IPV9 的实名路由和可信连接

谢建平 南湘浩

1 概要

信息网络中的路由器是互联网的基本部件。本方案在路由器设计中第一次采用标识鉴别技术，提供地址真实性证明，防止非法接入；提供本次连接新鲜性证明，防止重发攻击；第一次采用软件标识鉴别技术，提供路由器操作环境的可信性，防止木马等恶意软件的侵扰。本设计还提供加脱密功能，保证私密性。这是新一代互联网协议的关键的安全需求。本设计方法将与地理位置编址的新型寻址技术相结合，可构建下一代互联网的路由器。本技术也使用于电讯网络中的新型交换机的设计。

路由器工作在 OSI 七层协议中的网络层，其主要功能是将网络和网络连接起来，在网间进行数据包的转发。路由器已成为最重要的网络设备，因此，新一代路由器的研究将成为下一代互联网研究的核心技术。由于已往的互联网运行的 IPv4, IPv6 协议，不满足 Cyber Security（网际安全）可信连接的新要求。TCP/IP 协议没有考虑安全问题，不能提供地址真实性证明，不能防止非法接入，也不能抵抗 DOS 攻击。目前，在互联网上横行各种恶意软件和垃圾信息，严重污染互联网的使用环境，直接影响到互联网的生存。因此，各国纷纷开展新一代绿色互联网的研究。2008 年欧盟 65 个科研机构联合发表了布莱德宣言，呼吁开发新一代互联网。欧盟筹集了 91 亿欧元支持未来互联网的研发。美国奥巴马政府今年刚刚把标识认证（identity authentication）和地址编码系统（Addressing system）作为主要科研任务提出来，并强调了国际间的合作。国际标准组织 ISO 在 2007 年提出未来网络计划。

在我国还没有正式提出下一代互联网计划，但是各项工作在悄悄进行。我国 IPv9 已实现了地理位置寻址方法，解决了 IP 地址与地理位置相结合的实名地址问题。后来韩国也提出地理位置编址和寻址的思路，成为第二个提出新的寻址方式的国家。CPK 标识认证技术已成熟，可用于互联网协议中，实现可信连接。至此，我国已具备了研发下一代路由器和互联网协议的技术基础。

2 可信连接的要求

为了实现路由器之间和用户之间的可信连接，在用户名（Pc1）和路由地址(Alfa)作标识进行标识认证。在路由器之间，以 IP 地址作为标识互相认证，在用户之间以用户名作为标识互相认证。设 Pc1ID 是一个客户端的用户名，AlfaID 是一个路由器的 IP 地址，假设 AlfaID=“中国－北京－海淀－北京大学”，BetaID=“中国－北京－海淀－清华大学”。

现假设出发地址为 AlfaID，目的地址为 BetaID，其连接过程如图 1（虚线表示使用了 CPK-card 并进行了原发地址鉴别）

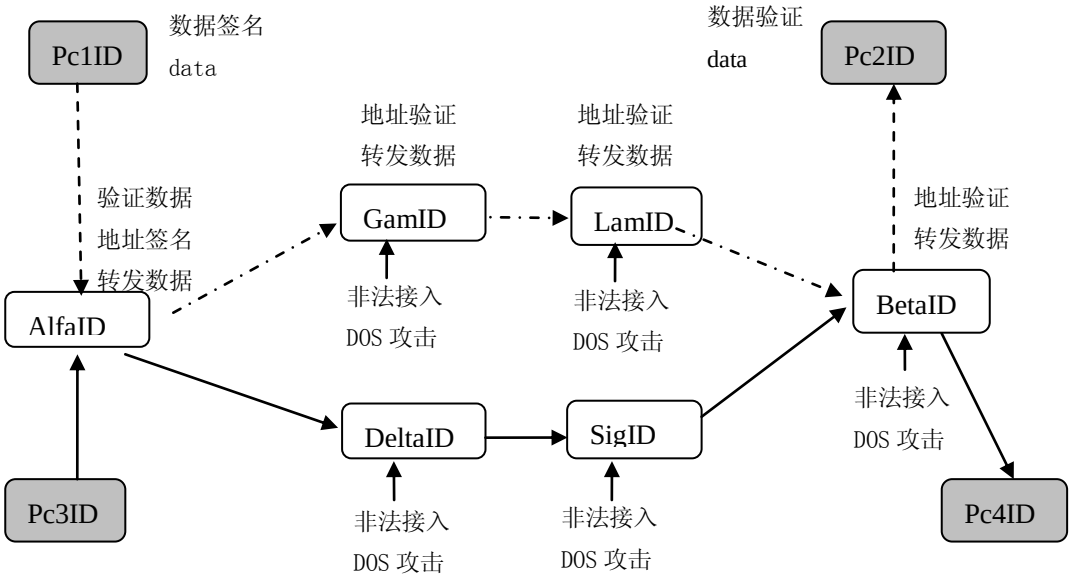


图 2 工作流图

出发路由器的 IP 包通过多个转接路由器，最后到达目的路由器，在中间转接路由器中很容易发生非法接入。从上面路由器的工作原理中可看出，以往的路由器只注重下一跳的路由，并不关心本数据包从何而来。因此如果不解决出发地址的验证，就无法克服非法接入。

