Emulação de Rede LTE Usando OpenAirInterface e Análise de Tráfego Via Protocolo de Rede

Virgínia Tavares, Lucas Nóvoa, Gabriel Couto, Aldebaro Klautau e Francisco Muller

***Resumo*— Este artigo apresenta a construção de uma rede 4G e sua análise de tráfego via protocolo de rede, com foco no uso de *softwares open-source* para a montagem dos principais módulos que constituem a arquitetura básica da tecnologia *Long Term Evolution* (LTE). A contribuição deste trabalho é demonstrar a emulação de uma rede LTE de baixo-custo *indoor* usando rádio definido por software e como resultado uma análise de tráfego da mesma via protocolos da camada de transporte para validar a emulação.**

***Palavras-Chave*— LTE, OpenAirInterface, Análise de Tráfego, Rádio Definido por Software.**

***Abstract*— This article presents the construction of a 4G network and its traffic analysis via network protocols. The main focus is the usage of open-source software to deploy the basic architecture of *Long Term Evolution* (LTE) technology main modules. The contribution of this work is to show an emulation of an indoor low-cost LTE network using software defined radio and as result a traffic analysis via transport layer protocols to validate the emulation.**

***Keywords*— LTE, OpenAirInterface, Traffic Analysis, Software Defined Radio.**

I. Introdução

De acordo com [1], o acelerado crescimento dos dados móveis criou desafios sem precedentes para as provedoras de serviços de telefonia. Para acompanhar o crescimento da rede móvel, tecnologias como o LTE estão evoluindo e moldando a base da quinta geração de rede móvel (5G).

A arquitetura LTE é constituída pelo *User Equipment* (UE), *Evolved Packet Core* (EPC) e *Evolved UMTS Terrestrial Radio Access Network* (E-UTRAN). O EPC é responsável por lidar com o tráfego de dados de forma eficiente do ponto de vista de desempenho e custos comparado a tecnologias anteriores como o *Universal Mobile Telecommunication System* (UMTS) e *Global System for Mobile Communications* (GSM). O EPC tem como entidades o *Home Subscriber Server* (HSS), *Mobility Management Entity* (MME), *Policy and Charging Rules* (PCRF), o *Packet Data Network Gateway* (PGW) e o *Serving Gateway* (SGW). O E-UTRAN, consiste em estações rádio-bases (eNodeB) interligadas pela interface X2, é encarregado pelas comunicações de rádio entre o UE e o EPC [2].

Para desenvolver novos padrões de telefonia e tráfego de dados, grandes esforços estão sendo conduzidos mundialmente. Nesse contexto, o presente artigo busca a emulação de uma rede LTE através de *software* de código aberto (mais precisamente *OpenAirInterface* - OAI) e *hardware* de baixo custo. E também uma análise da rede realizada através do analisador de pacotes *Wireshark* a fim de confirmar o funcionamento correto dos módulos criados. As próximas seções deste artigo estão organizadas da seguinte maneira: na Seção II são expostas as ferramentas utilizadas para emulação da rede. A Seção III descreve a construção do ambiente utilizado, enquanto na Seção IV são explorados os dados obtidos via *Wireshark*. Por fim, a Seção V traz as conclusões finais do artigo.

Os autores participam do LASSE – Grupo de Pesquisa em 5G & IoT, Universidade Federal do Pará (UFPA), Belém-PA, E-mails: {virginia.tavares, lucas.pinto, gabriel.couto}@itec.ufpa.br, {aldebaro, fmuller}@ufpa.br

II. Ferramentas utilizadas

O OAI foi utilizado como principal ferramenta por ser capaz construir e simular os módulos eNodeB e EPC. Também por fornecer *open-source hardware* e soluções de *software* para experimentação de redes de rádio. O uso do OAI permite uma monitorização completa, incluindo os dispositivos móveis conectados, em tempo real [3]. Assim como [4] foi utilizado o *PySim*, versão 2.3.0, *software* disponibilizado pelo projeto Osmocom da Sysmocom, para a programação dos SIMcards *sysmoUSIM-SJS1*.

O *Wireshark*, utilizada versão 2.6.8, é um programa analisador de protocolos de rede que permite capturar pacotes e analisar a estrutura de pacotes entre os módulos LTE. Ele possui destaque nesse trabalho pois permite solução de problemas de rede, análise, comunicação e desenvolvimento de protocolos de software. Esses dados podem ser utilizados, por exemplo, na análise de Qualidade de Serviço (QoS - *Quality of Service*) [5].

