Simulation of LTE Signaling

[1]Florin SANDU, [2]Szilárd CSEREY, [3]Eugen MILE-CIOBANU
[1]"Transilvania" University of Brasov Bd Eroilor nr. 29A RO-500036 Brasov sandu@unitbv.ro ,
[2,3]SIEMENS Program and System EngineeringBd Mihai Kogalniceanu nr.21 bl.C6 RO-500090 Brasov [1]sandu@unitbv.ro, [2]szilard.cserey@siemens.com, [3] eugen.mile@siemens.com

***Abstract* — This article aims to present a simulation and emulation software that was developed to simulate the call flows of a LTE (Long Term Evolution) network. LTE is the latest Mobile Telecommunications technology being currently in development and testing phase. The simulator can be used as an e-Learning software, for teaching the procedures and phases of different LTE scenarios. Call flows can be visualized trough the simulation panel, where signaling messages can be run continuously or step-by-step, for the purpose of detailed analysis. The simulator has the capability to generate real signaling packets, that are being sent to a virtual loopback adapter and captured / dissected using the Wireshark software. In this way a whole simulation environment is created that is very useful for teaching the latest mobile telecommunications technology, the LTE (Long Term Evolution) system.**

***Index Terms* — Communication Systems, Communication Standards, Communication System Signaling, Computer networks, Protocols**

I. INTRODUCTION

LTE (Long Term Evolution) is the latest Mobile Telecommunication technology, currently in development. In order to permit the teaching of the internals of this technology, we have developed a simulation and emulation software for the e-Learning community, which is able to simulate the call flows and signaling messages of the LTE network. Using this software a whole simulation environment can be created, the user is able to run the signaling call flows from the simulation panel (continuously, or step-by-step) and it can visualize in the same time the real signaling packets generated by the emulator, and captured / dissected using the Wireshark software.

II. DESIGN AND IMPLEMENTATION OF THE SIMULATOR

The software is built on top of the OMNeT++ 4.0 network simulator, and it is integrated into a simulation environment that relies on a set of third-party applications, like Wireshark, VirtNet virtual loopback adapter, Winpcap [5][7][8][9]. The application is divided in two parts, one is the simulator where the user has possibility to control the LTE call-flow simulation to run it simultaneously or step-by-step. The other part is the emulator that is being triggered by the simulator, each time a signaling message traverses the interface between two nodes, to generate the corresponding packet, and send it towards the VirtNet virtual loopback adapter. In order to view the content of these real packets, generated previously by the emulator, the user has to open the Wireshark application, and set it to monitor the virtual loopback adapter, to capture and dissect the generated packets. This is how the whole simulation environment is functioning, the simulation events are synchronously running together with the emulation events.

The LTE simulation is based on the signaling call flow between the following network nodes: UE (User Equipment), eNodeB, MME (Mobility Management Entity), HSS (Home Subscriber Server), S-GW (Serving Gateway), P-GW (Packet Data Network Gateway), these are the typical nodes in an LTE (Long Term Evolution) network [1]. For the simulation part of the software we have developed in C++ the behaviors of each network node, using the API of the OMNeT++ 4.0 network simulator, and for the emulation part we developed another C++ application that takes as input a text file, where it reads the hexadecimal content of each signaling packet and it sends them at specific times to the virtual loopback adapter. For the emulator we used the API (Application Programming Interface) from Winpcap, to send these packets to layer 2 of the operating system's protocol stack [8].

III. ARCHITECTURE OF THE LTE NETWORK

LTE is defined in the 3GPP R8 and R9 specification set, and the basic system architecture is divided into 4 major parts: the User Equipment (UE) domain, Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) domain, Evolved Packet Core Network (EPC), and the Services domain. The UE, E-UTRAN and EPC domains together form the Evolved Packet System (EPS), that is based on IP connectivity, all the services offered by this system is based on top of the IP transport [2][3]. UE domain contains the mobile users, with their User Equipment. The E-UTRAN domain is formed by a mesh of eNodeBs, these are sort of radio base stations distributed throughout the network coverage area. eNodeB is the termination point for all the radio protocols towards the UE, it forwards data between radio connection and IP connection towards the EPC (Evolved Packet Core) network [10].