有些人尝试能否用加密的方法解决非法接入问题，但在公钥体制条件下，这是徒劳的。比如 Beta 是接受方，而它的公钥是公开的，任何人都可以给 Beta 加密，因此 Beta 仍然无从知晓发方是谁。

为了实现可信连接,路由器 必须满足以下四个条件：

1）原发 IP 地址必须给出发送地址证明，可由任何一地都能验证；

2）所有路径路由器均对原发地址进行验证，如不符，拒绝转发；

3）能防止非法接入、抵抗 DOS 攻击。

4）路由器内部计算环境是可信的。

3 IPv9 连接环境

3.1 连接策略

路径 1（全部采用 IPV9 协议和 CPK-card）：

1） Pc1ID 用 pc1 对 data 签名，将签名数据交付路由器 AlfaID。

2） AlfaID 用 alfa 对 time 签名,转给下一个路由器，下一个路由器则验证原发地址签名，如果验证通过，则将 data 转发给下一路由器。

3）GamID、LamID、BetaID 等路由操作方式同上。

4）BetaID 路由将数据 data 转送至接收用户 Pc2ID。

路径 2（客户端采用 IPV9 协议，但不使用 CPK-card）：

1） Pc3ID 不使用 CPK-card 但通过 PT 转换成 IPV9 协议经由路由 AlfaID 发送数据给 Pc4ID。

2） AlfaID 路由获取数据包源地址作为公钥，并验证来源的正确性，发现不合法地址丢弃数据。

路径 3（客户端不采用 IPV9 协议，且不使用 CPK-card）：

1）Pc3ID 不使用 CPK-card 并采用 IPV4/IPV6 协议经由路由 AlfaID 发送数据给 Pc4ID。

2） 经过 DeltaID 和 SigID 路由到达 BetaID 路由并转发数据给 PC4ID。

路径 4（客户端采用 IPV9 协议，且使用 CPK-card，但中间 V9 路由不使用 CPK-card）：

1） Pc1ID 使用本机地址作为公钥进行签名，经由路由 AlfaID 发送数据给 Pc2ID。

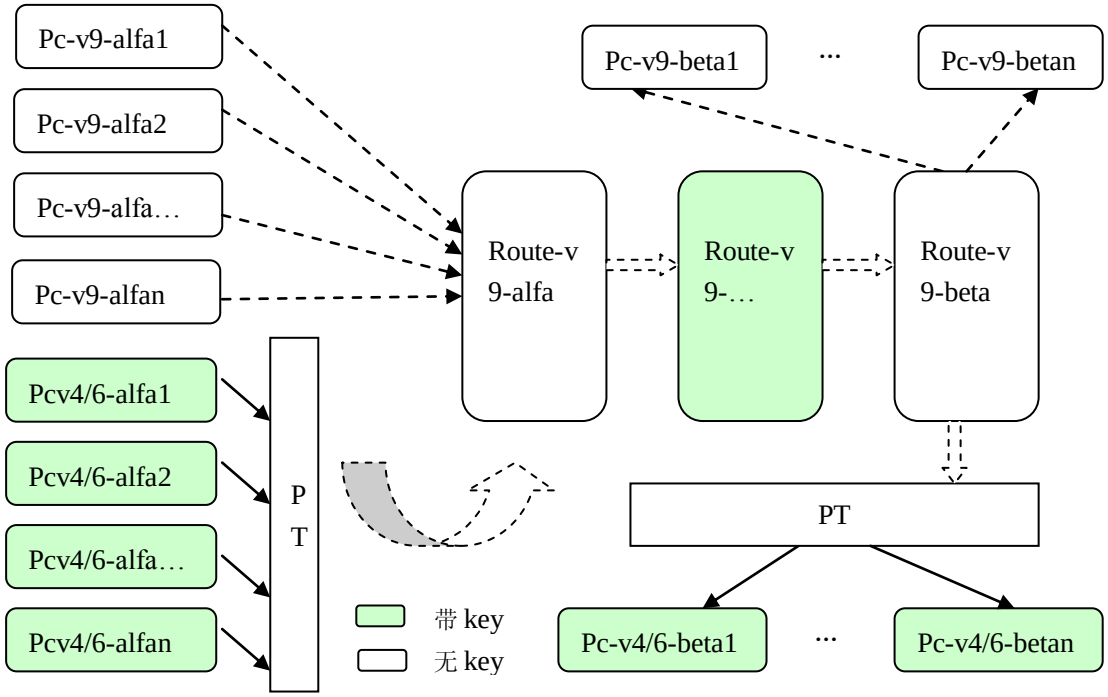
2） AlfaID 路由获取数据包源地址作为公钥，并验证来源的正确性，如不合法地址则丢弃数据。来源地址验证正确后，去除原先签名后再使用本机地址作为公钥签名。签名之后，进行正常的路由数据转发。

