(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 908 482**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.04.2018 E 18000330 (3)**

(97) Fecha y número de publicación de la concesión europea: **16.02.2022 EP 3389238**

(54) Título: **Método para proteger un sistema militar conectado en red**

(30) Prioridad:

12.04.2017 DE 102017003585
12.07.2017 DE 102017006572

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.04.2022

(73) Titular/es:

DIEHL DEFENCE GMBH & CO. KG (100.0%)
Alte Nußdorfer Strasse 13
88662 ÜBERLINGEN, DE

(72) Inventor/es:

GAGEL, FLORIAN;
SELZ, ANDRE;
KOLTES, ANDREAS y
KUSHAUER, JÖRG

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método para proteger un sistema militar conectado en red

La invención se refiere a un método para proteger un sistema militar conectado en red frente a participantes maliciosos, en el que las transacciones entre participantes del sistema militar conectado en red son almacenadas en una base de datos distribuida.

En un sistema militar conectado en red están implicados muchos actores, entre otros, por ejemplo, observadores, reconocedores, sensores (por ejemplo, radar), efectores, tropas en acción, agentes, centrales de control y de mando. Todos estos actores representan participantes del sistema militar conectado en red.

Dentro de un sistema militar conectado en red de este tipo tienen lugar diferentes transacciones entre los participantes, comenzando, por ejemplo, con la identificación y verificación de los participantes respectivos entre sí, intercambio de informaciones sobre amenazas y objetivo, emisión de órdenes a través del plano jerárquico para combatir al enemigo por medio de efectores y evaluación siguiente de los daños.

Se conoce proteger sistemas militares conectados en red para protección contra participantes maliciosos, llamados también intrusos, por medio de dispositivos físicos o diseñar tal sistema de forma redundante, para que en el caso de un fallo, se pueda adoptar un sistema de sustitución.

La utilización de la tecnología de la cadena de bloques en un sistema militar conectado en red para la protección de participantes maliciosos se describe en: Neil B Barnas: "Blockchains in national defense: Trustworthy systems in a trustless world", JPME-Papers, Joint Chief of Staff, US-Army, https://www.jcs.mil/Doctrine/Joint-Education/JPME-Papers.

Se conoce otra representación de la utilización de tecnología de cadena de bloques en el campo militar a partir de: Duncan Riley: "DARPA wants someone to build the DoD a new secure Blockchain based messaging platform" siliconangle [the voice of enterprise and emerging tech], https://siliconangle.com/2016/04/25/darpa-wants-someone-to-build-the-dod-a-new-secure-blockchainbased-messaging-platform.

Un cometido de la invención es indicar un método para proteger sistemas militares conectados en red frente a un participante malicioso, que ha conseguido convertirse en un participante del sistema, especialmente a través de mecanismos físicos de seguridad existentes.

Este cometido se soluciona por medio de un método según las características de la reivindicación 1 de la patente, en el que las transacciones se almacenan en bloques y solamente participantes representados en un bloque de base y participantes nuevos autorizados pueden generar tales bloques de datos, siendo autorizado un participante no autorizado todavía en la red como participante nuevo en la red cuando un participante autorizado para recepción nueva y representado como tal en un bloque de base autoriza el nuevo participante.

La invención parte de la consideración de que muchas transacciones entre los participantes presuponen una autentificación de los participantes implicados, así como un protocolo exacto de las transacciones con objeto de la posibilidad de reproducción.

La invención parte, además, de la consideración de que, por razones de robustez frente a acciones enemigas, los sistemas descentralizados son ventajosos, puesto que esto permite también un fallo de una parte del sistema militar completo conectado en red, sin que se pierda con ello la funcionalidad general o bien se ponga en peligro la operación realizada o a realizar.

La invención reconoce que un inconveniente de los sistemas distribuidos es la confianza de los participantes entre sí, puesto que también hay que contar con que intrusos / saboteadores se han convertido en participantes individuales y de esta manera pueden funcionar como participantes maliciosos. Tal participante malintencionado puede provocar hasta ahora tanto transacciones nocivas como también puede falsificar posteriormente el protocolo de las transacciones, en el caso de un acceso correspondiente.

Para solucionar este problema se conoce almacenar transacciones de categorías predeterminadas, en particular todas las transacciones de tal red descentralizada, es decir, del sistema militar conectado en red, en una base de datos distribuida. Tal base de datos distribuida se designa a continuación también como "cadena de bloques".

A este respecto, se almacena la base de datos en varios participantes. En este caso, toda la base de datos puede estar almacenada en todos o en algunos participantes. A este respecto, es conveniente que pueda ser visualizada por un grupo predeterminado de participantes, especialmente por todos los participantes. De esta manera, los participantes pueden completar transacciones anteriores a través del acceso a la base de datos o pueden verificar transacciones nuevas con la ayuda de transacciones anteriores.

Otra posibilidad consiste en que la base de datos esté distribuida en varios participantes, es decir, que no esté depositada totalmente en cada participante, sino en algunos participantes al menos en partes. También en este caso la base de datos debería poder ser llamada por los participantes a través de acceso a las partes.

La invención se puede aplicar con ventaja para todos los participantes concebibles de un sistema militar conectado en red, también personas y vehículos, especialmente aviones y/o vehículos acuáticos. Los participantes pueden ser una o varias instalaciones de procesamiento de datos en un edificio, aparatos de comunicación móviles, como Smart Phones u otros aparatos manuales basados en ordenador, misiles, balas y/o armas. A continuación, los participantes deseados o bien correctos del sistema militar conectado en red, designados también como red, se designan como "participantes" o también como participantes autorizados u homologados, y los participantes maliciosos se designan como "intrusos" o "participantes maliciosos".

La invención se puede aplicar de una manera especialmente ventajosa en un sistema de defensa aérea. Este sistema puede comprender como participante un Centro Táctico de Operaciones (TOC), al menos un sistema sensor para la supervisión aérea – por ejemplo, un sistema de radar – y al menos un sistema efector, como por ejemplo una lanzadera para el lanzamiento de misiles tierra-aire, un sistema láser de alta energía o un sistema efector basado en artillería, para la defensa de amenazas, por ejemplo, misiles. Una interferencia de tal sistema militar puede contrarrestarse para que se alcance una defensa aérea fiable.

Una transacción puede ser información intercambiada entre dos participantes de la red. En particular, cualquier información intercambiada entre dos participantes de la red es una transacción. En las transacciones se puede tratar, por ejemplo, especialmente del registro de un participante nuevo, una autorización de un participante o una transmisión de derechos tal vez de una central de mando a otra central de mando. De manera más ventajosa, con la ayuda de las transacciones almacenadas se puede verificar y realizar en cualquier momento acciones de categorías predeterminadas dentro de la red, es decir, dentro del sistema militar conectado en red, especialmente todas las acciones, por todos los participantes – en este caso se presupone el acceso intacto a la red.

En particular, las transacciones comprenden al menos información del grupo de:

- datos de movimiento detectados por un sistema sensor de amenazas, como por ejemplo misiles, los llamados datos de seguimiento,
- disparos o instrucciones de fuego,
- identificación de amenazadas como objetos voladores, especialmente aviones o misiles,
- asignación de un objetivo a un sistema efector, por ejemplo, una lanzadera,
- datos de registros de participantes en la red,
- estados de participantes,
- lugares geográficos de participantes,
- reglas de la red.

De manera más conveniente, se verifica la integridad de la base de datos distribuida por medio de algoritmos predeterminados por los participantes. De esta manera, se asegura contra manipulaciones de participantes individuales maliciosos. Tal manipulación conduciría a la identificación inmediata de un intruso y a la exclusión de uno o de varios componentes del sistema conectados con él, sin que, sin embargo, se limite el sistema principal distribuido o bien la red con participantes de esta manera en su operación.

