(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 657 298**

(51) Int. CI.:

H04W 28/22 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.08.2013 E 13182409 (6)**

(97) Fecha y número de publicación de la concesión europea: **25.10.2017 EP 2706781**

(54) Título: **Procedimiento de transmisión en una red ad hoc multisalto IP**

(30) Prioridad:

05.09.2012 FR 1202372

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.03.2018

(73) Titular/es:

THALES (100.0%)
45, rue de Villiers
92200 Neuilly Sur Seine, FR

(72) Inventor/es:

LEGUAY, JÉRÉMIE;
MARQUES, HELDER;
LAVAUX, DAMIEN;
KHALIFE, HICHAM y
CONAN, VANIA

(74) Agente/Representante:

SALVA FERRER, Joan

DESCRIPCIÓN

Procedimiento de transmisión en una red ad hoc multisalto IP

[0001] La presente invención se refiere a un procedimiento de transmisión de información en una red ad hoc multisalto comprendiendo, la transmisión de un mensaje de un nodo emisor de origen a un nodo de destino final a través de una sucesión de saltos de un nodo emisor a un nodo receptor inmediatamente posterior, en el que se implementa:

a) un mecanismo para la gestión de la fiabilidad comprendiendo:
- durante la o cada recepción correspondiente en cada salto, de al menos un mensaje por el nodo receptor, el envío de un mensaje de confirmación al único nodo emisor,
- la aplicación de una ley de retransmisión del mensaje en el salto, del nodo emisor al nodo receptor, dicha ley comprendiendo reglas de no transmisión de mensajes que conducen a la no retransmisión del mensaje,

b) un mecanismo de gestión de la congestión de los nodos proporcionando una limitación de la velocidad de envío de un nodo emisor a un nodo receptor debido a una información de congestión del nodo receptor enviada al nodo emisor.

[0002] Las redes ad hoc multisalto se utilizan en particular en las redes de radio, y en particular, en las redes militares en las que la comunicación generalmente solo es posible entre los nodos en el rango de radio. Un protocolo de enrutamiento asegura la repetición de los mensajes o paquetes de nodo en nodo para permitir la conectividad de extremo a extremo.

[0003] Los nodos en la red pueden ser móviles o no.

[0004] Estas redes son redes ad hoc, lo cual significa que la red no tiene una estructura definida previamente. A menudo, son definidas como MANET.

[0005] Debido a la movilidad de los nodos y a los problemas de propagación de radio, la conectividad varía considerablemente en el tiempo y el espacio complicando el transporte de datos, en particular debido a la falta de fiabilidad de la transmisión en cada uno de los saltos de radio entre un nodo emisor y un nodo receptor posterior y a la posible congestión de ciertos nodos que deben transmitir más mensajes de los que pueden.

[0006] En este contexto, las soluciones de transporte desarrolladas para las redes que utilizan el protocolo IP (InternetProtocol), por ejemplo, el protocolo de transporte TCP, resultan insuficientes por las razones siguientes.

[0007] El nodo de origen y el nodo de destino se coordinan para regular la velocidad de envío de los datos y decidir las retransmisiones. Las redes ad hoc requieren, sin embargo, controlar bien la velocidad de los flujos en cada salto de radio y evitar retransmitir sistemáticamente los paquetes perdidos desde el nodo de origen.

[0008] Los protocolos de transporte, desarrollados para las redes IP, han sido diseñados para redes de bajo índice de pérdida, bajo retraso y baja fluctuación. Por lo tanto, estos protocolos no reaccionan apropiadamente en las redes ad hoc. Por ejemplo, cuando se produce una pérdida de paquetes, el TCP reduce su velocidad pensando que se trata de una congestión, aunque no es sistemáticamente necesario.

[0009] Las redes de radio ad hoc actuales ofrecen un soporte de IP básico. Son capaces de enrutar paquetes entre un nodo de origen y un nodo de destino, pero no brindan un servicio de IP optimizado de extremo a extremo en la red ad hoc. Si la aplicación usa el protocolo de transporte TCP en esta red, el control de flujo se efectúa “al máximo”, es decir sin soporte de nodos de radio, lo que plantea problemas de rendimiento, y en especial una obstrucción de los nodos intermediarios, y de las retransmisiones de extremo a extremo.

[0010] Se han presentado soluciones para permitir la conservación del Protocolo IP en redes con características específicas. Se puede citar, por ejemplo, las soluciones siguientes, clasificadas por capas según el modelo OSI.

Capa 4

[0011] Los Performance Enhanced Proxies (PEP) (http://www.faqs.org/rfcs/rfc3135.html) o Split TCP permiten

mejorar el rendimiento del TCP cuando una conexión pasa por un enlace con alto índice de error o con pocos recursos (poco ancho de banda, alto retraso). Los PEP interceptan los flujos (por ejemplo, sesión TCP) para optimizar el transporte de datos en un segmento de red difícil. Dos PEP situados al borde del segmento (satélite, por ejemplo) pueden utilizar un protocolo específico entre ellos. En los PEP se utilizan numerosas técnicas, como por ejemplo la retransmisión local de segmentos TCP (H. Balakrishnan, S. Seshan y R. Katz. Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks. ACM Wireless Networks, Vol. 1, 1995) perdidos. Este mecanismo permite recuperar rápidamente los datos sin afectar la velocidad de la fuente. Los PEP son utilizados, generalmente, para optimizar el transporte en un segmento de mala calidad y no en varios. Sin embargo, esta solución ha sido puesta en práctica en una red ad hoc (Split TCP for mobile ad hoc networks. Kopparty, S.; Krishnamurthy, S. V.; Faloutsos, M.; Tripathi, S. K.; GlobeCom 2002) descomponiendo las conexiones de extremo a extremo en varios segmentos locales. Los proxis almacenan así los paquetes y los entregan al próximo proxy.

[0012] Esta solución se sitúa en el nivel de transporte (capa 4) interceptando las conexiones TCP de extremo a extremo. Por lo tanto, no funcionan de manera transparente frente al protocolo de transporte. Por otra parte, el mecanismo, salto por salto, ajusta la velocidad de salida proporcionalmente a la velocidad de las confirmaciones recibidas. No permite reaccionar de manera preventiva a una congestión y puede transmitir mensajes inútilmente, aunque el nodo posterior no tenga la capacidad de recibirlos.

