'CONTROLE DO ACESSO ÀS REDES DE TELECOMUNICAÇÕES DO SERVIÇO MÓVEL PESSOAL POR PARTE DE ESTAÇÕES MÓVEIS IRREGULARES

Marcelo Vaz Netto e José Marcos C. Brito

***Resumo* - Este artigo aborda a utilização ilegal de Estações Móveis (EM) irregulares nas redes do Serviço Móvel Pessoal (SMP) do Brasil, analisa as fragilidades nos atuais procedimentos de controle de acesso por parte das estações irregulares e propõe mudanças capazes de combaterem estas práticas ilícitas. Um novo procedimento de controle de acesso, capaz de impedir o acesso ao serviço por parte de estações irregulares é proposto.**

Palavras-Chave: Controle de acesso, fiscalização, EM irregulares.

***Abstract*— This paper addresses the illegal use of irregular Mobile Equipment (ME) in the Personal Communication Service (SMP) networks in Brazil. The weaknesses in the current procedures to avoid the access of irregular stations are analyzed. A new procedure do access control, able to avoid the use of the network by irregular stations is proposed.**

Keywords: Access control, supervision, irregular MEs.

I. INTRODUÇÃO

O crescimento das comunicações móveis no Brasil vem superando todas as expectativas. Em 2009, já havia 173,9 milhões de acessos móveis no país, com crescimento registrado de 15% naquele ano [1]. Parte significativa deste crescimento se deve ao sucesso do padrão adotado pela telefonia móvel em quase todo o globo, o padrão *Global System for Module Communications* (GSM), do qual, dentre tantas vantagens, destacam-se: a possibilidade de fazer e receber ligações fora da área de cobertura da operadora contratada (*roaming*), bem como a total liberdade de troca de estações móveis (aparelhos) com a permanência do número, através da simples inclusão de um "*chip*" em outro terminal de livre escolha do usuário.

Apesar das inúmeras vantagens, esta facilidade propiciou também o aparecimento de grande quantidade de estações móveis irregulares. Estudos recentes estimam que cerca de 20% [2] dos equipamentos operando nas redes do Brasil o fazem de forma irregular, trazendo enormes prejuízos para a economia do país. Este número vem crescendo vertiginosamente, ano após ano.

No caso específico da comunicação celular, tem-se observado o crescimento exponencial do mercado de aparelhos não homologados pela Anatel (Agência Nacional de Telecomunicações). Aparelhos estes, muitas vezes imitações de modelos de grandes fabricantes, que entram irregularmente no país e concorrem diretamente com os terminais regulares, beneficiando-se da total desoneração de impostos, face à rota da sonegação que se estende desde a entrada no território nacional até a aquisição pelos usuários finais. Dessa forma, além de alimentar uma grande rede de pirataria, o não recolhimento de impostos, tais como imposto de importação e imposto sobre operações relativas à circulação de mercadorias e sobre prestações de serviços de transporte interestadual, intermunicipal e de comunicação (ICMS), gera prejuízos aos Estados e à União.

Por normas da Regulação, a Anatel obriga as Prestadoras do SMP (Serviço Móvel Pessoal) o bloqueio dos terminais roubados através do seu *International Mobile Equipment Identity* (IMEI), um número de 15 dígitos que identifica o aparelho na rede. Entretanto, cabe também ao órgão regulador a eficiente fiscalização desta medida, visto que atualmente boa parte destes terminais bloqueados acabam retornando à rede através da clonagem do seu número IMEI, colocando por terra a eficácia desta medida.

Os procedimentos atuais de controle de acesso às redes do SMP por parte de estações móveis irregulares apresentam uma série de falhas e são incapazes de evitar o uso indevido da rede. Neste artigo analisamos estes procedimentos e identificamos seus pontos falhos. A partir destes, propomos outro capaz de evitar o uso da rede por parte de estações irregulares (roubadas, clonadas e não homologadas pela Anatel).

