Table of Contents

The Shortcomings of IPv6 and Upgrade of IPv4

Wang Tao
Shanghai Lizard Craft Technologies Co., Ltd.,
The visiting professor of Minzu University of China
e-mail: unsnet@163.com

Gao Jiaqiong
Sichuan Vocational and Technical College
Suining, 629000, China
e-mail: 516719510@qq.com

***Abstract*—IPv6 is to solve the problem of IPv4 address exhaustion, with the development of the Internet of things, big data and cloud storage and other technologies, these technologies are gradually applied in recent years, the continuous development of new technologies application show that the IPv6 address structure design ideas have some fatal defects. This paper proposed a route to upgrade the original IPv4 by studying on the structure of IPv6 "spliced address", and point out the defects in the design of IPv6 interface ID and the potential problems such as security holes.**

Keywords-IPv6; Spliced Address; Interface ID; IPv4 Upgrading

IPv6 is a solution to the problem of running out of IPv4 addresses. In other words, it is to upgrade the IP address because the original number of IPv4 addresses is not enough to assign to more computers. The first version of IPv6 appeared in 1995, at that time the internet is in its infancy, with the development of Internet of things, big data and cloud storage technologies being gradually applied in the last decade, IPv6 has certain defects in the design of its address structure by the continuous development and application of new technologies.

Although at that time, it was believed that IPv6 adopted 128-bit address, which was large enough to meet people's large demands, so it integrated the information of the physical layer and the application layer, confused the network layer, and formed a peculiar "splicing address" structure, thus bringing potential problems such as unresolved security vulnerabilities.

I. IPV6 CONFIGURATION

IPv6is abbreviated of Internet Protocol Version 6, also known as the next generation Internet Protocol, it is a new IP Protocol designed by the Internet Engineering Task Force (IETF) to replace the current IPv4 Protocol.

A. The architecture of IPv4

IPV4 is represented in 32-bit binary. Which divide into 4 group data with symbol ". ", each group of numbers is 8 bits of binary, from 00000000~11111111, converted to decimal is 0~255, different computers on the Internet have different IP addresses; the address format for IPv4 is for example 192.168.10.1.

B. The architecture of IPV6

The difference between IPV6 and IPV4is their binary bits, IPv6 USES 128-bit binaries, which are represented in hexadecimal. Segments are separated bysymbol ":", and 128-bits are usually divided into eight groups of four hexadecimal digits.

C. Subnet prefix address

IPv6 addresses have been assigned a number of special to purpose USES, such as：

Unspecified address ::/128

Loopback address ::1/128

Multicast address FF00::/8

Address of local join FE80::/10

In addition, the body of an IPv6 address can be aggregation as "global unicast addresses" with prefixes ranging from 001 to 111.This unicast address adopts the basic mode of "subnet prefix" plus "interface ID", and "aggregation of whole network unicast address" adopts the mode that the subnet prefix and interface ID each occupy 64 bits for allocation.

In the case of IPv6 version RFC2373, the details of its allocation are as follows：

| 3| 13 | 8 | 24 | 16 | 64 bits |

+--+-----+---+--------+--------+-----------------------

------+

|FP| TLA |RES| NLA | SLA | Interface ID |

| | ID | | ID | ID | |

+--+-----+---+--------+--------+-----------------------

------+

Where

FP 001-111: Format Prefix (3 bit) for Aggregatable Global Unicast Addresses

TLA ID: Top-Level Aggregation Identifier

RES: Reserved for future use

NLA ID: Next-Level Aggregation Identifier

SLA ID: Site-Level Aggregation Identifier

INTERFACE ID: Interface Identifier

D. IPv4-IPv6 Each other

In order to achieve IPv4 and IPv6 connectivity, IPv4 addresses are embedded into IPv6 addresses, which are often expressed as: X:X:X:X:X:X:d.d.d.d, the first 96b USES a colon to separate the hexadecimal, while the last 32b address USES IPv4's dotted decimal, for example::192.168.0.1 and ::FFFF:192.168.0.1 are two typical examples.

E. The specific address

Special addresses include an unspecified address and a loopback address. An unspecified address (0:0:0:0:0:0:0:0 or ::) is used only to indicate that an address does not exist. This is equivalent to IPv4 not specifying the address 0.0.0.0.

An unspecified address is usually used as the source address of a packet trying to verify the temporary address is unique, and is never assigned to an interface or used as a destination address. The loopback address (0:0:0:0:0:0:0:0:0:0:0:1 or ::1) is used to identify the loopback interface and allow nodes to send packets to themselves. This is equivalent to the IPv4 loopback address of 127.0.0.1. Packets that sent to the loopback address are never sent to a link or forwarded via an IPv6 router.

II. IPV6 "SPLICE CODING" STRUCTURE

IPv6 addresses are 128 bits long, and the IPv6 address space is commonly referred to as 128 bits. But that's not true, because IPv6's address structure is designed in such a way that the address space is not 128-bit as one might expect. To understand the structure of IP addresses, it can be reference with E.164 phone Numbers, The phone number structure is "country code + area code + phone number", and three different codes represent different levels.

In IPv4 addresses, the structure is "network ID (different lengths addresses of A, B, C, D, E) + host ID".In unicast address IPv6is widely used, it also seems to be a similar to IPv4 "network ID +host ID" structure, and IPv6 network ID are changed into finer three layers, and is a fixed length subnet prefix: "top polymerization ID + secondary polymerizationID + site level polymerizationID, and the host ID of IPv4 becomes a fixed 64 bit length "interface ID".

On the surface, such a design is in line with the general address structure design law.The problem is that it is needed to"layering” in terms of the most general communication protocols and the most

common communication structure USES seven-layer protocols.Different levels of tasks should be assigned to different levels of the protocol to complete, and the different protocol layer should be transparent.

Since IPv6 designers thought the 128-bit address was too rich, and if IP addresses need to be upgraded, then it's better to take the opportunity to solve more problems. As a result, IPv6 addresses have been heavily adulterated with other protocol layers that should not be considered by the IP address layer, leading to a series of fatal consequences. In principle, IP addresses should belong to the network layer protocol, which should be transparent with the physical layer and the application layer, but IPv6's design of two large address segments mixes the physical layer address and the application layer. In fact the two addresses adopted different addressing and distribution system design, this is a very strange design, and makes the IPv6 is not a single address, it is a bit like the six post code with 13 personal ID number, the two separate coding directly spliced together to form " splice coding".

A. IPv6 Interface ID

The IPv6 interface takes RFC4291 as an example and is described below : ModifiedEUI-64 format-based interface identifiers may have universal scope when derivedfrom a universal token (e.g., IEEE 802 48-bit MACor IEEE EUI-64 identifiers [EUI64]) or may have local scope where a global token is not available (e.g., serial links, tunnel end-points) or whereglobal tokens are undesirable (e.g., temporary tokens for privacy [PRIV]).

The interface ID is resolved according to a network-wide unique identity other than the IPv6 protocol. Typically, a networkunique 48-bit (actual length is 47 bits) length MAC address is used to generate or 64-bit length IEEE eui-64 identifiers.It is also possible to obtain locally unique identifiers in the case that the globally unique identifiers are difficult to obtain. It can also get a private policy without having awhole network unique identity.

There are three ways to generate the interface ID in the case of no physical address: Manual configuration; Generate a random number; Use the node ordinal.

In this design, the name "interface ID" clearly indicates that its fundamental purpose is to use the terminal physical address to establish this part of the code. The most common design principle is that physical addresses need to be globally unique. Moreover, in the IPv6 environment, the network-wide uniqueness of the interface ID is also has great value.This is mainly reflected in the following two aspects:First, it can support mobile needs well. If the physical address is not unique, they will produce IPv6 addresses that are indistinguishable and conflict, when the two terminal devices with the same physical address arrive at the same portandthe whole system will collapse if there are too many conflicts; the second consideration is security. It is through the whole network unique physical address to determine the identity of the terminaluniquely.

According to the above analysis of IPv6 address, it can be seen that the protocol will have the following serious problems.

B. IPv6 address allocation

Let's imagine, if a telecom operator has applied for a batch of subnet prefixes, how will it use these subnet prefixes for network planning and distribution?

For example, a mobile operator M can use its top aggregation ID to plan provinces or municipalities, its secondary aggregation ID to plan cities and urban areas, and its site aggregation ID to plan each base station and sector.What does that mean?When a mobile phone user generates its IPv6 address, the address information clearly shows the province or municipality, the city and the urban areawhere the user is located, up to the subnet prefix number such as base station and carrier-cell.

If a user visits the web site GOOGLE, then GOOGLE can easily obtain the network topology on the path of mobile operator M and even accurately locate the base station and sector on the user's location.If it were just a message, it wouldn't mean much. However, after a large number of users visit GOOGLE network, the website can quickly restore all network topologies of the entire operator M, including the location of the base station, sector direction, carrier frequency number and even network performance through big data analysis.

Of course, it is not technically impossible to counter this problem. Operator Mcould allocate Subnet prefixes randomly or even dynamically. However, this dynamic adjustment cannot be carried out casually, especially when the business is relatively large, the adjustment will cause a large number of business interruption for a certain period of time.And IPv6 makes such a design for subnet prefixes is purpose to greatly improve routing efficiency at beginning.The more consistent the address planning is with the network topology, the simpler the routing table is, and the routing can be done based only on address information at the partial subnet address prefix.It is somewhat similar to MPLS (Multi-Protocol Label Switching) in the IPv4;the partial hierarchical address in the subnet prefix is a mark that can aggregate IPv6 packets within the subnet for exchange. This is really good for routing efficiency and QoS enhancement.

This is why the address of the subnet prefix is called “aggregation”. If the subnet prefixes are not assigned according to the network topology but randomly, the fundamental benefit of aggregationwill lost.If only from the view of IP routing itself, IPv6 can be aggregated subnet prefix design is indeed a very prominent advantage, to improve the routing efficiency and enhance QoS is indeed beneficial. However, in the era of big data and mobile phone positioning has been popularized, this advantage may face serious security problems at the same time.When the number of users in M network is large to a certain extent, the big data could analysis the M network topology in a very short time even if random or even dynamic subnet prefix allocation is adopted for websites, especially those with very concentrated visits like GOOGLE.

C. E.164 and IPv6

The different levels of the telephone number structure also contain network topology information in E.164,Why would IPv6 have such aeffect when E.164 Numbers don't?The reason is that E.164 serves the telephone of fixed-line network. When the number is fixed, even if the phone number is known through the caller, there is no location information and the corresponding network topology cannot be determined.

By talking to each other at point-to-point, onecanonly know the other's number, and it is rare for all users to make frequent calls to a service point.Moreover, most cases telephone network is voice service rather than data service, with little big data analysis ability.

Caller’s information is an active service provided by telecom operator. If the telecom operator does not want the other party to know the call information, it cannot provide. If the user does not move, it is difficult to accurately distinguish the boundary point between the station number and the user number.

However, IPv6 is completely different. The technologies of "user mobility, especially those with fixed interface ID", "big data", "mobile location", "cloud computing" together make the network topology of operators using IPv6 completely transparent.Because the mobile phone can be accessed through fixed networksuch as Wi-Fi, the network architecture of fixed-line telecoms operators can also be easily cracked, not only does GOOGLE have this capability, but any IPv6 Internet site with a slightly larger user can have it.

The first version of IPv6 was RFC1884, released in December 1995, before the concept of big data and the

advent of the World Wide Web, the first popular browser Mosaic1.0 was developed outin November 1993, before GOOGLE was even founded, today's technology was never expected. Although IPv6 protocol has changed many times, such as RFC2373 was releasedin July 1998, RFC3513 in April 2003 and RFC4291in February 2006, the latest standard for interface ID design is RFC8064, which was released in February 2017.

D. IPv4 and IPv6

IPv6 embeds the physical layer of information into the basic design idea of IP address, which cannot be changed once it is first formed, only the details.For example, interface ID can not only use MAC address as the global unique address tool, but also can use other more physical layer address.

Why IPv4 does not have this problem but IPv6 have?Since IPv4 is purely a network-layer address, the IPv4 addresses of the various network topologies of telecom operators are mainly used just within the network, and the communication host (the information receiving terminal) will not know these addresses.In the telecom operator network, each node of the topology has a corresponding physical layer address, including the base station and sector number. They are only used within the operator's network;this information will be stripped awayonce out of the operator's network, the other side of the communication terminal would not getthisinformation.

IPv6 conflates all physical addresses with IP layer addresses, and both sides of the communication generally know the other's entire IP address information, because a complete IP header contains both sides of the communication's IP address information. The physical layer information of the telecom operator is completely exposed in the IP address information, equivalent to streaking.

A telecom operator's network topology and network performance is one of its core trade secret, if the operators understand the consequences of IPv6, and are willing to accept it?

III. IPV6EXPOSES INFORMATION

A. Operator information transparent

In the IPv6 address application process, the entire IP address segment is not applied like IPv4.IPv6 operators can only apply for the first 64-bit subnet prefix address, the latter of 64-bit interface ID is completely another set of allocation rules, which is not subject to the management and control of operators. Address allocation rules of different structural segments are completely different. In fact, the mechanism of the allocation rules for different segments of telephone numbers in E.164 is also different. The ITU assigns a country or region code to each country and each country assigns its own area code and operator codes to each city. And then operator assigns its own numbers to users.

IPV6 is a bit of the other way around. The subnet prefix is applied in bulk, and the specific encoding is assigned by the operator itself, while the interface ID in the back is not managed and assigned by the operator.A bit like a telephone network where the area code is assigned by the operator and the user number is not managed and assigned by the operator. It's a little of confusing.

B. Users information naked

Interface technologies of IPv6 not only make telecom operators information transparent, but also have huge security risks for users. The interface ID corresponds to the terminal user address. In general, this address is a MAC address and other physical address according to certain rules generated.Once a user communicates in this way, the other party can easily restore the user's MAC address from the interface ID according to IPv6 rules.

MAC addresses are equivalent to a user's Internet ID. It's too bad that when a user visits a navigation site, the site is tracking them all the time.To make matters

worse, people who don't understand Internet technology in general, a design flaw will unwittingly use MAC addresses to generate their own interface ID, while IPv6 allows for other methods, even random and manual.What is the result of it? Hackers, professional users, and others can know how to use these methods to be anonymous, and forming "anonymous or invisible IPv6 users."Thus IPv6 classifies users into "citizens" and "incognito" by whether their interface ID has a unique physical address for the entire network.Websites such as GOOGLE, BAIDU, TENCENT, and ALIBAB, which are likely to be widely used by all Internet users, can be easily analyzing their MAC addresses in IPv6 addresses and developing corresponding software for big data analysis.This causes the real-time monitoring of user traces and behavior.

What happens once the problem is widely recognized, especially after a safety incident? Most users require their interface ID to be anonymous, invisible, or even constantly changing. This will result in the generation of interface ID from unique physical addresses across the networkeventually be discarded.In essence, the interface ID must be unique in the whole network, and the only way to ensure the uniqueness of the whole network is uniform allocation of the whole network and fixed address.Other methods, especially the interface ID randomly generated by hackers, cannot be distributed across the whole network.

Conflict detection is also only carried out within a site, at most within the site covered by the same sub-aggregation ID, and cannot be carried out across the network.Now IPv6 is not widely available, so there is no sense of the problem. However, as the number of IPv6 users on the Internet increases, the chance of interface ID conflicts will increase.This is equivalent to all users in the world are random or give their own 64 bit interface ID; then address conflict will be more and more likely.

C. Huge design safety hazard

Communication security is similar to the process of the battle between the offensive and defensive sides in the war. The security evaluation of the same technology is completely opposite to that of the two sides.The security of communication technology is also evaluated in the opposite way for different stakeholders.The stakeholders involved in the communication system include not only the two sides of the communication, but also the security supervision of the communication system by the sovereign and the detection of potential hackers.

If the communication process can be monitored, it is not secure for the communicator, but it is more secure for the monitoring party.If the communication process is encrypted and cannot be monitored by the third party, it will be more secure for both sides of the communication, but there will be information security problems for the sovereign country.Therefore, any communication security technology will not bring security benefits to everyone at the same time.In this way, it is inevitable that the security of communication should be solved in the application layer, rather than in the IP layer, that is to say, the IP layer should be neutral or in terms of security.Because the IP layer is the most fundamental protocol for network communication, security technology designed at this level will easily cause permanent damage to the security of some network stakeholders.

Anonymity was once an advantage of the Internet, but the utter inability to identify users led to a proliferation of hackers.IPv6 tries to provide a solution to communication security in the IP layer, which is mainly reflected in two aspects:First, IPv6 address design USES the interface ID setting, which provides to confirm the physical terminal of the other party.Second, IPv6 also adds authentication header AH and encapsulated security data header (ESP) to its extensions.

These security designs provide a variety of security services: (1) verify the data source identity.This is through the use of hash technology to digital signature; (2) keep the data transmission process secret.If tunnel mode is used, not only the transmitted data can be kept secret, but even the IP packet header can be.

To understand the problems with the above design, we can consider the case of INTEL's CPU security design.INTELCompany once wanted to add globally unique serial Numbers to its CPUs to increase so-called security.But the design was so strongly opposed that it locked down the world's PC users that it had to be scrapped.

IPv6 interface IDis designed to add even more serial Numbers than CPU.Because the serial numbers in the CPU also need special software to enable, not just anyone can use, and once added to the CPU serial Numbers, all CPUs will have, and we are all equal.But IPv6's interface ID allows "citizen users" to send their IP packets to each other in the process, giving them the MAC address of their terminal in the first place at the first time.This is equivalently to putting one’sID number on his forehead and revealing your identity in all correspondence.

As people living in society, they have to accept that their identity is disclosed in many cases, for example, showing one's identity card when travelling by plane or train.But if you just go to the supermarket to buy a bottle of water, to the restaurant to eat a meal, isitneeds to show ID? However, IPv6 actually requires all IPv6 users to perform any service online under all conditions before showing their ID. Is it socially acceptable?

If the people can't accept INTEL Companyadding a unique global serial number to the CPU, it's hard to understand why it can accept IPv6's interface ID design.Now that IPv6 is not widely used, people simply don't understand what IPv6's interface ID is and won't accept it once they understand and have problems with it.

In the IPv4-based Internet, if a hacker attacks a user, it is possible to find the location of the attack by using an IP address.But if the tunneling of a secure gateway in IPv6 is adopted by hackers, it is impossible to verify the data packets from the Internet.If the tunnel method is adopted by the spy agencies and criminals of hostile countries, it will be difficult for the security agencies to track their activities.Not only was it unclear what the other side was communicating with, it was unable to find out the address and how to tell the packets from each other.Can it be accepted as a sovereign country?

In fact, all the IP layer has to do is do a good job on the IP layer. The security problem to be solved by the IP layer should be limited to the correctness and reliability of the data itself, that is, how to accurately, reliably and efficiently transfer the data from the source to the terminal and the problem that should not be solved by it will not be considered. The problem of confusing the network level with IPv6 in terms of security is a permanent and insurmountable harm to the network operators, the vast of users, and national communications bodies, which is clearly unacceptable.

IV. ABOUT THE IPV4 ADDRESS SPACE

A. NAT and SDN

The IPv4 address space exhaustion problem does not exist. This may be a very shocking conclusion, but it is a real objective reality.The IPv4 address space is not commonly known as a 32-bit address space.Because of the use of NAT(Network Address Translation) addresses, IPv4 addresses are in fact vastly expanded. It's just like an extension number in a telephone network.How much can theIPv4 address spaceextend?

NAT addresses use three different types of network ID.

Class A addresses: 10.0.0.0 to 10.255.255.255,

Class B addresses: 172.16.0.0 to 172.31.255.255

Class C addresses: 192.168.0.0 to 192.168.255.255

Even in class C addresses, a public IPv4 address can extend to 65,535 NAT IPv4 addresses. In fact, the problem of insufficient IPv4 addresses is far less serious, even from purely IPv4 public addresses.As the number of Internet users approaches the total, the consumption of IP addresses will slow down.As long as there are two orders of magnitude more theoretical space than IPv4, the address space is sufficient.

Years ago we used to hear about phone Numbers going up, but we haven't heard about that for years. The reason is that on the one hand, due to the development of mobile technology, the number of fixed-line telephone users increases to a certain extent and then declines, no longer requiring more number resources.NAT addresses have the potential to extend by four orders of magnitude with minimal class C addresses. The potential is even greater if class B or even class A addresses are adopted.

To be more precise, NAPT is now commonly used, with the port number of the NAT gateway IP address used as a mapping for temporary TCP/IP links, which will have a port number limit of 2 bytes and 16 bits (65,535). There is a better way to solve this limitation.Wang Tao, the author of this article, has designed a patent technology of super IPv4, which can well solve this problem.

In addition, with the current SDN (Software Defined Network) technology, it is also easy to solve the NAPT port number limit problem.None of these technologies are complex and are truly IPv4 compatible;it is almost extending the IPv4 address space infinitely.

They all require a simple software upgrade of the edge router and the terminal TCP/IP section, no IPv6 required. So, from the address space alone, IPv6 is a lot of it, and a lot of nothing.

B. IPv4 smooth upgrade

IP address is the basic protocol of the Internet, and it is extremely difficult to solve the problem through complete and thorough replacement.The original designers of IPv6 didn't do much research on this, and decided that the 32 address space problem with IPv4 could not be solved by a smooth upgrade, so it was easy to redesign it entirely from scratch.We only have to look at one more technology case to know how important it is to upgrade smoothly in the web space, and how much effort it worth to do so.

Television technology was originally black and white, and in order to develop color TV, the difficulty to overcome was not how to realize the color TV itself, but how to make the past black and white TV network compatible and smooth upgrade. In other words, black and white TV transmission equipment can be compatible with color TV signals. The original black and white TV can receive and display color TV signals (although it is still black and white), and the new color TV can also receive the original black and white TV signals.

To solve this problem, the color signals of the three primary colors are separated into brightness signals (equivalent to black and white TV signals) and chromaticity signals, which are mixed together by a comb spectral arrangement and separated by a comb filter at the receiver end. It took more than 30 years for the industry to crack all the technical problems. It can be said that color TV system is the peak of technical complexity in analog circuit era. However, once the problem of smooth upgrades was solved, color television soon became widespread.

In the same way, compatibility and smooth upgrading of new communications technologies with existing technologies are important to their success.

C. From IPv4 to IPv6

Because IPv6 tried to bypass the problem of smooth upgrades, it took more than 20 years to extensive promotionwithno hope of real popularity. Till now still want to rely on executive order to make IPv6 forcibly popularize.Due to the large number of Internet users

around the world, if you want to achieve IPv4 to IPv6 conversion, it is impossible to complete all the users at the same time;it must be a very long transition period.In the conversion process, if only part of the users adopt IPv6, whether using tunneling mode or dual stack mode for compatibility, the users using IPv6 is actually equivalent to a private network in IPv4, and all its assumed technical advantages cannot play out.In that case, why not just use IPv4's NAT network instead? IPv6 has now become a political and technical issue in the world of communications, with all operators and users daring to oppose it, even seeming to support it, but not actively embracing it.

Some people think that the Internet of things is the most suitable for IPv6, it is all decided viewpoints, NB-IOT terminal communication in low frequency, low rate, almost no requirement of communication performance, the NAT technology is the most appropriate, use an IPv4 public address and class A private network address to expand the number of millions of Internet of things terminal.If it is not used on a large scale, the potential technical defects of IPv6 in network devices will not be discovered, and users who adopt IPv6 in the first place may encounter many problems with poor service. It won't really work until all users adopt IPv6.

V. CONCLUSION

The Internet based on IPv4 also has many security problems, but people have adapted to it, or made up for it with other technologies, which is a bit ofpessimistic to say.So, even if we don't consider IPv6 huge security problems, if it really can spread so we are also welcome, but because its span is too big to smooth upgrade, IPv4 is simple and effectively enough to solve all IPv6 want to solve the problem at the same time, and IPv6 itself poses far more security problems than it solves.All of the people in the world support it on the surface, and even agree that it is the most ideal technology, but after 100 years, it cannot be popularized. For this reason, the whole society will never end up wasting a lot of resources unnecessarily for a technology that cannot be popularized at all. Don't assume that all technology changes for the better. Who wants their zip code to keep changing?

ABOUT THE AUTHOR

Wang Tao, the CEO of Shanghai Lizard Craft Technologies Co., Ltd., an independent director of Yunnan Aluminum Co. Ltd. (000807), a Management consultant of Zhejiang Uniview Technologies Co., Ltd., and the visiting professor of Central University for Nationalities. Nanjing University of Posts and Telecommunications, graduate student of Beijing University of Posts and Telecommunications. Former Vice President of ZTE (000063) International Market, General Manager of Sumavision (300079) International Market, President of Global Investment. He has won five invention patents for network technology, published such academic monographs as "the Manifesto of Communicast Network", "Beyond War", "the Population Theory of Ecological Society", "The Upcoming World War for Food", "EV Rule All the Land", "Experiment, Measure and Science", "Principles of Scientific Economics". He was the chief editor of the training textbook "Marketing and Strategy" which has been used in ZTE's internal marketing leading cadres.

REFERENCES

[1] R. Hinden, S. IP Version 6 Addressing, IP Version 6 Addressing Architecture, Deering, Network Working Group.RFC2373.1998, 07.

[2] R. Hinden, S. Deering. IP Version 6 Addressing Architecture, Network Working Group.RFC-4291. 2006,02.

[3] R. Hinden, S. Deering. IP Version 6 Addressing Architecture, Network Working Group.RFC-3513. 1998.07.

[4] S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6)-Specification, Network Working Group. RFC-1883, 1995.12.

[5] R. Hinden, S. Deering, IP Version 6 Addressing Architecture, Network Working Group. RFC-1884, 1995.12.

[6] F. Gont, A. Cooper, D. Thaler, W. Liu. Recommendation on Stable IPv6 Interface Identifiers, Internet Engineering Task Force (IETF), RFC-8064,2017, 02.

Research and Design of Next Generation Internet (IPV9) Datagram

Wang Zhongsheng
[1.]State and Provincial Joint Engineering Lab. of Advanced Network, Monitoring and Control, China
[2.]School of Computer Science and Engineering
Xi'an Technological University
Xi'an, China
e-mail: wzhsh1681@163.com

Lin Zhao
[1.]Chinese Decimal Network Working Group
Shanghai, China
[2.]Shanghai Decimal System Network Information Technology Ltd.
e-mail: chinalinzhao@126.com

Xie Jianping
[1.]Chinese Decimal Network Working Group
Shanghai, China
[2.]Shanghai Decimal System Network Information Technology Ltd.
e-mail: 13386036170@189.cn

Zhong Wei
[1.]Chinese Decimal Network Working Group
Shanghai, China
[2.]Shanghai Decimal System Network Information Technology Ltd.
e-mail: 13331860961@189.cn

***Abstract*—The current global Internet USES the TCP/IP protocol cluster. IP is the network layer protocol and the core protocol in this protocol family. The current version is IPv4 with 32-bit addresses. With the popularity of Internet applications, the limited address space defined by IPv4 has been exhausted. To expand the address space, the Internet Engineering Task Force (IETF) has designed the next generation IP protocol, IPv6, to replace IPv4. IPv6 redefines the address space, using a 128-bit address length that provides almost unlimited addresses. However, with the development and application of the Internet of things, big data and cloud storage, IPv6 has some shortcomings in its address structure design, security and network sovereignty, so it is urgent to develop a new generation or future internet with security and reliability, autonomy and controllable , and it becomes a research hotspot in the world.**

This paper developed a new generation Internet (IPV9) datagram by researching the existed IPv4 and IPv6, and it is based on the method of assigning addresses to computers connected to the Internet by full decimal character code which designed by the Chinese Decimal Network Working Group with the leader of Xie Jianping. It is a subsequent version with RFC1606, RFC1607, a new generation of network data structure, it is not the updating of IPv4 [RFC - 791] and IPv6 [RFC - 1883], [RFC - 2464], it is a new vision to demonstration and testing.

Keywords-Future Network; IPv4; IPv6; IPV9; Datagram

A datagram is the basic unit of data transmitted on the network. It contains a header and the data itself, in which the header describes the destination of the data and its relationship to other data. Datagram is a complete and independent data entity, which carries the information to be transferred from the source computer to the destination computer and does not rely on the previous exchange between the source and the destination and the transmission network [1]. TCP/IP protocol defines a packet that is transmitted on the Internet; called IP Datagram, which are the network layer protocol and the core protocol of the TCP/IP protocol family.

IP is a virtual package consisting of a header and data. The IPv4 header is a fixed length of 20 bytes, which is required for all IP datagram. After the fixed portion of the header are optional fields whose length is variable. Both the source and destination addresses in the header are IP protocol addresses. The current global Internet USES the TCP/IP protocol cluster, the current version is IPv4 with 32-bit addresses. With the popularity of Internet applications, the limited address space defined by IPv4 has been exhausted. To expand the address space, the Internet Engineering Task Force (IETF) has designed the next generation IP protocol, IPv6, to replace IPv4. IPv6 redefines the address space, using a 128-bit address length that provides almost unlimited addresses. However, with the development and application of the Internet of things, big data and cloud storage, IPv6 has some shortcomings in its address structure design, security and network sovereignty. The Chinese researchers developed a new generation Internet (IPV9) datagram by researching the existed IPv4 and IPv6, and it is based on the method of assigning addresses to computers connected to the Internet by full decimal character code. It is a subsequent version with RFC1606, RFC1607, a new generation of network data structure, it is not the updating of IPv4 and IPv6, it is a new vision to demonstration and testing.

I. OVERALL DESIGN OBJECTIVE

In order to be compatible with the existing Internet system, on the basis of studying the existing standard IPv4 [RFC -791] and IPv6 [RFC -1883] and [RFC -2464], the overall goal of IPV9 datagram design is formulated.

1) Extended address capacity

IPV9 increases the length of IP addresses from 32 (IPv4) and 128 (IPv6) bits to 2048 bits to support more address hierarchies, more addressable nodes, and simpler automatic address configurations. It also increases the IPv4 32 bit address length reduced to 16 bits, in order to solve mobile communication.

2) Variable length and uncertain number digits

In order to reduce the network overhead, this datagram designing adopts the method of indefinite length and uncertain number of digits. By adding a "range" field to the multicast address, the scalability of multicast routing is improved. It defines a new address type, "any broadcast address," for sending datagrams to any one of a set of nodes.

3) Simplify and improve header format

Some IPv4 header fields have been eliminated or made optional to reduce the overhead of common processing on packet control and to limit IPV9 header bandwidth overhead. The encoding of header options has been changed to allow more efficient forwarding, reduce restrictions on the length of options, and gain more flexibility to introduce new options in the future.

4) Label data streams

To attach labels to data streams belonging to a particular data communication, the sender may require special processing of these data streams, such as non-default quality of service or real-time service, such as using virtual circuits to achieve the purpose of circuit communication.

5) High safety and reliability

To get security and reliability, the new datagram added expansionary support for IP address encryption and authentication, data integrity, and data security (optional) in IPV9 designing. It extension headers and options take into account the length of packets, the semantics of flow control labels and categories, and the impact on high-level protocols.

6) Direct routing addressing

The ICMP (Internet Control Message Protocol) version of IPV9 contains all the requirements for implementing IPV9. The function of route character arrangement authentication, recognition and addressing is added, which reduces the routing cost and improves the efficiency.

7) Compatible with IPv4 and IPv6

In order to ensure a smooth transition from IPv4 to IPV9, considering the protection of the original investment and not changing user habits, this datagram defines IPV9 header and transitional header. The last segment address is used for the header of IPv4 or IPv6 is used, but the version number is changed to 9, the connection protocols used are IPv4 or IPv6.

8) The virtual and real circuit design

In order to smoothly transmit voice, image and video and other big data real-time applications, it is necessary to adopt long-stream code, absolute value, return code and other technologies, and adopt three-layer and four-layer network hybrid architecture. Three-layer and four-layer network hybrid architecture design should be implemented in virtual and real circuits.

II. GENERAL DESIGN OF SYSTEM

A. Some basic terminologies

The basic concepts in system designing are defined as follows.

1) Node: a device installed with IPV9 or IPV9 device compatible with IPv4 and IPv6.

2) Router: the device that is responsible for forwarding and explicitly not sending IPV9 data to itself.

3) Host: any node that does not belong to the router.

4) Upper agreement: Protocols located in the layer above IPV9. For example, transport layer protocols TCP, UDP, a communication facility or medium in the link layer, on which nodes can carry out link-layer communication, that is, the layer just below IPV9. Examples of links include Ethernet (or bridged), PPP links, X.25, frame relay, or ATM networks.

5) Neighbor: each node connected to the same link.

6) Interface: node to link connection.

7) Address: IPV9 layer identifier of an interface or a group of interfaces.

8) Packet: An IPV9 header plus load.

9) Link MUT (Maximum Transmission Unit): the Maximum Transmission Unit that can be transmitted on a section of link, namely the Maximum data packet length in eight-bit group.

10) Path MUT: the smallest MUT of all links in the path between the source node and the destination node.

Note: for a device with multiple interfaces, it can be configured to forward non-self-directed packets from one of its interfaces and drop from other interfaces. When such a device receives data from a previous interface or interacts with a neighbor, the protocol requirements of the host must be followed.

B. IPV9 header format

The format design of IPV9 datagram header is shown in table 1.

TABLE I. IPV9 HEADER FORMAT

<table>
<tr><td rowspan="2">Version Number</td><td colspan="4">Category Type</td><td rowspan="2">Flow Label</td></tr>
<tr><td>Address Length</td><td>Priority class Communication</td><td>Authentication Address</td><td>Absolute Communication</td></tr>
<tr><td>Payload Length</td><td colspan="4">Next Header</td><td>Hop Limit</td></tr>
<tr><td colspan="6">Source Address (16-2048 bit)</td></tr>
<tr><td colspan="6">Destination Address (16-2048bit)</td></tr>
<tr><td colspan="6">Time</td></tr>
<tr><td colspan="6">Authorization Code</td></tr>
</table>

The design of table 1 is explained below.

