# Research on Real-Name Routing and Trusted Connection Based on IPV9 and CPK-card

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

Nan Xianghao
[1.]Chinese Decimal Network Working Group, Shanghai, China
[2.]Shanghai Decimal System Network Information Technology Ltd. Shanghai, China
E-mail: nanxh2001@163. com

AliAbZoraghchin
Department of Computer Engineering Allame Mohaddes Noori Institute of Higher Education Mazandaran, Iran
E-mail: aliab@yahoo.com

***Abstract*—Router is the basic component of the Internet. In this scheme, identification technology is used for the first time in router design to provide address authenticity proof to prevent illegal access. Provide proof of connection freshness to prevent reissue attacks; the first use of software identification technology, to provide the credibility of the router operating environment, to prevent Trojan and other malicious software intrusion. The design also provides densification function to ensure privacy. This is a key security requirement for the next generation of Internet protocols. This design method will be combined with the new addressing technology of geographical location addressing to construct the next generation of Internet routers. The technology is also used in the design of new switches in telecommunications networks.**

***Keyword-IPV9; CPK-card; Real-Name Routing; Trusted Connection***

## I. INTRODUCTION

Routers work in the network layer of the OSI seven-layer protocol. Their main function is to connect the network with the network and forward packets between the networks. Routers have become the most important network equipment, so the research on the new generation of routers will become the core technology of the next generation of Internet research. Due to the IPv4, IPv6 protocols that used in the Internet, the new requirements for trusted Cyber Security connections are not met. The TCP/IP protocol has no security concerns, it does not provide address authentication, does not prevent unauthorized access, and does not protect against DOS attacks.

At present, all kinds of malicious software and spam information are rampant on the Internet, which seriously pollutes the use environment of the Internet and directly affects the survival of the Internet. As a result, all countries over the world have developed a new generation of green Internet research. In 2008 the European Union's 65 scientific institutions jointly issued the brad declaration, calling for a new generation of the Internet. The European Union has raised 9.1 billion Euros to support future Internet research and development. The U.S governments have also successive proposed identity authentication and Addressing system as major scientific research tasks, and emphasized international cooperation. ISO, the international standards body, put forward its plan for the future network in 2007.

In 2007, Chinese researchers Xie Jianping proposed the IPv9 geographical location addressing method, which solved the problem of combining IP address with geographical location. Later, South Korea also proposed the idea of geographical location addressing, and becoming the second country to propose a new method of addressing. CPK (Combined Public Key) identity authentication technology is mature and can be used in Internet protocol to realize trusted connection.

So far, China had already had the technology foundation that research and development next generation router and future network protocol.

## II. REQUIREMENTS FOR TRUSTED CONNECTIONS

In order to realize the trusted connection between routers and users, the user name (Pc1) and route address (Alfa) are identified for identity authentication. Among routers, mutual authentication is made with IP address as identity, and mutual authentication is made with user name as identity between users. Suppose that Pc1ID is the user name of a client and AlfaID is the IP address of a router. Assume that AlfaID="china-beijing-haidian-peking university" and BetaID="china-beijing-haidian-tsinghua university".

Now assume the starting address is AlfaID and the destination address is BetaID, and the connection process is shown in figure 1 (dotted lines indicate that CPK-card is used and the original address is identified)..

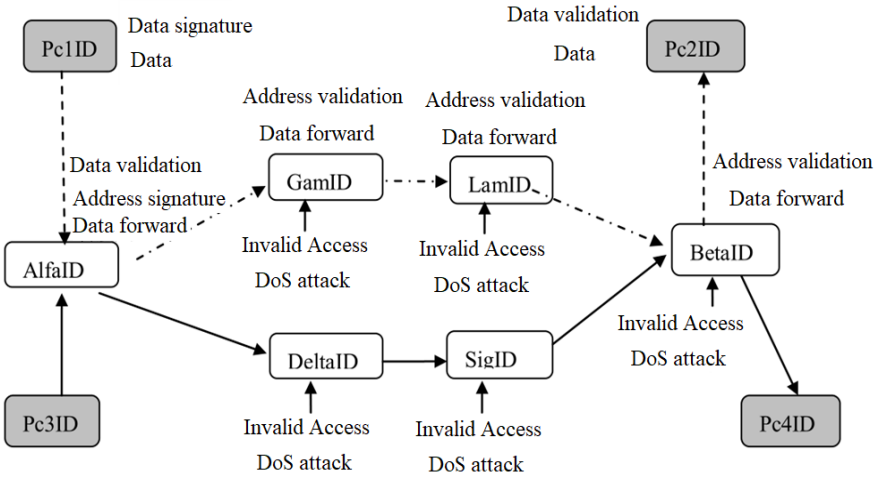


Figure 1. Data workflow diagram

The IP packet of the original router passes through multiple routing routers and finally arrives at the destination router. Illegal access is easy to access in the intermediate routing router. It can be seen from the working principle of the above router that previous routers only pay attention to the routing of the next hop and do not care where the packet comes from. Therefore, if we do not solve the origin address verification, we cannot overcome the illegal access.

