(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 604 214**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.01.2009 PCT/GB2009/000136**

(87) Fecha y número de publicación internacional: **23.07.2009 WO09090409**

(96) Fecha de presentación y número de la solicitud europea: **19.01.2009 E 09702595 (1)**

(97) Fecha y número de publicación de la concesión europea: **14.09.2016 EP 2235903**

(54) Título: **Sistema de comunicaciones seguras**

(30) Prioridad:

17.01.2008 GB 0800838

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.03.2017

(73) Titular/es:

AIRBUS DEFENCE AND SPACE LIMITED (100.0%)
Gunnels Wood Road, Stevenage
Hertfordshire SG1 2AS, GB

(72) Inventor/es:

BENTALL, MARK

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistema de comunicaciones seguras

La invención se refiere a sistemas de comunicaciones seguras.

El uso de criptografía para proporcionar comunicaciones seguras entre dos entidades a través de una red es bien conocido en el estado de la técnica. La figura 1 es un diagrama de bloques que muestra un sistema de comunicaciones típico. El sistema de la figura 1 indicado globalmente mediante la referencia numérica 1 comprende una primera entidad 2, una segunda entidad 4 y una tercera entidad 6. Las entidades se comunican a través de una red 8. La red puede ser de muchos tipos tal como una red empresarial interna o Internet. En el sistema 1 los datos enviados de una de dichas entidades a otra se envían a través de la red 8 de forma cifrada. Los datos provenientes de la primera entidad 2 los cifra un primer dispositivo de cifrado 10 y los datos enviados a la primera entidad 2 a través de la red 8 los descifra el primer dispositivo de cifrado 10. Análogamente los datos provenientes de la segunda entidad 4 los cifra un segundo dispositivo de cifrado 12 y los datos provenientes de la tercera entidad 6 los cifra un tercer dispositivo de cifrado 14. Además los datos enviados a la segunda entidad 4 a través de la red 8 los descifra el segundo dispositivo de cifrado 12 y los datos enviados a la tercera entidad 6 los descifra el tercer dispositivo de cifrado 14.

Por lo tanto, la red 8 transmite datos cifrados entre las entidades 2, 4 y 6. Análogamente si el procedimiento de cifrado es seguro los mensajes intercambiados entre los usuarios del sistema 1 no los pueden descifrar los terceros.

La figura 2 muestra un sistema, indicado globalmente con la referencia numérica 20, que es una variante del sistema 1.

El sistema 20 comprende una primera entidad 22, una segunda entidad 24, una tercera entidad 26 y una cuarta entidad 28 conectadas a una red 30 a través de dispositivos de cifrado 32, 34, 36 y 38 respectivamente.

En el sistema 20 las entidades están dispuestas en grupos y sólo se pueden comunicar con otras entidades del mismo grupo. El primer grupo comprende la primera y tercera entidades 22, 26 y el segundo grupo comprende la segunda y cuarta entidades 24, 28.

El sistema 20 se puede usar para proporcionar un sistema de comunicaciones de datos seguras en el que diferentes entidades tengan distintas clasificaciones de seguridad y sólo se pueden comunicar con otras entidades que tengan la misma clasificación de seguridad. Por tanto, unas entidades pueden, por ejemplo, estar clasificadas como de baja sensibilidad, sensibles o de alta sensibilidad. Las entidades clasificadas como de baja sensibilidad se pueden comunicar con otras entidades clasificadas como de baja sensibilidad pero no se pueden comunicar con otras entidades. Análogamente las entidades clasificadas como sensibles se pueden comunicar solamente con otras entidades clasificadas como sensibles y las entidades clasificadas como altamente sensibles sólo se pueden comunicar con otras entidades clasificadas como altamente sensibles.

Puesto que todos los datos transmitidos a través de la red 30 están cifrados la red es segura si el cifrado es seguro.

