(11) Número de Publicação: **PT 1432271 E**

(51) Classificação Internacional:
H04W 12/06 (2007.10) ***H04L 9/32*** (2007.10)
H04W 12/02 (2007.10)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2001.01.23**

(30) Prioridade(s): **2000.02.22 GB 0004178**

(43) Data de publicação do pedido: **2004.06.23**

(45) Data e BPI da concessão: **2010.06.30**
163/2010

(73) Titular(es):
NOKIA CORPORATION
KEILALAHDENTIE 4 02150 ESPOO **FI**

(72) Inventor(es):
JUKKA VIALEN **FI**
VALTTERI NIEMI **FI**

(74) Mandatário:
MANUEL ANTÓNIO DURÃES DA CONCEIÇÃO ROCHA
AV LIBERDADE, Nº. 69 1250-148 LISBOA **PT**

(54) Epígrafe: **VERIFICAÇÃO DE INTEGRIDADE NUM SISTEMA DE COMUNICAÇÃO**

(57) Resumo:

RESUMO

"VERIFICAÇÃO DE INTEGRIDADE NUM SISTEMA DE COMUNICAÇÃO"

É apresentado um nó para ser utilizado num sistema, que compreende o referido nó (6) e outro nó (20). É providenciada uma série de diferentes canais de comunicação entre os referidos nós, possuindo cada canal de comunicação um identidade diferente. O nó compreende meios para calcular um código de autenticação (XMAC-I) a partir de uma série de valores. Alguns dos referidos valores são os mesmos para os referidos vários canais de comunicação diferentes, enquanto pelo menos um dos referidos valores compreende informação relacionada com a identidade de um canal de comunicação (RB ID) dos referidos vários canais de comunicação. O nó compreende ainda meios para receber informação sobre um código de autenticação (MAC-I) calculado pelo referido outro nó, e meios para comparar informação relacionada com o código de autenticação (XMAC-I), calculado pelo referido nó, com informação sobre um código de autenticação (MAC-I) calculado pelo outro nó.

DESCRIÇÃO

"VERIFICAÇÃO DE INTEGRIDADE NUM SISTEMA DE COMUNICAÇÃO"

A presente invenção refere-se a um método para verificar a integridade das comunicações entre um primeiro nó e um segundo nó. Mais especificamente, mas não exclusivamente, a invenção refere-se a um método para verificar a integridade das comunicações entre uma estação móvel e uma rede celular.

Conhecem-se várias redes de telecomunicações diferentes. Uma rede de telecomunicação é uma rede de telecomunicação celular, em que a área coberta pela rede é dividida em múltiplas células. Cada célula é dotada de uma estação base, que serve estações móveis na célula associada à estação base. O equipamento de utilizador, como estações móveis, recebe assim sinais da estação base e transmite sinais para a mesma, podendo comunicar através das estações base. O sistema celular também compreende tipicamente um controlador de estação base, que controla a operação de uma ou mais estações base. Pelo menos algum do equipamento de utilizador no sistema pode conseguir comunicar simultaneamente num ou em mais canais de comunicação.

As telecomunicações debatem-se com o problema em garantir que a informação recebida seja enviada por um remetente autorizado e não por alguém não autorizado que tenta fazer-se passar pelo remetente. O problema é especialmente relevante para sistemas de telecomunicação celular, em que a interface aérea apresenta uma oportunidade potencial para alguém não autorizado para

espreitar e substituir os conteúdos de uma transmissão. O documento US 4.393.269 aborda um método e aparelho que incorpora uma sequência unidireccional para a transacção e verificação da identidade.

Uma solução para este problema é a autenticação das partes envolvidas na comunicação. Um processo de autenticação pretende descobrir e verificar a identidade de ambas as partes de comunicação, de modo a que cada parte receba informação sobre a identidade da outra parte, e possa confiar na identidade. A autenticação é normalmente realizada num procedimento específico no início de uma ligação. No entanto, este procedimento possibilita a manipulação, inserção e eliminação não autorizadas de mensagens subsequentes. Há necessidade de uma autenticação separada de cada mensagem transmitida. Pode fazê-lo, anexando um código de autenticação da mensagem (MAC-I) à mensagem no fim da transmissão, e verificando o valor do código de autenticação da mensagem MAC-I no fim da recepção.

Um código de autenticação da mensagem MAC-I é normalmente uma série relativamente curta de bits, que depende da mensagem que protege e de uma chave secreta conhecida pelo remetente e pelo destinatário da mensagem. A chave secreta é criada e autorizada durante o procedimento de autenticação no início da ligação. Em alguns casos, o algoritmo (que é usado para calcular o código de autenticação da mensagem MAC-I baseado na chave secreta e na mensagem) também é secreto, mas isto não é habitual.

O processo de autenticação de mensagens simples é frequentemente designado por protecção de integridade. Para proteger a integridade de uma mensagem, a parte

transmissora computoriza um valor de autenticação da mensagem baseado na mensagem a enviar e na chave secreta, utilizando o algoritmo especificado, e envia a mensagem com o valor do código de autenticação da mensagem MAC-I. O destinatário volta a computorizar um valor do código de autenticação da mensagem MAC-I baseado na mensagem e na chave secreta de acordo com o algoritmo especificado, e compara o código de autenticação da mensagem MAC-I recebido e o código de autenticação da mensagem MAC-I calculado. Se os dois valores dos códigos de autenticação da mensagem MAC-I coincidirem, o destinatário pode acreditar que a mensagem está intacta e foi enviada por quem era suposto.

Os esquemas de protecção da integridade podem ser atacados. Há dois métodos que uma parte não autorizada pode utilizar para forjar um valor do código de autenticação da mensagem MAC-I para uma mensagem modificada ou novas mensagens. O primeiro método envolve a obtenção da chave secreta e o segundo método envolve providenciar uma mensagem modificada ou nova sem conhecer a chave secreta.

A chave secreta pode ser obtida por uma terceira parte de duas maneiras:

- computorizando todas as possíveis chaves até encontrar uma chave que coincida com os dados dos pares do código de autenticação da mensagem MAC-I, ou interrompendo o algoritmo para produzir valores do código de autenticação da mensagem MAC-I; ou
- capturando directamente uma chave secreta memorizada ou transmitida.

As partes de comunicação original podem impedir uma terceira parte de obter a chave secreta, utilizando um algoritmo que é criptograficamente forte, utilizando uma chave secreta suficientemente comprida para evitar a procura exaustiva de todas as chaves e utilizando um método seguro para a transmissão e memorização das chaves secretas.

Uma terceira parte pode tentar interromper o envio da mensagem entre as duas partes sem uma chave secreta, adivinhando o valor correcto do código de autenticação da mensagem MAC-I, ou repetindo alguma mensagem anterior transmitida entre as duas partes. No último caso, o código correcto de autenticação da mensagem MAC-I para a mensagem é do conhecimento da transmissão original. Este ataque pode ser muito útil para uma terceira parte não autorizada. Por exemplo, pode multiplicar o número de outras acções favoráveis ao intruso. Até as transacções monetárias podem ser repetidas desta maneira.

Pode evitar-se adivinhar correctamente o valor do código de autenticação da mensagem MAC-I, se utilizar valores compridos do código de autenticação da mensagem MAC-I. O valor do código de autenticação da mensagem MAC-I deve ser suficientemente comprido para reduzir a probabilidade de adivinhar correctamente até um nível suficientemente baixo comparado com os benefícios obtidos por uma falsificação bem sucedida. Por exemplo, a utilização de um valor do código de autenticação da mensagem MAC-I de 32 bits reduz a probabilidade de adivinhar correctamente em 1/4294967296. Isto é suficientemente pequeno para a maior parte das aplicações.

A obtenção de um valor correcto do código de autenticação da mensagem MAC-I, utilizando o ataque repetido, ou seja, repetindo uma mensagem anterior, pode ser impedida através da introdução de um parâmetro de variação temporal no cálculo dos valores de autenticação da mensagem MAC-I. Por exemplo, pode utilizar-se um valor de carimbo de tempo ou um número de sequência como outra entrada para o algoritmo do código de autenticação da mensagem MAC-I, para além da chave de integridade secreta e da mensagem.

No caso de se usar uma sequência de números como parâmetros de variação temporal, é utilizado um mecanismo que evita a possibilidade de utilizar o mesmo número de sequência mais do que uma vez com a mesma chave secreta. Normalmente, ambas as partes de comunicação acompanham os números da sequência.

Se estiverem a ser utilizados vários canais de comunicação que utilizam todos a mesma chave secreta, ocorre o seguinte problema. Pode acontecer uma mensagem num canal de comunicação associado a um determinado número de sequência, por exemplo n, ser repetida noutro canal de comunicação em determinada altura, nomeadamente quando o número de sequência n pode ser aceite no outro canal.

Foi proposto aplicar uma protecção de decifração e de integridade no sistema UMTS para o padrão da terceira geração. Porém, o método proposto permite enviar a mensagem idêntica em dois diferentes suportes de rádio de sinalização em diferentes alturas. Isto torna o sistema vulnerável a ataques de homem no meio. Mais especificamente, este tipo de sistema pode ser vulnerável ao "ataque de repetição" acima descrita.

Normalmente, uma única mensagem de sinalização repetida não confere uma vantagem significativa à terceira parte não autorizada, mas é possível que a terceira parte possa tentar repetir um diálogo maior para, por exemplo, configurar uma chamada adicional e, assim, roubar partes de uma ligação.

O documento ETSI: "Sistema Universal de Telecomunicações Móveis (UMTS); Segurança 3G; Arquitectura de Segurança (3GPP TS 33, 102 Versão 3.3.1 Editado 1999)" ETSI TS 133 102 V3.3.1" Janeiro de 2000 (2000-01), páginas 1-64, XP002225628 descreve em detalhe um método de segurança para ser utilizado num sistema de telecomunicações 3G.

Um dos objectivos da presente invenção é abordar um ou mais problemas anteriormente discutidos.