Una posibilidad para tal algoritmo de verificación contiene que las transacciones son almacenadas en bloques sucesivos yuxtapuestos. Su contenido está de manera más conveniente conectado en red entre sí. La conexión en red se puede realizar de tal forma que en un bloque se almacena un código de prueba formado por al menos un bloque precedente. El código de prueba puede ser una suma de prueba. El código de prueba se puede calcular por medio de la función Hash, de manera que en el bloque está depositado un valor de Hash de las informaciones de al menos un bloque precedente. Tal yuxtaposición de bloques de datos se conoce a partir de la Tecnología de Cadena de Bloques.

En este caso, se puede establecer como regla en la red que una transacción se considera como verdadera entre los participantes cuando la transacción está almacenada en un bloque y el bloque está colgado en una cadena de bloques. Cuando son posibles ramificaciones de la cadena, se puede considerar como verdadero el contenido de los bloques de la cadena más larga. Los participantes están de acuerdo a este respecto en que tales transacciones, designadas, en general, también como informaciones, son verdaderas, independientemente de su probabilidad real. El bloque se puede colgar a través de la inserción de un código de prueba en el bloque, que indica inequívocamente de esta manera la posición del bloque en la cadena.

La utilización de la Tecnología de Cadena de Bloques abre nuevas posibilidades, a través de las cuales se puede verificar en cualquier momento la base de datos distribuida, es decir, la base de datos descentralizada de transacciones, por todos los participantes. De esta manera, el sistema general, es decir, el sistema militar conectado en red, puede seguir funcionando también en el caso de fallo o bien de exclusión de participantes individuales y no depende ya de un nodo central, que está diseñado actualmente también redundante para garantizar la seguridad de

aplicación necesaria. Es ventajoso que las propias transacciones sean tanto almacenadas como también verificadas en muy poco tiempo, además de que se puedan reconocer inmediatamente manipulaciones de participantes maliciosos individuales. Además, en el supuesto de que tenga la potencia de cálculo correspondiente, el método es muy rápido. Se pueden realizar transacciones en milisegundos.

La utilización de Tecnología de Cadena de Bloques para sistemas militares conectados en red, es decir, el almacenamiento de todas las transacciones entre participantes del sistema militar conectado en red en una base de datos distribuida, prepara, por una parte, un mecanismo de seguridad adicional para asegurar transacciones y para reconocer participantes maliciosos y, por otra parte, posibilita también una distribución descentralizada de la base de datos de protocolos. Ésta está asegurada contra el fallo de participantes individuales y no puede ser manipulada por participantes maliciosos.

Por lo tanto, es conveniente que las transacciones dentro del sistema militar conectado en red sean almacenadas de forma descentralizada en una cadena de bloques. Las estaciones participantes o bien los participantes de la red pueden actuar en este caso al mismo tiempo como nodos y mantener su copia propia de la base de datos de la cadena de bloques. Estos nodos verifican en este caso de manera más ventajosa adicionalmente las transacciones dentro de la red. Esto se puede realizar a través de las claves públicas de los participantes.

En general, los participantes están equipados de manera más ventajosa con una clave privada, que es de manera más conveniente secreta y a este respecto sólo es conocida por el participante, al que pertenece la clave privada. A partir de la clave privada se puede generar una clave pública, que es publicada para algunos o todos los otros participantes de la red. Las transacciones se publican de manera más conveniente encriptadas en la red. La codificación se realiza en este caso de manera más conveniente con la clave privada. Por medio de la clave pública se puede descifrar la transacción. Puesto que esta clave es pública, cada participante puede descifrar la transacción. Con la descodificación y especialmente la verificación de que la descodificación se ha realizado con la clave pública de aquel participante que ha enviado la transacción, se puede reconocer la transacción como verificada.

Como regla fundamental, dentro de la red se puede considerar una información o bien una transacción como verificada cuando la pluralidad de los participantes en la red han confirmado la verificación (ver también “Generales Bizantinos” o bien “Errores bizantinos”). Otra posibilidad consiste en que aquel participante, que ha generado el bloque actual y lo llena con datos de las transacciones, verifica las transacciones y deposita los datos verificados en el bloque. Si el bloque está colgado en la cadena de bloques, se puede considerar la transacción como verdadera y se almacena como verdad básica no falsificable en la cadena de bloques.

En el caso de la utilización de bloques de datos yuxtapuestos, un periodo de tiempo puede durar hasta que una transacción está depositada en un bloque actual y éste está colgado en la cadena de bloques presente. Sólo entonces se considera la transacción como verdadera y, por lo tanto, se puede cargar como completa. Esto se aplica independientemente del tipo de la generación del bloque a través del llamado Minado (Prueba de Trabajo) o una asignación algorítmica de una generación de bloques (Prueba de Participación). En un sistema militar, especialmente un sistema de defensa aérea, puede ser necesario, sin embargo, reaccionar muy rápidamente a amenazas o a otras informaciones. Por lo tanto, hay que aclarar la cuestión de cuándo una transacción, por ejemplo, una instrucción de fuego para combatir un misil que se aproxima volando, se considera como cargable y, por lo tanto, debería ser realizada.

Por lo tanto, a continuación, se distingue entre una transacción no verificada, una transacción verificada y su reconocimiento como verdadera. Una transacción no verificada es, por ejemplo, una instrucción de fuego en sí. Está verificada cuando se ha verificado – por ejemplo, desde el destinatario, en este ejemplo una lanzadera para el lanzamiento de un cohete tierra-aire, por ejemplo, a través de la descodificación con la clave pública del emisor. Una transacción es verdadera cuando está contenida en un bloque, que ha sido colgado en la cadena de bloques. No obstante, es suficiente que una transacción sólo verificada sea reconocida como ejecutable, aunque no sea todavía parte de la cadena de bloques. La verificación se puede realizar muy rápidamente, de manera que las instrucciones se pueden ejecutar con suficiente rapidez.

Sin embargo, si la verificación no se ha conseguido de manera satisfactoria o predeterminada, entonces se considera la información de la transacción como no ejecutable o en general: no grave. Un emisor puede ser verificado y, donde sea posible, excluirse del sistema. Una exclusión de un participante es registrada por todos los otros participantes, sin que se perjudique la capacidad operativa propia o la del sistema, lo que conduce a una mayor robustez del sistema general.

Para la formación de una red de cadenas de bloques descentralizada es conveniente crear una configuración básica segura. De manera más conveniente, se insertan informaciones básicas no detectables en un bloque de base. Un bloque de base puede ser el primer bloque de la cadena de bloques. Puede estar constituido por varios bloques, que están al comienzo de una cadena de bloques. Este bloque de base debería contener informaciones básicas sobre los participantes y debería crearse en un entorno, que está más protegido que un entorno operativo regular posterior. De esta manera, se puede contrarrestar la introducción no deseada de información falsa a través de un intruso.

En un bloque de base debería definirse un grupo de base de participantes, es decir, un grupo de participantes autorizados o bien homologados.

Una posibilidad para la formación de un entorno protegido puede ser la red cableada de los participantes durante la creación del bloque de base. De esta manera, se dificulta una intervención desde el exterior en el interior de la red. De manera más ventajosa, los participantes básicos cableados se encuentran, durante la creación del bloque de base, en un único edificio. De esta manera, se puede formar una red cableada cerrada hacia fuera, en la que es extremadamente difícil penetrar.

Se puede crear otra posibilidad para la formación de un entorno protegido en la creación del bloque de base, conectando el grupo de base después de la creación del bloque de base entre sí. El bloque de base puede ser formado por un único participante básico, por ejemplo, una central de mando o bien una Centro Táctico de Operaciones (TOC), especialmente sin que exista una conexión en red con una red sin cables o una red fuera del edificio, en el que se encuentra la central de mando.

Los participantes se conectan en red de manera más ventajosa para el intercambio de certificados, como por ejemplo su clave pública, en un entorno protegido, por ejemplo, en un depósito. La conexión en red se realiza en este caso de manera más conveniente a través de un medio protegido, como por ejemplo una conexión de cable. Por lo tanto, el entorno protegido se desvía del entorno operativo regular, como también se puede desviar el medio para la conexión en red. En el entorno operativo regular se pueden emplear tanto redes sin cables como también cableados o ambos. Se puede crear una configuración básica segura, después de cuya creación y deposición segura en bloques se inicia el funcionamiento regular o bien con una red sin cables. Se puede contrarrestar una influencia no deseada ya inicial de datos de base.