El inventor ha observado que la arquitectura de los sistemas del estado de la técnica anterior, como los sistemas 1 y 20 descritos anteriormente, impiden que las entidades obtengan información relativa a la propia red. La información que las entidades pueden querer obtener comprende, no limitativamente, los costes de uso de la red o de una ruta particular a través de la red (sea en términos de coste económico, esfuerzo u otra métrica de enrutamiento) y la calidad de servicio ofrecida por la red o la ruta; a estos datos se les hace referencia en general como datos de métricas de red o métricas de red. Por ejemplo, si la red hace uso de comunicaciones por satélite caras, entonces una entidad puede decidir no hacer uso de esa red para una comunicación particular. Los sistemas 1 y 20 descritos anteriormente ni proporcionan un mecanismo para habilitar datos de métricas relativos a la red en sí que se transmitan a las entidades.

La solicitud de patente US2005/010766 A1 describe un sistema de seguridad de red multinivel para un dispositivo terminal de cómputo conectado al menos una red de ordenadores. El sistema comprende una unidad de interfaz de red segura incluida en una pila de comunicaciones del dispositivo de cómputo que opera con un protocolo de comunicaciones de capa de usuario. La unidad se comunica con otras unidades de la red similares estableciendo una asociación, creando así un perímetro de seguridad global para las comunicaciones extremo a extremo.

La solicitud de patente EP1830517 A1 describe un procedimiento para la transferencia de información orientada a paquetes entre una unidad de comunicaciones central y varias unidades de comunicación periféricas a través de una red de comunicaciones. Los paquetes de datos transferidos por la red comprenden un campo de cabecera y un campo de datos. Al menos una parte de la información de la cabecera incluida en el campo de cabecera se cifra en el lado del emisor y se descifra en el lado del receptor. Los paquetes de datos recibidos se procesan basándose en la información de la cabecera descifrada.

La solicitud de patente US2007/0276958 A1 describe un sistema de cómputo, un procedimiento y un programa de enrutamiento. Se recibe un paquete de mensaje no cifrado. Como resultado se leen los datos del paquete de mensaje para determinar si los datos contienen información sensible. Si los datos contienen información sensible el paquete de mensaje se cifra y a continuación se enruta por una ruta de comunicaciones no seguras. Si los datos no contienen información sensible el paquete de mensaje se enruta por una ruta de comunicaciones no seguras sin cifrar el paquete de mensaje. Los datos se pueden leer para determinar si contienen información sensible determinando un estándar de formato del paquete de mensaje y basándose en el estándar determinar la ubicación de los datos dentro del paquete de mensaje y un tipo de datos correspondiente a la ubicación.

La presente invención pretende resolver al menos algunos de los problemas identificados mencionados.

La presente invención proporciona un sistema de comunicaciones que comprende una primera entidad, un primer dispositivo de cifrado y una red en el que dicho primer dispositivo de cifrado está configurado para descifrar utilizando un primer algoritmo de descifrado los datos enviados desde un primer destino hasta dicha primera entidad a través de dicha red caracterizado por que dicho primer dispositivo de cifrado está configurado para:

(i) transmitir datos de la métrica de la red relativos al menos a una ruta entre dicha primera entidad y dicho primer destino a dicha primera entidad sin aplicar a dichos datos de métrica de la red dicho algoritmo de descifrado pero
(ii) bloquear los datos de métricas de la red que no sean de un conjunto predeterminado de palabras de datos

Hay que entender que el destino puede ser, por ejemplo, una red, un terminal o una aplicación.

La presente invención también proporciona un procedimiento de operación de un sistema de comunicaciones seguras en el que una o más entidades envían datos a una o más entidades del sistema a través de la red y en el que al menos algunos de dichos datos se cifran y se descifran utilizando algoritmos de cifrado y descifrado comprendiendo el procedimiento:

(i) el paso de enviar datos de métrica de la red (habitualmente se dice métricas) desde dicha red a una o más de dichas entidades sin someter dichos datos de métricas de la red a dichos algoritmos de descifrado y
(ii) el paso de bloquear los datos de métricas de la red que no sean de un conjunto predeterminado de palabras de datos

Los datos de métricas de la red describen atributos de la red tales como datos de costes de transmisión de datos o datos de la calidad de servicio. Los datos de métricas de la red podrían evidentemente ser de otros tipos como es bien conocido en el estado de la técnica.

Al transmitir datos de métricas desde la red a una identidad de forma no cifrada las entidades tienen un acceso inmediato a estos datos útiles. Además, no se imponen requisitos de que los datos de métricas de la red se tengan que manipular o en la red o en la entidad en cuestión. La realización de la presente invención supone una transmisión de datos sin cifrar desde la red a las entidades pero no requiere la transmisión de datos no cifrados desde las entidades a la red.