De acordo com um aspecto da presente invenção, é providenciado um nó para ser utilizado num sistema, que compreende o referido nó e outro nó, sendo providenciada uma série de diferentes canais de comunicação entre os referidos nós, possuindo cada canal de comunicação uma diferente identidade. O nó real é caracterizado pela inclusão de meios para calcular um código de autenticação a partir de vários valores, sendo alguns dos referidos valores os mesmos para os referidos múltiplos canais de comunicação diferentes, em que pelo menos um dos referidos valores compreende informação relacionada com a identidade de um canal de comunicação dos referidos múltiplos canais de comunicação, meios para receber informação relacionada com um código de autenticação calculado pelo referido nó, e meios para comparar informação relacionada com um código de autenticação calculado pelo referido nó com informação

relacionada com um código de autenticação calculado pelo outro nó.

De acordo com outro aspecto da presente invenção, é providenciado um método para levar a cabo uma verificação de integridade num sistema, que compreende um nó e outro nó, sendo providenciada uma série de canais de comunicação entre o referido nó e o outro nó, possuindo cada canal de comunicação uma diferente identidade. O método é caracterizado pelos passos de receber no nó informação relacionada com um código de autenticação do outro nó, calcular outro código de autenticação, utilizando vários valores, alguns dos quais são os mesmos para os referidos vários canais de comunicação diferentes, em que pelo menos um dos referidos valores compreende informação relacionada com a identidade de um canal de comunicação dos referidos vários canais, e compara o outro código de autenticação com a referida informação relacionada com um código de autenticação recebido pelo outro nó.

De acordo com outro aspecto da presente invenção, é providenciado um sistema de comunicação que compreende um nó como acima descrito, e que está preparado para operar de acordo com o método acima descrito.

As versões da invenção permitem obter várias vantagens. Na solução da presente invenção, pode impedir-se o ataque de repetição mesmo quando são utilizados vários canais de comunicação paralelos. Uma vantagem é que as versões podem ser flexivelmente aplicadas a qualquer sistema, utilizando canais de comunicação paralelos dentro de uma ligação. A versão da presente invenção pode melhorar a segurança do utilizador em sistemas de comunicação, especialmente em sistemas de comunicação sem fios. As

versões podem assegurar que os canais de comunicação paralelos dentro de uma ligação nunca usem o mesmo conjunto de parâmetros de entrada para calcular o código de autenticação da mensagem MAC-I.

Para uma melhor compreensão da presente invenção e de modo a ilustrar como a mesma pode ser executada, passamos a fazer referência, a título exemplificativo, aos desenhos anexos, nos quais:

A Figura 1 mostra elementos de uma rede celular, com os quais as versões da presente invenção podem ser utilizadas;

A Figura 2 mostra a arquitectura de protocolo Uu da interface de razão entre o equipamento do utilizador UE e o Nó B e entre o equipamento do utilizador UE e o controlador da rede de rádio RNC da Figura 1;

A Figura 3 ilustra esquematicamente a função de protecção da integridade;

A Figura 4 mostra a função de protecção da integridade modificada de acordo com versões da presente invenção;

A Figura 5 mostra a função de protecção da integridade modificada de acordo com outra versão da invenção;

A Figura 6 mostra outra versão da presente invenção;

A Figura 7 mostra um procedimento de autenticação e de autorização de chave;

A Figura 8 mostra a criação de vectores de autenticação; e

A Figura 9 mostra um exemplo da função de autenticação do utilizador em USIM de acordo com uma versão da presente invenção.

Relativamente à Figura 1, esta descreve uma estrutura típica de sistema de telefone móvel. As partes principais do sistema de telefone móvel são: uma rede central CN2, uma rede de acesso de rádio terrestre UTRAN do UMTS 4, e equipamento de utilizador UE 6. A rede central CN 2 pode ser ligada a redes externas 8, que podem ser redes de Comutação de Circuitos (CS) 81 (por ex. PLMN, PSTN, ISDN) ou redes de Comutação de Pacotes (PS) 82 (por ex. a Internet). A interface entre a rede central CN 2 e a rede de acesso de rádio terrestre UTRAN 4 do UMTS é designada de interface lu, e a interface entre a rede de acesso de rádio terrestre UTRAN 4 do UMTS e o equipamento de utilizador UE 6 é designada de interface Uu. Como se pode ver na Figura 1, o RNC é ligado a dois nós CN (MSC/VLR e SGSN). Em algumas tipologias de redes, pode ser possível ligar um RNC a um ou mais nós CN.

A rede central CN 2 é composta por um Registo de Localização Residencial HLR 10, um Centro de Comutação de Serviços Móvel/Registo de Localização de Visitantes MSCNLRI 2, uma porta MSC GMSC 14, um GPRS Servidor (Serviço de Rádio de Pacote Geral) Nó de Suporte SGSN 16 e uma porta GPRS do Nó de Suporte GGSN 18.

A UTRAN 4 é composta por subsistemas de rede de rádio RNS 20 e 22. A interface entre dois subsistemas de rede

rádio RNS é designada por interface lur. Os subsistemas de rede de rádio RNS 20 e 22 são compostos por um controlador de rede de rádio RNC 24 e um ou mais nós Bs 26. A interface entre o controlador de rede de rádio RNC 24 e o nó B 26 é designada por interface lub.

O Controlador da Rede de Rádio RNC 24 é o elemento de rede responsável pelo controlo dos recursos de rádio da UTRAN 4. O RNC 24 liga, por meio de interface, a rede central CN 2 (normalmente a um MSC 12 e um SGSN 16) e também termina o protocolo do Controlo de Recursos de Rádio RRC que define as mensagens e os procedimentos entre o equipamento do utilizador UE 6 e UTRAN 4. O RNC 24 corresponde logicamente ao controlador da estação base do padrão GSM (sistema global para comunicações móveis).

A função principal do Nó B 26 é realizar o processamento da interface aérea L1 (codificar e intercalar o canal, adaptação da taxa, expansão, etc.). Também executa alguma operação básica de Gestão de Recursos de Rádio, como o controlo da potência do circuito interno. Corresponde logicamente à Estação de Emissor-Receptor Base do padrão GSM.

O equipamento do utilizador UE 6 é constituído por duas partes: o Equipamento Móvel ME 30 e o Módulo de Identificação do Assinante USIM do UMTS 32. O equipamento móvel ME é o terminal de rádio utilizado para a comunicação de rádio através da interface Uu entre o equipamento do utilizador UE 6 e o UTRAN 4. O USIM 32 é um cartão smart que guarda a identidade do assinante, realiza algoritmos de autenticação e guarda as chaves de autenticação e de encriptação e alguma informação de subscrição necessária no terminal.

Relativamente à Figura 2, esta descreve a arquitectura de protocolo de interface de rádio de acordo com as especificações 3GPP. As entidades do protocolo descritas operam entre:

o equipamento do utilizador UE 6 e o Nó B 26
e/ou
o equipamento do utilizador UE 6 e o RNC 24.

A divisão das camadas de protocolo entre o Nó B 26 e RNC 24 não vai ser descrita em mais pormenor.

Os protocolos de interface de rádio podem ser divididos num plano de controlo 50 e num plano de utilizador 52. O plano de controlo 50 é utilizado para toda a sinalização entre UE 6 RNC 24, e também entre o equipamento do utilizador UE 6 e a rede central CN 2. O plano do utilizador suporta os dados actuais do utilizador. Alguns dos protocolos de interface de rádio operam apenas num plano, enquanto alguns protocolos operam em ambos os planos.

Os protocolos de interface de rádio podem ser divididos em camadas, que são a camada 1 L1 54 (também designada por camada física), a camada 2 L2 56 (também designada por camada de ligação de dados) e a camada 3 L3 58 (também designada por camada de rede). Algumas camadas contêm apenas um protocolo, enquanto outras camadas contêm vários protocolos diferentes.

A camada física L1 54 oferece serviços à camada do Controlo de Acesso Médio (MAC) 60 através de canais de transporte, que são caracterizados pelo facto como e com que características os dados são transferidos.

Por sua vez, a camada de Controlo de Acesso Médio (MAC) 60, oferece serviços à camada de controlo de ligação de rádio RLC 62 através de canais lógicos. Os canais lógicos são caracterizados pelo tipo de dados que são transmitidos. Na camada de controlo de acesso médio MAC 60, os canais lógicos são mapeados para os canais de transporte.

A camada de Controlo de Ligação RLC 62 oferece serviços a camadas mais altas através de pontos de acesso de serviço SAP, que descreve como a camada de controlo de ligação de rádio RLC 62 manuseia os pacotes de dados e se, por exemplo, é utilizada uma função de pedido de repetição automático (ARQ). No plano de controlo 50, os serviços de controlo de ligação de rádio RLC são utilizados pela camada de controlo de recursos de rádio RRC 64 para sinalizar o transporte. Normalmente, é utilizado um mínimo de três entidades de controlo de ligação de rádio RLC 62 para sinalizar o transporte – um modo de entidade transparente, um desconhecido e um conhecido. No plano do utilizador 52, os serviços RLC são utilizados pelas camadas de protocolo específicas de serviço – protocolo de convergência de dados de pacote PDCP 66 ou controlo de transmissão múltipla BMC 68 – ou por outras funções do plano do utilizador da camada mais alta (por ex. codec de voz). Os serviços RLC são chamados Suportes de Rádio de Sinalização no plano de controlo e Suportes de Rádio no plano do utilizador para serviços que não utilizam os protocolos PDCP ou BMC.

O Protocolo de Convergência de Dados de Pacote (PDCP) existe apenas para os serviços do domínio de Comutação de Pacote PS (serviços encaminhados via SGSN) e a sua principal função é a compressão do cabeçalho, o que

significa a compressão da informação de controlo de protocolo redundante (por ex. cabeçalhos TCP/IP e RTP/UDP/IP) na entidade transmissora, e de descompressão na entidade de recepção. Os serviços oferecidos por PDCP são designados Suportes de Rádio.

O protocolo de Controlo de Múltipla Transmissão (BMC) existe apenas para o serviço de Transmissão de Células de curtas mensagens SMS, que deriva de GSM. O serviço oferecido pelo protocolo BMC é também designado por Suporte de Rádio.

