PROPOSTA DE IMPLEMENTAÇÃO DE UMA REDE MÓVEL COM FUNCIONALIDADES BÁSICAS DO SERVIÇO DE TELEFONIA GSM/GPRS BASEADA EM TECNOLOGIA OPEN-SOURCE

André Carrijo de Oliveira, Arthur Pires Ribeiro Silva, Bruna Lorena Rodrigues Gondin, Gabriel Fernandes Machado, Luiz Cláudio Theodoro, Paulo Sérgio Caparelli, Thiago Berger Canuto Alves

Universidade Federal de Uberlândia, Faculdade de Engenharia Elétrica,Uberlândia – MG, andre.carrijo90@gmail.com, arthurprs@gmail.com, bruna.lorenagondin@gmail.com, gfmachado22@gmail.com, lclaudio@feelt.ufu.br, pscaparelli@ufu.br, thiagocanuto.feelt@gmail.com

Resumo **- O objetivo deste artigo é propor a implementação de uma estrutura de rede móvel GSM composta por uma controladora de estações radio-base que desempenhe as funções de controle, gerenciamento, sinalização e transporte de chamadas de voz e de dados. Adicionalmente, permitir que se evolua para a implementação dos elementos de uma rede móvel de terceira geração especificamente para serviços de dados. Dessa forma pretende-se facilitar o aprendizado desta tecnologia e gerar novas aplicações sem a necessidade de ter uma infraestrutura de software adquirida junto aos fabricantes tradicionais. Todo o desenvolvimento deste projeto será baseado em soluções *open-source* integradas a equipamentos comerciais como rádios e aparelhos móveis. Ainda será necessária a interconexão com as centrais telefônicas tradicionais para efetuar chamadas para assinantes de outras redes.**

Palavras-Chave **– BSC, GPRS, GSM, OpenBSC, rede móvel, telefonia celular.**

IMPLEMENTATION PROPOSAL OF A MOBILE NETWORK WITH BASIC FUNCTIONALITIES OF THE GSM/GPRS TELEPHONY SERVICE BASED ON OPEN-SOURCE TECHNOLOGY

Abstract **– This essay aims at proposing the implementation of a GSM mobile network structure composed of a base station controller that assumes the function of control, management, signalization and transport of voice and data. It also permits the evolution for the implementation of elements in a mobile network of the third generation specifically for data services. Thus it is intended to facilitate the learning of this technology and generate new applications without needing to have a software infrastructure acquired with the traditional suppliers. This project's whole development will be based on open-source solution integrated to commercial equipments such as radios and mobile devices. It will still be needed an interconnection with the traditional carriers in order to make calls for subscribers of other networks.**

Keywords **- BSC, Cellular telephony, GPRS, GSM, mobile network, OpenBSC.**

Artigo publicado na IX CEEL
03 a 07 de outubro de 2011
Universidade Federal de Uberlândia - UFU
Uberlândia - Minas Gerais - Brasil

I. INTRODUÇÃO

A Telefonia Móvel é um dos serviços mais utilizados atualmente por uma série de fatores como aparelhos a preços acessíveis, mobilidade, inúmeras funções disponíveis e ainda ampla cobertura, podendo ser usado a nível global. A mobilidade, um dos fatores alavancadores da tecnologia só é possível graças à utilização da radiodifusão como meio físico de transmissão.

Nas primeiras implementações de sistemas de comunicação móvel, uma prática comum era tentar atingir grandes áreas de cobertura através de transmissores de alta potência. Essa tentativa era agravada pela limitação do número de usuários em função da alocação de uma frequência única para cada conexão. Posteriormente, surgiu o conceito de telefonia celular, que dividia em regiões denominadas células, as áreas a serem cobertas. Com a implementação do *handover* que permitia ao usuário se deslocar pelas células sem que o sinal caísse, essa proposta foi efetivamente adotada [1] [2].

Para criar condições de montar células que cobrissem áreas específicas foi instituída a figura da Estação Radio Base (ERB) que era a ligação entre uma central de comutação e o aparelho móvel. Entre o aparelho e a estação radiobase, o acesso era por radiodifusão e entre a estação radiobase e os demais elementos até a central, normalmente por interfaces físicas. Foi possível atender à crescente demanda de usuários simplesmente aumentando os canais disponíveis numa ERB para uma determinada região, tudo isso sem exigir muito da potência de transmissão. Com a possibilidade de reutilização das frequências em células não contíguas, tornou-se ainda mais eficiente o processo de atender as chamadas em larga escala.

