República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial.

(21) **PI0707583-9 A2**

BRPI0707583A2

(22) Data de Depósito: 09/02/2007
(43) Data da Publicação: 10/05/2011
(RPI 2105)

(51) Int.Cl.:
H04Q 7/38

(54) Título: **OBSCURECIMENTO DE IDENTIDADE TEMPORÁRIAS DE EQUIPAMENTO DE USUÁRIO**

(30) Prioridade Unionista: 10/02/2006 US 60/771,974, 27/03/2006 US 60/786,463

(73) Titular(es): Qualcomm Incorporated

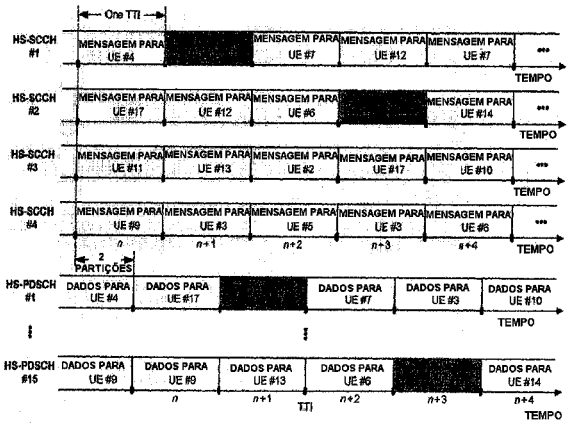
(72) Inventor(es): Nathan Edward Tenny

(74) Procurador(es): Montaury Pimenta, Machado & Lioce S/C Ltda

(86) Pedido Internacional: PCT US2007061939 de 09/02/2007

(87) Publicação Internacional: WO 2007/095471de 23/08/2007

(57) Resumo: OBSCURECIMENTO DE IDENTIDADES TMPORÁRIAS DE EQUIPAMENTO DE USUÁRIO. São descritas técnicas para ocultar identificadores temporários (IDs) atribuidos a equipamentos de usuário (UEs) por um sistema de comunicação sem fio. Em uma entidade de rede, um primeiro ID atribuído a um UE e possivelmente um valor salt são transformados, por exemplo, com base em uma função hash, para obter um segundo ID para o UE. Uma mensagem de saída dirigida ao UE é gerada com base em uma mensagem de entrada, o segundo ID e o valor salt (caso presente). A mensagem de saída é enviada via um canal comum compartilhado pelo UE e outros UEs. No UE, uma mensagem é recebida via o canal comum, e um valor salt (caso enviado) é obtida a partir da mensagem recebida. O primeiro ID e o valor salt são transformados para obter o segundo ID, que é utilizado para determinar se a mensagem recebida é destinada ao UE.



"OBSCURECIMENTO DE IDENTIDADES TEMPORÁRIAS DE EQUIPAMENTO DE USUÁRIO"

O presente pedido reivindica prioridade para Pedido U.S. provisório Número de Série 60/771.974, depositado em 10 de fevereiro de 2006, intitulado "OBSCURING TEMPORARY USER EQUIPMENT IDENTITIES," e Pedido U.S. Provisório Número de Série 60/786.463, depositado em 27 de março de 2006, intitulado "DOWNLINK DATA SCHEDULING WITH OPAQUE UE IDENTITIES IN E-UTRAN," ambos cedidos à cessionária do presente pedido e incorporados aqui a título de referência.

FUNDAMENTOS

I. Campo

A presente descrição refere-se, geralmente, à comunicação, e mais especificamente a técnicas para obscurecer identidades em comunicação sem fio.

II. Fundamentos

Redes de comunicação sem fio são amplamente aplicadas para prover vários serviços de comunicação como voz, vídeo, dados em pacote, troca de mensagens, broadcast, etc. Uma rede de comunicação sem fio pode incluir muitos Nós Bs (ou estações base) que podem se comunicar com muitos equipamentos de usuário (UEs). Os UEs podem ser atribuídos a vários identificadores ou identidades (IDs) utilizados para identificar exclusivamente esses UEs para várias finalidades. Em certas ocorrências, os IDs de UE podem ser enviados pelo ar livre sem nenhuma cifragem. Isso pode tornar possível para um espião (eavesdropper) ou adversário (attacker) montar um ataque de capacidade de link por monitorar um canal de comunicação para mensagens e determinar quais mensagens são dirigidas ao mesmo UE com o

passar do tempo. O ataque de capacidade de link pode ser capaz de ligar mensagens a UEs específicos porém pode não ser capaz de determinar as verdadeiras identidades dos UEs. O ataque de capacidade de link pode ser utilizado para rastrear as localizações dos UEs e também pode ser a base de outros ataques de segurança mais severos. Por exemplo, o adversário pode ser capaz de determinar qual ID de UE é atribuído a um UE específico por iniciar uma chamada para aquele UE e observar quais IDs de UE são utilizados aproximadamente ao mesmo tempo.

Há, portanto, necessidade na área por técnicas para combater ataques de capacidade de link sem impor cargas computacionais excessivas sobre os UEs e entidades de rede.

SUMÁRIO

Técnicas para ocultar IDs temporários atribuídos aos UEs por uma rede de comunicação sem fio são descritas aqui. Essas técnicas podem ser utilizadas para vários tipos de mensagens endereçadas a UEs específicos e enviadas livre sem cifragem via canais comuns. Essas técnicas podem ser utilizadas para melhorar a segurança, por exemplo, para frustrar ataques de capacidade de link.

Em um aspecto, em uma entidade de rede (por exemplo, um Nó B), um primeiro ID atribuído a um UE pode ser transformado para obter um segundo ID para o UE. O primeiro ID pode ser um Identificador Temporário de Rede Rádio (RNTI) atribuído ao UE no Sistema de Telecomunicação Móvel Universal (UMTS) ou algum outro tipo de ID em algum outro sistema de comunicação. O primeiro ID e possivelmente um valor salt (que é um valor não-estático) pode ser transformado com base em uma função hash para obter o segundo ID. Uma mensagem de saída dirigida ao UE pode ser

gerada com base em uma mensagem de entrada, o segundo ID, e o valor salt (caso presente). A mensagem de entrada pode ser uma mensagem de paging, uma mensagem de programação que contém informações de programação, uma mensagem de atribuição de recursos, etc. A mensagem de saída pode ser enviada via um canal comum compartilhado pelo UE e outros UEs.

Em outro aspecto, no UE, uma mensagem pode ser recebida via canal comum, e um valor salt (caso enviado) pode ser obtido a partir da mensagem recebida. O primeiro ID e o valor salt (se enviado) podem ser transformados para obter o segundo ID, que pode ser utilizado para determinar se a mensagem recebida é destinada ao UE.

Vários aspectos e características da descrição são descritos em detalhes adicionais abaixo.

BREVE DESCRIÇÃO DOS DESENHOS

A figura 1 mostra uma rede UMTS.

A figura 2 mostra transmissões para Acesso em Pacote Downlink com alta Velocidade (HSDPA).

As figuras 3A e 3B mostram dois desenhos para transformar um RNTI.

A figura 4A mostra um processador que envia um RNTI transformado livre.

A figura 4B mostra um processador que incorpora um RNTI transformado em uma mensagem.

A figura 5 mostra um processo para enviar mensagens de sinalização para um UE.

A figura 6 mostra um aparelho para enviar mensagens de sinalização para um UE.

A figura 7 mostra um processo para receber mensagens de sinalização em um UE.

A figura 8 mostra um aparelho para receber mensagens de sinalização em um UE.

A figura 9 mostra um diagrama de blocos de um UE, um Nó B e um RNC.

DESCRIÇÃO DETALHADA

As técnicas descritas aqui podem ser utilizadas para várias redes de comunicação como redes de Acesso Múltiplo por Divisão de Código (CDMA), redes de Acesso Múltiplo por Divisão de Tempo (TDMA), redes de Acesso Múltiplo por Divisão de Freqüência (FDMA), redes FDMA Ortogonais (OFDMA), redes FDMA de Portadora Única (SC-FDMA), etc. Os termos "redes" e "sistemas são freqüentemente utilizados de forma intercambiável. Uma rede CDMA pode implementar uma tecnologia de rádio como Acesso de Rádio Universal Terrestre (UTRA), UTRA evoluído (E-UTRA), cdma2000, etc. UTRA e E-UTRA fazem parte de UMTS. UTRA inclui CDMA-de banda larga (W-CDMA) e Taxa de Chip Baixa (LCR). Cdma2000 abrange padrões IS-2000, IS-95 e IS-856. Uma rede TDMA pode implementar uma tecnologia de rádio como Sistema Global para Comunicação Móvel (GSM). Uma rede OFDMA pode implementar uma tecnologia de rádio como Evolução de Longa Duração (LTE), IEEE 802.20, Flash-OFDM®, etc. UTRA, E-UTRA, UMTS, GSM e LTE são descritos em documentos a partir de uma organização denominada "3rd Generation Partnership Project" (3GPP). Cdma2000 é descrito nos documentos a partir de uma organização denominada "3rd Generation Partnership Project 2" (3GPP2). Essas várias tecnologias de rádio e padrões são conhecidas na técnica. Para clareza, certos aspectos das técnicas são descritas abaixo para UMTS, e terminologia 3GPP é utilizado em grande parte da descrição abaixo.

A figura 1 mostra uma rede UMTS 100 que inclui

uma Rede de Acesso de Rádio Universal Terrestre (UTRAN) e uma rede núcleo 140. A UTRAN inclui múltiplos Nós Bs 110 e um Controlador de Rede Rádio (RNC) 130. Um Nó B é geralmente uma estação fixa que se comunica com os UEs e também pode ser referido como um Nó B intensificado, uma estação base, um ponto de acesso, etc. Cada Nó B 110 provê cobertura de comunicação para uma área geográfica particular e suporta comunicação para os UEs localizados dentro da área de cobertura. O termo "célula" pode se referir a um Nó B e/ou sua área de cobertura dependendo do contexto no qual o termo é utilizado. RNC 130 acopla-se aos Nós Bs 110 e provê coordenação e controle para esses Nós Bs. RNC 130 também origina e termina mensagens para certos protocolos e aplicativos. Rede núcleo 140 pode incluir várias entidades de rede que suportam várias funções como roteamento de pacote, registro de usuário, gerenciamento de mobilidade, etc.

