(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 376 068**

(51) Int. CI.:
H04W 52/46 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08807400 .0**
(96) Fecha de presentación: **21.08.2008**
(97) Número de publicación de la solicitud: **2198658**
(97) Fecha de publicación de la solicitud: **23.06.2010**

(54) Título: **MÉTODO PARA REDUCIR LA APARICIÓN DE NODOS ENMASCARADOS, NODO Y PRODUCTO DE PROGRAMA INFORMÁTICO PARA EL MISMO.**

(30) Prioridad:
31.08.2007 EP 07301335

(45) Fecha de publicación de la mención BOPI:
08.03.2012

(45) Fecha de la publicación del folleto de la patente:
08.03.2012

(73) Titular/es:
KONINKLIJKE PHILIPS ELECTRONICS N.V.
GROENEWOUDSEWEG 1
5621 BA EINDHOVEN, NL

(72) Inventor/es:
WANG, Xiangyu y
ZAPPATERRA, Luca

(74) Agente/Representante:
Zuazo Araluze, Alexander

DESCRIPCIÓN

Método para reducir la aparición de nodos enmascarados, nodo y producto de programa informático para el mismo.

Campo técnico

La presente invención se refiere a un método para reducir la aparición de nodos enmascarados en una red de comunicación. La invención también se refiere a un producto de programa informático correspondiente y a un nodo ubicado en la red de comunicación.

Antecedentes de la invención

Las redes inalámbricas de saltos múltiples *ad-hoc*, o simplemente redes *ad-hoc*, son redes inalámbricas que transportan información a un nodo remoto meramente a través de enlaces inalámbricos que están entre nodos inalámbricos participantes. Las redes inalámbricas de saltos múltiples *ad-hoc* tienen la ventaja de una fácil implementación porque no se requieren cables, y una cobertura extensa puesto que la información se transmite a través de conexiones de saltos múltiples.

En las redes *ad-hoc* son importantes dos temas principales. El primero se refiere a buscar o mantener las rutas apropiadas dentro de las redes para transmitir información. El segundo se refiere a una gestión apropiada de acceso al medio inalámbrico puesto que todos los nodos dentro de una red comparten el medio inalámbrico subyacente.

Se han identificado problemas con el control de acceso al medio (MAC), en particular el MAC de IEEE 802.11, en redes *ad-hoc*. Hay algunos comportamientos negativos de las redes *ad-hoc*, cuando el MAC no está diseñado apropiadamente. Éstos incluyen enlace roto, ecuanimidad (es decir dar acceso a los nodos de una manera justa), rendimiento reducido o retardo largo.

El rendimiento de una red de área local inalámbrica (WLAN) depende mayormente de su esquema de control de acceso al medio (MAC). Algunas WLAN, tales como IEEE 802.11, usan un mecanismo de control de acceso al medio basado en un protocolo de acceso múltiple con detección de portadora (CSMA). Según el CSMA, se permite que un nodo de red transmita sólo si determina que el medio está en espera. Sin embargo, el CSMA no puede impedir las colisiones de paquetes provocadas por los nodos que están ubicados dentro del alcance de transmisión del receptor, pero no del emisor. Tales nodos se denominan nodos ocultos. El problema del nodo oculto se ilustra en la figura 1. El problema se produce si al menos tres nodos, en este ejemplo los nodos A, B y C, están operando próximos entre sí de modo que A y B, así como B y C están dentro del alcance de radio. Si A y C envían a B al mismo tiempo, se corromperán los datos recibidos en el nodo B. Esto puede suceder puesto que A y C están ocultos (es decir no pueden detectarse) entre sí.

Para impedir las colisiones de los paquetes de datos debido a nodos ocultos, se ha implementado un mecanismo de petición de envío (RTS)/listo para envío (CTS) en diversos sistemas de comunicación, tales como en IEEE 802.11.

El mecanismo RTS/CTS puede impedir colisiones de paquetes de datos cuando cada nodo en la proximidad del emisor y el receptor escucha al menos un paquete de control y difiere la transmisión de manera apropiada. Sin embargo, en las redes *ad-hoc* en general no se da esta suposición. Los nodos vecinos a menudo no pueden recibir los paquetes de control porque están enmascarados por transmisiones en curso desde otros nodos cerca de ellos. Esto significa que el mecanismo RTS/CTS no impide habitualmente colisiones de paquetes de datos, incluso en perfectas condiciones de operación, tales como ausencia de retardo de propagación despreciable, ausencia de desvanecimiento de canal y ausencia de movilidad de nodo. En la siguiente descripción un nodo que debe recibir un paquete RTS o un paquete CTS, pero que no puede interpretarlo correctamente debido a otra transmisión en curso, se denomina nodo enmascarado. El problema del nodo enmascarado está ilustrado en la figura 2. En este ejemplo el nodo B transmite el paquete 1 al nodo A y el nodo D transmite el paquete 2 al nodo C al mismo tiempo. Puesto que el nodo E recibe paquetes desde dos fuentes diferentes, no puede decodificar ninguno de los paquetes. Se dice que el nodo E es un nodo enmascarado puesto que cada transmisión enmascara a la otra.

Los nodos enmascarados se consideran tan fundamentales como los nodos ocultos. Cuando los nodos enmascarados intentan transmitir sus propios datos, sus transmisiones normalmente colisionarán con las transmisiones en curso. Por tanto, las colisiones debido a los nodos enmascarados desperdician significativamente recursos de radio en las redes inalámbricas. Aunque se hayan estudiado extensamente los nodos ocultos, al problema del nodo enmascarado se le ha prestado sólo poca atención.

El documento US 2005/0058151 publicado el 17/03/2005 da a conocer un método para reducir la aparición de nodos enmascarados en una red de comunicaciones inalámbrica en la que cuando un nodo detecta una intención de otro nodo de establecer un enlace de comunicaciones (transmisión RTS) que interferiría con el ya establecido, transmite un mensaje (OTS) para indicar al otro nodo una objeción. El otro nodo entonces tiene que ceder.

Por tanto, existe la necesidad de un método mejorado para reducir la aparición de nodos enmascarados en redes de comunicación.

Sumario de la invención

Según un primer aspecto de la invención se proporciona un método para reducir la aparición de nodos enmascarados en una red de comunicación según la reivindicación 1.

Por tanto, la presente invención proporciona una manera eficaz de reducir la aparición de nodos enmascarados y por tanto se reduce la interferencia en la red y se mejora el rendimiento de la red.

Según un segundo aspecto de la invención se proporciona un producto de programa informático que comprende instrucciones para implementar el método según el primer aspecto de la invención cuando se carga y se ejecuta en medios informáticos del segundo nodo.

Según un tercer aspecto de la invención se proporciona un nodo para una red de comunicación inalámbrica según la reivindicación 6.

Además, el nodo según el tercer aspecto de la invención puede estar dispuesto para implementar el método según el primer aspecto de la presente invención.

Breve descripción de los dibujos

Otras características y ventajas de la invención serán evidentes a partir de la siguiente descripción de realizaciones a modo de ejemplo no limitativas, con referencia a los dibujos adjuntos, en los que:

- la figura 1 ilustra el problema del nodo oculto en una red de comunicación;

- la figura 2 ilustra el problema del nodo enmascarado en una red de comunicación;

- la figura 3 es un diagrama que muestra resultados de simulación;

- la figura 4 muestra una arquitectura de la red, en la que pueden aplicarse las enseñanzas de la invención;

- la figura 5 muestra diferentes mensajes transmitidos en la figura 4 durante la configuración del enlace de comunicación de datos;

- la figura 6 es otro diagrama que muestra otros resultados de simulación;

- la figura 7 muestra diferentes mensajes transmitidos según una primera realización de la presente invención;

- la figura 8 es un diagrama de flujo que ilustra la primera realización de la presente invención;

- la figura 9 muestra diferentes mensajes transmitidos según una segunda realización de la presente invención; y

- la figura 10 es un diagrama de flujo que ilustra la segunda realización de la presente invención.