El primer dispositivo de cifrado puede configurarse para cifrar datos enviados por la primera entidad a través de la red utilizando un primer algoritmo de cifrado.

En muchas realizaciones de la invención el primer dispositivo de cifrado está configurado tanto para cifrar datos enviados desde una entidad a la red como para descifrar datos enviados desde dicha red a la entidad. De esta manera se puede conseguir una comunicación bidireccional segura entre entidades. El primer dispositivo de cifrado está configurado para bloquear los datos de métricas de la red que no sean de un conjunto predeterminado de palabras de datos. Dicha realización tiene la ventaja de reducir la exposición de las entidades a datos maliciosos como virus y troyanos que se envíen de la red a la entidad en forma no cifrada.

El sistema de la presente invención puede comprender una segunda entidad y un segundo dispositivo de cifrado en el que el segundo dispositivo de cifrado está configurado para cifrar datos enviados por dicha segunda unidad a través de dicha red utilizando un segundo algoritmo de cifrado y/o descifrar datos enviados a dicha segunda entidad a través de la red utilizando un segundo algoritmo de descifrado. El segundo dispositivo de cifrado puede estar configurado para transmitir datos de métricas de la red a dicha segunda entidad.

El sistema puede comprender una segunda entidad y un segundo dispositivo de cifrado en el que dicho segundo dispositivo de cifrado está configurado para descifrar, utilizando un segundo algoritmo de descifrado, los datos enviados desde un segundo destino a dicha segunda entidad a través de la dicha red. El segundo dispositivo de descifrado puede estar configurado para cifrar datos enviados por dicha segunda entidad a través de dicha red utilizando un segundo algoritmo de cifrado. El segundo dispositivo de cifrado puede estar configurado para transmitir datos de métricas de la red relativos al menos a una ruta entre dicha segunda entidad y dicho segundo destino a una segunda entidad sin aplicar a dichos datos de métricas de red el segundo algoritmo de descifrado.

Como se ha discutido anteriormente haciendo referencia al primer dispositivo de cifrado el segundo dispositivo de cifrado puede estar configurado para bloquear los datos de métricas de la red que no sean de un conjunto predeterminado de palabras de datos.

Puede ser que el primer algoritmo de cifrado y descifrado sean adecuados para comunicaciones de una primera clasificación de seguridad y que los segundos algoritmos de cifrado y descifrado sean adecuados para comunicaciones de una segunda clasificación de seguridad distinta.

El sistema de la presente invención puede incluir además una tercera entidad y un tercer dispositivo de cifrado donde el tercer dispositivo de cifrado esté configurado para cifrar datos enviados por dicha tercera entidad a través de dicha red utilizando un tercer algoritmo de cifrado y/o descifrar los datos enviados a dicha tercera entidad a través de dicha red utilizando un tercer algoritmo de descifrado. El tercer dispositivo de cifrado puede estar configurado para transmitir datos de métricas de la red a dicha tercera entidad. El tercer dispositivo de cifrado puede estar adaptado para bloquear datos de métricas de la red que no sean de un grupo predeterminado de palabras de datos.

El sistema puede comprender una tercera entidad y un tercer dispositivo de cifrado en el que el tercer dispositivo de cifrado esté configurado para descifrar, utilizando un tercer algoritmo de descifrado, los datos enviados desde un tercer destino a dicha tercera entidad a través de dicha red. El tercer dispositivo de cifrado puede estar configurado para cifrar datos enviados por dicha tercera entidad a través de dicha red utilizando un tercer algoritmo de cifrado. El tercer dispositivo de cifrado puede estar adaptado para transmitir datos de métricas de la red relativos al menos a una ruta entre dicha tercera entidad y dicho tercer destino a dicha tercera entidad sin someter dichos datos de métricas de la red a dicho tercer algoritmo de descifrado.

Puede ser que los terceros algoritmos de cifrado y descifrado sean adecuados para las comunicaciones según una clasificación de seguridad distinta a las clasificaciones de seguridad para las que los primeros y/o segundos algoritmos de cifrado y descifrado sean adecuados.