UEs 120 podem ser dispersos por toda a rede UMTS, e cada UE pode ser estacionário ou móvel. Um UE pode ser também referido como uma estação móvel, um terminal, um terminal de acesso, uma unidade de assinante, uma estação, etc. Um UE pode ser um telefone celular, um assistente digital pessoal (PDA), um dispositivo sem fio, um dispositivo portátil, um modem sem fio, um computador laptop, etc. Um UE pode se comunicar com um ou mais Nós Bs no downlink e/ou uplink em qualquer dado momento. O downlink (ou link direto) refere-se ao link de comunicação a partir dos Nós Bs para os UEs, e o uplink (ou link reverso) refere-se a um link de comunicação a partir dos UEs para os Nós Bs.

Em UMTS, dados e sinalização para os UEs são processados como canais lógicos em uma camada de Controle de Radioenlace (RLC). Os canais lógicos incluem um Canal de

Tráfego Dedicado (DTCH), um Canal Compartilhado de Downlink (DSCH), um Canal de Controle Dedicado (DCCH), um Canal de Controle Comum (CCCH), etc. Os canais lógicos são mapeados para transportar canais em uma camada de Controle de acesso ao Meio (MAC). Os canais de transporte carregam dados para vários serviços como voz, vídeo, dados em pacote, etc. Os canais de transporte são mapeados para canais físicos em uma camada física. Os canais físicos são canalizados com diferentes códigos de canalização e são ortogonais entre si no domínio de código.

Um UE em UMTS pode ser atribuído a uma variedade de IDs utilizados para identificar o UE para várias finalidades. Esses IDs de UE podem ter diferentes contextos ou escopos (por exemplo, célula, área de paging, etc.) e/ou diferentes períodos de vida útil (por exemplo, temporário ou permanente). Por exemplo, o UE pode ser atribuído a vários RNTIs que podem ser utilizados como IDs temporários. A tabela 1 lista alguns RNTIs que podem ser atribuídos ao UE e provê uma descrição curta de onde cada RNTI pode ser utilizado. Os C-RNTI e U-RNTI podem ser atribuídos ao UE por um RNC em serviço e pode ser estendido para uma conexão RRC em uma célula particular. O C-RNTI pode ser utilizado para mensagens enviadas no DTCH e DSCH. O U-RNTI pode ser utilizado para mensagens paging enviadas em um Canal de Paging (PCH) e para mensagens enviadas no DCCH. Os DSCH-RNTI, H-RNTI e E-RNTI podem ser estendidos para uma célula particular e utilizados para sinalizar mensagens enviadas no DSCH, um Canal Compartilhado de Downlink com alta Velocidade (HS-DSCH) e um Canal de Concessão Absoluta E-DCH (E-AGCH), respectivamente. Esses vários RNTIs podem ser coletivamente referidos como "X-RNTIs" e podem ser utilizados como IDs temporários em contexto local para endereçar o UE para mensagens de sinalização enviadas por

Controle de Recursos de Rádio (RRC) e protocolos MAC. Os X-RNTIs podem ser atribuídos por diferentes entidades de rede dentro do UTRAN (ou simplesmente, o UTRAN). Cada X-RNTI pode ser utilizado para sinalizar mensagens permutadas entre a entidade de rede de atribuição e o UE receptor.

Tabela 1

Símbolo	**Nome**	**Compri-mento**	**Uso**
C-RNTI	Célula RNTI	16 bits	Usado para mensagens enviadas em DTCH e DSCH
U-RNTI	UTRAN-RNTI	32 bits	Usado para mensagens paging enviadas em PCH e para mensagens enviadas em DCCH
DSCH-RNTI	Identificador de Rede Rádio DSCH	16 bits	Usado para sinalizar mensagens enviadas em DSCH
H-RNTI	Identificador de Rede Rádio HS-DSCH	16 bits	Usado para sinalizar mensagens enviadas em HS-DSCH
E-RNTI	Identificador de Rede Rádio E-DCH	16 bits	Usado para sinalizar mensagens enviadas em E-AGCH

Os X-RNTIs podem ser atribuídos a um UE em vários tempos pela UTRAN. As atribuições podem ocorrer via sinalização não cifrada devido à ausência de uma relação de segurança preexistente entre a UTRAN e UE no momento de atribuição. Entretanto, na atribuição de uma X-RNTI, a UTRAN endereça tipicamente o UE por uma Identidade de Assinante Móvel Temporário (TMSI) ou uma TMSI de Pacote (P-TMSI), que é atribuída ao UE em sinalização cifrada em uma camada de Estrato de Não Acesso (NAS). Desse modo, um

adversário pode observar qual X-RNTI foi atribuído por uma mensagem downlink, porém, na ausência de conhecimento adicional da TMSI ou P-TMSI, não seria capaz de determinar qual UE estava recebendo a atribuição.

Após um X-RNTI ser atribuído a um UE, o X-RNTI pode ser enviado livre sem cifragem em sinalização downlink e/ou uplink. Por exemplo, mensagens para UEs específicos podem ser enviadas no CCCH e endereçadas aos UEs receptores por seus U-RNTIs. Essas mensagens podem ser enviadas em radioportador de sinalização 0 (SRBO) e seriam não cifradas uma vez que SRBO pode conter mensagens para UEs que não têm ainda uma relação de segurança com a UTRAN. Para mensagens enviadas não cifradas em um canal comum, um adversário pode ser capaz de determinar que uma mensagem foi dirigida para um X-RNTI ou UE específico. Embora o adversário possa não saber a identidade desse UE fora do contexto de rádio, as informações disponíveis podem tornar possível se agregar informações sobre mensagens dirigidas ao mesmo UE em um denominado "ataque de capacidade de link". O adversário pode monitorar informações de programação não cifradas enviadas em um canal de controle e pode ser capaz de determinar transmissões de dados endereçadas ao mesmo UE. O adversário pode então rastrear potencialmente a mobilidade de UEs individuais entre células durante uma sessão de dados. Em qualquer caso, mensagens enviadas livres em um canal comum pode resultar em uma vulnerabilidade de segurança que pode levar a ameaças mais graves de segurança.

Técnicas para reduzir vulnerabilidade de segurança devido à transmissão de mensagens livres em um canal comum são descritas aqui. Essas técnicas podem ser utilizadas para várias mensagens de sinalização enviadas em várias camadas. As técnicas podem ser também utilizadas

para downlink e uplink. Para clareza, as técnicas são descritas abaixo para transmissão de informações de programação e mensagens paging no downlink em UMTS.

3GPP Release 5 e posteriores suportam HSDPA, que é um conjunto de canais e procedimentos que permitem a transmissão de dados em pacote com alta velocidade no downlink. Para HSDPA, um Nó V envia dados no HS-DSCH, que é um canal de transporte downlink que é compartilhado por todos os UEs tanto em tempo como em código. O HS-DSCH pode conter dados para um ou mais UEs em cada intervalo de tempo de transmissão (TTI). Para HSDPA, um quadro de 10 milissegundos (ms) é dividido em cinco subquadros de 2 ms, cada subquadro cobre três partições de tempo, e cada partição de tempo tem uma duração de 0,667 ms. Para HSDPA, um TTI é igual a um subquadro e é a menor unidade de tempo na qual um UE pode ser programado e servido. A partilha do HS-DSCH é dinâmica e pode alterar de TTI para TTI. Dados para o HS-DSCH são enviados em um Canal Compartilhado de Downlink Físico em Alta Velocidade (HS-PDSCH), e sinalização para o HS-PDSCH é enviada em um Canal de Controle Compartilhado para HS-DSCH (HS-SCCH).

Para HSDPA, um Nó B pode utilizar até quinze códigos de canalização de 16 chips com fator de espalhamento de 16 para o HS-PDSCH. O nó B pode utilizar também qualquer número de códigos de canalização de 128 chips com fator de espalhamento de 128 para HS-SCCH. O número de códigos de canalização de 16 chips para o HS-PDSCH e o número de códigos de canalização de 128 chips para o HS-SCCH são configuráveis. Os códigos de canalização para o HS-PDSCH e HS-SCCH são códigos de fator de espalhamento variável ortogonal (OVSF) que podem ser gerados em um modo estruturado. O fator de espalhamento (SF) é o comprimento de um código de canalização. Um

símbolo é espalhado com um código de canalização de comprimento SF para gerar chips SF para o símbolo.

Na descrição a seguir, HSDPA é considerado como tendo (a) até quinze HS-PDSCHs, com cada HS-PDSCH correspondendo a um código de canalização de 16 chips diferentes, e (b) qualquer número de HS-SCCHs, com cada HS-SCCH correspondendo a um código de canalização de 128 chips diferentes. Um UE pode ser atribuído até quatro HS-SCCHs na configuração da chamada e pode monitorar os HS-SCCHs atribuídos durante a chamada. O UE pode ser atribuído até quinze HS-PDSCHs em um dado TTI. Os HS-PDSCHs podem ser dinamicamente atribuídos e transferidos para o UE via sinalização enviada em um dos HS-SCCHs atribuídos para o UE.

A figura 2 mostra transmissões de exemplo nos HS-SCCHs e HS-PDSCHs para HSDPA. Um nó B pode servir um ou mais UEs em cada TTI. O Nó B envia uma mensagem de sinalização para cada UE programado nos HS-SCCHs e envia dados para o UE nos HS-PDSCHs duas partições depois. As mensagens de sinalização enviadas nos HS-SCCHs são endereçadas a UEs específicos com base nos H-RNTIs atribuídos a esses UEs. Cada UE que poderia receber dados nos HS-PDSCHs processa seus HS-SCCHs atribuídos em cada TTI para determinar se uma mensagem de sinalização foi enviada para aquele UE. Cada UE pode casar as mensagens de sinalização recebidas nos HS-SCCHs com seu H-RNTI para determinar se qualquer mensagem de sinalização é destinada àquele UE. Cada UE que é programado em um TTI dado pode processar os HS-PDSCHs para recuperar os dados enviados para aquele UE.