3）GamID 路由没有使用 CPK-card，获取数据包源地址作为公钥，并验证来源的正确性，如不合法地址则丢弃数据，进行正常的路由数据转发。

4）LamID、BetaID 等路由操作方式同上。

5）BetaID 路由将数据转发至目的地 Pc2ID

3.2 与 V4/V6 兼容



4 IPv9 鉴别功能

4 .1 CPK-Card

CPK 是基于公钥的密码体制，将任何实体的标识直接作为公钥，私钥则以 ID-card 形式分发。下面以 PC1, ALFA(大写) 等分别表示各自的公钥，pc1, alfa (小写)等分别表示各自的私钥。如果在任意路由器上插入定义为 AlfaID 的 CPK-card，那么这个路由器就变为标识为 AlfaID 的路由器。同理，任何路由器插入定义为 BetaID 的 CPK-card, 该路由器就变为标识为 BetaID 的路由器。

路由器配置 CPK-card, 使其具有数字签名和密钥交换功能，CPK-card 的内容如下：设路由器的 IP 地址为 alfa（Alfa 可能是中国.北京.海淀.北京大学等实名，经统一译名后变为机器可执行的代码）。

Counter ID-card

1	Z1:验证参数	16B	$E_{PWD}(R_1)=Z_1$

2	Z2:验证参数	16B	$E_{R1}(R_1) \oplus R_1=Z_2$
3	标识定义	25B	alfa
5	私钥 1	32B	$E_{R1}(csk_1)=Y_1$
6	私钥 2	32B	$E_{R1}(csk_2)=Y_2$
10	发放单位	25B	KMC
11	发放单位签名	48B	SIG_{kmc} （MAC）

4.2 原发地址鉴别

假设原发地为 AlfaID, 下一路由器为 GammaID, AlfaID 发出数据 data，

Mas1 AlfaID→GammaID: { Alfa, sign1， Beta, time data ,checksum}

其中 AlfaID 原发地址，sign1 是对原发地址的签名，即 sign1= $SIG_{alfa}(time)$, BetaID 是目的地址，SIG 是签名函数，alfa 是签名私钥，由 CPK-card 提供。其中 data 是数据，来自应用层，data 也许是明文，也可能是密文。路由器的任务是将 data 传送给下一路由器。

GammaID 验证原发地的签名： $SIG_{ALFA}^{-1}(time) = sign1'$,

其中 SIG^{-1} 是验证函数, ALFA 是公钥。如果 sign1=sign1'，则允许本次连接，转发 Msg1, 并审计。以对照时间的方式识别重放攻击。

5 IPv9 加密功能

数据 data 的结构定义如下：Data= { Pc1ID, Pc2ID, data, mac}，其中 Pc1ID 发信方，Pc2ID 是收信方。

当数据为明文时，Data={ Pc1ID, Pc2ID, clear-text, mac}

当数据为密文时，Data= { Pc1ID, Pc2ID,, coded-key, coded-data， mac}

如果加脱密功能是由路由器提供的，设 Alfa 加密，Beta 脱密，那么数据加密只能以非在线方式进行。

如果路由器承担加脱密功能，而本次数据 data 是加密数据，则需要解释 coded-key 和 coded-data，并执行系列步骤：

1) 产生随机数 R, AlfaID 计算密钥; key=R × (G); 其中 G 是椭圆曲线的基点;key 将用于数据的加密;

2) 计算发送用密钥：R (BETA) =coded-key, 其中 BETA 是 BetaID 的公钥. 将 coded-key 发送给 BetaID.

3) 对数据加密：E_{key} (data) =cipher-text;

将密文 cipher=text 和 coded-key 发送给 BetaID.

