WI-FI NETWORK SECURITY - GENDER DIFFERENCES IN CHINA
2014KANI23

Bachelor's thesis in Informatics (15 credits)
MA LIUXINWEI

Fall 2014
Title: Wi-Fi Network Security- Gender Differences in China

Year: 2014

Author/s: Ma Liuxinwei

Supervisor: Patrik Hedberg

Abstract

With the development of Wi-Fi networks, Wi-Fi connection become a very important part of people’s life, it seems that Wi-Fi networks are everywhere, especially in China. However, Wi-Fi networks not only bring convenience to users, but also bring some security threats. Nowadays, Wi-Fi security problems become increasingly acute. This thesis investigates the differences between male and female users regarding Wi-Fi network security. By distributing a questionnaire in China, specific questions have been asked about key factors within the area of Wi-Fi security. The questions focus on the usage situation, information security awareness and the knowledge level in Wi-Fi related fields. The found result is: Wi-Fi security issues are more prominent for female users than for male users.

Keywords:
Wi-Fi Network, Wi-Fi Security Threats, Public Wi-Fi, Home Wi-Fi, Router Security, Gender Different.
Acknowledgements
I want to thank my supervisor Patrik Hedberg for his kind and thoughtful help. I want to thank all respondents for taking time to answer my survey. My English isn’t too perfect. I want to thank Rolf Appelkvist for helping me with the language.
## Contents of Tables

Table 1 Number of Wi-Fi Hotspots in China ................................................................. - 9 -
Table 2 Number of Trouble Hotspots in Different Aspects .......................................... - 9 -
Table 3 Average Internet Speed of Different Companies in China ................................. - 10 -
Table 4 Example of Fake Public Wi-Fi ........................................................................... - 14 -
Table 5 Segmentation of Respondents ........................................................................... - 22 -
Table 6 Activities of Users Conducted by Using Wi-Fi Network ..................................... - 24 -
Table 7 Use Automatic Connection Software or Not ...................................................... - 26 -
Table 8 Distinguish the Real Public Wi-Fi before Use it .................................................. - 26 -
Table 9 Connect Wi-Fi Networks through VPN ............................................................... - 27 -
Table 10 Different Choice of Gender .............................................................................. - 28 -
Table 11 Different Choice of Age Group ........................................................................ - 28 -
Table 12 Using Different Ways to Access Internet ......................................................... - 31 -
Table 13 Number of Respondents Use Different Password in Different Gender (150 Respondents) ........................................................................................................ - 32 -
Table 14 Gender Knowledge of VPN Influence by ........................................................ - 34 -
Table 15 Different Chosen of the Questions ................................................................... - 34 -
Table 16 Mean Value of Different Gender ..................................................................... - 35 -
Table 17 ANOVA of Relationship between Gender and Factors .................................... - 35 -
Contents of Figures

Figure 1 Global Distribution of Wi-Fi Hotspots (ABI Research, 2014).................................................. - 2 -
Figure 2 Consumption of Smart Phones, Pads and Routers in China and Worldwide in 2013
(ABI Research, 2014)........................................................................................................... - 2 -
Figure 3 802.11 Protocol Group Parameters........................................................................................................... - 9 -
Figure 4 Procedure of DNS Hijacking.................................................................................................................. - 15 -
Figure 5 Five Steps of this Research Procedure......................................................................................................... - 18 -
Figure 6 Types of Wi-Fi Networks for Internet Access.............................................................................................. - 22 -
Figure 7 Time Spend on Wi-Fi Connection.................................................................................................................. - 23 -
Figure 8 Number of Devices in Wi-Fi Connection.......................................................................................................... - 23 -
Figure 9 Devices Use for Connect Wi-Fi Network ........................................................................................................... - 24 -
Figure 10 Satisfaction of Internet Speed..................................................................................................................... - 24 -
Figure 11 The Reason of Slowly Internet Speed........................................................................................................... - 25 -
Figure 12 Reasons Make the Wi-Fi Networks Robbed by Others.................................................................................. - 25 -
Figure 13 Ways to Access Internet............................................................................................................................... - 26 -
Figure 14 Ways of People Install the Router .................................................................................................................. - 27 -
Figure 15 Content of Connection Password.................................................................................................................. - 28 -
Figure 16 Main Setting Options of Routers Operated by Responders........................................................................... - 29 -
Figure 17 The Reasons Cannot Access to Internet (After Repaired)................................................................................ - 29 -
Figure 18 Problems among People When Use Routers................................................................................................. - 30 -
Figure 19 Percentage of People Cannot Configure Settings of Router......................................................................... - 32 -
Figure 20 Security Vulnerability Proportion of Public Wi-Fi.......................................................................................... - 33 -
## Abbreviations Used

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL</td>
<td>Asymmetric Digital Subscriber Line</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AP</td>
<td>Access Points</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>BSS</td>
<td>Basic Service Set</td>
</tr>
<tr>
<td>CCTV</td>
<td>China Central Television</td>
</tr>
<tr>
<td>CDPD</td>
<td>Cellular Digital Packet Data</td>
</tr>
<tr>
<td>CNNIC</td>
<td>China Internet Network Information Centre</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DOS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>Nmap</td>
<td>Network Mapper</td>
</tr>
<tr>
<td>QSS</td>
<td>Quick Set System</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WANET</td>
<td>Wireless AD HOC Network</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WDS</td>
<td>Wireless distribution system</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WNIC</td>
<td>Wireless Network Interface Card</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>WPA2</td>
<td>Wi-Fi Protected Access II</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless Personal Area Network</td>
</tr>
<tr>
<td>WSN</td>
<td>Wireless Sensor Network</td>
</tr>
<tr>
<td>WWAN</td>
<td>Wireless Wide Area Network</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Background

Internet access has become an integral part of our everyday lives. With the increased use of the Internet, and the widespread use of telecommunication technology, the use has become more mobile. While the use of mobile devices such as smartphones, netbooks, notebooks and computer tablets has exploded, so have the demand for Internet connectivity. The use of cloud storage services in China (e.g., Baidu, 360, 163, Dropbox, etc.), the spread of communication Apps and software (e.g., WeChat, QQ, Skype, etc.) and social networking Apps and software (e.g., WeChat, Weibo, Renren, Zhihu, Facebook, etc.) that run on mobile devices, and the movement of a record-setting volume of data across the networks, have caused a demand for reliable Wi-Fi services which are seamless, secure and always-on. In this mobile world, the traditional wired network cannot satisfy the requirements of users anymore (Wang, 2008), and the demand for mobile Internet traffic of users have gradually increased, and with the high cost of 2G, 3G and 4G traffic, it undoubtedly Wi-Fi network, when available, has become the best choice for network users.

1.1.1 Internet Development in China

In April 1994, China achieved its full-functional connection to the Internet by opening a 64 kbps international dedicated line to the Internet, and was then officially recognized as a country with full functional Internet accessibility. At the end of 2010, the Statistical Report on China’s Internet Development was released by the China Internet Network Information Centre (CNNIC), the number of internet users raised to 457 million, up 73.3 million from one year earlier. Therefore, the development of wireless local area networks is increasingly becoming the focus of public concern (Karygiannis & Owens, 2002). Wireless networks have been widely used in many fields. Wireless communication’s benefit to organizations and users in many ways, such as portability, flexibility, increased productivity as well as it has lower installation costs (Rong, et al., 2013).

According to the Statistical Report from CNNIC, by the end of June 2014, the overall number of Internet users was 632 million, with an increase by 1.1% compared to the end of 2013. By the end of 2014, 48.6% of Chinese Internet users think that the network environment in China is safe or very safe.

According to Wang’s (2008) and Karygiannis’s (2002) work, wireless networks serve as the transport mechanism between devices, and between devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), Wireless Local Area Networks (WLANs), and Wireless Personal Area Networks (WPAN). WWAN includes wide coverage area technologies such as: 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), and Mobitex. WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others.

1.1.2 The Development of Wi-Fi (IEEE 802.11)

“Wi-Fi”, the full name of which is Wireless Fidelity, actually is a brand certification from Wi-Fi Alliance, which certificate wireless local area network (WLAN) equipment in line with
criteria set up by IEEE standard 802.11, it also used as synonymous term for IEEE standard 802.11 protocol (IEEE Advancing Technology for Humanity, 2015). WLANs are based on the IEEE802.11 standard, which is to support medium range, higher data rate applications (Karygiannis & Owens, 2002).

As for 2014 official statistical data (ABI Research, 2014), in 2013 (see figure 1 below), the number of Wi-Fi worldwide hotspots reached 4.2 million, of which the Asia-Pacific region accounted for 68.6% of the hotspots, Latin America accounted for 12.3%, Europe for 9 percent, North America accounted for 8.7% and Middle East and Africa accounted for 1.4 percent. As the statistic predicted, the global number of Wi-Fi hotspots will increase 15% every year until 2018, the whole number of Wi-Fi hotspots will reach a peak of more than 10 million in 2018.

Figure 1 Global Distribution of Wi-Fi Hotspots (ABI Research, 2014)

Besides, with the development of Wi-Fi products’ market, the amount of consumption of technological equipment and Wi-Fi terminal equipment will have a considerable growth. Based on statistics data from ABI Research (2014), the consumption of global Wi-Fi client devices, including access point routers and gateways, (see figure 2) reached the number of more than 139 million pieces worldwide in 2013. The amount of routers’ consumption was approximately 50 million units in China in that year. Meanwhile, the consumption of smart phones and pads worldwide, reached the number of 1 billion and 217 million respectively, and in China 318 million and 23 million respectively.

In the light of different applications, according to Wang (2008) and Yang (2014), Wi-Fi networks can generally be divided in four different areas: personal Wi-Fi, family Wi-Fi, commercial Wi-Fi and public Wi-Fi. Personal Wi-Fi generally provides Wi-Fi service for individual users, who usually use the existing terminal equipment as a carrier, such as generating a small range of Wi-Fi hotspots. Family Wi-Fi generally refers to the wireless router in a home, providing wireless signal to
family members to get connected to an operator’s network. The family Wi-Fi is based on the rapid growth of IEEE standard 802.11 -a / -b / -g / -n Wi-Fi Access Points (Li, 2010). Commercial Wi-Fi means for business customers, providing customers service that include hardware, software, services and other content systems solutions. Public Wi-Fi refers to government-led and the enterprises-led Wi-Fi networks in wireless city construction possible to use by the public (Wang, 2008).

According to the statistical analysis, the main applications of Wi-Fi networks are in families and public contexts. From the statistics of public Wi-Fi hotspots in China, more than six million Wi-Fi access points could be found for public use (ABI Research, 2014); there are also various kinds of wireless routers in the ordinary household, which provide a convenient and efficient home wireless network (Li, 2010).

1.1.3 Wi-Fi Security Issues

Based on the above information, Wi-Fi has been playing an increasingly important role in our day-to-day life. Even though it brings us many benefits, it also creates some serious problems as well (Chenoweth, et al., 2010). A conspicuous one is the security issues, to which this situation has triggered intense attention. In July 2014, a group of pictures reprinted rapidly in various forums in China, illustrates a girl standing in front of a McDonald restaurant, holding a card that says “I lost 2000 yuan when I did the online shopping by the use of free Wi-Fi. Pay attention to it!” Consequently, China Central Television (CCTV) reported this news by the name of “Dangerous Wi-Fi”. This event makes more and more people becoming aware of the seriousness about Wi-Fi security (China Central Television, 2014). The reveal of personal information seems too many, not quite important, but the problems that come with it, for instance, the personal account reveal, online banking account and passwords stolen are more serious. Searching the key words “Wi-Fi security” on Baidu Search Engine (the biggest search engine in China), renders more than millions of results.