Es igualmente ventajoso que los participantes se conecten por cable entre sí e intercambien certificados, por ejemplo intercambien su clave pública y entonces se libere el cableado entre al menos una parte de los participantes y se establezca una red sin cables entre estos participantes.

Cuando las transacciones se almacenan en bloques, es conveniente que los bloques sean creados según un algoritmo establecido. Esta regla está establecida de manera más conveniente en un bloque de base. En lugar de una minería, es ventajoso el método de Prueba de Participación, no debiendo limitarse el concepto de participación a porciones materiales en la red, por ejemplo, porciones de la fuerza de cálculo de la red.

El algoritmo distribuye proporcionalmente los derechos para la creación del bloque entre los participantes de manera más conveniente. Así, por ejemplo, cada participante recibe una porción de todos los derechos de creación, que le son asignados de hecho con el algoritmo entonces con la operación. Si, por ejemplo, un participante recibe el 5% de los derechos de creación para la creación de bloques, entonces en el curso de la operación regular creará, visto estadísticamente, en realidad aproximadamente el 5% de los bloques, pudiendo desviarse considerablemente el valor también durante corto espacio de tiempo.

Un principio conveniente para la distribución de las porciones entre los participantes es la dimensión utilizando la seguridad de los datos de los participantes individuales. Un participante de datos seguros, por ejemplo, una central de mando, recibe una porción más elevada que un participante menos seguro. También se puede tener en cuenta un estado del cableado en la asignación de las porciones, para que, por ejemplo, un participante, que está cableado en la red con al menos otro participante, reciba una porción más elevada que un participante conectado sólo sin cables con los otros participantes y, en particular, un participante cableado exclusivamente en la red recibe una porción más elevada que un participante cableado parcialmente y conectado parcialmente sin cables con un participante.

Además, es ventajoso que el algoritmo distribuya los derechos para la creación del bloque según un método-pseudo-aleatorio. Tal método establece los derechos individuales de creación del bloque, en efecto, de manera determinista, pero no se puede predecir desde el exterior – sin conocimiento de un parámetro de creación –, por lo que aparece desde el exterior como método aleatorio. En este caso, es conveniente que la asignación de los derechos individuales, es decir, para la creación de un bloque, se pueda realizar para cada participante, puesto que la asignación es verificable de esta manera. De forma más ventajosa, la asignación de los derechos individuales de creación para cada participante se puede calcular con antelación con una seguridad, por término medio, mayor del 50%, con lo que se eleva la posibilidad de verificación desde el exterior.

En una red de cadenas de bloques cerrada es conveniente definir unívocamente los límites hacia fuera para impedir o al menos dificultar una penetración no permitida de un intruso. Se puede realizar una limitación especialmente rigurosa hacia fuera cuando las transacciones se depositan en bloques y solamente pueden generarse tales bloques de datos en un bloque de base de participantes registrados. De esta manera, no es posible una adición de participantes nuevos, de manera que permanecen los participantes originales de la red entre sí. Esto puede ser especialmente ventajoso en sistemas militares. Se puede conseguir una mayor variabilidad de la red, eludiendo la rigurosidad de los límites exteriores, cuando pueden entrar participantes nuevos en la red, pero son admitidos en la

red solamente según un método de admisión predeterminado como participantes nuevos autorizados. El método de admisión se reproduce de manera más conveniente en un bloque de base de la cadena de bloques.

Por medio de la invención se crea una posibilidad especialmente segura para la autorización de un participante nuevo en la red o bien en el sistema, siendo autorizado en la red un participante no autorizado todavía en la red como participante nuevo solamente cuando un participante autorizado para la nueva recepción autoriza el participante nuevo. Un participante autorizado para la nueva recepción es de manera más conveniente un participante que, con respecto a la seguridad de sus datos, está mejor blindado hacia fuera que la media de los restantes participantes, especialmente el mejor blindado de todos.

Se puede elevar la seguridad en la nueva admisión de participantes cuando un participante todavía no autorizado en la red solamente es admitido en la red como nuevo participante cuando varios participantes habilitados para la nueva aceptación, admiten unívocamente el nuevo participante.

Según la invención, el participante autorizado para nueva admisión está representado como tal en un bloque de base. De esta manera, se puede contrarrestar una manipulación posterior de una nueva admisión. Se puede conseguir una seguridad adicional contra un hackeo de un participante autorizado para la nueva admisión, cuando la decisión para la nueva admisión de un participante se toma por unanimidad por una o varias personas autorizadas para ello. La facultad o bien una regla, en la que se basa la facultad, puede estar depositada en un bloque de base.

Para elevar todavía más la seguridad contra la penetración no autorizada, puede estar previsto que solamente sea admitido un participante nuevo en la red como participante autorizado cuando al menos una verificación de la factibilidad para un nuevo participante, utilizando informaciones de bloques de una cadena de bloques, es positiva.

Las transacciones o bien las informaciones intercambiadas en la red, que están depositadas en un bloque y que están colgadas en el bloque en una cadena de bloques, se consideran de manera más conveniente como verdaderas. Para no dejar que falsedades reales lleguen como verdades a la cadena de bloques, es ventajoso que las transacciones sean almacenadas en bloques y solamente se puedan insertar datos por participantes registrados en un bloque de base y – cuando existen participantes nuevos autorizados – por estos participantes nuevos autorizados en estos bloques de datos. En efecto, se puede intercambiar información de participantes no autorizados en la red, pero no alcanzan el estado de una verdad.

La comunicación en la red o bien en el sistema y/o el modo de tratamiento por participantes se pueden establecer por medio de reglas. En este caso, es conveniente distinguir entre reglas fundamentales y reglas dinámicas. Una regla fundamental puede ser una regla invariable, en cambio una regla dinámica es variable, generable de nuevo y/o desechable. Una regla fundamental, en particular todas las reglas fundamentales, están identificadas como tales. De manera más conveniente, están depositadas en un bloque de base.

Además, es conveniente que al menos una regla fundamental defina la creación de reglas dinámicas, para que éstas sean protegidas contra manipulación. Una protección contra manipulación de reglas fundamentales se puede mejorar cuando las reglas fundamentales de la red están almacenadas en hardware en/dentro de al menos un participante.

Para proteger una regla fundamental es ventajoso, además, que los participantes estén conectados en red, por ejemplo, para la primera creación de una red o bien sistema, y se inserte una regla fundamental almacenada en un participante durante la creación de un bloque de base en este bloque. De esta manera, se puede impedir una modificación de la regla fundamental.

La invención se refiere, además, a un sistema militar conectado en red con varios participantes, en el que están almacenadas transacciones de los participantes entre sí en una base de datos distribuida. La base de datos puede estar distribuida en los participantes. De manera más conveniente, la base de datos está almacenada en cada caso totalmente en una pluralidad de participantes, especialmente en todos los participantes. De manera más ventajosa, el sistema está realizado para ejecutar el método según la invención.

La descripción presentada hasta ahora de configuraciones más ventajosas de la invención contiene numerosas características, que están reproducidas, en parte, en algunas reivindicaciones dependientes agrupadas. Pero las características se pueden considerar de manera más conveniente también individualmente y agruparse en otras combinaciones convenientes, especialmente en el caso de referencias cruzadas de reivindicaciones, de manera que una característica individual de una reivindicación dependiente se puede combinar con una, varias o todas las características de otra reivindicación dependiente. Además, estas características se pueden combinar en combinación adecuada discrecional tanto con el método según la invención como también con el dispositivo según la invención de acuerdo con las reivindicaciones correspondientes. De esta manera, características del método se pueden considerar como propiedades de la unidad de dispositivo correspondiente formuladas autónomas y las características funcionales del dispositivo se pueden considerar también como características correspondientes del método. El alcance de protección reivindicado se define por las reivindicaciones.