O restante deste artigo está organizado da seguinte forma: na Seção II descrevemos basicamente as numerações de identificação das estações móveis (IMEI e IMSI); na Seção III descrevemos brevemente algumas bases de dados disponíveis para auxiliar o procedimento de controle de acesso; na Seção IV os procedimentos atuais de controle de acesso são analisados e um novo procedimento é proposto; finalmente, as conclusões são apresentadas na Seção V.

II. SERIAL IMEI E IMSI

O *International Mobile Equipment Identity* (IMEI) é um número de *hardware* que identifica uma EM (Estação Móvel) individual. O IMEI é único para todas as EMs e, assim, fornece um meio para controlar o acesso às redes GSM. É uma forma das operadoras identificarem os equipamentos que estão usando as suas redes de telecomunicações.

O IMEI consiste de uma série de campos, totalizando 15 dígitos, todos com valores entre 0 e 9. O formato atualmente aprovado pela GSM *Association* (GSMA) e em uso em todos os EMs fabricados a partir de 01/01/03 é ilustrado na Figura 01: [3]

TAC	Nº de Série	Dígito de Checagem
NNXXXX YY	ZZZZZZ	A

Figura 01 - Formato do IMEI .

Marcelo Vaz Netto – Anatel – Agência Nacional de Telecomunicações, São Paulo / SP – e-mail: vaznetto@anatel.gov.br.

José Marcos C. Brito – Inatel – Instituto Nacional de Telecomunicações, Santa Rita do Sapucaí / MG – e-mail: brito@inatel.br.

Onde:

- TAC (Type Alloccation Code) é o código que identifica o modelo da EM;
- NN: RBI (*Reporting Body Identifier*) - Instituição responsável pela numeração do IMEI;
- XXXXYY: Identificador do Modelo da EM;
- ZZZZZZ: Número de série da EM;
- A: Dígito de verificação.

Enquanto o IMEI está relacionado ao *hardware* do EM, o *International Mobile Subscriber Identity (*IMSI) está relacionado ao número de acesso às prestadoras do SMP, sendo constituído de 15 dígitos, conforme ilustrado na Figura 02. [4]

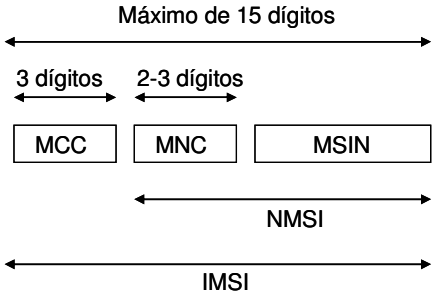

Figura 03 - Formato do IMSI.

Onde:

- MCC (*Mobile Country Code*): Consiste de 3 dígitos e identifica o país de domicílio[1];
- MNC (*Mobile Network Code*): Consiste de 2 ou 3 dígitos e identifica a prestadora do serviço de SMP;
- MSIN (*Mobile Subscriber Identification Number*): Identificação para o acesso do EM à rede da prestadora do SMP;
- NMSI (*National Mobile Subscriber Identity*): consiste da junção do *Mobile Network Code* e do *Mobile Subscriber Identification Number.* Trata-se de uma identificação nacional de todos os acessos no país.

Da mesma maneira que o IMEI, o IMSI é único para cada acesso às redes das prestadoras. É através do IMSI que as prestadoras fazem a validação do cliente e faturamento dos serviços contratados e prestados por ela.

A numeração do IMSI é gravada interiormente no (*Subscriber Identity Module*) SIM[2] e é enviada no momento de registro da EM com as respectivas (*Mobile Switching Center)* MSC, juntamente com o número de IMEI, para validação na rede das prestadoras como medida de segurança e identificação.

1 Para o Brasil a numeração de MCC é 724.

2 O *Chip* do padrão GSM.

III. GSMA E SUAS BASES DE DADOS

A GSM *Association* (GSMA), de acordo com os levantamentos no seu sítio na *Internet*[3], representa os interesses da indústria mundial de comunicações móveis e abrange 219 países, unindo cerca de 800 operadoras de telefonia móvel do mundo, bem como mais de 200 grandes companhias, incluindo fabricantes de celulares, empresas de *software*, fornecedores de equipamentos, companhias de Internet, mídia e agências reguladoras.