Capa 4

[0013] Se han propuesto numerosas adaptaciones de TCP para las redes ad hoc, como A-TCP (J. Liu, S. Singh. ATCP: TCP for Mobile Ad Hoc Networks. IEEE Journal on Selected Areas in Communications. 1999) o TCP-ELF (G. Holland and N. Vaidya, “Analysis of TCP performance over mobile ad hoc networks, “Proc. ACM Mobicom’99, Seattle, WA, 1999). Estas soluciones agregan un módulo que monitorea el estado de la red (basado en la ECN y los mensajes ICMP) y permite a la fuente la diferenciación de las pérdidas debido a una congestión de las mismas relacionadas con los errores de transmisión. Estas aproximaciones de extremo a extremo no permiten el control de flujo salto por salto. Además, las aproximaciones de capa 4 (y superior) no permiten ser transparentes frente al protocolo de transporte utilizado por la aplicación (por ejemplo, TCP, UDP).

Capa 4

[0014] Nuevos protocolos de transporte para las redes de radio ad hoc han sido definidas, como Hop (Block-switched Networks: A New Paradigm for Wireless Transport. Ming Li, Devesh Agrawal, Deepak Ganesan, and Arun Venkataramani in Proceedings of the 6th ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI 2009), Boston, Apr 2009. http://hop.cs.umass.edu/). Este protocolo define un control de flujo en cada salto y un bucle de extremo a extremo para asegurar la fiabilidad. Las aplicaciones deben utilizar un zócalo específico “hop” para poder comunicarse con este protocolo. No se trata de una aproximación transparente. Una aproximación similar llamada “Hop-by-hop TCP” (Hop-by-Hop TCP over MANET. Yao-Nan Lien, Yi-Fan Yu- IEEE APSCC 2008) modifica el TCP para dividirlo en dos mecanismos. Una parte de extremo a extremo que se ocupa principalmente del control de congestión y una parte en cada salto que asegura los saltos de radio. El procedimiento descrito en este documento se diferencia de Hop por los siguientes puntos.

[0015] Hop controla la fiabilidad total por bloque (de cualquier tamaño). El objetivo es asegurar la transmisión de los bloques salto por salto y luego de extremo a extremo, ya que Hop tiene como objetivo la fiabilidad total. La abstracción por bloque es utilizada para disminuir la sobrecarga de la red relacionada con las confirmaciones.

[0016] Hop funciona en modo conectado. Los nodos deben abrir y mantener las conexiones en cada salto de forma gradual hasta el destino. Se establece un mecanismo de *keep-alive* para garantizar que los bloques se transmiten en los nodos inferiores. Si una confirmación proveniente del destino final no es recibida antes de cierto tiempo, los nodos intermediarios pueden reemitir el bloque.

[0017] Hop controla la velocidad de los bloques con una solución stop-and-wait. Un bloque se envía al nodo siguiente solo si el bloque anterior ha sido reconocido.

[0018] Hop es un protocolo de transporte, por lo que debe modificarse la aplicación para poder utilizarlo.

Capa 3

[0019] Algunas soluciones de túnel IP utilizan un protocolo de transporte subyacente (proporcionando un

servicio de fiabilidad, entrega ordenada y control de flujo). Es el caso de los túneles vTun, SSH y de ciertos VPN basados en una conexión TCP. Esta solución se utiliza en redes como Internet, en la que la conexión TCP no está optimizada para cruzar una red restringida.

Capa 2

[0020] Las soluciones de tipo ARQ (Automatic Repeat Request) permiten compensar las pérdidas en un salto intentando varias transmisiones sucesivas en intervalos crecientes de tiempo. Estas soluciones no permiten el control global de la velocidad de un flujo y ocasionan variaciones en el retardo de ida / vuelta (RTT por las siglas en inglés de Round-Trip Time) que penalizan los protocolos de transporte como el TCP.

[0021] El control de flujo que se quiere realizar podría estar basado en:

En resumen, el estado de la técnica se descompone en 3 categorías:

- Las soluciones que proponen un nuevo protocolo de transporte y que, por tanto, requieren un cambio a nivel del origen y el destino (Hop).
- Las soluciones que rompen el control de flujo de extremo a extremo del TCP (PEP, Split TCP y otras variantes)
- Las adaptaciones de TCP que permanecen de extremo a extremo y requieren una transmisión desde la propia fuente, aunque la pérdida se sitúe cerca del destino.

[0022] Por lo tanto, se entiende que las soluciones elaboradas hasta entonces no permiten beneficiarse del servicio IP en una red ad hoc multisalto y particularmente en una red de radio, ofreciendo un servicio de IP transparente con una optimización del transporte de un flujo de paquetes independientemente del protocolo de transporte utilizado (TCP, UDP, SCTP…) y permitiendo el funcionamiento, especialmente, en un ambiente encriptado IP-Sec.

[0023] La invención tiene el objetivo de proporcionar una solución a este problema.

[0024] Para este propósito, el objeto de la invención es un procedimiento de transmisión de información según la reivindicación 1.

[0025] De acuerdo con modos particulares de implementación, el procedimiento comprende una o varias de las características siguientes:

- la ley de retransmisión para un nodo emisor determinado tiene en cuenta, para las reglas de no retransmisión, variables relacionadas con los nodos de los saltos anteriores entre el nodo emisor de origen y el nodo emisor;
- la ley de retransmisión para un nodo emisor determinado tiene en cuenta, para las reglas de no retransmisión, el número de nodos ya recorridos por los saltos sucesivos desde el nodo emisor de origen;
- dicho procedimiento comprende una etapa de marcado del tipo de información contenida en el mensaje y la ley de retransmisión tiene en cuenta, para las reglas de no retransmisión, el tipo de información contenida en el mensaje;
- el envío de un mensaje de confirmación tiene lugar solamente durante la recepción correspondiente de un conjunto de varios mensajes;
- el mecanismo de gestión de la congestión aplica, para el cálculo de la velocidad del nodo emisor, una ley de aumento aditivo y de disminución multiplicativa (AIMD por Increase Multiple Decrease en inglés);
- el mecanismo de gestión de la congestión aplica una no transmisión definitiva de ciertos mensajes del nodo emisor hacia el nodo receptor en caso de congestión del nodo receptor;
- la no transmisión de los mensajes es aplicada a los mensajes que han recorrido la menor cantidad de saltos hasta un nodo emisor y / o a los mensajes con la menor probabilidad de llegar al nodo receptor final;
- la información contenida en los mensajes transmitidos es información formateada para una transmisión en una red según el Protocolo IP y los mensajes transmitidos comprenden, además de la información en los formatos IP, un encabezado (HBH) correspondiente para asegurar los mecanismos de gestión de la fiabilidad y de gestión de la congestión; y
- el encabezado comprende una información representativa del protocolo transportado.