Compared to other countries’ public Wi-Fi, the easy connection that operate without encryption in China, not only provide convenience to the public, but also bring out the security issues. The aim is to provide an easy-to-use form, most of the public areas and merchants provide free Wi-Fi for citizens and customers without passwords (51CTO, 2014). This phenomenon leads to a serious safe problem, provides a chance for attackers to build up fake Wi-Fi networks or steal people’s personal information through encrypted networks (Li, 2010).

For the family Wi-Fi, the router is one of the most important parts to build up the wireless network at home. In China, most of the family routers have the same initial password for the configuration management, and are without password or user-defined passwords for the connection to the Internet (Jian, 2011). People need to choose the encryption mechanism for the routers, but the operation of routers is quite difficult and have numbers of options to set up (Bernard & Litchko, 2008).

1.2 Research Overview

The previous research about wireless networks includes different types, such as the application, development and the security mechanism of wireless networks. This paper focus on the 802.11 standard WLAN networks, but because of the less researches of these topic, the
literature review are based on the wireless network security aspect, the previous researches are:

Different types of wireless networks have their own characteristics; the different structures cause different threats of data security. Karygiannis & Owens (2002) focus on wireless networks security, especially the 802.11, Bluetooth and handheld devices, they talk about different applications of wireless local networks (WLANs) and wireless personal area networks (WPANs), and they analyse the mechanisms and security of specific wireless networks. Regarding different types of security threats, Sehgal & Kumar (2009) give and analyse about some common vulnerability of attacks to wireless networks.

Ren (2012) compares wired networks security, focusing on the difference between wired and wireless networks, gives a general research methods for solving security problems in wireless networks, points out what kinds of security threats could emerge in wired and wireless networks, compares the difference of security mechanisms between them and give some advice to solve the technological problems in security, but without the specific analysis about different types of the threats that appear in wireless networks.

Wireless security threat taxonomy (Welch D. & Lathrop S., 2003) and the solution of security issues (Li, Yuan; Wang, Yanhong; Zhang, Yuewei; GU, Weiwei, 2007) shows a classification of security threats. As for the wireless LANs using radio waves to transmit data through the air, so that all the users within the coverage area of the transmitter can get access to these data, at the same time, it means that the idea of only transmitting the data to one target recipient cannot be realized. Firewalls cannot act on a network of communication via radio waves. Everyone could intercept and insert data, deliberately steal personal information or business secrets, or destruct data in the coverage area.

In an overview of wireless sensor networks, Cui, Ju, Miao, Li, Liu and Zhao (2005) describes the basic conception of sensor networks and the hardware platform of them. They discuss the details about some important research areas, including data link layer protocol, network layer routing protocol, power management and network simulation tools. The article written by Singh (2011) reports a survey on network security, talk about the problems in technology that might happen, but do not give specific examples to show which different threats that can appear or the measures to solve them. They introduce different threats to sensors and routers. The attack-defence mechanism for wireless sensor networks (WSN) which talk about data security in the area of wireless sensor technology.

Deng (2002) talked about routing security in wireless ad hoc networks involve some argument about the physical platforms which could strengthen the safe of wireless networks.

For the public Wi-Fi network, Chenoweth, Minch and Tabor (2010) observe users’ behaviour of using firewalls or TCP ports when surfing at public networks. This study directly investigates how well wireless users are securing their computers and the threat level associated with wireless networks by using Nmap scans the users who used campus Wi-Fi, test whether they are using a firewall or not.

According to the literature referred to above, most articles and research focus on the arithmetic and security mechanisms, less of them talk about use habits and users’ behaviours that can lead to security issues.
1.3 Problem Discussion

Concluding the information from the previous sections, the Wi-Fi technique as an extension of the wired network, applied to various fields (Xu, 2012). Wi-Fi networks have been showing a significant growth in recent years due to its cheaper price, greater coverage and it’s attractive flexibility. Another salient feature is the mobility that supports the users not only “anytime anywhere” network access, but also the freedom of roaming while networking (Hasib, 2009).

However, among the security issues of wireless networks the major concern still remaining is that the Wi-Fi networks are susceptible to many forms of attacks as the interception of data in transit and eavesdropping on conversations are possible for anyone with access to the network (Karygiannis & Owens, 2002). Therefore, the widely use of Wi-Fi technique, not only provides a convenient tool in people’s life, but also includes many security threats.

As the news and events have shown before, a number of people involve into the hole of leaking personal information or financial loss, these security issues return to the focus of attention in public view. On the other hand, the current research are focus more on the technical parts, such as how to improve the encryption methods or hardware devices, while not any research investigates the practical use condition of the Wi-Fi networks. Meanwhile, because of the development of technology as well as the influence of economic factors, the security mechanisms of Wi-Fi technique is changing and is updated day by day (Ren, 2012), while the security issues when using Wi-Fi networks do not take a turn for the better, but become even more violent in China.

Furthermore, according to a combined research by Kaspersky Lab and B2B International (2014), the result shows that “Female Internet users are less concerned about how to protect themselves against online threats than males.” Therefore, does this situation also happen when users connect to Wi-Fi networks and does gender differences in use influence Wi-Fi network security?

1.4 Research Purpose and Question

An interesting question is: in spite of the high development of encryption techniques and mechanisms, the security situation and of Wi-Fi networks has not improved in China. Besides, as the survey done by Kaspersky Lab and B2B International (2014) shows, comparing male and female usage habits, females are easier involved in cyber threats, but this survey was not done in China, and the research was aimed at online Internet users, not specifically at Wi-Fi networks users.

Therefore, focusing on these points, one research interest here is: whether we should attention to the technical aspects, but also focus on the users’ point of view? That is whether users have a sufficient knowledge about Wi-Fi networks, and whether that is influenced by gender?

The insecure nature of wireless networks in general and public hotspots is particularly problematic given the rapid increased. One of the reasons is the public’s trust that information being electronically transferred is reasonably secure (Schmidt & Townsend, 2003). The blind trust of Wi-Fi networks, could also lead to security problems. Therefore, users’ trust level and awareness are also key points of this research.
The purpose of this study is to investigate the relationship between gender and Wi-Fi network security by investigating Wi-Fi usage in China. Theory will be analysed situations that could lead to security issues, and gender difference will be investigated theoretically and empirically about usage of Wi-Fi networks (Wi-Fi connection, security awareness, router setting, etc.

According to the problems and purpose discussed before, the research question is:
How does gender difference influence Wi-Fi network security in China?

1.5 Target Groups
This thesis covers specific details about male and female users’ behaviour when using Wi-Fi networks. The target groups are varied and could include to the following:

Researchers who are interested in: relationship between users’ behaviours and wireless network security.

Families who want to build up a wireless network in their home. This thesis points out some matters, that people need to pay attention to when they install a home Wi-Fi network.

People in general who usually use Wi-Fi networks to surf the internet. Some advice will be given about what normal users could do to make their information safer when they connect with the Wi-Fi to surf the internet.

Enterprises that plan to set up an official Wi-Fi network. Some advices given to chief information officers or system managers to build up safe Wi-Fi networks in office, as well as what problems they should pay attention on.

Engineers design wireless sensors or routers. The thesis points out some designs of routers that are not suitable or user-friendly, which part they could modify and improve.

1.6 Limitations
The main limitations of this paper are that it only focuses on the users’ perspective, that is what could lead to personal information reveal when using Wi-Fi networks, and it does not involve computer technology such as improvement of the arithmetic or encryption standards to protect the Wi-Fi security. This means it is only of use to improve users’ awareness and the operation level to prevent loss at financial and protects information security in the process of using Wi-Fi networks.
2 Theoretical Framework

The theoretical framework is divided in two parts. The first aspect focuses on wireless networks, Wi-Fi, and Wi-Fi security issues, including Wi-Fi security shortage and factors that could lead to Wi-Fi security threats. The second part focuses on difference of gender in security awareness and learning for that. These two parts are combined to explore the relationship between gender and Wi-Fi network security.

2.1 Wireless Networks

With the wide development of wireless networks, there are various types of it as well as different application environments with different users, such as governments, enterprises, individuals, etc. The wireless technique have also been used in global environment systems or the space network (Boncella, 2002). These days generally classified in eight types: Wireless local area network (WLAN), Wireless personal area network (WPAN), Wireless metropolitan area network (WMAN), Wireless wide area network (WWAN), Wireless mesh network (WMN), Cellular network, Global area network (GAN), Space network. Among these types, wireless local area network (WLAN) is the main usage wireless network, which operates within a local area such as a building or other limited area, it is an extension of the wired networks, and the Wi-Fi networks (IEEE 802.11 Standards) is one of the standards of wireless local area networks (Comaniciu, 2005).

2.1.1 Wireless Access Points (AP)

AP is the abbreviation of wireless access points, which is equivalent to a bridge between a wired network and a wireless network, its main role is to connect each wireless network client together, thereafter access them into Ethernet (Franceschetti & Stornelli, 2006). Wireless access points are increasingly becoming the entry points to the Internet (Potter, 2006), with the increasing connectivity options and security concerns (Chenoweth, et al., 2010). Attending to the public Wi-Fi, the particularly significant access points, commonly known as hotspots, which are often located in heavily populated areas such as airports, coffee shops, and hotels, are appealing to both business and casual users, but offer little or no security (Oliva, 2004). IEEE 802.11 wireless networks operate in one of two modes: ad-hoc mode or infrastructure mode (Li, 2010). The former mode, “ad-hoc”, is a cooperation of a series of independent wireless nodes and terminal devices. This mode is not dependent on the constant infrastructures and the distributed multi-hop network management, which is a self-created, self-organizing as well as self-managed network, such as Bluetooth technique (Jing, 2002). The later one includes a constant and wired base stations, access points (AP) and gateways, nodes transmission and reception the information to the base station when it is within the communication range, for example, the office wireless local area networks (Wang, 2008).

2.1.2 Basic Service Set (BSS)

The architecture of wired networks, WLANs, is built from stations and an access point (AP). The basic structure of a WLAN is the Basic Service Set (BSS). A BSS may either be an independent BSS or an infrastructure BSS. In an independent BSS, the stations communicate with one another directly if they are within range of each other. These sometimes referred to ad hoc networks and generally last for a short time. These ad hoc WLANs are typical used for meetings and allow the participants to share data with one another. To participate in an ad hoc
WLAN, the participants place the wireless network interface card (WNIC) of their devices into "ad hoc" mode. This mode allows a station to establish a connection with any other station in its proximity. An infrastructure BSS requires the use of an Access Point (AP) (Boncella, 2002).

2.1.3 Virtual Private Network (VPN)
A virtual private network (VPN) is a secure way of transporting private data across unknown networks. A VPN connection begins with the remote participant communicating with a corporate border device and agreeing that each recognizes the other, based on previously exchanged information. This can be in the form of a password, the IP address of either party, or an SSL certificate. Then, the two ends of the VPN link (the tunnel) agree on a means of encrypting their further conversation (Cassidy, 2015). Therefore, one conclusion could be that not using VPN Internet access could lead to Wi-Fi security issues.