III. Ambiente de emulação

Inicialmente, o módulo do EPC foi montado através do OAI em uma máquina virtual hospedada em um x86_64 de processador Intel® Core i5-7500 CPU @ 3.40GHz. A máquina hospedeira possuía o Ubuntu 16.04 LTS como sistema operacional (SO) e "4.8.0-52-lowlatency"como Kernel Linux. Enquanto, a máquina virtual possuía Ubuntu 16.04 LTS e Kernel Linux 4.7.7.

Seguindo os tutoriais oficiais [6], houve primeiramente a configuração dos arquivos referentes ao HSS, MME, SGW e PGW (estes dois últimos são reunidos no chamado SPG-W). Assim, tem-se o EPC+HSS construído. O OAI suporta funções de divisão IF4p5 para *Remote Radio Unit* (RRU) e *Radio Cloud Center* (RCC) no modo eNodeB. A partir disso houve a configuração dos arquivos de RRU e RCC para configurar o eNodeB na hospedeira, onde conectou-se uma USRP B210 [7]. A Figura 1 ilustra a arquitetura de módulos utilizada.

Através de um leitor padrão de SIMCards houve o registro de dados compatíveis com o HSS em nos SIMcards através do

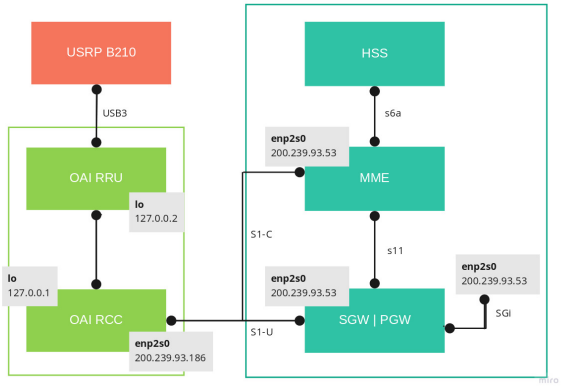
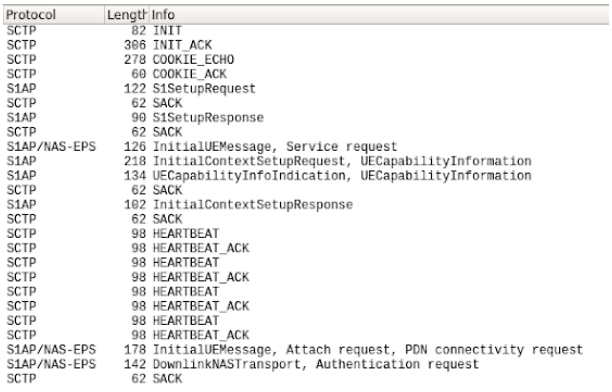


Fig. 1. Arquitetura de módulos, com detalhes de IP e interfaces utilizadas.



Protocol	Length	Info
SCTP	82	INIT
SCTP	306	INIT_ACK
SCTP	278	COOKIE_ECHO
SCTP	60	COOKIE_ACK
S1AP	122	S1SetupRequest
SCTP	62	SACK
S1AP	90	S1SetupResponse
SCTP	62	SACK
S1AP/NAS-EPS	126	InitialUEMessage, Service request
S1AP	218	InitialContextSetupRequest, UECapabilityInformation
S1AP	134	UECapabilityInfoIndication, UECapabilityInformation
SCTP	62	SACK
S1AP	102	InitialContextSetupResponse
SCTP	62	SACK
SCTP	98	HEARTBEAT
SCTP	98	HEARTBEAT_ACK
SCTP	98	HEARTBEAT
SCTP	98	HEARTBEAT_ACK
SCTP	98	HEARTBEAT
SCTP	98	HEARTBEAT_ACK
SCTP	98	HEARTBEAT
SCTP	98	HEARTBEAT_ACK
S1AP/NAS-EPS	178	InitialUEMessage, Attach request, PDN connectivity request
S1AP/NAS-EPS	142	DownlinkNASTransport, Authentication request
SCTP	62	SACK

Fig. 3. Colunas protocolo e informação dos pacotes da categoria “udp.dstport == 2123 || sctp”.

Pysim, em seguida um dos SIMs foi posto em um UE, Modem USB *Huawei E3272* [8], configurado com uma APN também compatível ao HSS, assim possibilitando a entrada do UE na rede.