En algunas realizaciones de la presente invención dichos datos de métricas de la red sólo se pueden usar para actualizar una entrada predefinida de una tabla. La presente invención puede evitar que dichos datos de métricas de la red se utilicen para otro propósito distinto al de la actualización de dicha entrada predefinida de dicha tabla.

Las entidades mencionadas anteriormente pueden ser usuarios. Alternativamente algunas o todas las entidades pueden ser grupos de usuarios, organizaciones o redes en sí.

De acuerdo con otro aspecto de la invención se proporciona un sistema de comunicaciones que comprende una primera entidad, un primer dispositivo de cifrado y una red en el que dicho primer dispositivo de cifrado está configurado para cifrar datos enviados por ficha primera entidad a través de dicha red utilizando un primer algoritmo de cifrado y/o descifrar datos enviados a dicha primera entidad a través de dicha red utilizando un primer algoritmo de descifrado, en el que dicho primer dispositivo de cifrado está configurado para transmitir datos de métricas de la red (comúnmente llamados datos de métricas de la red) a dicha primera entidad sin someter dichos primeros datos de métricas de la red a dicho primer algoritmo de descifrado.

Hay que entender que las características descritas haciendo referencia a un aspecto de la invención son igualmente aplicables a otros aspectos de la invención.

Los dispositivos y procedimientos de acuerdo con la invención se describirán a continuación por medio de ejemplos sólo, haciendo referencia a figuras esquemáticas adjuntas en los que:

- la figura 1 es un diagrama de bloques de un primer sistema de comunicaciones seguras de ejemplo
- la figura 2 es un diagrama de bloques de un segundo sistema de comunicaciones seguras de ejemplo
- la figura 3 es un diagrama de bloques de una variante de los sistemas de comunicaciones de las figuras 1 y 2 que muestran un aspecto de la presente invención
- la figura 4 es un diagrama de bloques que ilustra un aspecto de la presente invención

La figura 3 muestra un sistema indicado globalmente mediante la referencia numérica 40 que ilustra el problema resuelto por la presente invención.

El sistema 40 comprende una primera entidad 42, una segunda entidad 44 y una red 46. La primera entidad 42 está conectada a la red a través de un primer dispositivo de cifrado 48; la segunda entidad 44 está conectada a la red a través de un segundo dispositivo de cifrado 50. El sistema también comprende una tercera y cuarta entidades 52 y 54. La primera entidad 42 es capaz de comunicarse con la tercera entidad 52, la tercera entidad 52 es capaz de comunicarse con la cuarta entidad 54 y la cuarta entidad 54 es capaz de comunicarse con la segunda entidad 44. Por tanto, la primera y segunda entidades 42 y 44 son capaces de comunicarse bien a través de la red 46 o a través de la tercera y cuarta entidades 52 y 54.

La tercera y cuarta entidades 52 y 54 pueden ser otra red a la que tienen acceso la primera entidad 42 y la segunda entidad 44.

Asúmase que la primera entidad 42 quiere enviar un mensaje a la segunda entidad 44. El sistema 40 proporciona dos rutas por las que se podría enviar el mensaje, bien a través de la red 46 o a través de las tercera y cuarta entidades 52 y 54. Para decidir qué ruta usar, la primera entidad quiere comparar los datos de las métricas relativos a las dos rutas, de forma bien conocida en el estado de la técnica. Sin embargo dichos datos de métricas de la red 46 no están disponibles para la primera entidad 42.

La figura 4 muestra una parte del sistema de comunicaciones que incluye un aspecto de la presente invención. La figura 4 muestra una red 60 conectada a una entidad 62 a través de un dispositivo de cifrado 64. Al igual que en los sistemas de ejemplo 1 y 20 descritos anteriormente el dispositivo de cifrado se utiliza para cifrar la salida de datos de la entidad 62 hacia la red 60 y se utiliza para descifrar los datos de la red 60 que vayan dirigidos a la entidad 62.

En el uso normal del dispositivo de cifrado 64 los datos cifrados 66 se transmiten de la red 60 a la parte de texto cifrado del dispositivo de cifrado 64. Esos datos se descifran entonces y se proporcionan como datos 67 en el lado de texto claro del dispositivo 64.

