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

(21) **PI 0714096-7 A2**

BRPI0714096A2

(22) Data de Depósito: 26/07/2007
(43) Data da Publicação: 02/01/2013
(RPI 2191)

(51) Int.Cl.:
H04L 29/06

(54) Título: MÉTODO DE ACESSO CONDICIONAL LOCAL EM UM DISPOSITIVO MÓVEL

(30) Prioridade Unionista: 02/08/2006 EP 061183455

(73) Titular(es): Nagravision S.A

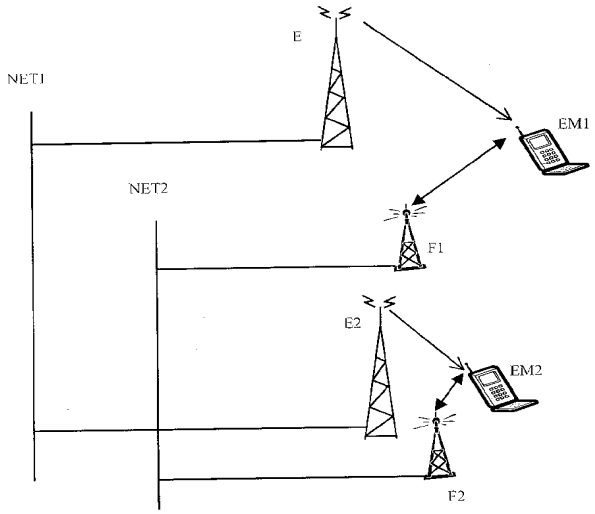
(72) Inventor(es): Guy Moreillon

(74) Procurador(es): Marcas Marcantes e Patentes Ltda

(86) Pedido Internacional: PCT EP2007057717 de 26/07/2007

(87) Publicação Internacional: WO 2008/015155de 07/02/2008

(57) Resumo: Oobjeto da presente invenção é o de possuir no mundo móvel os mesmos meios de restrição aplicados a receptores fixos. Este objeto é atingido utilizando um método de acesso condicional a um fluxo de dados digital criptografado com pelo menos uma palavra controle e emitido por meio de um transmissor em uma rede de transmissão para pelo menos um dispositivo móvel, em que o mencionado transmissor também emite um fluxo de mensagens de controle que contém as palavras controle e as condições de acesso e o mencionado dispositivo móvel de comumcação móvel por meio de um ponto de acesso móvel, em que o mencionado método é caracterizado pelo fato de que compreende as etapas a seguir: - recebimento do fluxo de mensagens de controle pelo dispositivo móvel;- determinação de um identificador de local para o mencionado dispositivo móvel, seja pelo identificador do ponto de acesso móvel ou pelo identificador do transmissor de rede de transmissão;- verificação das condições de acesso contidas na mensagem de controle, em que as mencionadas condições de acesso compreendem uma condição de recepção relativa a pelo menos um identificador de ponto de acesso móvel e/ou um identificador de um transmissor de rede de transmissão;- comparação do identificador determinado com o(s) identificador(es) contido(s) nas condições de acesso;- autorização ou bloqueio do acesso ao mencionado fluxo de dados, dependendo do resultado da mencionada comparação.



MÉTODO DE ACESSO CONDICIONAL LOCAL EM UM DISPOSITIVO MÓVEL

Campo da Técnica

A presente invenção refere-se ao campo de acesso condicional a um fluxo de dados digital transmitido por meio de link de rádio e recebido por uma série de dispositivos móveis, tais como telefone móvel, assistente digital pessoal PDA (Assistente Digital Pessoal), receptor de televisão digital portátil ou computador portátil.

Os dados transmitidos são criptografados e podem ser recebidos claramente apenas por dispositivos autorizados, cujos usuários tenham adquirido os direitos necessários. Estes direitos, armazenados em um módulo de segurança associado ao dispositivo móvel, consistem de um conjunto de teclas que permitem a decifração de palavras controle contidas em mensagens de controle ECM (Mensagem de Controle de Direitos) transmitidas no fluxo de dados de áudio e vídeo.