[0026] La invención se comprenderá mejor con la lectura de la siguiente descripción, dada únicamente a modo de ejemplo y hecha con referencia a los dibujos en los que:

- la **Figura 1** es una vista esquemática de una red en la que se aplica el procedimiento según la invención;

- la **Figura 2** es una vista esquemática que ilustra el flujo de información de nodo en nodo en la red;
- la **Figura 3** es una vista esquemática del encabezado de un mensaje utilizado en el protocolo según la invención; y
- la **Figura 4** es una vista esquemática de la arquitectura funcional de un nodo de la red.

[0027] En la Figura 1 se muestra una red ad hoc 10 o MANET cuyos nodos 12, representados con círculos, están formados, por ejemplo, por radios móviles transportados por vehículos militares.

[0028] La red 10 permite la comunicación entre los nodos mediante saltos sucesivos de nodo en nodo, pero también permite la comunicación desde y hacia los nodos exteriores a la red como los nodos 14 y 16.

[0029] Por lo tanto, los nodos de la red 10, en relación con los nodos exteriores a la red 10 como los nodos 14 y 16 aseguran una función de pasarela. Este es el caso de los nodos 18 y 20 en la Figura 1. Los otros nodos 12 de la red 10, aseguran solamente la transmisión y la recepción de información desde y hacia otros nodos de la red. Por tanto, constituyen solamente nodos de relevo.

[0030] Un nodo pasarela 18, 20 aloja por ejemplo una aplicación local o está conectado a otra red IP, por ejemplo, una red LAN o WAN que forman, de este modo, cada una un nodo exterior como los nodos 14 y 16.

[0031] Como se conoce por sí mismo, la red ad hoc 10 garantiza la transmisión de mensajes a partir de la dirección IP del nodo de destino mediante saltos sucesivos en la red 12. Por lo tanto, un mensaje enviado por el nodo de origen 14 al nodo de destino 16 transita primero por el nodo pasarela 18 y luego por dos nodos de relevo 12 de la red antes de llegar al nodo pasarela 20 y ser transmitido finalmente al nodo de destino 16.

[0032] El procedimiento según la invención disocia el tratamiento de la fiabilidad y el de la congestión con parámetros diferentes:

- Trata la fiabilidad en cada salto con una ventana W de mensajes y un parámetro de esfuerzo de fiabilidad p. La ventana W permite reducir la sobrecarga asociada a las confirmaciones y controla el envío simultáneo de transmisiones o retransmisiones. Los datos pueden perderse después de un determinado esfuerzo de fiabilidad p que puede ser, por ejemplo, de un tiempo o un número máximo de retransmisiones. Por lo tanto, el parámetro p define una regla de no retransmisión de un paquete, ya que, cuando el esfuerzo de retransmisión es superior a un esfuerzo máximo predefinido, no tiene lugar la retransmisión.
- Trata la congestión con un mecanismo de contrapresión (“back pressure” en inglés) salto por salto que regula la velocidad máxima de salida λ de un nodo en función de la congestión del nodo siguiente.

Aplicación en un contexto IP

[0033] Este procedimiento se implementa en una radio ad hoc como un servicio optimizado de transporte de paquetes IP. En este caso, no se requiere ninguna adaptación de la aplicación. El protocolo garantiza la regulación de la velocidad de datos para evitar la congestión de la red. Provee una fiabilidad de salto por salto regulable en función del protocolo y de las aplicaciones utilizadas anteriormente.

[0034] La necesidad de una fiabilidad configurable, y no total, proviene del hecho de que la mayoría de los protocolos de red o de aplicaciones por encima del IP implementan ellos mismos mecanismos de confirmación. Tratar de alcanzar una fiabilidad total en el nivel de IP podría empeorar la congestión e interferir fuertemente en los protocolos anteriores. Por el contrario, proporcionar un servicio no fiable no es efectivo en un ambiente de radio como el descrito anteriormente. Por lo tanto, se debe llegar a un acuerdo.

[0035] La Figura 2 muestra más detalladamente las operaciones que se realizan en los paquetes IP. Los paquetes IP son interceptados en el primer nodo pasarela 18 para ser asumidos por el procedimiento. Son restituidos como en el último nodo pasarela 20. Como parte de su aplicación para IP, el procedimiento proporciona una superposición de fiabilidad y de control de congestión sin por ello estar al nivel de transporte en el sentido OSI (nivel 4). Se define como perteneciente al nivel 3.5 según el modelo OSI, ya que añade un encabezado llamado HBH (Hop-By-Hop) entre el encabezado IP y el encabezado del transporte (TCP o UDP, por ejemplo). El procedimiento puede implementarse en diferentes niveles del modelo OSI, pero para simplificar la presentación en el ejemplo considerado, la implementación se hace en el nivel 3.5.

[0036] Los nodos son adecuados para enviar mensajes hacia otros nodos en función de la dirección IP del nodo de destino y de las reglas de enrutamiento correspondientes a la red IP. En cada recepción de uno o varios

mensajes y ventajosamente después de la recepción de un conjunto de mensajes en la ventana W, el nodo receptor devuelve, como se conoce en sí mismo, un mensaje de confirmación hacia el nodo emisor.

[0037] La Figura 2 ilustra igualmente los procesos y las colas de espera necesarias para el funcionamiento del procedimiento. Se detalla su uso en el siguiente documento.

[0038] En la Figura 2 se encuentran los nodos pasarelas 18, 20, así como los nodos intermediarios 12 de la red ad hoc. El nodo 18 recibe información de una aplicación IP señalada 30 o de un nodo de una red IP. Del mismo modo, el nodo de relevo 20 transmite la información a una aplicación IP o a un nodo de una red IP señalada 32.