A camada RRC 64 oferece serviços a camadas mais altas (ao Estrato Não Acesso) através de pontos de acesso de serviço. Toda a sinalização de camadas mais altas entre o equipamento do utilizador UE 6 e a rede central CN 2 (gestão de mobilidade, controlo de chamada, gestão de sessão, etc.) é encapsulada em mensagens RRC para a transmissão através da interface de rádio.

As interfaces de controlo entre RRC 64 e todos os protocolos de camadas mais baixas são utilizadas pela camada RRC 64 para configurar características das entidades de protocolo das camadas mais baixas, incluindo parâmetros para os canais físicos, de transporte e lógicos. As mesmas interfaces de controlo são utilizadas pela camada RRC 64, por exemplo, para comandar as camadas mais baixas para realizar certos tipos de medições, e pelas camadas mais baixas para reportar resultados de medições e erros ao RRC.

A versão da invenção é descrita no contexto de um UMTS (Sistema Universal de Telecomunicações Móvel). A presente invenção pode ser aplicada a todo o tipo de comunicação, sinalizando por exemplo serviços em tempo real e serviços não em tempo real. Note-se, porém, que as versões da

presente invenção podem ser aplicadas a qualquer outro sistema.

Na proposta para o padrão UMTS para a terceira geração, o SGSN 16 e o equipamento do utilizador UE 6, como por exemplo uma estação móvel, têm uma camada superior L3, que suporta a gestão de mobilidade MM (por vezes chamada GMM) e a gestão de sessão SM. Esta camada superior também suporta o serviço de mensagens curtas SMS. Estes protocolos de camadas superiores L3 derivam do sistema de segunda geração GPRS. O SMS suporta o serviço de mensagens curtas de origem e conclusão móvel descrito na especificação 3GPP TS 23.040 de terceira geração. A função de gestão de mobilidade gere a localização da estação móvel, que é um anexo da estação móvel à rede e autenticação. Por conseguinte, MM suporta a funcionalidade da gestão de mobilidade, como anexar, separar, segurança (por ex. autenticação) e actualizações de encaminhamento. De acordo com uma versão, as chaves de integridade podem ser calculadas durante o procedimento de autenticação de MM. Mais adiante será explicada uma versão exemplificativa deste aspecto da presente invenção.

O SGSN 16 e RNS20 têm uma camada de Protocolo de Aplicação da Rede de Acesso de Rádio (RANAP). Este protocolo é utilizado para controlar os suportes da interface lu, mas também encapsula e suporta a sinalização da camada superior. RANAP trata da sinalização entre SGSN 16 e RNS 20. RANAP é especificado na especificação da terceira geração 3GPP TS 25.413. A estação móvel 6 e o RNS 20 têm ambos um protocolo de controlo dos recursos de rádio RRC, que proporciona o controlo de suporte de rádio através da interface de rádio, por exemplo para a transmissão de

mensagens de sinalização da camada mais alta e mensagens SMS. Esta camada trata da maior parte da comunicação entre a estação móvel 6 e o RNC 24. Um RRC é especificado, por exemplo, na especificação de terceira geração 3GPPTS 25.331

As mensagens MM, SM e SMS são enviadas do SGSN 16 para o RNS 20 encapsulado numa mensagem de protocolo RANAP (a mensagem é designada por Transferência Directa nas especificações 3GPP). O pacote é reencaminhado pela camada RANAP do RNC 24 para a camada RRC do RNC 24. A função de repetição no RNS 20 retira efectivamente os cabeçalhos RANAP e reencaminha a carga útil para o protocolo RRC, utilizando um primitivo apropriado, de modo a que a camada RRC saiba que esta é uma mensagem de camada superior que tem de ser reencaminhada para a estação móvel 6. O RNC 24 insere uma soma de verificação da integridade na (RRC) mensagem, que suporta a mensagem de camada superior em carga útil (a mensagem RRC é designada por Transferência Directa nas especificações 3GPP). O RNC 24 também pode decifrar a mensagem. Vamos passar a descrever isto em pormenor. O RNS 20 reencaminha o pacote, através da interface aérea, para a estação móvel 6.

Na direcção de origem móvel, a camada RRC da estação móvel 6 recebe a mensagem de camada mais alta, encapsula-a numa mensagem de Transferência Directa RRC e adiciona um código de autenticação da mensagem antes de enviá-la para o RNS 20. A mensagem é estabelecida a partir da camada RRC para a camada RANAP do RNS 20. O RNS 20 verifica a informação associada à mensagem para ver se o pacote foi verificado quanto à integridade.

Vamos descrever agora o procedimento de verificação da integridade. A maior parte dos controlos de recursos de

rádio RRC, dos elementos de informação da gestão de mobilidade MM e da gestão de sessão SM (assim como outros protocolos de camada mais alta 3) são considerados sensíveis e também têm de ser protegidos para manterem a integridade. Graças a isto, pode ser aplicada uma função de integridade na maior parte das mensagens de sinalização RRC transmitidas entre a estação móvel e o RNS 20. No entanto, podem ignorar-se essas mensagens RRC que são enviadas antes da chave de integridade ser conhecida. Esta função de integridade usa um algoritmo de integridade com a chave de integridade IK para computorizar um código de autenticação da mensagem para uma determinada mensagem. Isto é levado a cabo na estação móvel e no RNS, que têm ambos a chave de integridade IK e o algoritmo de integridade.

Faz-se referência à Figura 3, que ilustra a utilização do algoritmo de integridade para calcular o código de autenticação da mensagem MAC-I.

Os parâmetros de entrada para o algoritmo são a chave de integridade IK, uma entrada dependente do número da hora ou da mensagem CONTAGEM-I, um valor aleatório criado pela rede FRESH, o bit de direcção DIRECÇÃO e os dados de sinalização MENSAGEM. A última entrada é a mensagem ou pacote de dados. Baseado nestes parâmetros de entrada, é calculado um código de autenticação da mensagem para a integridade dos dados (MAC-I) pelo algoritmo de integridade UIA. Este código MAC-I é, de seguida, anexado à mensagem antes do envio através da interface área para a, ou da, estação móvel.

O receptor desse código e mensagem também compreende um código de autenticação da mensagem para a integridade dos dados XMAC-I na mensagem recebida, utilizando o mesmo

algoritmo UIA. O algoritmo UIA possui as mesmas entradas como no fim do envio da mensagem. Os códigos calculados pelo algoritmo no fim do envio (MAC-I) e no fim da recepção (XMAC-I) devem ser os mesmos se pretende verificar a integridade dos dados da mensagem.

O parâmetro de entrada CONTAGEM-I é um valor incrementado por um de cada mensagem protegida quanto à integridade. CONTAGEM-I consiste de duas partes: o número de hiperquadro (HFN) como a parte mais significativa e um número da sequência da mensagem como a parte menos significativa. O valor inicial do número de hiperquadro é enviado pela estação móvel para a rede durante uma configuração de ligação. Quando a ligação é desfeita, a estação móvel guarda o maior número de hiperquadro utilizado a partir da ligação e incrementa-o em um. Este valor é, de seguida, utilizado como o valor HFN inicial para a próxima ligação. Deste modo, o utilizador sabe que nenhum valor CONTAGEM-I é reutilizado (pela rede) com a mesma chave de integridade para diferentes ligações. Após um procedimento de (re)autenticação, quando é criado e utilizado um novo IK, o valor HFN pode ser reposto a zero.

O parâmetro de entrada RECENTE protege a rede contra a repetição de mensagens de sinalização pela estação móvel. Na configuração da ligação, a rede cria um valor aleatório RECENTE e envia-o ao utilizador. O valor RECENTE é subsequentemente utilizado tanto pela rede como pela estação móvel durante o período de duração de uma única ligação. Este mecanismo garante à rede que a estação móvel não está a repetir nenhum código de autenticação de mensagem antiga MAC-I da ligação anterior.

A configuração da chave de integridade IK é conforme aqui descrita. A chave pode ser alterada as vezes que o operador da rede quiser. A configuração da chave pode ocorrer assim que se conhecer a identidade do assinante móvel. A chave IK é guardada no registo de localização do visitante e transferida para o RNC quando necessário. A chave IK é também guardada na estação móvel até ser actualizada na próxima autenticação.

Um identificador de configuração de chave KSI é um número associado com as chaves de decifração e de integridade derivadas durante o procedimento de autenticação. É guardada juntamente com as chaves de decifração e de integridade no MS e na rede. O identificador de configuração da chave é utilizado para permitir a reutilização da chave durante subsequentes configurações de ligação. O KSI é utilizado para verificar se o MS e a rede devem utilizar a mesma chave de decifração e de integridade.

É providenciado um mecanismo para garantir que uma determinada chave de integridade não seja utilizada por um período de tempo ilimitado e para evitar ataques usando chaves comprometidas. Na configuração da ligação não é obrigatória uma autenticação que crie chaves de integridade.

A estação móvel está preparada para activar a criação de uma nova chave de decifração e uma chave de integridade se o contador chegar a um valor máximo definido pelo operador e guardado na estação móvel na próxima mensagem de pedido de ligação enviada. Este mecanismo impede a reutilização de uma chave de integridade e de decifração mais vezes do que o limite definido pelo operador.

Note-se que pode existir mais do que um algoritmo de integridade e a informação é trocada entre a estação móvel e os controladores da rede de rádio que definem o algoritmo. Note-se que o mesmo algoritmo deve ser utilizado pelo remetente e o destinatário de mensagens.

Quando uma estação móvel quer estabelecer uma ligação com a rede, a estação móvel deve indicar à rede qual a versão ou versões do algoritmo que o MS suporta. Esta mensagem tem de ser, ela mesma, protegida para garantir a integridade e é transmitida ao RNC depois do procedimento de autenticação estar completo.

A rede deve comparar as suas capacidades e preferências de protecção de integridade, e quaisquer requisitos especiais da subscrição da estação móvel com os indicados pela estação móvel, e actuar de acordo com as seguintes regras:

1) Se a estação móvel e a rede não tiverem nenhuma versão do algoritmo em comum, a ligação deve ser desfeita.
2) Se a estação móvel e a rede possuírem, pelo menos, uma versão do algoritmo em comum, a rede deve seleccionar uma das versões mutuamente aceitáveis do algoritmo para ser utilizada na ligação.