Como muestra la figura 4 el dispositivo de cifrado 64 también recibe segundos datos 68, siendo dichos datos, datos de métricas de la red. Los datos de métricas 68 no están cifrados y simplemente se transmiten a través del dispositivo 64 sin descifrarse.

Al permitir que los datos de métricas pasen a través del dispositivo 64 sin descifrado el problema de ofrecer a la entidad acceso a los datos de métricas se resuelve de una forma simple y elegante.

Hay que tener en cuenta que en el sistema 60, si bien se permite que los datos no cifrados pasen de la red 60 a la entidad no se permite el paso de datos no cifrados de la entidad a la red. Los usuarios típicamente están más preocupados por los riesgos potenciales de transmitir datos no cifrados desde una entidad (como un usuario) a la red que al contrario.

El problema potencial de la configuración descrita anteriormente haciendo mención a la figura 4 es que el paso de los datos no cifrados de la red directamente a las entidades supone que las entidades potencialmente sean vulnerables a ataques, por ejemplo, de virus o troyanos. Esta cuestión, sin embargo, se puede solventar con la limitación de que los datos que pueden pasar de la red a la entidad sean de un conjunto predeterminado de palabras de datos. Un cortafuegos puede proporcionar dicha característica de seguridad.

A modo de ejemplo, asúmase que red 60 transmite una métrica de enrutamiento a una entidad haciendo uso de la red. La red tendrá toda la información relativa a la métrica de enrutamiento pero está restringida a definir una métrica mediante un conjunto pequeño de palabras binarias preseleccionadas. Además la palabra elegida solo se puede

utilizar para actualizar una fila particular de una tabla que mantenga la entidad. La tabla es accesible para la entidad cuando decida si usar o no usar la red. De esta manera la entidad tiene acceso a las métricas de enrutamiento pero los riesgos para la seguridad al permitir que datos no cifrados pasen directamente desde la red a la entidad queda reducida a un nivel que la mayoría de los usuarios considerarían aceptable.

REIVINDICACIONES

1. Sistema de comunicaciones (40) que comprende una primera entidad (42), un primer dispositivo de cifrado (48) y una red (46) donde dicho primer dispositivo de cifrado (48) está configurado para descifrar, utilizando un primer algoritmo de descifrado datos (66) enviados desde un primer destino a dicha primera entidad (42) a través de dicha red (46) **caracterizado porque** dicho primer dispositivo de cifrado (48) está configurado para:

(i) transmitir datos de métricas de la red (68) relativos al menos a una ruta entre dicha primera entidad (42) y dicho primer destino a dicha primera entidad (42) sin someter dichos datos de métricas de la red (68) a dicho primer algoritmo de descifrado pero
(ii) bloquear los datos de métricas de la red que no sean de un conjunto predeterminado de palabras datos.

2. Sistema de comunicaciones de acuerdo con la reivindicación 1 donde dicho primer dispositivo de cifrado está configurado para cifrar datos enviados por dicha primera entidad a través de dicha red utilizando un primer algoritmo de cifrado.

3. Sistema de comunicaciones de acuerdo con la reivindicación 1 o 2 donde dicho primer dispositivo de cifrado está configurado para bloquear los datos de métricas de la red que no sean de un conjunto predeterminado de palabras de datos.

4. Sistema de comunicaciones de acuerdo con cualquiera de las reivindicaciones anteriores que comprende además una segunda entidad y un segundo dispositivo de cifrado donde el segundo dispositivo de cifrado está configurado para descifrar utilizando un algoritmo de descifrado los datos enviados desde un segundo destino a dicha segunda entidad a través de dicha red.

5. Sistema de comunicaciones de acuerdo con la reivindicación 4 donde dicho segundo dispositivo de cifrado está configurado para cifrar datos enviados por ficha segunda entidad a través de dicha red utilizando un segundo algoritmo de cifrado.

6. Sistema de comunicaciones de acuerdo con la reivindicación 4 o 5 donde dicho segundo dispositivo de cifrado está configurado para transmitir datos de métricas de la red relativos al menos una ruta entre dicha segunda entidad y dicho segundo destino a dicha segunda entidad sin someter los datos de métricas de la red a dicho segundo algoritmo de cifrado.