[0039] El mensaje recibido de la aplicación 30 tiene un formato conocido en sí mismo, con la dirección IP de destino como encabezado, seguido de la indicación del protocolo de transporte utilizado, por ejemplo, TCP, seguido de la carga útil, es decir, los datos específicos del mensaje.

[0040] A la entrada del nodo 18 que actúa como nodo pasarela, durante una etapa señalada 34, el mensaje se modifica para añadir el encabezado HBH, entre el encabezado IP y el del protocolo de transporte utilizado para formar una trama como la designada con la referencia 36 en la Figura 2.

[0041] El detalle del encabezado agregado se ilustra en la Figura 3.

[0042] La información en el encabezado del protocolo es la siguiente:

- TPE: representa el tipo de paquete, o sea datos o confirmación (DATA o ACK).
- RQT: este indicador indica una petición especial. Una solicitud explícita de confirmación para un paquete DATA, o la indicación de una congestión para una ACK.
- OptionValue: representa el tamaño de la opción SACK para los paquetes ACK. Para los paquetes de datos DATA, se puede utilizar para decir al receptor que vacíe la cola ooList (en caso de pérdida definitiva de un paquete por el emisor, por ejemplo) y para añadir información de FEC, por ejemplo.
- SeqNb: contiene el número de secuencia para los paquetes DATA y el número de secuencia del paquete confirmado para los paquetes ACK.
- FlowID: contiene el valor único que identifica el flujo. Este valor es calculado en cada salto cuando se registra un nuevo flujo.
- Checksum: contiene el checksum del paquete.
- OrigProto: indica el número del protocolo transportado (TCP o UDP, por ejemplo).

[0043] El mensaje IP así completado se coloca en una cola de espera de salida 38 designada en lo siguiente como outputQ.

[0044] En función de la velocidad de salida λ, perteneciente al nodo 18, los mensajes presentes en la cola de espera son transferidos al nodo siguiente 12. El enrutamiento hacia el nodo 18 es realizado como se conoce en sí mismo a partir de la dirección IP presente en el mensaje 36.

[0045] Simultáneamente, el mensaje transmitido al nodo 12 también se transmite dentro del nodo 18 a otra cola de espera 40 designada en lo siguiente como nACKedQ. Esta cola de espera comprende los mensajes para los que no se ha recibido confirmación y que no han sido destruidos todavía.

[0046] Los mensajes 26 no confirmados que deben ser retransmitidos son transmitidos de la cola 40 a la cola 38 en función de reglas predeterminadas para permitir su retransmisión a velocidad de salida λ siguiendo el orden de la cola 38.

[0047] Las mismas etapas se implementan en los nodos intermediarios 12. En cada entrada en un nodo intermediario, el encabezado HBH se modifica para especificar especialmente la cantidad de nodos por los que ha transitado el mensaje, o la probabilidad de que el mensaje no llegue, calculada en función del número de saltos o del tiempo de expiración restante.

[0048] Al llegar en el nodo pasarela de salida 20, la trama del mensaje teniendo la forma 36, y comprendiendo el encabezado HBH después del encabezado IP y antes del de protocolo de transporte, es modificada para eliminar el encabezado HBH y es puesta en una cola de salida temporal 44 antes de ser enviada a la aplicación IP 32. El mensaje tiene así el formato de un mensaje IP clásico designado esquemáticamente con la

referencia 60 en la Figura 2.

[0049] Por lo tanto, para las aplicaciones 30 y 32, la modificación del mensaje operado en la red ad hoc para permitir la implementación del procedimiento es transparente.

[0050] El procedimiento proporciona un mecanismo de fiabilidad y un mecanismo de gestión de la congestión garantizando la gestión de la transmisión y de la retransmisión de los mensajes en la red 10.

[0051] Estos mecanismos se implementan en cada uno de los nodos como se ha expuesto anteriormente.

Mecanismo de fiabilidad

[0052] El mecanismo de fiabilidad se efectúa solamente salto por salto y no de extremo a extremo. Utiliza la ventana móvil W para controlar el envío de los paquetes. El tamaño de la ventana W define el número máximo de paquetes (transmisiones o retransmisiones) en espera de confirmación. La ventana W se actualiza en cada RTT (Round Trip Time) utilizando, por ejemplo, un mecanismo de aumento aditivo y de decremento multiplicativo conocido por sus siglas AIMD para Additive Increase Multiple Decrease en inglés. W tiene un valor mínimo y un valor máximo. W disminuye cuando se detecta una pérdida (expiración del RTO (Retransmission Time Out) para un paquete en la cola nACKedQ). Disminuir W en caso de pérdida permite ser más reactivo para detectar la desaparición de un nodo vecino, por ejemplo. El tamaño de la ventana W influye en la velocidad, pero no es utilizado aquí con ese objetivo. Los valores mínimos y máximos de W son preferentemente bastante próximos y no demasiado elevados, particularmente entre 5 y 10 paquetes, por ejemplo.

[0053] Los paquetes son enviados con un número de secuencia SeqNb que aparece en el encabezado para que el nodo receptor pueda identificar las pérdidas y reordenar los paquetes si es necesario. El nodo receptor utiliza un mecanismo de confirmación acumulativo y selectivo que indica al receptor los paquetes que han sido recibidos. El envío de las confirmaciones es activado por el nodo emisor que establece el indicador RQT en 1 en los paquetes de datos o en la detección de una pérdida gracias a los números de secuencia.

[0054] El nodo emisor necesita calcular el RTT para poder actualizar W y definir el RTO (Retransmission Time Out). Al recibir la confirmación del mensaje M, el procedimiento calcula el RTT, su varianza y el RTO con una media móvil.

[0055] El esfuerzo de fiabilidad p asociado a un flujo es un parámetro global que puede ser definido por el nodo pasarela en función de las características del flujo (protocolo de transporte, clase de servicio, requisitos de aplicación especial). Puede ser calculado, por ejemplo, a partir del:

- Número máximo de retransmisiones en cada salto
- Número máximo total de retransmisiones en la ruta
- Tiempo de expiración (estimado) del paquete en la capa de transporte

[0056] La fiabilidad del procedimiento es ventajosamente mejorada mediante la implementación de un código FEC (Forward Error Correction) para aumentar la utilidad de cada transmisión. La tasa de redundancia varía linealmente con respecto a la ventana W. Cuando W disminuye, la redundancia aumenta para mayor fiabilidad.