No exemplo mostrado na figura 2, um UE de interesse (UE #1) monitora quatro HS-SCCHs #1 até #4 atribuídos ao UE. UE #1 não é programado em TTI n, e

nenhuma mensagem de sinalização é enviada para UE #1 em qualquer HS-SCCHs. UE #1 é programado em TTI n + 1, e uma mensagem de sinalização é enviada para o UE em HS-SCCH #1. A mensagem de sinalização pode transferir vários parâmetros para a transmissão enviada nesse TTI. UE #1 não é programado em TTI n + 2, é programado em TTI n + 3, e receber uma mensagem de sinalização em HS-SCCH #2, e não é programado em TTI n + 4.

Outros RNTIs podem ser utilizados para outras mensagens de sinalização enviadas para UEs específicos em canais comuns. Por exemplo, mensagens de atribuição enviadas no E-AGCH são endereçadas a UEs específicos com base nas E-RNTIs atribuídas a esses UEs. Mensagens de paging são endereçadas a UEs específicos com base nos U-RNTIs atribuídas a esses UEs.

Em geral, um X-RNTI pode ser enviada em uma mensagem de sinalização transmitida no downlink e pode ser utilizada por cada UE para casar contra seu próprio X-RNTI para determinar se a mensagem de sinalização é destinada àquele UE, isto é, para determinar "essa mensagem é para mim?" Todas as informações no X-RNTI podem não ser necessárias para esse processo de casamento uma vez que o espaço possível de valores de X-RNTI não possa estar cheio. O X-RNTI pode ter 16 bits (ou 32 bits) de comprimento e pode prover identidades para muitos mais UEs do que um Nó B pode ser capaz de endereçar a qualquer momento. Por exemplo, o Nó B pode ter atribuído somente 1024 identidades na faixa de 0 a 1023. Nesse caso, somente 10 bits menos significativos (LSBs) do X-RNTI podem ser utilizados para identificar exclusivamente um dado UE. O Nó B pode enviar então valores aleatórios para os bits mais elevados e permitir que cada UE reconheça mensagens dirigidas àquele UE olhando somente os bits inferiores, que contêm a porção

"real" da identidade. O envio de valores aleatórios para os bits mais elevados pode resultar em muitos valores de X-RNTI diferentes sendo enviados para qualquer UE dado, o que pode mitigar ataque de capacidade de link. Entretanto, esse esquema de "truncamento" é essencialmente transparente. Um adversário que está ciente do esquema pode penetrar trivialmente no mesmo e examinar os bits inferiores para determinar quais mensagens são endereçadas aos mesmos UEs.

Em um aspecto, um X-RNTI pode ser transformado com base em uma função, e um RNTI transformado (em vez do X-RNTI original) pode ser enviada em uma mensagem de sinalização. Um UE que já conhece o X-RNTI pode ser capaz de determinar se a mensagem de sinalização é destinada ao UE com base no RNTI transformada. Entretanto, um adversário sem conhecimento prévio do X-RNTI pode ser incapaz de determinar a X-RNTI original com base no RNTI transformado enviado na mensagem. A transformação pode ser executada de várias maneiras.

A figura 3A mostra um projeto para transformar um X-RNTI. Uma unidade 310 recebe o X-RNTI, transforma o X-RNTI com base em uma função de transformar H, e provê um RNTI transformado que é indicado como $H(\text{X-RNTI})$. A função de transformar pode ser uma função irreversível que torna difícil determinar o X-RNTI original a partir do RNTI transformado. Por exemplo, a função de transformar pode ser uma função hash segura/criptográfica que mapeia uma mensagem (por exemplo, o X-RNTI) para uma compilação (por exemplo, o RNTI transformado) e tem propriedades criptográficas de modo que (i) a função entre a mensagem e sua compilação é irreversível e (ii) a probabilidade de duas mensagens mapeando para a mesma compilação é muito pequena. A saída da função hash pode ser mencionada como uma compilação, uma assinatura, um valor que sofreu hash,

etc.

O RNTI transformado pode ser enviado em uma mensagem de sinalização e pode permitir casamento da mensagem pelas UEs. Cada UE pode aplicar a mesma função de transformar o seu X-RNTI para obter um RNTI transformado. Cada UE pode casar então o RNTI transformado em uma mensagem recebida com o RNTI transformado localmente gerado para determinar se a mensagem é destinada para aquele UE.

O RNTI transformado pode evitar que um adversário infira o X-RNTI original. Entretanto, caso o mesmo RNTI transformado seja incluído em cada mensagem de sinalização enviada para um dado UE, então o adversário pode realizar um ataque de correlação. Para evitar isso, o RNTI transformado pode ser mudado com cada mensagem.

A figura 3B mostra um projeto para transformar um X-RNTI para obter diferentes RNTIs transformados. Uma unidade 320 recebe o X-RNTI e um valor salt σ, transforma o X-RNTI e o valor salt com base em uma função de transformar H_σ, e provê um RNTI transformado que é indicado como H_σ (X-RNTI). A função de transformar pode ser uma função irreversível, uma função hash criptográfica, etc. Um valor salt é um valor não estático que pode ser selecionado de qualquer modo. Valores salt diferentes podem ser utilizados para diferentes mensagens de sinalização de modo que um único X-RNTI possa originar RNTIs transformadas diferentes para diferentes mensagens.

Um RNTI transformado e um valor salt σ podem ser enviados em uma mensagem de sinalização e podem permitir casamento da mensagem pelos UEs. O valor salt σ pode ser enviado livre juntamente com o RNTI transformado. O valor salt σ e/ou o RNTI transformado pode ser também incorporado na mensagem de sinalização. Em qualquer caso, cada UE pode

casar seu X-RNTI contra o RNTI transformado na mensagem de sinalização. Cada UE pode aplicar a função de transformar H_σ em seu X-RNTI e o valor salt σ extraído a partir da mensagem e pode então comparar o RNTI transformado geralmente localizada com o RNTI transformado recebido na mensagem de sinalização.

A figura 4A mostra um diagrama de blocos de um projeto de um processador de mensagem 410 que envia um RNTI transformado livre em uma mensagem de sinalização. Processador de mensagem 410 recebe uma mensagem de entrada e um X-RNTI para um UE receptor e gera uma mensagem de saída dirigida ao UE.

No processador de mensagem 410, uma unidade 420 recebe um X-RNTI e possivelmente um valor salt σ, aplica uma função de transformar no X-RNTI e possivelmente o valor salt σ, e provê um RNTI transformado. Um multiplexador (Mux) 422 multiplexa o RNTI transformado, o valor salt σ (caso presente), e uma mensagem de entrada. Um encodificador 424 encodifica a saída de multiplexador 422 e provê uma mensagem de saída. Processador de mensagem 410 pode ser utilizado para mensagens de paging enviadas na PCH. Nesse caso, o ID de UE ou X-RNTI na figura 4A pode corresponder o U-RNTI.

A figura 4B mostra um diagrama de blocos de um projeto de um processador de mensagens 450 que incorpora um RNTI transformado em uma mensagem de sinalização. Processador de mensagens 450 recebe uma mensagem de entrada e um X-RNTI para um UE receptor e gera uma mensagem de saída dirigida ao UE. A mensagem de entrada pode compreender vários trechos de informações.

No processador de mensagens 450, uma unidade 460 recebe um X-RNTI e possivelmente um valor salt σ, aplica

uma função transformar no X-RNTI e possivelmente o valor salt σ, e provê um RNTI transformado. Um multiplexador 462 recebe e multiplexa informações de sinalização X_a e X_b e o valor salt σ (caso presente) e provê informações multiplexadas X_1. Um encodificador 464 encodifica as informações multiplexadas X_1 e provê informações codificadas. Uma unidade 466 mascara as informações codificadas com base no RNTI transformado e provê informações mascaradas S_1. Um multiplexador 472 recebe e multiplexa informações de sinalização X_c até X_f e provê informações multiplexadas X_2. Uma unidade 474 gera um teste de redundância cíclica (CRC) com base em informações X_1 e X_2, a seguir mascara o CRC com o RNTI transformado para obter um CRC específico de UE, e anexa o CRC específico de UE às informações X_2. Um encodificador 476 encodifica a saída da unidade 474 e provê informações codificadas R_2. Um multiplexador 478 recebe e multiplexa as informações mascaradas S_1 e as informações codificadas R_2 e provê as informações multiplexadas S_1 e R_2 como uma mensagem de saída.

Processador de mensagens 450 pode ser utilizado para mensagens de sinalização enviadas no HS-SCCHs. Nesse caso, X_a pode compreender informações de conjunto de código de canalização, X_b pode compreender informações de esquema de modulação, X_c pode compreender informações de tamanho de bloco de transporte, X_d pode compreender informações de processo HARQ, X_e pode compreender informações de versão de constelação e redundância, X_f pode compreender informações de indicador de dados novos, e o X-RNTI pode corresponder ao H-RNTI. Informações S_1 podem ser enviadas na primeira partição de um TTI, e informações R_2 podem ser enviadas nas duas últimas partições do TTI. Nesse caso, o valor salt σ

pode ser multiplexado com informações X_a e X_b enviadas na primeira partição do TTI, como mostrado na figura 4B. Isso pode permitir detecção prematura da mensagem de sinalização pelos UEs, sem ter de esperar para que a mensagem inteira seja recebida.

A figura 4A mostra um projeto no qual um RNTI transformado é enviado livre em uma mensagem de sinalização. O RNTI transformado pode ser também enviado livre de outras maneiras. A figura 4B mostra um projeto no qual um RNTI transformado é incorporado em uma mensagem de sinalização. A incorporação do RNTI transformado pode ser também obtida de outras maneiras. Por exemplo, uma mensagem de sinalização enviada no E-AGCH pode incluir um CRC específico de UE que pode ser gerado com base em um E-RNTI transformado. Em geral, um RNTI transformado pode ser enviado de várias maneiras (por exemplo, livre ou incorporado) em uma mensagem de sinalização de tal modo que um UE receptor possa identificar a mensagem como sendo dirigida àquele UE.

