(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 367 986**

(51) Int. Cl.:
H04L 12/28 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03810359 .4**
(96) Fecha de presentación : **05.08.2003**
(97) Número de publicación de la solicitud: **1589695**
(97) Fecha de publicación de la solicitud: **26.10.2005**

(54) Título: **Un procedimiento para el acceso del terminal móvil a la red WLAN y para la comunicación de datos a través de la conexión inalámbrica de forma segura.**

(30) Prioridad: **06.11.2002 CN 02 1 39508**

(45) Fecha de publicación de la mención BOPI:
11.11.2011

(45) Fecha de la publicación del folleto de la patente:
11.11.2011

(73) Titular/es: **CHINA IWNCOMM Co., Ltd.**
4F.C Xietong Building, No. 12 Gaoxin 2nd Road
Xi'an, Shanxi 710075, CN

(72) Inventor/es: **Tie, Manxia;**
Tang, Houjian;
Zhang, Bianling;
Zhang, Ning y
Ye, Xumao

(74) Agente: **Botella Reyna, Antonio**

DESCRIPCIÓN

Un procedimiento para el acceso del terminal móvil a la red WLAN y para la comunicación de datos a través de la conexión inalámbrica de forma segura

Campo de la Invención

La presente invención se refiere a un procedimiento para el acceso de forma segura del terminal móvil a la Red de Área Local Inalámbrica (WLAN) y para la comunicación de datos de forma segura a través de una conexión inalámbrica, un producto de la combinación de la tecnología de comunicación inalámbrica con la tecnología de la encriptación.

Tecnología Antecedente

El objeto de la comunicación personal es permitirnos realizar cualquier comunicación en cualquier momento, en cualquier lugar y con cualquier otra persona, y disfrutar libremente de los múltiples servicios que ofrecen las redes. Incorporando las dos tecnologías populares, tales como la tecnología IP y la tecnología de comunicación inalámbrica, la tecnología WLAN sigue la tendencia del desarrollo de la banda ancha y proporciona una estructura principal móvil o un terminal móvil con los servicios de acceso a Internet convenientes y de alta velocidad para satisfacer la demanda creciente de la red de alta velocidad y los servicios de comunicación multimedia. La WLAN no solo soporta la computación móvil, sino también posee la flexibilidad, agilidad y capacidad de expansión de una infraestructura. La Fig. 1 es un diagrama que muestra la estructura de la red de acceso inalámbrico de banda ancha basada en WLAN que comprende principalmente dispositivos tales como el terminal móvil (MT), punto de acceso (AP) y servidor de acceso inalámbrico (WAS), en la que el MT sigue siendo móvil libremente, el AP realiza las funciones de gestión de las celdas, incluyendo la transferencia entre las celdas, la gestión y el puenteo del MT, y el WAS realiza la gestión de itinerancia del MT entre redes. Desde el acceso fijo al acceso inalámbrico móvil a Internet, la tecnología IP inalámbrica de banda ancha basada en WLAN ha supuesto un concepto completamente nuevo, y ha tenido un impacto tremendo en el entorno de la red en todo el mundo. El sistema, que es de una aplicación extraordinariamente amplia, es muy útil en redes comerciales (principalmente la intranet corporativa), redes de usuarios institucionales (por ejemplo, departamentos de seguridad publica, financieros y gubernamentales), redes de área (por ejemplo, colegios, hospitales, barrios residenciales, monitor remoto o monitor concentrado), redes temporales (por ejemplo, reuniones temporales), suscriptores móviles en exteriores y lugares a los que es difícil tender los cables y que están en cambio constante.

En lo que respecta a la WLAN, el problema de su seguridad es un asunto mucho más serio que para las redes cableadas. Para este asunto, se incorporan varios niveles de medios en la WLAN para abordar el problema. En primer lugar, proporcionar un ID de Conjunto de Servicios (SSID) diferente para cada AP y obligar al MT a presentar el SSID correspondiente en el momento del acceso para permitir a los usuarios de grupos diferentes acceder y restringir de forma diferenciada el derecho de acceso a los recursos. Sin embargo, hacer uso del SSID es una de las maneras más visuales de autenticación y el nivel relativamente bajo de la autenticación de seguridad, ya que cualquiera que conozca el SSID puede acceder a una red. En segundo lugar está la restricción de dirección, es decir, evitar el acceso no autorizado colocando, en el AP, la tabla de dirección de Control de Acceso al Medio (MAC) de la tarjeta inalámbrica del MT autorizado. Sin embargo, la dirección MAC de la tarjeta inalámbrica no es difícil de obtener y es posible falsificarla. Por lo tanto, es también una autenticación de nivel relativamente bajo de autorización. De todos modos, ninguna de las dos maneras puede controlar eficazmente el acceso del MT, y es aún es más imposible garantizar la confidencialidad de la comunicación.

Además de los dos procedimientos anteriores, una medida más ampliamente usada es la introducción, sobre la base de la Norma Internacional (IE-EE802.11) de la WLAN, a la WLAN del mecanismo de confidencialidad de la Privacidad Equivalente a Cables basado en RC-4 (WEP) para el cifrado y la transmisión de datos. El algoritmo WEP usa el sistema de claves individual, es decir, usa la misma clave secreta para el cifrado/descifrado, y la clave secreta es de 64 o 128 bits de longitud, en la que 40 o 104 bits son la parte fija conocida como clave secreta de iniciación, concretamente la dispuesta en el AP y el MT, y los 24 bits restantes son una parte variable conocida como el vector de iniciación, que se va a cambiar por el software controlador de la tarjeta de red en el procedimiento de comunicación. Es decir, la clave de cifrado es variable, lo que garantiza, hasta cierto punto, la confidencialidad de la comunicación inalámbrica. Sin embargo, debido a la regularidad de la variación del vector de iniciación, el algoritmo WEP no es lo bastante seguro. Esto se descubrió por primera vez por un equipo de investigación de la Universidad de California, Estados Unidos en Marzo de 2001. Señalaron que la WLAN del algoritmo WEP puede romperse en 5 horas por este motivo: asumieron que los cambios del vector de iniciación a la velocidad de adición de 1 por marco, cada marco es de 1500 bits de longitud, y la velocidad de transmisión de datos es de 11 megabits, entonces el vector de iniciación se repite en el periodo de 1500 bytes/marco x 8 bits/byte x 1 segundo/(11 x 106 bits) x 224 marco≈18300 segundos≈5 horas, es decir, el texto de dos marcos cifrado por la misma clave secreta se obtiene en el intervalo de 5 horas, y por lo tanto es posible adivinar o calcular el valor de la clave secreta de iniciación. Hay que señalar aquí que la longitud de la clave secreta no afecta a su tiempo de descifrado, pero complica el adivinarla o calcularla. En agosto de 2001, tres de los mejores expertos en descifrado del mundo, dos expertos del Weizmann Research Institute, Israel y un investigador de la Cisco (思科) Incorporation, realizaron una prueba de seguridad

WEP. Descifraron en una hora la clave secreta usada para la WLAN según una pequeña parte de datos tomados de la red. El AT&T Laboratory también ha realizado el descifrado de la misma manera. Éste sabe suficientemente que el WEP no puede garantizar la seguridad de la WLAN. La cuestión de la seguridad se ha convertido en uno de los obstáculos que bloquean la amplia aplicación de la WLAN, y el acceso seguro y la comunicación confidencial han sido la parte más importante en la investigación de la tecnología WLAN.

El documento XP-002392979 de M. Casole, "WLAN security-Status, Problems and Perspective", European Wireless 2002, describe que Hiperlan/2 soporta múltiples procedimientos de autenticación. En el procedimiento de autenticación basado en certificados, las entidades implicadas en la autenticación son el Punto de Acceso (AP) y el Terminal Móvil (MT), y la autenticación mutua realizada entre ellos se basa en un mecanismo de desafío/respuesta.

Según las enseñanzas, el Punto de Acceso (AP) extrae el certificado del Terminal Móvil (MT), y la cadena de certificados del mismo, del depositario de certificados, y verifica directamente si el certificado del Terminal Móvil (MT) y la cadena de certificados, así como la MT_RESPUESTA al AP_DESAFIO son válidos. Dicha verificación se realiza directamente en el dispositivo del Punto de Acceso (AP), por lo que el coste depende del rendimiento de la CPU, memoria, etc. del dispositivo.

Además, el Terminal Móvil (MT) verifica la AP_RESPUESTA al MT_DESAFIO, pero la solución técnica de esta referencia no se pronuncia sobre si el Terminal Móvil (MT) verifica el certificado del Punto de Acceso (AP).