Marcado de los paquetes

[0057] El esfuerzo de fiabilidad p es ventajosamente definido de manera diferente en función de las características del flujo transportado. Un flujo en tiempo real requiere poca o ninguna fiabilidad, a diferencia de una transferencia de datos no críticos desde un punto de vista temporal.

[0058] Además, este esfuerzo p varía ventajosamente con el tiempo. En el caso de una transferencia TCP, por ejemplo, p debe ser elevado para evitar retransmitir los paquetes perdidos desde la fuente, pero debe ser suficientemente fiable como para evitar una retransmisión local de un paquete que ya estaría siendo retransmitido de extremo a extremo por la fuente.

[0059] El esfuerzo de fiabilidad p es ventajosamente aplicado de manera gradual a lo largo de una ruta. Con este fin, el esfuerzo de fiabilidad puede aumentarse en cada salto, ya que es más serio perder un paquete habiendo recorrido ya una parte sustancial del camino hacia el destino que un paquete que acaba de salir.

[0060] El parámetro ρ puede ser asociado al flujo en el nodo pasarela o en posición ascendente por un encriptador IPSec o un PEP TCP. Puede ser transportado, por ejemplo, a lo largo de la ruta en la cabecera del procedimiento o en una opción IP.

Mecanismo de gestión de congestión

[0061] El mecanismo de gestión de congestión es realizado solamente salto por salto y no de extremo a extremo.

[0062] La congestión se detecta mediante el uso de un umbral s1 que se compara con el número de paquetes en la cola outputQ más los de la cola nACKedQ. Ante la superación de este umbral, se envía una señal al nodo emisor anterior para que disminuya su velocidad. En cada nodo, la velocidad de emisión de cada flujo es controlada por un parámetro λ.

[0063] λ se inicia con un valor infinito, el procedimiento comienza en un modo “no congestionado”. Durante la recepción de una señal de congestión, λ se inicializa a la velocidad de flujo actual. Se activa entonces un modo de “evitación de congestión”. En este modo, λ evoluciona siguiendo, por ejemplo, un mecanismo de AIMD (Additive Increase Multiple Decrease), aumenta por adición de una constante en cada RTT y es multiplicado por otra constante cuando se recibe una señal de congestión.

[0064] Una vez activo el modo de “evitación de congestión”, el nodo puede:

- permanecer aquí de manera permanente
- regresar al modo congestionado según el estado de sus colas de espera.

[0065] La velocidad de un nodo emisor depende, por tanto, del estado de congestión del único nodo receptor siguiente.

[0066] En caso de fuerte congestión, existe ventajosamente un mecanismo de pérdida de paquetes en las colas outputQ y naCKedQ. Los paquetes que han recorrido menos camino o con la menor probabilidad de llegar a tiempo al destino podrían ser desechados. Variables representativas del camino recorrido o de la posibilidad de llegar a tiempo al destino son agregadas en el encabezado HBH presentado en este documento o son provistas por otro módulo del sistema (por ejemplo, número de saltos para el módulo de enrutamiento).

[0067] Para cada nodo y como se ilustra en la Figura 4, la arquitectura del nodo comprende un módulo de intercepción de los paquetes 70 alimentando un módulo de recepción 72 y un módulo de envío 74. Las diferentes colas son gestionadas por un módulo de gestión de flujos 76.

[0068] Las funciones de los diferentes módulos se detallan a continuación.

[0069] El módulo de intercepción 70 intercepta los paquetes IP entrantes en la red MANET 10 y registra los flujos desconocidos para el módulo de gestión de flujos 76. Los flujos son identificados, por ejemplo, con la tupla de IP de origen / destino y las informaciones complementarias (puertos de origen / destino si están accesibles, campo SPI en caso de cifrado por IP-Sec). Los paquetes pertenecientes a flujos conocidos son transferidos al módulo de recepción 72.

[0070] El módulo de gestión de flujos 76 mantiene la lista de los flujos activos. Para cada nuevo flujo, este módulo crea un tratamiento que se encargará de tratarlo. Este tratamiento está compuesto por módulos de recepción de flujo 72 y de envío 74. El módulo puede efectuar las operaciones siguientes:

- creación de los módulos de recepción de flujo 72 y de envío 74.
- actualización de los módulos “flow reception” y “flow dispatch” (por ejemplo, ajustar un parámetro como el umbral s1 descrito más adelante).
- terminación (por ejemplo, después de un periodo de inactividad).

[0071] Las operaciones de actualización o de terminación son ventajosamente activadas según los estados del sistema, ajenos al procedimiento. Por ejemplo, si el sistema sabe que nuevos recursos de radio van a ser asignados a un destinatario, el módulo de gestión de flujos 76 aumenta la velocidad autorizada λ (véase la

descripción del módulo “flow dispatch” y del mecanismo de back pressure). Este sería el caso de una red de radio cognitiva que reutiliza frecuencias disponibles de manera oportunista o planificada.

[0072] El módulo de recepción de flujo 72 recibe los paquetes del nodo emisor anterior en la cola de espera ooList designada 34 en la Figura 2. Se ocupa de confirmarlos y de verificar que el número de secuencia no sea absurdo (la diferencia entre los números de secuencia de los paquetes de la cola no debe ser superior a un umbral MaxReord, por ejemplo).

[0073] El módulo de envío de flujo 74 pone en práctica el protocolo de transporte salto por salto. Contiene las dos colas de espera outputQ (paquetes en espera de transmisión) y nACKedQ (paquetes en espera de ser confirmados) designadas 38, 40 en la Figura 2. Una vez que los paquetes IP llegan al último nodo de la red MANET, son emitidos en la red local o hacia la aplicación. Para los otros paquetes en tránsito, los paquetes de outputQ 38 son enviados hacia el próximo nodo a la velocidad λ, y luego son colocados en la cola nACKedQ 40 a la espera de ser confirmados.