Um módulo de segurança é um dispositivo à prova de adulteração bem conhecido que contém várias chaves de criptografia e decifração, informações utilizadas para identificar um usuário em uma rede e dados que definem os direitos adquiridos pelo usuário para o recebimento de conteúdo transmitido. O módulo de segurança pode existir em diferentes formas, tais como um cartão inteligente removível inserido em um leitor, um circuito integrado soldado sobre uma placa-mãe, um cartão de memória (SD ou MMC) no qual é embutido um chip de segurança ou uma placa do tipo SIM (Módulo de Identidade de Assinante) que pode ser encontrada na maior parte dos dispositivos portáteis.

Este módulo pode ser realizado na forma de software e pode ser parte do software de dispositivo móvel. Preferencialmente, este software será conduzido em uma zona específica da memória, a fim de minimizar a interferência com outros softwares.

Antecedentes da Técnica

Atualmente, dispositivos móveis configurados para o recebimento de programas de

televisão digital baseiam-se em tecnologias padrão, tais como OMA (Aliança Móvel Aberta), DVB-H (Transmissão de Vídeo Digital, Manual) ou DMB (Transmissão Multimídia Digital), que é, de certa forma, uma extensão de banda larga de DAB (Transmissão de Áudio Digital).

A tecnologia OMA implementa uma única solução completa para um dado mercado, tal como o mercado de telefones portáteis, em que todos os dispositivos e provedores de conteúdo implementam a tecnologia OMA.

A tecnologia DVB foi projetada para padronizar decodificadores de televisão digital (caixas sobre os aparelhos), a fim de reduzir os seus custos em larga escala. Ela padroniza os elementos envolvidos no acesso condicional a conteúdo transmitido em formatos MPEG-2 ou MPEG-4 para televisão móvel na Internet. Estes elementos consistem do algoritmo de criptografia do conteúdo transmitido, mensagens de controle ECM que contêm as chaves de decifração ou palavras controle, mensagens de administração de EMM que contêm direitos de usuários e a interface entre o decodificador e o módulo de segurança que administra o acesso condicional.

No caso específico de televisão móvel DVB-H, a proteção do conteúdo é desenvolvida pelo grupo DVB-CBMS (Transmissão de Vídeo Digital – Convergência de Serviços Móveis e Broadcast).

A padronização não engloba o conteúdo de valor agregado das mensagens de ECM e EMM, nem o método de proteção das mencionadas mensagens. Cada provedor de acesso condicional utiliza a sua própria estrutura de dados e os seus próprios meios de proteção para um conteúdo transmitido específico. A tecnologia DVB oferece, portanto, uma série de possibilidades de desenvolvimento de segurança de conteúdo.

Sabe-se bem que um transmissor pode ser autorizado a administrar o recebimento de um evento, dependendo da localização geográfica. De fato, as emissoras frequentemente tentarão impedir o acesso a conteúdo tal como transmissões esportivas na área vizinha ao local onde tem lugar o evento. Desta forma, conhecendo o local de cada receptor, um chamado sinal "blackout" é enviado para o receptor, por exemplo, com o(s) código(s) postal(is) de áreas que não está(ao) autorizada(s) a receber cobertura

do evento ao vivo. O módulo de segurança do receptor que contém as informações de localização (tais como o código postal do assinante do serviço ou CEP), ao receber esta mensagem, aplicará uma nova regra durante a verificação de direitos e, mesmo se o receptor possuir direitos para este evento, a mensagem "blackout" tem prioridade para impedir o acesso ao evento, ao não enviar de volta as palavras controle que são utilizadas para criptografar o evento.

No universo móvel, entretanto, esta noção de "código postal" não é mais válida e não é possível restringir uma recepção nesse dispositivo portátil.

Breve Descrição da Invenção

O propósito da presente invenção é o de permitir a aplicação dos mesmos meios de restrição no mundo móvel aos aplicados a receptores fixos.

Este propósito é atingido utilizando um método de acesso condicional a um fluxo de dados digital criptografado com pelo menos uma palavra controle e emitido por meio de um transmissor em uma rede de transmissão para pelo menos um dispositivo móvel, em que o mencionado transmissor também emite um fluxo de mensagens de controle que contém as palavras controle e as condições de acesso e o mencionado dispositivo móvel é adicionalmente conectado a uma rede de comunicação móvel por meio de um ponto de acesso móvel, em que o mencionado método é caracterizado pelo fato de que compreende as etapas a seguir:

- recebimento do fluxo de mensagens de controle pelo dispositivo móvel;

- determinação de um identificador de local para o mencionado dispositivo móvel, seja pelo identificador do ponto de acesso móvel ou pelo identificador do transmissor de rede de transmissão;

- verificação das condições de acesso contidas na mensagem de controle, em que as mencionadas condições de acesso compreendem uma condição de recepção relativa a pelo menos um identificador de ponto de acesso móvel e/ou um identificador de um transmissor de rede de transmissão;

- comparação do identificador determinado com o(s) identificador(es) contido(s) nas condições de acesso;

- autorização ou bloqueio do acesso ao mencionado fluxo de dados, dependendo do resultado da mencionada comparação.

