(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 394 107**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.11.2007 E 07291326 (2)**

(97) Fecha y número de publicación de la solicitud europea: **06.05.2009 EP 2056563**

(54) Título: **Red entre pares**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.01.2013

(73) Titular/es:

ALCATEL LUCENT (100.0%)
3, AVENUE OCTAVE GRÉARD
75007 PARIS, FR

(72) Inventor/es:

PIERER, MARCEL;
HERTLE, ANDREAS y
TOMSU, MARCO

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Red entre pares

Antecedentes de la invención

La invención se refiere a una red entre pares que comprende pares comunes que proporcionan la funcionalidad de la red. Una red entre pares se basa la potencia de computación, ancho de banda y otros recursos, estando distribuidos dichos recursos a través de muchos terminales y pares. Los pares son miembros iguales, de este modo no existe ninguna arquitectura de cliente y servidor en una red entre pares. Los pares están organizados en una red llamada de capa superpuesta, es decir los pares mantienen un conjunto de enlaces con todos los otros pares en la formación de tablas de encaminamiento/dedos. Las redes entre pares estructuradas como CHORD tienen una estructura definida, es decir sus encaminamientos y búsquedas están bien definidas. El protocolo de la red CHORD crea una topología de red de capa superpuesta basada en las Tablas Hash Distribuidas. Una red entre pares es escalable con el aumento del número de pares por lo que la gestión de procedimientos de estabilización definidos gestionan la rápida conexión o desconexión de pares. Las redes entre pares se usan para la realización de Voz sobre IP y soluciones multimedia debido a su bajo coste, auto-configuración, robustez y escalabilidad. Las redes abiertas, normalizadas, estructuradas y auto-organizadas entre pares forman la base de los sistemas de telecomunicaciones públicos, los servicios de colaboración/comunidad sobre Internet, la conferencia de voz/multimedia, la mensajería instantánea, las aplicaciones de pulsar para hablar, compartiendo la información / ficheros para transportistas y empresas.

Estas redes entre pares proporcionadas con una estructura centralizada mínima tiene aún varios problemas de seguridad sin resolver. Las arquitecturas de las redes entre pares de hoy en día o están clasificadas como restringidas o usan el mecanismo de reputación para establecer la seguridad y confianza entre pares. En el caso de aplicaciones restringidas el código software está cifrado para impedir abusos con el propósito de crear código malicioso. La arquitectura de red y los protocolos de comunicaciones están retenidos de la circulación general. Los mecanismos de reputación están o basados en el usuario donde los pares califican a los otros pares, o basados en la transacción, donde se calcula el valor de la confianza en base a todas las transacciones que un par ha realizado con otros pares. Dicho mecanismo de seguridad establecido no se puede aplicar a sistemas de telecomunicaciones públicos abiertos normalizados. Las aplicaciones restringidas requieren un sistema cerrado porque la seguridad solo se puede garantizar siempre que los secretos se mantengan secretos. Se ha propuesto y se ha investigado el uso de mecanismos de reputación, pero los hilos de seguridad podrían no estar resueltos. Los sistemas de reputación entre máquinas para un sistema de comunicaciones público tienen que estar basados en el comportamiento de transacciones y mensajes de los pares, no en el comportamiento de los usuarios.

El mecanismo de auto-organización implementado en la red entre pares crea una topología robusta y asegura la consistencia de los datos almacenados. El uso de un mecanismo de seguridad inteligente protegerá a los pares, es decir, los participantes en la red, la topología de red y los datos almacenados frente a pares maliciosos y la circulación de código malicioso.

El artículo "Introducción de Grupos de Pares Seguros en SP2A" de Amoretti y otros, Procedimientos del Segundo Taller Internacional 2005 sobre Temas de Actualidad en los Sistemas entre Pares (IEEE), desvela una red entre pares que comprende pares de la autoridad de certificación (CA) para la emisión de certificados firmados para los pares. Las Autoridades de Certificación Adicionales, llamadas CA externas, que no son parte de la red, también pueden estar presentes, proporcionando certificación fuera de línea para pares CA y posiblemente para pares.

