

Article

Computer aided judgment method of legal liability and laws and regulations for embezzlement of WLAN

Liangliang Zhou

Department of policy and law, Party School of Cangzhou municipal Party committee of CPC, Cangzhou, 061000, China
zlltg2021@163.com

ABSTRACT

With the increasingly perfect protection of citizens' information and computer systems in China, network security has become an important problem in the development of information age. The common embezzlement of WLAN has not been paid enough attention. The number of cases such as personal privacy leakages and property damage caused by this behavior is increasing. In this analysis, we investigated computer aided judgement methods and suggested various strategies in order to improves the security system of Chinas' industrial sector, banking sectors, education sectors, etc., by promoting country's laws and regulations. we also highlight the optimization methods of the legal liability for embezzlement of WLAN. Based on the clear different ways of embezzlement of WLAN, based on the different purposes and results of the embezzlement, the civil liability and criminal liability of the embezzlement are analyzed, and the problems existing in the application of law are explored, which provides legal basis for the construction of a safe network environment.

Journal of Commercial Biotechnology (2021) 26(2), 100–112. doi: 10.5912/jcb1091

Keywords: wireless local area WLAN; legal responsibility; computer; laws and regulations, Responsibility determination.

INTRODUCTION

Today with the development of information technology, the application of computer system is also increased. Computer system has its application in almost every field of life. Many sectors including education sector, industrial sector, banking sectors, etc., has been using computer instead of manual system for data storing, processing, and managing. Information technology has changed mans' life. The utilizing of computer system in our workplace has ability to

provide more reliable and comfortable environment to consumers. But along with the various applications of computer system, the security of the protection of computerized data has become significant issue from recent many years. Because the computer crimes are increasing with the passage of time. Some unauthorized persons are involving in various activities of computer crime including phishing, some kind of dangerous virus and malwares, hacking, identity theft etc. Furthermore, with the passage of time the computer crime cased has been increasing day by day. The most important issues are about bank

account hacking, personal account hacking, mobile hacking, leakage of personal information and property damage. It is also considered as a life threatened problem, because many people have committed suicide due the leakage of their personal information. That is why, it is very important to solve and manage these issues by implementing rules of law. Apart from this, in this research paper, we have studied various laws and regulations implemented by the government in order to improve security of the individuals and many organizations.

In the context of implementing the comprehensive rule of law and maintaining the security of cyberspace, aiming at the frequent occurrence of embezzlement of wireless local area network (WLAN), this paper first expounds the relevant concepts and ways of embezzlement of WLAN, and then divides the civil liability and criminal liability of embezzlement under different purposes. Finally, it explores the relevant problems existing in the application of law, so as to provide reference for the protection of citizens' personal information security and network security, so as to improve the national network security system. WLAN is the use of wireless communication technology and equipment to build a computer WLAN, is an extension of the existing WLAN or wired WLAN [1]. Wi-Fi network composed of wireless router or smart phone is the most widely used wireless network transmission technology. In the way of embezzlement, it is a common way to embezzle others' online account password, and the behavior of "rubbing the network" by using "password sharing" software is also a common way for current users to embezzle others' network. In particular, the app, a wireless internet tool represented by "Wi-Fi master key", can obtain other people's wireless WLAN information, including WIFI name, WIFI password, MAC address and location, etc. The active attack and embezzlement method based on VMware Workstation is adopted by more professional people [2]. They attack other people's wireless network to get the wireless network password through pin code and grab the wireless network handshake packet, so as to achieve the purpose of stealing other people's wireless network. Illegal users of wireless network intercept the personal information of legal users through the shared wireless network signal channel and change all kinds of information on the wireless network terminal equipment at will. No matter how to embezzle others' wireless local area network, this

behavior invades others' network, brings security risks such as personal information leakage to users, and infringes the legitimate rights and interests of users [3]. Therefore, government of the country should made Strick laws and regulation to reduce crime rate in the country especially the laws of security should be made for WLAN. In China, government of China has been working on the networking security laws from recent many years and it almost has been two years since the implementation of the "network security law". The security of cyberspace has been strengthened day by day, and the network security awareness of the whole society has been continuously improved. However, in reality, the behavior of embezzling wireless local area network has not been paid attention to. It has become a habit for people to connect to wireless local area network with the help of "network rubbing" software [4]. To some extent, everyone is an "embezzler", everyone is a "thief". Therefore, in order to maintain the security of cyberspace, it is necessary to clarify the status of embezzlement of wireless local area network in the law and explore the legal application of embezzlement of wireless local area network in different situations.

Research objective:

In this research paper, our aim was to investigate the computer aided judgment methods for legal liability as well as laws and regulations implemented by the government in order to improve the security system. Various methods of computer aided judgement for embezzlement of WLAN have been examined in the paper. Furthermore, many computer crimes have also been studied and the method to control the increasing computer crimes have also been investigated in this research.