Si el Terminal Móvil (MT) verifica el certificado del Punto de Acceso (AP), el Terminal Móvil (MT) debe inspeccionar la Lista de Revocación de Certificados (CRL) accediendo al depositario de certificados para determinar el estado del certificado del Punto de Acceso (AP). Pero el entorno operativo de la WLAN no tiene acceso directo del Terminal Móvil (MT) al depositario de certificados.

Si el Terminal Móvil (MT) no verifica el certificado del Punto de Acceso (AP), dicho esquema de Hiperlan/2 se convierte realmente en una autenticación de certificados de una vía que no puede evitar un ataque anterior al Punto de Acceso (AP).

El documento XP-002392979 propone una mejora con respecto al defecto de la complejidad de la computación del Punto de Acceso (AP) en Hiperlan/2, es decir, añadir un servidor externo para verificar el certificado del Terminal Móvil (MT) y la respuesta, y se opera un protocolo AAA típico (autenticación, autorización, contabilización) entre el Punto de Acceso (AP) y el servidor (consúltese el documento XP-002392979, 3.1.2 HIPERLAN/2).

Sin embargo, el esquema mejorado todavía tiene los siguientes defectos:

(1) el protocolo AAA (autenticación, autorización, contabilización) entre el Punto de Acceso (AP) y el servidor muestra que ha de preconfigurarse un canal seguro entre el Punto de Acceso (AP) y el servidor, pero esto aumenta directamente la complejidad de la estructura de la red y restringe la expansibilidad de la red;
(2) la adición del protocolo AAA hace que se de la autenticación entre el Terminal Móvil (MT) y el servidor, y se establezca una relación de confianza, después la relación de confianza se transfiere al Terminal Móvil (MT) y al Punto de Acceso (AP), pero este es un modo de autenticación indirecto;
(3) el servidor únicamente verifica el certificado y la respuesta del Terminal Móvil (MT), sin verificar el certificado del Punto de Acceso (AP), por lo que el estado del certificado del Punto de Acceso (AP) se considera naturalmente como válido, ya que el Terminal Móvil (MT) no puede verificar si el certificado del Punto de Acceso (AP) es valido, no puede realizar una autenticación de dos vías real, es decir, el esquema mejorado es todavía un esquema de autenticación de una vía.

El documento XP-002263321 "Security Solution in Ericsson Wireless LAN Systems" de Y. Kim, Ericsson, Mayo de 2001, describe una solución WLG (WLAN Guardián), en la que se añaden los elementos de red de seguridad WLG (WLAN Guardián) y la DBS (base de datos) a la red básica, en la que la WLG (WLAN Guardián) se localiza después del Punto de Accesos (AP), y la base de datos central DBS se localiza después de todas las WLG.

Cuando el Terminal Móvil (MT) accede a la red, la autenticación y la gestión de la clave secreta entre la WLG (WLAN Guardián) y el Terminal Móvil (MT) se realizan a través del IKE (Intercambio de Claves por Internet), a fin de que se construya un canal seguro entre el Terminal Móvil (MT) y la WLG (WLAN Guardián), y los datos pueden protegerse a través del protocolo IPSec.

Dicha solución tiene los siguientes defectos:

(1) el canal seguro es entre el Terminal Móvil (MT) y la WLG (WLAN Guardián) en lugar de entre el Terminal Móvil (MT) y el Punto de Acceso (AP), por lo que proporciona un servicio de seguridad a la capa de red en lugar de la capa de conexión inalámbrica;
(2) todas las WLG comparten un certificado, el sistema verifica el certificado del Terminal Móvil (MT) y el estado del mismo por la DBS, y el Terminal Móvil (MT) no verifica el estado del certificado en la WLG a través de la DBS (base de datos); en su lugar, el Terminal Móvil toma naturalmente el certificado del mismo como valido, por lo que este es

de hecho una autenticación de una vía y no puede conseguir la finalidad de seguridad de la autenticación de dos vías;
(3) las claves secretas han de compartirse entre las WLG y entre la WLG y la DBS, estas sin duda aumentarán la complejidad de la implantación de la red;
(4) la transmisión de los parámetros de asociación de seguridad entre la WLG y la DBS introduce un nuevo punto de ataque a la seguridad.

El documento EP-A-1 178 644 describe procedimientos de gestión de claves para las WLAN, en los que las claves de seguridad en los terminales móviles y puntos de acceso de una WLAN se crean, utilizan y gestionan para establecer una sesión de comunicación entre un terminal móvil y un punto de acceso. Tanto la protección de seguridad a nivel de una conexión WLAN como las funciones de seguridad en IP de la red usan el mismo protocolo de gestión de claves de Intercambio de Claves por Internet (IKE) y usan certificados en la misma jerarquía de certificados. Cuando el terminal móvil se asocia con la red, usa el protocolo IKE con claves y certificados privados para generar claves a nivel de conexión WLAN con el punto de acceso y proporcionan una autenticación mutua. Además, el documento US-A-5 371 794 describe un esquema de autenticación para garantizar la comunicación segura entre un Punto de Acceso (AP) y un Terminal Móvil (MT), es decir, el Terminal Móvil (MT) y el Punto de Acceso (AP) comprueban la exactitud del formato de los certificados entre sí, verificando los campos de firma de certificados entre sí; y verifican la firma entre ellos para comprobar si existe una clave privada que corresponda con el certificado.

De hecho, ambas partes únicamente han verificado el formato de los certificados y la exactitud de las claves privadas entre ellos, pero no verificaron si el estado actual de los certificados es válido. Por lo tanto, no consiguieron la finalidad de seguridad de autenticación y no pueden garantizar al suscriptor legal el uso de la red legal.

Resumen de la Invención

El objeto de la presente invención es superar las deficiencias técnicas que se han mencionado anteriormente y proporcionar un procedimiento para el acceso seguro del terminal móvil a la Red de Área Local Inalámbrica (WLAN) y para la comunicación de datos segura a través de una conexión inalámbrica. Combina la tecnología de cifrado de claves común y la tecnología de cifrado simétrico, resuelve la incapacidad de la WLAN para proporcionar un control eficaz en el acceso seguro del MT, y supera la confidencialidad limitada de la comunicación de datos a través de una comunicación inalámbrica, de tal forma que no solo ha logrado el control en el acceso del MT, sino que también garantiza la seguridad del acceso del MT y una alta confidencialidad de comunicación.

La presente invención proporciona un procedimiento para el acceso seguro del terminal móvil a la Red de Área Local Inalámbrica (WLAN) y para la comunicación de datos segura a través de una conexión inalámbrica, en el que, cuando el Terminal Móvil (MT) se conecta a un Punto de Acceso inalámbrico (AP), el certificado del Terminal Móvil (MT) y el certificado del Punto de Acceso (AP) se transmiten a un Servidor de Autenticación (AS) y se autentican a través del Servidor de Autenticación (AS), después el resultado de la autenticación se devuelve al Punto de Acceso (AP) y al Terminal Móvil (MT) con el fin de conseguir una autenticación de certificados de dos vías entre dicho Terminal Móvil (MT) y el Punto de Acceso (AP); y el Terminal Móvil (MT) y el Punto de Acceso (AP) realizan la negociación de la clave secreta para la conversación.

Según sus realizaciones preferidas, la presente invención ha proporcionado un procedimiento para el acceso seguro del terminal móvil a la Red de Área Local Inalámbrica (WLAN) y para la comunicación de datos segura a través de una conexión inalámbrica, en el que cuando el MT se conecta a un AP, el MT y el AP realizan dicha autenticación de certificados de dos vías a través del AS; después de que dicha autenticación de certificados de dos vías se realice con éxito, el MT y el AP realizan dicha negociación de la clave secreta para la conversación.

Según sus realizaciones preferidas, la presente invención ha proporcionado un procedimiento para el acceso seguro del terminal móvil a la Red de Área Local Inalámbrica (WLAN) y para la comunicación de datos segura a través de una conexión inalámbrica, en el que, cuando el MT se conecta al AP, el MT y el AP informan el uno al otro de sus respectivos certificados, y después realizan la negociación de la clave secreta para la conversación, y después de que dicha negociación de la clave secreta para la conversación se realiza, el MT y el AP realizan la autenticación de certificados de dos vías a través del AS, y determinan si el certificado usado por la otra parte es el mismo que el informado. Si no es así, la autenticación falla; si es así, el resultado de la autenticación depende del resultado de dicha identificación de certificados de dos vías.