A GSMA mantém um sistema exclusivo, o banco de dados DB_IMEI, que consiste em um banco contendo informações básicas sobre o número de série (IMEI) alocado em milhões de aparelhos GSM e 3G de todos os fabricantes que estão em uso em redes GSM no mundo – chamado de *White List*.

A GSMA provê o acesso ao DB_IMEI aos seus membros (operadoras de rede, fabricantes e agências reguladoras) em todo o mundo. As operadoras de rede utilizam as informações do *White List* no DB_IMEI para verificar quais modelos de dispositivos estão sendo utilizados pelos seus clientes, de modo que elas possam oferecer melhores serviços adaptados aos EM que estão acessando suas redes, bem como somente permitir o registro na sua rede por EM que tenha o IMEI alocado na *White List*; já as agências reguladoras, por sua vez, usam esta referência para auditoria nas redes das prestadoras.

O DB_IMEI também suporta o que é conhecido como *Black List*. A lista negra é uma lista de IMEI de dispositivos GSM que devem ter o serviço negado nas redes das prestadoras. Esta lista, basicamente, é constituída de EM reportados como perdidos, roubados, defeituosos ou impróprios para uso.

O DB_IMEI funciona como um sistema central para as operadoras de rede no sentido de compartilhar suas listas negras individuais para que os dispositivos negados por uma operadora não funcionem em outras redes, mesmo se o cartão SIM - módulo de identificação do assinante - for alterado.

Segundo orientações da GSMA, as operadoras devem implantar o EIR (*Equipment Identity Register*) em suas redes, para manter a *Black List* de forma a evitar o uso irregular de equipamentos dados como irregulares. Esta base de dados, no caso do Brasil, é compartilhada entre as operadoras do SMP no intuito de criar uma única base de dados para todas as operadoras, o Cadastro de Estações Móveis Impedidas (CEMI). A concentração desta base, atualmente, é feita pela Associação Brasileira de Recursos em Telecomunicações (ABRT).

O processo no DB_IMEI da GSMA, no tocante a *Black List,* consiste em receber de todas as prestadoras associadas, as notificações de equipamentos inválidos de suas bases individuais para atualizar a do *Black List* do DB_IMEI e redistribui-la às prestadoras associadas. Com essa atualização do banco de dados EIR local, todos os EM reportados como roubados em outras redes conectadas até o dia anterior são bloqueados na rede da prestadora em questão.

3 http://www.gsmworld.com

IV. COMBATE A "EM" IRREGULARES

A presente seção tem como objetivo mostrar os fluxos de processo e auditoria hoje existentes no Brasil, fazer uma análise das suas falhas e propor novos procedimentos que venham ao encontro do efetivo combate a terminais irregulares.

IV.1 Cenário Atual

Hoje, o diagrama de blocos de processo e auditoria no combate a terminais irregulares, no Brasil, está representado na Figura 04:

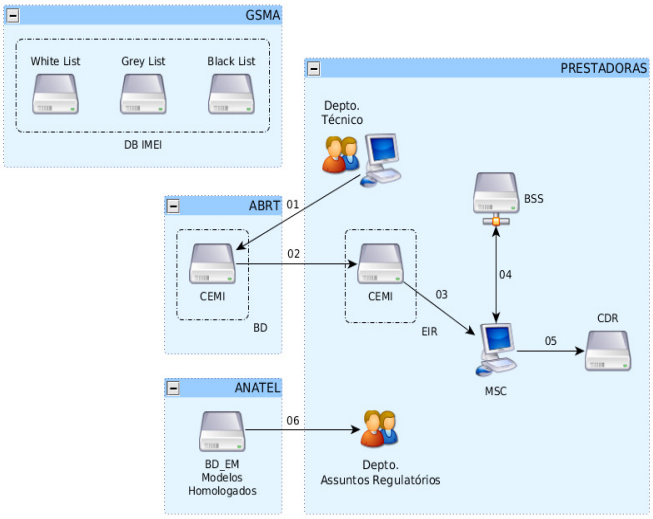

Figura 04 - Diagrama de Processo e Auditoria de IMEI irregulares Cenário Atual.