7. Sistema de comunicaciones de acuerdo con cualquiera de las reivindicaciones 4 a 6 donde dicho segundo dispositivo de cifrado está adaptado para bloquear los datos de métricas de la red que no sean de un conjunto predeterminado de palabras de datos.

8. Sistema de comunicaciones de acuerdo con cualquiera de las reivindicaciones 4 a 7 que comprende además una tercera entidad y un tercer dispositivo de cifrado en el que el tercer dispositivo de cifrado está configurado para descifrar utilizando un tercer algoritmo de descifrado los datos enviados desde un tercer destino a dicha tercera entidad a través de dicha red.

9. Sistema de comunicaciones de acuerdo con la reivindicación 8 donde dicho tercer dispositivo de cifrado está configurado para cifrar datos enviados por dicha tercera entidad a través de dicha red utilizando un tercer algoritmo de cifrado.

10. Sistema de comunicaciones de acuerdo con la reivindicación 8 o 9 donde el tercer dispositivo de cifrado está configurado para transmitir datos de métricas de la red relativos al menos a una ruta entre dicha tercera entidad y dicho tercer destino a dicha tercera entidad sin someter los datos de métricas de la red a dicho tercer algoritmo de descifrado.

11. Sistema de comunicaciones de acuerdo con cualquiera de las reivindicaciones anteriores en el que los datos de métricas de la red incluyen datos de costes de transferencia de datos.

12. Sistema de comunicaciones de acuerdo con cualquiera de las reivindicaciones anteriores en el que dichos datos de métricas de la red comprenden datos de calidad de servicio.

13. Sistema de comunicaciones de acuerdo con cualquiera de las reivindicaciones anteriores donde

dichos datos de métricas de la red sólo se pueden utilizar para actualizar una entrada predefinida de una tabla.

14. Procedimiento de operación de un sistema de comunicaciones seguras (40) donde una o más entidades (47) envían datos a una o más entidades del sistema (40) a través de una red (46) donde al menos algunos de dichos datos se cifran y descifran utilizando algoritmos de cifrado y descifrado **caracterizado porque** el procedimiento comprende:

(i) el paso de enviar datos de métricas de la red (68) desde dicha red (46) a una o más de dichas entidades sin someter los datos de métricas de la red (68) a dichos algoritmos de descifrado y
(ii) el paso de bloquear los datos de métricas de la red que no sean de un conjunto predeterminado de palabras de datos.

15. Procedimiento de acuerdo con la reivindicación 14 comprendiendo además el paso de impedir que datos de métricas de la red se pasen a la entidad si dichos datos de métrica de la red no son de un conjunto predeterminado de palabras de datos.

16. Procedimiento de acuerdo con la reivindicación 14 o 15 que comprende además el paso de usar dichos datos de métricas de la red para actualizar una entrada predefinida de una tabla.