Dicha identificación de certificados de dos vías comprende:

1) cuando el MT se conecta al AP, el MT envía al AP el mensaje de petición de autenticación de acceso que contiene el certificado del MT;
2) después de que el AP reciba dicho mensaje de petición de autenticación de acceso, añade el certificado del AP al mensaje, después envía al AS el mensaje de petición de autenticación de certificado que contiene dicho certificado del MT y el certificado del AP;
3) después de que el AS reciba dicho mensaje de petición de autenticación de certificado, el AS autentica el

certificado del AP y el certificado del MT en dicho mensaje, y después envía de vuelta al AP el mensaje de respuesta de autenticación de certificado con la firma del AS;

4) después de que el AP reciba dicho mensaje de respuesta de autenticación de certificado, el AP autentica la firma del AS, con el fin de obtener el resultado de la autenticación del certificado del MT, y después se envía de vuelta al MT el mensaje de respuesta de autenticación de certificado como el mensaje de respuesta de autenticación de acceso; y

5) después de que el MT reciba dicho mensaje de respuesta de autenticación de acceso, el MT autentica la firma del AS y obtiene el resultado de la autenticación del certificado del AP, a fin de completar dicha identificación de certificados de dos vías entre el MT y el AP.

Según sus realizaciones preferidas, la presente invención ha proporcionado un procedimiento para el acceso seguro del terminal móvil a la Red de Área Local Inalámbrica (WLAN) y para la comunicación de datos segura a través de una conexión inalámbrica, en el que 1) cuando el MT se conecta al AP, el MT envía al AP el mensaje de petición de autenticación de acceso que contiene el certificado del MT para realizar dicha autenticación de certificados de dos vías; 2) después de que el AP reciba dicho mensaje de petición de autenticación de acceso, añade el certificado del AP al mensaje, después envía al AS el mensaje de petición de autenticación de certificado que contiene dicho certificado del MT y el certificado del AP para realizar dicha autenticación de certificados de dos vías, y mientras tanto comienza con la negociación del MT de la clave secreta para la conversación; 3) después de que el AS reciba dicho mensaje de petición de autenticación de certificado, el AS autentica el certificado del AP y el certificado del MT en dicho mensaje, y después envía de vuelta al AP el mensaje de respuesta de autenticación de certificado con la firma del AS para realizar dicha autenticación de certificados de dos vías; 4) después de que el AP reciba dicho mensaje de respuesta de autenticación de certificado, el AP autentica la firma del AS, con el fin de obtener el resultado de la autenticación del certificado del MT, y después se envía de vuelta al MT el mensaje de respuesta de autenticación de certificado como el mensaje de respuesta de autenticación de acceso para realizar dicha autenticación de certificados de dos vías; y 5) después de que el MT reciba dicho mensaje de respuesta de autenticación de acceso, el MT autentica la firma del AS y obtiene el resultado de la autenticación del certificado del AP, con el fin de completar el procedimiento de dicha identificación de certificados de dos vías entre el MT y el AP, y después el MT realiza el procesamiento correspondiente para completar dicha negociación de la clave secreta para la conversación.

Según sus realizaciones preferidas, la presente invención ha proporcionado un procedimiento para el acceso seguro del terminal móvil a la Red de Área Local Inalámbrica (WLAN) y para la comunicación de datos segura a través de una conexión inalámbrica, en el que 1) cuando el MT se conecta al AP, el MT envía al AP el mensaje de petición de autenticación de acceso que contiene el certificado del MT para realizar dicha autenticación de certificados de dos vías; 2) después de que el AP reciba dicho mensaje de petición de autenticación de acceso, añade el certificado del AP al mensaje, después envía al AS el mensaje de petición de autenticación de certificado que contiene dicho certificado del MT y el certificado del AP para realizar dicha autenticación de certificados de dos vías; 3) después de que el AS reciba dicho mensaje de petición de autenticación de certificado, el AS autentica el certificado del AP y el certificado del MT en dicho mensaje, y después envía de vuelta al AP el mensaje de respuesta de autenticación de certificado que contiene la firma del AS para realizar dicha autenticación de certificados de dos vías; 4) después de que el AP reciba dicho mensaje de respuesta de autenticación de certificado, el AP autentica la firma del AS, con el fin de obtener el resultado de la autenticación del certificado del MT. El AP determina el resultado de la autenticación. Si la autenticación no tiene éxito, el AP envía de nuevo al MT dicho mensaje de respuesta de autenticación de certificado como el mensaje de respuesta de autenticación de acceso para realizar dicha autenticación de certificados de dos vías; si la autenticación es exitosa, el AP comienza a consultar con el MT la clave secreta para la conversación mientras que envía de vuelta al MT dicho mensaje de respuesta de autenticación de acceso; y 5) después de que el MT reciba dicho mensaje de respuesta de autenticación de certificado, el MT autentica la firma del AS y obtiene el resultado de la autenticación del certificado del AP, a fin de completar dicha identificación de certificados de dos vías entre el MT y el AP, y después el MT realiza el procesamiento correspondiente para completar dicha negociación de la clave secreta para la conversación.

Según sus realizaciones preferidas, la presente invención ha proporcionado un procedimiento para el acceso seguro del terminal móvil a la Red de Área Local Inalámbrica (WLAN) y para la comunicación de datos segura a través de una conexión inalámbrica, en el que 1) cuando el MT se conecta al AP, cada parte informa a la otra de su propio certificado, después completan dicha negociación de la clave secreta para la conversación, y, mientras tanto, el MT también completa la información del AP de la identificación de petición de autenticación de acceso; 2) el AP envía al AS el mensaje de petición de autenticación de certificado que contiene el certificado del MT y el certificado del AP para realizar dicha autenticación de certificados de dos vías; 3) después de que el AS reciba dicho mensaje de petición de autenticación de certificado, el AS autentica el certificado del AP y el certificado del MT en dicho mensaje, y después envía de vuelta al AP el mensaje de respuesta de autenticación de certificado que contiene la firma del AS para realizar dicha autenticación de certificados de dos vías; 4) después de que el AP reciba dicho mensaje de respuesta de autenticación de certificado, el AP autentica la firma del AS, con el fin de obtener el resultado de la autenticación del certificado del MT, y después envía de vuelta al MT dicho mensaje de respuesta de autenticación de certificado como el mensaje de respuesta de autenticación de acceso para realizar dicha autenticación de certificados de dos vías; y 5) después de que el MT reciba dicho mensaje de respuesta de autenticación de acceso, el MT autentica la firma del AS, y después determina si el certificado del AP en el mensaje

es el mismo del que ha informado el AP antes de la negociación de la clave secreta para la conversación. Si no es así, la autenticación falla; si es así, el MT obtiene el resultado de la autenticación del certificado del AP del mensaje, con el fin de completar dicho procedimiento de autenticación de certificados de dos vías entre el MT y el AP.

Dicho mensaje de petición de autenticación de acceso también comprende la identificación de petición de autenticación de acceso.

Dicho mensaje de petición de autenticación de certificado también comprende la identificación de petición de autenticación de acceso, o también comprende la identificación de petición de autenticación de acceso y la firma del AP.

Dicho mensaje de respuesta de autenticación de certificado también comprende, antes del registro de la firma del AS, la información del resultado de la autenticación del certificado del MT y la de la autenticación del certificado del AP.

Dicho mensaje de respuesta de autenticación de acceso es idéntico a dicho mensaje de respuesta de autenticación de certificado.

Dicha identificación de petición de autenticación de acceso es una cadena de datos aleatorios o un número de serie de autenticación.

Dicha información del resultado de la autenticación del certificado del MT comprende el certificado del MT, y el resultado de la autenticación del certificado del MT y la firma del AS, o comprende el certificado del MT y el resultado de la autenticación del certificado del MT.

Dicha información del resultado de la autenticación del certificado del AP comprende el certificado del AP, el resultado de la autenticación del certificado del AP, la identificación de petición de autenticación de acceso y la firma del AS, o comprende el certificado del AP, el resultado de la autenticación del certificado del AP y la identificación de petición de autenticación de acceso.

Cuando el MT quiere acceder al AP designado, en primer lugar el MT ha de obtener la información relevante del AP o el certificado del AP.

Dicha negociación de la clave secreta para la conversación se refiere al MT o al AP usando una clave común del AP o el MT y su clave privada respectiva para generar la clave secreta para la conversación.