2.1.4 Browsers
Compared with the wired network, there are more challenges about protecting personal information in the use of wireless networks. Therefore, it is much better for users to install some security software for laptops, pads and smartphones when using a non-encrypted Wi-Fi or unknown Wi-Fi in public places (He, 2012). For the browser software which much easier reveals users’ information, it is not only necessary to download the software from official websites, but also to develop a habit to upgrade the software regularly.

For example, some of the browsers have an automatic function to alert users that the Wi-Fi hotspots are without a password (Chenoweth, et al., 2010) and to alert them to disconnect the connection. This function undoubtedly has a practical effect for the users to avoid falling into phishing hotspots (Chenoweth, et al., 2010).

A large number of people for convenience, record the password when they surf the internet, but actually it is quite unsafe. When using browser login options, and you enter to the account by username and password, there is an option “whether to remember the password or not”, it is much better not to choose to remember it. Because the storage function of “remember the password sends the user’s account information to the browser’s cache folder, and then hackers could easily steal the personal information.

2.2 Wi-Fi Network (802.11 Standard WLAN)
2.2.1 Advantages of Wi-Fi
Wi-Fi is a brand certification from Wi-Fi Alliance, which certificate wireless local area network (WLAN) equipment that in line with IEEE (Institute of Electrical and Electronic Engineers) standard 802.11, it also used as synonymous terms IEEE802.11 protocol (Li, 2010). The biggest advantage of Wi-Fi networks is the high speed transmission, the long effective distance as well as it compatible with a variety of existing 802.11 DSSS (Direct Sequence Spread Spectrum) equipment. Wi-Fi is a series network protocol based on the 802.11. The first version was published in 1997, including the definition of media access control layer (MAC layer) and physical layer. After that, the widely used in different periods are a/b/g/n four standards (Wang, 2008). There are some following characteristics of Wi-Fi technology (Li, 2010):
• High speed of transmission, after the 802.11n protocol, speed could reach 300-600 Mbps.
• A wide range of radio coverage. The coverage radius of Bluetooth based technique is approximately 15 meters, while the coverage radius of Wi-Fi could reach 100 meters.
• Low cost without laying a large number of lines, while realizing network coverage through setting a certain number of hotspots.
• Low power, with a relatively good safe.

The follow graph (figure 3) shows the release date, bandwidth and maximum transmission speed of protocol group parameters in 802.11 (ABI Research, 2014).

Figure 3 802.11 Protocol Group Parameters

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Release Date</th>
<th>Bandwidth</th>
<th>Max Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>1997</td>
<td>2.4GHz</td>
<td>2Mbps</td>
</tr>
<tr>
<td>802.11a</td>
<td>1999</td>
<td>5GHz</td>
<td>54Mbps</td>
</tr>
<tr>
<td>802.11b</td>
<td>1999</td>
<td>2.4GHz</td>
<td>11Mbps</td>
</tr>
<tr>
<td>802.11g</td>
<td>2003</td>
<td>2.4GHz</td>
<td>54Mbps</td>
</tr>
<tr>
<td>802.11n</td>
<td>2009</td>
<td>2.4GHz/5GHz</td>
<td>600Mbps</td>
</tr>
<tr>
<td>802.11ac</td>
<td>2011.11 (Draft)</td>
<td>2.4GHz/5GHz</td>
<td>867Mbps</td>
</tr>
<tr>
<td>802.11ad</td>
<td>2012.12 (Draft)</td>
<td>60GHz</td>
<td>7000MHz</td>
</tr>
</tbody>
</table>

### 2.2.2 Public Wi-Fi Hotspot

Until 2014, the whole number of public Wi-Fi hotspots could be consulted by the Wi-Fi statistic website (http://www.Wi-Fiwlan.com/) (WI-FI Statistic, 2014) in China, there are more than 6 million. Of which there are more than 4 million hotspots of CMCC; ChinaNet hotspots over than 1 million, as well as the number of McDonald's, Starbucks, KFC, hotels, restaurants, and other businesses and subway public Wi-Fi hotspots build up by Government account for 1 million.

Table 1 Number of Wi-Fi Hotspots in China

<table>
<thead>
<tr>
<th>Name of Wi-Fi Hotspots</th>
<th>Number of Wi-Fi Hotspots</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMCC</td>
<td>4.22 million</td>
</tr>
<tr>
<td>ChinaNet</td>
<td>1 million</td>
</tr>
<tr>
<td>Commercial Public Wi-Fi (Restaurant, Hotels, Signpost, etc.)</td>
<td>1 million</td>
</tr>
<tr>
<td>Government Public Wi-Fi (Subway, Bus, Airport, etc.)</td>
<td>More than 0.18 million</td>
</tr>
</tbody>
</table>

Table 2 Number of Trouble Hotspots in Different Aspects

<table>
<thead>
<tr>
<th>Sampling</th>
<th>The Number of Wi-Fi are in Risks</th>
<th>ARP Attack</th>
<th>Fake Wi-Fi Hotspots</th>
<th>Unsafety Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>80000</td>
<td>17386</td>
<td>542</td>
<td>8</td>
<td>17203</td>
</tr>
</tbody>
</table>
In the 2014 sampling security survey of Cheetah Wi-Fi Company, it used 80000 public Wi-Fi hotspots as the sampling, and the result shows that there are 17386 free public hotspots at risks, accounting for 21 percent of all free public Wi-Fi hotspots in survey.

2.2.3 Average Internet Speed
The three communication companies in China publish the average internet speed of download and upload. From the statistic data, the average internet speed of download and upload of China Mobile Company are 2.95Mb/s and 3.12Mb/s respectively; the average speed of China Unicom Company are 2.71Mb/s and 2.35Mb/s respectively; the download and upload speed of China Telecom Company are 3.38Mb/s and 2.65Mb/s respectively.

<table>
<thead>
<tr>
<th>Company</th>
<th>Average Internet Speed</th>
<th>Download</th>
<th>Upload</th>
</tr>
</thead>
<tbody>
<tr>
<td>China Mobile Company</td>
<td>2.95Mb/s</td>
<td>3.12Mb/s</td>
<td></td>
</tr>
<tr>
<td>China Unicom Company</td>
<td>2.71Mb/s</td>
<td>2.35Mb/s</td>
<td></td>
</tr>
<tr>
<td>China Telecom Company</td>
<td>3.38Mb/s</td>
<td>2.65Mb/s</td>
<td></td>
</tr>
</tbody>
</table>

2.2.4 Wi-Fi Application Environments
According to previous literatures (Wang, 2008) & (Potter, 2006), Wi-Fi has penetrated into many aspects of the user’s life. Following context shown some specific application environments:
- Commercial areas: shopping malls, supermarkets, commercial streets, etc.
- Recreation areas: cafe, hotel, guesthouse, etc.
- Banks, hospitals, government agencies, etc.
- School areas: campus, dormitories, building, etc.
- Transport hub: airports, railway stations, bus stations, etc.
- Individuals: home, flat, apartment, etc.

2.3 Wireless Network Security

2.3.1 Wireless network security requirements
With the development and application of information technology, information security thought as that under the established security conditions, the ability of systems to withstand accidents or malicious acts, those events would endanger the data security among the procedure of data storage, processing and transmission as well as the natures of the systems (Feng & Xu, 2010). The below content illustrate the different qualities:

(1) Availability: although there may occur some emergencies, such as power interruption, natural disasters, accidents or attacks, user could gain and use the data, and the services are in normal operation state.

(2) Confidentiality: protect data against illegal interception and unauthorized browsing, which is important in sensitive data transmission procedure, meanwhile, it is necessary when handle the user’s private information in a telecommunication network.
(3) Integrity: ensure the data that be transmitted, received and storage are integral and has not be tamper. This is a key to guarantee the data accuracy.
(4) Non-repudiation: to guarantee the doer cannot deny the behaviour after processing data, such as information generation, issuance, acceptance etc. that could prevent the part of the particular communication exchange denied the fact after it.
(5) Authenticity: to guarantee the authenticity of entities’ (for example, people, process or system) identity, information or information source.
(6) Controllability: ensure the authentication, monitoring and management of information and information systems.

2.3.2 Wi-Fi network security

2.3.2.1 Wi-Fi Security Defect
Basic on the architecture and mechanism of Wi-Fi network, given the nature of it, there are a number of security defect currently existed, which were easy to attack (Boncella, 2002). According to the previous researches, there are following some specific defect in wireless local area networks.
- Insertion Attack: An insertion attack occurs when an unauthorized wireless client joins a BSS with the intent of accessing the distribution system associated with the ESS that contains the BSS.
- Interception and Unauthorized Monitoring: A wireless client may join a BSS with the intent of eavesdropping on members of the BSS.
- Denial of Service (DOS): Denial of service attacks can be carried out against WLAN by signal jamming. Since the signals are broadcast, it is a somewhat simple matter to jam them.
- Client-to-Client Attacks: Traditional DOS attacks can be carried out against WLAN by duplicating MAC or IP addresses. The usual TCP/IP service attacks can be carried out against wireless client providing these services (e.g., SNMP, SMTP, FTP).
- Brute Force Attacks against AP Passwords: Access to an AP is restricted by means of a password type scheme. This scheme can be compromised by password dictionary attacks.
- Encryption Attacks: The packets transmitted from a client to an AP can be encrypted by means of the WEP protocol. This protocol is easily compromised.
- Misconfigurations: Most APs ship in an unsecured configuration. The person installing the AP may use the default or factory settings for the AP.

2.3.2.2 Wi-Fi Security Mechanism
As the increasing usage of Wi-Fi, computer and network security is consuming a growth amount of time and resources for individuals and organizations (Chenoweth, et al., 2010), surveys have determined that approximately sixty percent of the wireless networks use no form of encryption (Housley, 2003), and that even the encryption is enabled, there are approximately seventy-five percent of them are using wired equivalent privacy (WEP), which has several well-documented security deficiencies (Potter, 2006). Furthermore, the 802.11 standards committee left many difficult security issues, such as key management and a robust authentication mechanism as open problems (Arbaugh, et al., 2001).
Hidden SSID:
The first and used for a long time way is hiding the SSID. SSID is “Service Set Identifier” (Li, 2010). In order to allow the wireless clients to identify different wireless networks. The parameter broadcast by wireless access point, the client only get this parameter or setting the same access point by hand. If we stop the broadcast, the normal people cannot connect with the network without find out the SSID. However, it should be noticed that if a hacker use other measures to obtain the appropriate parameters, it still could access to the destination network. Therefore, hiding SSID is only suitable to general home office environments.

MAC addresses filtering:
Another way is MAC address filtering, as the name suggests, this approach is input the specified MAC address or physical address of the wireless network interface card into the AP. The AP will make judgments about the getting data package, only transmit the data if it accord with the selection criteria. Otherwise, it will be discarded. There also some trouble with this method, it much complex and cannot support a large number of the clients. In addition, if the hacker steals the legitimate MAC address information, it still can login the network by counterfeit MAC address through several ways. Same to hiding the SSID, it only suit for the small office or home office environments (Li, 2010).

WEP encryption:
WEP is the abbreviation of Wired Equivalent Privacy, which uses the 64-bit or 128-bit RC4 encryption, could ensure the transmission data cannot interception in plaintext (Franceschetti & Stornelli, 2006). The mobile terminal and AP could configure four different WEP keys, which take turns to use it when transfer the encrypted data. It allows to dynamically changing of the encryption key. However, due to the key can only be the one of the four groups, so that, actually it is still the static WEP encryption. In addition, AP and all mobile terminals that connect with it are use the same encryption key, all the users who use the same AP also use the same encryption key. Therefore, it lead to the problem that once one of the user reveal the encryption key, all the users’ encryption key are revealing.