A evolução das tecnologias de telefonia celular foi organizada em gerações para melhor entendimento. A primeira, implementada a partir dos anos 80, tinha como característica marcante a transmissão analógica, mas mesmo assim atingia qualidades adequadas para chamadas de voz, porém inviável para transmissão de dados. No início da década de 90, a segunda geração confirmou toda a

expectativa da comunidade mundial num serviço eficiente de telefonia móvel, nesse momento, já utilizando o padrão digital permitia serviços confiáveis para voz e dados. Com a atuação maciça de pesquisadores, cientistas, engenheiros e demais profissionais, foram surgindo gerações intermediárias. Inicialmente criou-se a tecnologia *Global System for Mobile* (GSM), logo em seguida, aproveitando a infraestrutura do GSM surgiu a geração 2,5 também chamada *General Packet Radio Service* (GPRS) e 2,75 ou *Enhanced Data rate for GSM Evolution* (EDGE) com foco direcionado para o aumento da capacidade de transmissão de dados. A terceira geração (3G) consolidou definitivamente a aceitação global da telefonia celular como serviço adequado para os mais diversos fins, incluindo o acesso a internet. Neste momento, o mundo vive a fase de introdução da quarta geração que promete, principalmente taxas ainda maiores para as chamadas de dados.

Será então apresentada na seção II deste trabalho toda a base da estrutura de uma rede GSM, com elementos e algumas funções para entender a implementação do projeto que será mostrada na seção III, exemplificando quais softwares, equipamentos e equipes de colaboração serão envolvidos [3].

II. GSM

Por volta de 1980, os grupos envolvidos na especificação do padrão GSM perceberam que não teriam tempo hábil para desenvolver as especificações necessárias para todos os serviços e facilidades que imaginaram anteriormente. Assim, foi decidido que o GSM seria desenvolvido em fases, sendo a primeira limitada a um conjunto de funcionalidades. Cada nova fase é montada com base nos serviços oferecidos pelas fases pré-existentes. Na primeira etapa foram incluídos os seguintes serviços: tráfego de voz, *roaming* internacional, serviços básicos de fax e dados (até 9,6 Kbps), direcionamento e barramento de chamadas, *Short Message Service* (SMS), cifragem e a adoção do SIM card.

Uma rede de telefonia celular GSM é construída a partir de três elementos principais, como pode ser vista na Figura 1: o conjunto estação radiobase e controladora, a estação móvel e a central de comutação móvel [4].

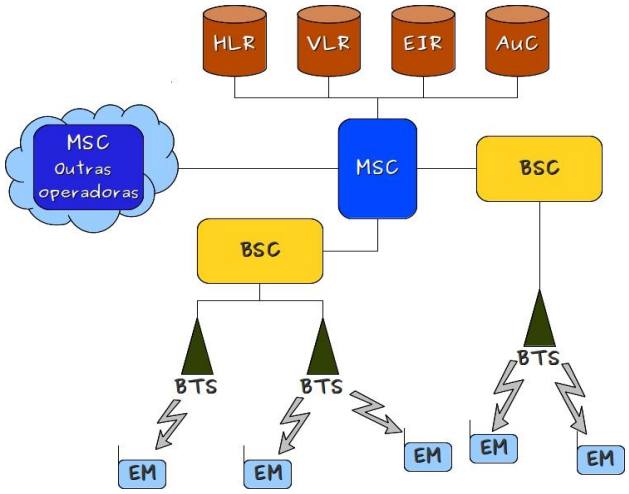

Fig. 1. Estrutura de rede GSM.

As estações móveis mantêm um transceptor de voz e dados que se comunica com os rádios das estações radiobase em qualquer um dos canais alocados, referenciados como link direto e link reverso. O processo exige que mensagens de controle sejam trocadas entre a estação móvel e a estação radiobase, por exemplo, pedido do móvel para acessar um canal, resposta para o móvel identificar o canal alocado e mensagens da base para o móvel, para que este sintonize outro canal, quando num momento de *handoff*.