El artículo "Selección del Super-modo Escalable en las Redes de Capa Superpuesta entre Pares" de Virginia Lo y otros, Procedimientos del Segundo Taller Internacional 2005 sobre Temas de Actualidad en los Sistemas entre Pares (IEEE), describe la optimización de la distribución de super-nodos en una red de capa superpuesta. Los super-nodos pueden mantener un certificado de seguridad de una autoridad central.

El artículo "Seguridad del Sistema de Gestión de la Red de Madeira" de R. Marin y otros en: Software, Telecomunicaciones y Redes de Ordenadores, Softcom 2007, IEEE desvela una autoridad de certificación distribuida usando los elementos del sistema de Gestión Distribuida de Madeira, MDM también denominados como dCA, Los dCA son capaces de detectar intentos de ataques y revocar los certificados de los posibles pares maliciosos.

El documento EP 1 282 289 A1 desvela el uso de relaciones de confianza en las redes descentralizadas, incluyendo las redes entre pares. Las relaciones de confianza pueden tener múltiples componentes o factores, incluyendo la confianza de los nodos, etc.

Objeto de la invención

Por lo tanto, un objeto de la invención es proporcionar un mecanismo de seguridad para un sistema de telecomunicaciones público abierto y normalizado.

Breve descripción de la invención

Dicho objeto se consigue, de acuerdo con la invención, con una red entre pares, que tiene las características de la reivindicación 1. Añadiendo el menos un par policía a la red entre pares, dicho al menos un par policía proporciona la seguridad dentro de la red y está certificado por una autoridad de certificación central que gestiona la certificación y posicionamiento de los pares.

El al menos un par policía funciona como un brazo extendido del sistema de autorización y proporciona / o soporta la seguridad en la red entre pares. La autoridad de certificación central gestiona los pares policía dentro de la red. Pero los pares policía serán los suficientemente inteligentes para operar de forma independiente y en cooperación con otros pares policía. De este modo, cuando se tiene que comprobar la funcionalidad de un posible par malicioso, el posible par malicioso se puede rodear por una pluralidad de pares policía.

Los pares policía se certifican, crean y se colocan por la unidad central, como la autoridad de certificación. Por lo tanto todos los pares policía se pueden identificar y verificar, ya que todos certificados de los pares policía se firman por la autoridad de certificación central. El número de pares policía se gestiona por la autoridad de certificación central. Los pares policía:

- pueden tomar cualquier posición dentro de la red para cumplir sus tareas,
- cumplen las mismas tareas en un modo invisible dentro de la red como los otros pares (por ejemplo, almacenamiento de datos, redirección de mensajes,),
- se pueden llamar por los otros pares para analizar un problema de red, como ataques de otros pares maliciosos,
- analizan las situaciones e inician las investigaciones para localizar pares maliciosos, si es necesario en cooperación con otros pares policía,
- se interconectan por una red de capa superpuesta adicional para proporcionar la cooperación, el almacenamiento y comunicación de datos segura,
- pueden promulgar la segregación de pares maliciosos de la red, por ejemplo por la retirada de certificados.
- se deberían elegir de una pila de pares con fiabilidad garantizada,
- pueden ser parte de un equipo escalable de representantes que actúan en nombre de la unidad central, por ejemplo para responder a las preguntas de verificación de la certificación,
- pueden ser pares para diversos servicios relevantes de confianza, por ejemplo el arranque de pares y mecanismos transversales NAT (TURN, STUN).

En una realización preferida de la invención, los pares comunican con la autoridad de certificación solo durante el procedimiento de unión de un nuevo par. Solo se involucra a una autoridad de certificación, cuando se tienen que asignar nuevos certificados o expiran certificados existentes. Este enfoque llamado híbrido reduce la necesidad de la autoridad de certificación y evita el impacto de la autoridad de certificación central sobre la escalabilidad de la red. Para asegurar la autenticación y certificación de todos los pares, dentro de la red, se propone una estructura de autenticación centralizada.

En cualquier caso, los propios pares policía se tiene que certificar y asignar por una autoridad de certificación central, como el sistema de autorización híbrido propuesto. Esto es necesario para evitar que los pares maliciosos imiten a los pares policía, lo cual es posible en un sistema de telecomunicaciones público, con el requisito específico de protocolos abiertos y normalizados. El sistema de autorización híbrido consiste de una autoridad de certificación localizada en la Internet, para gestionar la certificación y posicionamiento de los pares así como la seguridad proporcionada por una autoridad de policía. Esta autoridad de policía se representa por pares de policía en la red como un brazo extendido de la autoridad de certificación.