Computer aided determination of legal liability, laws, and regulations

- **Legal liability**

In the WLAN security, liability refers answerable or responsibility in laws and regulations which is legal obligated. Moreover, Legal liability involves both criminal or civil law and can emerge from a variety of sources, including agreements, litigation, taxation, and judgments imposed by government authorities. The complainant is the individual or

organization attempting to establish or show liability.

- **Laws and regulations of WLAN**

In most of the developing countries, the usage of WLAN has been increased with the emergence of technology. To use the applications of wireless LANs, government of the country made laws and regulation in order to secure data and information of the organization. In addition, Laws and Regulations refers to all immediate and long-term legal requirements, regulations, rules, codes, ordinances, permits, and orders. Compliance with laws and rules is a major focus for any organization's information security management.

- **Wireless Local area networks**

A WLAN or wireless LANs is a way of wirelessly connecting two or more computers. Wireless local area networks utilize radio waves of high frequency and frequently include an Internet access point. A Wireless network allows users to migrate throughout the service area, which is often a small office or house, while remaining connected to the network. To enable Internet connectivity to linked devices, Wi-Fi networks frequently connect to a wired connection or other devices having Internet connection. A link which joins two networks can be used to link WLANs and LANs.

1.1 legal responsibility authentication of embezzling WLAN

Although the telecommunication regulations of the People's Republic of China have been revised twice, there is no effective regulation on the embezzlement of WLAN. Among them, the regulation of Article 58 concerning disturbing the order of telecommunication market explicitly prohibits the copying of other people's telecommunication numbers but ignores the new form of embezzlement of WIFI network in WLAN [5]. Article 27 of the network security law implemented in 2017 stipulates that no individual or organization shall engage in activities that endanger network security such as illegal intrusion into other people's network, interference with other people's network normal functions, stealing network data and other activities. Although the network security law does not clearly embezzle the WLAN, it can be determined that the theft of other wireless WLAN in any way belongs to the category

of illegal intrusion into other people's networks. Secondly, whether the embezzlement of WLAN belongs to the activities endangering the network security, whether the embezzlement of WLAN can meet the standard of endangering the network security, whether the behavior of embezzling WLAN interferes with the normal functions of other people's networks, these problems still need to be clarified in the network security law [6]. In the division of legal responsibility, the Article 66 and 67 of telecommunication regulations are almost identical with the provisions of Article 63 of the network security law, that is, criminal liability shall be investigated for the acts constituting a crime; If the crime is not constituted, the punishment shall be carried out in accordance with the corresponding administrative provisions. In view of the specific situation of address spoofing attack in wireless link layer, we adopt an address deception detection algorithm based on serial number analysis. Defines the gap between the serial numbers of frames I and $i-1$ G :

$$G = S_i - S_{i-1} (\text{mod } 4096) \quad (1)$$

At present, there are many algorithms about pattern matching, the most famous of which are KMP algorithm and BM algorithm [7]. Both algorithms have linear search time in the worst case. But in practice, KMP algorithm is not much faster than the simplest c library function strip. BM algorithm is usually 3-5 times faster than KMP algorithm. But BM algorithm is not the fastest algorithm. The problem of pattern matching is described as follows

$$\begin{cases} P = P_1, P_2, \dots, P_n \\ T = t_1, t_2, \dots, t_m \end{cases} \quad (2)$$

It is required to find the substring equal to t in P . If there is a substring equal to t in P , it is called matching success and the position of the substring in P is returned. Otherwise, it is called matching failure and Q is returned. In the fuzzy comprehensive evaluation of the legal liability of misappropriating WLAN, the evaluation index set is firstly established [8]. The indicator set is $U = \{U_1, U_2, U_3, U_4, U_5\}$, in which u is the subset of "correct guidance", U_2 is the subset of "local area network content", U_3 is the subset of "power, benefit and supervision", U_4 is the subset of "social morality", and U_5 is the subset of "credit taint". According to

the evaluation value of the evaluation index, it can be divided into five grades, namely excellent, good, average, poor and very poor. Each comment level corresponds to a fuzzy subset [9]. Let the filled judgment matrix be:

$$R = P - T / G(r_{ij})_{n \times n} \quad (3)$$

$$R = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1j} & \dots & r_{1n} \\ r_{21} & r_{22} & \dots & r_{2j} & \dots & r_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ r_{i1} & r_{i2} & \dots & r_{ij} & \dots & r_{in} \\ r_{m1} & r_{m2} & \dots & r_{mj} & \dots & r_{mn} \end{bmatrix} \quad (4)$$

Table 1. Evaluation index system

Target layer	Base layer	Index layer
Responsibility	Power supervision	Information viewpoint
		Internal audit
	Correct guidance	Guiding principles
		Mass principle
	Content	Authenticity and objectivity
		Timeliness
	Social morality	Scientificity
		Protecting the interests of information sources
		No harm interview

Table 2. Meaning of importance scale

Importance scale	Index layer
	Indicators are equally important
1	
3	The former is more important than the latter
5	The former is more important than the latter
7	The former is more important than the latter
9	The former is more important than the latter
2,4,6,8	Represents the median of the above comparison

On the determination of the weight, 10 experts were invited from the field of law. After explaining the meaning of the index to the experts, they were asked to give their opinions on the importance of the index,

and scored the weight, forming a judgment matrix at all levels [10]. The judgment matrix of target layer is shown in the table 3.