Este método pode ser utilizado para bloquear o acesso por um dispositivo portátil em uma certa região (blackout) ou de outra forma, para autorizar o acesso apenas nessa região (ponto quente).

Segundo esta realização, a forma de determinar o identificador de local pode basear-se no identificador de células móveis (ponto de acesso móvel) ou no identificador do transmissor de rede de transmissão.

No primeiro caso, parece provável que a localização seja mais precisa devido à faixa limitada de pontos de acesso móveis.

No segundo caso, a rede de transmissão compreende uma série de transmissores que, além de emitirem o fluxo de dados, transmitem dados de serviços nos quais é possível identificar o transmissor no qual é sintonizado o dispositivo móvel.

Breve Descrição das Figuras

A presente invenção será mais bem compreendida graças à descrição detalhada a seguir que se refere às figuras anexas, fornecidas como exemplos não limitadores.

- A Figura 1 exibe um diagrama de bloco de um exemplo da configuração com dois transmissores colocados em locais diferentes e que se encontram dentro da distância de recepção de um dispositivo móvel local.

- A Figura 2 exibe um exemplo esquemático da cobertura dos transmissores da rede de transmissão e das células de rede móvel no interior dessas áreas de transmissão.

Descrição Detalhada da Invenção

Um fluxo de dados digital que forma um conteúdo (C) criptografado com palavras controle (CW) é transmitido junto com mensagens de controle ECM. Estes dados digitais podem compreender dados de programas de televisão de áudio e vídeo, bem como dados correspondentes a aplicações que podem ser conduzidas em um dispositivo móvel.

Um servidor de um provedor de conteúdo de acesso condicional é conectado a uma rede de transmissão (NET1). Esta rede transmite por meio de diversas antenas E1, E2 para dispositivos móveis EM1, EM2. Dependendo da localização de um dispositivo móvel, este último pode conectar-se a uma antena E1 e não a uma antena E2.

Da mesma forma, os dispositivos móveis EM1 e EM2 são ligados à rede de telecomunicações móveis NET2 por antenas apropriadas F1, F2.

O dispositivo móvel pode definir a sua posição geográfica por meio da rede de antenas de transmissão E1, E2 ou das antenas de telecomunicações móveis F1, F2. No protocolo de comunicação dos dois sistemas de comunicação, o identificador de antena é transmitido para o dispositivo móvel e, desta forma, é utilizado como um identificador de localização. O identificador é utilizado, por exemplo, para medir a qualidade de recepção de uma rede.

Este identificador, desta forma, não gera necessariamente uma indicação geográfica e pode ser um simples valor alfanumérico.

Ao mesmo tempo, o transmissor envia um fluxo de mensagens de controle com o fluxo de dados de áudio e vídeo. A mensagem de controle contém a(s) palavra(s) controle utilizada(s) para decodificar o conteúdo criptografado e contém ainda as condições de acesso a este conteúdo.

Segundo a presente invenção, as condições de acesso compreendem, além dos direitos necessários para o recebimento do conteúdo (tais como assinatura), um ou mais dos identificadores de antena relativos às zonas em que a recepção é restrita ou autorizada. Estes identificadores podem referir-se à rede de transmissão NET1 ou referir-se à rede de telecomunicações móveis NET2. Também é possível incluir uma lista conjunta que

compreende um ou mais identificadores das duas redes nas condições de acesso.

Como se pode observar na Figura 2, é preferível utilizar os identificadores C1 a Cn da rede de telecomunicações móveis. A cobertura para cada célula é menor, o que permite uma melhor demarcação da área restrita. Nas mesmas circunstâncias, entretanto, tal como para bloqueio ou autorização do acesso em toda uma cidade, é mais simples fazê-lo pelos identificadores de alguns transmissores da cidade.