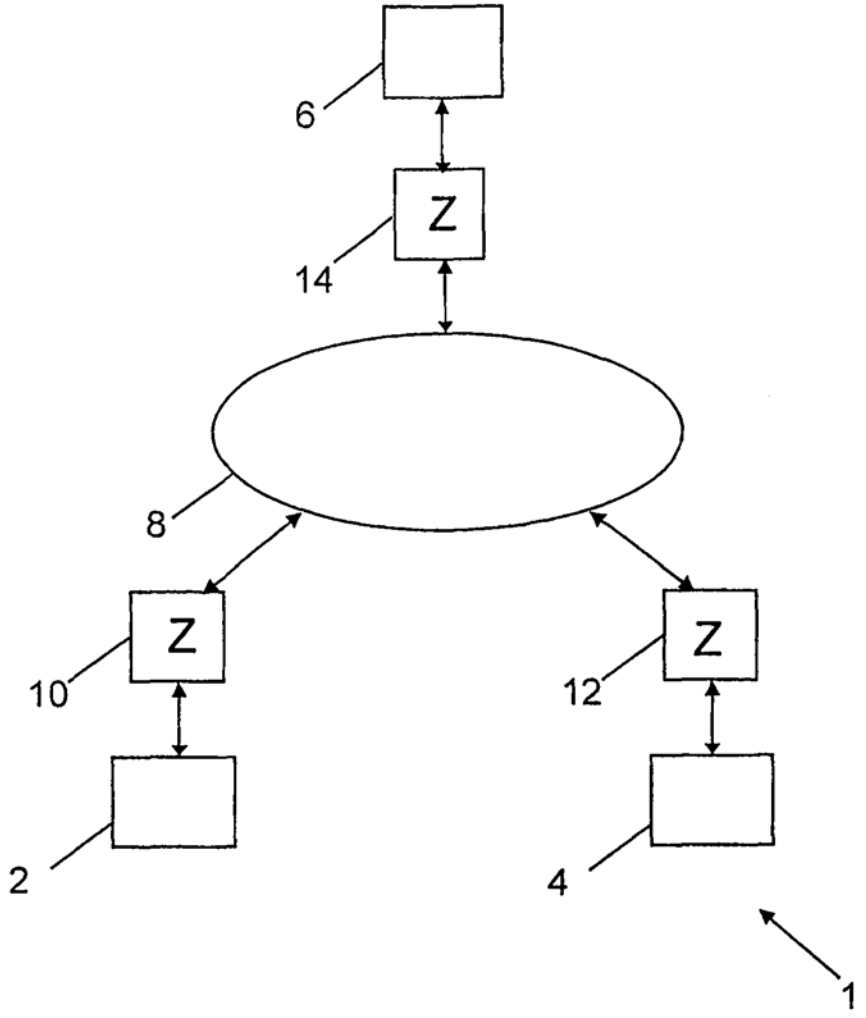

Fig. 1

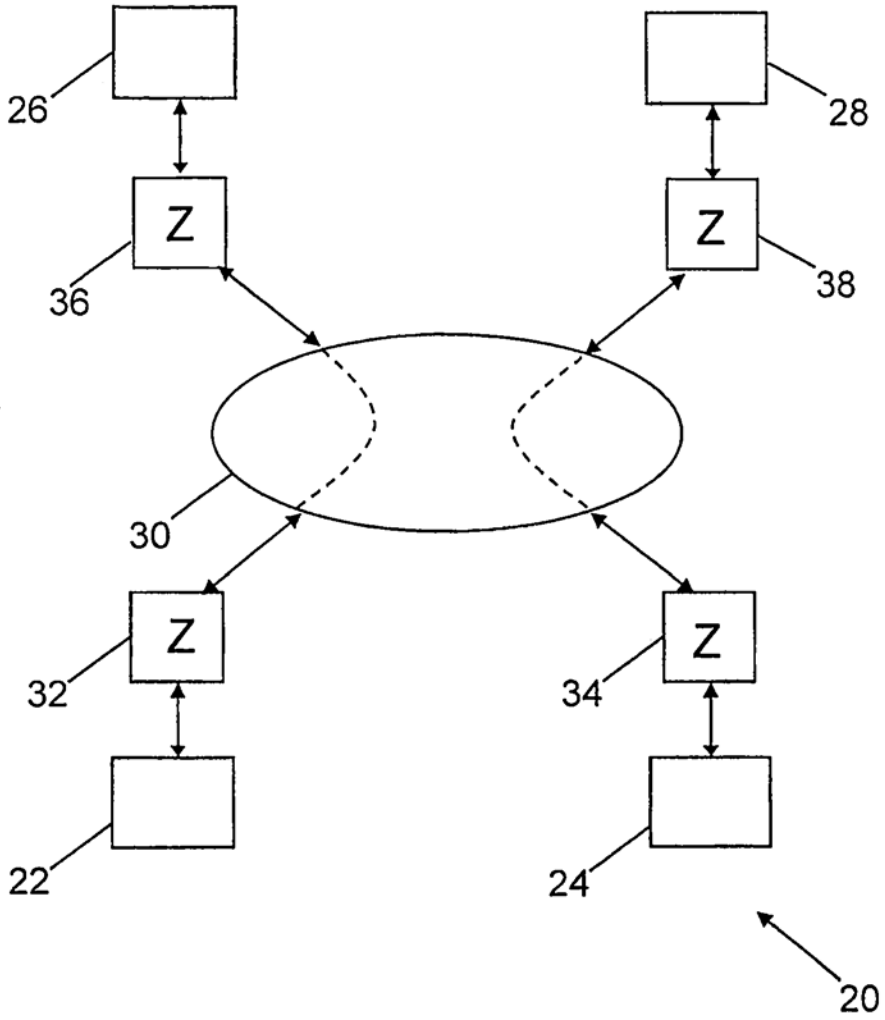

Fig. 2