As estações radiobase ou *Base Transceiver Station* (BTS), são elementos da rede GSM responsáveis pela comunicação entre a estação ou unidade móvel e o núcleo da rede. Sendo assim, as BTSs, juntamente com a *Base Station Controller* (BSC), constituem a rede de acesso até a central de comutação móvel. Uma BTS é constituída por uma estrutura física de torre e antenas que abrigam um *transceiver*, que transmite e recebe os sinais captados dos aparelhos móveis distribuídos na sua região de cobertura. Complementa um conjunto de microprocessadores que controlam, monitoram e supervisionam as chamadas entre os dispositivos móveis. A BTS também tem a responsabilidade de avaliar os níveis de sinal para verificar a necessidade de *handoff* [5].

Controlando diretamente as estações radiobase, encontra-se a BSC que se conecta à central de comutação móvel. Entre as várias funções da BSC, destacam-se o controle dos canais da BTS e da potência dos equipamentos, manipulação das conexões entre as estações móveis e supervisão dos enlaces entre as unidades móveis e a BTS.

Centralizando todas as operações da rede, por possuir uma visão sobre todas as células, a Central de Comutação Móvel ou *Mobile Switched Center* (MSC) é a responsável pelo gerenciamento e controle das BSCs, suporte às tecnologias de acesso e às atividades de processamento de chamadas possuindo ainda a nobre missão de interoperar com a Rede de Telefonia Pública Comutada (RTPC).

Vários outros elementos conectados à central auxiliam para que o serviço de telefonia móvel tenha resultados eficientes e úteis à população. Um deles, o *Home Locator Register* (HLR), uma base de dados sobre o usuário, armazena o perfil de serviço do assinante, a sua localização e outras informações essenciais que são complementadas por outra estrutura, o *Visitor Locator Register* (VLR) que controla o usuário em *roaming* ou fora de sua área de inscrição.

Atentando para aspectos envolvendo aparelhos, existe uma base de dados denominada *Equipment Identity Register* (EIR) que faz o registro da identidade do equipamento referenciado pelo *International Mobile Equipment Identity* (IMEI) e que é utilizado para identificação e bloqueio dos aparelhos sem autorização. Também integrada à MSC, é essencial a figura da Central de Autenticação (*Authentication Centre* - AuC), responsável por validar o processo de autenticidade e criptografia já que mantém as chaves e algoritmos para esse fim.

Todos estes elementos compõem o que denominamos de Rede GSM e executam o caminho de voz para atender universalmente ao serviço de chamadas telefônicas entre usuários de aparelhos móveis que desejam conversar entre si ou ainda com assinantes da telefonia fixa. De acordo com o

descrito até aqui, estruturas como essa, que evoluíram por gerações são providas por sistemas de software de altíssimo nível e que exigem por parte dos fornecedores um time de engenheiros e outros tantos profissionais em alta quantidade. Se atrever a implantar, mesmo num conjunto mínimo, uma solução que atenda às funcionalidades básicas do serviço é uma tarefa que exige um enorme esforço e que pode ser possível com a colaboração de vários pesquisadores espalhados pelo mundo [6].

Toda esta complexidade tecnológica é agravada com o fato de que cresceu assustadoramente nos últimos anos a demanda por transmissão de dados, forçando as empresas com soluções tecnológicas a proverem estruturas que aumentam cada vez mais a velocidade de transferência dos dados. De valores iniciais na faixa de poucos kbits por segundo o requisito atualmente é de valores além dos Gbits por segundo. As incorporações na rede GSM foram implementadas com a denominada rede GPRS e exigiu a inserção de novos elementos de forma integrada.

Um primeiro elemento neste novo contexto, mostrado na Figura 2, que pode ser comparado à camada física do modelo OSI (*Open Systems Interconnection*) é a *Packet Control Unit* (PCU). Ela é responsável por fazer o desvio das chamadas de dados para um caminho específico dentro da rede GSM/GPRS. Possui a responsabilidade de converter os dados trafegados para um formato que pode ser transmitido pela interface aérea e vice-versa. Também executa a gerência dos recursos de rádio e implementa as medições de Qualidade de Serviço (*Quality of Service* - QoS). Seguindo a rota interna na plataforma, a PCU é ligada a um elemento denominado de *Serving GPRS Support Node* (SGSN) que controla a conexão entre a rede e a estação móvel, possibilitando o controle da sessão e de funções de gerenciamento de mobilidade GPRS, como *handovers* e *paging*. Neste ponto também é feita a contagem do número de pacotes roteados. Complementando a rota, como segue na figura, o *Gateway GPRS Support Node* (GGSN) funciona como uma ponte entre a rede GPRS de origem e a rede de dados externa ou outras redes GPRS, fornecendo funções de gerência de autenticação e localização e de tarifação relativa ao consumo do assinante [7].