En una de las realizaciones preferidas de la presente invención, la negociación de la clave secreta para la conversación comprende lo siguiente:

1) el MT elige en secreto un número entero a, a partir del cual calcular el número entero f(a), combina el número entero f(a) y la firma del MT en éste en el mensaje de petición de negociación de clave secreta, y lo transmite al AP; dicha f es una función que hace que el número entero a sea incalculable a partir del número entero f(a);
2) después de que reciba dicho mensaje de petición de negociación de clave secreta, el AP elige en secreto un número entero b, a partir del cual calcular el número entero f(b), forma el número entero f(b) y la firma del AP en éste en el mensaje de respuesta de negociación de clave secreta, y lo transmite al MT; dicha f es una función que hace que el número entero b sea incalculable a partir del número entero f(b); y
3) el AP calcula g(b, f(a)), y el MT calcula g(a, f (b)) después de que reciba dicho mensaje de respuesta de negociación de clave secreta, como la clave secreta para la conversación en el procedimiento de comunicación; dicha g es una función que hace posible el cálculo de g(a, f(b)) = g(b, f(a)).

En otra realización preferida de la presente invención, dicha negociación de la clave secreta para la conversación comprende lo siguiente:

1) el AP elige en secreto un número entero b, a partir del cual calcular el número entero f(b), combina el número entero f(b) y la firma del AP en éste en el mensaje de petición de negociación de clave secreta, y lo transmite al MT; dicha f es una función que hace que el número entero b sea incalculable a partir del número entero f(b);

2) después de que reciba dicho mensaje de petición de negociación de clave secreta, el MT elige en secreto un número entero a, a partir del cual calcular el número entero f(a), combina el número entero f(a) y la firma del MT en éste en el mensaje de respuesta de negociación de clave secreta, y lo transmite al AP; dicha f es una función que hace que el número entero a sea incalculable a partir del número entero f(a); y

3) el MT calcula g(a, f(a)), y el AP calcula g(a, f (b)) después de que reciba dicho mensaje de respuesta de clave secreta, como la clave secreta para la conversación en el procedimiento de comunicación; dicha g es una función que hace posible el cálculo de g(a, f(b)) = g(b, f(a)).

En otra realización preferida de la presente invención, la negociación de la clave secreta para la conversación comprende lo siguiente:

1) el MT o el AP genera una cadena de datos aleatorios, y los transmite como el mensaje de petición de negociación de clave secreta al AP o el MT después del cifrado usando la clave común del AP o el MT;
2) después de que reciba dicho mensaje de petición de negociación de clave secreta del MT o el AP, el AP o el MT usa su propia clave privada para el cifrado, obtiene los datos aleatorios generados por la otra parte; después el AP o el MP generan de nuevo una cadena de datos aleatorios; y los envía como el mensaje de respuesta de negociación de clave secreta al MT o al AP después del cifrado usando la clave común del MT o el AP; y
3) Después de que reciba dicho mensaje de respuesta de negociación de clave secreta del AP o el MT, el MT o el AP usa su propia clave privada para el cifrado, obtiene los datos aleatorios generados por la otra parte; tanto el MT como el AP utilizan los datos aleatorios generados por la otra parte y por sí mismos para generar la clave secreta para la conversación.

En otra realización preferida de la presente invención, la negociación de la clave secreta para la conversación comprende lo siguiente:

1) el MT o el AP generan una cadena de datos aleatorios, y, después de utilizar la clave común del AP o el MT para el cifrado, fija su propia firma como el mensaje de petición de negociación de clave secreta, y lo transmite al AP o el MT; y

2) después de que el AP o el MT reciban dicho mensaje de petición de negociación de clave secreta del MT o el AP, utiliza la clave común del MT o el AP para autenticar la firma, y después utiliza su propia clave privada para descifrar el mensaje cifrado recibido; tanto el MT como el AP usan los datos aleatorios como la clave secreta para la conversación.

Además, dicha negociación de la clave secreta para la conversación también puede comprende la negociación del algoritmo de comunicación usado en el procedimiento de comunicación.

La presente invención tiene las siguientes ventajas sobre la técnica anterior:

Ha resuelto el problema del fallo en la WLAN para tener un control eficaz del acceso seguro del MT, y superar la limitación de la confidencialidad de la comunicación de datos a través de la comunicación inalámbrica. Además, combina el sistema de cifrado de claves común y la tecnología de cifrado simétrica, ha realizado la autenticación de certificados de dos vías entre el MT y el AP, y además mejoró la seguridad de acceso; además, ha conseguido, a través de la negociación dinámica de la clave secreta para la conversación, la revisión dinámica de la clave secreta en el procedimiento de cada autenticación, la clave secreta y la comunicación, para conseguir la comunicación de datos segura, y aumentó en gran medida la dificultad del descifrado. En conclusión, el procedimiento no solo ha logrado el control en el acceso del MT, sino también ha garantizado la seguridad del acceso del MT y la alta confidencialidad de la comunicación.

Breve Descripción de los Dibujos

La Fig. 1 es un diagrama que muestra la estructura del sistema IP inalámbrico de banda ancha convencional;
La Fig. 2 es un diagrama de bloques que muestra la estructura lógica del sistema de autenticación de seguridad de la banda ancha basado en el AS de la presente invención;
La Fig. 3 es un diagrama de flujo de autenticación de la presente invención en el momento del acceso del MT.

Descripción de las Realizaciones Preferidas

La siguiente es una descripción adicional de la presente invención sobre la base de los dibujos y realizaciones.

La Fig. 2 es un diagrama de bloques que muestra la estructura lógica del sistema de autenticación de seguridad de la WLAN basado en el AS (Servidor de Autenticación). Se usa la tecnología de cifrado de claves común. Cuando el MT se conecta al AP, la autenticación de certificados de dos vías ha de realizarse usando el AS. Únicamente el MT que posea el certificado autorizado puede acceder al AP que posea el certificado autorizado, de lo contrario, el AP rechaza el acceso del MT o el MT rechaza la conexión al AP. Después de la autenticación con éxito, el MT y el AP realizan la negociación de la clave común para la conversación, usan la tecnología de cifrado simétrica para realizar la comunicación segura de datos a través de la conexión inalámbrica. El procedimiento completo es como se muestra en la Fig. 3, en la que el contenido del certificado comprende principalmente el número de serie del certificado, el nombre de la persona que autoriza el certificado, periodo de validez del certificado, nombre del titular del certificado, información de la clave común del titular del certificado, algoritmo de firma usado por la persona que autoriza el certificado y firma de la persona que autoriza el certificado en el certificado.

1. Autenticación de Certificados de Dos Vías

Cuando el MT se conecta al AP, las dos partes realizan la autenticación de certificados de dos vías a través del AS como se muestra en el siguiente flujo de trabajo:

a) Petición de autenticación de acceso. El MT envía al AP el mensaje de petición de autenticación de acceso, es decir, enviar al AP el certificado del MT y una cadena de datos aleatorios o un numero de serie de autenticación, en el que la cadena de datos aleatorios o el número de serie de autenticación se denominan identificación de petición de autenticación de acceso;

b) Petición de autenticación de certificados. Después de que reciba el mensaje de petición de autenticación de acceso del MT, el AP envía al AS el mensaje de petición de autenticación de certificado, es decir, enviar al AS el certificado del MT, la identificación de petición de autenticación de acceso y el certificado del AP o el certificado del MT, la identificación de petición de autenticación de acceso, y el mensaje de petición de autenticación de certificado constituido por la firma de la clave privada del AP en ellos;

c) Respuesta de la autenticación de certificados. Después de que el AS reciba el mensaje de petición de autenticación de certificado del AP, si el mensaje contiene la firma del AP, en primer lugar el AS autentica la firma en cuanto a su autenticidad. Si no es autentica, el resultado de la autenticación se determina como fallo. Entonces autentica el certificado del AP y el certificado del MT en cuanto a su legitimidad. Cuando la autenticación esté hecha, el AS enviará de vuelta al AP [1] la información del resultado de la autenticación del certificado del MT incluyendo el certificado del MT y el resultado de la autenticación del certificado del MT, y la firma del AS en ellos, o únicamente incluyendo el certificado del MT y el resultado de la autenticación del certificado del MT, [2] la información del resultado de la autenticación del certificado del AP incluyendo el certificado del AP y el resultado de la autenticación del AP y la identificación de petición de autenticación de acceso, y la firma del AS en ellos, o solo incluyendo el certificado del AP y el resultado de la autenticación del certificado del AP, y la identificación de petición de autenticación de acceso, y [3] el mensaje de las respuestas de autenticación de certificados constituidos por las firmas del AS en [1] y [2];

d) Respuesta de la autenticación de acceso. El AP autentica la firma en el mensaje de respuesta de autenticación de certificado enviado de vuelta por el AS, y obtiene el resultado de la autenticación de certificados del MT. El AP envía de nuevo al MT el mensaje de respuesta de autenticación de certificado como el mensaje de respuesta de autenticación de acceso;

e) el MT autentica la firma en el mensaje de respuesta de la autenticación enviado de vuelta por el AP, y obtiene el resultado de la autenticación del certificado del AP.