1) Version Number: The length is 4 bits, representing the Internet protocol version number. For IPV9, this field must be 9.

2) Category Type: The length is 8 bits, the high 3 bits are used to specify the address length, its volume is 0 to 7, and it's 2 to the power. Contains address length of 1Byte ~ 128Byte; the default value is 256 bits, where 0 is 16 bits, 1 is 32 bits, 2 is 64 bits, 3 is 128 bits, 4 is 256 bits, 5 is 512 bits, 6 is 1024 bits, and 7 is 2048 bits. The last five bits specify the communication class and authentication for the source and destination addresses. 0 to 15 is used to specify the priority class of the communication, 6 to 7 is used to specify the communication method after the first authentication, which is used by the packet sending place for control and whether the source address and destination address authentication is needed. 8 to 14 are used to specify absolute communication that will not fall back when congestion is encountered, and 15 are used for virtual circuits. 16 and 17 are used to assign audio and video, called absolute value, to ensure the uninterrupted transmission of audio and video. The other values are reserved for future use.

3) Flow Label: with a length of 20 bits, it is used to identify packages belonging to the same business flow.

4) Payload Length (Net Load Length): the length is 16 bits, including the net load byte length, that is, the number of bytes contained in the packet after IPV9 header.

5) Next Header: the length is 8 bits. This field indicates the protocol type in the field following the IPV9 header.

6) Hop Limit: the length is 8 bits, and this field is subtracted one each time a node forwards a packet.

7) Source Address: the length is 8bit ~ 2048bit, and the sender address of IPV9 packet is specified. Adopt the method of Variable length and uncertain number digits.

8) Destination Address: the length is 8 bit ~ 2048 bit, and the destination address of IPV9 packet is specified. Adopt the method of Variable length and uncertain number digits.

9) Time: it is used to control the lifetime of the address in the header.

10) Authorization Code: it is used to identify the authenticity of the address in the header.

C. Extended headers of IPV9

In IPV9 datagrams, Internet optional information is placed in specialized headers which between the packet IPV9 header and the high-level protocol header. The number of such extended headers is not too much, and each identified by a different value for the next header. An IPV9 packet can have zero to more than one extension header, each of which is defined in the next header S field in the previous header, as shown in table 2.

TABLE II. EXTENDED HEADER FORMAT

IPV9 Header Label NEXT HEADER =TCP	TCP HEADER +DATA		
IPV9 Header Label NEXT HEADER = ROUTE	ROUTING HEADER NEXT HEADER =TCP	TCP HEADER +DATA	
IPV9 Header Label NEXT HEADER = ROUTE	ROUTING HEADER NEXT HEADER = DATA SEGMENT	DATA SEGMENT HEADER NEXT HEADER =TCP	TCP DATA SEGMENT HEADER +DATA

On the path of the packet passing, no node to checks or processes the extended header until the packet reaches the node specified by the destination address field in the IPV9 header (or, if it is a multicast address, it would be a group of nodes). For the normal multiplexing of the next header field of IPV9 header, the processing module is called to process the first extended header. If an extended header does not exist, the high level header is processed. Therefore, the extension headers must be processed exactly in the order in which they appear in the packet, and the receiver cannot scan the packet to find a particular extension header and process it before processing other preceding headers.

If a node, after processing the header wants to process the next header, but it does not recognize the value of the "next header" , it will lost the packet, and sends the source a "ICMP parameter problem" message, the message ICMP code has a value of 2 (can't identify the "next header" type), "ICMP indicator" contained in the field could not identify the "next header values" offset location in the original packets. The same is done if a node finds the "next header" field is 0 in any non-IPV9 header.

Each extended header is an integer multiple of the 8-bit array so that subsequent headers can be aligned along 8-bit array boundaries. In the extended header, the fields made up of multiple 8-bit groups are internally aligned with their internal natural boundaries, that is, the position in the fields of width n 8-bit groups are placed at the beginning of the header, an integer times n 8-bit groups, where n=1,2,4 or 8.

The fully installed IPV9 includes the following extension headers:

- Hop-by-Hop Option(segment options)
- Routing（type 0）
- Fragment;
- Destination Options;
- Authentication;
- Encapsulating Security Payload.

This paper defines the first four extension headers, and the next two additional definitions.

1) The sequence of extension headers

When multiple extension headers are used in the same packet, they appear in the following order:

a IPV9 header;
b segment options header;
c Destination options header(annotation 1);
d Routing header;
e Data segment header;
f Authentication header;
g Encapsulate security load header;
h Destination option header(annotation 2);
i The upper header;

Annotation 1: Options for the first destination node to appear in the IPV9 destination address field and for subsequent destination nodes listed in the routing header.

Annotation 2: The option to be processed only by the destination node of the packet.

Each extended header can occur at most once, but destination option headers can occur at most twice, once before routing headers and once before high-level headers.

If the high-level header is another IPV9 header (that is, when IPV9 is encapsulated in another IPV9 tunnel), it can be followed by its own extended headers, which, as a whole, follow the same sequence.

When defining other extended headers, it must specify a sequential relationship between them and the headers listed above

2) Options

When the extension header is defined the segment-by-segment option and the destination option header have an unequal number of options encoded in the form of Type length value (TLV). The format is shown in table 3.

TABLE III. OPTION FORMAT

Option Type	Option data length	Option data

Where,

Option type: 8-bit identifier.

Option data length: 8-bit unsigned integer. It is the length of the data field for this option, in 8-bit groups.

Option data: Variable length field, the data is related to the option type.

The order of the options in the header must be handled in strict accordance with the order in which they appear in the header. The receiver cannot scan the header for a particular type of option and cannot process it before processing all previous options.

The option type identifier is internally defined, and its highest two bits specify what must be done if the node handling IPV9 cannot identify the option type.

00: Skip this option and continue with the header.

01: Abandon the packet.

10: Abandon the packet and send a "ICMP parameter problem, code 2," message to the source address, regardless of whether the destination address is a multicast address, indicating that the option type is not recognized.

11: Abandon the packet. Only when the destination address of the packet is not a multicast address, send a message of "ICMP parameter problem, code 2" to the source address, indicating the type of option it cannot recognize.

The high third bit of the option type specifies whether the data for this option can change on the way to the destination of the packet.

0: Option data cannot be changed during transport.

1: Option data can be changed during transport.

When the authentication header appears in the packet, when calculating the authentication value of the packet, the whole field in which any data can change in the way is treated as an 8-bit group of all zeros.

Each option can have its own alignment requirements to ensure that the values of multiple 8-bit groups in the option data field fall to the natural boundaries. The alignment of the choices is required in terms of Xn+y, the option type must be an integer multiple of x 8-bit groups plus y 8-bit groups from the beginning of the header. Such as:

2n means the offset is any multiple of two 8-bit groups from the beginning of the header.

8n+2 means the offset is any multiple of eight 8-bit groups from the beginning of the header plus two 8-bit groups.

3) Pad option

a) Pad1 option(Alignment requirement: none)

0

Notice: the format of the Pad1 option is a special case where there is no length field or value field. The Pad1 option is used to insert an 8-bit group of fill bits in the header option field.

b) PadN option

If need to fill out multiple 8-bit groups, it should be used the PadN option instead of multiple Pad1 options. The PadN option format (alignment requirement: none) is shown in table 4.

TABLE IV. PADN OPTION FORMAT

1	Option data length	Option data

The PadN option inserts two or more 8-bit groups of fill bits into the header option field. To fill in N 8-bit groups, the value of the option data length field should be N-2, and the option data field contains N-2 all-0 8-bit groups.

4) Segment options header

Segment options header is used to carry the option information that must be checked and processed by all nodes on the path the packet travels through. In IPV9, the header of each network segment option is represented by the value of the next header is 0, as shown in table 5.

TABLE V. SEGMENT OPTIONS HEADER FORMAT

Next header	The extension length of the header	
Options		

Next header：It's an 8-bit selector. It is used to identify the header type just following the each segment header option. It is the same value as the IPv4 protocol field [rfc-1700].

The extension length of the header: It is an 8-bit unsigned integer. The length of the header of each segment option, in 8-bit groups, does not include the first 8-bit group.

Option: variable length field whose length makes the length of each segment header an 8-bit integer multiple. It contains one or more TLV encoding options.

In addition to the Pad1 and PadN options specified above, the large load options (alignment requirement: 4n+2) are defined, as shown in table 6.

TABLE VI. LARGE LOAD OPTION FORMAT

	194	Option data length
Heavy load length		

The large load option is used to send IPV9 packets with a load length of more than 65,535 8-bit groups, the large load length is the length of the packet, in 8-bit groups, excluding IPV9 headers but including segment option headers, it has to be greater than 65,535. If a packet with a large load option is received and the large load length is less than or equal to 65535, a message of "ICMP parameter problem, code 0" is sent to the source node, pointing to the high bit of the invalid large load length field.

If the packet has a large load option, the load length in the IPV9 header must be set to 0. If received a packet that contains both a payload length option and an IPV9 payload length field that is not 0, it need to send a message to the source node with "ICMP parameter has a problem, code 0" and pointing to the large payload option type field.

The large load option cannot be used in packets with segment headers. If the data segment header is encountered in the packet containing the high-load option, a message "ICMP parameter problem, code 0" will be sent to the source node, pointing to the first 8-bit group of the data segment header.

If the installed IPV9 does not support the large load option, it does not have an interface to a link with MTU greater than 65535 (IPV9 header with 72 8-bit groups, plus 4G 8-bit group loads).

5) Routing header

IPV9 USES the routing header to list one or more intermediate nodes that needs to be accessed on the path of the packet to the destination node. This function is very similar to the source routing options of IPv4. The routing header is identified by the next header field whose previous header median value is 43; the format is shown in table 7.

TABLE VII. ROUTING HEADER FORMAT

Next header	Length of the extension header	Routing type	Remaining data segment
Data related to type			

Next header: It's an 8-bit selector. It Use the same value as the IPv4 protocol field [RFC-1700].

Length of the extension header: It is an 8-bit unsigned integer. The routing header length is in 8-bit groups, does not contain the first 8-bit group.

Routing type 0: the route header variable's 8-bit identifier

Remaining data segment: It is an 8-bit unsigned integer. The number of remaining routing data segments, that is, the number of intermediate nodes explicitly listed, which are the nodes to be accessed before reaching the final destination node.

Data related to type: It is a variable length field, whose format is determined by the route type, its length makes the entire route header an integer, multiple of the 8-bit group.

If a node encounters an unrecognized routing type value while processing the received packet, the action that the node will take depends on the value of the remaining data segment field. It includes the following two cases:

a) If the value of the remaining data segment field is 0, the node must ignore the routing header and continue to process the next header of the packet. The header type is given in the header field next to the routing header.

b) If the value of the remaining data segment field is not 0, the node must abandon the packet and send a message of "ICMP parameter exists problem, code 0" to the source address of the packet, pointing to the unrecognized routing type

The format of the route header for type 0 is shown in table 8.

TABLE VIII. TYPE 0 ROUTING HEADER FORMAT

Next header	Length of extension header	Routing Type =0	Remaining data segment
Reserve	Strict/loose bit innuendo		
Address [1]			
Address [2]			
……			
Address [n]			

Next header: It is an 8-bit selector. Its identity follows the routing header type. it USES the same value as the IPv4 protocol field [RFC-1700].

Length of extension header: It is an 8-bit unsigned integer. The routing header length is in 8-bit groups that does not contain the first 8-bit group. For routing headers of type 0, the header extension length is equal to twice the number of addresses in the header and is an even number less than or equal to 46.

Routing type is 0.

Remaining data segment: It is an 8-bit unsigned integer. The number of remaining routing data segments, that is, the number of intermediate nodes explicitly listed, which are the nodes to be accessed before reaching the final destination node. The maximum effective value is 23.

Reserve: It is an 8-bit reserved field. The sender initializes it to 0, and the receiver ignores the field.

Strict/loose bit innuendo: 1 to 23 from left to right. For each routing data segment, indicate whether the next destination address must be the neighbor of the previous node: 1 indicates strict (must be neighbor), 0 indicates loose (need not be neighbor).

Address [1…..n]: It's a 256-bit address vector, value from 1 to n.

Multicast addresses cannot appear in routing header packets of type 0 or in routing header packets of type 0 in the destination address field of IPV9.

If the value of the zero bit of the Strict/loose bit innuendo is 1, the destination address field in the IPV9 header of the original packet must indicate a neighbor of the source node. If the zero bit is 1, the sender can

use any legal, non-multicast address as the initial destination address.

6) Data segment header

IPV9 source hosts use segment headers to send MTU packets that are longer than the packet delivery path. Different from IPv4, in IPV9, only the source host completes the segmentation, rather than the router on the path of the packet. The data segment header is identified by setting the next header to 44 in its previous header, as shown in table 9.

TABLE IX. DATA SEGMENT HEADER FORMAT

Next header	Reserve	Data segment offset	Reserve	M
Identifier				

Next header: It is an 8 bit selector. The initial header type (defined below) that identifies the data segment portion of the original packet. Use the same values as the IPv4 protocol fields [RFC-1700].

Reserve: It is an 8-bit field. It is initialized to zero at the sender and ignored at the receiver.

Data segment offset: It is an 8-bit field. The number of bytes moved forward or backward from the specified position.

M: Flag 1 indicates that there are more data segments, and 0 indicates the last data segment.

Identifier: It has 32-bit field. In order to send MTU packets whose length is longer than the transmission path, the source node can split the packet into several data segments and send each data segment as a separate data packet, and then reassemble the data packet at the receiver.

For each packet to be segmented, the source node generates an identifier value for it. Any piece of data in any recently delivered packet with the same source and destination addresses must have a different identifier. If a routing header is present, the destination address being considered is the final destination address.

7) Destination options header

The destination option header is used to carry the option that only needs to be checked by the packet's final node. The destination option header is identified by the header before it, with the next header field value of 60; the format is shown in table 10.

TABLE X. HEADER FORMAT OF DESTINATION ADDRESS OPTIONS

Next header	Length of extension header	
Option		

Next header: Bit selector. This is an identifier type of header that follows the destination option header. Use the same value as the IPv4 [RFC-1700].

Length of extension header: It is an 8-bit unsigned integer. The destination option header length is in 8-bit groups, and does not contain the first 8-bit group.

Option: It’s a Variable length field, whose length makes the destination option header length an integer multiple of 8-bit group. It contains one or more TLV encoding options.

Optional destination information in IPV9 packets is encoded in two ways: defined in the destination options header, or as a separate extended header. Data segment headers and authentication headers are two examples of the latter. Which one to take is depends on the action if the destination node could not recognize the option information.

a) If the destination node operation is want to abandon packets, and only in the destination node address of the packet is not the multicast address, then send the packet source address a "ICMP Unrecognized Type" message, and then these messages can be encapsulated into a separate header, or destination option in a header option, and the highest two digits of the option type are 11. This choice depends on a number of factors, such as fewer bytes, better alignment, or easy to parse.

b) If both operations are required, the messages must be encoded as an Option at the head of the destination Option, whose Option type has a highest two digits is 00, 01, or 10, specifying which actions will be take.

Note: When the next header field of an IPV9 header or any extended header is 59, which means there's nothing behind the header. If the IPV9 header payload length field indicates that there are 8-bit groups after the next header field of 59, these 8-bit groups must be ignored, and the content is passed as is when the packet must be forwarded.

III. PACKET LENGTH DESIGN

IPV9 requires a minimum of 576 MTU per link on the Internet. On any link, if it cannot pass 576 8-bit groups in one packet, then the data segment and reassembly associated with the link must be supported by the hierarchy below IPV9.

For each link directly connected to the node, the node must be able to accept packets as large as MTU. Links with configurable MTU (such as PPP links [RFC-1661]) must be configured with at least 576 8-bit groups, and larger MTU is recommended to accommodate possible encapsulations (such as tunnels) without fragmentation.

IPV9 nodes are recommended to implement Path MTU Discovery [RFCc-1191] in order to discover and take advantage of MTU links larger than 576. However, a minimal IPV9 implementation (such as in a BootROM) can simply restrict itself from sending packets larger than 576 and omit the Path MTU Discovery implementation.

In order to send MTU packets with a length greater than the link, the node can segment the packet at the source node and assemble it at the destination node by using the data segment header of IPV9. However, this fragmentation is not recommended in any application unless it can resize packets to fit the MTU of the link being measured.

A node must be guaranteed to accept segmented packets that exceed 1500 bytes after reassembly, including IPV9 headers. However, a node must ensure that it does not send segmented packets larger than 1500 bytes after reassembly unless it is explicitly told that the destination node can assemble such a large packet.

When sending an IPV9 Packet to an IPv4 node (that is packets go through the transition from IPV9 to IPv4)), the IPV9 source node may receive an "ICMP Packet TOO Big" (ICMP Packet is TOO Big) message reporting that next-hop MTU must be less than 576. In this case, IPV9 does not need to reduce the size of subsequent packets to less than 576, but must include a segment header in those packets so that the IPV9-IPv4 conversion router can obtain an appropriate identifier value for the constructed IPv4. This means that the load can be reduced to 496 8-bit groups (576 minus 72 bytes for IPV9 headers and 8 bytes for data segment headers) or even smaller if additional extended headers are used.

In order to send MTU data packets whose length is longer than the link, such as audio, image and video, long-stream code and absolute return code can be selected. The node can use the data segment header of IPV9 to identify the data packets in the source node without segmentation and assemble them in the destination node. However, when the sender and the receiver receive the signal disconnected by the return code, they will return to normal working condition.

Note: unlike IPv4, IPV9 does not require a "Don't Fragment" flag in the packet header to perform Path MTU Discovery, which is an implicit feature of IPV9. And the process associated with using MTU in RFC-1191 is not applicable to IPV9, because the message of IPV9 "Datagram Too Big" is always identifies the exact MTU being used.

Also, the procedures associated with the use of MTU tables in rfc-1191 are not applicable to IPV9 because the IPV9 version of the "Datagram Too Big" message always identifies the exact MTU being used.

Unlike IPv4 and IPv6, IPV9 can transmit the practical applications such as audio or video, it need to use the ever-flowing code and absolute return code, thus formed in the reserved the actual circuit actually has become a three layer structure, so there is no try to transfer the concept of content as guaranteed delivery channels and reliable safety, guarantee the transmission content don't interrupt. This results in the co-existence of the three - and four-tier architectures within the IPV9 network.

IV. FLOW LABEL

A data flow is a sequence of packets sent from one source to another destination address (point-to-point or multicast), and the source nodes require the intermediate router to have special control over these packets. These special processes can be transferred to routers through control protocols, such as resource reservation protocols, or through the information carried by the packets themselves in the data stream, such as segment options.

There may be multiple active streams between a pair of source and destination nodes, as well as many communications independent of any flow. A flow is uniquely identified by a combination of a source address and a non-zero flow label. The flow label field for packets that do not belong to any flow is set to 0.

The flow label is assigned by the source node of the data flow. New flow tags must be randomly selected (pseudo random), ranging from 1 to 16777215 (decimal). The purpose of the random assignment is to make the bits in the flow label suitable for use as hash keys in routers to find the relevant state of the flow.

All packets belonging to the same flow must be sent with the same source node address, destination node address, priority, and flow label. If any of these packets contain a segment option header, they must all have the same segment option header content. If any of their packets contain a routing header, all of their extended headers preceding the routing header must have the same content, including the routing header (except for the header field next to the routing header). Allows, but does not require, the router and destination node to check whether the above requirements are met. If a collision is detected, it should sending "ICMP parameter has a problem, code 0" message and then pointing to the high bit of the flow label (i.e., within the IPV9 packet with an offset of 1).

Routers are free to set the flow control state of based on "timing" even when there is no explicit flow control protocol, segment options, or other methods provide them with flow creation information. For example, when a flow label with an unknown, non-zero label is received from a particular source node, the router can process its IPV9 header and any other necessary extension headers as if the flow control label were 0.

The flow control state described above, after being set and cached according to "timing" must be discarded within 6 seconds, whether or not packets of the same class continue to arrive. If another packet with the same source address and flow control label arrives after the cache state has been discarded, then the packet must undergo full normal processing (as if the flow control label is 0), this process may cause the flow control state of the flow to be re-established and cached.

The lifetime of explicitly established flow control states, such as flow control states created by control protocols or segment options, must be specified as part

of the explicit establishment mechanism and can exceed 6 seconds.

During the lifetime of any flow control state that was previously created, the source node must not use this control label for new flows. Since any flow control state created depending on "timing" has a lifetime of six seconds, the minimum time between the last packet of a flow and the first packet of a new flow to use the same flow label is six seconds. The flow label has a longer lifetime and cannot be reused for new flows during the lifetime.

When a node is off and restarted (for example due to a system crash), care must be taken to avoid using flow label that it might have used for previously created flow that have not yet expired.

This can be achieved by record flow label in the memory, so that it can recall flow label previously used after a system crash, or until the previously created, there may be one of the biggest lifetime timeout before does not use flow label (at least for 6 seconds, if it use an explicit flow and establish a mechanism, and specifies the longer life span, even longer time). If the reboot time of a node is known (usually more than 6 seconds), the amount of time to wait before starting to allocate flow tags can be deducted accordingly.

V. CATEGORY TYPE DESIGN

The 8-bit Category Type field in the IPV9 header enables the source node to identify the desired level of packet delivery determination, certainly relative to other packets sent from the same node. Category Type bits contain two parts: 3 bits high is used to specify the address length, the value is 0 ~ 7, is 2 to the power, the address length is 1Byte ~ 128Byte; the default value is 256 bits, where 0 is 16 bits, 1 is 32 bits, 2 is 64 bits, 3 is 128 bits, 4 is 256 bits, 5 is 512 bits, 6 is 1024 bits, and 7 is 2048 bits. The last five bits specify two ranges of communication categories, with values 0 ~ 7 used to specify the information priority provided by the source node for congestion control, that is, the priority of information sent with a delay in the face of congestion, such as TCP information. 8 ~ 15 are used to specify the priority of messages that are sent without delay in the face of congestion, that is, the priority of "real time" packets that are sent at a fixed rate.

For crowd-constrained information, the following priority values can be used for specific application classes.

0: Non-character information,

1: Fill in the information (such as: net news),

2: Unattended information (such as: Email),

3: Reserve,

4: Large quantities of supervised information (such as: FTP、NFS),

5: Reserve,

6: Interactive information (such as: Telnet, X),

7: Internet control information (Such as: Routing protocol, SNMP),

8: For audio,

9: For video,

10: For video or audio compression will not be error due to alignment error,

11: Broadcast with audio and video,

12: Emergency use.

For messages that are not congested, the lowest rating value of 8 should be used for packets that the sender most wants to discard in crowded conditions (such as high-fidelity video messages), and the highest rating value of 15 should be used for packets that the sender least wants to discard (such as low-fidelity audio messages). There is no corresponding sequential relation between the rank of un-crowded and the priority of crowded.

VI. UPPER PROTOCOL DESIGN

A. Upper protocol check

If any transport protocol or other upper layer protocol includes the address in the IP header when calculating its checksum, then in order to be able to run on IPV9, the algorithm that calculates the checksum must be modified to include addresses with a length of 16-2048 bits rather than 32-bit IPv4 addresses. TCP and UDP headers for IPV9 are shown in table 11.

TABLE XI. TCP AND UDP HEADERS FOR IPV9

Source address	
Destination address	
Time	
Identify code	
Payload Length	
0	Next header

1) If the packet contains the routing header, the destination address in the pseudo-header is the final address. In the source node, this address is the last address in the routing header; at the receiver, this address will be in the IPV9 header address field.

2) The value of the next header in the pseudo-header identifies the upper protocol (e.g., TCP is 6, UDP is 17). If there is an extended header between the IPV9 header and the upper protocol header, the value of the next header in the pseudo-header is different from the value of the next header in the IPV9 header.

3) The value of the load length field in the pseudo-header is the length of the upper protocol packet, including the upper protocol header. If there is an extended Payload between the IPV9 Payload and the upper protocol Payload it will take less Payload Length than the IPV9 Payload Length (or in the large Payload option).

4) Different from IPv4, when a UDP packet is sent from an IPV9 node, UDP checksum is not optional. That is, whenever an IPV9 node sends a UDP packet, it must calculate the UDP checksum. The checksum is generated by the packet and pseudo-header, and if the result is 0, it must be converted to hex FFFF and placed in the UDP header. The IPV9 receiver must abandon the UDP packet containing the checksum 0 and record the error.

The checksum of ICMP version of IPV9 includes the above pseudo-header in its verification and calculation. This is a modification of the IPv4 version of ICMP, which does not include a pseudo-header in its verification and calculation. This change is made to ensure that ICMP is not passed incorrectly or corrupted by the IPV9 header fields on which it depends, which, unlike IPv4; these fields are not checked and protected by the Internet layer. The next header field in the pseudo-header of ICMP contains the value 58, which identifies the IPV9 version of ICMP.

B. Maximum packet lifetime

Unlike IPv4, IPV9 nodes like IPv6 do not require a mandatory maximum packet lifetime. This is why the "lifetime" field of IPv4 has been renamed IPV9's "segment limit".

In practice, very fewer IPv4 complies with the current packet lifetime, so this is not a practical change. Any protocol that relies on the Internet layer (whether IPV9 or IPv4) to limit the lifetime of packets should be upgraded to rely on its own mechanism to detect and discard stale packets.

C. Maximum upper layer load

When calculating the maximum load available for upper level protocol, it must be taking into account that the IPV9 header is larger than the IPv4 header.

For example, in IPv4, TCP's MSS option is calculated by the maximum datagram length (the default value obtained through Path MTU Discovery) minus 40 8-bit groups (20 8-bit groups for the minimum length of IPv4 headers and 20 for the minimum length of TCP headers) from.

When using TCP over IPV9, the MSS must be calculated by the maximum length minus 60 8-bit groups, because the minimum IPV9 header (when

IPV9 without an extended header) is 20 8-bit larger than the minimum IPv4 header.

VII. FORMAT OF OPTIONS

It is required to design the fields first when designing new options for segment option headers or destination option headers; these are based on the following assumptions.

1) Any field in the option data of an option that consists of multiple 8-bit groups should be aligned with their natural boundaries, that is, fields with n 8-bit groups of width should be placed at integer multiples of n 8-bit groups from the beginning of the segment header or destination option header, where n= 1,2,3,4 or 8.

2) Each segment header or destination option header takes up as little space as possible and must meet the requirement that the header length is an integer multiple of an 8-bit group.

3) It can be assumed that when any header with options appears, they only have a fewer options, usually only one.

These assumptions mean that it needs planning the individual fields of an option, arrange the fields from smallest to largest, with no padding in the middle, and then derive the alignment requirements for the entire field based on the alignment requirements for the largest field.

Examples are given below.

Case1. If option X requires two data fields, one with a length of 8 8-bit groups and one with a length of 4 8-bit groups, it should be arranged according to table 12.

TABLE XII. TWO FIELD DESIGN TABLE

	Option Type =X	Option data length =12
Four 8-bit group fields		
Eight 8-bit group fields		

Its alignment requirement is 8n+2 to ensure that the eight 8-bit fields start with an 8-fold offset from the header. The full segment header or destination header with the above options is shown in table 13.

TABLE XIII. FULL HEADER OR DESTINATION HEADER FORMAT

Next header	length of extension header =1	Option Type =X	Option data length =12
Four 8-bit group fields			
Eight 8-bit group fields			

Case2. If option Y requires three fields, one with a length of four 8-bit groups, one with a length of two 8-bit groups, and one 8-bit group, the format is shown in table 14.

TABLE XIV. THREE FIELD DESIGN FORMAT

		Option Length=Y
Option data length =7	One 8-bit group fields	Two 8-bit group fields
Four 8-bit group fields		

Its alignment requirement is 4n+3 to ensure that the four 8-bit leader fields start at a 4 times offset from the header. The full hop-by-hop or destination option header with the above options is shown in table 15.

TABLE XV. A THREE-FIELD FULL DATA FORMAT

Next header	length of extension header =1	Pad1 option =0	Option Type =Y
Option data length =7	One 8-bit group field	Two 8-bit group fields	
Four 8-bit group fields			
PadN option=1	Option data length =2	0	0

Case3. The segment header or destination header for each option X and option Y in both case 1 and case 2 should be one of the following two formats, depending on which option appears first, as shown in tables 16 and 17.

TABLE XVI. ONE FORMAT OF CONTAIN BOTH TWO - AND THREE-FIELD ADDRESS

Next header	length of extension header =3	Option Type=X	Option data length =12
Four 8-bit group fields			
Eight 8-bit group fields			
PadN Option =1	Option data length =1	0	Option Type=Y
Option data length =7	One 8-bit group fields	Two 8-bit group fields	
One 8-bit group fields			
PadN option=1	Option data length =2	0	0

TABLE XVII. ANOTHER FORMAT OF CONTAIN BOTH TWO - AND THREE-FIELD ADDRESS

Next header	length of extension header =3	PadN option=1	Option Type=Y
Option data length =7	One 8-bit group fields	Two 8-bit group fields	
Four 8-bit group fields			
PadN option=1	Option data length =4	0	0
0	0	Option Type =X	Option data length =12
Four 8-bit group fields			
Eight 8-bit group fields			

VIII. ENCAPSULATE SECURITY PAYLOAD HEADER DESIGN

A. Format of encapsulate security payload header

ESP (Encapsulating Security Payload) Header is designed to provide mixed security services in IPv4. The ESP mechanism can be applied with the authentication header or in a nested manner in tunnel mode alone. Security services may be provided between a pair of communicating hosts, or between a pair of communicating security gateways, or between a security gateway and a host.

The primary difference between the authentication header and the ESP mechanism is the effective area service. The encapsulation security payload mechanism does not protect any IP header fields unless they are encapsulated by the ESP, such as in tunnel mode where the IP header is encapsulated underneath.

The encapsulation security header is inserted after the IP header. In transport mode, the encapsulated security header is in front of the upper layer protocol header, and in tunnel mode, the encapsulated security header is in front of the encapsulated IP header.

ESP mechanisms provide services such as confidentiality, data origin authentication, connectionless integrity, anti-replay services (a form of partial sequence integrity), and limited communication confidentiality. The business provided by this mechanism depends on the options and the location of the application when the security association is established.

Confidentiality can be independent of other business options. However, the use of confidentiality alone without integrity authentication can lead to attacks that compromise the confidentiality of communication. Data origin authentication and connectionless integrity are federated services that can be provided as an option along with confidentiality services. The anti-replay service can only be selected if the data origin authentication service is selected, which is entirely up to the receiver.

The confidential service requires selection in tunnel mode, and this service is most effective when it used in the security gateway, because the clustering of communication on the gateway may mask the true source and host address modes. Note that while both confidentiality and authentication services are optional, at least one of them should be chosen.

A protocol header (IPv4 header, IPV9 base header, or extended header) that precedes the ESP header will have a value of 50 in its protocol field (if IPv4 header) or in its next header field (if it is the IPV9 extended header). The format of ESP groups and headers is shown in table 18.

TABLE XVIII. FORMAT OF ESP GROUPS AND HEADERS

0 8 16 24 31		
Security Parameters Index（SPI）		
Sequence Number		
Payload Data（variable length）		
	Fill field（0~255B））	
	Pad Length	Next Header
Authentication Data（variable length）		

Note: the scope of the certification business is the part before the certification data (authentication data is not included); the scope of the encryption service provided is the portion of the data that follows the serial number and precedes the authentication data (Serial Numbers and authentication data are not included).

B. Description of safe load format

The fields in the header format are explained below. The "optional" of the text indicates that if the field is not selected, the field is ignored and is not used when calculating the overall check value. If "required", this field must appear in the ESP group.

1) Security Parameters Index（SPI)

It is a required field of 32 bits. This field is associated with the security of the datagram that uniquely identifies the address of the address IP and the security protocol. The value of the SPI can be any, currently from 1 to 255 is reserved by IANA (). The value 0 of SPI is reserved for local, specific application use.

2) Sequence Number

It is a 32bit monotonically increasing counter (serial number). This field is required even if the receiver does not select to enable the playback service for a particular security association. The processing of this sequence number field is entirely done by the receiver, that is, the sender must transmit this field, and the receiver may or may not comply with the field.

When a security association is established, both sender and receiver counters are set to 0. If the anti-replay is started (default is enabled), the serial number

transferred does not allow loops. Therefore, after a secure association group, the sender and receiver counters must be reset.

3) Payload Data

It is a variable-length field that contains the data described by the next header field. The payload field is required and is an integer multiple of bytes in length.

4) Fill field

This field is used for encryption. The purposes of use fill fields in the ESP header are as follows.

a) If an encryption algorithm requires the body to be an integer multiple of bytes, the padding bytes are used to the body. (In addition to the filling fields themselves, the payload data, the filling length, and the next header fields are also included) to meet the data length requirements of the encryption algorithm.

b) Even *without considering the requirements of the encryption algorithm, fields need to be filled in to ensure the length of the* encrypted *data terminates at the boundary of 4B.* In particular, the length of the fill length field and the next header field must be aligned to 4B.

c) Apart from above algorithmic and alignment requirements, padding fields may also be used to hide the true length of the payload and partially encrypt the communication. However, this additional padding obviously consumes bandwidth resources and should be used with caution.

The sender can add 0 to the 255B to the fill field. Padding is optional in an ESP group, but all applications must support the generation and use of padding fields to satisfy the encryption algorithm for the length of the encrypted data while ensuring that the authentication data is aligned to the 4B boundary.

d) Pad Length

This field is required, and the valid fill length value should be from 0 to 255, with 0 indicating no fill bytes.

e) Next header

This field is required and is an 8-bit field indicating the data type in the payload data field.

f) Authentication Data

It is a variable-length field that contains the group's Integrity Check Value (ICV), which is calculated from the ESP group except the authentication data. This field is optional and only occurs if the authentication business is included in the security association. The authentication algorithm must account for the full length of the verification value and the relative rules of validation and processing steps.