Las propiedades, características y ventajas descritas anteriormente de esta invención, así como el modo en que se alcanzan, se comprenderán más claramente en conexión con la siguiente descripción de los ejemplos de realización, que se explican en detalle en relación con los dibujos. Los ejemplos de realización sirven para la explicación de la invención y no limitan la invención a la combinación de características indicadas, tampoco con relación a las características funcionales. Además, las características adecuadas de cada ejemplo de realización se pueden considerar también explícitamente aisladas, separadas de un ejemplo de realización, se pueden insertar en otro ejemplo de realización como complemento y/o se pueden combinar con cualquiera de las reivindicaciones.

La figura 1 muestra un sistema militar conectado en red en forma de un sistema de defensa aérea.

La figura 2 muestra un esquema de una estructura de un sistema militar conectado en red en un edificio.

La figura 3 muestra un esquema de una estructura de otro sistema militar conectado en red a través de consultas desde una central de mando, y

La figura 4 muestra un esquema de una comunicación del sistema militar conectado en red de la figura 3 durante su funcionamiento regular.

La figura 1 muestra un sistema militar conectado en red 2, que se designa a continuación de manera simplificada y general como red 2. El sistema 2 comprende una central de mando 4, llamada también Central Técnica de Operaciones (TOC), que está conectada a través de un cable de fibra óptica 12 con un sistema sensor en forma de un sistema de radar 6. El sistema de radar 6 sirve para la supervisión del espacio aéreo y forma con la central de mando 4 y una pluralidad de sistemas efectores en forma de lanzaderas 8 un sistema de defensa aérea conectado en red. En este sistema militar conectado en red 2 o bien sistema de defensa aérea, la central de mando 4, el sistema de radar 6 y las lanzaderas 8 forman participantes 10 de la red 2.

Las lanzaderas 8 están distribuidas sobre una superficie grande para poder defender un área grande contra ataques aéreos. Sin embargo, una de las lanzaderas 8 está en la proximidad de la central de mando 4 y está conectada con ella por medio de un cable de fibra de vidrio 12 - en general: cable de datos - como también el sistema de radar 6 está conectado con la central de mando 4. Las restantes lanzaderas 8 están más alejadas de la central de mando 4 y están conectadas con ésta por medio de una conexión sin cables 14, como se representa en la figura 1 por medio de las flechas irregulares. Las lanzaderas 8 comprenden varios contenedores 16, desde los que se pueden lanzar uno o varios misiles tierra-aire para interceptar un misil que se aproxima volando. El control de las lanzaderas 8 se realiza desde la central de mando 4, que ha asumido el control de las lanzaderas 8 en un control remoto, de manera que el personal de las lanzaderas 8 individuales está liberado del manejo de las lanzaderas 8 y solamente está apostado a cierta distancia de la lanzadera 8 respectiva para su defensa. Todos los participantes 10 son móviles y están colocados en vehículos, de manera que se pueden desplazar rápidamente y en caso necesario pueden huir también rápidamente ante los ataques.

La red 2 es una red cerrada hacia fuera, en la que los participantes 10 se comunican entre sí, pero, por lo demás, ningún otro participante tiene acceso a esta red 2. En efecto, existe una conexión de la red hacia fuera a través de la central de mando 4, indicada, en general, por un participante central 10, pero no es posible una comunicación desde fuera de la red 2 con uno de los participantes 10, con la excepción del participante central 10. Tal comunicación sólo sería posible a través de una penetración no permitida de un participante malicioso en la red 2.

Para la penetración no permitida existen generalmente dos posibilidades, que se designan a continuación simplemente como irrupción de software e irrupción de hardware. En el caso de una irrupción de hardware, el hardware es recibido por un participante malicioso, por ejemplo, se alcanza una lanzadera a través de un grupo de paracaidistas enemigos y es accionada en adelante por éstos, sin que los restantes participantes 10 de la red 2 tengan conocimiento de tal irrupción. En el caso de una irrupción de software, un participante malicioso penetra a través de una actividad de programación y/o de comunicación no autorizada en la red 2. Tal hackeo se puede realizar sin la recepción material de un participante 10.

Para la protección contra una penetración no permitida de un participante malicioso en la red 2, la red 2 está equipada con una base de datos distribuida 20 (figura 2), cuyo contenido está total o parcialmente distribuido sobre varios participantes 10 de la red 2, en particular sobre todos los participantes 10 de la red 2. Esto se ilustra a continuación con la ayuda del gráfico de la figura 2.

La figura 2 muestra los participantes 10 de una red 2 en una representación esquemática. Cada participante 10 está equipado con un sistema de procesamiento de datos 18, en el que está presente - de manera simplificada - una base de datos 20, que, para mayor claridad gráfica en la figura 2 - se designa de manera idéntica al sistema de procesamiento de datos 18. Evidentemente, también es posible que la base de datos 20 esté almacenada de alguna manera dentro del participante 10 y el sistema de procesamiento de datos 18 tenga acceso a ella. Es importante que la base de datos 20 y el sistema de procesamiento de datos 18 estén presentes dentro del participante 10 respectivo, por lo que es posible un acceso sin una actividad de la red 2 o bien una transacción a través de un cable

de datos 12 o bien una conexión sin cables 14. Por ejemplo, el sistema de procesamiento de datos 18 y la base de datos 20 están almacenados dentro del mismo vehículo, siendo esto válido igualmente para varios o bien para todos los participantes 10 de la red.

La comunicación en la red 2 se puede realizar por radiodifusión, especialmente en la red sin cables, como se indica en la figura 1 por medio de las conexiones sin cables 14. Tal radiodifusión se puede realizar a través de las conexiones de cables 12, de manera que una transacción entre dos o más participantes 10 es conocida por todos los participantes 10. No obstante, es igualmente posible que se intercambien transacciones entre participantes 10, es decir, instrucciones desde un participante 10 hasta al menos otro participante o en el sentido más amplio informaciones que son intercambiadas entre dos participantes 10, son direccionadas y son proporcionadas a un solo participante 10 o a varios participantes 10 direccionados, sin que esta transacción sea accesible a los otros participantes 10. En este caso, sólo es importante que tal transacción no pública sea publicada posteriormente en un bloque 22 a todos los participantes 10.

Todas las transacciones entre participantes 10 o aquellas transacciones en la red 2, que se catalogan a través de un catálogo establecido como almacenables de forma duradera, se introducen en un bloque 22, que se cuelga en una cadena de bloques 24. En la cadena de bloques 24 están depositadas, por lo tanto, todas las transacciones o todas las transacciones consideradas como esenciales, especialmente todas las informaciones intercambiadas entre participantes 10 de la red 2. Esta cadena de bloques 24 forma en este caso una base de datos 20, que contiene todas estas transacciones. La cadena de bloques 24 no sólo es accesible a todos los participantes 10 de la red 2, sino que está distribuida también sobre varios, especialmente sobre todos los participantes 10 de la red 2. En el ejemplo de realización representado en la figura 2, la cadena de bloques 24 está constituida, por ejemplo, actualmente por tres bloques 22, que están almacenados en la base de datos 20 de cada participante 10. No obstante, también es posible fragmentar la cadena de bloques 24 y proporcionar solamente porciones individuales a los participantes 10, siendo, sin embargo, importante que los participantes 10 tengan a través del acceso a varias bases de datos 20 de varios participantes 10, acceso a todos los bloques 22 de toda la cadena de bloques 24. No obstante, es más sencillo el almacenamiento completo de la cadena de bloques 24 en todos los participantes 10.