WPA/WPA2:
So far the safest way to encryption the wireless network is WPA2, provide data protection when users access to the internet by the manner authorized. Under this security mechanism, the unauthorized users cannot access to the data resources. WPA encrypts by use Temporal Key Integrity Protocol (TKIP) and RC4 arithmetic. Under this security mechanism, the unauthorized users cannot access to the data resources. WPA use the IEEE standard 802.1x access control, each user have their own encryption key, and could update the secret key to ensure the security. WPA2 compatible WPA, and support to AES (Advanced Encryption Standard), is the safest encryption method these days. Among all the security mechanism, it is much safer to use the WPA2 as the encryption approach for your home Wi-Fi (Li, 2010).

There are the advantages and disadvantages of the four basic security mechanisms (Boncella, 2002).

- Hidden SSID: stop the broadcast, other could not find the Wi-Fi hotspot signal, and connect with it. Easy to decryption, only suit to the some application environments.
- MAC addresses filtering: use particular physical address, screen the correct data to transfer. Easy to decryption, only suit for the simple environments.
• WEP encryption: use RC4 arithmetic. Dynamically change of the four secret keys. Actually is static encryption, once one of the secret key revealing, all the secret keys revealing.
• WPA/WPA2: TKIP, RC4, AES encryption, the safest mechanism currently.

2.3.3 Virtual Router
Virtual Router is a free, open source software based router for PCs running Windows 8, Windows 7 or Windows Server 2008 R2. Using Virtual Router, users can wirelessly share any internet connection (Wi-Fi, LAN, Cable Modem, Dial-up, Cellular, etc.) with any Wi-Fi device (Laptop, Smart Phone, iPod Touch, iPhone, Android Phone, Zune, Netbook, wireless printer, etc.) These devices connect to Virtual Router just like any other access point, and the connection is completely secured using WPA2 (the most secure wireless encryption.) (CodePlex, 2013). It also could choose different connection ways, for instance, unencrypted, WEP, WPA or WPA2. For the trail that will use the unencrypted way to create the wireless signal, which pretend to the public Wi-Fi.

2.4 Typicality Wi-Fi Security Traps

2.4.1 Wi-Fi Phishing
Many merchants offer a Wi-Fi service for guests in order to attract customers these days. Generally, customers need to ask for the password to access the Internet. These situations not only provide a convenient for customers, but also give hackers opportunity to attack by building the phishing sites (China News Service, 2015). Use the phishing sites is the lowest cost, but most damaging way to form the black chain, that is the reason why hackers like use this way to attack, there are three main aspects of the risks that suffer by “Darknet” (China Central Television, 2014):
• It forced to visit a phishing site, leading to the private accounts or personal information disclosure.
• The process of surfer the internet be monitored, history or other information be peeped.
• Hijacking the communication transmission by ARP attacks, leading to the accounts be stolen, such as, use other's Facebook account release the information.

2.4.2 Fake Public Wi-Fi Hotspots
Hackers can set up fake Wi-Fi hotspots in public places to access your information, e-mails and passwords without your knowledge. When you’re in a public place that offers Wi-Fi you may notice multiple networks available to join (KoolSpan, 2014). Let’s say that you’re at Starbucks and see “Starbucks” and “Free_ Starbucks” networks and automatically think, ‘I want the free Wi-Fi’. This network may be an ad hoc spot, a Wi-Fi hotspot set up in a public place used to steal transmitted data. If you are banking online or sending work e-mails from this fake hotspot, a hacker can see and steal your information (KoolSpan, 2014).

Besties pretend to the real public Wi-Fi hotspots, hackers could also build up a same name hotspot with the public one through use blank symbols which users could not conscious (China News Service, 2015).

For ordinary internet users, it is not easy to identify the safe Wi-Fi and risk Wi-Fi (He, 2012). The Wi-Fi hotspots constructed by attackers are more attractive, such as the name with the
suffix “Free”, are much attract people to connect. The public Wi-Fi established by government or mobile Companies are much safe, but it usually need verified by mobile phone number or other process. Therefore, the free Wi-Fi without passwords or verify are much attractive, while it always build up by the attackers (China News Service, 2015). Table 4 shows a name list of the public Wi-Fi, only one of them are the real public Wi-Fi. However, there are only several people could identify that.

As this table shows, there are 15 public Wi-Fi hotspots, all of them seems like the real public Wi-Fi, while there are only one real name of Wi-Fi among all these hotspots, it is “CMCC”. Therefore, it is hard for ordinary people to choose the real one to access in.

Table 4 Example of Fake Public Wi-Fi

<table>
<thead>
<tr>
<th>First Group</th>
<th>Second Group</th>
<th>Third Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cmcc</td>
<td>China Net</td>
<td>McDonal-OC</td>
</tr>
<tr>
<td>CMCC</td>
<td>CHINANET</td>
<td>McDonal-UC</td>
</tr>
<tr>
<td>CMCC-FREE</td>
<td>chinanet</td>
<td>McDonal-oc</td>
</tr>
<tr>
<td>CMCC1</td>
<td>ChinaNet</td>
<td>McDonal-uc</td>
</tr>
<tr>
<td>Cmcc</td>
<td>China-Net</td>
<td>mcdonald-oc</td>
</tr>
</tbody>
</table>

### 2.4.3 Attack Home Router

Pharming attacks are generally network-based intrusions where the ultimate goal is to redirect a victim’s web traffic to a hacker-controlled webserver, generally through a malicious modification of DNS settings (Mimoso, 2015)

The Wi-Fi networks is in dangerous because the DNS could easy tampered by hackers. DNS like a GPS for users when they surf the internet, once the coding of DNS be tampered, it means the speed of access the internet would be more slowly, the websites would force eject advertisements websites (Jian, 2011). Even the official websites of online banking would be tampered to the phishing websites, which means that people will reveal their personal information even lost their money.

Hijack home router generally in three steps: cracking password, control management background, modify DNS settings (Guan, 2014). After the DNS address modified by hackers, when users surf the internet, the browser tend to illegal websites, such as phishing websites, malicious advertisements, personal information revealing etc.

About the setting options of routers, the normal routers have two passwords, one for connection and one for background management. The management password need to setting through specific website which given by products companies. The initially password of management is setting by the company, which means it has same password with same products. If the management passwords cracked by hackers, it means the management background of router explore to hackers, they can modified the settings of Wi-Fi network, which lead a serious consequences.

The following graph (figure 4) shows the procedure of DNS hijacking (China News Service, 2015).
Security experts suggest that a password should include a mix of uppercase and lowercase letters and incorporate numerals and special characters. The more complex your password is, the more difficult it is to crack. As the first line of defense against internet attacks, it is important to use a different password for each of your sites (Brudno, 2013). Therefore, easy passwords of routers are easy to cause security issues when used with Wi-Fi networks.

### 2.5 Gender Difference in China

From an educational perspective, gender inequality is more pronounced in some aspects of the educational systems in China than in others (Jacobs, 1996). The education level of female students is lower than that of male students, while the situation has mixed evidence on improvements in gender inequality attainment over the past three decades (ZENG et al., 2014). Some authors state strongly that there is little gender inequality in education in China (Liu, 2004), while others conclude that there is considerable gender inequality in education in China (Davis et al., 2007). In China, gender differences in environmentally oriented behaviors, environmental knowledge, and general environmental concern (Xiao & Hong, 2010).

It is widely assumed that participation by females on the Internet is hampered by their attitudes towards computers, which in turn is reflective of their attitudes towards new technology. Research generally supports that female internet users have less experience with computers and are more likely than males to have negative attitudes towards computers. Although limited, research about users’ experiences and attitudes has found parallel gender differences, with females reporting lower levels of experience and more negative attitudes (Schumacher, 2001). Because of the different education level of female and male, the environment cognitive competence differences about Internet, compare with female, male might use Wi-Fi networks more safely.
3 Research method

The purpose of this chapter is to provide the reader with an understanding of the research approaches and the research method adopted in this paper work. This chapter explains the research perspective, strategies and methods, and describe why the methodology has been adopted, at the same time, the constraints associated with data collection and the limitations of the work will be discussed.

3.1 Research Approaches

3.1.1 Research Perspective

The fundamental step that researchers should raise before conducting research is to figure out which philosophy the research will adopt (Saunders & Thornhill, 2007). There are two main orientations: positivism, which is often close to quantitative research while post positivism or interpretative often have a link with qualitative research (Merriam, 1998). Bryman & Bell (2012), means that quantitative research than contain elements of interpretative.

“Positivism is an epistemological position that advocates the application of the methods of the natural sciences to the study of social reality and beyond.” (Bryman & Bell, 2011). The core idea of positivism is that the external social world exists, and its properties should be measured through objective methods, rather than being inferred subjectively through sensation, reflection or intuition (Easterby-Smith. & Thorpe, 1991). Gill & Johnson’s advice is (1997): Use positivism as the research philosophy, assume the role of an objective analyst, make detached interpretations about data collected in a value-free manner and emphasize on a highly structured methodology to facilitate replication. Compared to positivism, hermeneutics is often associated with the term social constructionism, which is a critical of positivism and argues that we need rich insights into this complex world. The role of hermeneutics is to seek understanding of subjective reality, in order to be able to make sense of and understand it’s motives, actions and intentions (Saunders & Thornhill, 2007).

3.1.2 Research Strategies

Work on the project, need to study the selection of the most appropriate research strategy between deductive and inductive, and then understand the approach, which is to improve the efficiency of the basic of the research (Saunders & Thornhill, 2007).

Inductive research is approach aimed to explore the meaning of human attachment to events, which closely linked collect qualitative type of data, and in which theories are emerged from specific observation. In inductive methods, the researchers are perceived to be a part of the research process, and the findings do not have to be generalized, which is the more flexible approach to research structure to ensure provisions for changes during the research. (Saunders & Thornhill, 2007)

However, in deductive approach, the explicit expectations of a hypothesis are built base on general principle which based on science, and the movement is done from theory to data. In deductive methods of casual relationships between variables need to be explained and the collected data is mainly in quantitative type, the approach was highly structured, and researcher is independent from the research process, as well as the findings need to be selected of a sufficient size in order to be able to generalize research conclusions, in which are different with the inductive research. (Saunders & Thornhill, 2007)
3.1.3 Research Methods
Quantitative research is a distinctive research strategy, which “describe as entailing the collection of numerical data and as exhibiting a view of the relationship between theory and research as deductive.” which asks a specific, narrow question and collects numerical data from participants to answer the question (Bryman & Bell, 2011). It is a systematic empirical investigation of social phenomena via statistical, mathematical or computational techniques (Thomas, 2003).

- Quantitative data is any data that is in numerical form such as statistics, percentages, etc.
- The researcher analyse the data with the help of statistics.
- The researcher is hoping the numbers will yield an unbiased result that could be generalized to some larger population. (Saunders & Thornhill, 2007)

Qualitative research is a research strategy that asks broad questions and collects word data from participants. It usually emphasizes words rather than quantification in the collection and analysis of data (Bryman & Bell, 2011). The researcher looks for themes and describes the information in themes and patterns exclusive to the set of participants (Thomas, 2003).

Merriam (1998) says that in qualitative research, an important assumption has to be made, which is: meaning lies in people’s experiences and that this meaning is mediated through the investigator’s own perceptions.