La red entre pares tiene una capa superpuesta estructurada, por ejemplo, una estructura de anillo proporcionada por el protocolo de red CHORD. Un desarrollo adicional de la red entre pares inventiva se caracteriza porque el certificado de dicho al menos un par policía contiene la firma común de un par común y además una firma de policía. Esto permite al par policía realizar investigaciones encubiertas. En el caso de que se añadan una pluralidad de pares policía a la red, los pares policía preferentemente están conectados en una red de capa superpuesta adicional.

También se puede aplicar un procedimiento para proporcionar seguridad en tal red entre pares que comprende pares comunes, al menos un par policía que proporciona la seguridad dentro de la red y una autoridad de certificación central que gestiona la certificación y posicionamiento de los pares que tiene tres etapas. Las tres etapas del procedimiento se gestionan y/o realizan por el al menos un par policía. En una primera etapa se comprueba la funcionalidad de posibles pares maliciosos. Si la malignidad del par malicioso se confirma, una autoridad de certificación declara en una segunda etapa el certificado del par malicioso como inválido y se invita al par malicioso a desconectarse de la red. Si falla la desconexión del par malicioso, sigue una tercera etapa, en la que todos los otros pares cierran sus conexiones con el par malicioso. En la primera etapa, el posible par malicioso se rodea por una pluralidad de pares policía.

Se pueden extraer ventajas adicionales de la invención a partir de la descripción y los dibujos adjuntos. Las características mencionadas anteriormente y a continuación se pueden usar de acuerdo con la invención bien individualmente o colectivamente en cualquier combinación. Las realizaciones mencionadas no se entenderán como

una enumeración exhaustiva sino que más bien tienen carácter de ejemplo para la descripción de la invención.

Dibujos

La red entre pares inventiva se muestra en los dibujos. Estos muestran:

Fig. 1 una red entre pares ejemplar durante la unión de un nuevo par;

Fig. 2 la red entre pares después de la unión de un nuevo par;

Fig. 3 la red entre pares y una red adicional de capa superpuesta de pares policía;

Fig. 4 las redes de acuerdo con la Fig. 3 que ilustran la funcionalidad de los pares policías;

Fig. 5 la red entre pares durante la comprobación de un posible par malicioso; y

Fig. 6a, 6b la red entre pares realizando la segregación de un par malicioso.

La **Fig. 1** muestra una red entre pares 100 que comprende los pares 0, 4, 10, 15, 20, 23, 28 localizados en posiciones de red dispuestas en una estructura de anillo. La certificación y posicionamiento de los pares 0, 4, 7, 10, 15, 20, 23, 28 se gestiona por una autoridad de certificación 110. Para asegurar la autenticación y certificación de todos los pares 0, 4, 7, 10, 15, 20, 23, 28 dentro de la red 100, se propone una estructura híbrida de autenticación centralizada. La autenticación es necesaria para verificar la identidad de los pares 0, 4, 7, 10, 15, 20, 23, 28 para construir la confianza entre los pares 0, 4, 7, 10, 15, 20, 23, 28. Se propone el enfoque híbrido para minimizar el impacto sobre la escalabilidad del sistema. Esto significa que la autoridad de certificación central 110 solo se solicita si se tienen que asignar nuevos certificados a los pares 0, 4, 7, 10, 15, 20, 23, 28. Esto es necesario si los nuevos pares 7 conectan con el sistema o los pares existentes 0, 4, 10, 15, 20, 23, 28 necesitan nuevos certificados. Un certificado compromete el tiempo de vida de los certificados, la posición de los pares, la Clave Pública de la autoridad de certificación110 y una firma para verificar el certificado. La posición de los pares 0, 4, 10, 15, 20, 23, 28 dentro de la red 100 se calcula a partir de la autoridad de certificación 110 para equilibrar la red 100 y para impedir que pares maliciosos elijan posiciones ventajosas. La firma del certificado se firma con la clave privada de la autoridad de certificación 110 y se puede verificar usando la clave pública de la autoridad de certificación 110, que conoce cada par 0, 4, 7, 10, 15, 20, 23, 28 (Infraestructura de Clave Pública). Por lo tanto los certificados se pueden verificar sin consultar de nuevo a la autoridad de certificación 110. La Fig. 1 muestra cómo el par 7 quiere unirse a la red 100 y está solicitando un certificado de la autoridad de certificación 110 (flecha 120). El par 10 verifica el certificado y permite al par 7 unirse a la red 100. Como los nuevos pares necesitan un punto fiable para unirse a la red, los pares policía pueden proporcionar servicios relevantes de confianza.

