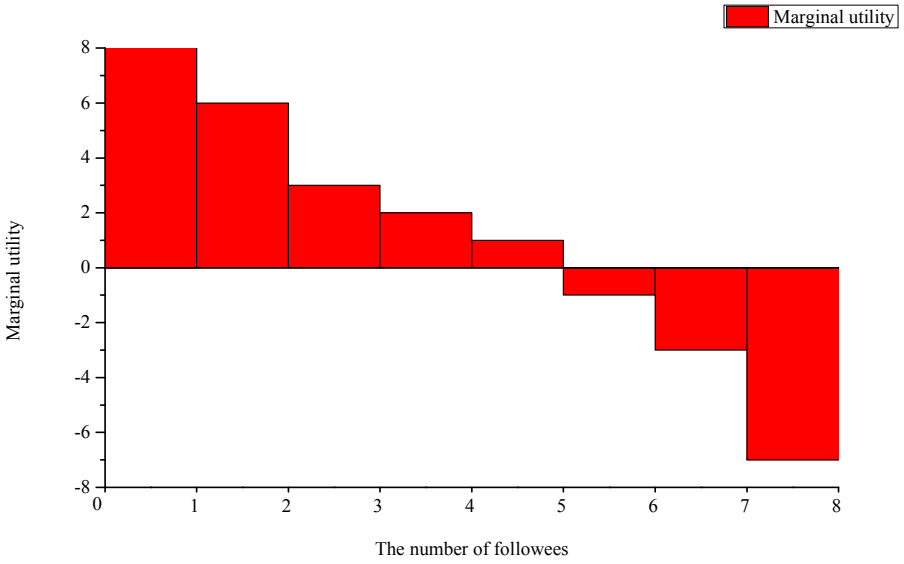
At the beginning, the user has not information source at all. When it chooses the first followee, the gain tweets are completely new for it. As in our assumption, persons prefer the most valuable goods and services to them. The first followee and its tweets would be greatly valuable to the user. Therefore, the marginal utility from the first followee would be large, and the total utility would increase greatly.

With the next adoptions, the marginal utility would be much less, as the law of diminishing marginal utility indicates. On one hand, the user already achieves some satisfactions from the current followees. It is not as eager for the information as at the very beginning. On the other hand, inevitably, there are some overlapped messages between the current followees and the new ones. Consuming the overlapped information would be a waste of time and attention, and cannot give the user any utility. In other words, after adopting some followees, the relative density and

absolute number of useful tweets from one additional followee are less, and marginal utility would decrease.



(a) The relationship between total utility and the number of followees



(b) The relationship between marginal utility and the number of followees

Figure 5-2. An Example of Law of Diminishing Marginal Utility

After the threshold, the total utility turns to decrease, and the marginal utility becomes negative. For example, in Fig. 5-2, if the user adopts the sixth followee, the marginal utility would -1, and the total utility would decrease from 20 to 19. At the threshold point, the user already gets enough information. Any additional tweets will only annoy the user without any positive affect. In practice, all users would hate to cross the threshold.

If the users have infinite time and attention, the best response to get information would be adopting as many followees as not beyond the threshold value. However, the time and attention in reality are the fairest currency. Everyone has the same and limited time and attention. So within social media, we have to consider how to allocate our currency to maximize our utility as:

$$\max\left(\sum_{C_i \in C}\left(U_{C_i} - CO_{C_i}\right)\right) = \max\left(\sum_{C_i \in C} U_{C_i} - Total\ cost\right) = \max\left(\sum_{C_i \in C} U_{C_i}\right) - Total\ cost \tag{5-2}$$

where U_{C_i} means the utility gain from the followees in category C_i, and CO_{C_i} means the corresponding cost. Because the total cost is constant for each individual user, we try to maximize the sum of utility.

Firstly, the marginal utility (*MU*) from each individual category is a function of multi dependent factors:

$$MU_{C_i} = f\left(Demand, Quantity_L, Quality_L, Quantity_{-L}, Quality_{-L}, Overlap(L, -L)\right)$$

where the $Quantity_L$ and $Quantity_{-L}$ mean the quantity of tweets from the last followee and all the others, respectively. Similarly, the $Quality_L$ and $Quality_{-L}$ are the measurement of the quality of tweets from the last followee and all the others, respectively. The $Overlap(L, -L)$ function is used to estimate the proportion of the last followee's tweets, which are the same as or very similar with some tweets from other followees.

To achieve the maximization of total utility, according to the equimarginal principle, we will allocate our attention on each topic, such that the ratio of marginal utility to price is the same for all categories.

$$\frac{MU_{C_1}}{Price_{C_1}} = \frac{MU_{C_2}}{Price_{C_2}} = \frac{MU_{C_3}}{Price_{C_3}} = \cdots = \frac{MU_{C_i}}{Price_{C_i}} = \cdots$$

The price of followees in different category is similar in most cases. So the equimarginal principle could be simplified as:

$$MU_{C_1} = MU_{C_2} = MU_{C_3} = \cdots = MU_{C_i} = \cdots = MU$$

(5-3)

At this balance, the users could get the maximum total utility. If the marginal utility for some categories changed, the users will adjust the allocation of attention to re-reach such balance. For example, if the marginal utility of one category *c* is lowered, the user would unfollow someone in the category and withdraw some attention from the category. Then it will reallocate the withdrawn attention to other categories. According to the law of diminishing marginal utility, the marginal utility of category *c* will increase, and other categories' marginal utility will decrease. As a result, the user would achieve the balance in equation 5-3 again.

If the marginal utility of category *c* increases, it becomes more valuable for investment. The user would reduce the attention paid on other categories and put more attention on followees in the category *c*. The reallocation won't stop until the balance is reached or closely approached.

The equimarginal principle would explain why one user would follow and unfollow the same entity for several times. If the number of followee is continuous, the user will achieve a balance point as in equation 5-3. However, the followee is indivisible, and the number of followee is discrete. We can only try to keep the marginal utility being approximately same for all categories.

In some cases, the difference in marginal utility is so great that it drives the user to reallocate the attention. However, the indivisibility of followees makes it impossible to achieve even an approximate balance. As a result, the user would follow and unfollow the entities frequently.

CHAPTER VI

MALICIOUS URLS ON SOCIAL MEDIA

Within recent years, social media has not only attracted the public's attention it has changed social behavior, especially of the younger ones, who spend remarkable time on them. Consequently, these platforms have attracted cyber-attackers.

6.1. Why Malicious URLs Are Widely Used on Social Media

Existing cyber-attacks reported on social media include spam, phishing, and malware distribution. These attacks share a significant characteristic: they are launched through malicious URLs. This is in spite of the fact that social media has strict security policies. Every time you upload a new file or update an existing file, the files will be scanned by the security software. If the attackers directly upload a malware on the social media, it will be easily detected and removed.

There are also content type constrains on social media. For example, on Facebook and Twitter, you could only upload text, images, and videos. Few general types of social media support to publish executable files directly. Some professional social networking services, such as SourceForge and GitHub, do support publication of binary files. However, these platforms do not have many general users but have lots of professional users, who are keeping an eye on the posts. As a result, some classic cyber-attacks, like malware distribution, could not be done directly on the social media platforms.

Note further that uploaded files might be cleared and regenerated. For example, in traditional cyber-attacks, the images could be used as an attack source. In 2004, a critical JPEG processing vulnerability was published by Microsoft. The attackers could generate a specially crafted image file (.JPG), which executes arbitrary code with buffer overrunning. If the original images could be directly accessed by the audience, it is a threat. However, social media platforms typically will not use the original images for showing. Security issue is one of the reasons. Additionally, the providers want to lossless compress the images to save the bandwidth and speed up the page loading. Finally, the resized images could easily fit to the site's design. Therefore, major social media applications, that focus on images, such as Instagram, will resize and regenerate all the original uploaded images.

Note also that posts on social media sometimes have the limitation on length. On Twitter, each tweet can contain only 140 characters or less, including punctuation marks and spaces. With the strict length constrain, it is hard for the attackers to hide much malicious content, like malware or a phishing page, in a normal message body.

Considering the previous reasons, it is nearly impossible to directly launch the typical cyber-attacks, such as malware distribution and phishing pages, on social media platforms. As a compromise, the attackers publish the URLs, which act as a gateway to external websites for further attacks.

The invisibility of cyber-attack is one of the top considered factors for the attackers. The URL itself is a string with purely ASCII texts and completely harmless. Therefore the attackers could publish them on any social media easily.