Los bloques 22 de la cadena de bloques 24 están conectados en red entre sí. Esta conexión se realiza no sólo a través de la concatenación, sino por que el contenido de uno o varios, especialmente de todos los bloques 22 anteriores están depositados, agrupados en un código de prueba 26, en el bloque 22 siguiente, por ejemplo, en la cabecera del bloque 22 siguiente. El código de prueba 26 puede ser un valor Hash, que está formado por el contenido del o de los bloques 22. En la figura 2 se representa cómo un primer bloque 22 – a la izquierda en la cadena de bloques 24 – contiene una pluralidad de transacciones 28, que se representan en la figura 2 por medio de puntos en el bloque 22. El contenido del primer bloque 22 se agrupa en un código de prueba 26, por ejemplo, un valor Hash, y se deposita en el bloque 22 siguiente. El segundo bloque 22 está también total o parcialmente lleno con transacciones 28 y contiene también adicionalmente el código de prueba 26. El tercer bloque 22 contiene un código de prueba 26, que se forma por todo el contenido de los bloques 22 precedentes, por ejemplo, un valor Hash del contenido de todos los bloques 22 precedentes. Este código de prueba 26 está depositado de nuevo en la cabecera del tercer bloque 22. También el tercer bloque 22 está total o parcialmente lleno con transacciones 28, etc. Esta conexión en red de los bloques 22 tiene la ventaja de que una modificación posterior del contenido de un bloque 22 implica una modificación de todos los bloques 22 de la cadena de bloques 24. No obstante, puesto que estos bloques 22 están almacenados en todos los participantes 10 de la red 2, la modificación de los bloques 22 en un participante 10 no es suficiente, de manera que una modificación sistemática siguiente de las transacciones 28 en los bloques 22 yuxtapuestos sólo es posible con dificultad. Por lo tanto, todos los participantes 10 pueden ver en cualquier instante qué transacciones 28 están presentes en la cadena de bloques 24, siendo fiable el contenido de verdad de estas transacciones 28 o bien bloques 22.

Si un participante malicioso consigue una irrupción de software o incluso una irrupción de hardware en la red 2, entonces no puede modificar posteriormente las transacciones 28, que le permite la red 2, sin que esto llame la atención a través de inconsistencias en las bases de datos 20 individuales de los participantes 10. De esta manera, se apreciaría inmediatamente una modificación por todos los participantes 10. Se pueden tomar medidas para defenderse de consecuencias resultantes de ello. Tampoco es posible que un participante malicioso se enclave entre dos participantes 10 de la red 2 y distribuya informaciones diferentes a los dos participantes 10. Si se coloca, por ejemplo, un participante entre la central de mando 4 y una lanzadera 8 y simula a la lanzadera 8 una central de mando y a la central de mando 4 la lanzadera imaginaria, entonces se asignan informaciones diferentes a la central de mando 4 y a la lanzadera 8. Éstas deberían inscribirse como transacciones 28 en el bloque actual 22, de manera que los restantes participantes 10 se dan cuenta de la discrepancia entre las informaciones o bien las transacciones 28. Se reconoce la irrupción y se pueden tomar contramedidas.

Para la seguridad adicional del sistema 2 se codifican todas las transacciones entre participantes 10 con una clave privada, en donde cada participante 10 presenta una clave privada individual. Esta clave privada sólo es conocida por el participante 10 respectivo. Cada participante 10 genera a partir de su clave privada propia una clave pública y la pone a la disposición de la red 2, de manera que cada clave pública está depositada también en la cadena de bloques 24. Una transacción 28 entre dos participantes 10 es codificada por el participante emisor 10 con su clave

privada y puede ser descodificada para el receptor 10 a través de la clave pública del participante emisor 10. De esta manera, se puede establecer sin lugar a dudas desde qué participante 10 proviene la transacción 28. En el caso de una irrupción de software, el participante malicioso irrumpido debería estar en posesión de la clave privada del participante 10 para poder emitir en la red 2 informaciones falsas no reconocidas. Esto es difícil - en el caso de deposición segura correspondiente de la clave privada de cada participante 10 -. En el caso de una irrupción de hardware, el participante malicioso puede acceder a la clave privada e introducir informaciones falsas no reconocidas en la red 2. Esto no es reconocible inmediatamente por los restantes participantes 10, cuando el participante 10 original, que ha sido recibido hostilmente por el participante malicioso, no se ha anunciado adicionalmente en la red 2. No obstante, en este caso se puede realizar un reconocimiento de participante malicioso con la ayuda de verificaciones de la factibilidad, que se realizan con la ayuda de las transacciones 28 desde la cadena de bloques 24, como se describe más adelante.

Para crear los bloques 22 existe en la red 2 un algoritmo, de acuerdo con cuyas reglas se crean los bloques 22. También este algoritmo está depositado en la cadena de bloques 24. En el ejemplo de realización representado, el algoritmo distribuye los derechos para la creación de bloques entre los participantes 10. Cada uno de los participantes 10 recibe, por lo tanto, la posibilidad para la creación de un bloque 22, siendo establecida la secuencia para la creación de los bloques 22 a través del algoritmo. En el ejemplo de realización mostrado en la figura 2, los derechos para la creación del bloque actual se encuentran en el segundo participante 10 más bajo en la columna derecha. El participante 10 llena el bloque 22 creado por él con transacciones 28 y cuelga el bloque 22 entonces, como se predetermina por el algoritmo, en la cadena de bloques 24. A más tardar al agregar el bloque 22 actual a la cadena de bloques 24, el bloque 22 se cierra, de manera que no se pueden introducir más transacciones 28 en éste. Por ejemplo, la entrada del código de prueba 26 es la última entrada en el bloque 22, antes de que éste sea colgado en la cadena de bloques 24. El bloque colgado 22 es enviado a todos los participantes 10 para el almacenamiento en las bases de datos 20, para que cada participante 10 esté en el estado actual de la información. Aquellas transacciones 28, que están registradas en un bloque 22 colgado en la cadena de bloques 24 son consideradas como verdades y cargables entre los participantes 10.

Ahora otro participante 10 obtiene la posibilidad de crear un bloque 22 de acuerdo con las reglas del algoritmo. Estas reglas pueden prever que los derechos para la creación de bloques 22 sean distribuidos proporcionalmente entre los participantes 10 de la red 2. En el ejemplo de realización mostrado en la figura 2, uno de los participantes 10, por ejemplo, la central de mando 4 tiene una porción del 40 %, como se representa en la figura 2. Otros cuatro participantes 10 tienen, respectivamente, una porción del 10 % y un participante 10 tiene una porción del 20 %. Las porciones entre los participantes 10 se pueden establecer según la seguridad de los datos de los participantes 10 individuales por el algoritmo. Por ejemplo, la central de mando 4 está mejor protegida y recibe la porción más alta, 40 %, en el ejemplo de realización. Si un participante 10 está cableado con la central de mando 4, esto significa una seguridad más alta de los datos, que se puede reducir en el dimensionado de las porciones. Así, por ejemplo, la lanzadera cableada 8 tiene la porción de 20 %. Puesto que el radar 6 es un objetivo principal para ataques aéreos enemigos, esto tiene - a pesar de su seguridad de los datos relativamente alta - una porción más reducida de la lanzadera cableada 8 y, por lo tanto, también sólo, por ejemplo, una porción del 10 %. Los derechos para la creación del bloque son distribuidos según el algoritmo de acuerdo con un método pseudoaleatorio. Respectivamente, en retrospectiva para cada participante 10 con una seguridad predeterminada es posible verificar la distribución para la creación del bloque actual 22, de manera que la distribución de los derechos para la creación del bloque actual 22 para los participantes 10 es transparente. Además, sólo pueden crear bloques 22 los participantes 10 autorizados en la red 2, es decir, registrados o autorizados en el algoritmo. También sólo las transacciones 28 de estos participantes 10 llegan a los bloques 22 y son almacenadas o bien depositadas allí.

En el ejemplo de realización representado en la figura 1, especialmente las siguientes informaciones pueden estar registradas como transacciones en la cadena de bloques 24: los datos de movimiento de misiles detectados por el sistema de radar 6, los llamados datos de seguimiento, los disparos o instrucciones de fuego emitidos por el sistema de mando 24, las identificaciones realizadas por el sistema de radar 6 de aviones o misiles, la asignación de un objetivo a una lanzadera 8 a través de la central de mando 4, los datos de registro de participantes 10 en la red 2, cuando éstos entran nuevos en la red 2 o entran de nuevo después de una interrupción en la red 2, los estados de participantes 10, como disponibilidad operativa, la preparación para el combate, un defecto técnico, número y estado de misiles de defensa en botes 16, los lugares geográficos de participantes 10 y/o las reglas de la red. También es conveniente el almacenamiento de ciclos completos sobre detección, seguimiento, evaluación, decisiones de combate, evaluación de combate y daño como transacciones en la cadena de bloques 24, para poder reconstruir la secuencia de eventos sin alteraciones después de una operación en cualquier momento.