Como mostrado na figura 2, um UE pode receber múltiplas mensagens de sinalização (por exemplo, até quatro) em cada TTI e pode verificar cada mensagem recebida para determinar se a mensagem é destinada ao UE. A função de transformar deve ser simples de forma computacional de modo que o UE possa aplicar a função de transformar para cada mensagem recebida sem causar impacto adverso sobre o desempenho. De modo ideal, o casamento de mensagem com o RNTI transformado deve exigir somente algumas instruções adicionais além do que é normalmente feito para casar o X-RNTI.

Para o projeto mostrado na figura 3B, um UE pode armazenar uma tabela de consulta de RNTIs transformados obtidas por hashing seu X-RNTI com todos os valores salt

possíveis. Os RNTIs transformados podem ser desse modo pré-computados uma vez e armazenados para uso posterior, em vez de ser computada sempre que mensagens de sinalização forem recebidas. Para cada mensagem recebida, o UE pode extrair o valor salt a partir da mensagem recebida, recuperar o RNTI transformado para aquele valor salt a partir da tabela de consulta, e verificar a mensagem recebida com o RNTI transformado recuperado.

A UTRAN pode atribuir um novo X-RNTI para um UE via sinalização cifrada no início de uma chamada e possivelmente durante a chamada. Versões transformadas do novo X-RNTI podem ser enviadas através do ar livremente uma vez que somente o UE tem a versão que não sofreu hash. Um adversário pode não ter informações suficientes para executar casamento de mensagens de sinalização enviadas com os RNTIs transformados. O adversário pode monitorar todas as mensagens de sinalização em uma célula durante um período de tempo e correlacionar essas mensagens de sinalização por manter um banco de dados de todos os X-RNTIs possíveis e checar cada mensagem recebida contra todos os X-RNTIs. Esse tipo de espionagem determinado pode ser combatido por atribuir periodicamente novos X-RNTIs aos UEs.

Várias funções de transformar podem ser utilizadas para gerar RNTIs transformados. Em geral, uma função de transformar deve ter as seguintes qualidades:

. Computação fácil e rápida (ou sensível a uma tabela de consulta no UE);

. RNTI transformado e valor salt devem ser pequenos;

. Difícil ou impossível de reverter; e

. Fácil para o UTRAN proteger contra colisões.

Um equilíbrio pode ser feito entre as qualidades

listadas acima para um dado aplicativo. Diferentes funções de transformar com diferentes características podem ser utilizadas para diferentes aplicativos. Por exemplo, a sinalização na Camada 2 pode favorecer alta eficiência de bits e rápida decodificação e pode ser capaz de aceitar um nível de segurança mais baixo como resultado. Sinalização na Camada 3 pode favorecer segurança mais forte às custas de maior overhead.

A importância de uma função altamente irreversível pode depender do nível de determinação assumido por parte de um adversário. Uma função de transformar pode simplesmente mascarar alguns bits em posições variáveis a partir do X-RNTI e pode utilizar o valor salt para selecionar os bits mascarados. Essa função de transformar pode ser suscetível a um ataque de força bruta no qual o adversário coleta mensagens de sinalização, experimenta todos os valores possíveis para os bits deletados, e observa para ver quais dos valores resultantes são repetidos. O adversário pode presumir que os valores repetidos são os X-RNTIs reais de vários UEs e pode armazenar esses valores para teste contra futuras mensagens de sinalização. Entretanto, isso pode representar um ataque significativamente mais laborioso do que a espionagem casual normalmente associado a ataques de capacidade de link.

Mesmo se uma função de transformar for de um certo modo fraca de modo criptográfico, o UTRAN pode atribuir novos X-RNTIs via sinalização cifrada. Nesse caso, um adversário pode não ter automaticamente um grupo de X-RNTIs conhecidos para testar mensagens recebidas contra. À luz da capacidade de atribuir novos X-RNTIs, a intensidade criptográfica da função de transformar pode ser considerada menos importante do que a computação simples e conservação

de bit através do ar.

Uma função de transformar pode ser definida com base em vários projetos. Por exemplo, uma função de transformar pode incorporar princípios de projeto utilizados em funções hash seguras/criptográficas como SHA-1 (Algoritmo Hash seguro), SHA-2 (que inclui SHA-224, SHA-256, SHA-384 e SHA-512), MD-4 (Compilação de mensagens), MD-5, ou outros algoritmos hash seguros conhecidos na técnica. Em um projeto, uma função de transformar única é utilizada e conhecida *a priori* tanto pela UTRAN como pelos UEs. Em outro projeto, um conjunto de funções de transformar é suportado, e uma função de transformar pode ser selecionada a partir do conjunto, por exemplo, no início de uma chamada, e transferido para um UE.

O comprimento do valor salt σ pode ser selecionado com base em um equilíbrio entre overhead e segurança. Um valor salt mais longo pode resultar em mais RNTIs transformados para um dado X-RNTI, que pode melhorar a segurança às custas de overhead maior e possivelmente maior probabilidade de colisão. O inverso pode ser verdadeiro para um valor salt mais curto.

Em um projeto, um RNTI transformado tem o comprimento igual ou aproximadamente igual ao do X-RNTI original. Para esse projeto, o valor salt σ pode ser enviado utilizando bits adicionais. Em outro projeto, o RNTI transformado e o valor salt σ têm comprimento igual ou aproximadamente igual ao do X-RNTI original para manter overhead igual ou aproximadamente igual. Para esse projeto, alguns bits podem ser "recuperados" fazendo o RNTI transformado mais curto do que o X-RNTI original. Por exemplo, o X-RNTI pode ser 16 bits, o RNTI transformado pode ser 10 bits, e o valor salt pode ser 6 bits. O X-RNTI,

RNTI transformado, e valor salt podem ter também outros comprimentos. A função de transformar pode ser projetada para obter as propriedades criptográficas desejadas com o RNTI transformado mais curto.

Uma colisão ocorre quando dois X-RNTIs para dois UEs são transformados no mesmo RNTI transformado, por exemplo, $H_\sigma(x) = H_\sigma(y)$, onde x e y são as dois X-RNTIs. Os dois UEs podem não ter modo para resolver a colisão entre seus RNTIs transformados. O RNTI transformado pode ser utilizado para enviar informações de programação para um dos dois UEs, por exemplo, como mostrado na figura 2. O UE receptor pode detectar adequadamente as informações de programação como sendo para aquele UE e pode decodificar os dados enviados para o UE. O UE não-receptor pode detectar falsamente as informações de programação, decodificar os dados destinados para o UE receptor, e obter resultado sem sentido após decriptografia (considerando que os dados enviados no HS-DSCH foram criptografados). Nesse caso, colisões podem ou não causar impacto adverso sobre o desempenho, dependendo do comportamento da aplicação.

Em geral, o impacto devido a colisões de X-RNTIs pode ser dependente do tipo de sinalização sendo enviada com esses X-RNTIs. O UTRAN pode tentar evitar colisões para evitar possíveis efeitos adversos.

Em um projeto para evitar colisões, o UTRAN seleciona X-RNTIs e valores salt conhecidos como não tendo colisões. A UTRAN pode manter um conjunto de todos os X-RNTIs atribuídos ou atribuíveis aos UEs. Para cada valor salt possível σ, o UTRAN pode gerar um conjunto de RNTIs transformados com base no conjunto de X-RNTIs e aquele valor salt. O UTRAN pode varrer o conjunto transformado para duplicatas e pode rejeitar esse valor salt caso

duplicatas sejam detectadas. Em geral, um valor salt que causa uma colisão para certos X-RNTIs pode ser ainda utilizado para outros X-RNTIs. Entretanto, para simplificar implementação, a UTRAN pode manter uma lista de valores salt que resultam em nenhuma duplicata sobre todo o conjunto de X-RNTIs. Os valores salt nessa lista podem ser selecionados para uso. Colisões também podem ser evitadas de outras maneiras.

A figura 5 mostra um processo 500 realizado por uma entidade de rede em uma rede de comunicação sem fio para enviar mensagens de sinalização para os UEs. A entidade de rede pode ser um Nó B, um RNC, etc., dependendo das mensagens de sinalização sendo enviadas.

Um primeiro ID atribuído a um UE pode ser transformado para obter um segundo ID para o UE (bloco 512). O primeiro ID pode ser um RNTI atribuído ao UE em UMTS ou algum outro tipo de ID em algum outro sistema de comunicação. O primeiro ID pode ser transformado com base em uma função irreversível, uma função hash, ou alguma outra função para obter o segundo ID. Uma mensagem de saída dirigida ao UE pode ser gerada com base em uma mensagem de entrada e o segundo ID (bloco 514). A mensagem de entrada pode ser uma mensagem de paging, uma mensagem de programação carregando informações de programação, uma mensagem de atribuição de recursos, etc. A mensagem de saída pode ser enviada através de um canal comum compartilhado pelo UE e outros UEs (bloco 516).

Em um projeto, o primeiro ID e um valor salt sofreram hash para obter o segundo ID. O valor salt pode ser enviado livre na mensagem de saída. O valor salt pode ser alterado cada vez que o primeiro ID é transformado e pode ser selecionado para evitar colisões entre todos os primeiros IDs atribuídos aos UEs. O primeiro ID pode ter um

comprimento que pode ser igual ao comprimento combinado do segundo ID e o valor salt.

Em um projeto, a mensagem de saída pode incluir a mensagem de entrada e o segundo ID livre, por exemplo, como mostrado na figura 4A. Em outro projeto, o segundo ID pode ser incorporado na mensagem de saída, por exemplo, como mostrado na figura 4B. Por exemplo, toda ou uma porção da mensagem de entrada pode ser mascarada com o segundo ID para gerar a mensagem de saída. Alternativamente, um CRC específico de UE pode ser gerado com base na mensagem de entrada e o segundo ID, e a mensagem de saída pode ser gerada com base na mensagem de entrada e o CRC específico de UE.

A figura 6 mostra um aparelho 600 para enviar mensagens de sinalização para os UEs. Aparelho 600 inclui elemento para transformar um primeiro ID atribuído a um UE para obter um segundo ID para o UE (módulo 612), elemento para gerar uma mensagem de saída dirigida ao UE com base em uma mensagem de entrada e o segundo ID (módulo 614), e elemento para enviar a mensagem de saída via um canal comum compartilhado pelo UE e outros UEs (módulo 616). Os módulos 612 a 616 podem compreender processadores, dispositivos eletrônicos, dispositivos de hardware, componentes eletrônicos, circuitos lógicos, memórias, etc., ou qualquer combinação dos mesmos.