The cost of attack is another important factor. To register a new domain name, the attackers only need to speed a couple of dollars, no more than $20 in most cases. More economically, they can get a free subdomain from some free hosting service.

Additionally, specially crafted URLs could be deceptive and misleading. For example, one malicious URL could be http://facebook.hack.com/login. If the users did not pay much attention, they may treat this URL as the official login page of Facebook and enter their password.

The widely used URL shorten service makes the malicious URL less recognizable. To adapt to the message length limitation, URL shorten service is popular. Some social media platforms, such as Twitter, will mandatorily apply URL shorten service to all the URLs on their platforms. With this service, the original URL is transformed to an URL of the service provider. For example, the shortened URLs for http://google.com/ and http://hack.com may be http://bit.ly/ABCDEF and http://bit.ly/ABCDEG, respectively. The shortened URLs are composed with random letters and digits. They have no literal meaning. It is hard for the viewers to investigate them before clicking.

The URL redirection service also makes the URL to be a better gateway. These service pages are typically designed for internal usage of the websites. Because of the lack of source restriction, the attackers use redirection service a lot for malicious purpose. For example, the following URL http://12580wap.10086.cn/w/jump.php?v=2&url=%09//example.com belongs to the domain 10086.cn, which is owned and operated by one major carrier "China Mobile" in China. Most users will trust this URL as they see it is from China Mobile. However, this URL will automatically redirect the visitors to example.com. As we can see from the file name jump.php, this file is used to jump among different pages, originally inside 10086.cn. The software engineer forgot to investigate the "Referer" section in HTTP request header to check the caller. Therefore, the attackers can use this jump service page to create "reliable" URLs to spread on social media platforms.

What is the most important is the attackers have the complete control over the broadcasted URLs. They could change the content and direction of the URLs after publication and without the

awareness of the platforms. Initially, the URL could point to a normal webpage, such as a news report. After a while, the attackers could change its path, and the same URL will lead the later visitors to the real cyber-attack webpage. If the social media platforms only check the URL statically according to its textual content, they will never notice the change. Otherwise, the dynamic check uses much more resource, such as time and bandwidth.

Malicious URL is rather an old attack method. Because of the constraints on other cyber-attacks and the benefits of malicious URLs on social media, it becomes the major threat on all these platforms. Therefore, a lot of researches have been done to detect these malicious URLs. Some methods are for the general malicious URLs issue (Canali et al., 2011) (Thomas, Grier, Ma, et al., 2011) (Whittaker & Ryner, 2008). Some of them are specially optimized and/or designed for the social media platforms (Benevenuto et al., 2010) (Song et al., 2011).

When we need to design a detection system, we have to decide one critical and also basic question: should we check the URLs only when it is posted or updated? Our analysis shows definitely no. We need a multi-check system.

6.2. The Simplest Model of One-Time Check Scheme

In this section, we will propose a basic and simple model about the URL attack and defense. This model is an ideal one for the simplest attack and defense. However, it provides a solid basis for further analysis and discussion.

Because we are going to prove the one-time check system is far from protecting us, in our following discussion, we assume all the malicious URL detection algorithms has zero false positive and zero false negative, while in reality they perform worse.

In this model, we have one attacker and one defender. The attacker will publish a malicious URL on the social media platform and keep it malicious. The defender will check only when the URL

is initially posted or updated. The payoff is measured by the percentage of all visitors during the URL's lifecycle. If we assume the accuracy of the detection algorithm is d, we could get the payoff of the attacker and defender as:

$$\begin{cases} Payoff_A = (1-d) * 100\% \\ Payoff_D = d * 100\% \end{cases}$$

where $Payoff_A$ is for the attacker, and $Payoff_D$ for the defender.

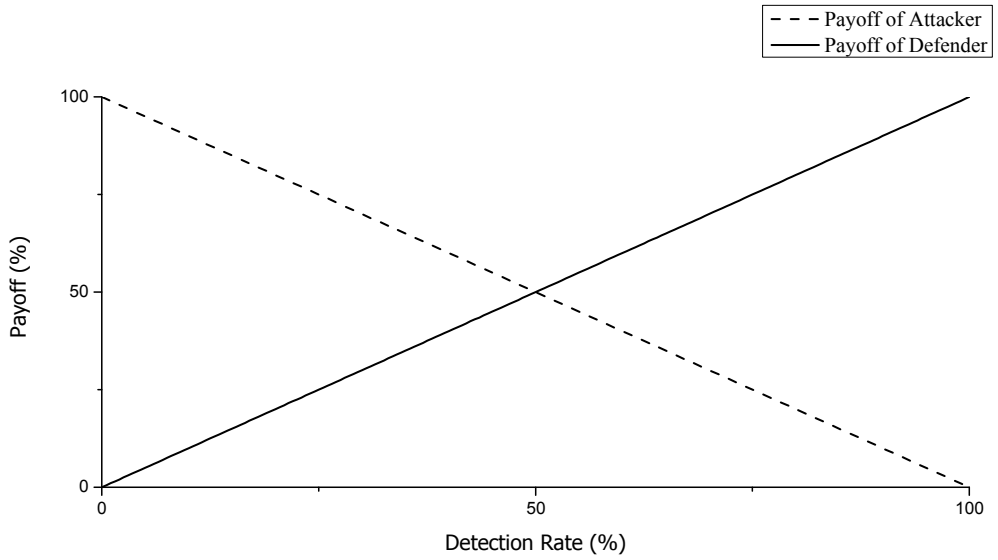


Figure 6-1. The Payoff of Attackers and Defender I – Always Malicious

The payoff of attacker is the expected percentage of the visitors, who access the malicious content from the URL. The payoff of defender is the expected percentage of the visitors, who are saved from viewing the malicious content. In this model, the payoff of attacker and defender is completely depending on the accuracy of the detection algorithm, which is between 0% and 100%. The relationship is shown in Fig. 6-1. If d is 0%, which is the worst case, the detection system is turned off or voided. It can never find out the malicious URLs. Consequently all users are threatened by the attackers. If d is 100%, which is the best but impossible condition, the

detection is so perfect that it discovers all the suspicious URLs. All the users are protected from any malicious content.

The sum of the payoffs would be 100%. In this model, the attackers will publish the URL, which is malicious during its lifecycle. All the visitors could be either attacked or protected, according to the detection accuracy. This model shows the importance of the suspicious URL detection method.

6.3. The Model of One-Time Check Scheme with Constant-Rate Partial Attack

The algorithm and method to discover malicious URLs are important, but not enough to protect us. The attackers will try every possible strategy to bypass the detections and capture as many victims as possible.

In this model, the attackers will take the advantage of their fully control over URLs to launch the partial attack. As we discussed in section 2.4 and 6.1, after the publication of URL, the owner could easily and stealthily change the corresponding content, which could be done with DNS flux, reversed proxy, or redirection. Being different from the first model in section 6.2, attackers do not always return the same content during the URLs' lifecycle.

The attackers could have a content pool, including different webpages. Some of the webpages are normal and even interesting, while others contain malicious content. When the URL is accessed, the attackers' server will choose one webpage from the pool randomly or with some pre-defined rules to return. Therefore, each request gets either a normal webpage or a malicious webpage, completely according to the attackers' choice. In the next discussion, we use p as the probability to get a malicious page for each individual request. The rate p is kept the same during the lifecycle.

Assuming the detector checks the URL at the *l* point (in percentage of its lifecycle), the payoffs of attackers and defenders are:

$$\begin{cases} Payoff_A = l * p + (1 - p * d) * (1 - l) * p \\ Payoff_D = p * d * (1 - l) * p \end{cases}$$

(6-1)

If some visitors use the suspicious URL but are not redirected to the malicious webpage, banning the URL does not stop this part of users from malicious content. Therefore the proportion of these lucky users is not counted in the defender's or attacker's payoff.