Descripción detallada de las realizaciones de la invención

Los sistemas WLAN tradicionales se aprovechan del concepto de reutilización de frecuencia definiendo células y dejando que las adyacentes usen diferentes frecuencias. El propósito de usar diferentes frecuencias por cada célula es limitar la interferencia procedente de células vecinas (interferencia cocanal).

El aumento continuo en la demanda de capacidad de usuario y eficacia del ancho de banda en las WLAN promueve el estudio de nuevas estrategias para optimizar la eficacia del espectro de radio que se define por el número de bits transmitido exitosamente en un periodo de tiempo dado, dentro de una banda de frecuencia dada ocupada en un área determinada.

La red celular virtual (VCN) es una posible manera de mejorar la eficacia del espectro. Consiste en una arquitectura de comunicación celular que usa toda la banda de frecuencia para cada enlace de comunicación. Además, en este concepto no hay estaciones base convencionales que gestionen asignaciones y traspasos de canal.

A continuación se describen algunas realizaciones de la presente invención en el contexto de las VCN que usan un protocolo basado en contienda sincronizado. El protocolo divide el tiempo en dos periodos: un periodo de control (CP) y un periodo de datos (DP). En el periodo de control, sólo los paquetes de control, tales como RTS/CTS, se

intercambian para establecer transmisiones de datos entre pares de nodos de origen y destino; y en el periodo de datos tienen lugar las transmisiones de datos reales. Este protocolo se parece a la estructura de canal común en el borrador de IEEE 802.11s actual (IEEE 802.11s Task Group, "IEEE P802.11s: ESS Mesh Networking", versión en borrador 0.03, Sección 9.14, agosto de 2006), excepto que en este caso sólo se usa un canal. Sin embargo, debe observarse que las enseñanzas de la invención no están restringidas a este tipo de red específico.

Se han realizado simulaciones en la red descrita anteriormente consistentes en algunos puntos de acceso (AP) y algunas estaciones (STA) por AP. Un nodo en la red de comunicación se denomina dispositivo que puede recibir y/o transmitir datos. Ejemplos de nodos son puntos de acceso y estaciones, tales como teléfonos móviles u ordenadores. El objetivo es mostrar cuántos nodos envían datos en el mismo DP en relación con la longitud de CP. En cuanto a la manera de recopilar cuántos nodos están enviando datos al mismo tiempo, es útil registrar dos estadísticas:

- *Datos enviados por ciclo*: representa el número de nodos dentro de 25 células que están enviando paquetes de datos en el mismo DP; estos nodos son los únicos que completaron exitosamente un intercambio RTS/CTS para reservar el medio en el CP anteriormente, de modo que ahora pueden transmitir datos. Debido al cuello de botella del modo de infraestructura, el número máximo ideal es de 25 transmisiones paralelas.

- *Datos correctamente recibidos por ciclo*: recoge el número de paquetes de datos enviados y con acuse de recibo en el mismo DP. Los valores son siempre inferiores a los datos enviados por ciclo porque la interferencia agrava el rendimiento, especialmente en el escenario simulado en el que se usan paquetes de datos largos.

Las estadísticas se recogen dejando que la red opere durante 2 segundos y promediando los valores obtenidos con el tiempo; los valores de longitud de CP oscilan desde 1 hasta 7,5 RTS/CTS_{tiempo} con un paso de 0,5. La variación de longitud de CP se normaliza en términos de tiempo de intercambio de RTS/CTS, donde

$$RTS/CTS_{tiempo}=DIFS+Tx\_tiempo_{RTS}+Tx\_tiempo_{CTS}+2xSIFS$$

El cálculo de RTS/CTS_{tiempo} depende de los parámetros de simulación de capa física, tal como tasa de transmisión. En la fórmula anterior DIFS indica el espacio entre tramas de función de coordinación distribuido. El DIFS se usa cuando una estación decide comenzar una transmisión. Una estación puede transmitir si detecta el medio libre para DIFS. SIFS indica el espacio entre tramas corto. El SIFS es el espacio entre tramas más corto. Se usa cuando una estación ha capturado el medio y necesita mantenerlo durante la duración de la secuencia de intercambio de tramas que va a realizarse. La normalización anterior se realiza para proporcionar una idea aproximada acerca de cuántos intentos exitosos consecutivos para reservar el medio podrían ser adecuados durante el CP considerado en el mismo alcance de comunicación.

En la figura 3 se muestran los resultados de simulación para la situación de carga saturada. El eje x es la longitud de periodo de control y el eje y representa las transmisiones paralelas por ciclo. La curva de datos enviados por ciclo representada como una curva discontinua crece rápidamente y se satura pronto puesto que no hay más oportunidades para que los nodos accedan al medio. El aumento desde 1 hasta 3 RTS/CTS_{tiempo} es abrupto, lo que significa que el aumento de la longitud de CP proporciona acceso al medio a muchos nodos más.

Con los valores de RTS/CTS_{tiempo} desde 3 hasta 3,5 hay todavía una mejora en el número de transmisiones paralelas, incluso si la curva no es tan abrupta. Con RTS/CTS_{tiempo} más alto que 3,5 el número de transmisiones paralelas no cambia significativamente.

Con respecto a la curva de datos correctamente recibidos por ciclo representados como una curva continua, sería razonable que siguiera más o menos el comportamiento de los datos enviados por curva de ciclo. Esto es verdadero en la parte abrupta, en la que RTS/CTS_{tiempo} varía desde 1 hasta 3,5. Entonces la curva disminuye suavemente. Esto se debe a un problema de espacio entre tramas extendido (EIFS) explicado más adelante.

Este problema se introdujo cuando se observó que la curva de datos correctamente recibidos por ciclo en el escenario de carga saturada estaba bajando cuando aumenta la longitud de CP. Este comportamiento no es intuitivo y se provoca por un aspecto de implementación particular de la MAC 802.11. Para este propósito es necesario realizar una explicación más profunda del EIFS.

Un nodo usará EIFS antes de una transmisión cuando determine que el medio está en espera tras la recepción de una trama para la que la capa física PHY indicó la presencia de un error, sin considerar el mecanismo de detección de portadora virtual. La duración de un EIFS para el escenario considerado se define para ser 94 µs. El nodo no comenzará una transmisión hasta la expiración del último del vector de acceso de red (NAV) y el EIFS. El EIFS se define para proporcionar tiempo suficiente para que otra estación reconozca lo que fue, para este STA, una trama recibida incorrectamente antes de que comience la transmisión. La recepción de una trama libre de errores durante el EIFS sincroniza de nuevo el nodo al estado ocupado/en espera real del medio.

La figura 4 representa una situación que puede suceder en el escenario implementado. Dos pares de estaciones (A-B y C-D) están intentando reservar el medio en el CP a través de un intercambio de RTS/CTS (mostrado con flechas continuas). Deducen colisiones en múltiples nodos en la red. Al tomar el nodo E por ejemplo, no recibe los paquetes RTS enviados por A y C; además recibe un anuncio de colisión desde la capa PHY porque ambos CTS procedentes de B y D llegan a E al mismo tiempo. Ahora E establece una comunicación con el nodo F, pero antes tiene que esperar un tiempo de retardo de envío más EIFS (en vez de retardo de envío más DIFS). Esta transmisión colisionará con la de desde A hasta B y desde C hasta D en los nodos B y D. Las transmisiones desde A hasta B y desde C hasta D fallarán incluso si se establecen correctamente.

El problema es que E (y otros nodos) no tiene un conocimiento correcto acerca de lo que está sucediendo en la red, puesto que podría inhibirse por la recepción de CTS; por el contrario comienza un intento para transmitir. En la figura 5 también se muestran diferentes mensajes enviados.

El problema de EIFS está presente sólo cuando la longitud de CP es grande. Esto es lógico porque con el uso del valor de tiempo de EIFS en vez de DIFS, los nodos tendrían dificultad para entrar en el CP, si éste es pequeño.