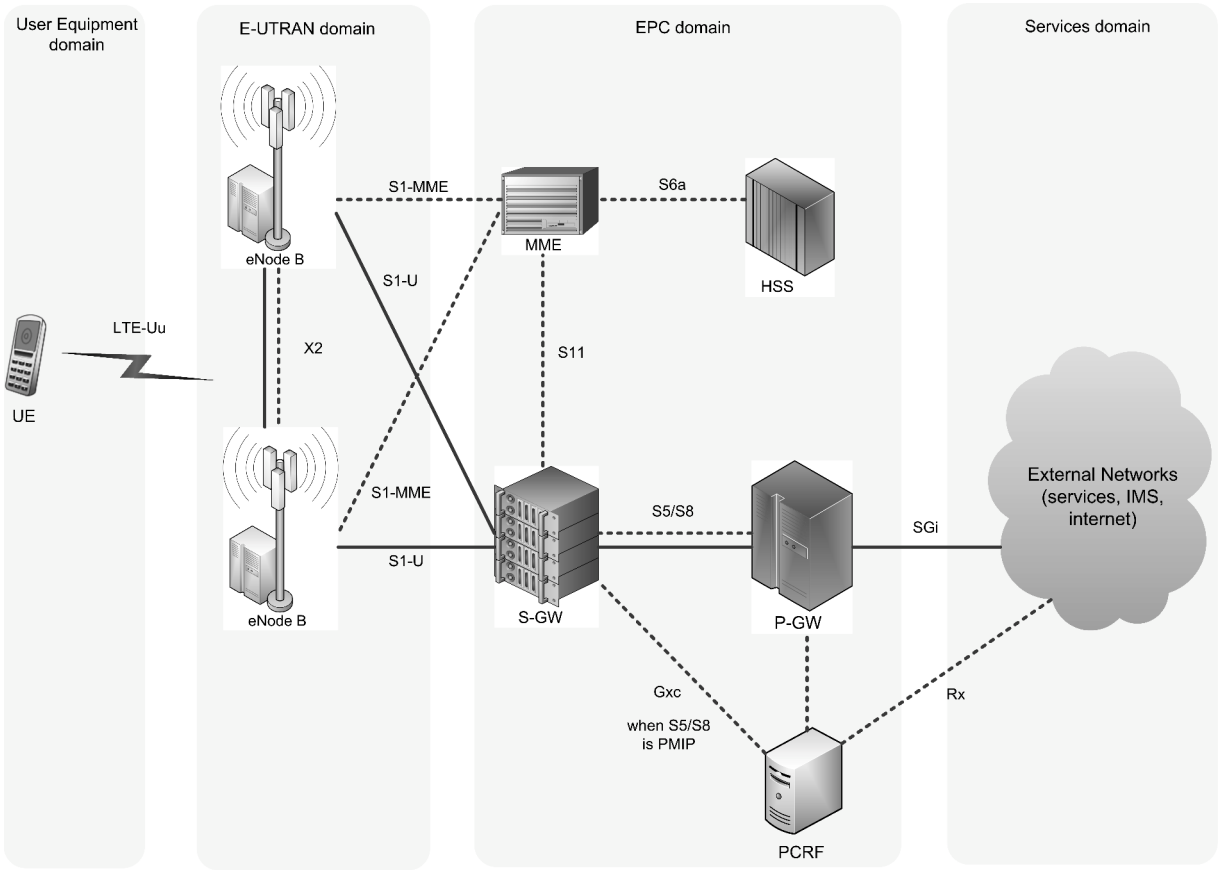


Fig. 1 Basic system architecture of the LTE (Long Term Evolution) network

The eNodeB has multiple functionalities, it performs coding/decoding of UP (User Plane) data, IP header compression/decompression, it is responsible for a number of CP (Control Plane) functionalities, RRM (Radio Resource Management), and MM (Mobility Management). When a User Equipment wants to attach to the network, it will first request connection to the network, and the eNodeB will route its request to the MME, that has been previously servicing that UE, or towards a new MME, if the other one is not available [4][6]. In LTE there is the concept of pooling, which means that the eNodeB may be connected to multiple MMEs, S-GWs, and other eNodeBs. The eNodeB will service multiple UEs under its coverage area. An UE can be connected to only one eNodeB at a time.