Como se ilustra en la **Fig. 2**, la red entre pares 100 contiene pares policía 10, 23 (círculo relleno) que son pares iguales y que realizan las mismas tareas que los pares comunes 0, 4, 7, 15, 20, 28. La autoridad de certificación 110 controla los pares policía 10, 23 (flechas 130a, 130b), es decir, asigna certificados específicos que contienen una firma de policía así como una firma común y gestiona la posición de los pares policía 10, 23. Por este medio, ningún otro par puede imitar a un par policía y se usa la firma común por los pares policía 10, 23 para investigar en secreto. Los pares 0, 4, 7, 15, 20, 28 obtienen información acerca de los pares policía más próximos 10, 23 durante el procedimiento de unión, en el caso ilustrado el nuevo par 7 está informado acerca del par policía 10.

En la **Fig. 3** se representa que los pares policía están organizados en una red de capa superpuesta adicional propia 140. Los pares policía 4, 23 de la red entre pares 100 toma las posiciones de la red 9 y 54 en la red de capa superpuesta adicional 140. La posición de los pares dentro de la red pública 100 y la red de autoridad policial, es decir la red de capa superpuesta adicional 140 no son iguales, ya que los pares policía 4, 23 pueden cambiar su posición dentro de la red pública 100, por ejemplo para las investigaciones. La red de capa superpuesta adicional 140, la red llamada de la autoridad policial, sirve para el almacenamiento de información acerca de los pares maliciosos y para una mejor comunicación y cooperación entre los pares policía. De este modo, todos los pares policía 4, 23 pueden usar la base de datos distribuida para almacenar la información acerca de los pares maliciosos, para la comunicación y cooperación aparte de la red pública 100.

La **Fig. 4** muestra la funcionalidad de la red entre pares 100 y la red de capa superpuesta adicional 140. Un par común 15 puede reportar un crimen definido al par policía 23 (flecha 150) que publica el crimen y hace una búsqueda de más información dentro de la red de capa superpuesta adicional 140 (flechas 160a, 160b). Durante el procedimiento de unión de los pares comunes 0, 4, 7, 15, 20, 28, la autoridad de certificación informa a los pares 0, 4, 7, 15, 20, 28 acerca de los pares policía más próximos 4, 23. Por lo tanto, cada uno de los pares 0, 4, 7, 15, 20, 28 pueden informar a un par policía 4, 23 en el caso de ataques o situaciones inusuales. Como se muestra en la Fig. 4, el par 15 informa al par policía 23. El par policía 23 que recibe tal mensaje puede usar a continuación la red de autoridad policial para recoger más información y cooperar con los otros pares policías a encontrar una solución.

La **Fig. 5** ilustra un procedimiento de investigación proporcionado por los dos pares policía 4, 9, por el que el par policía 9 se une después del posible par malicioso 7 (cuadrado). Un procedimiento de investigación comprende pruebas con los procedimientos normalizados similares a redirigir los mensajes, búsqueda, publicación y

recuperación de datos así como cualesquiera servicios proporcionados. Los pares policía 4 y 9 analizan la funcionalidad del posible par malicioso 7 (flechas 170a, 170b, 180). Para analizar una situación y localizar los pares maliciosos 7, los pares policía 4, 9, 23 pueden cambiar sus posiciones dentro de la red 100 y cooperar con otros pares policía 4, 9, 23. En la Fig. 5 el posible par malicioso 7 se rodea por los pares policía 4, 9. Los pares policía 4, 9 comprueban la funcionalidad del par 7, como redirigiendo los mensajes, almacenando y recuperando valores así como cualesquiera servicios proporcionados.