C. Processing of security payload header

Encapsulated security payloads (ESP) are used in two ways: transport mode or tunnel mode.

1) Transmission mode

Transmission mode applies only to host applications. In this mode, the ESP header only protects the upper layer protocol and not the IP header field. In this mode, the ESP header is inserted after other IP headers and before the upper layer protocols of TCP, UDP, and ICMP. In IPV9, the ESP header is treated as an end-to-end payload, so the header must appear after the hop-to-hop, route, and segment headers.

The host option header may appear before or after the ESP header, depending on the semantics required. The locations of the ESP headers in a typical IPV9 packet in transport mode are shown in tables 19 and 20.

TABLE XIX. DATAGRAMS BEFORE THE APPLICATION OF ESP HEADER

Basic header	Extension header(if any)	TCP	Data

TABLE XX. DATAGRAM AFTER THE APPLICATION OF ESP HEADER

Basic header	Hop-to-hop, Destination header Route header Segment header	ESP	Destination Options header	TCP	Data	ESP Trailer	ESP authentication

The encrypted portion of the above packet can be a basic header encryption or a host option header, TCP, data, and ESP tail. The authenticated part in addition to the above part is encrypted, but also the package security load.

2) Tunnel mode

The ESP header in tunnel mode can be used for host or security gateway. Tunnel mode must be used when the ESP header is applied to the security gateway to protect the user's transmission communication.

In tunnel mode, the "lower" IP header carries the final source and destination address, while the "upper" IP headers contain the other addresses, such as the address of a security gateway.

In tunnel mode, the ESP header is positioned relative to the "upper" IP header as it is in transport mode. The position of the ESP header in a typical IPV9 packet in tunnel mode is shown in table 21.

TABLE XXI. ESP HEADERS IN TYPICAL IPV9 PACKETS IN TUNNEL MODE

upper Basic header	Upper Extension header (if any)	ESP	lower Basic header	Upper Extension header (if any)	TCP	Data	ESP Trailer	ESP authentication

In the above group, the encrypted part can be the upper basic header, the lower basic header, the lower extended header, TCP, data and ESP. The authenticated part in addition to the above part is encrypted, but also the ESP.

IX. CONCLUSION

This paper is a specific research and design scheme of RFC1606 and RFC1607 for the future network. The 42-layer routing address space is described according to the document in RFC1606. IPV9 has a routing hierarchy of up to 42 layers, and this routing hierarchy is a key feature in its wide application.

In order to protect previous investments, IPv4 and IPv6 compatible addresses have been set inside, with layers 1-41 designed for IPv4 and IPv6 compatibility and layer 42 described in the RFC1606 document. The large number of address Spaces in IPV9 also makes it possible to allocate addresses in a direct way

In order to the application of IP mobile, IPTV, IP phone, Internet of things and other network applications that need to use Arabic numerals to represent and need to use characters that do not have to be analyzed again, this design also designed a character router.

IPV9 address length is designed according to the document of RFC1607 that the network address length is 1024 bits in the future network, and the address space length is designed as 2048 bits according to the actual demand, thus solves the address space capacity problem in the next 750 years.

In order to meet the technical demand of RFC1606 and RFC1607, the definitions of routing hierarchy, address length, address working mode, address space

resource, address text representation method, compression definition and separator were redefined, Please refer to other related articles of this design team.

REFERENCES

[1] Tang Xiaodan etc. Computer Operating System (third edition) [M]. Xi'an: Xidian university press, 2010.

[2] Xie Jianping etc. A method of assigning addresses to network computers using the full decimal algorithm [P]. CN: ZL00135182.6, 2004.2.6.

[3] Xie Jianping etc. Method of using whole digital code to assign address for computer [P]. US: 8082365, 2011.12.

[4] RFC - Internet Standard. Internet Protocol, DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 791, 1981.09.

[5] S. Deering, R. Hinden, Network Working Group. Internet Protocol, Version 6 (IPv6)-Specification, RFC-1883, 1995.12.

[6] M. Crawford. Network Working Group. Transmission of IPv6 Packets over Ethernet Networks. RFC-2464, 1998.12.

[7] J. Onions, Network Working Group. A Historical Perspective on the usage of IP version 9. RFC1606. 1994.04.

[8] V. Cerf, Network Working Group. A VIEW FROM THE 21ST CENTURY, RFC1607. 1994.04.

[9] Xie Jianping, Xu Dongmei, etc. Digital domain name specification. SJ/T11271-2002, 2002.07.

[10] Information technology-Future Network- Problem statement and requirement-Part 2: Naming and addressing, ISO/IEC DTR 29181-2, 2014, 12.

[11] Wang Wenfeng, Xie Jianping, etc. Product and service digital identification format for information procession. SJ/T11603-2016, 2016. 06.

[12] Radio frequency identification tag information query service network architecture technical specification. SJ/T11606-2016, 2016. 06.

Design and Research of New Network Address Coding

Lai Yufeng
[1.]State and Provincial Joint Engineering Lab. of Advanced Network, Monitoring and Control, China
[2.] School of Computer Science and Engineering
Xi'an Technological University
Xi'an, China
e-mail: 604612675@qq.com

Cheng Xiaowei
[1.]Chinese Decimal Network Working Group
Shanghai, China
[2.]Shanghai Decimal System Network Information
e-mail: xewei.cheng@em777.net

Xie Jianping
[1.]Chinese Decimal Network Working Group
Shanghai, China
[2.]Shanghai Decimal System Network Information
e-mail: 13386036170@189.cn

Li Yuyu
Shandong Radio, Television and Network Co., LTD.
Tai 'an Branch
e-mail: tagdjsb@126.com

***Abstract*—To solve a series of problems caused by address space and information security of contemporary Internet, Chinese scientists have proposed a new generation of network architecture. Since the release of IPv4 RFC791 in 1981, it has become the first widely used Internet of things protocol due to its characteristics of easy implementation and good operability. It constitutes the basic protocol of current Internet technology. However, due to the defects in address classification, address resources are largely wasted. As the scale of the Internet continues to grow, especially the number of addresses used to surge, the address shortage has limited the Internet further development. IPv6 has solved the problem of insufficient IPv4 addresses to some extent, but it is not widely for more than 20 years used because it integrates the information of physical layer and application layer, which confuses the network layer and brings many security risks. Based on the study of IPv4 and IPv6, this paper proposes a new generation network architecture, which is designed from the aspects of addressing model, address writing, address prefix writing and address type. The address structure is compatible with IPv4 and IPv6, so that the previous design results can be retained, fundamentally solve the space address and information security issues, and provide a new solution for the next generation of Internet applications and research.**

Keywords-Network Architecture; The Network Address; IPV9; IPv4; IPv6

PREFACE

Because IPv4 addresses are allocated on a first-come-first-served, on-demand basis, the distribution imbalance makes address allocation flawed. With the continuous development of the Internet (especially the explosive growth of the scale and the surge of address use), some inherent defects of IPv4 are gradually exposed, mainly focusing on address shortage. IPV4 does not provide encryption and authentication mechanisms to ensure the secure transmission of confidential data resources and other aspects. Although the use of NAT ("Network Address Translation"), CIDR ("Classless Inter-Domain Routing") and other technologies can alleviate the IPv4

crisis to some extent. But in fact, it has not fundamentally solved the problem. At the same time, it will bring new problems in cost, quality of service, security and other aspects, posing greater challenges.

To solve the problem of insufficient IPv4 addresses, scientists proposed IPv6.However, due to the limitations of the technology era, there are many defects in the design of IPv6 address structure. Not satisfied with the 128-bit address length, the designers did not follow the principle of transparency between different protocol layers and added the physical layer address and the application layer in the design of IPv6 address segment (the protocol of the network layer), which led to a series of fatal problems.

"IPv9" is an idea proposed in the early 1990s by the IETF (The Internet Engineering Task Force) in the June 1992 issue of RFC 1347 to address the deficiencies in Internet address domain names.In May 1995, IETF unilaterally abandoned its cooperation with ISO (International Organization for Standardization), disbanded TUBA, the institute for IPv9 research, and terminated its organized research and development activities for IPv9. However, no intellectual property rights and valuable technical data were formed in this research.

Inspired by RFC 1347, Xie Jianping, a Chinese expert, formed the Chinese IPV9 research and development team with Shanghai general chemical technology research institute as the gathering center. The difference between uppercase and lowercase indicates that the IPV9 developed in China is not a technical version following the Internet.

IP version 9 (IPV9) is a new version of the Internet protocol, also known as the decimal network, digital domain name. The decimal network technology protocol is developed independently by our country. The emergence of IPV9 fundamentally solves the problems of insufficient address and network security.

I. NEW NETWORK ADDRESS IPV9

A. Network Address

Internet addresses are assigned by ICANN（the Internet Corporation for Assigned Names and Numbers） .The association appoints three local organizations for the assignment of addresses: INTERNIC for North America, RIPENCC for Europe and APNIC for the Asia Pacific region. The purpose of uniform allocation is to ensure that the network address has global uniqueness, and the host address is assigned by the system administrator of each network. Therefore, the uniqueness of the network address and the host address within the network ensures the uniqueness of the IP address.

B. IPV9

IPV9 decimal network/digital domain name system (IPV9).Based on the study of IPv4 and IPv6, the following changes are proposed. IPV9 expands the address length to 2048 bits, reduces the network overhead by means of indefinite length and non-location, and guarantees the network security. This article defines the IPV9 address architecture, including a detailed description of the currently defined IPV9 address format.

C. IPV9 header format

The format design of IPV9 system header is shown in table 1.

TABLE I. IPV9 HEADER FORMAT

<table>
<tr><td>Version number</td><td colspan="4">communication stream type</td><td rowspan="2">stream label</td></tr>
<tr><td></td><td>Address length</td><td>Priority class traffic</td><td>Address the authentication</td><td>Absolute traffic</td></tr>
<tr><td>Payload length</td><td colspan="4">Next head</td><td>hop limit</td></tr>
<tr><td colspan="6">source address (16-2048 bit)</td></tr>
<tr><td colspan="6">Destination address (16-2048 bit)</td></tr>
<tr><td colspan="6">time</td></tr>
<tr><td colspan="6">Authentication code</td></tr>
</table>

The design of table 1 is explained below.

1) Version: 4-bit length, Internet protocol version number. For IPV9, this field must be 9.

2) Category: 8 bits in length. 3 bits high is used to specify the address length, the value is 0 ~ 7, is the power of 2, the address length is 1Byte ~ 128Byte; the default value is 256 bits. Among them, 0 is 16 bits, 1 is 32 bits, 2 is 64 bits, 3 is 128 bits, 4 is 256 bits, 5 is 512 bits, 6 is 1024 bits, 7 is 2048 bits. The last five bits specify the communication class and authentication for the source and destination addresses.0 to 15 is the priority value, where 0 to 5 is used to specify the priority class of the traffic; 6 to 7 are used to specify the communication method of authentication before communication. The address of packet sending is used for traffic control and whether authentication of source address and destination address is required.8 to 14 are used to specify absolute traffic that will not fall back when congestion is encountered; 15 for virtual circuits; 16 and 17 respectively assign audio and video, called absolute value, to ensure the uninterrupted transmission of audio and video. Other values are reserved for later use.

3) Flow label: With a length of 20 bits, it is used to identify packages belonging to the same business flow.

4) Net load length: The length is 16 bits, including the net load byte length, that is, the number of bytes contained in the packet after IPV9 header.

5) Next header: The length is 8 bits. This field indicates the protocol type in the field following the IPV9 header.

6) Hop limit: The length is 8 bits, and this field will be reduced by one every time a node forwards a packet.

7) Source address: 8-bit bit ~ 2048-bit bit, specifying IPV9 packet sender address. Use of variable length and location method.

8) Destination address: The length is 8 bit ~ 2048 bit, and the destination address of IPV9 packet is specified. Use of variable length and location method.

9) Time: Used to control the lifetime of the address in the header.

10) Authentication code: It is used to identify the authenticity of the address in the header.

II. IPV9 ADDRESS SPACE

A. Type of address

IPV9 addresses specify 256-bit identifiers for interfaces and interface groups. There are three types of addresses:

1) Unicast. A single interface has an identifier. A packet sent to a unicast address is passed to an interface identified by that address.

2) Arbitrary cast. Typically, a set of interfaces belonging to different nodes has an identifier. A packet sent to an arbitrary cast address is passed to an interface identified by that address that is the closest measured by the routing protocol distance.

3) Multicast. Typically, a set of interfaces belonging to different nodes has an identifier. A packet sent to a multicast address is passed to all interfaces at that address.

There are no broadcast addresses in IPV9, and its functionality is being replaced by multicast addresses. In this article, fields within the address are given a specified name, such as "user." When the name is followed by an identifier (such as "user ID"), it is used to represent the content of the name field. When a name is used with a prefix (such as "user prefix"), it represents all addresses up to and including this field.

In IPV9, any fields that are all "0" and all "1" are valid values unless specifically excluded. In particular, the prefix can contain a "0" value field or end with a "0".

B. Addressing model

All types of IPV9 addresses are assigned directly to the interface, not to the node.IPV9 unicast addresses belong to a single interface. Because each interface belongs to a single node, a node of multiple interfaces, any of its unicast addresses can be used as the identifier for that node. All interfaces need at least one link local unicast address. A single interface can specify multiple IPV9 addresses (unicast, arbitrary cast, multicast) or ranges of any type. Unicast addresses with greater link range are not required for interfaces that go from non-neighbor or to non-neighbor and are not the origin or destination of any IPV9 packets. This is sometimes used for point-to-point interfaces. There is one exception to this addressing model:

Handle the case of multiple physical interface implementations. If the state that emerges in the Internet layer is an interface, a unicast address or a group of unicast addresses can be assigned to multiple physical interfaces. This is useful for load-sharing across multiple physical interfaces.

Current IPV9 extends the Ipv4 model, with a subset prefix associated with a link. Multiple subset prefixes can be specified to the same link.

III. TEXT REPRESENTATIONS OF IPV9 ADDRESSES

This article has developed a way to represent IPV9 addresses, including “Brackets decimal” representation, "Curly braces" representation, and "Parentheses" representation.

A. Brackets decimal

The bracket decimal can be expressed in the following two ways:

The first method : 2048 bits are represented by "[]".The 2048 bits in "[]" are expressed in decimal and can be written in indefinite length. And you can omit the "[]" when writing in the browser.

The second method : The 256-bit IPV9 address representation is in the form of "y[y] [y] [y] [y] [y] [y]".

Each y represents a 32-bit portion of the address and is represented in decimal.232 =4294967296, so each “y” is a decimal number of ten digits. Each digit that is distinct from the decimal system ranges from 0 to 9.For example, the range of the first digit from the left is 0 to 4, so that there will be no overflow. For example:

0000170170[0000062062[0000000000[0000000000[0000000000[0000000000[0000000000[0000210210[0000422422

In address representation, multiple consecutive zeros to the left of each decimal number can be omitted, but a decimal number that is completely zero needs to be represented by a zero. For example, the above address can be written as:

170170[62062[0[0[0[0[0[210210[422422

To simplify the representation of addresses, successive all-zero fields in the address can be replaced by a pair of square brackets "[X]" (X is the number of

segments in the all-zero field).For example, the above address can be abbreviated as:

170170[62062[4][210210[422422

Another example:

0[0[0[0[0[0[0[1 can be abbreviated as [7]1

0[0[0[0[0[0[0[0 can be abbreviated as [8]

B. Decimal braces

This method divides the 256-bit address into four 64-bit decimal Numbers represented by curly braces separating them. The representation is in the form of "Z}Z}Z}Z", where each “Z” represents a 64-bit portion of the address and is represented in decimal. It's exactly the same as “Y”, and it's compatible with “Y”. You can mix the two. This greatly facilitates the current compatibility of these Ipv4 addresses in IPV9.Such as:

z}z}z}z;
z}z}y]y]y]y;
z}z}y]y]y]d.d.d.d;
z}z}z}y]d.d.d.d;
z}z}z}y]J.J.J.J;

In particular, the last address format is the most useful. Such as:

0}0}0}0]193.193.193.193

You can write it like this: {3}0]193.193.193.193

Finally, it should be noted that in symbolic representation, the brackets and Curly braces are used without distinction. That is, "{" and"} ", "[" and"] "are not dissimilar, since this will not cause any side effects and is more convenient for users.

C. Parentheses representation

Since IPV9 has an address length of 256 bits, whether you use four or eight segments, there are still many bits in each segment. For example, with an 8-segment representation, each segment still has 32 bits. This is what happens in a paragraph:

……]00000000000000000000000000110100]……

……]01011111111111111111111111111111]……

Such a situation is not only cumbersome input, and it is easy to lose less or more, the user is not conducive to the number of dazzling.For convenience, the parenthesis representation -- (K/L) is introduced.Where "K" means 0 or 1 and "L" means the number of 0 or 1.In this way, the above two examples can be abbreviated as:

……]（0/26）110100]……

……]010（1/29）]……

D. Text representation of address prefixes

The IPV9 address scheme is similar to the super netting and CIDR schemes of Ipv4 in that the address prefix is used to represent the network hierarchy. On the representation of IPV9 address prefix, a representation similar to CIDR is adopted, which is as follows:

IPV9 address/address prefixes length.

Where, IPV9 address is written in IPV9 address representation. The address prefix length is the length of consecutive bits that form the address prefix from the left. At this point, it is important to note that IPV9 addresses use decimal Numbers, but prefix length refers to binary. Therefore, prefixes must be calculated carefully. In binary Numbers is not intuitive, after consideration, it is considered that the IPV9 address prefix can be converted to hexadecimal is easier to understand, but the IPV9 address is still expressed in decimal Numbers.

For example, the 200-bit address prefixes 1314[0[0[0[224[169[0 can be expressed as:

1314[0[0[0[343[150[0[0/200
Or 1314[3]224[169[0[0/200
Or 1314[0[0[0[224[169[2]/200
Or 1314[3]224[169[2]/200

Note that in the representation of the address prefix, the IPV9 address portion must be legal. The IPV9 address to the left of the slash "/" must be restored to the correct address. In this address prefix, you can see that the address prefix is 200 in length. So, the prefix is really just the first 6 bits of the entire address plus the first 8 bits of paragraph 7 (32 times 6+8=200).So the key is in the seventh paragraph of the address.

This paragraph is expressed in hexadecimal as:"********". Because in hexadecimal, one digit is 4 bit, the prefix includes only the first two "*". Knowing this, you know that the value of this segment is 00000000 (hex) ~00FFFFFF (hex), or 0~16777215 in decimal. (Or this paragraph may be expressed in binary as: "**** **** **** **** **** **** **** ****". Because in binary, one bit is one bit, so the prefix includes the first eight "*", the range of values in this section is0000 0000 0000 0000 0000 0000~0000 0000 0000 1111 1111 1111 1111 1111That is, decimal 0~16777215.)

The IPV9 address portion can be generated by a pure address prefix by appending a 0 to its right, or it can be a real IPV9 address that contains the address prefix. For example, the address prefix in the above example can also be expressed as:

1314[3]224[169[a[b/200

"a" is any decimal number between 0 and 16777215, and "b" is any decimal number between 0 and 4294967296.

IV. IPV9 ADDRESS TYPE

1) Pure IPV9 address

The form of this address is Y[Y[Y[Y[Y[Y[Y[Y

Each Y represents a decimal integer from 0 to 232 =4294967296

2) IPV9 addresses compatible with Ipv4

The form of the address is Y[Y[Y[Y[Y[Y[Y[D.D.D.D

Each Y represents a decimal integer from 0 to 232 =4294967296. D represents a decimal integer between 0 and 255 from the original Ipv4.

3) IPV9 addresses compatible with Ipv6

The form of this address is: Y[Y[Y[Y[X:X:X:X:X:X:X:X

Each Y represents a decimal integer from 0 to 232=4294967296.The X represents a hexadecimal number that originally Ipv6 ranged from 0000 to FFFF.

4) Special compatibility address

In order to upgrade from Ipv4 and Ipv6 to IPV9 smoothly, some compatible addresses are designed. Among them, some Ipv6 addresses are designed to be compatible with Ipv4 addresses. To smooth the transition to IPV9 addresses, prefix these addresses appropriately. In order to make their representation more intuitive and avoid errors caused by negligence in writing, the abbreviation method is introduced:

y[y[y[y[x:x:x:x:x:x:d.d.d.d

Where, each "y" represents the address as 32 bits, represented in decimal. Each "x"represents the original Ipv6 address of 16 bits, in hexadecimal. Each "d" represents the original Ipv4 address of 8 bits, expressed in decimal.Such as:

0[0[0[0[14714747[1199933[223556889[147258369

Can be written as: 0[0[0[0[E0:877B:12:4F3D:D53:3519:3.198.252.1

Or: [4] E0:877B:12:4F3D:D53:3519:3.198.252.1

Such as: 0[0[0[0[0[0[0[562159487

Can be written as:[4]::33.129.223.127

(Analysis: ":" is IPv6 address compression form of the representation, multiple 0 blocks of a single continuous sequence by the double colon symbol "::".Decimal 562159487 is expressed as 33.129.223.127 in decimal.)

5) [] full decimal address

In order to facilitate the logistics code and decimal address application. Category number 5 is recommended. In the power of 10 to the power of 512, the method of fixed length and non-positioning is adopted according to the application needs.

6) IPV9 address of transition period

IPV9 can be compatible with IPv4 and IPv6 technical protocols for the Internet, but IPv4 and IPv6 technical protocols cannot be anti-compatible with IPV9.The concept of compatibility is parallel coexistence, gradual and moderate transfer of applications and data services, rather than direct replacement or replacement of existing protocols.

In order to solve the problem of IPv4 smooth transition to IPV9, considering the existing Internet has invested a lot of money so far, we specially designed IPV9's transition address, and took out a segment 232to allocate IPv4.Small changes can be made to the current system, where IPV9 has a section of J.J.J.J. where each J represents a decimal number from 0 to 28 which is 0 to 255.Where the previous [7] can be omitted in the middle of the local address, that is, local users (or designated users) can use J.J.J.J. to directly use and the original Ipv4 D.D.D.D. distinction.At the same time, this part of the user in order to smooth the transition to full decimal can be allocated at the same time decimal. In order to improve the software and hardware in the future without the need to reallocate addresses, such as [7]5211314 can be written as [7]3.48.155.175 in the region in an IP network can be directly written with 3.48.155.175, so that the original terminal can be used.There should be new records in the IPV9 DNS records for compatibility between the original user and the current user.The interim IPV9 address system can be modified to the original IPv4 system.Meanwhile, the Ipv4 header is used, but the version number is 9 to distinguish the original IPv4.However, the original terminal equipment may be used by user terminals in the territory.

When the address length is 16 bits when the class number is 0, the IPv4 physical address is discarded and the IPv4 host 16-bit address is used. The representation is decimal 65535 or dot decimal 0-255.0-255 as in hexadecimal FF.FF.

When the class number is 1, the address length is 32 bits, represented by decimal 0-4294967295 and the corresponding character length or dot decimal 0-255.0-255.0-255.0- 255.0-255 as in hexadecimal FF.FF.FF.FF

When the class number is 2, the address length is 64 bits, represented by decimal 10 or the corresponding character length.

When the class number is 3, the address length is 128 bits, represented by decimal or the corresponding character length.

When the class number is 4, the address length is 256 bits, represented by decimal or the corresponding character length.

When the class number is 4, the address length is 512 bits, denoted by decimal or the corresponding character length.

When the class number is 5, the address length is 1024 bits, denoted by decimal or the corresponding character length.

When the category number is 6, the address length is 2048 bits, represented by decimal or the corresponding character length.

When the class number is 7, the address length is an unfixed bit, represented by the corresponding decimal length or the corresponding character length.

V. ALLOCATION OF ADDRESS PACE

Specific types of IPV9 addresses are identified by the high boot bit field in the address. The length of these boot bit fields varies. In the protocol, they are called the format prefix FP.

TABLE II. IPV9 ADDRESS FORMAT PREFIX 1

Format prefix FP (n bits)	Address (256-n bits)

TABLE III. IPV9 ADDRESS FORMAT PREFIX 2

Format prefix FP (n bits)	Address (2048-n bits)

The following is an overview of the various address type prefixes.

TABLE IV. IPV9 ADDRESS FORMAT PREFIX FOR THE ORIGINAL ALLOCATION TABLE

	Address type	**Format prefix (binary code)**	**Format prefix (decimal code range)**	**Proportion of address space**
1	Reserved address	0000 0000 00	0——4194303	1/1024
2	Unassigned address	0000 0000 01	4194304——8388607	1/1024
3	IPV9 Decimal Network Working Group	0000 0000 1	8388608——16777215	1/512
4	IPX reserved address	0000 0001 0	16777216——25165823	1/512
5	Unassigned address segment	0000 0001 1	25165824——33554431	1/512
6	Unassigned address segment	0000 0010	33554432——50331647	1/256
7	Unassigned address segment	0000 0011	50331648——67108863	1/256
8	Unassigned address segment	0000 0100	67108864——83886079	1/256
9	Unassigned address segment	0000 0101	83886080—100663295	1/256
10	Unassigned address segment	0000 011	100663296— 134217727	1/128
11	Unassigned address segment	0000 1 0	134217728—201326591	1/ 64
12	Unassigned address segment	000 0 1 1	201326592—268435455	1/ 64
13	Unassigned address segment	0001 0	268435456—402653183	1/32
14	Unassigned address segment	00 0 1 1	402653184—536870911	1/32
15	Unassigned address segment	0010 0	536870912—671088639	1/32
16	Unassigned address segment	001 0 1	671088640—805306367	1/32
17	Unassigned address segment	0011	805306368—1073741823	1/ 16
18	Aggregable global unicast address	0100	1073741824—1342177279	1/16
19	Unassigned address segment	0101	1342177280-1610612735	1/16
20	Unassigned address segment	011	1610612736—2147483647	1/ 8
21	Geographical area unicast address	100	2147483648—2684354559	1/ 8
22	Geographical area unicast address	10 1	2684354560—3221225471	1/ 8
23	Unassigned address segment	1100	3221225472—3489660927	1/16
24	Unassigned address segment	1101	3489660928—3758096383	1/16
25	Unassigned address segment	1110 0	3758096384—3892314111	1/32
26	Unassigned address segment	1110 10	3892314112—3959422975	1/64

27	Unassigned address segment	1110 11	3959422976—4026531839	1/64
28	Unassigned address segment	1111 00	4026531840—4093640703	1/64
29	Unassigned address segment	1111 01 0	4093640704—4127195135	1/ 128
30	Unassigned address segment	1111 01 1	4127195136—4160749567	1/ 128
31	Unassigned address segment	1111 100	4160749568—4194303999	1/ 128
32	Unassigned address segment	1111 1010	4194304000—4211081215	1/256
33	Unassigned address segment	1111 1011	4211081216—4227858431	1/256
34	Unassigned address segment	1111 1100	4227858432—4244635647	1/256
35	Unassigned address segment	1111 1101	4244635648—4261412863	1/256
36	Unassigned address segment	1111 1110	4261412864—4278190079	1/256
37	Unassigned address segment	1111 1111 0	4278190080—4286578687	1/512
38	Unassigned address segment	1111 1111 100	4286578688—4288675839	1/2048
39	Local link unary address	1111 1111 1010	4288675840—4289724415	1/4096
40	Station single address	1111 1111 1011	4289724416—4290772991	1/4096
41	Multi-address	1111 1111 11	4290772992—4294967295	1/1024
42	Full decimal address	0	0 — 10 512	0 — 10 512

The aggregate global unary address and the cluster address belong to the unary address, they do not have any difference in form, only in the propagation mode of the message is different. Therefore, the same format prefix 0100 is used for the polymerizable monocular and cluster address assignments. The proposed network vendor monocular addresses and geographic area monocular addresses are merged into a polymerizable monocular address.

Both the local link unary address and the station unary address are used in the local scope. In order to facilitate the router to speed up the identification of these two kinds of addresses, two address format prefixes, 1111 1111 1010 and 1111 1111 1011, were assigned to them respectively.

Because the processing method of multi-destination address on the router and host is quite different from the processing method of single-destination address and cluster address, an address format prefix 1111 1111 11 was also assigned to the multi-destination address.

The design also reserved address space for "decimal Internet address and domain name decision and allocation organization" and IPX address. The corresponding address format prefix is 0000 0000 1 and 0000 0001 0.Some special addresses of IPV9, such as unspecified addresses, local return addresses and ipv4-compatible addresses, are prefixed by 0000 0000 00 as the address format.

Due to the length of this article, only the address format in the IPV9 address architecture is described in detail. For more knowledge of IPV9, please refer to the related articles.

VI. THE CONCLUSION

IPV9 is the core and key technology of the next generation Internet. In this paper, IPV9 address coding is researched and a new address coding is proposed.IPV9 increases the length of IP addresses from 32 bits and 128 bits to 2048 bits, and the default is 256 bits, to support more address hierarchies, more addressable nodes, and simpler automatic address configurations. In order to reduce the network overhead, the fixed location method is adopted,

changed the encoding of header options to allow more efficient forwarding. Reduce restrictions on option length for greater flexibility in introducing new options in the future. IPV9 adds expansionary support for IP address encryption and authentication, data integrity, and data privacy (optional). The new network address is not only the update and upgrade of the old network address, but also a brand new Internet system structure, which has laid a solid foundation for promoting the extensive application and integrated development of Internet and Internet of things.

INTRODUCTION OF XIE JIANPING

Xie Jianping, male, was born in Shanghai, China in 1951. He is a Chinese expert in the International Standards Organization (ISO/IEC JTC1/SO6). As the "decimal network standard working group" and "Electronic Labeling Standard Working Group Data Format Group" of the Ministry of Industry and Information Technology of the People's Republic of China, the "New Generation Security Controllable Information Network Technology Platform Overall Design" expert group and the Internet of Things Joint Standards Working Group Leader of the team. It is also the main editor of the ISO/C6 "Future Network naming and addressing" Chinese member.

Professor Xie has obtained more than 90 multinational patents. The patents on network resources, terminal equipment, networks transmission and information platform include "Methods for allocating addresses to computers using Internet with full digital codes" and "Methods for allocating computer addresses with all-decimal algorithms for networked computers", "Method and apparatus for implementing trusted network connection through a router or switch", "Method for uniformly compiling and allocating addresses of networked computers and intelligent terminals", "Decimal Gateway", "An IPV9/IPV4 NAT Router", "An IPV9 Website Browser Plugin", "A new generation of IPV9 routers", "A Networked Tax Control System and Its Method" and "Digital Remote Video Surveillance System Device"

REFERENCE

[1] Xie Jianping etc. A method of ssigning addresses to network computers using the full decimal algorithm[P]. CN: ZL00135182.6, 2004.2.6.

[2] Xie Jianping etc. Method of using whole digital code to assign address for computer [P]. US: 8082365, 2011.12.

[3] S. Deering, R. Hinden, Network Working Group. Internet Protocol, Version 6 (IPv6)-Specification, RFC-1883, 1995.12.

[4] RFC – Internet Standard. Internet Protocol, DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 791, 1981.09.

[5] P. Srisuresh. Network Working Group. IP Network Address Translator (NAT) Terminology and Considerations. RFC-2663, 1999.8.

[6] V. Fuller. Network Working Group. Classless Inter-domain Routing (CIDR):The Internet Address Assignment and Aggregation Plan. RFC-4632, 2006.8.

[7] Ross Callon. TCP and UDP with Bigger Addresses (TUBA), A Simple Proposal for Internet Addressing and Routing. RFC-1347, 1992.6.

Research of New Network Address Structure

Chong Jiao
[1.]State and Provincial Joint Engineering Lab. of Advanced Network, Monitoring and Control, China
[2.]School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710021, China
e-mail: 1342748406@qq.com

Xu Yinqiu
[1.]Chinese Decimal Network Working Group
[2.]Shanghai Decimal System Network Information Technology Ltd.
e-mail: 8918616209@126.com,

Xie Jianping
[1.]Chinese Decimal Network Working Group
[2.]Shanghai Decimal System Network Information Technology Ltd.
e-mail: 13386036170@189.cn

Zhao Hongwen
Shandong Radio, Television and Network Co., LTD.
Tai 'an Branch.
e-mail: tagdglcs@qq.com

***Abstract*—With the wide application of Internet technology, the number of hosts accessing the Internet has grown rapidly, and addresses will be more and more widely used in other intelligent terminals such as e-commerce logistics codes, space codes, identity codes, and 3D geocodes. The number of existing addresses is no longer sufficient for this development demand. The emergence of IPv6 temporarily alleviated the problem of IP address shortage, and IPv6 did not fully consider the security of data transmission at the beginning of design. Chinese researchers have proposed a new Internet address architecture, that is, method of using whole digital code to assign address for computer, referred to as IPV9. IPV9 extends address capacity; supports more address hierarchies, more addressable nodes, and simpler automatic address configuration. Based on the study of IPv4 and IPv6 address structure, this paper designs the standards of the new generation network address structure, including IPV9 unicast address structure, cluster address structure and multicast address structure, which provides a solid foundation for new generation of Internet research.**

Keywords-Addressing; Address Structure; IPV9; Decimal Network

I. INTRODUCTION

At the beginning of the Internet development, IPv4 addresses were sufficient and successful, but in the last 20 years of the 20th century, the global Internet was growing rapidly, and the number of hosts connected to the Internet was growing exponentially every year. Therefore, the number of existing addresses is no longer sufficient for this development demand. IPv6 solves the problem of address shortage in IPv4, but it does not fully consider the network security problem in design. There are many security risks, and IPv6 is not compatible with the original IPv4. In order to adapt to the network development, Chinese researchers proposed a new network address architecture. This structure adopts a method of using whole digital code to assign address for computer and intelligent terminal. It is input to a computer through various input devices of a computer and a smart terminal, and combines software and hardware of various computers. The external addresses of the networked computers and

intelligent terminals are compiled corresponding to the addresses of the internal operations of the computer through various transmission media.