Pode-se definir que existem 4 (quatro) *players* principais envolvidos no combate aos terminais irregulares operando na rede do SMP no Brasil:

- A GSMA com seu banco de dados DB_IMEI constituído do *white list, black list e grey list* (lista de IMEIs que estão em observação);
- a Anatel com sua base de dados dos EMs homologados (BD_EM), com autorização para serem comercializados e operados no Brasil;
- as Prestadoras do SMP como agentes diretamente envolvidos na prestação do serviço e controle de acesso das EMs negativadas no CEMI, e;
- como ponto intermediário a ABRT, como centralizadora do Banco de Dados do CEMI e responsável pela sua atualização em todas as Prestadoras.

O processo atual pode ser definido nos seguintes procedimentos e fluxos:

- Qualquer pessoa que tenha seu EM roubado, furtado ou perdido pode solicitar junto à sua prestadora o bloqueio do EM na rede do SMP. A prestadora, por intermédio do seu departamento técnico, insere o número de IMEI do EM na base de dados da ABRT **(fluxo 01 da Figura 04)**;
- com o procedimento anterior, o CEMI na ABRT ficará atualizado com o IMEI irregular cadastrado pela prestadora inicial. Como periodicamente a ABRT envia sua base de IMEI impedidos no CEMI para todas as operadoras do SMP **(fluxo 02 na Figura 04)**, a base de dados de todas as prestadoras passará a contemplar o IMEI irregular, e, por conseguinte, a EM com o IMEI negativado na prestadora de origem não funcionará em nenhuma outra prestadora;
- a Anatel mantém uma base de dados com todos as EMs certificadas e homologadas pela agência. Por força de regulamentação[4], o departamento de assuntos regulatórios das prestadoras é obrigado a orientar o departamento técnico a programar as MSCs para somente aceitarem as EMs que se enquadrem nesta condição **(fluxo 06 da Figura 04)**;
- o DB_IMEI da GSMA continua sua atualização internacional sem fluxo com as Prestadoras do SMP no Brasil, Anatel e ABRT.

O fluxo de processo e controle por parte das operadoras do SMP, nas MSCs, pode ser representado através da Figura 05:

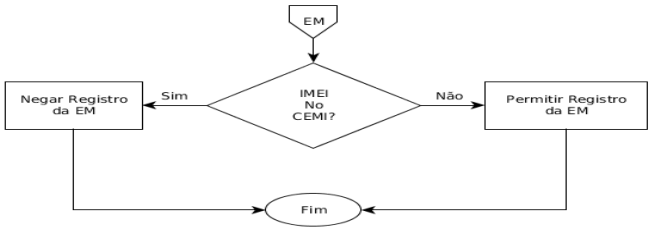

Figura 05 - Fluxo de controle atual nas prestadoras do SMP

Basicamente, o fluxo consiste em averiguar o IMEI da EM na base de dados do CEMI; se o IMEI da EM não estiver negativado no CEMI permite-se o registro na rede da prestadora. Caso contrário, nega-se o registro e consequentemente o EM não funcionará na rede.

IV.1.1 Problemas no Cenário Atual

Pelos procedimentos e fluxos acima expostos, denotam-se algumas falhas que passam a ser aqui descritas:

- Nota-se que não existe uma realimentação à Anatel e um controle de auditoria "permanente", por parte dessa, na base de registros de EM que acessaram as redes do SMP, disponíveis nos *Call Data Record* (CDR) das prestadoras **(fluxo 05 da Figura 04)**. Sem esta auditoria, a Anatel não tem um levantamento quantitativo e qualitativo do problema de acesso às redes do SMP, e por consequência não tem como saber se as prestadoras estão bloqueando

4 Art. 10. Além das outras obrigações decorrentes da regulamentação editada pela Anatel e aplicáveis a serviços de telecomunicações e, especialmente, ao SMP, constituem deveres da prestadora:
IV - utilizar **somente** (grifo nosso) equipamentos cuja certificação seja expedida ou aceita pela Anatel;
V - **somente** (grifo nosso) ativar Estações Móveis com certificação expedida ou aceita pela Anatel;
Resolução nº 477, de 7 de agosto de 2007.

