(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 390 902**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
G05B 19/418 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06847245 .5**
(96) Fecha de presentación: **06.10.2006**
(97) Número de publicación de la solicitud: **2070288**
(97) Fecha de publicación de la solicitud: **17.06.2009**

(54) Título: **Procedimiento para elegir nodos agregadores en una red**

(45) Fecha de publicación de la mención BOPI:
19.11.2012

(45) Fecha de la publicación del folleto de la patente:
19.11.2012

(73) Titular/es:
NEC CORPORATION (100.0%)
7-1, Shiba 5-chome Minato-ku
Tokyo 108-8001, JP

(72) Inventor/es:
WESTHOFF, DIRK y
ARMKNECHT, FREDERIK

(74) Agente/Representante:
ROEB DÍAZ-ÁLVAREZ, María

DESCRIPCIÓN

Procedimiento para elegir nodos agregadores en una red.

La presente invención se refiere a un procedimiento para elegir nodos agregadores en una red, en el que la red comprende una pluralidad de nodos sensores para medir datos, y en el que al menos uno de los nodos sensores funciona como nodo agregador para agregar datos detectados obtenidos por al menos un subconjunto de los nodos sensores, y en el que la red comprende además al menos un nodo recolector para recoger datos agregados por los nodos agregadores.

Los procedimientos según se mencionan anteriormente son bien conocidos en la práctica y son de especial importancia en el contexto de redes de sensores inalámbricas (WSN). Las WSN son redes ad hoc, compuestas por pequeños sensores con capacidades limitadas de cómputo y energía.

Todos los sensores de una red de sensores son nodos sensores que se comunican de forma inalámbrica y que consisten en general en una sonda, una unidad de procesamiento, un dispositivo de comunicación y una batería. Los nodos sensores comprenden la funcionalidad de adquisición de datos, comunicaciones y cómputo en un mínimo de espacio. Debido a sus capacidades limitadas, los nodos sensores, en general, no comprenden una unidad resistente a la alteración.

Las redes de sensores inalámbricas están adquiriendo una popularidad creciente en muchos ámbitos de la vida. A modo de ejemplos en los que se usan redes de sensores deben mencionarse la monitorización y el control de máquinas, el control de parámetros de salud (intra y extracorporales) o la monitorización del ambiente (como temperatura, humedad y actividad sísmica). Sin embargo, la gama de posibilidades de aplicación para redes de sensores es casi infinita. En campos concretos, como el análisis de la contaminación del agua o la predicción meteorológica, por ejemplo, es extremadamente ventajoso que los nodos sensores puedan realizarse en tamaño en miniatura y que sea posible fijarlos y usarlos fácilmente en regiones de difícil acceso.

Los parámetros críticos que limitan en ciertas circunstancias las posibilidades de aplicación de redes de sensores son en particular factores definidos físicamente de los nodos sensores individuales, como, por ejemplo, el alcance de su emisor, la potencia del procesador, la capacidad de la batería, el espacio de almacenamiento existente y similares. Dado que los nodos sensores individuales, a diferencia del nodo recolector en el que los datos detectados llegan juntos, están limitados físicamente en muchos sentidos, la organización eficiente energéticamente de la red de sensores es de excepcional importancia. En este contexto primero ha de indicarse que la transmisión de todos los datos detectados al nodo recolector provocaría un tráfico de datos excesivo, con lo que comúnmente los datos se acumulan primero en la red en nodos sensores especiales, que funcionan como los llamados nodos agregadores. El envío de todos los datos detectados a su destino final daría como resultado un tiempo de vida que sería inaceptablemente breve, dado que el consumo de energía de los dispositivos, es decir, los nodos sensores, durante el envío aumenta de forma lineal con la cantidad de datos para enviar.

En general, el tiempo de vida de las redes de sensores inalámbricas se divide en épocas, donde cada época tiene una duración específica. Un nodo agregador se elige comúnmente para la duración de una época durante la cual recibe datos de otros nodos sensores, realiza procesamiento en red de dichos datos y remite los datos resultantes. Para la siguiente época se elige un nuevo nodo sensor como nodo agregador.

Un objetivo importante del mecanismo de elección de nodos agregadores es repartir de forma equilibrada los recursos de energía restantes de los nodos sensores individuales de la red. En consecuencia, los nodos sensores con mayores recursos de energía restante deben elegirse preferentemente para la siguiente época dentro de la WSN.