A protecção da integridade é realizada anexando o código de autenticação da mensagem MAC-I à mensagem que se pretende proteger para manter a integridade. A estação móvel pode anexar o MAC-I a mensagens, assim que receber um valor RECENTE específico de ligação a partir do RNC.

Se o valor do número de hiperquadro HFN for superior ou igual ao valor máximo guardado na estação móvel, a estação móvel indica à rede na configuração de ligação RRC que é necessário inicializar um novo acordo de autenticação e de chave.

O RNC pode estar preparado para detectar a necessidade de novos parâmetros de segurança. Isto pode ser activado pela falha (repetida) de verificações de integridade (por ex. CONTAGEM-I saiu da sincronização), ou a transição para um novo RNC não suporta um algoritmo seleccionado pelo RNC antigo, etc.

É estabelecida uma nova chave de decifração CK sempre que realizar um procedimento de autenticação entre a estação móvel e o SGSN.

A chave de integridade IK pode ser mudada se a estação móvel transitar de uma estação base para uma estação base diferente

Note-se que em versões da invenção, a verificação de integridade só pode começar em qualquer ponto depois de configurar a ligação e a anexação.

Note-se que nas ligações de dados, a ligação pode ser aberta por períodos de tempo relativamente longos ou pode até ser permanentemente aberta.

Ficou acordado que pode ser estabelecido mais do um suporte de rádio de sinalização, que é um suporte de rádio no plano de controlo - serviço oferecido pelo RLC -, entre uma estação móvel ou outro equipamento de utilizador 6 e o RNS 20. A especificação 3GPP actual propõe providenciar até quatro suportes de rádio de sinalização.

Na especificação 3GPP actual, dois ou mais dos suportes de rádio de sinalização SRB podem ter os mesmos

parâmetros de entrada para o algoritmo de integridade ilustrado na Figura 3. Se todos os parâmetros de entrada para o algoritmo de integridade forem os mesmos, então a saída é a mesma.

Esta proposta actual, como anteriormente mencionado, deixa em aberto a possibilidade de um intruso ou um 'homem no meio' para repetir uma mensagem de sinalização de um suporte de rádio de sinalização noutro suporte de sinalização. O valor CONTAGEM-I é específico a cada suporte de rádio de sinalização e pode ser diferente em suportes de rádio diferentes. Considere o seguinte cenário. Foi enviada uma mensagem num primeiro suporte de rádio de sinalização SRB1 com um valor de CONTAGEM de 77. Quando o valor de contagem para um segundo suporte de rádio de sinalização SRB2 chega a 77, a parte não autorizada pode simplesmente repetir a mensagem anteriormente enviada em SRB1, utilizando SRB2.

Normalmente, uma única mensagem de sinalização de um suporte de rádio de sinalização repetida no segundo suporte de rádio de sinalização não confere uma vantagem significativa ao 'homem no meio', mas a parte não autorizada pode não poder repetir também um diálogo maior para, por exemplo, configurar uma chamada adicional, que o 'homem no meio' pode utilizar e, consequentemente, roubar partes da ligação. Um caso mais simples de 'ataque de repetição' seria a parte não autorizada, por exemplo, repetir um diálogo realizado via SMS, sendo o diálogo por ex. uma transacção monetária.

Com as propostas actuais da terceira geração, este problema pode ocorrer apenas num número limitado de circunstâncias. Isto deve-se ao facto da utilização dos

quatro suportes de rádio de sinalização (SRB) ser limitada. Apenas certas mensagens RRC podem ser enviadas em certos suportes de rádio de sinalização. O cenário do "ataque de repetição" seria possível para uma mensagem de Estrato Não Acesso (NAS) (mensagens CM/MM/SMS etc. suportadas em Transferência Directa RRC) ou um diálogo de mensagem NAS entre UE e SGSN/MSC. A Transferência Directa RRC é uma mensagem RRC, que suporta, em carga útil, todas as mensagens NAS através da interface aérea. No entanto, este problema pode prejudicar um utilizador móvel, como por ex. as mensagens SMS serem negativamente afectadas.

Há duas soluções básicas para o problema de 'ataque de repetição'. Em primeiro lugar, diferentes canais de comunicação a utilizar a mesma chave secreta podem coordenar a utilização dos números de sequência CONTAGEM-I, de modo a que cada número de sequência seja utilizado, no máximo, uma vez em qualquer um dos canais. Esta coordenação pode tornar-se incomodativa ou até impossível em algumas situações. Note-se que, quando as versões são aplicadas à interface de rádio da rede celular de 3ª geração UMTS, os canais de comunicação podem ser designados por suportes de rádio.

Como ainda será discutido em mais pormenor, as versões da presente invenção aplicam uma solução em que é utilizado um parâmetro adicional como uma entrada para o cálculo do código de autenticação da mensagem MAC-I. O valor deste parâmetro é único, pelo menos, para cada canal de comunicação que usa a mesma chave secreta. O valor pode ser único também para todos os canais de comunicação dentro de uma ligação entre o equipamento do utilizador UE 6 e RNS 20.

Noutra versão da presente invenção, o problema é evitado, assegurando que a mesma chave de integridade nunca é usada para diferentes canais de comunicação paralelos.

Na Figura 4 são descritas as modificações à conhecida função de protecção de integridade da presente invenção. Estas modificações não provocam mudanças no algoritmo de integridade actual UIA.

É adicionado um parâmetro específico do canal de comunicação como entrada ao algoritmo de protecção da integridade. Nas especificações 3GPP, este parâmetro específico do canal de comunicação é a identificação do suporte de rádio (RB ID). Num exemplo de uma aplicação da presente invenção, a identificação do suporte de rádio representa a identidade do suporte de rádio de sinalização no proposto sistema de terceira geração WCDMA e pode ser um número entre 0 e 3. Note-se que o parâmetro específico do canal de comunicação utilizado depende da camada de protocolo, em que é calculado o código de autenticação da mensagem. Tomando ainda a especificação 3GPP como exemplo, se o código de autenticação da mensagem fosse adicionado no protocolo RLC, o parâmetro seria uma identidade de canal lógico (ver Figura 2). Como outro exemplo possível, se a protecção de integridade fosse realizada na camada de protocolo PDCP ou na camada de protocolo RRC, o parâmetro adicional seria uma identidade de suporte de rádio (ver Figura 2). Note-se que, quando se discute o plano de controlo como parte da série de protocolos, os termos identidade do suporte de rádio de sinalização e identidade do suporte de rádio são equivalentes.

Uma vez que a identidade do suporte de rádio de sinalização é conhecida pelo remetente e pelo destinatário,

ou seja o equipamento do utilizador UE 6 e o RNS 20, não é necessário enviar a informação da identidade explicitamente através da interface de rádio.

A Figura 4 ilustra os possíveis lugares onde o novo parâmetro pode ser incluído sem modificar o algoritmo de integridade UIA. Uma vez que o remetente e o destinatário são similares, observado do ponto de vista do parâmetro de entrada (ver Figura 3), é apenas apresentado um lado na Figura 4. Note-se que as partes de recepção e transmissão executam o mesmo algoritmo. Como se pode ver na Figura 4, as versões privilegiadas incluem o novo parâmetro, anexando-o (como uma série) a um ou mais dos parâmetros de entrada do algoritmo existentes.

Numa versão, a identificação do suporte de rádio de sinalização RB IB faz parte dos parâmetros de entrada RECENTE ou CONTAGEM-I. Isto é ilustrado com os números '1' e '2' na Figura 4, respectivamente. Na prática, os parâmetros RECENTE e CONTAGEM-I incorporam tanto a informação RECENTE ou CONTAGEM-I e a informação de identificação. Por exemplo, se o valor RECENTE possuir bits *n*, a informação RECENTE seria representada por bits *a* e a informação de identificação por bits *b*, em que a+b=n. Isto teria como consequência reduzir o parâmetro RECENTE. Pode ser feita a mesma modificação ao parâmetro CONTAGEM-I. Numa modificação, parte da identificação do suporte de rádio de sinalização pode ser providenciada pelo parâmetro CONTAGEM-I e parte pelo parâmetro RECENTE. No entanto, se CONTAGEM-I for reduzido, pode levar menos tempo a 'dar a volta', isto é, a chegar ao valor máximo e regressar a zero. Se o parâmetro RECENTE for reduzido, pode acontecer aumentar a

probabilidade de repetir o valor acidentalmente (é escolhido à sorte).

Noutra versão, o ID do suporte de rádio de sinalização faz parte da chave de integridade IK. Isto é ilustrado com o número '4' na Figura 4. Por exemplo, se o valor IK possui bits *n*, a informação IK seria representada por bits *a* e a informação de identificação por bits *b*, em que a+b=n. Porém, se a chave IK for mais curta, há uma maior probabilidade para simplesmente adivinhar a chave.

Noutra versão da presente invenção, a identidade do suporte de rádio de sinalização pode estar incorporado na MENSAGEM que é introduzida no algoritmo de integridade. Isto é ilustrado com o número'3' na Figura 4. Uma vez que a identidade do suporte de rádio de sinalização é conhecida por parte do remetente e do destinatário, ou seja a estação móvel e o RNS 20, não é necessário enviar a informação da identidade através da interface de rádio com a MENSAGEM actual. For exemplo, se a MENSAGEM possuir bits *n* e a identidade RB ID possui bits *i*, a 'MENSAGEM' actual que seria introduzida no algoritmo de integridade teria bits n+i. Assim sendo, em vez de ser apenas a MENSAGEM a ser introduzida no algoritmo de integridade, a série de bits introduzida no algoritmo de integridade tornar-se-ia uma identidade de suporte de rádio de sinalização e na MENSAGEM. Esta solução não afecta as questões de segurança (por ex. comprimentos de contador) relacionadas com o algoritmo de integridade. Isto quer dizer que não é encurtado nenhum parâmetro introduzido no algoritmo:

Em algumas versões, é possível dividir a informação de identificação entre mais do que uma entrada.