A figura 7 mostra um processo 700 realizado por um UE para receber mensagens de sinalização a partir de uma rede de comunicação sem fio. Uma mensagem pode ser recebida via um canal comum compartilhado por uma pluralidade de UEs (bloco 712). Um primeiro ID atribuído ao UE pode ser transformado para obter um segundo ID para o UE (bloco 714). A transformação pode ser alcançada com uma tabela de consulta, hardware, software, firmware, etc. Em um projeto,

um valor salt pode ser obtido a partir da mensagem recebida, e o primeiro ID e o valor salt podem sofrer hash para obter o segundo ID. O fato de se a mensagem recebida é destinada para o UE pode ser determinado com base no segundo ID (bloco 716). Em um projeto de bloco 716, um terceiro ID pode ser obtido a partir da mensagem recebida e comparado com o segundo ID para determinar se a mensagem recebida é destinada ao UE. Em outro projeto de bloco 716, um CRC pode ser gerado com base na mensagem recebida e o segundo ID, um CRC específico de UE pode ser obtido a partir da mensagem recebida, e o CRC gerado pode ser comparado com o CRC específico de UE para determinar se a mensagem recebida é destinada ao UE. A mensagem recebida pode ser uma mensagem de paging, uma mensagem de programação, uma mensagem de atribuição de recursos, etc. Caso a mensagem recebida seja uma mensagem de programação, então informações de programação podem ser obtidas a partir da mensagem recebida e utilizadas para processar uma transmissão de dados enviada para o UE.

A figura 8 mostra um aparelho 800 para receber mensagens de sinalização. Aparelho 800 inclui elemento para receber uma mensagem via um canal comum compartilhado por uma pluralidade de UEs (módulo 812), elemento para transformar um primeiro ID atribuído a um UE para obter um segundo ID para o UE (módulo 814), e elemento para determinar se a mensagem recebida é destinada para o UE com base no segundo ID (módulo 816). Módulos 812 a 816 podem compreender processadores, dispositivos eletrônicos, dispositivos de hardware, componentes eletrônicos, circuitos lógicos, memórias, etc., ou qualquer combinação dos mesmos.

A figura 9 mostra um diagrama de blocos de um projeto de UE 120, Nó B 110, e RNC 130 na figura 1. No

uplink, dados e sinalização a serem enviados por UE 120 são processados (por exemplo, formatados, encodificados e intercalados) por um encodificador 922 e adicionalmente processados (por exemplo, modulados, canalizados e embaralhados) por um modulador (MOD) 924 para gerar chips de saída. Um transmissor (TMTR) 932 então condiciona (por exemplo, converte em analógico, filtra, amplifica, e converte ascendentemente em freqüência) os chips de saída e gera um sinal uplink, que é transmitido via uma antena 934. No downlink, a antena 934 recebe um sinal downlink transmitido por Nó B 110. Um receptor (RCVR) 936 condiciona (Por exemplo, filtra, amplifica, converte descendentemente em freqüência e digitaliza) o sinal recebido a partir da antena 934 e provê amostras. Um demodulador (DEMOD) 926 processa (por exemplo, desembaralha, canaliza e demodula) as amostras e provê estimativas de símbolos. Um decodificador 928 processa adicionalmente (por exemplo, deintercala e decodifica) as estimativas de símbolos e provê dados decodificados. Encodificador 922, modulador 924, demodulador 926, e decodificador 928 podem ser implementados por um processador de modem 920. Essas unidades podem realizar processamento de acordo com a tecnologia de rádio (por exemplo, UMTS) implementada pela rede de comunicação sem fio.

Um controlador/processador 940 orienta a operação no UE 120. Controlador/processador 940 pode realizar o processo 700 na figura 7 e/ou outros processos para as técnicas descritas aqui. Uma memória 942 armazena códigos de programa e dados para UE 120 e também pode armazenar IDs temporários atribuídos ao UE 120, ou IDs de UE.

A figura 9 também mostra um projeto de Nó B 110 e RNC 130. Nó B 110 inclui um controlador/processador 950 que realiza várias funções para comunicação com os UEs, uma

memória 952 que armazena códigos de programa e dados para Nó B 110, e um transceptor 954 que suporta comunicação de rádio com os UEs. Controlador/processador 950 pode realizar o processo 500 na figura 5 e/ou outros processos para as técnicas descritas aqui. Memória 952 pode armazenar IDs temporários atribuídos aos UEs por Nó B 110, ou NB UE IDs. RNC 130 inclui um controlador/processador 960 que realiza várias funções para suportar comunicação para os UEs e uma memória 962 que armazena códigos de programa e dados para RNC 130. Controlador/processador 960 pode realizar processo 500 na figura 5 e/ou outros processos para as técnicas descritas aqui. Memória 962 pode armazenar IDs temporários atribuídos aos UEs servidos pelo RNC 130, ou RNC UE IDs.

As técnicas descritas aqui podem ser utilizadas para mensagens de sinalização enviadas no downlink bem como no uplink. As técnicas também podem ser utilizadas para mensagens enviadas via um plano de controle bem como um plano de usuário. Um plano de controle é um mecanismo para portar sinalização para aplicativos de camada mais alta e é tipicamente implementado com protocolos específicos de rede, interfaces e mensagens de sinalização. Um plano de usuário é um mecanismo que porta sinalização para aplicativos de camada mais alta e é tipicamente implementado com protocolos abertos como Protocolo de Datagrama de Usuário (UDP), Protocolo de Controle de Transmissão (TCP), e Protocolo de Internet (IP). Mensagens podem ser portadas como parte de sinalização em um plano de controle como parte de dados (a partir de uma perspectiva de rede) em um plano de usuário.

As técnicas descritas aqui podem ser implementadas por vários elementos. Por exemplo, essas técnicas podem ser implementadas em hardware, firmware, software ou uma combinação dos mesmos. Para uma

implementação de hardware, as unidades de processamento utilizadas para realizar as técnicas em uma dada entidade (por exemplo, um UE, um Nó B, um RNC, etc.) podem ser implementadas dentro de um ou mais circuitos integrados específicos de aplicação (ASICs), processadores de sinal digital (DSPs), dispositivos de processamento de sinal digital (DSPDs), dispositivos de lógica programável (PLDs), arranjos de porta programável em campo (FPGAs), processadores, controladores, microcontroladores, microprocessadores, dispositivos eletrônicos, outras unidades eletrônicas projetadas para realizar as funções descritas aqui, um computador, ou uma combinação dos mesmos.

Para uma implementação de firmware e/ou software, as técnicas podem ser implementadas com módulos (por exemplo, procedimentos, funções, etc.) que realizam as funções descritas aqui. Os códigos de firmware e/ou software podem ser armazenados em uma memória (por exemplo, memória 942, 952 ou 962 na figura 9) e executados por um processador (por exemplo, processador 940, 950 ou 960). A memória pode ser implementada dentro do processador ou externamente ao processador.

A descrição anterior da revelação é provida para permitir que qualquer pessoa versada na técnica faça ou utilize a descrição. Várias modificações na descrição serão prontamente evidentes para aqueles versados na técnica, e os princípios gerais definidos acima podem ser aplicados a outras variações sem se afastar do espírito ou escopo da descrição. Desse modo, a descrição não pretende ser limitada aos exemplos descritos aqui, porém deve estar de acordo com o escopo mais amplo compatível com os princípios e características novas aqui revelados.

REIVINDICAÇÕES

1. Um aparelho compreendendo:

um processador configurado para transformar um primeiro identificador (ID) atribuído a um equipamento de usuário (UE) para obter um segundo ID para o UE, gerar uma mensagem de saída dirigida ao UE com base em uma mensagem de entrada e o segundo ID, e enviar a mensagem de saída via um canal comum compartilhado pelo UE e outros UEs; e

uma memória acoplada ao processador.

2. O aparelho, de acordo com a reivindicação 1, em que o processador é configurado para transformar o primeiro ID com base em uma função irreversível para obter o segundo ID.

3. O aparelho, de acordo com a reivindicação 1, em que o processador é configurado para hash o primeiro ID para obter o segundo ID.

4. O aparelho, de acordo com a reivindicação 1, em que o processador é configurado para hash o primeiro ID e um valor salt para obter o segundo ID.

5. O aparelho, de acordo com a reivindicação 4, em que o processador é configurado para enviar o valor salt na mensagem de saída.

6. O aparelho, de acordo com a reivindicação 4, em que o processador é configurado para alterar o valor salt cada vez que o primeiro ID é transformado.

7. O aparelho, de acordo com a reivindicação 4, em que o primeiro ID tem um comprimento igual a um comprimento combinado do segundo ID e o valor salt.

8. O aparelho, de acordo com a reivindicação 4, em que o processador é configurado para selecionar o valor salt para evitar colisões entre uma pluralidade de primeiros IDs atribuídos a UEs ativos.

9. O aparelho, de acordo com a reivindicação 1, em que o processador é configurado para gerar a mensagem de saída para incluir a mensagem de entrada e o segundo ID livre.

10. O aparelho, de acordo com a reivindicação 1, em que o processador é configurado para mascarar pelo menos uma porção da mensagem de entrada com o segundo ID para gerar a mensagem de saída.

11. O aparelho, de acordo com a reivindicação 1, em que o processador é configurado para gerar um teste de redundância cíclica (CRC) específico de UE com base na mensagem de entrada e o segundo ID, e gerar a mensagem de saída com base na mensagem de entrada e o CRC específico de UE.

12. O aparelho, de acordo com a reivindicação 1, em que a mensagem de entrada é uma mensagem de paging, uma mensagem de programação ou uma mensagem de atribuição de recursos.

13. O aparelho, de acordo com a reivindicação 1, em que o primeiro ID é um Identificador Temporário de Rede Rádio (RNTI) atribuído ao UE em Sistema de Telecomunicação Móvel universal (UMTS).

14. Um método compreendendo:

transformar um primeiro identificador (ID) atribuído a um equipamento de usuário (UE) para obter um segundo ID para o UE;

gerar uma mensagem de saída dirigida para o UE com base em uma mensagem de entrada e o segundo ID; e

enviar a mensagem de saída via um canal comum compartilhado pelo UE e outros UEs.