Por otra parte, con respecto al comportamiento malicioso es importante tener en cuenta que existen varias razones de peso para realizar acciones fraudulentas con los nodos sensores durante el procedimiento de elección de un agregador. Las motivaciones para las acciones fraudulentas pueden ser dobles: por una parte, los nodos sensores pueden tener interés en no convertirse en nodo agregador ya que no quieren desperdiciar su energía restante. Por otra parte, los nodos sensores pueden tener el interés contrario, es decir, un interés en convertirse en nodo agregador, ya que pretenden escrutar el mayor número de datos posible.

En el documento de J.N. Al-Karaki y col.: “Routing Techniques in Wireless Sensor Networks: A Survey”, IEEE Wireless Communications, Volumen 11, publicación 6 de diciembre de 2004, páginas 6-28 se desvela un procedimiento para elegir nodos agregadores en redes de sensores inalámbricas. Más concretamente, el documento describe el protocolo conocido comúnmente como Jerarquía de Agrupación Adaptativa de Baja Energía (LEACH, *Low Energy Adaptive Clustering Hierarchy*), para selección de agregadores en Redes de Sensores Inalámbricas. LEACH es un protocolo basado en grupos, que incluye formación de grupos distribuidos. LEACH selecciona

aleatoriamente algunos nodos sensores como cabezas de grupo (CH) y reparte de forma rotatoria esta función para distribuir uniformemente la carga de energía entre los sensores de la red. Después de un intervalo de tiempo dado, la rotación aleatorizada de la función de CH se realiza de manera que se obtiene una disipación de energía uniforme en la red de sensores.

Un objeto de la presente invención es mejorar y desarrollar adicionalmente un procedimiento del tipo descrito inicialmente para elegir nodos agregadores en una red de tal manera que el procedimiento de elección de nodos agregadores sea seguro, de confianza y equitativo en el sentido de que no se permite que un nodo sensor individual manipule el procedimiento de elección en ninguna dirección.

De acuerdo con la invención, el objeto mencionado anteriormente se alcanza mediante un procedimiento que comprende la característica de la reivindicación 1. Según esta reivindicación, dicho procedimiento se caracteriza por:

el establecimiento de claves secretas por pares entre un nodo agregador actual y cada nodo sensor del subconjunto de nodos sensores del cual el nodo agregador actual obtiene los datos detectados;

en cada uno de los nodos sensores de dicho subconjunto, la elección de un número aleatorio y la encriptación del número aleatorio usando la clave establecida;

el suministro de una cadena de comunicación entre los nodos sensores de dicho subconjunto y la suma de los números aleatorios encriptados de todos los nodos sensores de dicho subconjunto; y

la determinación de un nuevo nodo agregador sobre la base de la suma resultante según un esquema de cálculo predefinido.

De acuerdo con la invención se ha reconocido primero que cualquier manipulación, con independencia de cuál sea el motivo concreto de las intenciones fraudulentas de un nodo sensor, puede prevenirse cuando los procedimientos de elección en su conjunto se realizan de una forma totalmente aleatorizada. Por otra parte, se ha encontrado que un procedimiento de elección robusto de nodos de agregación con respecto a nodos sensores con intenciones fraudulentas es aquel en el que la intervención del nodo sensor en el procedimiento de decisión es de la misma calidad que la intervención de cualquier otro nodo sensor implicado. De acuerdo con la invención, el procedimiento de elección no se basa en ninguna métrica de elección en concreto y los atacantes no pueden suministrar valores aprovechables en el procedimiento de decisión con el fin de influir en la elección del nodo agregador de una manera controlada.

En lo que respecta al acuerdo de clave entre el nodo agregador actual y cada nodo sensor del subconjunto de nodos sensores del cual el nodo agregador actual obtiene datos de sensores, el nodo agregador actual puede difundir una multitud de pares de datos, comprendiendo cada par de datos una clave k_i y un identificador ID_i, respectivamente, de una manera oculta para todos los nodos sensores de este subconjunto. Cada nodo sensor del subconjunto puede elegir aleatoriamente a continuación un par de datos a partir de la multitud de pares de datos y romper la ocultación para obtener la clave k_i. Este procedimiento, que se conoce, como puede apreciarse por sí mismo, como Cifrado de Merkle, permite el establecimiento de claves secretas por pares entre el nodo agregador y cada nodo sensor, es decir, los nodos sensores desconocen de por sí las claves del acuerdo entre otros nodos sensores.