Table 3. Judgment matrix of target layer

	1	2	3	4	5
1	1	1/6	1/7	1/3	1/5
2	6	1	1/3	3	3
3	7	3	1	5	5
4	3	1/3	1/5	1	1/2
5	5	1/3	1/5	2	1

$$M_1 = \prod_{j=1}^5 a_{1j} = 1 \times 1/6 \times 1/7 \times 1/3 \times 1/5 = 0.00159$$

(5)

Calculate the n-th root:

$$\overline{W}_1 = \sqrt[5]{0.00159} = 0.2756 \quad (6)$$

The vector is normalized.

$$W_1 = \frac{\overline{W}_1}{M_1 - \sum_{j=1}^5 W_j} \quad (7)$$

Find the maximum eigenvalue of the judgment matrix.

$$AW = \begin{bmatrix} 1 & 1/6 & 1/7 & 1/3 & 1/5 \\ 6 & 1 & 1/3 & 3 & 3 \\ 7 & 3 & 1 & 5 & 5 \\ 3 & 1/3 & 1/5 & 1 & 1/2 \\ 5 & 1/3 & 1/5 & 2 & 1 \end{bmatrix} \begin{bmatrix} 0.0388 \\ 0.2507 \\ 0.4992 \\ 0.0887 \\ 0.1297 \end{bmatrix} = \begin{bmatrix} 0.2074 \\ 1.3051 \\ 2.0309 \\ 0.5644 \\ 0.7179 \end{bmatrix} \quad (8)$$

Then:

$$\lambda_{\max} = \sum_{i=1}^5 \frac{(AW)_i}{5W_i} \quad (9)$$

The consistency index of the judgment matrix is further calculated.

$$CI = \frac{\lambda_{\max} - n}{n - 1} \quad (10)$$

In order to test the consistency of different order judgment matrix, it is necessary to introduce the average random consistency index. The value of RI can be obtained by looking up the table according to the value of order n. The values of judgment matrix RI of order 1-9 are shown in the table 4.

Table 4. Mean random consistency index RI

1	2	3	4	5	6	7	8	9
0.0	0.0	0.58	0.90	1.12	1.24	1.33	1.42	1.46

When $CR < 0.10$, the judgment matrix can be considered to have satisfactory consistency, otherwise, corresponding adjustment should be made until it is satisfactory^[11]. According to the standard of liability form, the legal liability of misappropriating WLAN can be divided into direct tort liability and indirect tort liability. If any network user or network service provider commits an act of infringement, he or she shall bear direct responsibility for the act of infringement. To constitute joint and several liability of tort, there must be joint tort, the parties have joint fault subjectively, the fact of damage objectively, and the causal relationship between tort and the fact of damage". The third paragraph of Article" 36 of the tort liability law defines the tort liability for the direct infringement of Internet users and Internet service providers, and in the third paragraph and the third paragraph, discusses whether the Internet service provider, as a third party, should bear joint tort liability with Internet users in the case of direct infringement of Internet users^[12]. Therefore, according to the division standard of the tort liability law, that is, whether the infringer has directly carried out the tort, the legal liability of embezzling WLAN can be divided into direct tort liability and indirect tort liability. Indirect tort liability is mainly applicable to the infringement of copyright, which means that the behavior of the actor itself does not constitute a direct tort, but abets and helps others to implement the direct tort, so as to bear the responsibility for others' tort.

1.2 Wireless WLAN intrusion behavior judgment

Wireless intrusion detection agent is mainly composed of packet capture module, protocol decoding module, preprocessing module and detection analysis module. The functions of each module are as follows: packet capture module is responsible for monitoring and capturing the original packets in the network, and filtering the packets according to the filtering requirements^[13]. The protocol decoding module decodes the original packets captured and filtered by the packet capture module according to the protocol tree structure, so as to facilitate the intrusion analysis by the preprocessing module and the detection and analysis module; After the protocol decoding, the preprocessing module preprocesses the packets before the detection and analysis module^[14]. On the one hand, it can find the intrusion information, on the other hand, it makes the final preparation for the detection and analysis module. The rule parsing module analyzes the content of the rule file and loads the rules into memory to form a rule chain^[15]. The detection and analysis module compares and analyzes the data submitted by the preprocessing module by using the matching algorithm and the rules in the rule base, so as to determine whether there is an intrusion.