Por ejemplo, una central de mando 4 como participante 10 del sistema militar 2 conectado en red puede documentar sus derechos, es decir, su autorización para determinadas transacciones, a través de un certificado correspondiente. Tal certificado y/o el derecho en sí mismo puede ser una transacción. La transmisión de derechos, a la que pertenece también el registro de una central de mando 4 nueva a través de su certificado, es igualmente una transacción, que se almacena en la central de bloques 24 y de esta manera se da a conocer a todos los otros participantes 10 sin falsificación. De esta manera, se asegura, por ejemplo, la transferencia de la autoridad a otro participante 10, siempre ejecutable y protegida contra posibles intrusos.

Las informaciones básicas fundamentales en las que se basan las transacciones 28 de la red 2 están depositadas en la cadena de bloques 24 en bloques de base 30. En la figura 2 se resaltan dos de tales bloques de base 30 por medio de un enmarque grueso. Estos bloques de base 30 son los primeros bloques 22 de la cadena de bloques 24. Se pueden crear uno o varios bloques de base 30, según la capacidad de datos de los bloques de base 30 y la cantidad de las informaciones de base a inscribir. También éstas se designan a continuación transacciones 28, aunque no deben intercambiarse en sentido estricto entre participantes 10.

En un bloque de base 30 se pueden registrar los participantes 10 de la red 2, especialmente de forma concluyente. Además, un bloque de base 30 puede contener reglas fundamentales, que no son modificables. Una regla fundamental puede consistir en que sólo se pueden recibir transacciones en un bloque 22, cuando éstas han sido generadas por un participante 10 registrado en el bloque de base 30. Si existe la posibilidad de admitir otros participantes 10 en la red 2, se pueden registrar también transacciones de tales participantes 10 autorizados en bloques de datos 22, que se cuelgan en la cadena de bloques 24.

Para evitar una manipulación de informaciones de base, sobre las que se establece toda la comunicación en la red 2, es conveniente que se cree un bloque de base 30 en un entorno que es más seguro que un entorno regular posterior. Por ejemplo, todos los participantes 10 de una red 2 futura dentro de un edificio 32 se conectan, como se indica en la figura 2. Los participantes 10 pueden intercambiar transacciones 28 en un entorno protegido, que son depositadas en uno o varios bloques de base 30. Tales transacciones 28 pueden ser reglas fundamentales, que establecen una acción de un participante 10 y/o una interacción de los participantes 10 entre sí. Una regla fundamental de la red 2 puede estar almacenada por hardware en al menos un participante 10 y se transmite a través de la red correspondiente desde el participante 10, que lleva la regla fundamental, hacia el participante 10, que crea un bloque de base 30 e inscribe esta regla fundamental en el bloque de base 30.

Alternativa o adicionalmente, es conveniente que los participantes 10 se conecten exclusivamente por cable entre sí para la creación de los bloques de base 30, como se indica en la figura 2. De esta manera se dificulta considerablemente una irrupción en esta red 2 cableada. Después de la creación de los bloques de base 30 se pueden aflojar parcial o totalmente los cableados y se puede recurrir, por ejemplo, a conexiones sin cables 14, como se representa en la figura 1. Las informaciones de base depositadas entonces en los bloques de base 30 son correctas, y la red 2 puede descubrir informaciones falsas generadas a través de una interrupción posterior.

En el caso de una red 2 relativamente pequeña, la red cableada opuesta para la creación de los bloques de base 30 y/o la conexión en red en un edificio 32 es una protección inicial conveniente. Igualmente es conveniente que los participantes 10 en sí mismos estén indicados en un bloque de base 30, para que un participante malicioso no pueda participar de manera sencilla en la red 2, sin ser descubierto como malicioso.

En el caso de una red grande 2, que presenta, por ejemplo, participantes fluctuantes 10 que, por lo tanto, pueden ir y venir, no es posible sin más tal conexión en red básica o tal creación de bloques de base 30. Aquí es conveniente que el sistema 2 se conecte sólo después de la creación del bloque de base 30, en particular también sólo se conecte en red inicialmente. La creación de uno o de varios bloques de base 30 corresponde, por ejemplo, a un participante 10 muy seguro, como la central de mando 4. Este participante 10 crea uno o varios bloques de base 30 sin una conexión en red, es decir, en un entorno muy seguro contra irrupción. Los bloques de base 30 contienen entonces reglas fundamentales, que determinan una autorización o rechazo de participantes 10 nuevos o móviles.

Tal proceso se representa como ejemplo en la figura 3. La figura 3 muestra un participante 10 con una base de datos 20 con bloques de base 30 y con otro bloque 22 colgado en los bloques de base 30. Los bloques de base 30 son creados a demanda de un usuario 34, que proporciona a tal fin datos a un sistema de procesamiento de datos 18, con cuya ayuda el sistema de procesamiento de datos 18 crea los bloques de base 30. Éstos son verificados y liberados, por ejemplo, por el operador 34.

Después de crear uno o varios bloques de base 30, el participante 10 envía consultas a otros participantes 10, como se indica por medio de las flechas salientes en la figura 3. En respuesta a tal consulta, se conecta un participante 10 consultado con el primer participante 10 de acuerdo con las reglas indicadas en un bloque de base 30. A la inversa, también es posible que un participante externo 10 plantee una consulta de conexión a la red al primer participante 10, como se indica en la figura 3 por medio de una flecha entrante. Si la consulta o bien el participante consultor 10 cumple las reglas fundamentales de un bloque de base 30, entonces también este participante 10 es aceptado y conectado en la red 2 como participante 10 autorizado. Las transacciones correspondientes, es decir, las informaciones para los participantes 10 en sí mismos, es decir, las propiedades o bien los datos de los participantes 10, son depositadas como transacciones 28 en los bloques 22 siguientes, de manera que cada participante 10 conoce los otros participantes 10 de la red 2 y sus propiedades. Tal modo de proceder es conveniente en el caso de redes 2 grandes o en el caso de redes 2 con participantes 10 muy fluctuantes.

Un ejemplo de una red 2 de este tipo se explica a continuación con la ayuda de la representación de la figura 4. La red 2 comprende una pluralidad de participantes 10, que están conectados entre sí especialmente sin cables, por ejemplo, a través de una red de radio 36 y/o Internet. La red 2 es un sistema militar grande, que incluye personas y

vehículos como participantes 10, así como una central de mando 4 y diferentes armas. La red 2 ha sido conectada, por ejemplo, como se describe en la figura 3, y está en su funcionamiento regular.

Uno de los participantes 10 es un soldado 38 que, sin embargo, en primer lugar, debido a un permiso, no forma parte del sistema 2. El sistema 2 se encuentra, por ejemplo, en Afganistán. Después de su permiso, el soldado 38 se anuncia a un participante 10 autorizado para una nueva admisión en la red 2, en este ejemplo de realización la central de mando 4. Lleva un soporte de datos consigo, en el que está almacenada la clave pública 40. Los participantes 10 nuevos en la red 2 solamente pueden intercambiar transacciones en la red como participantes 10 autorizados cuando son admitidos en la red 2 por un participante 10 autorizada para la nueva admisión. Tal participante 10 autorizado para la nueva admisión está representado, además, como tal en un bloque de base 30 de la cadena de bloques 24 del sistema 2.

Una persona 42, por ejemplo, un oficial, recibe ahora el soporte de datos con la clave pública 40 del soldador 38 y conduce dos conjuntos de datos a un sistema de procesamiento de datos 18, a saber, el conjunto de datos con la clave del soldado 38 y un conjunto de datos con su propia clave pública 44. La clave 44 presenta la persona como autorizada para admitir un participante 10 nuevo en la red 2.