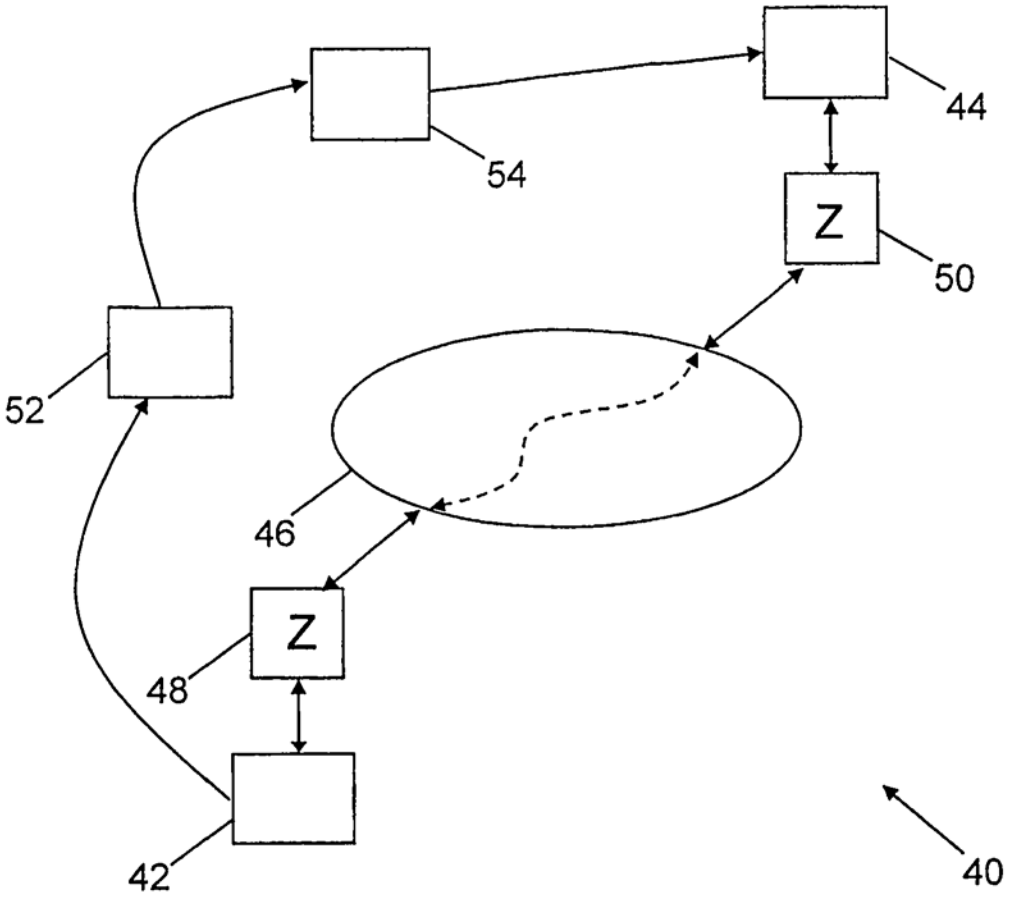

Fig. 3

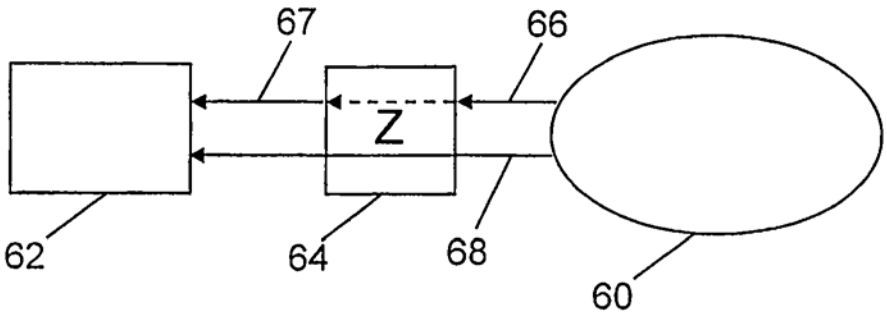

Fig. 4