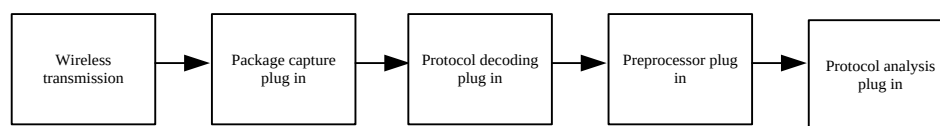


Fig. 1 Structure of modified wireless intrusion detection system

When working, the network interface of link layer should only respond to such two kinds of packets: one is that the destination MAC address of the packet matches the local network interface, the other is that the destination MAC address of the packet has a "broadcast address". For other packets, the network interface will be discarded. Similarly, the network layer will determine whether the destination IP address of the packet is the IP address bound to the local machine. If not, the packet will be discarded. Only the packet that meets its own IP address will be

handed over to the transport layer for processing^[16]. At that time, the AP sends the ID management frame at a specific frequency. After receiving the authorization, the client establishes the authorization by sending the authorization frame. After the authorization is successful, the client sends the associated frame, and finally the AP responds to the associated frame. IEEE802.11 defines a mechanism for tracking the authorization and connection status of a site^[17]. As shown in the figure 2, only the client in state 3 can be allowed to access the wireless network.

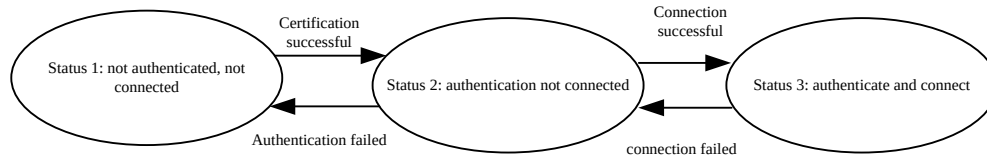


Fig. 2 site tracking authorization and connection state mechanism

The attacker embezzles MAC address to fake the client and sends a large number of authorization request information to AP constantly, so as to achieve the purpose of capturing the client state table (connection table) of AP device^[18]. If the AP uses open system authentication, the AP will send the authentication success frame to the client and create a table entry with status 2 for the client in the status table. If AP uses shared key authentication, AP will send an authentication waiting frame to the client and create a

table entry with the content of state 1 for the client (attacker). Because the attacker does not respond to the frame, AP will always set the state of the client to state 1. Regardless of the above situation, the state table of AP device will eventually overflow due to too many entries in state 1 and state 2. Once overflow occurs, legitimate clients will not be able to obtain AP authentication and connection, resulting in network paralysis, as shown in the figure 3:

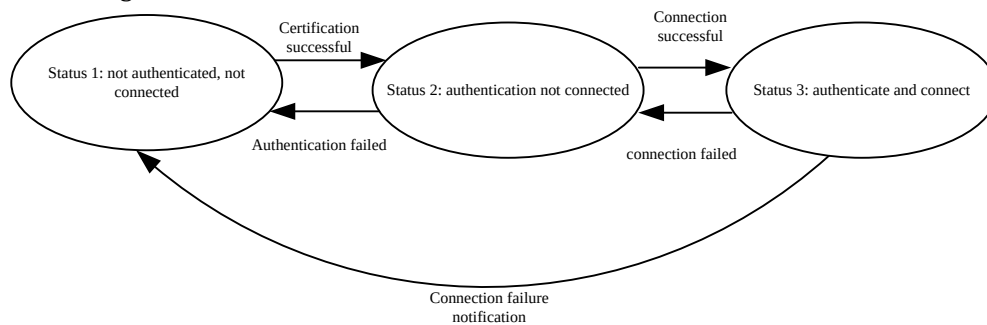


Fig. 3 authentication information flooding attack

In the transport layer, it will determine whether the TCP or UDP target port corresponding to the message has been opened locally^[19]. If so, it will submit the data

in the packet to the corresponding application layer. Otherwise, it will discard these packets.

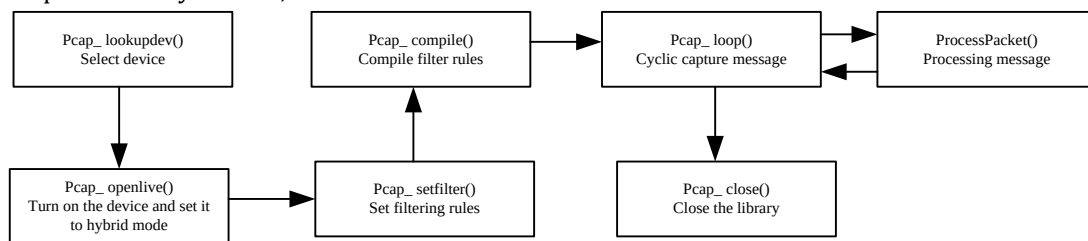


Fig. 4 flow chart of message capture

Therefore, to capture all packets flowing through the wireless network card, we must bypass the normal processing mechanism of the system and directly access the data link layer of the network, that is, the network card should be put in hybrid mode first. When the network interface is in this "hybrid" mode, the network interface has the function of "broadcast address", which will remind the operating system to process every packet flowing through the physical