La relación entre el empeoramiento presente en la curva de datos correctamente recibidos en los escenarios anteriores y el problema de EIFS se demuestra a través de una simulación. Tomando el escenario saturado ilustrado anteriormente, en la figura 6 se representan dos curvas: la diferencia promedio entre los datos enviados y los datos correctamente recibidos por ciclo representados como una curva discontinua y la cantidad promedio de datos enviados por ciclo comenzando con EIFS, es decir el número de nodos enmascarados en la red representado como una curva continua. Se toman los valores de abscisa comenzando desde la longitud de CP de 4 RTS/CTS_{tiempo} porque para valores menores el problema de EIFS no empeora el rendimiento.

Por la figura puede observarse una relación directa entre las dos curvas puesto que la diferencia crece cuando aumenta el número de transmisiones que comienzan con un EIFS. La diferencia entre las curvas es mayor cuando la longitud de CP es más larga. La proporcionalidad entre las dos curvas explica el comportamiento extraño de la curva de datos correctamente recibidos en la figura 3. El problema de EIFS no está presente en las redes con tráfico ligero porque las colisiones suceden menos frecuentemente.

Ahora se describirá una primera realización de la presente invención con referencia a las figuras 4 y 7. En esta realización los nodos A a F están situados tal como se muestra en la figura 4. La secuencia de mensajes se muestra en la figura 7.

En este caso los nodos A/B y los nodos C/D han reservado un periodo de transferencia de datos intercambiando en primer lugar mensajes de control de RTS/CTS. El nodo E recibió mensajes de CTS colisionados enviados por los nodos B y D y no conoce los datos reservados que se transfieren entre los nodos A/B y los nodos C/D. Cuando el nodo E envía un mensaje de RTS al nodo F que indica su intención de transmisión, el nodo B y/o el nodo D observa que cualquier posible transmisión desde el nodo E destruirá cualquier recepción por los mismos. Por eso los nodos B y D están en una buena posición para impedir que el nodo E realice una transmisión dañina. Para ello, los nodos B y D pueden enviar un mensaje gratuito, denominado no válido para enviar (ITS), que indica una advertencia. Los nodos B y D envían tal mensaje en el periodo de control justo después de la recepción del mensaje de RTS desde el nodo E y por tanto los mensajes de ITS coinciden con el CTS esperado desde el nodo F hasta el nodo E. Si el nodo F envía un mensaje de CTS, el nodo E no podrá recibirlo puesto que el mensaje gratuito enviado por el nodo B y/o el nodo D colisiona/n con éste. Si el nodo F no responde con un mensaje de CTS por cualquier motivo, el nodo E recibirá un mensaje gratuito desde el nodo B o D. Como el mensaje gratuito no es válido para enviarse al nodo E, éste no puede establecer su transmisión. Ahora la transmisión desde los nodos A y C puede recibirse exitosamente. Por tanto la idea es mitigar el efecto de los nodos enmascarados permitiendo que los nodos relevantes envíen mensajes gratuitos con el fin de prohibir que los nodos enmascarados realicen transmisiones dañinas.

El método anterior puede describirse con referencia al diagrama de flujo de la figura 8. En el diagrama de flujo el método se describe desde la perspectiva del nodo B. En primer lugar, en la etapa 801, el nodo B recibe un mensaje de RTS desde el nodo A. Como respuesta, el nodo B envía en la etapa 803 un mensaje de CTS al nodo A como una indicación de que está listo para recibir datos desde el nodo A. Como al mismo tiempo también otro nodo en la red, en este caso el nodo D, ha enviado un mensaje de CTS y colisionan en el nodo E, este nodo no conoce los mensajes de CTS enviados por los nodos B y D. Por tanto, E envía un mensaje de RTS, que se recibe por el nodo B en la etapa 805. Luego el nodo B envía en la etapa 807 un mensaje de ITS al nodo E con el fin de impedir que el nodo E envíe datos. Ahora en la etapa 809 el nodo B puede comenzar a recibir datos desde el nodo B sin que el nodo E le moleste.

En la primera realización el nodo enmascarado es un emisor, mientras que en la segunda realización se ilustra el caso en el que el nodo enmascarado es un receptor. La secuencia de mensajes se muestra en la figura 9.

Las posiciones de los nodos A a F sigue siendo las mismas que en la figura 4. Sin embargo, en este caso los nodos B y D han establecido en primer lugar sus transmisiones a los nodos A y C, respectivamente. Los mensajes de RTS

enviados por los nodos B y D colisionan en el nodo E. Por eso el nodo E no tiene conocimiento que está dentro del alcance de dos emisores. Posteriormente, el nodo F intenta establecer una transmisión al nodo E. El nodo E envía un mensaje de respuesta de CTS al nodo F. Este mensaje de CTS se oye por los nodos B y D porque están en el alcance de transmisión del nodo E. Ahora los nodos B y D se dan cuenta de que si se permite que el nodo F lance una transmisión de datos al nodo E, esto impediría sus propias transmisiones de datos. Por tanto, los nodos B y/o D envían en el periodo de control un mensaje de no válido para recibir (ITR) al nodo E. Después de enviar el mensaje de CTS, el nodo E está preparado para escuchar a sus nodos circundantes. Si se produce un mensaje de ITR o simplemente una colisión, supone que hay emisores alrededor y no debe poder recibir. El nodo E envía en el periodo de control un CTS negativo inmediatamente al nodo F, que cancela la transmisión previamente establecida. Sin embargo, el CTS negativo puede estar sujeto a una posible colisión en el nodo F. Por eso puede ser que siempre sea fiable cancelar la transmisión.

La segunda realización de la invención también puede describirse con referencia al diagrama de flujo de la figura 10. En la figura 10, el método se describe desde la perspectiva del nodo B. En la etapa 1001, el nodo B envía un mensaje de RTS al nodo A. Como respuesta el nodo A responde con un mensaje de CTS y este mensaje se recibe en la etapa 1003 por el nodo B. Puesto que también hay otro nodo, en este caso el nodo D, en la red que ha enviado un mensaje de RTS, el nodo F no se da cuenta de que las fuentes de red están reservadas y por tanto el nodo F envía un mensaje de RTS al nodo E. Entonces el nodo E responde a este mensaje enviando un mensaje de CTS, que se recibe en la etapa 1005 por el nodo B. Luego, en la etapa 1007, el nodo B envía un mensaje de ITR al nodo E con el fin de impedir que el nodo E reciba mensajes de datos y para impedir eventualmente que el nodo F envíe mensajes de datos. Por tanto el mensaje de ITR puede incluir información para el nodo E para enviar además un CTS negativo al nodo F con el fin de impedir que el nodo F envíe mensajes de datos. En este caso, el nodo E envía en la etapa 1009 un CTS negativo al nodo F. Entonces el nodo B puede enviar en la etapa 1011 un paquete de datos al nodo A sin que se vea afectado por las transmisiones desde el nodo F.

Las enseñanzas de la presente invención pueden aplicarse ampliamente a muchas soluciones de protocolo para redes de saltos múltiples en las que la separación entre el control y los datos se realiza o bien en el dominio de tiempo o bien en el dominio de frecuencia. Por eso puede aplicarse a redes WLAN y redes inalámbricas de área personal (WPAN) tales como ZigBee.

La invención se refiere de igual manera a un producto de programa informático que puede implementar cualquiera de las etapas del método de las realizaciones de la invención cuando se carga y se ejecuta en medios informáticos de los nodos de la red de comunicación. El programa informático puede almacenarse/distribuirse en un medio adecuado suministrado conjuntamente con o como una parte del otro hardware, pero también puede distribuirse de otras formas, tal como a través de Internet u otros sistemas de telecomunicaciones por cable o inalámbricos.

La invención se refiere de igual manera a un circuito integrado que está dispuesto para realizar cualquiera de las etapas del método según las realizaciones de la invención.

Aunque la invención se ha ilustrado y descrito en detalle en los dibujos y la descripción anterior, tal ilustración y descripción se considerarán ilustrativas o a modo de ejemplo y no restrictivas; la invención no se limita a las realizaciones dadas a conocer.