os EMs com IMEI irregulares do CEMI;

- o CEMI não é realimentado com os dados da GSMA. Sem este procedimento no fluxo, qualquer EM negativado fora do Brasil acessará e trabalhará normalmente na rede de SMP das prestadoras brasileiras, e vice-versa. Essa falha fomenta o roubo e furto de EM;
- não existe um fluxo do *white list* da GSMA para a Anatel, ficando essa sem condições de alocar TAC expedido pela GSMA em acordo com seu banco de dados de EM homologados. Sem esse procedimento as prestadoras trabalham em um ambiente discricionário de *white list* ao acesso de EM homologados pela Agência Reguladora, já que essa também não recebe o *white list* da GSMA. Essa falha no procedimento permite o acesso de EM não homologados pela Anatel, pois a prestadora não tem como saber se um determinado EM com um determinado IMEI é homologado, durante o registro na MSC **(fluxo 04 da Figura 04)**;
- por definição em regulamento, os usuários estrangeiros em *roaming* internacional podem acessar, de forma não permanente, as redes do SMP. Essa condição deve permitir o acesso, em caso excepcional, de EM não homologado pela Anatel, porém deve ter o IMEI alocado pela GSMA. Entretanto, conforme visto na Figura 04, as prestadoras não fazem uso do *white list* da GSMA e por consequência não tem como impedir o acesso de EM em *roaming* internacional com numeração de IMEI inválida, de acordo com a GSMA;
- Como se pode ver no processo, não existe controle de clone de EM; pois não existe uma base de dados com os IMEI clonados.

IV. 2 Cenário Proposto

Diante das falhas do procedimento atual, apresentadas na Seção IV.1, coloca-se agora em apresentação um cenário proposto, ilustrado na Figura 06:

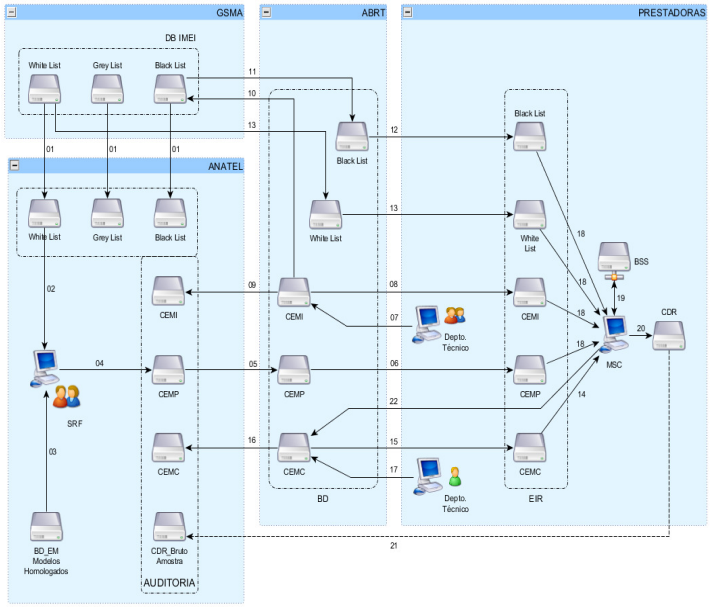

Figura 06 - Fluxo de Processo e Auditoria de IMEI irregulares
Cenário Proposto

O processo pode ser descrito nos seguintes procedimentos e fluxos:

- O CEMI, nesse cenário proposto, continuaria com seus fundamentos atuais acrescidos da condição de atualizar também o *black list* da GSMA via ABRT **(fluxo 10 da Figura 06)**. Esta nova base de dados continuaria a ser enviada **(fluxo 08 da Figura 06)** a todas prestadoras do SMP, fazendo com que as bases de dados dessas, nos EIR, sejam atualizadas com as ocorrências de roubo e furtos no Brasil. Além do acréscimo do **fluxo 10**, o qual permitirá a interação do CEMI com o *black list* da GSMA, é necessário que a base do CEMI fique a disposição permanente nas bases da Anatel, através do **fluxo 09**, permitindo por parte da fiscalização os procedimentos legais de auditoria nos processos das prestadoras. Com este procedimento os aparelhos roubados e furtados aqui no Brasil não funcionarão no Brasil e nas outras prestadoras associadas à GSMA;
- a Anatel passa a receber a base de dados da GSMA através do **fluxo 01**. Essa base de dados, além de ser elemento para auditoria dos processos das prestadoras, servirá no caso específico do *white list,* conjuntamente com a base de EM homologados pela Anatel (BD_EM), a criação de uma nova base de dados, doravante chamada de Cadastro de Estações Móveis Permitidas (CEMP), através dos **fluxos 02, 03 e 04**, que será enviada para a ABRT via **fluxo 05** e dessa para as prestadoras via **fluxo 06**. Com este procedimento, a Anatel entrega às prestadoras do SMP todos os TACs dos modelos de EMs autorizados (homologados) a acessar, de forma permanente, as redes do SMP. As prestadoras por sua vez, através dos **fluxos 18 e 19**, permitem somente o acesso às suas redes pelos TACs cadastrados no CEMP, impedindo o acesso à rede por EMs não certificados, vindo ao encontro do Art. 10 da Resolução nº 477, de 7 de agosto de 2007 (rodapé pág. 03);
- a ABRT passa a receber, também, o *white list* da GSMA e desta para as prestadoras via **fluxo 13**. É fundamental que as prestadoras tenham em sua EIR a base do *white list* da GSMA, pois somente através dessa base é que poderão validar os IMEIs dos EMs em *roaming* internacional (já que o CEMP, necessariamente, não contemplará um modelo de EM que não esteja homologado para operar no Brasil);
- por intermédio dos **fluxos 11 e 12** faz-se o *download* do *black list* da base de dados do DB_IMEI na GSMA. Este procedimento permitirá o controle de IMEI negativado internacionalmente, por parte de EM com IMSI internacional, em *roaming* nas redes das prestadoras do SMP no Brasil;
- havendo um maior controle no acesso de EM quanto aos IMEI e TAC, cadastrados no CEMI e no CEMP, respectivamente, haverá um aumento substancial no número de EM clonados. Como forma de coibir esta técnica de fraude, indo ao encontro da orientação na resolução 477, de 7 de agosto de 2007, foi criada nesta proposta de controle o Cadastro de Estações Móveis Clonadas (CEMC), **fluxos (14, 15, 16, 17 e 22)**, que consiste em permitir "somente" um IMEI "único" na base de dados do EIR (chave primária de controle);
- por fim, existe o fechamento do *loop* "permanente" de auditoria (realimentação) através da disposição dos CDRs das prestadoras, diretamente à Anatel, para auditoria de todo o processo descrito **(fluxo 21 Figura 06)**.

A Figura 07 apresenta o fluxograma do novo fluxo de controle proposto para as MSCs das operadoras do SMP.