local area network. The operating system will directly access the data link layer, intercept the relevant data, and filter the data by the application rather than the upper layer such as network layer and transmission layer protocol, so that all data flowing through the network card can be captured^[20]. In theory, the serial number of the frame sent out by the same source MAC address should be continuous, so as long as the sequence number gap is greater than 1, address

spoofing attack occurs. However, in the actual situation, because of the loss, retransmission, and disordered sequence of frames, if the sequence number gap of the frame is more than 1 as the detection basis, it will lead to high false alarm rate. Authentication server is usually a radius server that supports AAA protocol. It can store information about users, such as username, password, access traffic and time, user access control list, etc. The EA probe radius protocol is adopted from the authentication end to the authentication server. After the user passes the authentication, the authentication server will pass the relevant information of the user to the authentication system. The authentication system will build a dynamic access control list, and the subsequent traffic of the user will be regulated by the above parameters.

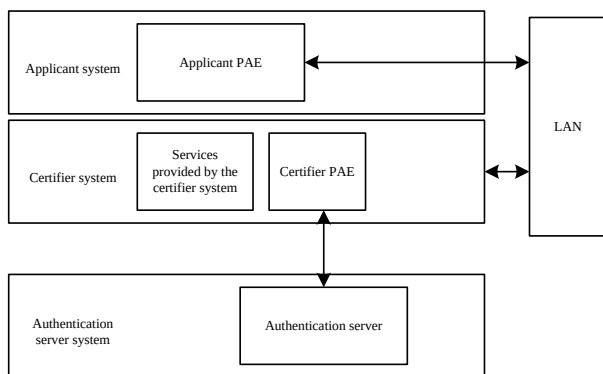


Fig. 5 core authentication system of wireless network security mechanism

Due to the anonymity and digitization of the network, the subject of legal responsibility for embezzlement of wireless local area network needs to create a virtual subject on the network. In the process of using, there will be a phenomenon that a subject of legal responsibility for embezzlement of wireless local area network corresponds to multiple virtual subjects or multiple subjects of legal responsibility for embezzlement of wireless local area network use a virtual subject. Although the virtual subject seems to have intention expression and certain capacity, it lacks the conditions to become a legal subject and should not be regarded as a legal subject. The fundamental reason is that the behavior and expression of will of the virtual subject are dependent on the real subject, and the responsibility is also borne by the real subject. Although the law has adopted a broad concept to regulate the network service provider, it will not hinder the legal status of its ultimate responsible subject. In other words, according to the network service provider to provide services, often need to establish a website to provide

services. These websites are built in a virtual environment, with virtuality, and ultimately also point to the real subject, if the content of the website or service infringement, also should be borne by the real subject. As for the true identity of the infringer, it can also be tracked through electronic signature or authentication such as IP address, authentication provided by third-party trading platform providers, government registration and electronic business license. At present, China's real name system has been gradually implemented, and the real name system has been used in some platforms. The infringed can apply for the network service provider to disclose the information of the infringer, so as to impute the real infringer.

Analysis of experimental results:

Through the design of the questionnaire, the author collects the views and opinions of the audience, analyzes the results of the questionnaire with spss20.0 software, and uses the AHP method to sort the importance, eliminate the weak correlation factors, extract the factors with large relevance, and finally form the evaluation index system of the paper. The questionnaire was widely distributed and recycled, the invalid questionnaire was eliminated, the data of the effective questionnaire was summarized, and the factor was removed and extracted by exploratory factor analysis. The method is mainly analyzed and tested by spss20.0 software package. This experiment is carried out in the environment of three computers with d-linkwua-2340 wireless network card and Windows XP operating system, one linksyswap54g wireless access point (AP), and one central console with WindowsXP operating system. The logical steps of factor analysis are shown in the figure 6:

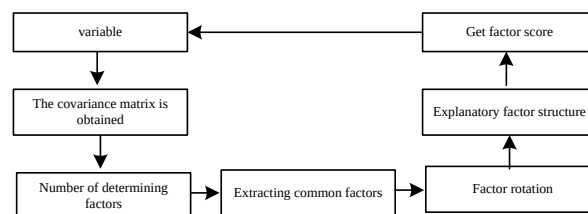


Fig. 6 logical steps of factor analysis

This questionnaire is mainly distributed in the form of electronic questionnaire. It is aimed at the audience who are over 18 years old and have the ability to perceive and understand the legal responsibility of embezzling wireless local area network, regardless of

educational background and occupation. The survey is as wide as possible. A total of 225 questionnaires were sent out, 218 were returned, 198 were valid, the

recovery rate was 96.88%, and the effective rate was 90.83%. The basic information of the respondents is shown in the table.