Pueden entenderse y realizarse otras variaciones a las realizaciones dadas a conocer por los expertos en la técnica al poner en práctica la invención reivindicada, a partir de un estudio de los dibujos, la descripción y las reivindicaciones adjuntas. En las reivindicaciones, la expresión “comprende” no excluye otros elementos o etapas, y el artículo indefinido “un” o “una” no excluye una pluralidad. Un solo procesador u otra unidad puede cumplir las funciones de varios elementos mencionados en las reivindicaciones. El mero hecho de que se mencionen diferentes características en reivindicaciones dependientes diferentes entre sí no indica que no puede usarse ventajosamente una combinación de estas características. Ningún signo de referencia en las reivindicaciones debe interpretarse como limitativo del alcance de la invención.

REIVINDICACIONES

1. Método para reducir la aparición de nodos enmascarados en una red de comunicación que comprende al menos un primer nodo (A), un segundo nodo (B) y un tercer nodo (E), operando los nodos en la misma banda de frecuencia y en el que el primer nodo (A) y el segundo nodo (B) están dentro del alcance de comunicación por radio entre sí, el método comprende las siguientes etapas realizadas por el segundo nodo (B):

- intercambiar (801, 803, 1001, 1003) información de control con el primer nodo (A) para establecer un primer enlace de comunicación de datos entre los mismos;

- detectar (805, 1005) un mensaje que indica una intención del tercer nodo (E) de establecer otro enlace de comunicación de datos, que interferiría con el primer enlace de comunicación de datos; e

- impedir (807, 1007) que el tercer nodo (E) establezca el otro enlace de comunicación de datos, en el que la etapa de impedir comprende que el segundo nodo (B) envíe (807) un paquete de datos al tercer nodo (E) para impedir que el tercer nodo (E) envíe paquetes de datos, transmitiendo el paquete de datos de modo que dicho paquete de datos coincida con un mensaje esperado por el tercer nodo para establecer el otro enlace de comunicación de datos.

2. Método según la reivindicación 1, en el que el intercambio comprende intercambiar (801, 803, 1001, 1003) un mensaje de petición de envío y un mensaje de listo para envío con el primer nodo (A).

3. Método según cualquiera de las reivindicaciones anteriores, en el que el tercer nodo (E) se enmascara por la información de control intercambiada entre los nodos primero (A) y segundo (B).

4. Método según cualquiera de las reivindicaciones anteriores, en el que la separación entre la información de control y los datos se realiza en un dominio de tiempo o dominio de frecuencia y en el que en un periodo de control se impide que el tercer nodo (E) establezca el enlace de comunicación de datos.

5. Producto de programa informático que comprende instrucciones para implementar las etapas de un método según una cualquiera de las reivindicaciones 1 a 4 cuando se carga y se ejecuta en medios informáticos del segundo nodo (B).

6. Nodo (B) para una red de comunicación inalámbrica que comprende además un segundo nodo (A) y un tercer nodo (E), estando dispuestos los nodos para operar en la misma banda de frecuencia y en el que el nodo (B) y el segundo nodo (A) están dentro de un alcance de comunicación por radio entre sí, el nodo (B) comprende:

- medios para intercambiar información de control con el segundo nodo (A) para establecer un primer enlace de comunicación de datos entre los mismos;

- medios para detectar un mensaje que indica una intención del tercer nodo (E) de establecer otro enlace de comunicación de datos, que interferiría con el primer enlace de comunicación de datos; y

- medios para impedir que el tercer nodo (E) establezca el otro enlace de comunicación de datos, en el que los medios para impedir que el tercer nodo (E) establezca el enlace de comunicación de enlace de datos comprenden medios para enviar un paquete de datos al tercer nodo (E) de modo que dicho paquete de datos coincida con un mensaje esperado por el tercer nodo para establecer el otro enlace de comunicación de datos.