In this paper, the quantitative method conducted the way to collect data, which make the results more precise; while, based on the data collected by questionnaire, there also some open questions which conducted qualitative research method to gain the answer form respondents. Therefore, the research methods chosen in this paper is a combination of quantitative and qualitative method.

3.1.4 Research Design
In order to build a basis for the collection and analysis of data and to constitute a decision about the priority being given to a range of dimensions of the research process, the research design is presented (Bryman and Bell, 2011). Referring to Dhawan (2010), research design is the conceptual structure of a research and it constitutes the blueprint for the collection, measurement and analysis of data. There are different types of research designs: experimental design, cross-sectional design or social survey design, longitudinal design, case study design, and comparative design (Bryman and Bell, 2011).

To answer the research question, the research procedure of this thesis divides into five steps. The first step of this research is a literature review about the Wi-Fi network security field which is a sort of deductive method. Next, conclude some of the factors could easy cause to Wi-Fi security threats. Third step is the questionnaire based on the factors, ask whether user have those usage situation or habits or not. The fourth step is analysing the results of the questionnaire according to the answer of female and male, which conducted by the mixed analysis method of quantitative and qualitative research. The final step is come up with the relationship between gender and Wi-Fi security, and gains the answer of research question. The following figure 5 illustrates the steps of this research.
3.2 Data collection

The data collection is an important part of the research, because of the analysis based on the collected data. The collected data can reflect the real situation, so it can prove the reliability of the research. In order to achieve the purpose of this paper, finding the answer of the research question, it is necessary to gather relevant data. According to Saunders (2007), the data could divide to primary data and secondary data. Primary data is aimed at the ongoing research. The collection of primary data takes more time and it may take several weeks or several months. While secondary data is not aim at the undergoing, research and it originally collected for other purposes. Usually, we can get these data easily and low cost. However, there are many disadvantages, such as it is not so reliable and relevant. The best way to increase the response rate whilst keeping survey costs down may be to combine data collection methods. (Addington-Hall, et al., 2007).

3.2.1 Primary and Second Hand Data

This paper has collected both primary data and second-hand data to answer the research question. According to the research methods, this paper adapted to a combination of qualitative and quantitative methods. Saunders (2007) also stated there is a variety of data collection methods could be employed: interviews, observation, and questionnaires, etc. The chosen method for data collection is according to the research purpose. Such as, if the researcher wants to know the general views may choose questionnaires while for depth investigation, interviews is the most useful method. Therefore, in order to collect the quantitative data, this study conducts the questionnaires as the method. While in the analysis parts it also involves with qualitative analysis. The secondary data collected by other researchers or collected by other organizations in the course of their studies, the resources include books, articles in journals, electronic database as well as the statistic data from the official statistic (Bryman & Bell, 2011).

The primary data include the statistic data collected by the questionnaire. The questionnaire in this thesis used ranking methods and choice questions. This study also used the secondary data to build the research overview and theory parts, which include scientific articles, independent surveys, books and previous research in relating areas. This study concerned to use literature, focus on the wireless networks relevant articles. The literature related research through scholar search engines such as Högskolan i Borås Search Engine Summon as well as Google Scholar. The keywords mainly used in this research:

### 3.2.2 Questionnaire

Questionnaire is when the researcher use a unified design of a series of questions and other prompts for the purpose of understand the situation or consult and gather the information from the respondents (Bryman & Bell, 2011).

The advantages of questionnaires:
- It can break through the constraints of time, over a wide range of survey conducted numerous investigations simultaneously.
- Facilitate the quantitative analysis for the results.
- Anonymity.
- Save human resources, time and fund.

In this research, use a questionnaire to investigate the research question is much more adaptable. As the background mentioned, when talk to the Wi-Fi security, there are two main aspects of the application: the public Wi-Fi security and home router security. These two parts also the main Wi-Fi security issues come from. However, because of the questionnaire are the tool to gain the answer between different genders, the data of questionnaire is more likely a description analysis, which adapts to the reciprocal analysis (Bryman & Bell, 2011): qualitative analysis of quantitative data.

**Questions setting:**
The insecure nature of wireless networks in public hotspots is especially problematic given the rapid increased. One of the reason lead to the issues is the public’s trust that the information being electronically transferred is reasonably secure (Schmidt & Townsend, 2003). Consequently, the questions about public Wi-Fi parts focus on the usage frequency, places, devices, connection ways, software, timing, trust level, security awareness, etc.

According to the theory of the router security, Bernard said: “Securing a router requires controlling physical access to the router, and also preventing unauthorized logical access to the router.” (Bernard & Litchko, 2008), logical access means logging on to the router's user interface with a name and password, which allows the users makes the changes to ensure the security of it. However, according to the introduction of the common router, there are approximately thirty setting options, therefore the questions are focused on the routers’ usage situations, encryption setting, passwords, etc.

The questions of the questionnaire include two aspects, the basic usage situation and specific questions in public Wi-Fi and home routers. The basic questions include age group, gender, connection devices, and usage frequency, usage timing, connection setting, connection place etc. in Wi-Fi network.

**Samples for questionnaire:** the web-based questionnaire aimed at Wi-Fi users in China. Put the questionnaire in the “SO JUMP” website, set the sample number at 200, the surveys stopped collected when it reaches to 200 questionnaires.
Platform of questionnaire: “SO JUMP” website, which is the biggest professional questionnaires, surveys website in China, it used social media and website advertisements attract people do the surveys. After doing the surveys, people could draw a lottery or raffle, which include telephone charge, money, make up products, etc. Therefore, this website gathering amount of people who could do the surveys. On the other hand, it has related links which could be distributed in social media.

3.3 Analysis of Collected Data

In this paper, the analysis of the questionnaire is a combination of quantitative and qualitative method. Because of the questionnaire could divide into five parts, some of the parts use the quantitative method to analyse, some of the parts are open questions which need to use qualitative analysis. For the quantitative parts, questions to gain the answer about different level used the SPSS to do the one-way ANOVA analysis, to verify the relationship of gender and specific factor. Other parts gain the “Yes or No” answers or the open questions’ answers, which much more use the description of the situation or phenomenon to do the analysis.

Analytic data is a check, sorting, transcription and found useful information processing, which has multiple aspects and methods, covering a variety of names in different technologies, different business, science and the social sciences (Bryman & Bell, 2011). Because of the questionnaire is made in China, so the entire context was in Chinese. Thereafter, translate the questionnaires and answers in English before analysis the collected data. Using statistical data given by SOJUMP, and used analysis software such as SPSS and Excel to analysis collected data. The discussed formulae that not presented because of that under the techniques, the necessary calculation procedure could easily carry out by using SPSS (Bryman & Bell, 2011).

Data initially obtained must be processed or organized for analysis. For instance, this may involve placing data into rows and columns in a table format for further analysis, such as within a spreadsheet or statistical software (O'Neil, 2014). However, as mentioned before, in order to gain the answer of the research question, use qualitative analysis of quantitative data. For this thesis, analyse questionnaire used tables, pie charts, column charts etc. to illustrate the data of the survey’s results.

3.4 Research credibility

It is important to address the credibility of the research findings when designed and conducted the research. This criterion helps readers to ensure the quality and correctness of the findings. Considering the credibility of the research, also reduce the possibility of getting wrong answers. Reducing the likelihood of getting the incorrect answer means that attention has to be paid to ‘reliability’ and ‘validity’ on research design (Saunders & Thornhill, 2007).

The reliability and validity are important criteria in establishing and assessing the quality of research for the quantitative researcher (Bryman & Bell, 2011). The reliability connected with the question whether or not the measure consisting with the concepts. If other researchers conduct the same study with the same measure, will they obtain the same results? If they have done it, that means, the measurement is reliable (Bryman & Bell, 2011). In order to reach the criteria of reliability, need to record the method in detail.
3.4.1 Reliability
It must be concerned that reliability is about the quality of the research method and procedures. It is emphasized that when other researchers make the same case by the same method and procedures, it was not a repeat of the results. The aim of reliability is to reduce the errors in the study (Yin, 2003).

According to Bryman and Emma (2011), the reliability of the study could evaluate through two facets: external reliability and internal reliability. External reliability refers to whether the study could duplicate. For the questionnaires, the criteria for the choice of the respondents, and the questionnaires questions described before. Therefore, other researchers can know the whole process and they can test the study. Internal reliability refers to the subjective judgments (Bryman & Bell, 2011). Different people have different understanding, such as the analysis of the content may have large subjective thoughts. For the questionnaires, the questions should avoid navigating respondents’ answers.

3.4.2 Validity
According to (Yin, 2003), the validity of the research could achieve through construct validity. The construct validity includes several criteria. One of it is to verify whether the method reaches the validity requirement, such as multiple source of evidence.

In the research process, in order to achieve a higher level of validity, it is necessary to use a multiple sources of evidence instead of the individual source of data. However, in this research, the collected data only come through questionnaires. Therefore, in order to enhance the validity, the questionnaire was tested carefully to avoid errors owing to misinterpretation or misunderstanding. It used the clear instructions and simple wording to ensure that the responses could be valid.
4 Empirical Findings
This chapter provides the results of the questionnaire, and the analysis of data that collected from the questionnaire. This questionnaire has 28 questions (see Appendix 1). Include segmentation of respondents, usage habits, Internet speed, security awareness and Wi-Fi connection situation, setting of routers, specific technical questions and open questions.

4.1 Respondents Segmentation
A total of 200 respondents filled out the questionnaire. Among them, all the respondents answer the question about their gender, and the respondents of female account for 62 percent (124 of 200), the percent of the male is 38 (76 of 200).

As for the age group of the respondents, the majority of them (91% or 182 of 200) are between 15 to 30 years old. People who in age group: 31 to 45 are accounted for 6 percent (12 people). The number of people age over 45 years old is 6 (3 percent).

Table 5 Segmentation of Respondents

<table>
<thead>
<tr>
<th>X/Y</th>
<th>&lt;15</th>
<th>15-30</th>
<th>31-45</th>
<th>&gt;45</th>
<th>Total number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Female</td>
<td>0</td>
<td>114</td>
<td>6</td>
<td>4</td>
<td>124</td>
</tr>
<tr>
<td>Male</td>
<td>0</td>
<td>68</td>
<td>6</td>
<td>2</td>
<td>76</td>
</tr>
</tbody>
</table>

4.2 Usage Habits
This part of questions (3 to 7) focus on the usage habits of respondents, from these questions could gain the answers from use place, timing, frequency, devices and the activities they conducted using Wi-Fi network.

4.2.1 Types of Wi-Fi Network for Internet Access
Figure 6 shows the types of Wi-Fi networks used by the respondents for access the Internet. This bar chart display the majority of the respondents (46%) use Wi-Fi at home, 23 percent of respondents use Wi-Fi in campus, 18% of them use Wi-Fi in office and 13% of respondents use the public Wi-Fi which provide by mobile company, such as CMCC from China Mobile Company.

Figure 6 Types of Wi-Fi Networks for Internet Access
4.2.2 Use Situations of Wi-Fi Networks

Figure 7 illustrates the connection time of respondents in Wi-Fi networks per day. Among all the options, selection of 4-8 hours was chosen by 84 respondents (42%), which account for the first place. The time spends less than 4 hours occupied the second place with a percentage of 36 (72 respondents). There are 10% of respondents spend 6 to 8 hours per day, and 22% of respondents spend more than 8 hours connect with the Wi-Fi network. There were no answer of the option “Never use it” in this question.