Ahora, el procedimiento de autenticación de certificados de dos vías se ha completado entre el MT y el AP. Su sus certificados se autentican con éxito, el AP permite al MT acceder, o rechaza su acceso, o el MT rechaza conectarse al AP. Ahora, el MT que tiene el certificado autorizado ha accedido con éxito al AP que tiene el certificado autorizado, y se ha completado la función del AP para controlar el acceso seguro del MT.

2. Negociación de la Clave Secreta para la Conversación

Después de que la autenticación de certificados de dos vías del MT y el AP se realice con éxito, es decir, conseguir la entrada con éxito del MT, entonces las dos partes usan cada clave común del otro y su propia clave privada respectiva para generar en el mismo la clave secreta para la conversación que se va a usar para el cifrado y descifrado de los mensajes de datos de comunicación, con el fin de realizar la comunicación inalámbrica segura y confidencial entre el MT y el AP. Sin embargo, vale la pena señalar que en el periodo de validez del certificado, la clave secreta para la conversación entre el MT y el AT permanece inalterada. Con el fin de realizar cada autenticación de cada clave secreta, es necesaria la negociación dinámica de la clave secreta para la conversación. La negociación dinámica de la clave secreta para la conversación procede como se indica a continuación:

a) La petición de negociación de clave secreta. El MT o el AP genera una cadena de datos aleatorios, y, después del cifrado usando la clave común del AP y el MT, envía al AP o al MT el mensaje de petición de negociación de clave secreta;

b) La respuesta de negociación de clave secreta. Después de que el AP o el MT reciba el mensaje de petición de negociación de clave secreta enviado desde el MT o el AP, el AP o el MT usa su propia clave privada para el cifrado, y obtiene los datos aleatorios generados por la otra parte. Después, genera localmente una cadena de datos aleatorios, y, después del cifrado usando la clave común del MT o el AP, responde al MT o al AP con respecto al mensaje de respuesta de negociación de clave secreta;

c) Después de que el MT o el AP reciba el mensaje de respuesta de negociación de clave secreta enviado desde el AP o el MT, el MT o el AP usa su propia clave privada para el cifrado, y obtiene los datos aleatorios de la otra parte; tanto el MT como el AP usan los dos datos aleatorios generados por sí mismos o la otra parte para generar la clave secreta para la conversación que se va a usar para el cifrado y el descifrado de los mensajes de datos de la comunicación.

Para mejorar adicionalmente la confidencialidad de la comunicación, después de que el MT y el AP realicen la comunicación durante un periodo de tiempo o intercambien una determinada cantidad de mensajes, la negociación de la clave secreta para la conversación puede realizarse una vez más.

La autenticación de certificados de dos vías completa el acceso seguro del MT y la negociación de la clave secreta para la conversación garantiza completamente la comunicación altamente confidencial entre el MT y el AP.

Especialmente se ha señalado que:

(1) Si el MT intenta acceder al AP designado, el MT debe, antes de la autenticación de certificados de dos vías, conocer aproximadamente la información relevante del AP o cumplir el certificado del AP, con el fin de que el MT determine el mensaje de respuesta de autenticación de acceso que recibe;

(2) La negociación de la clave secreta para la conversación también puede comprender la negociación de los algoritmos de comunicación, es decir, en el mensaje de petición de negociación de clave secreta se enumeran los algoritmos de comunicación soportados por la parte solicitante. La parte que responde elige uno de los algoritmos de comunicación proporcionados por la parte solicitante, y lo envía de vuelta a la parte solicitante a través del mensaje de respuesta de negociación de clave secreta. Después de que se complete la negociación de la clave secreta para la conversación, las dos partes usan el algoritmo de comunicación de negociación para realizar la comunicación confidencial.

(3) La negociación dinámica de la clave secreta para la conversación también puede realizarse como se indica a continuación. El MT o el AP genera localmente una cadena de datos aleatorios, fija su propia firma, y la envía a la otra parte después del cifrado, usando la clave común de la otra parte. Después de que el AP o MT la reciban, el AP o el MT usa la clave común de la otra parte para autenticar si este es el dato enviado por la otra parte, entonces usa su propia clave privada para descifrar el mensaje que recibe. Las dos partes usan los datos aleatorios como clave secreta para la conversación para descifrar los datos de comunicación.

(4) La negociación de la clave secreta para la conversación también puede proceder como se indica a continuación:

a) el MT elige en secreto un número entero a, calcula f(a), envía al AP f(a) y la firma del MT en éste, en el que f es una función que hace que el número entero a sea incalculable a partir del número entero f(a);

b) el AP elige en secreto un número entero b, calcula f(b), envía al MT f(b) y la firma del MT en éste, en el que la definición de la función f es la misma que en a);

c) el MT calcula g(a, f(a)) y el AP calcula g(b, f(a)), como la clave secreta para la conversación en el procedimiento de comunicación, en el que g es una función que hace posible el cálculo de g(a, f(b)) = g(b, f(a)).

(5) Como se ha mencionado anteriormente, realizar en primer lugar la autenticación de certificados de dos vías y después la negociación de la clave secreta para la conversación, pero en la implementación específica del procedimiento, también puede ser que la negociación de la clave secreta para la conversación se realice antes de la autenticación de certificados de dos vías, o los dos procedimientos se realicen juntos o alternativamente.

(6) La negociación de la clave secreta para la conversación es primero, y la autenticación de certificados de dos vías se realiza después específicamente como se indica a continuación:

a) Cuando el MT se conecta al AP, las dos partes informan la una a la otra de sus respectivos certificados;

b) Usando dicho procedimiento, el MT y el AP realizan la negociación de la clave secreta para la conversación;

c) Usando dicho procedimiento, el MT y el AP realizan la autenticación de certificados de dos vías, y determinan si el certificado usado por la otra parte es el mismo que el certificado informado por éste en la etapa a). Si no es así, la autenticación falla; o el resultado de la autenticación depende del resultado del proceso de la autenticación de certificados de dos vías.

(7) La autenticación de certificados de dos vías y la negociación de la clave secreta para la conversación se realizan de forma alterna como se indica a continuación:

Los procedimientos de autenticación de certificados de dos vías y la negociación de la clave secreta para la conversación son exactamente los mismos que anteriormente. La diferencia radica únicamente en la alternancia de la secuencia de mensajes. Es decir, cuando el MT se conecta al AP, el MT envía al AP el mensaje de petición de autenticación de acceso. Después de que reciba el mensaje, el AP, mientras envía al AS el mensaje de petición de autenticación de certificado, comienza la negociación con el MT de la clave secreta para la conversación, de tal forma que la autenticación de certificados de dos vías y la negociación de la clave secreta para la conversación se

realizan alternativamente a una velocidad mayor que la ejecución por separado.

(8) La autenticación de certificados de dos vías y la negociación de la clave secreta para la conversación se realizan en combinación como se indica a continuación:

Cuando el MT se conecta al AP, las dos partes en primer lugar realizan la autenticación de certificados de dos vías, y después la negociación de la clave secreta para la conversación. Pero cuando la autenticación está a punto de terminarse, es decir, el AP, mientras que envía de vuelta al MT el mensaje de respuesta de autenticación de acceso, comienza la negociación con el MT de la clave secreta para la conversación, es decir, puede añadir la información de petición de negociación de clave secreta al mensaje de respuesta de autenticación de acceso, de tal forma que la autenticación de certificados de dos vías y la negociación de la clave secreta para la conversación se realizan en combinación a una velocidad mayor que la ejecución por separado.

(9) La autenticación de certificados de dos vías y la negociación de la clave secreta para la conversación también pueden realizarse de la siguiente manera. Es decir, el procedimiento se simplifique en primer lugar realizando la negociación de la clave secreta para la conversación, y después la autenticación de certificados de dos vías. En el procedimiento en el que el MT y el AP informan el uno al otro de sus respectivos certificados y realizan la negociación de la clave secreta para la conversación, el MT también debe informar al AP de la identificación de petición de autenticación de acceso. Por lo tanto, después de realizar la autenticación de certificados de dos vías, el MT no necesita enviar al AP el mensaje de petición de autenticación de acceso. En su lugar, el AP envía directamente al AS el mensaje de petición de autenticación de certificado y comienza la autenticación de certificados de dos vías. Cuando el procedimiento de autenticación se completa, esto es únicamente necesario para el MT para determinar si el certificado usado por el AP es el mismo que el certificado del que informó el AP antes de la negociación de la clave secreta para la conversación. Si no es así, la autenticación falla; si es así, el resultado de la autenticación depende del resultado del proceso de la autenticación de certificados de dos vías.