El procedimiento para proporcionar la seguridad en la red entre pares 100 y la segregación del par malicioso 7, respectivamente, se ilustra en las **Fig. 6a, 6b**. El par policía 4 informa a la autoridad de certificación 110 para declarar el certificado del par malicioso 7 como inválido (flecha 190) y publica la información acerca del certificado invalidado de modo que los otros pares pueden reaccionar (flecha 200). A continuación el par policía 4 solicita al par malicioso 7 que se desconecte de la red 100 (flecha 210). Los pares comunes sucesivos y anteriores 28, 0, 10, 15 mantendrán aún las conexiones vivas (dedos) 230a, 230b con el par malicioso 7. En la siguiente etapa, los pares policía 23, 4 informan a los pares comunes sucesivos y anteriores 28, 0, 10, 15 para cerrar sus conexiones (dedos) 230a, 230b con el par malicioso 7 (flechas 240a, 240b, 240c, 240d). Como resultado, el par malicioso 7 se desconecta, es decir, se segrega de la red 100. El par 10 es ahora el siguiente par después del par 4, de este modo el par 7 se segrega de la red.

REIVINDICACIONES

1. Una red entre pares (100), que comprende:

pares comunes (0, 7, 10, 15, 20, 28) y una pluralidad de pares policía (4, 9, 23) en una capa superpuesta estructurada de la red (100), proporcionando el, al menos un par policía (4, 9, 23) la seguridad dentro de la red (100) comprobando la funcionalidad de los posibles pares maliciosos (7), y
una autoridad de certificación central (110) para gestionar la certificación de los pares (0, 4, 7, 9, 10, 15, 20, 23, 28) en la capa superpuesta estructurada de la red (100),

caracterizada porque
la autoridad central de certificación (110) está adaptada además para gestionar el posicionamiento de los pares en la capa superpuesta estructurada de la red (100), y **porque** la red entre pares (100) está adaptada para rodear a un posible par malicioso (7) por una pluralidad de pares policía (4, 9, 23).

2. La red entre pares de acuerdo con la reivindicación 1 **caracterizada porque** los pares (0, 4, 7, 9, 10, 15, 20, 23, 28) están adaptados para comunicar con la autoridad de certificación (110) solo durante el procedimiento de unión de un nuevo par (7).

3. La red entre pares de acuerdo con la reivindicación 1 **caracterizada porque** los certificados de dicha pluralidad de pares policía (4, 9, 23) contienen la firma común de un par común (0, 7, 10, 15, 20, 28) y además una firma de policía.

4. La red entre pares de acuerdo con la reivindicación 1 **caracterizada porque** se interconecta una pluralidad de pares policía (4, 9, 23) en una red de capa superpuesta adicional (140).