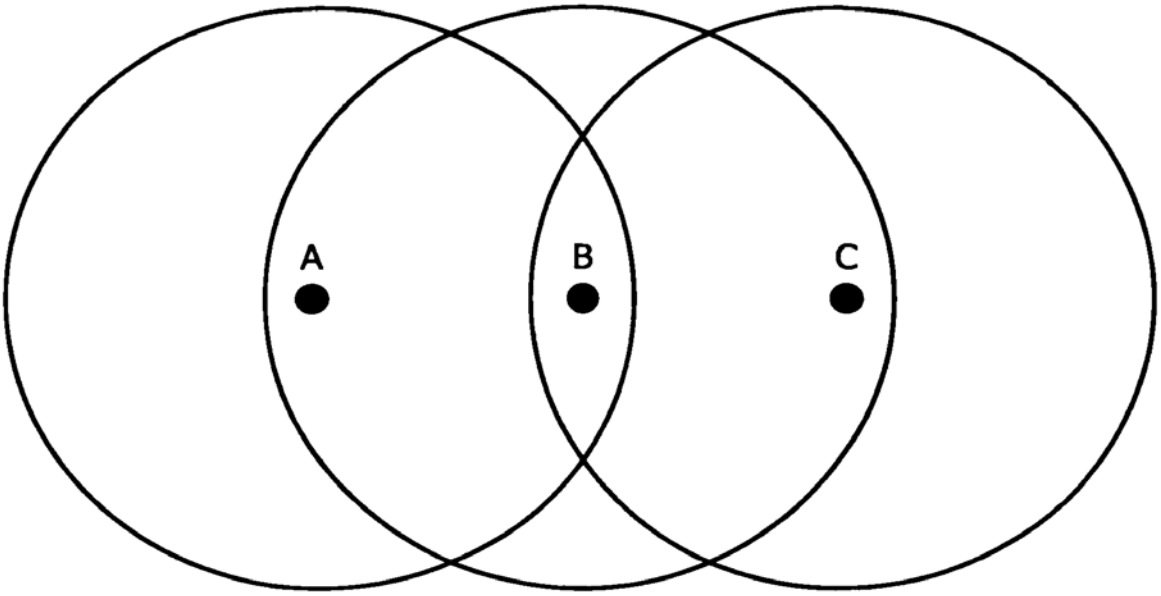

FIG. 1

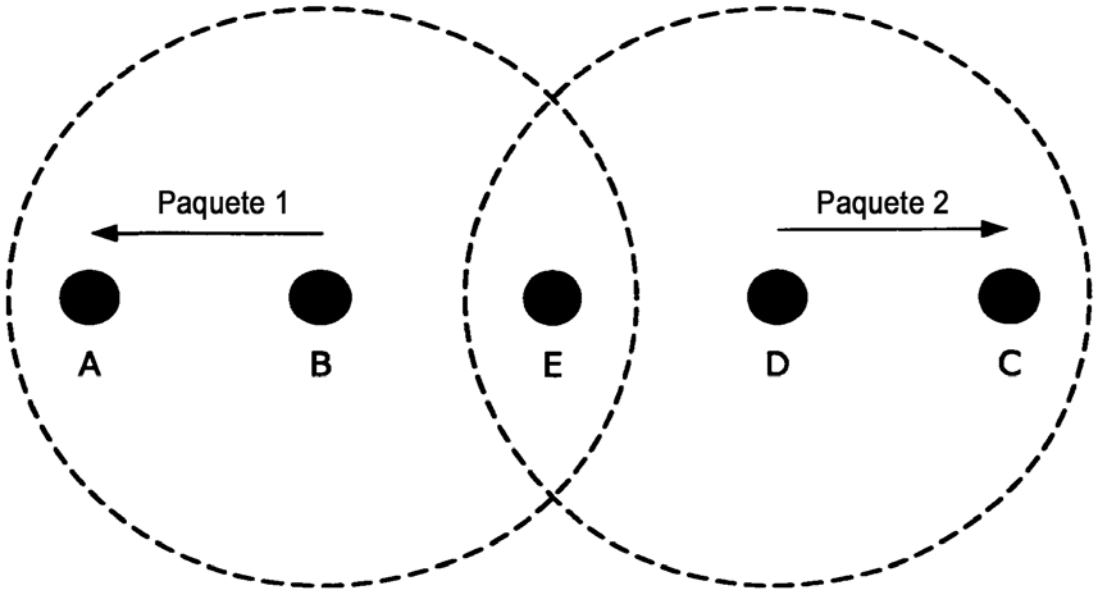

FIG. 2

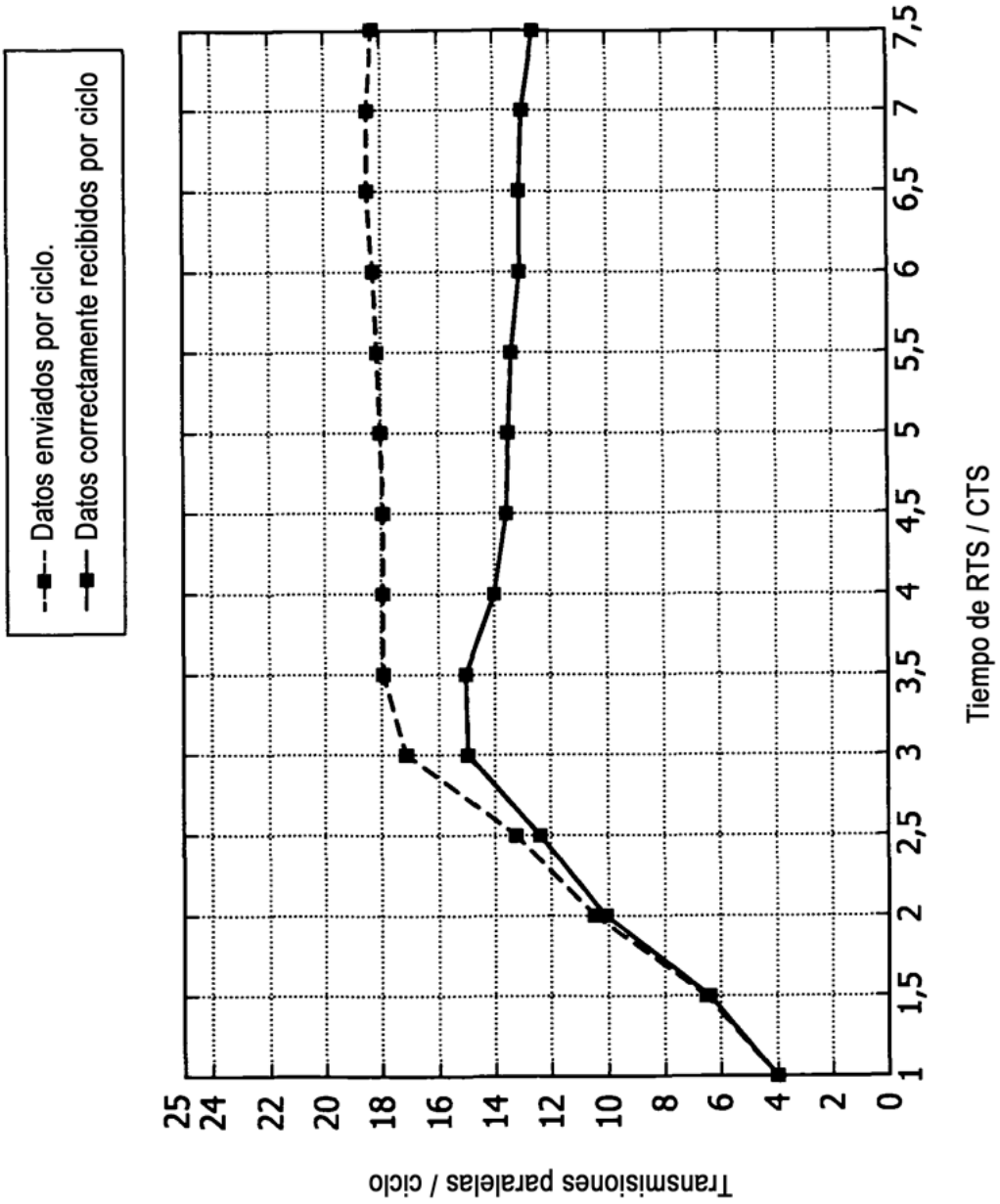
Datos enviados por ciclo.
Datos correctamente recibidos por ciclo
Transmisiones paralelas / ciclo
Tiempo de RTS / CTS
0
2
4
6
8
10
12
14
16
18
20
22
24
25
1
1,5
2
2,5
3
3,5
4
4,5
5
5,5
6
6,5
7
7,5