REIVINDICACIONES

1. Un procedimiento para el acceso seguro del terminal móvil a la Red de Área Local Inalámbrica, WLAN, y para la comunicación de datos segura a través de una conexión inalámbrica, en el que cuando el Terminal Móvil (MT) se conecta a un Punto de Acceso (AP) inalámbrico, el certificado del Terminal Móvil (MT) y el certificado del Punto de Acceso (AP) se transmiten a un Servidor de Autenticación (AS) y se autentifican a través del Servidor de Autenticación (AS), después la autenticación resultado del certificado del Terminal Móvil (MT) y el certificado del Punto de Acceso (AP) se devuelve al Punto de Acceso (AP) y el Terminal Móvil (MT) con el fin de conseguir una autenticación de certificado dos vías entre dicho Terminal Móvil (MT) y el Punto de Acceso (AP); y el Terminal Móvil (MT) y el Punto de Acceso (AP) realizan la negociación de la clave secreta para la conversación.

2. El procedimiento de acuerdo con la reivindicación 1, en el que:

cuando el Terminal Móvil (MT) se conecta a un Punto de Acceso (AP), el Terminal Móvil (MT) y Punto de Acceso (AP) realiza dicha autenticación de certificados de dos vías a través del Servidor de Autenticación (AS); después de que se haya realizado con éxito dicha autenticación de certificados de dos vías, el Terminal Móvil (MT) y el Punto de Acceso (AP) realizan dicha negociación de la clave secreta para la conversación.

3. El procedimiento de acuerdo con la reivindicación 1, en el que:

cuando el Terminal Móvil (MT) se conecta a un Punto de Acceso (AP), el Terminal Móvil (MT) y el Punto de Acceso (AP) se informan el uno al otro de sus respectivos certificados, y después, realizan la negociación de la clave secreta para la conversación; después de que se haya completado dicha negociación de la clave secreta para la conversación, el Terminal Móvil (MT) y el Punto de Acceso (AP) realizan dicha autenticación de certificados de dos vías a través del Servidor de Autenticación (AS), y mientras tanto determinan si el certificado usado por la otra parte es el mismo del que se ha informado por éste; si no es así, la autenticación falla; si es así, el resultado de la autenticación depende del resultado de dicha identificación de certificado de dos vías.

4. El procedimiento de acuerdo con las reivindicaciones 1, 2 ó 3, en el que: dicha autenticación de certificados de dos vías comprende las etapas de:

1) cuando el Terminal Móvil (MT) se conecta a un Punto de Acceso (AP), el Terminal Móvil (MT) envía al Punto de Acceso (AP) el mensaje de petición de autenticación de acceso que contiene el certificado del Terminal Móvil (MT);

2) después de que el Punto de Acceso (AP) reciba dicho mensaje de petición de autenticación de acceso, éste añade el certificado del Punto de Acceso (AP) al mensaje, después envía al Servidor de Autenticación (AS) el mensaje de petición de autenticación de certificado que contiene dicho certificado del Terminal Móvil (MT) y el certificado del Punto de Acceso (AP);

3) después de que el Servidor de Autenticación (AS) reciba dicho mensaje de petición de autenticación de certificado, el Servidor de Autenticación (AS) autentica el certificado del Punto de Acceso (AP) y el certificado del Terminal Móvil (MT) en dicho mensaje, y después envía de vuelta al Punto de Acceso (AP) el mensaje de respuesta de autenticación de certificado que contiene la firma del Servidor de Autenticación (AS);

4) después de que el Punto de Acceso (AP) reciba dicho mensaje de respuesta de autenticación de certificado, el Punto de Acceso (AP) autentica la firma del Servidor de Autenticación (AS), para obtener el resultado de la autenticación del certificado del Terminal Móvil (MT), y después envía de vuelta al Terminal Móvil (MT) el mensaje de respuesta de autenticación de certificado como el mensaje de respuesta de autenticación de acceso; y

5) después de que el Terminal Móvil (MT) reciba dicho mensaje de respuesta de autenticación de acceso, Terminal Móvil (MT) autentica la firma del Servidor de Autenticación (AS) y obtiene el resultado de la autenticación del certificado del Punto de Acceso (AP), con el fin de completar dicha identificación de certificados de dos vías entre el Terminal Móvil (MT) y el Punto de Acceso (AP).

5. El procedimiento de acuerdo con la reivindicación 1, en el que:

1) cuando el Terminal Móvil (MT) se conecta a un Punto de Acceso (AP), el Terminal Móvil (MT) envía al Punto de Acceso (AP) el mensaje de petición de autenticación de acceso que contiene el certificado del Terminal Móvil (MT) para realizar dicha autenticación de certificados de dos vías;

2) después de que el Punto de Acceso (AP) reciba dicho mensaje de petición de autenticación de acceso, éste añade el certificado del Punto de Acceso (AP) al mensaje, después envía al Servidor de Autenticación (AS) el mensaje de petición de autenticación de certificado que contiene dicho certificado del Terminal Móvil (MT) y el certificado del Punto de Acceso (AP) para realizar dicha autenticación de certificados de dos vías, y mientras tanto comienza con el Terminal Móvil (MT) la negociación de la clave secreta para la conversación;

3) después de que el Servidor de Autenticación (AS) reciba dicho mensaje de petición de autenticación de certificado, el Servidor de Autenticación (AS) autentica el certificado del Punto de Acceso (AP) y el certificado del Terminal Móvil (MT) en dicho mensaje, y después envía de vuelta al Punto de Acceso (AP) el mensaje de respuesta de autenticación de certificado que contiene la firma del Servidor de Autenticación (AS) para realizar dicha autenticación de certificados de dos vías;

4) después de que el Punto de Acceso (AP) reciba dicho mensaje de respuesta de autenticación de certificado, el Punto de Acceso (AP) autentica la firma del Servidor de Autenticación (AS), para obtener el resultado de la autenticación del certificado del Terminal Móvil (MT), y después envía de vuelta al Terminal Móvil (MT) el mensaje de respuesta de autenticación de certificado como el mensaje de respuesta de autenticación de acceso para realizar dicha autenticación de certificados de dos vías; y

5) después de que el Terminal Móvil (MT) reciba dicho mensaje de respuesta de autenticación de acceso, el Terminal Móvil (MT) autentica la firma del Servidor de Autenticación (AS) y obtiene el resultado de la autenticación del certificado del Punto de Acceso (AP), para completar el procedimiento de dicha identificación de certificado de dos vías entre el Terminal Móvil (MT) y el Punto de Acceso (AP), y después el Terminal Móvil (MT) realiza el procesamiento correspondiente para completar dicha negociación de la clave secreta para la conversación.

6. El procedimiento de acuerdo con la reivindicación 1, en el que:

1) cuando el Terminal Móvil (MT) se conecta a un Punto de Acceso (AP), el Terminal Móvil (MT) envía al Punto de Acceso (AP) el mensaje de petición de autenticación de acceso que contiene el certificado del Terminal Móvil (MT) para realizar dicha autenticación de certificados de dos vías;

2) después de que el Punto de Acceso (AP) reciba dicho mensaje de petición de autenticación de acceso, éste añade el certificado del Punto de Acceso (AP) al mensaje, después envía al Servidor de Autenticación (AS) el mensaje de petición de autenticación de certificado que contiene dicho certificado del Terminal Móvil (MT) y el certificado del Punto de Acceso (AP) para realizar dicha autenticación de certificados de dos vías;

3) después de que el Servidor de Autenticación (AS) reciba dicho mensaje de petición de autenticación de certificado, el Servidor de Autenticación (AS) autentica el certificado del Punto de Acceso (AP) y el certificado del Terminal Móvil (MT) en dicho mensaje, y después envía de vuelta al Punto de Acceso (AP) el mensaje de respuesta de autenticación de certificado que contiene la firma del Servidor de Autenticación (AS) para realizar dicha autenticación de certificados de dos vías;

4) después de que el Punto de Acceso (AP) reciba dicho mensaje de respuesta de autenticación de certificado, el Punto de Acceso (AP) autentica la firma del Servidor de Autenticación (AS), para obtener el resultado de la autenticación del certificado del Terminal Móvil (MT); el Punto de Acceso (AP) determina el resultado de la autenticación; si la autenticación no tiene éxito, el Punto de Acceso (AP) envía de vuelta al Terminal Móvil (MT) dicho mensaje de respuesta de autenticación de certificado como el mensaje de respuesta de autenticación de acceso para realizar dicha autenticación de certificados de dos vías; si la autenticación es exitosa, el Punto de Acceso (AP) empieza a consultar con el Terminal Móvil (MT) la clave secreta para la conversación mientras que envía de vuelta al Terminal Móvil (MT) dicho mensaje de respuesta de autenticación de acceso; y

5) después de que el Terminal Móvil (MT) reciba dicho mensaje de respuesta de autenticación de certificado, el Terminal Móvil (MT) autentica la firma del Servidor de Autenticación (AS) y obtiene el resultado de la autenticación del certificado del Punto de Acceso (AP), con el fin de completar dicha identificación de certificado de dos vías entre el Terminal Móvil (MT) y el Punto de Acceso (AP), y después el Terminal Móvil (MT) realiza el procesamiento correspondiente para completar dicho procedimiento de negociación de la clave secreta para la conversación.