This new address allocation method can provide sufficient address space for the future development of the Internet, and this new one also provides sufficient information for various personal information appliances and e-commerce logistics and personal communication terminal applications. This also ensures that the address hierarchies can have more layers. The IP address length from 32 bits to 128 bits to 2048, to support more address hierarchies, more addressable nodes and simpler automatic address configuration. At the same time, the 32 -bit address length of IPv4 has been reduced to 16 bits to solve the quick use of cellular communication in mobile communication.

II. ADDRESS TEXT REPRESENTATION

The decimal network address is expressed in "brackets in decimal", that is, y[y[y[y[y[y[y[y[y, where each y represents a 32- bit long integer in decimal. Such as: 0000030620[0000000000[0000000000[0000000000[0000000000[0009635485[0000000000[000005953246. In the address representation, multiple consecutive zeros on the left of each decimal number can be omitted, but all zero decimal numbers need to be represented by a zero. For example, the above address can be written as: 30620[0[0[0[0[9635485[0[5953246]. In order to further simplify the representation of address, we can address the entire continuous field zero can be represented by "[X]" (X is the number of stages of the all-zero field). For example, the above address can be abbreviated as 30620 [4] 9635485 [0 [5953246].

The decimal network address prefix uses a CIDR (Classless Inter-Domain Routing) like representation, which has the following form: IPV9 address/address prefix length. The IPV9 address is an address written by the IPV9 address representation, and the address prefix length is the number of consecutive digits from the leftmost part of the address to indicate the address prefix. The decimal number is used in the IPV9 address, but the prefix length refers to the binary. For example: 200-bit address prefix 3659[0[0[0[31548[150[0 can be expressed as: 3659[0[0[0[31548[150[0[0/200 or 1212[3]343[150[2]/200. In the representation of the address prefix, the IPV9 address to the left of the slash "/" must be restored to the correct address.

IPV9 addresses are assigned to interfaces, not nodes. The IPV9 address specifies a 256-bit identifier for the interface and interface group. There are three types of addresses: a single interface with a single unicast address, anycast address, and a multicast address.

III. UNICAST ADDRESS STRUCTURE

The unicast address is the identifier of a single network interface, and the packet with the unicast address as the destination address is sent to the unique network interface identified by it. The address hierarchy of the unicast address is very similar in form to the CIDR address structure of IPv4, and they all have consecutive address prefixes and address codes of arbitrary length. IPV9's unicast address has the following forms: aggregate global unicast address, decimal internet address and domain name decision and assignment organization address, IPX address, local IPV9 unicast address, and IPv4 compatible address.

The aggregatable global unicast address and cluster address belong to the unicast address. They are not different in form, but differ in the propagation mode of the message. Therefore, the aggregatable unicast address and cluster address are assigned the same format prefix 0100. Both the local link unicast address and the in-station unicast address are used in the local range. To facilitate the router to speed up the identification of these two types of addresses, 111111111010 and 111111111011 address format prefix are assigned to them respectively.

A. Aggregate Global Unicast Address

The Internet has a tree topology hierarchy. In order to better express this hierarchy, IPV9 introduces a multi-hierarchical addressable address. Organizations at all levels of the Internet are assigned their own identity (address prefix) in the address, and each organization identity is assigned based on the higher-level agency identity to which it is directly affiliated. Different levels of the Internet routing systems can only distinguish subnet identifiers in the address above its level, that is, low-level network structures are transparent in high-level nodes. In this way, the low-level subnets are aggregated at a high level, sharing a high-level subnet number, which are represented by an item in the high-level router routing table.

The aggregatable global unicast address is the most widely used unicast address when a node is connected to the Internet. This kind of address is used primarily to support network vendor-based address aggregation and network intermediary based address aggregation. The use of aggregatable global unicast addresses can effectively aggregate subnets in all levels of routing systems, thereby reducing the size of the routing table.

1) Introduction of Aggregatable Global Unicast Address

The multi-level network structure has good scalability, which is beneficial to solve the problem of routing addressing. Like the telephone network, IPV9 has a good hierarchical structure for aggregatable global unicast addresses, which can have the following three levels:

a) Public topology layer: The public topology layer is a collection of network providers and network intermediaries that provide public Internet transit services.

b) Site topology layer: The site topology layer is limited to specific sites or organizations that do not provide public Internet transit services to off-site nodes.

c) Network interface identification: The network interface identifier is used to identify the network interface on the link.

2) Structure of Aggregatable Global Unicast Address

The IPV9 aggregatable global unicast address consists of six domains: address format prefix (FP), top-level aggregation identifier (TLA), reserved domain (RES), secondary aggregation identifier (NAA), and site-level aggregation identifier (SLA), and network interface identification. In order to reduce the difficulty of readdressing when changing network access, the lengths of these six domains are fixed, the structure of aggregatable unicast addresses is shown in table 1:

TABLE I. AGGREGATE UNICAST ADDRESS STRUCTURE

4	26	18	48 bits	32 bits	128 bits
FP	TLA logo	RES	NLA identifier	SLA identifier	Network interface identifier
←Public topological layer→				Site topology layer	Network interface identifier

a) Format prefix: The format prefix of the aggregatable global unicast address is defined as a "0100" four-bit binary string. With this address format prefix, the routing system can quickly distinguish whether an address is an aggregatable global unicast address or other type of address.

b) Top level aggregation identifier: The top-level aggregate identifier is the highest level in the routing hierarchy. Default router must be given each

active polymerization top of an identifier correspondence, and provide the top aggregation in the identifier represents the address of the region of the routing information. Currently, the top-level aggregation identifier is 26 bits and can support 67108864 network switcher nodes, remote network providers, or backbone network service provider nodes.

c) Secondary aggregation identifier: The organization using two polymerization identification to establish internal addressing hierarchy and identifier within the site which have top level aggregation identifier. The organization with top-level aggregation identifier has 48-bits secondary aggregation identifier space, that is, if the organization directly allocates these secondary aggregation identifiers, it can allocate 248. The 48- bit long secondary aggregation identifier divides the first-level NLA1 of n bits, and the remaining (48-n) bits serve as site IDs.

The allocation scheme of the secondary aggregation identifier is a compromise between route aggregation efficiency and flexibility. When an organization allocates its internal secondary aggregation identifier, it can select an allocation scheme according to its own needs. Establishing a hierarchy allows the network to aggregate to a greater degree at all levels of the router, and to make the routing table smaller. Directly assigning a secondary aggregated identifier simplifies the allocation process, but results in excessive routing table size.

d) Site-level aggregation identifier: Site-level aggregation identifier is used for individual organizations (sites) to establish their internal addressing hierarchy and identity subnets. The site-level aggregate identifier is similar to the IPv4 subnet number, except that the IPV9 site can accommodate a larger number of subnets. The 32-bit site-level aggregation identifier domain can support 4,294,967,296 subnets, which is sufficient to support the subnet size within most organizations.

An organization can directly assign its site-level aggregation identifiers. There is no logical relationship between the site-level aggregation identifiers, and the routing table size of the router is large. It is also possible to divide two or more layers of structures within a site-level aggregation identifier domain.

e) Network interface identifier: The network interface identifier is used to identify the network interface on a link. On the same link, each network interface identifier must be unique. The aggregatable global unicast address ultimately identifies a network interface (or node) at the network interface level. In many cases, the network interface identifier is the same as the link layer address of the network interface, or based on the link layer address of the network interface. The same network interface identifier can be used on multiple interfaces of the same node, which are only treated as one network interface on the network.

B. Local Link Unicast Address

The local link unicast address is used for communication between nodes on the same link. This type of address has a separate address format prefix "1111 1111 1010" for efficient addressing on this link. This type of address is used for automatic configuration of addresses, neighbor detection, and there are no routers on the link. If there are routers on the link, these routers do not forward IPV9 packets to other links which have the local link unicast address as the destination address the source address.

The structure of the local link unicast address is very simple. It consists directly of the address format prefix and the 128- bit network interface identifier, and is filled with 54 bits of 0, as shown in the table 2.

TABLE II. LOCAL LINK UNICAST ADDRESS STRUCTURE

12 bits	116 bits	128 bits
1111 1111 1010	0	Network interface identifier

An in-site unicast address can be used when it is desired to address the network interface of the communication within the site and does not wish to use the global address format prefix. At the same time, the station's unicast address is also used for the addressing of isolated sites that are independent of the Internet, such as addressing in a campus network that is not connected to the Internet.

Because the scope of the unicast address in the station is much larger than the range of the local link unicast address, and a site often contains multiple subnets, the structure of the unicast address in the station is more than that of the local link. The format prefix assigned to the unicast address in the station is "1111 1111 1011". The specific structure of the address is shown in the table 3.

TABLE III. STRUCTURE OF THE UNICAST ADDRESS IN THE STATION

12 bits	84 bits	32 bits	128 bits
1111 1111 1011	0	Subnet identifier	Network interface representation

Similar to the use of the local link unicast address, IPV9 packets with the source address or destination address in the station can only be propagated within the site. The router cannot forward these packets out of the site.

C. Compatible Address

In IPV9, some mechanisms for smoothing the transition from IPv4 /IPv6 to IPV9 have been developed, including the use of existing IPv4 and IPv6 routing systems as tunnel forwarding IPV9 packet technologies. For IPV9 nodes using this technology, it is required to assign several special IPV9 addresses of "IPv4 compatible address", "IPv6 compatible address" and "special compatible address". The specific structure of these addresses is shown in the table 4-7:

TABLE IV. COMPATIBLE ADDRESS FORMAT

10 bits	19 bits	3 bits	64 bits	32 bits	96 bits	32 bits
Prefix	Reserved	Sign	0	Scope	DedicatedIPv6	IPv4address

TABLE V. IPV4 MAPPED ADDRESS FORMAT

96 bits	32 bits	96 bits	32 bits
0[0[0	0	0	IPv4address

TABLE VI. MAPPED ADDRESS FORMAT

96 bits	32 bits	128 bits
1[0[0	0	IPv6 address

TABLE VII. MAPPING ADDRESS FORMAT FOR SPECIAL COMPATIBLE ADDRESSES

96 bits	32 bits	96 bits	32 bits
2[0[0	0	0	IPv4address

IV. CLUSTER ADDRESS STRUCTURE

In many cases, there may be multiple servers on the network that provide the same service at the same time (for example, a mirror server). A host, an application or a user often only wants to get a service without paying attention to which server the service is provided, that is, only one of all these servers is required to serve the user. Anycast transmission mechanism is proposed to meet such needs on the network. The mechanism uses the cluster address to identify the set of servers that provide the same service. When a user sends a message to the cluster address, the network sends the message to at least one server that owns the cluster address.

A cluster address is a type of IPV9 address that is simultaneously assigned to multiple network interfaces. The IPV9 message destined for the destination address of the cluster address will be sent to the interface that owns the cluster address. The routing protocol considers the nearest one, that is, only one interface can receive the packet. The cluster address of IPV9 is allocated from the unicast address and is defined in the same format as the unicast address, that is, the cluster address is formally indistinguishable from the unicast address. When a unicast address is assigned to multiple network interfaces, it is functionally translated into a cluster address. The node that gets the cluster address must perform the appropriate configuration process to recognize that the address is a cluster address.

For each assigned cluster address, it always has a longest prefix P to identify the minimum containment level of all network interfaces that have the cluster address in the network topology. For example, each school in a school has an image of an FTP server, and the minimum inclusion of all of these servers may be the highest level in the school's network structure. The corresponding prefix P is used to identify the highest network level. Within the network hierarchy identified by the prefix P of a cluster address, each member that owns the address must be published as a separate item in the routing system (often referred to as host routing); outside the hierarchy identified by the prefix P All member network interfaces identified by the cluster address can be aggregated into one item to be published in the routing system.

It is worth noting that in the worst case, the prefix P of a cluster address may be 0 in length, that is, the distribution of the network interface that owns the cluster address in the Internet cannot form a topology, so all of these networks are included. The smallest hierarchy of interfaces is the entire Internet. In this case, each node corresponding to the cluster address must be published on the Internet as a separate item. This severely limits the number of such global cluster address sets that the routing system can support. Therefore, the Internet may not support a global set of cluster addresses, or only provide extremely restrictive support.

At present, the use and implementation mechanism of IPV9 for cluster addresses are still being researched and tried. There are three types of cluster addresses that have been identified so far:

- Identify a collection of routers in an organization that provides Internet services. At this time, the cluster address can be used as the intermediate router address in the extension header of the packet source path, so that the packet is converted by any router of the designated network service access organization.

- Identify the set of routers that connect to a particular subnet.
- Identify a set of routers that provide routing information to a certain network area.

Because the experience of using cluster addresses in a wide range is rare, and there are some known problems and dangers in the use of cluster addresses, before accumulating a lot of experience with cluster addresses and finding solutions to cluster address ills, The following restrictions must be adhered to when implementing an IPV9 cluster address:

- The cluster address cannot be used as the source address in the IPV9 message;
- The cluster address can only be assigned to the router at present, but not to the normal IPV9 host node.

Currently, the IPV9 protocol only predefines a cluster address – the subnet router cluster address. This kind of address must be owned and must be identifiable by each subnet router. The specific format is shown in the table 8:

TABLE VIII. SUBNET ROUTER CLUSTER ADDRESS

n bits	256-n bit
Subnet prefix	Host number (all 0)

The entire subnet router cluster address, as its name implies, is the cluster ID of all routers connected to the link subnet. Its purpose is to allow applications on one node to communicate with one of all router collections on the remote subnet.

V. MULTICAST STRUCTURES

Multicast is used when implementing the network multicast mechanism. The IPV9 protocol also adopts a multicast mechanism and specifically designed a multi-purpose address for multicast use. The address space prefixed with the 1111 1111 11 address format in the address space of IPV9 is reserved for multicast. The multicast address is assigned to multiple network interfaces in the same way as the cluster address. The difference between the two is that IPV9 packets with the destination address of the multicast address will be received by all network interfaces that have the multicast address at the same time. This sending process is called multicast. A collection of network interfaces that have the same multi-cast address is called a multicast group.

The multicast address of IPV9 consists of four parts, with "1111 1111 11" as the address format prefix. The specific structure is shown in the table 9.

TABLE IX. IPV9 MULTICAST ADDRESS FORMAT

10 bits	8 bits	4 bits	234 bits
1111 1111 11	Sign	Range of action	Group identification

The remaining three parts of the format followed by the address format prefix are the flag bit field, the address scope field, and the group identification field. The flag bit field consists of 8 bits, the flag bit field uses only the lowest bit of the 8 bits (T bit), and the remaining upper seven bits are reserved. The T bit is called the "temporary address bit" and it indicates that the assigned multicast address is temporarily valid or permanent. The address range is an integer consisting of 4 bits. It is used to limit the distribution range of multicast group members, thus limiting the effective range of the multicast address relative to the sender of

the message during multicast. Group identification field for a multicast group, it is in the low 234 among the entire address format. A multicast group identified by a group identity field may be a temporary or permanent multicast group within a given range.

A. Universal multicast address

In the design of IPV9, some common multicast addresses are predefined, such as reserved multicast address, all-node multicast address, all router multicast address, and the requested node multicast address. These addresses are typically used when neighboring nodes are probed and the address is automatically configured.

1) Reserved multicast address: multicast address with group identifier of 0 can only be reserved but cannot be assigned to any multicast group, that is, the flag bit is 0, the address range is arbitrary, and the group ID is all 0. The addresses at the time are all reserved multicast address addresses.

2) All node multicast address addresses: general multicast addresses 4230774016 [7]1 and 4230775040[7]1 are all node multicast addresses, which identify all nodes within the scope of the node and within the scope of the link. These two addresses function similarly to the broadcast address in IPv4 and are used to send broadcast messages within their corresponding scope.

3) All routers multicast address: It contains the following three general multicast address addresses, which identify all routers in range 1 (scop=1, on the same node), in range 2 (scop=2, on the same link). All routers and all routers in range 5 (scop=5, same site):

4290774016[7]2
4290775040[7]2
4290778112[7]2

4) The requested node multicast address: the requested node multicast address ranges from 4290775040[4]1[4294901760[0 to 4290775040[4]1[4294967295[42949 67295. The requesting node is a node for detection probe target node is the neighbor (there may be multiple simultaneous). In the process of neighbor discovery, the requested node multicast address is used as the address identifier of the requested target node, and its scope is on the local link.

B. Distribution of multicast addresses

The assignment process of the multicast address is the assignment of the multicast address group identification. In the format structure of the multicast address, the group representation is allocated 234 bits of space. In theory, these 234 bits can allocate 2 234 different group identifiers. However, because the current multicast Ethernet embodiment only the lower 64 bits of the IPV9 multicast address mapped to the MAC address of IEEE802, and the processing of the token ring network multicast address will also be different, in order to ensure IPV9 can be generated on the basis of the multicast address of the MAC address is unique, is currently only available in the 234 bit group identification assigned to the lower 64 bits of the group identifier, the remaining 170 bits are reserved (set to all zeros), The multicast address format is shown in table 10.

TABLE X. MULTICAST ADDRESS FORMAT WITH 64- BIT GROUP IDENTIFICATION

10 bits	8 bits	4 bits	170 bits	64 bits
1111 1111 11	Sign	Range of action	0	Group identification

The above scheme limits the permanent group identification of the IPV9 multicast address to 264, which has been able to meet the currently foreseeable needs. If the need for group identification exceeds this

limit in the future, multicast will still work but the processing speed will be slightly reduced; with the development of network equipment in the future, the 234-bit group identification space can be fully utilized.

VI. SUMMARY

IPV9 has a huge address capacity, can be compatible with IPv4 and IPv6, and USES a special encryption mechanism to make the network environment more secure. The application of IPV9 is being promoted in China, especially in the government, banking and other departments. This paper summarizes the current IPV9 address structure, including IPV9 unicast address structure, cluster address structure and multicast address structure, etc., and introduces the compatible address format of IPv4, IPv6 to IPV9 transition, and the aggregatable global unicast address. The aggregation logo provides a corresponding basis for future application development based on IPV9.

REFERENCE

[1] Xie Jianping etc. A method of assigning addresses to network computers using the full decimal algorithm[P]. CN: ZL00135182.6, 2004.2.6.

[2] Xie Jianping etc. Method of using whole digital code to assign address for computer [P]. US: 8082365, 2011.12.

[3] Zang Qianli etc. A Survey on IPv6 Address Structure Standardization Researches [J]. Chinese Journal of Computers. 2019: 1-23 [2019-03-04].

[4] V. Fuller, T. Li,Network Working Group. Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy, RFC-1519, 1993.9.

[5] Xie Xiren. The concise tutorial on computer network [M]. Publishing House of Electronics Industry, 2011.

[6] Information technology-Future Network- Problem statement and requirement-Part 2: Naming and addressing, ISO/IEC DTR 29181-2, 2014, 12.

Rotation center calibration based on line laser rotating platform

Lei Doudou
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710032, China
e-mail: ccdd007123@qq.com

Yao Huimin
Eighth of production plant, the company china petrdeum, Changqing oilfield, Xi'an
Xi'an, 710021, China

Liu Baolong
School of Computer Science and Engineering
Xi' an Technological University
Xi'an,710032 China
e-mail: liu.bao.long@hotmail.com

***Abstract*—Line lasers are of great significance in many fields such as industrial inspection, machine vision, cultural relics identification, mechanical design, and medical oral cavity. The three-dimensional reconstruction of the line laser can accurately obtain the three-dimensional information of the surface of the object, and quickly complete the three-dimensional contour reconstruction of the object to be tested. In the online laser rotation scanning, the object rotates around a certain point, which is a rotation center, and the calibration of the rotation center is the main factor that restricts the accuracy of the three-dimensional contour. At present, the calibration of the center of rotation is mainly obtained by the characteristics of a circle (ball, cylinder, cone, etc.). This paper mainly introduces the basic process of rotating scanning, rotating center, and rotating methods as well as their advantages and disadvantages. First, the basic process of rotating scanning is briefly introduced. Secondly, the definition and content of the rotating center are introduced. Then, the calibration methods of three rotating centers (ellipse fitting method, symmetry method, plane fitting method) are introduced. Finally, the advantages and disadvantages of the three calibration methods and their respective applications are summarized.**

Keywords-Line laser; rotary scanning; Rotation center; calibration

I. INTRODUCTION

In today's life, two-dimensional information can no longer meet people's daily needs. The three-dimensional information has thus been deeply researched and developed. Among them, the line laser is widely used in the three-dimensional reconstruction process. Line laser three-dimensional scanning is to project one or more line lasers to the measured object, extract the laser stripe in the image, and calculate the three-dimensional data of the surface of the laser line, usually using high-precision three-coordinate, rotating platform or camera alignment The laser sensor performs positioning to complete three-dimensional scanning of the surface of the object to be measured, and obtain surface data of the three-dimensional object[1][2].

According to the different mechanical displacement platforms, mechanical scanning mainly has two implementations of translation platform and rotary platform. Rotating scanning is more convenient and faster. A more accurate rotation center calibration can improve the accuracy of point cloud reconstruction and improve the 3D contour reconstruction of the measured object.

The reconstruction of the rotating platform can be divided into three types according to the different movement modes: the first is that the camera rotates around the rotating axis [3], and the measured object does not move; the second is that the camera does not move, and the object rotates with the rotating platform [4] The third is that the camera and the object are combined and rotated at the same time[5].

The rotating platform is suitable for scanning objects with swivel features. The object is placed on a rotating platform for linear laser rotation scanning. At

this time, the visible object is rigidly transformed around the axis of the rotating platform [6], and the left and right camera point clouds can be constructed by using the rotation center and the rotation angle obtained after the platform calibration process. The rotation matrix between the two, the rotation matrix is multiplied by the current point cloud, the point cloud obtained by the left and right cameras can be registered to the same coordinate system, thereby realizing the automatic registration of the point cloud on the surface of the rotating platform [7].

II. CAMERA CALIBRATION

Calibration is simply a matter of establishing a reference point between a pixel coordinate system of an image and a world three-dimensional coordinate system. The essence of the transformation relationship is the geometric principle of camera imaging. The ultimate goal of calibration is to obtain the camera's internal parameters as well as external parameters. The internal parameters of the camera are determined by the camera's own characteristics. The external parameters of the camera are used to establish the mutual conversion relationship between the local world coordinate system and the camera coordinate system in the actual process [8][9]. The camera's parameters have a direct impact on the accuracy of the reconstructed model, so the accuracy of the camera parameters is very important. In general, camera calibration is required before solving the center of rotation.

III. ROTATION CENTER CALIBRATION

Because the line laser scans once, it can only measure the surface of the object to be measured at a given angle of view. If you want to measure the contour of an object for a week, you can measure it by rotation, measure the object from multiple angles of view, and point cloud data from multiple angles of view. Spliced in the same coordinate system. Accurately calibrating the center of the turntable (rotation center) is the key to rotating measurements and multi-view assembly.

Rotation Center: In a plane, a figure rotates a certain angle around a point O to get the other figure to change into rotation, and point O is the center of rotation.

During the rotational scanning, the measured object starts from a fixed angle and starts to rotate 360 degrees around the axis of rotation or the center of rotation. However, the center of rotation of the rotating platform is unknown. In order to obtain the three-dimensional contour of the rotating object, it is necessary to obtain the rotation center of the rotating platform by means of a calibration block or a pasting marker point. After the center of rotation is obtained, the subsequent rotation and splicing can be performed. Since the subsequent splicing work is spliced according to the position of the center of rotation, the extraction work of the center of rotation is very important.

The schematic diagram of the line laser double triangle rotation scan is shown in the figure below, where the center of rotation is the center of the stage.

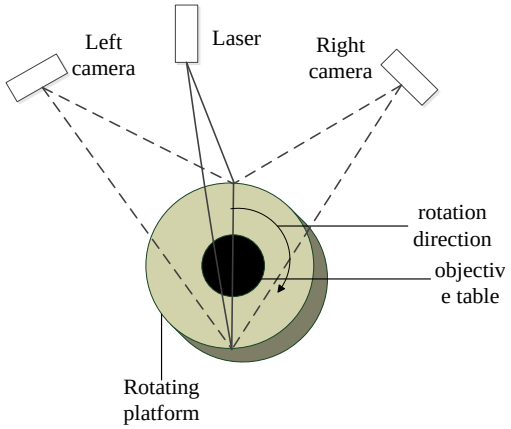


Figure 1. Schematic diagram of line laser double triangle rotation scanning

IV. ROTATION CENTER CALIBRATION METHOD

A. *Ellipse fitting method*

The center of rotation can also be obtained by dividing the plane edge of the rotating platform in the left and right images, and then performing ellipse fitting on the obtained plane edge, and obtaining the center coordinates of the ellipse by the least squares fitting method. It is the center of rotation of the rotating platform [10].

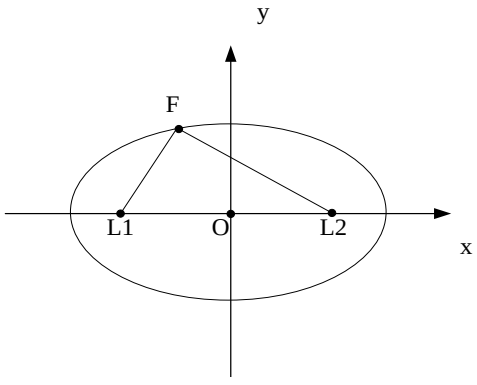


Figure 2. Ellipse Fitting

As shown in Figure 2 above, Point $F(x,y)$ is a point on the ellipse, and the focus of the ellipse is $L_1(x_1,y_1)$ and $L_2(x_2,y_2)$.

$$OL_1 + OL_2 = 2c \tag{1}$$

Since the sum of the distances from any point on the ellipse to the two focal points is a constant 2a, there is an error between the sum of the actual distances, and the error is θ. As shown in the following formula (2):

$$FL_1 + FL_2 = 2a + \theta \tag{2}$$

The above formula (2) is specifically expanded as follows:

$$\sqrt{(x-x_1)^2+(y-y_1)^2} + \sqrt{(x-x_2)^2+(y-y_2)^2} = 2a + \theta \tag{3}$$

Using the above formula, the point cloud of the elliptical edge can be fitted by the least squares method, and the estimated values of the five parameters are obtained, and then linearized and solved iteratively.

The criteria for the iterative solution process are:

It is necessary to eliminate the edge point cloud data whose absolute value of the error θ is greater than or equal to 2.6β after each ellipse fitting. (β: standard error of unit weight after each iterative fitting)

Between two adjacent iterative fittings, the absolute value of the distance of any elliptical focus position must be less than a certain pixel value (typically 0.001 pixels). If it is greater than or equal to this pixel, the iteration will end immediately.

In the formula (3), the order:

$$l_1 = \sqrt{(x-x_1^{'})^2+(y-y_1^{'})^2} \tag{4}$$

$$l_2 = \sqrt{(x-x_2^{'})^2+(y-y_2^{'})^2} \tag{5}$$

Let FL_1, FL_2 be partial to x_1, x_2, y_1, y_2. Then the above formula expands to:

$$\frac{x-x_1^{'}}{l_1}\Delta x_1 + \frac{y-y_1^{'}}{l_1}\Delta y_1 + \frac{x-x_2^{'}}{l_2}\Delta x_2 + \frac{y-y_2^{'}}{l_2}\Delta y_2 + 2\Delta a = l_1 + l_2 - 2a_0 + \theta \tag{6}$$

$x_1^{'}$, $y_1^{'}$, $x_2^{'}$, $y_2^{'}$ represents the initial value of the coordinate of the focus, and the focus satisfies the relationship as follows:

$$x_1 = x_1^{'} + \Delta x_1, \quad x_2 = x_2^{'} + \Delta x_2 \tag{7}$$

$$y_1 = y_1^{'} + \Delta y_1, \quad y_2 = y_2^{'} + \Delta y_2 \tag{8}$$

$$a = a_0 + \Delta a \tag{9}$$

The initial position obtained is used as the initial value, and the point cloud data of the ellipse edge is fitted by the least squares method step by step iteration [11], then the parameter (x_1, x_2, y_1, y_2, a) can be solved, and the elliptical center $O(x_0,y_0)$ of the last fitting is:

$$x_0 = \frac{x_1+x_2}{2}, \quad y_0 = \frac{y_1+y_2}{2} \tag{10}$$

B. Symmetry method

Since the image on the rotating platform has symmetry after being rotated by 180 degrees and is symmetrical about the center of rotation, a plurality of laser lines can be selected on the auxiliary pattern to perform calculation of the center of rotation to ensure accuracy. Finally, the parameters obtained can be optimized by methods such as BP neural network.

In order to accurately calibrate the center of rotation, the straight line equations of the two straight lines s_1s_2 and $s_1^{'}s_2^{'}$ are fitted on the premise that the rotation angle of the rotating platform is known. Find the intersection O between the two lines. The intersection point O is the rotation center of the rotating platform. The point s_1 is located at the position of the point $s_1^{'}$ after being rotated by 180 degrees, and point s_2 is rotated 180 degrees and is located at point $s_2^{'}$. s_1, O, $s_1^{'}$ three points are collinear, and after rotation, are symmetric with respect to the rotation center O before rotation [12]. The principle of symmetry is shown in Figure 4.2 below.

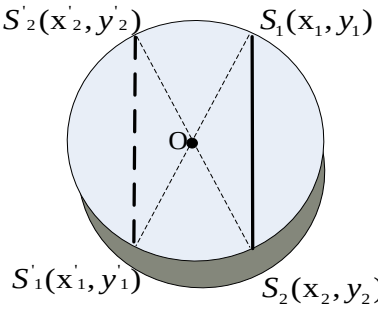


Figure 3. Symmetrical view of the center of rotation

The calibration process of the symmetrical rotation platform is:

(1) Firstly, the rotating platform is adjusted to the working position, the auxiliary pattern is pasted on the rotating platform or the circular calibration block is placed, and the line laser is passed through the center of the rotating platform;

(2) Rotate the rotating platform at an angle (15 degrees) and start collecting data;

(3) Extracting the center coordinates of the laser stripe in the data as pixel coordinates;

(4) Calculating the world coordinates corresponding to the pixel coordinate system and storing the sample set;

(5) After rotating 180 degrees, the sample set is derived for calculation of the rotation parameters.

C. Plane fitting

In the three-dimensional reconstruction of the rotating scanning mode, the obtained rotating point cloud is plane-fitted to fit the rotation center of the rotating platform [13]. The line laser emitter emits a laser beam that intersects the surface of the calibration block. As shown in the figure below, point A emits a line laser, and BC is the line of intersection between the laser and the calibration block. The plane formed between points A, B, and C is a light plane. The points in the light plane (Δ ABC) conform to the plane equation (11).

In online laser scanning, the acquired point clouds are all in the light plane, so all point clouds conform to the plane equation (11):

$$ax + by + cz + d = 0 \tag{11}$$

The n point cloud data obtained by the rotation scan are sequentially brought into the upper equation of the light plane.

$$\begin{cases} ax_1 + by_1 + cz_1 + d = 0 \\ ax_2 + by_2 + cz_2 + d = 0 \\ \vdots \\ ax_n + by_n + cz_n + d = 0 \end{cases} \tag{12}$$

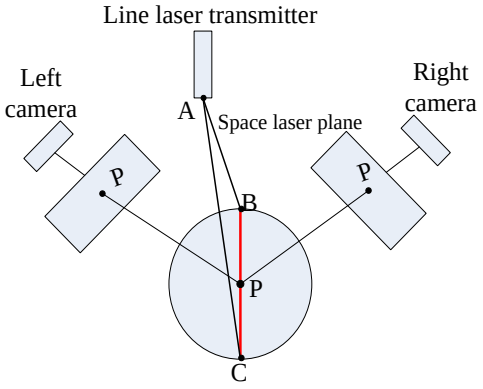


Figure 4. Light plane equation

There are 4 unknown n equations, and the values of four unknowns a, b, c, d can be solved by least squares method. The center of rotation of the rotating platform can be expressed as:

$$O = (\frac{1}{n}\sum_{i=1}^{n} x_i, \frac{1}{n}\sum_{i=1}^{n} y_i, \frac{1}{n}\sum_{i=1}^{n} z_i) \tag{13}$$

In general, by gradually increasing the height of the rotating platform, a series of center points can be fitted in a straight line, so that the rotation axis can be calibrated. Then through the Rodrigo rotation formula [14], we can complete the coordinate transformation and so on.

The comparison between the calibration methods of the center of rotation is shown in Table 1 below.

TABLE I. COMPARISON BETWEEN ROTATION CENTER CALIBRATION METHODS

calibration method	Advantage	Disadvantage	Applicable situation
Ellipse fitting method	It can reduce the error in the measurement process with high precision.	During the fitting process, the number of iterations is variable and it takes a lot of time.	Due to interference of factors such as position and angle, the extracted edge contour is elliptical. Or the calibration block is elliptical.
Symmetry method	The principle is simple and easy to understand, and the accuracy is high.	It is necessary to select multiple locations for testing, and to obtain an average value, which takes a lot of time.	Suitable for circular rotating platforms. Or a circular calibration block. The point cloud obtained by scanning has higher precision.
Plane fitting	The operation is simple, no need to manually paste the mark points, and the speed is fast.	The accuracy is low.	Suitable for circular rotating platforms. Or a circular calibration block.