BetaID 接到 AlfaID 的信号便自动进入脱密过程。

1) BetaID 计算私钥的逆： $beta^{-1}$

2) BetaID 计算会话密钥： $beta^{-1}$(coded-key) = key

3) 数据脱密：D_{key}(cipher-text)= data；

6 IPv9 包头格式

新的功能的增加要求制定新的 IP 包头格式，包头中至少包括出发地址，出发地址鉴别码，目的地址, 数据，校验和。数据加密只影响数据格式，不影响 IP 包头格式。

版本	类别	流标签	有效负载长度	下一个头	跳极限
源地址					
目的地址					
time					
鉴别码(签名) 40BYTE					

7 IPv9 可信计算

为了保证路由器运行的可信性，路由器中的所有执行代码，必须通过厂家认证（一级认证），即出场时由厂家对所有执行代码签名。每一台路由器均有鉴别功能（由 CPK-card 提供）。

7.1 软件代码的证明

厂家具有 CPK-card，可对路由器中的所有系统软件进行厂家(manufacturer)签名。执行软件分为软件标识（codeID）和软件本体(codeBD)，厂家对此分别签名：

$SIG_{manufacturer}$ (codeID)=sign1

$SIG_{manufacturer}$ (codeBD)＝sign2

其中，SIG 是签名函数，manufacturer 是厂家的私钥，codeID 是执行代码名，codeBD 是执行代码本体的 HASH 值。路由器中的任何一个执行代码均具有自身的证明码 sign1 和 sign2。

7.2 软件代码的鉴别

路由器插入 CPK-card，使其具有 CPK 认证功能。路由器的验证方法可由两种：一种是当开机时统一验证，没有通过验证的代码统一删除，保证路由器的系统恢复到原始状态；另一种是当调用软件代码时，先行验证后执行。

对 sign1 和 sign2 分别验证：

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

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

其中 MANUFACTURER 是厂家的公钥，如果 sign1=sign1'和 sign2=sign2'，则允许执行，否则拒绝执行。以此保证在本路由器中执行的代码均为厂家认证的代码，除此以外的代码一律不执行，免受病毒、木马的攻击。

8 结论

TCP/IP 协议不能保证可信连接，因此必须加以改造。本文在以地理位置编址和寻址的基础上，提出了可信连接的三个关键技术：采用地址能够鉴别的机制，防止非法连接；采用随机的问答机制，防止重放攻击；软件代码能够鉴别的机制，防止病毒、木马的侵扰。

以上设计方法，完全适用于物理层的可信连接。物理层有两种：一种是信息网络七层协议中定义的物理层，支持信息网络的平台是应用程序接口(API)。第二种是电信网络中定义的物理层电，支持电信网络的平台是信参考点（TRP）。在信息网络中，如果网络层能够保证传输的可信性，物理层的安全可以由网络层替代，无需再作物理层的工作。但是电信网络中的物理层，如果不作改造，就无法实现可信连接，无法防止非法接入。其改造的方法与路由器完全相同。

附录：编码格式

码段0	1	2	3	4	5	6	7
头字段	地域码		管理主体码	厂商代码	商品代码	单品代码	
	国家和地区码	行政区域码				年代轮换码	单件代码
2位	4位	6位	4位	14位	20位	8位	199位
		362300	3211	12345678912345	12345678912345678912	20090317	32564328

采用行标《商务领域射频识别标签数据格式》

企业产品编码数据格式：

1. 企业产品的基本数据格式为：

12345678912345-12345678912345678912-20090317-32564328

2. 当管理部门间进行数据交换时，企业产品数据格式为：

3221-12345678912345-12345678912345678912-20090317-32564328

3. 当地区及管理部门间数据交换时，企业产品数据格式为：

362300-3221-12345678912345-12345678912345678912-20090317-32564328

4. 当国家间数据交换时：

4.1 与ITU-T E164数据体系交换时，数据格式为：

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

4.2 与ISO的对象标识符数据体系交换时，数据格式为：

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

4.3 与国际标准化组织和国际电联联合体ISO-ITU-T的对象标识符数据体系交换时，数据格式为：

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

企业产品ipv9地址格式为：

1. 企业产品的基本ipv9地址格式为：

12345678912345]12345678912345678912]20090317]32564328

2. 当管理部门间进行数据交换时，企业产品ipv9地址格式为：

3221]12345678912345]12345678912345678912]20090317]32564328

3. 当地区及管理部门间数据交换时，企业产品ipv9地址格式为：

362300]3221]12345678912345]12345678912345678912]20090317]32564328

4. 当国家间ipv9地址交换时：

4.1 与ITU-T E164数据体系交换时，数据格式为：

00]8600]362300]3221]12345678912345]123456789123456789 12]20090317]32564328

4.2 与ISO的对象标识符数据体系交换时，ipv9地址格式为：

01]8600]362300]3221]12345678912345]123456789123456789 12]20090317]32564328

4.3 与国际标准化组织和国际电联联合体ISO-ITU-T的对象标识符ipv9地址体系交换时，ipv9地址格式为：

02]8600]362300]3221]12345678912345]123456789123456789 12]20090317]32564328