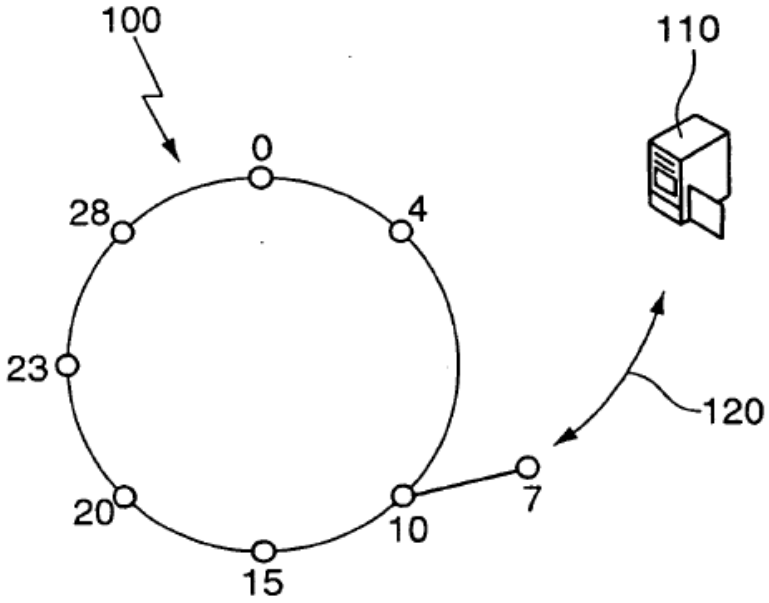
100
110
0
4
28
23
120
7
20
10
15

Fig. 1

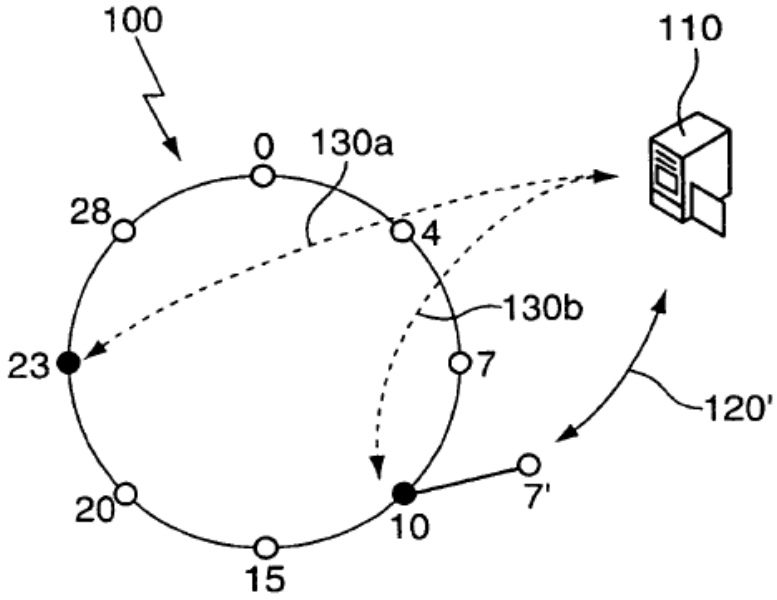
100
110
0
130a
28
4
130b
23
7
120'
7'
20
10
15

Fig. 2

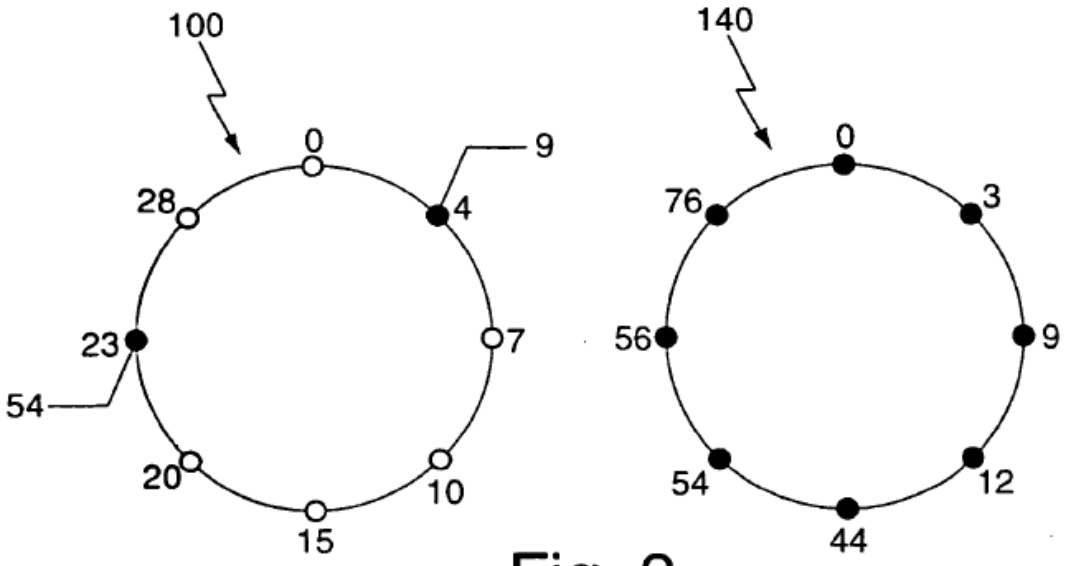
100
0
9
28
4
23
7
54
20
10
15
140
0
76
3
56
9
54
12
44