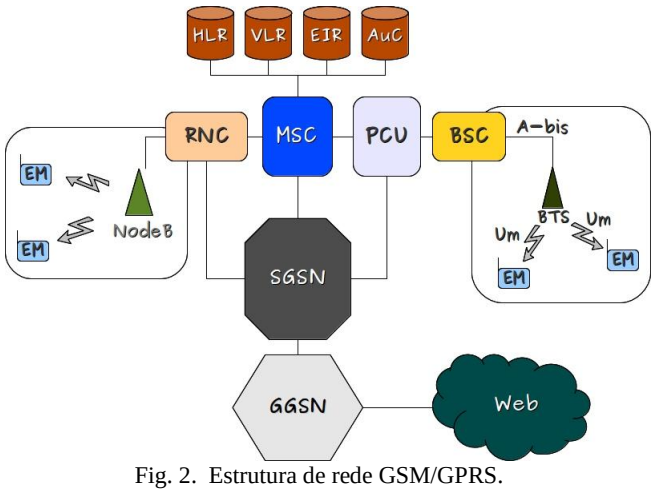

Fig. 2. Estrutura de rede GSM/GPRS.

A proposta deste projeto é implementar, por software, todas estas funções que permitem a operação real de um serviço de telefonia móvel usando a tecnologia GSM. Denominado como OpenBSC [6], projeto este que é uma extensão da proposta de colaboração implementada pelo grupo Osmocom, da Alemanha, objetiva incluir funcionalidades executadas pelos componentes descritos até agora: BSC, MSC, HLR, AuC, VLR e EIR. A parte de dados GPRS não será contemplada neste momento. Para atender a essa expectativa, espera-se evoluir a partir deste projeto para a rede 3G que demonstra ser mais interessante implantar a estrutura de chamadas de dados devido à maior capacidade de transmissão.

III. IMPLEMENTAÇÃO DA SOLUÇÃO

O desenvolvimento deste projeto é baseado na solução iniciada pelos pesquisadores da Osmocom, um grupo cooperativo que disponibiliza uma base de software que pode ser utilizada para pesquisa e colaboração por universidades e empresas no mundo inteiro. A solução provida pelo grupo permite a implementação deste ambiente e sugere alguns equipamentos que podem ser utilizados para tal fim.

A finalidade é montar uma rede para utilização acadêmica com os serviços básicos de telefonia móvel e num futuro, possivelmente substituir as soluções de software proprietárias comercializadas a altíssimos preços pelos grandes fabricantes. Atualmente, as aplicações oferecidas pelos grandes *players* são adquiridas pelas empresas que prestam o serviço de telefonia mas não tem acesso ao código-fonte, desta maneira ficam reféns dos fornecedores.

Efetivamente, usando um telefone compatível, o sistema desenvolvido permitirá originar e receber chamadas telefônicas e enviar e receber SMS. O foco do projeto está em desenvolver uma BSC, no lado do protocolo A-bis que é a interface de comunicação entre a BTS e a BSC. Será utilizada a especificação técnica GSM 88.5x e 12.21 que permite implementar um subconjunto mínimo da BSC, MSC e HLR.

O projeto pretende como resultado fornecer uma base para pesquisa e experimentação de uma rede móvel, permitindo desta maneira um aprendizado profundo sobre a rede GSM em baixo nível, mas operando equipamentos convencionais. Dessa forma, não se pretende, num primeiro momento, construir uma estrutura confiável e estável envolvendo uma MSC e BSC, já que uma rede comercial possui um alto nível de disponibilidade. Pontualmente, não se contemplará todos os detalhes de uma especificação GSM. Em contrapartida, levará até o pesquisador da área, um ambiente acessível para estudo, avaliação e desenvolvimento de novas funcionalidades, como desafios que envolvem segurança.