Quando uma mensagem de controle chega ao dispositivo móvel, esta mensagem é transmitida para os meios de segurança do dispositivo. Estes meios podem ser o cartão SIM do dispositivo móvel ou um circuito especializado (soldado diretamente sobre o circuito impresso), ou podem ser realizados em forma de software. Estes meios de segurança verificam se as condições de acesso especificadas na mensagem de controle são ou não atendidas. Estas condições podem apresentar várias formas, tais como um direito específico ao conteúdo, um direito geral a um dado canal ou sistema de pagamento por tempo conforme descrito no pedido WO 03/085959. Segundo a presente invenção, além de condições tais como as descritas anteriormente, e como o recebimento de conteúdo é limitado de acordo com a localização geográfica, os meios de segurança verificam se o identificador de localização obtido da antena de telecomunicação ou transmissão está presente na lista de identificadores compreendida na mensagem de controle. Caso o identificador de localização esteja incluído na lista do(s) identificador(es) transmitido(s) nas condições de acesso, os meios de segurança serão capazes de enviar a palavra controle para os meios de decifração (versão hot spot) ou, caso contrário, bloquear a transmissão da palavra controle para os meios de decifração (blackout).

Dever-se-á observar que a mensagem de controle é criptografada de tal forma que um terceiro não pode acessar os identificadores utilizados para restringir o acesso a dados de áudio e vídeo. Segundo um modo específico da presente invenção, o identificador de localização pode ser assinado, a fim de garantir a sua integridade. O centro de transmissão (ou centro de telecomunicações, segundo a realização) utiliza a sua chave privada (a partir de um par de chaves assimétricas) para assinar o identificador. Esta assinatura é realizada de uma forma convencional, utilizando, por exemplo, um método hash do identificador e criptografia do resultado pela chave privada.

Do lado da recepção, o módulo de segurança possui a chave pública correspondente, que permite que ele decifre a assinatura para obter o valor hash presumido e compare este valor com o calculado pelo módulo de segurança no identificador de localização (autenticação). A comparação entre o valor presumido e o valor calculado permite, caso sejam iguais, garantir que o identificador não foi modificado.

Em uma realização específica, o módulo de segurança é previamente inicializado por um valor de localização padrão. O identificador atual substitui este valor assim que ele é comunicado para o módulo de segurança.

Quando uma mensagem de controle chega ao mencionado módulo e considerando que ela contem um controle blackout, o valor padrão é considerado automaticamente parte dos identificadores de localização que necessitam ser colocados em lista negra.

Segundo uma realização, é possível definir um período durante o qual um identificador é válido. Após o vencimento dessa validade e caso não tenha sido transmitido um identificador mais recente para o módulo de segurança, o identificador padrão é novamente estabelecido e considerado, portanto, ativo em cada comando de blackout. Este período pode ser um parâmetro do módulo de segurança ou pode ser associado aos dados do identificador, tal como com a assinatura de autenticação. A fim de evitar a reutilização de um identificador, uma data atual é associada ao identificador, preferencialmente autenticada com o próprio identificador. Desta forma, um identificador colhido previamente em uma outra célula de rede não poderá ser reutilizado em um outro dispositivo móvel. A fim de reforçar toda a segurança, o módulo de segurança recusará todos os identificadores associados a uma data anterior à do identificador transmitido anteriormente.

Além das redes de telecomunicações bem conhecidas tais como GSM, GPRS ou UMTS, podem ser utilizados outros meios de localização, tais como Wifi, WiMax, Wibro ou qualquer rede que possua um conjunto de antenas. A precisão da localização dependerá diretamente da densidade das antenas. Dever-se-á observar que o identificador contido na mensagem de controle poderá incluir uma faixa identificadora. Caso todos os identificadores de antenas em uma cidade iniciem-se com ABC (ABCV120, ABCJ11 etc.), é possível enviar apenas o prefixo ABC para inclusão de

todas as antenas ABCxxx. Outras possibilidades podem incluir uma faixa tal como ABC100 a ABC200.