[0074] Al recibir la confirmación, los paquetes son eliminados de la cola nACKedQ 40. El mecanismo de ventana móvil con confirmaciones selectivas se utiliza para reducir el peso de las confirmaciones (véase la sección “fiabilidad” más adelante). Después de permanecer segundos por encima del RTO (Retransmission Time Out), los paquetes son colocados nuevamente y por orden de prioridad en la cola outputQ para ser retransmitidos. Se autorizan P retransmisiones como máximo. Las congestiones en la cola outputQ son detectadas mediante un umbral s1. Si se supera este umbral, se envía una señal al nodo anterior para que reduzca su velocidad (según el mecanismo de “back pressure” ya expuesto).

[0075] Las colas de espera ooList, outputQ y naCKedQ tienen un tamaño finito. Los nuevos paquetes se pierden cuando las colas están llenas. Se aplica ventajosamente un mecanismo de pérdidas aleatorias (tipo RED – Random Early Detection).

Gestión de la movilidad

[0076] Cuando un nodo intermediario ya no se encuentra en la ruta para un flujo determinado, los paquetes que ha confirmado, pero que todavía no ha enviado pueden perderse si no existe ninguna ruta para el destino.

[0077] El nuevo nodo intermediario registra el flujo como un nuevo flujo.

[0078] El procedimiento según la invención proporciona las ventajas siguientes:

- Transporta paquetes IP de extremo a extremo de manera eficaz.
- Proporciona una solución agnóstica al protocolo de transporte (por ejemplo, UDP, TCP).
- Es compatible con IPSec.
- Utiliza mejor los recursos (control de flujo local y protocolo de transporte adecuado en cada salto).
- Regula la velocidad del tráfico de extremo a extremo mediante “back pressure”.
- Proporciona fiabilidad de transmisión de extremo a extremo con un mecanismo de confirmación salto por salto configurable.
- Se basa en el enrutamiento IP habitual.
- Trata los flujos IP de manera unidireccional.
- Funciona en modo desconectado o “soft state”. Después de un tiempo determinado, si no se procesa ningún paquete, el contexto de memoria vinculado al flujo se destruye. Transporta un flujo de datos evitando las congestiones en los nodos intermediarios y dando fiabilidad parcial a las transmisiones en cada salto. El objetivo del mecanismo es prevenir las congestiones y repeler las pérdidas hacia el primer nodo en caso de congestión, y asegurar una fiabilidad configurable evitando las retransmisiones de extremo a extremo desde la fuente.

REIVINDICACIONES

1. Procedimiento de transmisión de información en una red ad hoc multisalto comprendiendo, la transmisión de un mensaje de un nodo emisor de origen a un nodo de destino final a través de una sucesión de saltos de un nodo emisor a un nodo receptor inmediatamente posterior, en el que se aplica:

a) un mecanismo de gestión de fiabilidad comprendiendo:
- durante la o cada recepción correspondiente en cada salto, de al menos un mensaje por el nodo receptor, el envío de un mensaje de confirmación hacia el único nodo emisor,
- la aplicación de una ley de retransmisión del mensaje en el salto, del nodo emisor al nodo receptor, dicha ley comprende reglas de no retransmisión de mensajes, conduciendo a la no retransmisión del mensaje,

b) un mecanismo de gestión de congestión de los nodos que proporciona una limitación de la velocidad de envío de un nodo emisor a un nodo receptor debido a una información de congestión del nodo receptor enviada al nodo emisor, caracterizado porque el mecanismo de gestión de congestión es aplicado solamente salto por salto, siendo transmitida la información de congestión solamente de un nodo receptor a un nodo emisor en un mismo salto para la limitación de la velocidad del único nodo emisor al único nodo receptor.

2. Procedimiento según la reivindicación 1, caracterizado porque la ley de retransmisión para un nodo emisor tiene en cuenta, para las reglas de no retransmisión, variables vinculadas a los nodos de los saltos anteriores entre el nodo emisor de origen y el nodo emisor.

3. Procedimiento según la reivindicación 2, caracterizado porque la ley de retransmisión para un nodo emisor tiene en cuenta, para las reglas de no retransmisión, el número de nodos ya recorridos por saltos sucesivos desde el nodo emisor de origen.

4. Procedimiento según cualquiera de las reivindicaciones anteriores, caracterizado porque comprende una etapa de marcado del tipo de información contenida en el mensaje y porque la ley de retransmisión tiene en cuenta, para las reglas de no retransmisión, el tipo de información contenida en el mensaje.

5. Procedimiento según cualquiera de las reivindicaciones anteriores, caracterizado porque el envío de un mensaje de confirmación tiene lugar solamente durante la recepción correspondiente de un conjunto de varios mensajes.

6. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado porque el mecanismo de gestión de las congestiones aplica, para el cálculo de la velocidad del nodo emisor, una ley de aumento aditivo y de disminución multiplicativa.

7. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado porque el mecanismo de gestión de congestión implementa una no transmisión definitiva de ciertos mensajes del nodo emisor hacia el nodo receptor en caso de congestión del nodo receptor.

8. Procedimiento según la reivindicación 7, caracterizado porque la no transmisión de los mensajes es aplicada a los mensajes habiendo recorrido el menor número de saltos hasta el nodo emisor y / o los mensajes con la menor probabilidad de llegar al nodo receptor final.

9. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que las informaciones contenidas en los mensajes transmitidos son informaciones formateadas para una transmisión en una red según el Protocolo IP y porque los mensajes transmitidos comprenden, además de la información de los formatos IP, un encabezado correspondiente para asegurar los mecanismos de gestión de la fiabilidad y de gestión de la congestión.

10. Procedimiento según la reivindicación 9, caracterizado porque el encabezado comprende una información representativa del protocolo transportado.