Figure 7 Time Spend on Wi-Fi Connection

![Bar Chart: Time Spend on Wi-Fi Connection]

Figure 8 Number of Devices in Wi-Fi Connection

![Bar Chart: The Number of Devices Connect with Wi-Fi Network]

Figure 8 shows the numbers of Wi-Fi connection devices of respondents. The percentage of 1-3 devices and 4-8 devices are similar, which are 48% and 45% respectively. The respondents who chose the option of 9 devices account for 7 percent, and there are no respondents chose 0 devices in this questionnaire.

Figure 9 illustrates the kinds of devices used by respondents to connect with Wi-Fi network. It is revealed that the majority of respondents “using laptop” (83%) and mobile phone (85%) for Internet access. The percentage of respondents use PC account for the third place with the number of 35%, and 30% of respondents use Pad to connect with Wi-Fi network. Only 10% of respondents use TV to access the Internet, and other 1 percent of people chose other ways to connect.
The following table 6 shows the activities of respondents, it illustrates the reasons of why users access to the Internet through use Wi-Fi network. The majority percentage of the activity is to use the social network software (86.5%), 58% of reason is to search and download information, and 49% of respondents play online games through Wi-Fi network. The option of “P2P download and online video viewing” account for the second place, with the number of 79%. For financial activities, the percentage is 37%, and 31.5% of check and answer email as well as other activities consumption 7% of respondents.

### Table 6 Activities of Users Conducted by Using Wi-Fi Network

<table>
<thead>
<tr>
<th>Activities of Users Conducted by Using Wi-Fi Network</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial transactions, like transfer payment or credit card payment</td>
<td>37%</td>
</tr>
<tr>
<td>Check and answer e-mails</td>
<td>31.5%</td>
</tr>
<tr>
<td>Search and download information</td>
<td>58%</td>
</tr>
<tr>
<td>Play on-line games</td>
<td>49%</td>
</tr>
<tr>
<td>Social networking, e.g. Weibo, WeChat</td>
<td>86.5%</td>
</tr>
<tr>
<td>P2P download and online video viewing</td>
<td>79%</td>
</tr>
<tr>
<td>Other activities</td>
<td>7%</td>
</tr>
</tbody>
</table>

#### 4.3 Internet Speed

According to the official data of the average internet speed in China (WI-FI Statistic, 2014), the download speed and upload speed are very slowly. Based on the statistic data, the question 8 to 11 are aim at the internet speed satisfaction and Wi-Fi networks rob.
The pie chart (figure 10) illustrates the satisfaction of Internet speed among all the respondents. More than half hundred percent of the respondents (51%) have a very dissatisfaction attitude about the internet speed. The option of “Dissatisfaction” is 24%. The smallest percentage is occupied by great satisfaction, which is 11 percent. The percentage of general satisfaction is quite similar to that of great satisfaction, which is 14%.

The figure 11 shows the thinking among the two hundred responders, the reasons of why the Internet speed is slowly. Among all the selections, the thinking of “operators shrinks the broadband speed” occupied the first place, which is 43%. Responders think the broadband is not enough for us, or it shrinking about the operator broadband package. Ranked the second place, the percentage of “P2P download and online video viewing” is 37. The reason “there are Wi-Fi squatters and computer virus or hacker’s attacks” are account for 9 per cent and 7 per cent respectively.

Aim at this phenomenon, the question “do you think there have Wi-Fi squatters used your Wi-Fi?” gives a view of respondents about what they think about the Wi-Fi squatter. There are 45% of respondents think their Wi-Fi networks were robbed by squatters, 22% of them think no Wi-Fi squatters, and 33% of respondents not sure about this situation.

The figure 12 shows the thinking of respondents about the reasons of why Wi-Fi networks robbed in the following pie chart. In this question, 35% of respondents think the Wi-Fi robbed because of the easy and simply password. 30% of people think the Wi-Fi password cracked by tools, and 15% of them believe it because of the router loophole attack. There are 10% of respondents have told others about the password before and 10% of respondents use Wi-Fi share software.
4.4 Connection of Wi-Fi Network

The questions about the connection of Wi-Fi networks focus on the connect approaches, and awareness of public Wi-Fi connection procedure. The following tables (7,8) shows the specific describe of the questions and answers.

Table 7 is a statistic which illustrates the use situation of automatic connection software among all the respondents. Looking through the answers of questionnaire, there are 54% of respondents use the automatic software to connect with the Wi-Fi network. 33% of them not use it and 13% of respondents don’t know about it.

Table 8 shows the percentage of respondents that whether thinking about the security issues like the authenticity of the Wi-Fi they will connect before they access the Internet. The result of this question shows that only 43% of respondents reflect on this situation, 37.5% of them not thinking whether the public Wi-Fi is true or not, and 19.5% of people never think about the security of public Wi-Fi.

### Table 7 Use Automatic Connection Software or Not

<table>
<thead>
<tr>
<th>Whether Use Automatic Connection Software or Not</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>54%</td>
</tr>
<tr>
<td>No</td>
<td>33%</td>
</tr>
<tr>
<td>Don't Know</td>
<td>13%</td>
</tr>
</tbody>
</table>

### Table 8 Distinguish the Real Public Wi-Fi before Use it

<table>
<thead>
<tr>
<th>Have Consicous to Distinguish Public Wi-Fi Before Connect</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>43%</td>
</tr>
<tr>
<td>No</td>
<td>37.5%</td>
</tr>
<tr>
<td>Never Think About It</td>
<td>19.5%</td>
</tr>
</tbody>
</table>

4.4.1 Ways to Access Internet

The question 14 and 15 ask the different ways of respondents about how to access Internet. Figure 13 shows the main way of respondents to access Internet at home or dormitory. Among all the respondents, 49% of them use ADSL virtual dial, and 41% of them use Dynamic IP (automatically obtain the IP address), 7% of respondents use Static IP (manually fill in the IP address), and other people choose other ways to access Internet.
### 4.4.2 VPN

This question asked whether or not they used VPN to access Internet when connect Wi-Fi network. The following table 9 shows the answers of respondents. Among them, only 11.5% of respondents use VPN to access Internet. The majority (53.5%) of respondents “Don’t know what VPN is”, and 35% of respondents not use VPN connect Wi-Fi network.

<table>
<thead>
<tr>
<th>Connect Wi-Fi Network through VPN</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>11.5%</td>
</tr>
<tr>
<td>No</td>
<td>35%</td>
</tr>
<tr>
<td>I Don’t know what VPN is</td>
<td>53.5%</td>
</tr>
</tbody>
</table>

#### Table 9 Connect Wi-Fi Networks through VPN

### 4.5 Home Router Setting

This part of the questionnaire asks about the router usage phenomenon. According to the result of questionnaire, the chart (figure 14) illustrates the number of each way that people installed their router. This question use the multi choice question, the percentage of respondents chooses “refer to the router instructions” is 57. That means the majority of people installed the router by following the instructions. However, there are 27% and 24% respectively that the ways of ask others for help and consult or search through the internet. There are 11% of respondents choose the option of “others”.

#### Figure 14 Ways of People Install the Router

### 4.5.1 Router Password

This section asks questions about settings of router password. According to the answer of question 17, There are even 52 percent (121 of 200) of responders do not know the routers have two password, one for normal connection and one for management control.

Table 10, 11 illustrate the different knowledge of Wi-Fi password among different gender and different age group. In the aspect of gender, 34 of male (total 76) don’t know the management password, 87 of female (total 124) don’t know the management password of router.

For the age group aspect, the respondents in age 15-30, 30-45 and over 45 years old, the percentage of not known two passwords are 60% (109 out of 182), 58.4% (7 out of 12) and 83.4% (5 out of 6) respectively.
Focus on the respondents (48%) who known about the management password, question 18 (only shows when respondents choose “Yes” in question 17) asks about whether they change the passwords or not and already finished settings of routers in management background, while only 32% (25 out of 79) of respondents choose “Yes”.

This statistic data means among all the respondents, only 12.5% (25 of 200) person already configured the settings of router from management control platform.

Based on question 19, the respondents who already configured the settings answer the question 20, about what kind of connection and management passwords they used. Among the 25 respondents, only 32% (8 of 25) people used complex passwords. This means among all the respondents of this questionnaire, only 4% of people used complex connection and management passwords and already configure settings for routers.

According to the previous question “reasons of Wi-Fi network robbed by others”, the option “use easy password” account for the majority place. In the following chart, figure 4-16 shows the different consists of the connection passwords used among all the responders. Among all the options of passwords, complex password occupied the smallest percentage (13% or 26 of 200). “Medium complex password” account for the majority of respond, with the number of 49% (98 out of 200). The number of respondents who choose “very easy” password such as “123123”, “abcdefg”, etc. account for the second place with 27 percent (54 of 200), and the respondents who not changed connection password and use the initial one with the number of 18% (36 of 200).

Figure 15 Content of Connection Password
When it comes to the habits of using the router (figure 4-11), more than 60 percent of the respondents choose to ignore it, and they let the router run day by day. For the setting options, 40 percent chose the option “didn’t do any settings before”. For other options, there are only a few respondents that have changed the settings before.

**Figure 16 Main Setting Options of Routers Operated by Responders.**

![The main setting options graph](image)

This graph (figure 16) shows the main options of the router in the management background, and the number shows how many people had operated it. As it is showing, there are 61 respondent used to setting the Wi-Fi options, such as change the username or connection password. 37 respondents are used to setting the internet environment. For other options, there are only a few respondents that have done some of the operations before, such as DNS setting, IP and MAC address binding etc.

**Figure 17 The Reasons Cannot Access to Internet (After Repaired).**

![The reasons that cannot access the internet](image)
Form the figure 17, there are three main reasons that lead to the equipment cannot access to the internet, they are installation or configuration errors, router problems and ADSL, cable effects. The number of them are 32 each, account for the main reasons of this question. And the figure 18 shows the router problems that appearance in the process of uses it.
5 Analysis and Discussion

In this chapter, analysis the collected data gathers from the questionnaire. Found the
difference factors influence between male and female. There are general four parts of the
factors: router setting, public Wi-Fi connection, usage habits and knowledge of the technique
question in Wi-Fi network.

5.1 Usage Habits

This part analyses different type use to access internet, spend timing on Wi-Fi connection, and
main activities of respondents, investigates different usage habits between male and female.

When being asked the difference types of Wi-Fi networks used for access the Internet. The
following table 12 shows the number of respondents in different ways to connect Wi-Fi
network, the percentage shows the proportion of choosing among different gender. The
majority of the respondents (46%) use Wi-Fi at home. Among all the female, 44.4% (55 of
124) of them use Wi-Fi at home, and among the male, 48.7% (37 of 76) use at home. The
proportion of use Wi-Fi at office is similar between male and female. While there are a
significant different between gender, among all the male respondents, only 9.2% (7 of 76) of
male use public Wi-Fi, but in female aspect, the 15.3% (19 of 124) of female use public Wi-Fi
to access Internet.