From the equation 6-1, the best strategy for defenders is to check the URL when it is published, because $Payoff_D$ is strictly decreasing with an increasing *l*. No matter when the system checks the URL, the probability, that the URL leads to malicious content and the system detects it, is always the same: $p * d$. However, if we check it earlier, we can protect more audience. Consequently, the equation 6-1 is simplified to:

$$\begin{cases} Payoff_A = (1 - p * d) * p * 100\% \\ Payoff_D = p * d * p * 100\% \end{cases}$$

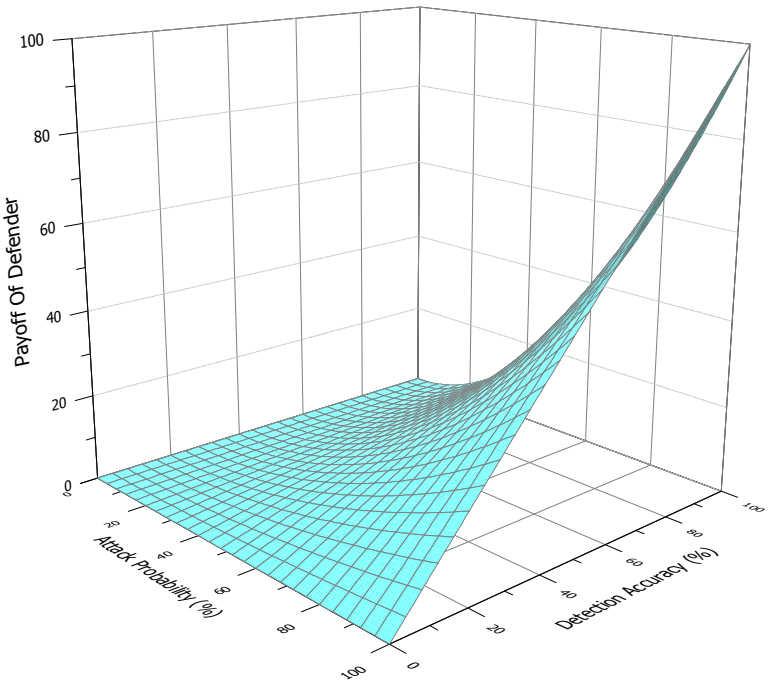
(6-2)

The payoff is determined by both players: attack' rate and detection's accuracy. The relationship is shown in Fig. 6.2. From the figure, the payoff of defender is strictly increasing with an increasing *p* and/or *d*. An excellent suspicious URL detection algorithm is essential and important in protecting us. A better method with higher accuracy will definitely save more users from being exposed to malicious content. The attacking rate also influents the defender's payoff. If the attacking rate is low, the potential victims are less. For payoff, we only consider these potential

victims, who will visit the malicious webpage rather than all visitors of the URL. As a result, the less potential victims make the attackers' payoff lower.

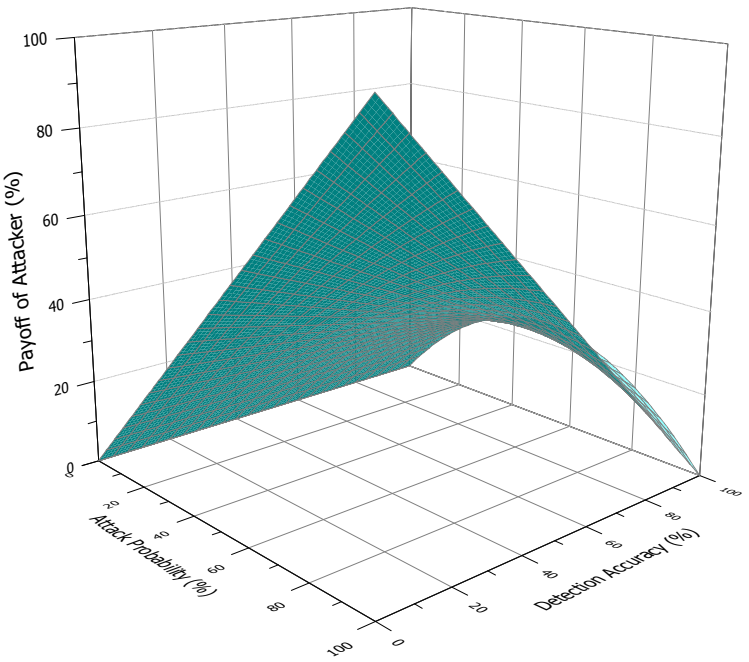
The payoff of attacker is more complicate. It is not strictly increasing or decreasing overall. When detection rate is smaller than 50%, it is strictly increasing. While in all the other given detection rate, the relationship between attack rate and payoff is in "n"-shape. To compute the peak point in equation 6-2, we get the maximal payoff as:

$$Payoff_A = \begin{cases} \frac{1}{4 * d} * 100\% & when\ p = \frac{1}{2 * d}\ and\ d \in [50\%, 100\%] \\ 100\% - d & when\ p = 100\%\ and\ d \in [0\%, 50\%) \end{cases} \tag{6-3}$$



(a) The Payoff of Defender

Figure 6-2. The Payoff of Attackers and Defender II – Partial Malicious



(b) The Payoff of Attacker

Figure 6-2. The Payoff of Attackers and Defender II – Partial Malicious (Cont.)

When the detection algorithm is not good enough, and the detection accuracy is lower than 50%, the attackers will publish the malicious URLs and keep them always leading the users to malicious webpages. In these cases, this model goes back to the one in section 6.2.

If our suspicious URL detector is better and has an accuracy being equal to or higher than 50%, the attacker will return normal webpages for $\left(1-\frac{1}{2*d}\right)*100\%$ of the requests, and malicious content for all the others. Under such condition, the payoff of defenders is $\frac{1}{4*d}*100\%$, which is completely the same as the payoff of attackers.

This maximal payoff is easy to achieve. The attackers could simply publish lots of prober URLs, which always point to malicious webpages with different content. After a while, they count how

many published malicious URLs are detected or blocked on the social media platform. Then an approximate detection accuracy rate could be estimated. Finally the attacker could determine their best strategy according to the equation 6-3.

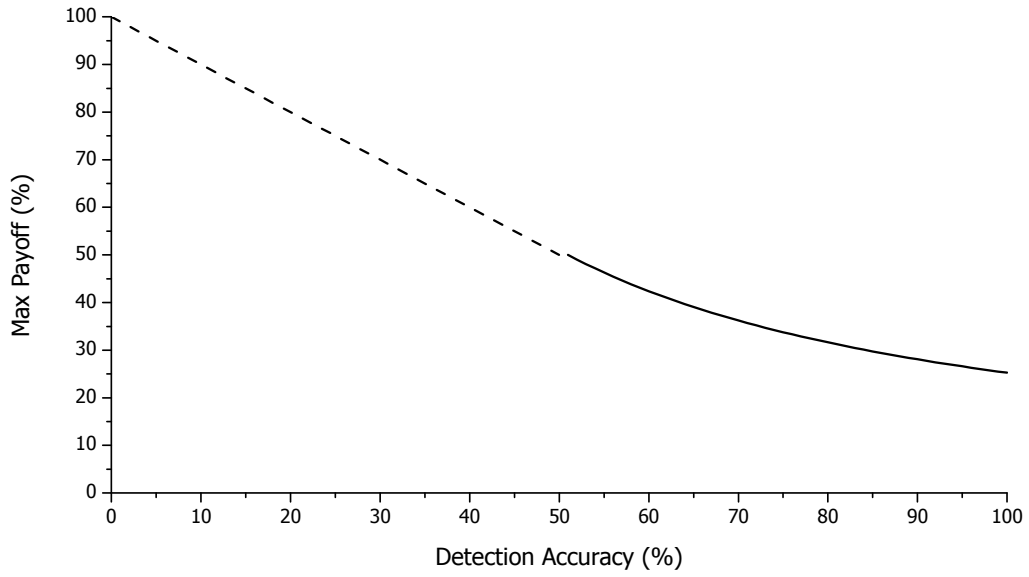


Figure 6-3. The Relation between Detection Rate and Maximal Attacker Payoff

If the attackers can adopt their best response, their payoff is remarkable, as shown in Fig. 6-3. Even though detectors with better accuracy do protect more users, the attackers could expect that, statistically at least a quarter of visitors will view their malicious webpages.

Even if the attackers made some bias during estimating the security system, the attacks could still get a noticeable number of victims. When the detection accuracy is perfectly 100%, the payoff of attackers with different strategy is shown in Fig. 6-4.

To get 20% or more payoff, the attacker needs to launch the malicious URLs with attacking rate between 28% and 72%. If the attacker lowers the expectation to 10% or more payoff, the attacking rate should be between 11% and 88%. These ranges are so wide that the attackers could nearly always get the “right” attacking strategy. In other words, if the detector only checks the

URLs when they are polished or updated, even with a perfect malicious URL detection algorithm, a reasonable attacker could easily get remarkable number of victims.