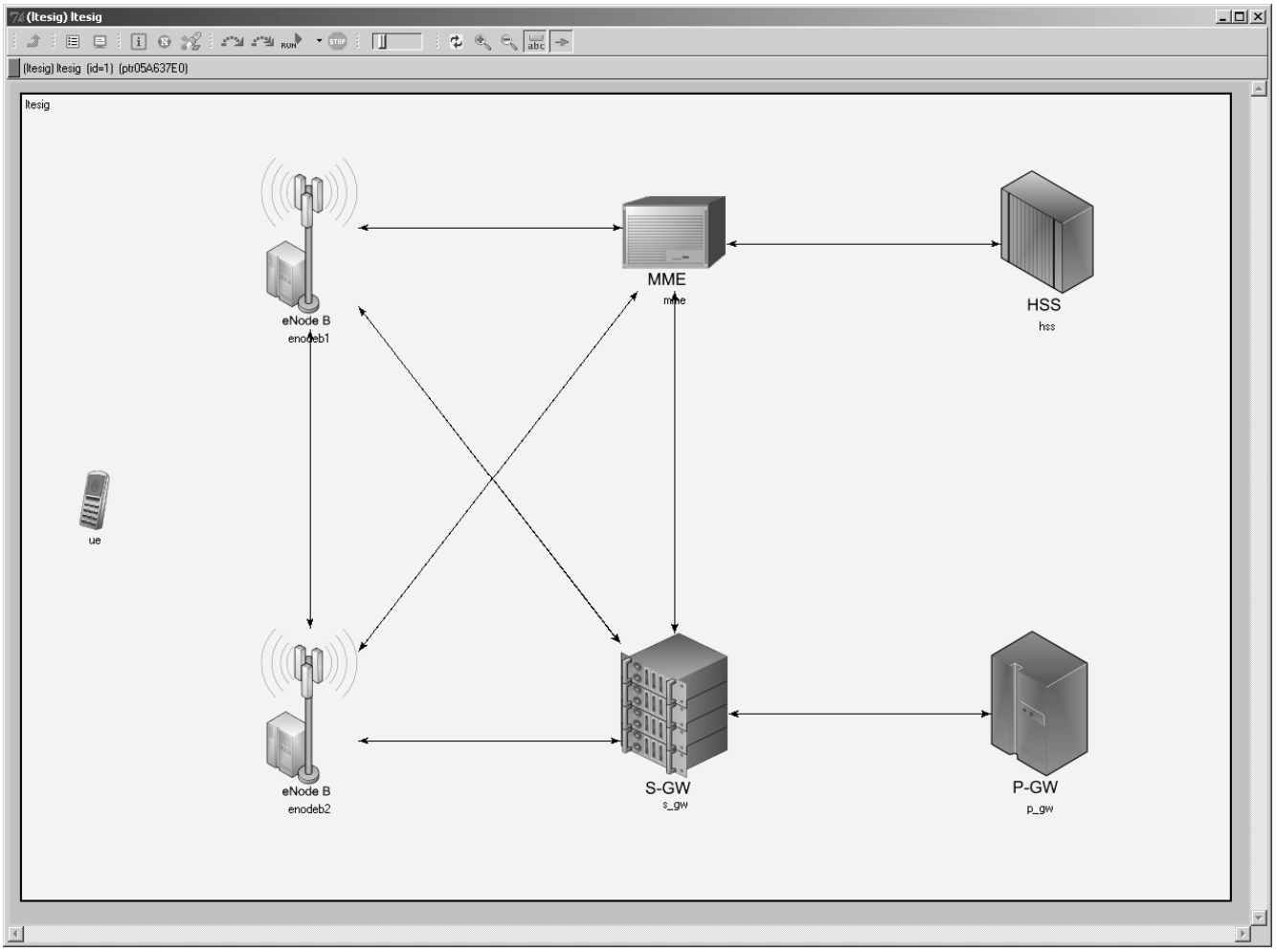
The MME (Mobility Management Entity) is the main control element in the EPC network. MME functionalities are: authentication and security, mobility management and management of subscription profile and service connectivity.

The main role of the S-GW (Serving Gateway) in the EPC network is the management and switching of the User Plane tunnel. User data is transmitted in IP packets which are encapsulated in GTP packets, this is called GTP tunneling. It controls the tunnels to eNodeBs, during mobility between eNodeBs, the S-GW will act as a local mobility anchor, it can switch the tunnel fom one eNodeB to another, and it is controlled by the MME. The S-GW relays all the user data between the eNodeB and P-GW, it can also monitor data in the tunnels, and collect them for accounting and user charging purposes, and it is also able to perform Lawful Interception [1].

The P-GW (Packet Data Network Gateway) is considered as the edge router between the Evolved Packet Core network and external packet data networks, it is the highest level of mobility anchor in the LTE system. It is the IP point of attachment for the UE, in networking this is called default gateway. The P-GW allocates the IP address to the UE, that enables it to communicate with other IP hosts in the external networks, or the internet. P-GW can also have DHCP functionality, or it can query external DHCP servers, to deliver the IP address to the UE. The P-GW maps the IP data flows into GTP tunnels, these tunnels are considered bearers.

The PCRF (Policy and Charging Resource Function) is the network element that is responsible for Policy and Charging Control, it performs decisions on how to handle the service in terms of QoS (Quality of Service), provides information to the PCEF (Policy and Charging Enforcement Function) located in the P-GW, or if necessary to BBERF (Binding and Event Reporting Function) located in the S-GW, to set up the appropriate bearers and policy.