A solução OpenBSC foi em grande parte desenvolvida em linguagem portável, entretanto existe uma parcela não-portável, o driver de entrada *Modular Integrated Services Digital Network* (mISDN) para o kernel do Linux. Vinculado a isto precisaremos de uma placa de conexão E1 compatível e uma BTS que utiliza a mesma interface, tendo tal interface uma taxa de transmissão de 2 Mbits por segundo. Exemplos de BTSs já testadas e compatíveis com a solução são a microBTS do fabricante Siemens e nanoBTS do fabricante

ip.access. Alguns equipamentos poderão ser adquiridos para teste da rede, pois a mesma deve ser capaz de se comunicar com as demais redes coexistentes, como outras redes GSM, redes de telefonia fixa e redes de Voz sobre IP.

Há dois modos de configuração previstos para a solução OpenBSC. O primeiro deles é uma solução unificada, onde as funcionalidades da BSC são concentradas em um único módulo, juntamente com as funções de outros elementos como MSC, HLR, VLR, etc. Esta implementação é muito diferente de uma rede clássica GSM, na qual a BSC é apenas um dentre os elementos da rede. Sendo assim, o único equipamento necessário será a BTS, que através da interface A-bis via conexão E1 ou IP (*Internet Protocol*) estará conectada ao controlador que utiliza o OpenBSC.

O segundo modo de configuração é chamado *only BSC* e requer a utilização dos outros elementos de rede descritos anteriormente. Este modo está previsto para ser implementado em parceria com uma operadora que abra parte de sua infraestrutura para desenvolvimento dessa solução [6].

O roteiro de implantação do projeto envolve algumas atividades específicas. A primeira delas é a inicialização da BTS ao estar preparada para assumir o controle do uso e da integridade dos recursos de rádio. A partir desta etapa, a BSC terá condições de alocar os canais e atribuí-los aos dispositivos demandantes da chamada.

Para prover os recursos de cadastro e perfil de serviço, a solução integrada dispõe de um HLR simples implementada como uma base de dados *Structured Query Language* (SQL). A partir de uma autenticação, os usuários do sistema podem ser liberados para usar o serviço de chamadas telefônicas após verificação do IMEI e do *International Mobile Subscriber Identity* (IMSI), informações recebidas do *Subscriber Identity Module card* (SIM card) [3]. Os critérios de autenticação envolvem chaves de criptografia baseadas no algoritmo COMP128v1. Este é utilizado pela maioria das concessionárias e também será neste projeto, apesar de existirem métodos mais seguros, pois já são conhecidos métodos de clonagem obtidos a partir da engenharia reversa deste algoritmo [8].

A transmissão de pacotes com o nome da operadora e definições de zona e horário local também é contemplada no OpenBSC, além de manter o registro de atualização da área de localização do último local que o aparelho móvel percorreu. Já a questão do *handover* é possível apenas entre múltiplas células de uma mesma BSC.

O serviço SMS pode ser disponibilizado na solução OpenBSC. Ele mantém um esquema de *"store and forward"* para o envio e recepção de mensagens curtas incluindo roteamento entre os assinantes. Será implementada a opção de enviar mensagens pela linha de comando e também por meio de aplicações externas a partir da gravação em tabelas de um banco de dados SQL.

A função de chamada de voz, ainda serviço principal de telefonia móvel GSM, será liberado para os usuários dessa solução tanto para chamadas originadas (*Mobile Originated* - MO) como para chamadas terminadas (*Mobile Terminated* - MT). Os codificadores de voz utilizados serão o *Enhanced Full Rate* (EFR) trabalhando com taxas de 12.2 kbit/s e o *Full Rate* (FR) nas taxas de 13 kbit/s. Já o esquema de compressão de áudio aprovado pelo *3rd Generation Partnership Project* (3GPP), *Adaptative Multi Rate* (AMR) é oferecido apenas para a segunda versão, *only BSC* e tem a grande vantagem de também ser utilizado nas redes *Universal Mobile Telecommunications System* (UMTS) [4].

Atendendo às atuais demandas, o serviço de transmissão de dados pode ser usufruído através das tecnologias GPRS e EDGE. A solução OpenBSC permitirá configurar uma nanoBTS para estas duas tecnologias e poderá interoperar com uma SGSN via interface Gb. O desenvolvimento deste projeto prevê cooperar na construção da versão beta do módulo OsmoSGSN [6].