Table 12 Using Different Ways to Access Internet

<table>
<thead>
<tr>
<th></th>
<th>Home</th>
<th>Campus</th>
<th>Office</th>
<th>Public wifi</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>37</td>
<td>19</td>
<td>13</td>
<td>7</td>
<td>76</td>
</tr>
<tr>
<td>Female</td>
<td>55</td>
<td>27</td>
<td>23</td>
<td>19</td>
<td>124</td>
</tr>
<tr>
<td>Total</td>
<td>92</td>
<td>46</td>
<td>36</td>
<td>26</td>
<td>200</td>
</tr>
</tbody>
</table>

Ps: Following Percent Shows Proportion Among Different Gender

Follow context talk about the difference between male and female in Wi-Fi network
connection time. Among all the options, selection of 4-8 hours was chosen by 84 respondents
(42%), which account for the first place. From the data collected in questionnaire, female
average spend 1 to 3 hours in Wi-Fi connection per day, while male always use 4 to 8 hours.
For the option “spend more than nine hours per day”, approximately 11.8% (9 of 76) male
choose it while only 4% (5 of 124) of female spend much hours in Wi-Fi connection.
Therefore, from the questionnaire could gather the information, male respondents usually
spend more time than female on Wi-Fi network connection.

5.2 Router Setting

Before exam the router security risks, the first to do is to compare the complex router market
and complicated situation of operating experience. In fact, this situation has a direct impact on
the security of the router and wireless networks. Search from the internet, there are dozens of
traditional routers brands in China, such as TP-Link, D-Link, Tenda, Lei Branch etc. each
brand have a number of different models. Some brands’ on sale models are more than 50.
Each product even has several different firmware versions. Traditional router have a very high
operation threshold, there are more than 30 setting options in the router’s management
background.
Besides, the router have two important passwords, one is for the Wi-Fi connection, that the one we used when we access to the Wi-Fi hotspots. If the Wi-Fi connection password revealed, that means, everybody who knows the password and within the coverage of the Wi-Fi hotspots could rob the internet, seize the broadband resources, which lead the internet speed become slowly (Jian, 2011). Besides, another password is for the router configuration, use for log into the management background of the routers. The management password aimed at the setting options of internet account, DNS, access devices etc. If the management password reveal to others, people who will get the full administration permissions of the router (Bernard, R. & Litchko, J., 2008).

When the password reveal, hacker can random change the Wi-Fi password, even put the virus, distort the DNS, setting phishing websites as the main websites etc. which could bring a serious security threats (China News Service, 2015). The complex login process, different misunderstanding setting options are the main reasons that lead to the majority of users ignore the importance of the router’s management password.

As the different knowledge of Wi-Fi password among different gender, 34 of male (total 76) and 87 of female (total 124) don’t know the management password of router.

From this questionnaire, question 17 to 23 is about the router settings. Analysis the setting options of different gender, there are 70 percent of male respondents could not configure the options, and approximately 90 percent of female could not operate it (figure 19).

Figure 19 Percentage of People Cannot Configure Settings of Router.

Table 13 Number of Respondents Use Different Password in Different Gender (150 Respondents).

<table>
<thead>
<tr>
<th>Password</th>
<th>gender * Password Crosstabulation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Count</td>
</tr>
<tr>
<td>gender</td>
<td></td>
</tr>
<tr>
<td>male</td>
<td>12</td>
</tr>
<tr>
<td>female</td>
<td>19</td>
</tr>
<tr>
<td>Total</td>
<td>31</td>
</tr>
</tbody>
</table>

Table 13 shows the different gender use different level of passwords. Because of the number of respondents are different, in order to analysis in the right way, random extract 75 of males and 75 of females from all the respondents. As the table shows, the password usage situation is quite different between female and male among all respondents. The percent of male respondents using complex password is approximately 63%, but only 37% of female use it. And for the medium complex password, the percentage is similar, which are 53.7% and 46.3% respectively. While the percentage of using initial and very easy password among male is 44%, but female are account for 56%.

For the question 22, it is interested that no respondents think their password is “So dangerous” even there are 18% (36 of 200) of respondents use the initial password. The majority (72% or
89 out of 124) of the females think their password is safe. And general male respondents think their password is medium safe, even though the percentage of them used complex password are bigger than female.

As the theory part mentioned before, the password should include a mix of uppercase and lowercase letters and incorporate numerals and special characters. The much complex you password is, the much difficult to crack it (Brudno, 2013). In the aspect of router setting, more complex password has been used, more it safe of the Wi-Fi network connection. Therefore, under these factors, males are tend to use complex password and know much about how to configure the setting options of routers than females, which means male respondents are less likely to involve into Wi-Fi network security threats.

5.3 Public Wi-Fi Network

“Are there a free public Wi-Fi?” This seems like a sentence that people always said in daily life, in addition to the home and office, people often some needs to connect with the Wi-Fi for laptop, pad, smartphone and some other mobile devices in order to access the Internet outside. Due to the limited circumstances in mainland of China, the price of 3G/4G traffic is quite higher, that is the reason why people often choose the free public Wi-Fi access in public areas.

However, the public Wi-Fi are in risks, from the statistic data of Cheetah Wi-Fi Company (2014), there are more than 6 million public Wi-Fi hotspots in China, and in the sampling survey, more than 21 percent of the Wi-Fi hotspots are in risks. There are more than 1.2 million of hotspots in China have several security vulnerabilities (China Central Television, 2014). Therefore, not all the public Wi-Fi networks is safe when users connect it.

According to the sampling survey done in China (China Central Television, 2014), more than 70 percent people would access into the free public Wi-Fi when then travel, eat outside, and entertainments, but more than half of them do not know that there are security risks among these Wi-Fi hotspots. More than 30 percent of interviewees said that they encountered the advertisements forced eject, and 5 percent of people express that their accounts be stolen or lost money after connect with the free Wi-Fi (figure 20).

Figure 20 Security Vulnerability Proportion of Public Wi-Fi.

Using “Free” public Wi-Fi is much probability fall into a “Darknet” build by the hackers (He, 2012). Hackers build a Wi-Fi network with the name much similar to the public Wi-Fi, such as CMCC, ChinaNet or Starbucks, set up the Wi-Fi hotspots called CMCC-FREE, ChinaNet-Free or Starbucks01, and not need the login password which enticing users enter it. When the user carried out the operations under the “Darknets”, the whole procedure of data transmission could be monitored by the third-party. This means if you log into your private
account, the hacker could find the user login information in the data package, thereby steal user’s email password, e-commerce accounts and other information (Arbaugh, et al., 2001).

Therefore, the awareness of users when they connect public Wi-Fi is quite important. Looking through the answer of the questionnaire, there are 54% of respondents use the automatic software to connect to the public Wi-Fi network. 33% of them not use it and 13% of respondents don’t know whether they have it or not. The result of question 14, ask whether people have conscious about the public Wi-Fi they connect maybe the fake one. The answer shows that only 43% of respondents reflect on this situation. Among them, 37 percent of female and 52 percent of male mentioned it. Among all the respondents, 37.5% of them not thinking whether the public Wi-Fi is true or not, and 19.5% of people never think about the security of public Wi-Fi. Therefore, for the public Wi-Fi connection part, could found that male also have good awareness of the security issues than female.

5.4 Knowledge about the Wi-Fi Network Technique

VPN is a secure way of transporting private data across unknown networks (Cassidy, 2015). Table 14 gives a point of view that the knowledge of VPN was influence by gender. The percentage of “not use VPN” and “don’t know what VPN is” of female is 93.5% (116 out of 124), and the percentage of male is 80% (61 out of 76). Among all the respondents who use VPN access Internet, male account for the majority parts of 65% (15 of 23) and female account the proportion for 35% (8 of 23).

Table 14 Gender Knowledge of VPN Influence by

<table>
<thead>
<tr>
<th>Gender * VPN Crosstabulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
</tr>
<tr>
<td>Gender</td>
</tr>
<tr>
<td>female</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

Table 15 Different Chosen of the Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Very clearly about #1</th>
<th>Not very clearly about #2</th>
<th>Basic understood #3</th>
<th>Just heard about #4</th>
<th>Never heard it before #5</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP/ WPA/ WPA2</td>
<td>26</td>
<td>30</td>
<td>34</td>
<td>38</td>
<td>22</td>
</tr>
<tr>
<td>MAC Address</td>
<td>15</td>
<td>19</td>
<td>26</td>
<td>54</td>
<td>36</td>
</tr>
<tr>
<td>SSID Filtering</td>
<td>13</td>
<td>23</td>
<td>24</td>
<td>51</td>
<td>39</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>9</td>
<td>14</td>
<td>27</td>
<td>46</td>
<td>54</td>
</tr>
<tr>
<td>ARP Mapping</td>
<td>9</td>
<td>14</td>
<td>27</td>
<td>46</td>
<td>54</td>
</tr>
</tbody>
</table>

From the questionnaire, could gain the answer that the usage situation of VPN is not normal in both male and female, but male are still a little better than female in use VPN to access Internet.

The question 24 is a multiple question contained five specific parts in it. Each small question divided into five different understanding levels, from very “clearly about it” to “never heard
about it”. Because there are 124 female and 76 male, in order to do the one-way ANOVA, chose 75 female and 75 male as the same of the password related questions done. Table 15 shows the total answer about the questions, the number in the cells present the how many people chose it.

The values from one-way ANOVA could test whether gender have a significant influence about the specific related technique knowledge (Table 16, 17).

The P-value of WEP WPA/WPA2 is (=0.108), which is bigger than the 0.05, therefore, it means there is not a significant different between female and male about the knowledge of WEP, WPA/WPA2. While the mean of male (= 2.8267) is lower than female (=3.1733), which males are have more understanding about the WEP, WPA/WPA2.

The situation about MAC Address, SSID Filtering, DHCP Sever and ARP Mapping is same, all the P-value are bigger than 0.05, therefore, there not have any significant influence between gender and the knowledge of Wi-Fi related technique questions. However, as the table 17 shows, all the mean values of male are less than female. Therefore, gained the answer from this question, males know more about the professional technique knowledge about Wi-Fi network security than female.

Table 16 Mean Value of Different Gender

<table>
<thead>
<tr>
<th>gender</th>
<th>WEP</th>
<th>WPA/WPA2</th>
<th>MAC Address</th>
<th>SSID</th>
<th>DHCP</th>
<th>ARP MAPPING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>2.8267</td>
<td>3.3467</td>
<td>3.4000</td>
<td>3.7087</td>
<td>3.7087</td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td>3.1733</td>
<td>3.6400</td>
<td>3.6400</td>
<td>3.9200</td>
<td>3.9200</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>3.0000</td>
<td>3.4933</td>
<td>3.5200</td>
<td>3.8133</td>
<td>3.8133</td>
<td></td>
</tr>
</tbody>
</table>

Table 17 ANOVA of Relationship between Gender and Factors

<table>
<thead>
<tr>
<th>Source of Variance</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP</td>
<td>1</td>
<td>4,507</td>
<td>2,611</td>
<td>.108</td>
</tr>
<tr>
<td>MAC Address</td>
<td>1</td>
<td>3,227</td>
<td>1,988</td>
<td>.161</td>
</tr>
<tr>
<td>SSID</td>
<td>1</td>
<td>2,160</td>
<td>1,359</td>
<td>.246</td>
</tr>
<tr>
<td>DHCP</td>
<td>1</td>
<td>1,707</td>
<td>1,197</td>
<td>.276</td>
</tr>
<tr>
<td>ARP MAPPING</td>
<td>1</td>
<td>1,707</td>
<td>1,197</td>
<td>.276</td>
</tr>
</tbody>
</table>
5.5 Discussion

These paper focuses on the key factors that influence Wi-Fi network security by investigate the different between male and female. Found how does gender difference influences Wi-Fi network security through these key factors.