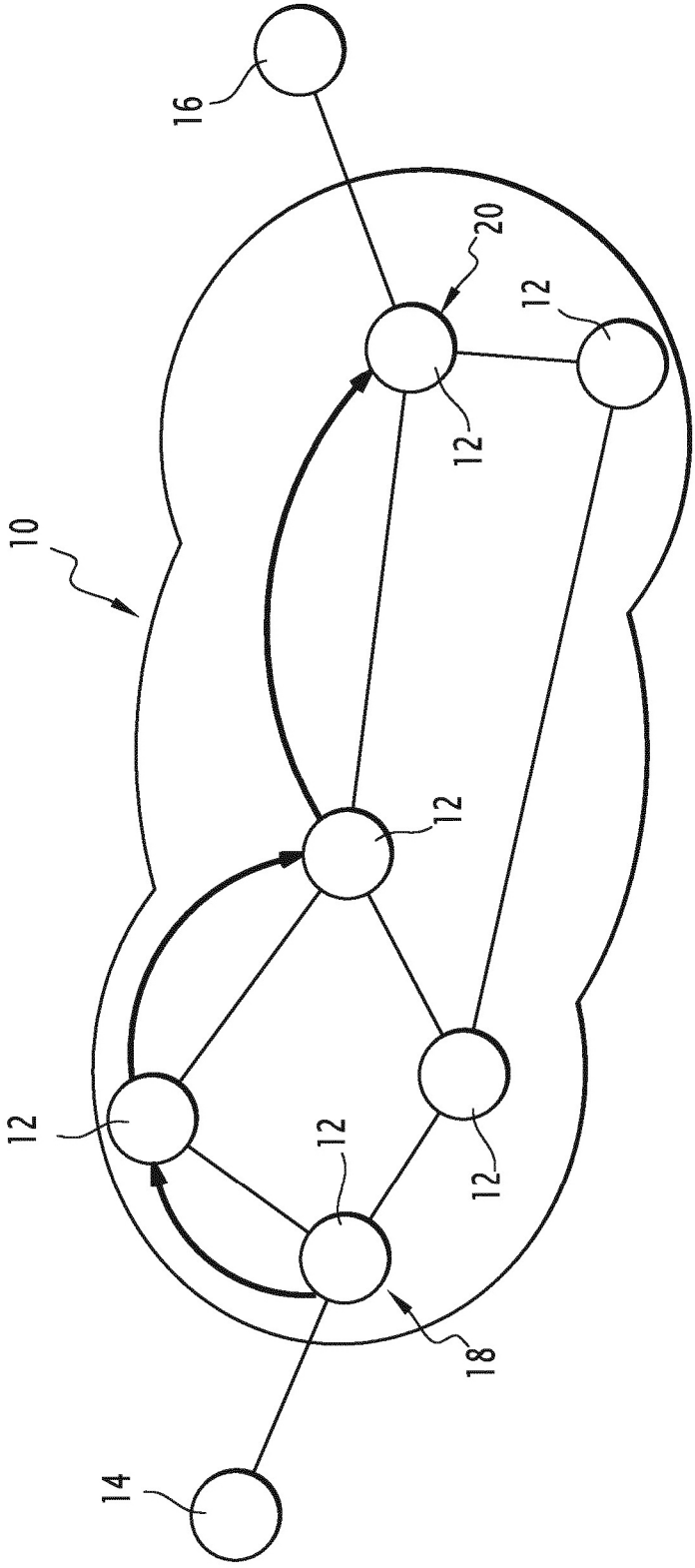

FIG.1

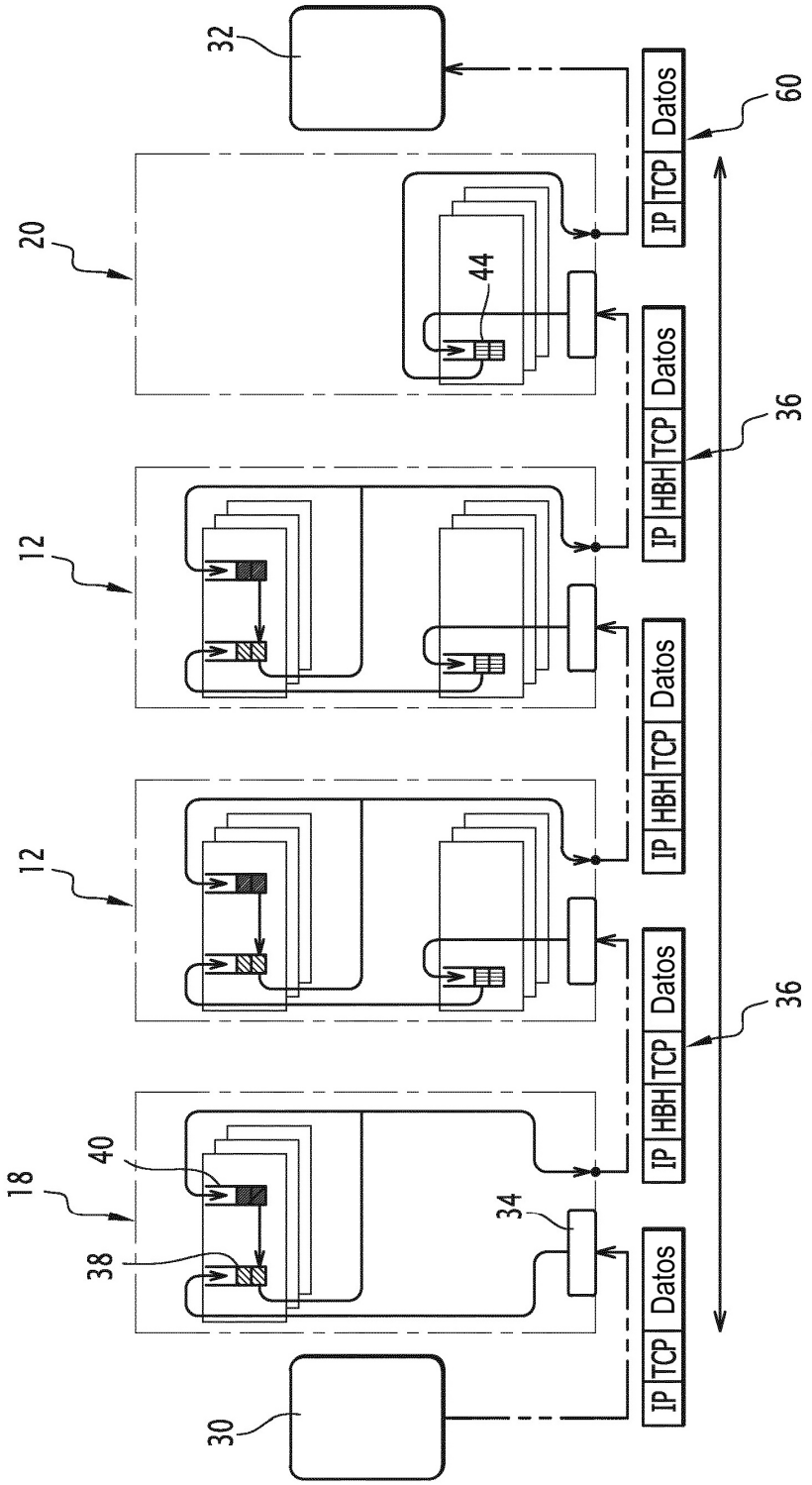
32
20
44
12
12
18
40
38
34
30
IP TCP Datos
IP HBH TCP Datos
IP HBH TCP Datos
IP HBH TCP Datos
IP TCP Datos
60
36
36