La ocultación de los pares de datos difundidos puede conseguirse por medio de una encriptación. Para conseguir un bajo esfuerzo de cómputo de cara a que los nodos sensores rompan la encriptación es ventajoso escoger una encriptación ligera. En concreto, sería posible usar un cifrado de bloques débil, por ejemplo RC5.

Como el envío de datos es una operación muy costosa, el número de pares de datos difundidos por el nodo agregador actual se especifica, en una manera ventajosa, según requisitos de seguridad dados. En concreto, si se espera que los atacantes tengan posibilidades más bien bajas es suficiente difundir menos pares de datos de lo que podría ser necesario en el caso de un atacante potencial y más poderoso. Suponiendo que pudiera disponerse de la tasa de eficacia de un atacante frente a los nodos sensores puede medirse de forma exacta un nivel de seguridad y puede determinarse exactamente el número requerido de pares de datos difundidos (así como la fuerza de la encriptación aplicada).

Como última etapa en el contexto del acuerdo de clave puede proporcionarse que cada nodo sensor difunda el identificador de su par de datos elegido. El identificador difundido puede servir como un compromiso de manera que cada nodo sensor tenga capacidad para verificar si los otros nodos sensores actúan de manera conforme.

En lo que respecta al procedimiento de suma, es posible que se defina un cierto orden de los nodos sensores dentro de la cadena de comunicación. Por ejemplo, puede determinarse un orden según la distancia de los nodos sensores al nodo agregador actual. Este procedimiento podría realizarse de acuerdo con un protocolo predefinido.

Alternativamente, el orden podría determinarse dinámicamente o según los ID de los nodos sensores. Según una alternativa adicional, el orden se determina simplemente en la parte del nodo agregador actual, aunque, en la parte del nodo agregador actual, este procedimiento permite un cierto ejercicio de influencia en el procedimiento de elección.

En una forma especialmente ventajosa, el esquema de encriptación E usado para encriptar los números aleatorios r_i según las claves k_i es homomórfico tanto con respecto a los números aleatorios r_i como a la clave k_i. Esto significa que:

$$E(k, r) + E(k', r') = E(k + k', r + r').$$

En concreto, podría emplearse un esquema de encriptación homomórfico según proponen C. Castelluccia, E. Mykletun y G. Tsudik en "Efficient Aggregation of encrypted data in Wireless Sensor Networks".

Con el fin de proporcionar a cada nodo sensor la posibilidad de verificar que el procedimiento de elección del nodo agregador ha sido efectuado correctamente y que ni el nodo agregador actual ni ningún otro nodo sensor ha cometido acciones fraudulentas, el nodo agregador actual puede revelar todas las claves establecidas después de que se complete la suma de los números aleatorios encriptados. Cuando las claves establecidas son difundidas por el nodo agregador actual, en primer lugar cada sensor puede verificar si su propia clave establecida reside entre las claves difundidas. Además, podría exigirse que el agregador revelara también que la clave se corresponde con el par oculto difundido al principio. Así se evitaría la colaboración del agregador con un nodo malicioso para introducir nuevas claves después de que se termine la fase del acuerdo de clave. En segundo lugar, cada nodo sensor puede sumar las claves establecidas y aplicar la suma resultante como una clave para desencriptar la suma de los valores aleatorios encriptados. Esta operación es posible debido a la doble característica homomórfica del esquema de encriptación empleado. Sobre la base del resultado del desencriptado puede determinarse el nuevo nodo agregador.

En lo que se refiere a una mayor prevención frente a acciones fraudulentas, puede definirse un intervalo de tiempo Δt para proporcionar el intervalo de tiempo máximo permitido entre el momento de la difusión de los pares de datos por el nodo agregador actual y el momento de la difusión de las claves establecidas. Esta característica tiene en cuenta que el nodo agregador actual sólo puede realizar acciones fraudulentas de una forma significativa si es conocedor de la suma encriptada final de los valores aleatorios de todos los nodos sensores implicados. Mediante la preconfiguración de Δt según se especifica anteriormente es posible restringir claramente el tiempo que queda para que el nodo agregador actual pueda realizar acciones fraudulentas modificando las claves de una forma significativa.