	Statistical items	Frequency	Percentage%	Cumulative percentage
Age	25-34 years old	32	16.16	26.76
	35-49 years old	134	67.68	94.44
	Over 50 years old	11	5.56	100.00
Education	Junior middle school	0	0	0
	High school	9	4.54	4.54
	Junior college	32	16.16	20.70
	Undergraduate college	89	44.95	65.45
Occupation	Student	25	12.63	12.63
	Civil servant	9	4.55	17.18
	Teacher	27	13.64	93.96
	Retired	2	1.01	94.07
	Other things	8	4.04	100.00

The main method of scale analysis is principal component analysis, which extracts the factors whose eigenvalue is greater than 1, and uses the maximum variation method for orthogonal rotation. In addition, according to the research practice and relevant requirements, it is also necessary to have the factor items whose number of factor items is less than 2. Firstly, KMO and Bartlett's spherical test were carried out on 27 items. The closer KMO value is to 1, it shows

that the sum of squares of simple correlation coefficients among all variables is far greater than the sum of squares of partial correlation, so it is more suitable for factor analysis. When KMO value is between 0.9 and 1, factor analysis is most suitable. When KMO value is between 0.9 and 0.7, factor analysis is barely acceptable. If KMO value is less than 0.5, it is not suitable.

Table 6 KMO and Bartlett test

Importance scale KMO and Bartlett's test		
Kaiser Meyer Olkin measure of sampling adequacy	Indicators are equally important	7.36
Bartlett's sphericity test	Approximate chi square	2569.43
	Sig.	0.000
	df	351

This result can also be seen in the graph, the number of factors before the slope turning is the number of factors to be extracted, and its characteristic root must be the factor greater than 1. The cumulative explained total variance of the five factors is 75.294%, indicating that it is suitable to extract five factors.

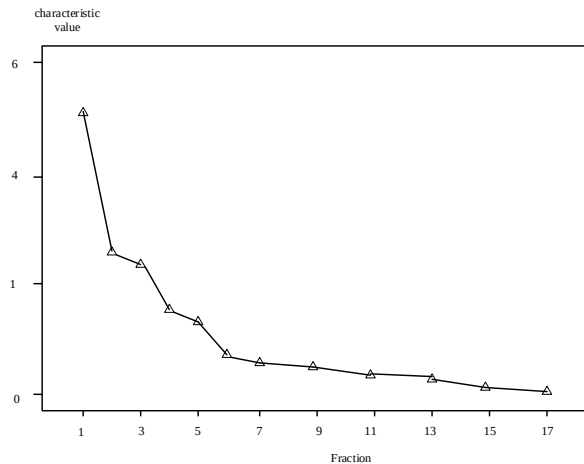


Fig.7 validity and reliability test results

The validity and reliability test is mainly through rotating the component matrix to check the factor load. When the load is greater than 0.67, it has high validity. Cronbach's alpha value was used to test the **Table 7**. Detailed description

Content	Explain
SSID	There is an SSID identifier in the network
STA	There are currently 13 sites working in the network
AP	Three APS are deployed in the network
Security	There are two serious security errors in the network
Performance	There are 11 critical performance errors in the network

Test the network encryption status. According to the test environment provided above, all network devices in the environment are long-term working devices in

reliability, and was used as the main index of internal consistency test. The Cronbach's alpha value is calculated according to Formula 1, and the Cronbach's alpha values of the five factors are 0.956, 0.877, 0.710, 0.798 and 0.887 respectively. The homogeneity reliability of the questionnaire on the legal responsibility evaluation dimension of embezzlement of WLAN is 0.579.

$$\alpha = \frac{k}{k-1} \left[1 - \frac{\sum_{i=1}^k \sigma_i^2}{\sum_{i=1}^k \sigma_i^2 + 2 \sum_i \sum_j \sigma_{ij}} \right] \quad (11)$$

In the test process, if a site temporarily joins the wireless network, the test results (mainly the site) will be different. From the test results of the two, using the tester to test can clearly understand the equipment information in the network, while using the protocol analysis software requires managers to have a certain early understanding of the network. If the network managers do not know much about the network, they need to check the equipment listed in the protocol analysis software one by one, in order to ensure that the equipment has taken the necessary encryption measures.

the environment, so all devices must set encryption mechanism to ensure the security of information transmission.

Table 8 item segments and reliability coefficient of the factors

Factor number	Factor name	Factor project	Number of projects	Cronbach's Alpha	Cronbach's Alpha
1	Correct guidance	D7、D8、D9	3	0.956	0.579
2	content	D10、D11、D12、D13、D14、D15	6	0.877	
3	Right supervision	D17、D18	2	0.710	
4	Social morality	D21、D22、D24	3	0.798	

When Cronbach's alpha value > 0.70 , the questionnaire has high reliability; when $0.35 < \text{Cronbach's alpha value} < 0.7$, the questionnaire has fair reliability; when Cronbach's alpha value > 0.35 , the questionnaire has poor reliability.

Research objective: Optimization of WLAN legal liability determination method

The subject of law should be legal and social, that is to say, the subject of legal relationship is determined by law, and the provision of law is determined by certain material living conditions. Therefore, to study the tort liability of each subject in the legal liability of embezzlement of WLAN, the first problem is to clarify the legal status of the subject of the legal liability of embezzlement of WLAN.