7. El procedimiento de acuerdo con la reivindicación 1, en el que:

1) cuando el Terminal Móvil (MT) se conecta a un Punto de Acceso (AP), cada parte informa a la otra de su propio certificado, después completan dicha negociación de la clave secreta para la conversación, y, mientras tanto, el Terminal Móvil (MT) también completa informando al Punto de Acceso (AP) de la identificación de petición de autenticación de acceso;

2) el Punto de Acceso (AP) envía al Servidor de Autenticación (AS) el mensaje de petición de autenticación de certificado que contiene el certificado del Terminal Móvil (MT) y el certificado del Punto de Acceso (AP) para realizar dicha autenticación de certificados de dos vías;

3) después de que el Servidor de Autenticación (AS) reciba dicho mensaje de petición de autenticación de certificado, el Servidor de Autenticación (AS) autentica el certificado del Punto de Acceso (AP) y el certificado del Terminal Móvil (MT) en dicho mensaje, y después envía de vuelta al Punto de Acceso (AP) el mensaje de respuesta de autenticación de certificado que contiene la firma del Servidor de Autenticación (AS) para realizar dicha autenticación de certificados de dos vías;

4) después de que el Punto de Acceso (AP) reciba dicho mensaje de respuesta de autenticación de certificado, El Punto de Acceso (AP) autentica la firma del Servidor de Autenticación (AS) con el fin de obtener el resultado de la autenticación del certificado del Terminal Móvil (MT), y después envía de vuelta al Terminal Móvil (MT) dicho mensaje de respuesta de autenticación de certificado como el mensaje de respuesta de autenticación de acceso para realizar dicha autenticación de certificados de dos vías; y

5) después de que el Terminal Móvil (MT) reciba dicho mensaje de respuesta de autenticación de acceso, el Terminal Móvil (MT) autentica la firma del Servidor de Autenticación (AS), y después determina si el certificado del Punto de Acceso (AP) es el mismo del que informó el Punto de Acceso (AP) antes de la negociación de la clave secreta para la conversación; si no es así, la autenticación falla; si es así, el Terminal Móvil (MT) obtiene el resultado de la autenticación del certificado del Punto de Acceso (AP) a partir del mensaje, con el fin de completar dicho procedimiento de autenticación de certificados de dos vías entre el Terminal Móvil (MT) y el Punto de Acceso (AP).

8. El procedimiento de acuerdo con la reivindicación 4, 5 ó 6, en el que: dicho mensaje de petición de autenticación de acceso también comprende la identificación de petición de autenticación de acceso.

9. El procedimiento de acuerdo con la reivindicación 4, 5, 6 ó 7, en el que: dicho mensaje de petición de autenticación de certificado también comprende la identificación de petición de autenticación de acceso, o también comprende la identificación de petición de autenticación de acceso y la firma del Punto de Acceso (AP).

10. El procedimiento de acuerdo con la reivindicación 4, 5, 6 ó 7, en el que: dicho mensaje de respuesta de autenticación de certificado también comprende, antes de la firma registrada del Servidor de Autenticación (AS), la información del resultado de la autenticación del certificado del Terminal Móvil (MT) y la de la autenticación del certificado del Punto de Acceso (AP).

11. El procedimiento de acuerdo con la reivindicación 4, 5, 6 ó 7, en el que: dicho mensaje de respuesta de autenticación de acceso es idéntico al de dicho mensaje de respuesta de autenticación de certificado.

12. El procedimiento de acuerdo con la reivindicación 7, 8 ó 9, en el que: dicha identificación de petición de autenticación de acceso es una cadena de datos aleatorios o un número de serie de autenticación.

13. El procedimiento de acuerdo con la reivindicación 10 u 11, en el que: dicha información del resultado de la autenticación del certificado del Terminal Móvil (MT) comprende el certificado del Terminal Móvil (MT), y el resultado de la autenticación del certificado del Terminal Móvil (MT) y la firma del Servidor de Autenticación (AS), o comprende el certificado del Terminal Móvil (MT) y el resultado de la autenticación del certificado del Terminal Móvil (MT).

14. El procedimiento de acuerdo con la reivindicación 10 u 11, en el que: dicha información del resultado de la autenticación del certificado del Punto de Acceso (AP) comprende el certificado del Punto de Acceso (AP), el resultado de la autenticación del certificado del Punto de Acceso (AP), la identificación de petición de autenticación de acceso y la firma del Servidor de Autenticación (AS), o comprende el certificado del Punto de Acceso (AP), el resultado de la autenticación del certificado del Punto de Acceso (AP) y la identificación de petición de autenticación de acceso.

15. El procedimiento de acuerdo con la reivindicación 1, 2, 3, 5, 6 ó 7, en el que: cuando el Terminal Móvil (MT) intenta acceder al Punto de Acceso (AP) designado, en primer lugar, el Terminal Móvil (MT) ha de obtener la información relevante del Punto de Acceso (AP) o el certificado del Punto de Acceso (AP).

16. El procedimiento de acuerdo con la reivindicación 1, 2, 3, 5, 6 ó 7, en el que: dicha negociación de la clave secreta para la conversación se refiere al Terminal Móvil (MT) o el Punto de Acceso (AP) usando una clave común del Punto de Acceso (AP) o del Terminal Móvil (MT) y sus propias claves privadas respectivas para generar la clave secreta para la conversación.

17. El procedimiento de acuerdo con la reivindicación 1, 2, 3, 5, 6 ó 7, en el que: dicha negociación de la clave secreta para la conversación comprende:

1) el Terminal Móvil (MT) elige en secreto un número entero a, a partir del cual calcular el número entero f(a), combina el número entero f(a) y la firma del Terminal Móvil (MT) en éste en el mensaje de petición de negociación de clave secreta, y lo transmite al Punto de Acceso (AP); dicha f es una función que hace que el número entero a sea incalculable a partir del número entero f(a);

2) después de que reciba dicho mensaje de petición de negociación de clave secreta, el Punto de Acceso (AP) elige en secreto un número entero b, a partir del cual calcular el número entero f(b), combina el número entero f(b) y la firma del Punto de Acceso (AP) en éste en el mensaje de respuesta de negociación de clave secreta, y lo transmite al Terminal Móvil (MT); dicha f es una función que hace que el número entero b sea incalculable a partir del número entero f(b); y

3) el Punto de Acceso (AP) calcula g(b, f(a)), y el Terminal Móvil (MT) calcula g(a, f(b)) que después recibe dicho mensaje de respuesta de negociación de clave secreta, como la clave secreta para la conversación en el procedimiento de comunicación; dicha g es una función que hace posible el calculo de g(a, f(b)) = g(b, f (a)).

18. El procedimiento de acuerdo con la reivindicación 1, 2, 3, 5, 6 ó 7, en el que: dicha negociación de la clave secreta para la conversación comprende:

1) el Punto de Acceso (AP) elige en secreto un número entero b, a partir del cual calcular el número entero f(b), combina el número entero f(b) y la firma del Punto de Acceso (AP) en éste en el mensaje de petición de negociación de clave secreta, y lo transmite al Terminal Móvil (MT); dicha f es una función que hace que el número entero b sea incalculable a partir del número entero f(b);

2) después recibe dicho mensaje de petición de negociación de clave secreta, el Terminal Móvil (MT) elige en secreto un número entero a, a partir del cual calcular el número entero f(a), forma el número entero f(a) y la firma del Terminal Móvil (MT) en éste en el mensaje de respuesta de negociación de clave secreta, y lo transmite al Punto de Acceso (AP); dicha f es una función que hace que el número entero a sea incalculable a partir del número entero f(a); y

3) el Terminal Móvil (MT) calcula g(a, f(a)), y el Punto de Acceso (AP) calcula g(a, f(b)) que después recibe dicho mensaje de respuesta de clave secreta, como la clave secreta para la conversación en el proceso de comunicación; dicha g es una función que hace posible el calculo de g(a, f(b)) = g(b, f(a)).