On the section of Wi-Fi networks usage situation, male respondents spend more time than female respondents, while both of their main activities is in the social network such as Weibo, WeChat, etc. In other aspects, female tend to online shopping and watching online video programs when connect Wi-Fi networks, while male respondent tend to games and download information through Wi-Fi network. From the theory part mentioned, people are easy to revealing their information in social networks (China News Service, 2015). “Hackers stolen identity information from social media sites” (Vacca, 2013). People use social network to interact with friends and associates through Wi-Fi networks, which not only changed the way to communicate, but also creates a high risk for security threats.

In the aspect of home Wi-Fi network, 30 percent of male respondents could configure the complex options of router, while only 10 percent of female done this. Also in the connection password setting, male tend to use complex password, and most of them have conscious that their password not safe enough. With the development of the encryption mechanism, decrypted technology also improved rapidly, there is no absolutely security of information, but use complex password mixed with letters, numbers and symbols could enhance the difficult to cracking. However, female respondents tend to use easy and medium complex password, but most of them consider their password is enough safe. This trend easy cause password revealing, especially the management password and the settings of routers, could easy modified by others.

Compare with male respondents, female account for a big proportion in use public Wi-Fi. However, only 37 percent of female users would check whether the public Wi-Fi hotspot is a fake one or not before they access. These days, people seek the Wi-Fi hotspots when they are in restaurants, coffee shops or shopping malls (He, 2012), but as the result shows, only a few people aware the dangerous of fake Wi-Fi, lowly awareness are easily lead to information securities (Chenoweth, et al., 2010). In this part, female respondents are easier face the security threats when they use public Wi-Fi networks.

Tend to the knowledge about the Wi-Fi networks related field; ask the understanding about professional technique in Wi-Fi security. Looking through the one-way analysis results, there not have a significant different between male and female in the understanding level of technique questions, but according to the mean values, male respondents always have a higher level than female.
6 Conclusion
This chapter gives a conclusion of the research. Answer the research question about how does gender difference influence the security of Wi-Fi network. Talk about the contribution in informatics field, the evaluation of the method and suggestion for further study.

6.1 Conclusion
Wi-Fi connection becomes to a very important part of people’s life, it seems the Wi-Fi networks are everywhere especially in China. Wi-Fi allows us to access the Internet wherever you want, which offer a convenient for us to maintain constant contact with family, friends and clients. However, with the cheap price, greater coverage and the attractive flexibility of Wi-Fi network, not only coming to the benefits of Wi-Fi network, but also to cause a series of security issues. According to China Internet Network Information Centre (CNNIC) statistic data, the number of female Internet users in China has a dramatically grown, from 41% in December 2013 to 47% in August 2014, and keep an increasing trend in 2015. Therefore, the research question in this paper is to investigate how does gender difference influence Wi-Fi network security. The answer of the research question is: Compare with male users, female users are easier to cause into Wi-Fi network security issues.

This answer concluded in three different aspects: usage habits of Wi-Fi network, security awareness, and knowledge about Wi-Fi network. In usage habits section, the female users tend to use easy password, connect unknown public Wi-Fi and leave the Wi-Fi routers in initial settings, these kinds of behaviours is easy lead to security issues like personal information revealing and financial loss, this also the reasons why amount of female users involve into Wi-Fi security events in China. Come to the security awareness, what interesting is that female users have more confident about their operation in Wi-Fi connection even though they have bad usage habits. Most of the female users in this research use easy and initially password but think it was enough safe. Therefore, in the aspect of security conscious, females not having a strong mind, which easily leads to faces security issues. In the understanding level of specific related knowledge of Wi-Fi networks, males are known much more than female, which means females more vulnerable to security threats because of the less understanding.

Combining the different sections, could easy conclude the result: compare with male, female are easy involve into Wi-Fi network security issues.

6.2 Contribution to the field of Informatics
The findings of this study give an answer about how gender different when access to Wi-Fi network, point out female users in Wi-Fi connection are easy to cause security issues.

Gives suggestions to female users, in order to avoid and resist security threat, improve security awareness and practical operate level is very important. Enterprises should give more concentrate on the female staffs in information security training. As well as a suggestion for router designers, the design of the routers could be more on usability, user-friendly and intelligent, because of the existing products have a higher threshold for users, that not easy to use it in a security way.
6.3 Method Evaluation
The research method in this study adapted to a combination of quantitative and qualitative methods, conducted a five steps research procedure which described in research method chapter. But there still some limitation of this research. Firstly, this study use questionnaire as the main research method, but because of the limitation of time and area, only 200 respondents answer this questionnaire, which cannot precisely present the Wi-Fi network usage situation in China. Secondly, among all respondents, there are 124 female respondents and 76 male respondents, because of the different number of them, some of the questions analysed through random sampling of the total 200 respondents, which leave 1 male respondent and 49 female respondents. Thirdly, the select of the key factors cannot cover all fields; there also other factors between gender and Wi-Fi network security, which could lead the answers different.

6.4 Suggestion for Further Research
Because of the limitation of choice, there is more factors influence Wi-Fi network security, thus, the further study can expand the factors lead information security in Wi-Fi network. In addition, future study cannot only focus on the gender but also age group or different areas or education level as the independent factors. Besides, choose a bigger based number of respondents and areas when investigate the problems in China can give a more precise answer.
References


Jing, Z., 2002. AD hoc wireless network, s.l.: s.n.


Appendix 1

Questionnaire

Information of respondents
1. Your gender is
   - Male
   - Female

2. Your age is
   - <15
   - 15-30
   - 31-45
   - >45

Usage habits
3. Which type of Wi-Fi do you usually use to access internet?
   - Use public Wi-Fi building by mobile company, such as CMCC, ChinaNet
   - Use Wi-Fi in office
   - Use Wi-Fi in campus
   - Use Wi-Fi at home

4. How long you spend time on Wi-Fi connection?
   - <2 hours
   - 2-4 hours
   - 4-6 hours
   - 6-8 hours
   - >8 hours

5. How many devices in your home could connect with the Internet?
   - 0
   - 1-3
   - 4-8
   - >9

6. Your main Internet equipment
   - PC
   - Laptop
   - Pad
   - Mobile phone
   - TV
   - Others

7. What activities have you conducted using Wi-Fi?
   - Financial transactions, like transfer payment or credit card payment
   - Online purchasing, like placing orders at shopping sites or auction sites
   - Check and answer e-mails
   - Search and download information
   - Play on-line games
• Social networking, e.g. Weibo, WeChat
• Other activities

8. Do you agree that your information is not safe when you use Wi-Fi?
  • Strongly agree
  • General agree
  • Medium
  • Not agree
  • Strongly not agree

**Internet speed**

9. Are you satisfied with the internet speed of your usual connection?
  • Highly Satisfied
  • Generally Satisfied
  • Dissatisfied
  • Very dissatisfied

10. Why do you think your internet speed is slowly?
  • Operators shrink the broadband speed
  • P2P download and online video viewing
  • Computer virus or hacker attacks
  • There are Wi-Fi squatters
  • Others

11. Do you think there are Wi-Fi squatters?
  • Yes, there are squatters using my Wi-Fi
  • No other people use my Wi-Fi
  • Not sure about that

12. What is the reason you think leads to that the Wi-Fi is robbed?
  • Password if very easy
  • Wi-Fi password cracked by tools
  • Router loophole attack
  • Told others the password before
  • Wi-Fi share software

**Connection awareness**

13. Have you used the automatic connection software on your internet access devices?
  • Yes
  • No
  • I don’t know

14. Do you have conscious that the public Wi-Fi you connect it could be the fake one?
  • Yes
  • No
  • Never think about it.

15. The main way you access the Internet at home or dormitory?
• ADSL virtual dial
• Dynamic IP (automatically obtain the IP address)
• Static IP (manually fill in the IP address)
• Others

16. Do you connect to Wi-Fi networks when using VPN?
   • Yes
   • No
   • I don’t know what is VPN

**Router settings**

17. How did your router installed?
   • Refer to the instructions
   • Ask others for help
   • Consult or search through the Internet
   • Other ways

18. Do you know there are two main passwords for home router, one for the connection and one for management?
   • No
   • Yes

19. Did you change the connection and management passwords and already configure the routers from management background? (18-Yes)
   • Yes
   • No

20. What is the composition of your management password? (19- Yes)
   • The initial password, never change it (eg: admin, guest, password)
   • Very easy (eg: 123123, 1234567, abcdefg)
   • Medium complex (eg: aoigyhoafj123852)
   • Complex (eg: sl9sge3hf7fhw8)

21. What is the composition of your password?
   • The initial password, never change it (eg: admin, guest, password)
   • Very easy (eg: 123123, 1234567, abcdefg)
   • Medium complex (eg: aoigyhoafj123852)
   • Complex (eg: sl9sge3hf7fhw8)

22. What do you think about your Wi-Fi password?
   • Very safe
   • Safe
   • Medium
   • Not safe
   • So dangerous
23. How do you use the router daily?
   - Ignore it, let it running
   - Turn on the power when use it, turn off the power when not use it
   - Insert the network cable when use it, pull it out when do not use it
   - Others

**Technique question**

24. What your understanding level about the following word?

<table>
<thead>
<tr>
<th></th>
<th>Very clearly about it</th>
<th>Not very clearly about it</th>
<th>Basic understand</th>
<th>Just heard about it</th>
<th>Never heard it before</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WPA WPA2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARP mapping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

25. Are you set up and used the following functions of router in your home?
   - Except access the Internet, have not used the other functions
   - Setting the Internet environment
   - Setting the Wi-Fi options (eg: change username or password )
   - IP bandwidth control
   - WDS wireless bridge
   - QSS quick Connect
   - Dynamic DNS setting
   - IP and MAC address binding
   - MAC address cloning
   - Parental Controls
   - Others

26. If you cannot access the Internet, what are the reasons after you repaired it?
   - Installation or configuration error
   - Internet problems, computer poisoning or setting error
   - Network service provider issues
   - Network cable, ADSL or other effects
   - Router problems
   - Others

27. What are the problems in the processing you use the wireless network? (Open)

28. How do you do when you have trouble in router or Internet? (Open)
University of Borås is a modern university in the city center. We give courses in business administration and informatics, library and information science, fashion and textiles, behavioral sciences and teacher education, engineering and health sciences.

In the School of Business and IT (HIT), we have focused on the students' future needs. Therefore we have created programs in which employability is a key word. Subject integration and contextualization are other important concepts. The department has a closeness, both between students and teachers as well as between industry and education.

Our courses in business administration give students the opportunity to learn more about different businesses and governments and how governance and organization of these activities take place. They may also learn about society development and organizations' adaptation to the outside world. They have the opportunity to improve their ability to analyze, develop and control activities, whether they want to engage in auditing, management or marketing.

Among our IT courses, there's always something for those who want to design the future of IT-based communications, analyze the needs and demands on organizations' information to design their content structures, integrating IT and business development, developing their ability to analyze and design business processes or focus on programming and development of good use of IT in enterprises and organizations.

The research in the school is well recognized and oriented towards professionalism as well as design and development. The overall research profile is Business-IT-Services which combine knowledge and skills in informatics as well as in business administration. The research is profession-oriented, which is reflected in the research, in many cases conducted on action research-based grounds, with businesses and government organizations at local, national and international arenas. The research design and professional orientation is manifested also in InnovationLab, which is the department's and university's unit for research-supporting system development.

Visiting address: Järnvägsgatan 5 · Postal address: Allégatan 1, SE-501 90 Borås · Phone: +46 33 435 40 00 · E-mail: inst.hit@hb.se · Web: www.hb.se/hit