Some people try to solve the problem of illegal access by means of encryption, but under the condition of public key system, this is futile. For example, Beta is the receiving party, and its public key is public, so anyone can encrypt Beta, so Beta still doesn't know who the sender is.

In order to achieve the trusted connection, the router must meet the following four conditions:

*1)* The primary IP address must be given to send proof of address; it can be verified by any one place;

*2)* All routing routers verify the original address, and reject forward if there is any discrepancy;

*3)* It can prevent illegal access and resist DOS attacks.

*4)* The internal computing environment of the router is reliable.

## III. IPV9 CONNECTION ENVIRONMENT

The connection policy is as follows.

**Path 1** (all using IPV9 protocol and CPK-card)

*1)* Pc1ID signs the data with pc1 and delivers the signed data to the router AlfaID.

*2)* AlfaID signs the time with alfa and forwards it to the next router, which verifies the signature of the original address. If the verification passes, the data is forwarded to the next router.

*3)* GamID, LamID, BetaID and other routing operations are the same as above.

*4)* The BetaID route forwards the data to the receiving user Pc2ID.

**Path 2** (Client adopts IPV9 protocol, but does not use CPK-card) :

*1)* Pc3ID does not use CPK-card but sends data to Pc4ID via routing AlfaID via PT converted to IPV9 protocol.

*2)* The AlfaID route obtains the packet source address as the public key and verifies the correctness of the source.

**Path 3** (The client does not use IPV9 protocol and CPK-card):

*1)* Pc3ID does not use CPK-card and USES IPV4/IPV6 protocol to route data to Pc4ID via AlfaID.

*2)* Route through the DeltaID and SigID routes to the BetaID route and forward the data to PC4ID.

**Path 4** (The client adopts IPV9 protocol and USES CPK-card, but the middle V9 route does not use CPK-card):

*1)* Pc1ID using the local address as the public key to sign the data and sends data to Pc2ID via route AlfaID.

*2)* The AlfaID route takes the source address of the packet as the public key and verifies the correctness of the source. After verification of the source address, remove the original signature and use the local address as the public key signature. After the signature, forward the normal routing data.

*3)* Instead of using CPK-card, GamID obtains the source address of the packet as the public key and verifies the correctness of the source. If the address is not legitimate, the data is discarded and the normal routing data is forwarded.

*4)* LamID, BetaID and other routing operations are the same as above.

*5)* The BetaID route forwards the data to the destination Pc2ID.

The IPV9 v4/v6 compatible data forwarding process is shown in figure 2.

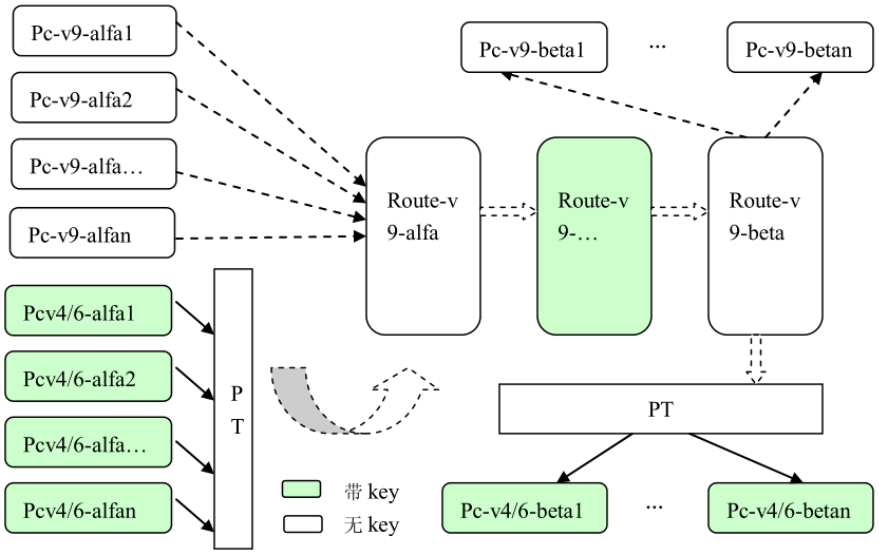


Figure 2. Data forward process diagram

## IV. IPV9 AUTHENTICATION FUNCTION

### A. *CPK-Card*

CPK is a public key-based cryptography system that takes the identity of any entity directly as the public key, while the private key is distributed in the form of ID-card. Now, for example PC1, ALFA (uppercase) and so on respectively represent their public keys, pc1, alfa (lowercase) and so on respectively represent their private keys. If it has been insert a CPK-card defined as AlfaID on any router, the router becomes the identified router as AlfaID. Similarly, any router inserts a CPK-card defined as BetaID, and the router becomes the identified router as BetaID.