REIVINDICAÇÕES

1. Método de acesso condicional local em um dispositivo móvel a um fluxo de dados digital criptografado com pelo menos uma palavra controle e emitido por meio de um transmissor em uma rede de transmissão para pelo menos um dispositivo móvel, em que o mencionado transmissor também emite um fluxo de mensagens de controle que contém as palavras controle e as condições de acesso e o mencionado dispositivo móvel é adicionalmente conectado a uma rede de comunicação móvel por meio de um ponto de acesso móvel, em que o mencionado método é **caracterizado** pelo fato de que compreende as etapas a seguir:

- recebimento do fluxo de mensagens de controle pelo dispositivo móvel;

- determinação de um identificador de local para o mencionado dispositivo móvel, seja pelo identificador do ponto de acesso móvel ou pelo identificador do transmissor de rede de transmissão;

- verificação das condições de acesso contidas na mensagem de controle, em que as mencionadas condições de acesso compreendem uma condição de recepção relativa a pelo menos um identificador de ponto de acesso móvel e/ou um identificador de um transmissor de rede de transmissão;

- comparação do identificador determinado com o(s) identificador(es) contido(s) nas condições de acesso;

- autorização ou bloqueio do acesso ao mencionado fluxo de dados, dependendo do resultado da mencionada comparação.

2. Método de acordo com a reivindicação 1, **caracterizado** pelo fato de que o acesso ao mencionado fluxo de dados somente é autorizado caso as condições de recepção compreendam o identificador de localização.

3. Método de acordo com a reivindicação 1, **caracterizado** pelo fato de que o acesso ao mencionado fluxo de dados somente é autorizado caso as condições de

recepção não compreendam o identificador de localização.

4. Método de acordo com qualquer das reivindicações 1 a 3, **caracterizado** pelo fato de que o identificador do ponto de acesso móvel é extraído dos dados de serviço recebidos do mencionado ponto de acesso móvel.

5. Método de acordo com qualquer das reivindicações 1 a 3, **caracterizado** pelo fato de que o identificador de transmissor da rede de transmissão é extraído dos dados de serviço recebidos do mencionado transmissor da rede de transmissão.

6. Método de acordo com qualquer das reivindicações 1 a 5, **caracterizado** pelo fato de que as condições de acesso compreendem uma lista de identificadores de transmissão da rede de transmissão.

7. Método de acordo com qualquer das reivindicações 1 a 5, **caracterizado** pelo fato de que as condições de acesso compreendem uma lista de identificadores de pontos de acesso móveis.

8. Método de acordo com qualquer das reivindicações 1 a 7, **caracterizado** pelo fato de que as condições de acesso compreendem pelo menos uma descrição de direitos relativa ao conteúdo transmitido e que o dispositivo móvel verifica a presença desses direitos para autorizar ou bloquear o acesso ao conteúdo.

9. Método de acordo com qualquer das reivindicações 1 a 8, **caracterizado** pelo fato de que o dispositivo móvel compreende meios de segurança responsáveis pelo tratamento das condições de acesso.

10. Método de acordo com qualquer das reivindicações 1 a 9, **caracterizado** pelo fato de que a rede de comunicações móveis é selecionada de acordo com um dentre os tipos GSM, GPRS, UMTS, WiMax, Wifi e Wibro.

11. Método de acordo com qualquer das reivindicações 1 a 9, **caracterizado** pelo fato de que o identificador contido nas condições de acesso define uma faixa dos identificadores de localização.

12. Método de acordo com qualquer das reivindicações 1 a 11, **caracterizado** pelo fato de que o identificador de local é assinado e o dispositivo móvel verifica a assinatura do identificador antes do seu uso em comparação com o(s) identificador(es) contido(s) nas condições de acesso.

13. Método de acordo com qualquer das reivindicações 1 a 12, **caracterizado** pelo fato de que o dispositivo móvel compreende um identificador padrão considerado parte do(s) identificador(es) contido(s) nas condições de acesso, causando o bloqueio do acesso ao mencionado fluxo de dados caso nenhum identificador adicional tenha sido introduzido.

14. Método de acordo com a reivindicação 13, **caracterizado** pelo fato de que um período é associado ao recebimento de um identificador pelo dispositivo móvel, em que o identificador padrão é novamente estabelecido após o vencimento desse período.