Para evitar cualquier colaboración entre el nodo agregador actual y uno de los nodos sensores puede proporcionarse que el procedimiento de elección sea cancelado y reiniciado desde el principio si al menos un nodo sensor registra alguna irregularidad. Por ejemplo, puede realizarse una cancelación y reinicio del procedimiento de elección si uno de los nodos sensores registra que el nodo agregador actual difunde algo más que las claves establecidas reales.

Existen varias maneras de diseñar y desarrollar adicionalmente la enseñanza de la presente invención de una forma ventajosa. Para este fin, es preciso referirse, por una parte, a las reivindicaciones de patente subordinadas a la reivindicación de patente 1 y, por otra parte, a la siguiente explicación de un ejemplo preferido de una forma de realización de la invención ilustrada por la figura. En relación con la explicación del ejemplo preferido de una forma de realización de la invención con ayuda de la figura, se explicarán en general formas de realización preferidas y desarrollos adicionales de la enseñanza.

En los dibujos:

La única FIG. es una vista esquemática de una forma de realización de un escenario de aplicación de un procedimiento según la invención para elegir nodos agregadores en una red.

En referencia más en particular a los dibujos, la única FIG. representa un escenario de aplicación de un procedimiento según la invención. La FIG. muestra, en forma de esquema, una red de sensores 1 con una multitud de nodos sensores que están etiquetados según su número de S_1 a S_n. Los datos detectados por los nodos sensores S_1 a S_n son agregados por un nodo agregador A_t. Comúnmente, a petición de un nodo recolector 2 (es decir, a diferencia de los nodos sensores S_i y el nodo agregador A_t, un dispositivo específico con recursos físicos suficientemente extensos), el nodo agregador A_t remite los datos agregados al nodo recolector 2. Para mayor claridad, en la FIG. sólo se muestra un único nodo agregador A_t y no existen nodos intermedios entre A_t y el nodo recolector 2.

La red de sensores 1 se muestra en el estado de una época t en la que el nodo sensor etiquetado como A_t funciona como nodo agregador. Al comienzo de la siguiente época t+1 se inicia un protocolo para elegir aleatoriamente uno

de los nodos sensores S_1 a S_n como el siguiente nodo agregador A_{t+1}. El procedimiento de elección del nodo agregador, en principio, puede diferenciarse en tres fases:

La primera fase es la fase del acuerdo de clave. El objetivo de esta fase es establecer claves secretas por pares entre el nodo agregador actual A_t y cada nodo sensor S_i. Para este fin, el nodo agregador A_t aplica el denominado Cifrado de Merkle para establecer claves por pares k_i con cada uno de los nodos sensores S_1, ..., S_n. Durante este procedimiento, cada nodo sensor S_i difunde un identificador ID_i conectado con su clave k_i que puede usarse como un compromiso con esta clave posteriormente si se necesita. Dado que el procedimiento de elección del agregador dura sólo un breve intervalo de tiempo bien definido, sólo es preciso mantener la seguridad proporcionada por el Cifrado de Merkle durante este tiempo. En la FIG. el acuerdo de clave está indicado por las líneas de puntos con flechas en los dos extremos de las mismas.

Después de que se haya completado el acuerdo de clave se lleva a cabo una segunda fase del procedimiento de elección del nodo agregador. El objetivo de esta segunda fase es calcular de forma segura la suma de la contribución de los sensores al procedimiento de elección. Seguro significa en el presente documento que ningún nodo ve la contribución de cualquier otro nodo antes de que se haya completado el cómputo de la suma, lo que evita que cualquiera con intenciones fraudulentas pueda influir en el resultado de una forma controlada.