A Figura 5 ilustra outra versão da invenção, que afecta o algoritmo de integridade actual UIA. Nesta versão, o algoritmo de integridade é dotado de um parâmetro adicional, como se pode ver na Figura 5. Neste exemplo, quando é realizada a protecção de integridade na camada de protocolo RRC, o parâmetro adicional é uma identificação de suporte de rádio (de sinalização) RB ID, que é única para o suporte de rádio (de sinalização). Este parâmetro é separadamente introduzido e é utilizado no cálculo realizado pelo algoritmo de integridade UIA.

A Figura 6 ilustra outra versão da invenção, que afecta o algoritmo de integridade actual UIA. Nesta versão, o novo parâmetro ID do suporte (RB ID) é combinado com o parâmetro DIRECÇÃO. Esta versão iria, de facto, aumentar o existente, ou seja 'antigo', parâmetro DIRECÇÃO e, por conseguinte, afectar o algoritmo de integridade actual UIA.

Numa versão alternativa, é produzida uma chave de integridade IK única para cada suporte de rádio. Isto pode ser conseguido, modificando o procedimento de autenticação de uma camada superior L3, que suporta a gestão da mobilidade MM e a gestão de sessão SM nas especificações UMTS propostas. Como já foi antes resumidamente explicado, a função de gestão de mobilidade gere a localização da estação móvel, que é um anexo da estação móvel à rede e autenticação. O algoritmo de integridade realizado em cada um dos suportes de rádio de sinalização durante um procedimento de autenticação modificado pode obter resultados únicos, evitando o tipo de ataque anteriormente delineado.

Passamos a fazer referência às Figuras 7 a 9, que mostram possíveis procedimentos de acordo de autenticação e

chave. Os mecanismos descritos obtêm uma autenticação mútua pelo facto do utilizador e da rede tomarem conhecimento de uma chave secreta K, que é partilhada entre e está disponível apenas ao Módulo de Identidade de Serviços do Utilizador USIM e ao Centro de Autenticação AuC no Ambiente Home HE do utilizador. Além disso, o USIM e o HE acompanham os contadores SEQ_{MS} e SEQ_{HE} respectivamente para suportar a autenticação de rede.

O procedimento pode ser concebido de modo a ser compatível com, por exemplo, a arquitectura da segurança GSM actual e facilitar a migração de GSM para UMTS. O método é composto por um protocolo de desafio/resposta idêntico ao protocolo de estabelecimento da chave e da autenticação do assinante GSM combinado com um protocolo de exploração única e sequência baseada em números para a autenticação da rede derivada do padrão ISO/IEC 9798-4. Antes de explicar a formação das chaves de integridade, será discutido um mecanismo de acordo de autenticação e de chave. A Figura 7 mostra uma vista geral de um possível acordo de autenticação e de chave. A Figura 8 mostra um possível procedimento para a criação de vectores de autenticação.

Uma vez recebido um pedido de VLR/SGSN, o HE/AuC envia uma rede ordenada de vectores de autenticação *n* (o equivalente a um "tripleto" GSM) ao VLW SGSN. Cada vector de autenticação consiste dos seguintes componentes: um número aleatório RAND, uma resposta esperada XRES, uma chave de decifração CK, uma chave de integridade IK e um testemunho de autenticação AUTN. Cada vector de autenticação é bom para um acordo de autenticação e de chave entre VLWSGSN e USIM.

Quando VLR/SGSN inicia um acordo de autenticação e chave, selecciona o próximo vector de autenticação a partir da rede e envia os parâmetros RAND e AUTN para o utilizador. O USIM verifica se AUTN pode ser aceite e, em caso afirmativo, produz uma resposta RES, que é devolvida a VLR/SGSN. O USIM também computoriza CK e IK. VLR/SGSN compara o RES recebido com XRES. Se coincidirem, o VLR/SGSN considera a troca do acordo de autenticação e chave como um processo completado com sucesso. As chaves estabelecidas CK e IK serão transferidas pelo USIM e VLR/SGSN para as entidades, que realizam as funções de decifração e integridade. No sistema UMTS proposto, estas entidades podem, preferencialmente, ser alguns dos protocolos da interface de rádio descritos na Figura 2. As entidades encontram-se, preferencialmente no Equipamento do Utilizador UE e no Controlador de Rede de Rádio RNC.

VLR/SGSNs pode oferecer um serviço seguro, mesmo quando as ligações HE/AuC não estão disponíveis, permitindo que usem chaves de decifração e de integridade anteriormente derivadas para um utilizador, de modo a configurar ainda uma ligação segura sem necessidade de um acordo de autenticação e de chave. A autenticação baseia-se, nesse caso, numa chave de integridade partilhada, através da protecção da integridade dos dados de mensagens de sinalização.

As partes de autenticação serão AuC do HE do utilizador (HE/AuC) e o USIM na estação móvel do utilizador. O mecanismo pode consistir dos seguintes procedimentos:

Distribuição de informação de autenticação a partir de HE/AuC para VLWSGSN. Presume-se que o HE do utilizador pode confiar em VLR/SGSN para tratar a informação de autenticação com segurança. Presume-se também que as ligações intra-sistema entre VLR/SGSN para o HE/AuC são convenientemente seguras. Presume-se ainda que o utilizador confie no HE.

- Autenticação mútua e estabelecimento de novas chaves de decifração e integridade entre VLWSGSN e MS.
- Distribuição dos dados de autenticação de um VLR anteriormente visitado para o VLR recentemente visitado. Presume-se
que as ligações entre VLR/SGSNs são convenientemente seguras.

A finalidade da distribuição dos dados de autenticação do HE para SN é dotar VLR/SGSN com uma rede de novos vectores de autenticação do HE do utilizador para realizar uma série de autenticações do utilizador. O VLR/SGSN invoca os procedimentos, pedindo vectores de autenticação para o HE/AuC. O pedido de dados de autenticação deve incluir uma identidade do utilizador. Se o utilizador é conhecido no VLR/SGSN através do IMUI, o pedido de dados de autenticação deve incluir o IMUI. Se o utilizador é identificado através de uma entidade permanente codificada, a mensagem HLR da qual o HE pode derivar o IMUI pode ser, em vez disso, incluída. Neste caso, este procedimento e o procedimento do pedido de identidade do utilizador ao HLR são, preferencialmente, integrados.

Uma vez recebido o pedido de dados de autenticação a partir do VLWSGSN, o HE pode ter previamente computorizado o número exigido de vectores de autenticação e pode tê-los devolvido à base de dados HLR ou pode computorizá-los a pedido. O HE/AuC devolve uma resposta de autenticação ao VLR/SGSN que contém uma rede ordenada de vectores de autenticação n AV(1 ..n). O HE/AuC cria um novo número de sequência SQN e um desafio imprevisível RAND. Para cada utilizador, o HE/AuC também acompanha um contador que é SQNHE.

O mecanismo para verificar o quão recente são os números de sequência no USIM, permite, em certa medida, a utilização desordenada dos números de sequência. Isto garante manter a taxa de falhas de autenticação suficientemente baixa, devido a falhas de sincronização. Isto requer a capacidade do USIM guardar a informação sobre eventos de autenticação com sucesso no passado (por ex. números de sequência ou suas partes relevantes). O mecanismo deve assegurar que um número de sequência continue a ser aceite se estiver entre os últimos números de sequência x = 50 criados. Isto não exclui o facto de um número de sequência ser rejeitado por outras razões, como um limite de idade para números de sequência com base no tempo.

Tem de ser usado o mesmo número mínimo x ao longo dos sistemas para garantir que a taxa de falhas de sincronização seja suficientemente baixa sob vários cenários de uso, em particulares registos simultâneos nos domínios CS e de serviço PS, movimento do utilizador entre VLRs/SGSNs que não trocam a informação de autenticação, redes super-cobradas.

A utilização de SEQHE pode ser específica ao método de criação de números de sequência. Pode ser incluído um campo de gestão da autenticação e de chaves AMF no testemunho de autenticação de cada vector de autenticação.

Subsequentemente, podem ser computorizados os seguintes valores:

- um código de autenticação da mensagem MAC = $f1_K$(SQN || RAND || AMF), em que f1 é uma função de autenticação da mensagem;
- uma resposta esperada XRES = $f2_K$ (RAND), em que f2 é uma função de autenticação da mensagem (possivelmente cortada);
- uma chave de decifração CK = $f3_K$ (RAND), em que f3 é uma função de criação de chaves;
- uma chave de integridade IK = $f4_K$ (RAND), em que f4 é uma função de criação de chaves;
- uma chave de anonimato AK = $f5_K$ (RAND), em que f5 é uma função de criação de chaves ou

f5 ≡ 0.

De acordo com as versões da presente invenção, é criado mais do que um IK. Isto pode ser conseguido, por exemplo, modificando a função f4, de modo a produzir o desejado número de IKs (por ex 4: ver Figura 9). Uma possibilidade é especificar que a função f4 tem de ser activada várias vezes durante a criação de um vector de autenticação. Isto pode ser implementado, por exemplo, através da introdução, na segunda volta, do primeiro IK[1] produzido como entrada para a função f4, em vez de um novo

RAND. Na terceira 'volta', o IK[2] produzido na segunda volta seria introduzido na função f4 para obter uma terceira chave de integridade IK[3]. Uma possibilidade é também introduzir um número desejado de RANDS na função f4. Por conseguinte, é possível produzir a quantidade necessária de IK:s para o sistema em questão. Por exemplo, no sistema UMTS de acordo com as especificações 3GPP lançamento'99, seriam precisas quatro chaves de integridade.

Pode ser construído o testemunho de autenticação AUTN = SQN *O* AK || AMF || MAC. AK é a chave de anonimato utilizada para ocultar o número de sequência, pois este pode expor a identidade e localização do utilizador. A ocultação do número de sequência é para proteger apenas contra ataques passivos. Se não for preciso ocultar, então f5≡0.

O objectivo do procedimento do acordo de autenticação e chave é autenticar o utilizador e estabelecer um novo par de chaves de decifração e integridade entre VLR/SGSN e MS. Durante a autenticação, o utilizador verifica o quão recente é o vector de autenticação utilizado. VLR/SGSN invoca o procedimento, seleccionando o próximo vector de autenticação não utilizado a partir da rede desordenada de vectores de autenticação na base de dados VLR. VLR/SGSN envia ao utilizador o desafio aleatório RAND e um testemunho de autenticação para autenticação de rede AUTN a partir do vector de autenticação. Uma vez recebido, o utilizador procede conforme ilustrado na Figura 9.