FIG. 3

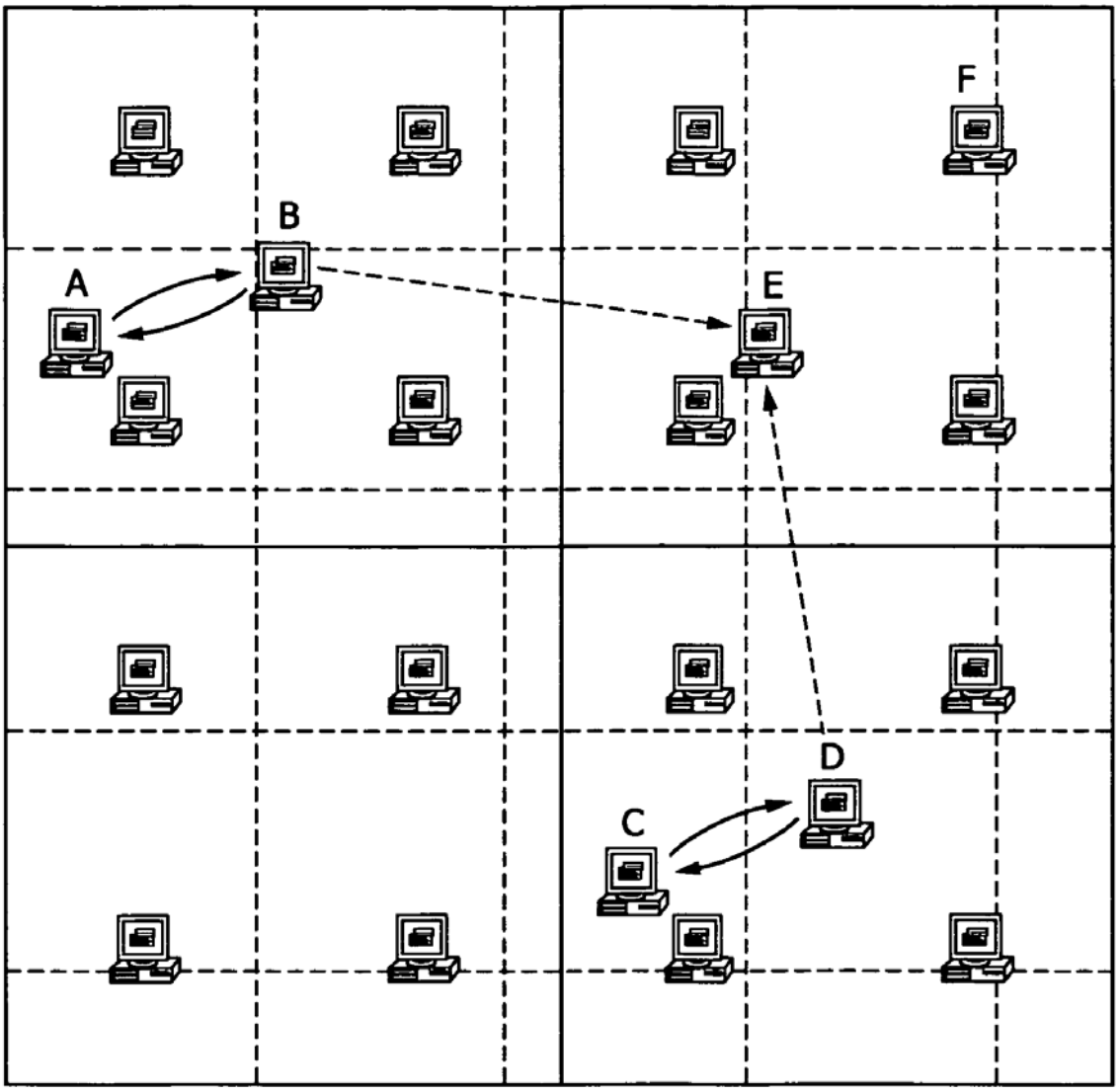

FIG. 4

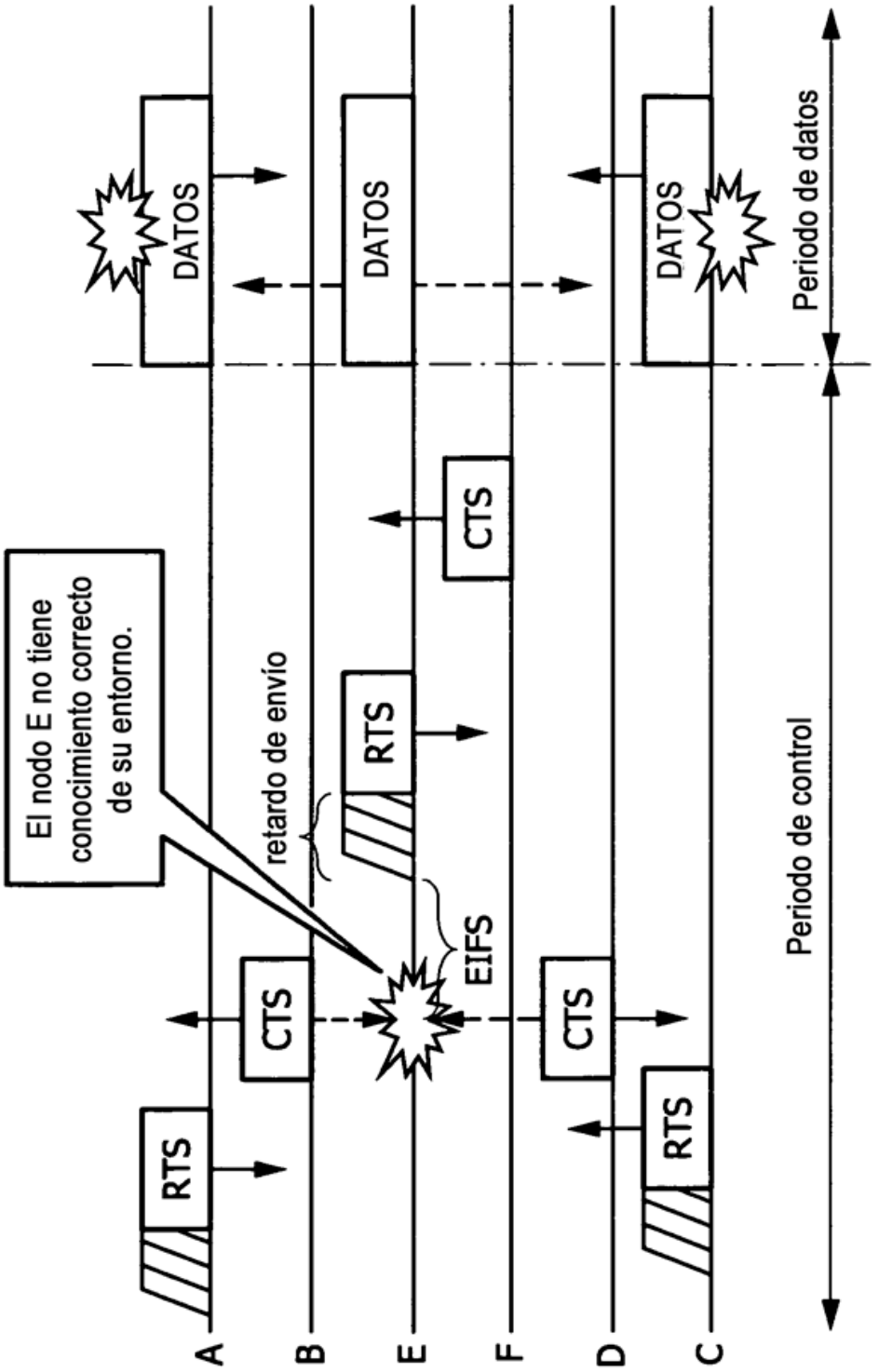
A
B
E
F
D
C
RTS
CTS
RTS
CTS
CTS
RTS
DATOS
DATOS
DATOS
El nodo E no tiene conocimiento correcto de su entorno.
retardo de envío
EIFS
Periodo de datos
Periodo de control

FIG. 5

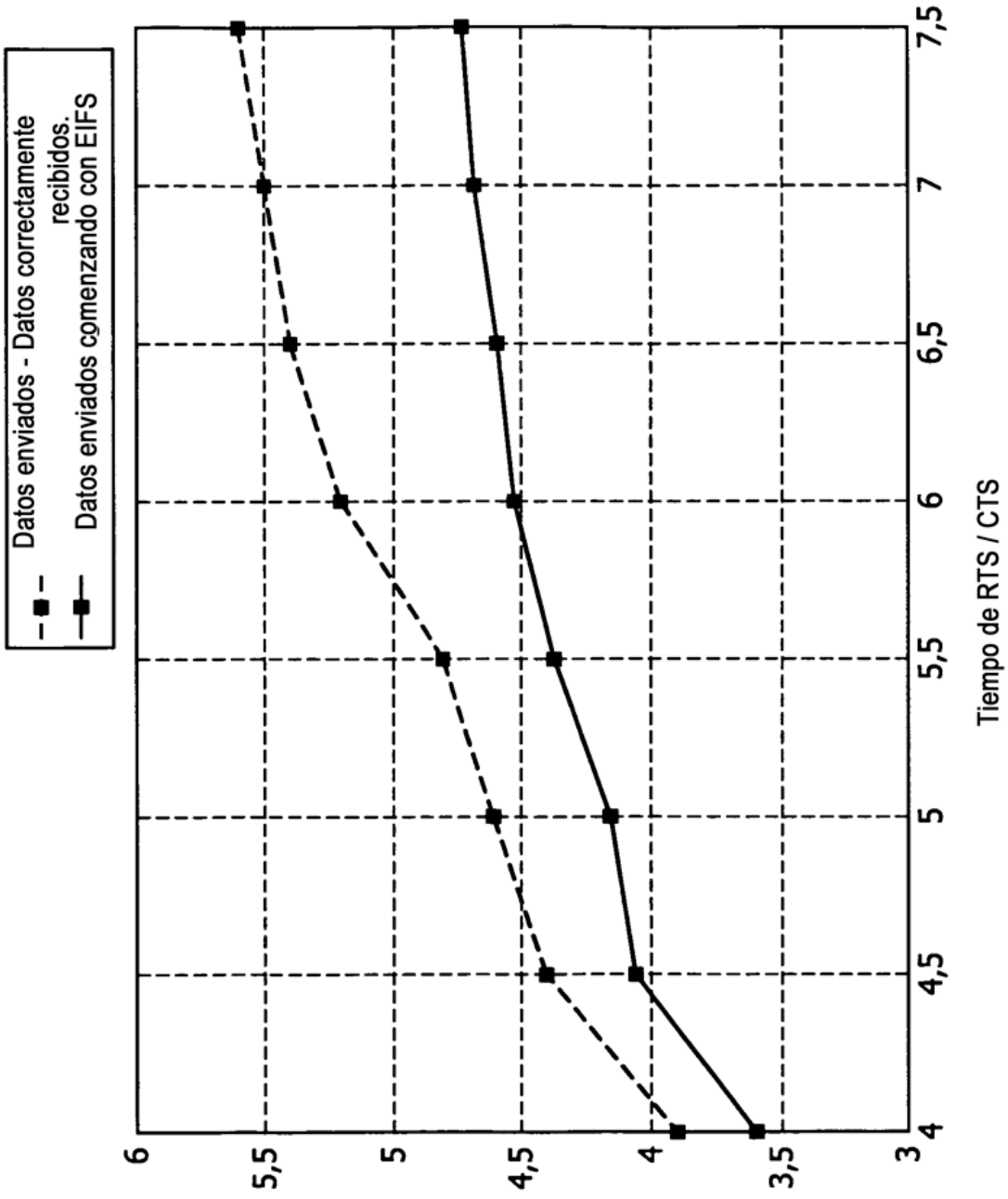
Datos enviados - Datos correctamente recibidos.
Datos enviados comenzando con EIFS
6
5,5
5
4,5
4
3,5
3
4
4,5
5
5,5
6
6,5
7
7,5
Tiempo de RTS / CTS