Cada nodo sensor S_i elige su contribución aleatoria r_i al procedimiento de elección y la encripta con E y k_i. E(k, r) denota la encriptación de r según una clave k mediante un esquema de encriptación E que es homomórfico en k y r. Esto significa que:

$$E(k, r) + E(k', r') = E(k + k', r + r').$$

Cada nodo sensor S_i combina el resultado con la contribución aleatoria encriptada que proviene de otros nodos sensores S_i. Más exactamente, se proporciona una cadena de comunicación entre los nodos, es decir, S_1 se comunica con S_2, S_2 con S_3, y así sucesivamente. En concreto, cuando S_i recibe

$$SUM_{i-1} = E(k_1 + ... + k_{i-1}, r_1 + ... + r_{i-1}),$$

calcula

$$SUM_i = E(k_i, r_i) + SUM_{i-1} = E(k_1 + ... + k_i, r_1 + ... + r_i),$$

empezando en S_1 con $SUM_1 = E(k_1, r_1)$. Posteriormente S_i remite SUM_i a S_{i+1}. El procedimiento termina cuando todos los nodos n han contribuido a la suma encriptada de las contribuciones.

Ningún nodo sensor S_i puede realizar acciones fraudulentas de una forma significativa, ya que no puede prever el impacto de su propio valor aleatorio r_i en el resultado final $R = r_1 + ... + r_n$ sin conocer las contribuciones de los otros nodos sensores S_i, lo cual requeriría el conocimiento de sus claves.

El procedimiento de elección del nodo agregador termina con una tercera fase. En esta fase el nodo agregador real A_t difunde las claves reales a todos los nodos sensores S_i. Cada S_i desencripta SUM_n calculando $k = k_1 + ... + k_n$ y el desencriptado

$$D(k, SUM_n) = R = r_1 + ... + r_n.$$

El nodo sensor S_i para el cual se cumple que $i = R \ mod \ n$ se determina como nuevo nodo agregador A_{t+1}.

Al experto en la materia al que se dirige la invención que tiene la ventaja de las enseñanzas presentadas en la descripción anterior y los dibujos asociados le vendrán a la mente muchas modificaciones y otras formas de realización de la invención expuesta en la presente memoria descriptiva. Por tanto, debe entenderse que la invención no está limitada a las formas de realización específicas desveladas y que se pretende incluir las modificaciones y otras formas de realización dentro del ámbito de las reivindicaciones adjuntas. Aunque en la presente memoria descriptiva se emplean términos específicos, se usan sólo en un sentido genérico y descriptivo y no con el fin de limitarla.

REIVINDICACIONES

1. Un procedimiento para elegir nodos agregadores en una red, en el que la red (1) comprende una pluralidad de nodos sensores (S_i) para medir datos, y en el que al menos uno de los nodos sensores (S_i) funciona como nodo agregador (A) para agregar datos detectados obtenidos por al menos un subconjunto de los nodos sensores (S_i), y en el que la red comprende además al menos un nodo recolector (2) para recoger datos agregados por los nodos agregadores (A), comprendiendo el procedimiento:

el establecimiento de claves secretas por pares (k_i) entre un nodo agregador actual (A_t) y cada nodo sensor (S_i) del subconjunto de nodos sensores a partir del cual el nodo agregador actual (A_t) obtiene datos detectados;

en cada uno de los nodos sensores (S_i) de dicho subconjunto, la elección de un número aleatorio (r_i) y la encriptación del número aleatorio (r_i) usando la clave establecida (k_i);

el suministro de una cadena de comunicación entre los nodos sensores (S_i) de dicho subconjunto y la suma de los números aleatorios encriptados (r_i) de todos los nodos sensores (S_i) de dicho subconjunto; y

la determinación de un nuevo nodo agregador (A_{t+1}) sobre la base de la suma resultante según un esquema de cálculo predefinido.

2. El procedimiento según la reivindicación 1 , en el que el nodo agregador actual (A_t), en el contexto del acuerdo de clave, difunde una multitud de pares de datos, comprendiendo cada par de datos una clave (k_i) y un identificador (ID_i), respectivamente, de una manera oculta para todos los nodos sensores (S_i) de dicho subconjunto.

3. El procedimiento según la reivindicación 2, en el que cada nodo sensor (S_i) de dicho subconjunto elige aleatoriamente un par de datos entre la multitud de pares de datos y rompe la ocultación para obtener la clave (k_i).

4. El procedimiento según la reivindicación 2 o 3, en el que la ocultación de los pares de datos difundidos se obtiene por medio de una encriptación ligera.

5. El procedimiento según la reivindicación 4, en el que los pares de datos difundidos están encriptados con un cifrado de bloques débil o usando una clave corta.