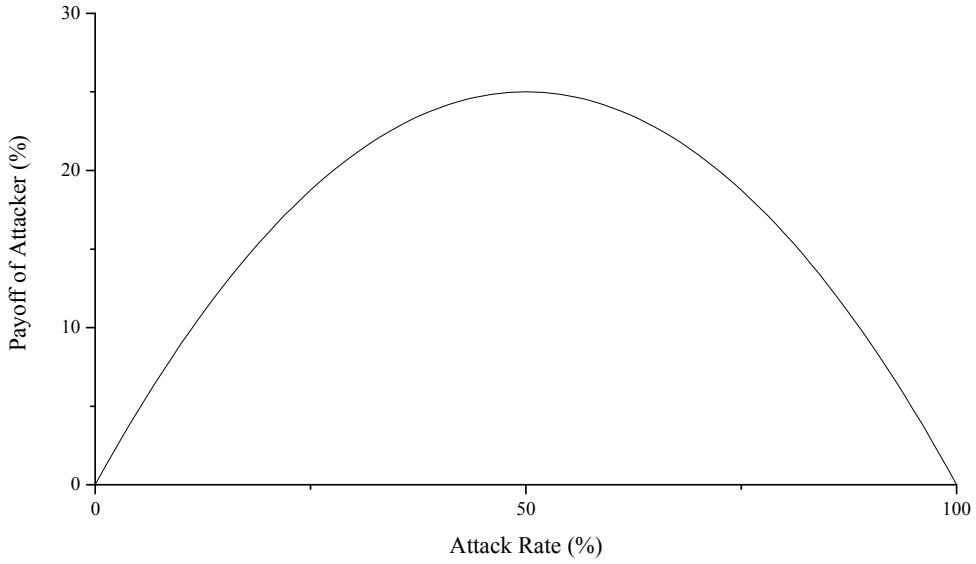


Figure 6-4. The Attacker's Payoff under Best Security

6.4. The Simplest Model of One-Time Check Scheme with Hibernation

In section 6.1, the importance of the detection algorithm is shown. However, in the section 6.2, the analysis result proves that a perfect detection algorithm is far from protecting us. The deployment scheme is also important. In this section, we will show another case, which also proves the weakness the one-check security system. In this model, we assume the detection algorithm is perfect with 100% accuracy, 0% false negative, and 0% false positive.

In this model, initially the malicious URLs have some time for hibernation. During the hibernation, the URLs will lead all the visitors to one normal webpage. After the hibernation, the URLs switch to attack mode, in which they return malicious content to all the visitors. Therefore, the attackers need to choose a start point between 0% and 100% in URLs' lifecycle to begin the

attacks. 0% means they will launch the attacks at the very beginning without any hibernation. 100% means they will never do attacks.

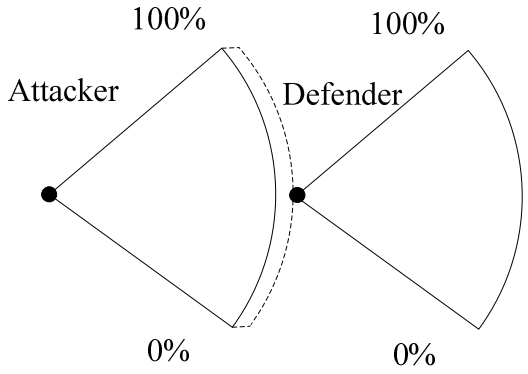


Figure 6-5. The Extended Form of the Game

Similarly, the defender needs to choose a point of the URL's lifecycle from 0% to 100% to check it. 0% means the system will investigate the URL when it is published or updated. 100% means the system does not take any security check. If both attackers and defenders choose 0%, this model is reduced to the one in section 6.2. Otherwise, this model is a game between the attackers and defenders. The extended form of the game is shown in Fig. 6-5.

The payoff for attackers is the percentage of visitors, which are exposed to the malicious webpages:

$$Payoff_A = \begin{cases} d - a & 0\% \le a \le d \le 100\% \\ 100\% - a & 0\% \le d < a \le 100\% \end{cases} \tag{6-4}$$

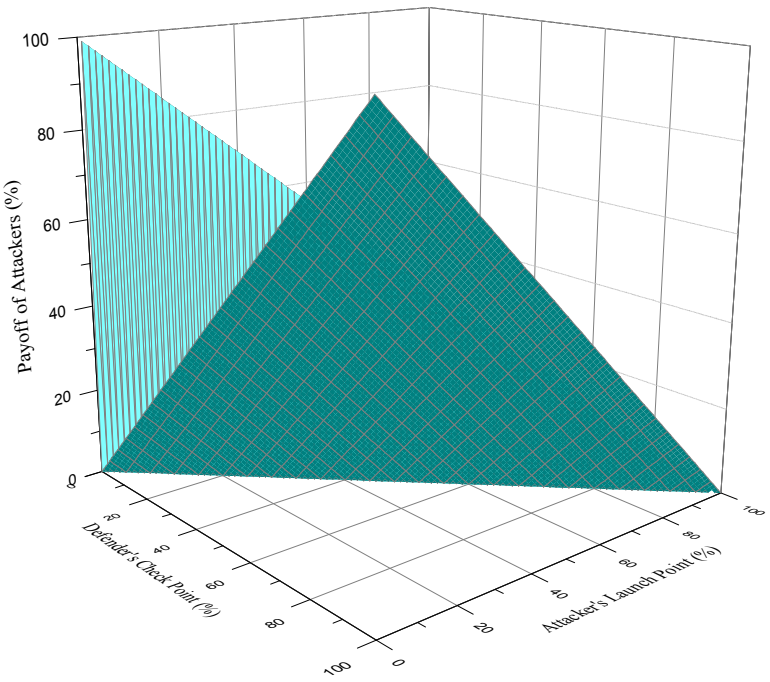
where *a* and *d* is the choices of the attacker and defender respectively.

Similarly the payoff for the defender is the percentage of users, who are saved from being exposed to the malicious content:

$$Payoff_D = \begin{cases} 100\% - d & 0 \le a \le d \le 100\% \\ 0 & 0 \le d < a \le 100\% \end{cases} \quad (6\text{-}5)$$

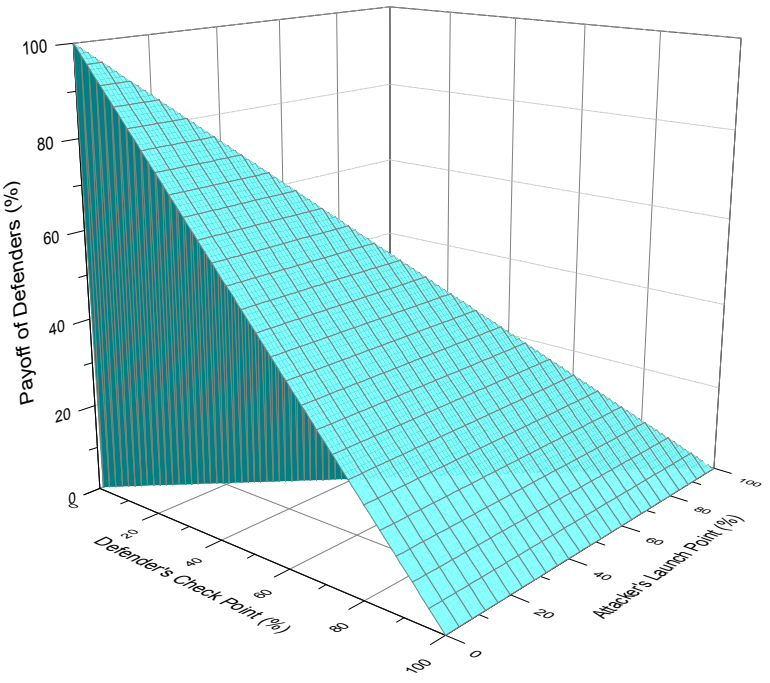
Like the models in section 6.2 and 6.3, the visitors before attacks have no chance to watch any malicious webpage. It is not because of the effort of defenders. Therefore, this part of users is not counted in the defender's payoff.

In this game, there is no pure strategy Nash equilibrium. If the choices of attacker and defender are different, the defender could always get more payoffs by moving to the attacker's point. However, if they choose one same point to take action, the attacker could always capture more



(a) The Payoff of Attacker

Figure 6-6. The Payoff of Attackers and Defender III – With Hibernation



(b) The Payoff of Defender

Figure 6-6. The Payoff of Attackers and Defender III – With Hibernation (Cont.)

victims by moving to any other point. In sum, there is no pure strategy Nash equilibrium, where both attackers and defenders have no motivation to change their choices. However, this game does have some mixed strategy Nash equilibriums.