15. O método, de acordo com a reivindicação 14, em que a transformação do primeiro ID compreende hashing o primeiro ID e um valor salt para obter o segundo ID.

16. O método, de acordo com a reivindicação 14, em que a geração da mensagem de saída compreende

gerar a mensagem de saída para incluir a mensagem de entrada e o segundo ID livre.

17. O método, de acordo com a reivindicação 14, em que a geração de mensagem de saída compreende

gerar um teste de redundância cíclica (CRC) específico de UE com base na mensagem de entrada e o segundo ID, e

gerar a mensagem de saída com base na mensagem de entrada e o CRC específico de UE.

18. Um aparelho compreendendo:

elemento para transformar um primeiro identificador (ID) atribuído a um equipamento de usuário (UE) para obter um segundo ID para o UE;

elemento para gerar uma mensagem de saída dirigida ao UE com base em uma mensagem de entrada e o segundo ID; e

elemento para enviar a mensagem de saída via um canal comum compartilhado pelo UE e outros UEs.

19. O aparelho, de acordo com a reivindicação 18, em que o elemento para transformar o primeiro ID compreende

elemento para efetuar hash o primeiro ID e um valor salt para obter o segundo ID.

20. O aparelho, de acordo com a reivindicação 18, em que o elemento para gerar a mensagem de saída compreende

elemento para gerar a mensagem de saída para incluir a mensagem de entrada e o segundo ID livre.

21. O aparelho, de acordo com a reivindicação 18, em que o elemento para gerar a mensagem de saída compreende

elemento para gerar um teste de redundância cíclica (CRC) específico de UE com base na mensagem de entrada e o segundo ID, e

elemento para gerar a mensagem de saída com base na mensagem de entrada e o CRC específico de UE.

22. Meio legível por computador incluindo instruções armazenadas no mesmo, compreendendo:

um primeiro conjunto de instruções para transformar um primeiro identificador (ID) atribuído a um equipamento de usuário (UE) para obter um segundo ID para o UE.

um segundo conjunto de instruções para gerar uma mensagem de saída dirigida ao UE com base em uma mensagem de entrada e o segundo ID; e

um terceiro conjunto de instruções para enviar a mensagem de saída via um canal comum compartilhado pelo UE e outros UEs.

23. Um aparelho, compreendendo:

um processador configurado para receber uma mensagem via um canal comum compartilhado por uma pluralidade de equipamentos de usuário (UEs), transformar um primeiro identificador (ID) atribuído a um UE para obter um segundo ID para o UE, e determinar se a mensagem recebida é destinada ao UE com base no segundo ID; e

uma memória acoplada ao processador.

24. O aparelho, de acordo com a reivindicação 23, em que o processador é configurado para obter um valor salt a partir da mensagem recebida e efetuar hash do primeiro ID e o valor salt para obter o segundo ID.

25. O aparelho, de acordo com a reivindicação 23, em que o processador é configurado para obter um terceiro ID a partir da mensagem recebida e comparar o segundo ID com o terceiro ID para determinar se a mensagem recebida é destinada ao UE.

26. Aparelho, de acordo com a reivindicação 23, em que o processador é configurado para gerar um teste de

redundância cíclica (CRC) com base na mensagem recebida e o segundo ID, obter um CRC específico de UE a partir da mensagem recebida, e comparar o CRC gerado com o CRC específico de UE para determinar se a mensagem recebida é destinada ao UE.

27. Aparelho, de acordo com a reivindicação 23, em que o processador é configurado para determinar que a mensagem recebida é destinada ao UE, obter informações de programação a partir da mensagem recebida, e processar uma transmissão de dados com base nas informações de programação.

28. O aparelho, de acordo com a reivindicação 23, em que a mensagem recebida é uma mensagem de paging, uma mensagem de programação, ou uma mensagem de atribuição de recursos destinada ao UE.

29. Um método compreendendo:

receber uma mensagem via um canal comum compartilhado por uma pluralidade de equipamentos de usuário (UEs);

transformar um primeiro identificador (ID) atribuído a um UE para obter um segundo ID para o UE; e

determinar se a mensagem recebida é destinada ao UE com base no segundo ID.

30. O método, de acordo com a reivindicação 29, em que a transformação do primeiro ID compreende

obter um valor salt a partir da mensagem recebida, e

efetuar hash do primeiro ID e o valor salt para obter o segundo ID.

31. O método, de acordo com a reivindicação 29, em que a determinação de se a mensagem recebida é destinada ao UE compreende

obter um terceiro ID a partir da mensagem

recebida, e

comparar o segundo ID com o terceiro ID para determinar se a mensagem recebida é destinada ao UE.

32. O método, de acordo com a reivindicação 29, em que a determinação de se a mensagem recebida é destinada ao UE compreende

gerar um teste de redundância cíclica (CRC) com base na mensagem recebida e o segundo ID,

obter um CRC específico de UE a partir da mensagem recebida, e

comparar o CRC gerado com o CRC específico de UE para determinar se a mensagem recebida é destinada ao UE.

33. Um aparelho compreendendo:

elemento para receber uma mensagem via um canal comum compartilhado por uma pluralidade de equipamentos de usuário (UEs);

elemento para transformar um primeiro identificador (ID) atribuído a um UE para obter um segundo ID para o UE; e

elemento para determinar se a mensagem recebida é destinada ao UE com base no segundo ID.

34. O aparelho, de acordo com a reivindicação 33, em que o elemento para transformação do primeiro ID compreende

elemento para obter um valor salt a partir da mensagem recebida, e

elemento para efetuar hash o primeiro ID e o valor salt para obter o segundo ID.

35. O aparelho, de acordo com a reivindicação 33, em que o elemento para determinação de se a mensagem recebida é destinada ao UE compreende

elemento para obter um terceiro ID a partir da mensagem recebida, e

elemento para comparar o segundo ID com o terceiro ID para determinar se a mensagem recebida é destinada ao UE.

36. O aparelho, de acordo com a reivindicação 33, em que o elemento para determinação de se a mensagem recebida é destinada ao UE compreende

elemento para gerar um teste de redundância cíclica (CRC) com base na mensagem recebida e o segundo ID,

elemento para obter um CRC específico de UE a partir da mensagem recebida, e

elemento para comparar o CRC gerado com o CRC específico de UE para determinar se a mensagem recebida é destinada ao UE.

37. Meio legível por computador incluindo instruções armazenadas no mesmo, compreendendo:

um primeiro conjunto de instruções para receber uma mensagem através de um canal comum compartilhado por uma pluralidade de equipamentos de usuário (UEs);.

um segundo conjunto de instruções para transformar um primeiro identificador (ID) atribuído a um UE para obter um segundo ID para o UE; e

um terceiro conjunto de instruções para determinar se a mensagem recebida é destinada ao UE com base no segundo ID.