Fig. 3

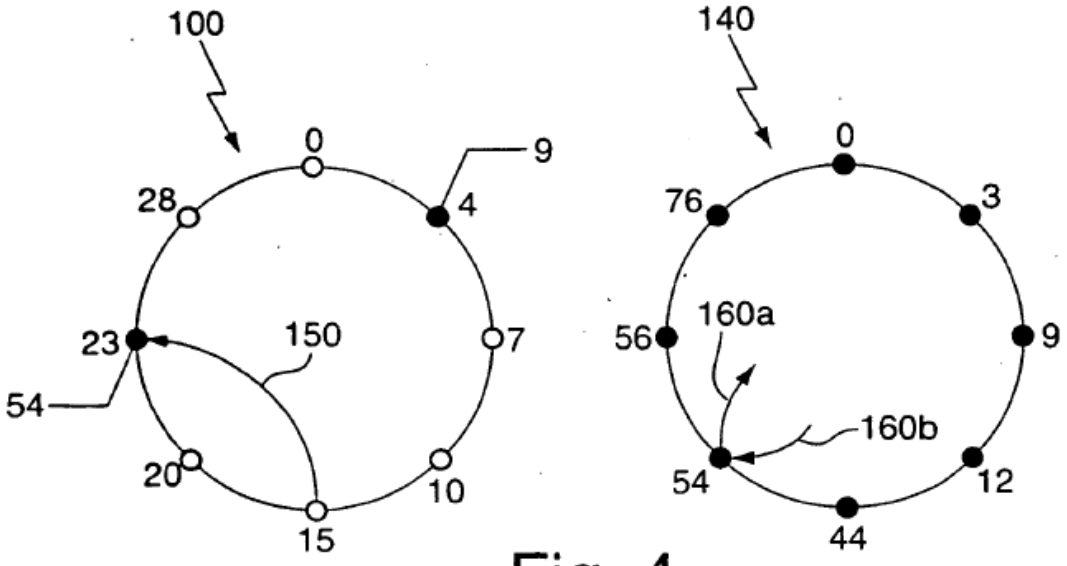
100
0
9
28
4
23
150
7
54
20
10
15
140
0
76
3
160a
56
9
160b
54
12
44

Fig. 4

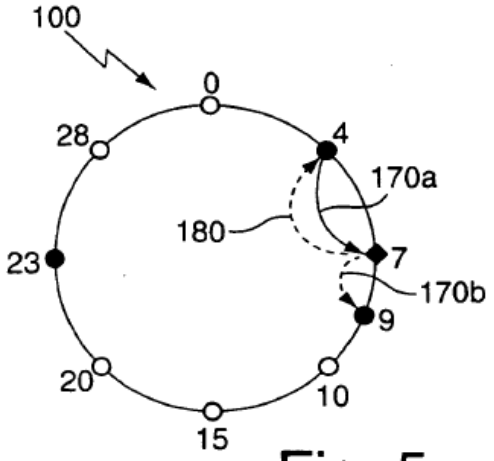

Fig. 5

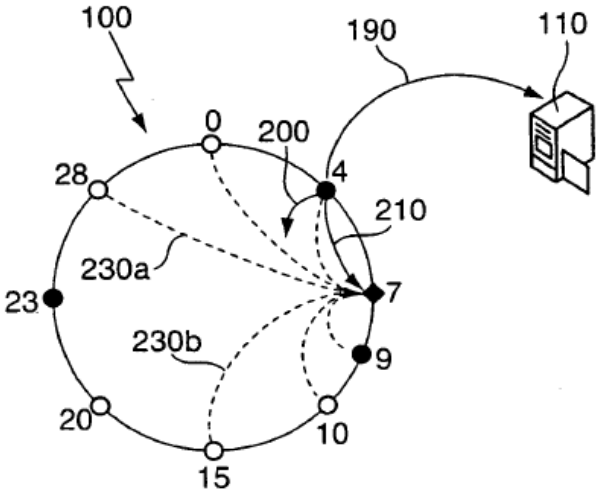

Fig. 6a

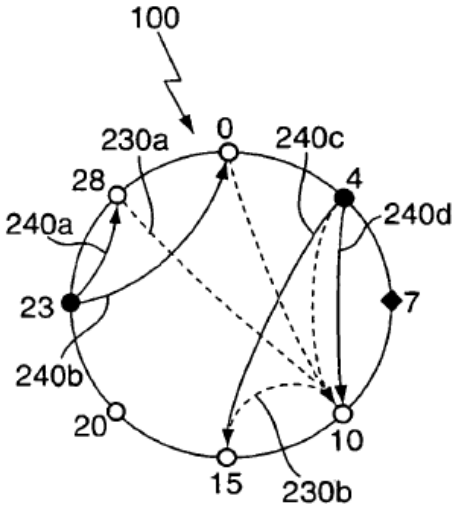

Fig. 6b