FIG. 6

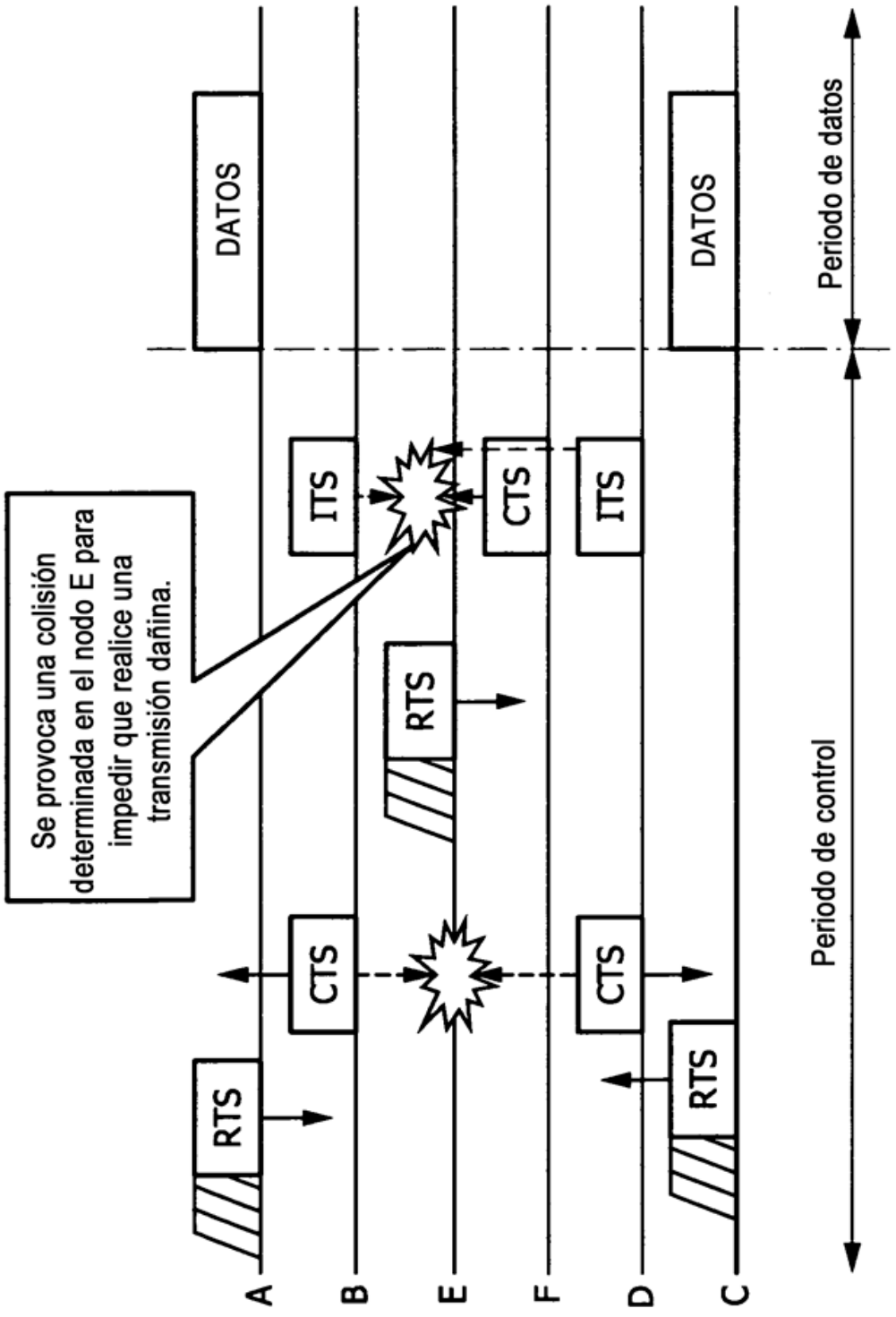
Se provoca una colisión determinada en el nodo E para impedir que realice una transmisión dañina.
DATOS
ITS
CTS
RTS
CTS
ITS
DATOS
RTS
CTS
RTS
Periodo de datos
Periodo de control
A
B
E
F
D
C

FIG. 7

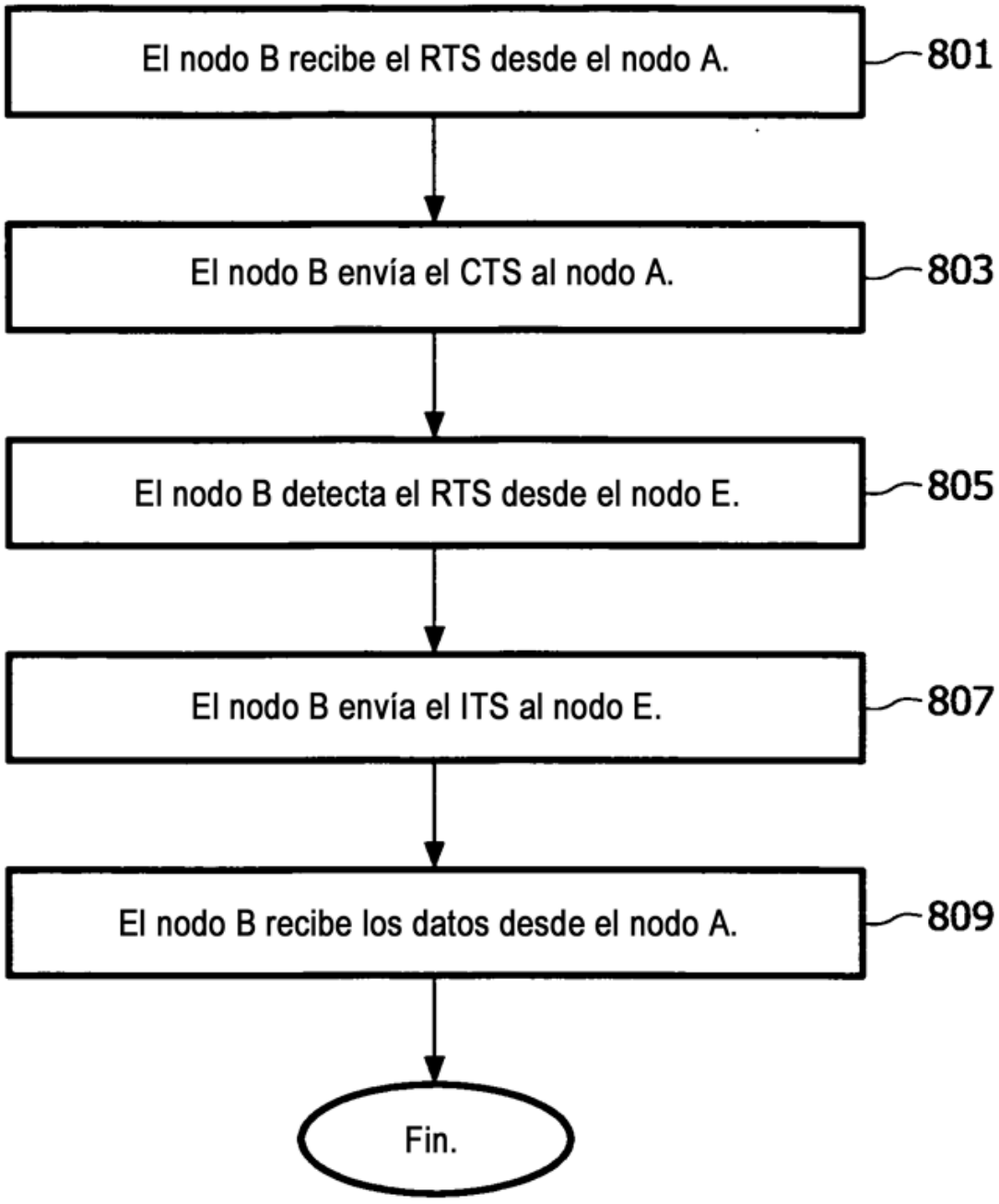
El nodo B recibe el RTS desde el nodo A.
801
El nodo B envía el CTS al nodo A.
803
El nodo B detecta el RTS desde el nodo E.
805
El nodo B envía el ITS al nodo E.
807
El nodo B recibe los datos desde el nodo A.
809
Fin.