Uma vez recebido RAND e AUTN, o utilizador computoriza primeiro a chave de anonimato AK = $f5_K$ (RAND) e restaura o número de sequência SQN = (SQN O AK) O AK. De seguida, o

utilizador computoriza XMAC = $f1_K$ (SQN || RAND || AMF) e compara isto com MAC, que está incluído em AUTN. Se forem diferentes, o utilizador devolve a rejeição da autenticação do utilizador ao VLR/SGSN com uma indicação da causa e o utilizador abandona o procedimento. De seguida, USIM verifica se o número de sequência recebido SQN está dentro da área correcta.

De acordo com uma versão da presente invenção, o USIM cria mais do que um IK, em vez de criar apenas um IK. Como anteriormente explicado. Isto pode ser conseguido, por exemplo, modificando a função f4, especificando que a função f4 tem de ser activada várias vezes durante a criação de um vector de autenticação ou introduzindo um número desejado de RAND na função f4. Isto pode exigir que a rede (SNNLR) envie o número desejado de RAND e AUTN ao UE e que o UE possa precisar de produzir também um RES para cada RAND e devolver todos os RES produzidos à rede, como foi acima descrito para o caso de um RAND+AUTN.

As versões da presente invenção podem ser utilizadas em qualquer sistema, que permita a sinalização não-decifrada e a utilização de somas de verificação de integridade em, pelo menos, dois suportes de rádio paralelos.

As versões da presente invenção foram descritas no contexto de uma rede de telecomunicações celular sem fios. No entanto, podem ser utilizadas versões alternativas da presente invenção com qualquer outro tipo de rede de comunicações sem fios ou não. As versões da presente invenção podem ser utilizadas em qualquer forma ou comunicação, em que as verificações de integridade ou

idêntico são dotadas de vários suportes de rádio ou idêntico em paralelo.

DOCUMENTOS APRESENTADOS NA DESCRIÇÃO

Esta lista dos documentos apresentados pelo requerente foi exclusivamente recolhida para informação do leitor e não faz parte do documento europeu da patente. Apesar de ter sido elaborado com o máximo cuidado, o IEP não assume, porém, qualquer responsabilidade por eventuais erros ou omissões.

Documentos de patente apresentados na descrição

US 4393269 A

Documentação não relativa a patentes citada na descrição

Sistema Universal de Telecomunicações Móveis (UMTS); Segurança 3G; Arquitectura de Segurança (3G PP TS 33, 102 Versão 3.3.1 Editado 1999). *ETSI TS* 133 102 V3.3.1, Janeiro de 2000, 1-64 **[0017]**

Lisboa, 18/08/2010

REIVINDICAÇÕES

1. Um nó para ser utilizado num sistema, que compreende o referido nó (6, 20) e um outro nó (20, 6), vários canais de comunicação diferentes entre os referidos nós, possuindo cada canal de comunicação uma identidade diferente, em que referido nó compreende:

meios para calcular um código de autenticação (XMAC-I) a partir de uma série de valores, alguns dos quais são os mesmos para os vários canais de comunicação diferentes, meios para receber informação relacionada com um código de autenticação (MAC-I) calculado pelo referido outro nó;

e

meios para comparar informação relacionada com um código de autenticação (XMAC-I) calculado pelo referido nó com informação relacionada com um código de autenticação (MAC-I) calculado pelo outro nó; e

caracterizado pelo facto

de, pelo menos, um dos referidos valores compreender informação relacionada com a identidade de um canal de comunicação (RB ID) dos referidos vários canais de comunicação.

2. Um nó de acordo com a reivindicação 1, compreendendo um controlador de rede de rádio (24).

3. Um nó de acordo com a reivindicação 1, compreendendo um equipamento de utilizador (6).

4. Um nó de acordo com qualquer uma das reivindicações anteriores, compreendendo meios para comunicar via uma ligação sem fios.

5. Um sistema de comunicação com um nó conforme reivindicado em qualquer uma das reivindicações anteriores.

6. Um método para levar a cabo uma verificação de integridade num sistema, que compreende um nó e um outro nó (6, 20), vários canais de comunicação entre o referido nó e o outro referido nó, possuindo cada canal de comunicação uma diferente identidade (RB ID), em que o referido método inclui os passos de:

receber no nó, informação relacionada com um código de autenticação (MAC-I), a partir do outro nó;
calcular um outro código de autenticação (XMAC-I), utilizando vários valores, alguns dos quais são os mesmos para os referidos vários canais de comunicação diferentes, comparando o outro código de autenticação (XMAC-I) com a referida informação relacionada com um código de autenticação (MAC-I) recebido do outro nó e **caracterizado pelo facto** de, pelo menos um dos referidos valores compreender informação relacionada com a identidade de um canal de comunicação (RB ID) dos referidos múltiplos canais.

7. Um método de acordo com a reivindicação 6, compreendendo a introdução de informação relacionada com a identidade do canal de comunicação (RB ID) dos referidos vários canais de comunicação, como um valor de entrada

separado num algoritmo de integridade (UIA) para calcular o código de autenticação (XMAC-I).

8. Um método de acordo com a reivindicação 6, compreendendo providenciar um valor de entrada combinado, combinando a informação relacionada com a identidade do canal de comunicação (RB ID) dos referidos vários canais de comunicação com, pelo menos, um outro valor de entrada, e introduzindo o valor de entrada combinado num algoritmo de integridade (UIA) para calcular o código de autenticação (XMAC-I).

9. Um método de acordo com as reivindicações de 6 a 8, em que os referidos valores para calcular o código de autenticação da mensagem (XMAC-I) compreendem um ou mais dos seguintes valores de uma arquitectura de segurança do Projecto de Parceria de Geração 3G (3GPP) do Sistema Universal de Telecomunicações Móvel (UMTS): uma chave de integridade (IK); um valor de direcção (DIRECÇÃO), um valor novo (RECENTE), um valor de mensagem (MENSAGEM) e um valor de contagem (CONTAGEM-I).

10. Um método de acordo com as reivindicações de 6 a 9, em que os referidos canais de comunicação compreendem um suporte de rádio.

11. Um método de acordo com a reivindicação 10, em que o referido suporte de rádio é um suporte de rádio de sinalização.

Lisboa, 18/08/2010

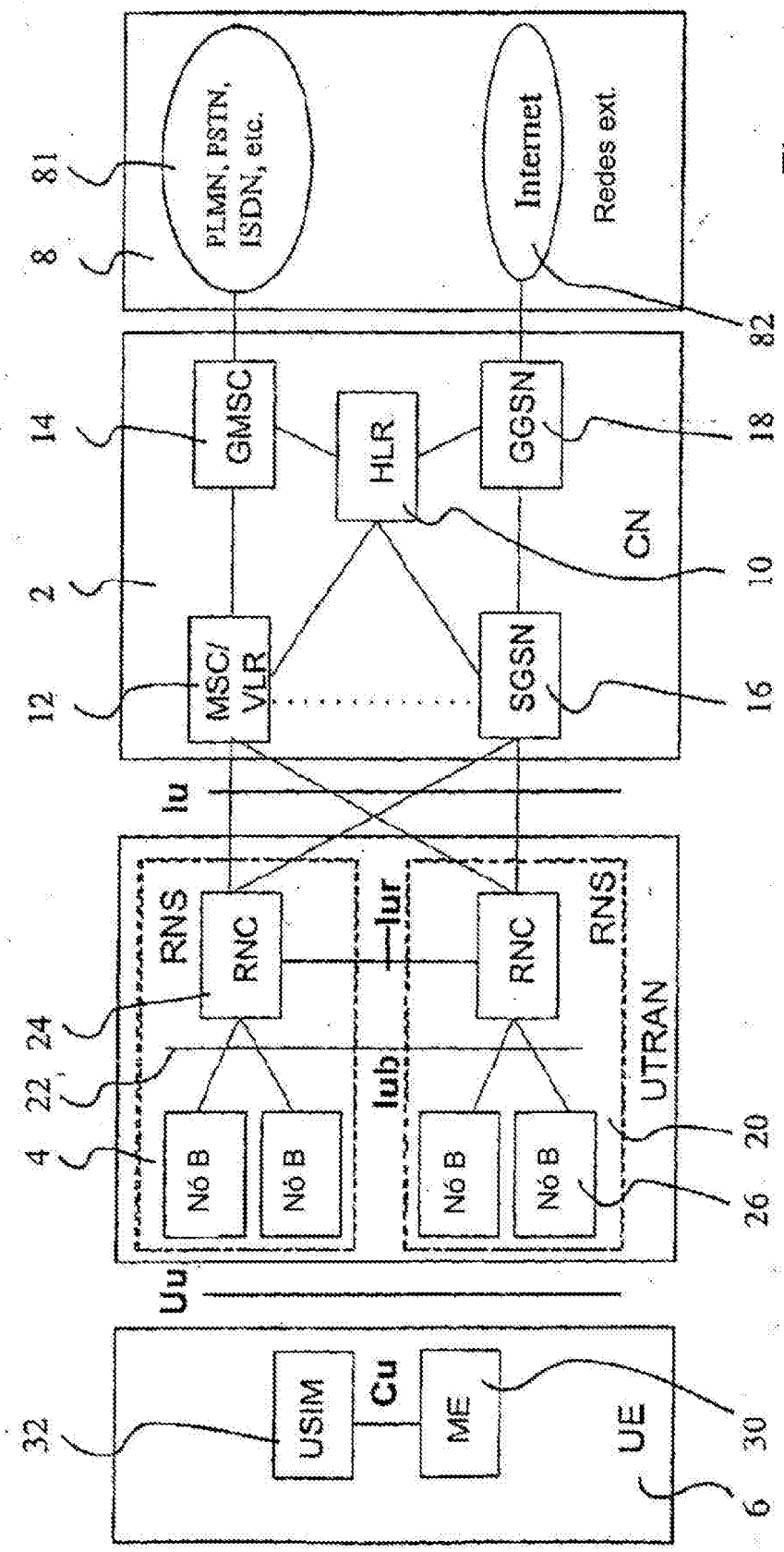
PLMN, PSTN, ISDN, etc.
Internet
Redes ext.
GMSC
HLR
GGSN
MSC/ VLR
SGSN
CN
Iu
RNS
RNC
Iur
RNC
RNS
Iub
Nó B
Nó B
Nó B
Nó B
UTRAN
Uu
USIM
Cu
ME
UE
81
8
82
14
18
2
10
12
16
24
22
4
20
26
32
30
6