The HSS (Home Subscription Server) stores all the user data, it is a kind of repository, it registers the location of the user in the visited network. Actually it is a database server, which stores the master copy of the subscriber profile, that contains information about the services which are applicable to the user. Service information could be the allowed PDN (Packet Data Network) connection, or the decision whether roaming to a particular visited network for a user is allowed or not.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.102.114.199	10.102.114.4	S1AP	id-S1Setup
2	0.400176	10.102.114.4	10.102.114.199	S1AP	id-S1Setup
3	0.826099	10.102.114.200	10.102.114.4	S1AP	id-S1Setup
4	1.227125	10.102.114.4	10.102.114.200	S1AP	id-S1Setup
5	1.630758	10.102.114.200	10.102.114.4	S1AP/NAS-EMM/NAS-ESM	id-initialUEMessage / Attach request / PDN connectivity request
6	1.913023	10.102.114.132	10.203.64.192	DIAMETER	cmd=3GPP-Authentication-InformationRequest(651) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=22 e2e=22
7	2.198557	10.203.64.192	10.102.114.132	DIAMETER	SACK cmd=3GPP-Authentication-InformationAnswer(651) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=22 e2e=22
8	2.482455	10.102.114.132	10.203.64.192	DIAMETER	SACK cmd=3GPP-Update-LocationRequest(650) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=23 e2e=23
9	2.759616	10.203.64.192	10.102.114.132	DIAMETER	cmd=3GPP-Update-LocationAnswer(650) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=23 e2e=23
10	3.045263	10.102.114.68	10.102.240.141	GTPv2	Create Session Request[Malformed Packet]
11	3.331168	::ffff:10.102.241.199	::ffff:10.102.241.200	MIPv6	Binding Update
12	3.619658	::ffff:10.102.241.200	::ffff:10.102.241.199	MIPv6	Binding Acknowledgement
13	3.911107	10.102.240.141	10.102.114.68	GTPv2	Create Session Response
14	4.211789	10.102.114.4	10.102.114.200	S1AP/NAS-EMM/NAS-ESM	id-InitialContextSetup / Attach accept / Activate default EPS bearer context request
15	4.502790	10.102.114.200	10.102.114.4	S1AP	SACK id-InitialContextSetup
16	4.815453	10.102.114.200	10.102.114.4	S1AP/NAS-EMM/NAS-ESM	id-uplinkNASTransport / Attach complete / Activate default EPS bearer context accept
17	5.102903	10.102.114.68	10.102.240.141	GTPv2	Modify Bearer Request
18	5.411214	::ffff:10.102.241.199	::ffff:10.102.241.200	MIPv6	Binding Update
19	5.696888	::ffff:10.102.241.200	::ffff:10.102.241.199	MIPv6	Binding Acknowledgement
20	5.982700	10.102.240.141	10.102.114.68	GTPv2	Modify Bearer Response
21	6.284032	10.102.240.141	10.102.114.68	GTPv2	Echo Request
22	6.572790	10.102.114.68	10.102.240.141	GTPv2	Echo Response
23	6.908121	10.102.114.199	10.102.114.200	X2AP	id-handoverPreparation
24	7.214001	10.102.114.200	10.102.114.199	X2AP	SACK id-handoverPreparation
25	7.511786	10.102.114.199	10.102.114.200	X2AP	SACK id-snStatusTransfer
26	7.795983	10.102.114.199	10.102.114.4	S1AP	id-PathSwitchRequest
27	8.081748	10.102.114.68	10.102.240.141	GTPv2	Modify Bearer Request
28	8.395192	::ffff:10.102.241.199	::ffff:10.102.241.200	MIPv6	Binding Update
29	8.680803	::ffff:10.102.241.200	::ffff:10.102.241.199	MIPv6	Binding Acknowledgement
30	8.966985	10.102.240.141	10.102.114.68	GTPv2	Modify Bearer Response
31	9.264223	10.102.114.4	10.102.114.199	S1AP	id-PathSwitchRequest
32	9.563372	10.102.114.200	10.102.114.199	X2AP	id-UEContextRelease
33	9.905459	10.102.240.141	10.102.114.68	GTPv2	Echo Request
34	10.195268	10.102.114.68	10.102.240.141	GTPv2	Echo Response
35	10.511131	10.102.114.199	10.102.114.4	S1AP/NAS-EMM	id-uplinkNASTransport / Tracking area update request
36	10.816215	10.102.114.4	10.102.114.199	S1AP/NAS-EMM	id-downlinkNASTransport / Tracking area update accept
37	11.124569	10.102.114.199	10.102.114.4	S1AP/NAS-EMM	id-uplinkNASTransport / Detach request
38	11.415692	10.102.114.68	10.102.240.141	GTPv2	Delete Session Request
39	11.703558	::ffff:10.102.241.199	::ffff:10.102.241.200	MIPv6	Binding Update
40	11.991959	::ffff:10.102.241.200	::ffff:10.102.241.199	MIPv6	Binding Acknowledgement
41	12.279337	10.102.240.141	10.102.114.68	GTPv2	Delete Session Response
42	12.576820	10.102.114.4	10.102.114.199	S1AP/NAS-EMM	id-downlinkNASTransport / Detach accept
43	12.891257	10.102.114.4	10.102.114.199	S1AP	SACK id-UEContextRelease
44	13.182977	10.102.114.199	10.102.114.4	S1AP	id-UEContextRelease

Fig. 2 The picture above shows the simulation panel of the LTE simulator. The picture below displays the signaling messages generated by the emulation part of the LTE simulator, which were captured and dissected (analyzed, interpreted) by the Wireshark software