The principle of imputation is the core of tort law, the theory of tort law and the judicial practice of tort law. In Article 36 of tort liability law, the provisions on the liability of embezzlement of wireless local area network are not disputed. For the indirect tort liability when the network users infringe, the principle of liability for fault is the principle of fault liability applied by the network service provider.

In the current judicial practice, although the relevant legislation on the legal liability of misappropriation of wireless local area network has confirmed its imputation principle as fault liability principle, once the legal liability of misappropriation of wireless local area network occurs, especially the infringement of network users, due to the virtual identity of network users, it is often difficult for the infringed to find the real infringer. This causes problems in the relief of liability. Therefore, the infringed often choose the

network service provider as the defendant because of the compensation ability and relative certainty of the network service provider. This is different from the traditional tort field, although the corresponding tort liability for network users is formulated, it can not be used in practice. In addition, in the distribution of the burden of proof, it is also a question worthy of discussion whether we should consider the burden of proof of network users and network service providers.

Network service providers are in different positions in information dissemination because of their service types. For example, the content service provider of electronic announcement has the ability to edit and control the information uploaded by users, which is equivalent to the role of "network publisher and publisher". Therefore, in terms of rights and obligations, it should be given certain review obligations. But different from the traditional publishers and publishers' tort liability, there is no active review obligation of network service providers in China's legislation, and it is also clearly stated in the interpretation that network service providers have no active review obligation. Due to the huge amount of information in WLAN, network service providers cannot and should not review it in advance, which is different from traditional WLAN tools. However, the network service provider has the duty to review after the event, which is reflected in the regulations on the right of information network communication and the interpretation.

Although there is no difference between the legal liability of embezzlement of WLAN and that of traditional tort law in general, there are some particularities in the specific implementation. For example, the legal liability of embezzlement of WLAN will involve the infringement of virtual property, so how to return the virtual property? Based on the

openness and communication of the network, the damage caused by the infringement of network personality rights often does not have the feasibility of specific identification in practice, so this paper discusses this problem in detail.

China's tort liability law stipulates that the ways of bearing civil liability include stopping the infringement, removing the obstruction, eliminating the danger, returning the property, restoring the original state, compensating for the loss, making an apology, eliminating the influence, restoring the reputation and so on. The way of civil liability for infringement of property rights usually includes returning property, restitution, compensation for losses and so on, which also applies to the tort liability of virtual property. It should be pointed out that the right of claim for real right includes the right to exclude the nuisance, the right to eliminate the danger and the right to return the original object. The purpose of its exercise is to restore the perfect state of control over the object.

As mentioned above, the legal liability environment of embezzlement of wireless local area network is virtual, which requires that in the bearing of legal liability, it may be different from that of traditional tort liability in the actual application. For example, in the return of virtual property, because virtual property can be created by network technology, In return, we will take measures such as technical recovery to make it return to the default state or the state at a specific time. We may need to use technical means to confirm it in practice. If you can use the identity authentication measures, if you can't identify it through the above channels, you can choose to use the evidence rules to solve it.

Conclusion:

In conclusion, it is studied that with the rapid advancement in the field of information technology, computer system has also increased its application in every field of life including banking, sports, industries, education. In this research paper, we examined that with the increase in the application of computer, the computer related crimes have also been increased including leakage of personal information, mobile hacking, bank accounts hacking, phishing etc., Apart from this, we explore various application of computer in different field and the problem related to the use of computer system also have been discussed in the paper. In addition, we investigated research in order to analyze the computer aided judgment method of

legal liability for embezzlement of WLAN. Moreover, various methods have been investigated for embezzlement of WLAN. In this research study, we conducted research from various organization utilizing computer system in China. Apart from this, we studied about the various rules and regulations of network security. It is also highlighted that governance of WLAN network system in China has been working on the laws of network security from many years and it was almost 2 years to implement laws of network security in China WLAN. Furthermore, we point out the direction to promote the establishment of China's network security system and establish a correct network security concept. From the network special legislation to the network security system construction, from the protection of user privacy information to strengthen the network security review, the network security barrier is increasingly firm, and the network security foundation is constantly consolidated. Apart from this, authorized and unauthorized utilization of computer system has also been highlighted. We collected sample data through questionnaire survey method and analyzed by using various software including SEM, Smart plus, fuzzy analysis method etc., and it was examined that today the computer crimes are increasing day by day. Therefore, there is essential need to make rules of law in order to control the unauthorized use of computer system in various organization. Furthermore, we investigated the optimization methods of WLAN legal liability determination. It is studied that in order to study the tort liability various subjects in the embezzlement of WLAN legal liability, the first and foremost challenge was to highlight and understand the legal status of the subject. So, by analyzing the problems of the computer aided judgement methods of legal liability, we can improve the security of the WLAN. Apart from this, it is highlighted that at present, people still need to see the problems existing in the field of network security, especially the embezzlement of wireless local area network (WLAN) in the rapid development of information network, in order to improve the network security system, but in reality, there are some problems, such as vague laws and regulations, unclear definition of embezzlement, difficult to identify the amount of traffic, derivative results and so on. This not only needs the improvement of legislation, but also needs the participation of all parties in the society, the combination of law and technology and other means to promote the construction of network power.