First of all, here are some notations used in the next discussion:

x and z: a position between 0% and 100%.

$f(x)$: the probability that attacker choose *x* point to launch the attacks.

$F(z) = \int_0^z f(x)dx$: the probability that the attacker launch the attacks at or before *z*.

$g(x)$: the probability that defender choose *x* point to check the URL.

$G(z) = \int_0^z g(x)dx$: the probability that the defender check the URL at or before *z*.

All of them are using the percentage (%) as unit. Then the expected payoff for the attacker with chosen *x* point is:

$$EPA(x) = \int_0^x g(y) \times (100 - x)dy + \int_x^{100} g(y) \times (y - x)dy$$

$$= 100 \times G(x) - x + \int_x^{100} g(y) \times ydy$$

(6-6)

According to the Nash equilibrium theory, the defender will adopt the strategy to minimize the maximal expected payoff of the attacker:

$$EPA'(x) = 100 \times g(x) - 1 - g(x) \times x = 0$$

$$g(x) = \frac{1}{100 - x}$$

(6-7)

$G(z)$ is strongly connect with $g(x)$. From its definition and meaning, we can easily get its equation and range as [0%, 100%]:

$$G(z) = \int_0^z g(x)dx = \log_e 100 - \log_e(100 - z) \in [0, 100]$$

Then we could get the range of z:

$$0 \leq z \leq 100 - e^{\log_e 100 - 1} \approx 63.212$$

Combining the range of z and the equation 6-7, we could get the defender's best probability strategy as following:

$$g(x) = \begin{cases} \dfrac{1}{100 - x}, & when\ 0 \le x \le 100 - e^{\log_e 100 - 1} \\ 0, & when\ x > 100 - e^{\log_e 100 - 1} \end{cases}$$

(6-8)

If the defenders adopt this mixed strategy, $EPA'(x)$ is always 0. The payoff of attackers is always a constant value, no matter what attack strategy is used:

$$EPA(x) = EPA(y), \qquad \forall x, y \in [0, 100 - e^{\log_e 100 - 1}]$$

Combining the equation 6-6 and 6-8, for all x between 0 and $100 - e^{\log_e 100 - 1}$, we could get:

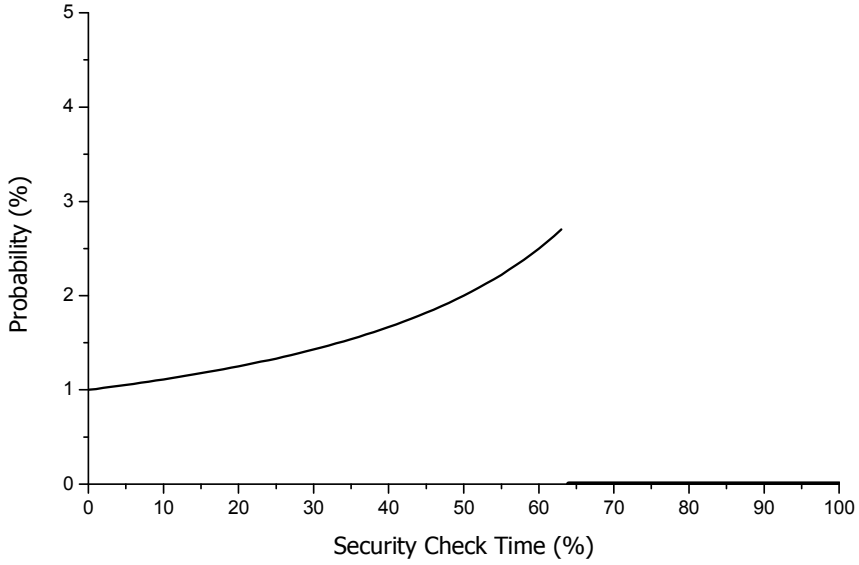
$$EPA(x) = EPA(0) = \int_0^{1000} g(y) * y dy$$

$$= \int_0^{100 - e^{\log_e 100 - 1}} g(y) * y dy$$

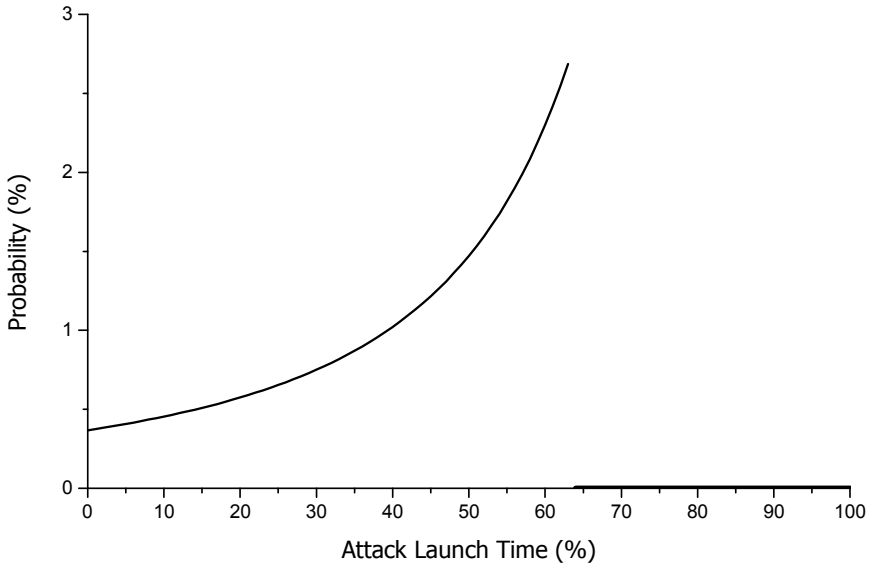
$$= e^{\log_e 100 - 1}$$

$$\approx 36.7879\%$$

For the range between $100 - e^{\log_e 100 - 1}$ (%) and 100%, because the security system would never check the URLs, the best response for attackers is to launch the attack at point $100 - e^{\log_e 100 - 1} + \varepsilon$, where ε is infinitesimal. As $100 - e^{\log_e 100 - 1} + \varepsilon = 100 - e^{\log_e 100 - 1}$, like the defenders, the attackers would never take any attack actions in this range. In summary, neither attackers nor defenders will take any actions inside this range.



(a) The Mixed Strategy for Defenders



(b) The Mixed Strategy for Attackers with C Being $e^{\log_e 100-1}$

Figure 6-7. The Mixed Strategy at the Nash Equilibrium (Cont.)

Similarly, the expected payoff of defender on point *y* is:

$$EPD(y) = \int_0^y f(x) * (100 - y)dx + \int_y^{100} f(x) * 0dx$$

$$= (100 - y) * F(y)$$

To minimize the maximal expected payoff of defenders, all the choices of y need to have the same output:

$$EPD'(y) = -F(y) + (100 - y) * f(y) = 0$$

$$F(y) = (100 - y) * f(y)$$

(6-9)

With the equation 6-9 and the definition of F(y) function, we get:

$$\int_0^y f(x)dx = (100 - y) * f(y)$$

Then we make derivation of y on both sides:

$$f(y) = -f(y) + (100 - y) * f'(y)$$

$$\frac{2}{100 - y} = \frac{f'(y)}{f(y)} = (\log_e f(y))'$$

$$\log_e f(y) = \int \frac{2}{100 - y} dy = \log_e \frac{C}{(100 - y)^2}$$

$$f(x) = \frac{C}{(100 - y)^2} \quad , \ where\ C\ is\ a\ positive\ constan\ number$$

(6-10)

Considering the equation 6-9 and 6-10, we can get:

$$\begin{cases} f(x) = \dfrac{C}{(100-x)^2} \in [0\%, 100\%] \\ F(x) = \dfrac{C}{100-x} \in [0\%, 100\%] \end{cases}$$

$$=> \ x \in [0, 100 - C]$$

(6-11)

As shown in our previous discussion, the attackers would never launch any attack in the range from $(100 - e^{\log_e 100-1})\%$ to 100%. Therefore, we can get:

$$100 - C \leq 100 - e^{\log_e 100-1}$$

$$C \geq e^{\log_e 100-1}$$

The sum of defenders' payoff and attackers' payoff must be equal to or less than 100%. So we can get:

$$EPA(0) + EPD(0) \leq 100$$

$$e^{\log_e 100-1} + C \leq 100$$

$$C \leq 100 - e^{\log_e 100-1}$$

In total, the range of C must be:

$$e^{\log_e 100-1} \leq C \leq 100 - e^{\log_e 100-1}$$

(6-12)

Combing equation 6-11 and 6-22, we could get the best strategy for attackers:

$$f(x) = \begin{cases} \dfrac{C}{(100-x)^2}, & when\ x \le 100 - C \\ 0, & when\ x > 100 - C \end{cases}$$

(6-13)

With this strategy, the defender's payoff is represented with C as:

$$EPD(y) = \begin{cases} C, & when\ y \in [0, 100 - C] \\ 0, & when\ y \in [100 - C, 100] \end{cases}$$

In other words, there is more than one best strategy for attackers. With any one of these strategies, the defenders will have a constant payoff, no matter how they take actions. At the same time, the attackers' payoff is already determined by the defenders' strategy. The choice among these candidate strategies does not influent attackers' payoff.