Figura 1

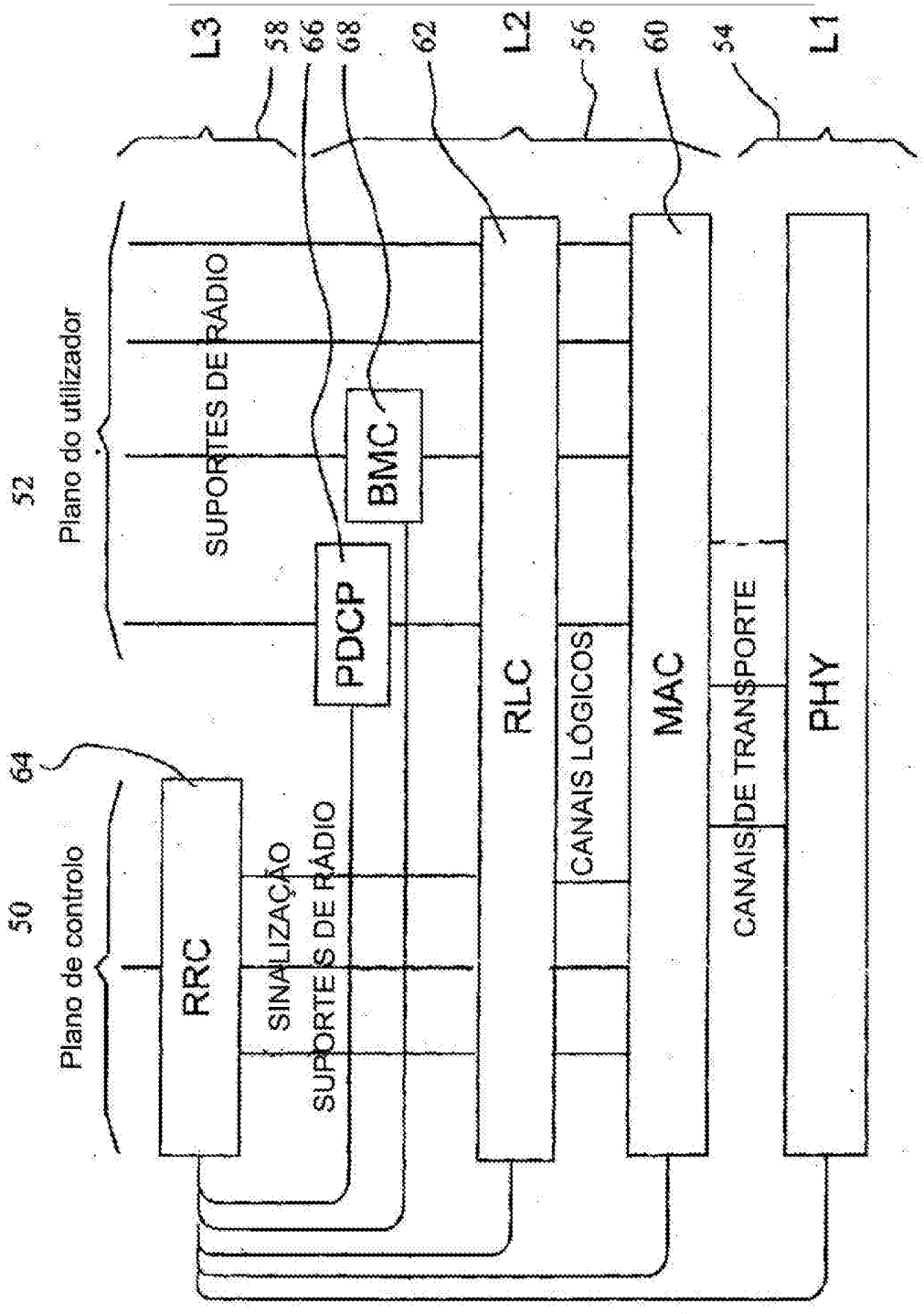
L3
58
66
68
62
L2
56
60
54
L1
52
Plano do utilizador
SUPORTES DE RÁDIO
BMC
PDCP
RLC
MAC
PHY
CANAIS LÓGICOS
CANAIS DE TRANSPORTE
64
50
Plano de controlo
RRC
SINALIZAÇÃO
SUPORTES DE RÁDIO