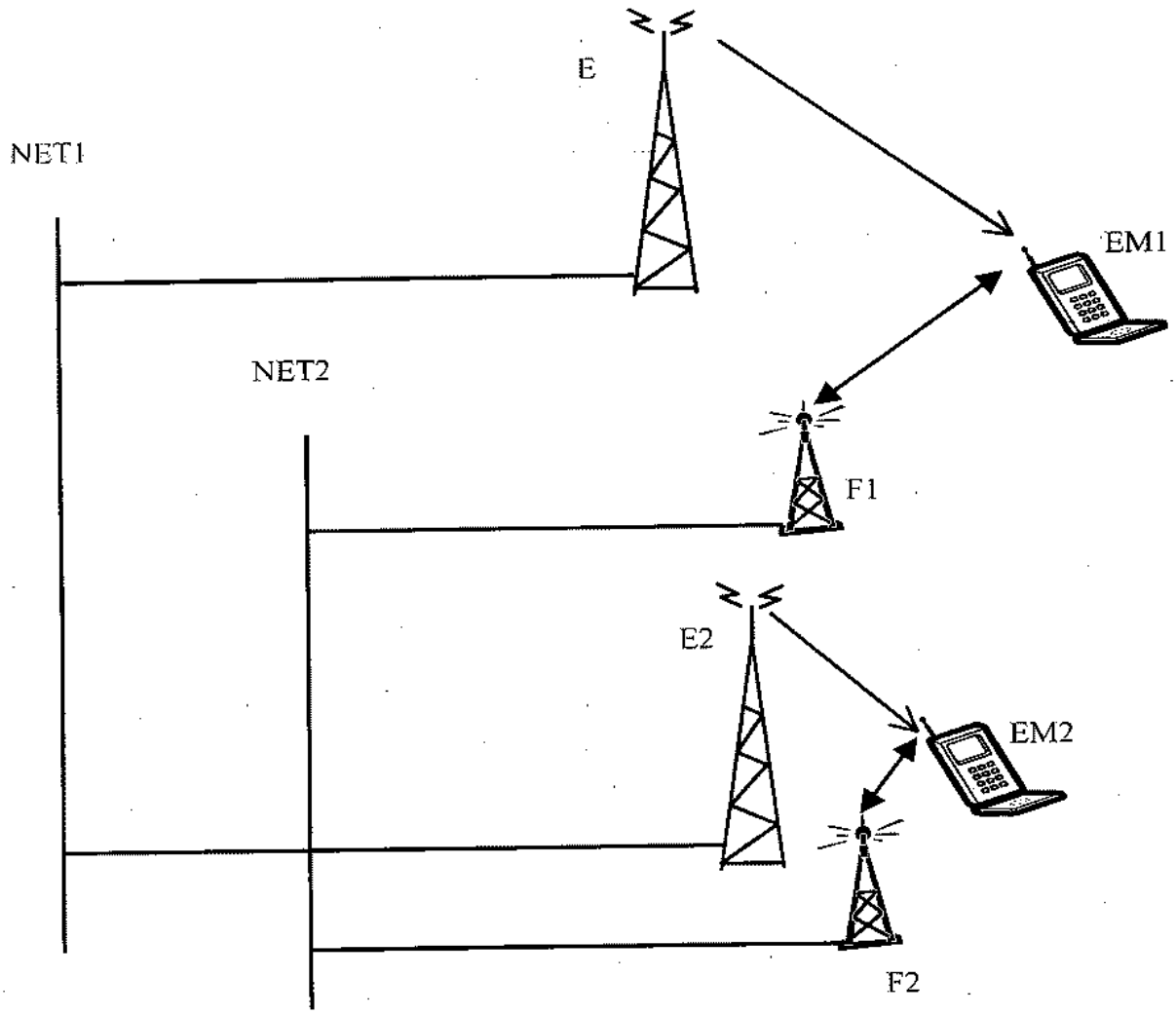


Fig. 1

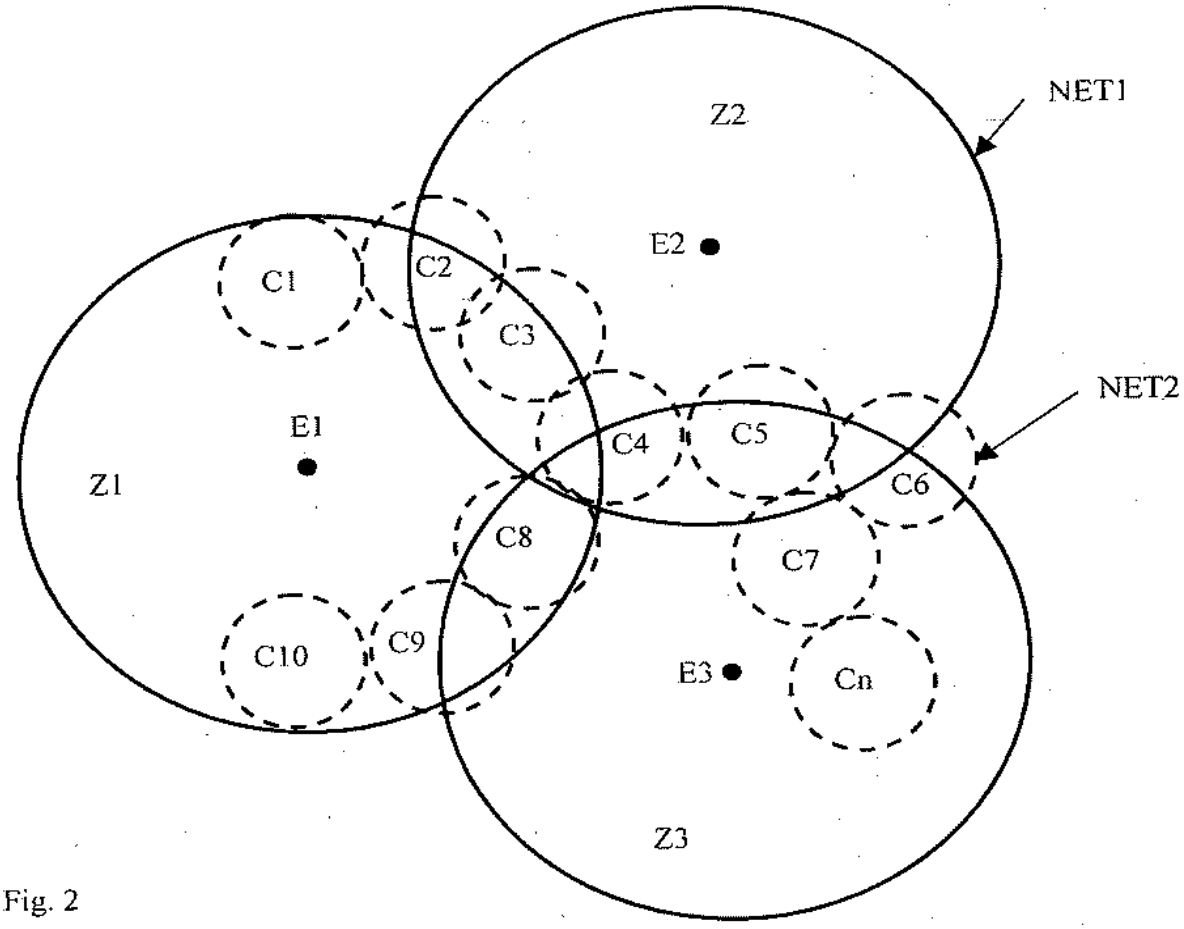


Fig. 2

RESUMO

O objeto da presente invenção é o de possuir no mundo móvel os mesmos meios de restrição aplicados a receptores fixos.

Este objeto é atingido utilizando um método de acesso condicional a um fluxo de dados digital criptografado com pelo menos uma palavra controle e emitido por meio de um transmissor em uma rede de transmissão para pelo menos um dispositivo móvel, em que o mencionado transmissor também emite um fluxo de mensagens de controle que contém as palavras controle e as condições de acesso e o mencionado dispositivo móvel é adicionalmente conectado a uma rede de comunicação móvel por meio de um ponto de acesso móvel, em que o mencionado método é caracterizado pelo fato de que compreende as etapas a seguir:

- recebimento do fluxo de mensagens de controle pelo dispositivo móvel;

- determinação de um identificador de local para o mencionado dispositivo móvel, seja pelo identificador do ponto de acesso móvel ou pelo identificador do transmissor de rede de transmissão;

- verificação das condições de acesso contidas na mensagem de controle, em que as mencionadas condições de acesso compreendem uma condição de recepção relativa a pelo menos um identificador de ponto de acesso móvel e/ou um identificador de um transmissor de rede de transmissão;

- comparação do identificador determinado com o(s) identificador(es) contido(s) nas condições de acesso;

- autorização ou bloqueio do acesso ao mencionado fluxo de dados, dependendo do resultado da mencionada comparação.