V. CONCLUSION

This paper introduces the basic process of linear laser rotation scanning. The measured object starts from a fixed angle and starts to rotate 360 degrees around the rotation axis or rotation center to obtain the three-dimensional contour of the rotating object. The basic knowledge of the rotating center of the rotating platform parameters during the rotating scanning process is introduced, and the calibration methods of the three rotating centers are summarized. The principles and steps of these three calibration methods are analyzed in detail. The advantages and disadvantages of the three methods and their application are summarized. It lays a theoretical foundation for the study of the calibration method of the rotating center.

ACKNOWLEDGMENT

This work is partially supported by Science & Technology Program of Weiyang District of Xi'an City with project “201836".

REFERENCES

[1] Choi S, Kim P, Boutilier R, et al. Development of a high speed laser scanning confocal microscope with an acquisition rate up to 200 frames per second[J]. Optics Express, 2013, 21(20):23611-23618.

[2] Wei Z, Huadong G, Qi L, et al. Fine Deformation Monitoring of Ancient Building Based on Terrestrial Laser Scanning Technologies[C].IOP Conference Series: Earth and Environmental Science. IOP Publishing, 2014:682-691.

[3] Zhong S D , Xiong J , Liu Y . 3-D reconstruction technology based on full circle multiple views[J]. Robot, 2004, 26(6):558-562.

[4] Wei H . An Approach for Multiple-view Data Capture by a Single-view 3D Camera Using a Simple Revolve Device[J]. Journal of Applied Sciences, 2001.

[5] Zhang A W, Ming-Zhe L I, Shao-Xing H U. 3D Surface Measurement Key Technique Based on Computer Vision[J]. Systems Engineering & Electronics, 2001.

[6] Zhou L, Zheng S. A Registration Algorithm for Point Clouds Obtained by Scanning Objects on Turntable[J]. Acta Geodaetica Et Cartographica Sinica, 2013, 42(1):73-79.

[7] Xi L , Yuexian Z , Renju L I , et al. 3-D surface integration in structured light 3-D scanning[J]. Journal of Tsinghua University, 2002, 42(4):477-480.

[8] Zhang Z. A Flexible New Technique for Camera Calibration[J]. Microsoft Research, 2000, 22(11):1330-1334.

[9] Tsai R Y. A versatile camera calibration technique for high-accuracy 3D machine vision metrology using off-the-shelf TV cameras and lenses[J]. IEEE Journal on Robotics & Automation, 2003, 3(4):323-344.

[10] Cheng H , Huaming Y, Zgang J . Structural light based computer vision [M]. National Defense Industry Press, 2015.

[11] Mingjing C , Yuanmin F , Jie C . Fitting of circular curve based on least square method and iterative method[J]. Science of Surveying & Mapping, 2016.

[12] Fuxing L. Accuracy Analysis of Determining Coordinates of Rotation Center of Indexing Table[J]. Mechanical industry standardization and quality, 2005(10):28-29.

[13] Wq. 3D Reconstruction Based on the Structured light and Turntable[D].University of Electronic Science and Technology,2017.

[14] Zelinsky A . Learning OpenCV---Computer Vision with the OpenCV Library (Bradski, G.R. et al.; 2008)[On the Shelf][J]. IEEE Robotics & Automation Magazine, 2009, 16(3):100-100.

A Full Decimal Method of Address Assignment for Networked Computer

Zhan Xin
Department of Information Technology
Xi'an Medical University
Xi'an, China
e-mail: 282981652@qq.com

Jin Liming
[1.]Chinese Decimal Network Working Group
[2.]Shanghai Decimal System Network Information Technology Ltd.
e-mail: jlm1978@163.com

Xie Jianping
[1.]Chinese Decimal Network Working Group
[2.]Shanghai Decimal System Network Information Technology Ltd.
e-mail: 13386036170@189.cn

Lai Jiawen
[1.]Chinese Decimal Network Working Group
[2.]Shanghai Decimal System Network Information Technology Ltd.
e-mail: 13918335279@163.com

***Abstract*—The full decimal method of address assignment for networked computers and intelligent terminals which input into the computer through various input devices of the computer and intelligent terminals is realized, and then, the external address of networked computer and intelligent media stored in the database and the internal arithmetic address are created correspondingly through a variety of transmission media by combination of different computer hardware and software. The new address assignment method can provide sufficient address space for development of Internet in the future, and it also provides enough address for application of various personal information household appliances and logistics in electronic commerce and other entities and personal communication terminals while ensuring multiple levels of address structure. This paper mainly introduces the decimal address allocation algorithm and address format, which provides a solid foundation for the next generation Internet architecture design.**

Keyword-Decimal; Future Network; IPV9; Address Assignment

I. INTRODUCTION

With the rapid development of science and technology, the world has entered an information age of data communication. The most famous data network is the Internet, which can be seen all over the world. In 1969, in order to develop a computer network capable of resisting nuclear attacks, the US Department of Defense funded the establishment of a packet-switched network named ARPANET, which was the earliest prototype of today's Internet and was regarded as the forerunner of the information superhighway. Nowadays, almost all the countries and regions have joined the Internet. China has also established a number of international exports connected to the world's largest Internet and achieved rapid increase in user terminals.

Every single computer connected to the Internet shall be provided with one and unique address so that the information can be correctly transmitted to the destination through the Internet. At the present, there are three methods for address preparation in and out of

China: first, the "IP address", which is composed of four segment of numbers separated by decimal points; second, the "domain name", which is generally composed of five character strings (subdomains); and third, the "Chinese domain system", which is composed of three levels of domain names separated by decimal points and slashes. Although the above address system guarantees each computer a unique address, it is with the unfavorable disadvantages of complex and not uniform, and is difficult to remember and input.

At present, the addressing scheme used in the Internet is still based on the original IPv4 protocol, which uses four segments of 8-bit decimal numerals to allocate the addresses of hosts and other devices connected to the Internet. In the meantime, the addresses are marked by the method of "dotted decimal notation". Although those addresses seem to meet the needs of the entire world in the early stage of Internet development and IPv4 made incredible success, in the last two decades in the 20th century, Internet ushered rapid development all over the world and the number of hosts connected to the Internet have been doubled every year, therefore, current amount of addresses can no longer meet such development momentum. What's more, addresses have been more and more extensively applied in logistics code in e-commerce, space code, identity code, digital currency and three-dimensional geographical code and other intelligent terminals, the existing address assignment techniques fail to meet the needs of social development. It is of vital significance to develop an address identification method that can meet activities of human for several years.

II. DECIMAL ADDRESS ASSIGNMENT ALGORITHM

The algorithm in this study can provide a new address assignment method that offers sufficient address space for development of Internet in the future, and provides enough address for application of various personal information household appliances and logistics in electronic commerce and other personal communication terminals in a simpler, more convenient way under a lower cost while ensuring multiple levels of the address structure.

The method by which address assignment of a networked computer by full-digital codes is with the following characteristics: the foresaid network access number refers to the stipulated numeral number of the website established in accordance with the national and regional regulations; the foresaid telephone number consists of international direct distance dialing codes of the country of the telephone user, area code for domestic direct dialing of the user and the telephone number of the organization where the user works or the user's personal telephone number; the classification number is the numeric number preceded by the country or the area for unified classified business categories.

The technical scheme is: a full decimal method of address assignment for networked computers and intelligent terminals that is characterized with, address inputting into the computer through input devices of networked computers and intelligent terminals, such as keyboard, bar code, two-dimensional code input device, visual input device and voice input device, and corresponding preparation of external address of networked computer and intelligent media stored in the database and the internal arithmetic address by combination of various computer hardware and software via a variety of transmission media. The address assignment is conducted by the following steps:

1) External addresses of all networked computers and intelligent terminals are localized at decimal numbers with the representing range of all decimal integers from 100 to 10256, address are input into the computers via input ports of networked computers and intelligent terminals such as keyboard, voice input device etc.;

2) Internal address of all networked computers and intelligent terminals are localized at binary numbers

with the representing range of all decimal numbers from 20 to 21024;

3) The addresses can either be corresponded to the binary internal addresses either by the method through which address is with fixed length but variable location or address is with fixed location but variable length;

4) In addition to the external addresses, the above mentioned database also stores the original domain names applied in the form of numbers, English and Chinese and other different languages, as well as communication numbers such as the existing telephone numbers, area numbers, city numbers, mobile phone numbers, MAC address, and the latest digital domain names based on decimal coding;

5) The address in the database is directly corresponding to the binary internal address of the computer, and data flow is pointed to the host via computer hardware and software, for instance, the gateway through optical cable through microwave and coaxial cable and other transmission media; the decimal address for character domain name can be found after being resolved through a domain name resolver and pointed to the address of the host, the telephone number; by pointing to the gateway, the mobile phone number and other communication numbers are directly indicated in the communication system to which the communication number is belong.

III. ADDRESS FORMAT AND ALGORITHM

In all the address assignment methods for networked computers and other intelligent terminals mentioned above, the entire external addresses is evenly divided into 4 domains, 8 domains, 16 domains or 256 domains and each domain address is with the numerical range of the decimal integers from 100 to 1064, 100 to 1032, 100 to 1016 or 100 to 101. In a corresponding way, the internal address is also evenly divided into 4 domains, 8 domains, 16 domains or 256 domains and each domain address is with the numerical range of the binary numbers from 20 to 2256, 20 to 2128 , 20 to 264 or 20 to 24.

Each domain address must be separated from each other by a separator. If there is a contiguous all-zero domain within the foresaid address or the internal address, a pair of braces or square brackets can be used to replace the all-zero domain.

If there are more than one contiguous all-zero domain in the address or internal binary address, each contiguous all-0 domain may be replaced by a pair of braces or square brackets, and a Arabic numeral are used to mark the specific amount of all-zero domains in the segment of domain within the brackets.

When there is a continuous segment of Arabic numerals found in the foresaid address or one domain of the internal binary address, the segment of Arabic numerals can be replaced by a pair of round brackets and the omitted numerals, the amount of connectors and omissions shall be clearly marked from the left to the right within the round brackets.

In addition, an external address is an address with a multilevel structure, which can be the interface of a single network, namely a unicast address. The unicast address structure is with the following three levels.

1) Public topology layer: a collection of network providers and network switching equipment for public Internet switching service. The public topology layer consists of a address prefix, top-level aggregation identifier, reserved domain, and second-level aggregation identifier.

2) Station topology layer: a specific local station or organization that not provides public Internet switching service outside the station. It is composed of a station-level aggregation identifier.

3) Network interface identifier: it is a network interface used for identifying the link. Besides, the foresaid second-level aggregation identifier can be further divided into internal multilevel hierarchical

structures and the foresaid station-level aggregation identifier can be used to establish its internal addressing structure and identification sub-network, the foresaid network interface identifier can be used in several interfaces at the same node.

In many cases, communication between network nodes is limited to a relatively independent region; there is no need for global aggregation of unicast address. But it is necessary to provide a address specially used for local communication, namely, local unicast address, which can be applied in communication between nodes at the same link and generating the unicast address of the local link with the structure of address format prefix and network interface identifier and a zero in the middle.

The local unicast address can also be applied in addressing of the communication Internet interface within the range of the station and generating the unicast address in station with the structure of a format prefix, sub-network identifier and network interface identifier, together with a 0 between the format prefix and sub-network identifier.

The address coding method in this study also defines some addresses for special purposes. For example, the address composed of all zeros belongs to a unspecified address and cannot be assigned to any node, which means that the network interface has not obtained a formal address for the time being.

In addition, some addresses can be assigned to more than one network interfaces at the same time, and generate a cluster address with the same structure of that of the unicast address. The address can also be assigned to a multicast address, and the address message with the destination of a multicast address would be received simultaneously by all the network interfaces provided with the multicast address.

The technical scheme adopting the above address assignment method provides sufficient address space for the development of the Internet in the future, realizes simpler address representation, convenient use and more standardized address assignment. Meanwhile, the technical scheme has given full consideration to the size of routing table of the existing router and the current computing power of the computer.

The way to Internet access with the address prepared by the above coding method is characterized with: successful access to Email or the Internet realized after inputting the address into the computer modem via a push-button dialing telephone or the computer keyboard and linking into corresponding digital code, which is translated into a IP address or Chinese domain name system, all full-digital coded address is corresponding to an existing IP address or Chinese domain name system.

IV. ASSIGNMENT EXAMPLES

The specific address assignment algorithm is fully explained by the following examples:

A. Example I

Through this algorithm, external address of networked computers and intelligent media stored in the database and the internal arithmetic address are created correspondingly.

We can evenly divide the entire external address into 8 domains with each address of a decimal integer from 100-1032 and square brackets are used to separate all the 8 domains. Thus, the address is in the format of Y]Y]Y]Y]Y]Y]Y]Y], in which, every Y represents a domain address in the form of a 32-bit decimal number. The entire internal address is also divided into 8 domains with each address of a binary number from 20-212 in the format of X]X]X]X]X]X]X]X], in which, every X represents a domain address in the form of a 128-bit binary number.

For instance:

000000000333897322227788303783030]00000000000000000000000000000]00000000000000000000000000000]00000000000000000000000000000]00000000000000000000000000000]0000000000

9875679484593909387401]0000000000897465383920958

In this address, the multiple continuous zeros at the left part of each decimal number can be omitted but the all-zero decimal numbers shall be represented at least by a zero. Thus, the above address can be written as:

3338973222277883037830 3]0]0]0]0]98756794845939093 87401]989989021893]897465383920958

For further simplifying the address presentation, the continuous zeros in the address can be replaced by a pair of "[ ]". For instance, the above address can be further simplified as:

3338973222277883037830 3[ ]98756794845939093 87401]989989021893]897465383920958

For another instance:

0] 0] 0] 0] 0] 0] 0] 1 can be abbreviated as [ ] 1or[7] 1

0] 0] 0] 0] 0] 0] 0] 0 can be abbreviated as [ ] or [8]

It should be noted that in abbreviation of the above addresses, you can only use "[]" once to represent a contiguous all-zero field, because multiple uses of [] can result in ambiguous addresses.

For instance, address

0] 0] 0]12345678]987654]0]0]0 can be abbreviated as:

[3]12345678] 987654][ ]or[3]12345678]987654][3], also 0] 0] 0]12345678]

987654][3].

but not [ ]12345678]987654][ ], otherwise, the number of all-zero fields of the left and right part of the address may be confusing during restoration of the address and then result in ambiguous addresses.

Besides, for the purpose of further simplification of the address, if there is a continuous sequence of the same Arabic numeral in a address domain, such sequence can be replaced by a pair of round brackets, and the omitted numerals, the number of separators and omissions shall be clearly marked from the left to the right in the brackets.

For instance:

0]0]12345678000000000]987654000000]9800980000]0]0]0] can be abbreviated as [ ]12345678(0/9)]987654(0/6)]980098(0/4) [3]

In the process of address preparation of networked computers and intelligent terminals, the external address must be corresponding with the internal binary address. For such purpose, the method by which address with fixed length and variable location is adopted to make the two corresponding with each other in this example.

For instance, the external address [7]19 will be corresponding to the internal binary address [7](0/251) 10011, and the address [7]21 will be corresponding to [7](0/251)10101.

The address prepared by the method mentioned above can be assigned to network interfaces, and if assigned to single network interface, the identifier is then regarded as a unicast address, and message with the destination of a unicast address will be delivered to the only network interface identified by itself. Unicast address is with the same good flexibility as that of the multilevel network structure, which is good for solving the difficult problem of router addressing. For instance, a w aggregation global unicast address is provided with three layers, namely the public topology layer, station topology layer and network interface identifier, in which, the public topology layer is consisted of a address prefix (FP), top-level aggregation level(FLA), reserved domain (RES) and second-level aggregation identifier (NLA), the station topology layer is consisted of station-level aggregation identifier, and the foresaid network interface identifier is merely consisted of network interface identifier. The specific structure is as shown in Table 1 in the following:

TABLE I. STRUCTURAL TABLE OF GLOBAL UNICAST ADDRESS

FP(4bits)	TLA Identifier (26 bits)	RES(18bits)	NLA Identifier （48 bits）	SLA Identifier (32 bits)	Network Interface Identifier (128 bits)
← Public topology layer →				← Station-level topology layer →	← Network interface identifier →

For instance, the FP of an address is 1001, TLA identifier is 8960, RES is 9806, NLA identifier is 9999999, SLA identifier is 8887, and the network interface identifier is 0, then, the entire address is identified by 1001(0/24)8960](0/4) 9806(0/14)] (0/25)9999999](0/28)8887][4].

In such address, by the format prefix routing system, it is easy to tell whether the address is a unicast or other type of address. The top-level aggregation identifier is the highest level at the routing hierarchy, and in case of missing of a router, every top-level aggregation identifier shall be provided with a corresponding item in the routing table together with the routing information of provided with top-level aggregation identifiers shall employ second-level aggregation identifiers in establishment of addressing hierarchical structure and identification of internal stations in the process of internal addressing. And any organization is free to select the assignment plan according to their own needs in allocation of their second-level aggregation identifiers so as to establish their own internal addressing hierarchy. Establishment of a hierarchical structure is conducive to aggregation of routers at all levels to be greater extent, and realization of a smaller size of the routing table. A structure can be established as shown in Table 2.

TABLE II. HIERARCHICAL STRUCTURE

N L A1	Station Identifier

Station-level aggregation identifiers are used for recognition of establishment of internal addressing hierarchical structure and identification of sub-network number by some organizations (stations). The structure can be shown in Table 3 in the following.

TABLE III. STRUCTURE OF STATION-LEVEL AGGREGATION IDENTIFIERS

S L A1	Sub-network number

In which, the amount of the hierarchies in the station-level aggregation identifier field and the length of SLA identifier at all levels shall be decided by the organizations themselves according to the topology layer structure of their internal sub-network.

For a global unicast address prepared and assigned by the above method; address preparation of a station itself is relatively independent of that of the Internet. If a station needs to be readdressed, among all the addresses within the station, only the two parts, namely the top-level aggregation identifiers and second-level aggregation identifiers (public topology layer) need certain modifications and the station-level aggregation identifiers and network interface identifiers can remain the same. With such assignment approach, great convenience is brought to management and allocation of Internet network addresses.

B. Example II

In this example, unified address assignment for various computers and intelligent terminals are basically conducted by the same steps as in Example I, but corresponding preparation of external address and internal address can be conducted by way of address with fixed location and variable length. By this method, a variety of external addresses of all computers and intelligent terminals are localized at decimal numbers with the representing range of all decimal integers

between 100 and 10256; and internal addresses of all computers and intelligent terminals are localized at binary numbers with the representing range of all binary numbers from 20 to 21024. And then a method by address with fixed location and variable length can be adopted to correspond the external addresses with binary internal addresses. To be specific, every bit of the decimal number of the external address are corresponding to 4 bits of binary numbers of the internal address of the computer.

For instance, external address of [ ]7]7]7]7]7]8]8]3]3] can be corresponding to the binary internal address of [ ]0111]0111]011l]011l] 0111]1000]1000]0011]0011]. In this example, every bit of the decimal number of the address is corresponding to 4 bits of binary numbers of the internal address.

In the technical scheme employed in Example I and Example II, external address and binary internal address can be evenly divided into 4 domains, 16 domains or 256 domains, and the above mentioned address can be assigned to more than one network interfaces at the same time to foster a cluster address with the same structure of that of unicast address. Besides, the foresaid address can also be assigned to multicast address. Message with the destination of multicast address can be received simultaneously by all the network interfaces provided with the multicast address. The address coding method in Example I and Example II above also defines some addresses for special purposes. For example, the address composed of all zeros belongs to a unspecified address and cannot be assigned to any node, which means that the network interface has not obtained a formal address for the time being. If the address is all one, namely the local loopback address, it is expected to loop back the message to itself at a certain node. The local loopback address is usually used when a test is conducted to see whether a protocol stack works properly.

V. ASSIGNMENT ALGORITHM INTERPRETATION

The method by which address assignment of a networked computer by full-digital codes, including full-digital coded address consisted of network access number, telephone number and classification number. The above mentioned network access number refers to the stipulated numeral number of the website established in accordance with the national and regional regulations, for example, the network access number of “Shanghai Hotline” in Shanghai, China is “8888”; the foresaid telephone number consists of the international direct distance dialing codes of the country of the telephone user, the area code for domestic direct dialing of the user and the telephone number of the organization where the user works or the user’s personal telephone number, for example, the telephone number is 008602162572047, in which, 0086 is the international distance dialing code in China, 021 is the area code of Shanghai, and 62572047 is the user's phone number, the three parts jointly serve as "telephone number" in the code. This is the key reason why this research adopts the full-digital character code address assignment -- it is simple, easy to remember and would never be duplicated. The classification number is numeric number preceded by the country or the area for unified classified business categories. Such digital numbers can be established according to the regulations of the country, area or website of the user, and can either be specified at the main category or subcategory level.

Since not all access is to be done with subcategories. Therefore, in general, those numbers are only specified at a main category level. In such case, digital number of the subcategories can be led after the category number by way of option. In actual use, if customers want to encrypt their addresses, the confidential digital numbers can be led after network access number or telephone number, which can be provided by customers themselves and registered in the address preparation organizations. In the process of use,

customers can choose telephone number dialing or input all the correct digital numbers in a continuous way via computer keyboard and surf the Internet after successful connection, which is convenient and efficient.

Given that many users surf the Internet only to send and receive E-mails, and only even apply for a work Email, Internet service providers shall establish an Email for the user which is usually named with three parts of a user name, Email server and "@" and indicated by character strings when users apply for an Internet account. For easy and unified input, Email addresses can be prepared by full-digital coding, and consist of digital number of the user name and the digital number of the domain name of the Email server which the Email is belongs to.

When the above coding method is adopted in Email access and browsing the Internet, you can use the push-button dialing telephone or the computer keyboard to input its computer modem, and link the corresponding digital code, and then, through the translation software conversion, you can get access to the Email or browse the Internet.

For the purpose of universal use, it is necessary to build a converter which correspond the digital address of the technology in this study with the domain name and IP address of the existing Internet. The converter is composed of translation software. Only by designating a full-digital coded address, it can be converted to the corresponding IP address, domain name or Chinese domain name system, and each full-digital coded address is corresponding to an existing IP address, domain name or Chinese domain name system. Since computers could only identify IP address, in this study, it is not only necessary to build a converter to converting full-digital coded address into universal domain name and IP address, but also to designate a server to translate the numeric address established through the technology in this study into IP address so that the computer can identify the address for operation.

VI. CONCLUSION

The methods designed in this study could not only assign a fixed static address to each networked computer but also allocate a dynamic address to a temporarily networked computer, thus, it is easy for users to apply the digital address. Besides, the auxiliary information database is established, with which, the full-digital coded address established through the technology in the study and the existing addresses with Internet access, including: domain name, IP address and Chinese domain system etc. are listed and corresponding with each other, and users can inquire the address with Internet access they need just by opening the database installed in the website. Thus, it is easy for users to choose different ways to access the Internet by inputting. The database could also be complied into a written document for users to look up and consult.

REFERENCES

[1] Xie Jianping etc.A method of assigning addresses to network computers using the full decimal algorithm[P]. CN: ZL00135182.6, 2004.2.6.

[2] Xie Jianping etc. Method of using whole digital code to assign address for computer [P]. US: 8082365, 2011.12.

[3] RFC - Internet Standard. Internet Protocol, DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 791, 1981.09.

[4] S. Deering, R. Hinden, Network Working Group. Internet Protocol, Version 6 (IPv6)-Specification, RFC-1883, 1995.12.

[5] M. Crawford. Network Working Group. Transmission of IPv6 Packets over Ethernet Networks.RFC-2464, 1998.12.

[6] J. Onions, Network Working Group. A Historical Perspective on the usage of IP version 9. RFC1606. 1994.04.

[7] V. Cerf, Network Working Group. A VIEW FROM THE 21ST CENTURY, RFC1607. 1994.04.

[8] Xie Jianping, Xu Dongmei, etc. Digital domain name specification.SJ/T11271-2002, 2002.07.

[9] Information technology-Future Network- Problem statement and requirement-Part 2: Naming and addressing, ISO/IEC DTR 29181-2, 2014,12.

[10] Wang Wenfeng, Xie Jianping, etc. Product and service digital identification format for information procession. SJ/T11603-2016, 2016.06.

From Network Security to Network Autonomous

Wang Yubian*
Department of Railway Transportation Control
Belarusian State University of Transport
34, Kirova street,Gomel,246653
Republic of Belarus
*is the communication author.
e-mail: alika_wang@mail.ru

Yuri Shebzukhov
Department of the International Relations
Belarusian State University of Transport
Republic of Belarus
34, Kirovastreet, Gomel, 246653
Republic of Belarus
e-mail: oms@bsut.by

***Abstract*—In the 20th century, the emergence of the Internet has completely changed the work and life of human beings around the world. Today, people are increasingly inseparable from network. The Internet has been integrated with the global industry, agriculture, education, science,technologyand national defense. The current Internet was originated in the United States. The Internet systems based on IPv4 and IPv6,they are controlled by the United States completely. Computers connected to the Internet are subject to data retention and backup in the United States. Data security is greatly threatened. In addition, due to limitations and loopholes in the design of the Internet, the Internet is subject to many different types of attacks. Internet research which based on security autonomy has received the attention of sovereign countries in the world. This paper mainly introduces the Future Internet system developed by Chinese researchers based on the current research on Internet servers,which is a new generation network system,the research and application of this system will have a profound impact on the world's Internet.**

Keywords-Network Security; Root Server; Network Autonomous; Future Internet

People can't live without the internet;internet has become a necessity in daily life.The share of the network economy has accounted for 22% of the global GDP. The importance of the network has become more and more prominent, so the basic work about the network is even more important. Now the Internet has two biggest problems. One is the cyber sovereignty, which is about the network's belongs. It is obviously that the United Stateshold the internet. How to adhere to cyber sovereignty is still a challenge. Another problem is that many countries hope the operators will speed up and reduce the cost at the same time. It need the operators to reduce the bandwidth cost of access to the Internet by SMEs, and how to reduce the bandwidth fee for accessing the Internet is a problem. This two major problems are now more difficult to solve, and why? We need specific analysis of specific issues and tell everyone what solutions we have.

I. CYBERSPACE

First of all, there must be a definition of cyberspace. This is very important. How do we adhere to the sovereignty of cyberspace?Currently,there is noaccurate definition in the media, and we think it should be definedproperly. Cyberspace is a virtual space that contains three basic elements.In the space,virtual and real are contained, and dominated by virtual.

In this virtual cyberspace, it is not these infrastructures that are in the most important leadership position, nor our application environment, but the full root system. This must be clear, if this is not clear, many explanations will go wrong. The core embodiment of cyberspace sovereignty is the standard protocol for data communication technology. At present, it includes the IPv4, IPv6 and future network/IPV9 network data communication standards and protocols of the existing equipment running in the world, and the formed network space address naming rights, distribution rights, resolution rights and route addressing operation management rights.

The core resources of cyberspace include: the parent root server, the primary server, the 13 root name servers, the IP address of the address and domain name resolution system, asset equipment and operation management rights. Therefore, it can be said who owns the core assets of cyberspace, who masters the sovereignty of cyberspace.

II. INTERNET SERVER

The working principle of the current public network is not thoroughly understood. Actually, this is very important. This determines how to adhere the cyberspace sovereignty. This is determined the basic principles. Any time we access the network, including any computer on the Internet, phone Internet access and mobile Internet access. Firstly, we must access the root server. The root system consists of the parent root server and the primary root server (the publishing host). This hidden publishing host only 13 root domain name servers (13 root domain name servers are equal rights) that can be accessed to maintain this hidden publishing host. The 13 root domain name servers read the primary root server, then read the parent root server and obtain the data, then read by the mirror server, and spread to the entire network.

The root server is mainly used to manage the home directory of the Internet. All parent, root, and sub-servers of IPv4 are managed by ICANN, an Internet domain name and number assignment authority authorized by the US government are responsible for the management of global Internet domain name root servers, domain name systems, and IP addresses. There are only 13 root name servers in the world. Ten of them are in the United States, two in Europe, in the United Kingdom and Sweden, and one in Asia in Japan. These 13 logical root servers direct web browsers such as Firefox or Internet Explorer and email programs to control Internet communications. Because the root server has more than 1000 Internet domain name suffixes (such as .edu, .com, etc.) approved by the US government and all national domain names (such as .us in the US, .cn in China, etc.).

Since the establishment of the Internet, the world has become very dependent on the United States. The United States has controlled the entire Internet by controlling the root server, posing a potentially major threat to cybersecurity in other countries. The so-called dependence, embodied in the working mechanism of the Internet, lies in the problem of "root server". In theory, any form of standard domain name to be analyzed, in accordance with the technical process, must be completed through the work of the global "hierarchical" domain name resolution system.

The first layer of the "hierarchical" domain name resolution system is the root server, which is responsible for managing domain name information of countries all over the world. Below the root server is a top-level domain name server, that is, a database of relevant national domain name management institutions, such as CNNIC in China, and then at the next level. The domain name database and the ISP's cache server. A domain name must first be parsed by the root database before it can be redirected to the top-level domain name server.

III. INTERNET ACCESS AND SECURITY

Any network access in the world should firstvisit the United States, and now some people say that many visits are not going abroad, and indeed some businesses do not feel abroad for the time being. In fact, the mirror root serversare working and cache serversare working. The Internet set up mirror servers in some countries without root servers, but these servers are completely controlled by the United States. Commonly used URLs can be parsed locally, and data can cache locally to prevent network congestion. However, the root of the Internet can back up the entire network. Traffic can still go out, although most of the data traffic business is domestic. This is why the United States monitors the world through the Internet, and because of economic reasons, the data traffic to the root system is two-way billing.

Since the widespread use of the Internet, the Internet has been constantly challenged, and various types of attacks from all over the world have continued. Typical server failures are as follows.

A. Failure in 1997

In July 1997, a new general list of Internet address assignments was automatically passed between these domain name servers, but this list is actually blank. This human error led to the most severe local service disruption on the Internet, resulting in inaccessible web pages within a few days and the inability to send emails.

B. Attack in 2002

On October 21, 2002, at 4:45 pm ET, the 13 servers were hit by the most serious and largest cyber-attack in history. The attack was a DDoS attack (Distributed Denial of Service). With the help of client/server technology, this attack combines multiple computers as attack platforms and launches attacks on one or more targets, thus doubling the power of denial of service attacks. Data that is 30 to 40 times more than the conventional number rushed to these servers and caused 9 of them to not function properly. Seven units lost their ability to handle network communications, and the other two were immediately behind.

This attack may not be affected by the average user. If you only analyze from the "consequences" of this incident, some people may think that "not all root name servers will be attacked, so you can rest assured", or

"the root name server has no problem with the root name server", it is still too early. But they are not clear about the root cause.

Not all root name servers are affected; the attack ends in a short period of time; the attack is relatively simple, so it is easy to take appropriate measures. Since there is no particularly effective solution for DDoS attacks, imagine that if the attack time is extended, the attack is a bit more complicated, or there is one more server, the global Internet will have quite a few web browsing and e-mail services. This will be completely interrupted.

C. DNS failure at the beginning of 2014

Beginning around 15:00 on January 21, 2014, there was a problem with DNS resolution of a large number of Internet domain names around the world. Some well-known websites and all non-existent domain names were incorrectly pointed to 65.49.2.178 (Fremont, California, United States, Hurricane Electric). China's DNS domain name resolution system has experienced a wide range of access failures, which have been confirmed by several DNS domain name resolution service providers, including DNSPod. The accident affected the whole country. Nearly two-thirds of the websites had access faults in different areas and network environments to varying degrees.

The framework of the entire network information security can be divided into three levels.

- Information security of various services at the network application layer, killing viruses, anti-Trojans, hardening firewalls and proactively defending against network attacks are the main tasks of network security departments in different countries. Andmany information security is mainly supported by encryption technology. As long as they are targeted by capable hackers, it is only a matter of time before information encryption and decryption are made.
- The network core equipment and terminal equipment, including the CPU core chip and the OS operating system/database are all from the United States. The information of this equipment is transparent to the United States and the NSA, and there is no security possibility.
- The problem of network information security caused by the lack of network sovereignty is a more global problem. Each bit under each communication IP address is monitored by the US Internet root system. All data is analyzed by the US National Security Bureau for big data analysis, and then stored and archived. The encrypted information is decrypted according to the specific situation!

In order to change the situation, China's cyberspace is in a serious strategic passive situation, in order to defend the network sovereignty and build a new generation of sovereign networks with domestically controllable security, some countries have carried out research and development of some network system structures.

IV. THE NEW GENERATION OF THE INTERNET

In 2001, Ministry of Information Industry of China established the "Decimal Network Standard Working Group". In 2007, Ministry of Information Industry of Chinadefined IPV9 as a new generation Internet to distinguish IPv6 officially.

In order to break through the future network basic theory and support the next generation Internet experiment and build the future network test facilities, including: original network equipment system, resource monitoring management system, covering cloud computing services, Internet of things applications, spatial information network simulation, network information security open network test systems such as high-performance integrated circuit verification and quantum communication networks.

In December 2014, the core parts of the future international standards published by ISO/IEC, such as "Name and Addressing" and "Safety", are dominated by Chinese experts and have core intellectual property rights. The future network has clear and unique definitions. Major countries such as the United States, Russia, Canada, and South Korea have voted in favor.

On June 1,2016, Ministry of information Industry of China published the relevant industry standards for IPV9 implementation in the country: SJ/T11605, SJ/T11604, SJ/T11603, SJ/T11606.

This marks the 20-years hard workingreceive rewards. The Chinese government has adopted the mature IPV9 main root/mother root/13 root name server system named from NZ. The core backbone router and user router product series have begun to build autonomous, intellectual property rights, and computer communication networks that are independent of the US Internet but are Internet compatible.

The main features of the future network/IPV9 are as following.