In this more complicate model with hibernation, the attackers get remarkable more payoff than they did in the previous models. With a perfect malicious URL detection algorithm with 100% accuracy, 0% false negative, and 0% false positive, in section 6-2, the attackers would get no victim. With partial attacks as in section 6-3, they could get up to 25% of the URL's audience being victims. With hibernation, they increase their payoff to nearly 36.7879%.

In summary, the model in section 6-2 proves the importance of the malicious URL detection algorithm and method. However, the models in section 6-3 and 6-4 prove that, an excellent or even perfect single-check method is far from enough to protect us.

We need to have a sub-system to monitor the real content of these URLs, and find out when it is polished and changed. For example, we could use similar ideas to assign a threat rank to each URL (Benevenuto et al., 2010) (K. Lee et al., 2010) (Stringhini et al., 2010). Then a sub-system will check the content of these URLs according their threat ranks. The URLs with higher threat

rank will be checked more frequently. The ones from reliable sources are less investigated. Every time the URL is published and the webpage for the URL is significantly changed, we need to use the malicious URL detection system to check it.

CHAPTER VII

DISCUSSION, FURTHER WORK AND CONCLUSION

In this dissertation, we analyzed how users adopt professional followees with empirical dataset, then explain these phenomena from an attention economics perspective, and finally talked about the malicious URLs on social media.

7.1. Discussion

The used datasets were sampled and provided by Tencent Inc. and they chose the most active users in the sampling period. However, the datasets do not provide the precise definition of "active" users. We do not know the standard by which the professional entities were chosen and labeled by the employees of Tencent Inc. Finally, the recommendation algorithm will have some impact on the result in chapter 5. However, at the statistical level, a few outliers cannot affect the general trend. A deeper examination on how different factors affect the results should be studied in the future.

There are still many open issues in this topic. Although we provide confirmation that the maximum number of professional followees in one individual category fits to power law, the factors which affect the upper limit of professional followees in a category for each user are not clear, and the model of adopting professional followees is not provided.

In addition, why the in-degree of professional entities varies greatly is unknown. It appears that being well-known in real life does not guarantee success on social networking service. This question requires further research from the perspective of microblogging marketing.

In our analysis, we used some theories and models of material economics. With the aggregate demand-aggregate supply model, we analyzed the capacity of followees in each category. Then game theory was used to investigate the interactions among followees and followers. Finally, utility theory is applied to determine how users choose followees in one individual category. These theories and models are shown to be useful.

In practice, we could use the indifference curve to get the aggregate demand-aggregate supply curves. But within social media, we don't know how to obtain accurate demand and supply curves. This is partly because attention is hard to measure and compare. To investigate the attention market better, we have to understand the users' demand and followees' supply.

With the interactions among followers and followees, the pure strategy Nash equilibrium is difficult to find or does not exist. Under such case, how should the followees determine their market position to maximize their market share? This is an open issue and the answer will be important for social media marketing.

When we measure the utility of users, our analysis combines multiple parameters, such as the user's demand, the quantity and quality of tweets from the last followee and all the others, and the overlap among the tweets. It is easy to figure out the general effect of each factor. But lacking a deep examination, we do not know the exact impact of each factor.

The detection schemes for malicious URLs are also discussed. A lot of researches on malicious URLs detection algorithm have been done. We are not focus on these algorithms, but the deployment of them. We proved that, even if the detection algorithm is real-time and perfect, the one-time check strategy is far from protecting us. The attackers are still able to spread these

URLs with a little effort. The result proves the necessary of a good-designed deployment scheme, in addition to an excellent detection method.

In practice, we cannot check the URLs too frequently because of the cost. Taking both the cost and threat into consideration, we have to find a balance between security and cost. According to the game theory, what is the best strategy for a multi-check system, such as the frequency and interval? This open challenge is significant for our information security.

7.2. Future Work

In future research, there should be a fuller investigation of the complex question of the nature of interactions among followers and followees. This represents a major departure from the work of previous researchers who consider all users within social media on the same footing. As we have seen, the motivations and goals of information providers and seekers are different. Classifying the users into groups and investigating their interactions based on a game–theoretic model will provide new insights. Also the extension of current game–theoretic model for malicious URL attacks could guide us to protect the users better.

The work presented in the dissertation and further extensions of it are based on the assumption that the followers are reasonable, and prefer the most valuable service to maximize their payoff. The payoff might include not only useful information, but also social satisfaction. For example, if friends of user u are following a specific topic, user u is more likely to pay attention to this topic to better integrate into the friends' circle.

Future research should focus on the following four topics:

1. It should be investigated how users add and drop followers. We have already found that statically the maximum capacity of followees in any individual category fits the power law distribution. However, it is not clear about the major factors that lie behind the

behavior of users and why and how users unfollow their current followees. For example, when a user has too much information in one category than wanted, he might need to choose one followee to unfollow. However, what controls the specific choice? From the perspective of the followee, what should be done to minimize the risk of being unfollowed?

2. The question of what is the best strategy for followees to maximize their market share and user's stickiness should be examined. For example, we would like to know what the optimized productivity rate is and what position in the market should be held. We will also investigate what the followees are currently doing with or without pure strategy Nash equilibrium point, and what they should do to increase their followers. For example, in the Hotelling's model, it is assumed, when one provider cannot get the same payoff as others, he will quit the market. In practice, some followees expect less return on investment than others. With these additional assumptions, the analysis will be different.

3. The matter of equilibrium points in the social network should be investigated by using results from multi-party game theory. At the equilibrium points, the common users have enough information with affordable attention, while the professional users get abundant attention. If there are multiply points, which one is global optimized?

4. Another important part of the research for future extensions of our work is design mechanisms to achieve the equilibrium point or best response point for the followees. If there are points as a win-win outcome, how could the social networking service be designed to drive the players to these points? In any society, various regulatory mechanisms keep economic and other participatory systems working in a stable manner. Should the social networking service providers develop similar regulatory mechanisms? Further, how should the interventions of the regulatory mechanisms be operated?

5. It should also be determined what kind of multi-check system is best in detecting these malicious URLs on social media. If we check the content of the URLs with frequency too high, the cost for security system, such as time and network bandwidth, is unaffordable. However, if we do it with a big interval, we cannot protect our users well. Therefore, guided by game theory, we need to find a balance between the security and cost.

7.3. Conclusion

The results of this study could be useful in microblogging marketing. Marketing personnel could discover potential customers better with the results of this proposal. Users with less than 3 followees in the one category do not show significant interest in corresponding field, and have a relative low adoption rate for recommendations. If the microblogging marketers propagate themselves to these users, the efficiency will be low, because of low adoption rate. On the other hand, users following more than 9 entities in the category show great interest, and have a higher adoption rate. However, the number of these users is small. In addition, according to their extraordinary interest in their topics, they are not likely to be common users. As a result, on balance, users who follow 3 to 9 professional entities in the category are the best ones to be targeted for promotion.

In addition, analyzing the distribution of users' followees will be helpful in automatic classification of the users. If some users follow many more entities in a single category than most of the masses, they show an extraordinary interest in corresponding field. Such information could be used to find these "uncommon" users.

Finally, our game–theoretic models for malicious URL attacks prove the importance of both the detection algorithms and their deployment schemes. A one-time-check deployment is definitely insufficient. We must put as much attention on deployment schemes as that on detection

algorithms. These models again witness the usefulness of game theory in information security field.

In summary, in our analyses, we found that many ideas of traditional material economics are also useful in explaining the phenomena of attention economics in social media. These different fields of economics have many differences in details. For example, in traditional economics, the goods are in scarcity. In contrast, in attention economics, the attention of customers is the scarcest thing. However, essentially they have the same focuses: what to produce, how to produce, whom to be serviced.