The router is configured with CPK-card, which has the functions of digital signature and key exchange. The contents of CPK-card are as follows: let the router's IP address be alfa (alfa may be the real name of China. Beijing. Haidian. Peking University etc. and it can be changed into machine executable code after the unified name translation). ID-card format and size is as table 1.

### *B. Original address identification*

Suppose the original place is AlfaID, the next router is GammaID, AlfaID sends data, Mas1 AlfaID→GammaID:{Alfa, sign1, Beta, time data, checksum}

Where, sign1 is the signature of the original AlfaID address, that is sign1= SIGalfa (time), BetaID is the destination address, SIG is the signature function, and alfa is the private key of the signature, provided by CPK-card. Where data is data from the application layer, data may be plaintext or ciphertext. The router's job is to pass the data to the next router.

TABLE I. ID-CARD FORMAT AND SIZE

| | | | |
|---|---|---|---|
| 1 | Z1: Validate parameter | 16B | EPWD(R1)=Z1 |
| 2 | Z2: Validate parameter | 16B | ER1(R1) ⊕ R1=Z2 |
| 3 | Identify definition | 25B | alfa |
| 5 | Private key 1 | 32B | ER1(csk1)=Y1 |
| 6 | Private key 2 | 32B | ER1(csk2)=Y2 |
| 10 | Issue unit | 25B | KMC |
| 11 | Signature of issue unit | 48B | SIGkmc （MAC） |

GammaID verifies the signature of original address: SIG -1ALFA(time )=sign1'

Where SIG-1 is the validation function and ALFA is the public key. If sign1=sign1', allow this connection, forward Msg1, and audit. Identify replay attacks against time.

## V. IPV9 ENCRYPTION FUNCTION

The structure of data is defined as follows: Data={Pc1ID,Pc2ID,data, mac}, Where Pc1ID is the sender and Pc2ID is the receiver.

When the data is in plaintext: Data={ Pc1ID, Pc2ID, clear-text, mac};

When the data is in ciphertext: Data={Pc1ID, Pc2ID, coded-key, coded-data, mac};

If the encryption and decryption function is provided by the router, and Alfa encryption and Beta decryption are set, then data encryption can only be done in a non-online way.

If the router is responsible for encryption and decryption, and this data is encrypted data, coded key and coded data need to be interpreted and a series of steps shall be performed:

*1)* Generate random number R, AlfaID calculation key: key=R × (G); where G is the base point of the elliptic curve; key will be used to encrypt the data;

*2)* 2) Calculate the sending key: R(BETA)=coded-key, where BETA is the public key of BetaID and coded-key is sent to BetaID.

*3)* 3) Encrypt data: Ekey (data) =cipher-text;

Send ciphertext cipher=text and coded-key to BetaID.

BetaID receives a signal from the AlfaID and automatically enters the decryption process.

- BetaID computes the inverse of the private key: beta-1 ;
- BetaID calculates the session key: beta-1(coded-key)=key;
- Data decryption：Dkey(cipher-text)= data.

## VI. IPV9 PACKET HEADER FORMAT AND ENCODING FORMAT

### *A. Packet header format*

The new features require the development of a new IP header format that includes at least the original address, the start address identifier, the destination address, the data, and the checksum. Data encryption only affects the data format, not the IP packet header format.

| **Version** | **Category** | **Flow label** | **Payload Length** | **Next Header** | **Hop limit** |
|---|---|---|---|---|---|
| Source address | | | | | |
| Destination address | | | | | |
| time | | | | | |
| Identification code (signature) 40BYTE | | | | | |

*B. IPV9 coding format*

The encoding format of IPV9 is shown in the following table 2.

TABLE II. ENCODING FORMAT OF IPV9

| **segment** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|
| Head segment | Address area | | Entity code | Vendor code | Product code | Product class code | |
| | Country code | District code | | | | Year code | Single product code |
| 2 | 4 | 6 | 4bit | 14bit | 20bit | 8bit | 199bit |
| | | 362300 | 3211 | 123345678912345 | 12345678912345678912 | 20090317 | 32564328 |

When the industrial standard "business RFID label data format" is adopted, the enterprise product coding data format is as follows:

*1)* The basic data format of enterprise products is as follows:

12345678912345-12345678912345678912-20090317-32564328

*2)* When data exchange is used between management departments, the format of enterprise product data is:

3221-12345678912345-12345678912345678912-20090317-32564328

*3)* When data is exchanged between regions and management departments, the format of enterprise product data is:

362300-3221-12345678912345-12345678912345678912-20090317-32564328

*4)* When data are exchanged between countries:

*a) When exchanging with the itu-t E164 data system, the data format is:*

00-8600-36230 — 3221-12345678912345-12345678912345678912-20090317-32564328.