A. *Increasing the geographical and national concepts get increase*

It is distributed and managed by countries, and it is close to the analysis, and the flow of information is reasonable. End-to-end communication can be realized according to requirements, and it is not necessary to be controlled by the United States like IPv4 and IPv6. It is low-cost, high-efficiency, and it saves network expenses andachieves environmental protection.

B. *Realizing the unification of electronic tag and barcodes*

The huge address capacity of IPv9 realizes the uniqueness of address allocation. The combination of IP address, digital domain name and electronic tag and bar code coding technology will extends the network to every corner of sensor technology. IPv9 enables bar codes to have the same Internet access function as electronic tags, and can track and control the circulation of goods and equipment from the production plant. The bar code can also be identified when the RFID electronic tag wireless channel is disturbed. China's unique barcode and RFID electronic label hybrid technology will greatly reduce the management costs of the global manufacturing and logistics industries.

C. *Realize multi-code integration*

IPv9 not only makes the domain name and IP address unified, but also can be combined with the global unique identifier of the person or thing, so that the phone number, mobile phone number, domain name and IP address can be combined into one number; The same code for electronic tags and barcodes is a solution and application platform for the future information society and the realization of “ubiquitous” networks.

D. *Real-name Internet access*

IPv9 network can realize real-name Internet access, and can also protect customers' privacy rights. It can open up a certain number of anonymous addresses for blog use, but it does not allow anonymous address users to enter banks, government, social welfare, commodity circulation, etc.

E. *IPv9 has address encryption*

Different from the current means of encrypting applications, IPv9 innovatively designed address encryption to extend security protection to the network layer, greatly improving the country's information security. Whether it is IPv4 currently in use or the next-generation Internet protocol IPv6 proposed by foreign countries is unmatched.

The IPv9 communication protocol packet structure is designed reasonably, and the packet item function is clear. The IPv9 protocol is better than the IPv4 protocol in terms of address space, service quality, and security. When the application support and network device support are mature, the IPv9 protocol can replace the IPv4 protocol and become a communication protocol for network interconnection.

The address representation of the data packets of the IPv9 protocol is different from that of the IPv4 or IPv6 protocol. Therefore, the data packet header of the IPv9 protocol will not be recognized by the IPv4 or IPv6 system and will not be directly transmitted in these systems. Therefore, using IPv9 protocol communication, its data messages will not be directly transmitted to other protocols' networks, thus controlling the data transmission range and improving the security of communication to a certain extent.

F. *Currently, all hacker attacks and all online eavesdropping software are developed based on IPv4*

IPv6 routers and V9 NICs will not release these attack packets from hackers and hackers, and will build a Great Wall for hacking and online intelligence.

V. SUMMARY

The new generation Internet based on IPV9, the main root/mother root server system, the domain name resolution system, the backbone router/user router are all independently developed and produced by China, and are compatible with IPv4/IPv6. They support all existing applications of IPv4, and the underlying network itself adds IPv4/IPv6. There is no security mechanism, the address itself can be encrypted, and the communication can be verified first. At the same time, the new generation network address is extremely rich, and it also includes information such as geographic location/industry category. In the future, the network/IPV9 starts with the address 2^256 power, and the number of addresses for managing digital assets can reach 2^2048 power, future network. /IPV9 can not only meet the global 750-year communication address demand, but also an important tool for digital asset management. It is the core foundation for the future digital world/digital global and the future community of cyberspace destiny.

REFERENCES

[1] Xie Jianping etc.Method of using whole digital code to assign address for computer [P]. US: 8082365, 2011.12.

[2] S. Deering, R. Hinden, Network Working Group. Internet Protocol, Version 6 (IPv6)-Specification, RFC-1883, 1995.12.

[3] M. Crawford. Network Working Group. Transmission of IPv6 Packets over Ethernet Networks.RFC-2464, 1998.12.

[4] J. Onions, Network Working Group. A Historical Perspective on the usage of IP version 9. RFC1606. 1994.04.

[5] V. Cerf, Network Working Group. A VIEW FROM THE 21ST CENTURY, RFC1607. 1994.04.

[6] Information technology-Future Network- Problem statement and requirement-Part 2: Naming and addressing, ISO/IEC DTR 29181-2, 2014, 12.

[7] Radio frequency identification tag information query service network architecture technical specification. SJ/T11606-2016, 2016. 06.

A Survey of Calibration Methods for Traditional Cameras Based on Line Structure Light

Wu Ruixia
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710032, China
e-mail: wuruixiagirl@qq.com

Yao Huimin
Eighth of production plant, the company china petrdeum, changqing oilfield, Xi'an
Xi'an, 710021, China

Liu Baolong
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710032, China
e-mail: liu.bao.long@hotmail.com

***Abstract*—The line structure light three-dimensional reconstruction system is a kind of three-dimensional non-contact measurement system, which has the advantages of high precision, high speed, small damage to objects and strong adaptability. Camera calibration is a major factor that constrains the accuracy of 3D measurement systems. The camera calibration is based on the pinhole imaging model, and through a series of complex calculations, the camera's internal parameters (focal length, distortion coefficient) and external parameters (rotation matrix and translation vector).The different calibration methods use different calibration targets, which can be divided into 3D calibration targets, 2D calibration targets, and one-dimensional calibration targets according to the characteristics of the calibration targets. This paper mainly discusses: calibration content and significance, calibration methods for different targets and evaluation methods for calibration of different targets. Firstly, the content and significance of calibration are expounded. Then, according to different calibration targets, the calibration algorithm is analyzed. Finally, the calibration algorithm is analyzed and summarized, and the development trends, advantages and disadvantages of different calibration methods are pointed out.**

Keywords-Calibration Target; Internal Reference; External Parameter

I. INTRODUCTION

Vision plays an important role in human understanding and transformation of the world. 80% of human information comes from vision[1].Three-dimensional measurement technology is of great significance in the fields of culture, film and television entertainment, medicine and cultural relics protection. With the continuous development of computer technology, the functions of computers are becoming more and more powerful. People use the camera to obtain the three-dimensional information of the object, and the obtained three-dimensional information is converted into data that can be processed by the computer through a series of calculations, and then the data is used to reconstruct the object. The method for measuring the line structure light is a technique of obtaining a three-dimensional point coordinate at the intersection of the plane and the surface of the object to be measured by projecting a line laser plane onto the surface of the object [2]. The three-dimensional measurement technology of line structure light has the advantages of fast measurement speed, high precision and low measurement environment requirements, and is widely welcomed [3].Camera calibration is the main factor that restricts the accuracy of 3D measurement, which has attracted wide attention from scholars and improved step by step.

II. CAMERA CALIBRATION CONTENT

Wherever Times is specified, Times Roman or Times New Rom The camera calibration method is different according to the way of solving the parameters (such as whether to use external reference objects, whether the camera needs precise motion, etc.). The camera calibration algorithm can be divided into three calibration methods: traditional calibration

method, self-calibration method, active vision camera calibration method [4].As shown in Figure1 below, this article focuses on traditional camera calibration.

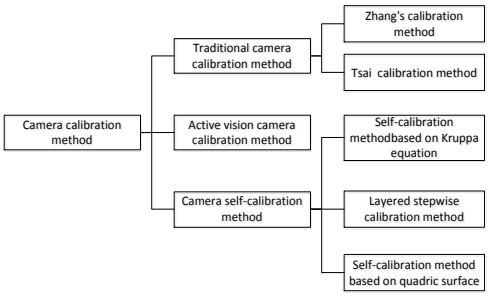


Figure 1. Classification method of calibration method

The camera calibration technology is mainly based on the linear model of small hole imaging, the geometric model established by the conversion between the two-dimensional image coordinate system of the known feature points and the three-dimensional world coordinate system. Using the optimal algorithm to derive the internal and external parameters of the camera model considering distortion, the process of solving the camera parameters is called camera calibration. Figure 2 below is the conversion diagram of the coordinate system. In the figure, $\{O-UV\}$, $\{O_o-XY\}$, $\{O_c-X_cY_cZ_c\}$ and $\{O_w-X_wY_wZ_w\}$ representing a pixel coordinate system, an image coordinate system, a camera coordinate system, and a world coordinate system, respectively. O_cO_o for the optical axis of the camera, f Indicates the focal length of the camera. Point P is a point on the object to be measured, and P' is the coordinate of P corresponding to the image coordinate system. Suppose the world coordinates of point P are (x_w,y_w,z_w) , Camera coordinates are (x_c,y_c,z_c) , Image coordinates are (x,y) , Pixel coordinates are (u,v) , Ideally, there is a certain conversion relationship between pixel coordinates and image coordinates, image coordinates and camera coordinates, camera coordinates, and world coordinates. If the world coordinates and image coordinates of some points are known, the internal and external parameters of the line structure light can be calculated using the conversion relationship.

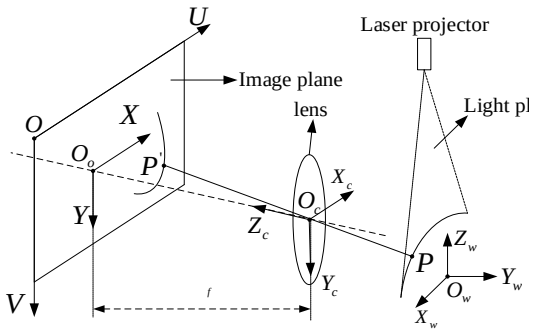


Figure 2. Coordinate system conversion diagram

After acquiring the three-dimensional coordinate point, the camera shifts the theoretical point P due to camera distortion and other factors[5], as shown in Figure 3 below.

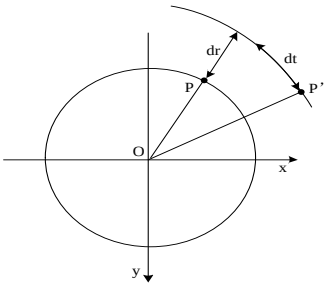


Figure 3. Distortion model diagram

The main factors affecting distortion are radial distortion and tangential distortion, as shown in Figures 4 and 5 below are common radial and tangential distortions.

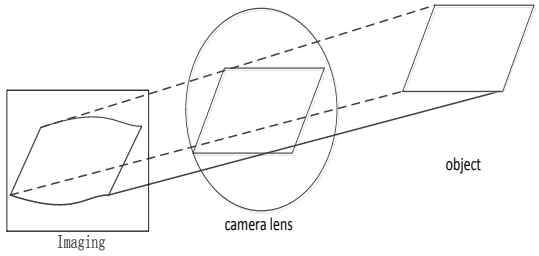


Figure 4. Radial distortion

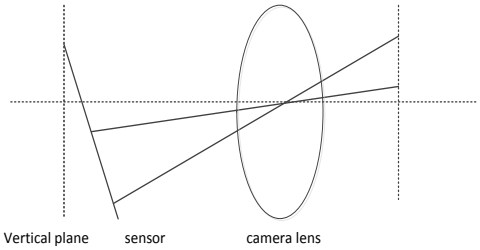


Figure 5. Tangential distortion

III. TRADITIONAL CALIBRATION METHOD

The calibration target is generally divided into a 3D calibration target, a 2D calibration target, and a one-dimensional calibration target[6].Common targets are shown in Figure 6 below:

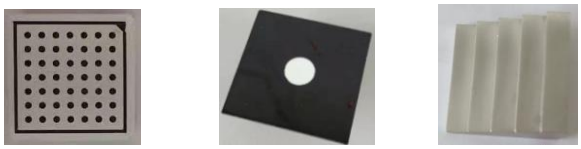


Figure 6. Schematic diagram of commonly used targets

A. Camera model

In this paper, the pinhole model is used as a camera model for research. The 2D calibration target is represented by $m = (\mathrm{u}, v, 1)^T$, the 3D calibration target is represented by $M = [X, Y, Z, 1]^T$, and the corresponding homogeneous vectors are $\tilde{m} = [u, v, 1]^T$, $\tilde{M} = [x, y, z, 1]^T$, respectively. Then the relationship between the 3D point M and its projection point m is as follows[7]:

$$s\tilde{m} = A[R, t]\tilde{M} \tag{1}$$

Where R is the rotation matrix, $t = \begin{bmatrix} t_x & t_y & t_z \end{bmatrix}^T$ for the translation vector,and describes the external parameters of the camera that the camera is calibrated. $f_u = a_x / d_x, f_v = a_y / d_y, d_x, d_y$ indicates the physical size of each pixel in the Y-axis Y-axis direction. f_u, f_v, u_0, v_0 is only related to the internal parameters of the camera, which is the internal parameters that the camera needs to calibrate.

B. Camera calibration based on three-dimensional targets

This paper introduces the calibration of 3D calibration targets, using the classic Tsai[8].two-step calibration algorithm. The Tsai two-step method is based on the calibration method of the radial correction constraint (RAC. Radial Alignment Constraint).

The camera distortion model shown in Figure 7 below, The following model includes five coordinate systems, which are camera coordinate system O_C, image pixel coordinate system O_i, world coordinate system O_W actual image physical coordinate system O_d, and ideal image physical coordinate system O_u. The solution process assumes that u0, v0 is known to only consider second-order radial distortion. The main point is both the center of the image and the center of the radial distortion.

The first step ： uses a radial alignment constraint (RAC) linear solution.

Step 2: Find the remaining parameters for nonlinear optimization.

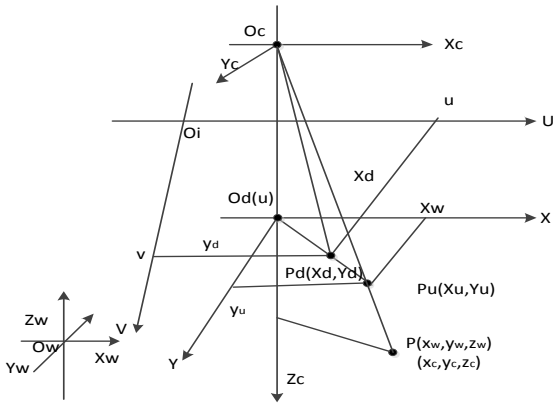


Figure 7. Camera distortion model diagram

Advantages: Applicable to any camera model, high calibration accuracy.

Insufficient: calibration needs to calibrate targets, which is difficult to achieve in some applications.

C. Camera calibration based on two-dimensional targets

In this paper, the research method of two-dimensional calibration target is explained by Zhang Zhengyou calibration method[9][10].To facilitate the operation, the template is defined on a plane parallel to the X-Yplane (Z = 0) in the world coordinate system..

From the above formula (1):

$$s\begin{bmatrix} u \\ v \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha & \gamma & u_0 & 0 \\ 0 & \beta & v_0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} R & t \\ 0^T & 1 \end{bmatrix} \begin{bmatrix} x_w \\ y_w \\ z_w \\ 1 \end{bmatrix} \tag{2}$$

$$R = \begin{bmatrix} r_1 & r_2 & r_3 \\ r_4 & r_5 & r_6 \\ r_7 & r_8 & r_9 \end{bmatrix} \tag{3}$$

Where is the u_0、v_0 principal point coordinate, α、β is the vector of the (u, v) , the

coordinate axis in the image, and γ is the perpendicularity of the two coordinate axes. Let the template plane $Z_W = 0$ be in the world coordinate system, you can get:

$$s\tilde{m} = H\tilde{M} \tag{4}$$

Where $H = [h_1 \quad h_2 \quad h_3] = \lambda A[r_1 \quad r_2 \quad r_3]$, λ is the scaling factor scalar, r_1, r_2 is the two column vectors of the rotation matrix, and t is the translation matrix.

By the nature of the rotation matrix, a constraint matrix is available for each image:

$$\left\{ \begin{array}{c} h_1^T A^{-T} A^{-1} h_2 = 0 \\ h_1^T A^{-T} A^{-1} h_1 = h_2^T A^{-T} A^{-1} h_2 \end{array} \right\} \tag{5}$$

make:

$$B = A^{-T} A^{-1} = \begin{bmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \end{bmatrix} = \begin{bmatrix} \frac{1}{\alpha 2} & -\frac{\gamma}{\alpha^2 \beta} & \frac{v_0 \gamma - u_0 \beta}{\alpha^2 \beta} \\ -\frac{\gamma}{\alpha^2 \beta} & \frac{\gamma^2}{\alpha^2 \beta^2} + \frac{1}{\beta^2} & -\frac{\gamma(v_0 \gamma - u_0 \beta)}{\alpha^2 \beta^2} - \frac{v_0}{\beta^2} \\ \frac{v_0 \gamma - u_0 \beta}{\alpha^2 \beta} & -\frac{\gamma(v_0 \gamma - u_0 \beta)}{\alpha^2 \beta^2} - \frac{v_0}{\beta^2} & \frac{\gamma(v_0 \gamma - u_0 \beta)^2}{\alpha^2 \beta^2} + \frac{v_0^2}{\beta^2} + 1 \end{bmatrix} \tag{6}$$

From (6): B is a symmetric matrix, which can be represented by the following 6D vector:

$$b = [B_{11} \quad B_{12} \quad B_{13} \quad B_{22} \quad B_{23} \quad B_{33}]^T \tag{7}$$

Let the ith column vector $h_i = [h_{i1} \quad h_{i2} \quad h_{i3}]$ in H be obtained:

$$hi^T B h_j = v_{ij} T b \tag{8}$$

Then you can write (5)as:

$$\begin{bmatrix} v_{12}^T \\ [v_{11} - v_{12}]^T \end{bmatrix} b = 0 \tag{9}$$

Suppose you take n images of the template plane and get n images.

Vb=0 n is the matrix of $2n \times 6$ (10)

If $n \geq 3$,you can get the unique solution b and matrix B, you can get:

$$\begin{aligned} r_1 &= \lambda A^{-1} h_1 \\ r_2 &= \lambda A^{-1} h_2 \\ r_3 &= r_1 r_2 \\ t &= \lambda A^{-1} h_3 \end{aligned} \tag{11}$$

Get the internal and external parameters of the camera for optimization:

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \| m_{ij} - \hat{m}(A, R_i, t_i, M_j) \|^2 \tag{12}$$

Where $m(A, k_1, k_2, k_3, R_i, T_i, M_j)$ represents the coordinate point at which the jth point is projected onto the i-th image according to equation (4).

D. Camera calibration based on one-dimensional target

As shown in Figure 8, AB is a one-dimensional calibration with a length of L[11].

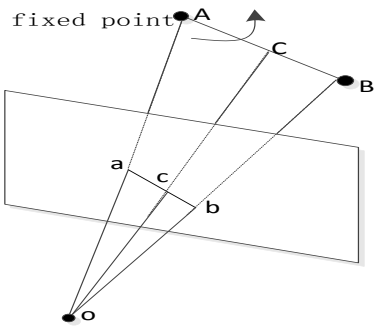


Figure 8. One-dimensional calibration target

$$\| A-B \| = L \tag{13}$$

Since the ratio of the line segments is known, B points can be calculated in the case where points A and C are known.

Then, according to the formula (2-1), there is a following formula, where Z_A, Z_B, Z_C is the depth of the corresponding point on the one-dimensional calibration object.

$$Z_C = \mathrm{Z_A}\lambda_{\mathrm{A}}\mathrm{a} + \mathrm{Z_B}\lambda_{\mathrm{B}}\mathrm{b} \tag{14}$$

Where $\lambda_B = BC / AB$, $\lambda_B = AC / AB$ Representation ratio.

According to (13):

$$\| K-1(Z_B b - Z_A a) \| = L \tag{15}$$

According to (14):

$$Z_A{}^2 h^T K^{-T} K^{-1} h = L^2 \tag{16}$$

The parameters of the camera can be obtained by (16). According to the theory of higher geometry, the projection of the absolute quadratic curve on the image plane is actually described.

IV. EVALUATION OF CALIBRATION RESULTS

At present, the standard for calibration evaluation is mainly calibration accuracy and speed. The calibration target has a slight influence on the accuracy of the calibration. The commonly used calibration target materials are ceramic and metal and glass. The calibration target of the strong reflective material is easy to introduce noise, and the accuracy of the diffuse reflection calibration is better.

According to the above analysis of the algorithm, the advantage of the one-dimensional calibration target is that the construction of the calibration target is relatively simple and easy to implement; the disadvantage is that the number of points on the calibration object is small, the coordinates are unknown, and the calibration accuracy for the nonlinear distortion coefficient is not high. Based on the calibration method of two-dimensional and three-dimensional calibration targets, a large number of known coordinate systems on the calibration target can be used for calibration. The calibration accuracy is high and the speed is fast, but it is easy to appear blind spots due to its own characteristics. The three-dimensional calibration target is expensive to manufacture, and the commonly used fabrication methods mainly include photolithography, grinding, printing, and the like.

Different calibration targets are suitable for different calibration systems, and one-dimensional calibration targets are suitable for systems with less budget and less demanding calibration accuracy. The production of three-dimensional calibration targets is difficult, mainly machine processing, suitable for high precision requirements and sufficient funds. The calibration algorithm of the two-dimensional calibration target is easy to extract features, and the reconstruction effect is worse than the three-dimensional calibration target.

ACKNOWLEDGMENT

This work is partially supported by Science & Technology Program of Weiyang District of Xi'an City with project “201836".

REFERENCES

[1] Xiao Yujie, Huang Wei, Zhang Ting. Overview of Camera Calibration Technology[J]. Communications, 2015(14): 206-207.

[2] Zhang Xi , Zhang Jian . Summary on calibration method of line-structured light sensor[C]// 2017 IEEE International Conference on Robotics and Biomimetics (ROBIO). IEEE, 2018.

[3] Li Yuhua, Zhou Jingbo, Liu Lijian. Research progress of line structure light measurement technology[J]. Journal of Hebei University of Science and Technology, 2018, 39(2): 115-124.

[4] Su Jin. Research on Camera Calibration Method [D]. Northeastern University, 2010.

[5] Lin Xintao. Research on Calibration Te , ' logy of 3D Measurement System Based on Line-Structured Light[D].

[6] Pan Jing, Li Weimin. Camera Calibration Algorithm Based on 3D Stereo Target[J]. Mechanics & Electronics, 2007(5):3-5.

[7] Li Xuyong. Research on Modeling and Calibration Technology of Underwater Camera[D]. Ocean University of China, 2010.

[8] Tsai R Y. A versatile camera calibration technique for high-accuracy 3D machine vision metrology using off-the-shelf TV cameras and lenses[J]. IEEE Journal on Robotics & Automation, 2003, 3(4):323-344.

[9] Zhang Z. A Flexible New Technique for Camera Calibration[J]. Microsoft Research, 2000, 22(11):1330-1334.

[10] Zhang Z. Camera calibration with one-dimensional objects.[J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2004, 26(7):892-899.

[11] Wang Tao, L ü Naiguang, Yang Jian. High-precision calibration based on one-dimensional calibration[J]. Journal of Beijing University of Information Science and Technology(Natural Science), 2010, 25(1).

[12] Lu P, Liu Q, Guo J. Camera Calibration Implementation Based on Zhang Zhengyou Plane Method[M]// Proceedings of the 2015 Chinese Intelligent Systems Conference. 2016.

[13] Lin P D, Sung C K. Comparing two new camera calibration methods with traditional pinhole calibrations[J]. Optics Express, 2007, 15(6):3012-3022.

[14] Wang J T. Camera self-calibration method based on traditional calibration method[J]. Computer Engineering & Applications, 2010, 46(35):205-208.

[15] Lenz R , Tsai R . Techniques for calibration of the scale factor and image center for high accuracy 3D machine vision metrology[J]. Proc IEEE Icra, 1988, 74(11):-.

[16] From R B T . A Versatile Camera Calibration Techniaue for High-Accuracy 3D Machine Vision Metrology Using Off-the-shelf TV Cameras and Lenses[J].

Research on Harris Corner Detection Method in Palmprint Recognition System

Wu Hejing
East University of Heilongjiang
150086
e-mail: 499917928@qq.com

***Abstract*—Palmprint location is the premise of feature space extraction and feature recognition,the speed and accuracy of palmprint location directly affect the speed and accuracy of palmprint recognition system, and the extraction of contour feature points is the key of palmprint location. The contour of palmprint is extracted by gray morphological gradient;then, based on the analysis of palmprint appearance characteristics, Harris corner is used to extract the key feature points of the image, and the reference coordinate system is established according to the key points to realize the location and segmentation of palmprint.**

Keywords-Palmprint Recognition System; Palmprintlocation; Harris Corner

I. EXTRACTION OF CONTOUR FEATURE POINTS BY IMPROVED HARRISCORNER DETECTION METHOD.

Figure 1. Palmprint corner detection

Harris corner detection algorithm is a common corner extraction algorithm at present, but it can not get ideal effect when we use it directly to extract the contour feature points defined by us. As shown in Figure 1, this paper improves Harris corner detection algorithm purposefully, thus realizing the extraction of palmprint contour feature points.

II. HARRIS CORNER DETECTION

The predecessor of Harris algorithm is Morave algorithm. Morave's corner detection formula is:

*1) In formula E, the brightness change occurs when a small window (u, v) is moved at a point (x, y). w (x, y) is a Gaussian smoothing factor.*The essence of formula (2.11) is the autocorrelation of two-dimensional signals. The above formula is expanded by Taylor series:

2) Formula: Represents the horizontal and vertical derivatives of the point in the image respectively. Ignore the higher order terms and write them into quadratic form:

$$E(u,v)\big|_{(x,y)} \approx [u,v]M\begin{bmatrix} u \\ v \end{bmatrix}$$

3) Formula:

After M similar diagonalization, the results are as follows:

The eigenvalue of matrix M is obtained. Because matrix M has rotation invariance and is proportional to

the curvature of gray scale of pixel points, if the minimum eigenvalue is greater than a given threshold, it is determined as a corner point.

Harris algorithm needs to determine threshold, variance of Gauss function and constant variable K. When the image size is, the window size of derivative is, and the window size of Gauss filter is, the complexity of the operator is, and the algorithm is slow.

III. IMPROVEMENTS OF HARRIS CORNER DETECTION ALGORITHMS

In Harris algorithm, the eigenvalues of matrix M are closely related to the first derivatives of pixel points in X and Y direIn the edge region, there is only a large change in the horizontal or vertical direction, that is, only one of them is largections; In flat areas, the changes in horizontal and vertical directions are the smallest, that is, they are small;Corner area in the horizontal and vertical direction of the changes are larger points, that is, larger. According to this feature, the corner detection algorithm is improved.

The feature points of palmprint contour extracted by us are located in the convex and concave areas between fingers on Palmprint contour. They are composed of some flat areas and points that vary in a certain range of slope areas.

In the image region, the difference between the third line and the first line is close to the derivative in the Y direction.The difference between the third column and the first column is close to the derivative in the X direction. Firstly, two templates DX and Dy are designed. For any image region Z, the derivatives of center point Z5 in X and Y directions can be defined, respectively:

$$Z = \begin{bmatrix} z1 & z2 & z3 \\ z4 & z5 & z6 \\ z7 & z8 & z9 \end{bmatrix}$$

$$dx = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix} \quad dy = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

Figure 2. The image region

The input image is the palm edge image after thinning. According to the principle of image graphics, it is a closed curve composed of continuous single pixel points. Its gray value is only 0 and 255. It can be defined that the black edge point is response point 1 and the white background is non-response point 0, then when there is no response point in Z region (that is, all white back) ==0;

For the refined contour line, the corner function value C is calculated. In the case of C > 0, the candidate corner points are obtained. As shown in Figure 2 (b), the X coordinate values of the candidate corner points are sorted, the array of corner points is determined, and then the maximum y value of each corner point group is obtained as the corner points we want, as shown in Figure 2 (c). In order to further verify the feasibility of this algorithm, we have searched for some representative images to test the performance of corner detection algorithm, such as pentagonal star edges and some building blocks edges as shown in Fig. 3 (a), and detected the points that satisfy the condition C > 0. The results are shown in Fig. 3 (b). When C > 0 (i.e., the detected feature points).

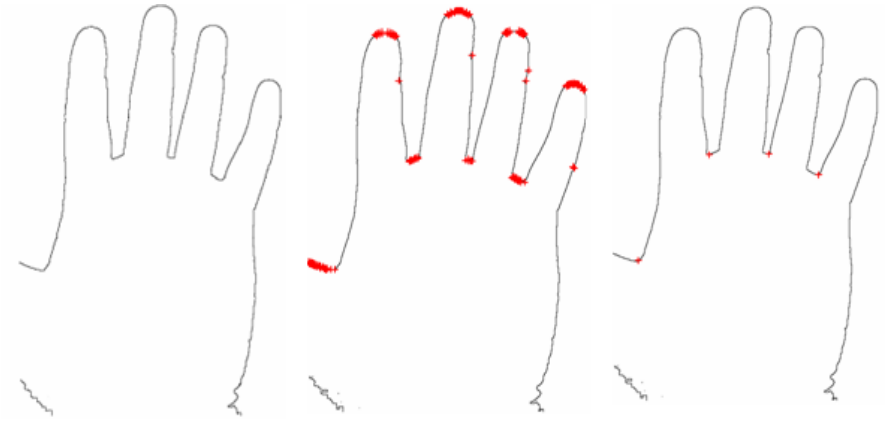


Figure 3. Extraction of palmprint contour feature points

IV. EXTRACTION PROCESS OF PALMPRINT CONTOUR FEATURE POINTS

Consistent with our previous deduction, it contains not only the points in the top corner areas, but also the points on the edge of the inclined angle, which is up and down the horizontal line (as shown in the shadows in

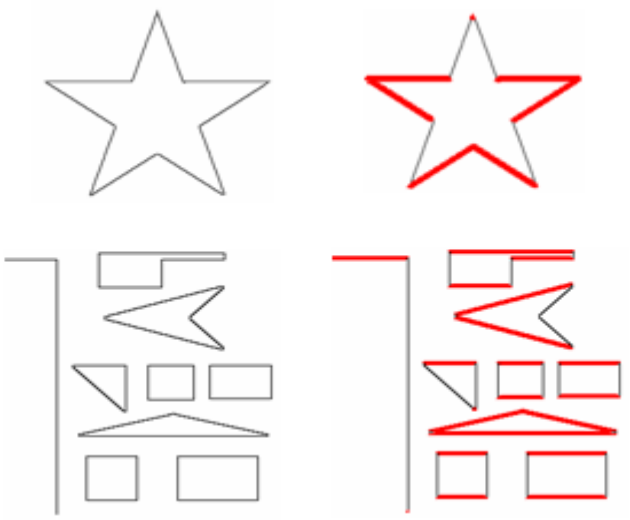


Figure 4. Palmprint contour feature points

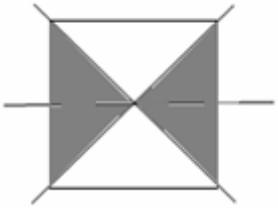


Figure 5. Declination range

The purpose of localization and normalization of palmprint image is to extract appropriate reference points from Palmprint and establish reference coordinate system to reduce the influence of non-linear factors such as rotation, translation and distortion introduced in the sampling process and improve the robustness of matching recognition algorithm. Good positioning results can not only provide reference frame for other palmprint features, but also provide benchmark for palmprint matching and feature matching. At the same time, it can segment the central area of palmprint, reduce unnecessary noise interference, reduce the complexity of subsequent matching algorithm, achieve azimuth-independent matching, ensure the accuracy and effectiveness of the recognition system, and in palmprint identification system. It has very important significance.

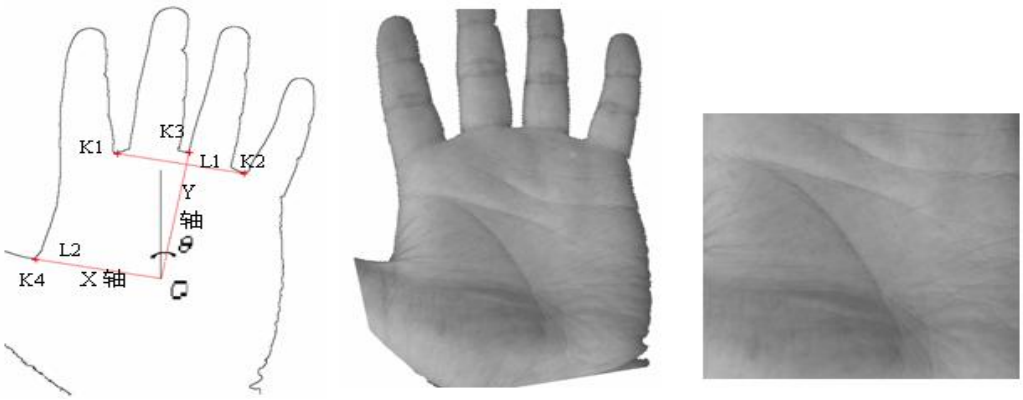


Figure 6. Palmprint location and feature space extraction

After extracting the corner points, we set up the coordinate system according to the following steps: make the line L1 = K1K2, draw an axis perpendicular to the line L1 from K3, and we set it as the Y axis; make a line L2 parallel to the line L1 and the crossing point K4, obviously the line L2 is perpendicular to the Y axis, which can be defined as the X axis, and the intersection point of the X axis and the Y axis as the O point, as shown in Fig.6 (a).The palmprint image is rotated counter-clockwise along the O-point, as shown in Fig.6(b), then the central area of palmprint is extracted and normalized as the Palmprint Feature space, as shown in Fig.6(c).

Under the above acquisition conditions, a palmprint test image database is established, which is composed of 80 images with a size of 40*2 (40 persons, each person collects 2 images).The positioning accuracy is shown in Table 1. The experimental results show that the desired feature points can also be found for the images with unsatisfactory collection effect. Among them, 79 images can be located accurately according to the above algorithm, so the accuracy rate is 98.75%.

TABLE I. LOCATION RESULTS

Total image count	Correct Location Number	Error Location Number	Location accuracy
80	79	1	98.75%

According to the analysis of palmprint images, the main reasons for wrong location are insufficient extension of palm, incorrect placement of palm, or insufficient separation of four fingers. If the position and posture of the palm are further standardized, the error positioning rate can be further reduced. The experimental results show that the above method is simple, effective, fast and can locate and score palmprints quickly and accurately.