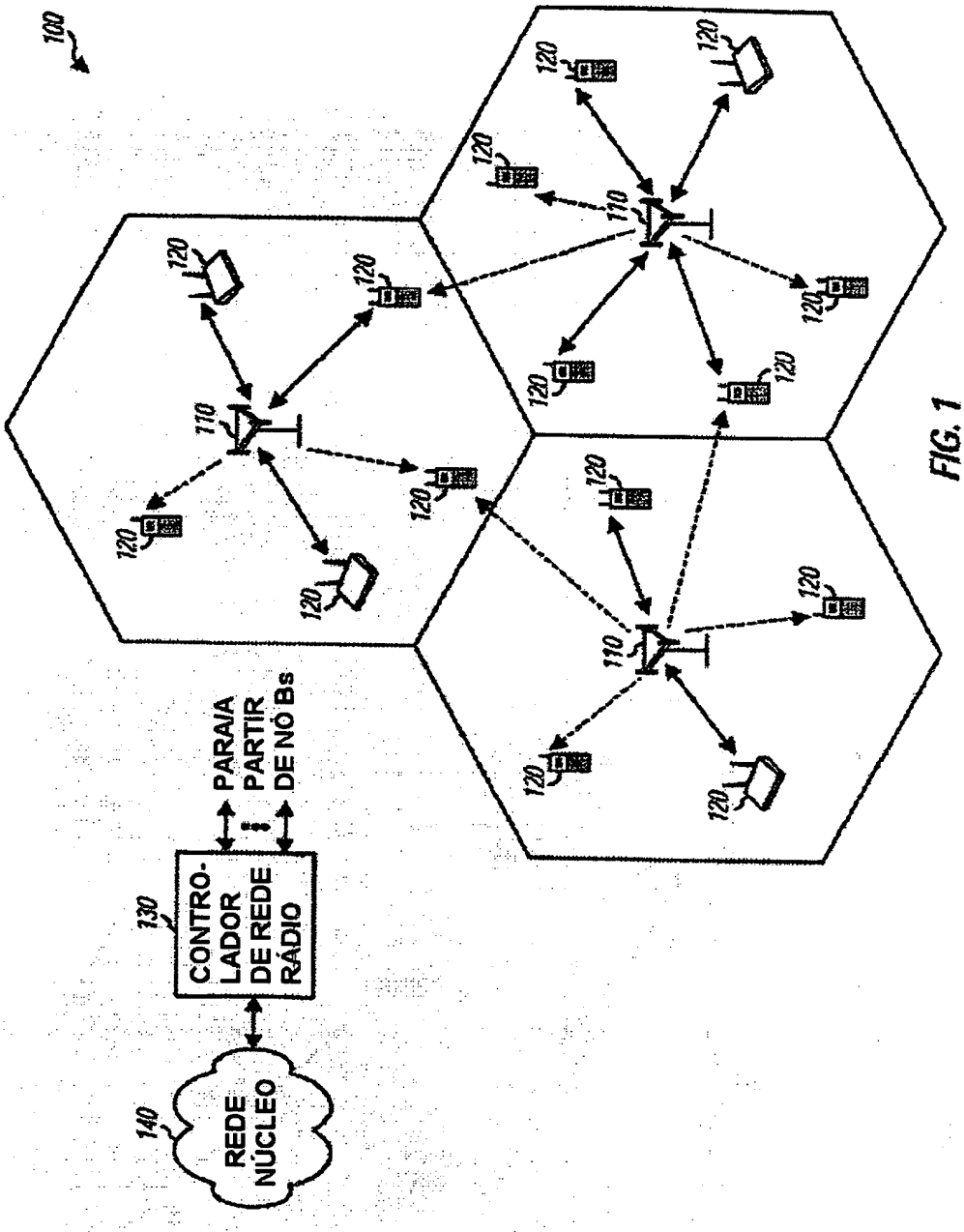

100
110
120
130
140
CONTRO-LADOR DE REDE RÁDIO
PARA/A PARTIR DE NÓ Bs
REDE NÚCLEO

FIG. 1

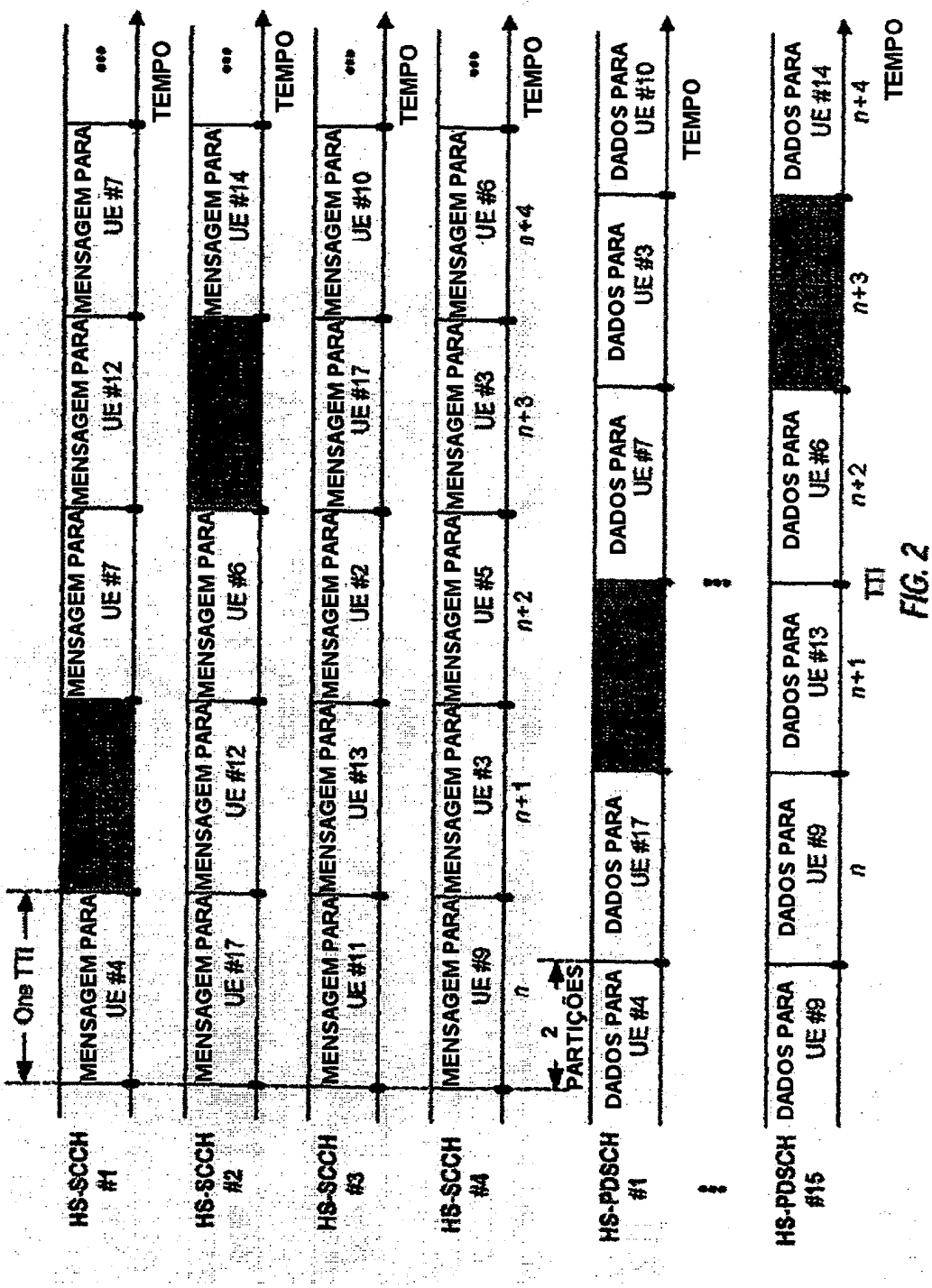

HS-SCCH #1
HS-SCCH #2
HS-SCCH #3
HS-SCCH #4
HS-PDSCH #1
HS-PDSCH #15
MENSAGEM PARA UE #4
MENSAGEM PARA UE #7
MENSAGEM PARA UE #12
MENSAGEM PARA UE #17
MENSAGEM PARA UE #6
MENSAGEM PARA UE #14
MENSAGEM PARA UE #11
MENSAGEM PARA UE #13
MENSAGEM PARA UE #2
MENSAGEM PARA UE #10
MENSAGEM PARA UE #9
MENSAGEM PARA UE #3
MENSAGEM PARA UE #5
MENSAGEM PARA UE #6
DADOS PARA UE #4
DADOS PARA UE #17
DADOS PARA UE #7
DADOS PARA UE #3
DADOS PARA UE #10
DADOS PARA UE #9
DADOS PARA UE #13
DADOS PARA UE #6
DADOS PARA UE #14
One TTI
2 PARTIÇÕES
n
n+1
n+2
n+3
n+4
TEMPO
TTI