19. El procedimiento de acuerdo con la reivindicación 1, 2, 3, 5, 6 ó 7, en el que: dicha negociación de la clave secreta para la conversación comprende:

1) el Terminal Móvil (MT) o el Punto de Acceso (AP) genera una cadena de datos aleatorios, y los envía al Punto de Acceso (AP) o el Terminal Móvil (MT) como el mensaje de petición de negociación de clave secreta después de la encriptación usando la clave común del Punto de Acceso (AP) o del Terminal Móvil (MT);

2) después recibe dicho mensaje de petición de negociación de clave secreta del Terminal Móvil (MT) o del Punto de Acceso (AP), el Punto de Acceso (AP) o el Terminal Móvil (MT) que usa su propia clave privada para el descifrado, obtiene los datos aleatorios generados por la otra parte; después el Punto de Acceso (AP) o el MP genera de nuevo una cadena de datos aleatorios; y los envía al Terminal Móvil (MT) o al Punto de Acceso (AP) como el mensaje de respuesta de negociación de clave secreta después del cifrado usando la clave común del Terminal Móvil (MT) o el Punto de Acceso (AP); y

3) después recibe dicho mensaje de respuesta de negociación de clave secreta del Punto de Acceso (AP) o el Terminal Móvil (MT), el Terminal Móvil (MT) o el Punto de Acceso (AP), que usa su propia clave privada para el descifrado, obtiene los datos aleatorios generados por la otra parte; tanto el Terminal Móvil (MT) como el Punto de Acceso (AP) utilizan los datos aleatorios generados por la otra parte y por sí mismos para generar la clave secreta para la conversación.

20. El procedimiento de acuerdo con la reivindicación 1, 2, 3, 5, 6 ó 7, en el que: dicha negociación de la clave secreta para la conversación comprende:

1) el Terminal Móvil (MT) o el Punto de Acceso (AP) genera una cadena de datos aleatorios y, después utiliza la clave común del Punto de Acceso (AP) o el Terminal Móvil (MT) para el cifrado, adjunta su propia firma como el mensaje de petición de negociación de clave secreta, y lo transmite al Punto de Acceso (AP) o al Terminal Móvil (MT); y

2) después el Punto de Acceso (AP) o el Terminal Móvil (MT) recibe dicho mensaje de petición de negociación de clave secreta del Terminal Móvil (MT) o el Punto de Acceso (AP), utiliza la clave común del Terminal Móvil (MT) o el Punto de Acceso (AP) para autenticar la firma, y después utiliza su propia clave privada para descifrar el mensaje cifrado recibido tanto en el Terminal Móvil (MT) como en el Punto de Acceso (AP) que usan los datos aleatorios como la clave secreta para la conversación.

21. El procedimiento de acuerdo con la reivindicación 17, 18 ó 19, en el que: dicha negociación de la clave secreta para la conversación también comprende posiblemente la negociación del algoritmo de comunicación usado en el procedimiento de comunicación.

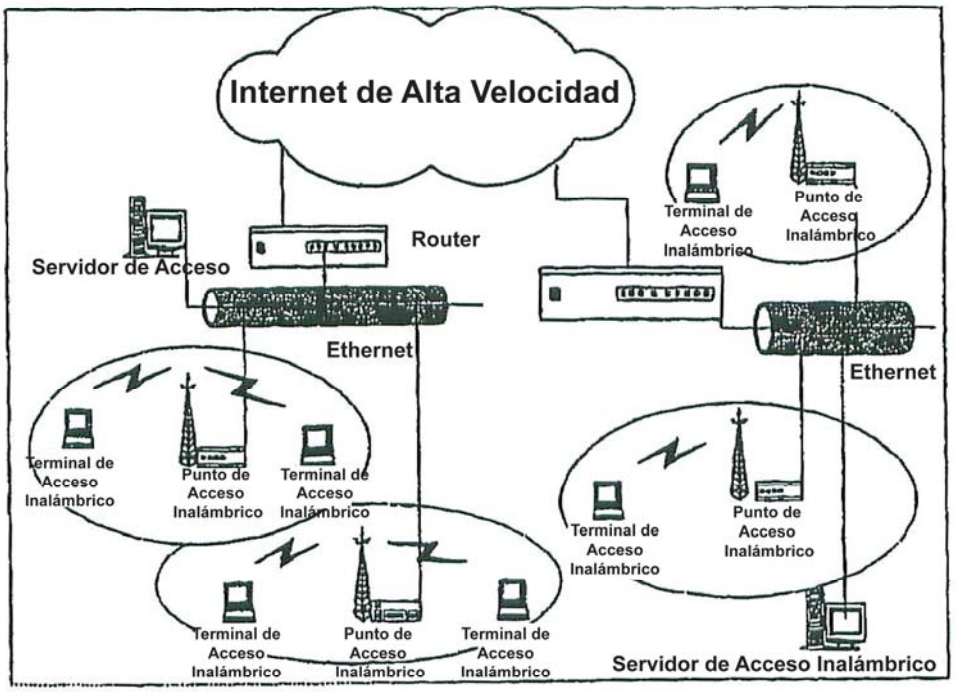
Internet de Alta Velocidad
Router
Servidor de Acceso
Ethernet
Terminal de Acceso Inalámbrico
Punto de Acceso Inalámbrico
Terminal de Acceso Inalámbrico
Terminal de Acceso Inalámbrico
Punto de Acceso Inalámbrico
Ethernet
Terminal de Acceso Inalámbrico
Punto de Acceso Inalámbrico
Terminal de Acceso Inalámbrico
Punto de Acceso Inalámbrico
Terminal de Acceso Inalámbrico
Servidor de Acceso Inalámbrico

Fig. 1

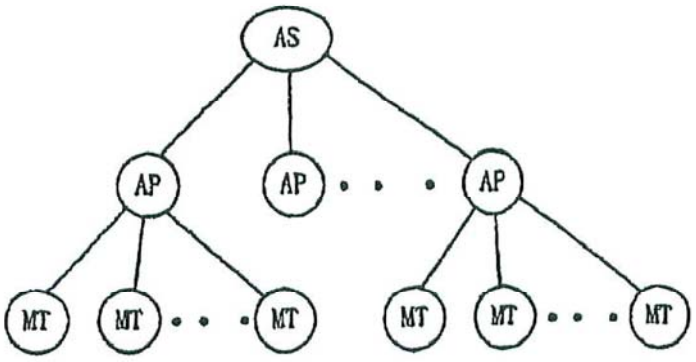
AS
AP
AP
AP
MT
MT
MT
MT
MT
MT

Fig. 2

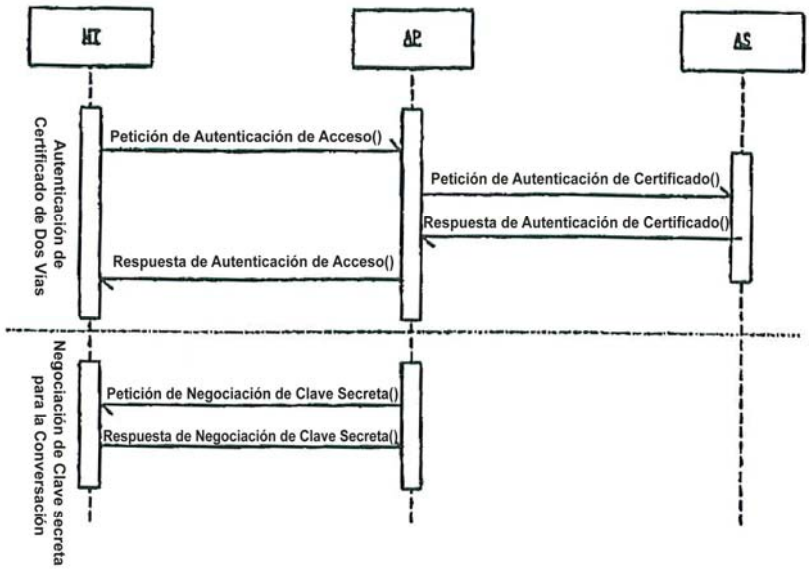
MT
AP
AS
Autenticación de Certificado de Dos Vías
Petición de Autenticación de Acceso()
Petición de Autenticación de Certificado()
Respuesta de Autenticación de Certificado()
Respuesta de Autenticación de Acceso()
Negociación de Clave secreta para la Conversación
Petición de Negociación de Clave Secreta()
Respuesta de Negociación de Clave Secreta()

Fig. 3