V. CONCLUSION

In this paper, a new and purposeful exploration is made on the extraction of contour feature points in palmprint images, and the Harris corner detection algorithm is improved to realize the effective extraction of contour feature points. This algorithm avoids the need to determine the threshold artificially in the traditional corner detection algorithm, simplifies it, reduces the amount of calculation, grouping candidate corners and taking only one feature point in each group, thus improving the robustness of the algorithm, and

provides a new and effective method for solving the problem of palmprint location in palmprint recognition.

REFERENCE

[1] Jain, R.Bole, S.Pankanti. Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers. 1999

[2] The David Zhang. Automated Biometrics is one Technologies and Systems. Kluwer Academic Publishers. 2000

[3] N.Duta, A.K.Jain, K.V.Mardia. Matching of Palmprint. Pattern Recognition Leters.2001, 23(4): 477-485

[4] David Zhang. Automated Biometrics-Technologiesand Systems. Kluwer Academic Publishers, 2000

[5] A.Jain, R.Bolle, S.Pankanti .Biometrics: Personal identification in Networked Society. Kluwer Academic Publishers, 1999

[6] WeiShu, D.Zhang. Palmprint verification: an implementation of biometric technology. IEEE International Conference on Pattern Recognition. 1998, 1:219-221

[7] N.Duta, A.Jain, K.Mardia. Matching of palmprint. Pattern Recognition Leters.2001,23 (4):477-485

[8] C.Han, H.Chen, C.Lin, K.Fan. Personal authentication using palm-print features. Pattern Recognition.2003,36 (2):371-381

[9] C.Poon, D.C.M.Wong, H.C.Shen. A New Method in Locating and Segmenting Palmprint into Region-of-Interest Proceedings of the 17th International Conference on Pattern Recognition IEEE

[10] S.Mallat. Multi-frequency Channel Decomposition of Images and Wavelet Model. IEEE Transactions on Information Theory.1989,37(12)

Research on Digital Camouflage Design and Camouflage Material of Tent Cloth

Hu Zhiyi
Engineering Design Institute Army Academy of PLA
Beijing 100000, China
e-mail: 18992899862@163.com

YU Jun
School of Computer Science and Engineering
Xi'an Technological University
Xi'an 710021, Shanxi, China
e-mail: yujun@xatu.edu.cn

Xian Tong
School of Computer Science and Engineering
Xi'an Technological University
Xi'an 710021, Shanxi, China

Su Haitao
Engineering Design Institute Army Academy of PLA
Beijing 100000, China

***Abstract*—Aiming at the distortion of texture details in Digital Camouflage design, as well as the poor camouflage performance, fast fading and short life of camouflage tent cloth, this paper presents a design method of Digital Camouflage based on target background, develops a camouflage coating with good weather resistance, color difference and spectral reflectance meeting the limited requirements, and realizes the paint printing of camouflage tent cloth. The results show that the digital camouflage pattern designed by this method can be printed on the surface of camouflage tent cloth by coating printing process, which can effectively change the original contour of the target tent, make it better integrate with the surrounding background, reduce the probability of detection, and achieve good camouflage effect.**

Keywords-Digital Camouflage; Tent Cloth; Target Background; Design; Camouflage Coatings; Paint Printing

I. INTRODUCTION

With the rapid development of space and space reconnaissance technology, the resolution of satellite imaging reconnaissance to the ground is getting higher and higher. Camouflage camouflage, as the most basic measure against military reconnaissance and weapon attack, is a common method of "weapon equipment" anti-reconnaissance detection, and also an important symbol of the camouflage technology level of a country.

In the reconnaissance environment of multi-dimension, intelligence and fine resolution, the camouflage function of traditional camouflage is basically lost. As a new type of camouflage pattern, digital camouflage is a kind of camouflage pattern which uses computer image technology to extract the basic features of natural background such as color, texture, structure and so on, and displays in the form of digital "pixel" dot matrix. It copies the camouflage pattern on the target surface by camouflage paint, imitates the background or divides the outline of the target shape in color and texture, greatly improves the adaptability of digital camouflage to different landforms, and has greater concealment advantage than traditional camouflage.

As the backbone equipment of army camping, military tents play an important role in training and executing tasks. Tent cloth is the main material for making military tents. Its camouflage performance determines the camouflage effect of the tent. Therefore, the key to improve camouflage performance is to design scientific Digital Camouflage Patterns and print them on tent cloth.

This paper studies the design and implementation process of camouflage. Firstly, a new design method of digital camouflage is proposed. The digital camouflage pattern is designed by simulating the color and texture of the target background. Secondly, the camouflage pattern will be printed on the tent cloth by using inorganic pigment printing technology, and then the tent cloth will be made into military camouflage tent, which can improve the camouflage performance, weatherability and service life of the tent.

II. MAINPROBLEMS OF CAMOUFLAGE TENT CLOTH AT PRESENT

Tent cloth is the main material for making military tents. At present, there are two main problems in military tent cloth.

First, the texture details of the camouflage pattern are distorted, so that the fusion effect with the natural background is not good. At present, many army tents still use traditional camouflage patterns, which are not in harmony with the surrounding background.

Second, the camouflage performance of tent cloth is poor, weatherproof performance is not good, and the service life is short. At present, most camouflage tent cloths are printed and dyed with organic dyes. Their camouflage performance can not meet the requirements of spectral reflectance limitation. Moreover, they are affected by strong ultraviolet rays, high temperature and high humidity in the field. After three months, the camouflage pattern will fade seriously and disappear, so they can not be used normally.

In order to solve the above problems, three measures are adopted. Firstly, by extracting the basic features of natural background, the size of digital unit that can simulate the texture features of background is determined, and then the digital camouflage pattern is designed [1]. Second, by developing inorganic functional pigments and researching the weather resistant printing emulsion synthesis technology, the camouflage of camouflage patches can meet the requirement of spectral reflectivity, and improve the weatherability and service life of the tent. Thirdly, paint printing technology of inorganic functional pigments was used to print the surface of tent cloth, and good simulation performance was obtained.

III. DESIGN OF DIGITAL CAMOUFLAGE PATTERNS

The steps of digital camouflage design are shown in Figure 1[1-3].

Assuming the number of dominant colors in the target background is $N(3 \le N \le 6)$, the main steps of digital camouflage design are as follows:

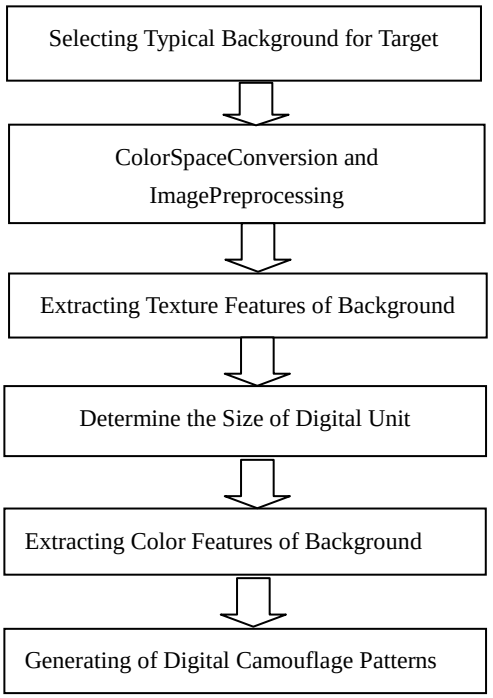


Figure 1. Design flow of Digital Camouflage

1) Select the typical background of the target

Analyzing the surrounding environment of the target, the selected background area is within 16-32 times the size of the target area. The background image of the target is captured by digital camera, UAV and other image recording devices. The background types that can represent typical environmental characteristics are analyzed and determined. Several typical background images are selected as background image M to be processed.

2) Color space conversion and image preprocessing

The principle of choosing color space is to see whether it is suitable for human visual characteristics and color perception characteristics. At present, the commonly used color space is HIS, HSV, Lab model, etc. Image M should be converted from RGB space to other color space, calculated and processed accordingly, and then converted back to RGB space for display. Before image M processing, appropriate filtering methods should be adopted to eliminate and reduce the noise of the image, so as to increase the reliability and validity of the image.

3) Texture feature extraction of image M. For N-color Digital Camouflage design, 2N-1 order texture needs to be extracted.

4) Determine the size of digital *units (i.e. mosaic squares), and design the arrangement and layout of mosaic squares.*

5) Color feature extraction of image M. According to the region divided by each gray scale corresponding to the target image M, the individual color features of each region are calculated to obtain the characteristic color, and these colors are arranged according to the gray value.

6) Digital camouflage pattern generation. The above arranged colors are filled into the corresponding areas of mosaic gray-scale image in turn, so that the digital camouflage pattern can be obtained.

After obtaining the final Digital Camouflage pattern, we are ready to print the pattern onto the tent cloth.

IV. Development of Camouflage Pigments and Preparation of Coatings

Inorganic pigments determine the weatherability and camouflage performance of tent cloth[4], and can solve the key problems of fast fading and short life of tent cloth materials in the field environment. In this paper, the green camouflage ceramic pigments system was developed by firing green camouflage functional ceramic pigments. Aiming at the technical requirements of camouflage camouflage background, a set of camouflage coatings with good weatherability, color difference and spectral reflectivity to meet the limited requirements was developed by studying the special printing emulsion and functional inorganic pigment system of acrylic ester.

Through a series of experiments, four camouflage colors, dark green, medium green, yellow green and black, were identified, and polyacrylate emulsion was synthesized. Finally, the camouflage coatings with four colors were prepared through the formulation test of the coatings. Table 1 shows the formulation of woodland inorganic pigment printing paint.

TABLE I. FORMULATION OF INORGANIC PIGMENT PRINTING COATING ON WOODLAND TYPE

Camouflage type		**Woodland**			
Item		***Forest green(g)***	***Medium green(g)***	***Kelly (g)***	***Black (g)***
Raw material	Polyacrylate emulsion	40	40	40	40
	Homemade green pigment	35	30	28	15
	Iron yellow	/	5	7	/
	Iron red	/	/	/	/
	Iron black	/	/	/	20
	Additive	8	8	8	8
	Water	17	17	17	17

V. PAINT PRINTING OF CAMOUFLAGE TENT CLOTH

After preparing the four-color camouflage coatings mentioned above, the camouflage coatings are printed on the surface of the cloth with polyester base cloth and circular screen printing technology[5]. The camouflage coatings are printed on the surface of the cloth by the coating printing process, and then baked to make the camouflage patterns firmly fixed on the cloth and become camouflage coated cloth, i.e. camouflage tent cloth. This completes the printing of Digital Camouflage Patterns on the tent cloth. The process is shown in Figure 2. Finally, the tent cloth is made into field military tents and placed in the original natural background.

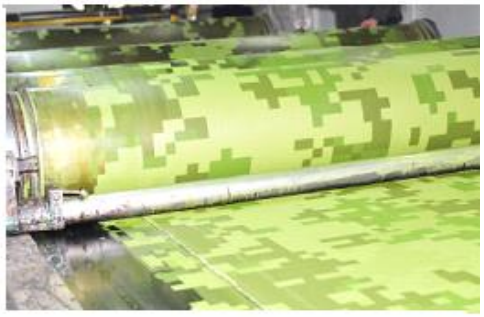


Figure 2. Paint printing of tent cloth

VI. CAMOUFLAGE PERFORMANCE EVALUATION OF CAMOUFLAGE TENT CLOTH

A. Camouflage performance evaluation of tent cloth

The main camouflage performance indicators of camouflage tent cloth include: color difference, spectral reflectance.

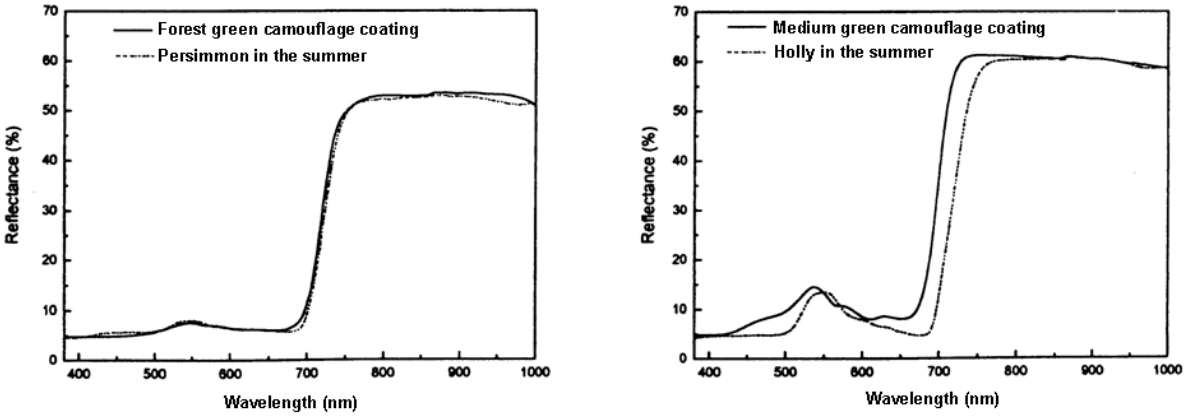
Digital camouflage tent cloth produced with inorganic pigments is compared with standard color. The color difference of each color patch is less than 3L*a*b* unit, which meets the color difference requirement.

The Digital Camouflage tent cloth produced with inorganic pigments is consistent with the spectral reflectance characteristics of the corresponding natural background, which meets the limited requirements of spectral reflectance.

In terms of weatherability of tent cloth, after 400 hours of artificial climate aging, the color difference of each color patch is 2-3L*a*b* unit, and the spectral reflectance of each color patch is basically unchanged.

For example, in Figure 3, pictures (a) and (b) show the spectral reflection characteristics of dark green and

medium green coatings, respectively. It can be seen that the spectral reflectance characteristics of the two green patches are consistent with those of the corresponding vegetation.



(a) forest green coating and persimmon tree; (b) medium green coating and holly tree.

Figure 3. Spectral reflectance of forest/medium green coatings and plants.

B. Actual camouflage effect

In order to observe the actual camouflage effect of the tent cloth, the Digital Camouflage tent cloth produced in front of it was made into a tent and placed in the forest background in the field. As shown in Figure 4. Picture (a) is the original woodland background. Picture (b) is our Digital Camouflage design. Figure (c) shows the camouflage effect of woodland tents. The red pane represents the target. Obviously, the Digital Camouflage of woodland tents is almost integrated with the natural background.

(a) woodland background; (b) designed digital camouflage; (c) camouflaged effect

Figure 4. Woodland type camouflage effect

VII. CONCLUSION

In this paper, camouflage design, camouflage material development and production in camouflage camouflage have carried out a series of research. Aiming at the problem of texture distortion in camouflage design, a design method of Digital Camouflage based on background features is proposed. Aiming at the problems of poor camouflage performance, fast fading and short life of tent cloth, camouflage coatings with good weather resistance, color difference and spectral reflectance satisfying the limited requirements are developed, and Digital

Camouflage tent cloth is produced by coating printing process. After testing, the camouflage performance of tent cloth meets the requirements and the camouflage effect is good. It is of great significance to improve the level of camouflage design and technology implementation of Digital Camouflage in China, and to promote the development of camouflage materials and camouflage technology.

REFERENCE

[1] Qin Lei, Hu Jianghua, Fu Tianqi. A New Digital Camouflage Generation Method [J]. Application of Photoelectric Technology, 2013, 28(5).

[2] Yu Jun, Yang Wuxia, Ho Zhiyi. Research on the Generation Algorithms of Digital Camouflage [J]. Opto-Electronic Engineering,2010, 37(11): 110-114.

[3] Cai Yunqian, Xue Shiqiang, Zhou Zhiyong and Huang Yun. Research on the Method of Generating Digital Camouflage Patterns Based on Fractal Brownian Model[J]. Journal of China Ordnance, 2016, 37(1):186-192.

[4] Zhang Chaoyang, Cheng Haifeng and Wang Qian. Preparation and characterization of multi-band camouflage coatings[J]. New Teehnology and New Process, 2005(12):44-46.

[5] Shang Hongyan. Application of New Paint Printing Technology[J]. Screen Printing, 2010(2):15-16.

The Researchof a New Iteration of the Circular Algorithm

Xu Shuping
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710021, China
e-mail: 563937848@qq.com

Chen Li
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710021, China

Huang Menyao
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710021, China

Xu Pei
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710021, China

***Abstract*—It is a problem of spectra analysis of flue gas that how to separate and calculate the concentration of different kinds of gas from continuous mixed gas absorption spectrum signal. So based on experimental data, a new iteration of the circular algorithm is put forward on the basis of Lambert-Beer's law. The algorithm uses different UV-light wavelengths at 190nm-290nm for different characteristics of UV light with different absorption peaks. The iteration is repeated until the concentration difference between adjacent two gases is less than a certain value. It is considered that the elemental gas The exact concentration, and through the programming to achieve the results. it has strong anti-jamming capability and is suitable for practical application of engineering.**

Keywords—Circular Iteration; Characteristic Absorption Peak; Iterative Algorithm; Gas Concentration

I. INTRODUCTION

With the industrial production, centralized heating of boilers and the popularization of transportation tools, a large number of soot and toxic and harmful gases will be discharged. Hazardous substances accumulate gradually in the atmosphere and reach a certain concentration, which will make the normal composition of air change, thus endangering the health of human beings and various animals and plants. Various problems caused by air pollution have attracted the attention of environmental protection departments . In order to achieve accurate and real-time monitoring of environmental quality, ecological environment and pollution sources, and provide accurate basis for supervision and management of environmental protection departments at all levels and environmental decision-making of the government, a large number of modern environmental monitoring instruments are urgently needed.

At present, there are three main methods for gas detection of portable spectrometers in domestic and foreign markets: differential algorithm, electrochemical analysis and infrared spectroscopy. Differential absorption algorithm can accurately calculate the concentration of most gases, but it will lose the broadband continuous absorption information in the characteristic absorption of gases, leading to some gas concentration measurement can not come out. For example, the absorption spectrum of nitrogen dioxide molecule in the ultraviolet band is mostly gradual continuous absorption, so differential absorption algorithm may think that the absorption information of nitrogen dioxide is filtered out by scattering, resulting in the detection of nitrogen dioxide. If the absorption curves of nitric oxide and nitrogen dioxide have the same absorption peaks, the fitting absorption curves are superimposed at the measuring points, so it is still impossible to distinguish the two gases. The electrochemical analysis method has the advantages of simple structure and easy operation. It mainly depends on gas sensors, a gas sensor can only detect a corresponding gas, and the sensitivity of gas sensors is high, but after a period of time, the sensitivity of sensors to gas will decline, it is necessary to replace gas sensors in time, and gas sensors are expensive, which increases the use cost for users. The main principle of gas sensor is to use the oxidation or reduction reaction of gas to generate current, but if there are both oxidizing gas and reducing gas, the measurement results will be inaccurate . Infrared spectroscopy overcomes the shortcomings of

electrochemical analysis, but can only measure the approximate concentration of nitrogen oxides, can not accurately measure the specific concentration of NO and NO2, and infrared spectroscopy for environmental humidity, temperature and other external conditions require higher technology is more complex .

Based on defects and deficiencies of the above gas detection methods, an iterative evolution gas solution algorithm is proposed in this paper. According to the good absorption of ultraviolet light by gas at the wavelength of 190-290 nm, the number of absorbed photons can be obtained by measuring the ultraviolet light absorbed by gas. The actual concentration of gas can be obtained from the number of photons by using the iterative gas calculation algorithm.

II. THE PINCIPLE AND COMPUTATIONAL PROCEDURE OF ITERATIVE ALGORITHMS

A. *Algorithm Principle*

Mixed gases have characteristic absorption peaks in the range of ultraviolet wavelength 190-290 nm. Gas absorbance has multiple superposition. Assuming that some elementary gas does not absorb other gases on its best characteristic absorption peak, the corresponding table of absorbance and concentration of this single substance gas is searched to obtain the initial concentration of the gas, and then switch to another characteristic absorption peak. The photon number of the gas is subtracted from the total photon number measured, and the initial concentration of another gas is obtained. By analogy, the initial concentration of each gas is obtained one by one. Then, the characteristic absorption peak of the first gas is returned to, and the absorption photon number of other gases is subtracted from the total photon number absorbed, and the iterative concentration of the first gas is obtained again. By analogy, the initial concentration of each elemental gas is obtained again. By repeating the iteration until the difference of gas concentration between two adjacent times is less than a certain value, it is considered that the concentration of the elemental gas is obtained.

B. *Algorithm Steps*

1) The initial concentration c_1 of the first elementary gas in the mixed gas is solved. According to the characteristic absorption peak of the gas at wavelength λ_1 , the number of photons B $S_{\lambda 1}$ absorbed by the gas is read.Solving the value of $\frac{R_{\lambda 1}-D_\lambda}{S_{\lambda 1}-D_\lambda}$ (R_λ is the number of incident photons; S_λ is the number of photons passing through the medium.; D_λ is the number of photons in dark spectrum(Also known as dark spectral noise); λ is the wavelength of a certain ultraviolet wave, K is a constant, c is the concentration of elemental gas),The initial concentration c_1 of the elemental gas was obtained by inquiring the comparison table of absorbance and gas concentration..

2) The initial concentration c_2 of the second primary gas in the mixed gas is solved. too, Select the characteristic absorption peak λ_2 of the elemental gas and read the absorption photon number $S_{\lambda 2}$ of the elemental gas.Assuming that there are only two gases in this band, According to the formula

$$\frac{R_\lambda - D_\lambda}{S_\lambda - D_\lambda} = \frac{R_{\lambda 1} - D_\lambda}{S_{\lambda 1} - D_\lambda} * \frac{R_{\lambda 2} - D_\lambda}{S_{\lambda 2} - D_\lambda} \tag{1}$$

the absorbance of the second gas is calculated, and the concentration of the second gas is calculated by querying the absorbance and concentration table again, as the initial concentration c_2 of the second gas.

3) Solve the concentration of other elemental gases in mixed gases. Methods 1 and 2. Selecting the characteristic peak absorption wavelength of other elemental gases and reading the number of absorbed photons at that wavelength.The absorbance was calculated by formula

$$A = \frac{R_\lambda - D_\lambda}{S_\lambda - D_\lambda} = \frac{R_{\lambda 1} - D_\lambda}{S_{\lambda 1} - D_\lambda} * \frac{R_{\lambda 2} - D_\lambda}{S_{\lambda 2} - D_\lambda} * \frac{R_{\lambda 3} - D_\lambda}{S_{\lambda 3} - D_\lambda} * \ldots * \frac{R_{\lambda n} - D_\lambda}{S_{\lambda n} - D_\lambda} \tag{2}$$

(A is absorbance), and the initial concentration of gas was obtained by looking up the table.

4) Iterative Recursion of the Concentration of the First Element Gas.The concentration of all elemental gases obtained at present is substituted into the formula

$$\frac{R_\lambda - D_\lambda}{S_\lambda - D_\lambda} = \frac{R_{\lambda 1} - D_\lambda}{S_{\lambda 1} - D_\lambda} \times \frac{R_{\lambda 2} - D_\lambda}{S_{\lambda 2} - D_\lambda} \times \frac{R_{\lambda 3} - D_\lambda}{S_{\lambda 3} - D_\lambda} \times \ldots \times \frac{R_{\lambda n} - D_\lambda}{S_{\lambda n} - D_\lambda} \tag{3}$$

and the corresponding $S_{\lambda 1}$ of wavelength λ_1 is read again. The iterative concentration c_1 of the first elemental gas is obtained by checking the corresponding table of concentration absorbance.

5) Repeat 2) and 3) to find the iteration concentration c_{m1} of the elemental gas M.

6) Calculate the error of the calculation results of the same elemental gas in the adjacent two times. The first-order iteration error of each elemental gas is calculated.

$$\Delta_{m1} = \left| c_{0m} - c_{m1} \right| \tag{4}$$

7) Repeat 4, 5 and 6 until the error of two iterations of the same gas concentration is less than 3%.

$$\Delta_n < \Delta_G \tag{5}$$

The last calculated gas concentration is regarded as the final concentration of various elemental gases.

III. ALGORITHM VERIFICATION

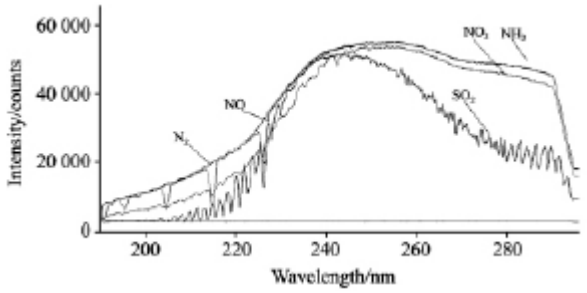


Figure 1. Mixed gas UV spectral absorption curve

Fig.1 is the absorption spectra of NO, SO_2 NH_3 and NO_2 mixed gases. Among them, N_2 is a zero gas whose spectral line is called zero gas line. Zero gas is not absorbed in ultraviolet light of 190-290 nm. Because there is Rayleigh scattering in the gas to be detected, the influence of scattering can be eliminated by using the zero-gas line spectrum as the reference spectrum.

From the observation in Fig.1, we can see that NO and NH_3 can find non-interference absorption wavelengths. These two wavelengths are just the absorption peaks of NO and NH_3, and there is no NO absorption at the NH_3 absorption peak, and there is no NH_3 absorption at the NO absorption peak. So it is easy to distinguish the two gases if we only distinguish them.The problem now is that SO_2 and NO_2 both absorb at the absorption peaks of these two gases. At the wavelength of 220 nm, the maximum absorption peaks of NO and NO_2 are close, and SO_2 absorbs a lot of ultraviolet light in this section.So if we can know the concentration of SO_2 and NO_2 beforehand, we can use the superposition of absorbance to subtract the absorbance of NO and NH_3 from the total absorbance of SO_2 and NO_2. We can get the absorbance of NO and NH_3 by looking up tables.Therefore, in order to obtain the specific concentration of various elemental gases in mixed gases, the concentration of SO_2 and NO_2 must be required first, and then the concentration of NO and NH_3 can be calculated. In this way, the concentration of four kinds of elemental gases in the mixture can be calculated.

A. Calculating the Concentrations of SO_2 and NO_2

NO_2 and SO_2 interfere with each other in the whole working band. Now it is assumed that there are two kinds of elemental gases in the mixture, NO_2 and SO_2, respectively. It is now known that the absorption spectra of mixed gases at 231.33 nm and 273.33 nm, and the absorbance of gases NO_2 and SO_2 at 231.33 nm and 273.33 nm (231.33 nm and 273.33 nm, respectively, are the maximum absorbance of gases NO_2 and SO_2 at this point). Now calculate the respective concentrations of NO2 and SO2.

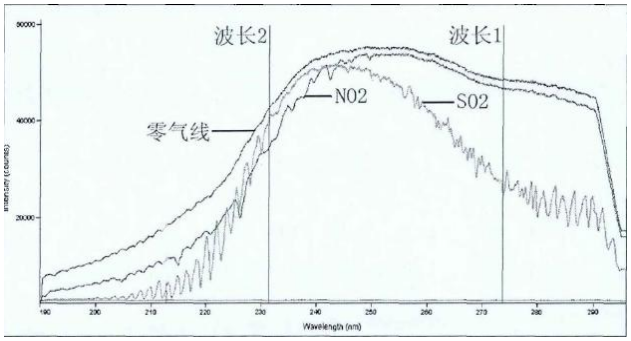


Figure 2. Absorption spectra of SO2 and NO2

TABLE I. SPECTRAL TABLES FOR SO_2 AND NO_2 AT WAVELENGTH 273.33NM AND WAVELENGTH 231.33NM

Wavelength	231.33	273.33
NO_2 absorbance	0.03003444	0.00456189
SO_2 absorbance	0.00482312	0.07984884

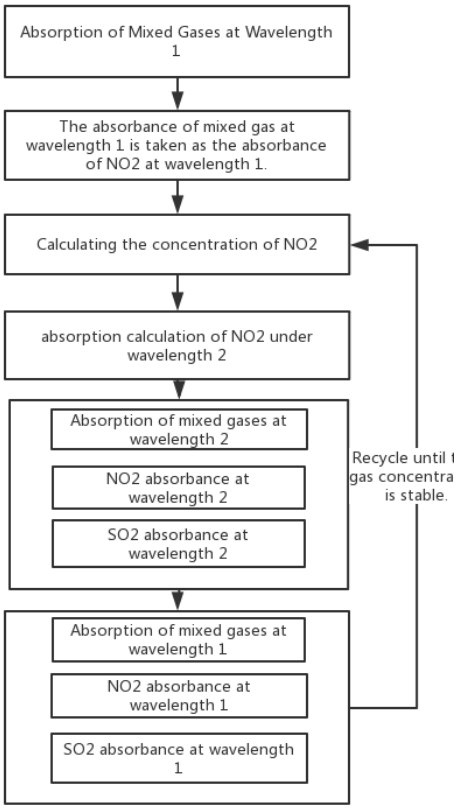


Figure 3. NO_2 and SO_2 gas concentration iterative algorithm flow chart

Fig. 3 is the flow chart of the iterative algorithm for the concentration of NO_2 and SO_2 mixed gases. After several iterations, the real concentrations of these two gases can be calculated from the mixture.

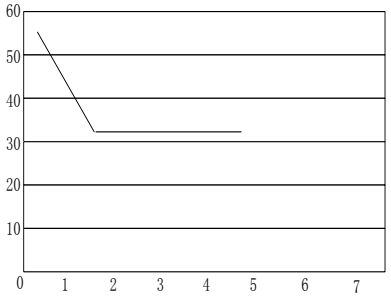


Figure 4. SO_2 concentration and the number of iterations curve

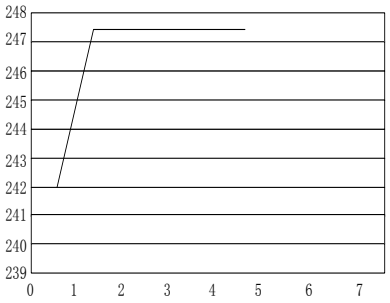


Figure 5. NO_2 concentration and the number of iterations curve

After two iterations, the numerical value of the algorithm tends to be stable, and the precise gas concentrations of NO_2 and SO_2 are basically obtained.

B. Calculating the Gas Concentrations of NO and NH_3

There is no interference between NO and NH_3 at their maximum absorption peaks, so the total absorbance and the concentration of NO_2 and SO_2 can be calculated according to the superposition of ultraviolet light. Assuming that the concentrations of NO_2 and SO_2 in mixed gases are c_1 and c_2, respectively, and the concentrations of NO and NH_3 are c_3 and c_4, the multivariate superposition of absorbance at wavelength 225.88 nm can be obtained as follows:

$$A = A_1 + A_2 + A_3 \tag{6}$$

A_1 is the absorbance of NO_2 at 225.8 nm in c_1 concentration, A_2 is the absorbance of SO_2 at 225.8 nm in c_2 concentration, A is the total absorbance of mixed gas at 225.88 nm and A_3 is the total absorbance of NO at 225.88 nm.

$$A_3 = A - A_1 - A_2 = \lg(\frac{I_0}{I}) - A_1 - A_2 \tag{7}$$

I_0 is the spectral intensity at 225.88 nm through zero gas, I is the transmission intensity at 225.88 nm through the mixture gas to be measured, the intensity can be obtained directly by spectrometer, A_2 and A_3 are calculated by the concentration of SO_2 and NO_2. In this way, the absorbance A_3 of NO at 225.88 nm can be obtained, and then the concentration of NO can be calculated according to the corresponding table between the concentration of NO at 225.88 nm and the absorbance. The absorbance

A_4 of NH_3 can be obtained by the same method at 208.23 nm, and the concentration of NH_3 can be calculated according to the corresponding relationship between NH_3 concentration and absorbance at 208.23 nm.

C. Composition of Platform Experiment System

Ultraviolet flue gas analyzer consists of three parts: flue gas data acquisition module, data processing module and data display module.

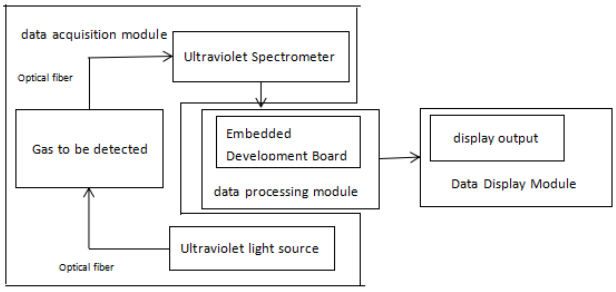


Figure 6. Experimental system composition diagram

The data acquisition module is composed of ultraviolet light source and marine optical Maya2000 Pro ultraviolet spectrometer. Ultraviolet light source outputs stable ultraviolet light. Ultraviolet light passes through the optical fiber through the detected gas. After the gas is fully absorbed, the remaining ultraviolet light is transmitted into the ultraviolet spectrometer by the optical fiber. After the optical processing and photoelectric conversion of the gas by the spectrometer, the gas information becomes an electrical signal, waiting for the data processing module to read. In this system, the ultraviolet spectrometer is actually a flue gas acquisition sensor. Data processing module is composed of embedded development board. The embedded development board reads the gas information from the ultraviolet spectrometer, calculates the actual concentration of the elemental gas through the iterative algorithm, and visualizes it through the data display module. This is the composition and working principle of the experimental system.

D. Absorption Spectroscopy of Elemental Gas and Zero Gas

N_2 is introduced into the system, and its absorption spectrum is measured when the gas concentration is stable. After that, the number of photons absorbed by NO_2, NO, SO_2 and NH_3 gases was measured in turn, and the curve was drawn by using the number and wavelength of photons.