IV. Resultados obtidos pelo Wireshark

No *Wireshark*, instalado junto ao eNodeB, foi utilizado o filtro “udp.dstport == 2123 || sctp”. Este filtro dentro da rede procura pelos pacotes usando como referência a porta UDP de destino 2123 ou relacionados ao SCTP (*Stream Control Transmission Protocol*). Verifica-se diretamente a porta UDP de destino 2123, pois é a porta vinculada à interface S11, usada para sinalização entre o MME e o S-GW através do protocolo GTPv2-C (usado para verificar a QoS de uma sessão específica) [9].

Como retorno ao filtro se obteve todo o tráfego na categoria desejada, todas as unidades exibidas tinham como característica ter como destino o IP (*Internet Protocol*) do EPC e origem o IP do eNodeB, ou o contrário.

Para exemplificar, foi selecionado um frame específico dentro da categoria. A primeira linha mostra o resumo e as linhas seguintes mostram a camada de enlace de dados, a camada de rede, a camada de transporte e, finalmente, os dados reais contidos, como pode ser visto na Figura 2.

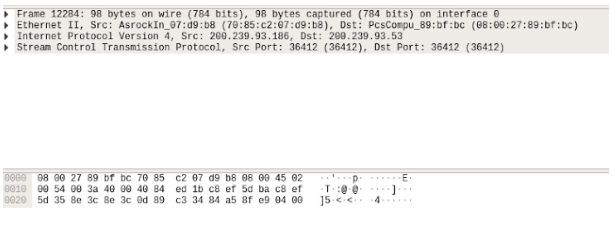


Fig. 2. Detalhes frame dos packages UDP.

Além disso, a filtragem mostrou também que o uso do protocolo S1AP, que fornece o serviço de sinalização entre o eNodeB e o EPC, é requisitado de maneira efetiva. A conexão feita entre eles utiliza do protocolo SCTP que opera sobre o IP, a Figura 3 mostra a conexão com base nesses parâmetros, onde cada mensagem trocada têm uma confirmação SACK (*Selective Acknowledgement*).

V. Conclusões

Neste artigo foi discutida a construção e emulação de uma rede LTE *indoor* completa de baixo custo utilizando rádio definido por software através do OAI e programação de SIMs. Também foi analisado o cenário de fluxo de pacotes para porta UDP de destino 2123 ou de protocolo SCTP via *Wireshark* durante a conexão de um UE à rede, ou seja, acompanhou-se a comunicação do MME e do S-GW pelo ponto de vista de pacotes. Com isto, foi possível confirmar o funcionamento correto dos módulos principais do LTE, conexão do usuário à rede e acesso à Internet pelo mesmo.

VI. Agradecimentos

Este trabalho foi financiado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), número do processo 2015/24508-9, com apoio da PROEX/UFPA.

Referências

[1] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, “Millimeter wave mobile communications for 5g cellular: It will work!,” *IEEE Access*, vol. 1, pp. 335–349, 2013.

[2] A. Toskala and T. Lunttila, *LTE for UMTS: Evolution to LTE-Advanced, Second Edition*, pp. 67 – 82. 03 2009.

[3] C. Bonnet, D. Camara, R. Ghaddab, A. Hayar, L. Iacobelli, F. Kaltenberger, R. Knopp, B. Mercier, N. Nikaein, D. Nussbaum, E. Yilmaz, and B. Zayen, “Openairinterface and agile spectrum access,” pp. 662 – 663, 06 2011.

[4] E. M. Sánchez, “Study of RAN slicing in a real SDN-NFV platform,” M.S. thesis, Universitat Politècnica de Catalunya, Barcelona, 2018.

[5] S. Wang, D. Xu, and S. Yan, “Analysis and application of wireshark in TCP/IP protocol teaching,” in *2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)*, vol. 2, pp. 269–272, April 2010.

[6] O. Eurecom, “OpenAirUsage,” 2016. [Online]. Disponível em: `https://gitlab.eurecom.fr/oai/openairinterface5g/wikis/OpenAirUsage`. [Acessado em 20 de Abril, 2019].

[7] ETTUS, “USRP B210 (board only).” [Online]. Disponível em: `http://www.ettus.com/all-products/UB210-KIT/`. [Acessado em 16 de Abril, 2019].

[8] VIVO, “Huawei E3272.” [Online]. Disponível em: `https://configuraraparelhos.vivo.com.br/?pagina=device/modems-usb/huawei-e3272/`. [Acessado em 25 de Abril, 2019].

[9] B. Dhindsa, A. Kaur, and S. Ahuja, “LTE interfaces and protocols,” in *2015 International Conference on Advances in Computer Engineering and Applications*, pp. 870–874, March 2015.