Figura 2

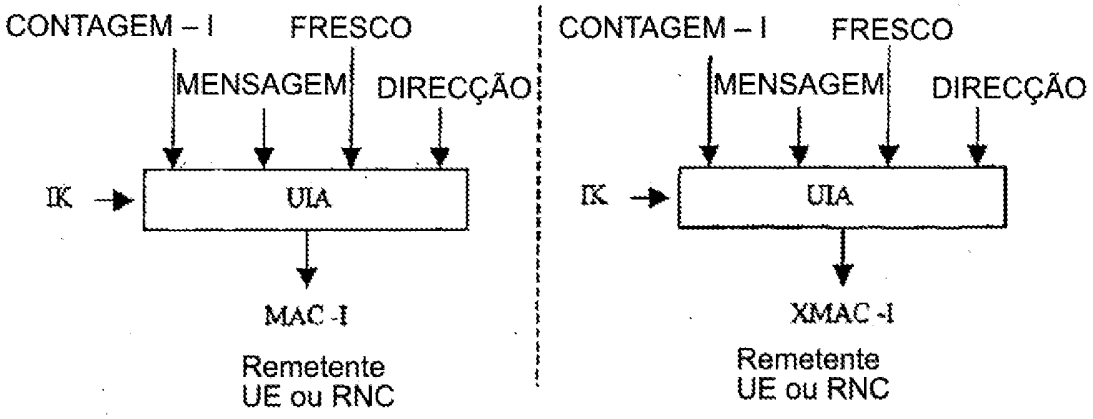

Figura 3

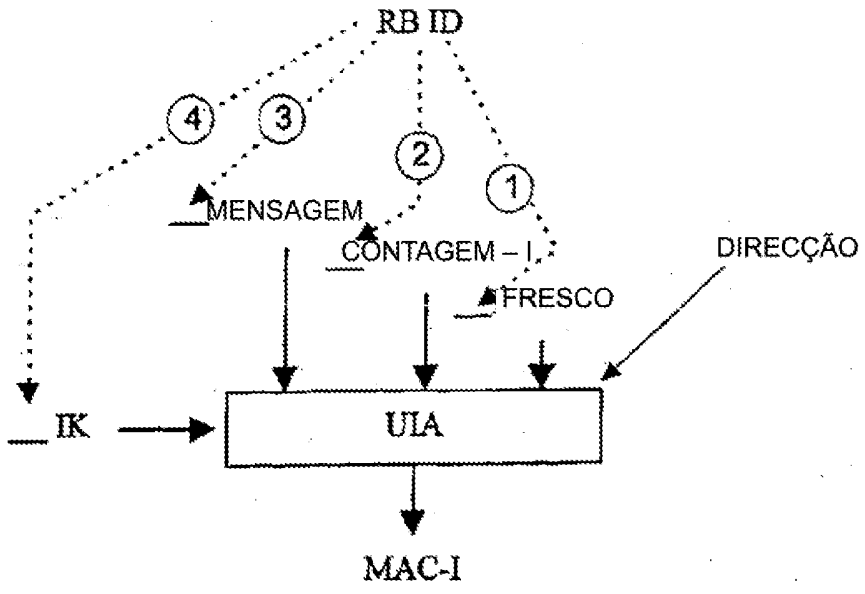

Figura 4

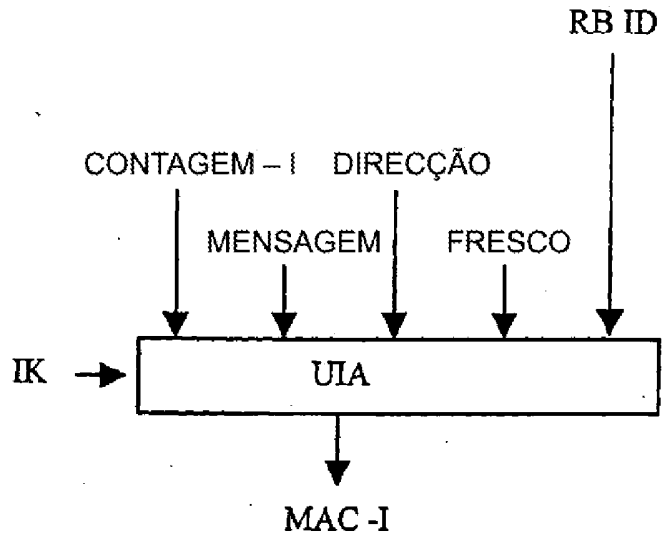

Figura 5

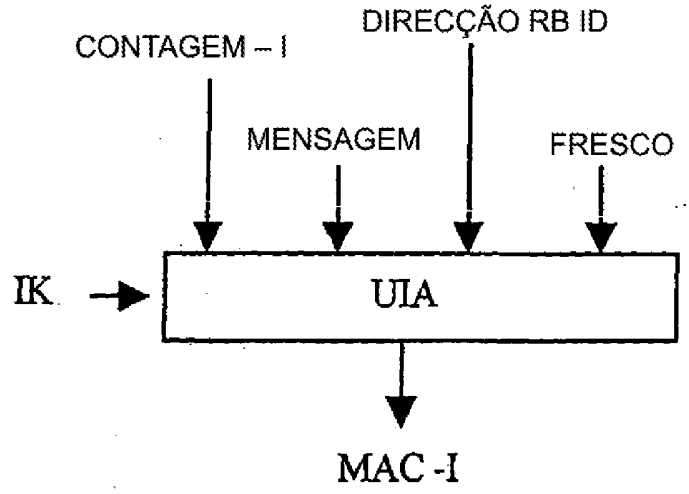

Figura 6

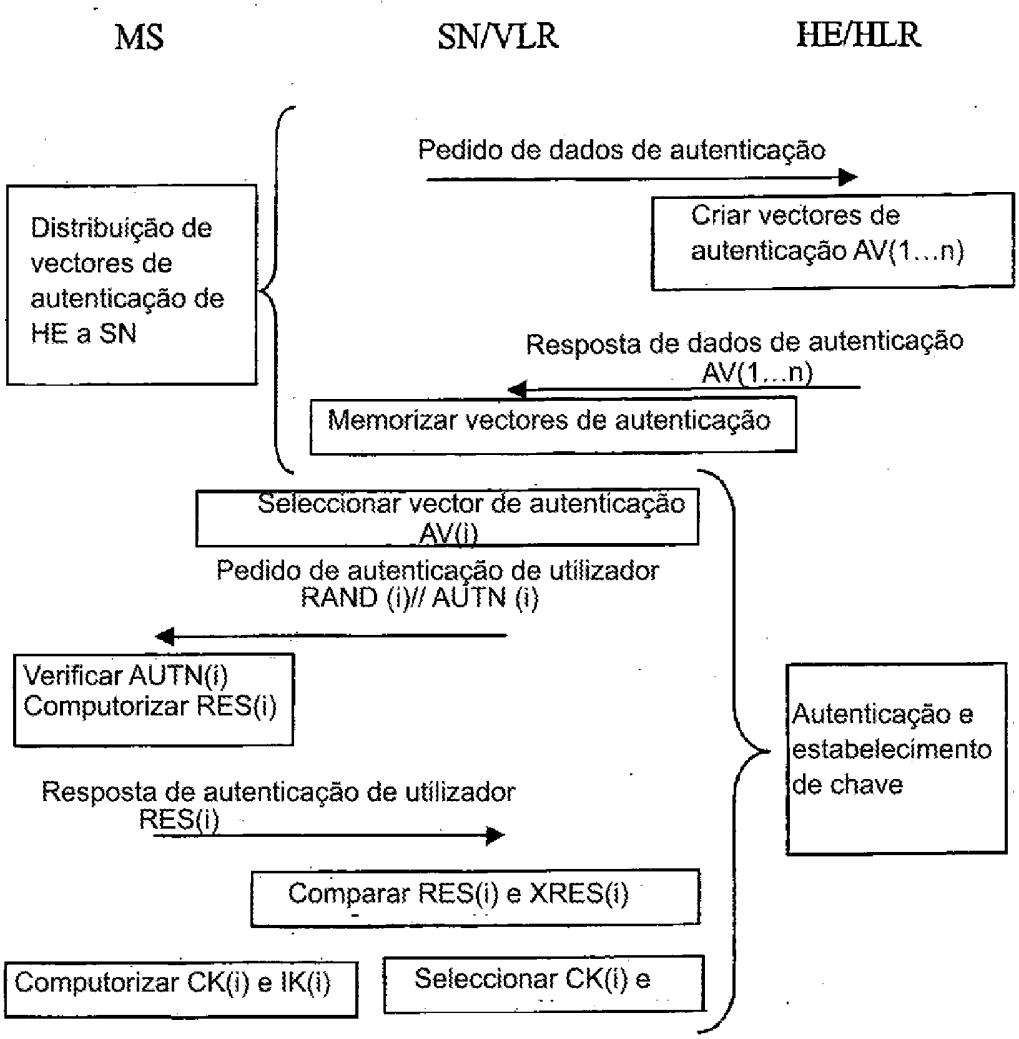
MS
SN/VLR
HE/HLR
Pedido de dados de autenticação
Criar vectores de autenticação AV(1...n)
Distribuição de vectores de autenticação de HE a SN
Resposta de dados de autenticação AV(1...n)
Memorizar vectores de autenticação
Seleccionar vector de autenticação AV(i)
Pedido de autenticação de utilizador RAND (i)// AUTN (i)
Verificar AUTN(i) Computorizar RES(i)
Autenticação e estabelecimento de chave
Resposta de autenticação de utilizador RES(i)
Comparar RES(i) e XRES(i)
Computorizar CK(i) e IK(i)
Seleccionar CK(i) e

Figura 7

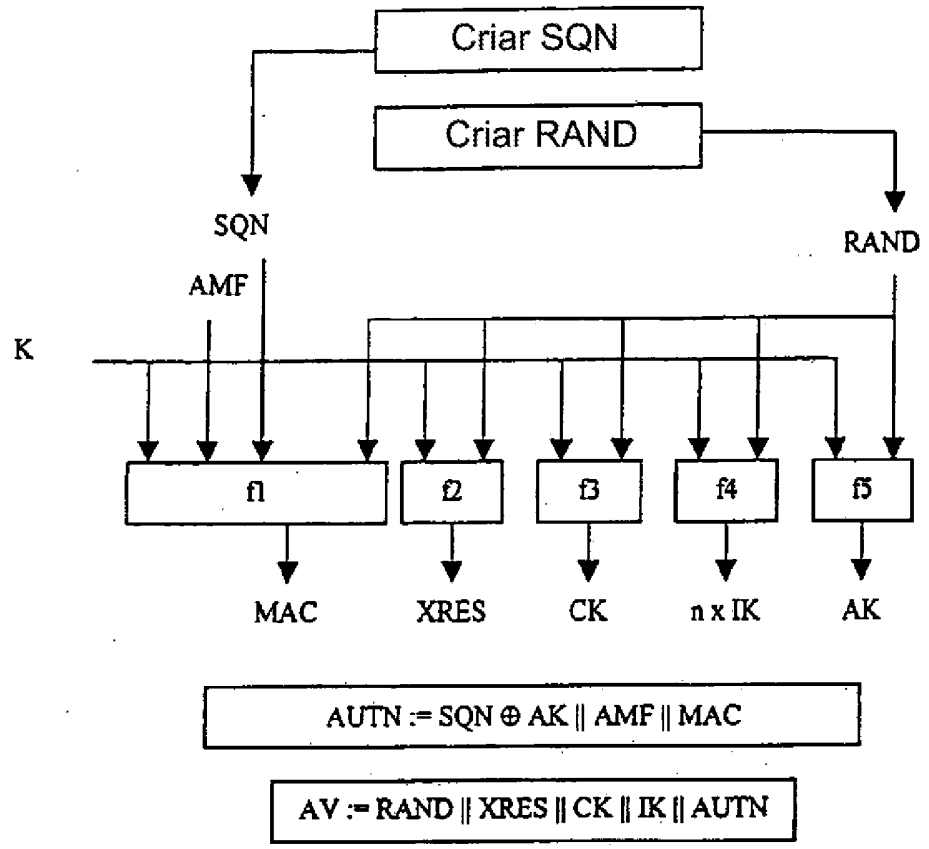
Criar SQN
Criar RAND
SQN
RAND
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
n x IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Figura 8

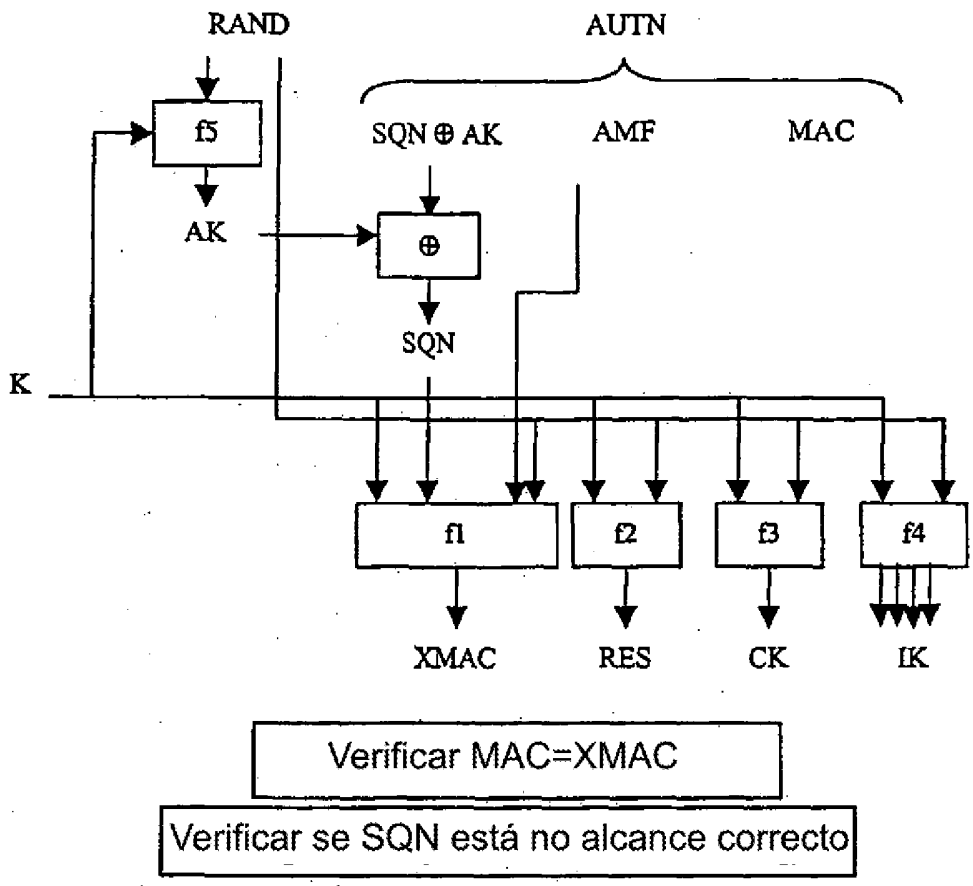
RAND
AUTN
f5
SQN ⊕ AK
AMF
MAC
AK
⊕
SQN
K
f1
f2
f3
f4
XMAC
RES
CK
IK
Verificar MAC=XMAC
Verificar se SQN está no alcance correcto

Figura 9