Con respecto a la clave pública 40 del soldado 38, el sistema de procesamiento datos 18 verifica ahora con la ayuda de transacciones, que están almacenadas en la cadena de bloques 24 del sistema 2, si la nueva admisión del soldado 38 es factible. A tal fin, se utilizan informaciones, que están asociadas al soldado 38 o bien a su clave pública 40, como se indica por las dos flechas en el sistema de procesamiento de datos 18 en la figura 4. Se muestra, por ejemplo, que el soldado 38 ha volado ya hace cuatro días a Frankfurt y ha llegado hace tres días a Kabul, por lo que han transcurrido tres días hasta que ha llegado a la central de mando 4. Este periodo de tiempo es demasiado largo y no se admite en la verificación. El resultado correspondiente es indicado a la persona 42 a través del sistema de procesamiento de datos 18. Éste puede verificar ahora la permanencia del soldado 38.

En el caso de la verificación de si un participante nuevo puede ser admitido en la red 2, se aplican reglas, que están depositadas en la cadena de bloques 24. Estas reglas pueden ser reglas fundamentales o reglas dinámicas. En el ejemplo con el soldado 38 se verifica con la ayuda de reglas dinámicas si el participante 10 nuevo puede ser admitido en la red 2. Cada regla dinámica puede crearse de acuerdo con una regla fundamental, que establece la creación y también de nuevo la anulación de una regla dinámica. La regla dinámica aplicada en el ejemplo dice que la verificación de la factibilidad negativa se puede compensar positivamente por medio de una consulta a través de una persona autorizada 42, cuando la persona 42 lo considera conveniente y presenta una clave pública 44 correspondiente, que está asociada a una facultad correspondiente. Pero esta regla se puede modificar también por una persona de mayor jerarquía de acuerdo con una regla fundamental.

También puede estar previsto que la decisión a través de la persona autorizada 42 propiamente dicha sea verificada de nuevo automáticamente por un participante 10 en forma de un rango superior. Este participante 10 se puede tratar, por ejemplo, de un ordenador de una instancia de control central, que verifica automáticamente todas las transacciones / decisiones en la cadena de bloques 24 y envía los resultados a un equipo de verificación.

En el ejemplo de realización mostrado, el soldado 38 es admitido en la red 2 y es enviado a un emplazamiento, donde presta su servicio. Así se registra con su clave pública 40, por ejemplo, en un arma, por ejemplo, una lanzadera 8, que notifica este proceso a la red 2, por ejemplo, por medio de una conexión sin datos 14 con la central de mando 4. Ésta verifica si tal inscripción es factible y -en caso afirmativo - libera el soldado 38 o bien su arma para comunicación en la red 2. El soldado 38 presta ahora su servicio hasta que se da de baja de nuevo en la red 2 y hace entonces necesaria una nueva admisión en la red 2 de nuevo de una persona 42 autorizada para ello.

Lista de signos de referencia

2	Sistema / red
4	Central de mando
6	Sistema sensor, sistema de radar
8	Sistema efector, lanzadera
10	Participante
12	Cable de datos
14	Conexión sin cables
16	Bote
18	Sistema de procesamiento de datos
20	Base de datos
22	Bloque
24	Cadena de bloques
26	Código de prueba
28	Transacción
30	Bloque de base
32	Edificio

34 Operador
36 Red de radio
38 Soldado
40 Clave
42 Persona
44 Clave

REIVINDICACIONES

1. Método para proteger un sistema militar conectado en red (2) frente a participante maliciosos, en el que se almacenan transacciones (28) entre participantes (10) del sistema militar conectado en red (2) en una base de datos (20) distribuida,

en el que las transacciones (28) se almacenan en bloques yuxtapuestos (22), cuyo contenido está conectado entre sí, de tal manera que en un bloque (22) se almacena un código de prueba formado a partir de al menos un bloque (26) anterior,

caracterizado por que solamente participantes (10) registrados en un bloque de base (30) y participantes (10) nuevos autorizados pueden generar tales bloques de datos (22), en el que el bloque de base (30) es el primer bloque de los bloques (22) yuxtapuestos y un participante (10) no autorizado todavía en la red (2) solamente es admitido en la red (2) como nuevo participante (10) cuando un participante (10) autorizado para una nueva admisión y registrado como tal en un bloque de base (30), autoriza el nuevo participante (10).

2. Método según la reivindicación 1, caracterizado por que la base de datos (20) está almacenada en varios participantes (10) y es visible para todos los participantes (10).

3. Método según la reivindicación 1 o 2, caracterizado por que el sistema militar (2) incluye personas y vehículos como participantes (10).

4. Método según una de las reivindicaciones anteriores, caracterizado por que el sistema militar (2) es un sistema de defensa aérea, que comprende los participantes (10), una central de mando (4), al menos un sistema sensor (6) para la supervisión aérea y al menos un sistema efector (8) para la defensa de amenazas.

5. Método según una de las reivindicaciones anteriores, caracterizado por que las transacciones (28) comprenden al menos información del grupo de:

- datos de movimiento detectados por un sistema sensor (6) de amenazas,
- disparos o instrucciones de fuego,
- identificación de amenazadas,
- asignación de un objetivo a un sistema efector (8),
- datos de registros de participantes (10) en la red (2),
- estados de participantes (10),
- lugares geográficos de participantes (10),
- reglas de la red.

6. Método según una de las reivindicaciones anteriores, caracterizado por que una transacción (28) entre los participantes (10) se considera como verdadera cuando la transacción (28) está almacenada en un bloque (22) y el bloque (22) está colgado en una cadena (24) de bloques (22).

7. Método según una de las reivindicaciones anteriores, caracterizado por que se deposita la información de base de los participantes (10) en un bloque de base (30), que se crea en un entorno, que está protegido frente a un entorno operativo regular posterior.

8. Método según la reivindicación 7, caracterizado por que en el bloque de base (30) se define un grupo de base de participantes (10).

9. Método según la reivindicación 7 u 8, caracterizado por que los participantes (10) están conectados por cable cuando se crea un bloque de base (30).

10. Método según la reivindicación 7 u 8, caracterizado por que los participantes (10) del grupo de base están conectados ya entre sí después de la creación del bloque de base (30).

11. Método según la reivindicación 10, caracterizado por que los participantes (10) se conectan en red entre sí para el intercambio de certificados en un entorno protegido.

12. Método según una de las reivindicaciones anteriores, caracterizado por que las transacciones (28) se almacenan en bloques (22), y los bloques (22) son creados según un algoritmo establecido.

13. Método según la reivindicación 12, caracterizado por que el algoritmo divide proporcionalmente los derechos para la creación de bloques entre los participantes (10).

14. Método según la reivindicación 12 o 13, caracterizado por que el algoritmo mide la distribución de las porciones entre los participantes (10) según la seguridad de los datos de los participantes (10) individuales.

15. Método según una de las reivindicaciones 12 a 14, caracterizado por que el algoritmo distribuye los derechos para la creación de los bloques según un método-pseudo-aleatorio.

16. Método según una de las reivindicaciones anteriores, caracterizado por que la decisión sobre la nueva admisión de un participante (10) es tomada por una persona.

17. Método según una de las reivindicaciones anteriores, caracterizado por que un participante (10) nuevo solamente es admitido en la red (2) como participante (10) autorizado cuando al menos una verificación de la factibilidad sobre el nuevo participante (10) es positiva utilizando informaciones de bloques (22) de una cadena de bloques (24).

18. Método según una de las reivindicaciones anteriores, caracterizado por que las transacciones (28) son almacenadas en bloques (22) y solamente se pueden insertar datos de participantes (10) registrados en un bloque de base (30) y de participantes (10) nuevos autorizados en estos bloques de datos (22).

19. Método según una de las reivindicaciones anteriores, caracterizado por que están registradas reglas fundamentales de la red (2) en un bloque de base (30).

20. Método según la reivindicación 19, caracterizado por que al menos una regla fundamental define la creación de reglas dinámicas.

21. Método según la reivindicación 19 o 20, caracterizado por que las reglas fundamentales de la red (2) están almacenadas en hardware en al menos un participante (10).