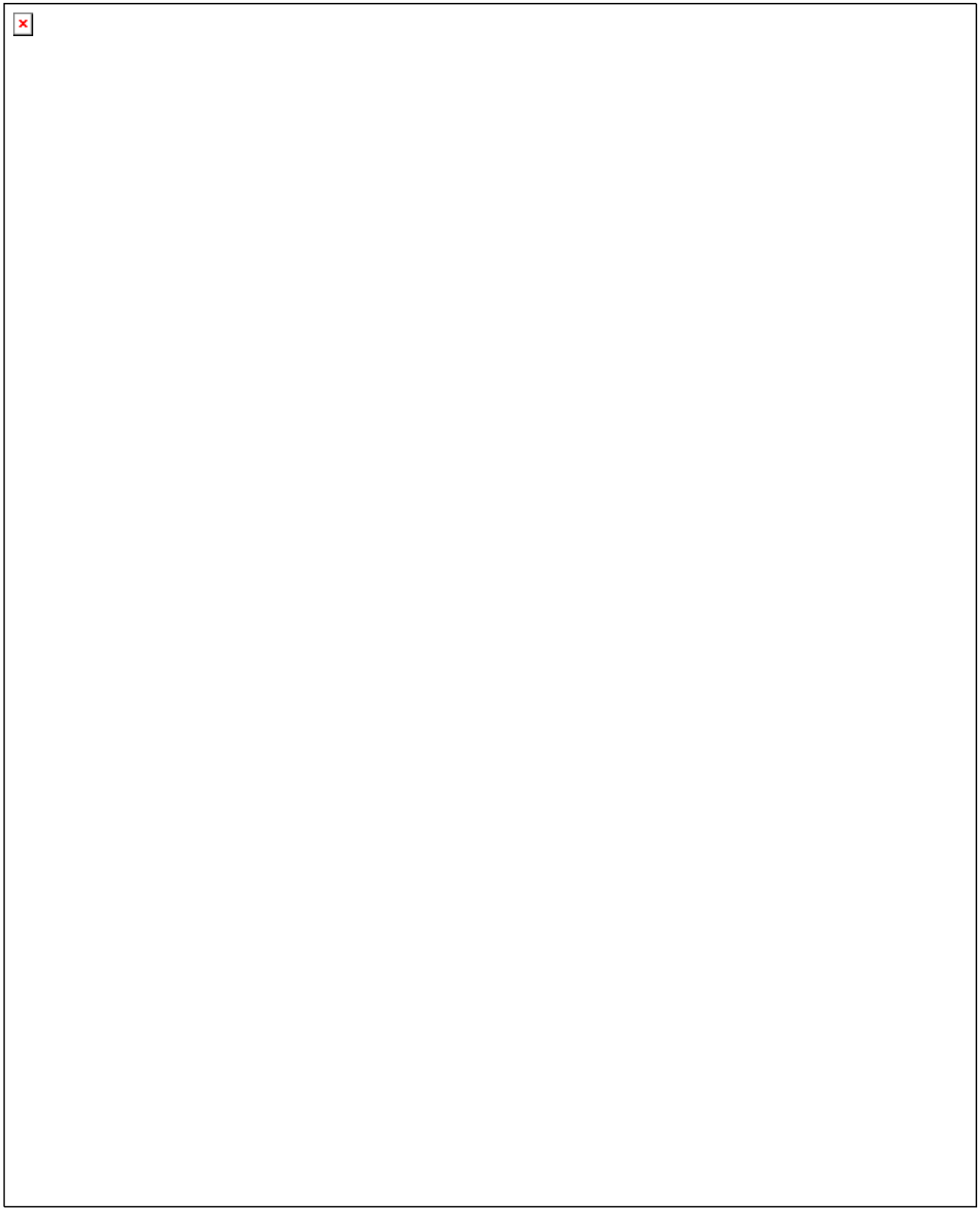


Fig. 3 This picture illustrates the LTE call flow signaling that is performed by the LTE simulator

The Services domain can include various sub-systems with several types of services like: IMS (IP Multimedia Subs-system) based operator services (which uses the SIP – Session Initiation Protocol, for signaling), non-IMS based services like video streaming service, and other services not provided by the mobile network operator.

IV ANALYSIS OF THE CALL FLOW GENERATED BY THE LTE SIMULATOR

The simulation involves the following network elements from the LTE system: two eNodeBs, MME, HSS, S-GW and P-GW. The call flow generated by the LTE simulator contains several procedures or scenarios like, the UE performing an LTE initial attach / default bearer establishment, UE handover between two eNodeBs, and UE detach from the network. Fig. 3 shows a detailed illustration of the call flow that is being simulated by this application. The first 4 messages represent the call flow of the Setup Procedure.

In our call-flow, first eNodeB 2 initiates a Setup Procedure with the MME (Mobility Management Entity) after that eNodeB 1 does the same thing. The S1 Setup Procedure is used to exchange the application-level data that is needed for the eNodeB and MME to interoperate correctly on the S1 interface The procedure is initiated by eNodeB and information like eNodeB ID, Tracking Area Code, MME code are exchanged during the S1 Setup Procedure. During this procedure some basic application-level configuration data for system operation is being exchanged. A basic application data, that can be configured via the S1 SETUP procedure is the tracking area identities, these are very important for system operation, because tracking areas represent the zones on which UEs are paged. The mapping of the tracking areas to eNodeBs must remain consistent between the E-UTRAN and EPC. Tracking area identities are sent within the S1 SETUP REQUEST message to all the relevant MME nodes. After the S1 SETUP procedure has been completed, the S1 interface is in operation.