FIG. 2

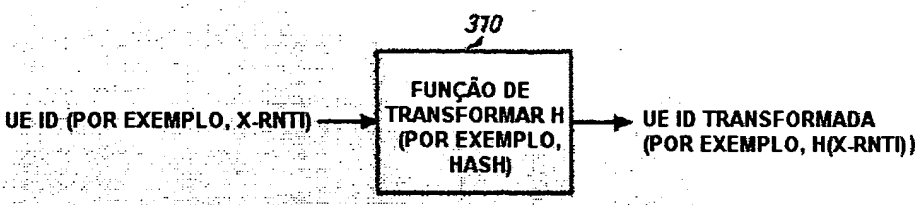


FIG. 3A

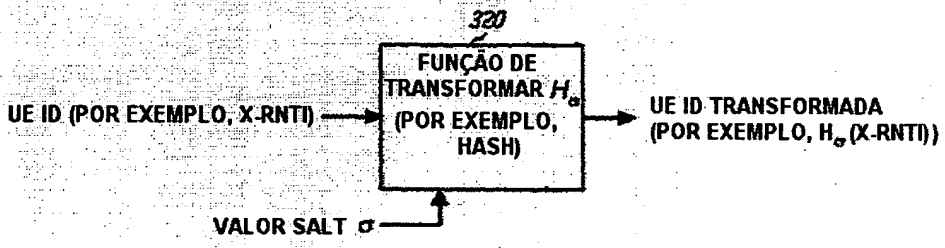


FIG. 3B

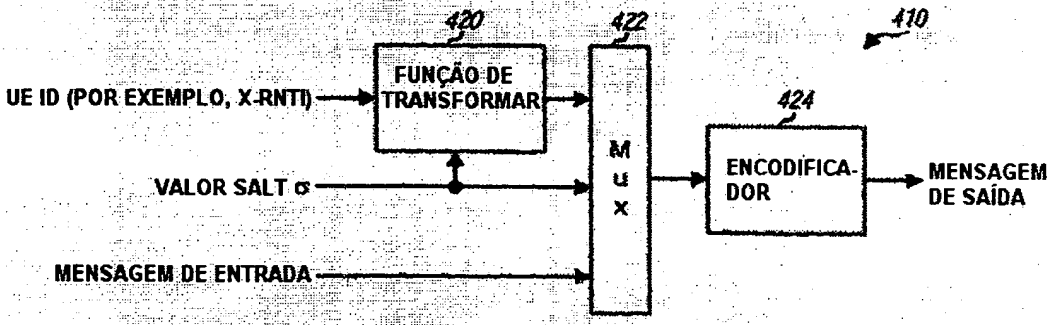


FIG. 4A

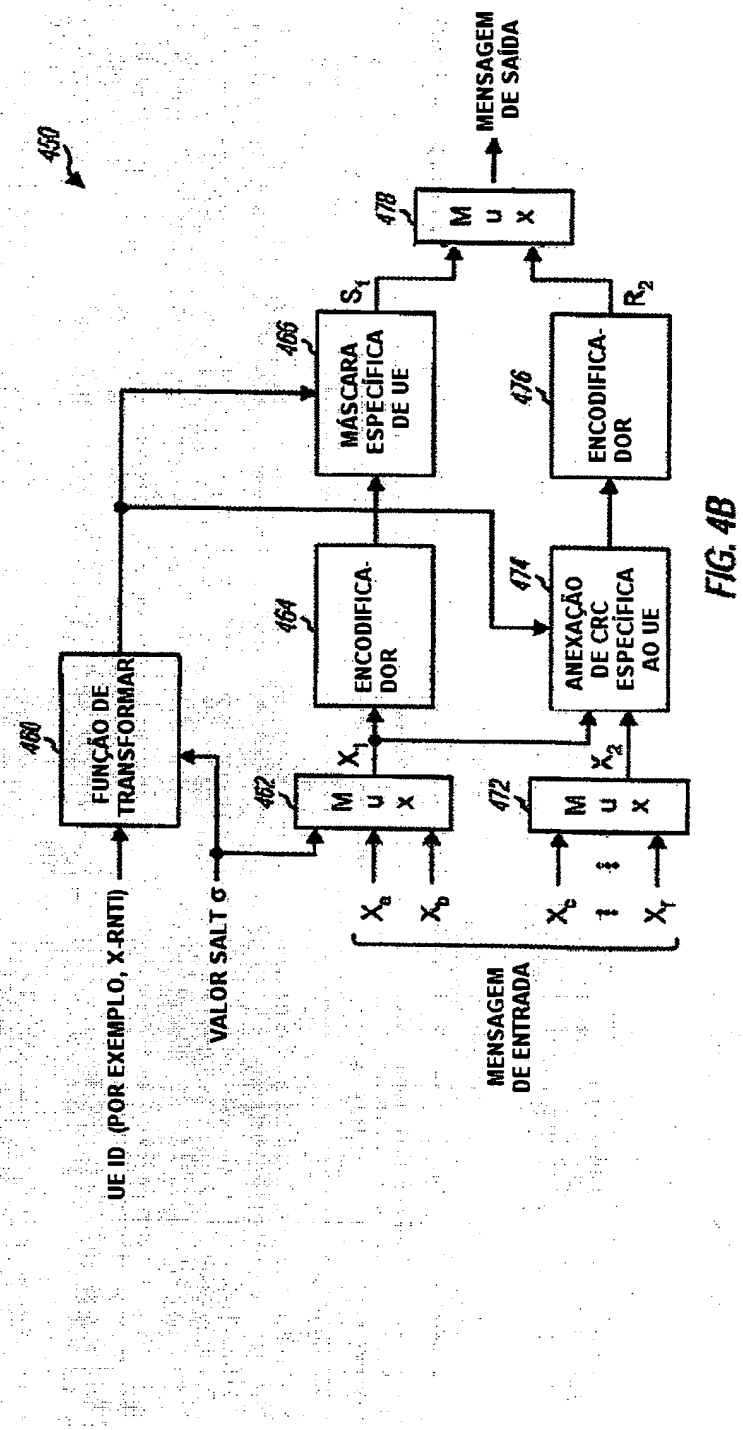

450
480
FUNÇÃO DE TRANSFORMAR
UE ID (POR EXEMPLO, X-RNTI)
VALOR SALT σ
462
M u x
464
ENCODIFICA-DOR
466
MÁSCARA ESPECÍFICA DE UE
472
M u x
474
ANEXAÇÃO DE CRC ESPECÍFICA AO UE
476
ENCODIFICA-DOR
478
M u x
MENSAGEM DE ENTRADA
MENSAGEM DE SAÍDA

FIG. 4B

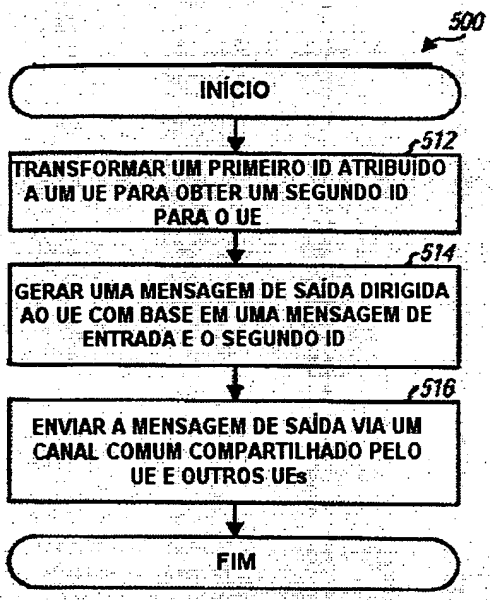


FIG. 5

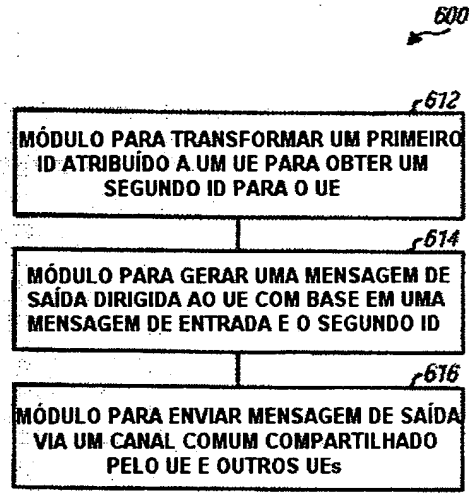


FIG. 6

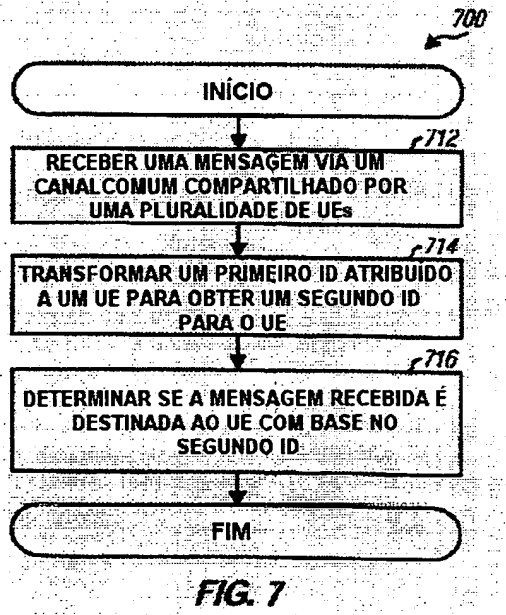


FIG. 7

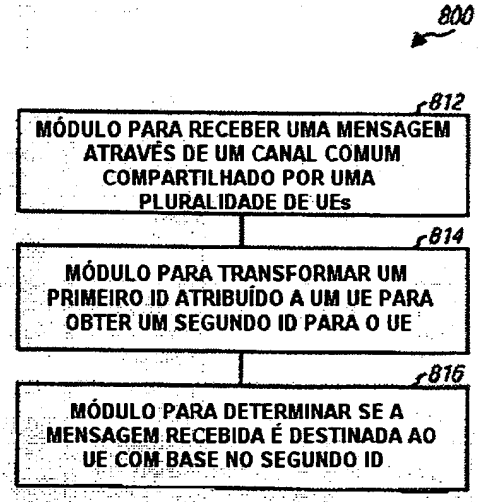


FIG. 8

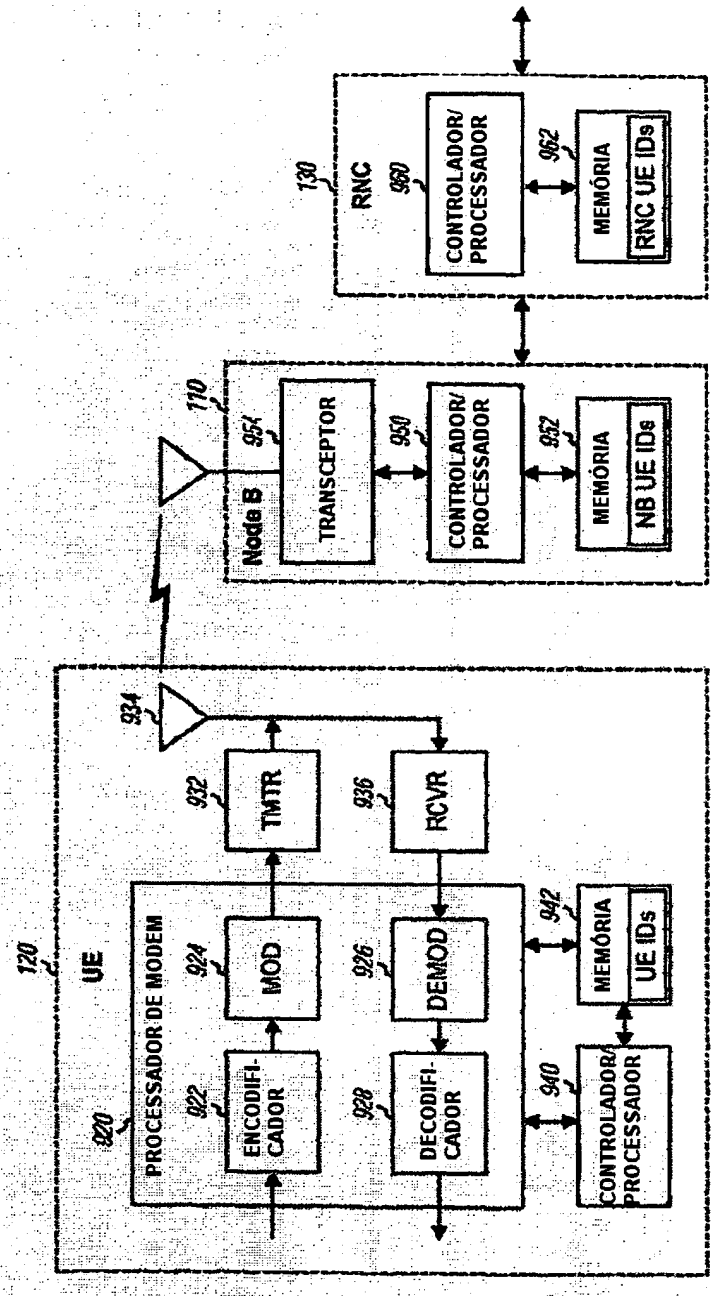

130
RNC
960
CONTROLADOR/ PROCESSADOR
962
MEMÓRIA
RNC UE IDs
110
Node B
954
TRANSCEPTOR
950
CONTROLADOR/ PROCESSADOR
952
MEMÓRIA
NB UE IDs
120
UE
934
932
TMTR
936
RCVR
920
PROCESSADOR DE MODEM
922
ENCODIFI-CADOR
924
MOD
926
DEMOD
928
DECODIFI-CADOR
940
CONTROLADOR/ PROCESSADOR
942
MEMÓRIA
UE IDs

FIG. 9

PI0707583-9

RESUMO

"OBSCURECIMENTO DE IDENTIDADES TEMPORÁRIAS DE EQUIPAMENTO DE USUÁRIO"

São descritas técnicas para ocultar identificadores temporários (IDs) atribuídos a equipamentos de usuário (UEs) por um sistema de comunicação sem fio. Em uma entidade de rede, um primeiro ID atribuído a um UE e possivelmente um valor salt são transformados, por exemplo, com base em uma função hash, para obter um segundo ID para o UE. Uma mensagem de saída dirigida ao UE é gerada com base em uma mensagem de entrada, o segundo ID e o valor salt (caso presente). A mensagem de saída é enviada via um canal comum compartilhado pelo UE e outros UEs. No UE, uma mensagem é recebida via o canal comum, e um valor salt (caso enviado) é obtida a partir da mensagem recebida. O primeiro ID e o valor salt são transformados para obter o segundo ID, que é utilizado para determinar se a mensagem recebida é destinada ao UE.