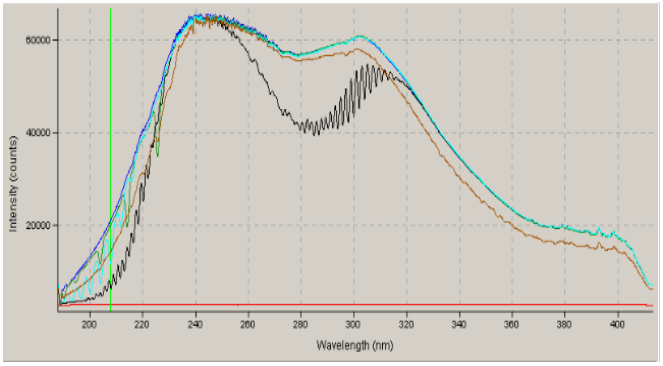


Figure 7. Four gas photon spectrum line graph

E. Data Verification

The following data are obtained when a mixture of SO_2 and NO is injected into the experimental system.

TABLE II. 200 PPM SO_2 AND NO GAS SPECTRAL DATA

	271.98nm	225.94nm	dark noise
zero gas	56434	43973	2900
SO_2 100ppm	52851	42754	2900
zero gas	56434	43973	2900
NO_2 100ppm	56386	40749	2900

Table 2 shows the number of absorbed photons and dark noise photons at 271.98 and 225.94 nm measured by ultraviolet spectrometer in a mixture of SO_2 and NO_2 at 100 ppm, respectively.

TABLE III. SPECTRAL DATA FOR MIXED GAS

	271.98nm	225.94nm	dark noise
zero gas	56434	43973	2900
mixed gas	52050	39588	2900

Table 3 shows the number of absorbable photons at 271.98 nm and 225.94 nm for zero and mixed gases, as well as the number of dark spectral noise photons measured by spectrometer. In practical calculation, the number of photons measured should be subtracted from the number of photons of dark spectral noise to obtain the actual number of photons of zero gas and mixed gas.

Based on the above data, the photon number absorption curves of elemental gases at their maximum absorption peaks are fitted.

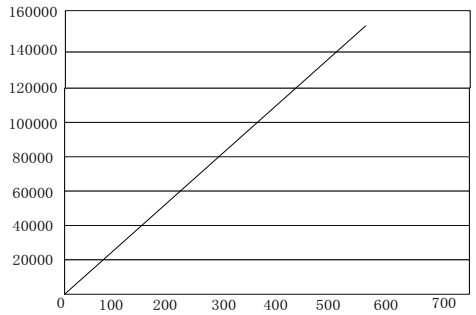


Figure 8. Fitting curve of SO_2 at 271.98 nm

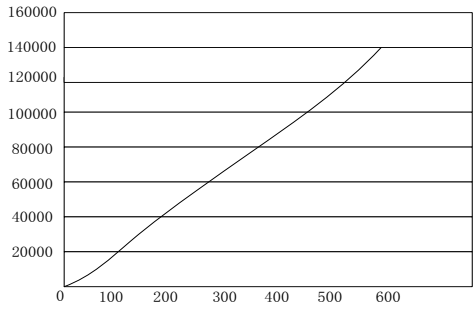


Figure 9. Fitting curve of NO at 225.94 nm

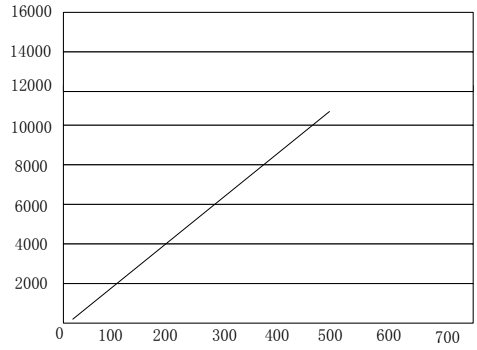


Figure 10. Fitting curve of NO at 271.98 nm

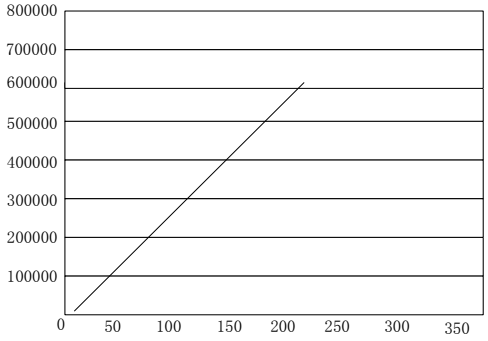


Figure 11. Fitting curve of NH3 at 271.98 nm

Figure 8-11 is a curve drawn by a single gas at the maximum absorption wavelength of ultraviolet light. Analysis table of experimental results

TABLE IV. ANALYSIS OF RESULTS

gas species	standard value （ppm）	measured value （ppm）	difference value	maximum difference	error
SO2	102	104	2	-4	0.8%
	200	196	-4		
	499	501	2		
NO	104	108	4	-7	1.4%
	200	206	6		
	500	493	-7		
NO2	116	112	-4	-9.7	1.94%
	201.5	195	-6.5		
	501.7	493	-9.7		
NH3	50	53	3	3	1.5%
	200	199	-1		
conclusion	Accuracy error is less than 3%, which meets the design standard.				

In Table 4, the standard value is the concentration of the standard elemental gas put in the test, and the measured value is the concentration of the elemental gas calculated from the mixed gas using an iterative algorithm. From the experimental results, it can be seen that the maximum error of the measured value is less than the standard value, and the maximum error of the accuracy is 1.94%, which is much less than the original design standard of 3%, which is within the normal standard.

IV. SOFTWARE IMPLEMENTATION

The software algorithm is written in JavaScript, including the analysis and implementation process of the iterative algorithm gas. The main code is as follows:

```
/*
*Iterative calculation of gas concentration
*/
function GetGasC() {
//1. Obtain absorbance from NO2
var NO2A_1 = GetAByWa(gasWavebanc['NO2']);
//2. Find the concentration of this point
var NO2C_1, NO2A_2, SO2A_2, SO2C_2,
SO2A_1, ONA_3, NH3A_4, ONC_3, NH3C_4;
for(var i = 0; i < 2; i++) {
NO2C_1=GetCByA_Data(NO2_data_231,
NO2A_1);
//3.Calculate the absorbance of NO2 at 273.33.
//NO2A_2;
NO2A_2= getAByC_Data(NO2_data_273,
NO2C_1);
```

```
//4. Obtain the total absorbance of SO2 in the optimum band and subtract the absorbance of NO2 here.
SO2A_2=GetAByWa(gasWavebanc["SO2"])
-NO2A_2;
//5. Looking up Table to Find DeSO2C_1
SO2C_2 = GetCByA_Data(SO2_data_273, SO2A_2);
//6. The absorbance of SO2 at 231.33 was obtained by //looking up the table.
SO2A_1 = getAByC_Data(SO2_data_231, SO2C_2);
//7. NO2A_1 is the total absorbance minus the //absorbance of SO2A_1 at 231.33.
NO2A_1 = NO2A_1 - SO2A_1;
}
currentGasC_NO2 = NO2C_1;
currentGasC_SO2 = SO2C_2;
//The absorbance of NO at the optimum band is the //total absorbance S-SO2 absorbance minus the //absorbance of NO2.
ONA_3 = GetAByWa(gasWavebanc["NO"]) - getAByC_Data(NO2_data_225, NO2C_1) - getAByC_Data(SO2_data_225, SO2C_2);
//Concentration of NO obtained
currentGasC_NO = GetCByA_Data(NO_data_225, ONA_3);
NH3A_4 = GetAByWa(gasWavebanc["NH3"]) - getAByC_Data(NO2_data_208, NO2C_1) - getAByC_Data(SO2_data_208, SO2C_2);
currentGasC_NH3 = GetCByA_Data(NH3_data_208, NH3A_4);
$("#NO2_C").html("No2 " + currentGasC_NO2);
$("#SO2_C").html("So2 " + currentGasC_SO2);
$("#NO_C").html("NO " + currentGasC_NO);
$("#NH3_C").html("NH3 " + currentGasC_NH3);
}
```

V. CONCLUSION

Aiming at the detection requirement of main harmful components in air pollution, a fast iteration algorithm of mixed flue gas is designed by using the continuous frequency division method of ultraviolet grating in the experimental system, and the effectiveness of the algorithm is verified. Ultraviolet spectrometer is used as a sensor. The embedded development board reads and calculates the gas concentration. The analysis and calculation of the algorithm are realized by programming. The results show that the iterative algorithm can accurately measure the concentration of flue gas and keep the error within 3%. It can meet the design requirements and solve many kinds of gases at the same time. It is suitable for practical engineering applications.

ACKNOWLEDGMENT

Thank you, Shaanxi Education Department. This work was supported in part by a grant from Shaanxi Provincial Department of Education Project (15JF019).

The authors wish to thank the cooperators. This research is partially funded by the Project funds in shanxi province department of education (15JF019), a the Project funds in engineering laboratory project (GSYSJ2018011) and the project funds in innovation and entrepreneurship training for college students (1070214033)

ABOUT THE AUTHOR

Xu Shuping (1974-), Female, Professor, School of Computer Science and Engineering, Xi'an Technological University, majoring in embedded and computer control. Email: 563937848@qq.com, Mobile: 13772148209.

REFERENCES

[1] Chen Zhi-gang. Discussion on Experimental Application of Lambert-Beer Law[J]. Acta Metrologica Sinica. 2015(1)

[2] Pop,Paul. Embedded systems design:Optimization challenges.Lecture Notes in ComputerScience, 2014, 35(24):16-20

[3] Shi Bao-song Sun Shou-hong Zhang Wei. Application of CCD in the portable spectrometer[J]. Electronic Measurement Technology. 2016(11)

[4] Limited ARM Development Guide 2000-2001.ARM DOI.2013.06.

[5] Tang Qu. “Research and design of ultraviolet flue gas analyzer [J]”. Nanjing University of Technology. 2013

[6] Jiang Xuqian. “Design of portable ultraviolet flue gas analyzer [J]”. Nanjing University of Technology. 2012

[7] Chen Bin. “Design of ultraviolet flue gas analyzer [J]”.Nanjing University of Technology. 2016

[8] Juwu ,Wu Yihui. Micro-miniaturization of spectrometer [J]. Journal of Instrumentation, 2013. 22 (4): 131-133

[9] Yu Zhiqiang, Wenzhi Yu, Xie Yingke, Zhou Suyi. The control system of multi-parameter water quality tester based on raspberry pie [J]. Instrumentation technology and Sensors, 2015 (06): 20-23.

[10] Han Xiao, Wenzhi Yu, Xie Yingke, Wei Kanglin, Zhou Xiaofeng. Software design of control and signal processing system for multi-parameter water quality tester [J]. Instrumentation technology and Sensors, 2014 (08): 20-22

Application of Chaotic Encryption in RFID Data Transmission Security

Yang Jianfang
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, China
e-mail: perfectyjf@163.com

Yao Huimin
Eighth of production plant, the company china petrdeum
Changing oilfield, Xi'an
Xi'an, 710021, China

Liu Baolong
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710032, China
e-mail: liu.bao.long@hotmail.com

***Abstract*—In order to improve the security performance of data transmission in the RFID system, the sequence generated by the chaotic map is used to encrypt the data transmitted between the reader and the tag in the RFID. Based on the unpredictability, extreme sensitivity to initial conditions, and pseudo-random characteristics of chaotic sequences, the information of each electronic tag is encrypted with a unique chaotic sequence. The same operation mechanism is used to encrypt and decrypt data, and a security model based on chaotic encryption is established. At the same time, the read/write control mechanism and security issues are explained**.

Keywords-Chaotic Encryption; Chaotic Sequence; RFID System; Security Model;

I. INTRODUCTION

Radio Frequency Identification (RFID), which is a wireless non-contact automatic identification technology, automatically identifies surrounding objects through radio frequency signals, spatial coupling (including inductive coupling and electromagnetic coupling). The basic components of RFID system mainly include background server, reader and tag. In the RFID data transmission, the wired transmission between background server and reader is considered as a secure channel, while the wireless transmission between reader and tag is considered as an unsafe channel. The basic components of the RFID system are shown in the figure:

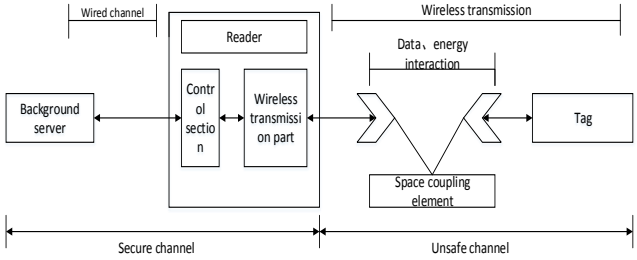


Figure 1. Diagram of the components of the RFID system.

RFID technology has been widely used in various fields due to its low cost, fast recognition speed and long service life, such as warehouse transportation management, train/car identification, baggage security inspection, access control attendance and so on. However, a lot of security problems have emerged in the process of widespread application of RFID, and it is precisely because of the remaining security problems of RFID technology that its further application and development are restricted. The security issues of RFID technology mainly come from the wireless transmission channel of readers and electronic tags, including privacy theft between authentication and data transmission. The authentication problem mainly includes the confirmation of the legality of readers and electronic tags, while the data privacy issues include tracking and leaking data information [1]. The purpose of the RFID system is to popularize the application, which requires that the cost of the reader and the electronic tag in the RFID cannot be too high, and the overly complicated security algorithm cannot be used

in the tag, which creates a difficulty for the security solution of the RFID to some extent.

In most of the currently proposed RFID system security solutions, it can be roughly divided into physical security methods, cryptographic-based security methods, and a combination of the two. The physical security method is mainly for the protection of electronic tags, including Kill command mechanism, electrostatic shielding, blocking tags, active interference, etc [2]. Some of these methods can affect the functionality of the tag. For example, the Kill command mechanism can't respond to the reader's commands by making the tag ineffective. This prevents the corrupted tag from being activated again and cannot be used again. Although electrostatic shielding can shield the interference from illegal readers or tags, it can also make the tag unrecognizable by legitimate readers and cannot be used effectively. The blocking tag evades the legal tag by simulating a large number of tags, and the active interference is to protect the legitimate tag from being detected by sending unwanted electromagnetic signals to interfere or hinder the operation of the illegal reader. The security method based on cryptography may generally include a security protocol based on a hash function, an encryption algorithm, read and write access control and so on.

Chaos is a complex behavior controlled by nonlinear dynamic laws and is a similar random phenomenon that appears in deterministic systems. It has the characteristics of extreme sensitivity of initial values, long-term unpredictability, randomness, and similar broadband spectral noise. These characteristics make chaotic systems very suitable for information encryption [3]. Logistic mapping is one of the most typical types in chaotic systems. The content of this paper is mainly to use Logistic chaotic map to generate chaotic sequences to encrypt the data transmitted between readers and tags in RFID system, which guarantees RFID system security to some extent.

II. CHAOTIC SEQUENCE ENCRYPTS RFID TRANSMISSION DATA

A. *Introduction to chaotic mapping*

The essence of chaotic encryption is serial cipher encryption. The basic principle is to divide the plaintext data into multiple parts of continuous characters, and then use the generated chaotic key stream sequence to perform encryption calculation with the plaintext characters bit by bit, and use the synchronous generated key stream when the sequence is decrypted, and its basic schematic is shown below:

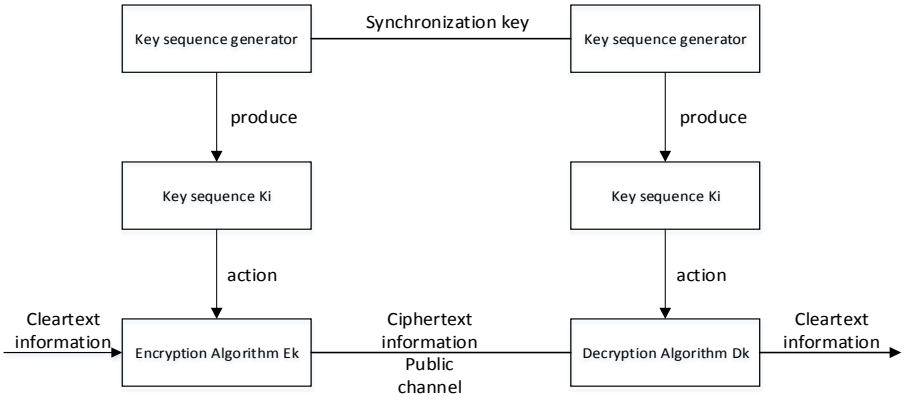


Figure 2. Data information encryption/decryption schematic.

The chaotic sequence generator is the core of chaotic encryption, which used to generate the chaotic key sequence. It then converted into an encrypted sequence for encrypting plaintext information through the conversion operation. The chaotic sequence generator can be represented by several parts in the following figure:

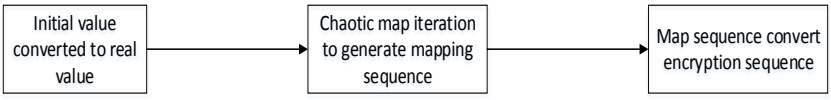


Figure 3. Chaotic sequence generator process diagram.

Chaotic map is an important part of chaotic sequence generator, and its general form can be expressed as:

$$x_{n+1} = \mu(x_n - x_n^{\,2}) \tag{1}$$

Among them, μ represents the system parameter, its value range is (0,4), x_n represents the iteration value, and takes values in the range of [0,1]. The above equation is used as a mathematical equation for chaotic mapping, and a chaotic iterative sequence for encryption is generated by multiple iterations.

Based on the purpose of deep analysis of the characteristics of Logistic mapping, this paper is simulated by matlab, and the logistic mapping bifurcation diagram obtained by taking the initial value is 0.6, while the parameter values are different, is shown in the following figure:

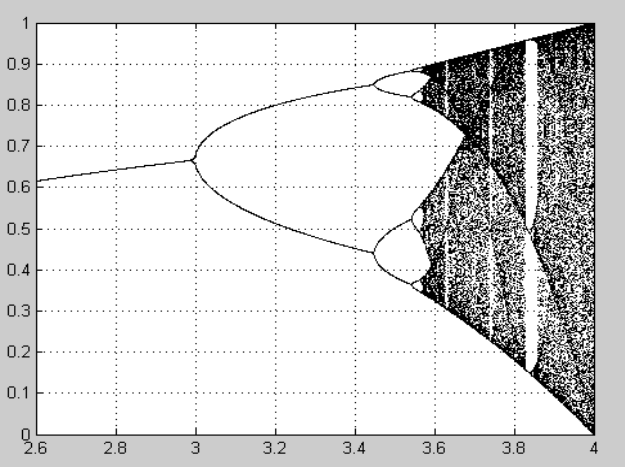


Figure 4. Logistic map bifurcation diagram.

As can be seen from the above figure, the Logistic map is from the double-period bifurcation into the chaotic state. When the value of μ is about 3.5699,the Logistic map enters the chaotic state. Therefore, the μ value range of the Logistic map in the chaotic state is (3.5699, 4), and although the Logistic map is a one-dimensional system, it can generate complex chaotic behavior.

It can be found that the Logistic mapping system only generates chaotic behavior when the initial value and the parameter value are within a certain range, and the degree and randomness of chaos are also affected by different initial values and different parameters.

B. Implementation of chaotic encryption

The chaotic sequence is a sequence of chaotic real values generated by chaotic mapping after multiple iterations, and then formed by some transformation operations. Theoretically, the chaotic sequence is a non-periodic sequence with statistical properties close to Gaussian white noise [4]. The initial value and parameter value required for chaotic mapping in the process of starting the iteration are determined by the label, The initial value x_0 is obtained by the serial number of the unique identification label, and the value of parameter μ is obtained by the read operation keyword, and it is determined according to the user's own needs. Thus, there exists a security policy that the data information of each tag uses a unique chaotic sequence to encrypt. In addition, the iterative sequence generated by the chaotic map is the real field value, and the data processed by the RFID is a binary field. Therefore, the real field value generated by the chaotic map must be converted into a binary sequence for encryption, and the corresponding domain conversion is described in the next section.

The following is a detailed explanation of the general encryption process of Logistic chaotic map. The specific process is as follows:

a) select the parameter value for μ in (3.5699,4), and design the chaotic sequence generator using (1) to generate the key stream factor sequence*;*

b) use the serial number of the tag as the initial value and enter it into the Logistic system;

c) iterate from the current position;

d) converting the iterative chaotic real value into a binary form of the key stream sequence, extracting a part as an encrypted sequence;

e) select the plaintext data of the specified location as the data to be encrypted;

f) the binary encryption sequence extracted in step d) with the plaintext information sequence to perform encryption calculation to obtain a ciphertext sequence;

g) The current operation track is used as the initial parameter of the next stage of encryption, and is reserved for use;

h) Determine whether the encryption operation is completed. If it is completed, it will enter the end state, otherwise it will return to step c).

The above process can be represented by a flow chart as follows:

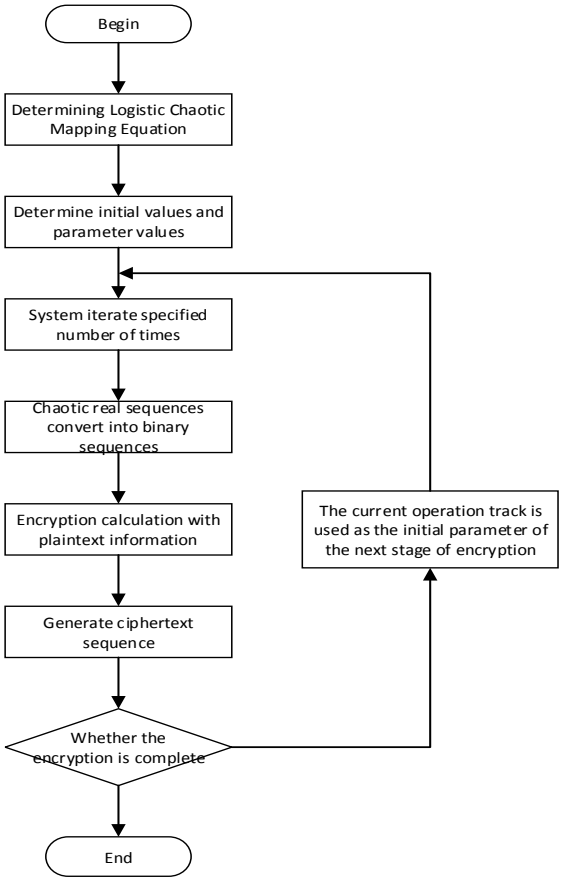


Figure 5. Logistic chaotic encryption flow chart.

It can be seen that the information is written into the electronic tag after being encrypted by the uniquely determined chaotic sequence, which greatly improves the security of the tag data to a certain extent.

C. Domain conversion of chaotic systems and encryption systems

The domain of chaotic system processing is the real number field, and the data processed by the RFID system is binary. This inevitably requires the conversion of real and binary values. The conversion mechanism between them is introduced below.

When the chaotic sequence generator iteratively generates the chaotic sequence, it is necessary to determine the initial value and the parameter value. In the process of designing, the initial value and the parameter value are associated with the label, and the serial number of the unique identification label is used as the initial value, and the user-defined read operation keyword is used as the parameter value. Here, the serial number and the read operation key are expressed in binary form. The process of converting the real value is as follows:

Initial value calculation process: Assuming that the RFID system uses a 16-bit binary number, and the range in which the serial number is converted to a decimal number is (0, 65535). The initial value x_0 of the Logistic chaotic system ranges from (0,1), First the calculation factor of x_0 is $(1-0)/65535 \approx 1.526\times10^{-5}$, The value which obtained by converting the binary number of the serial number into a decimal number and multiplying by the calculation factor is taken as the value of the initial value x_0. Listed below: the binary form of the serial number (1000 0000 0000 1010) converted to a decimal number of 32778, multiplied by the calculation factor (1.526×10^{-5}) and the initial value x_0=0.50019228.

Parameter value calculation process: In the RFID system, the read operation keyword is also a 16-bit binary number. The value of the parameter μ in the Logistic chaotic system is (3.5699456, 4). First, the calculation factor of the parameter μ is determined to be $(4-3.5699456)/65535 \approx 6.5622\times10^{-6}$, and the binary number corresponding to the parameter μ is converted into a decimal number and multiplied by the calculation factor, and finally 3.5699456 is added as the decimal value of the parameter μ. Listed below: The binary form of read operation keyword (1100 0010 0010 0100) is converted to a decimal number of 49700, which multiplied by a calculation factor (6.5622×10^{-6}) and equal to 0.32614134, parameter value μ=0.32614134+3.5699456=3.89608694.

It should be noted that the initial value x_0 is determined by the serial number of the unique identification tag, which indicates that its uniqueness determines that the chaotic sequence iterated by is also uniquely determined, and can be utilized as a private key in the encryption and decryption system. The parameter μ is determined by the read operation keyword, and the read operation keyword can be shared by the reader and the tag, and can be utilized as a public key in the encryption and decryption system.

The above is the process of converting the binary value into a real value when the chaotic sequence is started. After the chaotic encryption sequence is obtained, it needs to be binarized when encrypting the data transmitted between the reader and the tag in the RFID system. The chaotic signal $x(n)$ is converted into a binary sequence stream $b(n)$,and the quantization

function $T[x(n)]$ must be introduced in the process of conversion. The mathematical definition is as follows [5][6]:

$$T[x(n)]=\begin{cases}0 & x(n)\in\bigcup_{i=0}^{2^k-1} I_{2i}^k \\ 1 & x(n)\in\bigcup_{i=0}^{2^k-1} I_{2i+1}^k\end{cases} \quad (2)$$

Where k is an arbitrary integer greater than $0, I_0^k, I_1^k, I_2^k, \cdots$ are 2^k consecutive contiguous partitions of the initial value x_0. The above equation shows that if the chaotic signal $x(n)$ falls within the defined interval of the odd number of the quantization function as the initial bit, the corresponding binary value is 1, if it falls within the defined interval of the even number of the quantization function as the initial bit, the corresponding binary value is 0. After the conversion, because of maintaining the good randomness and unpredictability of the chaotic sequence $\{x(n)\}$, The experimental analysis proves that the above quantitative method has excellent statistical characteristics such as uniform 0-1 ratio distribution and autocorrelation [7].

III. RFID SYSTEM SECURITY MODEL AND READ/WRITE CONTROL MECHANISM, SECURITY DESCRIPTION

A. RFID system security model

The chaotic sequence generated by the above method is used to encrypt and calculate the data information written in the tag, and then sent to the wireless transmission part of the reader for transmission, and the data read back by the tag, the reader also uses the same chaos sequence to decrypte and sent to the background server for processing. In this link, the data touched by the tag, the wireless transmission and reception part and the airborne signal transmission are all chaotically encrypted data, and the ciphertext does not have any useful information. Without knowing the structure of the reader and the details of chaotic encryption, it is impossible to illegally obtain the data in the tag to be decrypted into the original data information, which greatly improves the confidentiality and security of the RFID system. The security model of the RFID system is shown below:

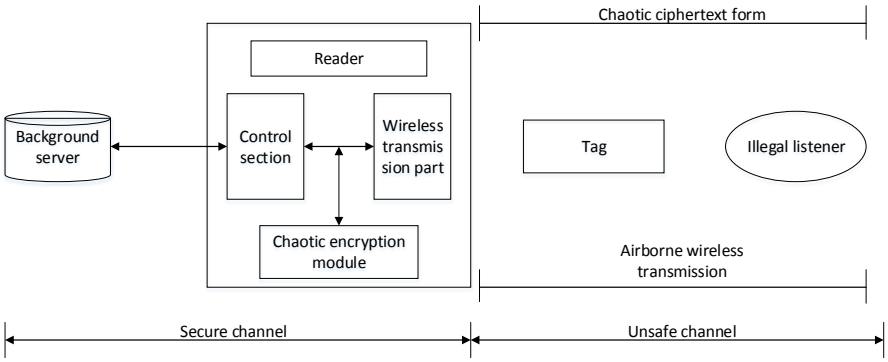


Figure 6. RFID system security model.

Based on the above RFID system security model, coupled with the read and write control mechanism of the next section, the security of RFID data is effectively guaranteed.

B. read and write control mechanism of Chaotic encryption

The legality of the reader and the tag must be verified before the RFID data transmission, which requires the establishment of a read-write control mechanism between them. This control mechanism is established in the case of chaotic encryption, which is in the unsafe communication channel between the reader and the tag. The read and write control mechanism of the RFID system is shown in the following figure:

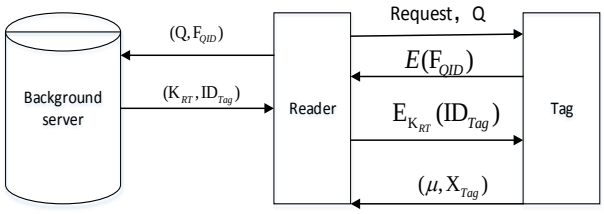


Figure 7. Read and write control mechanism after chaotic encryption.

The basic process is as follows:

K_{RT} is a shared key only by legitimate readers, tags, and servers, and ID_{Tag} is a unique number that identifies tag information.

a) The reader sends an authentication request to the surrounding tags, the tag is activated and waits for the command;

b) The tag calculates the received random number Q and its own ID_{Tag} , such as $F_{QID} = f(Q, ID_{Tag})$, the f operation is a reversible operation, then the tag encrypts F_{QID} by the shared key K_{RT} to $E(F_{QID}) = e_{K_{RT}}(F_{QID})$, and then the encrypted result $E(F_{QID})$ sent to the reader;

c) After the reader receives the $E(F_{QID})$, the decryption operation obtains F_{QID}, and then sends it to the background server together with the random number Q;

d) The background server calculates f reversible operation to get $ID_{Tag}^{'}$, and queries the local ID_{Tag} to see if $ID_{Tag} = ID_{Tag}^{'}$ exists. If it exists, it proves the validity of the label, and then sends the matching (K_{RT}, ID_{Tag}) to the Read. , otherwise the information which returned to the Reader is that the Tag is illegal;

e) After the reader receives the information (K_{RT}, ID_{Tag}) of the background server, it encrypts and calculates $E_{K_{RT}}(ID_{Tag}) = f(K_{RT}, ID_{Tag})$, and the f operation is reversible and then sent to the label;

After the tag receives $E_{K_{RT}}(ID_{Tag})$, it calculates $ID_{Tag}^{'} = f^{-1}(K_{RT}, E_{K_{RT}}(ID_{Tag}))$ to see if it is equal to its own ID_{Tag}. If it is equal, it proves the legality of the reader, so the tag will. passed the data information (μ, X_{Tag}) in the memory to the Reader. After the Reader obtains the parameter μ and the data information X_{Tag} , which generates a chaotic decryption sequence together with the initial value x_0 ,and decrypted to obtain the original correct information with the obtained data information. If they are not equal, the Reader is not legal and the Tag does not respond.

C. Safety instructions

In the RFID system security model, the data transmitted by the RFID is encrypted by using the nonlinear characteristics of the chaotic system [8],so that the encrypted RFID data ciphertext is basically similar to the white noise sequence, and there is no law at all, and it is completely impossible to find some characteristics of the original information. Even if the information in the tag is illegally obtained, the original information cannot be decrypted correctly; under the strict protection of the read/write control mechanism, the identity information of the reader and the tag can be effectively verified, and the illegal reader and the illegal tag are avoided. It ensures the legality and security of the data transmitted by the RFID system.

IV. CONCLUSION

In the context that the wireless unsecure channel between the Reader and the Tag of the RFID system may be subjected to various types of attacks, this paper uses the chaotic encryption sequence generated by the Logistic chaotic map to encrypt the data transmitted by the RFID. The generated ciphertext sequence is equivalent to the noise sequence, having the characteristic of confusion and unpredictability. As a result, the difficulty of ciphertext analysis after encryption is greatly increased. It correspondingly enhanced security and confidentiality of RFID data. In addition, the read-write control mechanism and the domain conversion of the chaotic system and the encryption system are described in detail. However, the chaotic encryption mechanism discussed in this paper still has some drawbacks and shortcomings, such as how to solve the nonlinear dynamic degradation problem of Logistic map and to ensure the randomness of chaotic sequences. These shortcomings need to be studied and solved in the future.

ACKNOWLEDGMENT

This work is partially supported by Science & Technology Program of Weiyang District of Xi'an City with project “201836".

REFERENCES

[1] ZHANG Yong-ping, WANG Feng-jian. Research of Chaotic Encryption Based RFID System Information Security[J]. Computer Security, 2010.

[2] ZHAO Yu-hua. The research of security protocol in RFID system based on theory of chaotic cryptography[D].Master's Degree Thesis of Hunan University, 2011.

[3] DENG Ai-ping, XIAO Ben. Application of Chaotic Encryption Algorithm in RFID Secure Mechanism[J].Materials Science and Information Technology, 2012.

[4] DING Xin. Hyper-chaotic Encryption Based RFID System Informaton Security[J].China Conference, 2006.

[5] ZHAO Yu-xin, WANG Wei, LIU Li-qiang. A Design and Analysis for Non-linear Combination Chaotic Stream Cipher Based on Logistic Map[J].Journal of Projectiles and Guides, 2007.

[6] QIU Yue-hong, HE Chen, ZHU Hong-wen. One Chaotic Map with Infinite Collapses and Its Quantified Sequences[J].Journal of Shanghai Jiaotong University, 2002.

[7] WU Hong, DING Qun, ZHOU Ping. Logistic Chaotic Sequence Design and Aplication in Data Encription [J].Journal of Instrumentation, 2009.

[8] Geo-Su Yim. Design of an RFID Communication Protocol Using Synchronized Chaotic Systems[J].Journal of Korea Institute of Information and Telecommunications Technology, 2016.