The S1 SETUP procedure contains 2 messages: S1 Setup Request and S1 Setup Response, these are used by the eNodeB to initiate an S1 interface towards an MME node.

The next message is an "Attach Request / PDN connectivity request" message, which belongs to the LTE Attach procedure. This procedure is used by the UE (User Equipment) to attach to an EPC (Evolved Packet Core) for accessing the packet services of the EPS (Evolved Packet System). Using the LTE Attach procedure, a context is established between the UE and the MME and a default bearer is created between the UE and the P-GW (Packet Data Network Gateway).

After the "Attach Request" message was sent by the UE and forwarded trough the eNodeB towards MME, this MME will send an "Athentication information request" to the HSS (Home Subscription Server), which will respond back with an "Authentication information answer" message. During the attach procedure the MME has to check if the UE (User Equipment) that tries to access the EPC network is known in the HSS. The MME sends the "Authentication Information Request" message to request from the HSS the authentication vector for the subscriber. The HSS verifies whether the IMSI (International Mobile Subscriber Identity) of the subscriber is known and will send the E-UTRAN authentication vector to the MME using the "Authentication information answer" message. When a UE (User Equipment) attaches to the network, a mutual authentication of the UE and the network is performed between the UE and the MME/HSS. This authentication function establishes the security keys which are used for the encryption of the bearers.

When a UE registers to the network for the first time, the MME initiates the authentication, by performing the following activities: it finds out the UE's permanent identity either from the previously visited network or from the UE itself. Then the MME requests from the HSS (Home Subscription Server) that resides in the UE's home network, the authentication vectors which contain the authentication challenge – response parameter pairs, then the MME sends the challenge parameter to the UE, and compares the response received from the UE with the one received from the home network. This procedure is used to authenticate the UE to assure that the UE is the one who it claims to be. The MME calculates the UE's ciphering and integrity protection keys from the master key received in the authentication vector from the home network. These functions are used to protect the communication from eavesdropping and from alteration by unauthorized third parties. In order to protect the User Equipment's privacy, the MME also allocates each UE a temporary identity called the Globally Unique Temporary Identity (GUTI), so that the UE's permanent identity, the IMSI (International Mobile Subscriber Identity), does not need to be sended over the radio interface. The GUTI may be re-allocated periodically to prevent unauthorized tracking of the UE.

After this step the "Update Location Request" and "Update Location Answer" messages are exchanged between the MME and HSS. This is the Update Location Procedure which is used between the MME and HSS to inform the HSS about the identity of the MME currently serving the user and to update the MME with user subscription data. During this procedure the following information is provided by the HSS: the Access Point Name, P-GW address and the Quality of Service parameters for default bearer establishment. The MME verifies whether it holds the subscription data for the UE identified by the GUTI, if no subscription data is found in the MME, this will send an "Update Location Request" message to the HSS, which will respond with an "Update Location Answer" message. This response contains the Subscription Data that contains the subscription contexts. Each PDN (Packet Data Network) subscription context contains an "EPS subscribed QoS profile" and the subscribed APN-AMBR (Access Point Name – Aggregate Maximum Bit Rate). The new MME validates the UE's presence in the new Tracking Area and constructs a context for the UE [1][4][6].

Next the "Create Session Request" message is sent on the S11 interface by the MME to the S-GW as part of the E-UTRAN Initial Attach procedure. The S-GW (Serving Gateway) selection is based on the TAI (Tracking Area Identity) that is given by the eNodeB during the attach procedure. The TAI (Tracking Area Identity) is used to

identify the tracking areas, this identity is constructed from the MCC (Mobile Country Code), MNC (Mobile Network Code) and TAC (Tracking Area Code). Thus the S-GW (Serving Gateway) selection is based on the subscriber location but not on the subscriber identity itself. On the other hand the P-GW selection is based on the Access Point Name (APN) that is given by the HSS during the Attach procedure, so the P-GW (Packet Data Network Gateway) is based on the subscriber identity only.

During the Attach procedure the UE sent a PDN Connectivity request message to the MME in order to inform the network that it needs a bearer to transmit data.

Now the MME creates a GTP (GPRS Tunneling Protocol) message called "Create Session Request" and it forwards to the S-GW (Serving Gateway). At this time the MME assigns an EPS bearer ID to the bearer. The S-GW sends a "Proxy Binding Update" message to the P-GW. The "Proxy Binding Update" and "Proxy Binding Acknowledgement" messages are exchanged between the S-GW and P-GW trough the S5/S8 interface. Here a Binding procedure is initated by the S-GW towards the P-GW in order to create a new PDN (Packet Data Network) connection for the UE that attaches to the EPC (Evolved Packet Core) network for the first time. The establishment of binding achieves the following results: PDN selection, the P-GW selects the PDN (Packet Data Network) based on the APN (Access Point Name) contained in the PBU (Proxy Binding Update); IPv4 home address assignment, the P-GW assigns to the UE's PDN connection an IPv4 home address valid in the selected PDN; GRE (Generic Routing Encapsulation) tunnel establishment, a GRE tunnel is established between the S-GW and P-GW with the assigned GRE keys to carry the uplink and downlink traffic that the UE sends and receives on the PDN connection.