*b) When exchanging with ISO's object identifier data system, the data format is:*

01-8600-362300 — 3221-12345678912345-12345678912345678912-20090317-32564328.

*c) When exchanging with the object identifier data system of ISO/ITU, the data format is:*

02-8600-362300 — 3221-12345678912345-12345678912345678912-20090317-32564328.

*C. Enterprise product IPV9 address format*

*1)* The basic IPV9 address format of enterprise products is:

12345678912345]12345678912345678912]20090317]32564328.

*2)* When data exchange is used between management departments, the IPV9 format of enterprise product data is:

3221]12345678912345]12345678912345678912]20090317]32564328.

*3)* When data is exchanged between regions and management departments, the IPV9 format of enterprise product data is:

362300]3221]12345678912345]12345678912345678912]20090317]32564328

*4)* When data are exchanged between countries, the IPV9 format is:

*a) When exchanging with the ITU-T, E164 data system, the IPV9 data format is:*

00]8600]362300]3221]12345678912345]12345678912345678912]20090317]32564328

*b) When exchanging with ISO's object identifier data system, the IPV9 data format is:*

01]8600]362300]3221]12345678912345]12345678912345678912]20090317]32564328

*c) When exchanging with the object identifier data system of ISO/ITU-T, the IPV9 data format is:*

02]8600]362300]3221]12345678912345]12345678912345678912]20090317]32564328

## VII. IPV9 TRUSTED COMPUTING

In order to ensure the credibility of the operation of the router, all the execution code in the router must be certified by the manufacturer (level 1 certification), that is, the manufacturer sign on the appearance of all the execution code. Each router has an authentication function (provided by CPK-card).

### *A. Proof of software code*

The manufacturer has a CPK-card, which can carry out manufacturer signature on all system software in the router. Implementation software is divided into software identity (codeID) and software ontology (codeBD), which are signed by the manufacturer respectively:

$$SIG_{manufacturer}(codeID) = sign1$$

$$SIG_{manufacturer}(codeBD) = sign2$$

Where, SIG is the signature function, manufacturer is the private key of the manufacturer, codeID is the name of the executing code, and codeBD is the HASH value of the executing code ontology. Any executing code in the router has its own authentication codes, sign1 and sign2.

### *B. Identification of software code*

The router inserts the CPK-card so that it has the CPK authentication function. There are two ways to verify the router: one is to uniformly verify when the router is turned on, and the code that fails to pass the verification is uniformly deleted to ensure that the router system returns to the original state; the other is that when software code is invoked, it is validated first and then executed.

Verify sign1 and sign2 respectively:

$$SIG^{-1}_{MANUFACTURER}(codeID)=sign1'$$

$$SIG^{-1}_{MANUFACTURER}(codeBD)=sign2'$$

Where MANUFACTURER is the public key, it is allowed execute if sign1=sign1'and sign2=sign2', otherwise it is rejected. In this way to ensure that the implementation of the router code is the manufacturer certification code, other code will not be executed, from the attack of viruses, Trojans.

## VIII. CONCLUSION

The TCP/IP protocol does not guarantee trusted connections, so it must be modified. Based on geographical encoding and location addressing, three key techniques of trusted methods are proposed in this paper. Use address identification mechanism to prevent illegal connection; Adopt random Q&A mechanism to prevent replay attack; Software code can be identified by the mechanism, to prevent the intrusion of viruses, Trojans.

The above design method is fully applicable to the trusted connection of the physical layer. There are two kinds of physical layer: one is the physical layer defined in the seven-layer information network protocol, and the platform supporting the information network is the application program interface (API). The second is the physical layer defined in the telecommunications network, and the platform supporting the telecommunications network is the telecommunications reference point (TRP). In the information network, if the network layer can guarantee the credibility of transmission, the security of the physical layer can be replaced by the network layer. However, the physical layer of the telecom network, without modification, cannot achieve trusted connection, cannot prevent illegal access. It is modified in exactly the same way as the router.

## REFERENCES


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

[2] Nan Xiang-hao. CPK Combined Public Key System [J]. Information Security and Communication Confidentiality, 2013(03):39-41.

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

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

[5] Nan Xianghao. CPK Public Key System and Identification Identification. [M]. Beijing: People's Posts and Telecommunications Press, 2013.

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

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

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

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