Todas estas funções descritas, atestam que uma rede móvel com boa parte dos serviços disponíveis pode ser implementada a partir de uma versão básica desenvolvida pelo grupo de pesquisa Osmocom e, seguindo alguns procedimentos de instalação, configuração, avaliação e adaptação tem-se como resultado uma aplicação que representa toda a estrutura de uma controladora de estação radiobase que estará interoperando com uma BTS e que poderá ou não unificar os outros elementos de rede.

Com essa solução adaptada aos elementos de terceiros ou implementados pela nossa equipe, a maioria das funções poderão ser simuladas, estudadas, avaliadas e utilizadas a nível comercial para a telefonia celular GSM e assim permitir a criação de novos serviços ou a migração para uma rede de nova geração.

VI. CONCLUSÕES

Com a ampla aceitação e expansão dos serviços de telefonia móvel, onde a tecnologia GSM se estabeleceu efetivamente, pesquisadores do mundo inteiro se preocuparam em melhorar cada vez mais as técnicas e aplicações para prover o melhor serviço. Apesar do GSM trazer uma documentação aberta de fácil acesso, a implementação de novas pesquisas ainda depende de facilidades junto às operadoras que mantém toda a infraestrutura da rede.

Há uma restrição ao acesso às controladoras, estações radiobases e centrais, inacessíveis principalmente pelo caráter de segurança necessário nas estruturas comerciais. Além disso, as operadoras possuem certa resistência às mudanças propostas em pesquisas, devido à dificuldade e custos para a transição da tecnologia. Implementar e disponibilizar uma rede que permita fácil manipulação e acesso a pesquisadores, estudantes e professores se tornou uma possibilidade quase remota.

No entanto, a proposta deste projeto pode tornar realidade uma antiga necessidade, que além de facilitar o aprendizado dos envolvidos nas tecnologias de comunicação móvel permitirá que se crie novas aplicações envolvendo os desafios atuais e ainda que se evolua para redes de nova geração como 3G e *Long Term Evolution* (LTE).

Assim, as escolas com estrutura similar ao utilizado pelas empresas que prestam serviço de telefonia móvel poderão contribuir de forma efetiva no crescimento dos países através da evolução tecnológica [1].

REFERÊNCIAS BIBLIOGRÁFICAS

[1] J. U. Sverzut, "Redes: GSM, GPRS, EDGE e UMTS – Evolução a Caminho da Quarta Geração", Editora Ética, 2ª Edição, São Paulo, Brasil, 2008.

[2] T. S. Rappaport, "Comunicações Sem Fio – Princípios e Práticas", Tradução, 2ª Edição, Pearson Education, EUA, 2009.

[3] C. –K. Toh, Ph. D., "Ad. Hoc. Mobile Wireless Networks – Protocols and System", Prentice Hall PTR, New Jersey, EUA, 2002.

[4] R. K. Tektronix, "UMTS Signaling - UMTS Interfaces, Protocols, Message Flows, and Procedures Analyzed and Explained", Inc., Germany and Torsten Ruedebusch - Tektronix, Inc., Germany, Copyright © Tektronix Berlin GmbH & Co KG. Company confidential, 2º Edição, 2007.

[5] R. W. Yeung, "Information Theory and Network Coding", Springer, Hong Kong, 2008.

[6] H. Welte, "OpenBSC Network-Side GSM Stack. A Tool for GSM Protocol Level Security Analysis", SSTIC 2010, Rennes, França, Junho 2010.

[7] J. Networks. "MobileNext Control Gateway Next-Generation –SGSN/MME Solution for 2G/3G and LTE Mobile Networks", Juniper Networks, Inc, California, EUA, Fevereiro 2011.

[8] E. Brewer, N. Borisov, I. Goldberg, D. Wagner. (s.d.). *GSM Cloning*. Acedido em 18 de julho de 2011, em http://www.isaac.cs.berkeley.edu/isaac/gsm.html

[9] T. Masson, "Wireless Technology Seminar: Third Generation (3G) Basics CDMA-2000 & 3GPP W-CDMA", UK Regional Specialist, Agilent Technologies, Dezembro 2000.

[10] B. Turner, M. Orange, "3G Tutorial", Fall VON 2002, NMS Communications, 2002.

[11] A. Fares, Ph. D., "UTRAN Signaling and Protocols", EUA, 2008.