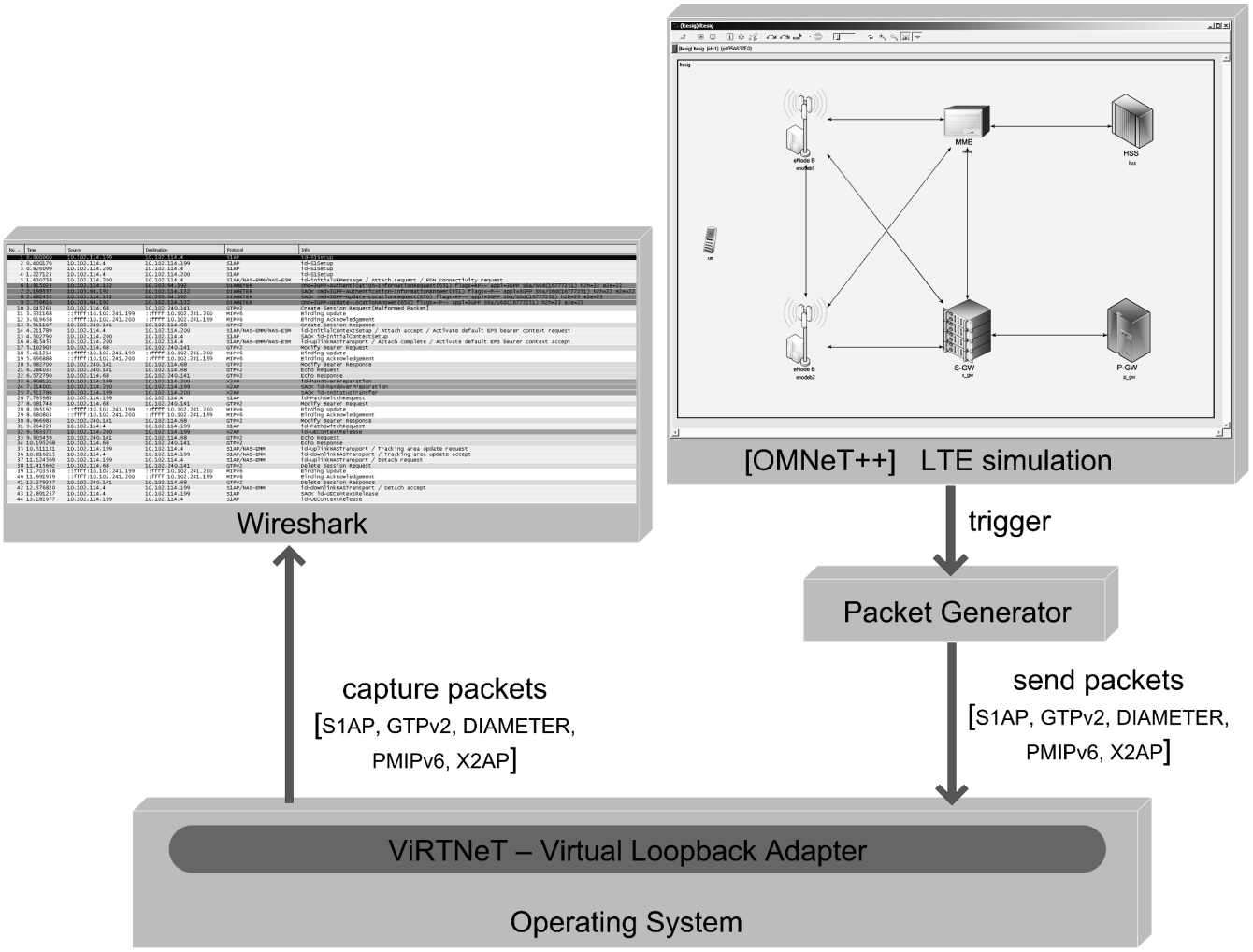


Fig. 4 System architecture diagram of the LTE simulation environment

The "Create Session Response" message is sent on the S11 interface by the S-GW to the MME as part of the E-UTRAN Initial Attach procedure. After that MME responds to the eNodeB with the "Initial context setup / Attach accept / Activate default EPS bearer context request message". The "Initial context setup request" message is sent by the MME to the eNodeB to request a setup of a UE context, in this message the Radio Access Bearer QoS (Quality of Service) parameters are sent to the eNodeB. The eNodeB in this way is informed about the S-GW–S1U–IP in order to establish the direct tunnel to S-GW for user data transfer. At this step the subscriber has been successfully authenticated and a default bearer has been created towards the PDN (Packet Data Network). "Attach accept" and "Activate default EPS bearer context request" messages are sent to the UE as response to "Attach request" and "PDN connectivity request" messages. The mobile UE (User Equipment) is informed about the APN (Access Point Name) used for default bearer creation and the assigned IP for default bearer. The "Initial Context Setup Response" message is sent by the eNodeB to confirm the setup of the UE context.