6. El procedimiento según cualquiera de las reivindicaciones 2 a 5, en el que el número de pares de datos difundidos por el nodo agregador actual (A_t) se especifica según requisitos de seguridad dados.

7. El procedimiento según cualquiera de las reivindicaciones 2 a 6, en el que cada nodo sensor (S_i) difunde el identificador (ID_i) de su par de datos elegido como un compromiso.

8. El procedimiento según cualquiera de las reivindicaciones anteriores, en el que el orden de los nodos sensores ($S_|$) dentro de la cadena de comunicación está determinado según una regla bien definida.

9. El procedimiento según cualquiera de las reivindicaciones anteriores, en el que el esquema de encriptación E usado para encriptar los números aleatorios (r_i) según las claves (k_i) es homomórfico con respecto a los números aleatorios (r_i) y a las claves (k_i).

10. El procedimiento según la reivindicación 9, en el que, después de completar la suma de los números aleatorios encriptados (r_i), el nodo agregador actual (A_t) difunde las claves establecidas (k_i) a todos los nodos sensores (S_i) de dicho subconjunto.

11. El procedimiento según la reivindicación 9 o 10, en el que cada nodo sensor (S_i) de dicho subconjunto suma las claves establecidas (k_i) y aplica la suma resultante (k) para desencriptar la suma de los valores aleatorios encriptados (r_i).

12. El procedimiento según cualquiera de las reivindicaciones anteriores, en el que el nodo sensor (S_i) de dicho subconjunto para el que se cumple que i = R *mod n*, con R denotando la suma de los valores aleatorios (r_i), está determinado como nuevo nodo agregador (A_{t+1}).

13. El procedimiento según cualquiera de las reivindicaciones 10 a 12, en el que se define un tiempo permitido máximo Δt entre el momento de la difusión de los pares de datos y el momento de la difusión de las claves establecidas (k_i).

14. El procedimiento según cualquiera de las reivindicaciones anteriores, en el que el procedimiento de

elección se cancela y vuelve a iniciarse desde el principio si al menos un nodo sensor (S_i) registra alguna irregularidad.

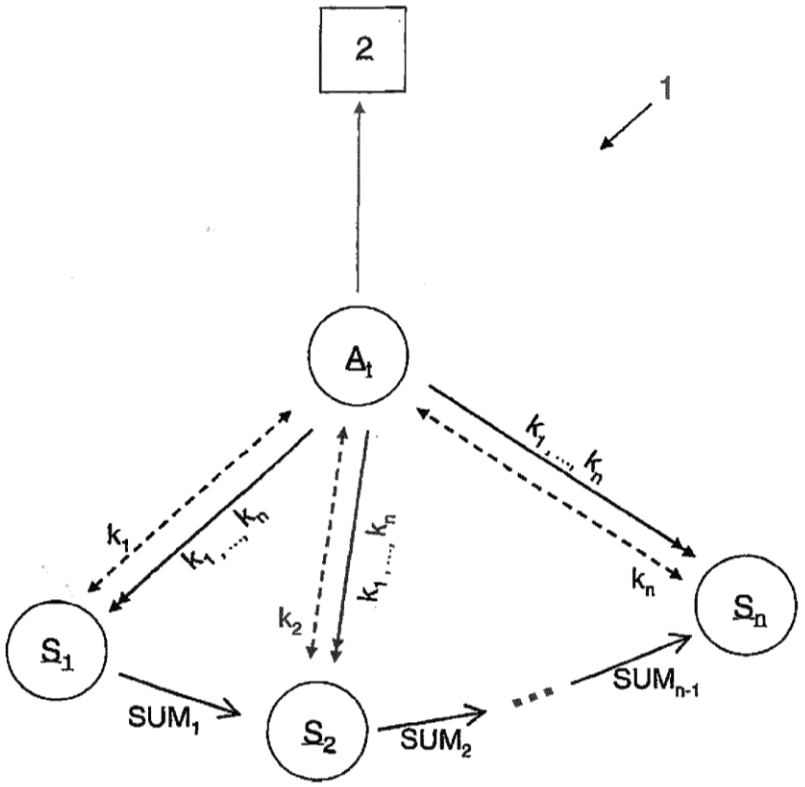

Fig.