REFERENCES

Acock, A. C., & Hurlbert, J. S. (1990). Social Network Analysis: A Structural Perspective for Family Studies. *Journal of Social and Personal Relationships*, *7*(2), 245–264. doi:10.1177/0265407590072006

Ahn, Y.-Y., Han, S., Kwak, H., Moon, S., & Jeong, H. (2007). Analysis of topological characteristics of huge online social networking services. In *Proceedings of the 16th international conference on World Wide Web - WWW '07* (p. 835). New York, New York, USA: ACM Press. doi:10.1145/1242572.1242685

Asur, S., & Huberman, B. A. (2010). Predicting the future with social media. In *2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology* (pp. 492–499). Computers and Society; Physics and Society, IEEE. doi:10.1109/WI-IAT.2010.63

Barabási, A., & Albert, R. (1999). Emergence of scaling in random networks. *Science*, *286*(5439), 1–11. Retrieved from http://www.sciencemag.org/content/286/5439/509.short

Benevenuto, F., Magno, G., Rodrigues, T., & Almeida, V. (2010). Detecting spammers on twitter. *Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference (CEAS)*, *6*, 12.

Borgatti, S. P., Mehra, A., Brass, D. J., & Labianca, G. (2009). Network analysis in the social sciences. *Science (New York, N.Y.)*, *323*(5916), 892–5. doi:10.1126/science.1165821

Bothos, E., Apostolou, D., & Mentzas, G. (2010). Using social media to predict future events with agent-based markets. *IEEE Intelligent Systems*, *25*, 50–58. doi:10.1109/MIS.2010.152

Canali, D., Cova, M., Vigna, G., & Kruegel, C. (2011). Prophiler : A Fast Filter for the Large-Scale Detection of Malicious Web Pages Categories and Subject Descriptors. In *Proc. of the International World Wide Web Conference (WWW)* (pp. 197–206). doi:10.1145/1963405.1963436

Cartwright, D., & Harary, F. (1956). Structural balance: a generalization of Heider's theory. *Psychological Review*, *63*(5). Retrieved from http://psycnet.apa.org/?fa=main.doiLanding&uid=1957-06811-001

Cha, M., Haddadi, H., Benevenuto, F., & Gummadi, K. (2010). Measuring user influence in Twitter: the million follower fallacy. In *Proceeding of the fourth international AAAI conference on weblogs and social media* (pp. 10–17).

Acock, A. C., & Hurlbert, J. S. (1990). Social Network Analysis: A Structural Perspective for Family Studies. *Journal of Social and Personal Relationships*, *7*(2), 245–264. doi:10.1177/0265407590072006

Ahn, Y.-Y., Han, S., Kwak, H., Moon, S., & Jeong, H. (2007). Analysis of topological characteristics of huge online social networking services. In *Proceedings of the 16th international conference on World Wide Web - WWW '07* (p. 835). New York, New York, USA: ACM Press. doi:10.1145/1242572.1242685

Asur, S., & Huberman, B. A. (2010). Predicting the future with social media. In *2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology* (pp. 492–499). Computers and Society; Physics and Society, IEEE. doi:10.1109/WI-IAT.2010.63

Barabási, A., & Albert, R. (1999). Emergence of scaling in random networks. *Science*, *286*(5439), 1–11. Retrieved from http://www.sciencemag.org/content/286/5439/509.short

Benevenuto, F., Magno, G., Rodrigues, T., & Almeida, V. (2010). Detecting spammers on twitter. *Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference (CEAS)*, *6*, 12.

Borgatti, S. P., Mehra, A., Brass, D. J., & Labianca, G. (2009). Network analysis in the social sciences. *Science (New York, N.Y.)*, *323*(5916), 892–5. doi:10.1126/science.1165821

Bothos, E., Apostolou, D., & Mentzas, G. (2010). Using social media to predict future events with agent-based markets. *IEEE Intelligent Systems*, *25*, 50–58. doi:10.1109/MIS.2010.152

Canali, D., Cova, M., Vigna, G., & Kruegel, C. (2011). Prophiler : A Fast Filter for the Large-Scale Detection of Malicious Web Pages Categories and Subject Descriptors. In *Proc. of the International World Wide Web Conference (WWW)* (pp. 197–206). doi:10.1145/1963405.1963436

Cartwright, D., & Harary, F. (1956). Structural balance: a generalization of Heider's theory. *Psychological Review*, *63*(5). Retrieved from http://psycnet.apa.org/?fa=main.doiLanding&uid=1957-06811-001

Cha, M., Haddadi, H., Benevenuto, F., & Gummadi, K. (2010). Measuring user influence in Twitter: the million follower fallacy. In *Proceeding of the fourth international AAAI conference on weblogs and social media* (pp. 10–17).

Cha, M., Mislove, A., & Gummadi, K. P. (2009). A measurement-driven analysis of information propagation in the flickr social network. In *Proceedings of the 18th international conference on World wide web - WWW '09* (p. 721). New York, New York, USA: ACM Press. doi:10.1145/1526709.1526806

Chris, A. (2007). The Long Tail: Why the Future of Business Is Selling Less of More. *Journal of Product Innovation Management*, *24*(3), 274–276. doi:10.1111/j.1540-5885.2007.00250.x

Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2010). Who is Tweeting on Twitter: Human, Bot, or Cyborg? In *Proceedings of the 26th Annual Computer Security Applications Conference on - ACSAC '10* (p. 21). doi:10.1145/1920261.1920265

Congleton RD. (2002). The Median Voter Model. Retrieved from http://rdc1.net/forthcoming/medianvt.pdf

Dutt, A. (2002). Aggregate demand-aggregate supply analysis: A history. *History of Political Economy*, *34*(2), 321–363. Retrieved from http://europepmc.org/abstract/MED/10170332

Eation, B. C., & Lipsey, R. G. (1975). The Principle of Minimum Differentiation Reconsidered: Some New Developments in the Theory of Spatial Competition. *The Review of Economic Studies*, *42*(1), 27–49.

Ebel, H., Mielsch, L.-I., & Bornholdt, S. (2002). Scale-free topology of e-mail networks. *Physical Review E*, *66*(3). doi:10.1103/PhysRevE.66.035103

Eckersley, P. (2010). How unique is your web browser? In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 6205 LNCS, pp. 1–18). doi:10.1007/978-3-642-14527-8_1

Enelow, J. M., & Hinich, M. J. (1989). A general probabilistic spatial theory of election. *Public Choice*, *61*, 101–113.

Erik, B., & Joo, H. O. (2013). The Attention Economy: Measuring the Value of Free Digital Services on the Internet.

Erik, B., Yu, J. H., & Michael, D. S. (2006). From niches to riches: Anatomy of the long tail. *MIT Sloan Management Review*, *47*(4), 67–71. doi:10.2139/ssrn.918142

Essig, M., & Arnold, U. (2001). Electronic Procurement in Supply Chain Management: An Information Economics-Based Analysis of Electronic Markets. *The Journal of Supply Chain Management*, *37*(4), 43–49. doi:10.1111/j.1745-493X.2001.tb00112.x

Evans, P. B., & Wurster, T. S. (1997). Strategy and the new economics of information. *Harvard Business Review*, *75*(5), 70–82. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/10170332

Facebook Data Team. (2012). Anatomy of Facebook. Retrieved January 06, 2012, from https://www.facebook.com/notes/facebook-data-team/anatomy-of-facebook/10150388519243859

Goel, S., Broder, A., Gabrilovich, E., & Pang, B. (2010). Anatomy of the Long Tail : Ordinary People with Extraordinary Tastes. In *Proceedings of the third ACM international conference on Web search and data mining - WSDM '10* (p. 201). New York, New York, USA: ACM Press. doi:10.1145/1718487.1718513

Grier, C., Thomas, K., Paxson, V., & Zhang, M. (2010). @ spam : The Underground on 140 Characters or Less Categories and Subject Descriptors. In *Proceedings of the 17th ACM*

conference on Computer and communications security (pp. 27–37). doi:10.1145/1866307.1866311

Guo, Y., & Chen, J. (2010). A Case Study: Social Network and Knowledge Sharing. In *2010 International Conference on E-Business and E-Government* (pp. 1715–1718). IEEE. doi:10.1109/ICEE.2010.434

Hanson, R. D., & Hanson, R. (2006). Foul Play in Information Markets. In *Information Markets: A New Way of Making Decisions* (pp. 126–141).