The eNodeB sends the transport layer address for data traffic in order that the MME can communicate it to the S-GW (Serving Gateway) over the S11 interface. When the default bearer is activated as part of the attach procedure, the UE sends the "Activate Default EPS Bearer Context Accept" message together with the "Attach Complete" message. The "Attach Complete Message" confirms that the mobile accepts the assigned GUTI (Globally Unique Temporary ID). The "Modify Bearer Request" and "Modify Bearer Response" messages are used to establish the data tunnel on the S1U interface between the eNodeB and S-GW. During this procedure the P-GW is contacted over the S5 interface (with a Proxy Binding Update message) and informed about the data tunnel. At this point the "LTE initial attach / Default Bearer Establishment" is finished and the mobile UE is able to transfer data to the PDN (Packet Data Network). The mobile UE (User Equipment) moves to the coverage area of the second eNodeB and a handover takes place. The communication between the eNodeBs is being done over the X2 interface using the X2AP protocol. The handover procedure implies the establishment of the RAB (Radio Access Bearer) at the new eNodeB, the switching of the data tunnel to the new eNodeB and the release the radio resource in the old eNodeB. The purpose of the Path Switch Request procedure is to request the switch of a downlink GTP tunnel towards a new GTP tunnel endpoint, in our case to the new eNodeB. The MME modifies the bearer towards the S-GW with the new tunnel information. A "Path switch request acknowledge" message is sent by the MME to inform the eNodeB that the path switch has been successfully completed in the EPC (Evolved Packet Core) network. After the successful handover the mobile UE performs a "Tracking Area Update" procedure in order to update the location information in the MME. At the end of the call flow, a Detach procedure is initiated by the UE by sending a "Detach Request" message. The "Detach Type" IE (Information Element) included in the message indicates whether detach is due to a "switch off" or not. The network and the UE will deactivate the EPS bearer contexts without peer-to-peer signaling between the UE and the MME and thus the UE is marked as inactive in the network for EPS (Evolved Packet System) services. The network now enters into the (EPS Mobility Management) EMM-Deregistered state. After the detach procedure the MME instructs the eNodeB, using the "UE Context Release Command" to release all radio resources. After radio resources are released at the eNodeB, this will respond with a "UE Context Release Complete" message [1][4][6][10].

V CONCLUSION

The LTE simulator presented in this article is deployed in the system configuration shown in Fig.4. This software application is a great tool that can be used by students or new employees who wish to learn the internals of the LTE signaling. In this way the students can get an overview of how mobile communication systems are being tested in real mobile network testbeds. An interesting aspect of the work we performed here, is that we integrated real network packets that were generated by real LTE equipments in mobile communication testbeds, we have reused these valuable information for the purpose of e-Learning. These signaling messages were captured during system/network integration tests in mobile communication testbeds, and they contain a lot of information about the behaviors of different network elements in an LTE system, as well as information about different scenarios, procedures and call-flows. All these information are only accessible in complex 3GPP specifications, but now using this tool the student can understand much better and have a greater overview about the whole signaling process in an LTE (Long Term Evolution) network.

REFERENCES

[1] H. Holma, A. Toskala, "LTE for UMTS – OFDMA and SC-FDMA Based Radio Access", John Wiley & Sons Ltd., ISBN 978-0-470-99401-6, 2009.

[2] S. Sesia, I. Toufik, M. Baker, "LTE – The UMTS Long Term Evolution From Theory to Practice", John Wiley & Sons Ltd, ISBN 978-0-470-69716-0, 2009.

[3] P. Lescuyer, T. Lucidarme, "The LTE and SAE Evolution of 3G UMTS", John Wiley & Sons Ltd., ISBN 978-0-470-05976-0

[4] S. Kumar Dornal, "LTE Whitepaper", wired-n-wireless.blogspot.com

[5] A. Varga, "OMNeT++ Discrete Event Simulation System, Version 4.0 User Manual", www.omnetpp.org.

[6] "Long Term Evolution (LTE) Attach (Moving from Old to New MME)" call-flow, "Long Term Evolution (LTE) Tracking Area Update (Moving from Old to New MME (Serving GW Change))" call-flow www.eventhelix.org.

[7] Virtual Network Adapter VirtNet 1.0 www.ntkernel.com/w&p.php?id=32.

[8] WinPcap: The Windows Packet Capture Library www.winpcap.org

[9] Ulf Lamping: Wireshark Developer's Guide www.wireshark.org

[10] 3GPP TS 23.401 version 9.3.0 Release 9 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access" www.3gpp.org