FIG.2

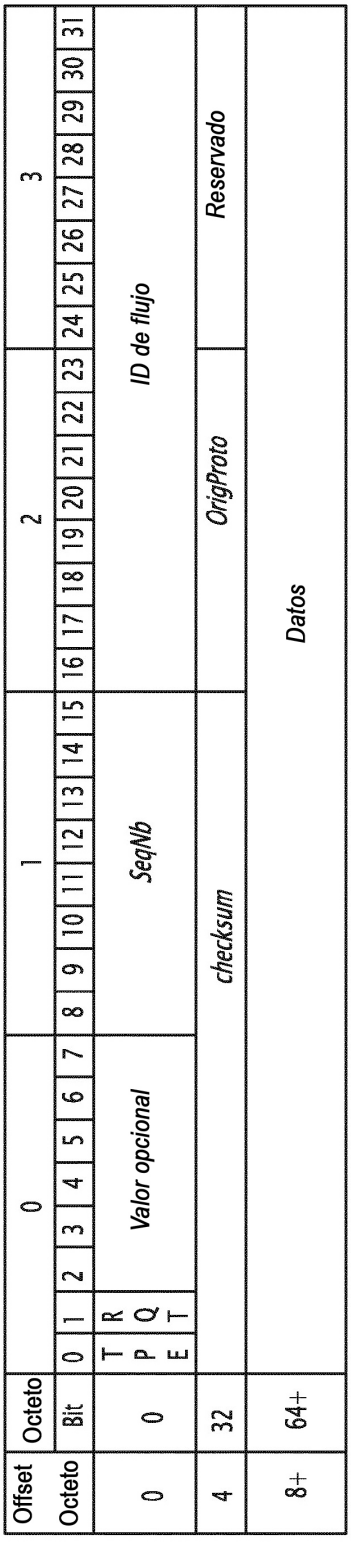
Offset
Octeto
Octeto
Bit
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
0
0
T
E
P
R
Q
T
Valor opcional
SeqNb
ID de flujo
4
32
checksum
OrigProto
Reservado
8+
64+
Datos

FIG.3

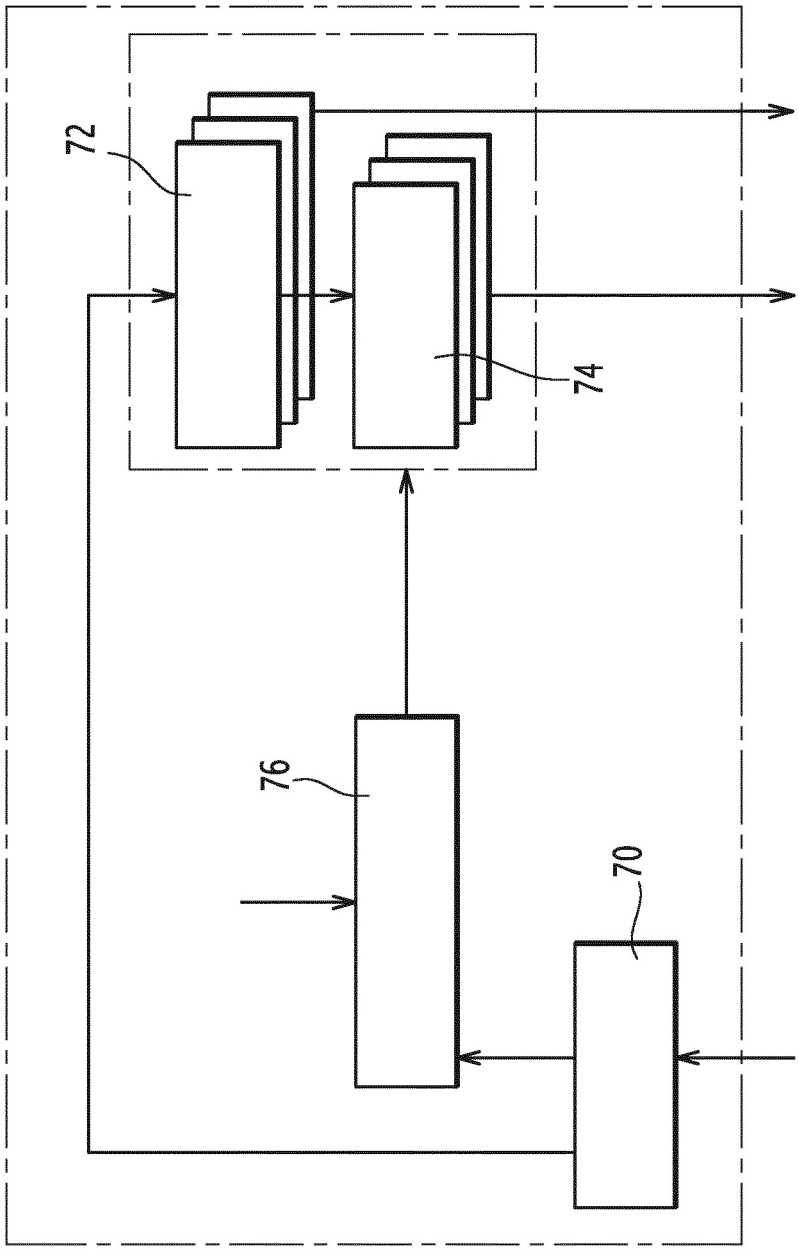

FIG.4