22. Método según una de las reivindicaciones anteriores, caracterizado por que los participantes (10) se conectan en red y se introduce una regla fundamental almacenada en un participante (10) durante la creación de un bloque de base (30) en éste.

23. Sistema militar conectado en red (2) con varios participantes (10) con medios para realizar un método según una de las reivindicaciones anteriores, en el que las transacciones (28) de los participantes (10) entre sí están almacenadas en una base de datos distribuida (20).

FIG 1

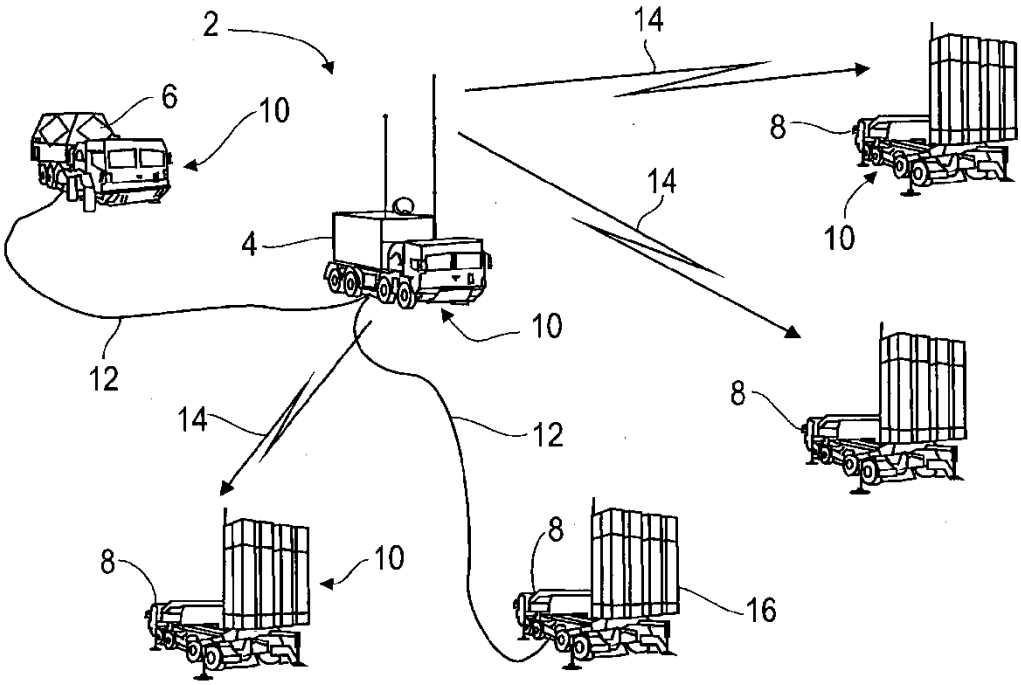

2
14
6
10
8
14
4
10
12
8
14
12
8
10
8
16

FIG 2

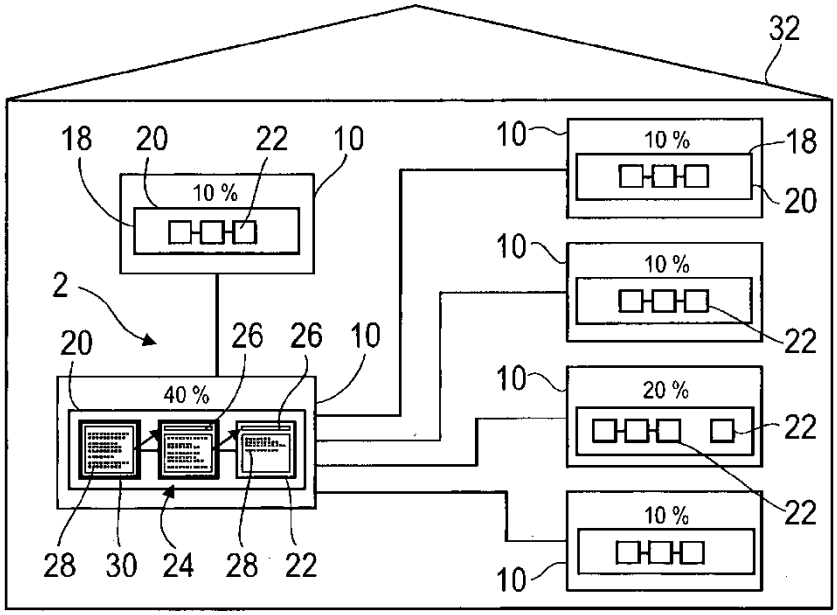

32
18
20
22
10
10 %
10
10 %
18
20
2
10
10 %
22
20
26
26
10
10
20 %
22
40 %
22
10 %
28
30
24
28
22
10

FIG 3

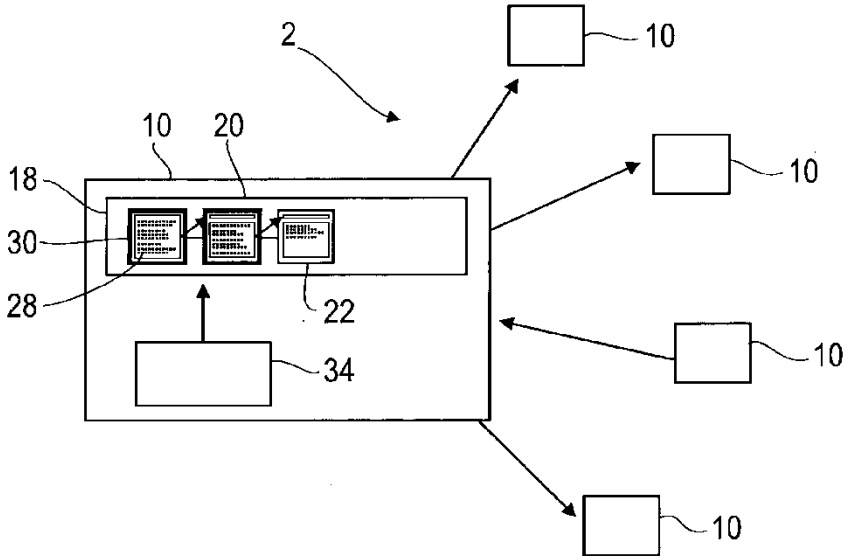
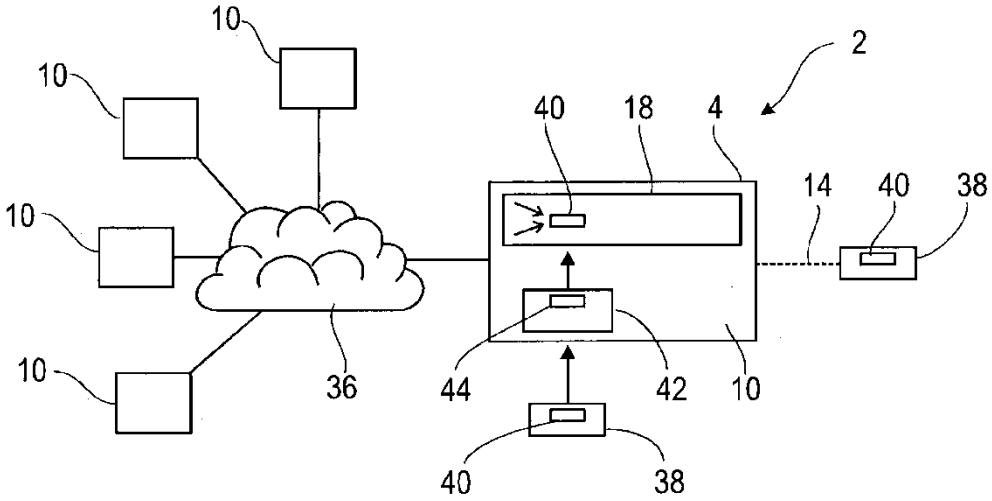

2
10
10
20
18
30
28
22
34
10
10
10

FIG 4


10
10
10
10
10
2
40
18
4
14
40
38
36
44
42
10
40
38