Hassan, A. S., & Rafie, M. A. M. (2010). A survey of Game Theory using Evolutionary Algorithms. In *2010 International Symposium on Information Technology* (pp. 1319–1325). IEEE. doi:10.1109/ITSIM.2010.5561648

Heider, F. (1946). Attitudes and cognitive organization. *The Journal of Psychology*, 1–3. Retrieved from http://www.tandfonline.com/doi/pdf/10.1080/00223980.1946.9917275

Holcombe, R. G. (1989). The median voter model in public choice theory. *Public Choice*, *61*(2), 115–125. doi:10.1007/BF00115658

Huberman, B. A., Romero, D. M., & Wu, F. (2008). Social networks that matter: Twitter under the microscope. Computers and Society; Physics and Society. Retrieved from http://arxiv.org/abs/0812.1045

Java, A., Song, X., Finin, T., & Tseng, B. (2007). Why we twitter: understanding microblogging usage and communities. In *Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 workshop on Web mining and social network analysis - WebKDD/SNA-KDD '07* (pp. 56–65). New York, New York, USA: ACM Press. doi:10.1145/1348549.1348556

Kleinberg, J. (2000). The small-world phenomenon : an algorithmic perspective. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing - STOC '00* (pp. 163–170). New York, New York, USA: ACM Press. doi:10.1145/335305.335325

Kwak, H., Lee, C., Park, H., & Moon, S. (2010). What is Twitter, a social network or a news media? In *Proceedings of the 19th international conference on World wide web - WWW '10* (p. 591). New York, New York, USA: ACM Press. doi:10.1145/1772690.1772751

Lee, K., Caverlee, J., & Webb, S. (2010). Uncovering social spammers: social honeypots+ machine learning. In *SIGIR'10, July 19–23, 2010, Geneva, Switzerland. Copyright* (pp. 435–442). doi:10.1145/1835449.1835522

Lee, S., & Kim, J. (2013). Warning bird: A near real-time detection system for suspicious URLs in twitter stream. *IEEE Transactions on Dependable and Secure Computing*, *10*, 183–195. doi:10.1109/TDSC.2013.3

Leskovec, J., & Horvitz, E. (2008). Planetary-scale views on a large instant-messaging network. In *Proceeding of the 17th international conference on World Wide Web - WWW '08* (p. 915). New York, New York, USA: ACM Press. doi:10.1145/1367497.1367620

McGrath, D. K., & Gupta, M. (2008). Behind phishing: an examination of phisher modi operandi. In *Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET)* (p. 4).

Mendoza, M., Poblete, B., & Castillo, C. (2010). Twitter Under Crisis : Can we trust what we RT ? In *Proceedings of the First Workshop on Social Media Analytics - SOMA '10* (pp. 71–79). New York, New York, USA: ACM Press. doi:10.1145/1964858.1964869

Michael H Goldhaber. (1997). The Attention Economy and the Net. *First Monday*, *2*(4), 1–27.

Mislove, A., Marcon, M., Gummadi, K. P., Druschel, P., & Bhattacharjee, B. (2007). Measurement and analysis of online social networks. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement - IMC '07* (p. 29). New York, New York, USA: ACM Press. doi:10.1145/1298306.1298311

Mockapetris, P. V. (1987). RFC 1035 - Domain names: Implementation and Specification. *Network Working Group*, 55. Retrieved from http://tools.ietf.org/html/rfc1035

Obied, A., & Alhajj, R. (2009). Fraudulent and malicious sites on the web. *Applied Intelligence*, *30*, 112–120. doi:10.1007/s10489-007-0102-y

Pope, N. (2007). The Economics of Attention: Style and Substance in the Age of Information (review). *Technology and Culture*, *48*(3), 673–675. doi:10.1353/tech.2007.0128

Quiggin, J. (1982). A theory of anticipated utility. *Journal of Economic Behavior & Organization*, *3*(4), 323–343. doi:10.1016/0167-2681(82)90008-7

Sakaki, T., Okazaki, M., & Matsuo, Y. (2010). Earthquake shakes Twitter users: real-time event detection by social sensors. In *Proceedings of the 19th international conference on World wide web - WWW '10* (p. 851). New York, New York, USA: ACM Press. doi:10.1145/1772690.1772777

Shaked, A. (1982). Existence and computation of mixed strategy Nash equilibrium for 3-firms location problem. *The Journal of Industrial Economics*, *31*(1), 93–96. Retrieved from http://www.jstor.org/stable/10.2307/2098006

Song, J., Lee, S., & Kim, J. (2011). Spam filtering in twitter using sender-receiver relationship. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 6961 LNCS, pp. 301–317). doi:10.1007/978-3-642-23644-0_16

Starmer, C. (2000). Developments in non-expected utility theory: The hunt for a descriptive theory of choice under risk. *Journal of Economic Literature*, *38*(2), 332–382. Retrieved from http://www.jstor.org/stable/10.2307/2565292

Stringhini, G., Kruegel, C., & Vigna, G. (2010). Detecting spammers on social networks. In *Annual Computer Security Applications Conference(ACSAC)* (p. 1). doi:10.1145/1920261.1920263

Thomas, K., Grier, C., Ma, J., Paxson, V., & Song, D. (2011). Design and evaluation of a real-time URL spam filtering service. In *Proceedings - IEEE Symposium on Security and Privacy* (pp. 447–462). doi:10.1109/SP.2011.25

Thomas, K., Grier, C., Song, D., & Paxson, V. (2011). Suspended accounts in retrospect: an analysis of twitter spam. *Proceedings of the 2011 ACM ...*, 243–258. doi:10.1145/2068816.2068840

Tumasjan, A., Sprenger, T. O., Sandner, P. G., & Welpe, I. M. (2010). Predicting elections with Twitter : what 140 characters reveal about political sentiment. In *Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media* (pp. 178–185).

Watts, D. J. (2004). The "New" Science of Networks. *Annual Review of Sociology*, *30*(1), 243–270. doi:10.1146/annurev.soc.30.020404.104342

Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of "small-world" networks. *Nature*, *393*(6684), 440–2. doi:10.1038/30918

Whittaker, C., & Ryner, B. (2008). Large-Scale Automatic Classification of Phishing Pages. *Design*.

Wilson, M., & Nicholas, C. (2008). Topological analysis of an online social network for older adults. In *Proceeding of the 2008 ACM workshop on Search in social media - SSM '08* (p. 51). New York, New York, USA: ACM Press. doi:10.1145/1458583.1458596

Wolfers, J., & Zitzewitz, E. (2004). Prediction Markets. *Journal of Economic Perspectives*. doi:10.1257/0895330041371321

Yang, C., Harkreader, R. C., & Gu, G. (2011). Die free or live hard? Empirical evaluation and new design for fighting evolving twitter spammers. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 6961 LNCS, pp. 318–337). doi:10.1007/978-3-642-23644-0_17

Yu, S., & Kak, S. (2012, March 7). A Survey of Prediction Using Social Media [Physics and Society]. Retrieved March 11, 2013, from http://arxiv.org/abs/1203.1647

Yu, S., & Kak, S. (2014). Social Network Dynamics: An Attention Economics Perspective. In W. Pedrycz & S.-M. Chen (Eds.), *Social Networks: A Framework of Computational Intelligence* (Vol. 526, pp. 225–258). Cham: Springer International Publishing. doi:10.1007/978-3-319-02993-1

Yu, S., Zhou, S., & Wang, S. (2010). Fast-flux attack network identification based on agent lifespan. In *Proceedings - 2010 IEEE International Conference on Wireless Communications, Networking and Information Security, WCNIS 2010* (pp. 658–662). doi:10.1109/WCINS.2010.5541861

Zhao, P., & Hoi, S. C. H. (2013). Cost-sensitive online active learning with application to malicious URL detection. *Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD '13*, 919. doi:10.1145/2487575.2487647

VITA

Sheng Yu

Candidate for the Degree of

Doctor of Philosophy

Thesis: APPLICATIONS OF ATTENTION ECONOMICS IN STUDYING EQUILIBRIA IN SOCIAL NETWORKING

Major Field: Computer Science

Biographical:

Education:

Completed the requirements for the Doctor of Philosophy in Computer Science at Oklahoma State University, Stillwater, Oklahoma in December, 2014.

Completed the requirements for the Master of Science in Information and Communication Engineering at University of Electronic science and Technology of China, Chengdu, China in 2010.

Completed the requirements for the Bachelor of Science in Information Security at University of Electronic science and Technology of China, Chengdu, China in 2007.