References:

1. Antonioli R P , Pettersson J , Maciel T F . 2020, Split Responsibility Scheduler for Multi-Connectivity in 5G Cellular Networks. *IEEE Network*, PP(99):1-8.
2. Binsawad M H . 2020, Corporate Social Responsibility in Higher Education: A PLS-SEM Neural Network Approach. *IEEE Access*, PP(99):1-1.
3. Coronado E , Bayhan S , Thomas A. 2021, AI-Empowered Software-Defined WLANs. *IEEE Communications Magazine*, 59(3):54-60.
4. D Tripathi, Srivastava D K , Verma R K . 2021, Bandwidth Enhancement of Slotted Rectangular Wideband Microstrip Antenna for the Application of WLAN/WiMAX. *Wireless Personal Communications*, 2(1):1-15.
5. Duan C , Yao F , Xiu G. 2020, Multi-Period Closed-Loop Supply Chain Network Equilibrium: Perspective of Marketing and Corporate Social Responsibility. *IEEE Access*, PP(99):1-1.
6. Duvvada R S , Narayanaswamy P , Phani M. 2021, Circularly Polarized Jute Textile Antenna for WiMAX, WLAN and ISM Band Sensing Applications. *Applied Computational Electromagnetics Society Journal*, 35(12):1493-1499.
7. Dwijaksara M H , Jeon W S , Dong G J . 2019, User Association for Load BaWLANcing and Energy Saving in Enterprise WLANs. *IEEE systems journal*, 13(3):2700-2711.
8. Garroppo R G , Nencioni G , Tavanti L. 2021, Optimal Access Point Power Management for Green IEEE 802.11 Networks. *Sensors*, 21(6):2076.
9. Ha V N , Kaddoum G , Poitou G . 2021, Joint Radio Resource Management and Link Adaptation for Multicasting 802.11ax-based WLAN Systems. *IEEE Transactions on Wireless Communications*, PP(99):1-1.
10. Han Z , Tao L , Lu Z. 2019, Artificial Intelligence Based Handoff Management for Dense WLANs: A Deep Reinforcement Learning Approach. *IEEE Access*, PP(99):1-1.
11. Jadidi I , Honarvar M A , Khajeh-Khalili F . 2019, COMPACT TRI-BAND MICROSTRIP FILTER USING THREE TYPES OF RESONATORS FOR BLUETOOTH, WIMAX, AND WLAN APPLICATIONS. *Progress in Electromagnetics Research C*, 91(6):241-252.
12. Kim S , Lee K , Kim Y. 2019, Dynamic Control for On-Demand Interference-Managed WLAN Infrastructures. *IEEE/ACM Transactions on Networking*, PP(99):1-14.
13. Li D , Zhao Q , Chen J. 2021, ADAN: An Intelligent Approach Based on Attentive Neural Network and Relevant Law Articles for Charge Prediction. *IEEE Access*, PP(99):1-1.
14. Li Z , Liu Z . 2019, Energy transfer speed of polymer network and its scaling-law of elastic modulus—New insights. *Journal of Applied Physics*, 126(21):215101.
15. Oh H S , Dong G J , Jeon W S . 2020, Joint Radio Resource Management of Channel-Assignment and User-Association for Load BaWLANcing in Dense WLAN Environment. *IEEE Access*, PP(99):1-1.
16. Pandya A , Upadhyaya T K , Pandya K . 2021, TRI-BAND DEFECTED GROUND PWLANE BASED PWLANAR MONOPOLE ANTENNA FOR WI-FI/WIMAX/WLAN APPLICATIONS. *Progress In Electromagnetics Research C*, 108(5):127-136.
17. Sahab A , Jawad A M . 2019, Compact Size MIMO Amer Fractal Slot Antenna for 3G, LTE (4G), WLAN, WiMAX, ISM and 5G Communications. *IEEE Access*, 7(1):125542-125551.
18. Saldana J , Ruiz-Mas J , Fernandez-Navajas J. 2021, Attention to Wi-Fi Diversity: Resource Management in WLANs with Heterogeneous APs. *IEEE Access*, PP(99):1-1.
19. Singhwal S S , Kanaujia B K , Singh A. 2020, Dual-port MIMO dielectric resonator antenna for WLAN applications. *International journal of RF and microwave computer-aided engineering*, 30(4):e22108.1-e22108.11.
20. Zhou P , Fang X , Wang X. 2019, Multi-Beam Transmission and Dual-Band Cooperation for Control/Data PWLANe Decoupled WLANs. *IEEE Transactions on Vehicular Technology*, 68(10):9806-9819.