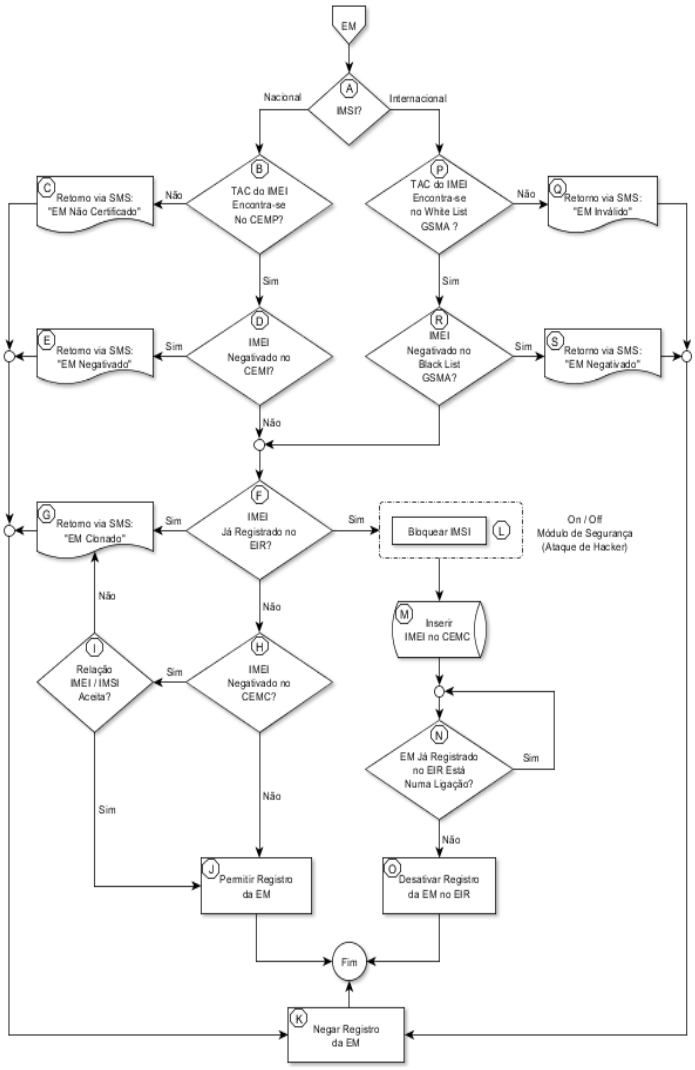

Figura 07 - Fluxo de controle proposto nas MSC das prestadoras do SMP

Denota-se no fluxo de controle proposto acima que existe uma diferenciação de controle quanto à procedência dos EM relativo ao seu IMSI (Nacional ou Internacional).

Se o equipamento estiver em *roaming* internacional, o controle nas MSC's baseará nos dados armazenados na GSMA: TAC registrados no *White List* e IMEI negativado do *Black List*. Esse procedimento é necessário visto que a EM em *roaming* pode ainda não ter sido homologado pela Anatel para trabalhar nas redes das prestadoras do SMP no país, consequentemente o seu TAC não estará do CEMP. Já o CEMI é constituído de IMEI negativado (roubo ou furto) que foram homologados inicialmente pela Anatel para trabalharem nas redes (obrigatoriamente estão no CEMP). Como o EM com IMSI internacional não consta no CEMI, pelo fato de não constar no CEMP, deve-se buscar o seu controle no *Black List* da GSMA.

V. CONCLUSÕES

Os serviços de comunicações móveis no Brasil crescem a taxas elevadas. O número de acessos móveis hoje já suplanta em muito o número de acessos fixos à rede telefônica. Cerca de 20% das estações móveis que utilizam a rede são irregulares, trazendo inúmeros problemas para o país, inclusive de ordem financeira.

Os procedimentos atuais para controlar o acesso às redes do SMP por estações irregulares apresentam uma série de falhas e são incapazes evitar o uso ilegal da rede por estas estações irregulares.

Neste artigo, nós analisamos os pontos falhos dos procedimentos atuais e, com base nesta análise, propomos um novo procedimento para controlar o acesso das estações móveis às redes do SMP. O procedimento proposto elimina as falhas nos atuais (CEMI) e ainda acrescenta facilidades hoje inexistentes, como o impedimento de acesso por parte de dispositivos clonados (CEMC) e não homologados (CEMP).

REFERENCES

[1] **Anatel – Relatórios.** Relatórios anuais. Disponível em http://www.anatel.gov.br/Portal/exibirPortalInternet.do. Acesso em outubro de 2010.

[2] **Folha de São Paulo – 14 de fevereiro de 2011**. Disponível em http://www1.folha.uol.com.br/mercado/875189-celulares-clandestinos-ja-sao-20-do-total.shtml. Acesso em 14 de fevereiro de 2011.

[3] **IMEI Allocation and Approval Guidelines**, pag. 05. Disponível em http://www.gsmworld.com/documents/DG0640.pdf. Acesso em 07 de setembro de 2010.

[4] ***3GPP TS 03.03 v7.8.0 – Technical Specification***, pag. 08. Disponível em: http://www.3gpp.org/ftp/ Specs/html-info/SpecReleaseMatrix.htm. Acesso em 07 de setembro de 2010.