FIG. 8

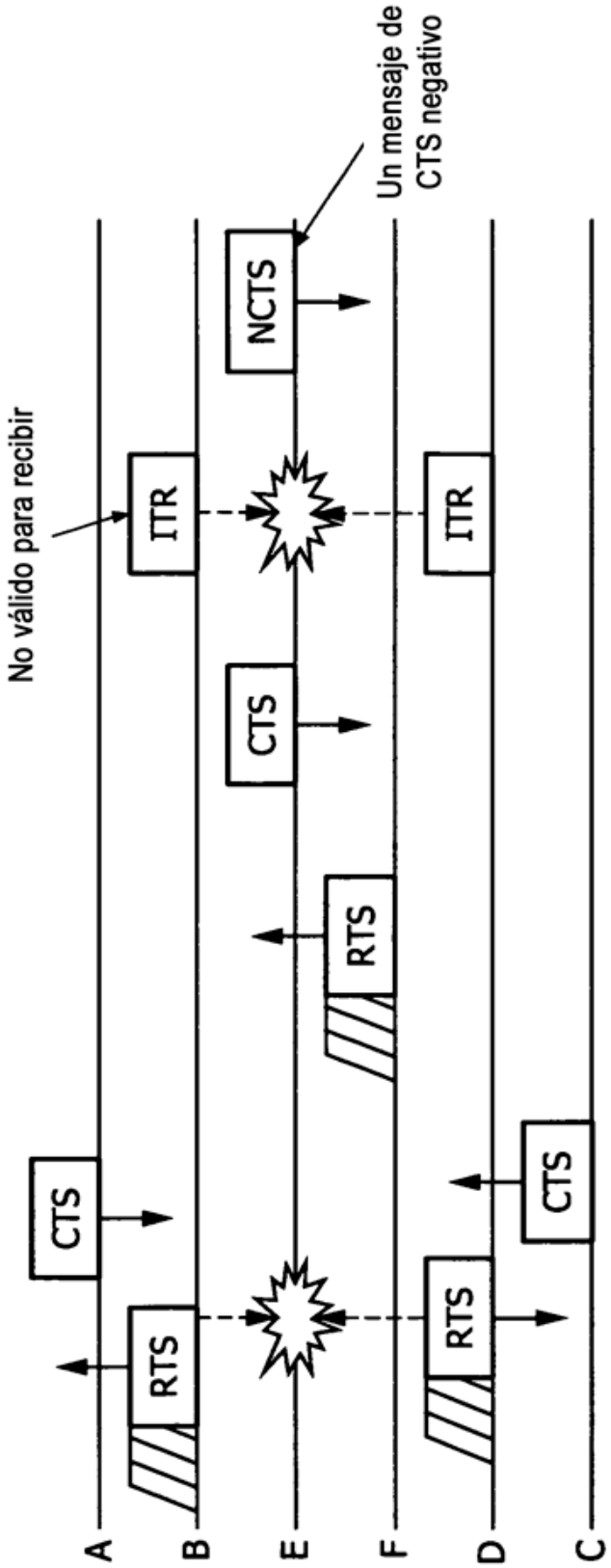
Un mensaje de CTS negativo
No válido para recibir
NCTS
ITR
ITR
CTS
RTS
CTS
RTS
CTS
A
B
E
F
D
C

FIG. 9

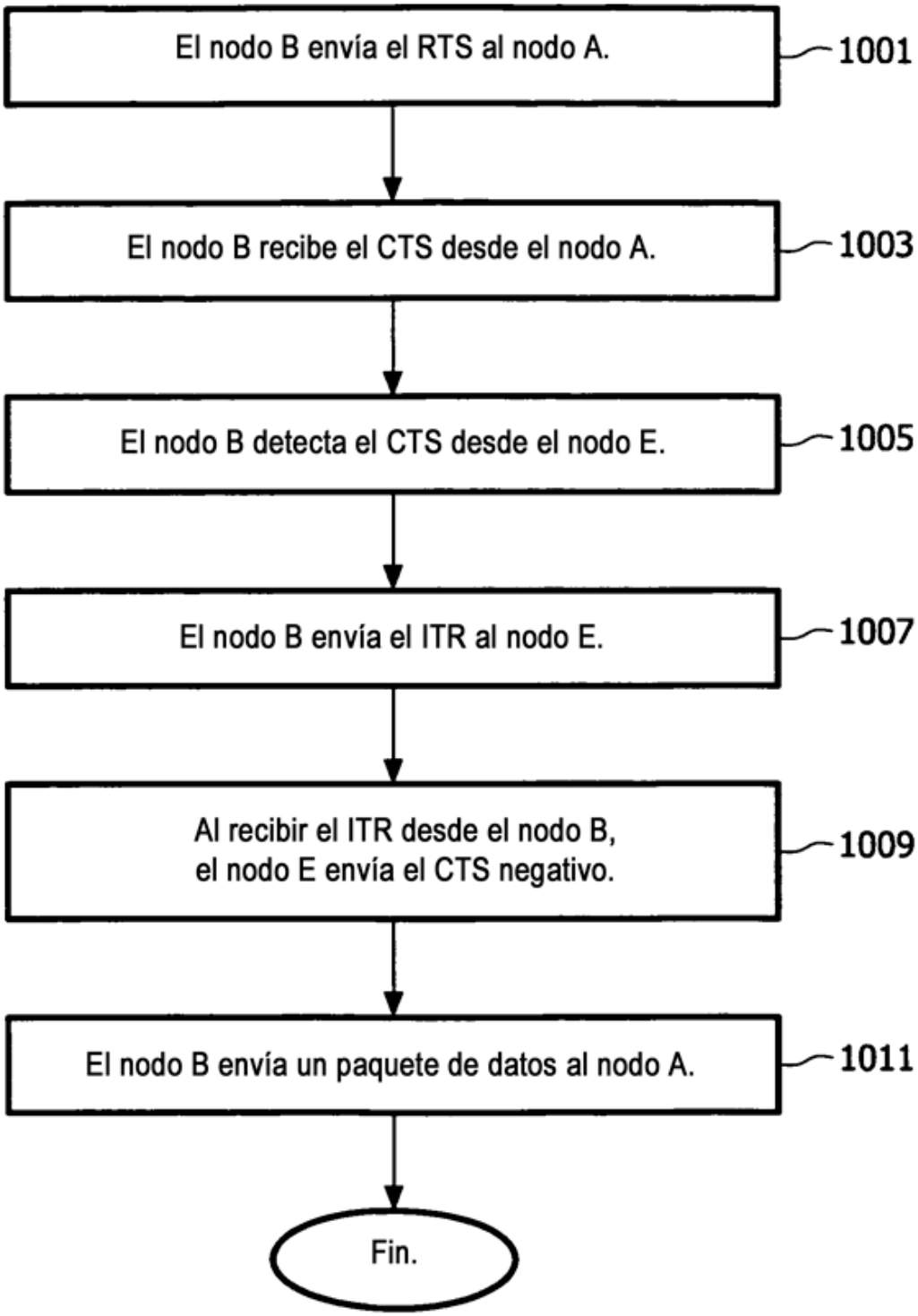
El nodo B envía el RTS al nodo A.
1001
El nodo B recibe el CTS desde el nodo A.
1003
El nodo B detecta el CTS desde el nodo E.
1005
El nodo B envía el ITR al nodo E.
1007
Al recibir el ITR desde el nodo B,
el nodo E envía el CTS negativo.
1009
El nodo B envía un paquete de datos al nodo A.
1011
Fin.

FIG. 10